ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Topic 1, Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 ES subscription.

Existing Environment

Requirement

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	None
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Planned Changes

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automaticity.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must NOT use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- Configure Windows Information Protection (W1P) for the Windows 10 devices.

Question: 1

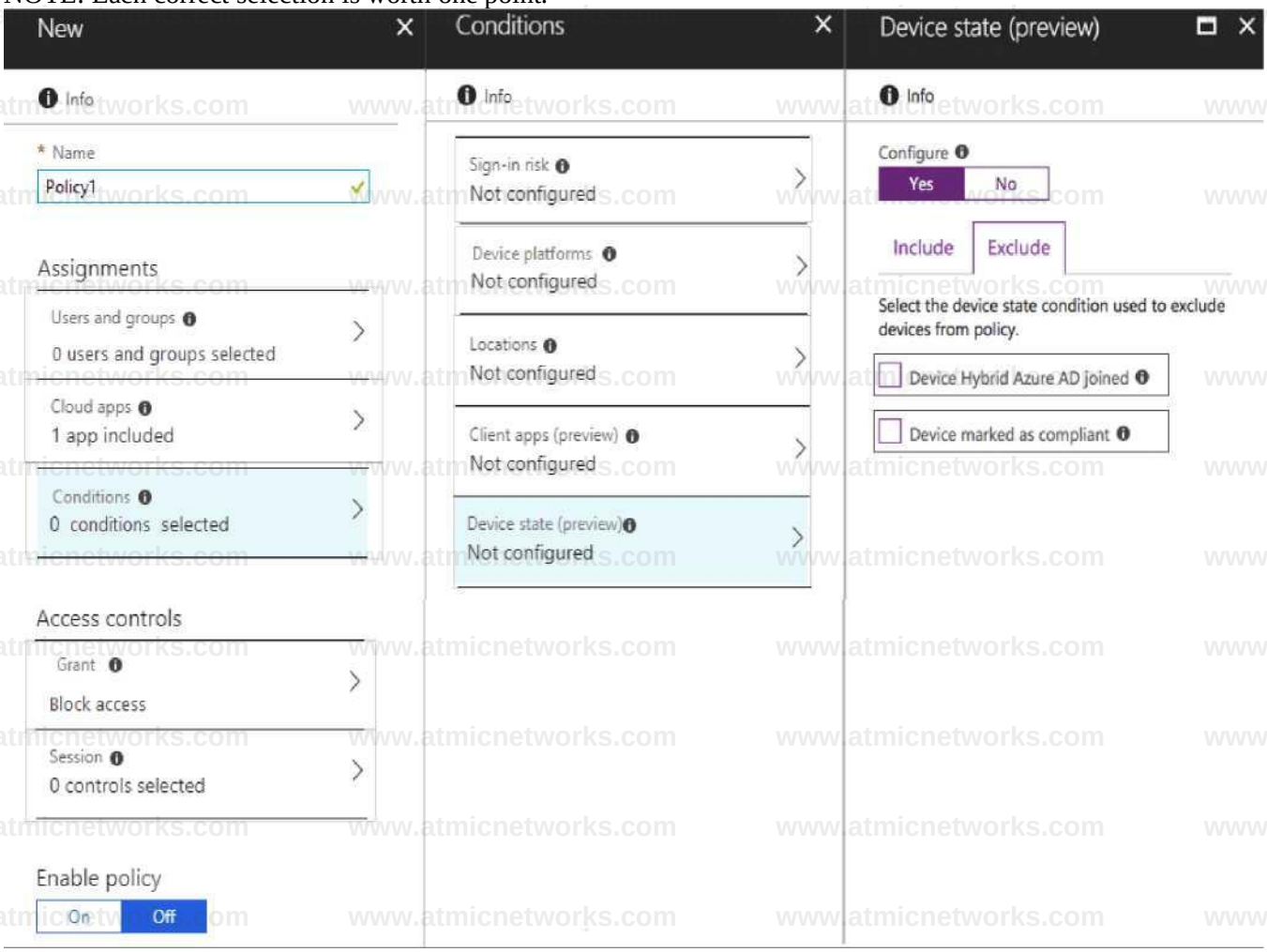
HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements.

You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

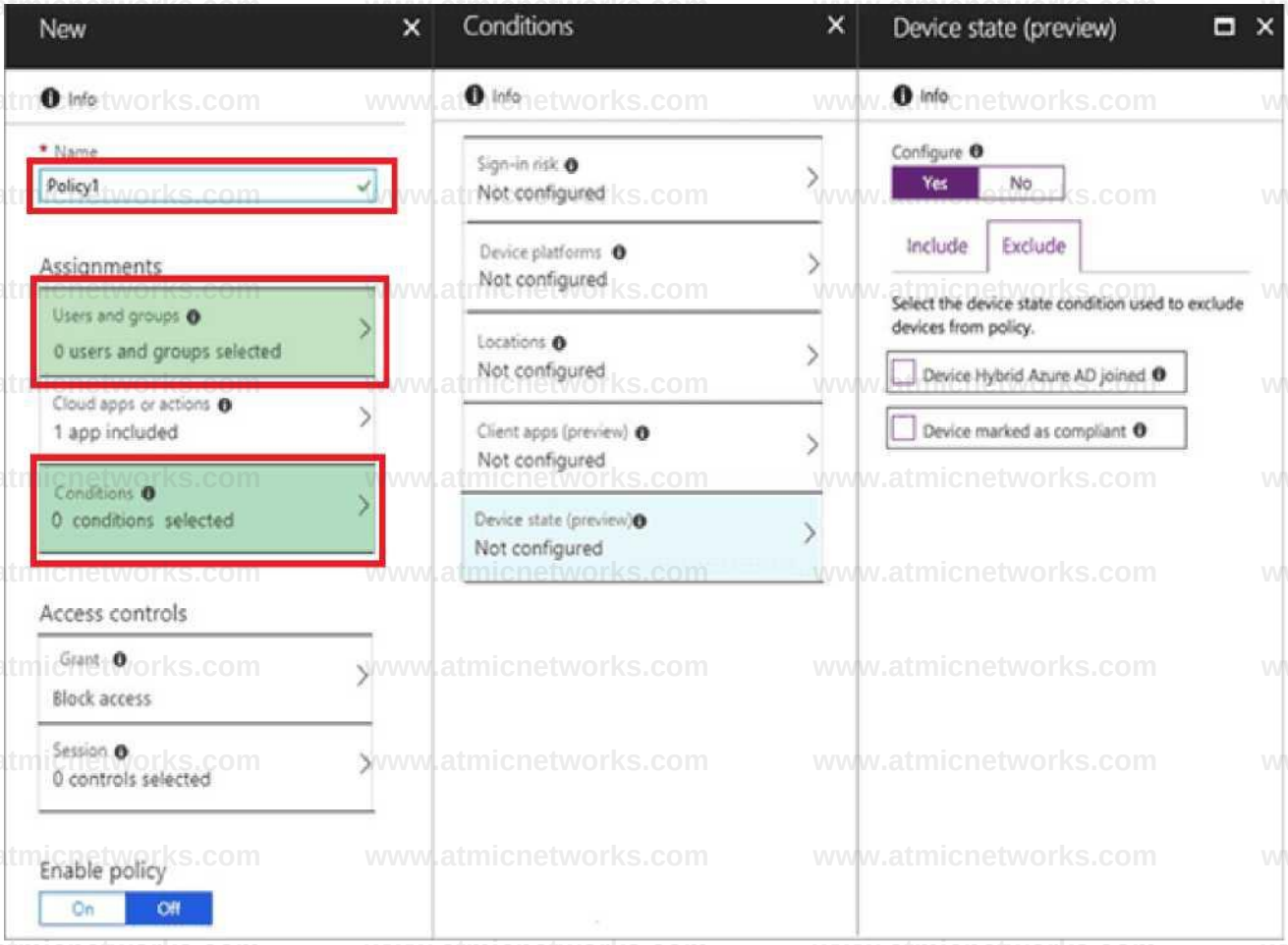
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Suggested Answer:



Reference:https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

Question: 2

On which server should you install the Azure ATP sensor?

A. Server 1

B. Server 2

C. Server 3

D. Server 4

E. Server 5

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer

is correct. BTW, ATP now known as Defender for Identity.

Question: 3

You need to meet the compliance requirements for the Windows 10 devices.

What should you create from the Intune admin center?

A. a device compliance policy
B. a device configuration profile
C. an application policy
D. an app configuration policy

Answer: C

Explanation:

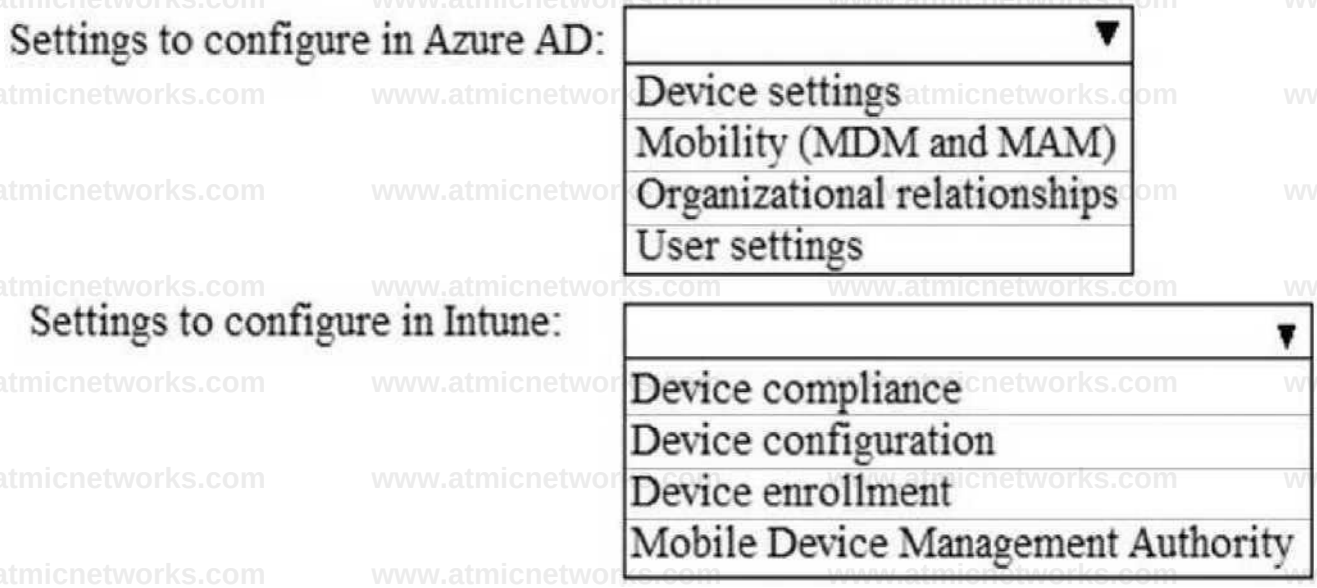
Question: 4

HOTSPOT

You need to meet the Intune requirements for the Windows 10 devices.

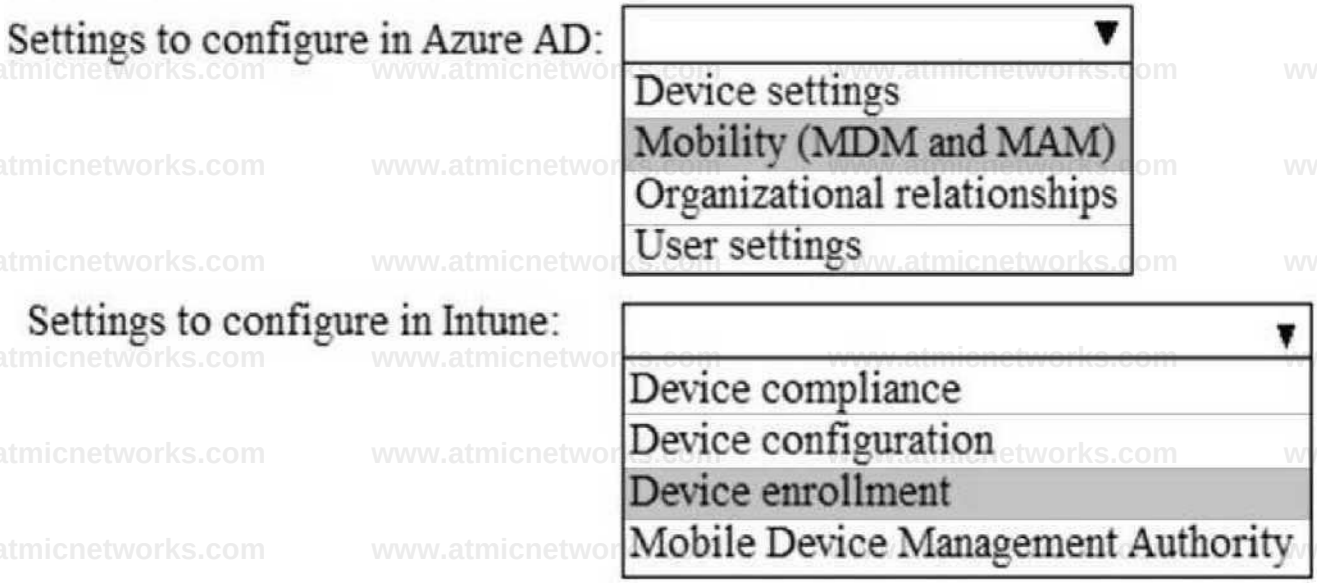
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/intune/windows-enroll

Question: 5

HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To

answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Explanation:

Answer:

https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date

Reference:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature- updates-windows-10

Question: 6

You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator rote.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
C. From the Intune admin center, add User1 as a device enrollment manager.
D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device- enrollment-manager

Question: 7

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

A. 1
B. 4
C. 7
D. 31

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device- enrollment-manager

Question: 8

You need to create the Microsoft Store for Business. Which user can create the store?

A. User2
B. User3
C. User4
D. User5

Answer: C

Explanation:

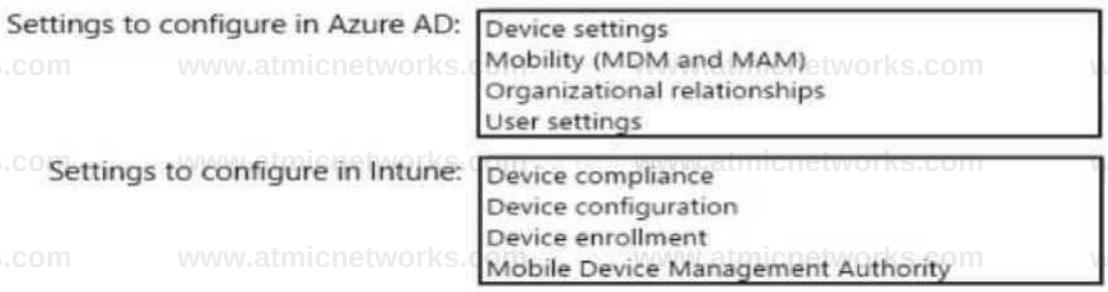
Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for- business

Question: 9

HOTSPOT

You need to meet the technical requirements and planned changes for Intune. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Reference:

https://docs.microsoft.com/en-us/intune/windows-enroll

Question: 10

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 network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure a pilot for co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.

Does this meet the goal?

A. Yes

B. NO

Answer: A

Explanation:

Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

Question: 11

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 network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure a pilot for co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2. Client agent setting for hybrid Azure AD-join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager

https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client

Question: 12

On which server should you use the Defender for identity sensor?

A. Server1
B. Server2
C. Server3
D. Server4
E. Servers5

Answer: A

Explanation:

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

Topic 2, A. Datum

Case Study:

Overview

Existing Environment

This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Current Infrastructure

A. Datum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the

country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

A. Datum uses and processes Personally Identifiable Information (PII).

Problem Statements

Requirements

A. Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Business Goals

A. Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.

A. Datum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

A. Datum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received

email messages containing sensitive U.S. PII data.

Question: 13

You need to meet the technical requirement for the EU PII data.

What should you create?

A. a retention policy from the Security & Compliance admin center.
B. a retention policy from the Exchange admin center
C. a data loss prevention (DLP) policy from the Exchange admin center
D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

Question: 14

You need to meet the technical requirement for large-volume document retrieval. What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center
B. an alert policy from the Security & Compliance admin center
C. a file policy from Microsoft Cloud App Security
D. an activity policy from Microsoft Cloud App Security

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

Question: 15

DRAG DROP

You need to meet the requirement for the legal department.

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

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Answer:

Explanation:

Assign eDiscavery permissions

Create an eDisc every case.

Create a hold.

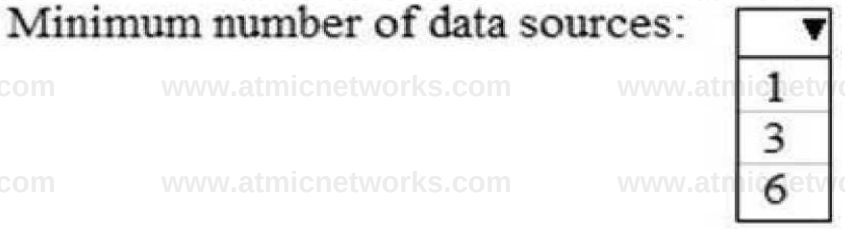
Reference:
https://www.sherweb.com/blog/ediscovery-office-365/

Question: 16

HOTSPOT

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

Question: 17

Which report should the New York office auditors view?

A. DLP policy matches

B. DLP false positives and overrides
C. DLP incidents
D. Top Senders and Recipients

Answer: C

Explanation:

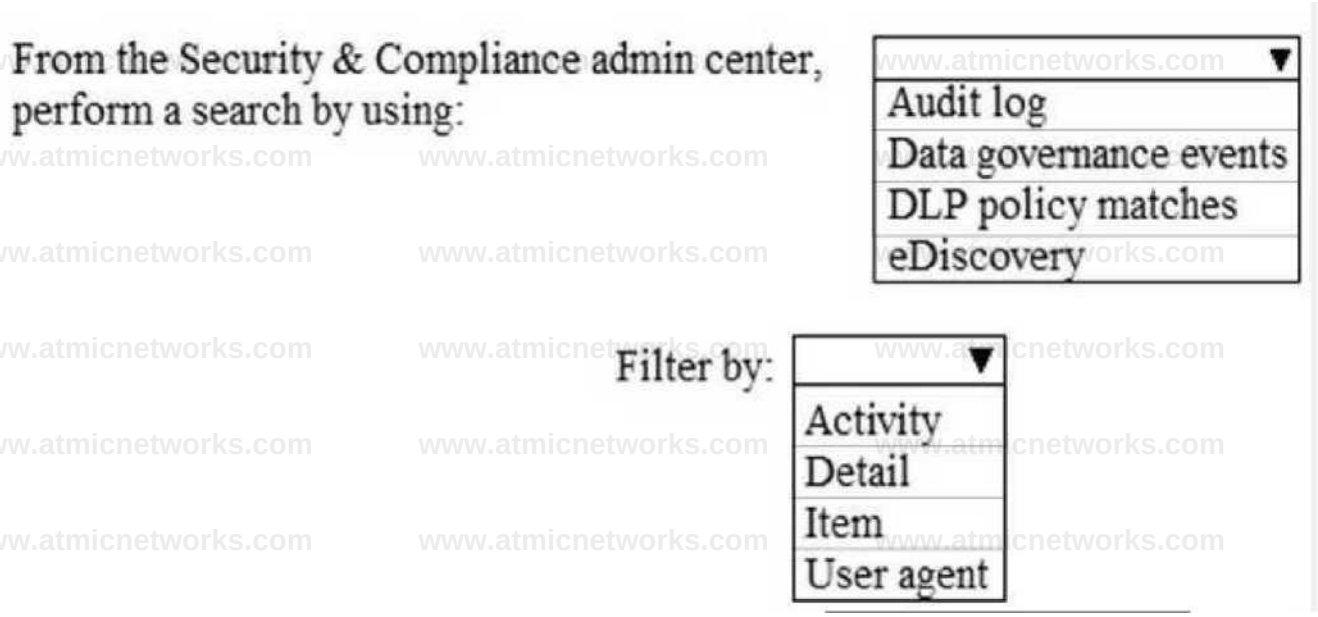
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

Question: 18

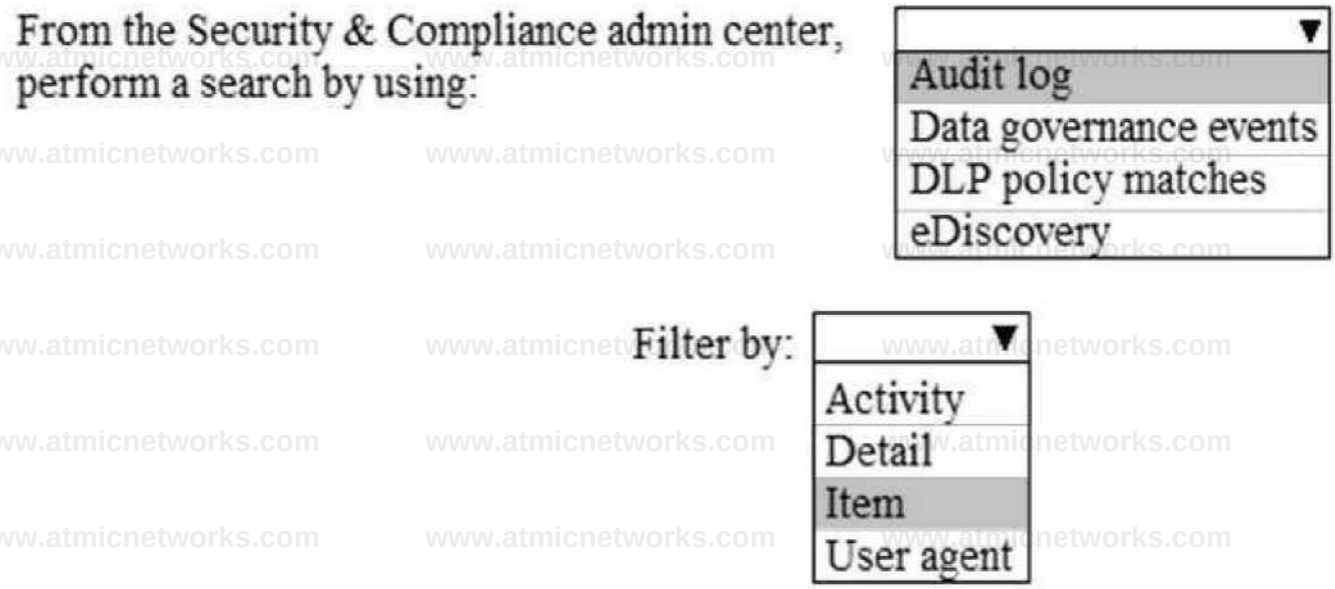
HOTSPOT

You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in- security-and-compliance#step-3-filter-the-search-results

Question: 19

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management

B. Microsoft Azure Active Directory (Azure AD) Identity Protection

C. Microsoft Azure Active Directory (Azure AD) conditional access policies

D. Microsoft Azure Active Directory (Azure AD) authentication methods

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept- conditional-access-conditions#sign-in-risk states clearly that Sign-in risk

Question: 20

You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

Answer: A

Explanation:

Topic 3, Litware Inc.

Case Study

Overview

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overviews

Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment

Existing Environment

The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
Used	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

Name	Platform
Device 1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Devices	Android

Litware.com contains the security groups shown in the following table.

Name	Members
UserGroupI	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroupI	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Audit log search is turned on for the litware.com tenant.

Problem Statements

Litware identifies the following issues:

Users open email attachments that contain malicious content.

Devices without an assigned compliance policy show a status of Compliant.

User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear. Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.

Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.

Implement data loss prevention (DLP) policies to protect confidential information.

Grant User2 permissions to review the audit logs of he litware.com tenant.

Deploy new devices to the Seattle office as shown in the following table.

Name	Platform
Device6	Windows 10
Device?	Windows 10
Device8	iOS
Device9	Android
Device 10	Android

Implement a notification system for when DLP policies are triggered.

Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:

Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.

Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.

All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically

when the devices are joined to or registered with Azure AD.

Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.

A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.

User2 must be granted the permissions to review audit logs for the following activities:

- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Azure AD

Users must be able to apply sensitivity labels to documents by using Office for the web.

Windows Autopilot must be used for device provisioning, whenever possible.

A DLP policy must be created to meet the following requirements:

- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.

The principle of least privilege must be used.

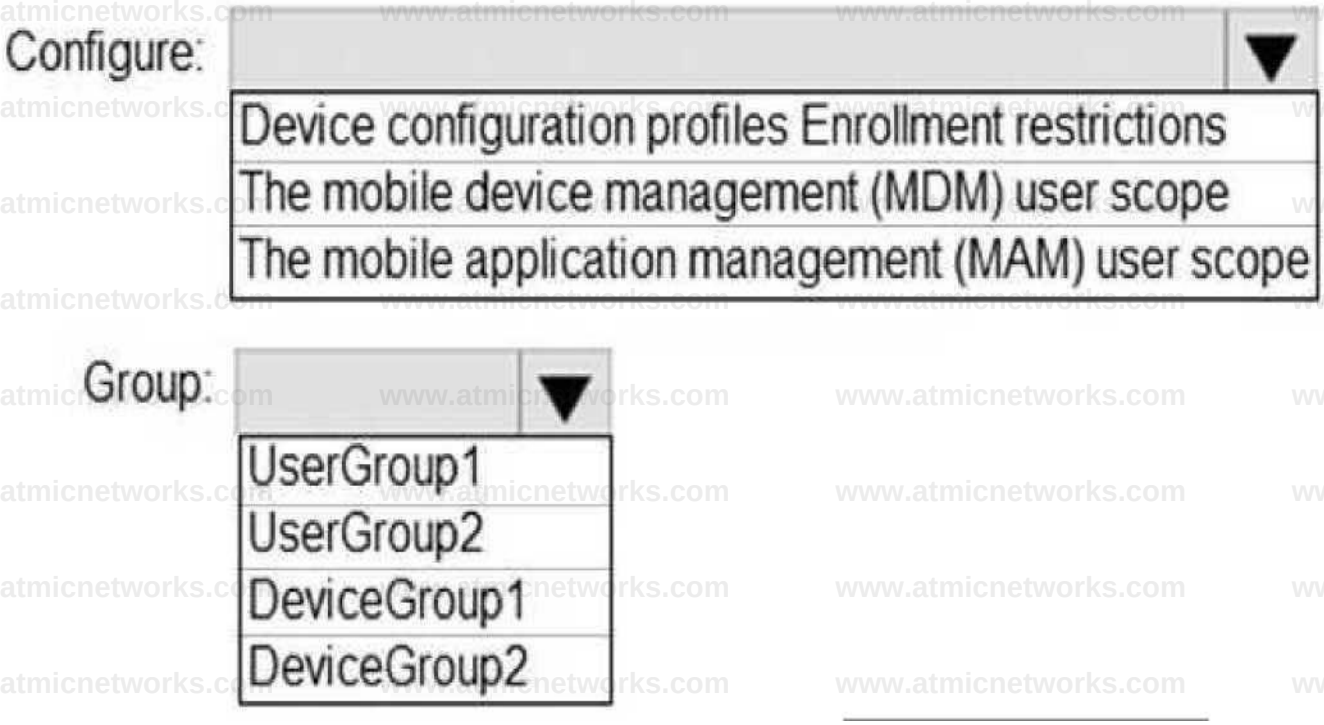
Question: 21

HOTSPOT

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.

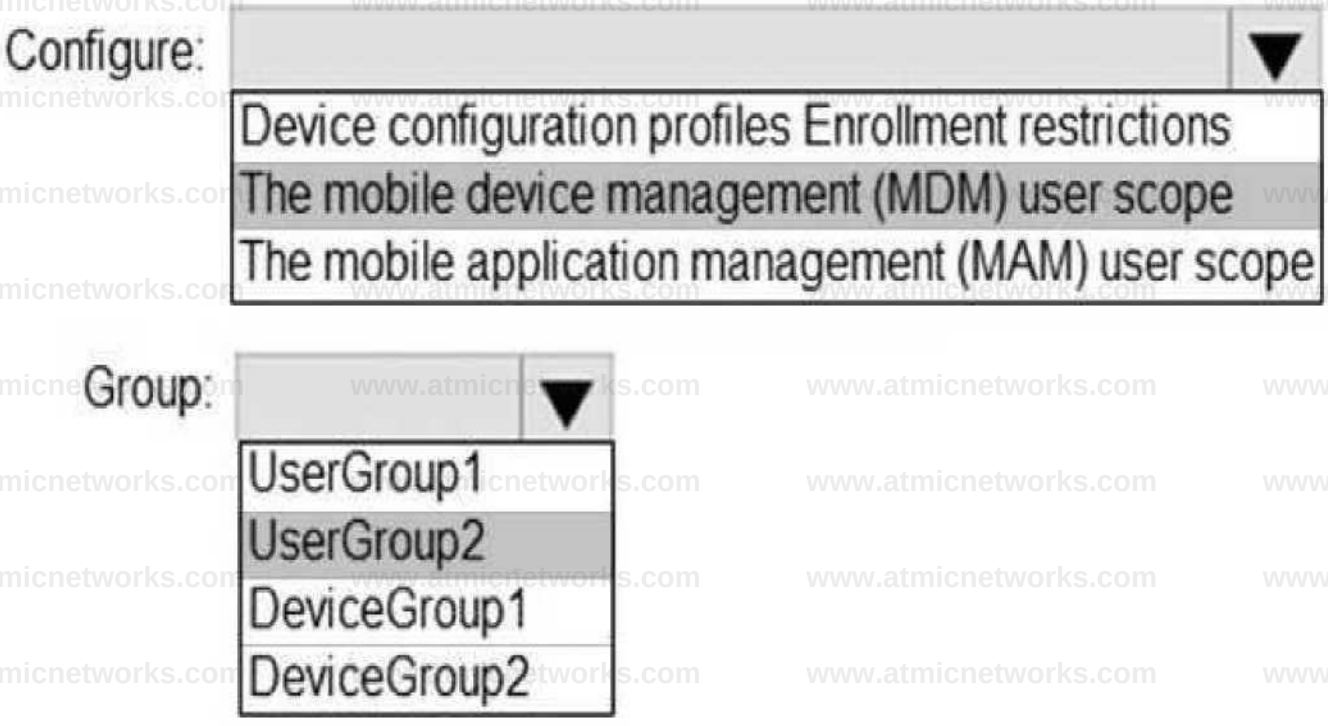
What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Explanation:

Answer:



Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

Question: 22

You need to create the Safe Attachments policy to meet the technical requirements.

Which option should you select?

A. Replace
B. Enable redirect
C. Block
D. Dynamic Delivery

Answer: D

Explanation:

Reference:

https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md

Question: 23

HOTSPOT

You plan to implement the endpoint protection device configuration profiles to support the planned changes.

You need to identify which devices will be supported, and how many profiles you should implement.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Supported devices: ▼

- Devi cel only
- Devicel and Device2 only
- Devicel and Device3 only
- Devicel, Device2, and Devices
- Devicel, Device4, and Devices
- Devicel, Device2, Devices, Device4, and Device5

Number of required profiles: ▼

- 1
- 2
- S
- 4
- 5

Answer:

Explanation:

Supported devices: ▼

- Devicel only
- Devicel and Device2 only
- Devicel and Devices only
- Devicel, Device2, and Devices
- Devicel, Device4. and Device5

Devicel. Device2, Devices. Device4, and Devices

Number of required profiles: ▼

1
2
3
4
5

Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

Question: 24

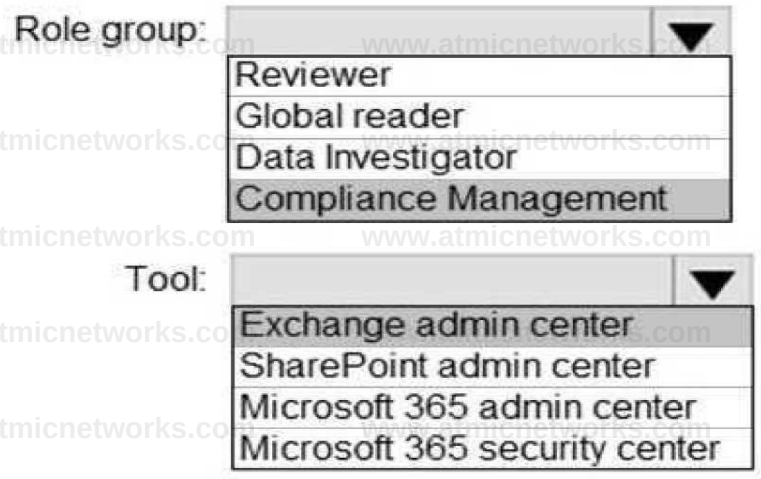
HOTSPOT

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.

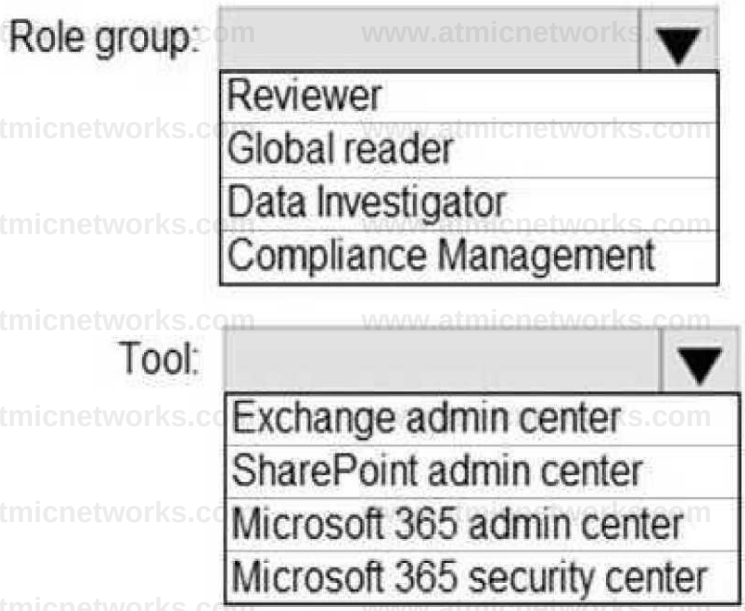
To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security- and-compliance?view=o365-worldwide

Question: 25

You need to configure Office on the web to meet the technical requirements.

What should you do?

A. Assign the Global reader role to User1.
B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
C. Configure an auto-labeling policy to apply the sensitivity labels.
D. Assign the Office apps admin role to User1.

Answer: B

Explanation:

Reference:

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

Question: 26

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements.

What should you do?

A. From the Microsoft 365 security center, configure an alert policy.
B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
C. From the Microsoft 365 admin center, configure a Briefing email.
D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

Question: 27

You need to configure the compliance settings to meet the technical requirements.

What should you do in the Microsoft Endpoint Manager admin center?

A. From Compliance policies, modify the Notifications settings.
B. From Locations, create a new location for noncompliant devices.
C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
D. Modify the Compliance policy settings.

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Question: 28

You need to create the DLP policy to meet the technical requirements.

What should you configure first?

A. sensitive info types
B. the Insider risk management settings
C. the event types
D. the sensitivity labels

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

Question: 29

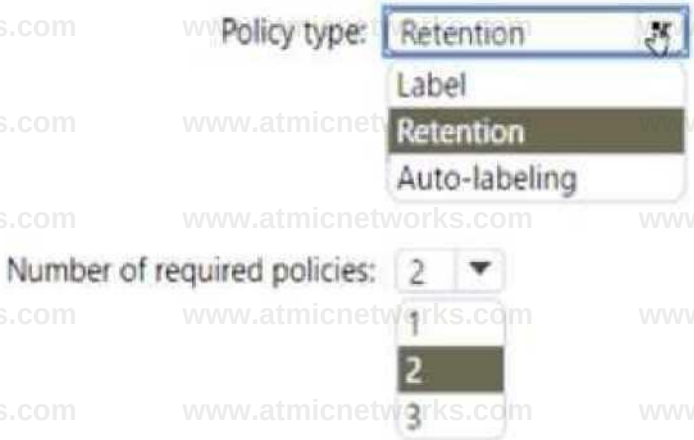
HOTSPOT

You need to configure the information governance settings to meet the technical requirements.

Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Policy type: Retention

Number of required policies:

Topic 4, FabrikamOverview

Overview

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment

Active Directory Environment

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented

by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements

Planned Changes

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable. A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.

Microsoft 365 Apps for enterprise applications must be installed from a network share only. Disruptions to email access must be minimized.

Application Requirements

Fabrikam identifies the following application requirements:

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.

The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements

Fabrikam identifies the following security requirements:

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question: 30

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.
Which DNS record should you recommend?

A. host (A)
B. host information
C. text (TXT)
D. alias (CNAME)

Answer: C

Explanation:

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:
There are several versions of this question in the exam. The question has two possible correct answers:
Text (TXT)
Mail exchanger (MX)

incorrect answer options you may see on the exam include the following:
alias (CNAME)

Host (A)
host (AAA)
Pointer (PTR)
Name Server (NS)
host information (HINFO)
pointer (PTR)

Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records- at-any-dns-hosting-provider

Question: 31

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.

Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication
B. pass-through authentication and seamless SSO
C. password hash synchronization and seamless SSO
D. password hash synchronization

Answer: C

Explanation:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications

automatically.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

Question: 32

Which role should you assign to User1?

Available Choices (select all choices that are correct)
A. Hygiene Management
B. Security Reader
C. Security Administrator
D. Records Management

Answer: C

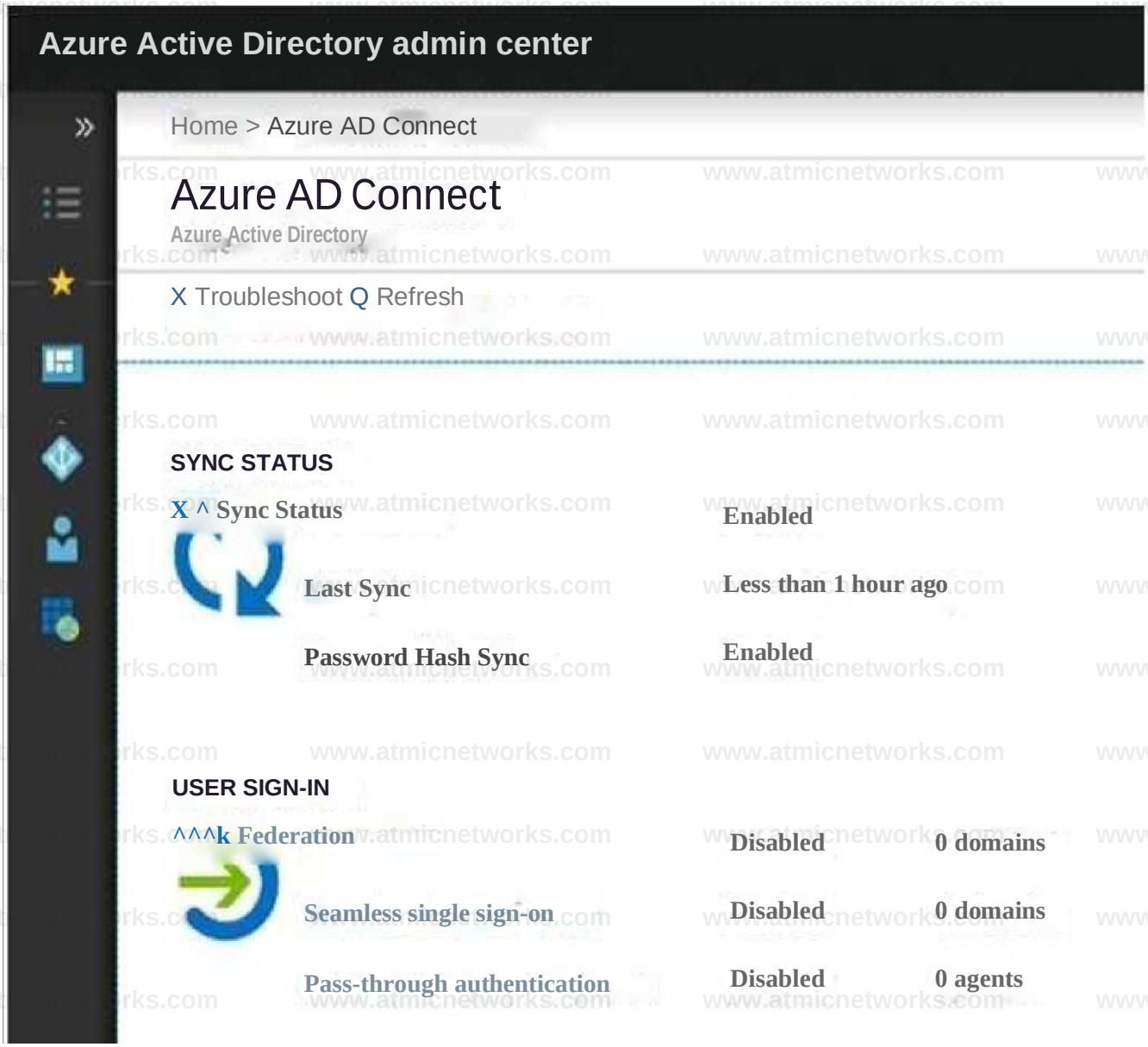
Explanation:

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign- admin-roles

Question: 33

HOTSPOT

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

During Project1, sales department users can access **[answer choice]** applications by using SSO.

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

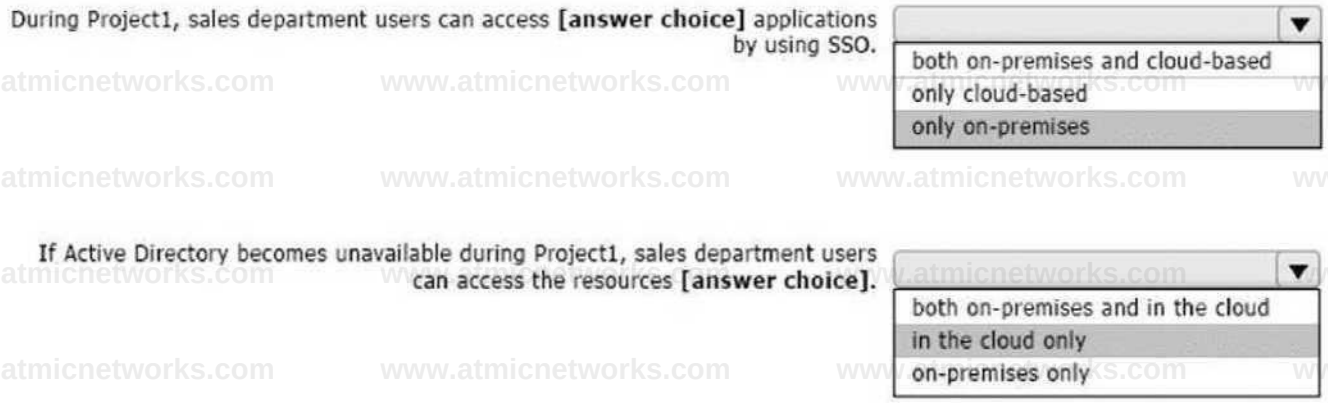
If Active Directory becomes unavailable during Project1, sales department users can access the resources **[answer choice]**.

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

Answer:

Explanation:

Answer Area



Box 1: only on-premises

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 onpremises 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.

Box 2: in the cloud only

Topic 5, Litware, Irk

Overview

Litware, Irk. is a consulting company that has a main office in Montreal and a branch office in Seattle?

Ltware collaborates with a third-party company named A. Datum Corporation.

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Adm nl	UtwareAdmins
Admm2	LitwareAdmins

AdminS	X.*,3'-Admins
Admin4	XwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.
Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.
The subscription contains a verified DNS domain named litware.com.
Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the UtwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Adminl	Gleba Aamnistratc
Admin2	Helpdesk Administrate!
AdminS	Security Administrator
AdmiM	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure AD tenant has Security defaults enabled.
Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to

the company.

- Litware users must be able to invite A. Datum users to participate in the following activities:

o Join Microsoft Teams channels,

o Join Microsoft Teams chats,

o Access shared files.

- Just in time access to critical administrative roles must be required.
- Microsoft 365 incidents and advisories must be reviewed monthly.
- Office 365 service status notifications must be sent to Admin2.
- The principle of least privilege must be used.

Question: 34

HOTSPOT

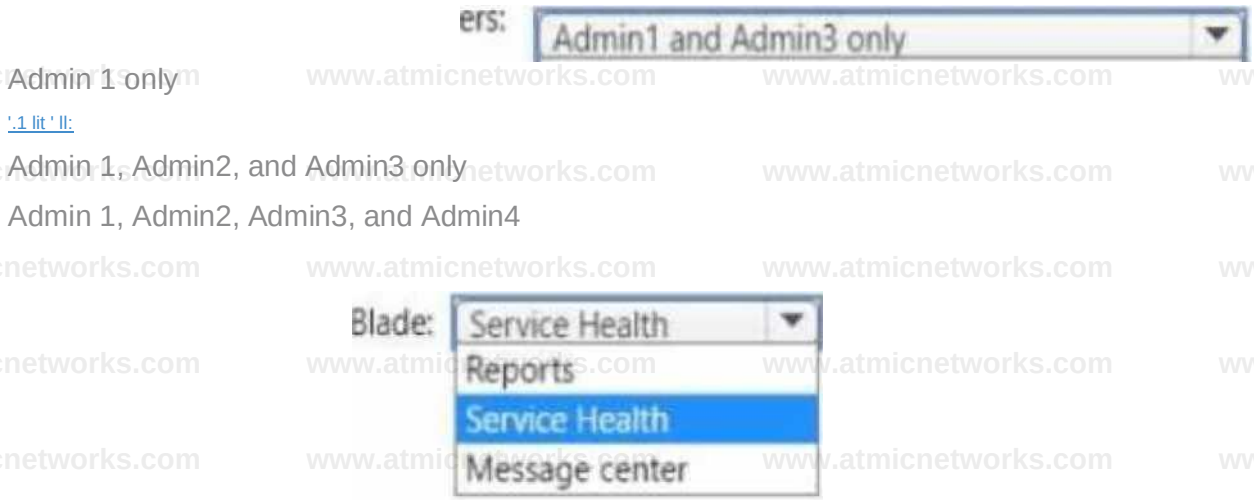
You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.

Which users can review the incidents and advisories, and which blade should the users use?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Users: Admin! and Ad mm3 only

Blade: Service Heal?

Question: 35

You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.

What should you do?

A. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.

B. From PowerShell, run the Add-ADSyncConnectorAttnbuteinclusion cmdlet.

C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.

D. From the Microsoft Azure AD Connect wizard, select Manage federation.

Answer: A

Explanation:

Question: 36

HOTSPOT

You need to ensure that Admin4 can use SSPR.

Which tool should you use. and which action should you perform? To answer, select the appropriate options m the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Action: Rv^ oaswnrd wnr*h*:k !▼

Enable app registrations.

Enable password hash synchronization.

Disable password hash synchronization.

Tool: Azur^^onnec^^^^^^^^^^^^^*

Synchronization Rules Editor

Microsoft Entra admin center

Answer:

Explanation:

Answer Area

Action: Enable password writeback

Tool: Azure AD Connect

Question: 37

HOTSPOT

You are evaluating the use of multi-factor authentication (MFA).

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.		
Users must use the Microsoft Authenticator app to complete MFA.		
After registering, users must use MFA for every sign-in.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.		
Users must use the Microsoft Authenticator app to complete MFA.		
After registering, users must use MFA for every sign-in.		

Question: 38

You need to configure just in time access to meet the technical requirements.

What should you use?

A. entitlement management
B. Azure AD Privileged Identity Management (PIM)
C. access reviews
D. Azure AD Identity Protection

Answer: B

Explanation:

Question: 39

HOTSPOT

You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements. What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To configure the notifications: Briefing email

- **Briefing email**
- Help desk information
- Organization information

To limit access: Release preferences

- Privileged Access
- **Release preferences**
- (Office installation options

Answer:

Explanation:

Answer Area

To configure the notifications: [Briefing email

To limit access: Release preferences

Topic 6, Misc. Questions

Question: 40

HOTSPOT

You have a Microsoft 365 subscription.

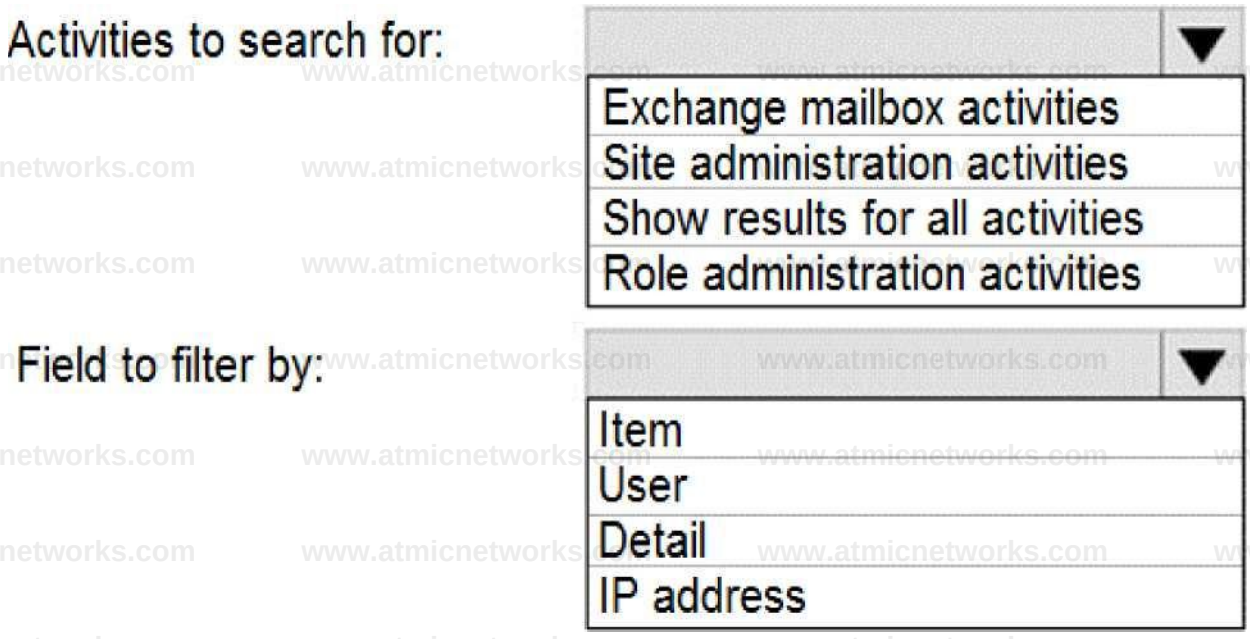
Your network uses an IP address space of 51.40.15.0/24.

An Exchange Online administrator recently created a role named Role1 from a computer on the network.

You need to identify the name of the administrator by using an audit log search.

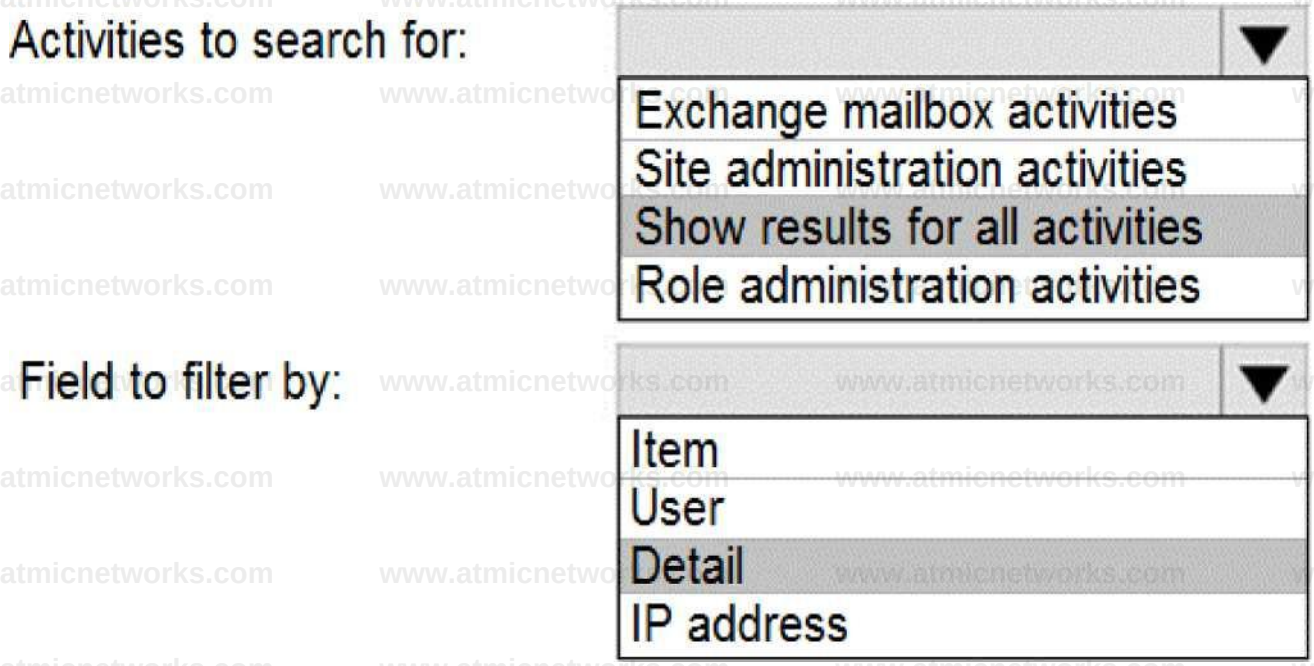
For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 41

You have a Microsoft 365 subscription that uses Security & Compliance retention policies.

You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point?

A. Add locations to the policy
B. Reduce the duration of policy
C. Remove locations from the policy
D. Extend the duration of the policy
E. Disable the policy

Answer: A,B

Explanation:

Question: 42

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

D18912E1457D5D1DDCBD40AB3BF70D5D

What should you create to ensure that the DLP policy can detect the customer IDs?

A. a sensitive information type

B. a sensitivity label

C. a supervision policy

D. a retention label

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide

Question: 43

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

You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.

Which role should you assign to User1?

A. View-Only Audit Logs in the Security & Compliance admin center

B. View-Only Audit Logs in the Exchange admin center

C. Security reader in the Azure Active Directory admin center

D. Security Reader in the Security & Compliance admin center

Answer: B

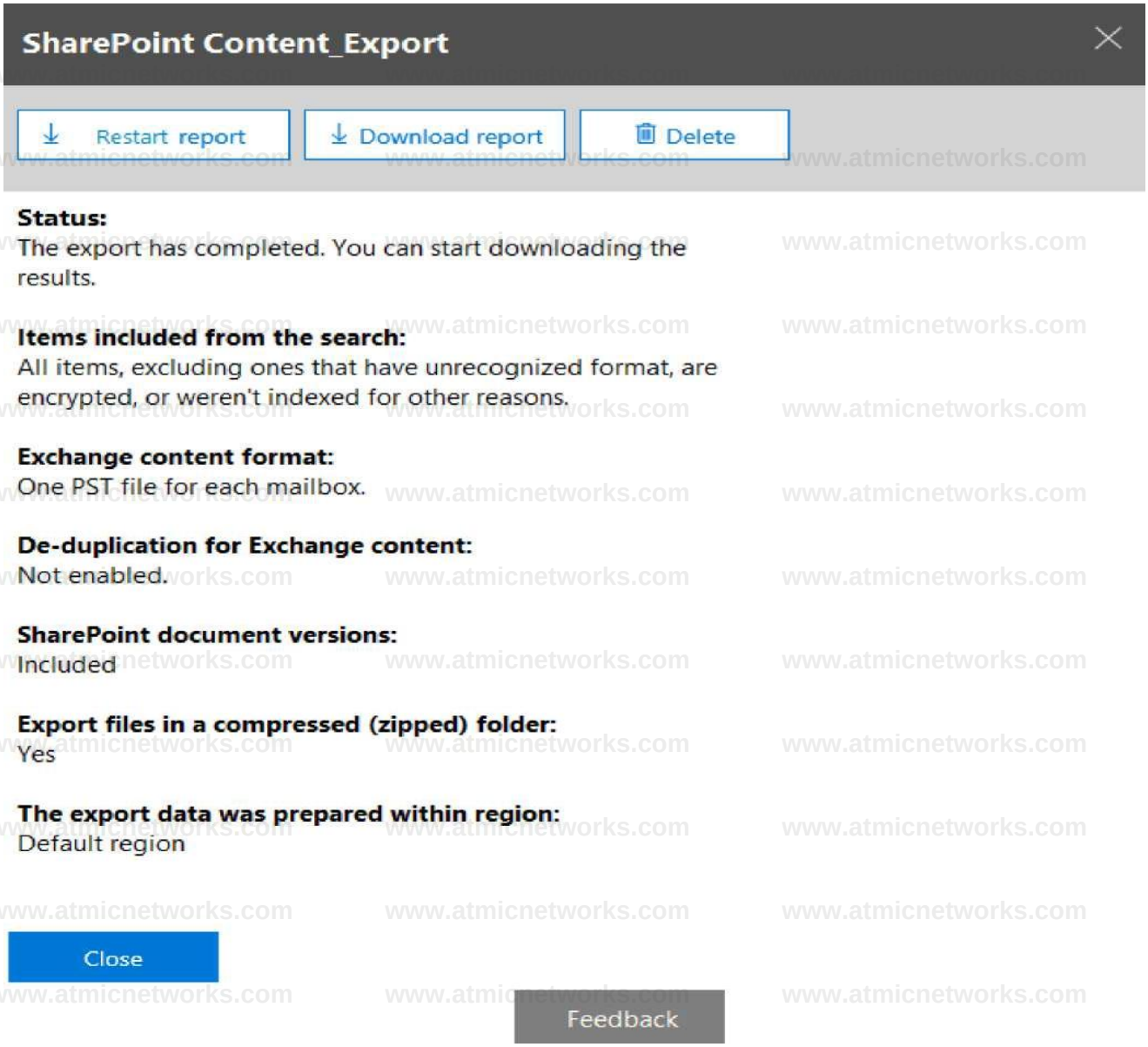
Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

Question: 44

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



What will be excluded from the export?

A. a 10-MB XLSX file
B. a 5-MB MP3 file
C. a 5-KB RTF file

D. an 80-MB PPTX file

Answer: B

Explanation:

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in- content-search?view=o365-worldwide

https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search- report

Question: 45

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the forest functional level to Windows Server 2016. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

A. yes
B. No

Answer: B

Explanation:

Question: 46

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.

Does this meet the goal?

A. yes
B. No

Answer: A

Explanation:

Question: 47

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

A. yes
B. No

Answer: A

Explanation:

Question: 48

You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.

You have the devices shown in the following table.

Name	Platform	Configuration
Device 1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

You plan to enable co-management.You need to identify which devices support co-management without requiring the installation of additional software.

Which devices should you identify?

A. Device1 only
B. Device2 only
C. Device3 only
D. Device2 and Device3 only
E. Device1, Device2, and Device3

Answer: D

Explanation:

Question: 49

HOTSPOT

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

Name	Member of	Azure Active Directon (Azure AD) role
Userl	Group 1	Global administrator
User!	Group?	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

Settings

The enrollment status page appears during initial device setup If enabled users can see the installation progress of assigned apps and profiles

Show app and profile installation progress.

Show time limit error when installation takes longer than specified number of minutes

Show custom message when time limit error occurs

Allow users to collect logs about mstalattion errors

Only show page to devices provisioned by out-of-box experience (OOBE)

Block device use until all apps and profiles are installed

You assign the policy to Group1.

You purchase the devices shown in the following table.

Name	Platform
Device 1	Windows 10
Device!	Android

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

NOTE: Each correct selection is worth one point.

Yes No

60

Yes No

No

Statements	Yes	No
If Useri performs the initial device enrollment for DeviceI, the Enrollment Status Page will show.	O	
If Useri performs the initial device enrollment for Device2, the Enrollment Status Page will show.	O	
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	Q	Q

Answer:

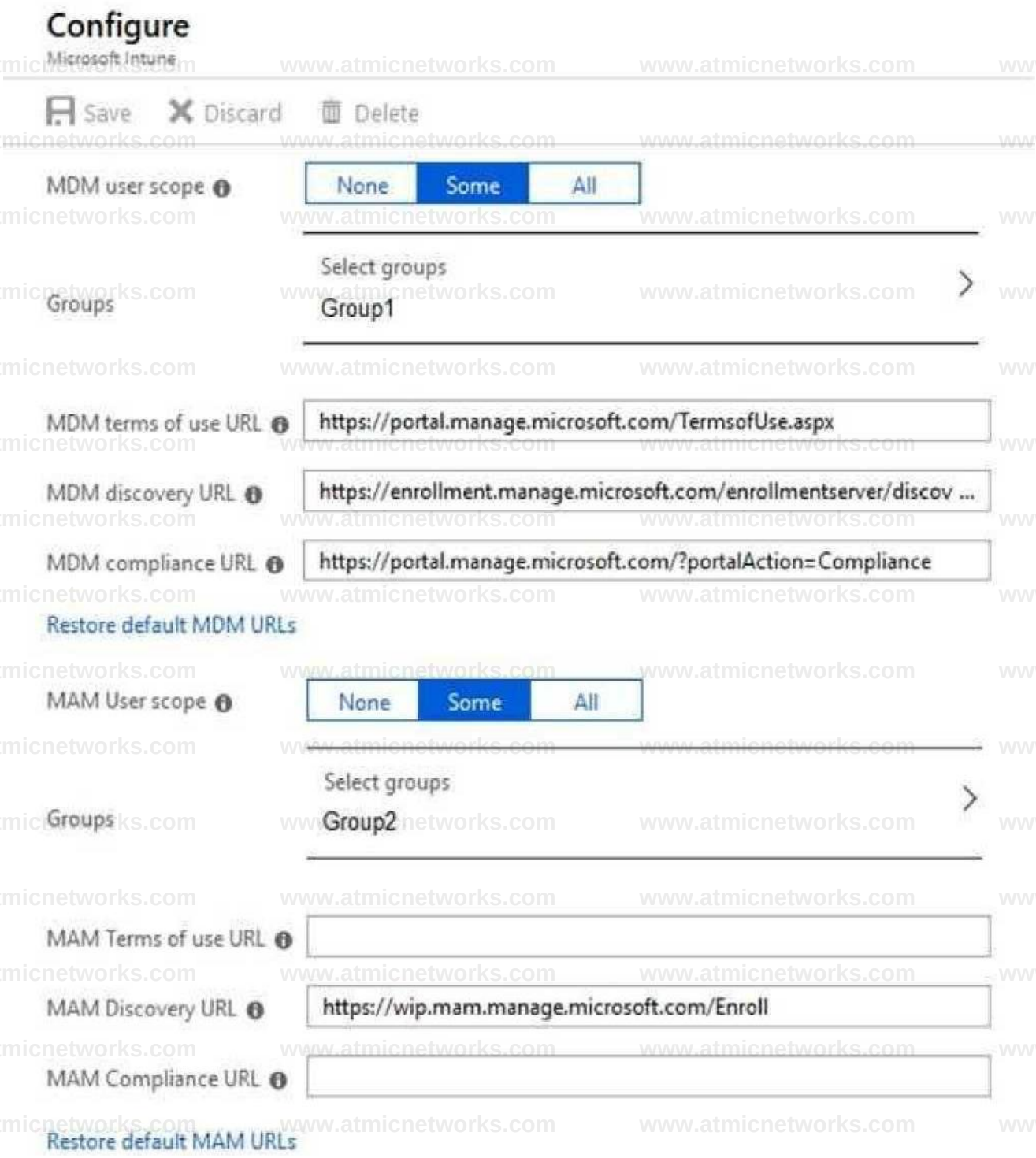
Question: 50

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

>aine	**Member of**
Userl	Group 1
User!	Group!
UserS	Group L GroupZ

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



You purchase a Windows 10 device named Device1.

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

NOTE: Each correct selection is worth one point.

Statements

yM

^

If Userl joins Devicel to contoso.com, Devicel is enrolled in Intune automatically.	Q	Q
If User2 joins Devicel to contoso.com, Devicel is enrolled in Intune automatically.	Q	Q
If User3 registers Devicel in contoso.com, Devicel is enrolled in Intune automatically.	O	O

Answer:

Explanation:

Statements	Yes	No
If Userl joins Devicel to contoso.com, Devicel is enrolled in Intune automatically.	0	0
If User2 joins Devicel to contoso.com, Devicel is enrolled in Intune automatically.	0	0
If User3 registers Devicel in contoso.com, Devicel is enrolled in Intune automatically.	0	0

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

Question: 51

You have a Microsoft 365 subscription.

You need to identify which administrative users performed eDiscovery searches during the past week.

What should you do from the Security & Compliance admin center?

A. Perform a content search
B. Create a supervision policy
C. Create an eDiscovery case
D. Perform an audit log search

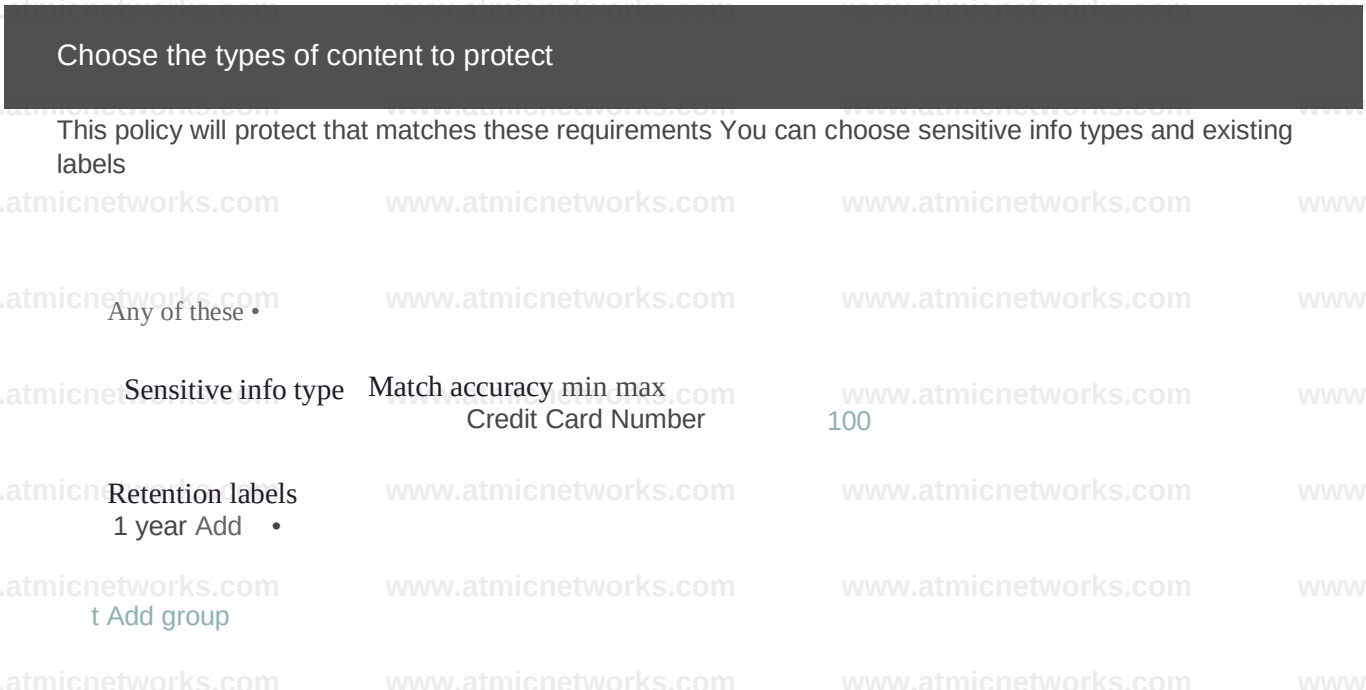
Answer: D

Explanation:

Question: 52

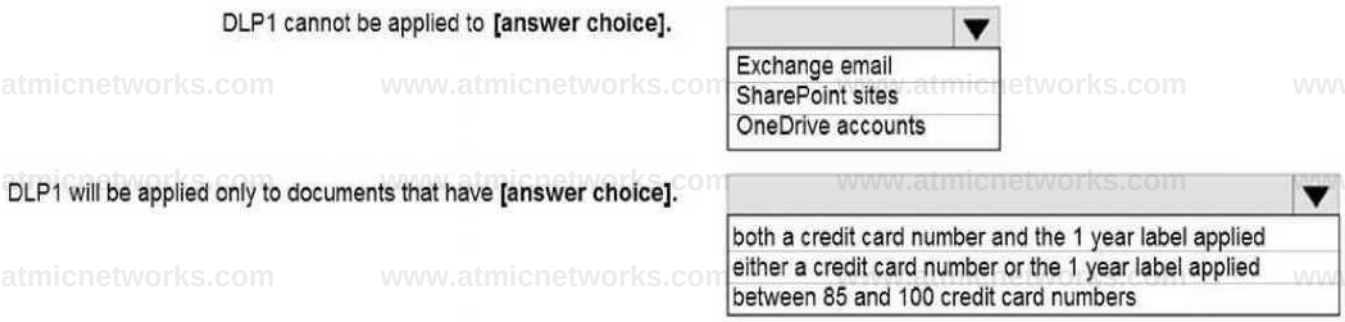
HOTSPOT

You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.



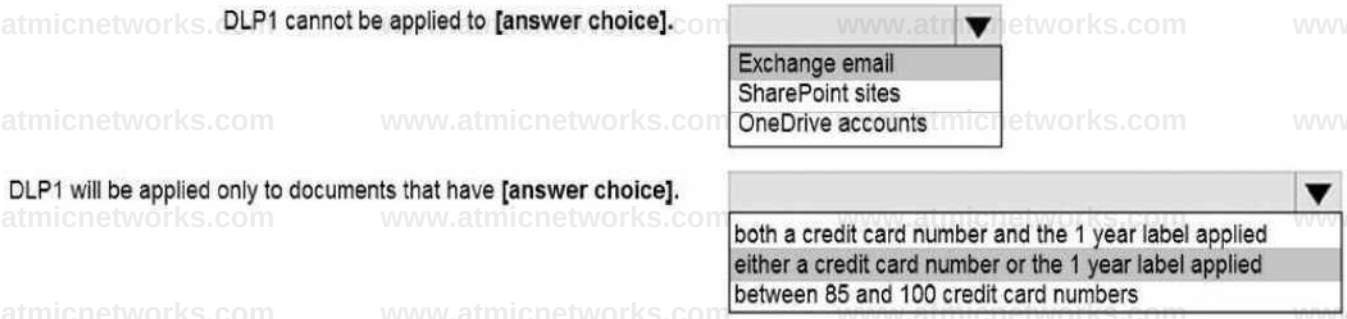
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

nce:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention- policies?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

Question: 53

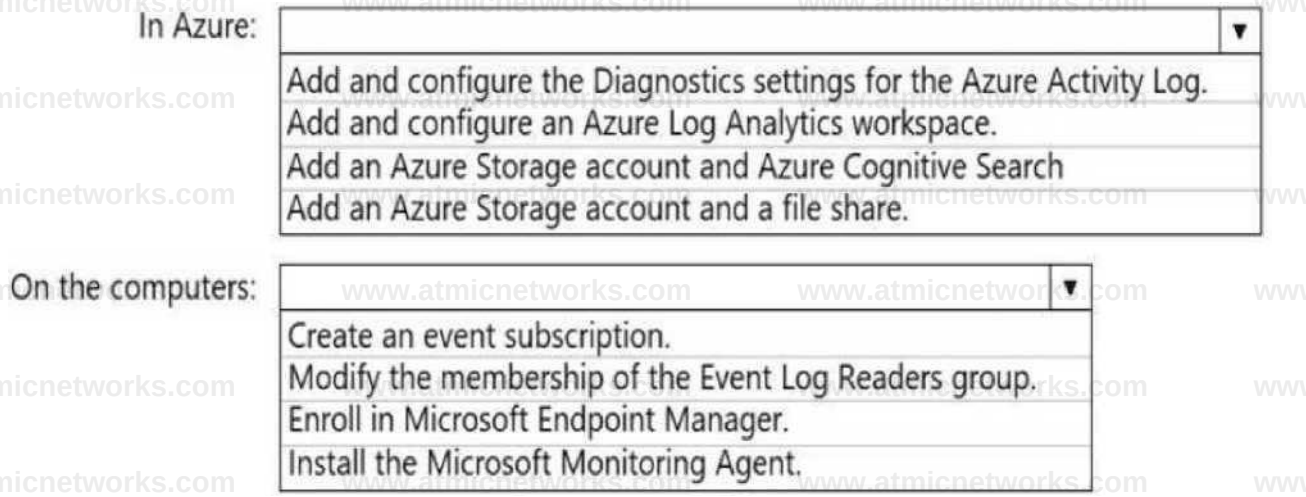
HOTSPOT

You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

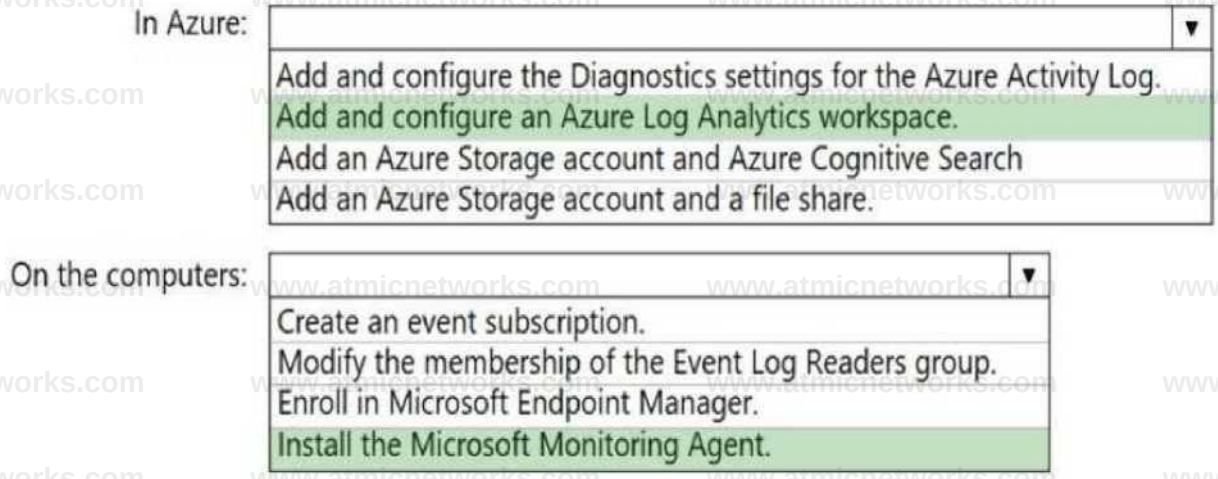
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer

Question: 54

You enable the Azure AD Identity Protection weekly digest email.

You create the users shown in the following table.

Name	Role
AdminI	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

Which users will receive the weekly digest email automatically?

A. Admin2, Admin3, and Admin4 only
B. Admin1, Admin2, Admin3, and Admin4
C. Admin2 and Admin3 only
D. Admin3 only
E. Admin1 and Admin3 only

Answer: E

Explanation:

By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

Question: 55

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

A. OneDrive accounts
B. Exchange email
C. Teams chat and channel messages
D. SharePoint sites

Answer: B

Explanation:

Question: 56

HOTSPOT

You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

A user named User1 stores documents in Microsoft OneDrive.

You need to place the contents of User1's OneDrive account on an eDiscovery hold.

Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

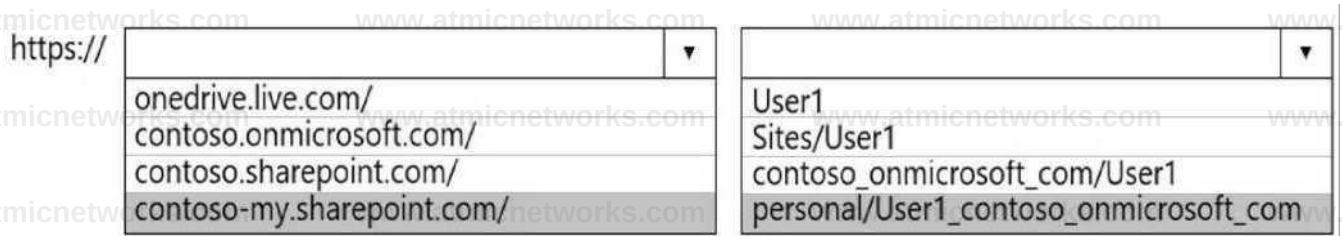
NOTE: Each correct selection is worth one point.

https://

onedriveJiye.com/	Useri
contoso.onmicrosoft.com/	Sites/Userl _
contoso.sharepoint.com/	contosoj3nmicrosoft.com/User1
contoso-my.sharepoint.com/	personal/User1_contoso_onmicrosoft_com

Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds

Question: 57

HOTSPOT
: 218
HOTSPOT

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following

table:

Name	Role
AdminI	Conditional Access administrator
Admin?	Security administrator
AdminS	User administrator

The tenant has a conditional access policy that has the following configurations:

Name: Policy1
Assignments:
- Users and groups: Group1

- Cloud aps or actions: All cloud apps

Access controls:

Grant, require multi-factor authentication

Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Adminl can set Enable policy for Policy! to On.	o	o
Admin2 can set Enable policy for Policy! to Off.	o	o
Admin3 can set Users and groups for Policy! to All users.	o	o

Answer:

Explanation:

Statements	Yes	No
Adminl can set Enable policy for Policy! to On.	o	o
Admin2 can set Enable policy for Policy! to Off.	o	o
Admin3 can set Users and groups for Policy! to All users.	o	o

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

Conditional Access policies can be enabled in report-only mode.

During sign-in, policies in report-only mode are evaluated but not enforced.

Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details. Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept- conditional-access-report-only

Question: 58

DRAG DROP

: 219

DRAG DROP

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

Block emails that contain financial data.
Display the following policy tip text: Message blocked. From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

Use the following location: Exchange email.
Display the following policy tip text: Message contains sensitive data.
When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Results

The email wilt be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

Answer Area

When the user sends an email that contains financial data and health records: Result

When the user sends an email that contains only financial data: Result

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer:

Explanation:

When the user sends an email that contains financial data and health records: The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked. If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin- centers

Question: 59

DRAG DROP

: 220

DRAG DROP

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Serveri	Windows Server 2016	File Server Resource Manager (FSRM)
Server?	Windows Server 2016	*None*

You use Azure Information Protection.

You need to ensure that you can apply Azure Information Protection labels to the file stores

on Server1.

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.

Actions

Authorize Server!.

Install the Microsoft Rights Management connector on Server2.

Install a certificate on Servers.

Install a certificate on Server!.

Register a service principal name for Server!.

Run GenConnectorConfig.ps! on Server!.

Run GenConnectorConfig.psi on ServerS.

Answer Area

Answer:

Explanation:

Answer Area

Install the Microsoft Rights Management connector on Server2.

Authorize Server1.

Run GenConnectorConfig.ps1 on Server1.

Reference:

https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms- connector

https://docs.microsoft.com/en-us/azure/information-protection/configure-servers-rms- connector

Question: 60

: 221

You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.

Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Devicel	Android	Userl	Yes
Device?	Android	Userl	No
Device?	iOS	Userl	No
Device4	Windows 10	User?	Yes
Devices	Windows 10	User?	No
Device6	iOS	User?	Yes

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

A. Device1, Device4, and Device6
B. Device2, Device3, and Device5
C. Device1, Device2, Device3, and Device6
D. Device1, Device2, Device4, and Device5

Answer: C

Explanation:

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

Question: 61

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRestl	Android, Windows (MDM)	Groupl
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRestl	7	Group2
2	LimitRest2	10	Groupl
3	LimitRest3	5	Group3

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Useri can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager	O	0
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager	Q	g
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	O	

Answer:

Explanation:

Statements	Yes	No
Useri can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager	0	0
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager	0	0
User3 can enroll up to five Android devices in Microsoft Endpoint Manager	O	O

Question: 62

: 223

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

A. a custom detection rule
B. an allowed/blocked list rule
C. an alert suppression rule
D. an indicator

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/manage-indicators

Question: 63

HOTSPOT

: 224

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.

All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.

You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)

New audit retention policy

Name •:

Policy I

Description

Record Types

AzureActiveDirectory -

Activities

Added user, Deleted user, Reset user password, Changed user password, Changed user license, ..(7) -

Users:

Admin 1

Duration ‘;

® 90 Days

6 Months

1 Year

Priority •:

100

Cancel

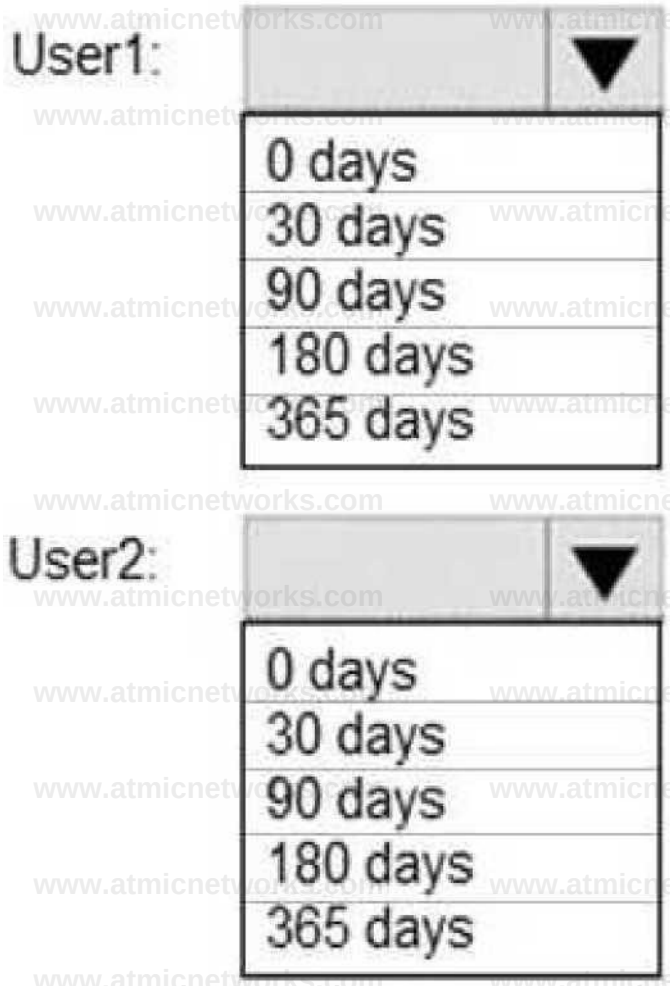
After Policy1 is created, the following actions are performed:

Admin1 creates a user named User1.

Admin2 creates a user named User2.

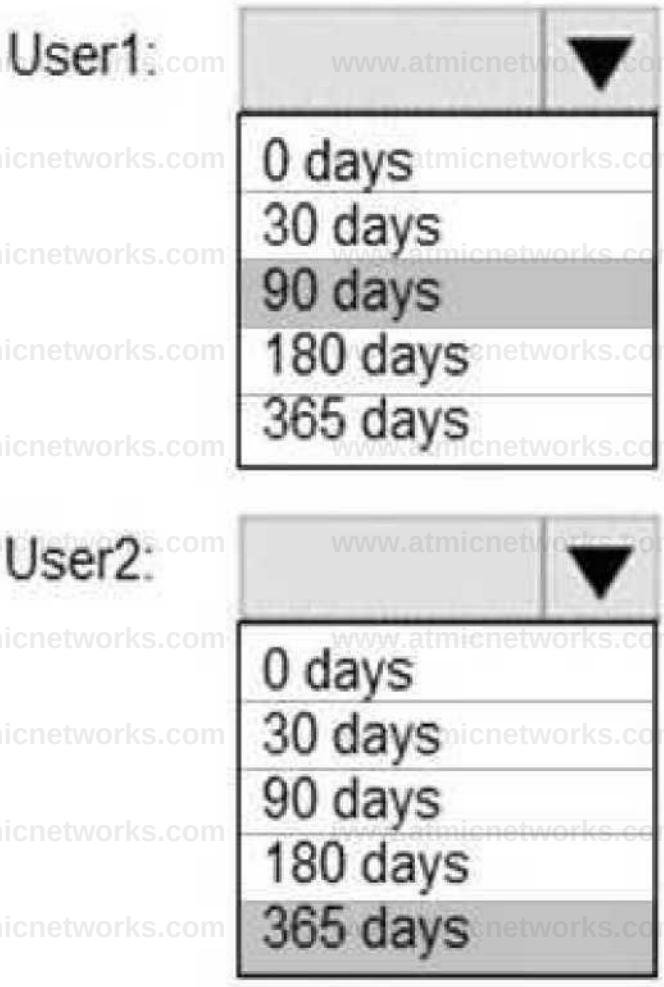
How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



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

Question: 64

: 225

You implement Microsoft Azure Advanced Threat Protection (Azure ATP).

You have an Azure ATP sensor configured as shown in the following exhibit.

How long after the Azure ATP cloud service is updated will the sensor update?

A. 20 hours

B. 12 hours

C. 7 hours

D. 48 hours

Answer: B

Explanation:

Question: 65

HOTSPOT

: 226

HOTSPOT

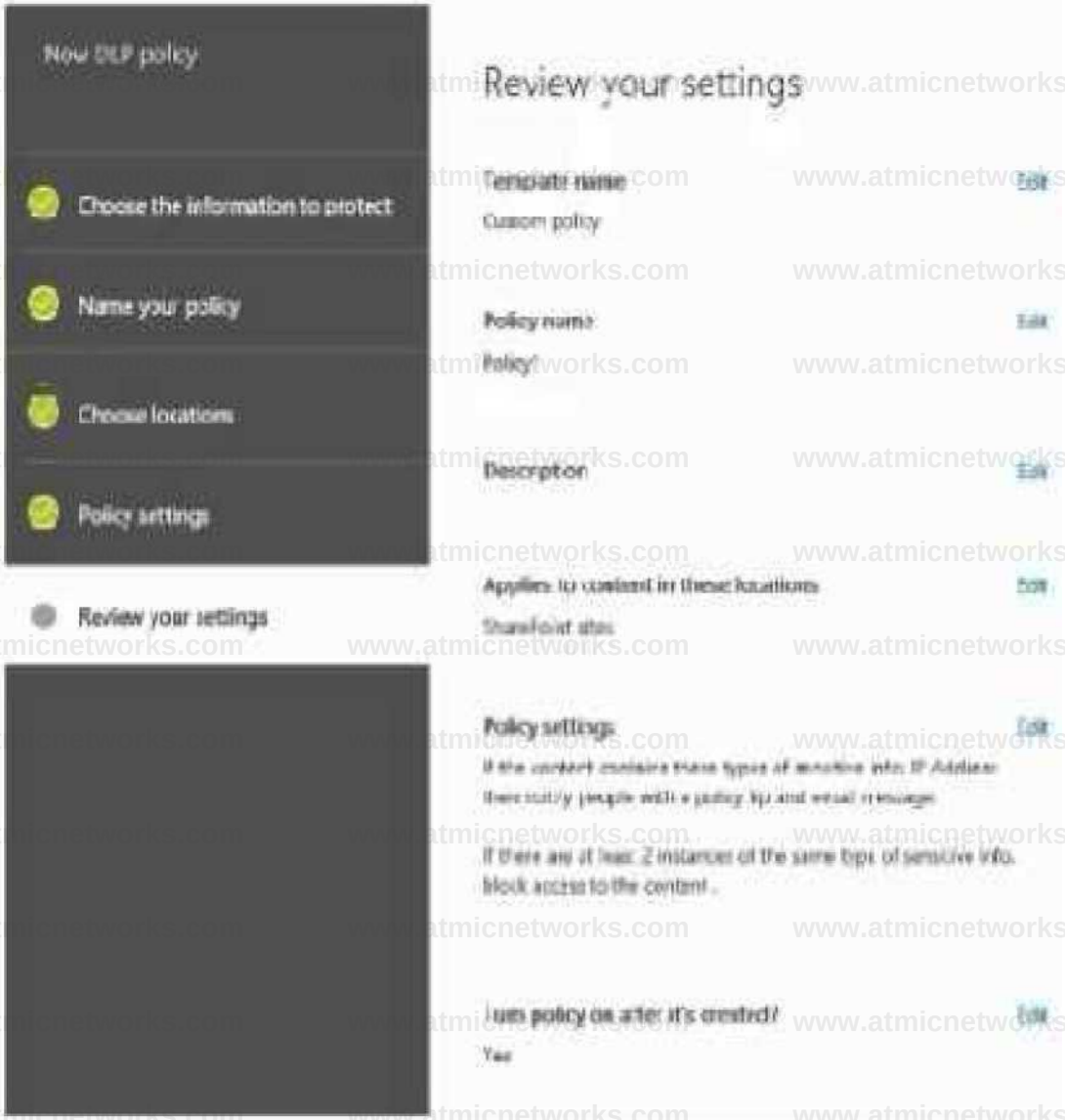
You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he files in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.pptx	3

The Site1 users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data less prevention (DLP) policy names Policy1 as shown in the following exhibit.



How many files will be visible to user1 and User2 after Policy' is applied to answer, selected select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

AJ»HH **Arw**

Lst: i; i

Answer:

Explanation:

A/uwvi Aru

I.Wi: . *

L^n: 2 *

Question: 66

: 227

You have a Microsoft 365 F5 subscription.

You plan to deploy 100 new Windows 10 devices.

You need to order the appropriate version of Windows 10 for the new devices. The version must Meet the following requirements.

Be serviced for a minimum of 24 moths.

Support Microsoft Application Virtualization (App-V)

Which version should you identify?

A. Window 10 Pro, version 1909

B. Window 10 Pro, version 2004

C. Window 10 Pro, version 1909

D. Window 10 Enterprise, version 2004

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/windows/release-health/release-information

https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported- configurations

Question: 67

: 228

You have a Microsoft 365 subscription.

You discover that some external users accessed center for a Microsoft SharePoint site.

You modify the sharePoint sharing policy to prevent sharing, outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the Security $ Compliance admin center you create a threat management policy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 68

DRAG DROP

: 229

DRAG DROP

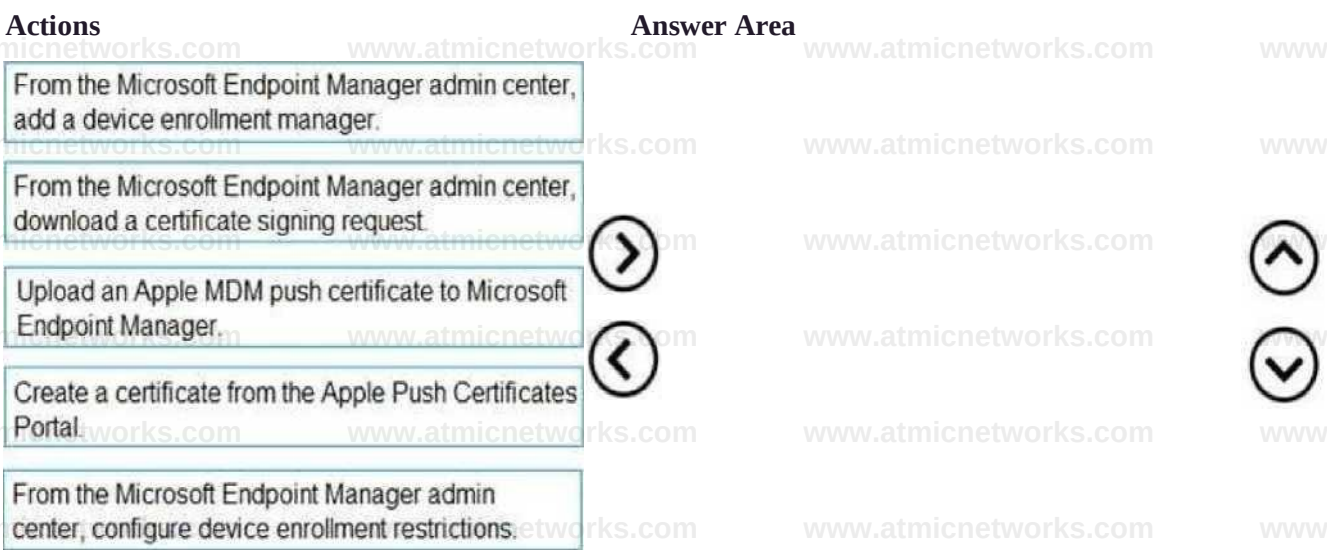
You have a Microsoft 365 E5 subscription.

Several users have iOS devices.

You plan to enroll the iOS devices in Microsoft Endpoint Manager.

You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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.



Answer:

Explanation:

From the Microsoft Endpoint Manager admin center download a certificate signing request.

Create a certificate from the Apple Push Certificates Portal

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

Question: 69

: 230

You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).

You need to create a detection exclusion in Azure ATP.

Which tool should you use?

A. the Security & Compliance admin center
B. Microsoft Defender Security Center
C. the Microsoft 365 admin center
D. the Azure Advanced Threat Protection portal
E. the Cloud App Security portal

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/what-is

https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections

Question: 70

: 231

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.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Endpoint Management admin center, you create a device configuration profile.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You need to create a trusted location and a conditional access policy.

Question: 71

: 232

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 72

: 233

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

You need to assign the Security Administrator role.

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

Question: 73

: 234

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Service Administrator role.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

You need to assign the Security Administrator role.

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

Question: 74

: 235

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:

- Assign licenses to users.
- Procure apps from Microsoft Store.
- Manage private store availability for all items.

The solution must use the principle of least privilege.

Which Microsoft Store for Business role should you assign to User1?

A. Basic Purchaser

B. Device Guard signer

C. Admin

D. Purchaser

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

Question: 75

: 237

You have a Microsoft 365 E5 tenant.

You plan to deploy 1.000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.

You need to recommend a Microsoft Intune enrollment option that meets the following requirements:

- Minimizes user interaction
- Minimizes administrative effort
- Automatically installs corporate apps

What should you recommend?

A. Automated Device Enrollment (ADE)

B. bring your own device (BYOD) user and device enrollment

C. Apple Configurator enrollment

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

Question: 76

HOTSPOT

: 238
HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Microsoft 365 role
Useri	Cloud application administrator
User2	Application administrator
UserS	Application developer
User4	**None**

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
Useri	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the

answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

Question: 77

: 239

Your company has offices in five cities.
The company has a Microsoft 365 tenant.
Each office is managed by a local administrator.
You plan to deploy Microsoft Intune.
You need to recommend a solution to manage resources in intune that meets the following requirements:
Local administrators must be able to manage only the resources in their respective office. Local administrators must be prevented from managing resources in other offices.
Administrative effort must be minimized.

What should you include in the recommendation?

A. device categories
B. scope tags
C. configuration profiles
D. conditional access policies

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

Question: 78

: 240

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device'	MacOS
Device^	Windows 10 Pro
Devices	Windows 10 Enterprise
Device^	Ubuntu 13.04 ITS

You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

A. Device 1, Device2, and Device3 only

B. Device3 only

C. Device2 and Device3 only

D. Device1, Device2, Devices and Device4

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack- surface-reduction?view=o365-worldwide#requirements

Question: 79

: 241

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

A. Microsoft Store for Business

B. Apple Business Manager

C. Apple iTunes Store

D. Apple Configurator

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

Question: 80

: 242

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts Qs/ViHi/p^
Pg hey 1	Attack surface reduction (ASR)	Audit mode
Policy 2	Microsoft Defender ATP Baseline	Disable
PoheyS	Device configuration profile	Not configured

A. only the settings of Policy!

B. only the settings of Policy2

C. only the settings of Policy3 D. no settings

Answer: C

Explanation:

Question: 81

: 243

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.

B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.

C. From the Microsoft 365 admin center, modify Organization information.

D. From the Microsoft 365 admin center, modify Help desk information.

Answer: A

Explanation:

Reference:

https://systemcenterdudes.com/intune-company-portal-customization/

Q

Question: 82

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You need to configure Microsoft Defender ATP on the computers.

What should you create from the Endpoint Management admin center?

A. a device configuration profile

B. an update policy for iOS

C. a Microsoft Defender ATP baseline profile

D. a mobile device management (MDM) security baseline profile

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

Question: 83

HOTSPOT

You have a Microsoft 365 tenant.

You need to create a custom Compliance Manager assessment template.

Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Answer Area

Application: Microsoft Excel

File format csv

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-create?view=o365-worldwide

Question: 84

HOTSPOT

: 247
HOTSPOT

				actions				
SP800	15444	incomplete	72%	3 of 450 completed	887 of 887 completed	Group 1	Microsoft 365	NIST SOO-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group?	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP80O assessment.		
The SP800 assessment score will increase by 54 points.		
The Data Protection Baseline score will increase by 9 points.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment	•	
The SP800 assessment score will increase by 54 points.		○ ®
The Data Protection Baseline score will increase by 9 points.	•	

Question: 85

DRAG DROP

: 248
DRAG DROP

You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:

- Use a file plan to manage retention labels.
- Identify, monitor, and automatically protect sensitive information.
- Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

ilutWm

Data Jors prevention

Information governance

Insider rifk management

Record* management

Answer Area

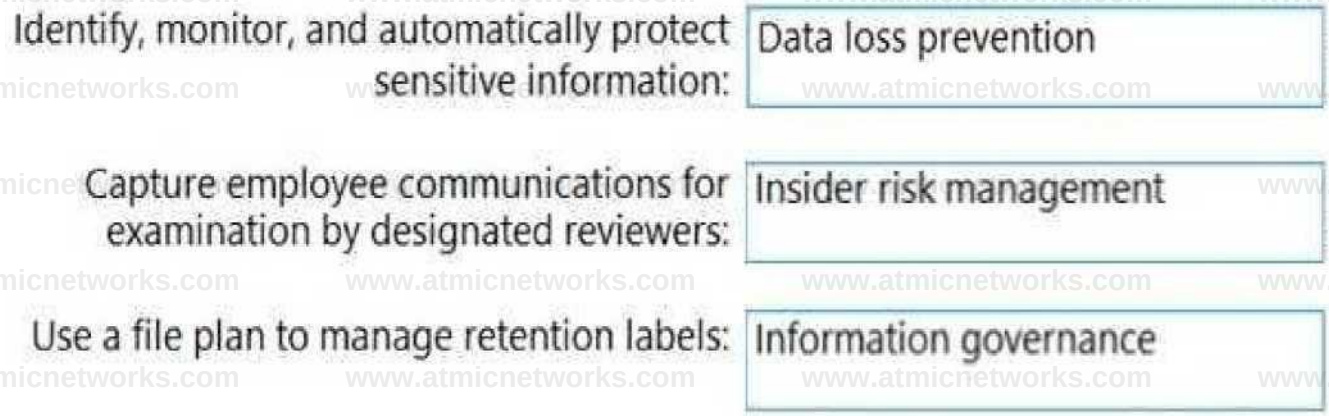
irfentify, monitor and automaiKaHy protect sensitive information:

Capture employee communications for examination by designates reviewers. ”

Use a He plan to manage retention labels

Answer:

Explanation:



Question: 86

HOTSPOT

: 249
HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
Useri	UserGroupI
User?	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Devicel	Userl	*None*	Windows 10	Enrolled
Device?	User?	App2	Android	Not enrolled
Devices	User3	*None*	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
App1 can be assigned as a required install for User3.	O	O
App2 can be uninstalled from Device? by using Microsoft Endpoint Manager, o		O
App3 can be installed automatically for UserGroupI.	0	O

Answer:

Explanation:

Statements	Yes	No
App1 can be assigned as a required install for User3.	0	
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager,o		O
App3 can be installed automatically for UserGroupI.	0	O

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy

https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy

Question: 87

: 250

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager.

You need to configure the security settings in Microsoft Edge.

What should you create in Microsoft Endpoint Manager?

A. an app configuration policy
B. an app
C. a device configuration profile
D. a device compliance policy

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

Question: 88

HOTSPOT

: 251
HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
Useri	Global admin
User2	*None*
User3	*None*

You provision the private store in Microsoft Store for Business.

You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
Useri	*None*
User2	Purchaser
User3	Basic Purchaser

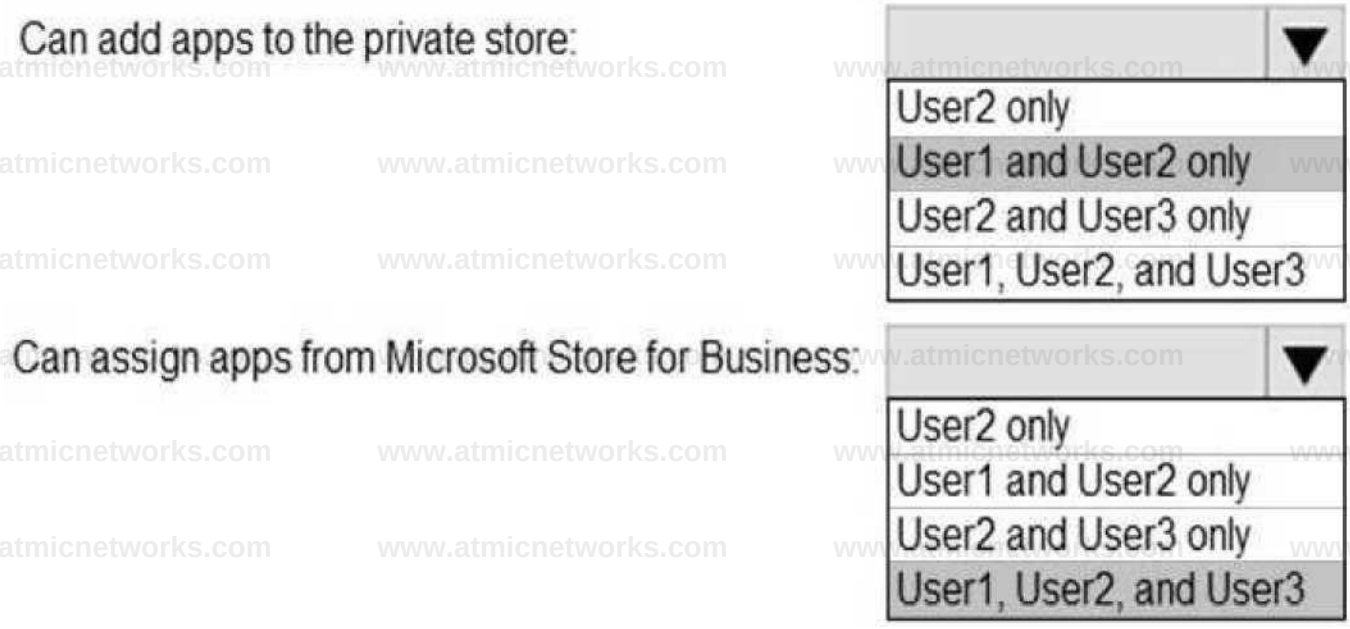
You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for- business#basic-purchaser-role

Question: 89

You have a Microsoft 365 E5 tenant that contains the resources shown in the following table.

Name	Type
Mailbox!	Microsoft Exchange Online mailbox
Account!	Microsoft OneDrive account
Sitel	Microsoft SharePoint Online site
Channel.	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

A. Mailbox1 and Site1 only
B. Mailbox1, Account1, and Site1 only
C. Account1 and Site1 only
D. Mailbox1, Account1, Site1, and Channel1
E. Account1, Site1, and Channel1 only

Answer: E

Explanation:

Reference:

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

Question: 90

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

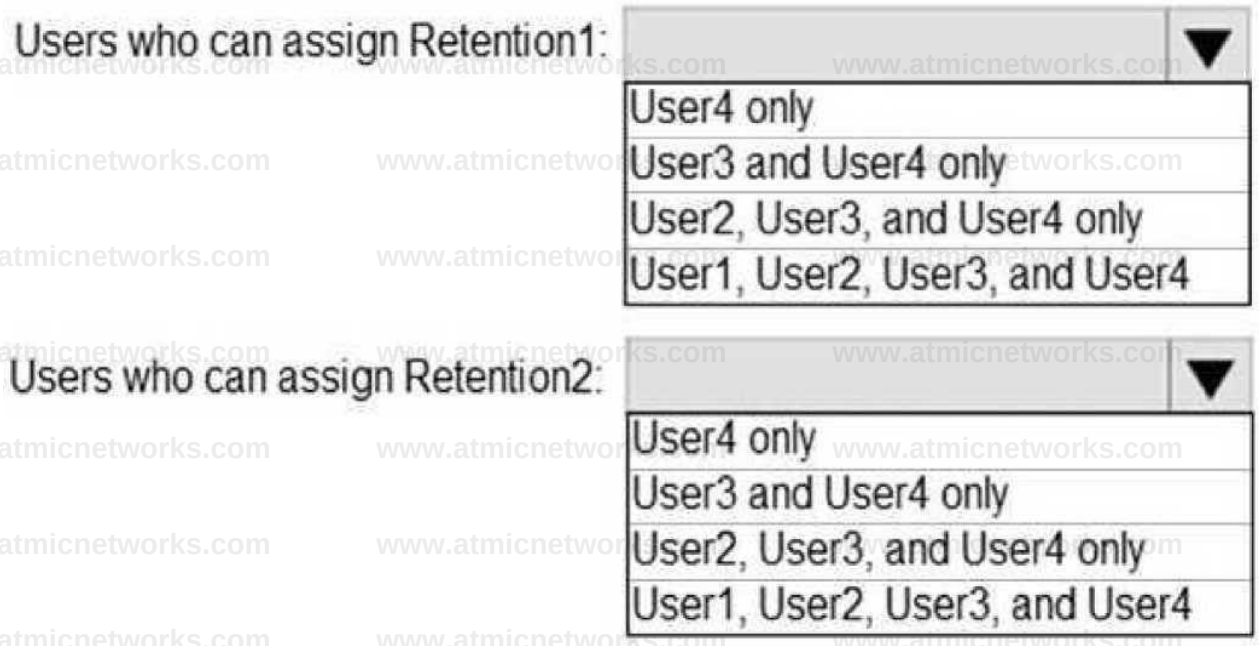
Name	Mailbox size
Used	5 MB
User2	15MB
UserG	25 MB
User4	55 MB

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.

You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.

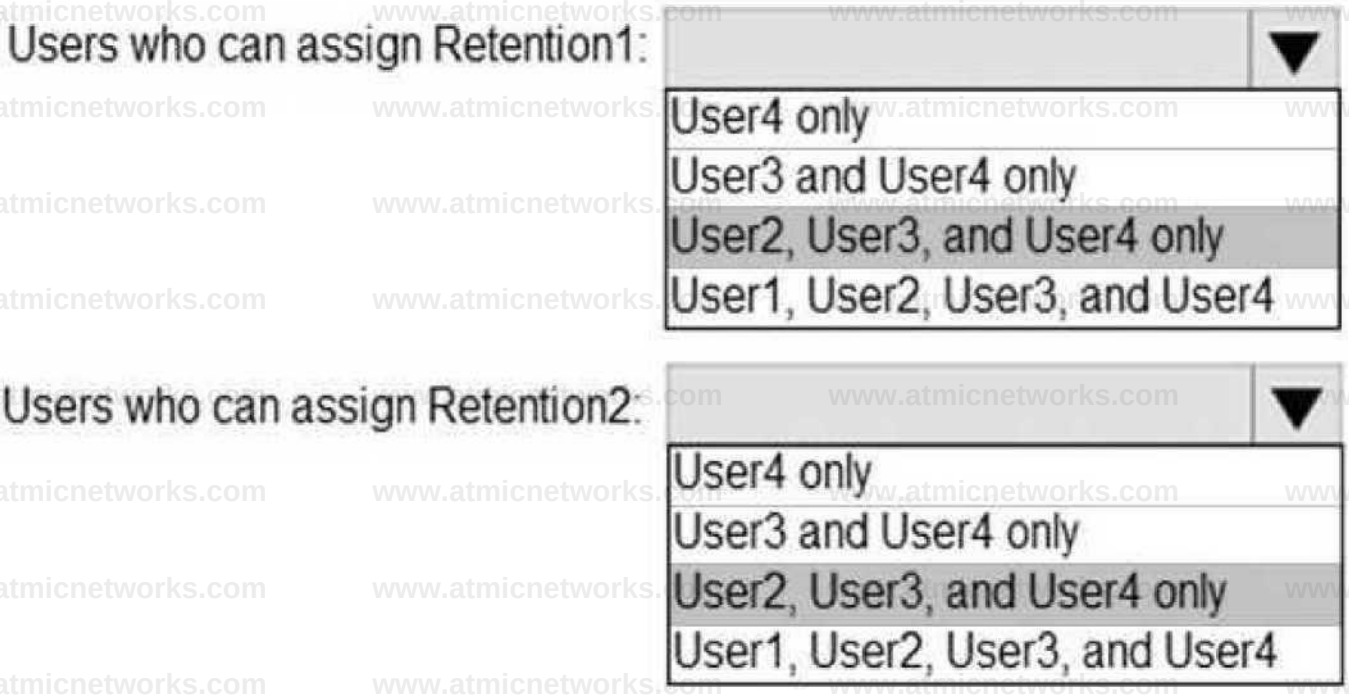
Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:

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

Question: 91

HOTSPOT

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Groupl	Useri
Group2	User2, Groupl

You have a Microsoft Intune enrollment policy that has the following settings:

MDM user scope: Some
Groups: Group1
MAM user scope: Some
Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Useri can enroll Devicel in Intune by using automatic enrollment	O	0
Useri can enroll Device2 in Intune by using automatic enrollment	0	0
User2 can enroll Device2 in Intune by using automatic enrollment	0	0

Answer:

Explanation:

Statements	Yes	No
Useri can enroll Devicel in Intune by using automatic enrollment	O	O
Useri can enroll Device2 in Intune by using automatic enrollment	O	O
User2 can enroll Device2 in Intune by using automatic enrollment	O	O

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

Question: 92

HOTSPOT

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

Deploy a VPN connection by using a VPN device configuration profile.

Configure security settings by using an Endpoint Protection device configuration profile.

You support the management tasks.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Answer:

Explanation:

VPN device configuration profile: Device1, Device2 and Device3

Endpoint Protection device configuration profile: Device1 only

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos

Question: 93

DRAG DROP

You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.

You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.

Which four 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.

Actions	Answer Area
Create an app configuration policy	
Link the account to Intune	
Create a Microsoft account	
Configure a mobile device management (MDM) push certificate	
Add the app	
Create a Google account	
Assign the app	

Answer:

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a- managed-google-play-app-to-android-enterprise-fully-managed-devices

Question: 94

You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager.
To which devices can you deploy Microsoft 365 Apps for enterprise?

A. Device1 only
B. Device1 and Device3 only
C. Device2 and Device4 only
D. Device1, Device2. and Device3 only
E. Device1, Device2, Device3, and Device4

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

Question: 95

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform	Azure Active Directory (Azure AD)
Devicel	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics. Which devices can you monitor by using Endpoint analytics?

A. Device1 only
B. Device1 and Device2 only
C. Device1, Device2, and Device3 only

D. Device1, Device2, and Device4 only

E. Device1, Device2, Device3, and Device4

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/analytics/overview

Question: 96

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.

What should you configure in the profile?

A. Microsoft Defender Credential Guard

B. BitLocker Drive Encryption (BitLocker)

C. Microsoft Defender

D. Microsoft Defender Exploit Guard

Answer: A

Explanation:

Question: 97

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From Device Manager, you view the computer properties.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system- am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

Question: 98

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: At a command prompt, you run the winver.exe command.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system- am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

Question: 99

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select Update & Security to view the update history.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 100

DRAG DROP

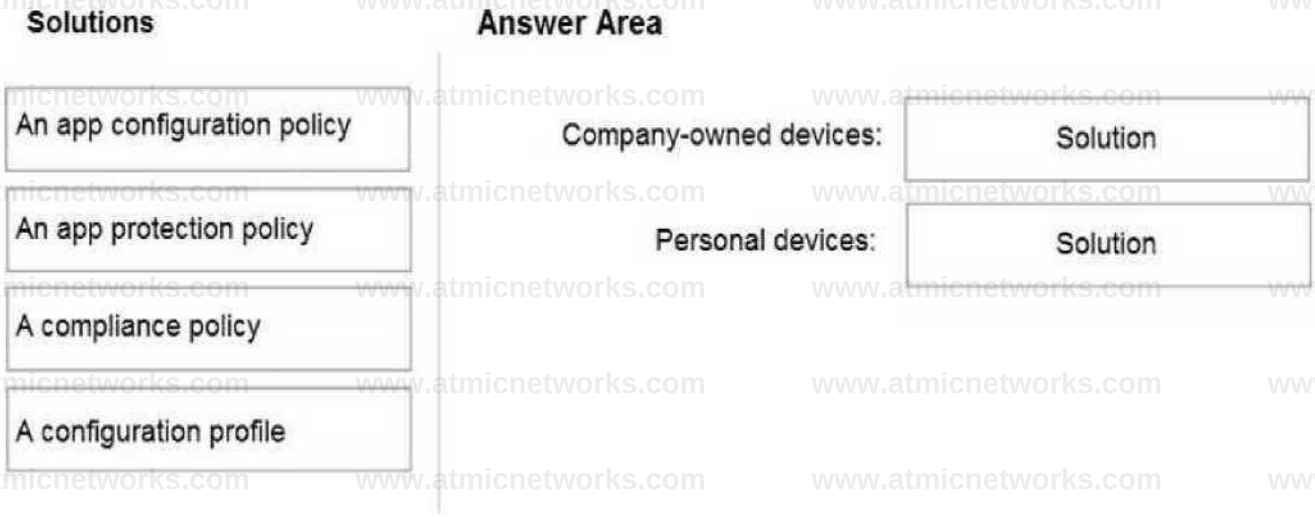
Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Question: 101

HOTSPOT

You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

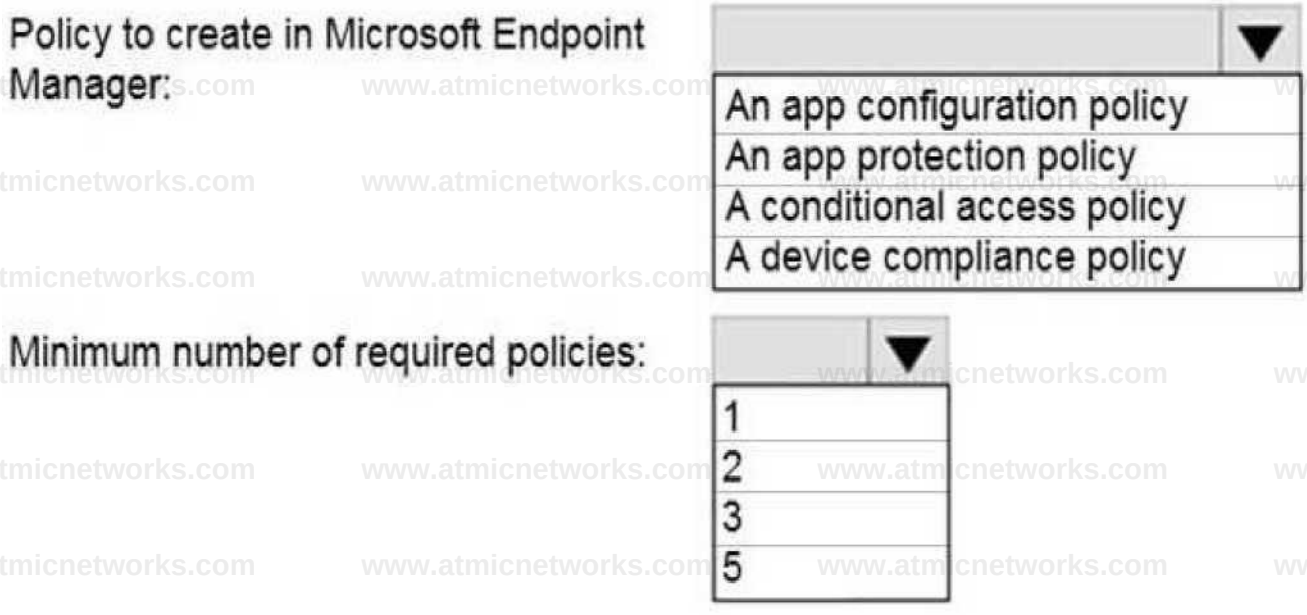
Name	Platform
Device 1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

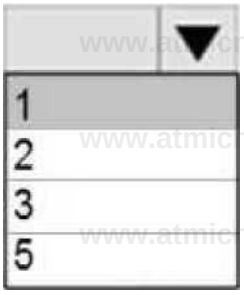


Answer:

Explanation:

Policy to create in Microsoft Endpoint Manager: An app configuration policy
An app protection policy A conditional access policy A device compliance policy

Minimum number of required policies:



Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

Question: 102

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 security center.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

A. Microsoft Cloud App Security
B. Azure Sentinel
C. Azure Web Application Firewall
D. Azure Defender

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

Question: 103

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 security center.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

A. Microsoft Defender for CloudUse the
B. Microsoft Purview
C. Azure Arc
D. Microsoft Defender for Identity

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

Question: 104

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data.

What should you do in the Microsoft 365 compliance center?

A. Create a Data Subject Request (DSR)

B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data

C. Create an assessment based on the EU GDPR assessment template

D. Create an assessment based on the Data Protection Baseline assessment template

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan

Question: 105

You have a Microsoft 365 E5 tenant.

You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.

Which two policies can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a data loss prevention (DLP) policy

B. a sensitivity label policy

C. a Microsoft Cloud App Security file policy

D. a communication compliance policy

E. a retention label policy

Answer: A,D

Explanation:

Question: 106

You have a Microsoft 365 E5 tenant.

You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.

You need to deploy the policy.

What should you do first?

A. Review the sensitive information in Activity explorer
B. Turn on the policy
C. Run the policy in simulation mode
D. Configure Azure Information Protection analytics

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

Question: 107

You have a Microsoft 365 tenant and a LinkedIn company page.

You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.

Where can you store data from the LinkedIn connector?

A. a Microsoft OneDrive for Business folder

B. a Microsoft SharePoint Online document library

C. a Microsoft 365 mailbox

D. Azure Files

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin- data?view=o365-worldwide

Question: 108

HOTSPOT

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.

You deploy a third-party antivirus solution to the devices.

You need to ensure that the devices are marked as compliant.

Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption		
Encryption of data storage on device	Require	
Device Security		
Firewall	Require	
Trusted Platform Module (TPM)	Require	
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimatware	luire	Not configured
Microsoft Defender Antimalware minimum riot configured version		
Microsoft Defender Antimalware security intelligence up-do-date	mire	
Real-time protection	require	Not configured Not configured

Answer:

Explanation:

Windows 10 compliance policy

Windows 10 and later

Encryption		
Encryption of data storage on device	Require	ot conftqure
Device Secunty		
Firewall	Require	^■i il'[1] li i Fi '^»
Trusted Platform Module (TPM)	Require	F Not configured 1
Antivirus	Require	K Not configured J
Antispyware	Require	__^^■J'hFTTiTT^BH^
Defender		
Microsoft Defender Antimalware	^^KSIjns^^HB	Not configured
Microsoft Defender Antimalware minimum N_0(configured version		
Microsoft Defender Antimalware secunty ^^^HL&TTT^^^^^D Not configured |intelligence up-do-date		
Real-time protection	<^HU&>!!I1£^HH*	Not configured

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

Question: 109

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:

Name: AutoLabel1

Label to auto-apply: Sensitivity1

Rules for SharePoint Online sites: Rule1-SPO

Choose locations where you want to apply the label: Site1

Rule1-SPO is configured as shown in the following exhibit.

Edit rule

Name

Rulel-SPO

Description

Rulel description

Conditions

We'll apply this policy to content that matches these conditions.

Content contains sensitive info types

Default All of these

Sensitive info types

IP Address Accuracy 85 to 100 instance count 2 to Any Add x/

Create group

I Add condition

Save **Cancel**

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Sensitivityl is applied to Filel .docx.	O	O
Sensitivityl is applied to File2.txt.	O	0
Sensitivityl is applied to File3.xlsx.	O	O

Answer:

Explanation:

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	O	O
Sensitivity1 is applied to File2.txt.	O	O
Sensitivity1 is applied to File3.xlsx.	O	O

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

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

Question: 110

You plan to use Azure Sentinel and Microsoft Cloud App Security. You need to connect Cloud App Security to

Azure Sentinel.

What should you do in the Cloud App Security admin center?

A. From Automatic log upload, add a log collector.
B. From Automatic log upload, add a data source.
C. From Connected apps, add an app connector.
D. From Security extension, add a SIEM agent.

Answer: D

Explanation:

Question: 111

HOTSPOT

You have a Microsoft 365 ES tenant.
You have the alerts 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

Answer:

Explanation:

Answer Ares

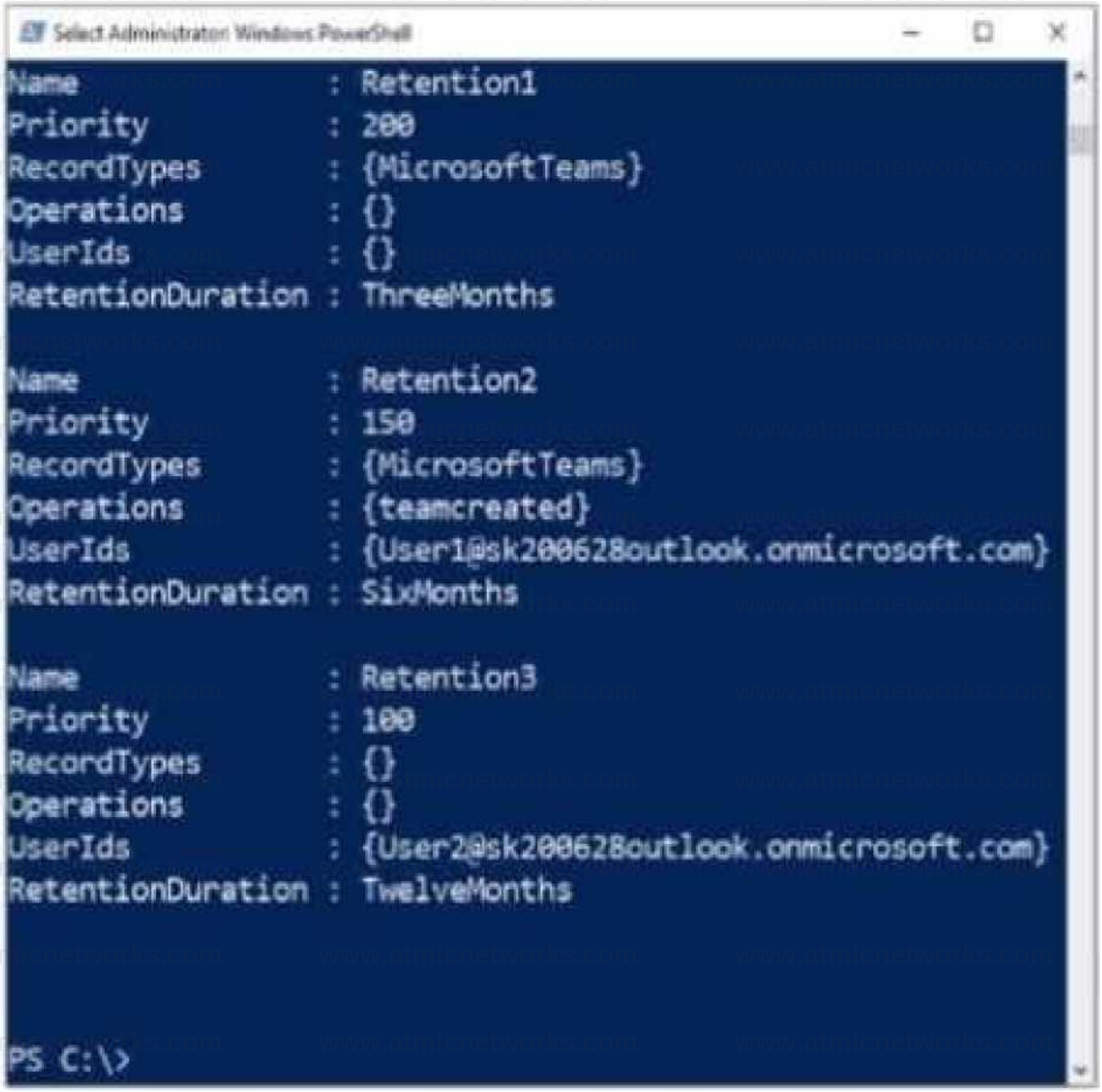
For Alert!, you an chmse Suu to kwntigjtvq only

For Alert), you can not ctwnge SuUn

Question: 112

HOTSPOT

You have a Microsoft 365 ES subscription that has three auto retention policies as show 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

If User1 creates a team in Microsoft Teams, the event is [answer choice].

- not retained
- retained for 90 days
- retained for six months
- retained for one year

If User2 adds a channel in Microsoft Teams, the event is [answer choice].

- not retained
- retained for 90 days
- retained for six months
- retained for one year

Answer:

Explanation:

Answer Area

If User1 creates a team in Microsoft Teams, the event is [answer choice]. retained for six months

If User2 adds a channel in Microsoft Teams, the event is [answer choice]. retained for 90 days

Question: 113

HOTSPOT

You have a Microsoft 365 E5 tenant.

You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.

Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Explanation:

Answer:

Answer Are*

Policy type Alert

Role Security Admen stietor

Question: 114

You have a Microsoft 365 E5 tenant.

industry regulations require that the tenant comply with the ISO 27001 standard.

You need to evaluate the tenant based on the standard

A. From Policy in the Azure portal, select Compliance, and then assign a pokey
B. From Compliance Manager, create an assessment
C. From the Microsoft J6i compliance center, create an audit retention policy.
D. From the Microsoft 365 admin center enable the Productivity Score.

Answer: B

Explanation:

Question: 115

You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.

You need to enable unified labeling for Microsoft 365 groups.

Which cmdlet should you run?

A. set-unifiedGroup
B. Set-Labelpolicy
C. Execute-AzureAdLebelSync
D. Add-UnifiedGroupLinks

Answer: C

Explanation:

Question: 116

You have a Microsoft 365 E5 tenant.

You configure sensitivity labels.

Users report that the Sensitivity button is unavailability in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.

You need to ensure that the users can apply the sensitivity labels when they use Word for the web.

What should you do?

A. Copy policies from Azure information Protection to the Microsoft 365 Compliance center
B. Publish the sensitivity labels.
C. Create an auto-labeling policy
D. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.

Answer: B

Explanation:

Question: 117

You have a Microsoft 365 E5 tenant.

You plan to deploy a monitoring solution that meets the following requirements:

Captures Microsoft Teams channel messages that contain threatening or violent language.
Alerts a reviewer when a threatening or violent message is identified.

What should you include in the solution?

A. Data Subject Requests (DSRs)
B. Insider risk management policies
C. Communication compliance policies
D. Audit log retention policies

Answer: C

Explanation:

Question: 118

Your company has a Microsoft 365 subscription.

you implement sensitivity Doris for your company.

You need to automatically protect email messages that contain the word Confidential m the subject line.

What should you create?

A. a sharing policy from the Exchange admin center
B. a mail flow rule from the Exchange admin center
C. a message Dace from the Microsoft 365 security center
D. a data loss prevention (DLP) policy from the Microsoft 365 compliance center

Answer: B

Explanation:

Question: 119

You have a Microsoft 365 tenant that contains two groups named Group1 and Group2. You need to prevent the members or Group1 from communicating with the members of Group2 by using Microsoft Teams.

The solution must comply with regulatory requirements and must not affect other user in the tenant.

What should you use?

A. information barriers
B. communication compliance policies
C. moderated distribution groups
D. administrator units in Azure Active Directory (Azure AD)

Answer: A

Explanation:

Question: 120

You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

tame	Hnttam
DMttl	MMOS
pMtc^	M^IQM Who for VfafkoUtiois
De-^?	Wrdowc 10 Efuewrise

Dev£e4	ICS
DM^J	AWXrf

You plan to enable VPN access for the devices.
What is the minimum number of configuration policies required?

A. 3
B. 5
C. 4
D. 1

Answer: D

Explanation:

Question: 121

HOTSPOT

You have device compliance policies shown in the following table.

Name	farfwni	AH^nmml
[PgtQI	Window*. 10MO'4ter	Delicti
. **#	Wtncfom ID Md WK	
> ***-.	Wirxfc« ID ana J:^	>VIMZ
W i	Windom ID mcl Mp	. wlcti
s^S ?otocy6	IOS/IPKYS IDS^MOS	>vw3 >vlcri

The device compliance state for each policy is shown in the following table.

Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

NOTE: Each correct selection is worth one point.

Answer Area Statements **Yes No**

Devicel has an oser^s compliance state of Co* pi .ant

Device? hat an over compliance state of Not compfeant

Owe.' lias an OMM* compliancr state of In 91 .• - per 00

Answer:

Explanation:

Answer Area

Statements **Yes No**

! Mwel has an .era# compliance state of Compliant

Device? has anosera* compliance state of Not comphant *

Owe j has an cvera* compliance state of In grace pesca •

Question: 122

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.

You plan to use Endpoint analytics to identify hardware issues.

You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

A. Configure the Endpoint analytics baseline regression threshold.

B. Create a configuration profile.

C. Create a Windows 10 Security Baseline profile

D. Create a compliance policy.

Answer: B

Explanation:

Question: 123

HOTSPOT

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.

In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

Device limit restrictions

Defin* how many tfwcw wh uwr tMi enroll

Priority	Name	Devito limit
Default	All then	2

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM). For each of the following statement, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Userl can enrol ore, fee devices m lr r.ne		
Userl can join only fee devices to Azure AD		
Uteri can enrol al me devices in intune		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Usefl can enec<l only fee devices in Irrune	•	
Userl can foes only Ive devrces to Anae AD	•	
Uteri can enrol al the oevices In intune	•	

Question: 124

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles.

Which platform can you manage by using the profile?

A. Android
B. CentOS Linux
C. iOS
D. Window 10

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

Question: 125

You purchase a new computer that has Windows 10, version 2004 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

A. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.

B. install the West feature update and the latest quality update only.

C. install all the feature updates released since version 2004 and the latest quality update only.

D. install the latest feature update and all the quality updates released since version 2004.

Answer: B

Explanation:

Question: 126

HOTSPOT

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
Useri	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.

The Products & services settings in Microsoft Store for Business are shown in the following

exhibit.

Microsoft Remote Desktop

Free • Online ♦ Product Details

Install

Licenses

Unlimited licenses

0 used

Billing

€0.00 (Free app)

Settings & Actions

Not in private store

More actions available on details page

Excel Mobile

Free • Online • Product Details

Install

Licenses

Unlimited licenses

0 used

Billing

€0.00 (Free app)

Settings & Actions

In private store

Mote actions available on details page

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	O	O
Useri can install the Microsoft Remote Desktop app from Microsoft Store for Business	O	O
User4 can manage the Microsoft Remote Desktop app from the private store.	O	O

Answer:

Explanation:

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store	O	O
Useri can install the Microsoft Remote Desktop app from Microsoft Store for Business	O	O
User4 can manage the Microsoft Remote Desktop app from the private store	O	O

Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for- business

Question: 127

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select System, and then you select About to view information about the system.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Reference:

https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system- am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

Question: 128

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

Name	Severity	Status	Comment	Category
Alertl	Medium	Active	Commentt	Threat management
Alert2	Low	Resolved	Comment2	Other

Which properties of the alerts can you modify?

A. Status only
B. Status and Comment only
C. Status and Severity only
D. Status, Severity, and Comment only
E. Status, Severity, Comment and Category

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update- alert?view=o365-worldwide#limitations

Question: 129

DRAG DROP

Your company purchases a cloud app named App1.

You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.

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.

Actions

Deploy Azure Active Directory (Azure AD) Application Proxy.

From the Cloud App Security admin center, add an app connector

SignintoAppl

Create a conditional access policy.

From the Azure Active Directory admin center, configure the Diagnostic settings.

From the Azure Active Directory admin center, add an app registration for Appl

Answer Area

Answer:

Explanation:

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security

Question: 130

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.

Devices are onboarded by using Microsoft Defender for Endpoint.

You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.

What should you create first?

A. a device configuration policy
B. a device compliance policy
C. a conditional access policy
D. an endpoint detection and response policy

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

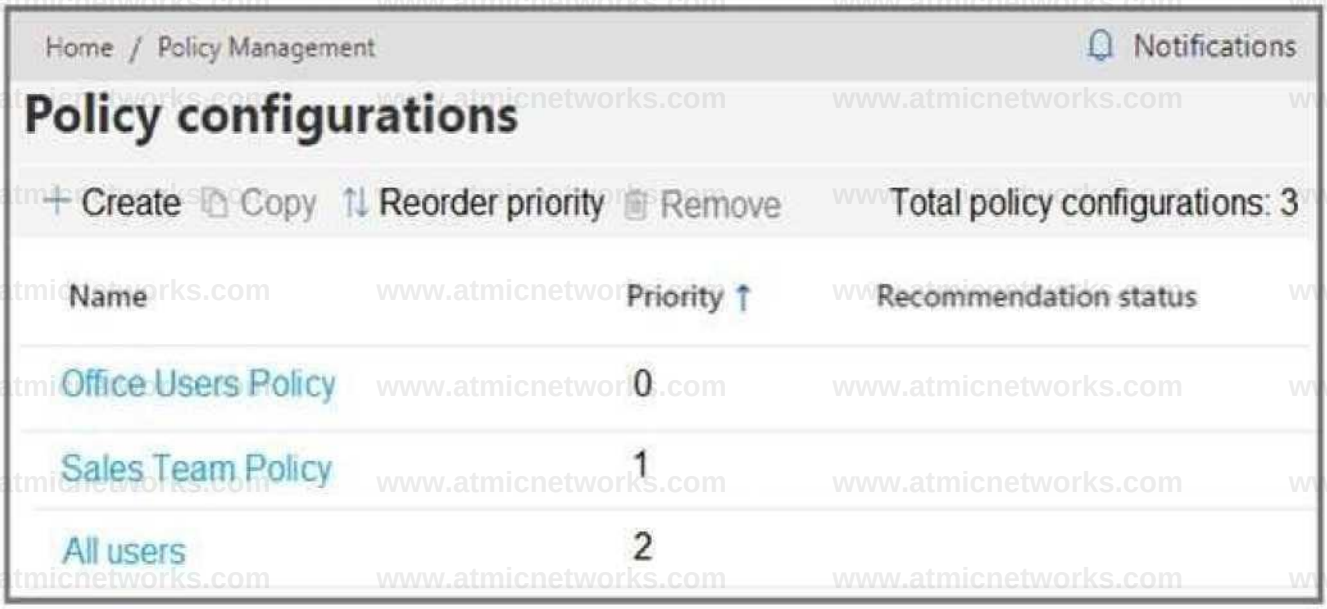
Question: 131

HOTSPOT

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

Name	Member of
Userl	All users, Sales team
User2	All users, Office users

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following exhibit.



The policies use the settings shown in the following table.

Policy	Default Shared Folder Location	Default Office Theme
All users	https //sharepoint contoso com/addins_all_users	Colorful
Office Policy	https //sharepoint contoso com/addms_office_users Users	White
Sales Team Policy	https //sharepoint contoso com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The default shared folder location for Userl is: ,

https sharepoint contoso com addins_all_users https://sharepoi
nt contoso com/addi ns_offi ce_users
https//sharepoint contoso.com/addins sales team users

The default Office theme for User 2 is: ▼

Colorful Dark Gray White

Answer:

Explanation:

The default shared folder location for Useri is: 1

https://sharepoint.contoso.com/addins_all_users
https://sharepointcontoso.com/addins_office_users
https //sharepoint contoso com/addins sales team users

The default Office theme for User 2 is: ▼

Colorful
Dark Gray
White

Reference:

https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

Question: 132

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.

From Microsoft Defender Security Center, you perform a security investigation.

You need to run a PowerShell script on the device to collect forensic information.

Which action should you select on the device page?

A. Initiate Live Response Session
B. Initiate Automated Investigation
C. Collect investigation package
D. Go hunt

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

Question: 133

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft 365 compliance policies to meet the following requirements:

Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
Report on shared documents that contain PII.

What should you create?

A. an alert policy
B. a data loss prevention (DLP) policy
C. a retention policy
D. a Microsoft Cloud App Security policy

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365- worldwide

Question: 134

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Useri	Groupi, Group2
User2	Group?, Group3
User3	Groupi, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policyl	0	Groupi
Policy?	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policyl	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Used has their cache cleared on close.	O	O
User? has Cursor movement set to Visual.	Q	Q
User3 has Cursor movement set to Visual.	O	O

Answer:

Explanation:

Statements	Yes	No
User1 has their cache cleared on close.	O	O
User2 has Cursor movement set to Visual.	O	O
User3 has Cursor movement set to Visual.	O	O

Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

Question: 135

You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?

A. an attack surface reduction (ASR) policy
B. an app configuration policy

C. a device compliance policy
D. a device configuration profile

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

Question: 136

You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.

You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.

Which policy type should you configure?

A. conditional access
B. account protection
C. attack surface reduction (ASR)
D. Endpoint detection and response

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Question: 137

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policyl	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.

Which policy settings will be applied to Device1?

A. only the settings of Policy1
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Answer: D

Explanation:

Question: 138

HOTSPOT

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

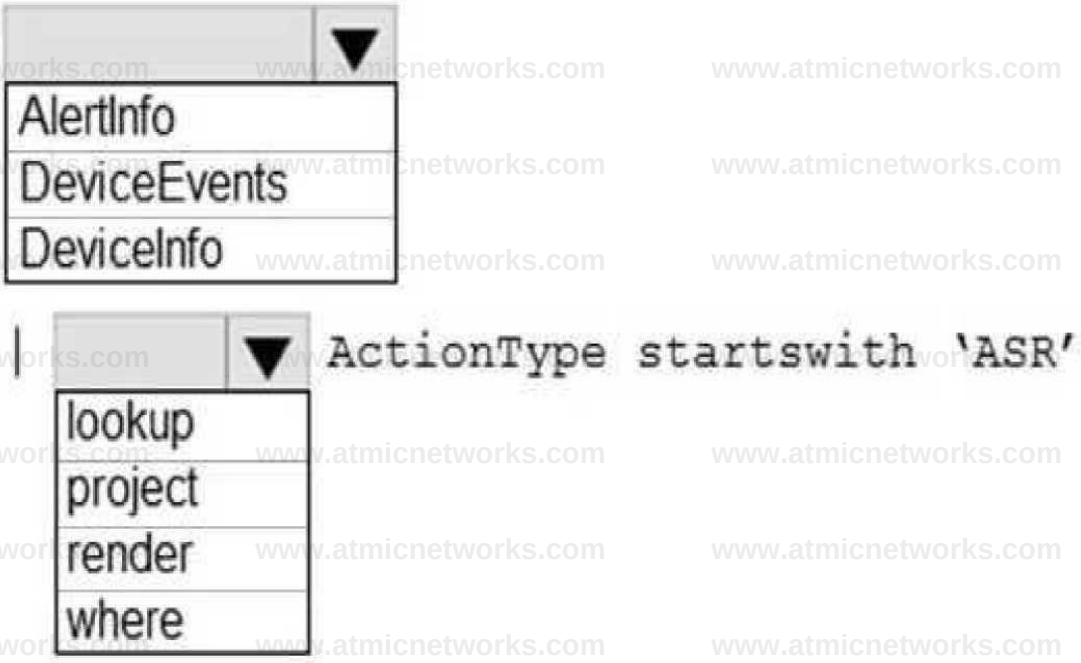
You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.

You need to find the ASR rules that match the activities on the devices.

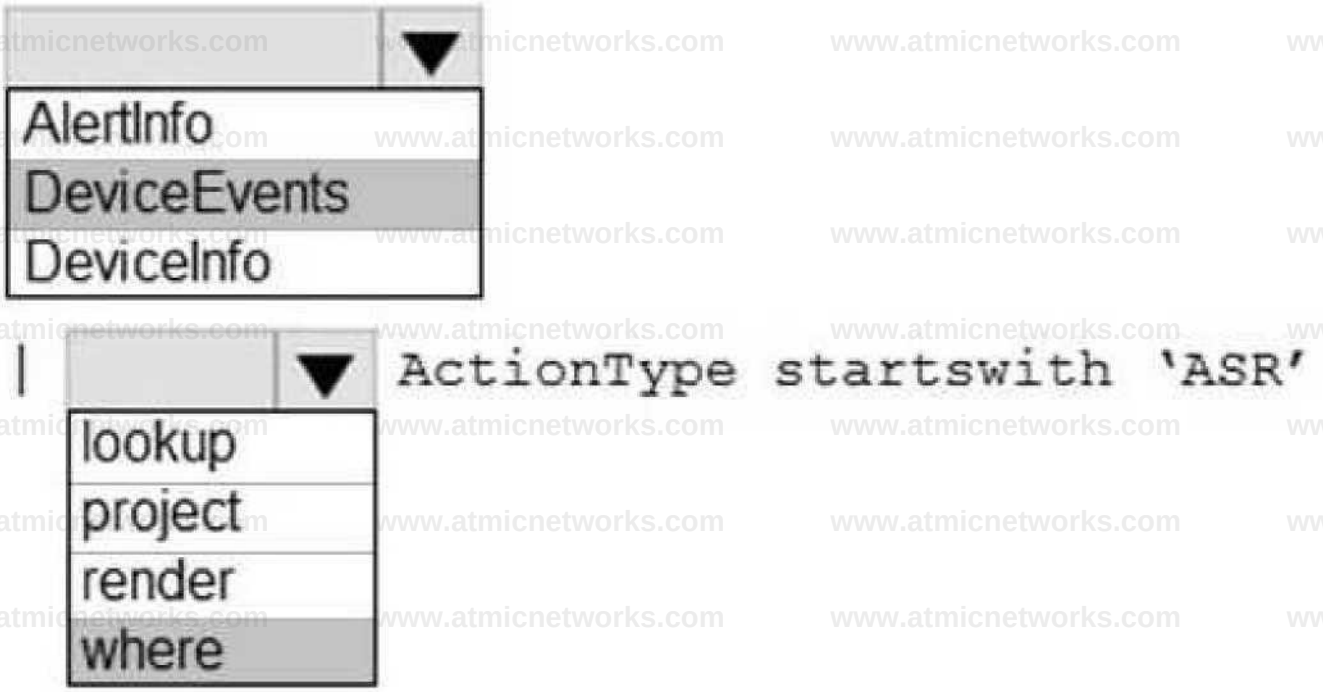
How should you complete the Kusto query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying- attack-surface-reduction-rules-part-3/ba-p/1360968

Question: 139

HOTSPOT

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows8.1
Devices	iOS
Device4	Android

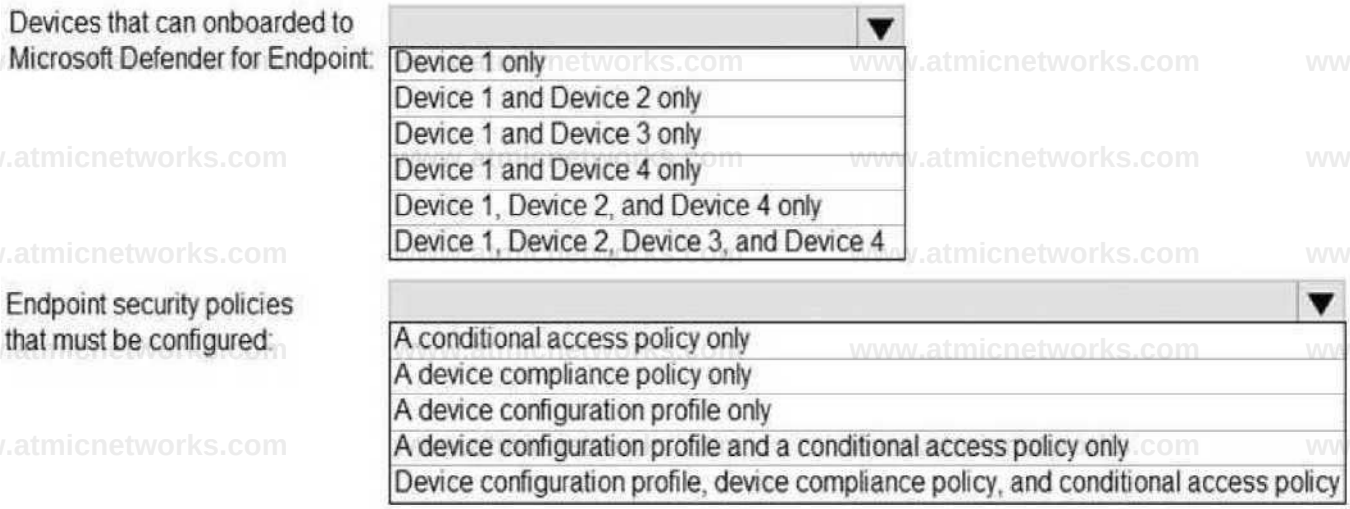
You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant.

Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

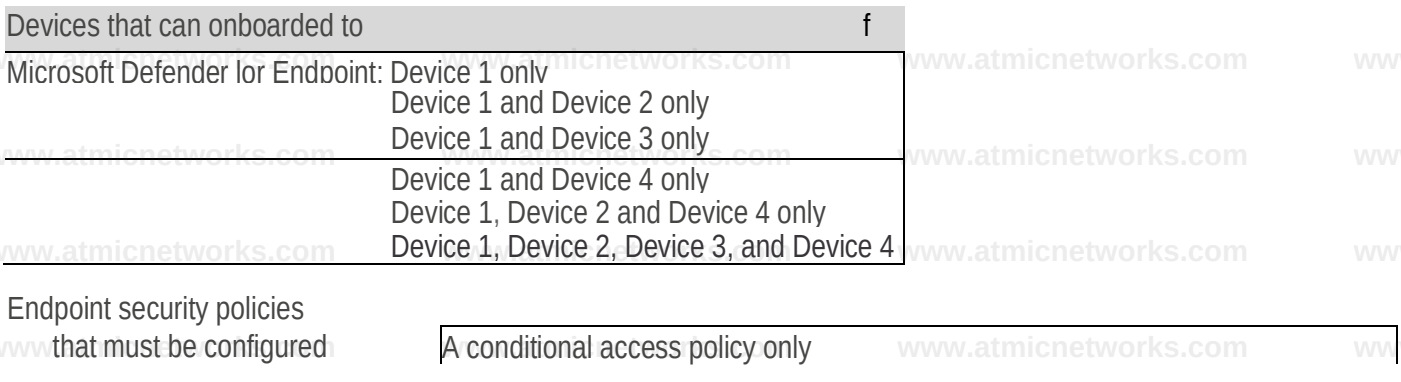
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



A device compliance policy only
A device configuration profile only
A device configuration profile and a conditional access policy only
Device configuration profile device compliance policy, and conditional access

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure- machines-onboarding?view=o365-worldwide

Question: 140

You have a Microsoft 365 E5 tenant that contains a user named User1.

You plan to implement insider risk management.

You need to ensure that User1 can perform the following tasks:

Review alerts.
Manage cases.
Create notice templates.
Review user emails by using Content explorer.

The solution must use the principle of least privilege.

To which role group should you add User1?

A. Insider Risk Management
B. Insider Risk Management Analysts
C. Insider Risk Management Investigators
D. Insider Risk Management Admin

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management- configure?view=o365-worldwide

Question: 141

Your company has a Microsoft 365 E5 tenant that contains a user named User1.

You review the company's compliance score.

You need to assign the following improvement action to User1:Enable self-service password reset.

What should you do first?

A. From Compliance Manager, turn off automated testing.
B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users- assign-role-azure-portal

Question: 142

Your company has a Microsoft E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard.

You need to assess the company's current state of compliance.

What should you use?

A. eDiscovery
B. Information governance
C. Compliance Manager
D. Data Subject Requests (DSRs)

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

Question: 143

You have a Microsoft 365 E5 tenant.

Users store data in the following locations:

Microsoft Teams
Microsoft OneDrive
Microsoft Exchange Online
Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

A. 1
B. 2
C. 3
D. 4

Answer: C

Explanation:

Reference:

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

Question: 145

You have a Microsoft 365 E5 tenant.

You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.

You need to export the existing template.

Which file format should you use for the exported template?

A. CSV
B. XLSX
C. JSON
D. XML

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template

Question: 146

You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.

Company policy requires that the devices have the following configurations:

Require complex passwords.

Require the encryption of removable data storage devices.

Have Microsoft Defender Antivirus real-time protection enabled.

You need to configure the devices to meet the requirements.

What should you use?

A. an app configuration policy

B. a compliance policyC a security baseline profileD a conditional access policy

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Question: 147

HOTSPOT

You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group 1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a compliance policy named Compliance1.

You need to identify the groups that meet the following requirements:

Can be added to Compliance1 as recipients of noncompliance notifications

Can be assigned to Compliance1

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

Answer:

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

- Group1 and Group4 only
- **Group3 and Group4 only**
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- **Group1, Group3, and Group4 only**
- Group1, Group2, Group3, and Group4

Reference:
https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in- microsoft-endpoint-manager-intune/

Question: 148

HOTSPOT

You have a Microsoft 365 E5 tenant.

You configure a device compliance policy as shown in the following exhibit.

Compliance settings Edit

Microsoft Defender ATP

Require the device to be at or under the machine risk score.	Low

Device Health

Rooted devices	Block
Require the device to be at or under the Device Threat Level	

System Security

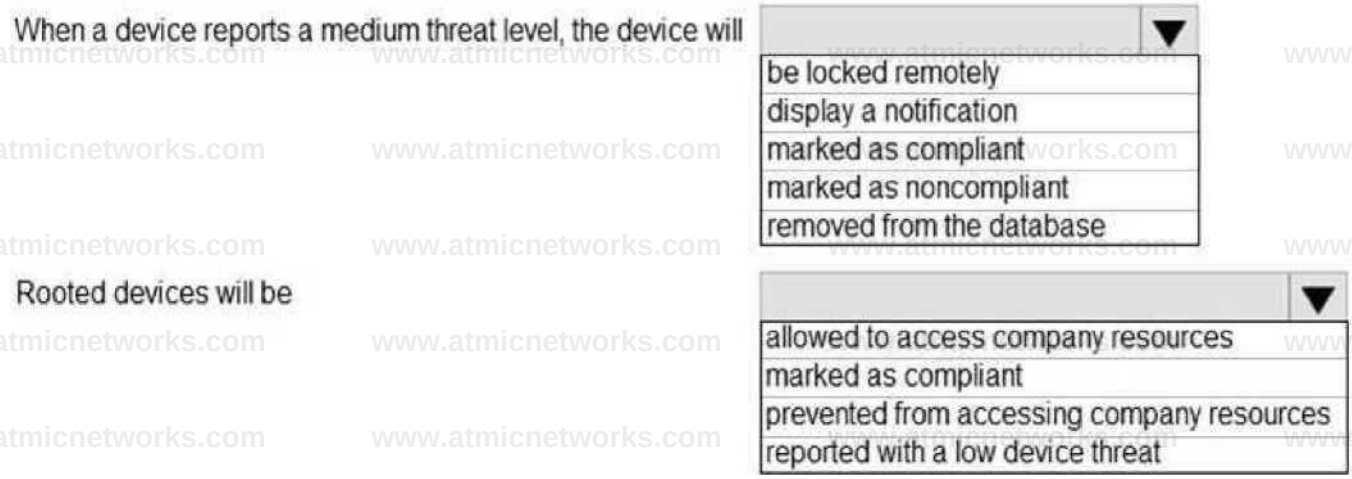
Require a password to unlock mobile devices	Require
Required password type	Device default
Encryption of data storage on device.	Require
Block apps from unknown sources	Block

Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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:

Explanation:

When a device reports a medium threat level, the device will

be locked remotely display a notification marked as compliant marked as noncompliant removed from the database

Rooted devices will be

allowed to access company resources ___ marked as compliant prevented from accessing company resources reported with a low device threat

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android

Question: 149

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

When users attempt to apply Retention1, the label is unavailable.

You need to ensure that Retention1 is available to all the users.

What should you do?

A. Create a new label policy

B. Modify the Authority type setting for Retention!

C. Modify the Business function/department setting for Retention 1.

D. Use a file plan CSV template to import Retention1.

Answer: A

Explanation:

Reference:

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

Question: 151

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Devicel	Windows 10 Pro	Registered	Microsoft Intune
Device?	Windows 10 Enterprise	Joined	Microsoft Intune
Devices	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Devices	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.

You plan to create a policy to show only the private store in Microsoft Store for Business.

To which devices can the policy be applied?

A. Device2 only
B. Device1 and Device3 only
C. Device2 and Device4 only
D. Device2, Device3, and Device5 only
E. Device1, Device2, Device3, Device4, and Device5

Answer: C

Explanation:

Question: 152

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You have devices enrolled in Intune as shown in the following table.

Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1, Group3	Tag1
Device2	Android	Group2	Tag2

You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profilel	Windows 10 and later	Groupi	Groups	Tag1, Tag?
Profile?	Android Enterprise	All devices	Group?	Tag1, Tag?
Profiles	Android Enterprise	Group?, GroupS	GroupS	Tag1
Profile4	Windows 10 and later	Groups	None	Default

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Device1:

- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device2:

- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

Answer:

Explanation:

Device1:

- No profiles
- Profile1 only
- Profile4 only
- **Profile1 and Profile4 only**
- Profile1, Profile1, and Profile4 only

Device2:

- No profiles
- Profile1 only
- Profile2 only
- **Profile3 only**
- Profile1 and Profile2 only
- Profile2 and Profile3 only

Question: 153

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune.
What should you create?

A. scope tags
B. device configuration profiles
C. device categories
D. device compliance policies

Explanation:

Answer: C

Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

Question: 154

HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
Useri	Application administrator	Basic Purchaser	Groupl
User2	None	Purchaser	Group2
User3	None	Basic Purchaser	Group3

You perform the following actions:

Provision the private store in Microsoft Store for Business.
Add an app named App1 to the private store.
Set Private store availability for App1 to Specific groups, and then select Group3.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No

Useri can install	App1	from the private	store.	O O
User2 can install	App1	from the private	store.	O O
User3 can install	App1	from the private	store.	O O

Answer:

Explanation:

Statements				Yes	No
Useri can install	App1	from the private	store.	O	O
User2 can install	App1	from the private	store.	O	O
User3 can install	App1	from the private	store.	O	O

Reference:
https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store- for-business#private-store-availability

Question: 155

Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?

A. scope tags

B. configuration profiles

C. device categories

D. conditional access policies

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

Question: 156

HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

Show app and profile configuration progress: Yes

Allow users to collect logs about installation errors: Yes

Only show page to devices provisioned by out-of-box experience (OOBE): No Assignments: 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.

Statements	Yes	No
If Useri enrolls Devicel in Microsoft Endpoint Manager, the enrollment status page will appear.	O	O
If User2 enrolls Devicel in Microsoft Endpoint Manager, the enrollment status page will appear.	O	O
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	O	O

Answer:

Explanation:

Statements	Yes	No
If Useri enrolls Devicel in Microsoft Endpoint Manager, the enrollment status page will appear.	O	O
If User2 enrolls Devicel in Microsoft Endpoint Manager, the enrollment status page will appear.	O	O
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	O	O

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

Question: 157

You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group!	Distribution
Group?	---------- 1
Groups	Security

You plan to create a new Windows 10 Security Baseline profile.

To which groups can you assign to the profile?

A. Group3 only
B. Group1 and Group3 only
C. Group2 and Group3 only
D. Group1. Group2. and Group3

Answer: A

Explanation:

Reference:

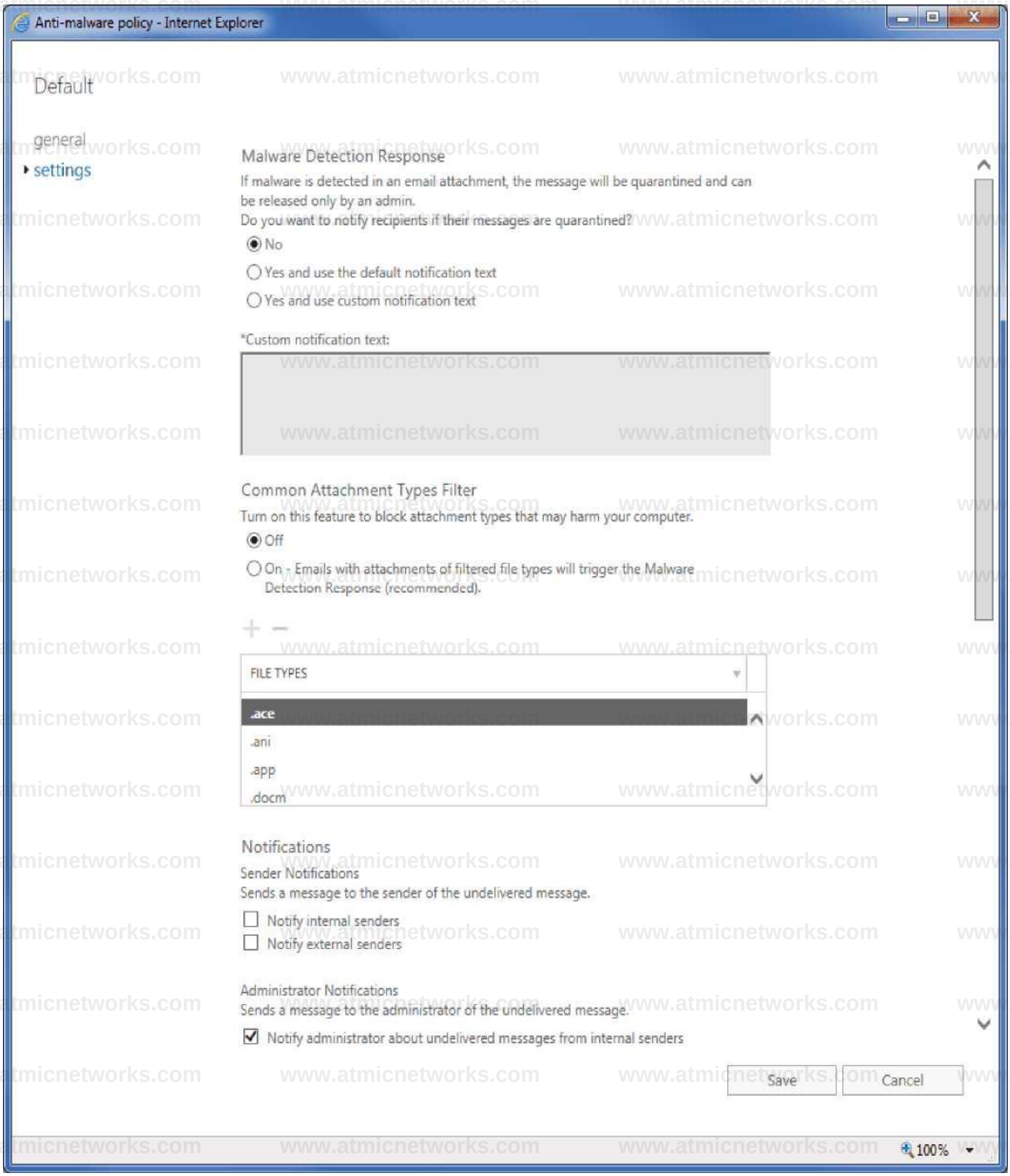
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the- profile

https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare- groups?view=o365-worldwide

Question: 158

You have a Microsoft 365 E5 subscription that contains a user named User1.

The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.

How will the email message and the attachments be processed?

A. Both attachments will be removed. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'

B. The email message will be quarantined, and the message will remain undelivered.

C. Both attachments will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed."

D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

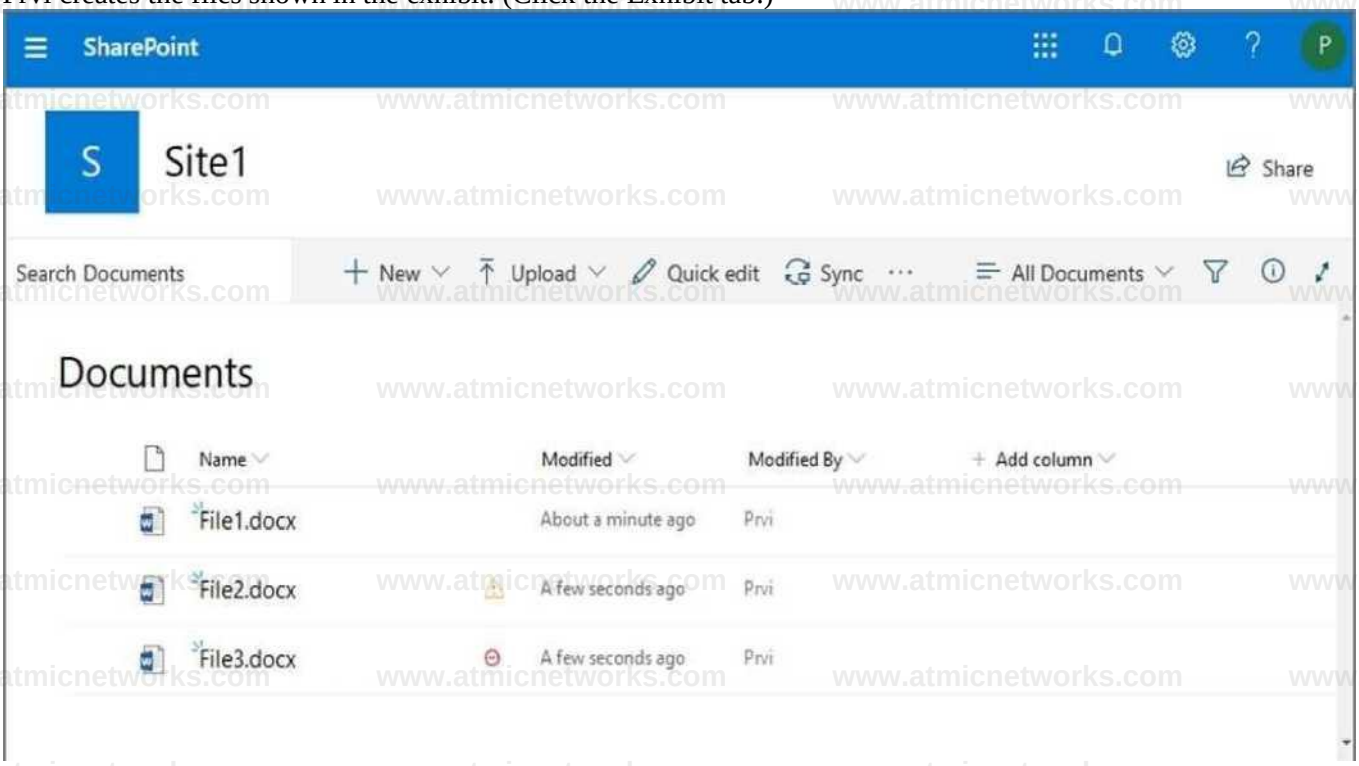
Question: 159

HOTSPOT

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	Useri
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Useri:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

Answer:

Explanation:

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

Reference:
https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/
https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

Question: 160

You have a Microsoft 365 E5 tenant.
The Microsoft Secure Score for the tenant is shown in the following exhibit.

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

4 Export 12 items P Search T Filter (= Group by

Applied filters:

Rank 0	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	♦16.95%	0/10
2	Ensure all users can complete multi-factor authentication for...	+1525%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+ 11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	♦ 1.69%	0/1

You plan to enable Security defaults for Azure Active Directory (Azure AD).

Which three improvement actions will this affect?

A. Require MFA for administrative roles.
B. Ensure all users can complete multi-factor authentication for secure access
C. Enable policy to block legacy authentication
D. Enable self-service password reset
E. Use limited administrative roles

Answer: A,B,C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals- security-defaults

Question: 161

You have a Microsoft 365 E5 subscription.

You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.

What should you do?

A. From the Cloud App Security admin center, select Users and accounts.
B. From the Microsoft 365 security center, view the Threat tracker.
C. From the Microsoft 365 admin center, view the Security & compliance report.
D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Answer: A

Explanation:

Question: 162

HOTSPOT

You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.

You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen.

Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ASR1:

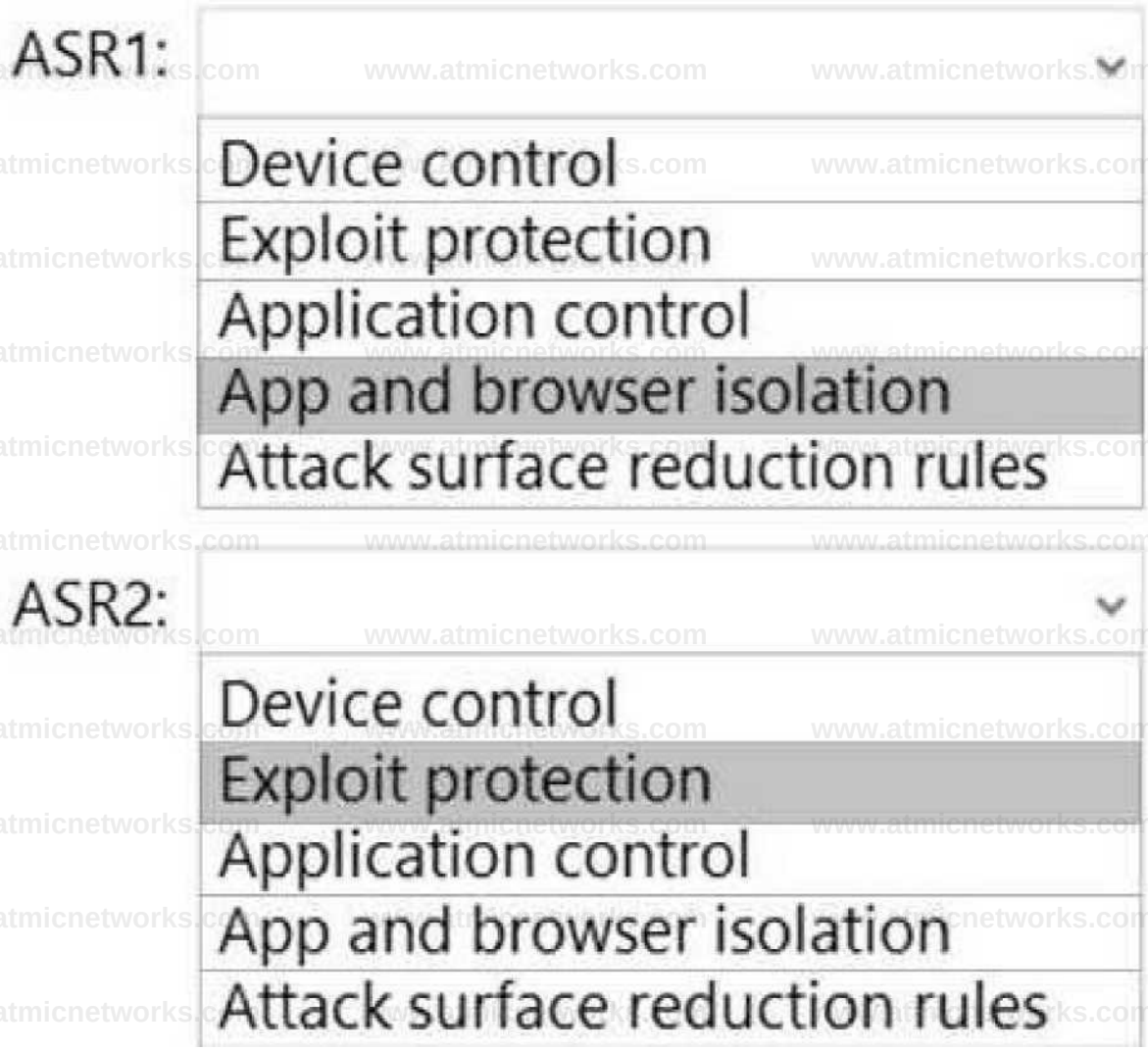
Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

ASR2:

Device control Exploit protection
Application control App and browser isolation Attack surface reduction rules

Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy

Question: 163

HOTSPOT

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	**15444**	**Incomplete**	**72%**	**3 of 450 completed**	**887 of 887 completed**	**Group1**	**Microsoft 365**	**NIST 800 53**
Data Protection Baseline	**14370**	**Incomplete**	**70%**	**3 of 489 completed**	**835 of 835 completed**	**Group2**	**Microsoft 365**	**Data Protection Baseline**

The SP800 assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	**None**	**+9 points**	**0/9**	**NIST 800-53, Data Protection Baseline**
Establish and document a configuration management	**None**	**+9 points**	**0/9**	**NIST 800-53, Data Protection Baseline**

You perform the following actions:

For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment	0	0
The SP800 assessment score will increase by 54 points.	O	O
The Data Protection Baseline score will increase by 9 points.	O	O

Answer:

Explanation:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	O	O
The SP800 assessment score will increase by 54 points.	B	1° I o S
The Data Protection Baseline score will increase by 9 points.		

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager- assessments?view=o365-worldwide#create-assessments

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score- calculation?view=o365-worldwide#action-types-and-points

Question: 164

You have a Microsoft 365 tenant.

Company policy requires that all Windows 10 devices meet the following minimum requirements:

Require complex passwords.
Require the encryption of data storage devices.
Have Microsoft Defender Antivirus real-time protection enabled.

You need to prevent devices that do not meet the requirements from accessing resources in the tenant.

Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a configuration policy
B. a compliance policy
C. a security baseline profile
D. a conditional access policy
E. a configuration profile

Answer: B,D

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Question: 165

You have a Microsoft 365 E5 tenant.

You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.

Which policy should you use?

A. a retention policy
B. a retention label policy
C. an auto-labeling policy
D. an insider risk policy

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

Question: 166

DRAG DROP

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to automatically label the documents on Site1 that contain credit card numbers.

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.

Actions

Create a sensitivity label.

Create an auto-labeling policy.

Create a sensitive information type.

Wait 24 hours, and then turn on the policy.

Publish the label.

Create a retention label.

Wait eight hours, and then turn on the policy.

Answer Area

Answer:

Explanation:

Create a sensitivity label

Publish the label.

Create an auto-labeling policy

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365- worldwide#what-label-policies-can-do

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

Question: 167

HOTSPOT

You have a Microsoft 365 tenant that contains the compliance policies shown in the following table.

Name	Require BitLocker	Require the device to be at or under the machine risk score
Policyl	Required	High
Policy?	Not configured	Medium
Policy?	Required	Low

The tenant contains the devices shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Devicel	Configured	High	Policyl, Policy?
Device?	Not configured	Medium	Policy?, Policy?
Device?	Not configured	Low	Policyl, Policy?

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

Statements	Yes	No
Devicel is marked as compliant.	O	O
Devices is marked as compliant	O	O
Devices is marked as compliant.	O	O

Answer:

Explanation:

Statements	Yes	No
Devicel is marked as compliant.	O	O
Device2 is marked as compliant.	O	O
Devices is marked as compliant.	O	O

Question: 168

DRAG DROP

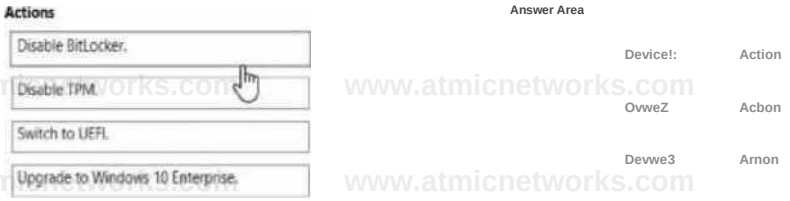
You have a Microsoft 365 subscription.

You have the devices shown in the following table.

Name	TPM version	Operating system	WO5/UEFI	Miocker Drive Encryption (Miocker)
Devicel	[PM U	Windom 10 Pro	BIOS	trebled
Device?	TPM?	Windows 10 Home	RIOS	**Not applicable**
Device 3	TPM?	Windows 8 1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD)

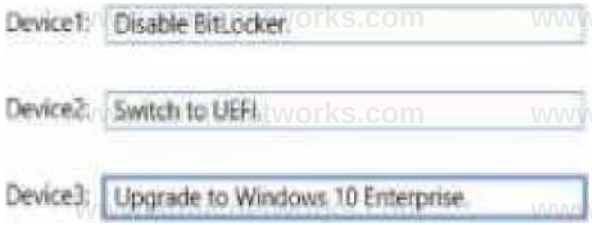
What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area



Question: 169

HOTSPOT

Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.

You plan to implement co-management.

You need to configure Azure AD Connect and the domain to support co-management.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To configure Azure AD Connect: B
Configure hyond Azure AD join Fnahle device wmeback.
Cnacie passviord hash iynclypniation

To configure the domain: I
Add an alternative UPN suffix
Register a service connection point
Register a service pinmpai iwe H'M

Answer:

Explanation:

Answer Area

To configure Azure AD Connect: Enable password hash syncnronizabon

To ronAgun* #w domain Adil an altamatiw UPN wfh«

Question: 170

You have a Microsoft 365 E5 subscription that uses Microsoft intune.

in the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices,
You enable device clean-up rules

What can you configure as the minimum number of days before a device a removed automatically?

A. 10
B. 30
C. 45
D. 90

Answer: D

Explanation:

Question: 171

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

- Retention period 7 years
- Start the retention period bated on: When items were created

You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

A. Retain items even If users delete
B. Mark items as a record
C. Mark items as a regulatory record
D. Retain items forever

Answer: B

Explanation:

Question: 172

HOTSPOT

You have several devices enrolled in Microsoft Endpoint Manager

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown In the following table.

Name	Role	
Used UwP	Cloud Own jdmiHtetii>lur Inline artmf nr ft iter	GroupA GmupR
Uw3	Nene	None

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

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager
For each of the following statements, select Yes if the statement is true. Otherwise, select No

Answer Area Statements	Yes	No
Uteri can enroll a maximum of 10 devices in Endpoint Manager.		
Uteri can enroll a maximum ol 10 devices in Endpoint Manager		
Uteri can enroll an unlimited number of devices In Endpoint Manager		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Uteri can enroll a maximum of 10 devices in [nopoint Manager	•	
UMI2 can enroll a maximum of 10 devices m Endpoint Manager.	j •	
Uteri can enroll an unlimited numbet of devices in Endpoint Manager •		

Question: 173

HOTSPOT

Your company has a Microsoft 365 tenant
You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)
The device type restriction 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 restriction are configured as shown in the following table.

Priority	Nome	Device limit	A tinned to
	Lntj meeting	IS	blunter trig
2	West Region		toy inccr trig
Ddduli	All users	10	AH users

Answer Area

Answer:

Explanation:

Answer Area

Device limit 15

Allowed platform Android only

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change- enrollment-restriction-priority

Question: 174

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

You need to ensure that Used can place a hold on all mailbox content.
What permission should you assign to User1?

A. the Information Protection administrator ide from the Azure Active Directory admin center.

B. the eDiscovery Manager tote from the Microsoft 365 compliance center.

C. the Compliance Management role from the Exchange admin center.

D. the User management administrator role from the Microsoft 365 admin center.

Answer: B

Explanation:

Question: 175

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 176

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com.

You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	**None**
User2	Defender for Identity Contoso Users	**None**
User3	**None**	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User3 to modify the Defender for identity sensor configuration.

Does this meet the goal?

A. Yes

8. No

Answer: A

Explanation:

Question: 177

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com.

You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User1 to modify the Defender for identity sensor configuration.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 178

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com.

You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

N*™	Member of group	Azure AD role

I Isol	**Deform for Wentrty Certoso AdmmistrAlflK**	**None**
	Mehdi* (dr Watty Carton Umi	**No nr**
Ubp|3	**Nene**	S«juiitj admwiialrJLui
U«r4	['- 'ondof f'-r den*'y fCTTCSO I ^an Gkbal rlmm^rra' - ■	

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User4 to modify the Defender for identity sensor configuration.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 179

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

A. Ubuntu Linux

B. macOS

C. iOS

D. Android

Answer: B

Explanation:

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices

Note:

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

Windows 10

macOS

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

Android Enterprise
Windows 8.1

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

Question: 180

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 E5 subscription that contains a user named User1.

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

Question: 181

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 E5 subscription that contains a user named User1.

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

Question: 182

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 E5 subscription that contains a user named User1.

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

Question: 183

HOTSPOT

You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.

How do you want the alert to be triggered?

O Every time an activity matches the rule

Q When the volume of matched activities reaches a threshold

More than or equal to 15 activities

During the last 60 minutes

On All users v

(•) When the volume of matched activities becomes unusual

On All users v

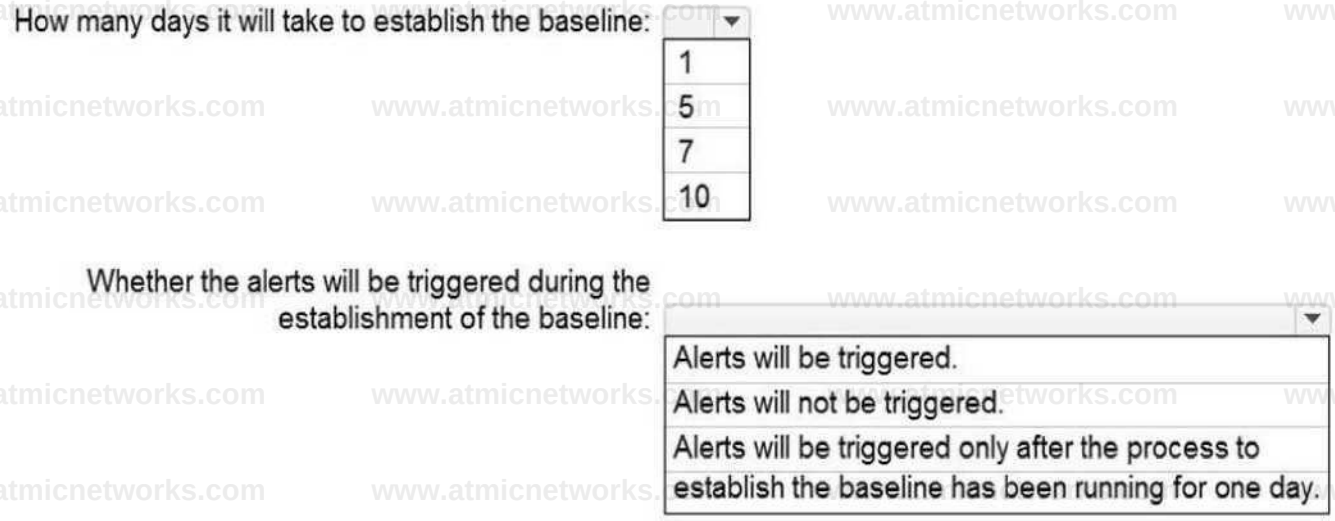
You need to identify the following:

How many days it will take to establish a baseline for unusual activity.

Whether alerts will be triggered during the establishment of the baseline.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

How many days it will take to establish the baseline:

- 1
- 5
- 7
- 10

Whether the alerts will be triggered during the establishment of the baseline:

- Alerts will be triggered.
- Alerts will not be triggered.
- Alerts will be triggered only after the process to establish the baseline has been running for one day.

ence:

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

Question: 184

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort.

What should you do first?

A. From the Microsoft 365 admin center, create a mail-enabled security group.
B. From the Microsoft 365 Defender portal, create a device group.
C. From the Microsoft Endpoint Manager admin center, create a device category.
D. From the Azure Active Directory admin center, create a dynamic device group.

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine- groups?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

Question: 185

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

You need to assign the Security Administrator role.

Reference:

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

Question: 186

You have a Microsoft 365 E5 subscription.

You plan to implement records management and enable users to designate documents as regulatory records.

You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.

What should you do first?

A. Configure custom detection rules.
B. Create an Exact Data Match (EDM) schema.
C. Run the Sec-RegulacoryComplianceUI cmdlet.
D. Run the Sec-LabelPolicy cmdlet.

Answer: C

Explanation:

Reference:

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

Question: 187

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.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 188

HOTSPOT

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.

You need to configure Intune to meet the following requirements:

Prevent users from enrolling personal devices.
Ensure that users can enroll a maximum of 10 devices.

What should you use for each requirement? To answer, select the appropriate options in the

answer area.

NOTE: Each correct selection is worth one point.

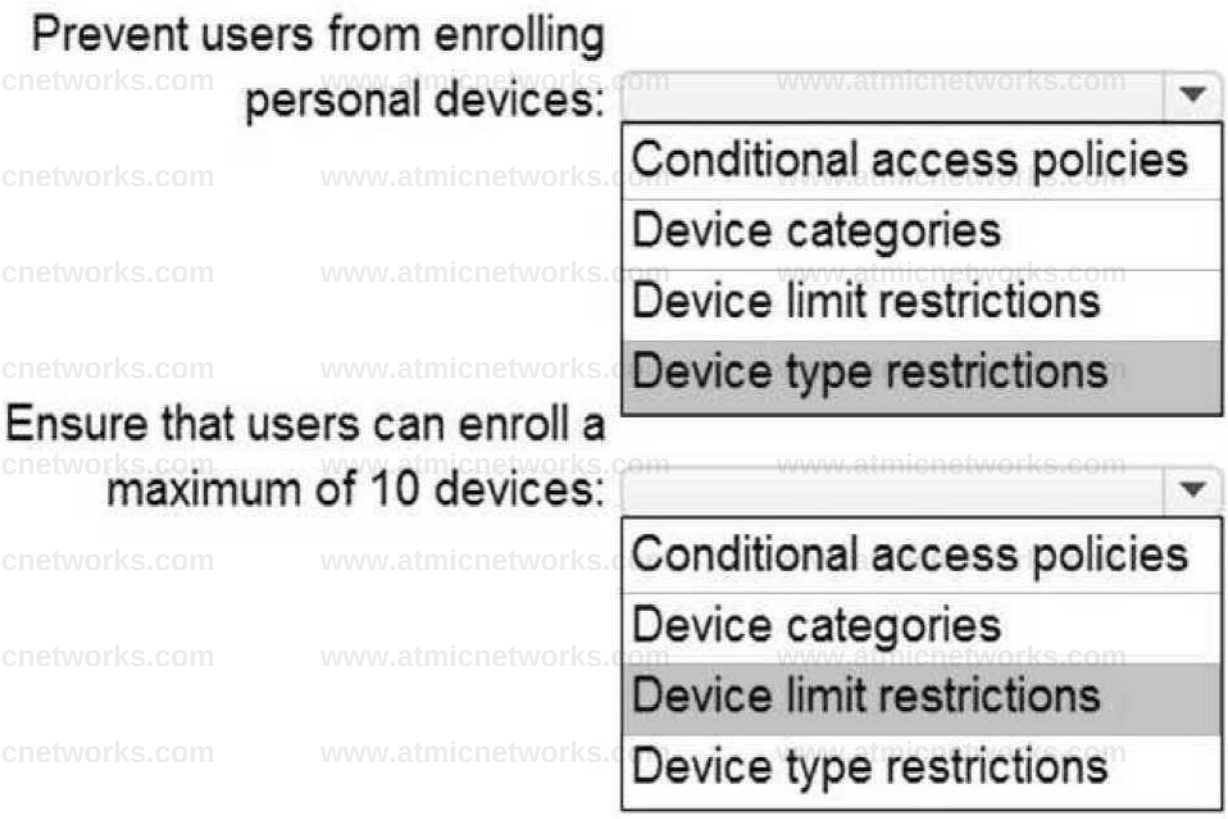
Prevent users from enrolling personal devices:

Ensure that users can enroll a maximum of 10 devices:

Conditional access policies
Device categories
Device limit restrictions
Device type restrictions

Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions- set#blocking-personal-windows-devices

Question: 189

HOTSPOT

You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

Name: Case1

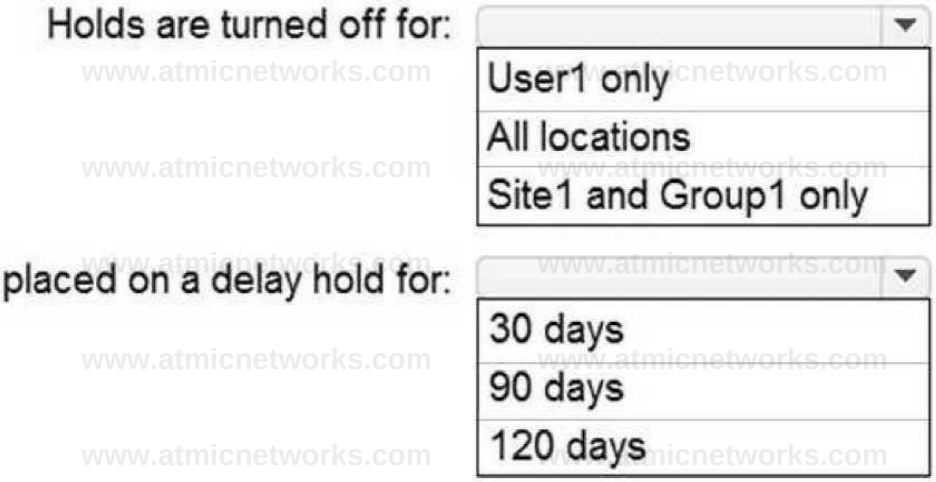
Included content: Group1, User1, Site1

Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders

The investigation for Case1 completes, and you close the case.

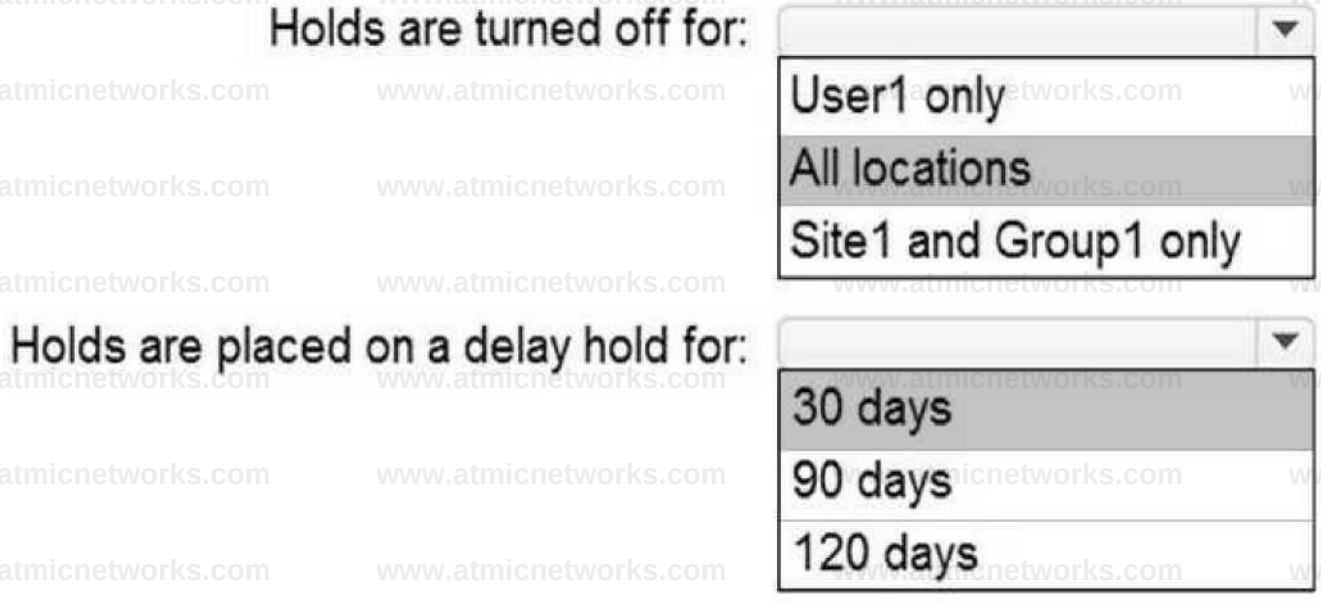
What occurs after you close Case1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/close-or-delete-case?view=o365- worldwide

Question: 190

HOTSPOT

You have a Microsoft 365 E5 tenant

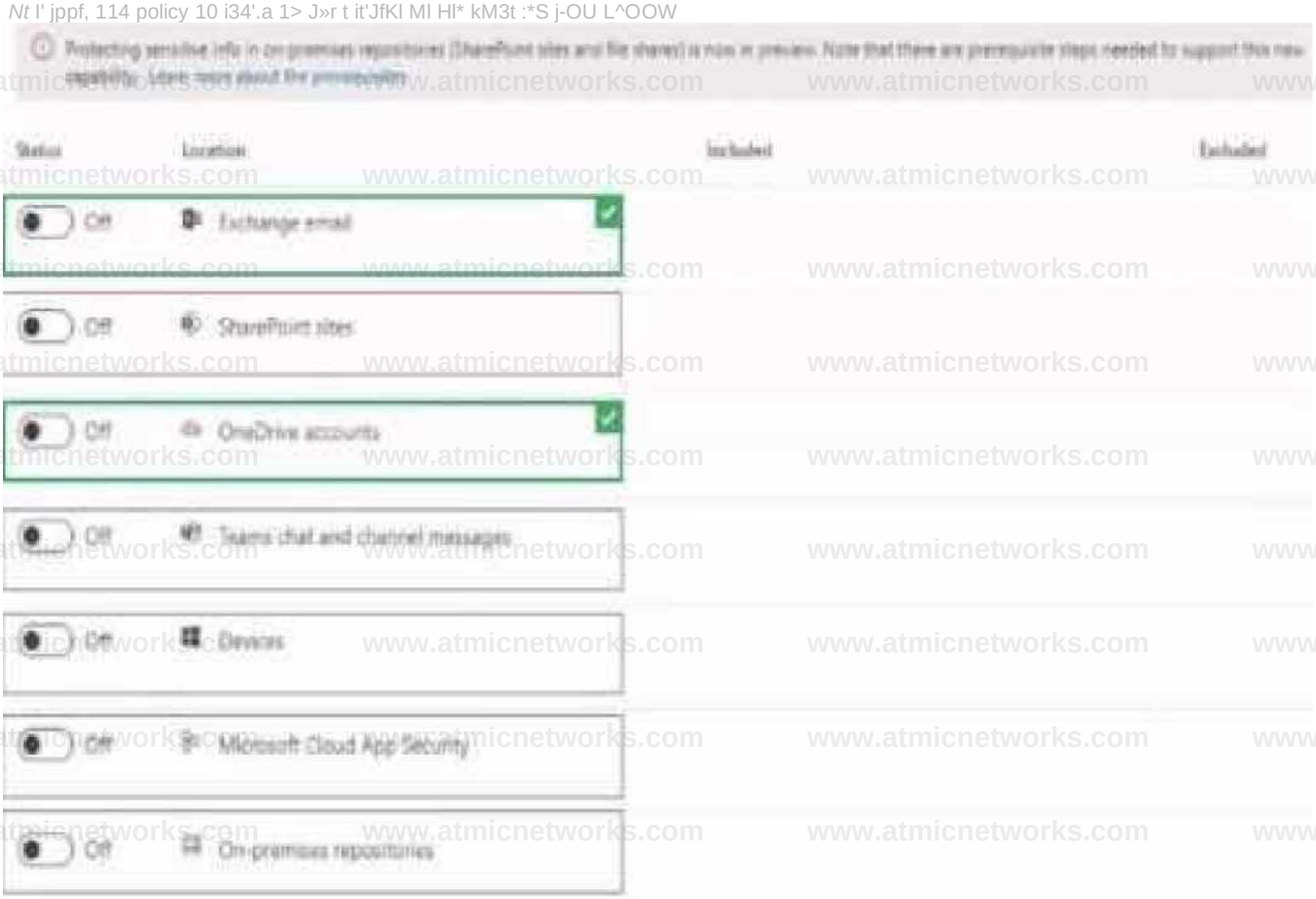
You create a data toss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.

To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

Choose locations to apply the policy

Nt I' jppf, 114 policy 10 i34'.a 1> J»r t it'JfKl MI Hl* kM3t :*S j-OU L^OOW

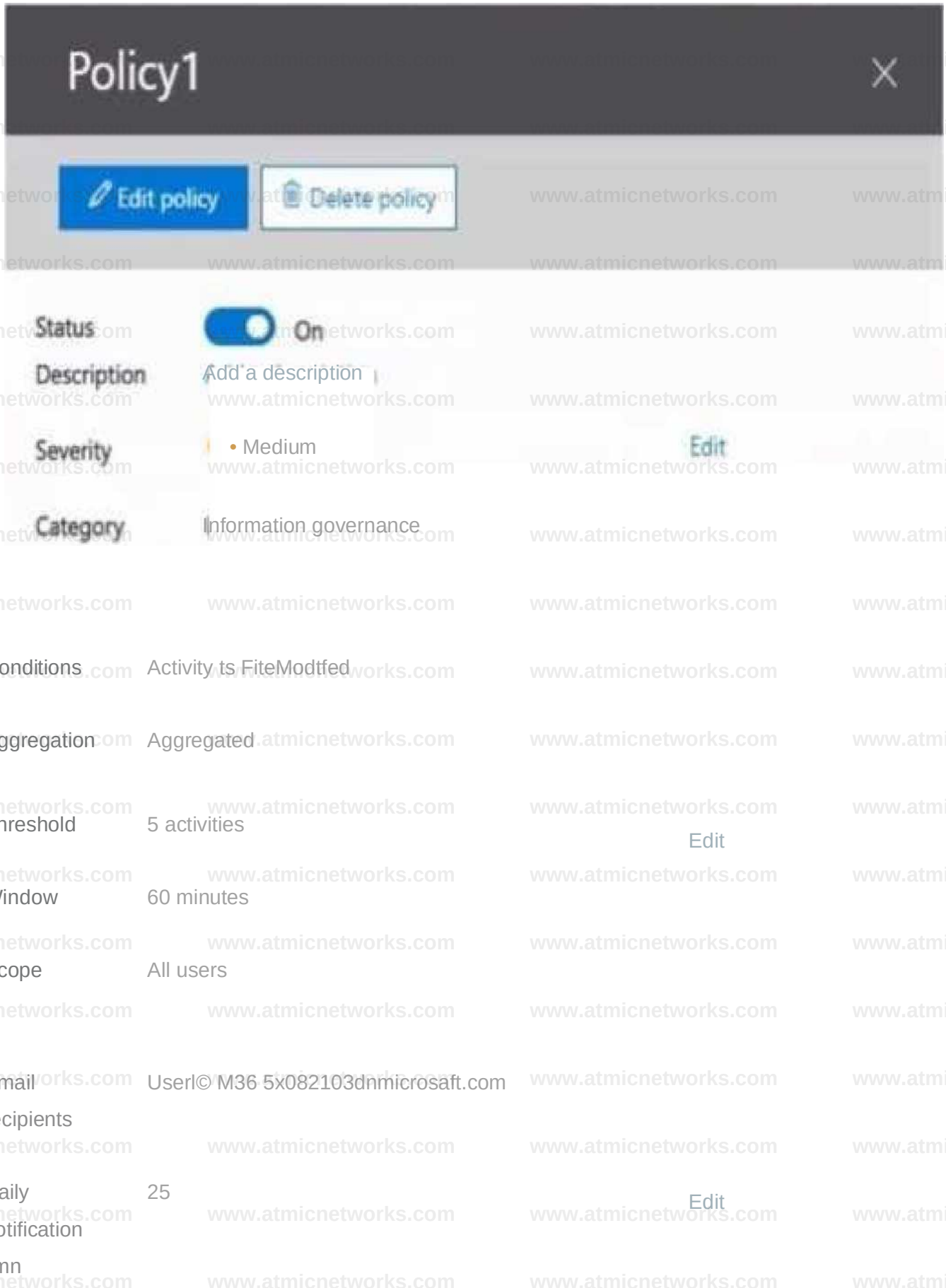


Answer:

Explanation:

Question: 191

You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.



User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every

four minutes and runs for a period of two hours.
How many alerts will User1 receive?

A. 2
B. 5
C. 10
D. 25

Answer: D

Explanation:

Question: 192

HOTSPOT

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	Bitlocker Drive Encryption (BitLocker)	Member of
Device[1]	Windows 10	Disabled	G roup 1 Group?
Device?	Windows 10	Disabled	Group?. Groups
Device^	Windows 10	Disabled	GroupS

The device compliance policies in Endpoint Manager are configured as shown in the following table.

Name	Require BitLocker	Mark noncom pliant after (days)	Assigned
Policy!	Require	5	No
Pc 'ky?	Require	10	Yes
Policy 3	Net configured	15	Yes

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy2	Group2
Policy3	Group3

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

Answer Area

Statements	Yes	No
Device! is marked as noncomphant after 10 days.		
Device? is marked as noncomphant after 10 days.	0	C
Devices is marked as noncomphant after 15 days.	0	0

Answer:

Explanation:

Answer Area

Statements	Yes	No
Device! is marked as noncomphantafter 10 days.	•	
Device? is marked as noncomphantafter 10 days.	•	
Device3 is marked as noncomphantafter 15 days.	•	)

Question: 193

HOTSPOT

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Devicel	Windows 10	Disabled	Group?
Device?	Windows 10	Disabled	Groups Groups
Devices	Windows 10	Disabled	Group?

The device compliance policies in Endpoint Manager are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy!	Windows 10 and later	Require	Yes
Policy?	Windows 10 and later	Not configured	Yes
Policy 3	Windows 10 and later	Require	No

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	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.

Answer Area

Statements Vto No

Device) 15 compliant

Device? is compliant

Devices is compliant

Answer:

Explanation:

Answer Area

Statements	Yes	No
Devicel is compliant.		
Device? is compliant		
Device? is compliant		

Question: 194

You have a Microsoft 365 E5 subscription.

Al users have Mac computers. ATI the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.

You need to configure Microsoft Defender for Endpoint on the computers.

What should you create from the Endpoint Management admin center?

A. a Microsoft Defender for Endpoint baseline profile
B. an update policy for iOS
C. a device configuration profile
D. a mobile device management (MDM) security baseline profile

Answer: D

Explanation:

Question: 195

You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:

- Windows 10
- Android
- iOS

On which devices can you configure the Endpoint DLP policies?

A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and macO Sonly
D. Windows 10, Android, and iOS

Answer: A

Explanation:

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.

https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn- about?view=o365-worldwide

Question: 196

Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1. Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).

You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

A. Windows 11 and Windows 10 only
B. Windows 11, Windows 10-Windows8.1.andmacOS
C. Windows 11 and macOS only
D. Windows 11 only
E. Windows 11. Windows 10, and Windows8.1 only

Answer: C

Explanation:

Question: 197

HOTSPOT

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
UKT s	Groupl
Useri	-Gw[1] G'^2
Useri	Mine

The device type restrictions in Endpoint Manager are configured as shown in the following table.

M-? * -life- l	Name	Allowed platform	Assigned to
	fobcyl	-TO&d >35 Winders MDMi	Atone
	fobcyZ	[yiHWWiUDM]	Grcup2
	PobcyS	Anu'LVJ. iOS	jfOup ‘
Default	AH user*	Anci'isd, Wimtovn fM^M	All unit

Answer Area Statements **Yes No**

User' can enroll Windows devices in Endpoint Manager

User? can enroll Android devices in Endpoint Manager

User3 can enroll iOS devices in Endpoint Manager

Answer:

Explanation:

Answer Area

Statements	Yes	No
Use' can enroll Windows devices in Endpoint Manager.	•	
User? can enroll Android devices in Endpant Manager ‘	•	
User? can enroll iOS devices ei Endpant Manager	•	

Question: 198

HOTSPOT

You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint device groups shown in the following table

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Answer Area

Computefl-London: I

Groupi
Group?
Group?
UwJKvJPM machine*.

Serveri-London: I . Groupi® Group? Group? Ungrouped machines

Answer:

Explanation:

Answer Area

Computeri-London: Group 1

Sewl-London: Groupi

Question: 199

You have a Microsoft 365 E5 subscription.

You create an account tor a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

A. Yes
B. no

Answer: B

Explanation:

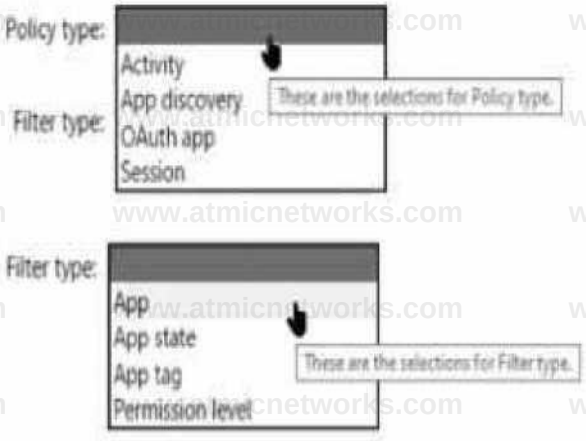
Question: 200

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps. You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.

What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Policy type App discovery

Fitter type Permission levei

Question: 201

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

You have labels in Microsoft 365 as shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

The content in Microsoft 365 is assigned labels as shown in the following table.

Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

You have labels In Microsoft 365 as shown in the following table.

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

Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	○	○
Admin2 can view the contents of File1 by using Content explorer.	○	○
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	○	○

Answer:

Explanation:

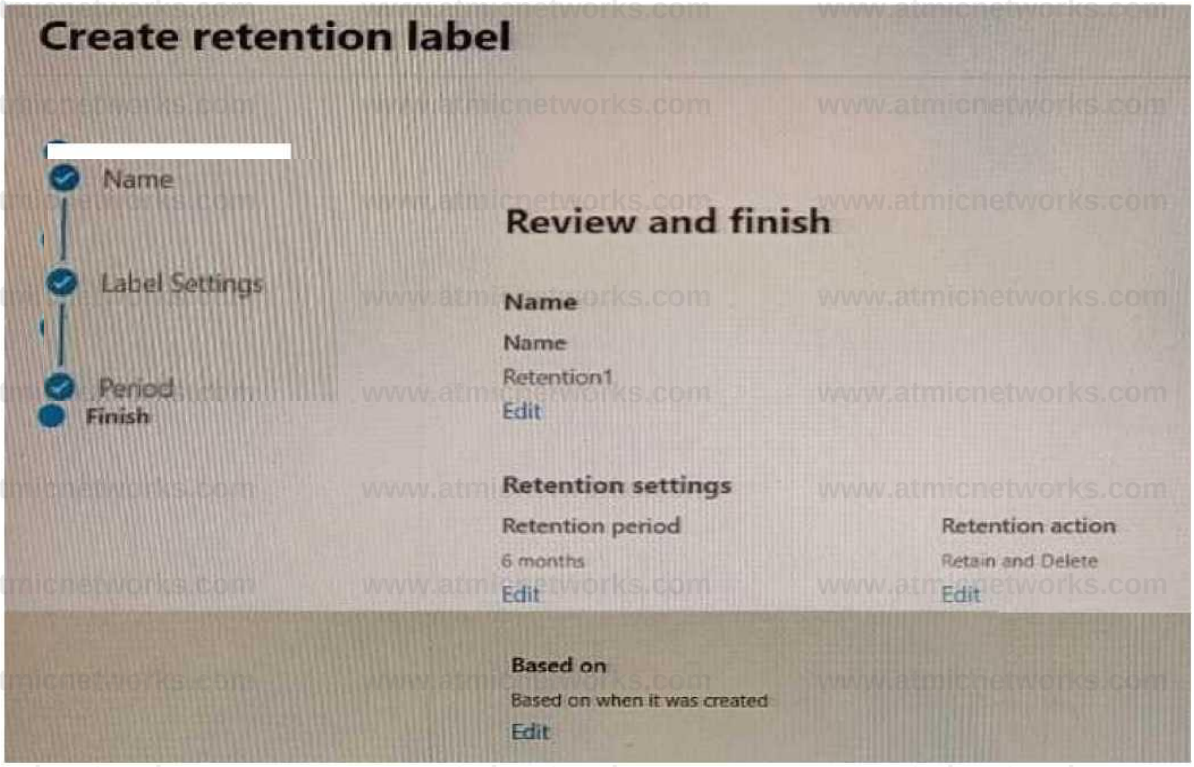
Answer Area

Statements	Yes	No
Admin 1 can view the contents of Pilei by using Content explorer.	9	
Admin? can view the contents of File! by using Content explorer.		
Admin? can use Content explorer to verify that Label? is assigned to Maili.		'ft'

Question: 202

You have a Microsoft 365 subscription.

You create a retention label named Retention1 as shown in the following exhibit.



You apply Retention! to all the Microsoft OneDrive content.

On January 1, 2020, a user stores a file named File1 in OneDrive.

On January 10, 2020, the user modifies File1.

On February 1, 2020, the user deletes File1.

When will File1 be removed permanently and unrecoverable from OneDrive?

A. February 1, 2020
B. July 1.2020
C. July 10, 2020
D. August 1, 2020

Answer: B

Explanation:

Question: 203

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD.

You purchase a Microsoft 365 E3 subscription

You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.What should you do?

A. From the Microsoft Endpoinf Manager admin center, create a Windows Autopilot deployment profile. Assign the profile to all the computers. Instruct users to restart their computer and perform a network restart.

B. Enroll the computers in Microsoft Intune. Create a configuration profile by using the Edition upgrade and mode switch template. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer. C. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online site. Instruct users to run the provisioning package from SharePoint Online.

D. From the Azure Active Directory admin center, create a security group that has dynamic device membership. Assign licenses to the group and instruct users to sign in to their computer.

Answer: B

Explanation:

Question: 204

HOTSPOT

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

- Microsoft 365 Apps for enterprise
- Office for the web
- Office 2016
- Office 2019

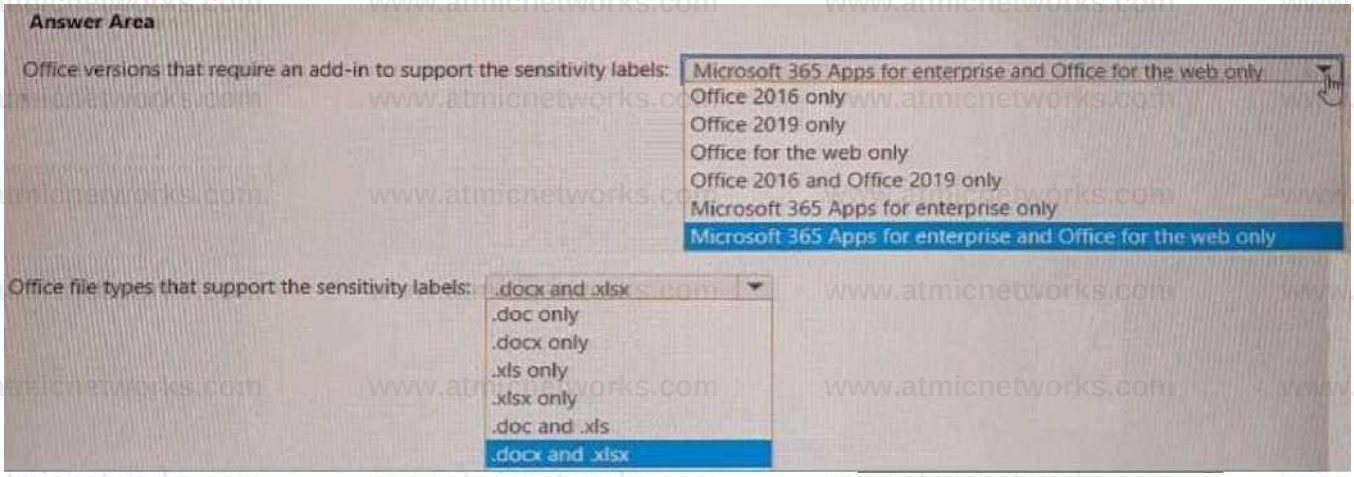
The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- xls

You plan to use sensitivity labels. You need to identify the following:

- Which versions of Office require an add-in to support the sensitivity labels.
- Which file types support the sensitivity labels.

What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.



Explanation:

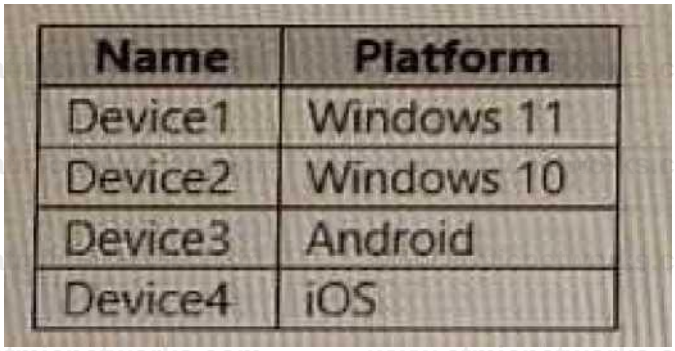
Answer:

Answer Area

Office versions that require an add-in to support the sensitivity labels: Microsoft 365 **Apps for enterpnse and Office for the web only '**

Office file types that support the sensitivity labels: .docx and .xlsx

Question: 205



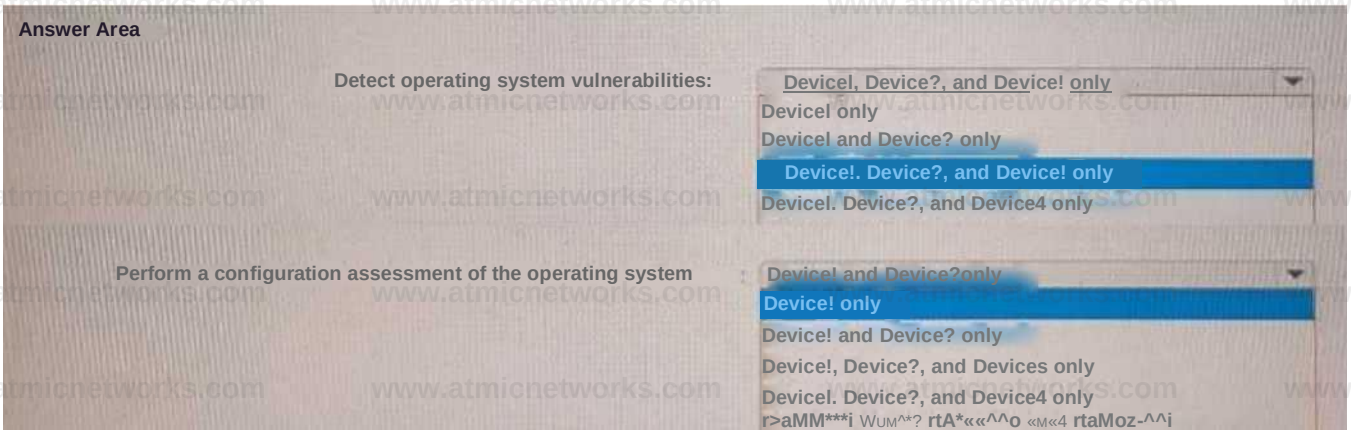
Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.
All the devices are onboarded To Microsoft Defender for Endpoint

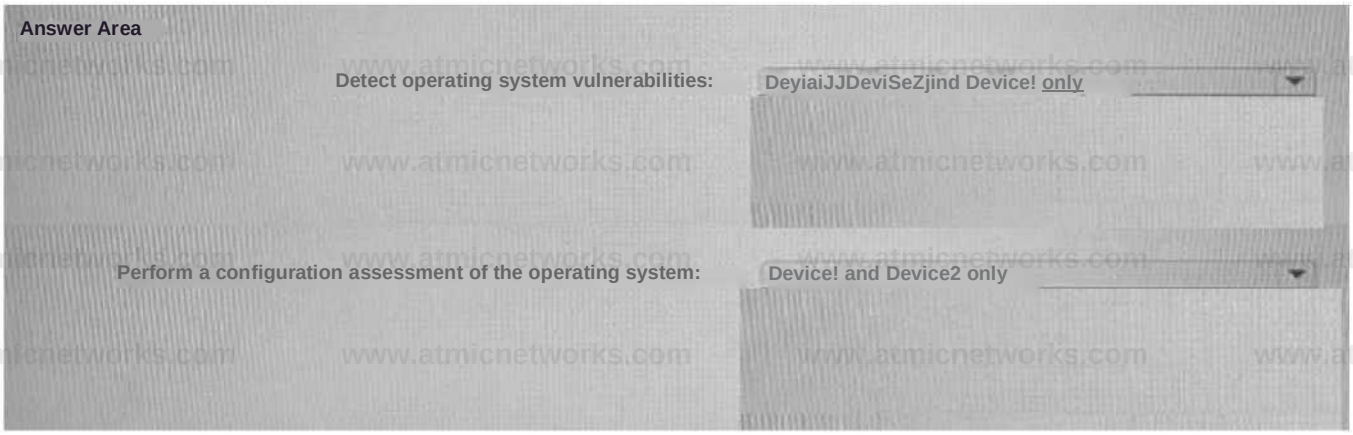
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

- Detect operating system vulnerabilities.



Answer:

Explanation:

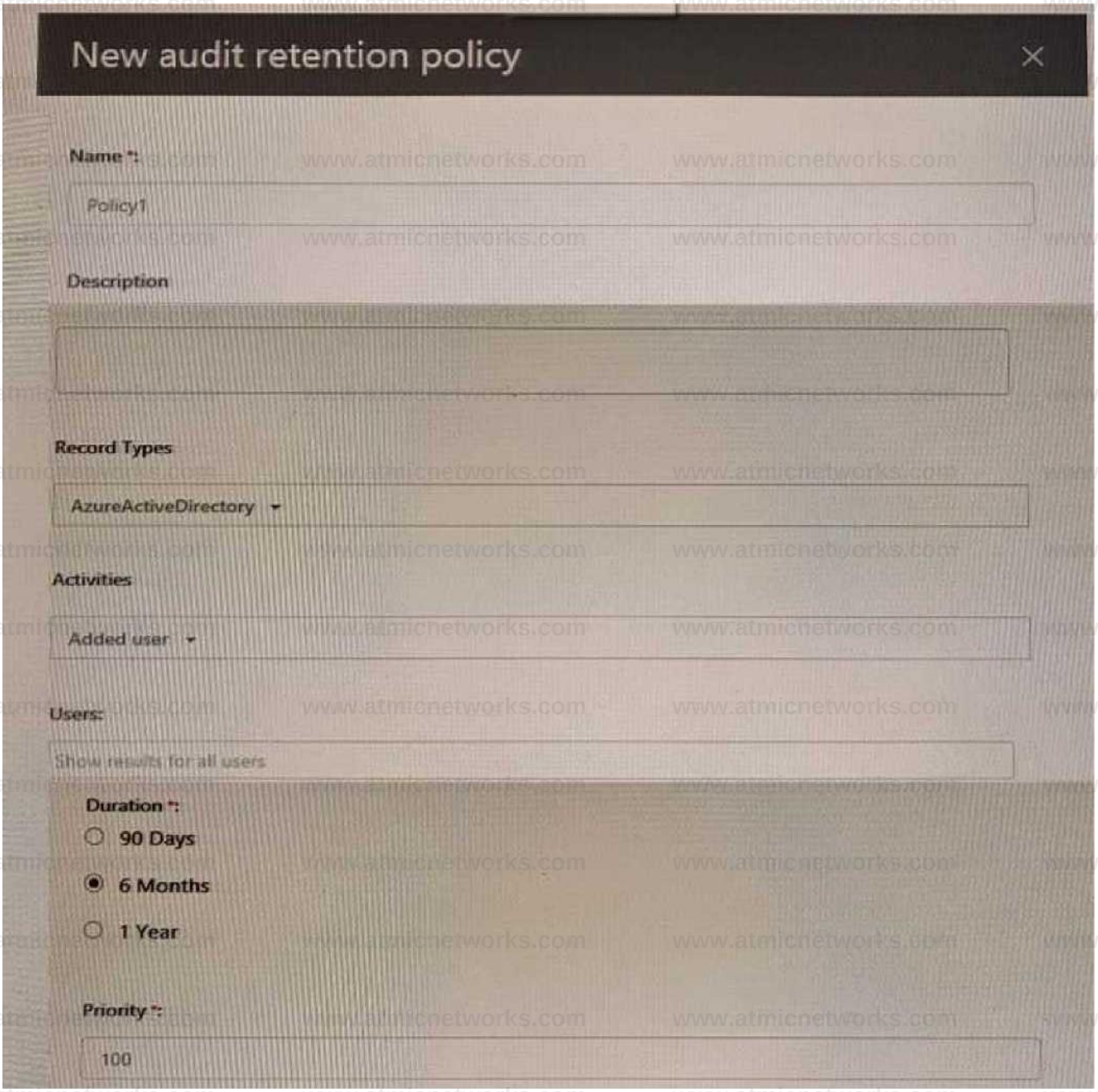


Question: 206

HOTSPOT

You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

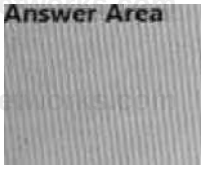


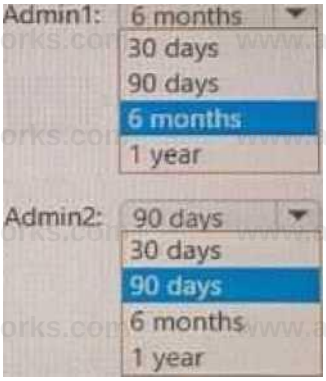
You plan to create a new user named User1.

How long will the user creation audit event be available if Admin1 or Admin2 creates User1?

To answer, select the appropriate options in the answer area.

Each correct selection is worth one point.





Answer

Explanation:

Question: 207

You have a Microsoft 365 subscription.

From Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 208

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

A Built-in protection preset security policy is applied to the subscription.

Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Anti-malware
B. Anti-phishing
C. Safe Attachments
D. Anti-spam
E. Safe Links

Answer: C,E

Explanation:

Question: 209

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to identify the settings that are below the Standard protection profile settings in the preset security policies.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Portal: Microsoft 365 Defender portal
- Microsoft 365 admin center
- **Microsoft 365 Defender portal**
- Microsoft Purview compliance portal

Feature: Configuration analyzer
- **^Configuration analyzer**
- Preset security policies
- Threat tracker

Answer:

Explanation:

Answer Area

Portal: Microsoft 365 Defender portal

Feature: Configuration analyzer

Question: 210

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
Userl	User	Gtoupl
Devicel	Device	Gioupl

User1 is the owner of Device1.

You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.

On Thursday, you review the results of the app deployments.

Name	Shows In Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group 1 - Required	Word	Monday
App2	Yes	Group? • Required	Excel	Tuesday
App3	Yes	Group1 * Available	PowerPoint	Wednesday

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

Answer Area

Statements	Yes	No
Word is installed on Devicel.	$	.8
App3 is displayed in the Company Portal.		
Excel is installed on Devicel.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Word is installed on Device1.		
App3 is displayed in the Company Portal.	ft	
Excel is installed on Device1	•	

Question: 211

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune.
Which platform can you manage by using the profiles?

A. Ubuntu Linux
B. macOS
C. Android Enterprise
D. Windows 8.1

Answer: D

Explanation:

Question: 212

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps.

You configure a session control policy to block downloads from SharePoint Online sites. Users report that they can still download files from SharePoint Online sites.
You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites.
What should you configure?

A. an access policy
B. a data loss prevention (DLP) policy
C. an activity policy
D. a Conditional Access policy

Answer: A

Explanation:

Question: 213

HOTSPOT

You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

Name	Retention period	During the retention period
Retentionl	5 years	Retain items even if users delete
Retention	5 years	Mark items as a record
Retentions	5 years	Mark items as a regulatory record

Site1 contains the files shown in the following table.

Name	Label
Filel	*None*
File?	Retention 1
FileS	Retention?
File4	Retention?

The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.

You need to identify the following information:

- The number of email messages quarantined by zero-hour auto purge (ZAP)
- The number of times users clicked a malicious link in an email message

Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP: Threat protection status '•'

Maiiflow status report Spoof detections

Threat protection status

URL threat protection

To identify the number of times users clicked a malicious link Mailflow status report in an email:

Maiiflow status report

Spoof detections Threat protection status URL threat protection

Answer:

Explanation:

Answer Area

To identify the number of emails quarantined by ZAP: Threat protection statu;

To identify the number of times users clicked a malicious link Maiiflow status report in an email:

Question: 215

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Devicel	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.

What should you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Devicel: Microsoft Endpoint Manager

A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device?: A local scnpt

A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Answer:

Explanation:

Answer Area

Devicel: Microsoft Endpoint Manager

Device2: A local script

Question: 216

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels Label, policies Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the.settings you choose. For example, you can create labels that encrypt fries add content marking, and control user access to specific sites.
Learn more about sensitivity labels

+ Create a label Q Publish labels O Refresh

Name f		Order	Created by	Last modified
Label 1		0 ■ highest	Prvi	04/24/2020
label?	...	1	Prvi	04/24/2020
Label]		0* highest	Prvi	04/24/2020
Label4	•••	0-highest	Prvi	04/24/2020
labeb	...	5	Prvi	04/24/2020

Which labels can users apply to content?

A. Label1, Label2, and Label5 only
B. Label3. Label4, and Label6 only
C. Label1, Label3, Labe2, and Label6 only
D. Label1, Label2, Label3, Label4, Label5. and Label6

Answer: D

Explanation:

Question: 217

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1. you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do first?

A. From the Exchange admin center create a mail flow rule.
B. From Microsoft 365 Defender, start a message trace.
C. From Microsoft Defender for Cloud Apps, create an activity policy.
D. From the Microsoft Purview compliance portal, create a label and a label policy.

Answer: D

Explanation:

Question: 218

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
DeviceI	Windows 10 Enterprise
Device?	iOS

Devices	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings.

Which devices will support the settings?

A. Device1 only

B. Device1 and Device4

C. Device1, Device3, and Device4

D. Device1, Device2, Device3, and Device4

Answer: A

Explanation:

Question: 219

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

Name	Type
Policy 1	Anti-phishing
Pol icy 2	Anti-spam
Policy?	Anti-malware
f o cy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

A. Policy1 and Policy2 only

B. Policy2 and Policy4 only

C. Policy3 and Policy4 only

D. Policy1 and Policy3only

Answer: A

Explanation:

Question: 220

You purchase a new computer that has Windows 10, version 21H1 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

A. Install all the feature updates released since version 21H1 and the latest quality update only.

B. Install the latest feature update and all the quality updates released since version 21H1.

C. Install the latest feature update and the latest quality update only.

D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

Answer: C

Explanation:

Question: 221

You have a Microsoft 365 E5 tenant.

You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.

What should you use to create the policy?

A. the Microsoft 365 admin center

B. the Microsoft Purview compliance portal

C. the Microsoft Defender for Cloud Apps portal

D. the Microsoft Apps admin center

Answer: C

Explanation:

Question: 222

DRAG DROP

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

Name	Operating system	Microsoft Intune
Devicel	Windows 11 Enterprise	Enrolled
Device?	iOS	Enrolled

Device?	Android	Not enrolled

You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

- Word files created by using Windows devices must be encrypted automatically.
- If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
- For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of polio/ should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Question: 223

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft SharePoint Online site. What should you do?

A. From the SharePoint Online site, create an alert.

B. From the SharePoint Online admin center, modify the sharing settings.

C. From the Microsoft 365 Defender portal, create an alert policy.

D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

Answer: C

Explanation:

Question: 224

HOTSPOT

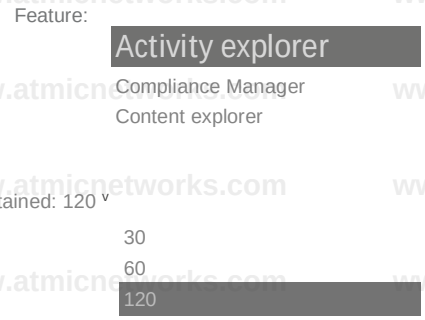
You have a Microsoft 365 E5 subscription that.

You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription.

Which feature should you use, and how many days will the data be retained? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Feature: Activity explorer

Number of days the data will be retained: 120

Question: 225

HOTSPOT

You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune.

You create an Android app protection policy named Policy! that is targeted to all Microsoft apps and assigned to all users.

Policy! has the Data protection settings shown in the following exhibit.

Data transfer

Backup pig data to Android backup senates 0		Block
Send org data to other apps ©	Policy managed apps	v
Select apps to exempt		
Sa_e copes of era data 0	Allow	
Allow user to save copies to selected services ©	SharePoint	v |
transfer telecommunication data	Any dialer app	V
Dialer App Package ID		
Dialer App Name		
Receive data from ether apps 0	All AppS	v
Open data into Org documenta 0		
Allow users to open (lata from selected jewel 0		
Restrict cut copy, and paste between other apps 0	Policy managed apps with paste in	v |
Screen capture and Google Assistant	^^^^^^^Ts^^^^^^^B	Block
Approved keyboards I-	Require	
Select keyboards to approve	Select	

Use the drop-down menus to select 'he answer choice that completes each statement based on the information presented in the graphic.

Answer Area

A user can copy files from Microsoft OneDnve to **(answer choice!** only.[Microsoft SharePoint Online
OneDnve local storage _
Microsoft SharePoint
Microsoft SharePoint Online and

A user can copy and paste text from **(answer choice)** to a Microsoft Word document stored
In Microsoft OneDnve

any app
any app
only managed apps
only unmanaged apps

Answer:

Explanation:

Answer Are*

A user an copy files from Microsoft OneDrive to [answer choice] only. Microsoft SharePoint Online

A user can copy and paste text from (answer choice) to a Microsoft Word document stored any ape in Microsoft OneDrive.

Question: 226

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You ate implementing Microsoft Defender for Endpoint

You need to enable role-based access control (RBAQ to restrict access to the Microsoft 365 Defender portal.

Which users can enable RBAC, and winch users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area

Users that can enable RBAC: [Admin! and Admin? only
Admtnl only
Admin! and Admin? only
Admin!. Admin?, and Admin5 only
Admin! Admin?, AdminS. and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal: [Admin3, Admln4, and AdminS only J]
Admin5 only
Admin3 and Admin4 only
Admin4 and AdminS only
Admin3, AdmiM, and Admm5 only

Answer:

Explanation:

Answer Area

Users that can enable RBAC Admin! and Admin? only

Users that will no longer have access to the Microsoft 365 Defender portal: AdminS, AdminA and AdminS only

Question: 227

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to be notified when a single user downloads more than 50 files during any 60-second period.

What should you configure?

A. a session policy
B. a file policy
C. an activity policy
D. an anomaly detection policy

Answer: D

Explanation:

Question: 228

HOTSPOT

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
Used	Group 1
User2	Groups
Used	Groups

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint ^J ■ mJ: 7h. i .'default)	View data. Alens investigation. Active remediation actions, Manage security settings	Group?
total	Viewdata Alens investigation	Group 1
tola?	View data	Groups

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Devicel	Gi oup1
Last	Ungrouped devices (default)	Device^	Groups

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

Answer Area

Statements	Yes	No
Useri can run an antivirus scan on DeviceZ.	0	0

User? can collect an investigation package from Device? Users can isolate Devicel.

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can run an antivirus scan on DeviceZ.	O	®
User2 can collect an investigation package from DeviceZ		•
User3 can isolate Devicel.	®	

Question: 229

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 230

Your company has a Microsoft 365 subscription.

You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group used to assign the license.
What should you use?

A. Active users in the Microsoft 365 admin center
B. Reports in Microsoft Purview compliance portal
C. the Licenses blade in the Microsoft Entra admin center
D. Reports in the Microsoft 365 admin center

Answer: D

Explanation:

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center
Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21
Microsoft browser usage	Yes	No[1]	No	No[1]	No'
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations^]	Yes	Yes	Yes	Yes	Yes

Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports

Question: 231

HOTSPOT

HOTSPOT

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

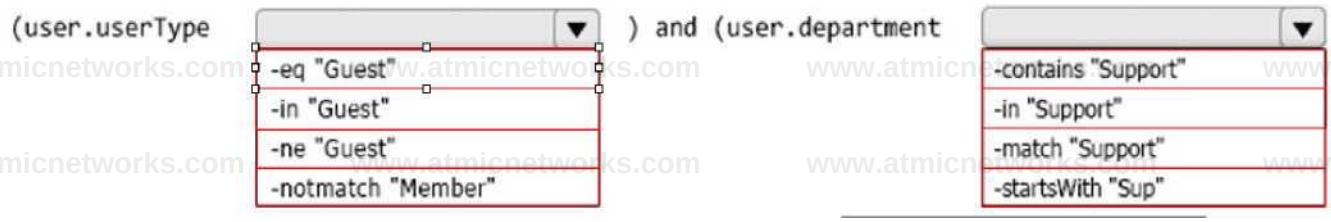
Name	Type	Department
Useri	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.

How should you complete the membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

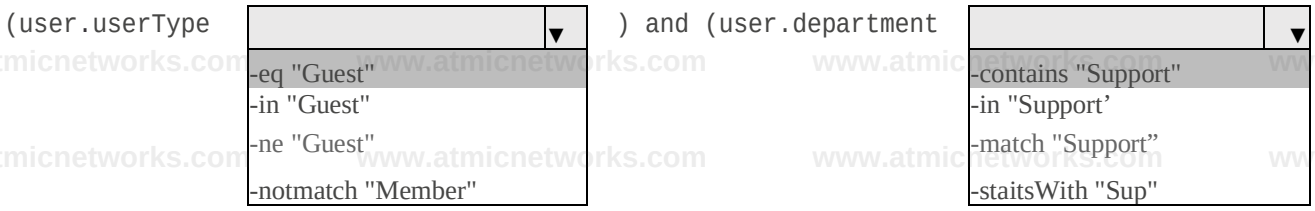
Answer Area



Explanation:

Answer:

Answer Area



Box 1: -eq "Guest"

Dynamic membership rules for groups in Azure Active Directory

Supported expression operators

The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

* Equals

-eq

* Contains

-contains

* Etc.

Box 2: -contains "Support"

Incorrect:

* -in

If you want to compare the value of a user attribute against multiple values, you can use the - in or -notIn operators.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic- membership

Question: 232

HOTSPOT

HOTSPOT

Your company uses a legacy on-premises LDAP directory that contains 100 users.

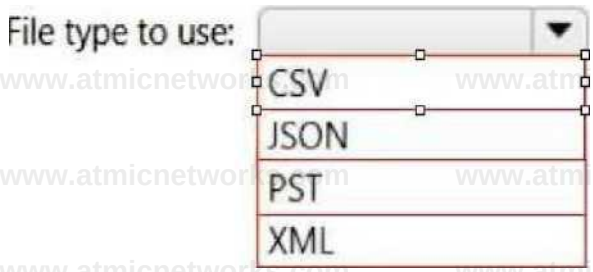
The company purchases a Microsoft 365 subscription.

You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.

Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Required properties for each user

Display Name and Department First Name and Last Name

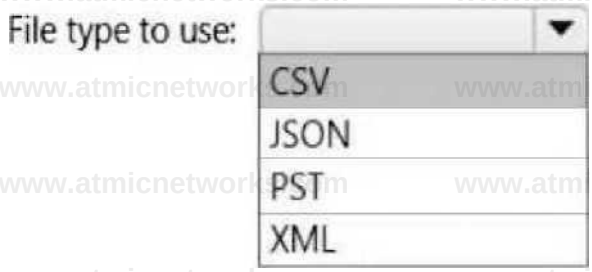
User Name and Department User Name and Display

Name

Answer:

Explanation:

Answer Area



Required properties for each usee

Display Name and Department
First Name and Last Name
User Name and Department
User Name and Display Name

Box 1: CSV

Add multiple users in the Microsoft 365 admin center

Sign in to Microsoft 365 with your work or school account.

In the admin center, choose Users > Active users.

Select Add multiple users.

On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.

Etc.

Note: More information about how to add users to Microsoft 365

Not sure what CSV format is?

A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

Box 2: User Name and Display Name

What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have

some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

Reference:
https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time

Question: 233

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

Name	Department
Useri	Human resources
User2	Research
User 3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:

To all users, deploy an Office 365 E3 license without the Power Automate license option.
To all users, deploy an Enterprise Mobility + Security E5 license.
To the users in the research department only, deploy a Power BI Pro license.
To the users in the marketing department only, deploy a Visio Plan 2 license.
What is the minimum number of deployment groups required?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

Explanation:
One for all users, one for the research department, and one for the marketing department.

Note: What are Deployment Groups?

With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.

Reference:

https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available- sharing-of-targets-and-more

Question: 234

You have a Microsoft 365 subscription.

You view the Service health Overview as shown in the following exhibit.

Service health

October 18. 2022 4:20 PM

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. Learn more about Service Health

Li Report an issue © Customize

Active issues

v Issue title	Affected service	Issue type
> Microsoft service health (6)		
Issues in your environment that require action (0)		

Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

You need to ensure that a user named User1 can view the advisories to investigate service health issues.

Service	Status
Exchange Online	O 3 advisones
Microsoft 365 suite	O 2 advisories
Microsoft Teams	1 advisory
OneDrive for Business	O 1 advisory
	# 2 advise

Which role should you assign to User1?

A. Message Center Reader

B. Reports Reader
C. Service Support Administrator
D. Compliance Administrator

Answer: B

Explanation:

Service Support admin

Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:

- Open and manage service requests
- View and share message center posts
- Monitor service health

Incorrect:

* Message center reader

Assign the Message center reader role to users who need to do the following:

- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups

* Reports reader

Assign the Reports reader role to users who need to do the following:

- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Azure AD
- View data returned by Microsoft Graph reporting API

Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

Question: 235

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Adminl	Group 1
Admm2	Group2
Admin3	Groupl, Group2

You add the following assignment for the User Administrator role:

Scope type: Directory
Selected members: Group1
Assignment type: Active
Assignment starts: Mar 15, 2023
Assignment ends: Aug 15, 2023

You add the following assignment for the Exchange Administrator role:

Scope type: Directory
Selected members: Group2
Assignment type: Eligible
Assignment starts: Jun 15, 2023
Assignment ends: Oct 15, 2023

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On July 15,2023, Admin! can reset the password of a user.		
On June 20,2023, Admin2 can manage Microsoft Exchange Online.		
On May 1, 2023, Admin3 can reset the password of a user.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
On July 15,2023, Adminl can reset the password of a user.		
On June 20,2023, Admin2 can manage Microsoft Exchange Online.	○	●
On May 1, 2023, Admin3 can reset the password of a user.	●	○

Box 1: Yes

Admin1 is member of Group1.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

July 15, 2023 is with the assignment period.

A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.

Box 2: No

Admin2 is member of Group2.

The Exchange Administrator role assignment has Group2 as a member.

The assignment type: Eligible

June 20, 2023 is with the assignment period.

The assignment must be approved.

Note: Eligible assignment requires member or owner to perform an activation to use the role.

Activations may also require providing a multi-factor authentication (MFA), providing a

business justification, or requesting approval from designated approvers.

Box 3: Yes

Admin3 is member of Gropu1 and Group2.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

May 1, 2023 is with the assignment period.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member-owner

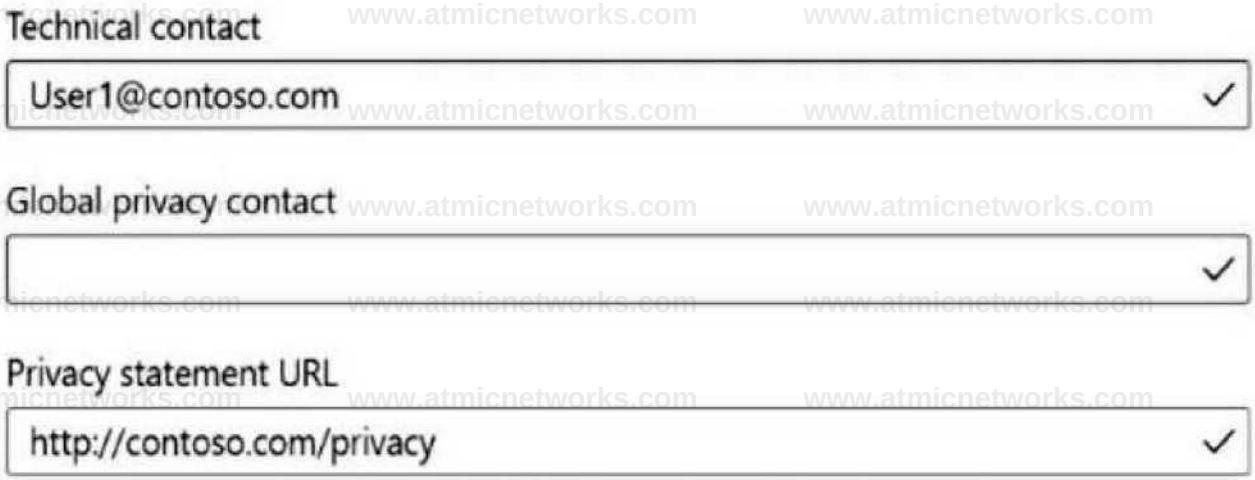
Question: 236

You have a Microsoft 365 subscription.

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
Useri	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.



Which users will be contacted by Microsoft if the tenant experiences a data breach?

A. Used only
B. User2 only
C. User3 only
D. Used and User2 only
E. User2 and User3 only

Answer: B

Explanation:

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration.
The customer's tenant administrator will be notified.

Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

Question: 237

Your network contains an Active Directory forest named contoso.local.

You purchase a Microsoft 365 subscription.

You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.

You need to prepare for the planned move to Microsoft 365.

What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

A. Purchase a third-party X.509 certificate.
B. Create an external forest trust.
C. Rename the Active Directory forest.
D. Purchase a custom domain name.

Answer: D

Explanation:

The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on-premise Active Directory if it's a routable domain name, for example, contoso.com.

If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.

Incorrect:

Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization

Question: 238

You have a Microsoft 365 subscription.

You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.

Which type of group should you use to assign the Reports Reader role and to access App1?

A. a Microsoft 365 group that has assigned membership
B. a Microsoft 365 group that has dynamic user membership
C. a security group that has assigned membership
D. a security group that has dynamic user membership

Answer: C

Explanation:

To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.

Note: You can add the following types of groups:

Assigned groups - Manually add users or devices into a static group.

Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.

Note:

Security groups

Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.

Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.

Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.

Security groups can be added to a team.

Microsoft 365 Groups can't be members of security groups.

Microsoft 365 Groups

Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps

https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?

https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

Question: 239

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

A. Enable auditing.

B. Enable Microsoft 365 usage analytics.

C. Create an Insider risk management policy.

D. Create a communication compliance policy.

Answer: A

Explanation:

Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Note: Permissions alert policies

Example: Elevation of Exchange admin privilege

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.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview

https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Question: 240

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 Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.

You plan to onboard all the devices to Microsoft Defender for Endpoint.

You need to store the Microsoft Defender for Endpoint data in Europe.

What should you do first?

A. Delete the workspace.

B. Create a workspace.

C. Onboard a new device.

D. Offboard the test devices.

Answer: B

Explanation:

Storage locations

Understand where Defender for Cloud stores data and how you can work with your data:

* Machine information

- Stored in a Log Analytics workspace.
- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace

Question: 241

You have a Microsoft 365 E5 subscription that contains a user named User1.

User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.

You need to remove User1 from the Restricted entities list.

What should you use?

A. the Exchange admin center
B. the Microsoft Purview compliance portal
C. the Microsoft 365 admin center
D. the Microsoft 365 Defender portal
E. the Microsoft Entra admin center

Answer: D

Explanation:

Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal

In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam

Question: 242

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?

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

B. Modify the safe links policy Global settings.

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

D. Create a new safe links policy.

Answer: D

Explanation:

Use the Microsoft 365 Defender portal to create Safe Links policies

In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use https://security.microsoft.com/safelinksv2.

1. On the Safe Links page, select Create to start the new Safe Links policy wizard.

2. On the Name your policy page, configure the following settings:

Name: Enter a unique, descriptive name for the policy.

Description: Enter an optional description for the policy.

3. When you're finished on the Name your policy page, select Next.

4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):

Users: The specified mailboxes, mail users, or mail contacts.

*-> Groups:

Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).

The specified Microsoft 365 Groups.

Domains: All recipients in the specified accepted domains in your organization.

Etc.

Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure

Question: 243

You have a Microsoft 365 E5 subscription.

You need to compare the current Safe Links configuration to the Microsoft recommended configurations.

What should you use?

A. Microsoft Purview
B. Azure AD Identity Protection
C. Microsoft Secure Score
D. the configuration analyzer

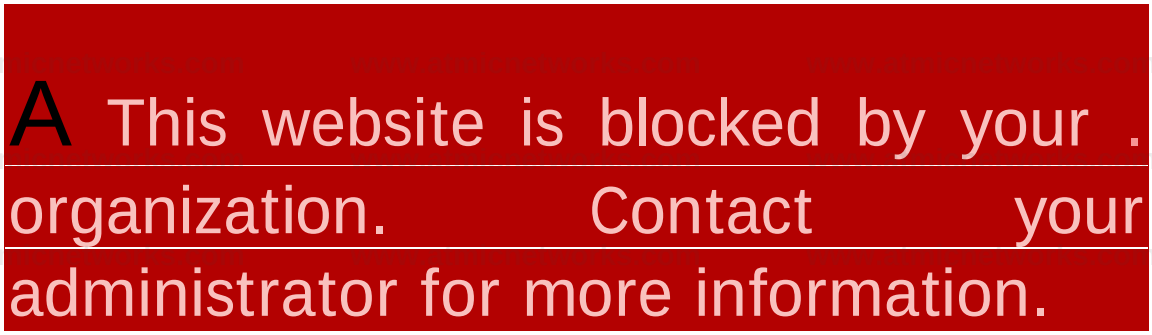
Answer: C

Explanation:

Question: 244

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.



You need to enable user access to the partner company's portal.

Which Microsoft Defender for Endpoint setting should you modify?

A. Alert notifications
B. Alert suppression
C. Custom detections
D. Advanced hunting
E. Indicators

Answer: E

Explanation:

Reference:

https://jadexstrategic.com/web-protection/

Question: 245

HOTSPOT

HOTSPOT

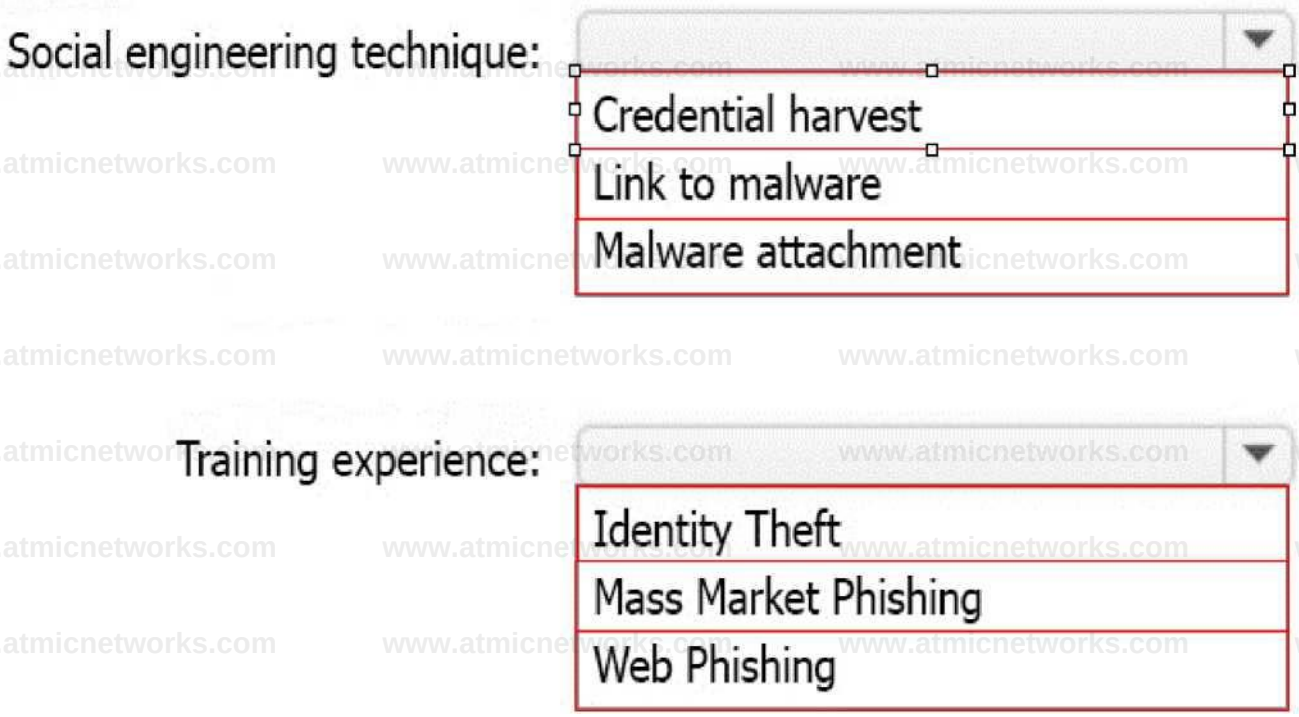
You have a Microsoft 365 E3 subscription.

You plan to launch Attack simulation training for all users.

Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

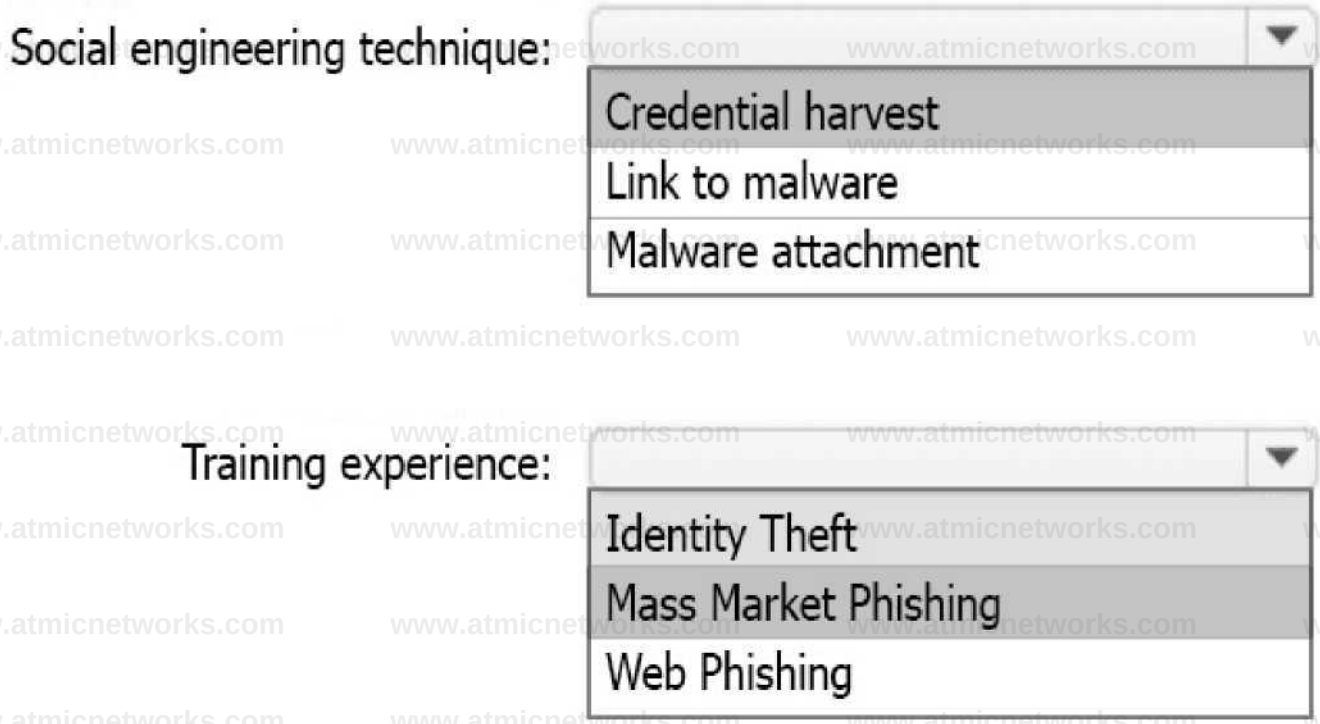
Answer Area



Answer:

Explanation:

Answer Area



Box 1: Credential Harvest

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.

Note: In Attack simulation training, multiple types of social engineering techniques are available:

Credential Harvest

Malware Attachment

Link to Malware

Etc.

Box 2: Mass Market Phishing

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack- simulation-training-get-started

Question: 246

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.

What should you do?

A. Create a newAnti-malware policy
B. Configure the Safe Links global settings.
C. Create a new Anti-phishing policy
D. Configure the Safe Attachments global settings.

Answer: D

Explanation:

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint, OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After files are asynchronously scanned by the common virus detection engine in Microsoft 365, Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation). Safe Attachments for SharePoint, OneDrive, and Microsoft Teams also helps detect and block existing files that are identified as malicious in team sites and document libraries.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe- attachments-for-spo-odfb-teams-about

Question: 247

HOTSPOT

HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device group	Members
1	Groupi	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	***Not applicable***

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.

Settings > Endpoints > computed

computeri

Device summary

Risk level 0

None

Device details

Domain

adatum.com

OS

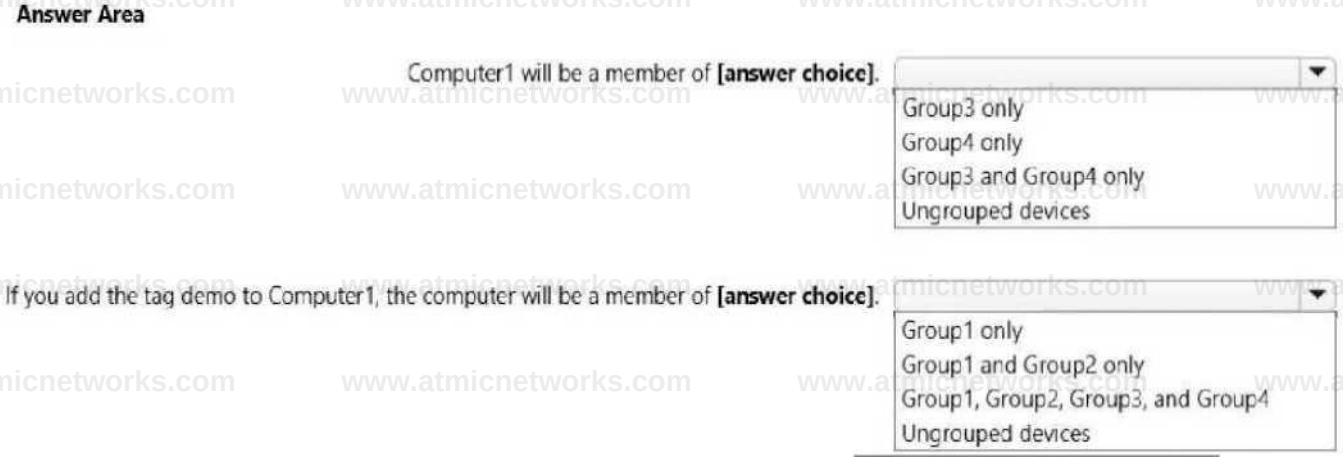
Windows 10 64 bit

Version 21H2

Build 19044.2130

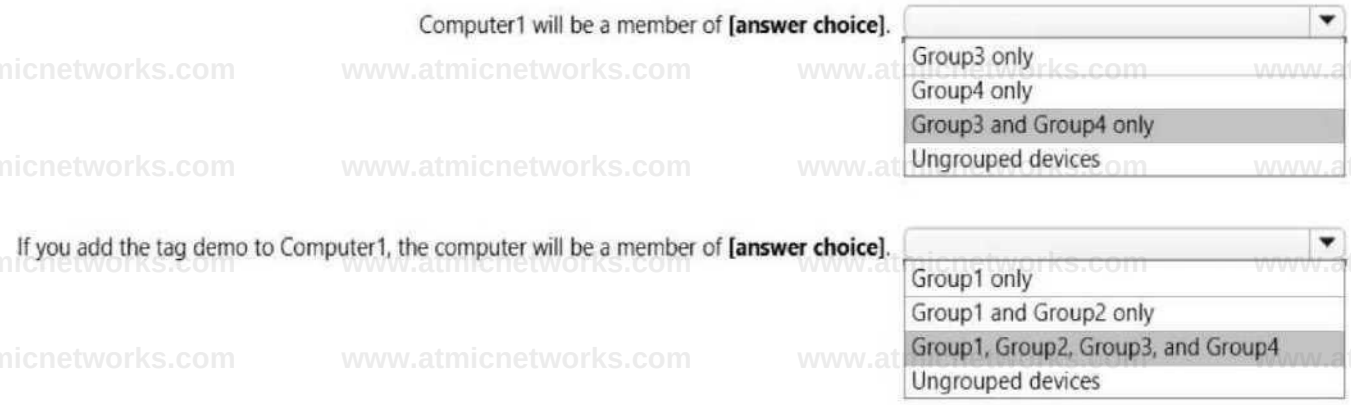
Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Box 1: Group3 and Group4 only
Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10.

Box 2: Group1, Group2, Group3 and Group4

Question: 248

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.

Your company purchases Microsoft 365 and creates an Azure AD tenant named

contoso.onmicrosoft.com.

You plan to install Azure AD Connect on a member server and implement pass-through authentication.

You need to prepare the environment for the planned implementation of pass-through authentication.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From a domain controller install an Authentication Agent

B. From the Microsoft Entra admin center, confiqure an authentication method.

C. From Active Director,' Domains and Trusts add a UPN suffix

D. Modify the email address attribute for each user account.

E. From the Microsoft Entra admin center, add a custom domain name.

F. Modify the User logon name for each user account.

Answer: A,B,E

Explanation:

Deploy Azure AD Pass-through Authentication

Step 1: Check the prerequisites

Ensure that the following prerequisites are in place.

In the Entra admin center

1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.

E.) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.

(A) In your on-premises environment

1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.

2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is supported.

3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.

4. Etc.

(B) Step 2: Enable the feature

Enable Pass-through Authentication through Azure AD Connect.

If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.

Incorrect:

Not C: From Active Directory Domains and Trusts, add a UPN suffix

Not D. Modify the email address attribute for each user account.

Not F. Modify the User logon name for each user account.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta- quick-start

Question: 249

HOTSPOT

HOTSPOT

You have a new Microsoft 365 E5 tenant.

Enable Security defaults is set to Yes.

A user signs in to the tenant for the first time.

Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

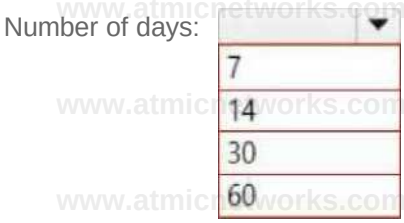
MFA method: □ □

i Call to phone

| Email message

Secunty questions Text message to phone

Notification to Microsoft Authenticator app

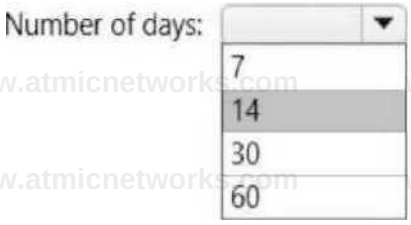


Answer:

Explanation:

Answer Area

MFA method:
Call to phone
Email message
Secunty questions Text message to phone
Notification to Microsoft Authenticator app



Box 1: Notification to Microsoft Authenticator app

Do users have 14 days to register for Azure AD Multi-Factor Authentication?

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Box 2: 14

Azure AD Identity Protection will prompt your users to register the next time they sign in

interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they'll be required to register before they can complete the sign-in process.

Reference:
https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work- remotely-secure-sign-in
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity- protection-configure-mfa-policy

Question: 250

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

Name	Configuration
Groupl	Global security group
Used	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.

Which objects will sync to Azure AD?

A. Group1 only
B. User1 and User2 only
C. Group1 and User1 only
D. Group1, User1, and User2

Answer: D

Explanation:

Disabled accounts
Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.

The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad- connect-sync-user-and-contacts

Question: 251

You have a Microsoft 365 E5 subscription.

You need to create Conditional Access policies to meet the following requirements:

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android and iOS devices.
Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

What is the minimum number of Conditional Access policies you should create?

A. 3
B. 4
C. 5
D. 6
E. 7
F. 8

Answer: B

Explanation:

* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1. One Policy.

* Only users in the R&D department must be blocked from signing in from both Android and iOS devices. One Policy.

* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

One policy

* All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android One Policy

Reference:

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

Question: 252

HOTSPOT

HOTSPOT

Your network contains an on-premises Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Required group membership:

Domain Admins
Domain Users
Server Operators
Enterprise Admins

Answer:

Explanation:

Answer Area

Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.

The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Window's Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.

Incorrect:

* AccessChk

Box 2: Enterprise Admins

IdFix permissions requirements

The user account that you use to run IdFix must have read and write access to the AD DS domain.

If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.

* Enterprise Admins

The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.

Incorrect:

* Domain Admins

Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

* Server Operator

Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.

* Domain Users - too few permissions

The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

Reference:
https://microsoft.github.io/idfix/
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security- groups

Question: 253

HOTSPOT

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
Useri	Groupl	Disabled
User2	Group 1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location 1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:

Users or workload identities assignments: All users

Cloud apps or actions assignment: App1

Conditions: Include all trusted locations

Grant access: Require multi-factor authentication

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When Useri connects to App1 from a device that has an IP address of 131.107.50.10, Useri must use MFA.		O
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.		Q
When User2 connects to Appl from a device that has an IP address of 131.107.5.5, User2 must use MFA.		O

Answer:

Explanation:

Answer Area

Statements	Yes	No
When Useri connects to App1 from a device that has an IP address of 131.107.50.10, Useri must use MFA.		
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	0	0
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.		

Box 1: Yes

131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.

Box 2: Yes.

131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.

Box 3: No.

IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24

Reference:

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

Question: 254

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure AD.

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

A. From the Microsoft Entra admin center, create a conditional access policy
B. From the Microsoft 365 admin center, configure the Modem authentication settings.
C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
D. From Multi-Factor Authentication, configure the service settings.

Answer: A

Explanation:

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi- factor-authentication

Question: 255

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

Identify when a user's credentials are compromised and shared on the dark web. Provide users that have compromised credentials with the ability to self-remediate. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To identify when users have compromised credentials, configure: ____ n ____
registration policy °
JA sign-in risk policy
A user risk policy
A multifactor authentication registration policy

To enable self-remediation,

Generate a temporary password
Require multi-factor authentication
Require password change

Answer:

Explanation:

Answer Area

To identify when users have compromised credentials, configure:

A registration policy
A sign-m risk policy
A user risk policy
A multifactor authentication registration policy

To enable self-remediation, select:

Generate a temporary password Require multi-factor authentication
Require password change

Box 1: A user risk policy
Identify when a user's credentials are compromised and shared on the dark web.

User risk-based Conditional Access policy

Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:

Block access
Allow access but require a secure password change.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.

Box 2: Require password change

Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent

unnecessary noise for administrators

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity- protection-policies#user-risk-based-conditional-access-policy

Question: 256

HOTSPOT

HOTSPOT

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.

The domain contains the users shown in the following table.

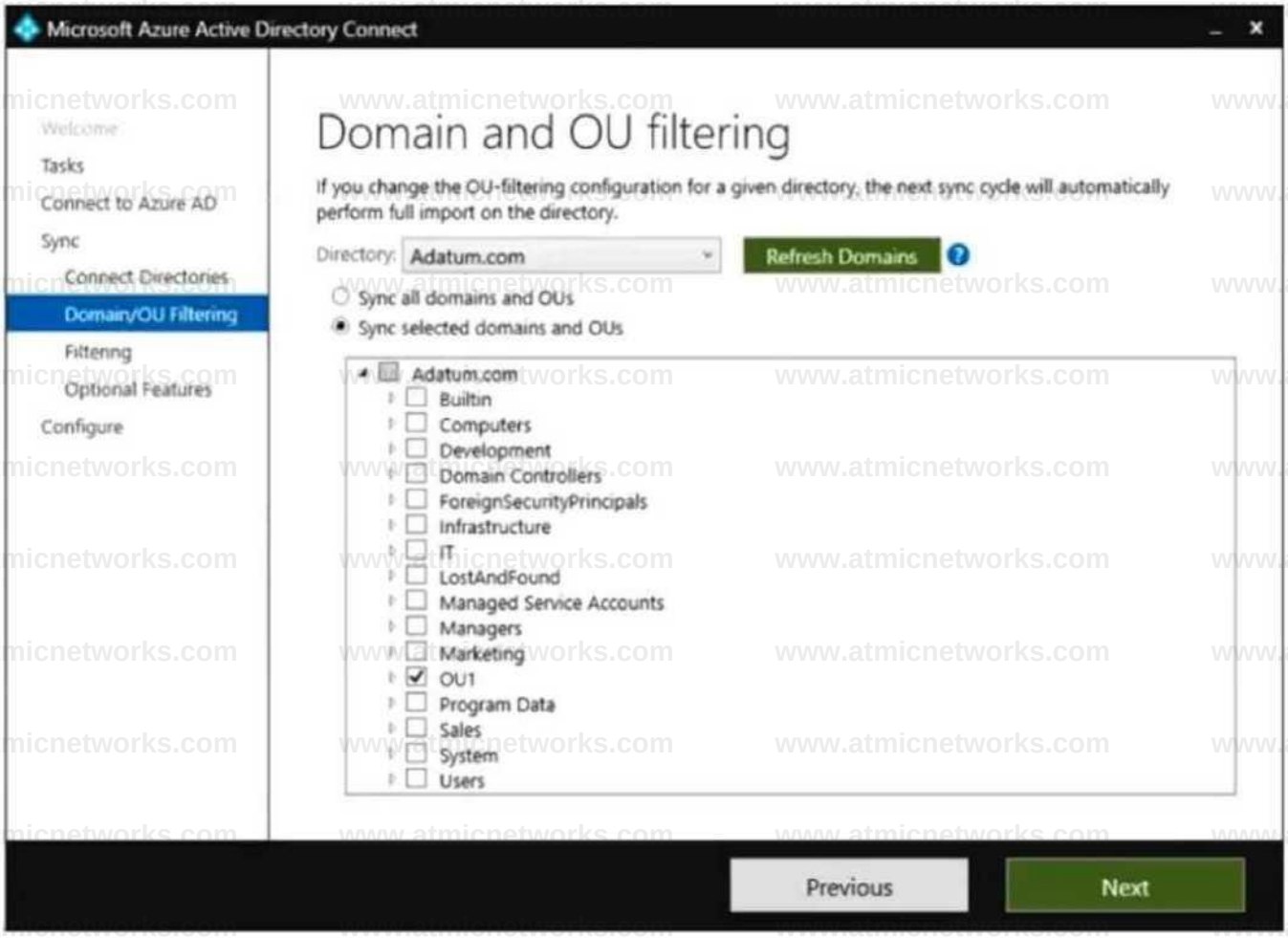
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

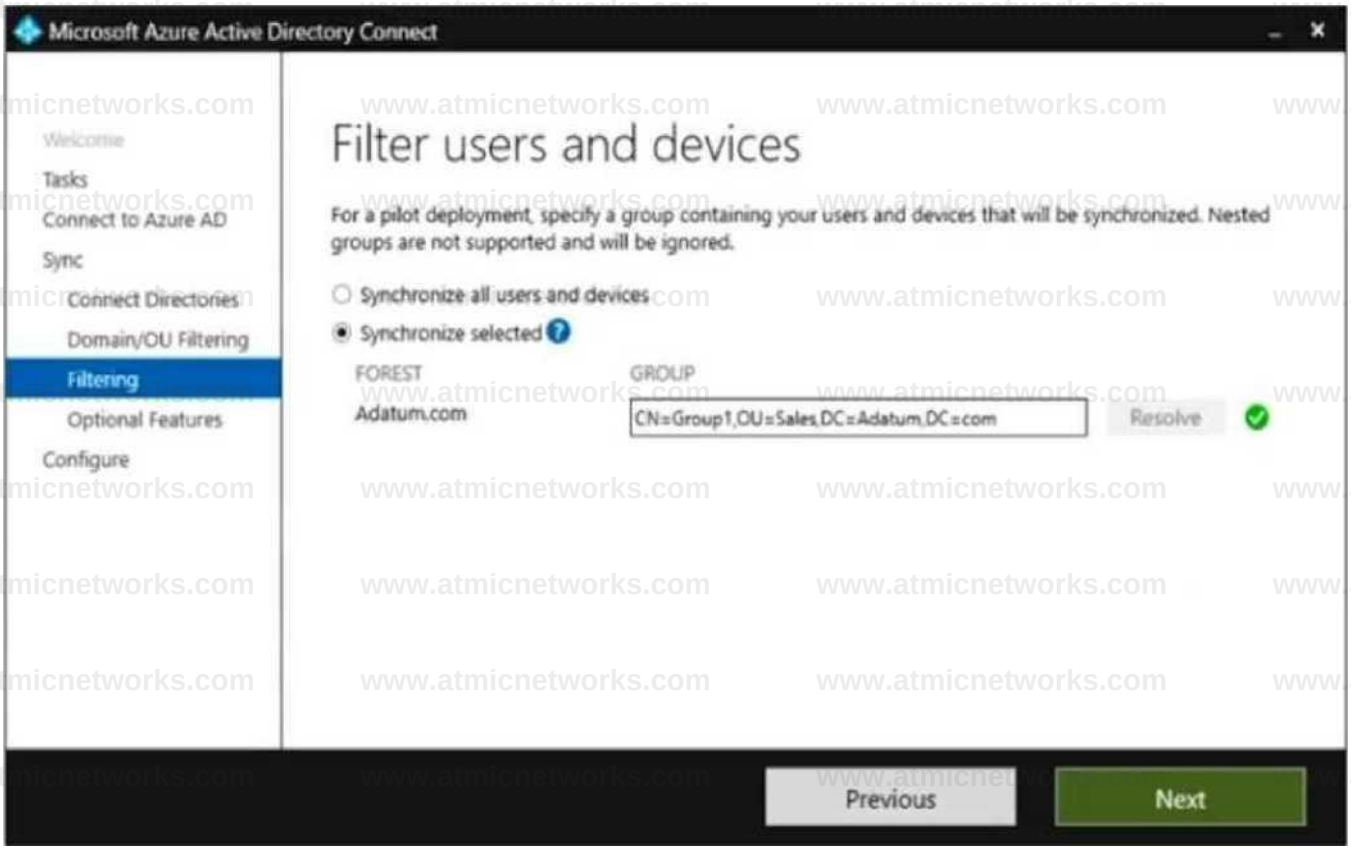
Name	Member of	In OU
Group1	*None*	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.

You configure Domain and OU filtering as shown in the following exhibit.



You configure Filter users and devices as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Useri syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Answer:

Explanation:

Answer Area

Question: 257

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) method registered
Useri	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Groupl	*None*

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.

Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Used will be prompted for passwordless authentication once Useri sets up phone sign-in in ^J the Microsoft Authenticator app.		
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.		
User 3 can use passwordless authentication without further action.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Used will be prompted for passwordless authentication once Useri sets up phone sign-in in the Microsoft Authenticator app.	0	
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	0	
UserS can use passwordless authentication without further action.		1

Box 1: Yes

User1 is member of Group1.

User1 has MFA registered method of Microsoft Authenticater app (push notification)

The Microsoft Authenticator authentication method policy is configured for Group1,

registration is optional, authentication method is any.

Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.

This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.

Box 2: No
User2 is member of Group2.
The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2.

Box 3: No
User3 is member of Group1.
User3 has no MFA method registered.
User3 must choose an authentication method.

Note: Enable passwordless phone sign-in authentication methods
Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they'd like to use.

Reference:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication- passwordless-phone

Question: 258

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII).
Report on shared documents that contain PII.
What should you create?

A. a data loss prevention (DLP) policy
B. a retention policy
C. an alert policy
D. a Microsoft Defender for Cloud Apps policy

Answer: A

Explanation:

Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

From the Security & Compliance tab of your browser, click Home.

Click Data loss prevention > Policy.

Click + Create a policy.

In Start with a template or create a custom policy, click Custom > Custom policy > Next.

In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens Etc.

Reference:

https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting- in-office365-dev-test-environment

Question: 259

You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1.

To which resource can you apply Label1?

A. Group1 only
B. Group2 only
C. Sitel only
D. Groupl and Group2 only
E. Group1, Group2, and Sitel

Answer: E

Explanation:

Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory

Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.

In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.

When you configure a label policy, you can:

Choose which users and groups see the labels. 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://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups- sites

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

Question: 260

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription.

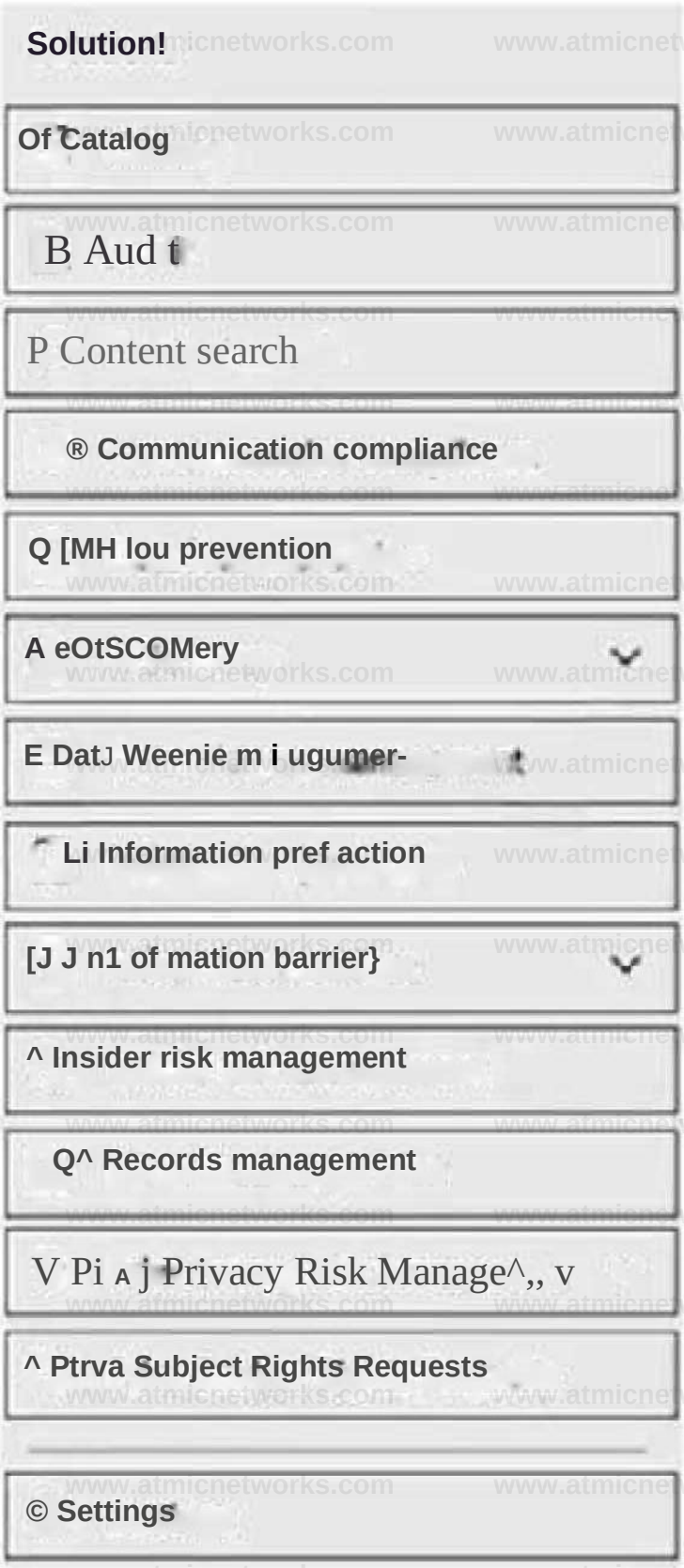
You need to meet the following requirements:

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection

All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.

To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:

In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.

Note: Encryption of data at rest

Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.

BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology. Box 2: Settings

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring

Question: 261

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all

available locations.

Which conditions can you use in the DLP rules of the policy?

A. sensitive info types
B. content search queries
C. keywords
D. sensitivity labels

Answer: C

Explanation:

Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:

Specific types of sensitive information.
Specific keywords that match a query you create.
Pattern matches for a trainable classifier.

Note: Retention policies can be applied to the following locations:

Exchange mailboxes
SharePoint classic and communication sites
OneDrive accounts
Microsoft 365 Group mailboxes & sites
Skype for Business
Exchange public folders
Teams channel messages (standard channels and shared channels)
Teams chats
Teams private channel messages
Yammer community messages
Yammer user messages

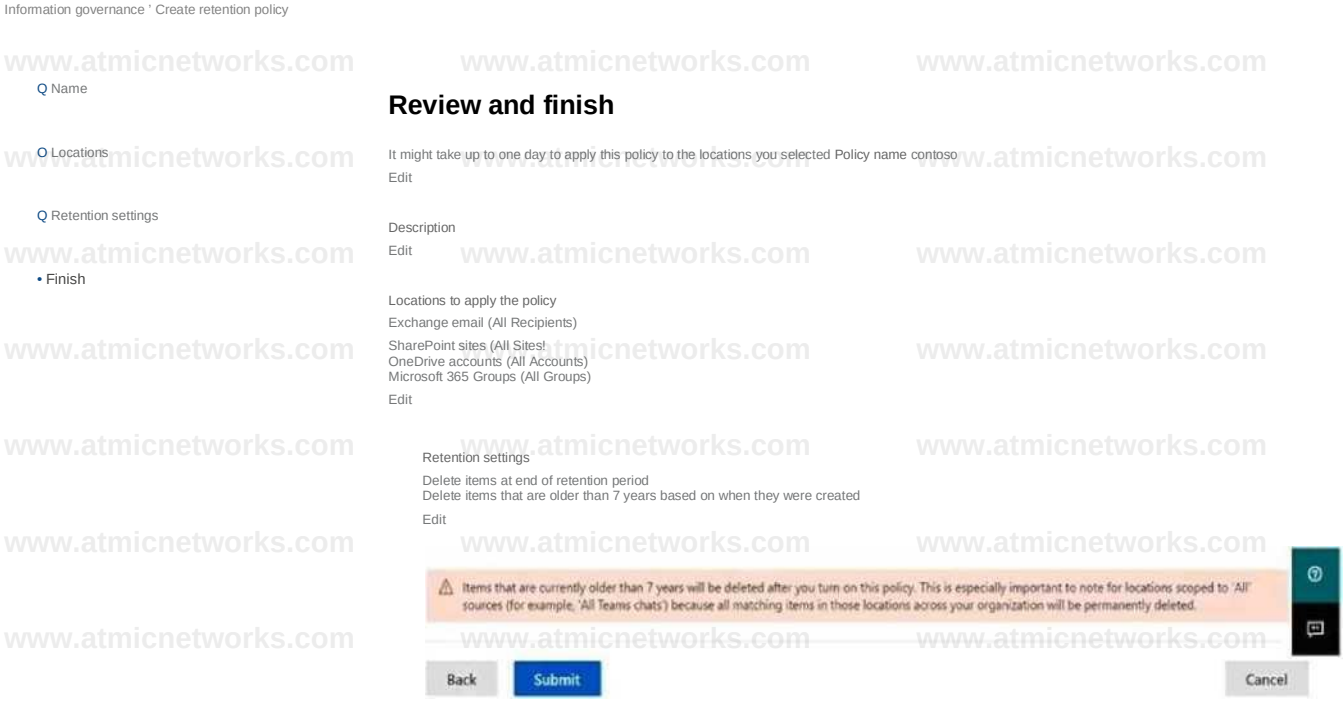
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and- actions

Question: 262

HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy 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

Microsoft SharePoint files that are affected by the policy will **be [answer choice].**

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, **[answer choice],**

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Answer:

Explanation:

Answer Area

Microsoft SharePoint files that are affected by the policy will **be [answer choice].**

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

ZE

Once the policy is created, **[answer choice].**

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Box 1: Deleted seven years after they were created.

From the exhibit:

The retention policy applies to SharePoint sites.

Delete items that are older than 7 years based on when they were created.

Box 2: data will retained for a minimum of seven years

The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.

Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).

For example, if all documents in a SharePoint site should be retained for 5 years, it's more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5 years and others retained for 10 years, a retention policy wouldn't be able to do this. When you need to specify retention settings at the item level, use retention labels.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

Question: 263

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements:

Defines sensitive data based on existing data samples

Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a trainable classifier

B. a sensitive info type

C. an insider risk policy

D. an adaptive policy scope

E. a data loss prevention (DLP) policy

Answer: A,E

Explanation:

A: Classifiers

This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.

Where you can use classifiers

Classifiers are available to use as a condition for:

Office auto-labeling with sensitivity labels

Auto-apply retention label policy based on a condition

Communication compliance

Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.

Data loss prevention

E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

Question: 264

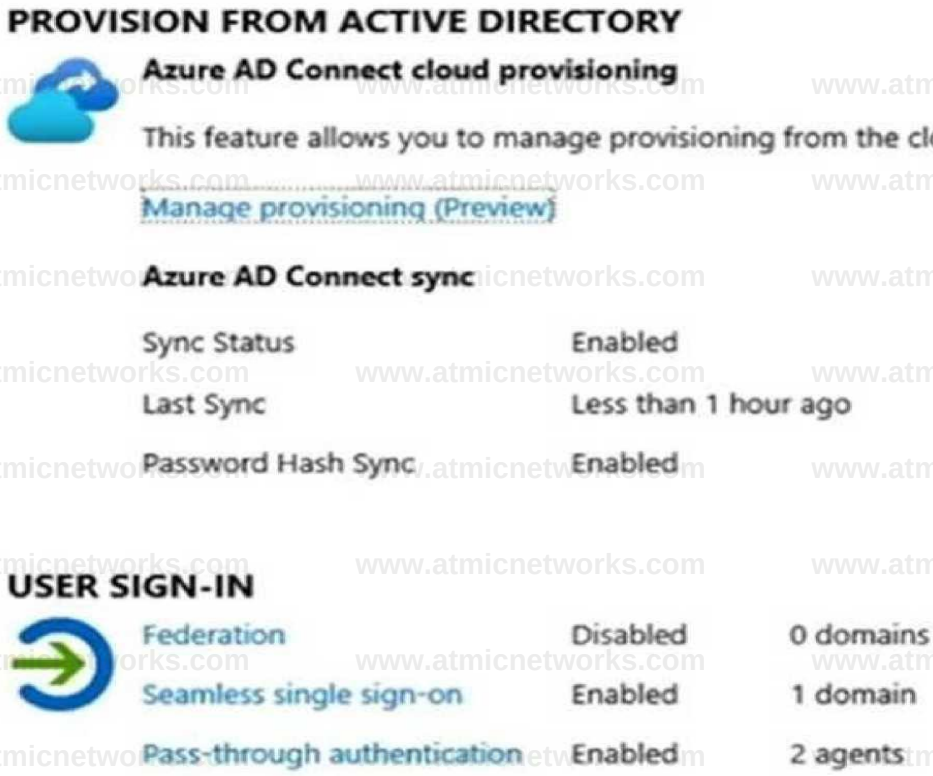
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role.
You instruct User2 to sign in as user2@contoso.com.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

Question: 265

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

Question: 266

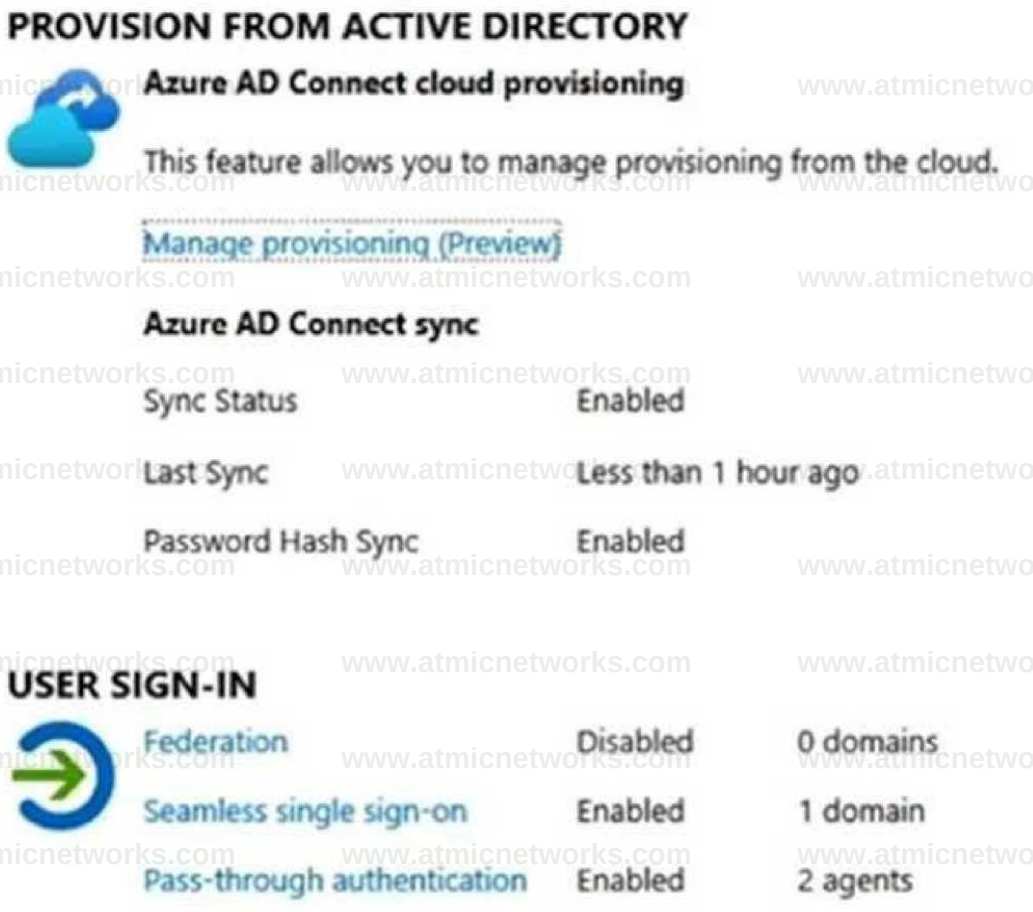
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different

UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

Question: 267

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 network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: You run idfix.exe and export the 10 user accounts.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The question states that “all the user account synchronizations completed successfully”. If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.

It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

Question: 268

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 network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The question states that “all the user account synchronizations completed successfully”.

Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

Question: 269

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 network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The question states that “all the user account synchronizations completed successfully”. Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

Question: 270

HOTSPOT

HOTSPOT

You have a Microsoft 365 subscription.

You need to review metrics for the following:

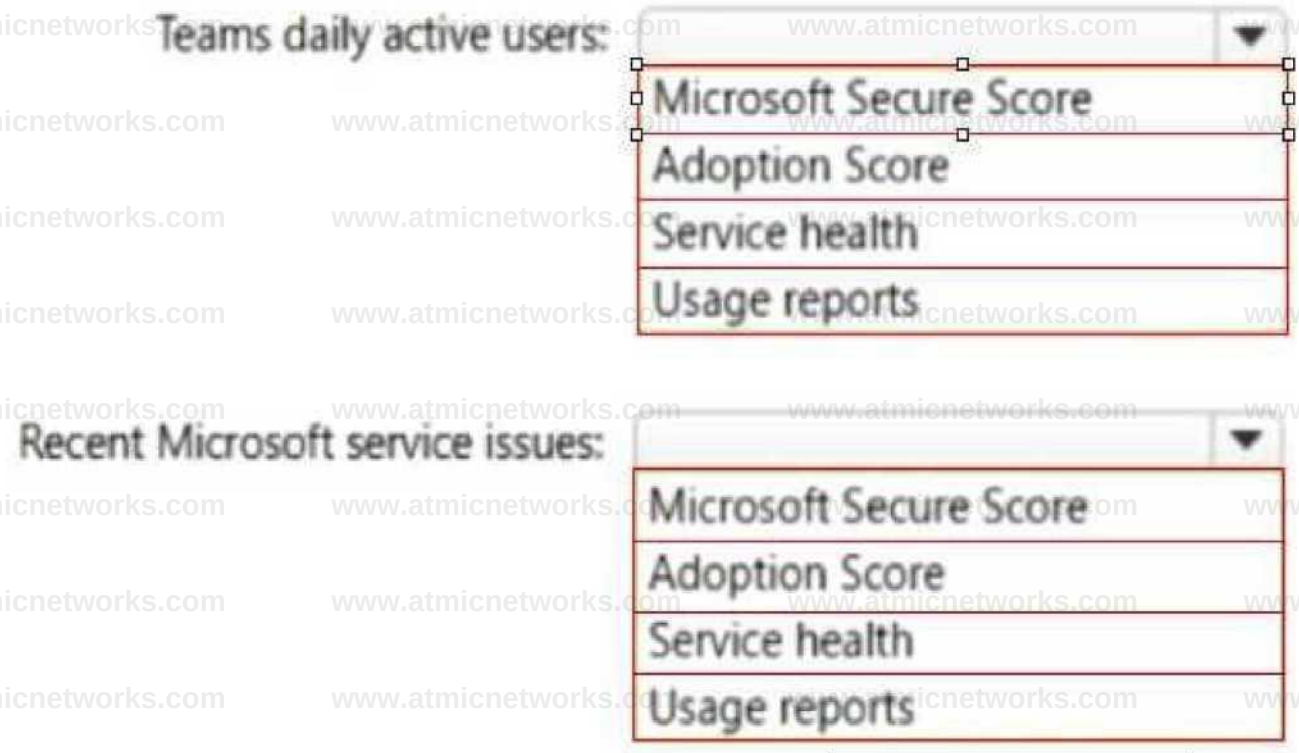
The daily active users in Microsoft Teams

Recent Microsoft service issues

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

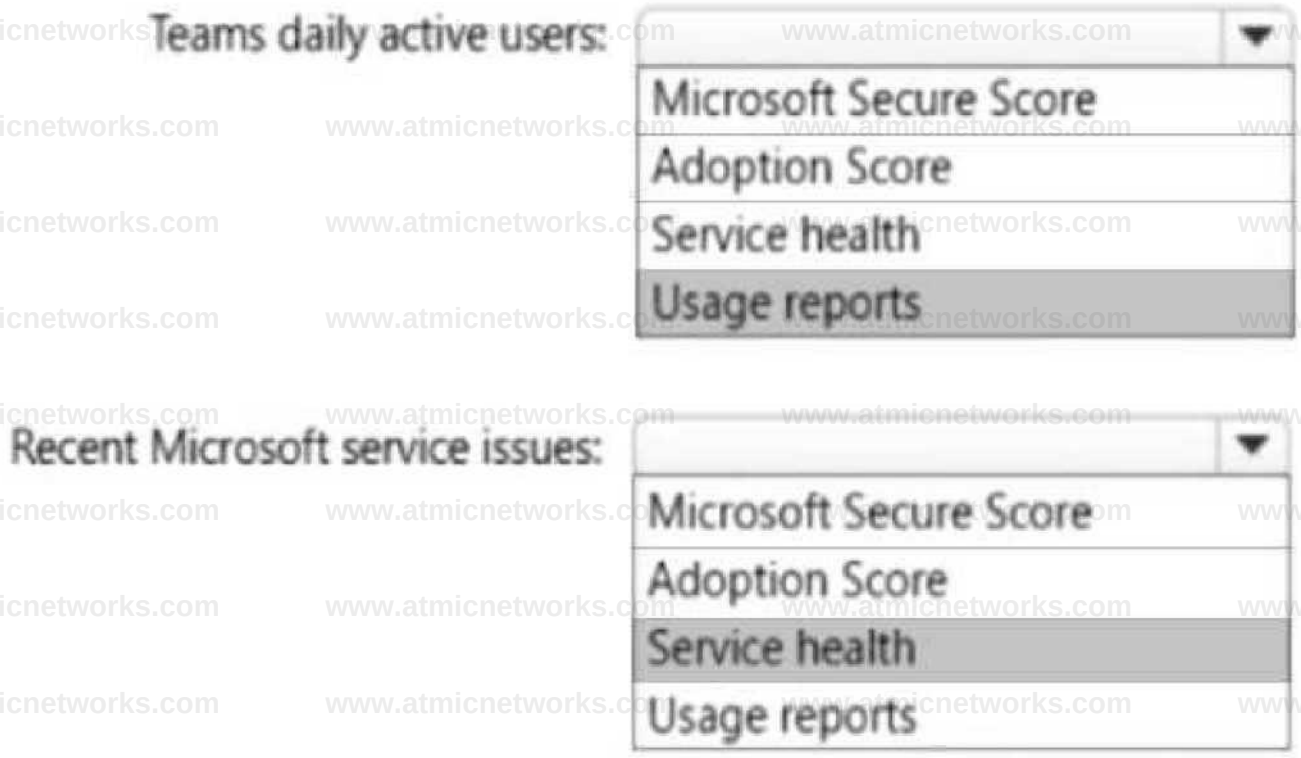
Answer Area



Answer:

Explanation:

Answer Area



Box 1: Usage reports
The daily active users in Microsoft Teams

Microsoft 365 Reports in the admin center - Microsoft Teams usage activity

The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.

Box 2: Service Health

Recent Microsoft service issues

You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft 365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams- usage-activity
https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health

Question: 271

DRAG DROP

DRAG DROP

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.

You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Groupl	• Manage service requests. • Purchase new services. • Manage subscriptions. • Monitor service health.
Group2	• Assign licenses. • Add users and groups. • Create and manage user views. • Update password expiration policies.

The solution must use the principle of least privilege.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles

{'Billing Administrator

"Global Administrator

Helpdesk Administrator

'License Administrator

"Service Support Administrator

User Administrator

Answer Area

Groupi: Role

Group2: Role

Answer:

Explanation:

Roles

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

Answer Area

Groupi: Billing Administrator

Group2: User Administrator

Box 1: Billing admin manage service request Purchase new services Etc.

Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.

Box 2: User admin

User admin

Assign the User admin role to users who need to do the following for all users:

- Add users and groups

- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles

Question: 272

You have a Microsoft 365 subscription.

You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

A. 1

B. 2

C. 5

D. 10

Answer: C

Explanation:

You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq

Question: 273

HOTSPOT

HOTSPOT

You have an Azure AD tenant that contains the administrative units shown in the following table.

Name	Members
AU1	
AU2 \	

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	○
User2 can update the display name of User1.	○	○
User1 can reset the password of User2.	○	○

Box 1: No

User1 is assigned the Password Administrator for AU1 and AU2.

User3 is in AU2. User3 is User Adminstrator.

Password administrators cannot reset User Administrators passwords.

Note: Password Administrator

Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.

Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
User Admin	I^^^^			✓	✓	✓
Usage Summary Reports Reader			5/		V*	

Box 2: Yes

Box 3: No

User1 is assigned the Password Administrator for AU1 and AU2.

User2 is in AU1. User2 is User Adminstrator.

Password administrators cannot reset User Administrators passwords.

Note: User Administrator

Can manage all aspects of users and groups, including resetting passwords for limited admins.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who- can-reset-passwords

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Question: 274

Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.

The domain contains 100 user accounts.

The city attribute for all the users is set to the city where the user resides.

You need to modify the value of the city attribute to the three-letter airport code of each city.

What should you do?

A. From Windows PowerShell on a domain controller, run the Gec-ADUser and Sec-ADUser cmdlets.

B. From Azure Cloud Shell, run the Gec-ADUser and Sec-ADUser cmdlets.

C. From Windows PowerShell on a domain controller, run the Gec-MgUser and Updace- MgUser cmdlets.

D. From Azure Cloud Shell, run the Gec-MgUser and Update-MgUser cmdlets.

Answer: A

Explanation:

The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the onpremise Active Directory.

You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.

Note:

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

1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.

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

1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.

2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set- AzureADUser cmdlets.
3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.

Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser

Question: 275

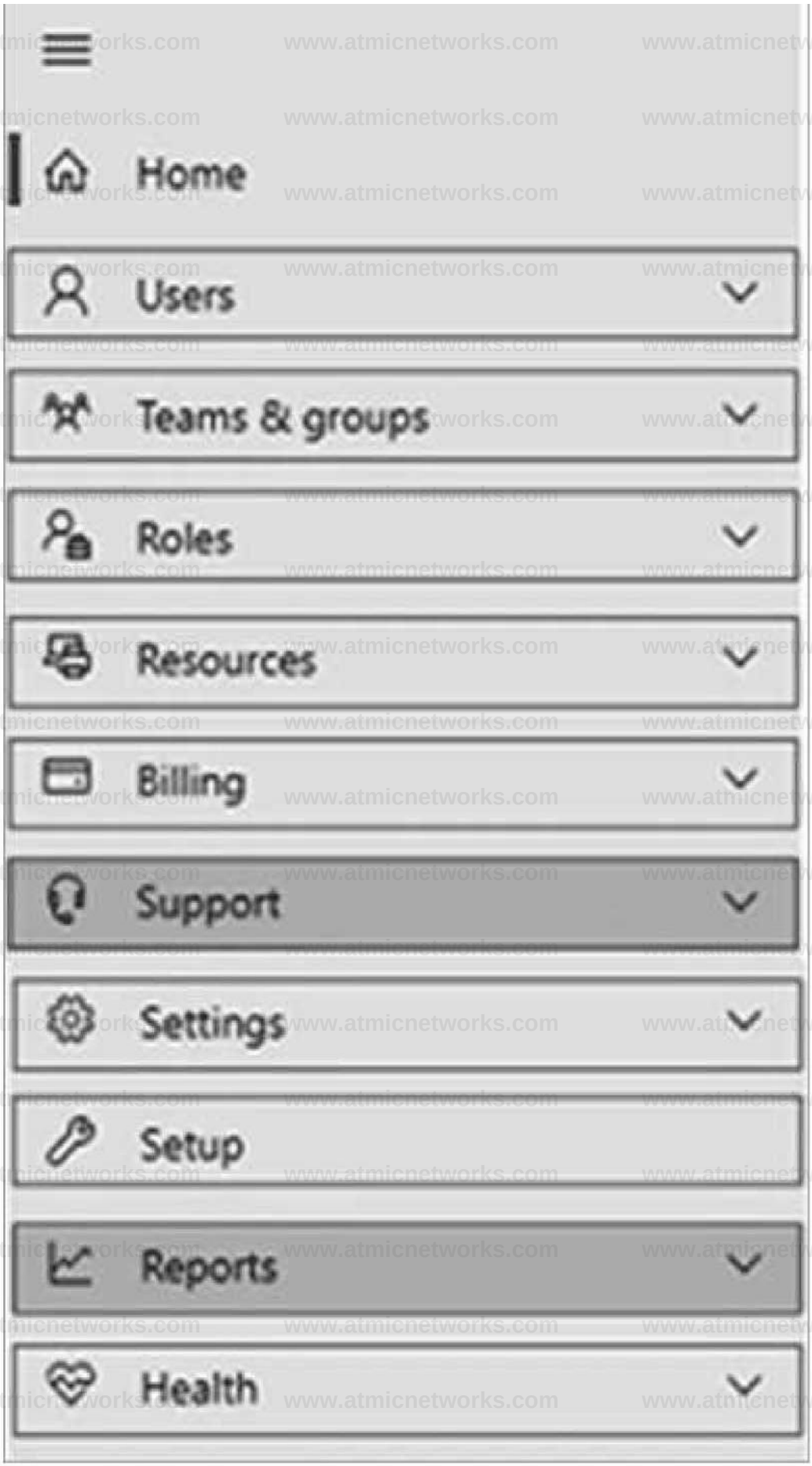
HOTSPOT

HOTSPOT
Your company has a Microsoft 365 E5 subscription.
You need to perform the following tasks:
View the Adoption Score of the company.
Create a new service request to Microsoft.

Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:


Home
Users
Teams & groups
Roles
Resources
Billing
Support
Settings
Setup
Reports
Health

Box 1: Reports
View the Adoption Score of the company.

How to enable Adoption Score
To enable Adoption Score:

Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score
Select enable Adoption Score. It can take up to 24 hours for insights to become available.

Box 2: Support
Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New service request.

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score

https://support.microsoft.com/en-us/topic/contact-microsoft-office-support-fd6bb40e-75b7- 6f43-d6f9-c13d10850e77

Question: 276

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User!	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	*None*

You add another user named User5 to the User Administrator role.
You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Delete User2 and User4 only.
B. Reset the password of User4 only
C. Reset the password of any user in Azure AD.
D. Delete User1, User2, and User4 only.
E. Reset the password of User2 and User4 only.
F. Delete any user in Azure AD.

Answer: A,E

Explanation:

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).

Only on users who are non-admins or in any of the following limited admin roles:

- Directory Readers
- Guest Inviter
- Helpdesk Administrator
- Message Center Reader
- Reports Reader
- User Administrator

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign- admin-roles#available-roles

Question: 277

HOTSPOT

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1.

Group1 is configured as shown in the following exhibit.

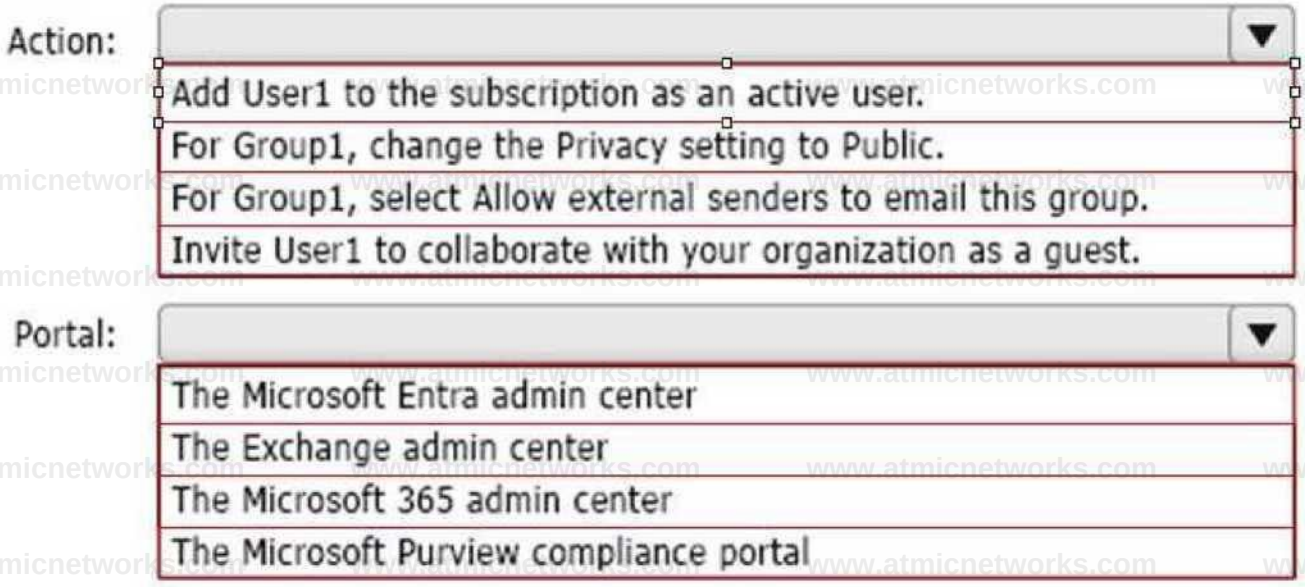
An external user named User1 has an email address of user1@outlook.com.

You need to add User1 to Group1.

What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

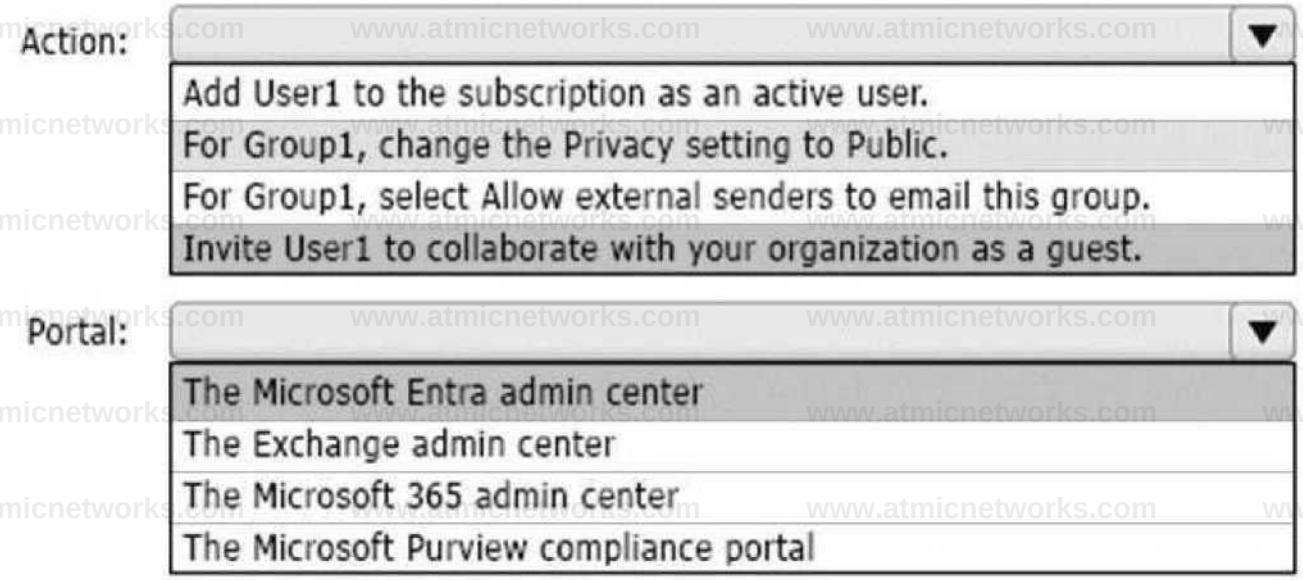
Answer Area



Answer:

Explanation:

Answer Area



Box 1: Invite User1 to collaborate with your organization as a guest.

To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.

Navigate with your Web browser to https://admin.microsoft.com.

On the left pane, click on “Users”, then click “Guest Users”.

On the “Guest Users” page, to create a new guest user, click on either the “Add a guest user”

link on the top of the page or click on “Go to Azure Active Directory to add guest users” link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.com.

On the “New user” page in the Microsoft Azure portal, you must choose to either “Create user” or “Invite user”. If you choose the “Create user” option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the “Invite user” option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the “Invite user” option.

Box 2: The Microsoft Entra admin center

Microsoft Entra admin center unites Azure AD with family of identity and access products

Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

Reference:

https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users

https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with- family-of-identity-and-access-products

Question: 278

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

User1 requires admin access to perform the following tasks:

Manage Microsoft Exchange Online settings.

Create Microsoft 365 groups.

You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.

What should you use?

A. zure AD Identity Protection
B. Microsoft Entra Verified ID
C. Conditional Access

D. Azure AD Privileged Identity Management (PJM)

Answer: D

Explanation:

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.
Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources
Assign time-bound access to resources using start and end dates
Require approval to activate privileged roles
Enforce multi-factor authentication to activate any role
Use justification to understand why users activate
Get notifications when privileged roles are activated
Conduct access reviews to ensure users still need roles
Download audit history for internal or external audit
Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- configure

Question: 279

HOTSPOT

HOTSPOT

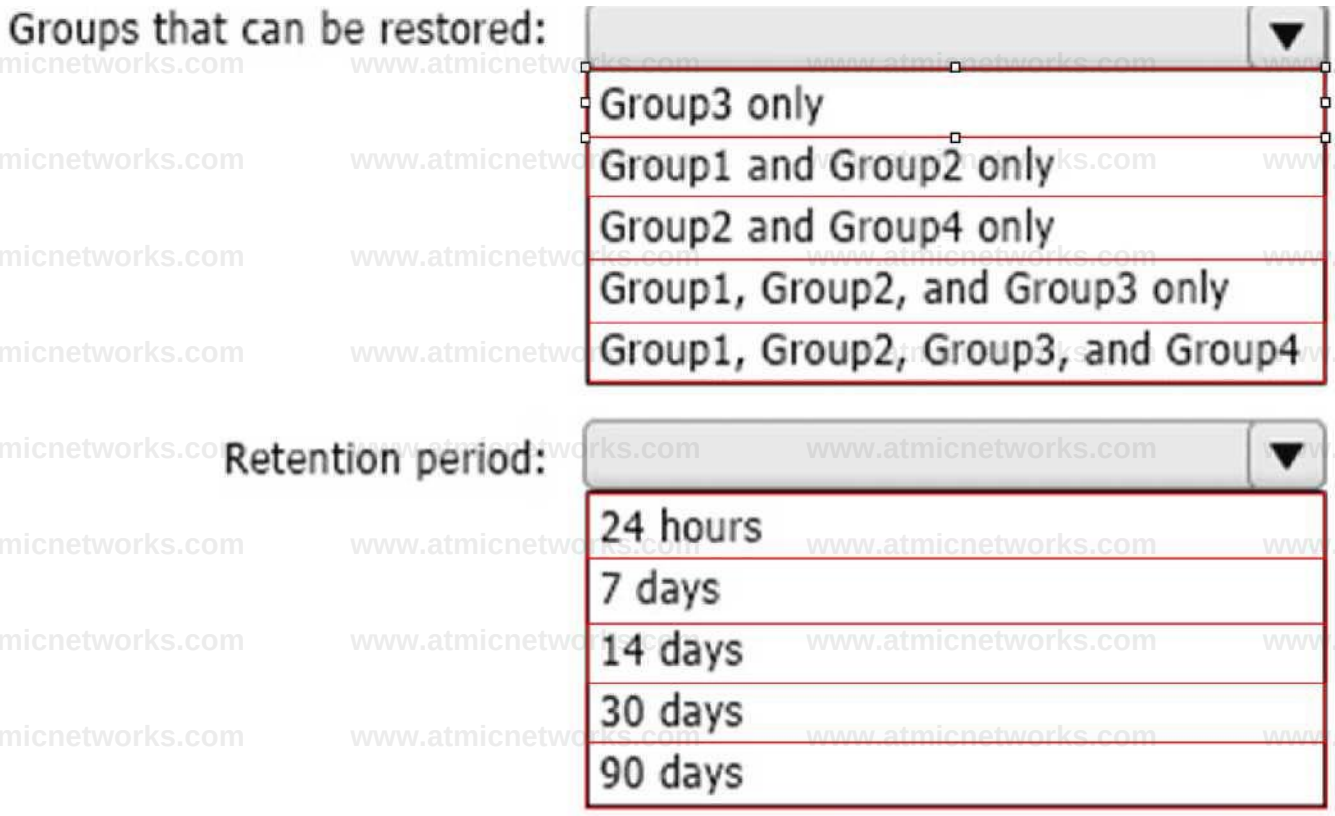
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

All the groups are deleted.

Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.

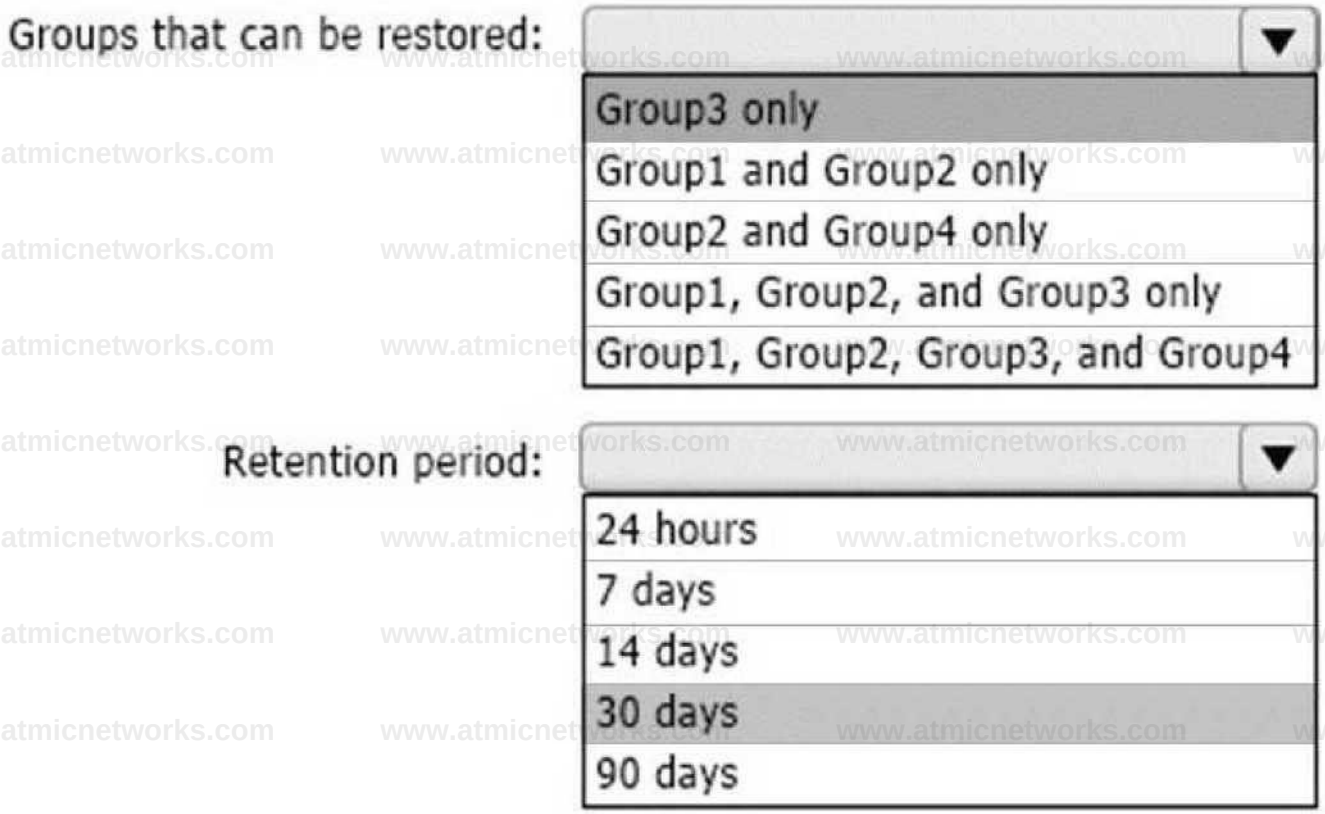
NOTE: Each correct selection is worth one point.



Explanation:

Answer:

Answer Area



Box 1: Group3 only

Box 2: 30 days
If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/restore-deleted-group

Question: 280
HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

Setting	State
Activation maximum duration (hours)	8 hourfs)
On activation, require	Azure MFA
Require justification on actuation	Yes
Require ticket information on activation	NO
Require approval to activate	NO
Approvers	None

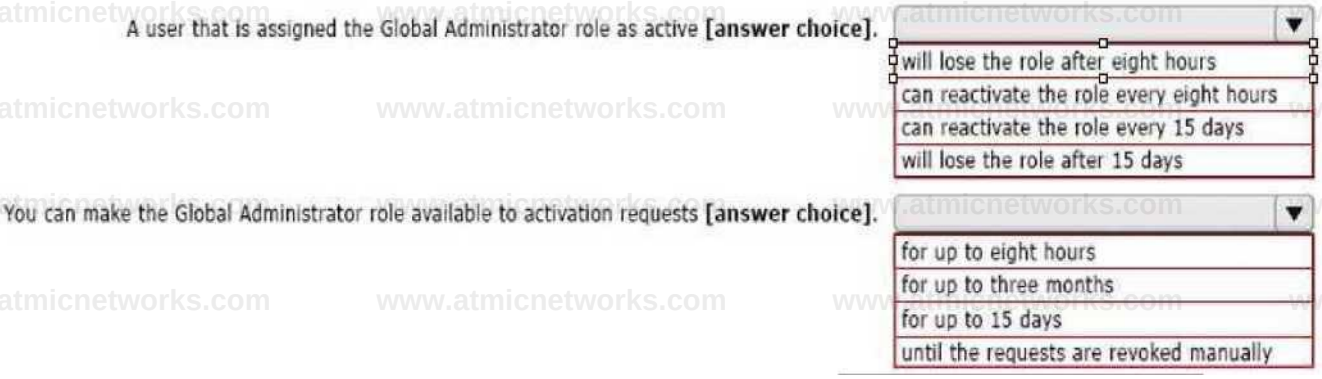
Assignment

Setting	State
Allow permanent eligible assignment	NO
Expire eligible assignments after	3 month($)
Allow permanent active assignment	NO
Expire active assignments after	!5day(s)
Require Azure Multi factor Authentication on active assignment	Yes
Require justification on active assignment	ves

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



Answer

Explanation:

Answer Area

A user that is assigned the Global Administrator role as active [answer choice],

will lose the role after eight hours
can reactivate the role every eight hours
can reactivate the role every 15 days
will lose the role after 15 days

You can make the Global Administrator role available to activation requests [answer choice],

for up to eight hours
for up to three months
for up to 15 days
until the requests are revoked manually

Box 1: will lose the role after eight hours

From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)

Box 2: for up to three months

We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

Question: 281

HOTSPOT

HOTSPOT

You have a Microsoft 365 subscription.

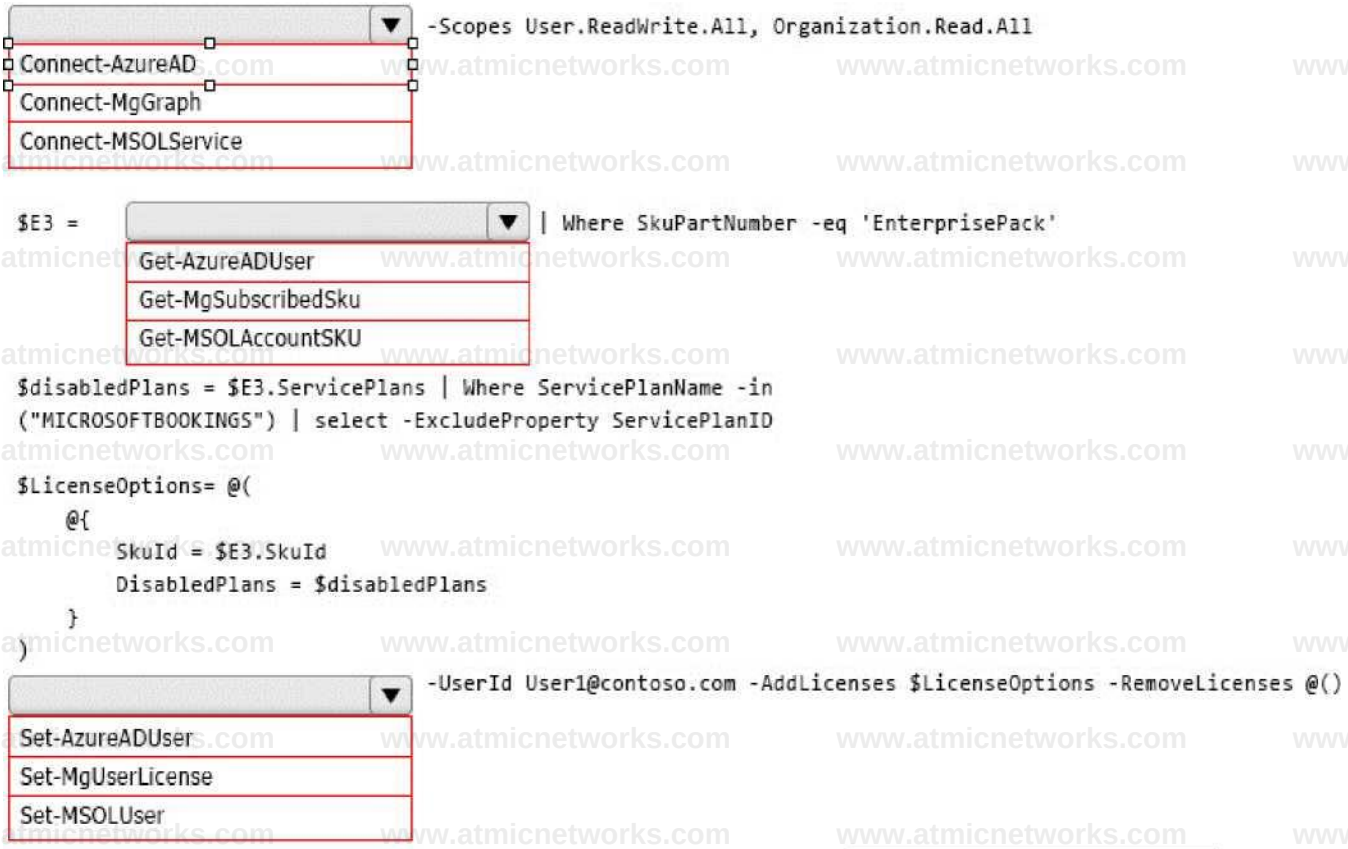
A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

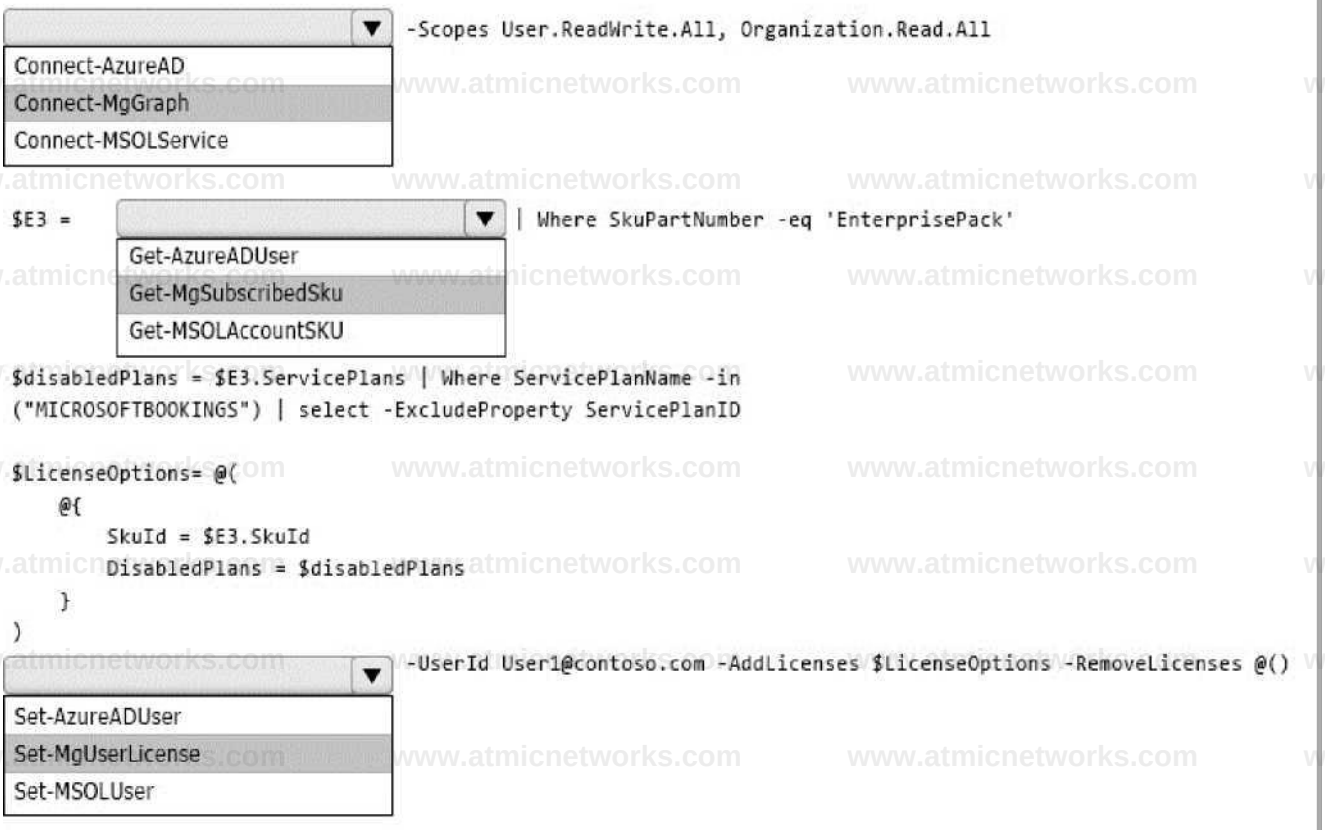
Answer Area



Answer:

Explanation:

Answer Area



Box 1: Connect-MgGraph

Assign Microsoft 365 licenses to user accounts with PowerShell

Use the Microsoft Graph PowerShell SDK

First, connect to your Microsoft 365 tenant.

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All

Box 2: Get-MgSubscribedSku

Run the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.

Box 3: Set-MgUserLicense

Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} -RemoveLicenses @()

This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5' Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId = $e5Sku.SkuId} -RemoveLicenses @()

Reference:
https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell

Question: 282

You have a Microsoft E5 subscription.

You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time.

What should you implement?

A. Azure AD Privileged Identity Management (PIM)
B. a conditional access policy
C. a communication compliance policy)
D. Azure AD Identity Protection
E. groups that have dynamic membership

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

Question: 283

You have a Microsoft 365 subscription.

You suspect that several Microsoft Office 365 applications or services were recently updated.

You need to identify which applications or services were recently updated.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. From the Microsoft365admin center review the Service health blade

B. From the Microsoft365admin center, review the Message center blade.

C. From the Microsoft365admin center review the Products blade.

D. From the Microsoft365Admin mobile agg, review the messages.

Answer: B,D

Explanation:

The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.

The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.

Reference:

https://docs.microsoft.com/en-us/office365/admin/manage/message-center

https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app

Question: 284

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.

Domains

Add domain B Buy domain _ Refresh

Domain name ’	Status	03 Choose columns
□ Sub1.contoso221018.onmicrosoft.com (D... :	A Posable service issues	
D contoso.com	; 0 Incomplete setup	
□ contoso221018.onmicrosoft.com	Q heathy	

J Sub2.contoso221018.onmicrosoft.com 0 Incomplete setup

Which domain name suffixes can you use when you create users?

A. only Sub1.contoso221018.onmicrosoft.com
B. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com
C. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
D. all the domains in the subscription

Answer: B

Explanation:

Question: 285

You have a Microsoft 365 subscription.

You plan to implement Microsoft Purview Privileged Access Management.

Which Microsoft Office 365 workloads support privileged access?

A. Microsoft Exchange Online only
B. Microsoft Teams only
C. Microsoft Exchanqe Online and SharePoint Online only
D. Microsoft Teams and SharePoint Online only
E. Microsoft Teams, Exchanqe Online, and SharePoint Online

Answer: A

Explanation:

Privileged access management

Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero

standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management- solution-overview

https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management

Question: 286

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User'	Global Administrator
User2	Semite Support Administrator
Users	Cloud Application Administrator
User4	None

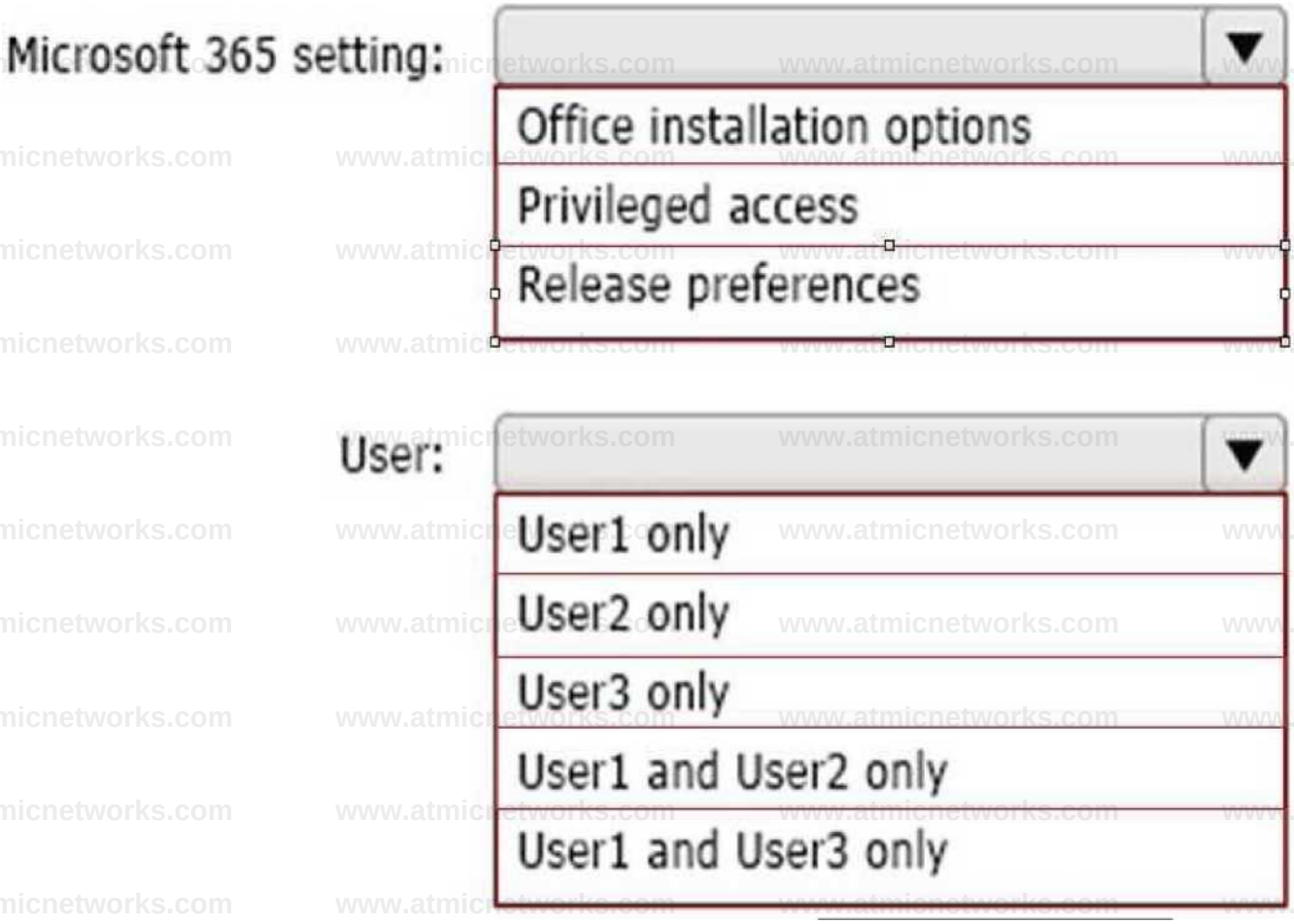
You plan to provide User4 with early access to Microsoft 365 feature and service updates.

You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

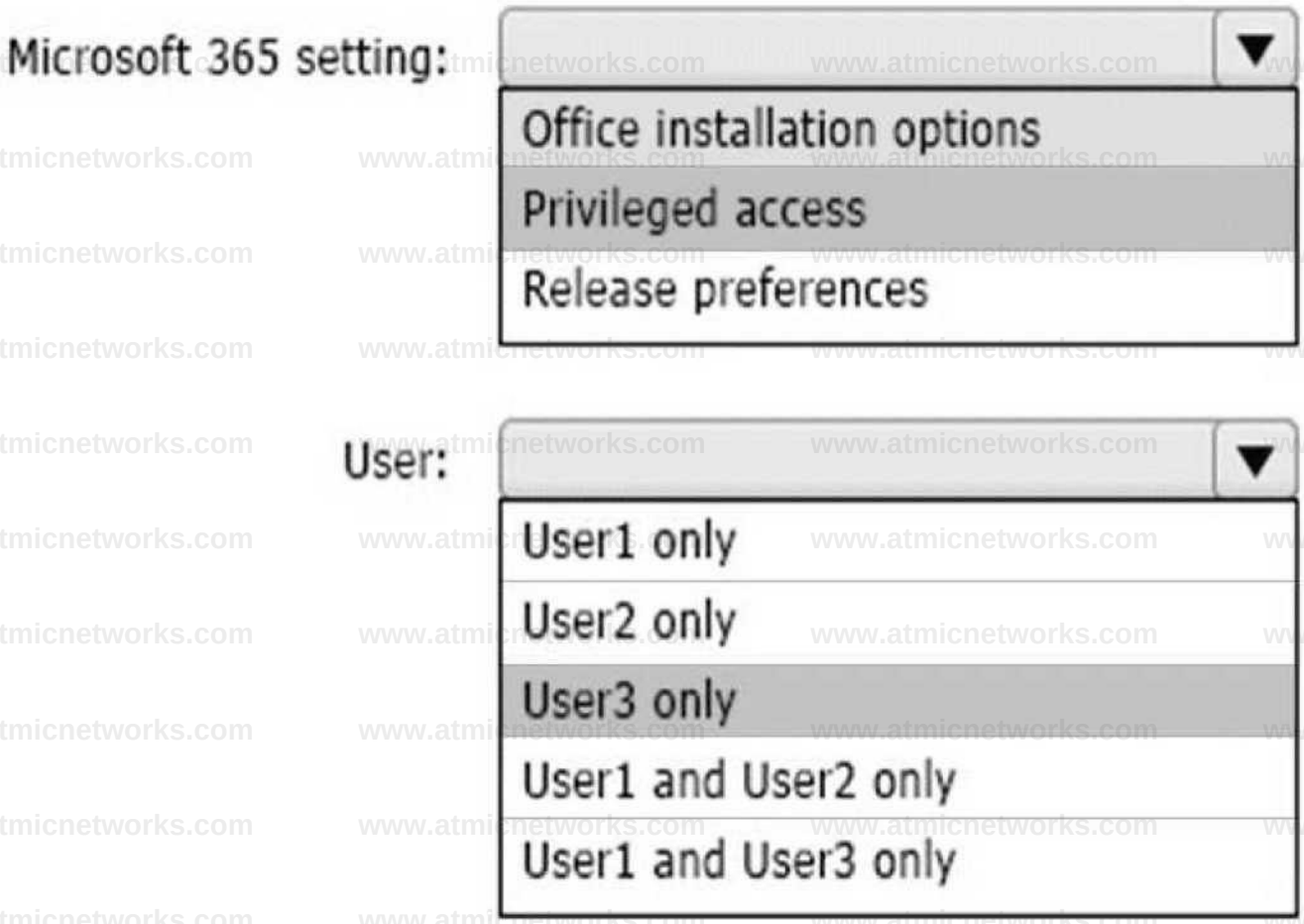
Answer Area



Answer:

Explanation:

Answer Area



Question: 287

HOTSPOT

HOTSPOT
You have a Microsoft 365 subscription.
You are planning a threat management solution for your organization.
You need to minimize the likelihood that users will be affected by the following threats:
Opening files in Microsoft SharePoint that contain malicious content
Impersonation and spoofing attacks in email messages
Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Opening files in SharePoint that contain malicious content: I

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

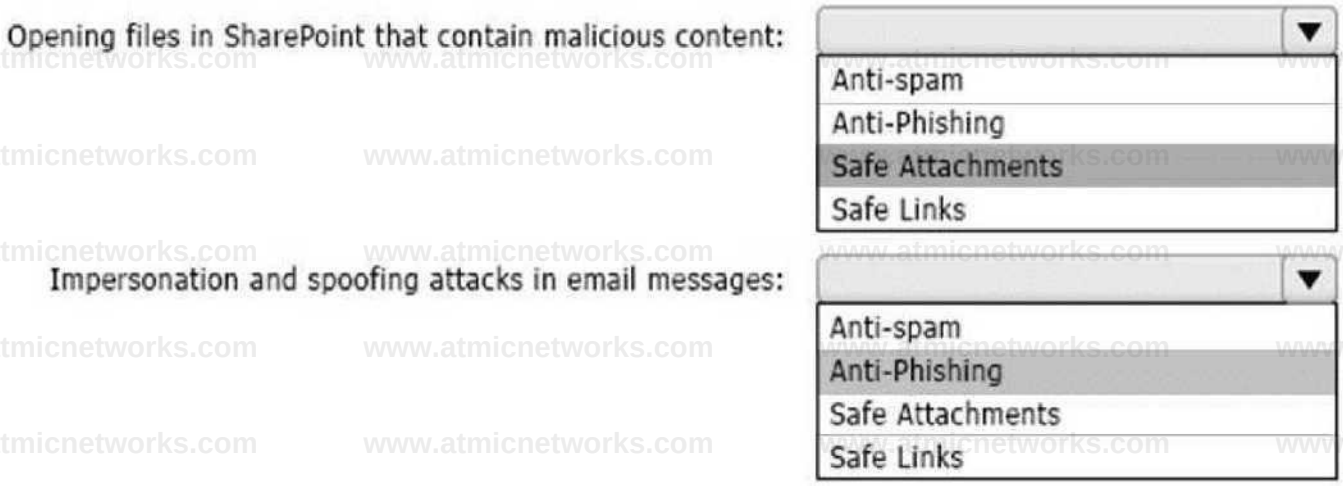
Impersonation and spoofing attacks in email messages: j

Anti-spam
Anti-Phishing Safe Attachments
Safe Links

Answer:

Explanation:

Answer Area



Question: 288

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. advanced hunting
B. security reports
C. digital certificate assessment
D. device discovery
E. attack surface reduction (ASR)

Answer: B,E

Explanation:

B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting
The Microsoft 365 Defender portal (https://security.microsoft.com) provides easy access to information about detected threats and actions to address those threats.

The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created.

The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.

The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab. The Reports section includes reports that show threats detected and their status.

F. What can you expect from Microsoft Defender for Endpoint P1?

Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:

Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks. (E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.

Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.

The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Incorrect:

Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender- endpoint-plan-1

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender- for-endpoint-plan-1-now-included-in-m365-e3/ba-p/3060639

Question: 289

You are reviewing alerts in the Microsoft 365 Defender portal.

How long are the alerts retained in the portal?

A. 30 days
B. 60 days
C. 3 months
D. 6 months
E. 12 months

Answer: C

Explanation:

Data retention information for Microsoft Defender for Office 365

By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.

Defender for Office 365 Plan 1

* Alert metadata details (Microsoft Defender for Office alerts)

90 days.

Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data- retention

Question: 290

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.

What is the longest time range that can be included in the report?

A. 1 day

B. 7 days

C. 30 days

D. 90 days

Answer: C

Explanation:

View email security reports in the Microsoft 365 Defender portal

The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email- security

Question: 291

HOTSPOT

HOTSPOT

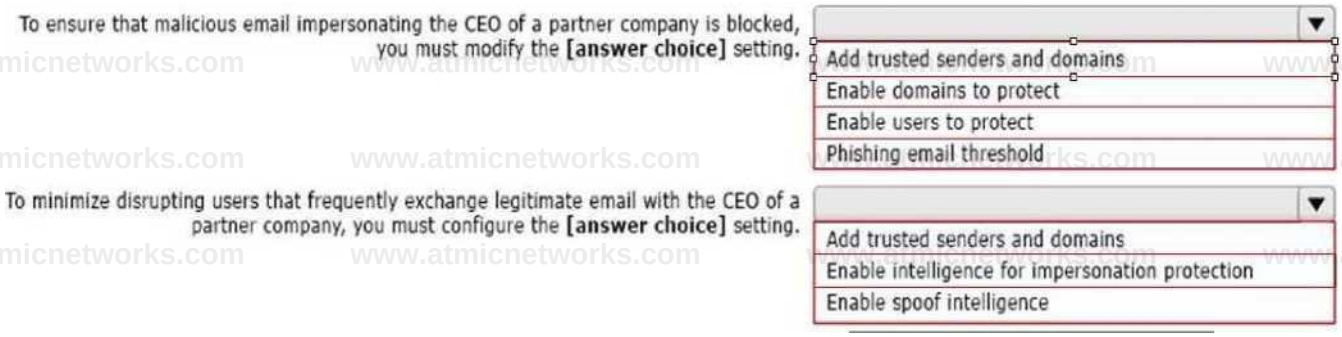
You have a Microsoft 365 subscription.

You deploy the anti-phishing policy 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.

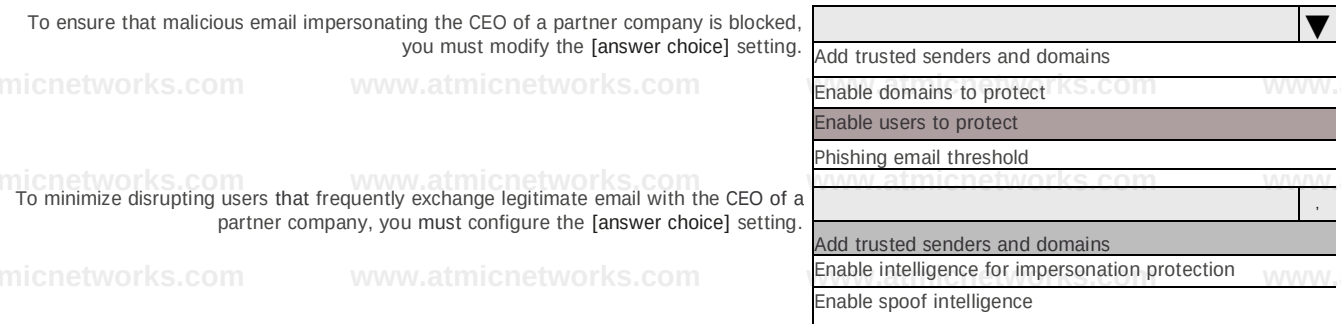
Answer Area



Answer:

Explanation:

Answer Area



Box 1: Enable users to protect

Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.

User impersonation protection

User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.

You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).

When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.

Box 2: Add trusted senders and domains

Trusted senders and domains

Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing- policies-about

Question: 292

DRAG DROP

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to configure policies to meet the following requirements:

Customize the common attachments filter.

Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Policy Types	Answer Area
[3] Anti-malware [0] Anti-phishing [3]Anti-spam 'Safe Attachments	Customize the common attachments filter Enable impersonation protection for sender domains:

Answer:

Explanation:

Policy Types	Answer Area
Anti-malware Anti-phishing Anti-spam Safe Attachments	Customize the common attachments filter Anti malware Enable impersonation protection for sender domains: Anti-phishing

Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

1. Use the Microsoft 365 Defender portal to create anti-malware policies

In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware in the Policies section.
To go directly to the Anti-malware page, use https://security.microsoft.com/antimalwarev2

2. On the Anti-malware page, select Create to open the new anti-malware policy wizard.

On the Name your policy page, configure these settings:

Name: Enter a unique, descriptive name for the policy.
Description: Enter an optional description for the policy.

3. When you're finished on the Name your policy page, select Next.

4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions)

5. On the Protection settings page, configure the following settings:

Protection settings section:

Enable the common attachments filter: If you select this option, messages with the specified attachments are treated as malware and are automatically quarantined. You can modify the list by clicking Customize file types and selecting or deselecting values in the list.

6. Etc.

Box 2: Anti-phishing
Enable impersonation protection for sender domains.

Anti-phishing policies in Microsoft 365

The high-level differences between anti-phishing policies in EOP and anti-phishing policies in Defender for Office 365 are described in the following table:

Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	y	✓
Create custom policies	7	
Common policy settings'	7	y
Spoof settings	7	y
First contact safety tip	7	y
impersonation settings		
Advanced phishing thresholds		y

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware- policies-configure

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing- policies-about

Question: 293

You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?

A. User1
B. User2
C. User3
D. User4

Answer: A

Explanation:

Question: 294

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

Block a vulnerable app until the app is updated.
Block an application executable based on a file hash.

The solution must minimize administrative effort.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Block a vulnerable app until the app is updated:	An alow or block file A file indicator A remediation request An update ring
Block an application executable based on a file hash:	An alow or block file A file indicator A remediation request An update ring

Answer:

Explanation:

Answer Area

Block a vulnerable app until the app is updated:	An alow or block file A file indicator A remediation request An update ring
Block an application executable based on a file hash:	An alow or block file A file indicator A remediation request An update ring

Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.

Select a security recommendation to see a flyout with more information.

Select Request remediation.

Select whether you want to apply the remediation and mitigation to all device groups or only a few.

Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.

Pick a Remediation due date and select Next.

Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied. Review the selections you made and Submit request. On the final page you can choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability- management/tvm-block-vuln-apps

Question: 295

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group 1	**Tog Contains Inventory And OS in Android**
2	Group2	**Hare Starts with Device And Tag Contains Inventory**
Last	Ungrouped devices (default)	*Not applicable*

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	**Rule!**
Alert severity	Low
Dewce group scope	Group i. Groups
Recipient em^c address	Usef1@contcso.com

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Devicel, an incident email notification will be sent	○	○
If a low-severity incident is triggered for Computeri, an incident notification email will be sent.	○	○
If a low-seventy incident is triggered for Devices, an incident notification email will be sent	○	○

Answer:

Explanation:

Answer Area

Statements	Yes	No
If a high-seventy incident is triggered for Devicel an incident email notification will be sent		
If a low-severity incident is triggered for Computer!, an incident notification email will be sent		
If a low-seventy incident is triggered for Devices, an incident notification email will be sent.		

Box 1: No
Device1 is in Group2 as Name starts with Device and Tag contains Inventory.
However, the Group2 has alert severity low.

Box 2: No
Computer1 does not belong to either Group1 or Group2

Box 3: Yes
Device3 belongs to both Group1 and Group2.

Note: Understanding alert severity
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.

The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue

Question: 296

Your company has 10,000 users who access all applications from an on-premises data center.

You plan to create a Microsoft 365 subscription and to migrate data to the cloud.

You plan to implement directory synchronization.

User accounts and group accounts must sync to Azure AD successfully.

You discover that several user accounts fail to sync to Azure AD.

You need to resolve the issue as quickly as possible.

What should you do?

A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.

B. Run idfix.exe, and then click Edit.

C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.

D. Run idfix.exe, and then click Complete.

Answer: B

Explanation:

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch- with-idfix

Question: 297

HOTSPOT

HOTSPOT

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

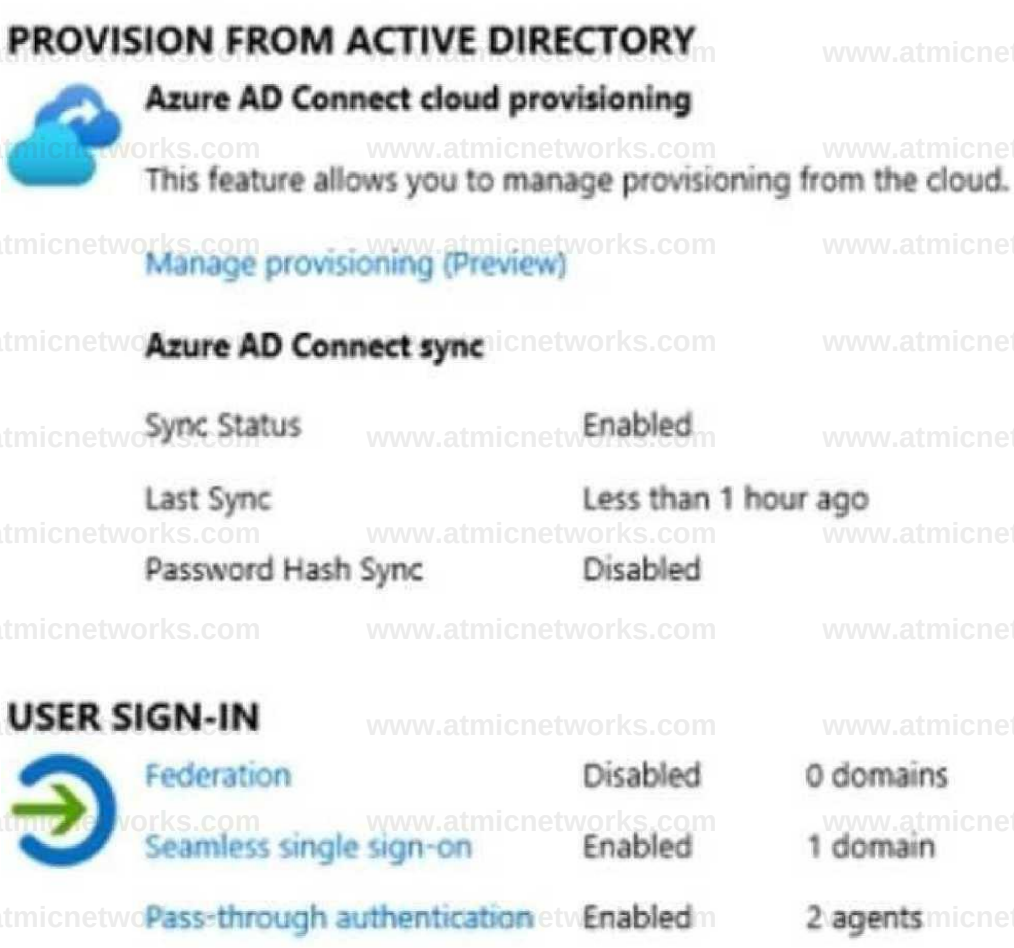
Contoso.com

East.contoso.com

The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Useri can authenticate to Azure AO by using a username of user1@contoso.com.	☐	☐
User? can authenticate to Azure AD by using a username of user2@contoso.com.	☐	☐
UserS can authenticate to Azure AD by using a username of user3@contoso.com.	☐	☐

Answer:

Explanation:

Box 1: Yes

The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.

Box 2: No

The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.

Box 3: No

The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

Question: 298

HOTSPOT

HOTSPOT

Your network contains an on-premises Active Directory domain. The domain contains the

servers shown in the following table.

Name	Operating system	Configuration
Serveri	Windows Server 2022	Domain controller
Server?	Windows Server 2016	Member server
Server?	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Install:

The Azure AD Application Proxy connector
Azure AD Connect
The Azure AD Connect provisioning agent
Active Directory Federation Services (AD FS)

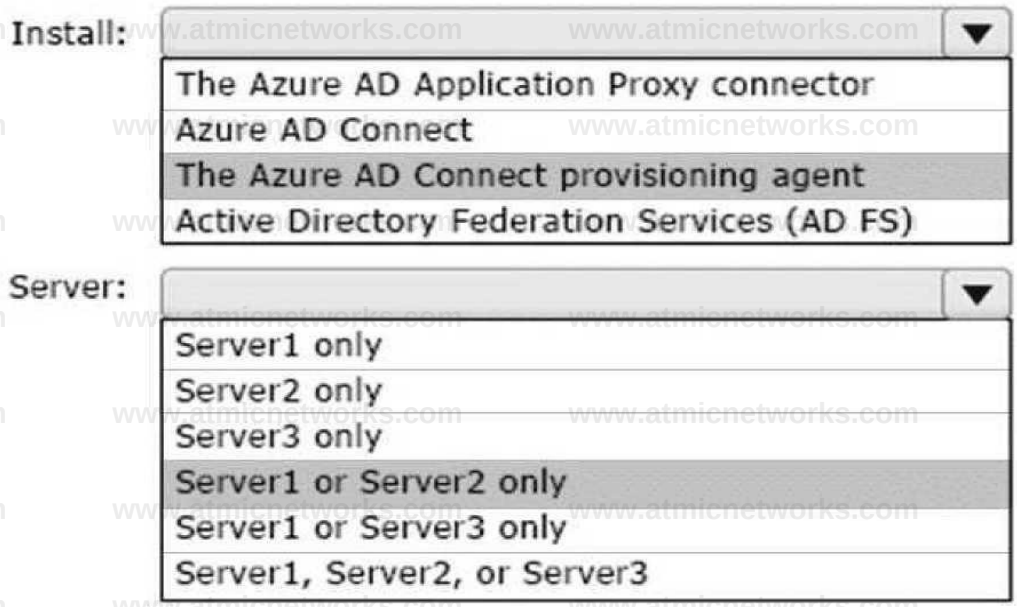
Server:

Serveri only
Server? only
Seiver3 only
Server! or Server? only
Serveri or Servers only
Serveri, Server?, or Server?

Answer:

Explanation:

Answer Area



Box 1: The Azure AD Connect provisioning agent

Install the Azure AD Connect provisioning agent

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

* An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites

Question: 299

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings: 1.Assignments

Users or workload identities: Group1

Cloud apps or actions: Office 365 SharePoint Online

Conditions

- Filter for devices: Exclude filtered devices from the policy
- Rule syntax: device.displayName -startsWith "Device"

2. Access controls

Grant

- Grant: Block access

Session: 0 controls selected

3. Enable policy: On

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Useri can access Sitel from Devicel.	○	○
User? can access Sitel from Device?.	○	○
User2 can access Sitel from Device3.	○	○

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can access Sitel from Devicel.	pj	0
User2 can access Sitel from Device?.	0	
User2 can access Sitel from Devices.		

Box 1: No

User1 is member of Group1 and has Device1.

Device1 is not Azure AD joined.

Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.

Box 2: Yes

User2 is member of Group1 and has devices Device2 and Device3.

Device2 is Azure AD joined.

Device2 is excluded from CAPolicy1 (which would block access to Site1).

Box 3: Yes

User2 is member of Group1 and has devices Device2 and Device3.

Device3 is Android and is Azure AD registered.

Device3 is excluded from CAPolicy1 (which would block access to Site1).

Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto- conditional-access-policy-compliant-device

Question: 300

You have a Microsoft 365 E5 subscription.

Conditional Access is configured to block high-risk sign-ins for all users.

All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month. You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.

What should you configure?

A. an exclusion group
B. the MFA registration policy
C. named locations
D. self-service password reset (SSPR)

Answer: D

Explanation:

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

Question: 301

You have a Microsoft 365 E5 subscription that contains the following user:

Name: User1

UPN: user1@contoso.com

Email address: user1@marketmg.contoso.com

MFA enrollment status: Disabled

When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.

You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.

What should you do?

A. Assign an MFA registration policy to User1.
B. Reset the password of User1.
C. Add an alternate email address for User1.
D. Modify the UPN of User1.

Answer: D

Explanation:

Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.

Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.

Configure the Azure AD multifactor authentication registration policy

Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.

Reference:

https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname

Question: 302

HOTSPOT

HOTSPOT

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

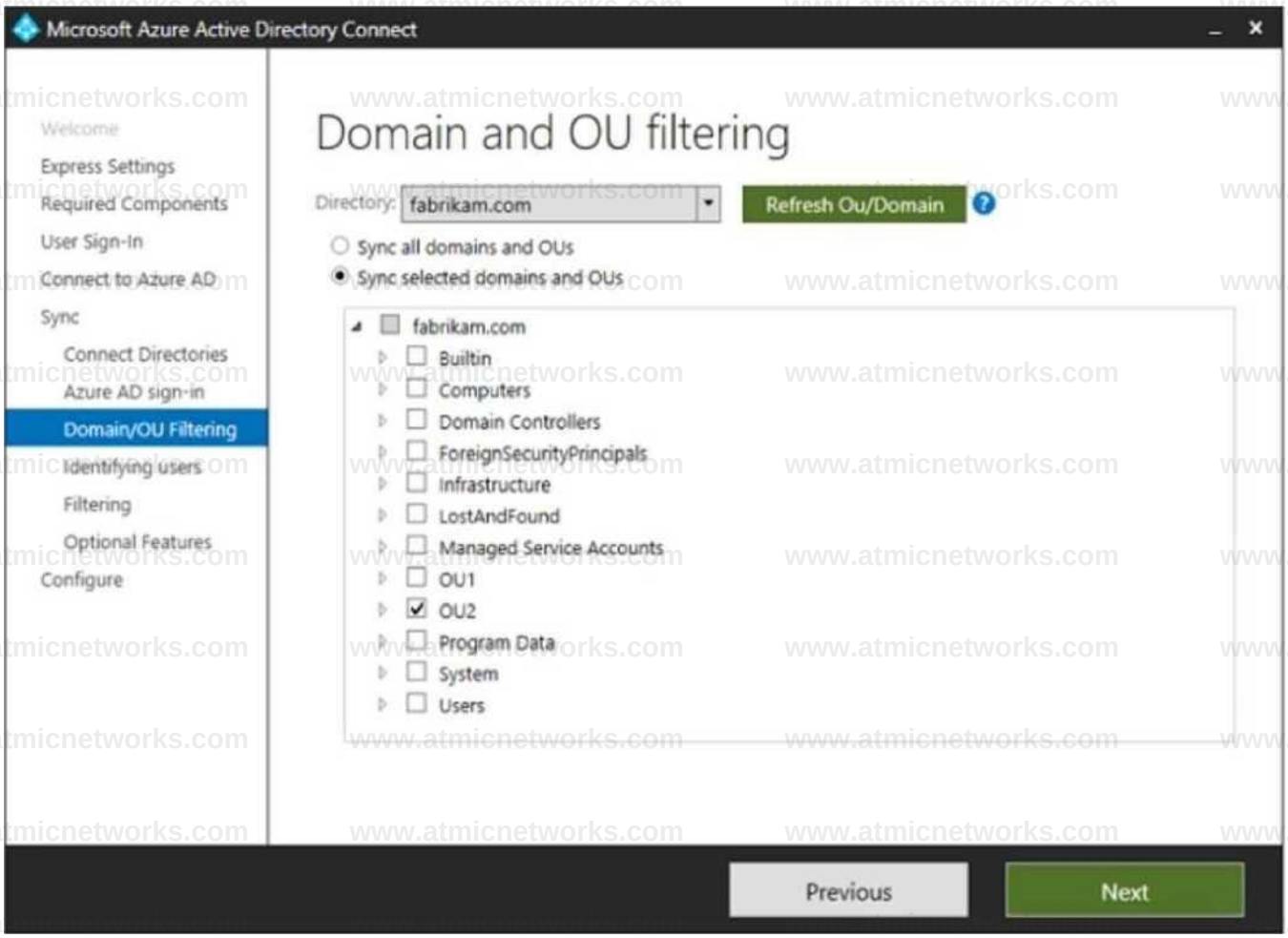
Name	Type	In organizational unit (OU)
Used	User	OU1
I User?	User	OU1
Groupl	Security Group - Global	GUI
User?	User	ou?
Group?	Security Group - Global	OU2

The groups have the members shown in the following table.

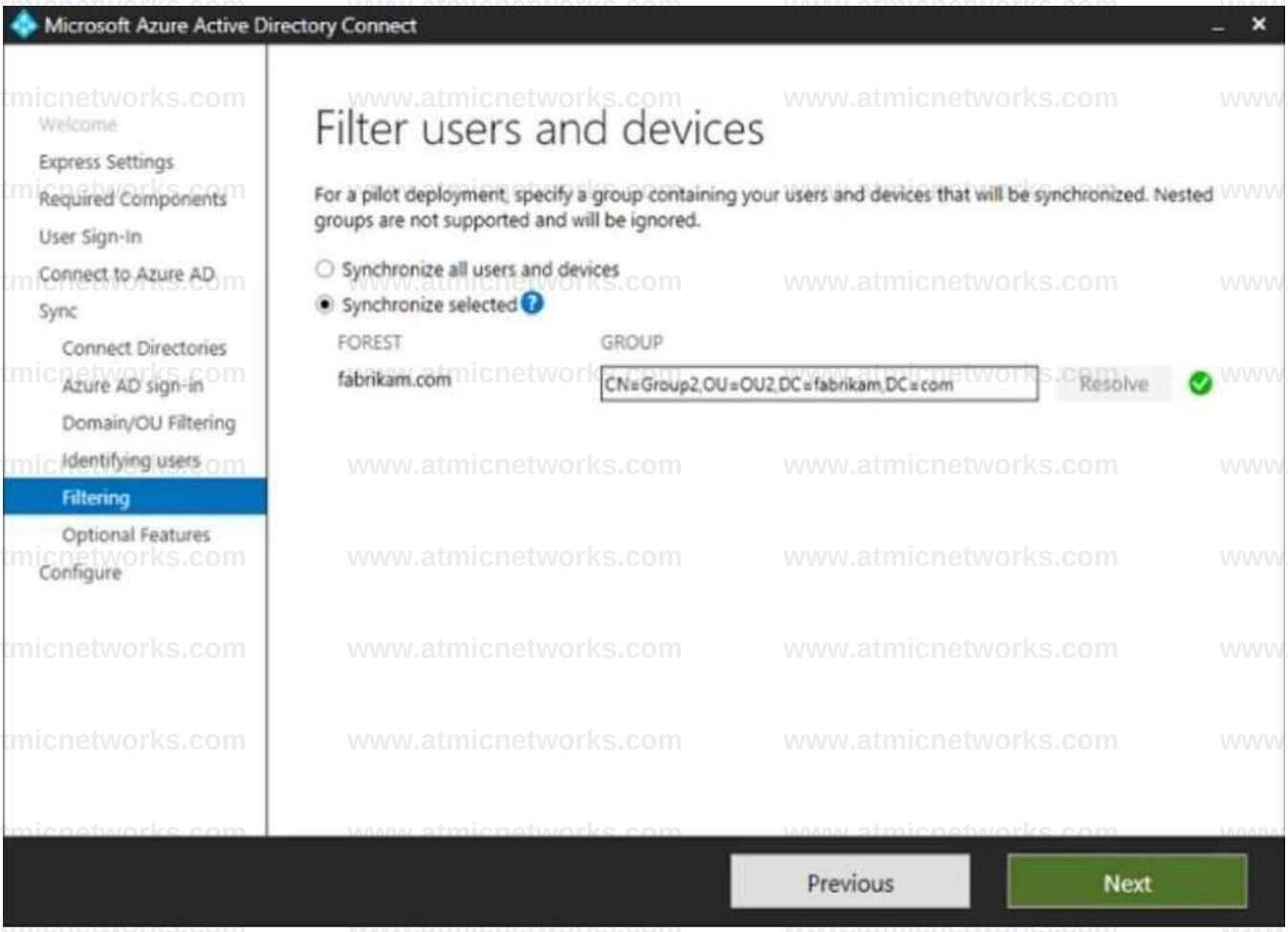
Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	○	○
Group2 will synchronize to Azure AD.	○	○
User3 will synchronize to Azure AD.	○	○

Answer:

Explanation:

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	○	○
Group2 will synchronize to Azure AD.	○	○
User3 will synchronize to Azure AD.	○	○

Box 1: No

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.

User2 is in Group2. However, the User2 account object is in OU1 so User2 will

not synchronize to Azure AD.

Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering#group-based-filterin

Question: 303

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

Assignments: All users

Controls: Require Azure AD multifactor authentication registration

Enforce Policy: On

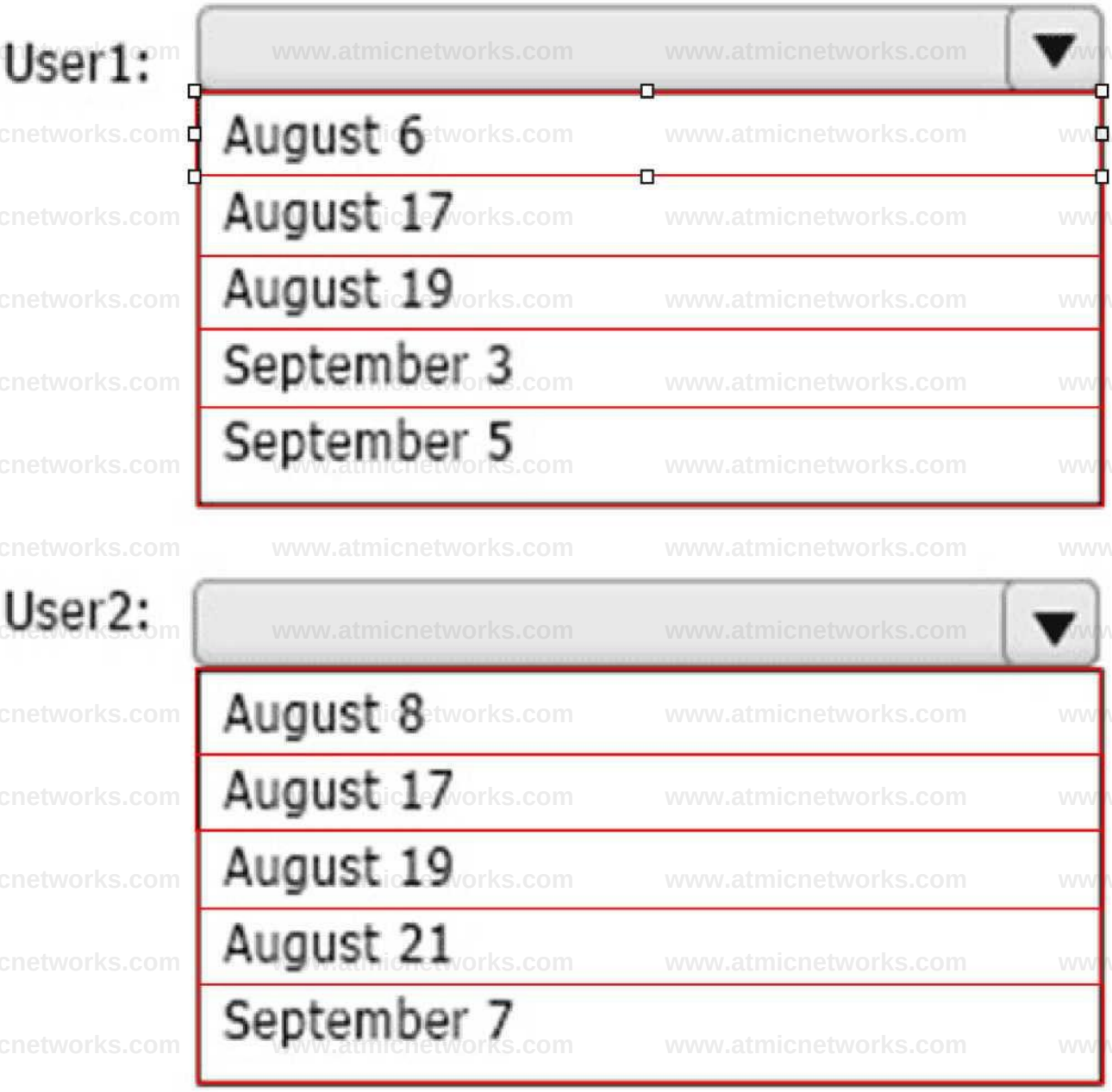
On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.

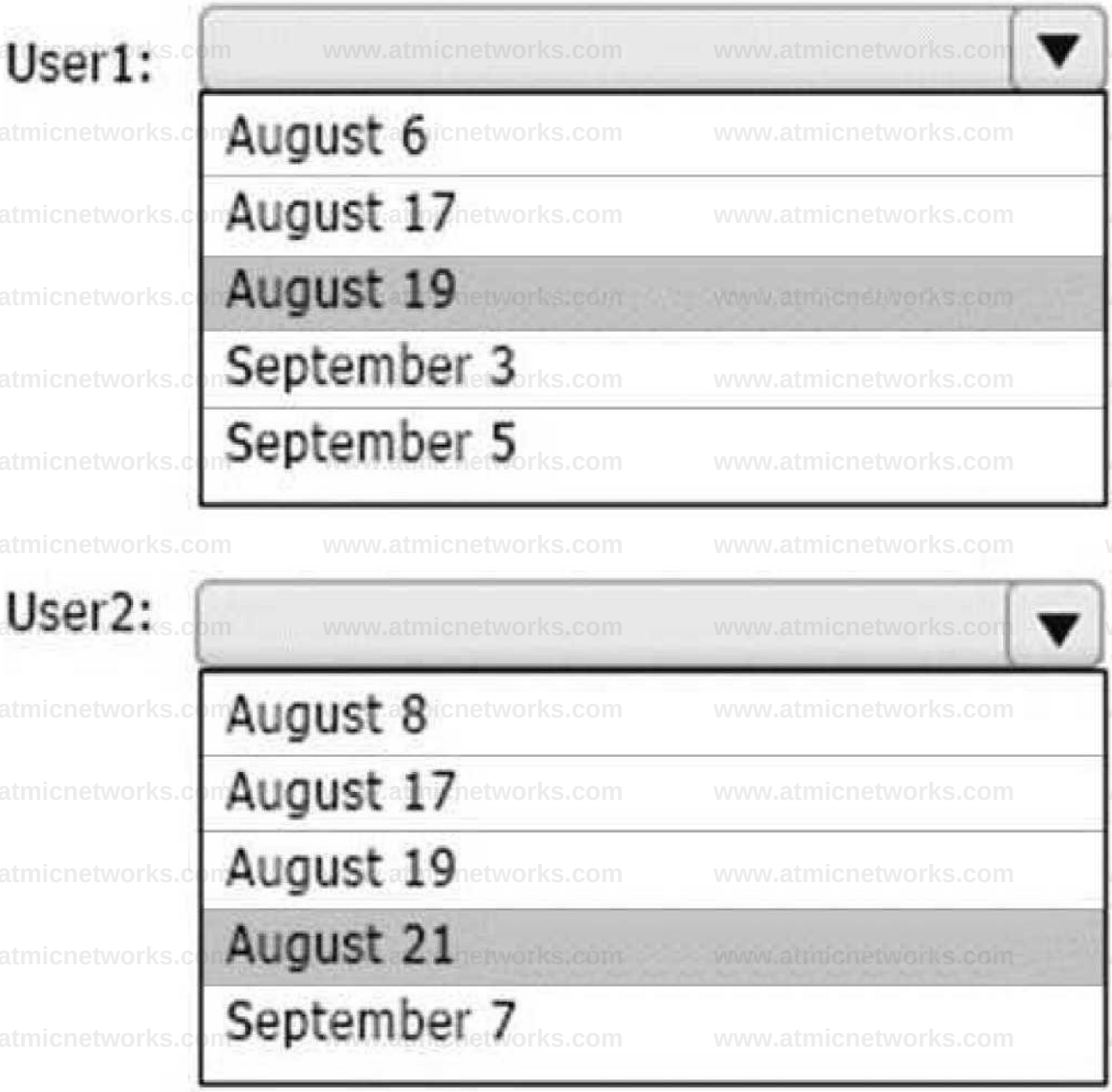
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area



Box 1: August 19

Note: Security defaults will trigger a 14 day grace period for registration after a user's first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.

Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period. Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi-Factor Authentication, then the user must be able to pass that MFA request.

Box 2: August 21

Reference:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview- identity-protection

Question: 304

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:
On-premises Active Directory password complexity policies must be enforced.
Users must be able to use self-service password reset (SSPR) in Azure AD.
What should you use?

A. password hash synchronization
B. Azure AD Identity Protection
C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
D. pass-through authentication

Answer: D

Explanation:

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.

Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their

passwords in the cloud, but most companies also have an on-premises Active Directory

Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the onpremises AD DS environment.

Password writeback is supported in environments that use the following hybrid identity models:

Password hash synchronization
Pass-through authentication
Active Directory Federation Services

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr- writeback

Question: 305

You have a Microsoft 365 E5 subscription.

Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.

From Azure AD Identity Protection, you enable a sign-in risk policy.

Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.

What should you configure?

A. the Tenant restrictions settings in Azure AD
B. a trusted location
C. a Conditional Access policy exclusion
D. the Microsoft 365 network connectivity settings

Answer: B

Explanation:

There are two types of risk policies in Azure Active Directory (Azure AD) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:

Sign-in risk policy
User risk policy

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Question: 306

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1.

Azure AD Password Protection is configured as shown in the following exhibit.

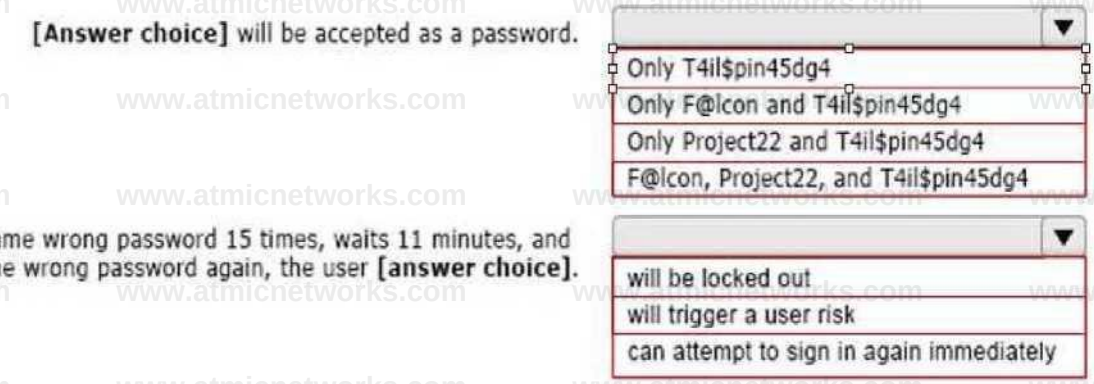
User1 attempts to update their password to the following passwords:

F@lcon
Project22
T4il$pin45dg4

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.

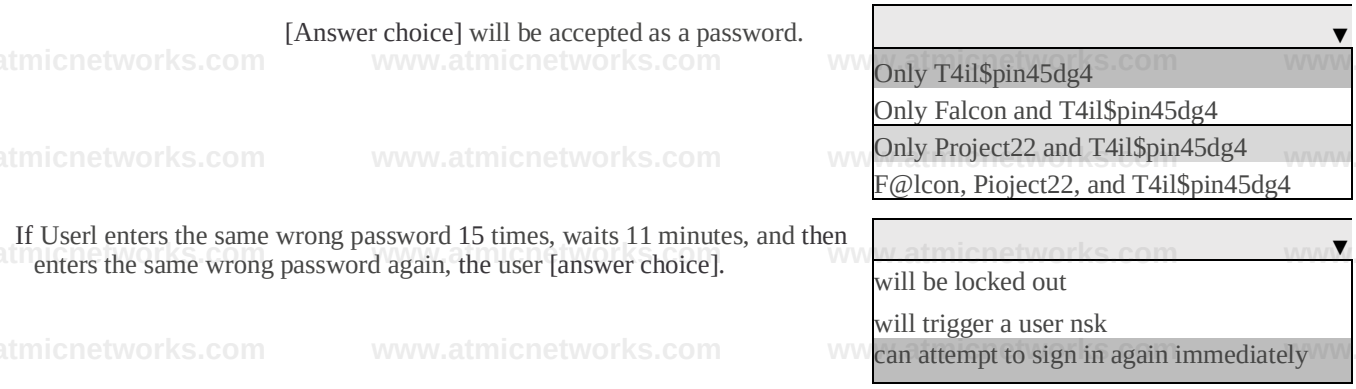
Answer Area



Answer:

Explanation:

Answer Area



Box 1: Only T4il$pin45dg4

Box 2: can attempt to sign in immediately

Note: Manage Azure AD smart lockout values

Based on your organizational requirements, you can customize the Azure AD smart lockout values. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.

To check or modify the smart lockout values for your organization, complete the following steps:

Sign in to the Entra portal.

Search for and select Azure Active Directory, then select Security > Authentication methods > Password

protection.

Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.

The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.

Set the Lockout duration in seconds, to the length in seconds of each lockout.

The default is 60 seconds (one minute).

If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password- smart-lockout

Question: 307

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
Useri	Azure AD	Yesterday
User2	Active Directory Domain Services (ADDS)	Two days ago
(Jser3	Active Directory Domain Services (ADDS)	Never

Azure AD Connect has the following settings:

Password Hash Sync: Enabled

Pass-through authentication: Enabled

You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.

Which users should you identify?

A. none

B. Used only1

C. User1 and User2 only

D. User1. User2, and User3

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

Question: 308

Your network contains an on-premises Active Directory domain named contoso.com.

For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.

You plan to sync contoso.com to an Azure AD tenant.

You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.

What should you include in the recommendation?

A. pass-through authentication

B. conditional access policies

C. password synchronization

D. Azure AD Identity Protection policies

Answer: A

Explanation:

Reference:

https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

Question: 309

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create an Azure AD tenant.

You plan to sync the on-premises Active Directory to Azure AD.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails. What should you include in the recommendation?

A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode

B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode

C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Answer: A

Explanation:

Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.

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

Question: 310

You have a Microsoft 365 subscription.

You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy 1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy 2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx.

File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.

When will File1.docx be deleted automatically?

A. January 1,2023

B. January 1,2024

C. January 31, 2023

D. January 31, 2024

E. never

Answer: D

Explanation:

Retention wins over deletion.

Note:

Explanation for the four different principles:

1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
2. Etc.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

Question: 311

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group 1	Microsoft 365
Group2	Distribution
<3roup3	Mail-enabled security
Groups	Security

You plan to publish a sensitivity label named Label1.

To which groups can you publish Label1

A. Group1 only
B. Group1 and Group2 only
C. Group1 and Group4 only
D. Group1, Group2, and Group3 only
E. Group1 Group2, Group3, and Group4

Answer: A

Explanation:

In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups- sites

Question: 312

HOTSPOT

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rulel	0	Notify users by using email and policy tips. Customize the policy tip as Rulel tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

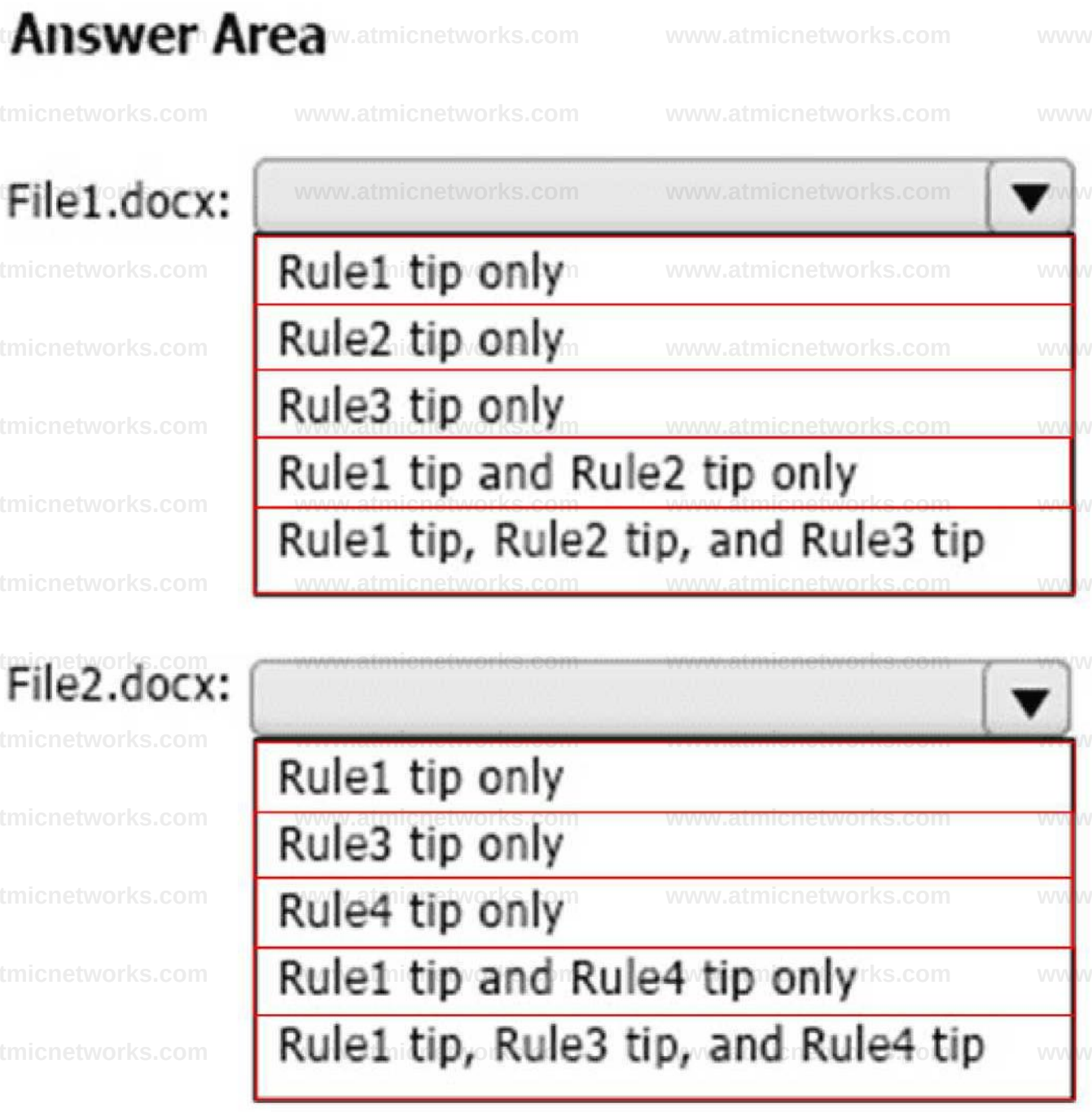
Site1 contains the files shown in the following table.

Name	Matched DLP rule
Filel.docx	Rulel. RuleZ Rule3
Fiie2.docx	Rulel, Rulel Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the

answer area.

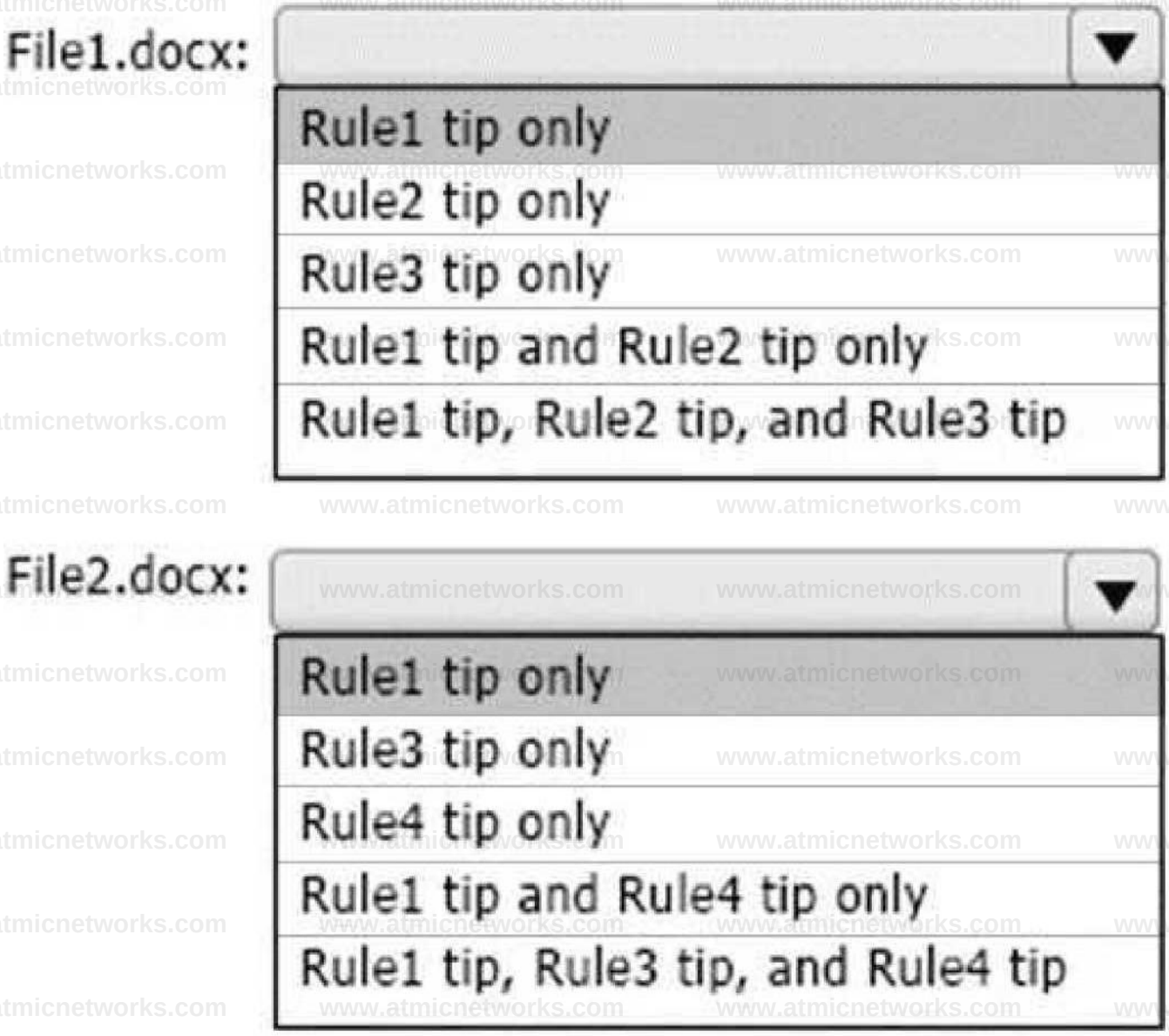
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area



Box 1: Rule1 tip only

File1 matches Rule1, Rule2, and Rule3.

Rule1 has the highest priority.

Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.

Box 2: Rule1 tip only

Note: User Override support

The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).

It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp

https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips

Question: 313

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

A. actions
B. incident reports
C. exceptions
D. user overrides

Answer: D

Explanation:

A DLP policy can be configured to allow users to override a policy tip and report a false positive.

You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.

If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.

Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

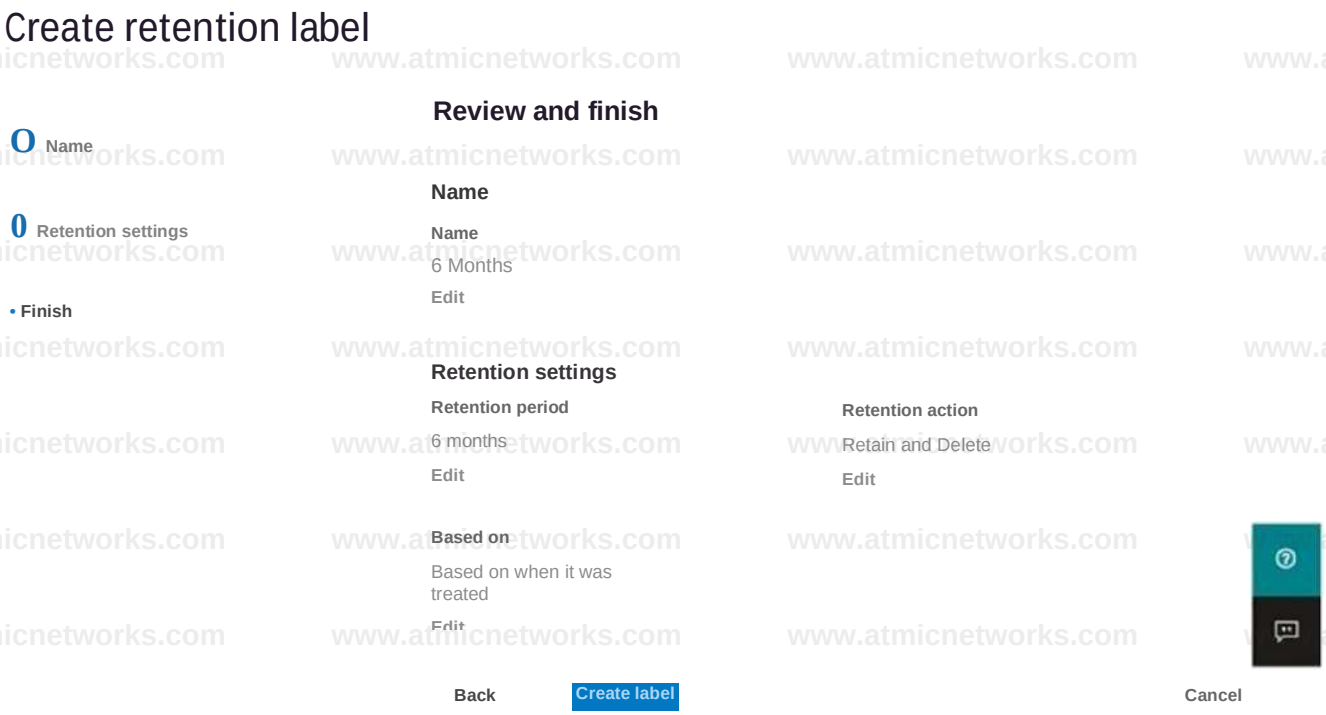
Question: 314

HOTSPOT

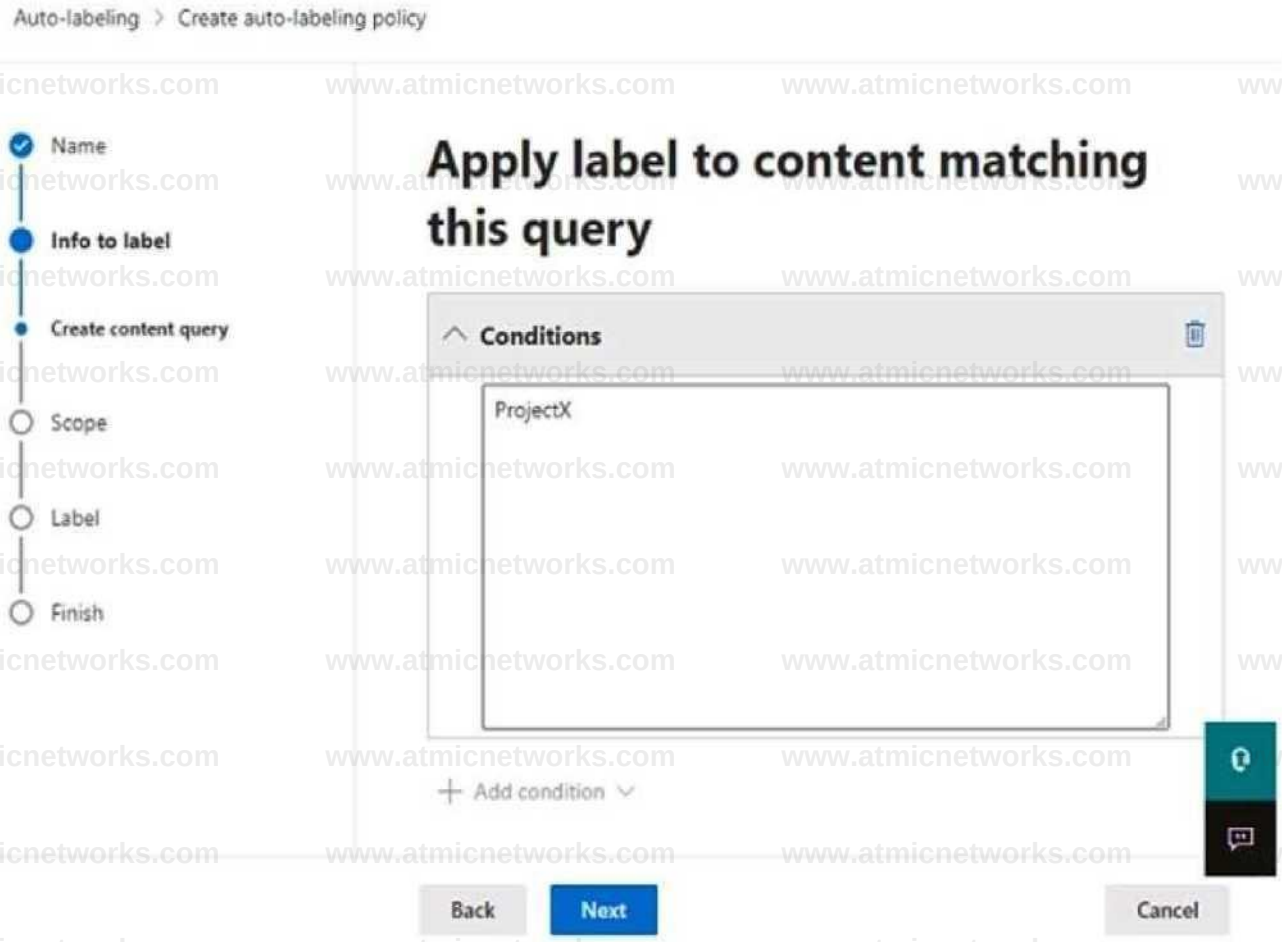
HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)



You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)



The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	O	O
Any sent email message that contains the word ProjectX will be retained for six months.		
Users are required to manually apply a label to email messages that contain the word ProjectX.		

Answer:

Explanation:

Answer Area Statements Yes No

Any sent email message that contains the word ProjectX will be deleted immediately.

Any sent email message that contains the word ProjectX will be retained for six months.

Users are required to manually apply a label to email messages that contain the word ProjectX.

Box 1: No
Box 2: Yes
Box 3: No

Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

Question: 315

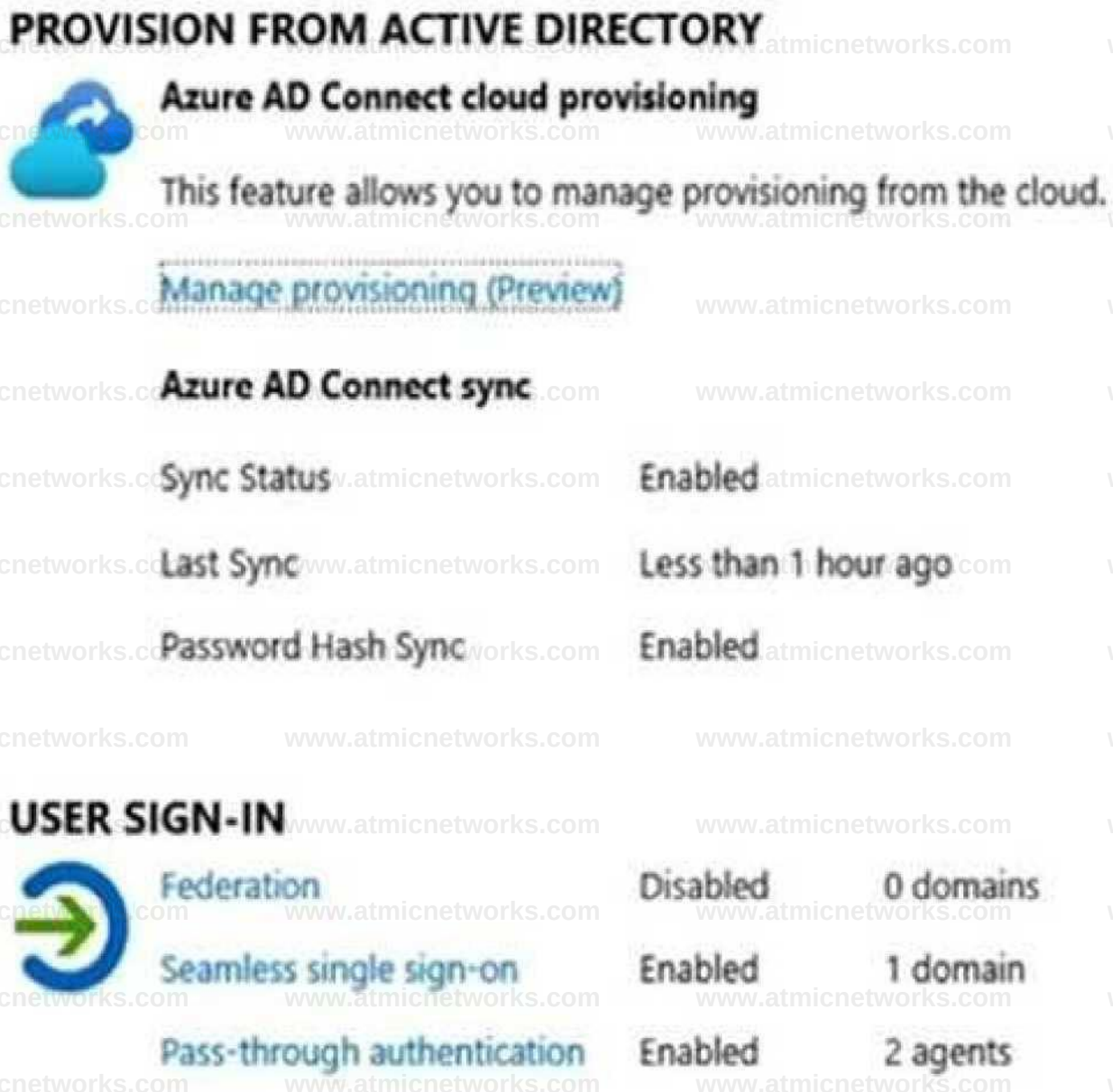
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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.

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

This is not a permissions issue.

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

You need to assign the Security Administrator role.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You need to assign the Security Administrator role.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

Question: 318

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

You need to create a group and assign the Endpoint Security Manager role to the group.

Which type of group can you use?

A. Microsoft 365 only
B. security only
C. mail-enabled security and security only
D. mail-enabled security, Microsoft 365, and security only
E. distribution, mail-enabled security, Microsoft 365, and security

Answer: D

Explanation:

Question: 319

HOTSPOT

You have a Microsoft 365 subscription.

You need to create two groups named Group! and Group2. The solution must meet the following requirements:

- Group1 must be mail-enabled and have an associated Microsoft SharePoint Online site.
- Group2 must support dynamic membership and role assignments but must NOT be mail- enabled.

Which types of groups should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Groupl: Microsoft 365

Group2: Security

Question: 320

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Useri	Groupl
User 2	Group 2
User3	*None*

You create an administrative unit named AU1 that contains the members shown in the following exhibit.

AU1

Members Role assignments

Add users and groups, or select and remove them. The administrators assigned to this unit will manage these users and groups. Adding groups doesn't add users to the unit it lets the assigned admins manage group settings.

-. Add users ^ Add groups f Upload users ••• V Filter ^ Search this list

Members	Email address	last sign-in	Member type
Useri	Useri @sk220912outloolconmicrosoftcom	November 4 2022 at 10-25 PM	User
User}	User3@sk220912outlook.onmicrosoftcom	November 4 2022 at 1027 PM	User

General Assigned Permissions

You can assign this role to users and groups, and select users and groups to remove or manage them.
Learn more about assigning admin roles

A. Add users ^ Add groups

Admin name	Last sign-in	Scope 0
Groupl	Unavailable for groups	Organization
Group2	Unavailable for groups	AU1

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

Answer Area

Statements	Yes	No
Useri can reset the password of UserS.	0	✓"X
User2 can reset the password of User3.	0	
User2 can reset the password of Used.		o

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can reset the password of User3.	0	©
Us«2 can reset the password of User3.	O	©
User2 can reset the password of Useri.	0	©

Question: 321

HOTSPOT

Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
Useri	Password Administrator
UserZ	Security Administrator
UserS	User Administrator
User4	*None*

You need to identify which users can perform the following administrative tasks:

- Reset the password of User4.
- Modify the value for the manager attribute of User4.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Reset the password of User4: Userl and User? only ▼

- Userl only
- User? only
- Userl and User? only
- Userl and User3 only
- Userl, User?, and User3

Modify the value for the manager attribute of User4:

- User? only
- User? only
- User 3 only

1

Userl and User3 only User? and User?
only Userl. User?, and User?

Answer:

Explanation:

Answer Area

Reset the password of User4: User! and User? only

Modify the value for the manager attribute of User4: UserB only

Question: 322

DRAG DROP

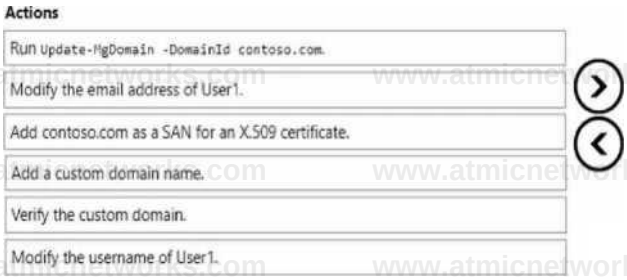
Your company has an Azure AD tenant named contoso.onmicrosoft.com.

You purchase a domain named contoso.com from a registrar and add all the required DNS records.

You create a user account named User1. User1 is configured to sign in as userl@contoso.onmicrosoft.com.

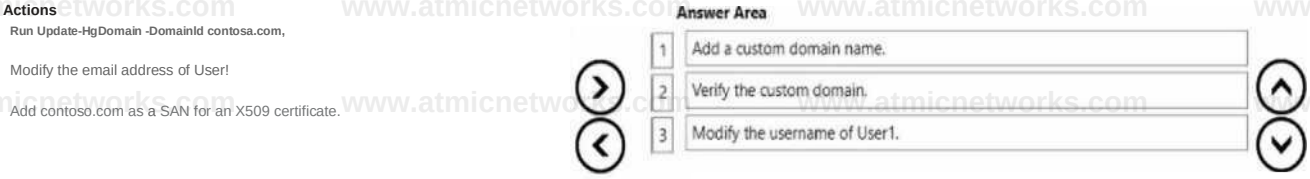
You need to configure User1 to sign in as user1@contoso.com.

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.



Answer:

Explanation:



Question: 323

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to access service health alerts from a mobile phone.

What should you use?

A. the Microsoft Authenticator app
B. the Microsoft 365 Admin mobile app
C. Intune Company Portal
D. the Intune app

Answer: B

Explanation:

Question: 324

HOTSPOT

You work at a company named Contoso, Ltd.

Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.

Contoso purchases a company named Fabrikam, Inc.

Contoso plans to add the following domains to the Microsoft 365 subscription:

- fabrikam.com
- east.fabrikam.com
- west.contoso.com

You need to ensure that the devices in the new domains can register by using Autodiscover.

How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in

the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Domains; 3

Enterpriseregistration DNS records: 3

Question: 325

HOTSPOT

Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.

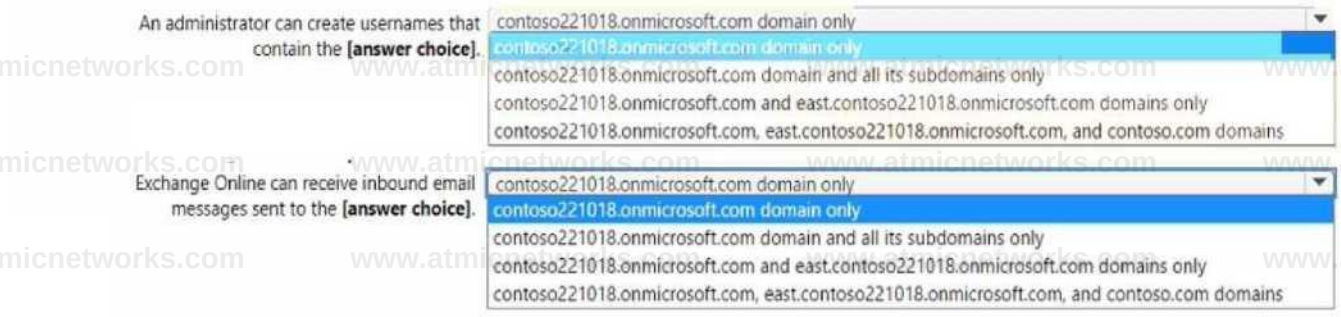
Domains

Add domain 5 Buy domain Q Refresh

Domain name *	Status	K Choose columns
contoso221018.onmicrosoft.com (Default)	9 Healthy	
contoso.com	0 Incomplete setup	
eastcontoso2210l8.onmicrosoft.com	sendees selected	

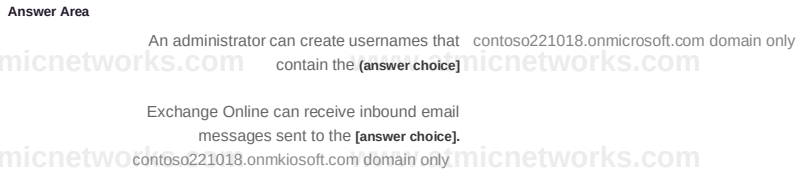
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE; Each correct selection is worth one point.



Answer:

Explanation:



Question: 326

You have a Microsoft 365 E5 subscription.

You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

- Support KQL for querying data.
- Retain report data for at least one year.

What should you include in the recommendation?

A. a security report in Microsoft 365 Defender

B. End point analytics

C. Microsoft 365 usage analytics

D. Azure Monitor workbooks

Answer: D

Explanation:

Question: 327

HOTSPOT

You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.

All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).

You plan to create a user named Admin1 that will perform following tasks:

- View BitLocker recovery keys.
- Configure the usage location for the users in contoso.com.

You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

Devices

- [ ] Cloud Device Administrator
- [ ] Desktop Analytics Administrator
- [ ] Intune Administrator
- [ ] Printer Administrator
- [ ] Printer Technician
- [ ] Windows 365 Administrator

Global

- [ ] Global Administrator

Identity

- [ ] Application Administrator
- [ ] Application Developer
- [ ] Authentication Administrator
- [ ] Cloud Application Administrator
- [ ] Conditional Access Administrator
- [ ] Domain Name Administrator
- [ ] External Identity Provider Administrator
- [ ] Guest Inviter
- [ ] Helpdesk Administrator
- [ ] License Administrator

Explanation:

Answer:

Answer Area

Question: 328

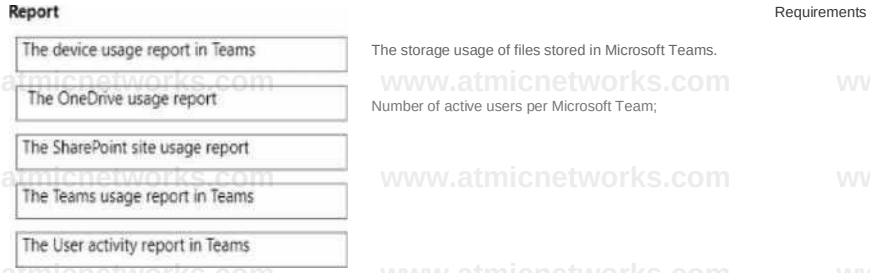
DRAG DROP

You have a Microsoft 365 subscription.

You need to review reports to identify the following:

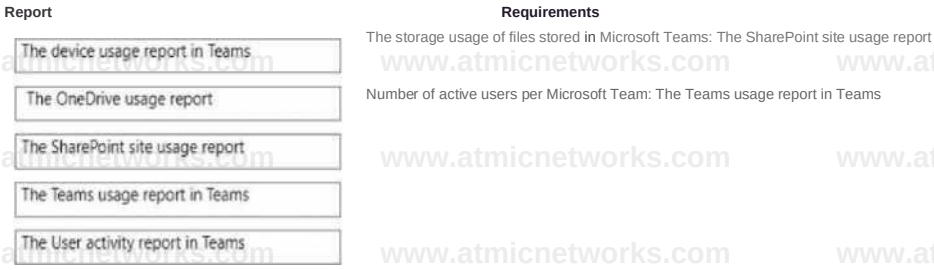
- The storage usage of files stored in Microsoft Teams
- The number of active users per team

Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content



Answer:

Explanation:



Question: 329

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Portal: The Microsoft 365 admin center

Group types: The Microsoft 365 Defender portal
The Microsoft Entra admin center
The Microsoft Purview compliance portal

Group types: [Security only ,
Microsoft 365 only

The Microsoft 365 admin center

Security only
Security and mail-enabled security only
Microsoft 365 and distribution only
Microsoft 365, mail-enabled security, and distribution only
Security, Microsoft 365, mail-enabled security, and distribution

Answer

Explanation:

Answer Area

Portal: The Microsoft 365 admin center

Group types; Security only

Question: 330

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Security enabled	Role assignments allowed
Groupl	Microsoft 365	No	No
Group2	Microsoft 365	No	No
Group3	Security	Yes	Yes
Group4	Security	Yes	No
Groups	Security	Yes	No
Group6	Distribution	No	No

Which groups can be members of Group1 and Group4? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Groupl; None of the groups

- None of the groups
- Group? only
- Group? and Groups only
- Groupi Groups. Groups, and Group6 only
- Group?. Groups, Groups Groups, and Gro up6

Group4; I Group5 only

- None of the groups
- Group5 only
- Groups and Groups only
- Group 1. Group?, Groups, and GroupS only
- Groupl, Group2, Groups, Groups, and Groups

Answer:

Explanation:

Answer Area

Group 1: None of the groups

Group4: Groups only

Question: 331

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.

The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.

To which role should you add User1?

A. Security Reader

B. Global Administrator

C. Owner

D. User Administrator

Answer: A

Explanation:

Question: 332

You have a Microsoft 365 E5 subscription.

You need to create a mail-enabled contact.

Which portal should you use?

A. the Microsoft 365 admin center

B. the SharePoint admin center

C. the Microsoft Entra admin center

D. the Microsoft Purview compliance portal

Answer: A

Explanation:

Question: 333

Your company has an Azure AD tenant named contoso.com that includes the users shown in the following table.

Name	Usage location	Membership
Used	United States	Groupl, Group!
User?	*Not set*	Group!
User3	*Not set*	Groupl
User4	Canada	Groupl

Group2isa member of Group1.

You assign an Office 365 Enterprise E3 license to Group1.

How many Office 365 E3 licenses are assigned?

A. 1

B. 2

C. 3

D. 4

Answer: C

Explanation:

Question: 334

You have a Microsoft 365 E5 subscription that contains the labels shown in the following table.

Name	Type
Label 1	Sensitivity
Label 2	Retention

You have the items shown in the following table.

Name	Stored in	Description
Filel	Microsoft SharePoint	File document that has Labell applied
File2	Microsoft Teams channel	File document that has Label2 applied
Maid	Microsoft Exchange Online	Email message that has Labell applied
Mail?	Microsoft Exchange Online	Email message that has Label2 applied

Which items can you view in Content explorer?

A. File1 only
B. File1 and File2 only
C. File1 and Mail! only
D. File2 and Mail2 only
E. File1, File2, Mail1, and Mail2

Answer: C

Explanation:

Question: 335

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.
The tenant contains the users shown in the following table.

Name	Username	Type
Used	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
UserS	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (Pll) from being emailed to users outside your organization.

To which users can User! send documents that contain Pll?

A. User2only
B. User2and User3only
C. User2, User3, and User4 only
D. User2, User3, User4, and User5

Answer: B

Explanation:

Question: 336

You have a Microsoft 365 subscription.

You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.

You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.

What should you modify?

A. the policy rule exceptions
B. the DLP policy locations
C. the policy rule conditions
D. the policy rule actions

Answer: C

Explanation:

Question: 337

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. Site! contains the files shown in the following table.

Name	Number of IP addresses in the file
Riel	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rulel	3 or more IP addresses	Tipi	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tip is displayed for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Filel: Tip2 only

Tip2 only
Tip3 only
Tip2 and Tip3

File2; Tip! and Tip2 only

Tip! only
Tip3 only

Tipi and Tip2 only
Tipi Tip2 and 1 ip3

Answer:

Explanation:

Answer Area

Filel: Tip2 only

File2: Tipi and Tip2 only

Question: 338

HOTSPOT

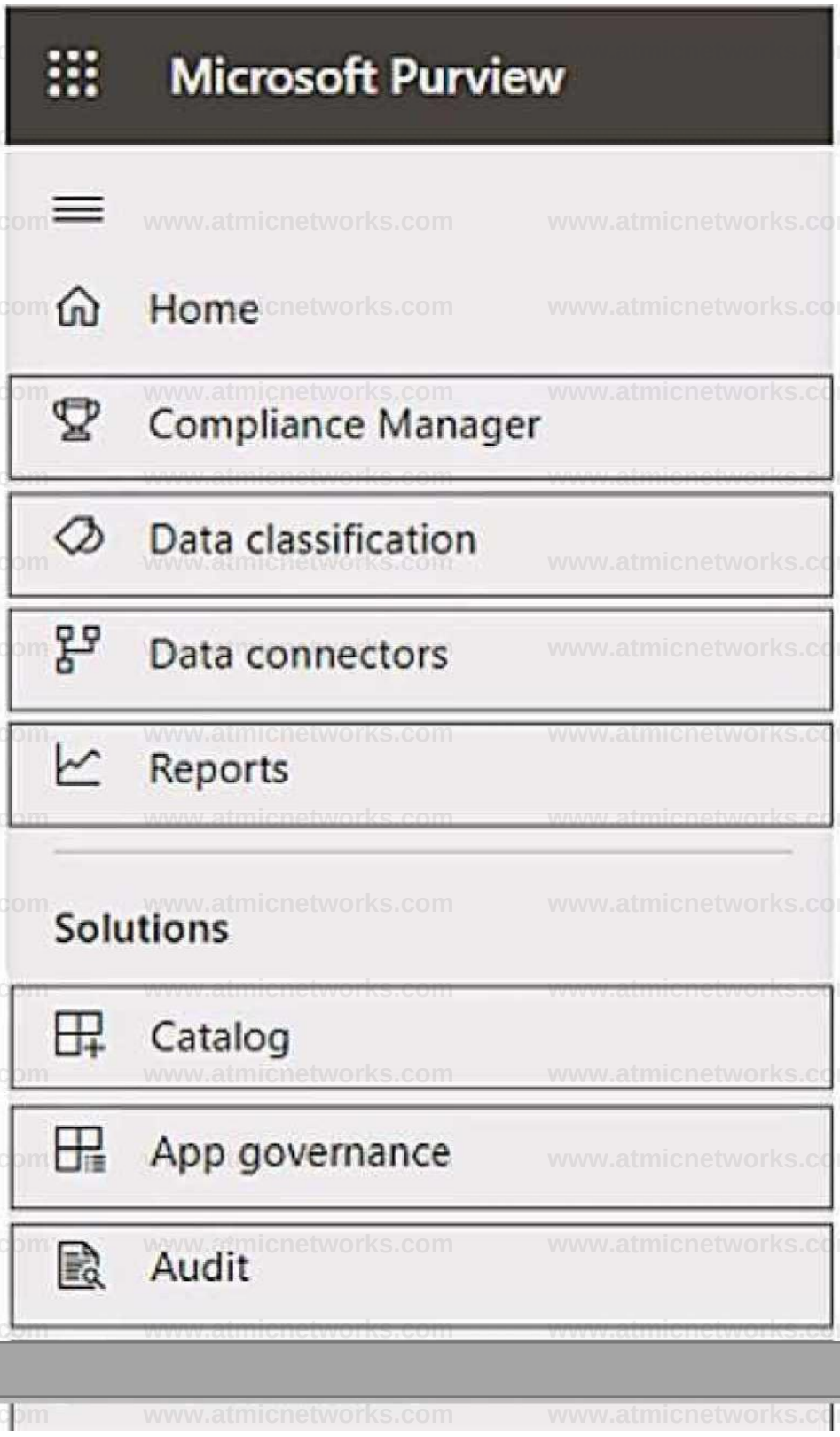
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:

- Create a sensitive info type named SIT1 based on a regular expression.
- Add a watermark to all new documents that are matched by SIT1.

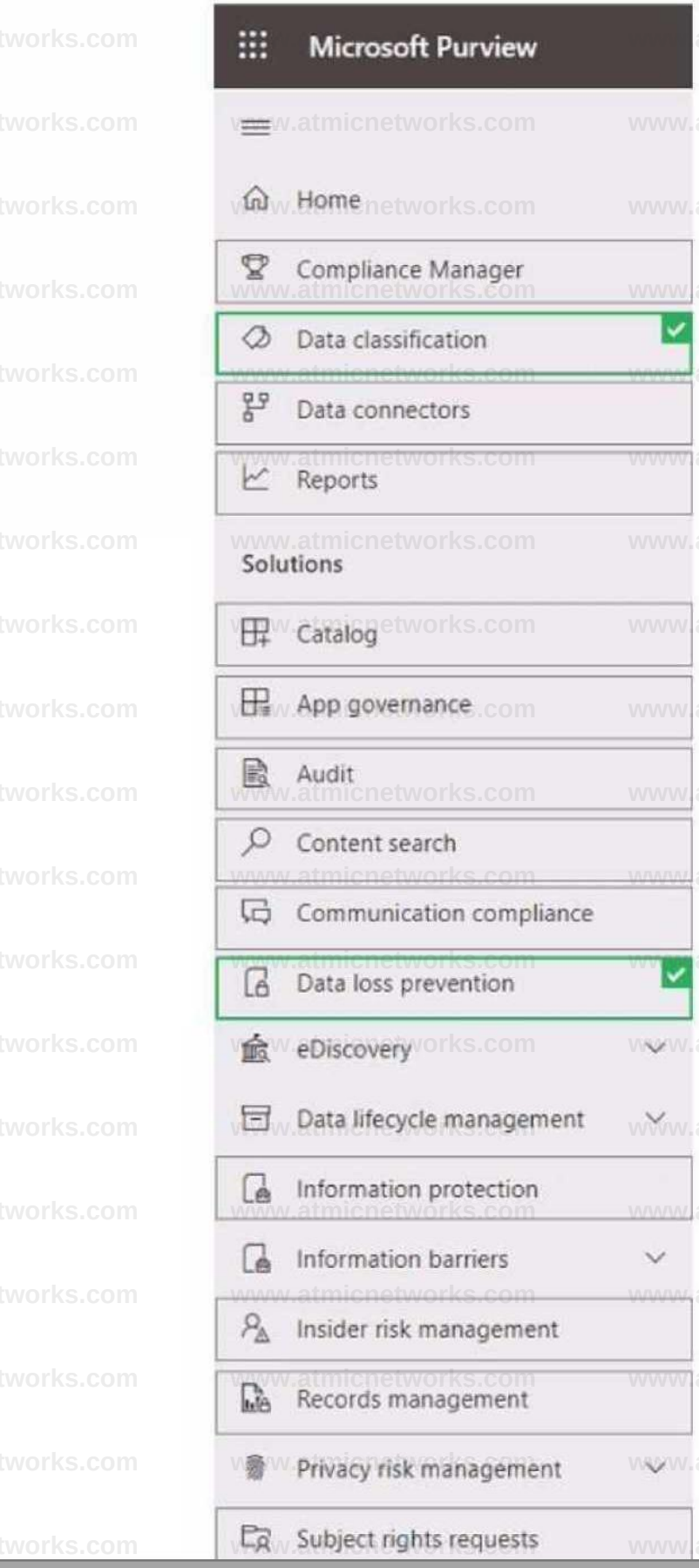
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer Area



Question: 339

HOTSPOT

Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Devicel	ATP1
Device?	ATP1
Devices	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Device
Alert 1	Devicel
Alert2	Device2
AlertS	Devices

You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 device group

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

NOTE: Each correct selection is worth one point

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert 1 is visible in the alerts queue,	O	O
After you create the suppression rule, Alert? is visible in the alerts queue,	O	
After you create the suppression rule, a new alert triggered on Device? is visible in the alerts queue.	O	

Answer:

Explanation:

Answer Area

Statements	**Yes**	**No**

After you create (he suppression rule, Alertl is visible in the alerts queue. ® 0

After you create the suppression rule, Alert3 is visible in the alerts queue, • 0

0 ®

After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.

Question: 340

You have a Microsoft 365 E5 subscription.

You need to be alerted when Microsoft 365 Defender detects high-severity incidents.
What should you use?

A. a custom detection rule
B. a threat policy
C. an alert policy
D. a notification rule

Answer: C

Explanation:

Question: 341

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.

User1 emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.
You need to prevent this issue from reoccurring.
What should you configure?

A. anti-spam policies
B. Safe Attachments policies
C. anti-phishing policies
D. anti-malware policies

Answer: A

Explanation:

Question: 342

HOTSPOT

You have a Microsoft 365 E5 subscription.

All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.

You need to meet the following requirements:

* View an assessment of the device configurations against the Center for Internet Security (CIS) vl.0.0 benchmark.

- Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.

What should you do? To answer, select the appropriate options in the answer area.

Answer Area

To view the device configuration assessment: Create a baseline assessment profile. [Add a connected application.

Create a baseline assessment profile.
Filter the Vulnerable devices report.

To protect C:\Foider1, enable: Controlled folder access

Controlled folder access
Exploit protection
Removable storage protection

Answer:

Explanation:

Answer Area

To view the device configuration assessment: Create a baseline assessment profile.

To protect C:\Folder1, enable: Controlled folder access

Question: 343

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to configure Microsoft Defender for Office 365 to meet the following requirements:

- A user's email sending patterns must be used to minimize false positives for spoof protection.
- Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

A user s email sending patterns must be used to minimize false positives for spoof protection: Domains to protect

Mailbox intelligence

Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using (Global settings for safe attachments T j

The Safe Attachments policy settings

The Safe Links policy settings

Answer

Explanation:

Answer Area

A user's emait sending patterns must be used to minimize false positives for spoof protection: Domains to protect T

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Global settings for safe attachments Defender for Office 365:

Question: 344

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

You plan to perform device discovery and authenticated scans of network devices.

You install and register the network scanner on a device named Device1.

What should you do next?

A. Connect Defender for Endpoint to Microsoft Intune.

B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.

C. Create an assessment job.

D. Download and run an onboarding package.

Answer: C

Explanation:

Question: 345

You have a Microsoft 365 subscription.

You need to receive a notification each time a user in the service desk department grants Full Access permissions for a user mailbox.

What should you configure?

A. a data loss prevention (DLP) policy

B. an alert policy
C. an audit search
D. an insider risk management policy

Answer: B

Explanation:

Question: 346

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

All the devices in your organization are onboarded to Microsoft Defender for Endpoint. You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours. What should you do?

A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
B. From Alerts queue, create a suppression rule and assign an alert.
C. From Advanced hunting, create a query and a detection rule.
D. From the Microsoft Purview compliance portal, create an audit log search.

Answer: C

Explanation:

Question: 347

HOTSPOT

You have a Microsoft 365 E5 subscription.

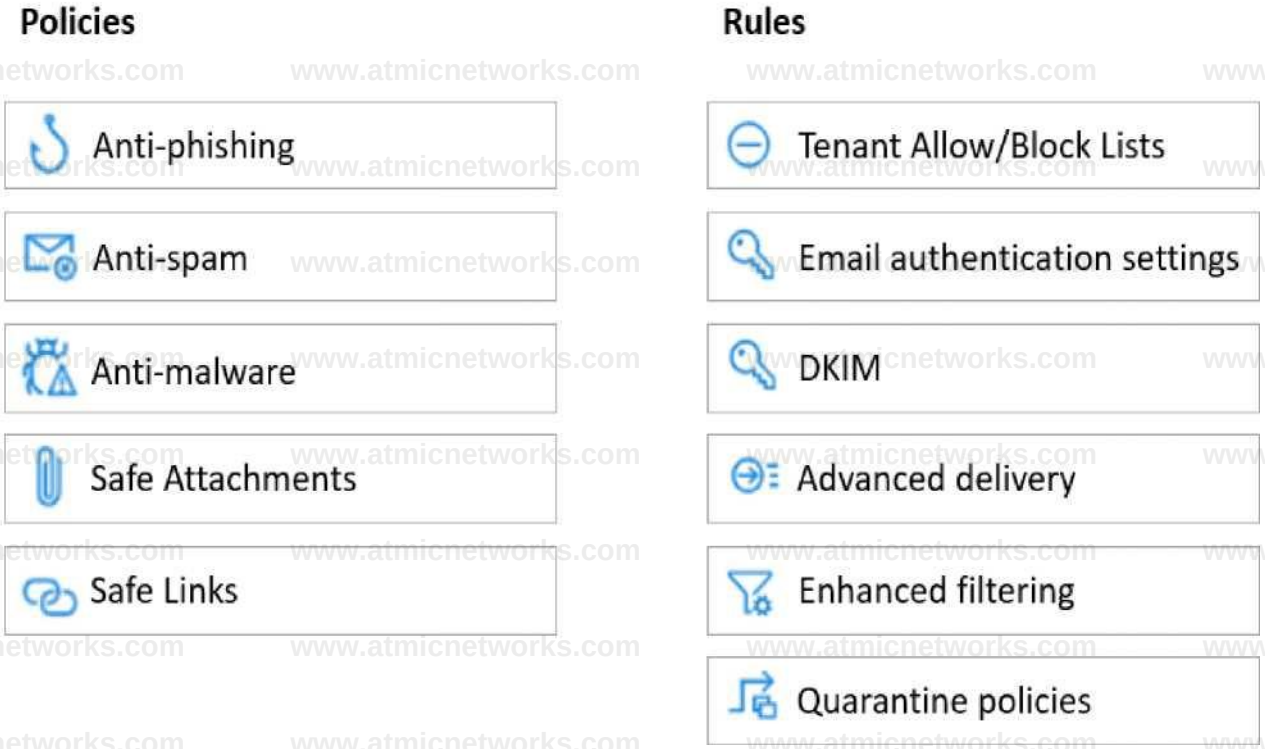
You plan to use a mailbox named Mailbox1 to analyze malicious email messages.

You need to configure Microsoft Defender for Office 365 to meet the following requirements:

- Ensure that incoming email is NOT filtered for Mailbox1.
- Detect impersonation and spoofing attacks on all other mailboxes in the subscription.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

Answer Area



Answer:

Explanation:

Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments. This will ensure that incoming email is not filtered for

Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.

Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

Question: 348

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.

You plan to use Mailbox1 to collect and analyze unfiltered email messages.

You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.

What should you do?

A. Configure a retention policy for Mailbox1.
B. Create a mail flow rule.
C. Configure Mailbox! as a SecOps mailbox.
D. Place a litigation hold on Mailbox1.

Answer: D

Explanation:

Question: 349

HOTSPOT

You have a hybrid deployment of Azure AD that contains the users shown in the following table.

Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

You need to identify which users can perform the following tasks:

- View sync errors in Azure AD Connect Health.
- Configure Azure AD Connect Health settings.

Which user should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

View sync errors in Azure AD Connect Health: User2

Configure Azure AD Connect Health settings: User 1

Question: 350

HOTSPOT

Your network contains an Active Directory domain and an Azure AD tenant.

You implement directory synchronization for all 10.000 users in the organization.

You automate the creation of 100 new user accounts.

You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area

Answer

Explanation:

Answer Area

Question: 351

HOTSPOT

You have a Microsoft 365 Enterprise E5 subscription.

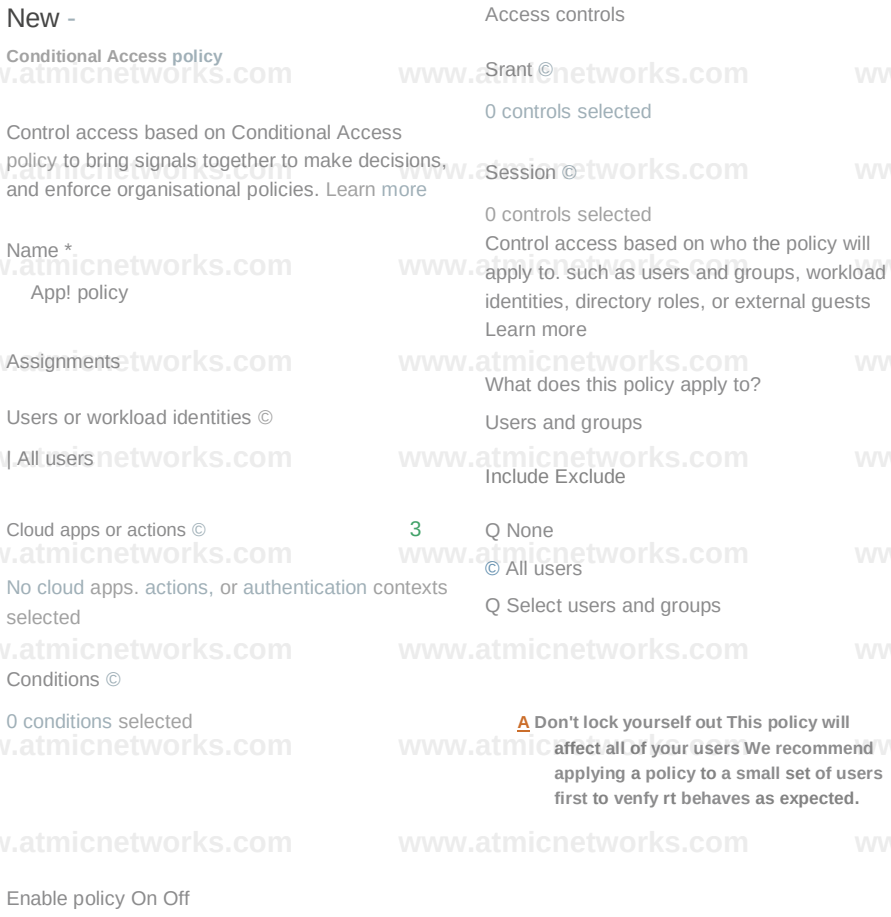
You add a cloud-based app named App1 to the Azure AD enterprise applications list.

You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.

Which three settings should you configure from the policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

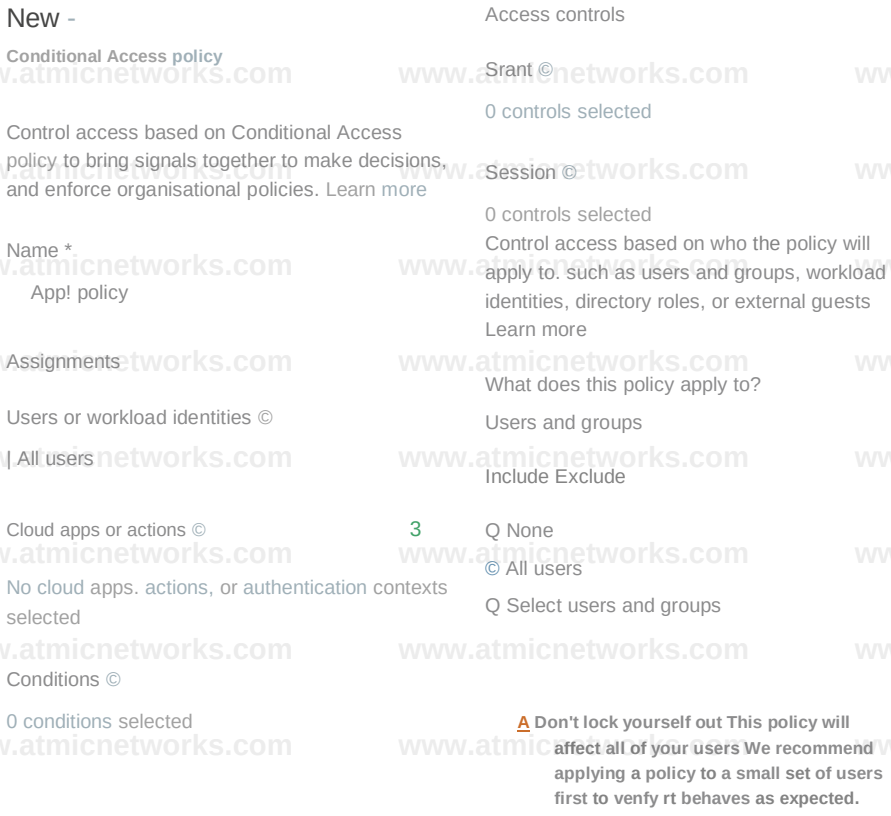
Answer Area



Answer:

Explanation:

Answer Area



Question: 352

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User!	Groupl	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
	Groupl, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

Microsoft Authenticator settings - X

Q Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. team more

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more.

Enable and Target Configure

Enable ^0

Include Exclude

Target O Afi users (•) Select groups

Add groups

Name	Type	Registration	Authentication mode
Group!	Group		.Passwordless v j X

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User! can use number matching during sign-in.		
User2 can use number matching during sign-in.		
User3 can use number matching during sign-in.	O	0

Answer:

Explanation:

Answer Area

Statements

User 1 can use number matching during sign-in.

User2 can use number matching during sign-in.

User3 can use number matching during sign-in.

Question: 353

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement a hybrid configuration that has the following requirements:

- Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
- Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Password Hash Synchronization

B. Password writeback

C. Directory extension attribute sync

D. Enable single sign-on

E. Pass-through authentication

Answer: A,B

Explanation:

Question: 354

Your company has three main offices and one branch office. The branch office is used for research.

The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.

You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.

What should you include in the recommendation?

A. Azure AD password protection

B. a Microsoft Intune device configuration profile

C. a Microsoft Intune device compliance policy

D. Azure AD conditional access

Answer: D

Explanation:

Question: 355

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy. Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sign-in risk policy r——————————————————————————————

| Leaked credentials

] Atypical travel

Leaked credentials

| Possible attempt to access Primary Refresh Token (PRT)

User risk policy Malicious IP address

[leaked credentials

Malicious IP address

| Suspicious browser

Answer:

Explanation:

Answer Area

Sign-in risk policy Leaked credentials | *

User risk policy Malicious IP address w

Question: 356

You have a Microsoft 365 E5 subscription.

You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event.

You need to reduce false positives for impossible travel when the users sign in from the corporate network.

What should you configure?

A. exclusion groups

B. multi-factor authentication (MFA)

C. named locations

D. user risk policies

Answer: C

Explanation:

Question: 357

HOTSPOT

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
Useri	Global Administrator
User?	Billing Administrator
User3	Mow

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self-service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

User!; Phone number and email address

User2: Phone number and email address

User3: Security questions only

Question: 358

You have a Microsoft 365 E5 subscription.

Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.

You need to implement passwordless authentication. The solution must support all the devices.

Which authentication method should you use?

A. Windows Hello
B. FID02 compliant security keys
C. Microsoft Authenticator app

Answer: C

Explanation:

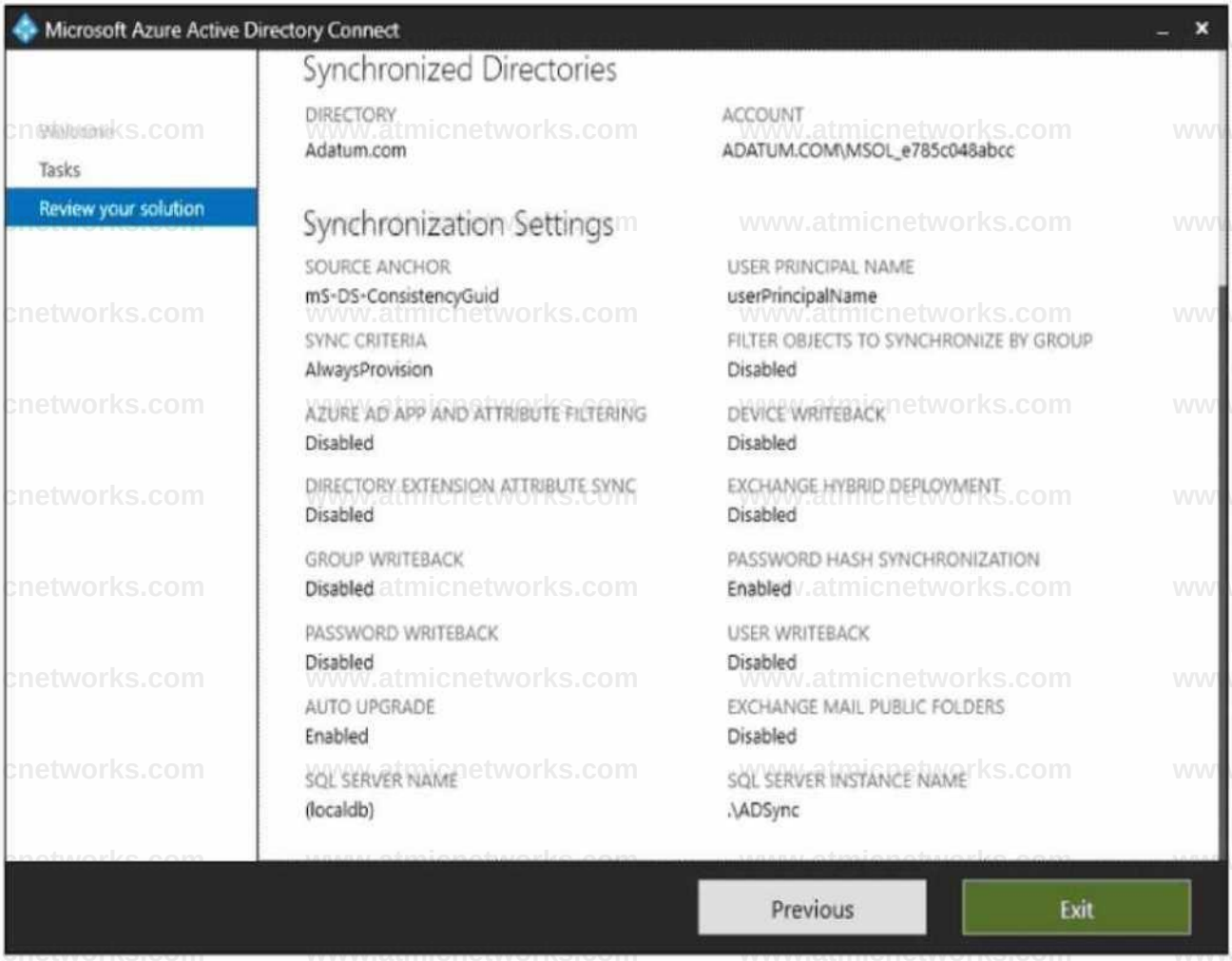
Question: 359

HOTSPOT

Your company has a hybrid deployment of Microsoft 365.

An on-premises user named User1 is synced to Azure AD.

Azure AD Connect is configured 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

User1 [answer choke] , I cannot change her password from any Microsoft portals
cannot change her password from any Microsoft portals
can change her password by using self-service password reset feature only can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory, | the password hash will be synchronized to Azure AD
the password hash will be synchronized to Azure AD
a new randomly generated password will be assigned to User1 the password hash in Azure AD will be unchanged

Answer:

Explanation:

Answer Area

User1 **[answer choke)** cannot change her password from any Microsoft portals

If the password for User1 is changed in Active Directory, the password hash will be synchronized to Azure AD
[answer choke]

Question: 360

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 network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From Azure AD Connect, you modify the filtering settings.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 361

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

A. the status of the DLP policy
B. the user overrides of the DLP policy rule
C. the locations of the DLP policy
D. the conditions of the DLP policy rule

Answer: D

Explanation:

Question: 362

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1. You need to ensure that site1 meets the following requirements:

- Retains all data for 10 years
- Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a retention policy
B. a sensitive info type
C. a data loss prevention (DLP) policy
D. a sensitivity label

E. a retention label

F. a retention label policy

Answer: C,E

Explanation:

Question: 363

You have a Microsoft 365 E5 subscription that contains a user named User1

You create a retention label named Retention1 that is published to all locations.

You need to ensure that User1 can label email messages by using Retention1 as soon as possible.

Which cmdlet should you run in Microsoft Exchange Online PowerShell?

A. Start-MpScan

B. Start-Process

C. Start-ManagedFolderAsslstant

D. Start-AppBackgroundTask

Answer: C

Explanation:

Question: 364

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to create the data loss prevention (DLP) policies shown in the following table.

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

You need to create DLP rules for each policy.

Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sender is condition: | DLP1 only

DLP1 only
DLP2 only
DIPS only
DLP2 and DLP3 only
DLP1, DLP2. and DLP3

File extension is condition:

DLP1, DLP2, and DLP3
DLP1 only
DLP2 only
DIP 3 only
DLP1, DLP2. and DLP3

Answer:

Explanation:

Answer Area

Sender is condition: DLP1 only

File extension is condition: DLP1, DLPZ and DLP3

Question: 365

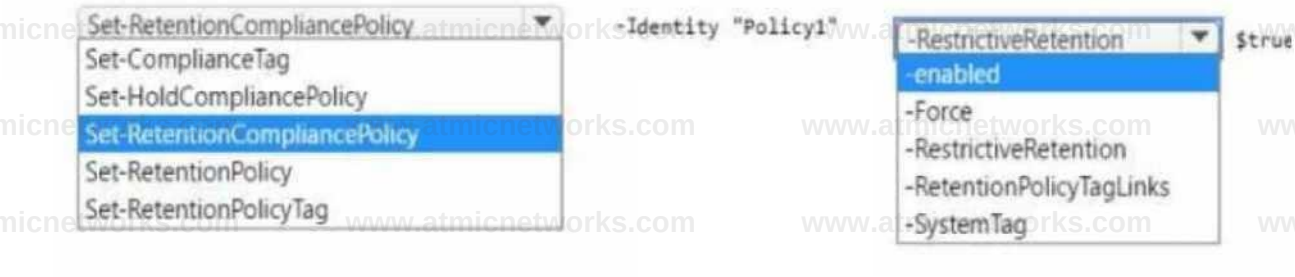
HOTSPOT

From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.

You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Set-RetentronCompliancePoftcy ' -identity "Policyl* - Restr ictiveRetention * strut

Question: 366

HOTSPOT

Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
Used	*None*	Compliance Data Administrator
User?	Global Administrator	*None*

You create a retention label named Label 1 that has the following configurations:

- Retains content for five years
- Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

- Applies to content that contains the word Merger
- Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

Set-RetentionConpliancePolicy Policy1 -RestrictiveRetention Strue -Force

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Useri can add Exchange email as a location to Policy 1.		
User? can remove SharePoint sites from Policy!.	O	o
User? can add the word Acquisition to Policy!.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Used can add Exchange email as a location to Policy 1.	•	

User? can remove SharePoint sites from Policyl. O t

User? can add the word Acquisition to Policyl.

Question: 367

You have a Microsoft 365 E5 subscription.

Your company s Microsoft Secure Score recommends the actions shown in the following exhibit.

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

I Export

Rank	Recommended action	Score impact	Points achieved	Status
□ 1	Require multifactor authentication for administrative roles	>4.15%	0/10	0 To address
□ J	Ensure all users can complete muftifactor authentication	-373%	0/9	0 To address
□ '	Create Safe Links policies for email messages	-3.73%	0/9	O To address
□ *	Enable policy to block legacy authentication	-3.32%	0/8	O To address
□ '	Turn on Safe Attachments In block mode	*332%	0/8	Q To address
□ 6	Ensure that intelligence for impersonation protection is enabled	-332%	0/8	O Tc address
□ '	Move messages that are detected as impersonated users by mailbox intelligence	*332%	0/8	Q To address
□ 0	Enable impersonated domain protection	*332%	0/8	O To address

You select Create Safe Links policies for email messages and change Status to Risk accepted in the Status & action plan settings.

How does the change affect the Secure Score?

A. remains the same
B. increases by 1 point
C. increases by 9 points
D. decreases by 1 point
E. decreases by 9 points

Answer: A

Explanation:

Question: 368

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Useri	Group!
User2	Group!, Groups
User?	Group2

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
- Priority: 0
- Induce these users, groups and domains

o Users: User3

o Groups: Group1

- Exclude these users, groups and domains

o Groups: Group2

- Message limits

o Set a daily message limit 100

- Name: AntiSpam2
- Priority: 1
- Include these users, groups and domains

o Users: User! o Groups: Group2

- Exclude these users, groups and domains

o Users: User3

- Message limits

o Set a daily message limit 50

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

NOTE: Each correct selection is worth one point.

Answer Area Statements	Yes	No
User 1 can send a maximum of 150 email messages per day.	0	
User2 can send a maximum of 50 email messages per day.		
UserS can send a maximum of 100 email me*53^ P^ day.		

Answer:

Explanation:

Answer Area

0

Statements	Yes	No

Useri can send a maximum of 150 email messages per day. 0 ®

User? can send a maximum of 50 email messages per day. ® 0

UserS can send a maximum of 100 email messages per day. 0 ®

Question: 369

DRAG DROP

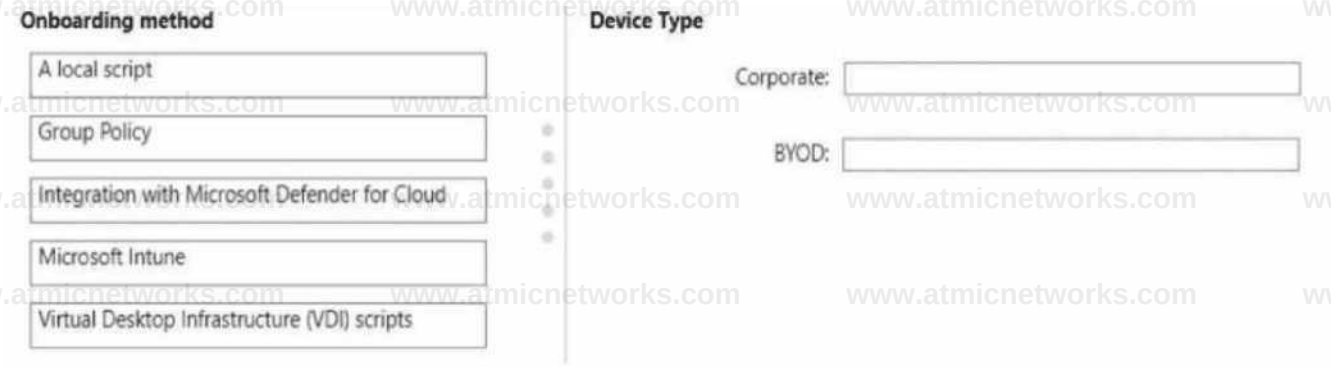
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined. Microsoft Intune-managed
Bring your own device (BYOD)		Windows 11	Unmanaged

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.

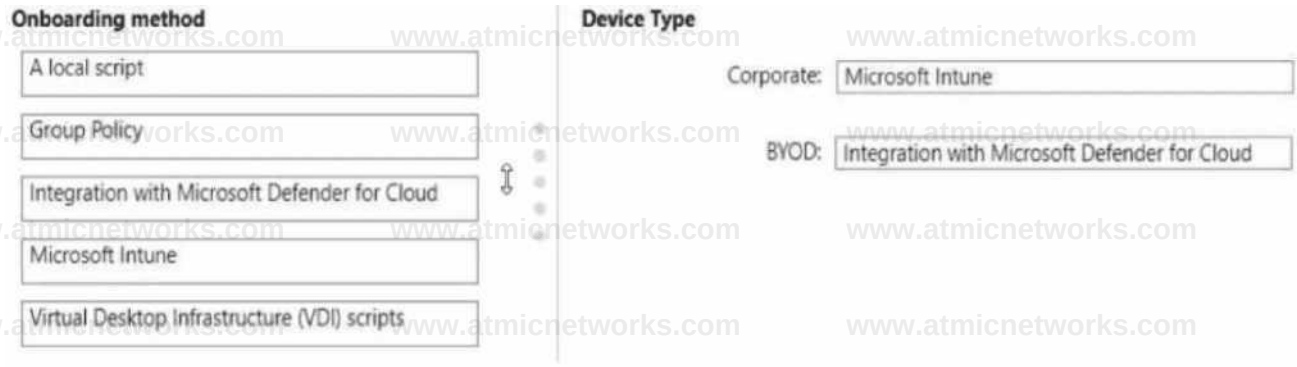
What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 370

You have a Microsoft 365 E5 subscription.

You onboard all devices to Microsoft Defender for Endpoint

You need to use Defender for Endpoint to block access to a malicious website at www.contoso.com.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. Create a web content filtering policy.

B. Configure an enforcement scope.

C. Enable Custom network indicators.

D. Create an indicator.

E. Enable automated investigation.

Answer: A,C

Explanation:

Question: 371

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.

User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:

- Which administrators can unblock User1
- What to configure to allow User1 to send at least 2,000 emails per day without being blocked

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Administrators: Admin2 only

Settings: Anti-spam

Question: 372

HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Member
1	Groupi	Name starts with Comp
2	Group2	Name starts with Comp And OS in Windows 10
	Group3	OS In Windows Server 2016
Last	Ungrouped devices (default	Not applicable

You onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer! and Computed members? To answer, select the appropriate options in The answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Computeri: Groupl only £

Computer?: Groupl only T

Question: 373

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Group
Devicel	DeviceGroupi
Device-2	DeviceGroupi

- Name: Notification!
- Notification settings

o Notify on alert seventy: Low

o Device group scope: All (3)
o Details: First notification per incident
- Recipients: Userl@contoso.com, User2@contoso.com

At 08:02. you create an incident notification rule that has the following configurations:

- Name: Notification
- Notification settings

o Notify on alert severity: Low. Medium
o Device group scope: DevtceGroup1, DeviceGroup2

- Recipients: Userl@contoso.com

in Microsoft 365 Defender, alerts are logged as shown in the following table.

Time	Alert name	Severity	Impacted assets
08:05	Activity!	Low	Device!
08:07	Activity!	Low	Device!
08:08	Activity!	Medium	Device!
08:15	Activity?	Medium	Device?
08:16	Activity?	Medium	Device?
08:20	Activityl	High	Device!
08:30	Activity?	Medium	Device?
08:35	Activity?	High	Device?

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.
NOTE: Each correct selection is worth one point.

Answer Area Statements	Yes	No
User 1 ©contoso.com will receive two incident notification emails for the alert at 08:05		
User2@contoso.com will receive an incident notification email for the alert at 08:07.		
User1@contoso.com will receive an incident notification email for the alert at 08:20.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
User 1 ©contoso.com will receive two incident notification emails for the alert at 08:05	O	•

User2@contoso.com will receive an incident notification email for the alert at 08:07.

*

Useri ©contoso.com will receive an incident notification email for the alert at 08:20.

O •

Question: 374

HOTSPOT

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.

Policyl

^ Edit policy 0 Delete policy

Status w On

Name your alert

Description

Add a description

Severity

• Low

Category

Threat management

Policy contains tags

Create alert settings

Conditions

Activity is FileMalwareDetected

Aggregation

Aggregated

Scope

All users

Threshold

20

Window

2 hours

Severity

• Low

in

Set your recipients

Recipients

Userl @sk220912outtook.onmicro$oft .com

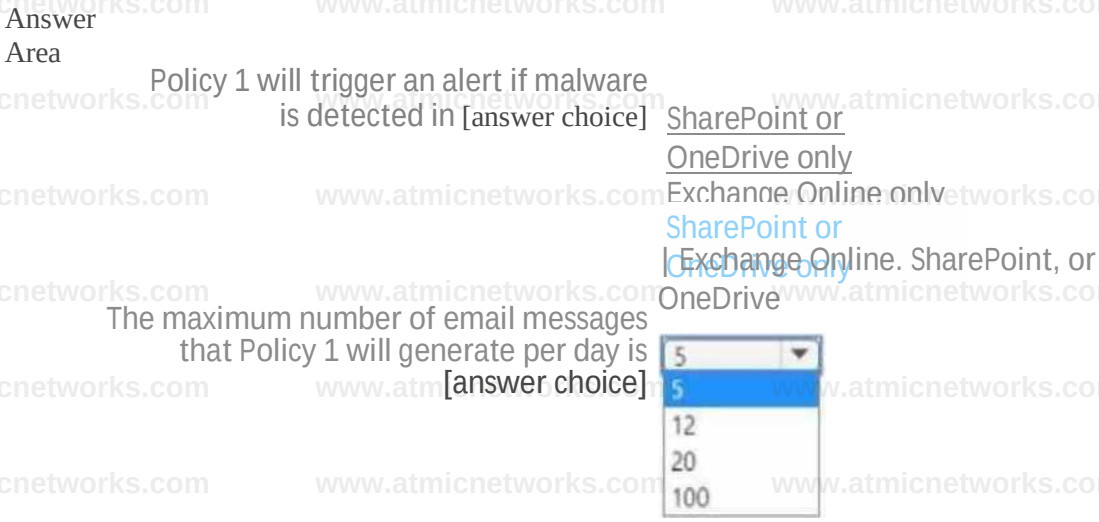
Daily notification limit

100

e

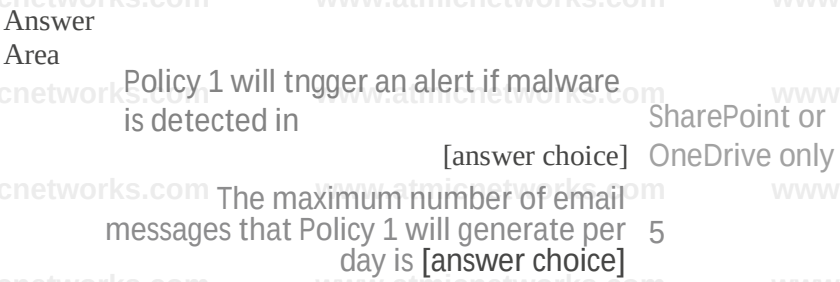
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 375

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature.

You need to block users from downloading a file named File1.exe.

What should you use?

A. an indicator

B. a suppression rule

C. a device configuration profile

Answer: A

Explanation:

Question: 376

You have an Azure AD tenant that contains the users shown in the following table

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

You need to compare the permissions of each role. The solution must minimize administrative effort.

Which portal should you use?

A. the Microsoft Purview compliance portal
B. the Microsoft 365 admin center
C. the Microsoft 365 Defender portt1
D. the Microsoft Entra admin center

Answer: A

Explanation:

Question: 377

HOTSPOT

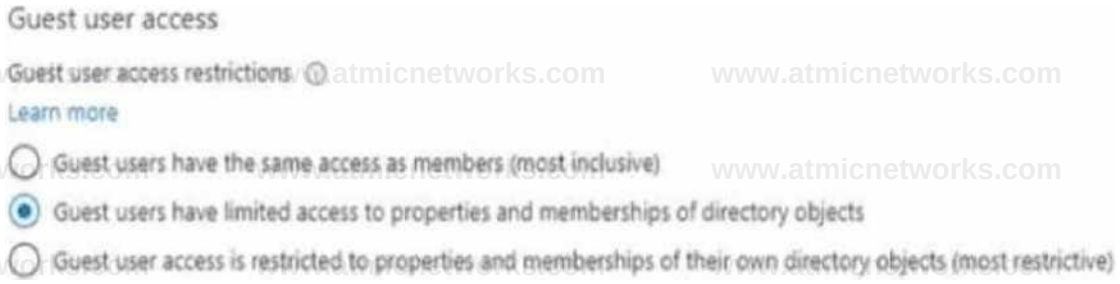
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Role
Group1	Security	Helpdesk Administrator
Group2	Security	*None*
Group3	Microsoft 365	User Administrator

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

In Azure AD, you configure the External collaboration settings as shown in the following exhibit.



Guest invite settings

Guest invite restrictions

Collaboration restrictions

(•) Allow invitations to be sent to any donum (most inclusive;

0 Deny invitations to the specified domains

Cj Allow invitations only to the specified domains (most restrictive)

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

NOTE: Each correct selection is worth one point.

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

Answer Area Statements	Yes	No
Used can invite guest users.		O
User2 can invite guest users.		
User3 can invite guest users.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Used can invite guest users.		
User2 can invite guest users.	●	O
User3 can invite guest users.	●	O

Question: 378

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

Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
Used	Global Administrator	*None*
User2	Exchange Administrator	*None*
User3	Service Support Administrator	*None*
Used	*None*	Organization Management

You plan to use Exchange Online to manage email for a DNS domain.

An administrator adds the DNS domain to the subscription.

The DNS domain has a status of Incomplete setup.

You need to identify which user can complete the setup of the DNS domain. The solution must use the

principle of least privilege.

Which user should you identify?

A. User1

B. User2

C. User3

D. User4

Answer: A

Explanation:

Question: 379

DRAG DROP

You have a Microsoft 365 subscription.

You need to meet the following requirements:

- Report a Microsoft 365 service issue.
- Request help on how to add a new user to an Azure AD tenant.

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Features	Answer Area
Message center	To report issues regarding a Microsoft 365 service: _____
New service request	To request help on how to add a new user to the tenant: _____
Product feedback	
Service health	

Answer:

Explanation:

Question: 380

You have a Microsoft 365 subscription.

You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.

What should you do?

A. Enable Endpoint analytics.
B. Run the Microsoft 365 network connectivity test on each device.
C. Enable privileged access.
D. Configure Support integration.

Answer: A

Explanation:

Question: 381

HOTSPOT

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

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

The groups contain the members shown in the following table.

Name	Members
Group1	User1
Group2	User2, User4

The users are assigned the roles shown in the following table.

Name	Role	Scope
User1	None	Not applicable
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	None	Not applicable

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

Answer Area

Statements	Yes	No
User2 can reset the password of Useri. User2 can reset the password of User4.	O	
User3 can assign licenses to Useri.		

Answer:

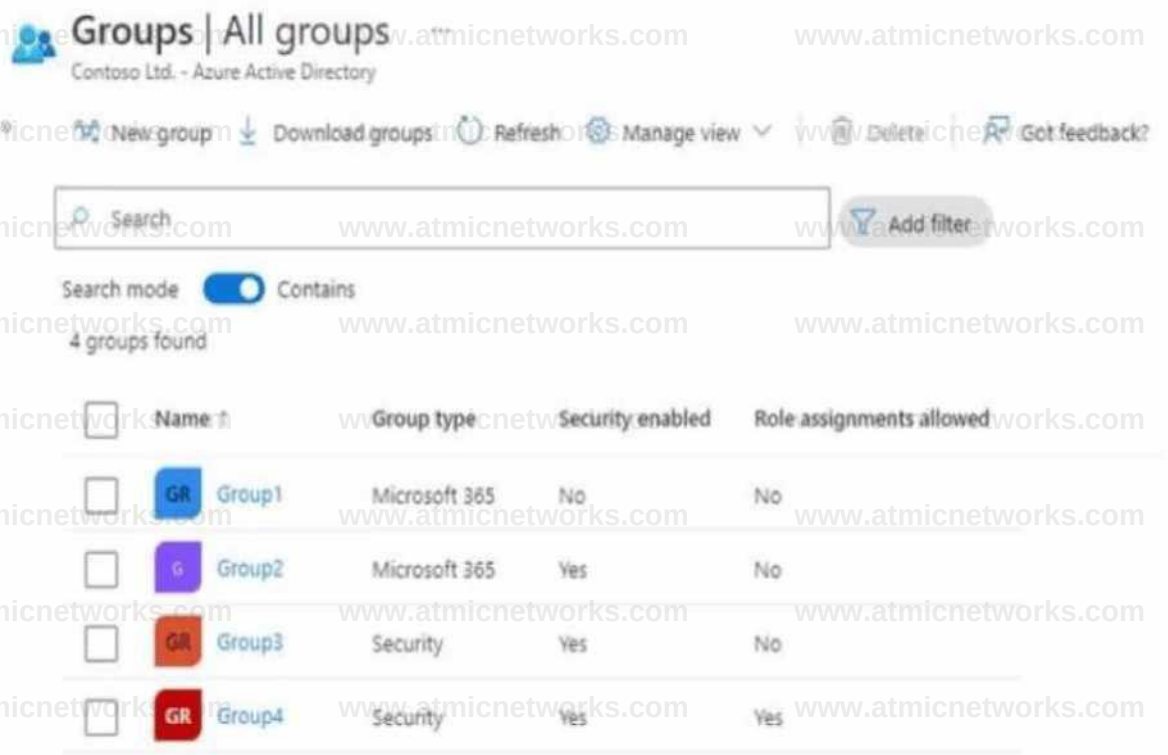
Explanation:

Answer Area

Statements	Yes	No
User2 can reset the password of Useri.	•	
User2 can reset the password of Used.	O	•
Used can assign licenses to User!.	#	

Question: 382

You have a Microsoft 365 E5 subscription that contains the groups shown in the following exhibit.



To which groups can you assign Microsoft 365 E5 licenses?

A. Group! and Group2 only

B. Group2 and Group3 only

C. Group3 and Group4 only
D. Group 1, Group2. and Group3 only
E. Group2, Group3, and Group4 only

Answer: C

Explanation:

Question: 383

HOTSPOT

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
Userl	Global Administrator
User?	Security Administrator, Guest Inviter
User;	tone
1 U$er4	Password Administrator

External collaboration settings have default configuration.

You need to identify which users can perform the following administrative tasks:

- Modify the password protection policy.
- Create guest user accounts.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Modify the password protection policy Userl only

Create new guest users in Azure AD: Userl and User2 only

Question: 384

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Userl	Reports Reader
User2	Exchange Administratoi
UserJ	User Experience Success Manager

Which users can review the Adoption Score in the Microsoft 365 admin center?

A. User! only

B. User2onry

C. User1 and User2 only

D. User! and User3 only

E. User1, User2. and User3

Answer: E

Explanation:

Question: 385

HOTSPOT

You have a Microsoft 365 E5 subscription.

You have an Azure AD tenant named contoso.com that contains the following users:

- Admin1
- Admin2
- User1

Contoso.com contains an administrative unit named AIM that has no role assignments. User1 is a member of AU1. You create an administrative unit named AU2 that does NOT have any members or role assignments. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can add Adminl as a member of AU1.		
You can add Useri as a member of AU2.	O	O
You can assign Admin2 the User administrator role for AU1.	O	Q

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can add Adminl as a member of AU1.	•	
You can add Useri as a member of AU2.	•	O

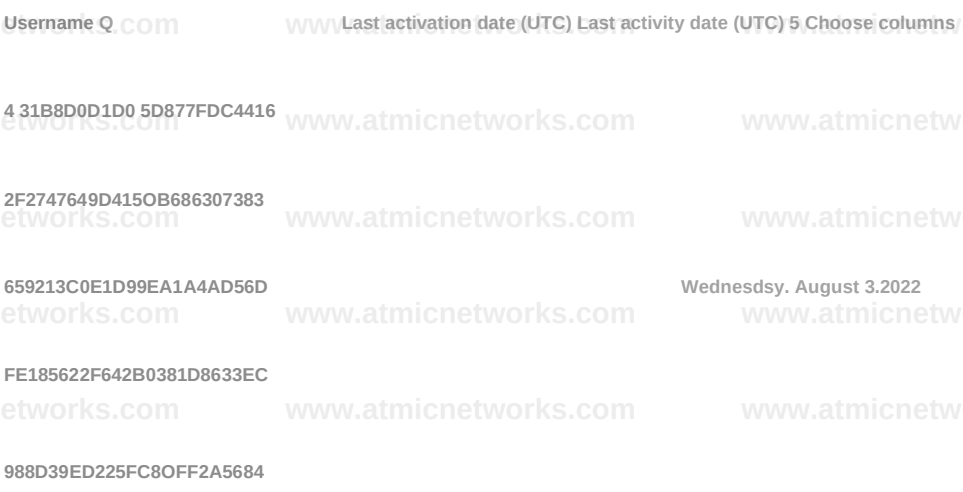
You can assign Admin2 the User administrator role for AU1. C •

Question: 386

HOTSPOT

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.



You need ensure that the report meets the following requirements:

- The Username column must display the actual name of each user.
- Usage of the Microsoft Teams mobile app must be displayed.

What should you modify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

The Username column must display the actual

Reports m Org settings
Privacy profile in Org
Reports in Org settings
The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

Microsoft Teams in Org settings
Microsoft learns in Org settings
The columns in the report

Answer:

name of each user

Explanation:

Answer Area

The Username column must display the actual name of each user Reports in Org settings

Usage of the Teams mobile app must be displayed: Microsoft Teams in Org settings

Question: 387

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
Useri	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations.

Which users can the policy protect?

A. User2 and User4 only

B. User1 and User3 only

C. Userl1 only

D. User1, User2, User3, and User4

Answer: C

Explanation:

Question: 388

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Each user has an Android device with the Microsoft Authenticator app installed and has set up phone sign-in.

The subscription has the following Conditional Access policy:

- Name: Policy1
- Assignments

o Users and groups: Group1, Group2

o Cloud apps or actions: All cloud apps

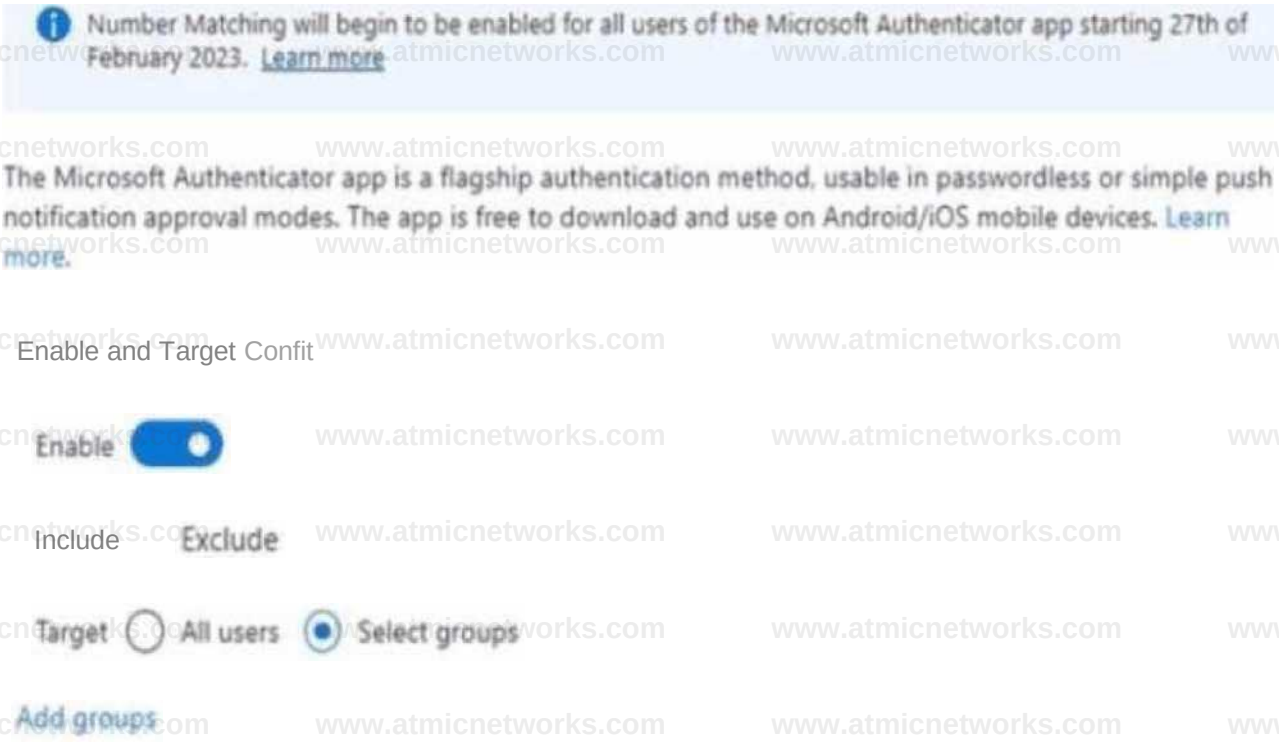
- Access controls

o Grant Require multi-factor authentication

- Enable policy: On

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

Microsoft Authenticator settings



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

NOTE: Each correct selection is worth one point.

rawer Area

Statements	Yes	No
User 1 can sign in by using number matching in the Microsoft Authenticator app		
User2 can sign in by using a username and password		
User J can sign in by using number matching in the Microsoft Authenticator app.		

Answer:

Explanation:

Answer Area Statements	Yes	No
User 1 can sign in by using number matching in the MicrosoftAuthenticator app	•	
User2 can sign in by using a username and password.	O	$
User 3 can sign in by using number matching in the MicrosoftAuthenticator app.		O

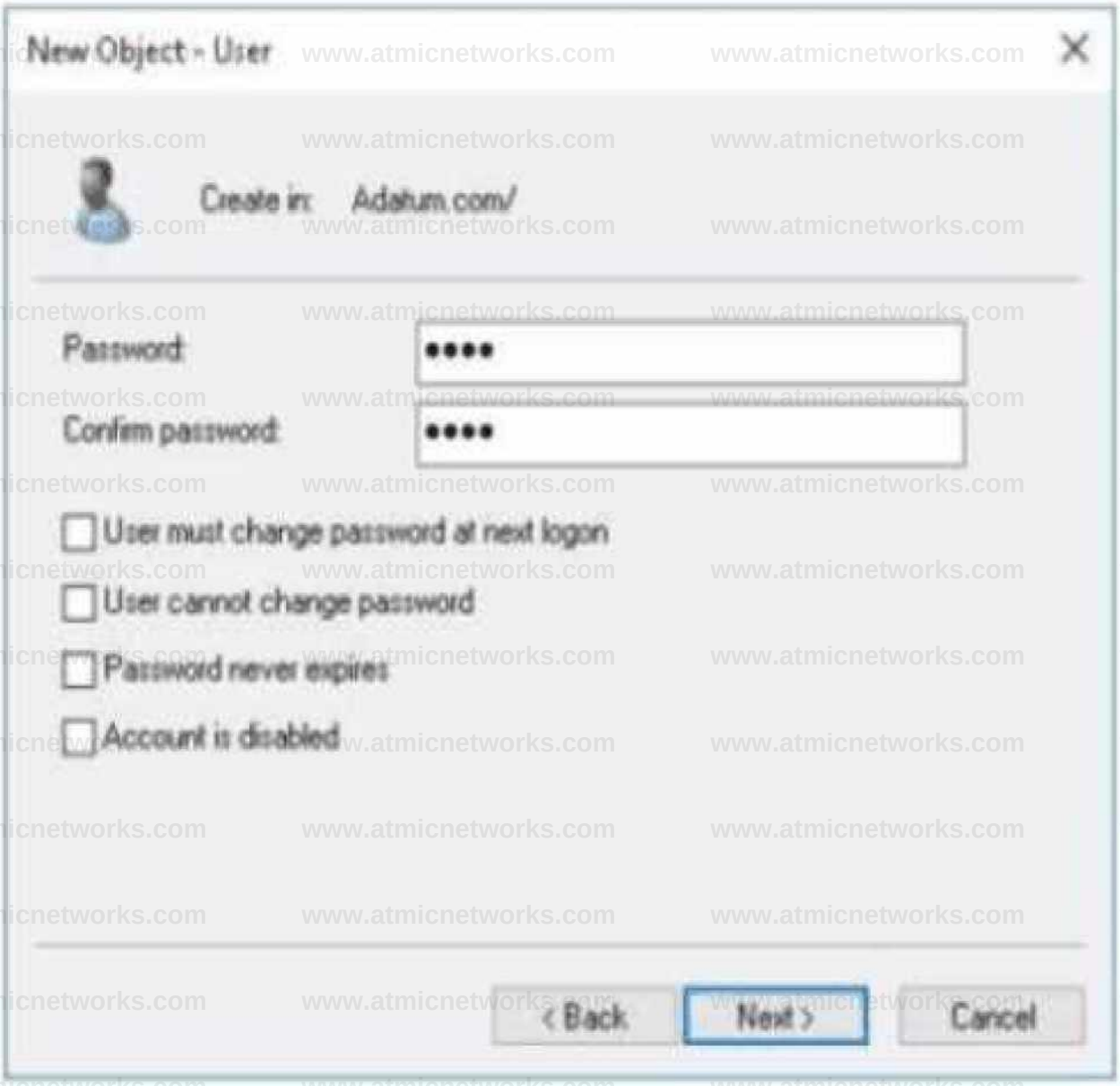
•

Question: 389

HOTSPOT

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password write back is disabled.

You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



The Azure AD password policy is configured as shown in the following exhibit.

Password policy

Set the password policy for all users in your organization.

Days before passwords expire 90

Days before a user is notified about expiration 14

You confirm that User1 is synced to Azure AD.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Useri can sign in to Azure AD		

Used can change the password immediately by using the My Apps portal.

From Azure AD, User 1 must change the password every 90 days.

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can sign in to Azure AD.	♦	
Used can change the password immediately by using the My Apps portal.		•
From Azure AD. User 1 must change the password every 90 days.	•	

Question: 390

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

On Tuesday, User1 signs in for the first time and perform the following actions:

- Signs in to Microsoft Exchange Online from an anonymous IP address
- Signs in to Microsoft SharePoint Online from a device in New York City.
- Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections

Which types of sign-in risks will Azure AD Identity Protection detect for User1?

A. anonymous IP address only

B. anonymous IP address and atypical travel

C. anonymous IP address, atypical travel, and unfamiliar sign-in properties

D. unfamiliar sign-in properties and atypical travel only

E. anonymous IP address and unfamiliar sign-in properties only

Answer: A

Explanation:

Question: 391

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.

Corporate policy states that user passwords must not include the word Contoso.
What should you do to implement the corporate policy?

A. From Azure AD Identity Protection, configure a sign-in risk policy.
B. From the Microsoft Entra admin center, create a conditional access policy.
C. From the Microsoft 365 admin center, configure the Password policy settings.
D. From the Microsoft Entra admin center, configure the Password protection settings.

Answer: D

Explanation:

Question: 392

HOTSPOT

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

From the Sign-ins blade of the Microsoft Entra admin center for which users can User1 and User2 view the sign-ins? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

UserI can view the sign-ms for the following users: | ^^ ^^ user] and User

UserI only
UserI and User2 only
UserI, User2. and User3 only

User2 can view the sign-ins for the following users: User' and User2 only I User2 only

UserI, User2, and User3 only
UserI, User2, User3, and User4

Answer:

Explanation:

Answer Area

UserI can view the sign-ms for the following users: UserI, User2. User3, and User4

User2 can view the sign-ins for the following users: and User2 only

Question: 393

Your company has on-premises servers and an Azure AD tenant.

Several months ago, the Azure AD Connect Hearth agent was installed on all the servers.

You review the health status of all the servers regularly.

Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.

You suspect that another administrator removed Server1 from the list.

You need to ensure that you can view the health status of Server1.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. From Azure Cloud shell, run the Connect-Azure AD cmdlet.

B. From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)

C. From Server1, change the Azure AD Connect Health Services Startup type to Automatic D. From Windows PowerShell, run the Rejister-ArureADConnectHealthsyncAgent cmdlet. E. From Server1, reinstall the Azure AD Connect Health agent

Answer: D,E

Explanation:

Question: 394

HOTSPOT

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

Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

You create a conditional access policy that has the following configurations:

- Users or workload identities:

o Include: Group1

o Exclude: Group2

- Cloud apps or actions: Include all cloud apps
- Conditions:

o Include: Any location

o Exclude: Montreal

- Access control: Grant access, Require multi-factor authentication

User1 is on the multi-factor authentication (MFA) blocked users list.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Used can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.		
Used can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.		
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.1020.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Used can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	•	
Useri can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	(	•
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.1020.	•	

Question: 395

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.

Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Answer Area

Users that can use SSPH

- User L User2, and User4 only
- Useri and User2 only
- User!, User?, and User4 only
- Useri, User?, User3, and User4

Users that must answer secunty questions to reset their password:

- Useri and User? only
- Useri only
- User? only
- User 1 and User? only
- Useri, User?, and User? only
- User! User2. and User4 only
- Useri, UserZ User3, and User4

Answer:

Explanation:

Answer Area

Users that can use SSPR: Useri, User! and User4 only

Users that must answer security questions to reset their password: User 1 and User2 only

Question: 396

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 network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 397

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 network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 398

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 network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 399

Your network contains an Active Directory forest named Contoso. Local.

You have a Microsoft 365 subscription.
You plan to implement a directory synchronization solution that will use password hash synchronization.
From the Microsoft 365 admin center, you successfully verify the contoso.com domain name. You need to prepare the environment for the planned directory synchronization solution. What should you do first?

A. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.
B. From the Microsoft 365 admin center verify the Contoso. Local domain name.
C. From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.
D. From Active Directory Users and Computers, modify the UPN suffix for all users.

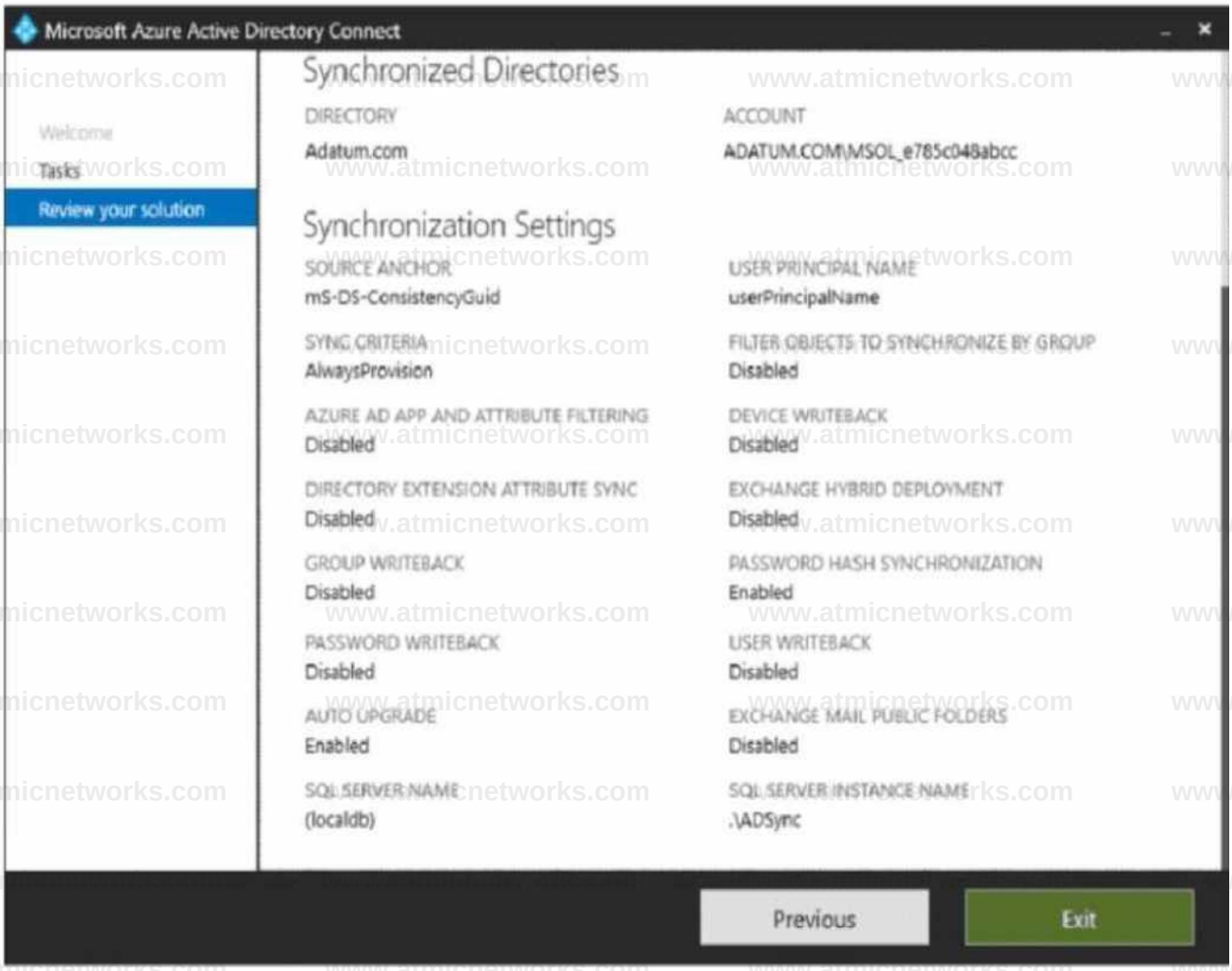
Answer: A

Explanation:

Question: 400

HOTSPOT

Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.



An on-premises Active Directory user account named Allan You is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan @>ddatum.onmicrosoft.com.

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

Answer Area Statements	Yes	No
From the Azure portal,you can reset the password of Allan Yoo.	O	Q
From the Azure portal, you can configure the job title of Allan Yoo		
From the Azure portalyou can configure the usage location of Allan Yoo.	O	Q

Answer:

Explanation:

Answer Area

Statements	Yes	No
From the Microsoft Entra admin center, you can reset the password of Allan Yoo.	•	
From the Microsoft Entra admin center, you can configure the job title of U » Allan Yoo.		
From the Microsoft Entra admin center, you can configure the usage location • of Allan Yoo,		

Question: 401

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.

You purchase a Microsoft 365 subscription.

You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO).

You need to ensure that users can use Seamless SSO from the Windows 10 computers.

What should you do?

A. Join the computers to Azure AD.
B. Create a conditional access policy in Azure AD.
C. Modify the Intranet zone settings by using Group Policy.
D. Deploy an Azure AD Connect staging server.

Answer: C

Explanation:

Question: 402

You have a Microsoft 365 subscription.

You add a domain named contoso.com.

When you attempt to verify the domain, you are prompted to send a verification email to

admin@contoso.com.

You need to change the email address used to verify the domain.

What should you do?

A. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
B. Add a TXT record to the DNS zone of the domain.
C. From the domain registrar, modify the contact information of the domain.
D. Modify the NS records for the domain.

Answer: C

Explanation:

Question: 403

You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.

You purchase 100 Microsoft 365 Business Voice add-on licenses.

You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically.

What should you do?

A. From the Microsoft 365 admin center, modify the settings of the Voice group.
B. From the Licenses page of the Microsoft 365 admin center, assign the licenses.
C. From the Microsoft Entra admin center, modify the settings of the Voice group.

Answer: C

Explanation:

Question: 404

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the security groups shown in the following table.

Name	Membership type	Membership rule
Groupi	Assigned	*Not applicable*
Group 2	Dynamic	**(user.department -eq "Finance")**
Groups	Dynamic	(user.department -eq "R&D")

The subscription contains the users shown in the following table.

Name	Department	Assigned group membership
Useri	Finance	Groupi
User2	Technical	*None*
UserB	R&D	Groupi

You have a Conditional Access policy that has the following settings:

- Assignments

o Users

- Include: Groupi
- Exclude: Group2. Group3

o Target resources

- Cloud apps
- App1
- Access controls
- Grant
- Block 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.

Answer Area

Statements	Yes	No
Used can sign in to Appt		0
User2 can sign in to Appt	0	o
User3 can sign in to Appt	O	0

Answer

Explanation:

Answer Area

Statements	
Useri can sign in to App!	
User2 can sign in to Appt	
User3 can sign in to Appt	

Question: 405

DRAG DROP

You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.

All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.

You plan to implement self-service password reset (SSPR).

You need to ensure that when a user resets or changes a password, the password syncs with AD DS.

Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer Area

From the Microsoft Entra admin center, configure on-premises integration password writeback-

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Step 1; Validate permissions for the Microsoft Entra Connect account.

Step 2:

Step 3:

Answer:

Explanation:

Question: 406

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.

You need to compare your company's security configurations to Microsoft best practices and review improvement actions to increase the security posture.

What should you use?

A. Microsoft Secure Score
B. Cloud discovery
C. Exposure distribution
D. Threat tracker
E. Exposure score

Answer: A

Explanation:

Question: 407

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 goats. 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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint. and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint Administrator role.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 408

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 goats. 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 network contains an Active Directory domain.

You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant. Solution: From Microsoft Entra Connect, you modify the filtering settings.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 409

HOTSPOT

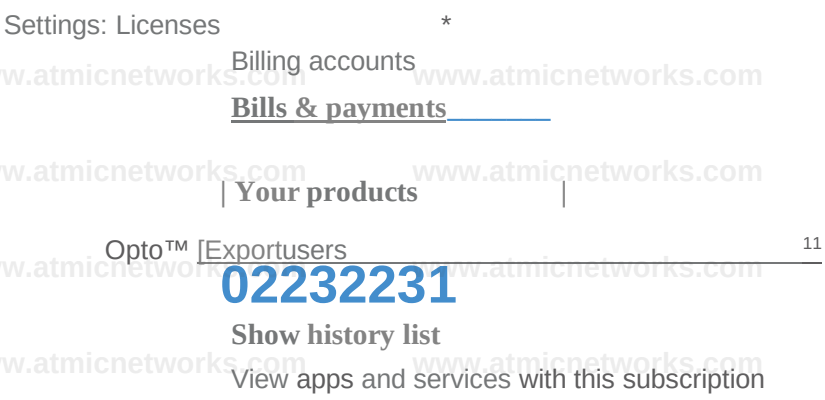
You have a Microsoft 365 subscription.

You need to identify all users that have an Enterprise Mobility + Security plan, and then provide a list of the users in the CSV format.

Which settings should you use in the Microsoft 365 admin center, and which option should you select? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Question: 410

HOTSPOT

You have a Microsoft 365 subscription That contains two administrative units named AU1 and AU2.

The subscription contains the users shown in the following table.

Name	Administrative unit	Role	Scope
Userl	Ware	User Ad ministrrtftar	AU1
UserZ	AU1	Global Administrator	Mtwie
User3	None	*None*	Organization

The subscription contains the groups shown in the following table.

Name	Members	Administrative unit
Groupl	UserS	AU2
Group2	UserZ User3	AU1

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

Answer Area

Statements	Yes	No
Userl can reset the password of User?		
User! can modify the membership of Groupl		
User* can reset the password of User!		

Answer:

Explanation:

Answer Area

Statements	Yes	No
User' can reset the password of User!		
UserZ can modify the membership of Groupl,	«.	0

User' can reset the password of User3. *

Question: 411

You have a Microsoft 365 ES subscription.

From the Microsoft 365 Defender portal, you review your company's Microsoft Secure Score.

You discover a large number of recommended actions.

You need to ensure that the actions can be filtered based on specific department names.

What should you create first?

A. a dynamic security group

B. a tag

C. an administrative unit

D. a custom detection rule

Answer: C

Explanation:

Question: 412

HOTSPOT

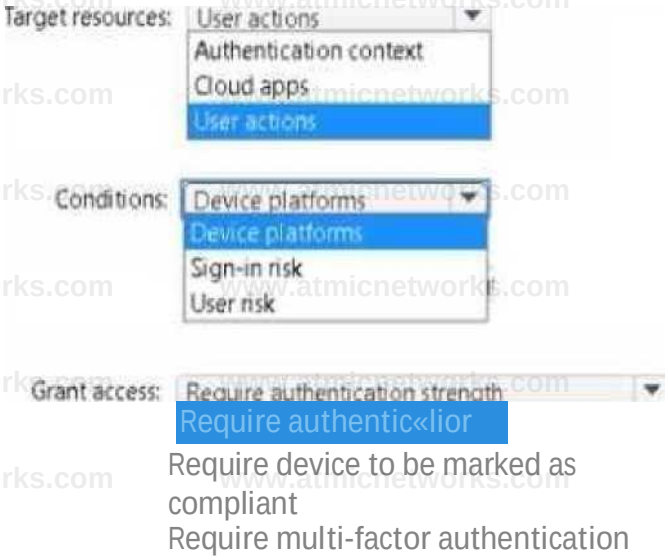
You have a Microsoft 365 E5 subscription.

You need to create a Conditional Access policy that will require the use of FID02 security keys only when users join their Windows devices to Microsoft Entra ID.

How should you configure the policy? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Grant access:

Question: 413

Your network contains an Active Directory domain.

You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant. Solution: From Microsoft Entra Connect you modify the Microsoft Entra credentials. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 414

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create a Microsoft Entra tenant

You plan to sync the on-premises Active Directory to the Microsoft Entra tenant.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete and as quickly as possible if a single server fails. What should you include in the recommendation?

A. one Microsoft Entra Connect sync server and one Microsoft Entra Connect sync server in staging mode

B. three Microsoft Entra Connect sync servers and one Microsoft Entra Connect sync server in staging mode

C. six Microsoft Entra Connect sync servers and three Microsoft Entra Connect sync servers in staging mode

D. three Microsoft Entra Connect sync servers and three Microsoft Entra Connect sync servers in staging mode

Answer: A

Explanation:

Question: 415

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Linux
Device3	MacOS

You plan to create an Endpoint security policy by using the Defender Update controls template. To which device can you apply the policy?

A. Device1 only

B. Device1 and Devke2 only

C. Devke1 and Device3 only

D. Devke1, Device2. and Devke3

Answer: A

Explanation:

Question: 416

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named user1@contoso.com and user2@contoso.com and a Microsoft SharePoint site named Site1.

You create a data loss prevention {DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Nanw	Content contains	User notifications	Priority
	4&imoie |P.?rfili?w5	User 1 $ contoso.com	0
Rule?	2 OF more IP addresses	User1@conto5o.com	1
Rule?	re nose IP addresses	U$er2@contoso com	2

DLP1 is applied to Site1.

You have the files shown in the following table.

Name	Number of IP addresses in the file
Filei.xht	2
Fiie2.doc	3
Fiielpptc	4

Fiie4.txt	6

You copy the files to Site1.

low many notifications will each user receive? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

User1@contoso.com: 2 notifications
User2@contoso.com: 1 notification

User1@contoso.com: 2 notifications
File3.pptx contains 4 IP addresses, which matches Rule1 (4 or more IP addresses), triggering

a notification to User1.

File4.txt contains 6 IP addresses, which also matches Rule1, triggering another notification to User1. Therefore, User1 receives 2 notifications.

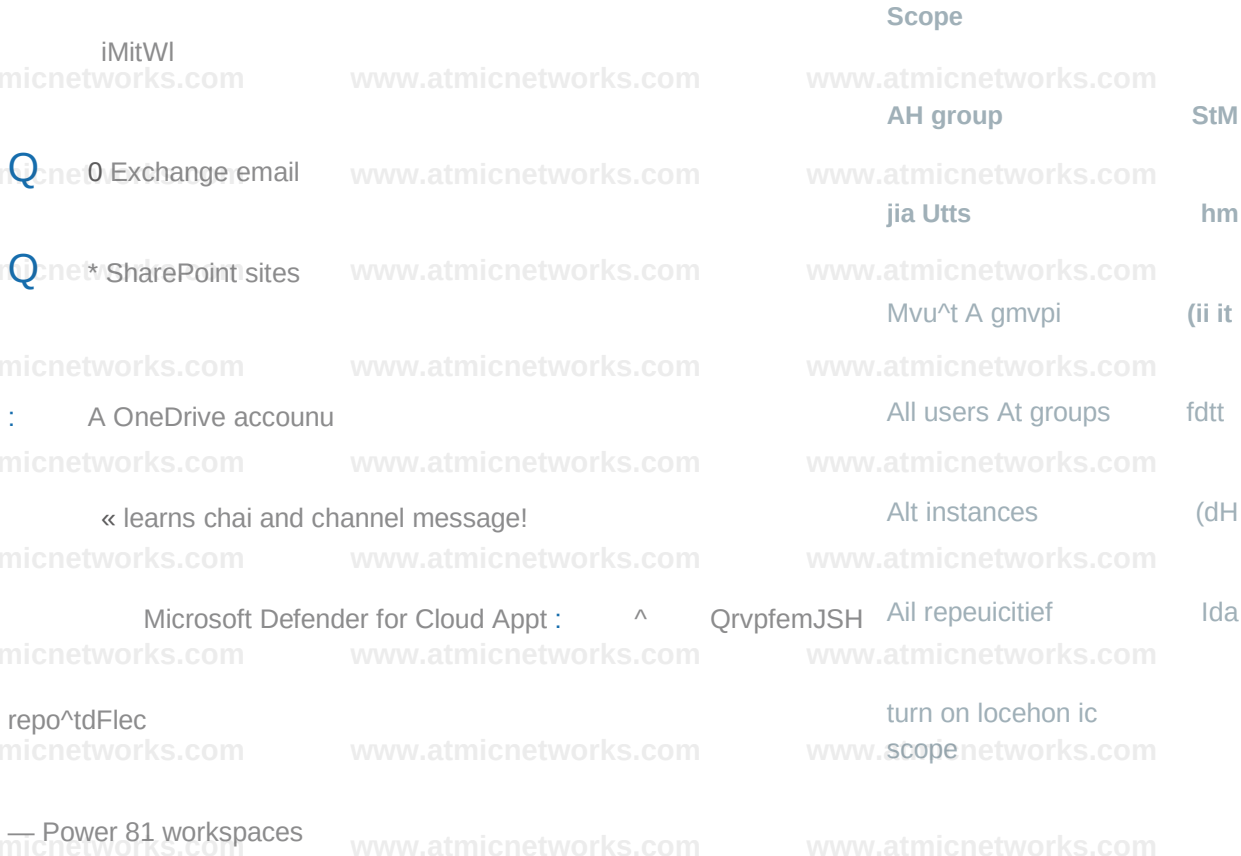
User2@contoso.com: 1 notification

File2.doc contains 3 IP addresses, which matches Rule3 (3 or more IP addresses), triggering a notification to User2. Therefore, User2 receives 1 notification.

Question: 417

You have a Microsoft 365 E5 subscription.

You are creating a data loss prevention (DLP) policy applied to the locations as shown in the following exhibit.



Which condition can you use in the DIP rules of the policy?

A. sensitive info types
B. sensitivity labels
C. content search queries
D. keywords

Answer: A

Explanation:

Question: 418

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft Defender XDR. Which Microsoft service source will appear on the Incidents page of the Microsoft Defender portal? A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for Cloud

C. Azure Arc

D. Azure Information Protection

Answer: D

Explanation:

Question: 419

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure Microsoft Entra Password protection.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 420

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a SharePoint site named Site1. Site1 contains the files shown in the following table.

Name	Number of [p addresses in the file
Filel	2
File2	5

You have the users shown in the following table.

Name	Role
User1	Site owners for Site1
User2	Site members for Site1
Admin1	SharePoint admins

You create a data loss prevention (DLP) policy with an advanced DLP rule and apply the policy to Site1. The DLP rule is configured as shown in the following exhibit.

Edit rule

Conditions

We II apply this policy to content that matches these conditions.

A Content contains

X Create group

Default — Any of these

Sensitive info types

Add

- Add condition

Exceptions

Actions

Use actions to protect content when the conditions are met

A Restrict access or encrypt the content in Microsoft 365 locations

| Restrict access or encrypt the content in Microsoft 365 locations

- i Block users from receiving email or accessing shared SharePoint OneOnve. and Teams files

By default users are blocked from sending Teams chits and channel messages that contain the type of content you re protecting But you can choose who is blocked from receiving emafs or accessing tiles shared from SharePoint. OneDnve, and Teams

- I Block everyone

Q Block only people outside your organisation G

-) Block only people who were given access to the content thro ugh the Anyone with the

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Userl can open FHe2	0	0

U$er2 can open Filet	0	0
Admin 1 can open File!	0	0

Answer:

Explanation:

User1 can open File2: No
User2 can open File1: Yes
Admin1 can open File2: Yes

User1 can open File2: No

The DLP policy specifies that if a file contains 3 or more IP addresses, access to that content should be restricted. File2 contains 5 IP addresses, which exceeds the threshold set by the DLP policy. Therefore, User1, who is a site owner, will not be able to access File2 because it matches the conditions set in the DLP rule to block access.

User2 can open File1: Yes

File1 contains only 2 IP addresses, which is below the threshold of 3 set by the DLP policy. Since the DLP policy does not apply to files with fewer than 3 IP addresses, User2, who is a site member, can access File1 without any restrictions.

Admin1 can open File2: Yes

Admin1 is part of the SharePoint admins group, which typically has elevated privileges. Despite the DLP rule, SharePoint admins are generally not restricted by the same DLP rules that apply to regular users. Therefore, Admin1 can access File2.

Question: 421

HOTSPOT

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	**Policy name**	Managers
	Description Applied to	
		If the email is sent to 1 tvinS SM365x28975$.OnMicrosoft com Mmam<>@M365x289755 OnMicrosoft.com Except if the email is sent to member of: test 1 ww? M365x289755.onmrcroFcft.com
	Safety tips > Oser impersonation Safety tips	Off
	> Domain impersonation Safety tips >	Off
	Unusual characters Mailbox tntelbgencr	Off Off
Spoof	**Enable antispoofing protection**	On
	Action	Quarantine the message
Advanced settings	**Advanced phishing thresholds**	3 More Aggressive

Use the drop-down menus to select the answer choke that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

if a message is identified as a domain impersonation [answer choice]

- the message <s delive'eJiSie Inbox foldei
- the message is moved to the Deleted Items foldei
- the messages is moved to the Junk Email folder
- the message is NOT delivered

To teduce the likelihood ot tne impersonation policy generating false positives, configure [answer choice]

- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

Answer:

Explanation:

If a message is identified as a domain impersonation: the message is moved to the Junk Email folder

According to the anti-phishing policy settings shown in the exhibit, messages identified as domain impersonation should be moved to the Junk Email folder to reduce the risk of phishing attacks.

To reduce the likelihood of the impersonation policy generating false positives, configure: Mailbox intelligence

Mailbox intelligence helps in reducing false positives by using machine learning and historical email patterns to make better decisions about which emails are legitimate and which are not.

Question: 422

HOTSPOT

You have a Microsoft 365 E5 subscription.

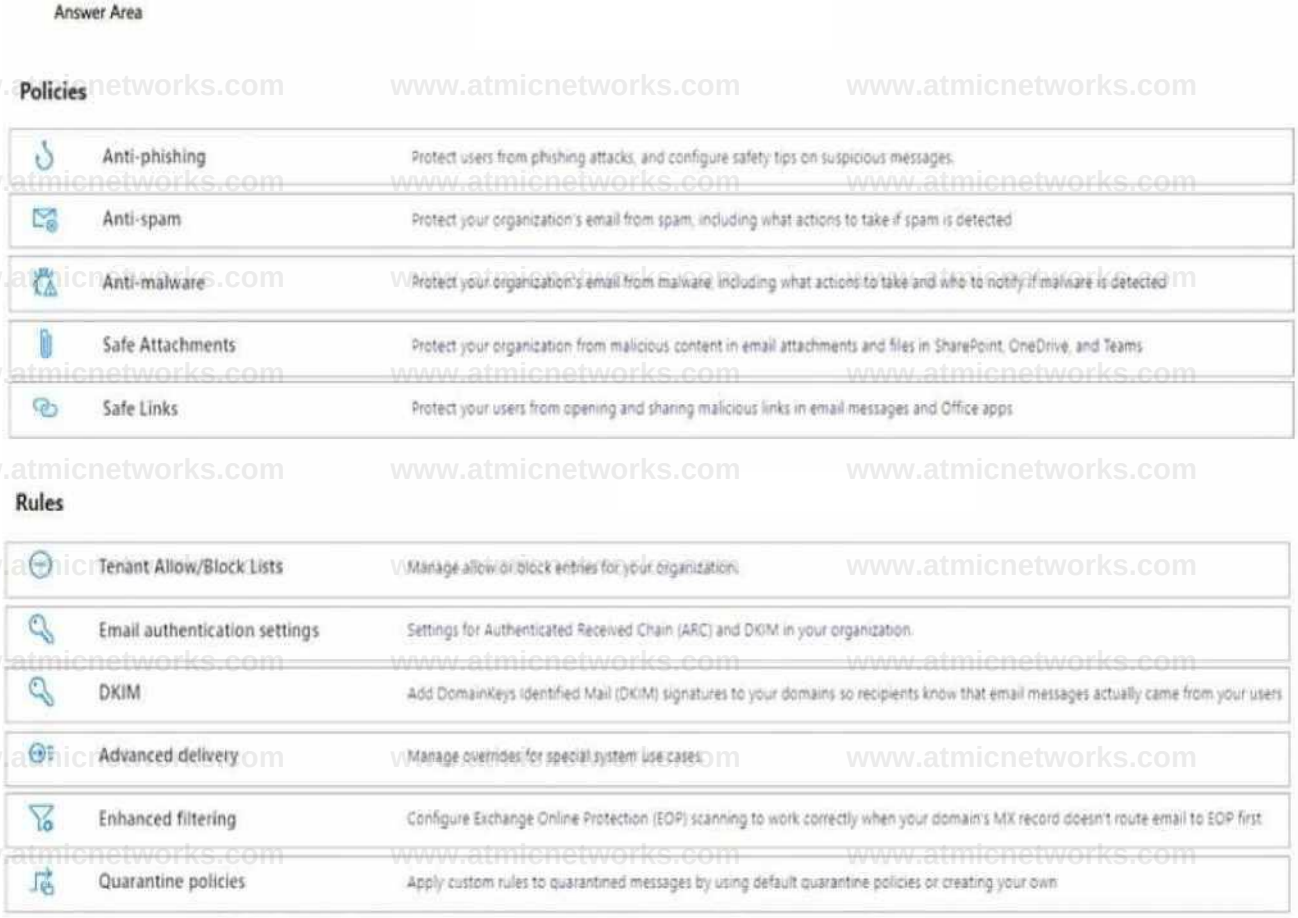
You need to configure threat protection tor Microsoft 365 to meet the following requirements:

- Limit a user named User 1 from sending more than 30 email messages per day.
- Prevent the delivery of a specific file based on the file hash.

Which two threat policies should you configure in Microsoft Defender for Office 365? To answer, select the appropriate threat policies in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Limit a user named User 1 from sending more than 30 email messages per day: Anti-spam policy

The anti-spam policy in Microsoft Defender for Office 365 allows you to configure outbound spam settings, including limiting the number of email messages a user can send per day. This helps prevent spam and potential email abuse within the organization.

Prevent the delivery of a specific file based on the file hash: Safe Attachments policy The Safe Attachments policy in Microsoft Defender for Office 365 can be configured to block or quarantine emails with attachments that match specific file hashes. This ensures that potentially malicious files are not delivered to users' inboxes.

Question: 423

HOTSPOT

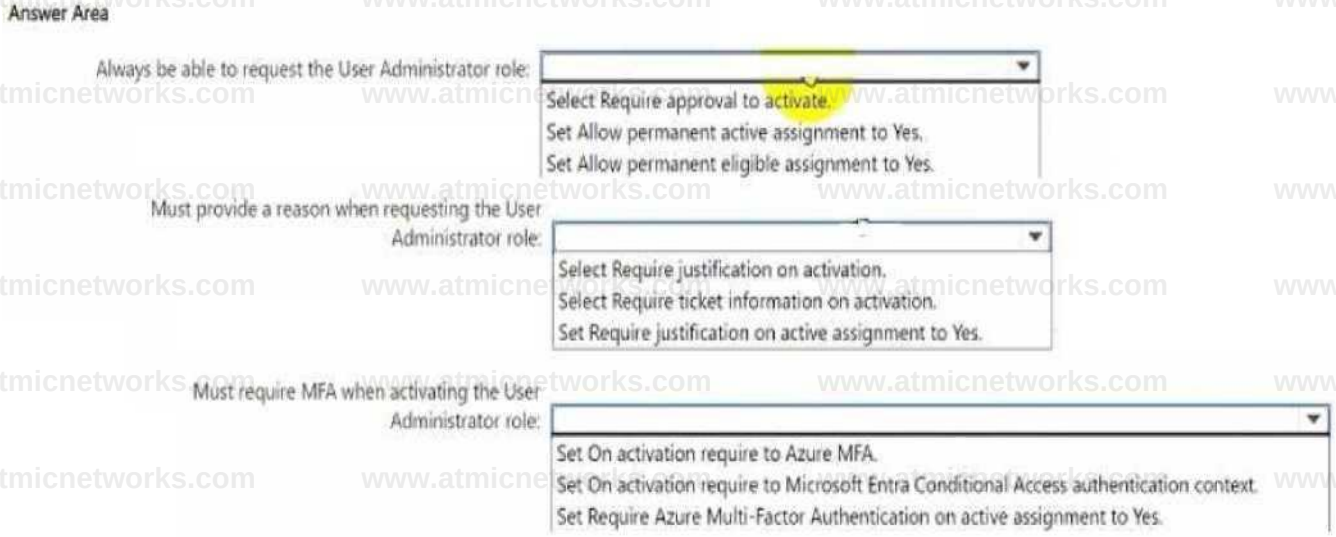
You have a Microsoft 365 E5 subscription.

You need to configure Privileged Identity Management (PIM) for the User Administrator role in Microsoft Entra. Eligible users must meet the following requirements:

- Always be able to request the User Administrator role.
- Must provide a reason when requesting the User Administrator role
- Must require multi-factor authentication (MFA} when activating the User Administrator role

The solution must minimize administrative effort.

Answer Area



Answer

Explanation:

Always be able to request the User Administrator role: Setting "Allow permanent eligible assignment to Yes" ensures that users can always request the User Administrator role when needed.

Must provide a reason when requesting the User Administrator role: Selecting "Require justification on activation" ensures that users must provide a reason each time they activate the User Administrator role, which adds a layer of accountability and tracking.

Must require MFA when activating the User Administrator role: Setting "Require Azure Multi-Factor Authentication on active assignment to Yes" ensures that users must perform MFA to activate the User Administrator role, enhancing security.

Question: 424

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Mu lti- Factor Auth Status
Useri	Groupl	Disabled
User?	Giwpl,Grwp2	Enabled
Useri	Group?	Disabled

You configure a Multifactor authentication registration policy that has the following settings:

• Assignments:

* Include: Group1

* Exclude: Group2

- Controls: Requite Microsoft Entra ID multifactor authentication registration
- Policy enforcement: Enabled

You create a conditional access policy that has the following settings:

- Name: Policy1

• Assignments:

* Include: Group1

* Exclude; Group1

- Grant: Require multifactor authentication
- Enable policy. On

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

NOTE: Each coned selection is one point.

Answer Area

Statements	Yes	No
Useri will be required to register for MFA on the next sign-in.		
User2 will be required to register for MFA on the next sign-in		
User 3 will be required to register for MFA on the next sign-in.		

Answer:

Explanation:

User1 will be required to register for MFA on the next sign-in: Yes

User1 is a member of Group1, which is included in the MFA registration policy. Since User1 is not excluded, they will be required to register for MFA on the next sign-in.

User2 will be required to register for MFA on the next sign-in: No

User2 is a member of both Group1 and Group2. Since Group2 is excluded from the MFA registration policy, User2 will not be required to register for MFA.

User3 will be required to register for MFA on the next sign-in: No

User3 is a member of Group2, which is excluded from the MFA registration policy.

Therefore, User3 will not be required to register for MFA.

Question: 425

HOTSPOT

You have a Microsoft 365 E5 subscription.

You create a Conditional Access policy named Policy1 and assign Policy1 to all users.

You need to configure Policy1 to enforce multi factor authentication (MFA) if the user risk level is high.

Which two settings should you configure in Policy1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer

Explanation:

Conditions: Set "User risk" to "High"

To enforce MFA based on user risk, you need to configure the Conditional Access policy to trigger when the user risk level is high. This setting ensures that the policy is applied only to users who have a high-risk level.

Grant: Require multi-factor authentication

This setting enforces MFA for users who meet the condition set (high user risk). Requiring

MFA ensures that users must provide additional verification, enhancing security for high-risk sign-ins.

Question: 426

HOTSPOT

You have a Microsoft 365 subscription.

From Microsoft Entra Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Global Administrator | Role settings

Privileged ‘deputy Management | Microsoft tntra rotes

^ EAt

Activation

Selling State

Activation maximum duration (hours) 8 hourfs)

Altaic permanent active a mgr

Atut£ MFA

Assignment

Setting	State
-"?.■■ ~Frrr..i^nt .-■ g,D - r^gnme^i	No
E npire digit ir mlgnmenu n-r	15 cay [si

Allow permanent active assignment »es

Expire active assignments a Her -

Require AZLre Mu 11 ■ F a dor Au t hgntitflJ t ez

Require justification on active assignment No

You make a user named admin1@contoso.com eligible for the Global Administrator role. Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the

Answer Area

To use the Global Administrator role, adminl (Scontoso com must provide (answer choice]

Azure Multi Fitta Authentication (MFA) and requites admin approval justification and Azure Multi-Factor Authentication (MFA) ticket information and justification ticket information and requires admin approval

To make a new user eligible for the Global Administrator role, a PIM administrator must configure [answer choice]

an assignmen Azure MultiF justification and ticket

These are the selections lor the statement To make a new user eligible for the Global Administrator r administrator must configure [answer choke].

Explanation:

Answer:

To use the Global Administrator role, admin1@contoso.com must provide: Azure MultiFactor Authentication (MFA)

The role settings indicate that "Require Azure Multi-Factor Authentication" is set to "Yes" for active assignments. Therefore, admin1@contoso.com must provide Azure MFA to use the Global Administrator role.

To make a new user eligible for the Global Administrator role, a PIM administrator must configure: an assignment that expires after 15 day(s)

The settings show that eligible assignments expire after 15 days. Therefore, to make a new user eligible, a PIM administrator must configure an assignment with this expiration period.

Question: 427

HOTSPOT

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

Name	Department	Job title
Userl	IT enginttring	Technician
User?	Engineering	Senior executive
Useri	Finance	Manager

You create a new administrative unit named AU1 and configure the following AU1 dynamic membership rule.

The subscription contains the role assignments shown in the following table.

Name	Role
AdminI	AUTMta Admi^i nfator
Admin?	Global Adniin^liatot

Answer Area

Statements	Yes	No
AdminI can reset the password of Used	0	0
AdminI can reset the password of User2.		
Admm2 can reset the password of User3		

Answer:

Explanation:

Admin1 can reset the password of User1: Yes

Admin1 has the User Administrator role within AU1. User1 is a member of Group1, which is included in AU1's dynamic membership rule.

Admin1 can reset the password of User2: No

User2 is a member of both Group1 and Group2. However, User2's job title contains "Executive," which excludes them from AU1's dynamic membership rule. Therefore, Admin1 cannot reset User2's password.

Admin2 can reset the password of User3: Yes

Admin2 has the Global Administrator role, which grants the ability to reset passwords for any user within the organization, including User3.

Question: 428

HOTSPOT

Your company has a Microsoft Entra tenant that contains the users shown in the following table.

Name	Role

Useri	Privileged Re Ie Admrnsualoi
User2	User Administrator
UserS	S^Uiity AdTiinitKecr
User#	Si 11ng Administrator

The tenant includes a security group named Admin1. Admin1 will be used to manage administrative accounts. External collaboration settings have default configuration. You need to identify which users can perform the following administrative tasks:

Answer Area

Create guest user accounts

- User4 only
- User 2 only
- User? only
- Usei2 and UserS only
- Useri, User?, and User J only

Add UsetS to Admin 1: I

- User? only
- User3 only
- User4 only
- User? and User 3 only
- Used, User? and UserS only
- Used, User?, User3 and U$er4

Answer:

Explanation:

Create guest user accounts: User1, User2, and User3 only

User1: Privileged Role Administrator role has the ability to manage role assignments in Azure AD, including creating guest accounts.

User2: User Administrator role can manage user accounts, including creating guest accounts.

User3: Security Administrator role does not typically include permissions for creating guest accounts, but in some configurations, they might have limited guest user management capabilities.

Add User3 to Admin1: User2 only

User2: User Administrator role has the permissions to add users to security groups like Admin1.

Question: 429

HOTSPOT

You have a Microsoft 365 subscription that uses a domain name of adatum.com.

In Microsoft Entra ID. you set Guest invite restrictions to Only users assigned to specific admin roles can invite guest users.

A user named used@adatum.corn reports that they can no longer invite external users from a domain namedcontoso.com to collaborate in Microsoft Teams.

You need to modify the Microsoft Entra ID configuration to meet the following requirements:

- Ensure that User1 can invite the contoso.com users to Teams
- Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant.
- Follow the principle of least privilege

What should you do for each requirement' To answer, select the appropriate options in the answer area.

Answer Area

Ensure that User! can invite the contoso com users to Teams

- Assign the Guest Invitei row to User 1
- Assign the User Administrator role to Userl
- Assign the Teams Administratoi role to Userl
- Add User 1 as a orouo ownei to each team in Teams

Ensure that only the contoso com users can be invited as guests to the Microsoft Entra tenant

- From the Cross tenant acceasettings, edit the Outbound access settings.
- From the External collaboration settings, edit the Collaboration restrictions settings
- From the External collaboration settings, edit the Guest user access restrictions settings

Answer

Explanation:

Ensure that User1 can invite the contoso.com users to Teams: Assign the Guest Inviter role to User1

Assigning the Guest Inviter role ensures that User1 has the necessary permissions to invite external users, such as those from contoso.com, to Microsoft Teams.

Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant: From the External collaboration settings, edit the Guest user access restrictions settings

Modifying the Guest user access restrictions settings under External collaboration ensures that only users from specific domains, like contoso.com, can be invited as guests to the Microsoft Entra tenant.

Question: 430

HOTSPOT

You have a Microsoft Entra tenant that contains the groups shown in the following exhibit.

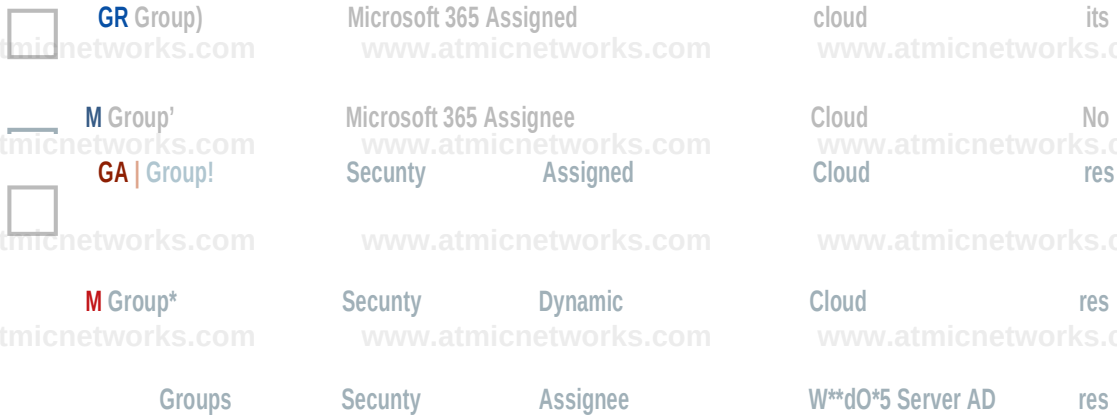
"^ K«v\ group * Download groups _'Refresh K Columns [1] A* Got feedback'

£ ^| V Add filter

Search mode Contains

5 groups found

Name *	Group type	Membership type	Source	Secunty enabled



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each cont'd selection is worth one point.

Answer Area

You can add a Microsoft Entra cloud user to **[answer choice]**

- Groupl only
- Groupl and Group? only
- Groupl. Group2. and Group? only
- Groupl. Group?, and Group4 only
- Groupl. Group2, Group?. Group4. and Group?

You can add Groups to **[answer choice]**

- Groupl only
- Group? only
- Group! and Group? only
- Group!. Group?, and Group4 only
- [1] Group!. Groups Group?, and Group-I

Answer

Explanation:

You can add a Microsoft Entra cloud user to: Group1, Group3, and Group4 only Group1: Microsoft 365 group with assigned membership type and security enabled. Group3: Security group with assigned membership type and security enabled. Group4: Security group with dynamic membership type and security enabled. Group2 is not security enabled, so it cannot have security-related tasks assigned.

Group5 is sourced from Windows Server AD, which may limit direct cloud user additions. You can add Group5 to: Group1, Group2, Group3, and Group4

Group5 can be added to other groups regardless of the membership type or source, as long as those groups (Group1, Group2, Group3, and Group4) are security-enabled and support such additions.

Question: 431

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and Microsoft Intune.

All devices run Windows 11 and are Microsoft Entra joined.

You are alerted to a zero-day attack.

You need to identify which devices were affected by the attack and send a request to Intune administrators to update the affected devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Incidents & alerts, select the latest incident.
B. From Vulnerability management, open the security recommendation.
C. Select the affected devices and request remediation.
D. From Threat analytics, view the list of vulnerable devices.

Answer: C,D

Explanation:

Question: 432

Your company has a Microsoft Entra tenant named contoso.com and a Microsoft 365 subscription. All users use Windows 10 devices to access Microsoft 365 apps. All the devices are in a workgroup.

You plan to implement passwordless sign-in to contoso.com.

You need to recommend changes to the infrastructure for the planned implementation. What should you include in the recommendation?

A. Deploy the Microsoft Entra Connect provisioning agent.
B. Join all the devices to contoso.com.
C. Deploy Microsoft Entra Application Proxy.
D. Deploy the Microsoft Authenticate app.

Answer: D

Explanation:

Question: 433

You have a Microsoft 365 subscription.

You need to be notified to your personal email address when a Microsoft Exchange Online service issue occurs. What should you do?

A. From the Microsoft 365 admin center, customize the Service health settings.
B. From the Microsoft Outlook client configure an Inbox rule.
C. From the Microsoft 365 admin center, update the technical contact details.
D. From the Exchange admin center, create a contact.

Answer: A

Explanation:

Question: 434

HOTSPOT

You have a Microsoft 365 E5 subscription.

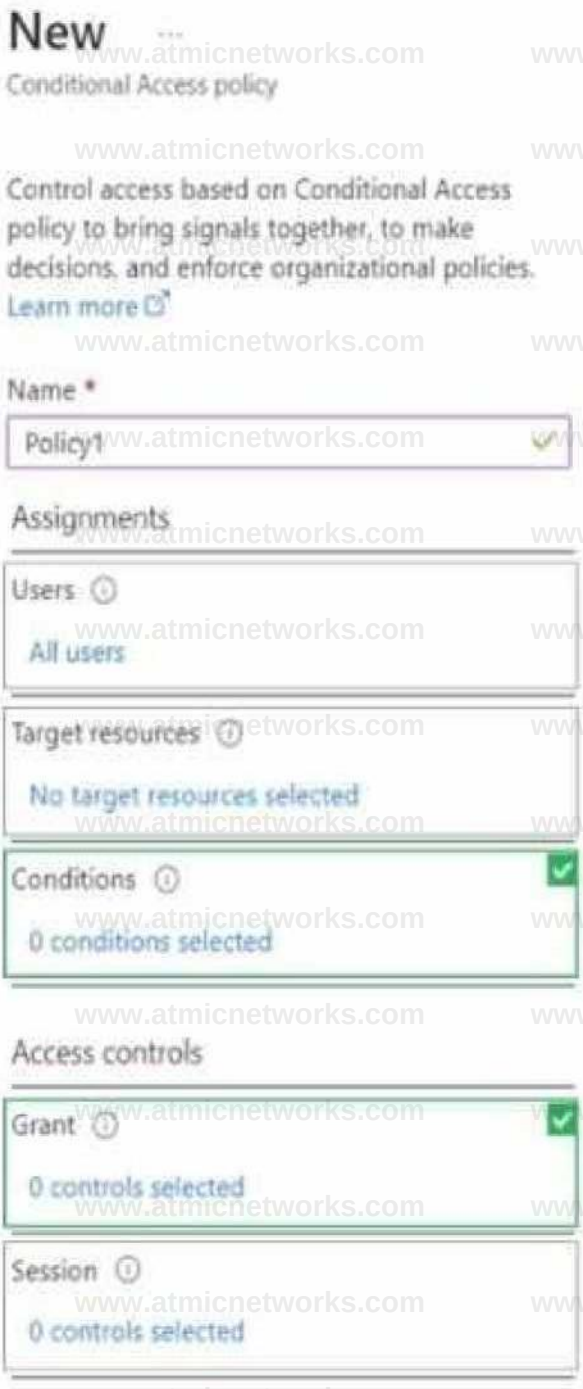
You need to create a Conditional Access policy named Policy that meets the following requirements:

- Applies to high-risk users
- Requires multifactor authentication (MFA)

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

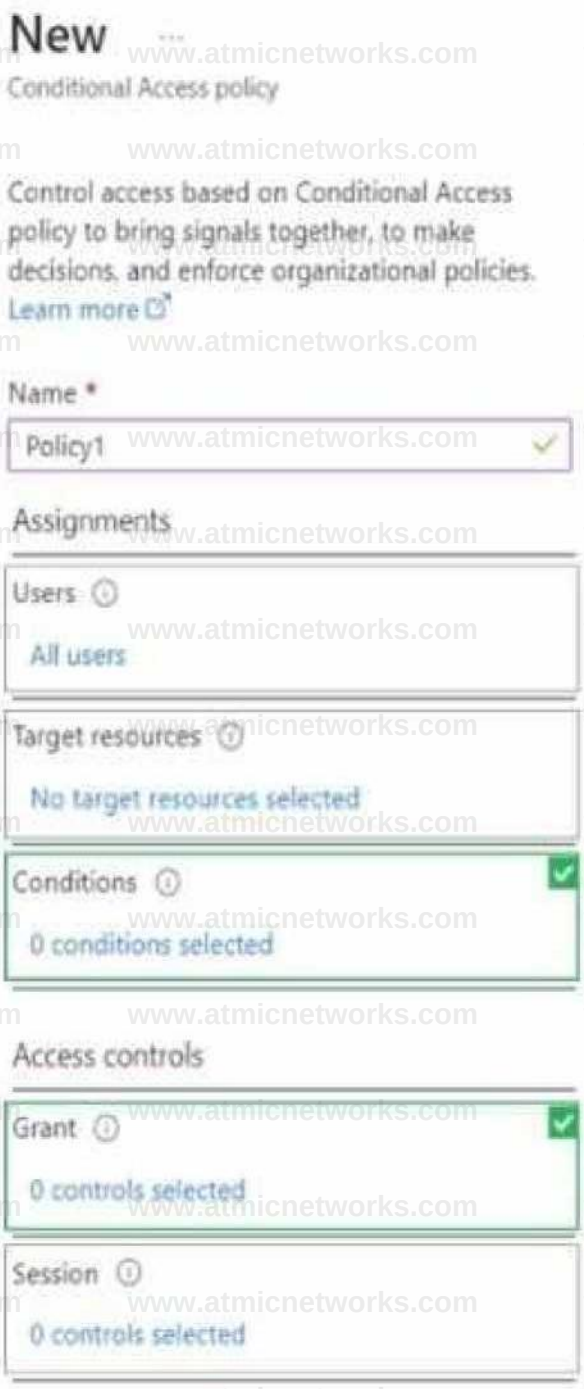
Answer Area



Answer

Explanation:

Answer Area



Question: 435

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to create a Conditional Access policy named Policy.

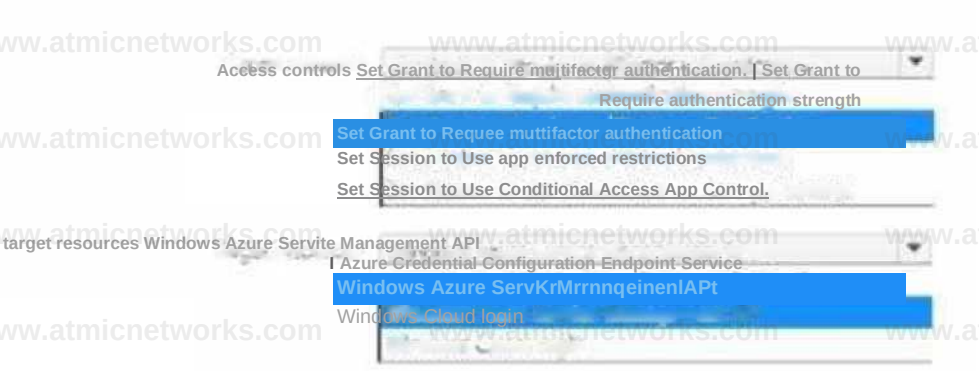
You need to ensure that only Passwordless MFA authentication methods are used when

administrators attempt to access the Azure portal. Azure PowerShell. or Azure CommandLine Interlace (CU).

How should you configure Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Question: 436

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Endpoint. The subscription contains the devices shown in

NARK	Plttfann
Devicel	Windows 11
Devices	Android
Devices	Lihux

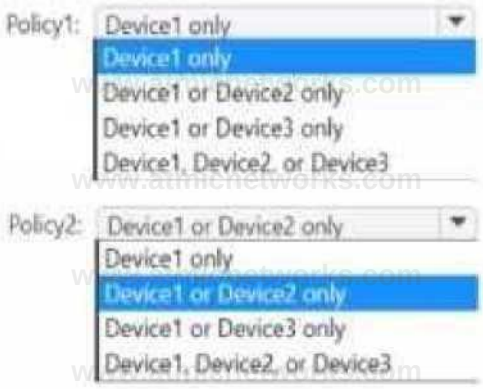
You need to create the Endpoint security policies shown in the following table.

Name	IETF itr
Pblcyl	M crosoft Defender Antivirus
Policy^	Crevice Control

To which device can you apply each policy? To answer, select the appropriate options in the

answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Policyl: Devicel only

Policy? Devicel or Device? only

Question: 437

You have a Microsoft 365 subscription.

All uses are assigned Microsoft 365 Apps for enterprise licenses.

You need to ensure that reports display the names of users that have activated Microsoft 365 apps and on how many devices. What should you modify in the Microsoft 365 admin center? A. Organization information

B. Org settings for Privacy profile

C. Org settings for Reports

D. the Reports reader role

Answer: C

Explanation:

Question: 438

You have a Microsoft 365 E5 subscription. You need to create a mail-enabled contact. Which portal should you use?

A. the Microsoft Entra admin center
B. the Intune admin center
C. the Microsoft Purview compliance portal
D. the Exchange admin center

Answer: D

Explanation:

Question: 439

You have a Microsoft 365 IS subscription and use Microsoft Defender for Cloud Apps. You register a cloud app named App1 in Microsoft Entra 10. You need to create an access policy for Appl. What should you do first?

A. Configure an app connector to Defender for Cloud Apps.
B. Add a security Information and event management (SlEM) agent to Defender for Cloud Apps.
C. Create an app tag for App1.
D. Deploy Conditional Access AppControl toApp1.

Answer: C

Explanation:

Question: 440

You have a Microsoft 365 ES subscription that contains a domain named contoso.com

You deploy a new Microsoft Defender (or Office 365 anti-phishing policy named Policy1 that has user impersonation protection enabled for a user named user1@contoso.com.

You discover that Policy1 blocks email messages from a regular contact named usei1@fabnkam.com.

You need to ensure that the messages are delivered successfully

What should you do for Policy1?

A. Select Enable mailbox intelligence
B. Select Enable domains to protect.
C. Configure the Phishing email threshold setting.
D. Configure which users to protect.

Answer: A

Explanation:

Question: 441

HOTSPOT

You have a Microsoft 365 ES subscription that contains the use's shown in the following table.

Name	Rott
Adrrinl	Global Administ idler
AdminS	Security Administ'ata'
AdminS	Security Operates
Admiral	Security Reader
Ac mini	Application Administrator

You are implementing Microsoft Defender for Endpoint.

You need to enable role-based access control (RBAC) to restrict access to the Microsoft Defender portal.

Which users can enable RBAC, and which users will no longer have access to the Microsoft Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Aww ATM

Users that can enable RBAC Admin! and Admin? only •

lAdnvnl only

EHEEJESEB I Admin 1, Admin? and AdminS only lAdmint Admin? Admin} and Admin5 only

Users that will no longer have access to the Microsoft Defender portal Admin} and AdmnrA only *

AdmmS only

Admin4 and AdmmS only Admin}. AdminA and AdminS only

Answer:

Explanation:

Answer Area

Users that can enable RBAC Admin! and Admm2 only

Users that will no longer have access to the Microsoft Defender portal

Admin3 and Adm<n4 only

Question: 442

HOTSPOT

You have a Microsoft 365 subscription.

You integrate Microsoft Defender for Cloud Apps with Microsoft Defender for Endpoint.

You need to create a policy to block users from accessing discovered apps that have a risk score of 4 or lower.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App^ notching a# of (he following

Setoctaftar V

4* Add a Wttf 3

Apply io EMMHUOM report*

| trigger a policy mate* it all ma tollcw/'g occur on m<

Alerts

Governance actions

Answer:

Explanation:

Answer Area

App^ notching a# of (he following

Setoctaftar V

4* Add a Wttf 3

Apply io EMMHUOM report* ˅

| trigger a policy mate* it all ma tollcw/'g occur on m<

Alerts

Create an alert for each matching event with the policy's severity

Governance actions

Tag app as sanctioned
Tag app as unsanctioned
Tag app as monitored
Tag app with custom tag

Question: 443

HOTSPOT

You have a Microsoft 36S E5 subscription.

You connect a cloud app that contains a group named Group1 to Microsoft Defender tor Cloud Apps.

You need to configure the Cloud apps settings to monitor all activities performed by the members of Group1.

Which two settings should you configure? to answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Question: 444

HOTSPOT

You have a Microsoft 36S E5 subscription.

You have devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Platform
Devicel	Windows 11
Computer?	**Windows 11**
Device?	Android

You create the device groups shown in the following table.

Rink	Na™	Matching rule
1	Group!	NJM Starts with Qw
2	Groups	OS In Window! 11
Ldlt	Ungrcuped device dshjh	Atof ti^6caW?

IP address indicators are defined as shown in the following table.

IP address	Action	Scope
131.107.10.50	Block	Group2
20.30.40.50	Block	Group1
2.23.10.15	Block	UnassignedGroup

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

NOTE: Each correct selection is worth one point

Answer Awa

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20304050 hom Devtcel.	O	O
Defender for Endpoint Modes access to IP address 221101$ from Computer2.	O	O
Defender for Endpoint blocks access to IP address 131.107.1050 from Dev>ce3.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Defender foi Endpoint blocks access to IP address 7O.3O.4O.SO from Devicel		
Defender for Endpoint blocks access to IP address 221101$ from Computer!	O	*
Defender for Endpoint blocks access to IP address 131 107.1050 from Devrees	O	*

Question: 445

You have a Microsoft 365 IS subscription and use Microsoft Defender for Cloud Apps.

From Policy management you open Information protection as shown in the following exhibit.

Which type of policy can you create?

A. file policy
B. access policy
C. activity policy
D. OAuth app policy
E. session policy

Answer: A

Explanation:

Question: 446

You have a Microsoft 365 is subscription that includes Microsoft Intune.

You manage all iOS devices by using Intune.

You plan to protect corporate-owned iOS devices by using Microsoft Defender for Endpoint.

You configure a connection between Intune and Defender for Endpoint.

You need to onboard the devices to Defender for Endpoint.

What should you do?

A. Enable Microsoft Defender for Cloud.
B. Create an app protection policy.
C. Download an onboarding package.
D. Add an app to Intune.

Answer: B

Explanation:

Question: 447

You have a Microsoft 365 ES subscription.

You integrate Microsoft Defender for Endpoint with Microsoft Intune.

You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled In Intune.

Solution: You create an endpoint detection and response (EDR) policy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 448

You have a Microsoft J65 E5 subscription.

You integrate Microsoft Defender for Endpoint with Microsoft Intune.

You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled in Intune.

Solution: You enable co-management.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 449

You have a Microsoft J65 E5 subscription.

You integrate Microsoft Defender for Endpoint with Microsoft Intune.

You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled in Intune.

Solution: You configure a device configuration profile.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 450

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to a Microsoft Entra tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

User2 fails to authenticate to the Microsoft Entra tenant when signing in as usef2@fabfikam.com

You need to ensure that User2 can access the resources in Microsoft Entra ID.

Solution: From the Microsoft Entra admin center, you add <abrlkam.com as a custom domain You insttud User2 to sign in as user2@fabrikam.com

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 451

You have a Microsoft 365 E5 subscription.

You create the users shown in the following table.

Name	Assigned role
Admin1	Security
Admin2	Security Operator

AdminS	Security Reader

You plan to use Microsoft Entra ID Protection.
Which users will be added automatically to the Users at risk detected alerts list?

A. Admin1 only
B. Admin2 only
C. Admin1 and Admin2 only
D. Admin1 and Admin3 only
E. Admin1, Admin2, and Admin3

Answer: D

Explanation:

Question: 452

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

You need to sync the domain with the subscription. The solution must meet the following requirements:

- On-premises Active Directory password complexity policies must be enforced.
- Users must be able to use Microsoft Entra Self-Service Password Reset (SSPR).

What should you use?

A. Microsoft Entra ID Protection
B. Microsoft Entra Seamless Single Sign-On (Microsoft Entra Seamless SSO)
C. pass-through authentication
D. password hash synchronization

Answer: C

Explanation:

Question: 453

Your company has three main offices and one branch office. The branch office is used for research.

The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.
You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.
What should you include in the recommendation?

A. Microsoft Entra conditional access
B. a Microsoft Intune device compliance policy
C. a Microsoft Intune device configuration profile

D. Microsoft Entra password protection

Answer: A

Explanation:

Question: 454

Youi network contains an Active Directory domain.

You have a Microsoft Entra tenant that has Security defaults disabled.

Microsoft Entra Connect Sync is configured for directory synchronization. Password hash synchronization and pass-through authentication are disabled.

You need to enable Microsoft Entra ID Protection to detect leaked credentials.

What should you do first?

A. From Microsoft Entra Connect, enable password hash synchronization.

B. From the Microsoft Entra admin center, enable Security defaults.

C. From Microsoft Entra Connect, enable pass-through authentication.

D. From the Microsoft Entra admin center, configure verifiable credentials.

Answer: A

Explanation:

Question: 455

You have a Microsoft 365 E5 subscription that contains a user named User1. You create an anti-phishing policy named Policy! that has the following settings:

- Include these users, groups and domains: User1
- Phishing email threshold: 3 - More Aggressive

User1 receives the email messages shown in the following table.

Name	Phishing confidence level <PCQ
Maili	low
Mail?	**Medium**
Maiti	High
MaiM	Very high

Which messages are phishing email?

A. Mail4 only
B. Mail3 and Mail4 only
C. Mail2, Mail3, and Mail4 only
D. Mail1, Mail2, Mail3, and Mail4

Answer: B

Explanation:

Question: 456

You have a Microsoft 365 E5 subscription. You create a data loss prevention (DLP) policy named DLP1.

You need to ensure that endpoint rule actions are available in the advanced DLP rules for DLP1. To which location should you apply DLP1?

A. Instances
B. Devices
C. OneDrive accounts
D. On-premises repositories

Answer: B

Explanation:

Question: 457

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Endpoint Defender for Endpoint has tamper protection enabled.

You have a device named Device1 that is onboarded to Defender for Endpoint. You need to configure antivirus and real-time protection for Device1.

What should you do in the Microsoft Defender portal?

A. Enable troubleshooting mode.
B. Initiate a live response session.
C. Isolate Device1.
D. Create a device group.

Answer: A

Explanation:

Question: 458

You have a Microsoft 365 E5 subscription. Administrators are issued FID02 security keys.

You need to create a Conditional Access policy that will use a FID02 security key as an authentication method. Which Access controls option should you select for the policy? A. Require token protection for sign-in sessions

B. Require approved client app

C. Require authentication strength

D. Require multifactor authentication

Answer: C

Explanation:

Question: 459

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Endpoint. The subscription contains Windows 11 devices.

You need to create a policy to restrict users from accessing the Device security settings and the Account protection settings in Windows Defender Security Center on the devices.

Which type of policy should you create, and which template should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Policy type: Endpoint security policy

Question: 460

You have a Microsoft 365 E5 subscription.

You plan to create an anti-malware policy named Policy1.

You need to ensure that Policy1 can detect malicious email messages that were already delivered to a user's mailbox.

What should you do in the Microsoft Defender portal?

A. Enable zero-hour auto purge (ZAP).

B. Modify the common attachments filter.

C. Configure a quarantine policy.

D. Enable enhanced filtering.

Answer: A

Explanation:

Question: 461

You have a Microsoft 365 E5 subscription that contains devices onboarded to Microsoft Defender for Endpoint. You integrate Microsoft Defender for Cloud Apps with Defender for Endpoint. You need identify which cloud apps and services were used most during the last 30 days What should you do?

A. Generate a Cloud Discovery snapshot report.

B. Generate a monthly security summary report

C. Create a threat analytics alert notification.

D. Generate a Cloud Discovery executive report

Answer: B

Explanation:

Question: 462

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps. You need to create a file policy named Policy1 that meets the following requirements:

• Inspects files in connected software as a service (SaaS) apps

* Inspects protected files

Which two settings should you configure? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Information Protection

- Admin quarantine
- Microsoft Information Protection ✓
- Azure security
- Files ✓

Conditional Access App Control

- General Settings
- User monitoring
- Device identification
- App onboarding/maintenance
- Edge for Business protection

App governance

- Service status

Answer:

Explanation:

Answer Area

Question: 463

You have a Microsoft 365 E5 subscription.

You need to use Microsoft Defender for Cloud Apps to monitor user mailbox activities. What should you do?

A. Create an activity policy.
B. Enable mailbox audit logging.
C. Create an app connector for Microsoft 365.
D. Create an access policy.

Answer: B

Explanation:

Question: 464

You have a Microsoft 365 E5 subscription.

You integrate Microsoft Defender for Endpoint with Microsoft Intune.

You need to ensure that devices automatically onboard to Defender for Endpoint when they are enrolled in Intune.

Solution: You create a compliance policy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 465

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two security groups named Group1 and Group2.

You need to enable multi-factor authentication (MFA) for the members of Group1 and Group2. The solution must meet the following requirements:

- The Group1 members must be prompted for MFA only when authenticating to Microsoft Entra ID from Android devices.
- The Group2 members must be prompted for MFA only when accessing Microsoft Exchange Online from outside the corporate network.
- Administrative effort must be minimized.

What should you configure for each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Groupl: Conditional Access

Group2 Conditional Access

Question: 466

You have a Microsoft 365 E5 subscription.

You plan to ingest syslog data from a supported firewall device to Microsoft Defender for Cloud Apps.

You need to configure automatic log upload.

Which two components should you configure for the log collector? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a connection string

B. the receiver type

C. the data source

D. the username and password

E. the host IP address or FQDN

Answer: C,E

Explanation:

Question: 467

You have a Microsoft 365 E5 subscription. The subscription contains a Microsoft SharePoint Online site named Site1. Site1 contains the following files:

- File.docx
- ImportantFile.docx
- Filejmportant.docx

From Microsoft Defender Cloud Apps, you create a file policy named Policy1 that has the filter shown in the following exhibit.

To which files will Policy1 apply?

A. File.docx, ImportantFile.docx, and Filejmportant.docx
B. Filejmportant.docx only
C. ImportantFile.docx and Filejmportant.docx only
D. File.docx only
E. ImportantFile.docx only

Answer: B

Explanation:

Question: 468

You have a Microsoft 365 E5 subscription that contains a user named User1.

You create an outbound anti-spam policy named Policy1 as shown in the following exhibit.

Protection settings

Set your outbound Mi spam settings tex this policy.

Mt^yf limits

Set in external message limn

10

Sei an Internal message limit

20

Set a dally message limit 1000

Restriction placed on users who reach the message limit Restrict the user from sending mail until the following day ■

Forwarding rules

Automatic forwarding rules

Automatic - System con trolled

Notifications

I Sena a copy of suspicious outbound messages or message that exceed these hmm to these users and groups

Notify These users end grctjps rl a WCfr g blocked due to

You assign Policy1 to User1.

What is the maximum number of email messages that User1 can send in a 24-hour period?

A. 30

B. 720

C. 1000

D. 1030

Answer: B

Explanation:

Question: 469

You have a Microsoft 365 subscription that uses Microsoft Defender XDR

From Automatic remediation in the Microsoft Defender portal, you set Automation level to Semi - require approval for non-temp folders for the endpoints.

You need to identify the impact of the Automation level setting on the endpoints.

Which two actions will occur based on the remediation settings? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Devices will be remediated automatically if a threat is detected in the \windows\ folder.

B. Devices will be remediated automatically if a threat is detected in the \program files (X86) \" folder.

C. Devices will be remediated automatically if a threat is detected in the \users\"\downloads\" folder.

D. Devices will be remediated only after end-user approval.

Answer: A,B

Explanation:

Question: 470

You have a Microsoft 365 subscription that includes Microsoft Defender XDR.

From the Microsoft Defender portal, you review the Microsoft Secure Score improvement actions shown in the following table.

Recommended action	Status	Points achieved
Enable Conditional Access policies to block legacy authentication	To address	0/9
Ensure user consent to apps accessing company data on their behalf is not allowed	To address	0/4
Create an app discovery policy to identify new and trending cloud apps in your org	To address	0/3

You plan to update the status of the improvement actions as shown in the following table.

Recommended action	Status
Enable Conditional Access policies to block legacy authentication	Risk accepted
Ensure user consent to apps accessing company data on their behalf is not allowed	Resolved through third party
Create an app discovery policy to identify new and trending cloud apps in your org	Planned

How many points will the Secure Score increase after the update?

A. 0
B. 4
C. 7
D. 13
E. 16

Answer: C

Explanation:

Question: 471

You have a Microsoft 365 E5 subscription.

You plan to configure multi-factor authentication (MFA).

You need to select an authentication method for users. The solution must ensure that each time a user is prompted for MFA, the application name that requires MFA is provided.

What should you select?

A. Microsoft Authenticator
B. a FID02 security key
C. a voice call
D. SMS
E. email OTP

Answer: A

Explanation:

Question: 472

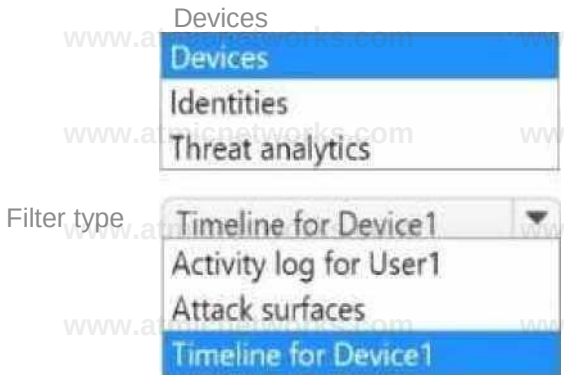
HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1. User1 has a Windows 11 device named Device1 that is onboarded to Microsoft Defender for Endpoint. User1 reports that various files were deleted from Device1.

You need to create a filter to identify which service deleted the files.

Which settings should you configure, and which type of filter should you create in the Microsoft Defender portal? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Settings:

Answer:

Explanation:

Answer Area

Question: 473

You have a Microsoft 365 subscription that contains more than 2,000 guest users.

You need to ensure that when guest users are added to Microsoft 365 groups in the subscription, their membership is validated by the group owner every 30 days. What should you configure?

A. access reviews
B. Conditional Access policies
C. retention policies
D. group expiration policies

Answer: A

Explanation:

Question: 474

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Office 365.

You need to implement a threat policy that will apply a balanced baseline protection profile to protect against spam, phishing, and malware.

Solution: You create a Strict preset security policy.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 475

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Office 365.

You need to implement a threat policy that will apply a balanced baseline protection profile to protect against spam, phishing, and malware.

Solution: You create an anti-malware policy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 476

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Office 365.

You need to implement a threat policy that will apply a balanced baseline protection profile to protect against spam, phishing, and malware.

Solution: You create an anti-phishing policy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 477

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Role assignments allowed	Security enabled
Group1	Security	No	Yes
Group2	Microsoft 365	Yes	No
Group3	Distribution	*Not applicable*	*Not applicable*

You plan to create 10 new users and configure group-based licensing to assign each user a Microsoft 365 E5 license.

To which group should you add the users, and which portal should you use to assign the license? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Group: Group2 ᵀI Group1

Group?
'Grcup3]

Portal: The Mkrosoft 365 admin center The
Microsoft 365 admin center The
Microsoft Entra admin center
The Microsoft Purview compliance portal

Answer:

Explanation:

Answer Area

Group: Group2 ▼

Portal: The Mkrosoft 365 admin center

Question: 478

You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:

- Windows 11
- Android
- iOS

To which devices can you apply Endpoint DLP policies?

A. Windows 11 only
B. Windows 11 and Android only
C. Windows 11 and iOS only
D. Windows 11, Android, and iOS

Answer: A

Explanation:

Question: 479

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to use Microsoft Graph PowerShell to assign a Microsoft 365 E5 license to a new user named user1 @contoso.com.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Question: 480

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.

You have a cloud app named App1.

You need to implement a security solution for App1 that meets the following requirements:

- Enables the real-time monitoring of user activities
- Blocks specific activities as needed

What should you include in the solution for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Enables the real-time monitoring of user activities: Conditional Access App Control

Conditional Access App Control
Microsoft Purview Information Protection
Score metrics

Blocks specific activities as needed: A session policy
A file policy

A session policy
An access policy

Answer:

Explanation:

Answer Area

Enables the real-time monitoring of user activities: Conditional Access App Control

Blocks specific activities as needed: A session policy

Question: 481

HOTSPOT

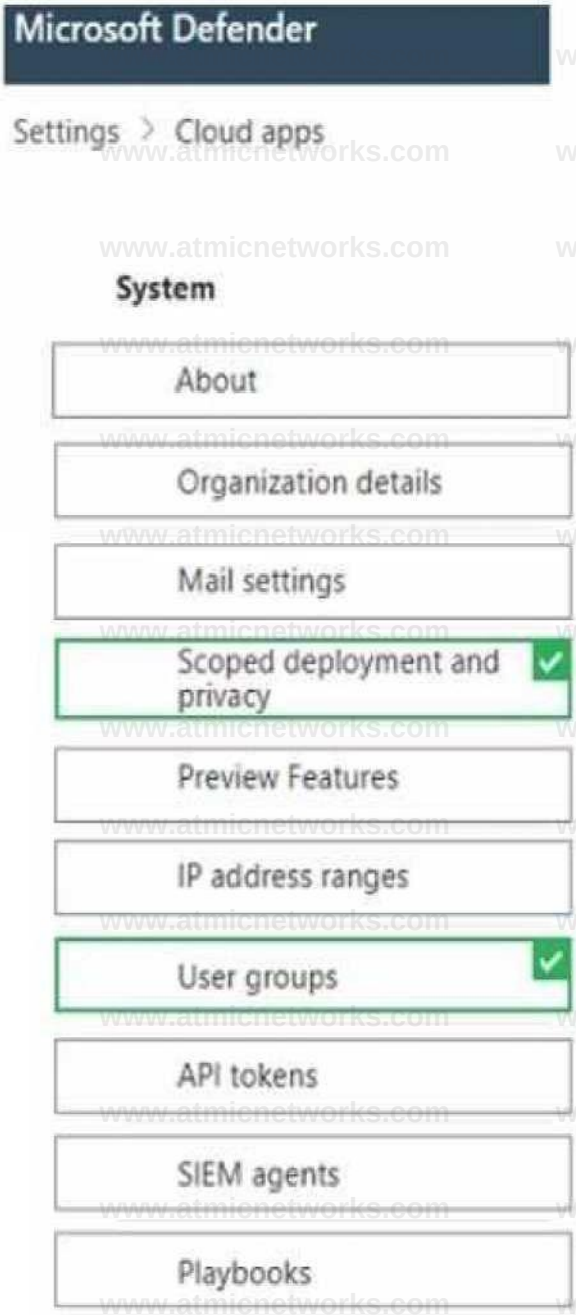
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.

User1 reports that after sending 1.000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:

- Which administrators can unblock User1
- What to configure to allow User1 to send at least 2.000 emails per day without being blocked

What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

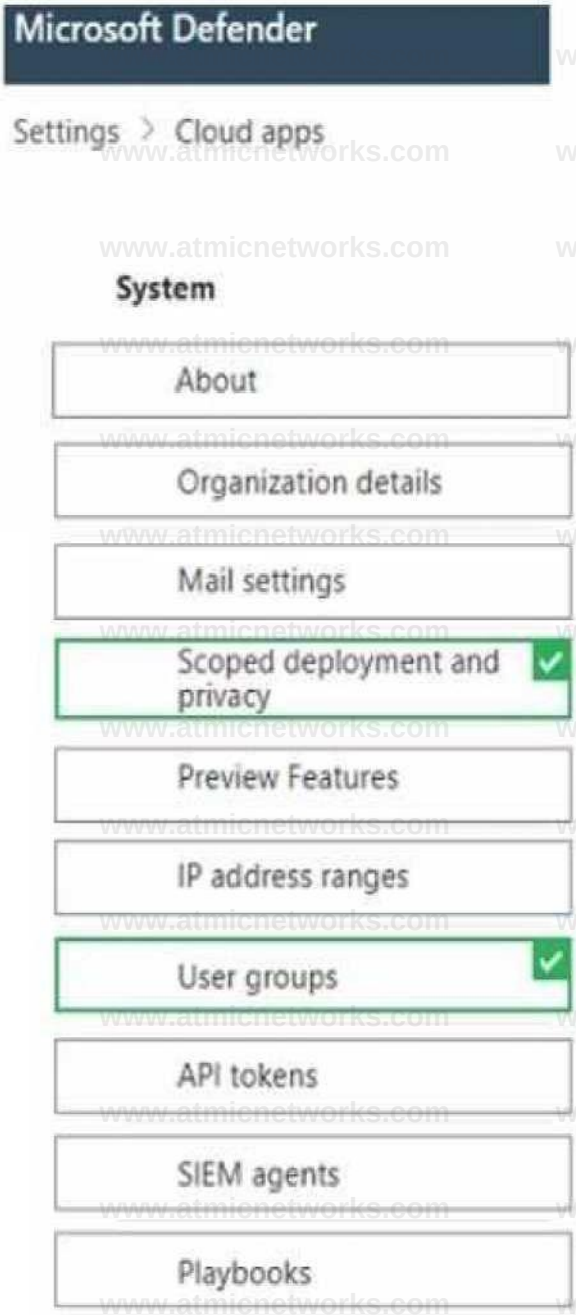
Answer Area



Answer:

Explanation:

Answer Area



C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg

Question: 482

You have a Microsoft 365 E5 subscription and use Microsoft Purview. The subscription contains the devices shown in the following table.

Name	Platform
Device!	Windows 11
DeviceZ	macOS

Devices	Android
Device4	Linux

All the devices are onboarded to Microsoft Defender for Endpoint. You plan to deploy Endpoint data loss prevention (Endpoint DLP) policies. Which devices can be protected by using the DLP policies?

A. Device1 only
B. Device1 and Device2 only
C. Device1, Device2, and Device 3 only
D. Device1, Device3, and Device 4 only
E. Device1, Device2, Device3, and Device4

Answer: B

Explanation:

Question: 483

You have a Microsoft 365 subscription and use Microsoft Defender for Office 365.

You need to recommend a solution to educate users on topics that relate to social engineering risks. The users must receive a weekly reminder to complete a learning task.

What should you use in the Microsoft Defender portal?

A. Campaigns
B. Attack simulation training
C. Threat tracker
D. Learning hub

Answer: B

Explanation:

Question: 484

You have a Microsoft 365 E5 subscription that contains Windows 11 devices. All the devices are onboarded to Microsoft Defender for Endpoint.

You need to compare the configuration of the devices against industry standard benchmarks. What should you use?

A. Events

B. Initiatives

C. Attack surface map

D. Security baselines assessment

Answer: D

Explanation:

Question: 485

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named Admin1.

Your company deploys a new branch office named Branch!

You need to provide Admin1 with the ability to manage Branch1. The solution must meet the following requirements:

- Admin1 must only be able to manage users that have Office location set to Branch1.
- Admin1 must be able to reset passwords, manage user licenses, and modify user attributes only for the users in Branch1.

What should you use to organize the Branch1 users, and which role should you assign to Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use: An administrative unit

A Microsoft 365 group A security group

An administrative unit

Role: User Administrator

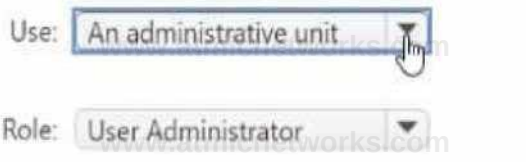
Help Desk Administrator

Password Administrator

Answer:

Explanation:

Answer Area



Question: 486

HOTSPOT

You have a hybrid deployment of Microsoft Entra that contains the users shown in the following table.

Name	Description
Useri	On-premises directory synchronization service account
User2	Contributor for Microsoft Entra Connect Health
User3	Application Administrator in Microsoft Entra ID

You need to identify which users can perform the following tasks:

- View sync errors in Microsoft Entra Connect Health.
- Configure Microsoft Entra Connect Health settings.

Which user should you identify for each task? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

View sync errors in Microsoft Entra Connect Health: User2

Useri

User3

Configure Microsoft Entra Connect Health settings: Useri

Useri

User2

User3

Answer:

Explanation:

Answer Area

View sync errors in Microsoft Entra Connect Health: User2

Configure Microsoft Entra Connect Health settings: Useri

Question: 487

HOTSPOT

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Per-user multifactor authentication status
Userl	Groupl	Disabled
User2	Group!	Enforced

Per-user multifactor authentication is configured to use 131.107.5.0/24 as trusted IPs.
The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location!	131 107.20.0/24	
Location?	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:

- Users: All users
- Target resources assignment: App1
- Conditions: Include all trusted locations
- Grant access: Require multi-factor authentication

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

Statements	Yes	No
When Userl connects to App1 from a device that has an IP address of 131.107.50.10, Userl must use MFA.	O	O
When User2 connects to App1 from a device that has an IP address of 131 10720 15, User2 must use MFA.	O	O
When User2 connects to App1 from a device that has an IP address of 131 107.5.5, User2 must use MFA.	O	O

Answer:

Explanation:
Answer Area

Statements	Yes	No
When Userl connects to App1 from a device that has an IP address of 131.107.50.10, Userl must use MFA.	®	O
When User2 connects to App1 from a device that has an IP address of 131 10720 15, User2 must use MFA.	®	O

When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.

Question: 488

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps. The subscription contains users that have Windows 11 devices.

You need to use the Cloud Discovery snapshot report to analyze cloud app usage on the devices. What should you do before generating a report?

A. Create an activity policy.
B. Deploy the Azure Monitor Agent on the devices.
C. Create an app discovery policy.
D. Export traffic logs from firewalls and proxies.

Answer: D

Explanation:

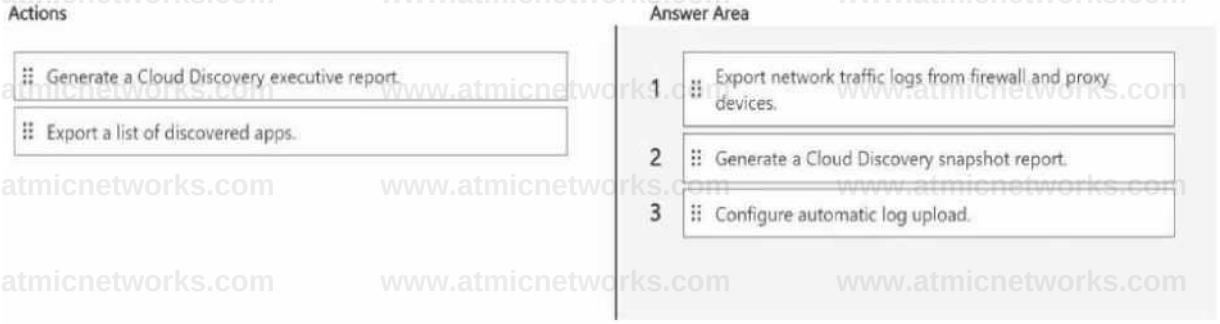
Question: 489

DRAG DROP

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.
You need to configure Cloud Discovery to generate a report that identifies top potential risks and provides a workflow to mitigate and manage the risks.
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.

Answer:

Explanation:



Question: 490

You have a Microsoft 365 E5 subscription that contains a user named User1.

User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

A. the Microsoft Defender portal
B. the Exchange admin center
C. the Microsoft 365 admin center
D. the Microsoft Purview portal
E. the Microsoft Entra admin center

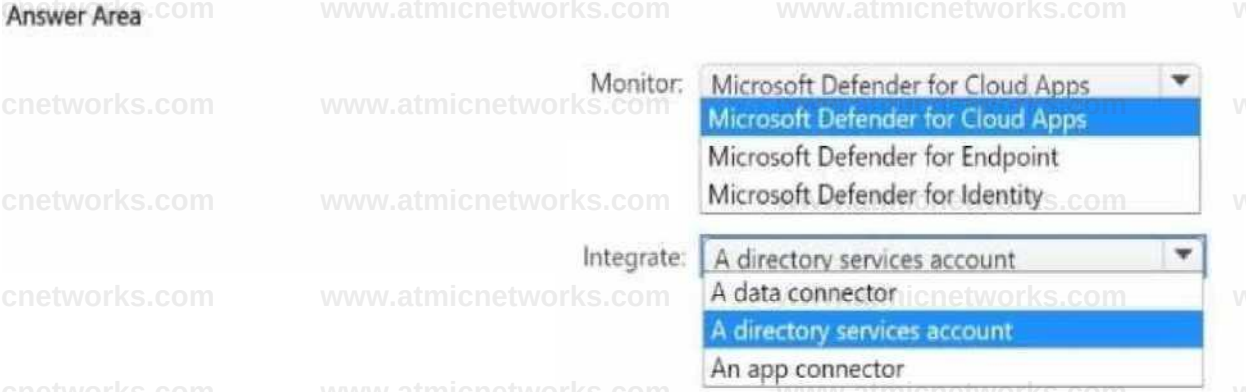
Answer: D

Explanation:

Question: 491

HOTSPOT

You have an Azure subscription and a Microsoft 365 E5 subscription.
You are licensed to use Microsoft Defender XDR
You need to monitor activities from suspicious IP addresses and unusual administrative activities in Azure.
What should you use to monitor the activities, and what should you use to integrate Azure with Microsoft Defender XDR? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area

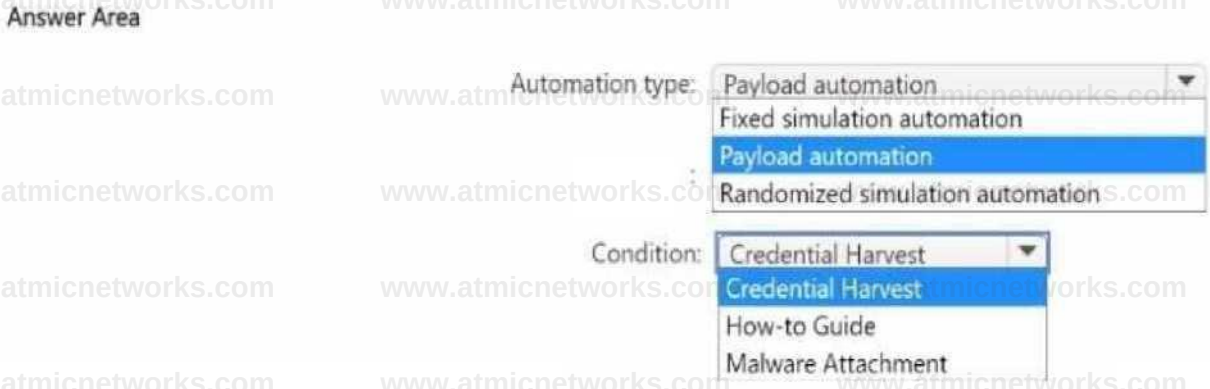
Monitor: Microsoft Defender for Cloud Apps

Integrate A directory services account

Question: 492

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
You need to automate Attack simulation training for users when a phishing campaign is detected in real-time.
Which type of automation should you use. and which condition should you configure for the Attack simulation training? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area

Automation type: Payload automation

Condition: Credential Harvest

Question: 493

You have a Microsoft 365 E5 subscription. The subscription contains users that have Windows 11 devices.

You plan to onboard the devices to Microsoft Defender for Endpoint. The devices will connect to Defender for Endpoint through a proxy service.
You need to ensure that the devices use consolidated URLs and static IP ranges when connecting to Defender for Endpoint. What should you do?

A. Enable device discovery.
B. Use the streamlined connectivity type.
C. Use the standard connectivity type.
D. Configure a device group.

Answer: B

Explanation:

Question: 494

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.
You have the documents shown in the following table.

Name	Number of credit card numbers in the document	Number of SWIFT codes in the document	Stored on
Documentl	3	3	Sitel
Document2	7	2	Site2
Documents	15	0	Sitel

You DLP1 that has the advanced DLP rule as shown in the exhibit. (Click the Exhibit tab.)
You apply DLP1 to Site1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
DLP1 applies to Document!	o	O
DLP1 applies to Document?.	0	o
DLP1 applies to Documents		

Answ

Explanation:

Answer Area

Statements	Yes	N
DLP1 applies to Document!.	O	•
DLP1 applies to Document?.	0	•
DLP1 applies to Documents	0	®

Question: 495

You have a Microsoft 365 E5 subscription. You plan to use Microsoft Entra ID Protection.

You need to ensure that account passwords must be changed if account credential. What should you configure?

A. Password protection
B. self-service password reset (SSPR)
C. a sign-in risk policy
D. a user risk policy

Answer: D

Explanation:

Question: 496

Your company has offices in Seattle and Denver.

You have a Microsoft 365 subscription.

You plan to create a Conditional Access policy named Policy1 that will enforce multifactor

authentication (MFA).

You need to ensure that users at the Seattle office are excluded from MFA. Users at the Denver office must always be prompted for MFA.

What should you configure for Policy1?

A. Authentication strengths

B. a named location that has IP ranges location set to the Seattle office

C. a named location that has Countries location set to United States

D. VPN connectivity from the Seattle office

Answer: B

Explanation:

Question: 497

You have a Microsoft 365 E5 subscription that contains the identities shown in the following table:

Name	Type
User1	User
Group1	Microsoft 365 group
Group2	Mail-enabled security group
Group3	Distribution group

You create a shared mailbox named Shared1.

Which identities can you add to Shared1 as a member?

A. User1 only

B. User1 and Group1 only

C. User1 and Group2 only

D. User1 and Group3 only

E. User1, Group2, and Group3 only

Answer: C

Explanation:

Question: 498

Your network contains an Active Directory domain and a Microsoft Entra tenant.

The network uses a firewall that contains a list of allowed outbound domains.

You begin to implement directory synchronization, but it fails.

The firewall currently allows only:

- microsoft.com
- office.com

You need to ensure that directory synchronization completes successfully.

What is the best approach to achieve the goal?

A. From Microsoft Entra Connect, modify the Customize synchronization options task.

B. From the firewall, modify the list of allowed outbound domains.

C. From the firewall, allow the IP address range of the Azure data center for outbound communication.

D. Deploy a Microsoft Entra Connect Sync sync server in staging mode.

Answer: B

Explanation:

Question: 499

Your network contains an on-premises Active Directory domain. You have a Microsoft 365 subscription.

You implement a directory synchronization solution that uses pass-through authentication.

You configure Microsoft Entra Password protection as shown in the following exhibit.

You discover that Active Directory users can use the passwords in the custom banned passwords list.

You need to ensure that banned passwords are banned for all users.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From a domain controller, install the Microsoft Entra Application Proxy connector.

B. From Active Directory, modify the Default Domain Policy.

C. From a domain controller, install the Microsoft Entra Password Protection Proxy.

D. From Custom banned passwords, modify the Enforce custom list setting.

E. From all the domain controllers, install the Microsoft Entra Password Protection DC Agent.

F. From Password protection for Windows Server Active Directory, modify the Mode setting.

Answer: C, E, F

Explanation:

Question: 500

You have a Microsoft 365 E5 subscription that contains users in the United States, Europe, and Asia.

You use Microsoft Entra ID Protection.

You have a virtual desktop infrastructure (VDI). All VDI servers are located in the United States.

Users connect to Microsoft 365 from laptops and the VDI.

Some VDI users report that they are blocked from signing in to Microsoft 365 due to a high sign-in risk.

You need to reduce the likelihood that the VDI users will be erroneously blocked from signing in to Microsoft 365. The solution must ensure that sign-ins from the VDI environment are protected by using ID Protection.

A. ExpressRoute for Microsoft 365

B. A Conditional Access policy

C. A trusted location

D. A Satellite Geography location

Answer: C

Explanation:

Question: 501

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the objects shown in the following

table.

Name	Type	In organizational unit (OU)
Useri	User	0U1
User?	User	OU1
Groupl	Secunty Group -	OU1
User3	User	OU?

Answer Areo

Statements	Yes	No
User? will synchronize to the Microsoft Entra tenant	0 O	
Group? will synchronize to the Microsoft Entra tenant	O	1

User3 will synchronize to the Microsoft Entra tenant 0

O

Answer:

Explanation:

Answer Area

Statements	Yes	No
User2 will synchronize to the Microsoft Entra tenant	1	
Group? will synchronize to the Microsoft Entra tenant	•	
User3 will synchronize to the Microsoft Entra tenant	®	

Question: 502

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

From Microsoft Defender for Endpoint, you turn on the Allow or block file advanced feature.

You need to block users from downloading a file named File1.exe.

A. A suppression rule

B. An indicator

C. A device configuration profile

Answer: B

Explanation:

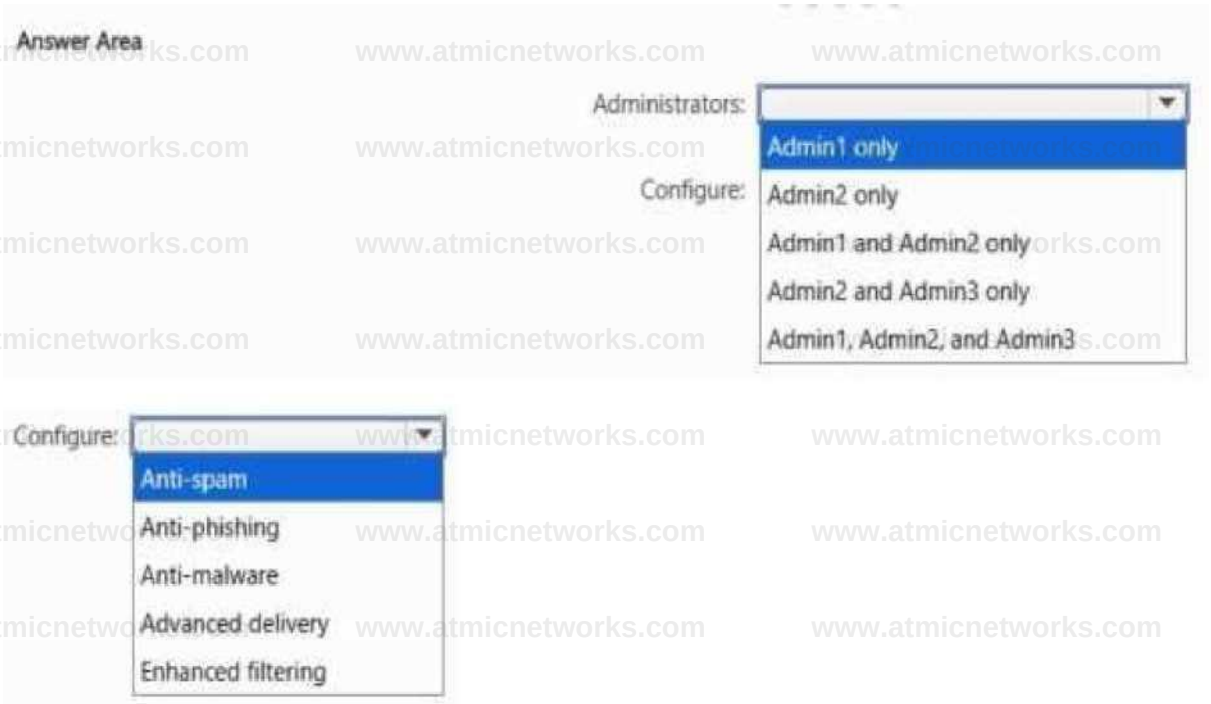
Question: 503

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.

Name	Role
Admin1	Exchange
Admin2	Security
Admin1	User Administrator

User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:



Answer:

Explanation:

Answer Area

Administrators Admin2 only

Configure Anti-spam

Question: 504

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You notice that it takes several days to notify email recipients when an incoming email message is marked as spam, and then quarantined.

You need to ensure that the email recipients are notified within 24 hours.

A. Modify the default inbound anti-spam policy.

B. Modify the global settings for quarantine policies.

C. Add a custom quarantine policy.

D. Modify the DefaultFullAccessPolicy quarantine policy.

Answer: B

Explanation:

Question: 505

You have a Microsoft 365 E5 subscription that contains a user named User1.

You have a Conditional Access policy applied to a cloud-based app named App1. App1 has Conditional Access App Control deployed.

You need to create a Microsoft Defender for Cloud Apps policy to block User1 from printing from App1.

A. Cloud Discovery anomaly detection policy

B. Session policy

C. Activity policy

D. OAuth app policy

Answer: B

Explanation:

Question: 506

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.

You plan to perform a security audit of all the apps detected by Cloud Discovery.

You need to track which apps were audited. The solution must ensure that the list of audited apps can be displayed in the cloud app catalog.

A. Apply a custom app tag to each app.

B. Generate a Cloud Discovery snapshot report.

C. Deploy Conditional Access App Control.

D. Define each app as a critical asset.

E. Enable app governance.

Answer: A

Explanation:

Question: 507

You use Microsoft Defender for Office 365.

You plan to automate an attack simulation campaign.

Any users that fail the simulation must take additional training based on the simulation results.

What is the maximum number of days the training will be available to the users after the simulation?

A. 7

B. 15

C. 30

D. 45

Answer: C

Explanation:

Question: 508

HOTSPOT

You have a Microsoft 365 E5 subscription.

The subscription contains users that have devices onboarded to Microsoft Defender for Endpoint. Defender for Endpoint is configured to forward signals to Microsoft Defender for Cloud Apps.

Cloud Discovery identifies a risky web app named App1.

You need to block users from connecting to App1 from Microsoft Edge. Users must be able to bypass the restriction.

Which type of app tag should you use, and what should you configure to integrate Defender for Endpoint with Defender for Cloud

Answer Area

App tag type: [

Monitored

Integrate by configuring:

Sanctioned

Unsanctioned

Answer:

Explanation:

Answer Area

App tag type: Unsanctioned

Integrate by configuring: Enforce app access

Question: 509

Your company has a Microsoft 365 E5 subscription.

You onboard a device on the company's network to Microsoft Defender for Endpoint.

In the Microsoft Defender portal, you notice that the device inventory displays many devices that have an Onboarding status of Can be onboarded.

You need to ensure that onboarded devices are prevented from polling the network for device discovery but can still discover devices with which they communicate directly.

What should you configure in the Microsoft Defender portal?

A. device discovery exclusions

B. standard discovery

C. basic discovery

D. a network assessment job

Answer: C

Explanation:

Question: 510

HOTSPOT

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

Name	Departmen	Job title
Userl	IT engineering	Technician
U$er2	Engineering	Senior
User3	Finance	Manager

You create a new administrative unit named AU1 and configure the following AU1 dynamic membership rule.

Answer ATM Statements Yes No

Ad mini can reset the password of Usefl.

Admin 1 can reset the password of User!

Admin2 can reset the password of User3.

Answer:

Explanation:

Answer Area

Statements	Yes	No
Adminl can reset the password of Usefl.	♦	
Adrian 1 can reset the password of User?.		O
Admin2 can reset the password of Usef3.	^	

Question: 511

You have a Microsoft 365 E5 subscription.

You create a new data loss prevention (DLP) policy named DLP1 that protects financial data from being shared by using Microsoft Teams messages. You apply DLP1 to the users in the finance department.

An incident is raised when a finance department user named User1 shares financial data in a Teams channel that includes external members.

When User1 uses Teams to send the same message in a 1:1 chat or a private channel, the message is blocked as expected.

You need to ensure that User1 is prevented from sharing financial data in Teams channels that include external members.

What should you do?

A. Edit the policy rules of DLP1.

B. Edit the settings of the team that contains the channel.

C. Modify the licenses assigned to User1.

D. Edit the Locations settings of DLP1.

Answer: A

Explanation:

Question: 512

HOTSPOT

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains a server named Server1 that runs Windows Server. The domain contains the users shown in the following table.

Name	DtstinguishedName	UserPrincipalNa	Email address
User	CN=Uset1,OU=Department1,DC=Contoso,DC=LOCA	user1@contoso.c	user1@contoso.c
User2	C N=User 2. OU - Team 1 .OU - Department?.DC -	user2@contoso	user? @co ntoso.
User]	C N=UserJ.OU=Departments DC=Contoso,	usef3@contosox	user3@contoso.c

You have a Microsoft 365 subscription that contains the following user accounts:

Answer Area

Statements	Yes	No
User! syncs with user l@contoso.com	O	0
User? syncs with user2@contO5O.com	O	0
User3 is created as a new user in Microsoft 365.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri syncs with user1@contoso.com	•	

User? syncs with user2@contcso.com.

User! is created as a new user in Microsoft 365.

Question: 513

You need to configure Microsoft Entra Connect Sync to support the planned changes for the Montreal Users and Seattle Users OUs.

What should you do?

A. From PowerShell, run the Add-ADSyncConnectorAttributeInclusion cmdlet.

B. From the Microsoft Entra Connect wizard, select Customize synchronization options.

C. From PowerShell, run the Start-ADSyncSyncCycle cmdlet.

D. From the Microsoft Entra Connect wizard, select Manage federation.

Answer: B

Explanation:

Question: 514

You have a Microsoft 365 subscription that uses a third-party multifactor authentication (MFA) product.

While reviewing Microsoft Secure Score, you discover that there are no points listed for the Ensure multifactor authentication is enabled for all users recommendation.

You need to ensure that you receive all the points for the recommendation. The solution must minimize administrative effort.

What should you do?

A. Configure a data connector.

B. Modify the recommendation tags.

C. Deploy a Microsoft Defender for Identity sensor.

D. Modify the status of the recommendation.

Answer: D

Explanation:

Question: 515

You have a Microsoft 365 E5 subscription.

You need to assign a Microsoft Defender for Endpoint baseline.

Which portal should you use?

A. the Microsoft 365 admin center

B. the Microsoft Purview portal

C. the Microsoft Defender portal

D. the Microsoft Intune admin center

Answer: D

Explanation:

Question: 516

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two sensitivity labels named Label1 and Label2. The subscription contains a Windows device named Device1 that is onboarded to Microsoft Purview. Device1 contains the files shown in the following table.

Name	Location	Sensitvrty
File 1	CATemp\	Labell
File2.doc	C:\Temp\FoWer1\	Label?
File3	C:\lefnp\Folder2\	Labell

You create a data loss prevention (DLP) policy named Policy1 that has the following configurations:

Answer Area

Statements	Yes	No
A user on Devicel can pnnt Filel.docx.		
A user on Dewed can print File2docx.		
A user on Dewed can print File3.docx,		

Answer

Question: 517

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to identify the settings that are configured less secure than the Standard protection profile settings in the preset security policies.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

^ | Microsoft Defender portal
Microsoft 365 admin center
Microsoft Defender portal
Microsoft Purview portal

Feature: |
Configuration analyzer
Preset security policies
Threat tracker

Answer:

Explanation:

Answer Area

Portal: Microsoft 365 admin center

Feature Configuration analyzer

Question: 518

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.

You need to ensure that when a user-based alert is triggered in Defender for Cloud Apps, the user is marked as compromised.

Which two options can you use to automate the response?

Each correct answer presents a complete solution.

A. a block script

B. a custom detection rule

C. a user tag

D. an automated remediation level

E. a Microsoft Power Automate playbook

Answer: C, E

Explanation:

Question: 519

You have a Microsoft 365 subscription.

You need to add additional domains with the onmicrosoft.com suffix to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

A. 1

B. 2

C. 5

D. 10

Answer: A

Explanation:

Question: 520

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Endpoint.

You integrate Microsoft Defender for Endpoint with Microsoft Intune.

From Microsoft Defender Vulnerability Management, you review the top security recommendations and discover a recommendation to update Microsoft Edge (Chromium) to a later version.

You need to ensure that a security task is added to Intune to address the recommendation.

What should you do?

A. From the Microsoft Intune admin center, configure a security baseline.

B. From the Microsoft Intune admin center, configure Windows Autopatch.

C. From the Microsoft Defender portal add an incident notification rule.

D. From the Microsoft Defender portal, select Request remediation.

Answer: D

Explanation:

Question: 521

You have a Microsoft 365 E5 subscription that contains a group named Group1. The subscription uses Microsoft Defender for Cloud Apps.

You configure cloud discovery.

You need to ensure that you can create a custom report that details shadow IT usage by the members of Group1.

What should you do first?

A. Add an app connector.

B. Disable anonymization.

C. Configure user enrichment.

D. Configure user monitoring.

Answer: C

Explanation:

Question: 522

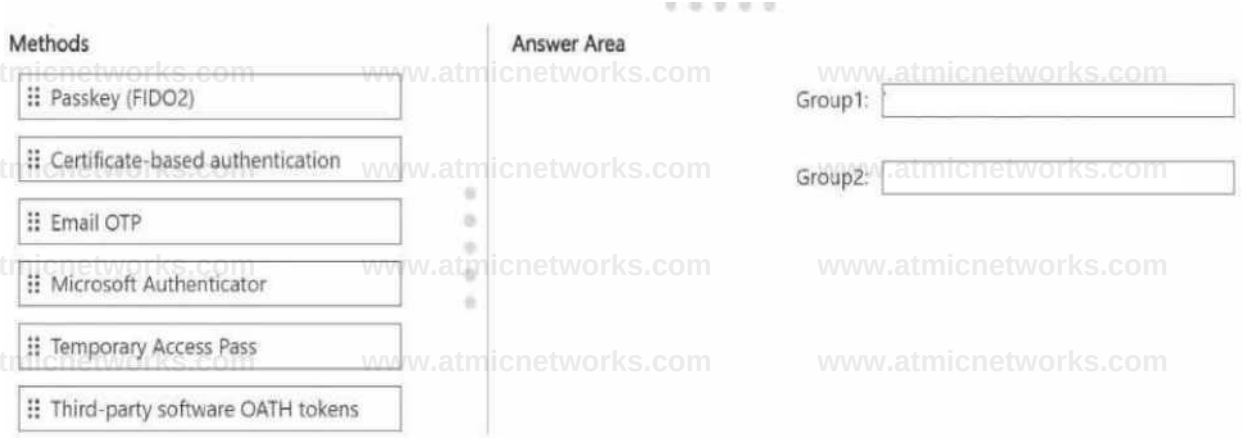
DRAG DROP

You have a Microsoft 365 E5 subscription that contains two security groups named Group1 and Group2. You need to recommend an authentication solution that meets the following requirements:

- Members of Group1 must be able to authenticate by using a hardware token.
- Members of Group2 must be able to authenticate by using a public key infrastructure (PKI).

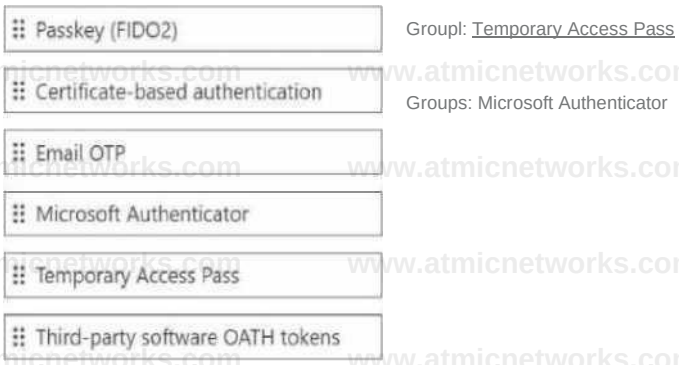
Which authentication method should you recommend for each group? To answer, drag the appropriate methods to the correct groups. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one



Answer:

Explanation:



Question: 523

HOTSPOT

You configure a data loss prevention (DLP) policy named DLP1 with a rule configured as shown i n the following exhibit.

Answer Area

DLP1 cannot be applied to **[answer choice].** OneDrive accounts | Exchange email SharePoint sites

OneDrive accounts

DLP1 will be applied only to documents that have [answerchoice], both a credit card number and the RetentionLabell label applied

both a credit card number and the RetentionLabell label applied

either a credit card number or the RetentionLabell label applied between 85 and 100 credit card numbers

Answer

Explanation:

Answer Area

DLP1 cannot be applied to [answer choice}. OneDrive accounts b*

DLP1 will be applied only to documents that have [answer choice], both a credit card number and the RetentionLabell label applied

Question: 524

You have a Microsoft 365 E5 subscription.

You are implementing Microsoft Defender for Cloud Apps.

You need to ensure that you can create OAuth app policies.

Solution: You configure Cloud Discovery.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 525

You have a Microsoft 365 E5 subscription. You are implementing Microsoft Defender for Cloud Apps.

You need to ensure that you can create OAuth app policies.

Solution: You add an API token to Defender for Cloud Apps.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 526

You have a Microsoft 365 subscription that includes Microsoft Intune and Microsoft Defender XDR.

All users have devices that run Windows 11.

From the Microsoft Defender portal, you review the Microsoft Secure Score recommendations. One of the top recommendations is to block all Microsoft Office applications from creating child processes.

You need to increase the secure score by addressing the recommendation.

What should you do?

A. Create an attack surface reduction (ASR) policy.

B. Configure an endpoint detection and response (EDR) policy.

C. Create a policy for Office applications.

D. Select Safe Documents for Office clients.

Answer: A

Explanation:

Question: 527

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Windows 11 device named Device1.

Device1 is onboarded to Microsoft Defender for Endpoint.

You need to ensure that Device1 is blocked from connecting to IP address 131.107.10.15.

What should you configure in the Microsoft Defender Endpoint settings? To answer, select the appropriate settings in the answer

area.

NOTE: Each correct selection is worth one point.

Answer Area

Advanced features:

Custom network indicators
Custom network indicators
Live Response
Web content filtering

Rules: Indicators

Asset rule management
Indicators
Process Memory Indicators

Answer:

Explanation:

Answer Area

Advanced features: Custom network indicators

Rules: Indicators

Question: 528

You have a Microsoft 365 E5 subscription.

You are evaluating Microsoft Defender for Cloud Apps.

Which two types of policy rely on Conditional Access App Control? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. app discovery policy

B. OAuth app policy

C. access policy

D. file policy

E. session policy

F. activity policy

Answer: C, E

Explanation:

Question: 529

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to ensure that an alert is generated when an app is registered in Microsoft Entra and is assigned the Directory.Readwrite.ALL Microsoft Graph permission.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use: Microsoft Defender for Cloud Apps
| Microsoft Defender for Cloud
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint Microsoft Defender for Identity Microsoft Defender for Office 365

Configure: an OAuth apps policy _____ an Access policy an App discovery policy a Conditional Access policy
an OAuth apps policy
| a Session policy

Answer:

Explanation:

Answer Area

Use: Microsoft Defender for Cloud Apps

Configure: an OAuth apps policy

Question: 530

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to enable password less authentication for all users.

Which authentication method and portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Authentication method: Microsoft Authenticator ▼

Email OTP

SMS Voice call

Portal: Microsoft 365 admin center

Microsoft 365 admin center

| Microsoft Entra admin center

Answer:

Explanation:

Answer Area

Question: 531

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Office 365.

You need to implement a threat policy that will apply a balanced baseline protection profile to protect against spam, phishing, and malware.

Solution: You create a Standard preset security policy.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 532

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.

You plan to configure a data loss prevention (DLP) strategy that meets the following requirements:

- Members of Group1 must be prevented from sharing documents that contain credit card numbers.
- Members of Group2 must be prevented from sharing documents that are classified as internal by Microsoft Purview Information Protection.
- The solution must minimize administrative effort

You need to create a DLP policy for each group.

Which condition should you add to each DLP policy rule for each group? To answer, select the appropriate options in the answer

area.

NOTE: Each correct selection is worth one point.

Answer Area

Group1: _____

Select Document name contains words or phrases.

Select Document property is.

Set Content contains to Sensitive info types

Set Content contains to Sensitivity labels.

Groups [

Select Document name contains works or phrases.

select document property is.

Set Content contains to Sensitive info types.

Set Content contains to Sensitivity labels.

Answer:

Explanation:

Answer Area

Groupl: Set Content contains to Sensitive info types. ’

Group2: Set Content contains to Sensitivity labels. *

Question: 533

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the identities shown in the following table.

Name	Type	Member of
Useri	User	Groupl
User?	User	Group?
UserS	User	*None*
Groupl	Group	*None*
Group?	Group	Groupl

From the Microsoft Defender portal, you create an anti-spam inbound policy named Policy1 that has the following settings:

- Include these users, groups and domains

o Users: User3 o Groups: Group1

- Exclude these users, groups and domains

o Users: User1

Policy1 has the following Bulk email threshold & spam properties settings:

- Mark as spam

o Empty messages: On o Object tags in HTML On o Sensitive words: Off o Backscatter On

Policy1 has the following Actions settings:

- Message actions

o Spam: Move message to Junk Email folder

o High confidence spam: Move message to Junk Email folder

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If Useri sends an empty email message to User2, Policy 1 will move the message to the Junk Email folder of User2.	O	Q
If User2 sends User3 an email message that contains sensitive words, Policy 1 will move the message to the Junk Email folder of User3.		
If User3 sends an empty email message to Useri. Policyl will move the message to the Junk Email folder of Useri.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
If User 1 sends an empty email message to User2. Policyl will move the message to the Junk Email folder of User2.	O	®
If User2 sends User3 an email message that contains sensitive words, Policyl will move the message to the Junk Email folder of User3.	O	•
If User3 sends an empty email message to User 1. Policyl will move the message to the Junk Email folder of Useri.	•	

Question: 534

You have a Microsoft 365 E5 subscription.

You create a user named Admin1.

You need to ensure that Admin1 can view Endpoint security policies from the Microsoft Defender portal. The solution must follow the principle of least privilege.

Which Microsoft Entra role should you assign to Admin1?

A. Security Administrator

B. Cloud Device Administrator

C. Global Reader

D. Security Reader

E. Security Operator

Answer: D

Explanation:

Question: 535

You have a Microsoft 365 subscription.

From the Microsoft Entra authentication methods policy, you configure the Microsoft Authenticator on companion applications settings as shown in the following exhibit.

Microsoft Authenticator on companion applications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview, team more —

Status Enabled v

Target Include Exclude

• All users

Select group

You need to ensure that users can complete the authentication process from their mobile device.

What should each user install on their device?

A. Microsoft 365 Copilot

B. Microsoft Outlook

C. Company Portal

D. Microsoft Teams

Answer: C

Explanation:

Question: 536

You have a Microsoft 365 subscription.

You need to identify which shadow IT apps users connect to by using Cloud Discovery in Microsoft Defender for Cloud Apps. What should you create first?

A. a session policy

B. an app discovery policy

C. a Conditional Access policy

D. a Cloud Discovery snapshot report

Answer: D

Explanation:

Question: 537

You have a Microsoft 365 E5 subscription.

You plan to configure Privileged Identity Management (PIM) for the User Administrator role in Microsoft Entra, You need to ensure that a user can make a role assignment request for the User Administrator role only during the next six months. How should you configure the assignment?

A. Set Assignment type to Eligible

B. Set Allow permanent eligible assignment to Yes

C. Set Allow permanent active to assignment Yes

D. Set Assignment type to Active.

Answer: A

Explanation: