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, Case Study Contoso, Ltd.

Overview

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

Contoso has a Microsoft 365 E5 subscription.

Network Environment

The network contains an on-premises Active domain named Contoso.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC	Windows Server 2019	Domain controller
Served	Windows Server 2016	Member server
Server?	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named Contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups

The Contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
useri	Cloud device administrator	Basic Purchaser	GroupA
User?	Azure AD r<?<ned device local administrator	Device Guard signer	GroupB
User 3	Global reader	Purchaser	GroupA Groups
User4	Global administrator	**None**	Group 1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group and Group have a Membership type of Assign

Devices

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Devicel	Corporate-owned	Group1	Default
Device?	Corporate-owned	Group!. Group?	Tag?
Device3	Personally-owned	Group!	Tagl
Device	Personally-owned	Group?	Tag?
Devices	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocket Drive Encryption (Bit locket)	Secure Boot	VPN connection
DeviceI	Yes	No	VPN1
DeviceZ	Yes	Yes	VPN1, VPN3
Device]	No	No	VPN3
Device4	No	Yes	None
Devices	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder 1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

The Compliance policy settings are shown in the following exhibit.

Hun sittings ccc'^t* th* way th* compliance Mn*C* Vaals d*VK*S Exh dr>ic*

r . abates thf^f ri a B^t-n Devic* Comp 5- -- Poky* which is refected m c- re monitoring.

Maric devicM with no compliant* policy ^E5!H^® Not Comphant

assigned as 0

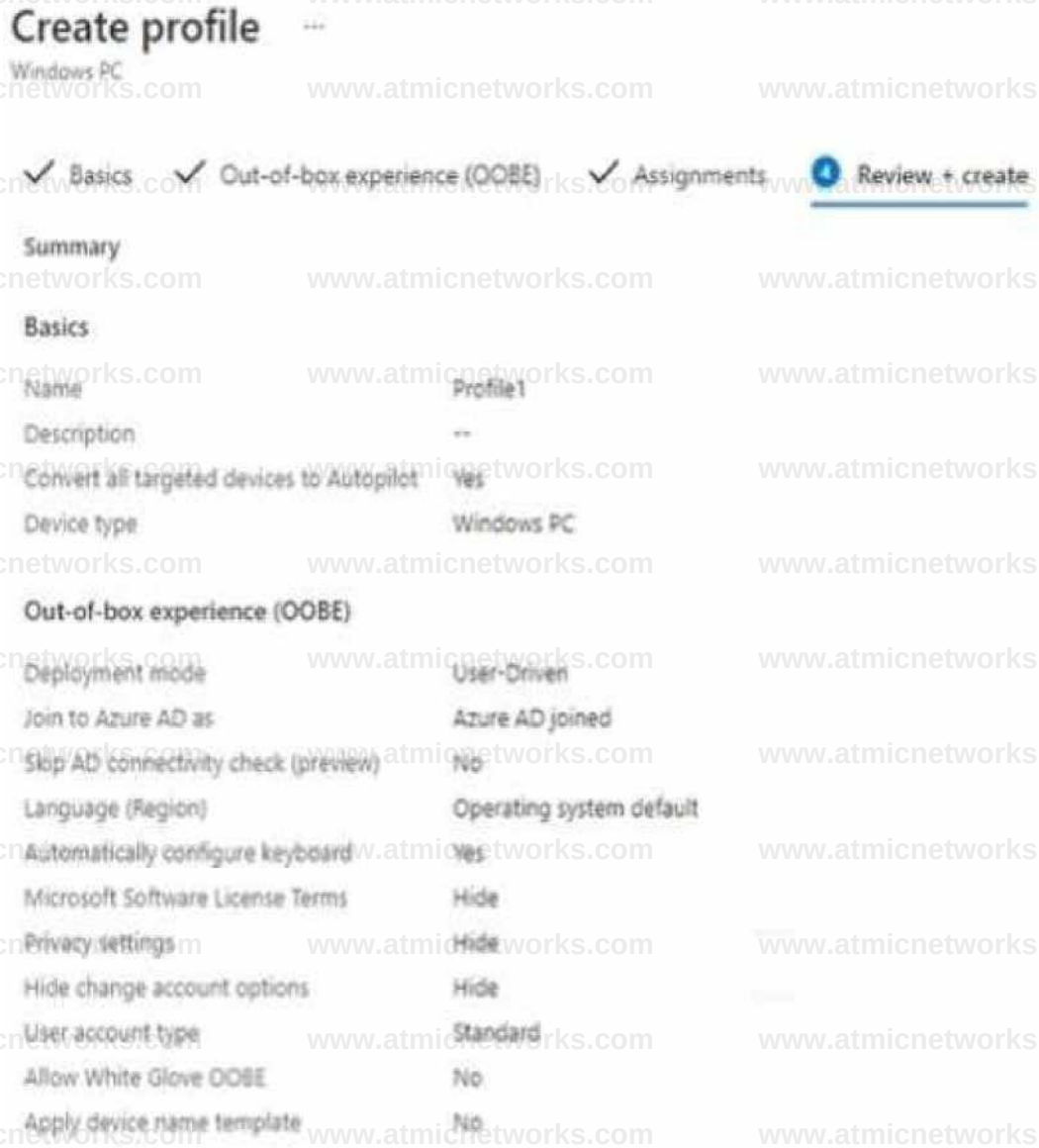
The Automatic Enrolment settings have the following configurations:

- MDM user scope GroupA
- MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

- Name: Protection1
- Folder protection: Enable
- List of apps that have access to protected folders: CV\AppA.exe
- List of additional folders that need to be protected: D:\Folderi1
- Assignments

Windows Autopilot Configuration



Currently, there are no devices deployed by using Window Autopilot

The Intune connector tor Active Directory is installed on Server 1.

Planned Changes

Contoso plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AO joined.
- Deploy a network boundary configuration profile that will have the following settings:
- Name Boundary 1
- Network boundary 192.168.1.0/24
- Scope tags: Tag 1
- Assignments;
- included groups: Group 1. Group2
- Deploy two VPN configuration profiles named Connection! and Connection that will have the following settings:
- Name: Connection 1
- Connection name: VPNI
- Connection type: L2TP

- Assignments:
- Included groups: Group1. Group2, GroupA
- Excluded groups: —
- Name: Connection
- Connection name: VPN2
- Connection type: IKEv2 i Assignments:
- included groups: GroupA
- Excluded groups: GroupB
- Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements

Contoso must meet the following technical requirements:

- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

Question: 1

Which user can enroll Device6 in Intune?

A. User4 and User2 only
B. User4 and User 1 only
C. User1, User2, User3, and User4
D. User4. User Land User2 only

Answer: C

Explanation:

Question: 2

HOTSPOT

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 Are*

Statements	Yes	No
if Useri adds a shortcut to the desktop of Device 1 when Useri signs in to Devices the same shortcut will appear on the desktop		
If User! sets the desktop background to blue on Device?. when User 1 signs tn to Device4 the desktop background will be blue		
if User? increases the sire of the font In the command prompt of Device?, when User? signs in to Device}, the command prompt wil show the increased font sue.		

Answer:

Explanation:

Statements	Yes	No
If Userl adds a shortcut to the desktop of Devicel, when Userl signs in to Device3, the same shortcut will appear on the desktop.		
If Userl sets the desktop background to blue on Device2, when Userl signs in to Device4, the desktop background will be blue.		
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3(the command prompt will show the increased font size.		

Question: 3

Which users can purchase and assign App1?

A. User3 only
B. User1 and User3 only
C. User1, User2, User3, and User4
D. User1, User3, and User4 only
E. User3 and User4 only

Answer: B

Explanation:

Reference:

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

https://docs.microsoft.com/en-us/microsoft-store/assign-apps-to-employees

Question: 4

HOTSPOT

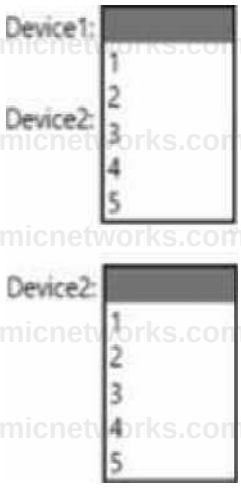
You implement the planned changes for Connection1 and Connection2

How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2?

To answer select the appropriate options in the answer area.

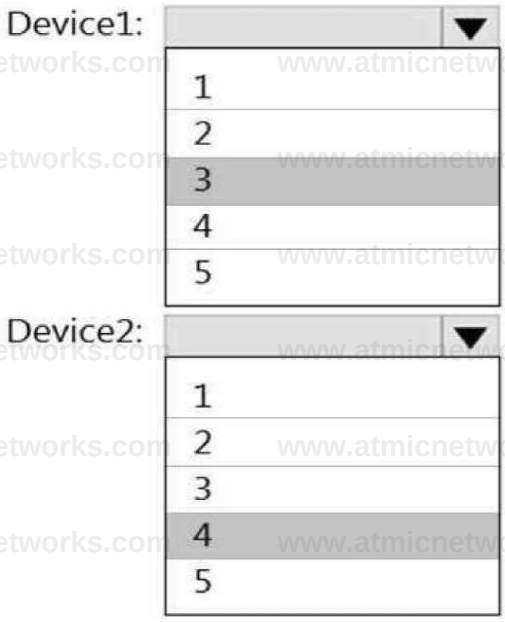
NOTE; Each correct selection is worth one point.

Answer Area



Answer:

Explanation:



Question: 5

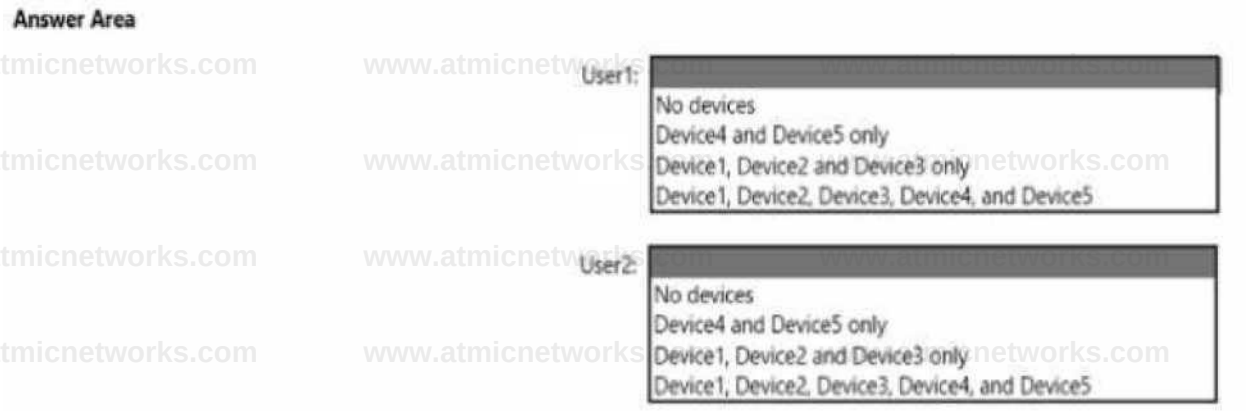
HOTSPOT

User1 and User2 plan to use Sync your settings.

On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.

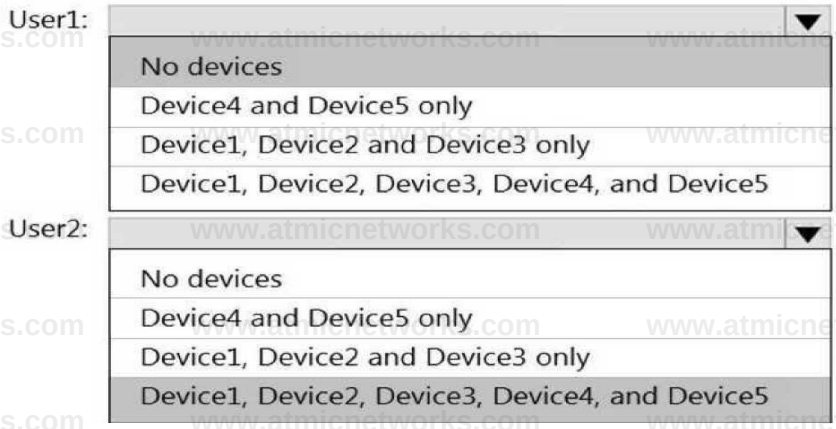
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:



Reference:

https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/

Question: 6

You need to ensure that computer objects can be created as part of the Windows Autopilot

deployment. The solution must meet the technical requirements.

To what should you grant the right to create the computer objects?

A. Server2
B. Server1
C. GroupA
D. DC1

Answer: B

Explanation:

Reference:
https://blog.matrixpost.net/set-up-windows-autopilot-production-environment-part-2/

Question: 7

HOTSPOT

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
Devicel is marked as compliant.	Q	Q
Device4 is marked as compliant.	o	0
Devices is marked as compliant.	O	0

Answer:

Explanation:

Statements	Yes	No
Devicel is marked as compliant.	O	O
Device4 is marked as compliant.	O	O
Devices is marked as compliant.	O	O

Question: 9

You implement Boundary1 based on the planned changes.

Which devices have a network boundary of 192.168.1.0/24 applied?

A. Device2 only
B. Device3 only
C. Device 1. Device2. and Device5 only
D. Device 1, Device2, Device3, and Device4 only

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows

Question: 10

Which devices are registered by using the Windows Autopilot deployment service?

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

Answer: C

Explanation:

Scenario: Windows Autopilot Configuration

Assignments
Included groups: Group1
Excluded groups: Group2
Device1 is member of Group1.
Device2 is member of Group1 and member of Group2.
Device3 is member of Group1.
Group1 and Group2 have a Membership type of Assigned.

Exclusion takes precedence over inclusion in the following same group type scenarios.

Reference: https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

Topic 2, Litware inc

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. When you are ready to answer a question, click the Question button to return to the question.

Existing Environment

Current Business Model

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11:00 to 22:00.

Litware has a Microsoft System Center 2012 R2 Configuration Manager deployment. During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain joined
Marketing	8.1	Configuration Manager	Hybrid Azure ADjoined
Research	10	Configuration Manager	Hybrid Azure ADjoined
HR	8.1	Configuration Manager	Hybrid Azure ADjoined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements

Business Goals

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements

Litware identifies the following device management requirements:

Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.

Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements

Litware identifies the following technical requirements for the planned deployment:

Re-provision the sales department computers by using Windows AutoPilot.

Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.

Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits

Settings

Windows 10 and later

Update settings

Servicing channel ft	Semi-Annual Channel (Targeted) V
’ Microsoft product updates ft	Allow / Block
■ Windows drivers ft	Allow / Block
’ Quality update deferral period (days) ft	7
■ Feature update deferral period (days) ft	14
■ Set feature update uninstall period (2 - 60 days) ft	10

User experience settings

Automatic update behavior ft	Auto install at maintenance time V
Active hours start ft	SAM
Active hours end ft	5PM
Restart checks ft	Allow / Skip
Delivery optimization download mode ft	Simple download mode with no peering v

OK

Question: 11

You need to capture the required information for the sales department computers to meet the technical requirements.

Which Windows PowerShell command should you run first?

A. Install-Module WindowsAutoPilotIntune

B. Install-Script Get-WindowsAutoPilotInfo
C. Import-AutoPilotCSV
D. Get-WindowsAutoPilotInfo

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices "This topic describes how to convert Windows 7 or Windows 8.1 domain-joined computers to Windows 10 devices joined to either Azure Active Directory or Active Directory (Hybrid Azure AD Join) by using Windows Autopilot"

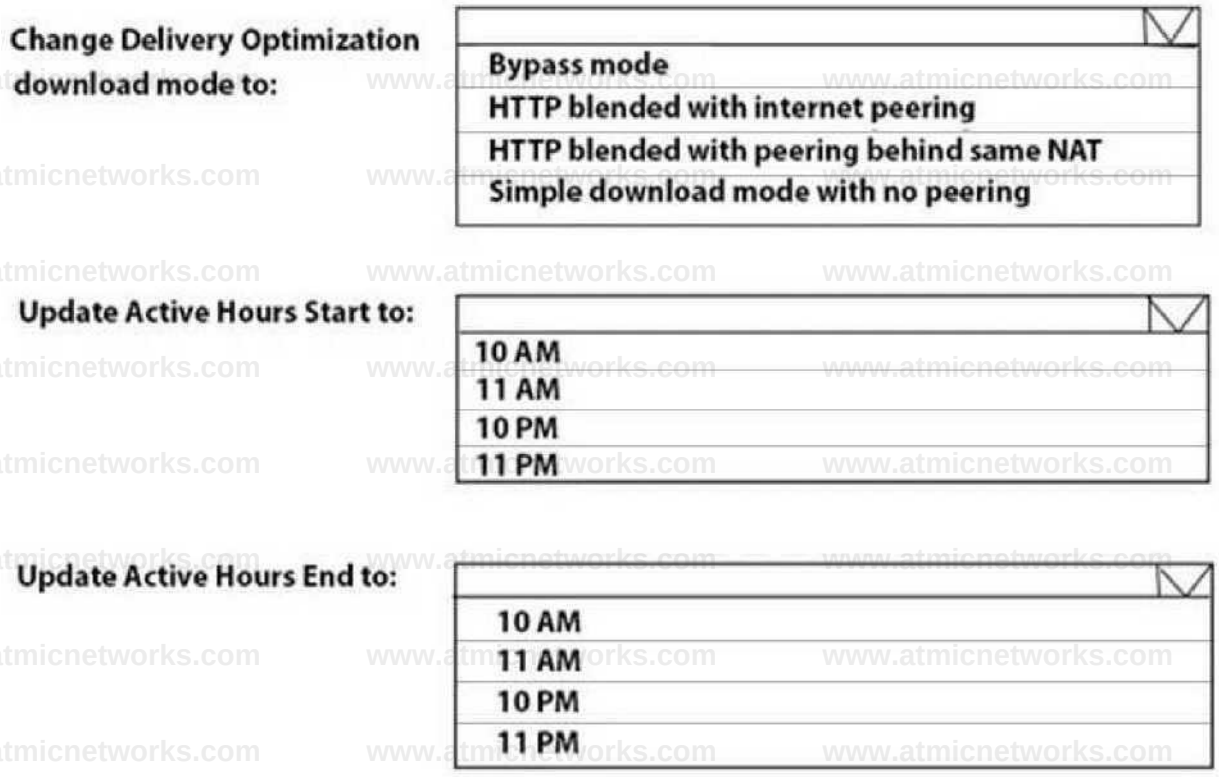
Question: 12

HOTSPOT

You need to resolve the performance issues in the Los Angeles office.

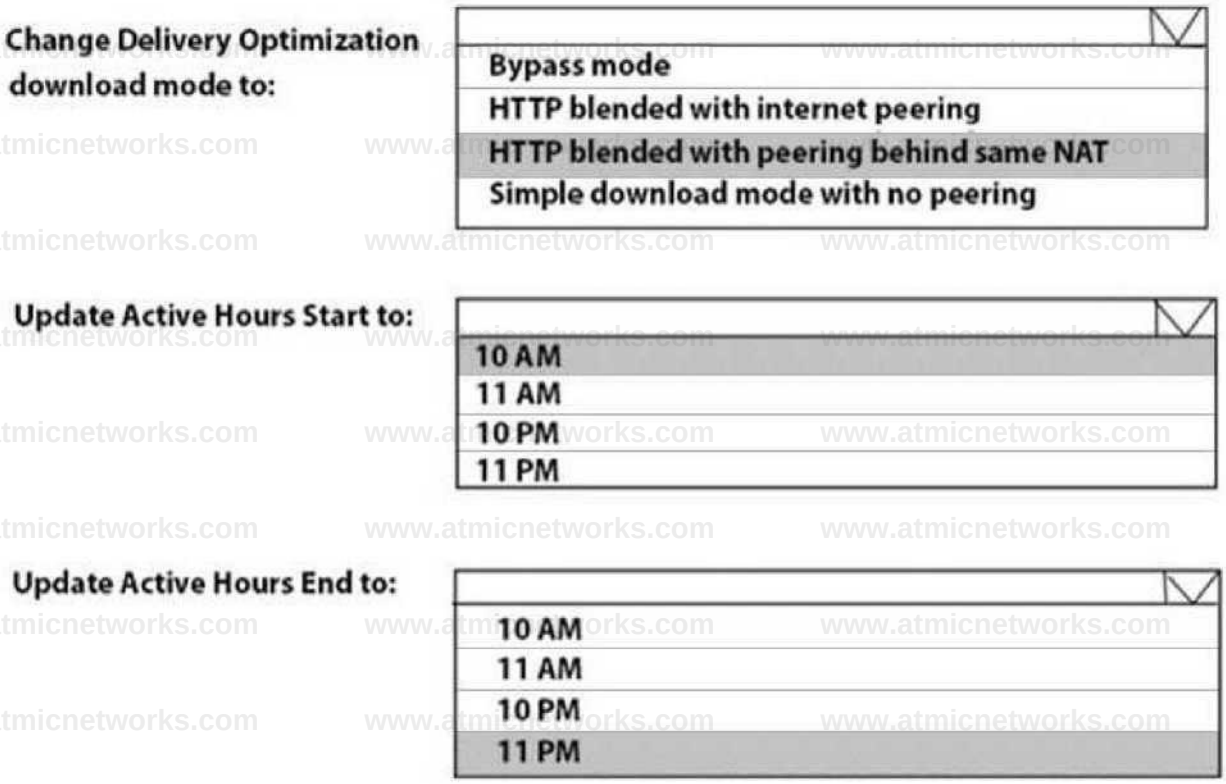
How should you configure the update settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization
https://2pintsoftware.com/delivery-optimization-dl-mode/

Question: 13

What should you configure to meet the technical requirements for the Azure AD-joined computers?

A. Windows Hello for Business from the Microsoft Intune blade in the Azure portal.
B. The Accounts options in an endpoint protection profile.
C. The Password Policy settings in a Group Policy object (GPO).
D. A password policy from the Microsoft Office 365 portal.

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-inorganization

Question: 14

HOTSPOT

You need to meet the OOBE requirements for Windows AutoPilot.

Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Overview

Getting started

Manage

Users

Groups

Organizational relationships Roles and administrators Enterprise applications Devices

App registrations

App registrations (Preview) Application proxy

Licenses

Azure AD Connect

Custom domain names Mobility (MDM and MAM) Password reset

Company branding

User settings

Properties

Notifications settings

Answer:

Explanation:

Reference:

https://blogs.msdn.microsoft.com/sgern/2018/10/11/intune-intune-and-autopilot-part-3-preparing- your-environment/

https://blogs.msdn.microsoft.com/sgern/2018/11/27/intune-intune-and-autopilot-part-4-enroll- your-first-device/

Question: 15

What should you use to meet the technical requirements for Azure DevOps?

A. An app protection policy
B. Windows Information Protection (WIP)
C. Conditional access
D. A device configuration profile

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional- access?view=azure-devops

Question: 16

HOTSPOT

You need to recommend a solution to meet the device management requirements.

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

NOTE: Each correct selection is worth one point.

For the Research department employees:	**An app configuration policy** **An app protection policy** **Azure information Protection** **iOS app provisioning profiles**
For the Sales department employees:	**An app configuration policy** **An app protection policy Azure information Protection** **iOS app provisioning profiles**

Answer:

Explanation:

For the Research department employees:	**An app configuration policy** **An app protection policy** **Azure information Protection** **iOS app provisioning profiles**
For the Sales department employees:	**An app configuration policy**

An app protection policy
Azure information Protection
iOS app provisioning profiles

Reference:
https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md

https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-not- forward-option-for-emails

Question: 17

HOTSPOT

You need to meet the technical requirements for Windows AutoPilot.

Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Overview

Getting started

Manage

Users

Groups

Organizational relationships

Roles and administrators

Enterprise applications

Devices

App registrations

App registrations (Preview)

Application proxy

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

Question: 18

What should you upgrade before you can configure the environment to support co-management?

A. the domain functional level
B. Configuration Manager
C. the domain controllers
D. Windows Server Update Services (WSUS)

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

Question: 19

You need to meet the device management requirements for the developers. What should you implement?

A. folder redirection
B. Enterprise State Roaming
C. home folders
D. known folder redirection in Microsoft OneDrive

Answer: B

Explanation:

Litware identifies the following device management requirements:

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.

Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming- windows-settings-reference

Topic 3, Contoso Ltd, Case 2

Overview

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

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices

Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft System Center Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organization unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration

The domain has die users shown in the following table.

Name	Role	Member of
Userl	Intune administrator	GroupA
User?	*None*	GroupB

User? is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table

Name	Platform	Encryption	Member of
Device 1	Android	Disabled	Group1
Device?	iOS	Not applicable	Group?, Group?
Device3	Android	Disabled	Group?.. Group?
Device4	iOS	Not applicable	Group?

The device compliance policies in Intune are configured as shown in the. following table

Name	Platform	Require encryption	Assigned
Policy 1	Android	Not configured	Yes
Policy?	iOS	Not applicable	Yes
Policy?	Android	Require	Yes

The device compliance policies have the assignments shown in the following table:

Name	Include	Exclude
Policy 1	Group?	*None*
Policy?	Group?	Group?
Policy?	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction!	15	GroupB
2	Restriction?	10	GroupA
Default	All users	5	All users

Requirements

Planned Changes

Contoso plans to implement the following changes:

Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.

Start using a free Microsoft Store for Business app named App1.

Implement co-management for the computers.

Technical Requirements:

Contoso must meet the following technical requirements:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question: 20

HOTSPOT

You need to meet the technical requirements for the new HR department computers.

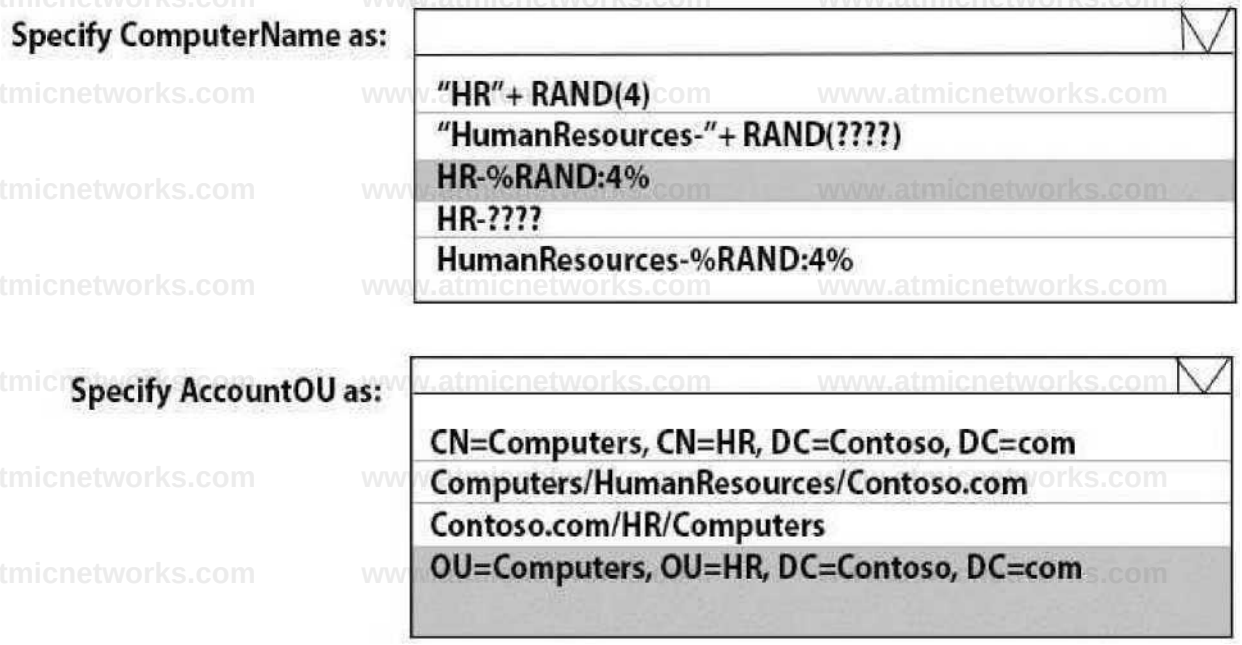
How should you configure the provisioning package? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Specify ComputerName as:	**"HR"+ RAND(4)** **"HumanResources-"+ RAND(????)** **HR-%RAND:4%** **HR-????** **HumanResources-%RAND:4°/o**
Specify AccountOU as:	**CN=Computers, CN=HR, DC=Contoso, DC=com** **Computers/HumanResources/Contoso.com** **Contoso.com/HR/Computers** **OU=Computers, OU=HR, DC=Contoso, DC=com**

Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts

Question: 21

You need to meet the technical requirements for the iOS devices.
Which object should you create in Intune?

A. A compliance policy
B. An app protection policy
C. A Deployment profile
D. A device configuration profile

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-configure
https://docs.microsoft.com/en-us/intune/device-restrictions-ios

Question: 22

HOTSPOT

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policy!:	
	Devlcel only
	Devlce2 only
	Devices only
	Devlce4 only
	Devlce2 and Devices only
	Devlcel and Devices only
	Devlcel, Devlce2, and Device 3

Policy2:	
	Device! only
	Devlce2 only Devices only Devlce4only
	Devlce2 and Devices only
	Device! and Devices only
	Devlcel, Devlce2, and Device 3

Answer:

Explanation:

Policy1:

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device 3

Policy2:

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device 3

Reference:

https://docs.microsoft.com/en-us/intune/device-profile-assign

Question: 23

HOTSPOT

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Useri can enroll a maximum of:	IV
	5 devices 10 devices
	15 devices 1,000 devices
	An unlimited number of devices

User! can enroll a maximum of:	N/
	5 devices
	10 devices
	15 devices
	1,000 devices
	An unlimited number of devices

Answer:

Explanation:

Useri can enroll a maximum of:	
	5 devices 10 devices 15 devices 1,000 devices An unlimited number of devices

User2 can enroll a maximum of:	
	5 devices 10 devices 15 devices 1,000 devices An unlimited number of devices

Question: 24

You need to meet the technical requirements for the IT department.

What should you do first?

A. From the Azure Active Directory blade in the Azure portal, enable Seamless single sign-on.
B. From the Configuration Manager console, add an Intune subscription.
C. From the Azure Active Directory blade in the Azure portal, configure the Mobility (MDM and MAM)

settings.

D. From the Microsoft Intune blade in the Azure portal, configure the Windows enrollment settings.

Answer: C

Explanation:

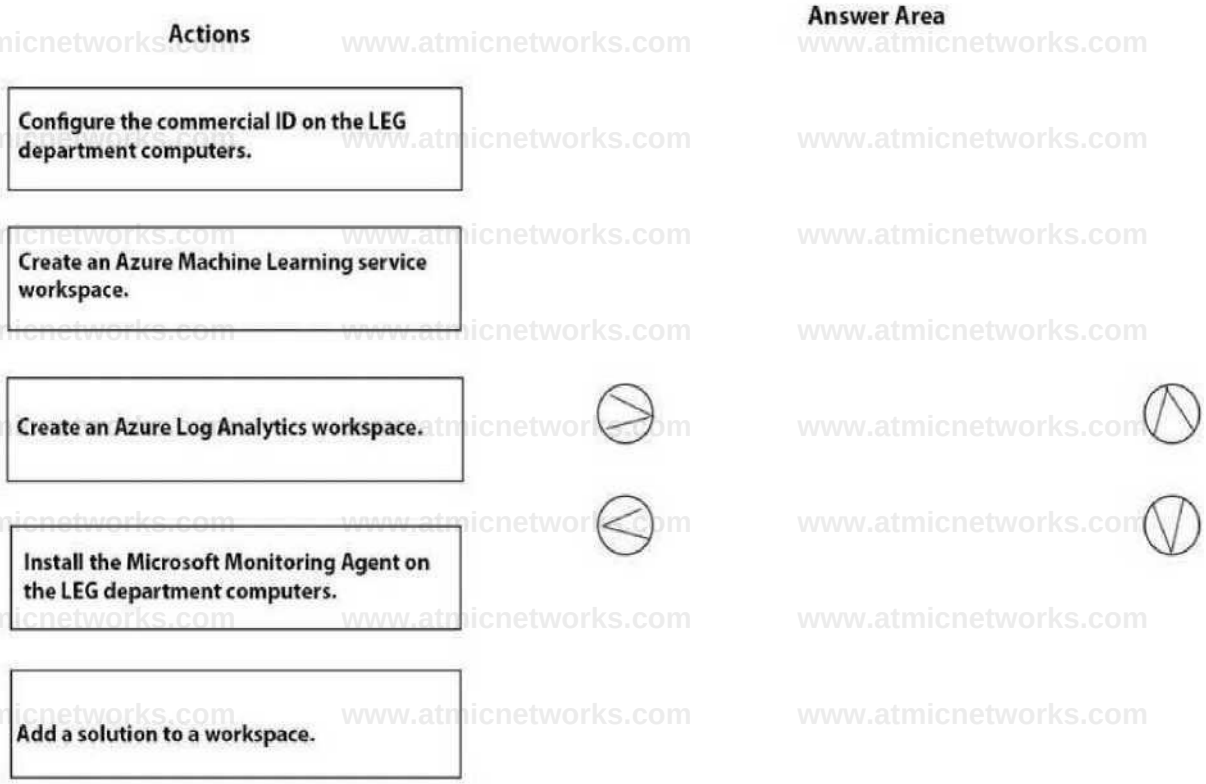
Reference:
https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

Question: 25

DRAG DROP

You need to meet the technical requirements for the LEG department computers.

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:

Create an Azure Log Analytics workspace.

Add a solution to a workspace.

Configure the commercial ID on the LEG department computers.

Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-azure-portal

Question: 26

You need to prepare for the deployment of the Phoenix office computers.

What should you do first?

A. Extract the hardware ID information of each computer to a CSV file and upload the file from the Devices settings in Microsoft Store for Business.

B. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory blade in the Azure portal.

C. Generalize the computers and configure the Device settings from the Azure Active Directory blade in the Azure portal.

D. Extract the hardware ID information of each computer to an XLSX file and upload the file from the Devices settings in Microsoft Store for Business.

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#manage-autopilot- deployment-profiles

Question: 27

HOTSPOT

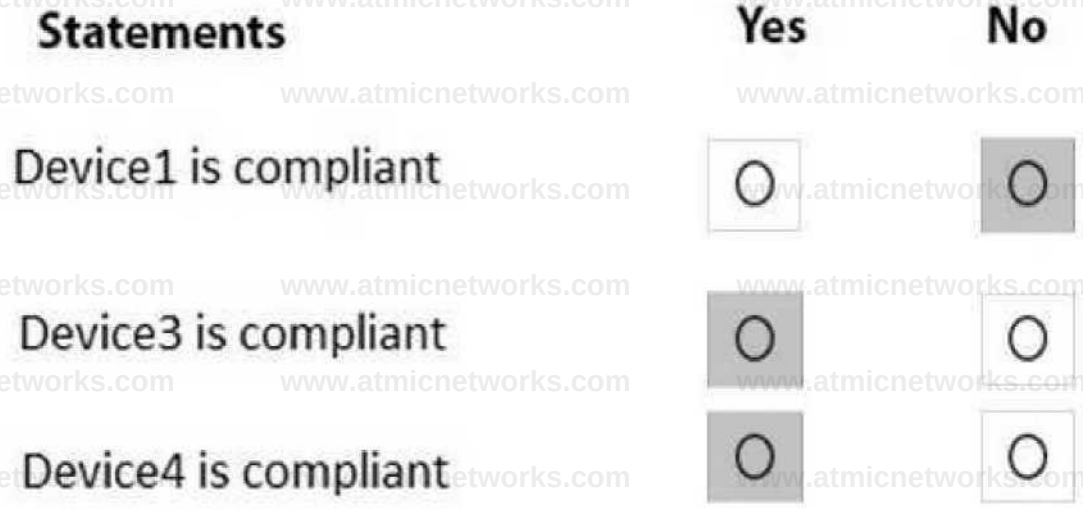
You are evaluating which devices are compliant.

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:

Explanation:



Question: 28

You need to meet the requirements for the MKG department users. What should you do?

A. Assign the MKG department users the Purchaser role in Microsoft Store for Business
B. Download the APPX file for App1 from Microsoft Store for Business
C. Add App1 to the private store
D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business
E. Acquire App1 from Microsoft Store for Business

Answer: E

Explanation:

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

Enable the users in the MKG department to use App1.

The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.

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

Question: 29

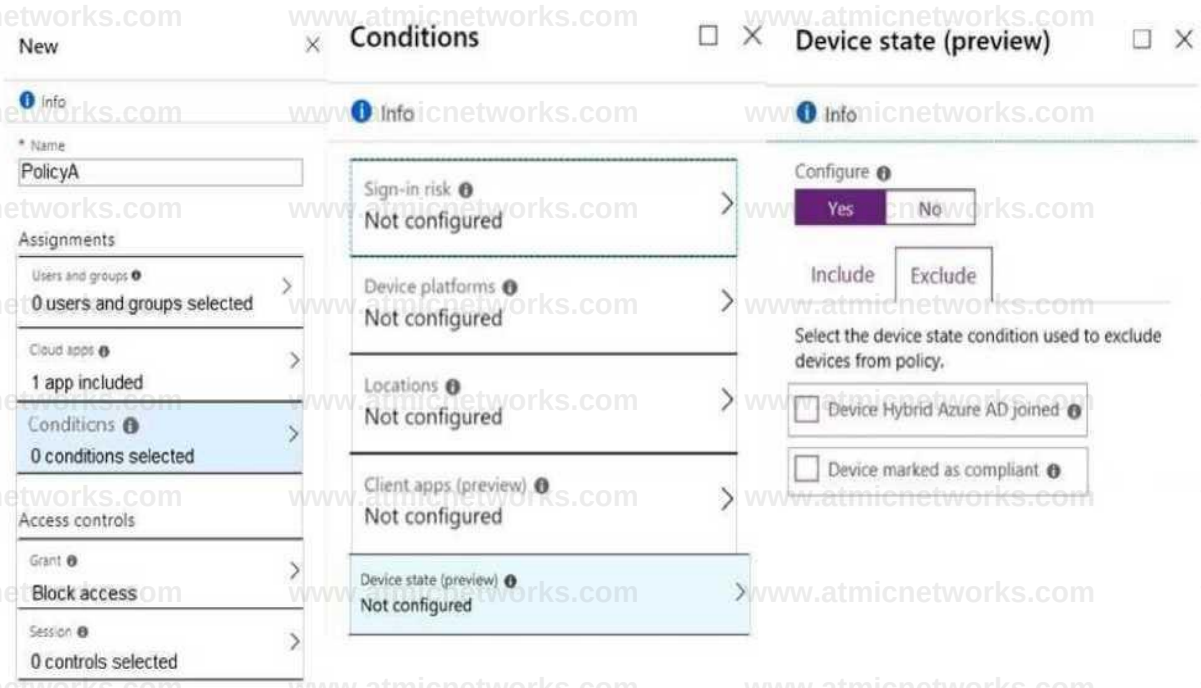
HOTSPOT

You need a new conditional access policy that has an assignment for Office 365 Exchange Online.

You need to configure the policy to meet the technical requirements for Group4.

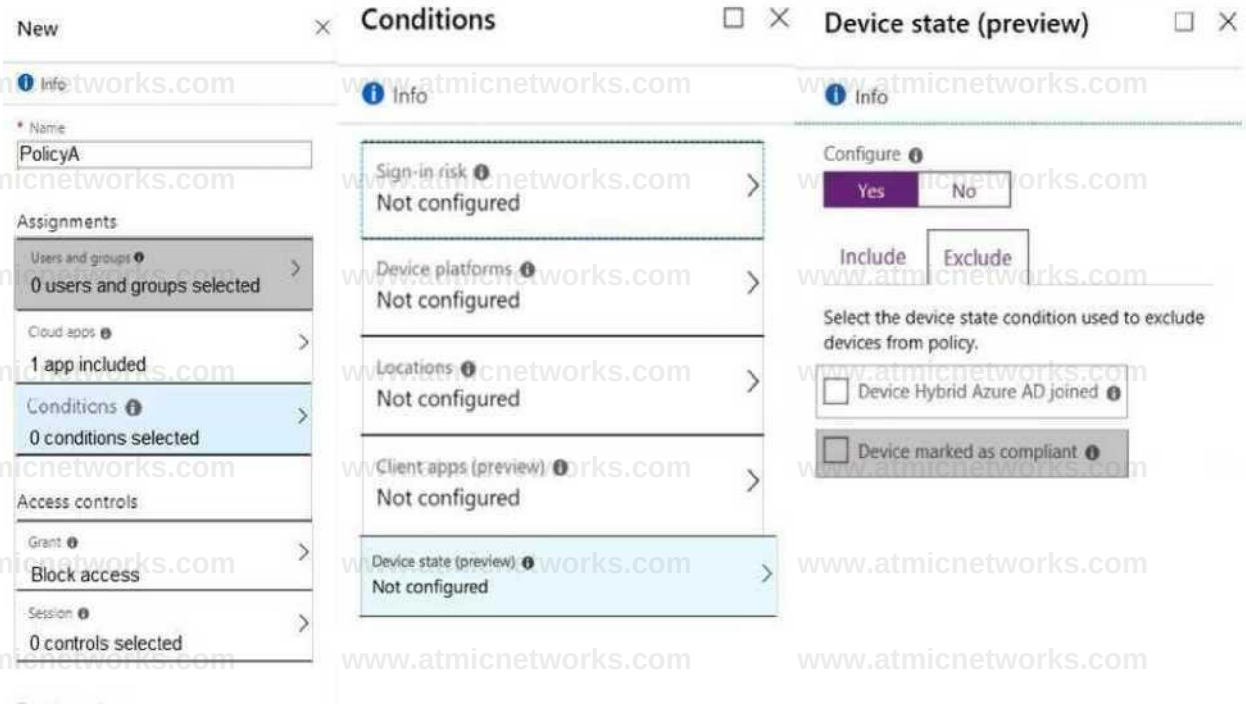
Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



The policy needs to be applied to Group4 so we need to configure Users and Groups.

The Access controls are set to Block access

We therefore need to exclude compliant devices.

From the scenario:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.

Reference:

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

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

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

Question: 30

You need to prepare for the deployment of the Phoenix office computers.

What should you do first?

A. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory admin center.

B. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

C. Extract the hardware ID information of each computer to an XML file and upload the file from the Devices settings in Microsoft Store for Business.

D. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices

Topic 4, Mix Question

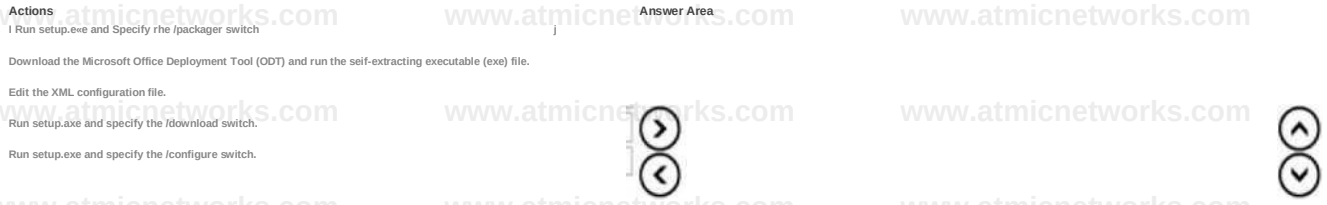
Question: 32

DRAG DROP

You have a Microsoft 365 E5 subscription and a computer that runs Windows 11.

You need to create a customized installation of Microsoft 365 Apps for enterprise.

Which four actions should you perform in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.



Answer:

Explanation:

1. Download ODT application
2. Create a configuration file (XML)
3. setup.exe /download to download the installation files
4. setup.exe /configure to deploy the application

https://learn.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-local-source

Question: 33

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

Name	Platform
Device 1	Windows 10
Device2	Windows 11
Devices	Android
Device4	iOS

On which devices can you apply app configuration policies?

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

Answer: D

Explanation:

Question: 34

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

AH devices contain an app named App1 and are enrolled in Microsoft Intune.

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Policy type: | App protection policy ~
App configuration policy
App protection polrcy

Conditional access policy
Device compliance policy

Minimum number of policies: 1

3
4
5

Answer:

Explanation:

Answer Area

Policy type: App protection policy

Minimum number of policies: 1

Policy type: App protection policy Minimum number of policies: 1 Comprehensive Explanation of

Correct Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices1. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps2. You only need one policy to apply this setting to all devices that have App1 installed1. Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies- overview 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protection- policies/troubleshoot-cut-copy-paste

Question: 35

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

You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps.

You need to ensure that App1 is installed before App2 on every device.

What should you configure?

A. the App1 deployment configurations
B. a dynamic device group
C. a detection rule
D. the App2 deployment configurations

Answer: C

Explanation:

The correct answer is D because you can configure the dependencies for a Win32 app in the deployment configurations1. Dependencies are other Win32 apps that must be installed before your Win32 app can be installed1. You can add Win32 app dependencies only after your Win32 app has been added and uploaded to Intune2. In this case, you need to configure the App2 deployment configurations to add App1 as a dependency2. Reference: 1: Microsoft Intune Win32 App Dependencies - MSEndpointMgr https://msendpointmgr.com/2019/06/03/new-intune-feature- win32-app-dependencies/ 2: Add and assign Win32 apps to Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add

Question: 36

You have a Microsoft Intune subscription.

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

Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage Appl

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: B

Explanation:

The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The

app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios

Question: 37

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.

You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.

Which extension should you select for the app package file?

A. .intunemac
B. apk
C. jpa
D. .appx

Answer: C

Explanation:

iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.

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

Question: 38

You have a Microsoft 365 E5 subscription that contains a user named User! and a web app named Appl.
App1 must only accept modern authentication requests.
You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:

- Assignments
  ° Users or workload identities: User1
  ° Cloud apps or actions: App1
- Access controls
  ° Grant: Block access

You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

A. Filter for devices
B. Device platforms
C. User risk
D. Sign-in risk
E. Client apps

Answer: E

Explanation:

you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13. Reference: 1: Conditional Access: Block legacy authentication | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy- authentication 2: What is legacy authentication? | Microsoft Learn https://learn.microsoft.com/en- us/mem/identity-protection/conditional-access/legacy-authentication 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn https://learn.microsoft.com/en- us/mem/identity-protection/conditional-access/client-apps-condition

Question: 39

HOTSPOT

You have a Microsoft 365 subscription.All users have Microsoft 365 apps deployed.

You need to configure Microsoft 365 apps to meet the following requirements:

- Enable the automatic installation of WebView2 Runtime.
- Prevent users from submitting feedback.

Which two settings should you configure in the Microsoft 365 Apps admin center? 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: 40

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM).

You need to deploy the Microsoft 36S Apps for enterprise suite to all the computers.

What should you do?

A. From the Microsoft Intune admin center, create a Windows 10 device profile.
B. From Azure AD, add an app registration.
C. From Azure AD. add an enterprise application.
D. From the Microsoft Intune admin center, add an app.

Answer: D

Explanation:

To deploy Microsoft 365 Apps for enterprise to Windows 10 devices that are enrolled in Intune, you need to add an app of type "Windows 10 app (Win32)" in the Microsoft Intune admin center and configure the app settings. You can then assign the app to groups of users or devices. Reference: https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management

Question: 41

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

You use Microsoft Intune to manage devices.

You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been ofline for 30 days.

You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained.

What should you use?

A. a Delete action
B. a Retire action
C. a Fresh Start action
D. an Autopilot Reset action

Answer: B

Explanation:

A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are ofline for more than 30 days. Reference: https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

Question: 42

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You need to review the startup times and restart frequencies of the devices. What should you use?

A. Azure Monitor
B. intune Data Warehouse
C. Microsoft Defender for Endpoint
D. Endpoint analytics

Answer: D

Explanation:

Endpoint analytics is a feature of Microsoft Intune that provides insights into the performance and health of devices. You can use endpoint analytics to review the startup times and restart frequencies of the devices, as well as other metrics such as sign-in times, battery life, app reliability, and software

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

Question: 43

HOTSPOT

You have a Microsoft 365 E5 subscription.

You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings Edit

Update settings	
Microsoft product updates	Allow
Wmcows drivers	Allow
Quality update deferral period (days)	0
Mature update deferral period (days)	
Upgrade Windows 10 devices to Latest Windows 11 release	NO
Set feature update uninstall period (2 * 60 da vs)	10
Servicing channel	General Availability channel
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	NO

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

Updates that contain fixes and improvements to existing Windows I can be deferred for 30 days

functionalfty [answer choice]. deferred indefinitely

can be deferred for 30 days

will be installed immediately

Updates that contain new Windows functionality will be installed 1 day

1 day

30 days

60 days

Answer:

Explanation:

*Updates that contain fixes and improvements to existing Windows functionality can be deferred for 30 days. This is because the update rings policy named Policy1 has the "Quality updates deferral period (days)" setting set to 30. This means that quality updates, which include fixes and improvements to existing Windows functionality, can be deferred for up to 30 days from the date they are released by Microsoft. After 30 days, the devices will automatically install the quality updates. Reference: https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure *Updates that contain new Windows functionality will be installed within 60 days of release.

This is because the update rings policy named Policy1 has the "Feature updates deferral period (days)" setting set to 60. This means that feature updates, which include new Windows functionality, can be deferred for up to 60 days from the date they are released by Microsoft. After 60 days, the devices will automatically install the feature updates. Reference: https://docs.microsoft.com/en- us/mem/intune/protect/windows-update-for-business-configure

Question: 44

You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs.

The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

A. 1 only
B. 2 and 3 only
C. 1 and 3 only
D. 1, 2, and 4 on
E. 1, 2, 3, and 4

Answer: E

Explanation:

All events from Windows event logs are collected in the Log Analytics workspace, regardless of the event level or source. Therefore, events 1, 2, 3, and 4 are all collected in the workspace. Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events

Question: 45

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

A. General
B. Users and Accounts
C. System security
D. Device experience

Answer: D

Explanation:

To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. Reference: https://docs.microsoft.com/en- us/mem/intune/configuration/device-restrictions-android-for-work#device-experience

Question: 46

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.

You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.

What should you do?

A. Onboard the macOS devices to the Microsoft Purview compliance portal.
B. From the Microsoft Intune admin center, create a security baseline.
C. Install Defender for Endpoint on the macOS devices.
D. From the Microsoft Intune admin center, create a configuration profile.

Answer: C

Explanation:

To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices. Reference: https://docs.microsoft.com/en-us/windows/security/threat- protection/microsoft-defender-atp/mac-install-with-intune

Question: 47

You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.

You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices.

The solution must minimize administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.

B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.

C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.

D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.

E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.

F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

Answer: CE

Explanation:

To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices.
Reference: https://docs.microsoft.com/en- us/mem/intune/protect/endpoint-protection-windows-10

Question: 48

You have an Azure AD group named Group1. Group! contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile! to Group1. You need to ensure that Profile! applies to Device1 only. What should you modify in Profile 1?

A. Assignments
B. Settings
C. Scope (Tags)
D. Applicability Rules

Answer: D

Explanation:

To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1. You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability rule that matches Device1's properties and excludes Device2's properties. Reference: https://docs.microsoft.com/en- us/mem/intune/configuration/device-profile-assign#applicability-rules

Question: 49

DRAG DROP

You have a Microsoft 365 subscription that includes Microsoft Intune.

You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:

- Enforces compliance for Defender for Endpoint by using Conditional Access
- Prevents suspicious scripts from running on devices

What should you configure? 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

Adeviceratriaiai policy

IA security baseline

An attack surface reduction (ASR) rule

An Intune connection

Answer Area

Enforces compliance:

Prevents suspicious scripts:

Answer:

Explanation:

Features

A device restriction policy

IA security baseline

An attack surface reduction (ASR) rule

An Intune connection

Answer Area

Enforces compliance: An Intune connection

Prevents suspicious scripts: An attack surface reduction (ASR) rule

To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in Defender for Endpoint. You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. Reference: https://docs.microsoft.com/en- us/windows/security/threat-protection/microsoft-defender-atp/conditional-access

To prevent suspicious scripts from running on devices, you need to configure an attack surface reduction (ASR) rule in Intune. ASR rules are part of the endpoint protection settings that you can apply to devices by using device configuration profiles. You can use the ASR rule “Block Office applications from creating child processes” to prevent Office applications from launching child processes such as scripts or executables. Reference: https://docs.microsoft.com/en- us/mem/intune/protect/endpoint-protection-windows-10#attack-surface-reduction-asr-rules

Question: 50

Your network contains an on-premises Active Directory domain and an Azure AD tenant.

The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordlength	
Passwordcomplexity	True
PasswordHistoiySize	24

Which device configuration profile type template should you use?

A. Administrative Templates
B. Endpoint protection
C. Device restrictions
D. Custom

Answer: A

Explanation:

To configure the settings shown in the table, you need to use the Administrative Templates device configuration profile type template. This template allows you to configure hundreds of settings that are also available in Group Policy. You can use this template to configure settings such as password policies, account lockout policies, and audit policies. Reference: https://docs.microsoft.com/en- us/mem/intune/configuration/administrative-templates-windows

Question: 51

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.

Which three types of data can you collect from the computers by using Log Analytics? Each correct answer a complete solution.

NOTE: Each correct selection is worth one point.

A. error events from the System log
B. failure events from the Security log
C. third-party application logs stored as text files
D. the list of processes and their execution times
E. the average processor utilization

Answer: A, C, E

Explanation:

You can collect error events from the System log, third-party application logs stored as text files, and the average processor utilization from the computers by using Log Analytics. These are some of the types of data that you can collect by using data sources such as Windows event logs, custom logs,

and performance counters. You cannot collect failure events from the Security log or the list of processes and their execution times by using Log Analytics. Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-overview

Question: 52

You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

A. an attack surface reduction (ASR) policy
B. a security baseline
C. an endpoint detection and response (EDR) policy
D. an account protection policy
E. an antivirus policy

Answer: C

Explanation:

To onboard the devices to Microsoft Defender for Endpoint, you need to create an endpoint detection and response (EDR) policy in the Microsoft Intune admin center. This policy enables EDR capabilities on devices that are enrolled in Intune and allows you to configure various settings for EDR functionality. You can then assign the policy to groups of users or devices. Reference: https://docs.microsoft.com/en-us/mem/intune/protect/edr-windows

Question: 53

Your company uses Microsoft Intune to manage devices.
You need to ensure that only Android devices that use Android work profiles can enroll in intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.
NOTE Each correct selection is worth one point.

A. From Platform Settings, set Android device administrator Personally Owned to Block.
B. From Platform Settings, set Android Enterprise (work profile) to Allow.
C. From Platform Settings, set Android device administrator Personally Owned to Allow
D. From Platform Settings, set Android device administrator to Block.

Answer: AB

Explanation:

To ensure that only Android devices that use Android work profiles can enroll in Intune, you need to perform two configurations in the device enrollment restrictions. First, you need to set Android device administrator Personally Owned to Block. This prevents users from enrolling personal Android devices that use device administrator mode. Second, you need to set Android Enterprise (work profile) to Allow. This allows users to enroll corporate-owned or personal Android devices that use work profiles. Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-

restrictions-set

Question: 54

HOTSPOT

You have the device configuration profile shown in the following exhibit.

Kiosk - X

Wmdoi

Basics 0 Configuration settings

Configure your devices to run in kiosk mode Before you select a kiosk mode review your app assignments in the Mobile Apos blade. Apps that you want to run in bosk mode should be assigned to a Windows device, team more about Windows kiosk mode.

Select a bosk mode	Single app, full-screen bosk
User logon typ-	**| Auto logon (Window* 10. version 1803*)**
Application type	Add Microsoft Edge browser

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. Learn more about Microsoft Edge kiosk mode.

■ doe Kiosk URL 7	https://contoso.com
Microsoft Edge kiosk mode type 0	Public Browsing (InPrivate)
Refresh browser after idle time	5

Specify Maintenance Window for App Restarts* Q	Require	Not configured
Maintenance Window Start Time	MM/DD/YVYY	h:mmss A
intensive window Recurrence		

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

Users lanswer choice]. I cannot View the address os- in Muosoft r: .e
can access any URL
cannot view the address bar in Microsoft Edge
can only access URLs that include contoso.com
can only access URLs that start with https://conioso.com/

Windows 10 and later devices can have (answer choice] j a single Microsoft Edge instance th.r rias i ub
a single Microsoft Edge instance that has a single tab
a single Microsoft Edge instance that has multiple tabs multiple Microsoft Edge instances that have multiple tabs multiple Microsoft Edge instances that each has a single tab

Answer:

Explanation:

Users can only access URLs that start with https://contoso.com/

Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab he device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:

Kiosk mode: Enabled

Kiosk type: Multi-app

Allowed URLs: https://contoso.com/*

Address bar: Disabled

These settings mean that users can only access URLs that start with https://contoso.com/ and cannot view the address bar in Microsoft Edge. The kiosk type of Multi-app allows users to open multiple instances of Microsoft Edge, but each instance can only have a single tab. Therefore, users cannot access any URL, cannot view the address bar in Microsoft Edge, and can have multiple Microsoft Edge instances that each has a single tab.

Reference: https://docs.microsoft.com/en- us/mem/intune/configuration/kiosk-settings#kiosk-browser-settings

Question: 55

HOTSPOT

You have 100 Windows 10 devices enrolled in Microsoft Intune.

You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Delivery Optimization setting: | Bandwidth optimization type ~
Bandwidth optimization type
Download mode VPN peer caching

Intune object: | A configuration profile
A configuration profile
App configuration policies
Windows 10 and later quality updates
Windows 10 and later update tings

Answer:

Explanation:

Delivery Optimization setting: B. Download mode Intune object: A configuration profile

To configure the devices to retrieve Windows updates from the internet and from other computers on a local network, you need to configure the Download mode setting in a Delivery Optimization device configuration profile. This setting specifies how the devices use Delivery Optimization to download updates. You can choose from several options, such as HTTP only, LAN only, or Group. For example, you can set the Download mode to Group and specify

a group ID for the devices to share updates among themselves and with other devices that have the same group ID. You can also set the Download mode to Internet to allow the devices to download updates from Microsoft or other devices on the internet that use Delivery Optimization. Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows

Question: 56

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2

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

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group1
Device3	iOS	Group2

From Intune, you create and send a custom notification named Notification1 to Group1.

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
User1 receives Notification1 on Device1.	○	○
User2 receives Notification1 on Device2.	○	○
User1 receives Notification1 on Device3.	○	○

Answer:

Explanation:

Statements	Yes	No
Useri receives Notificationl on Devicel.	○	○
User2 receives Notificationl on Device2.	○	○
Useri receives Notificationl on Devices.	○	○

Reference:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications

Question: 57
You use Microsoft Intune and Intune Data Warehouse.

You need to create a device inventory report that includes the data stored in the data warehouse.

What should you use to create the report?

A. the Azure portal app
B. Endpoint analytics
C. the Company Portal app
D. Microsoft Power BI

Answer: D

Explanation:

You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:

Devices
Enrollment
App protection policy
Compliance policy
Device configuration profiles
Software updates
Device inventory logs

Note: Load the data in Power BI using the OData link

With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.

Sign in to the Microsoft Endpoint Manager admin center.
Select Reports > Intune Data warehouse > Data warehouse.
Retrieve the custom feed URL from the reporting blade, for example:
https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?a pi-version=v1.0
Open Power BI Desktop.
Choose File > Get Data. Select OData feed.
Choose Basic.
Type or paste the OData URL into the URL box.
Select OK.
If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials.
To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
Select Organizational account.
Type your username and password.
Select Sign In.
Select Connect.
Select Load.

Reference: https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link- powerbi

Question: 58

You have a Microsoft 365 E5 subscription and 25 Apple iPads.

You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method.

What should you do first?

A. Upload a file that has the device identifiers for each iPad.
B. Modify the enrollment restrictions.
C. Configure an Apple MDM push certificate.
D. Add your user account as a device enrollment manager (DEM).

Answer: C

Explanation:

Reference:
https://www.manageengine.com/mobile-device-management/help/enrollment/mdm_creating_apns_certificate.html

Prerequisites for iOS enrollment Before you can enable iOS devices, complete the following steps: Make sure your device is eligible for Apple device enrollment. Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority. Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS and macOS devices.

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

Question: 59

HOTSPOT

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD).

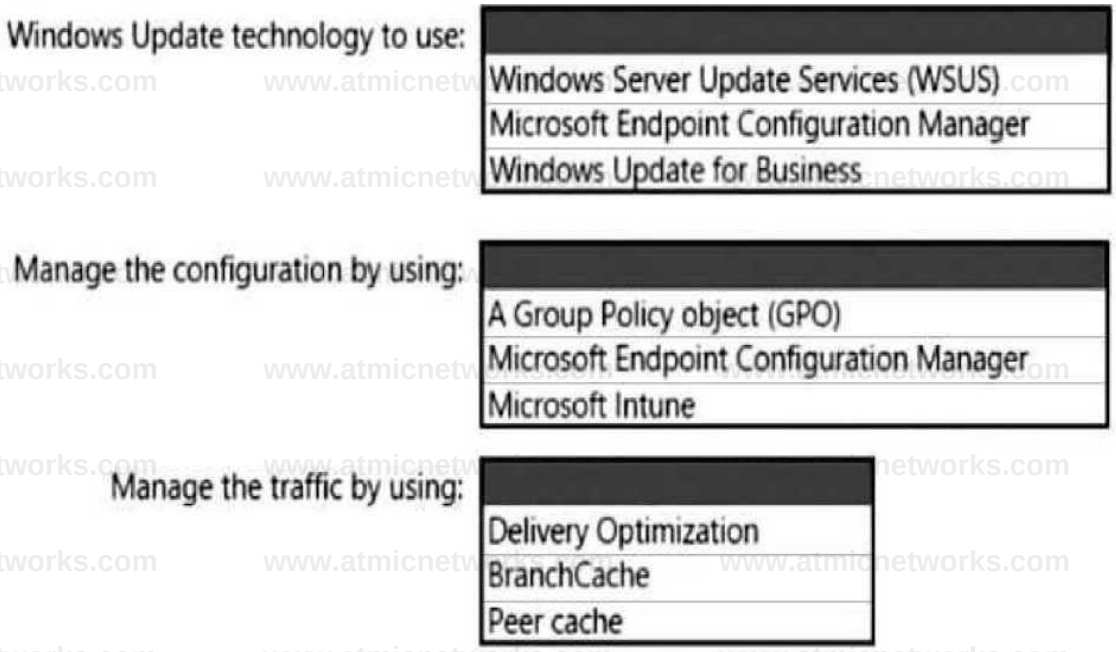
The computers have different update settings, and some computers are configured for manual updates.

You need to configure Windows Update. The solution must meet the following requirements:

The configuration must be managed from a central location.
Internet traffic must be minimized.
Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box 1: Windows Server Update Services (WSUS)
Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.

Windows Server Update Services is a built-in server role that includes the following enhancements: Can be added and removed by using the Server Manager
Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS Etc.

Box 2: A Group Policy object
In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).

Box 3: BranchCache
BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them. BranchCache has two operating modes: Distributed Cache mode and Hosted Cache mode.

Reference: https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache
https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update- services/deploy/4-configure-group-policy-settings-for-automatic-updates

Question: 60

You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:

- Allow downloads from the internet and from other computers on the local network.
- Limit the percentage of used bandwidth to 50.

What should you use?

A. a configuration profile
B. a Windows Update for Business Group Policy setting
C. a Microsoft Peer-to-Peer Networking Services Group Policy setting
D. an Update ring for Windows 10 and later profile

Answer: C

Explanation:

A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more. A configuration profile is a template that contains one or more settings that you can apply to groups of devices. Reference:

Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn Delivery Optimization settings in Microsoft Intune

Question: 61

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.

Name	Type	Location
Group!	Universal distribution group	Contoso.com
Group?	Global security group	Contoso.com
Group?	Group	Computeri
Group4	Group	Computer!

Which groups can you add to Group4?

A. Group2only
B. Group1 and Group2 only
C. Group2 and Group3 only
D. Group1, Group2, and Group3

Answer: C

Explanation:

Question: 62

DRAG DROP

You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:

- Requires BitLocker Drive Encryption (BitLocker) on each device
- Requires a minimum operating system version

Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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, Settings Answer Area

(ggHwith ~|
I Device Properties I
II
| Microsoft Defender for Endpoint | System Security

Requires Bitlocker |'
Requires a minimum operating system version: I

Answer:

Explanation:

Settings

| Device Health j
I Device Properties I
II
Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker. | System Security]
Requires a minimum operating system version: | Device Properties

Question: 64

DRAG DROP

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

Name	Type
Device"!	Windows 10
Devrce2	iOS
DevrceB	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system build can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting 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: 65

DRAG DROP

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

You plan to create and monitor the results of a compliance policy used to validate the BIOS version of 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

| Review the compliance dashboard for results.|

Create and assign a compliance policy (hat has System Security settings configured.

\ Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

Answer Area

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Answer:

Explanation:

Actions

2 Upload the PowerShell script to Intune.

j Upload the JSON file to Azure AD.

41 Create and assign a custom compliance policy.

Answer Area

Create a PowerShell discovery script and a JSON file.

Question: 66

DRAG DROP

You have a computer that runs Windows 10 and contains two local users named User! and User2.

You need to ensure that the users can perform the following anions:

- User 1 must be able to adjust the date and time.
- User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group 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.

Or men

AOnmums

t^m too A<B#n

Arrtwrwrrr: og Iran

[WKW

50km Maraged Accoumi Croup

Amer Area

UMtt: [ ]

VW/

Answer:

Explanation:

Groups

| Administrators |

I Event log Readers I

I1

| Performance Log Users

| Power Users

I System Managed Accounts Group

Answer Area

Useri: [Administrators

User?: | Event Log Readers

Question: 67

HOTSPOT

You have an Azure AD tenant named contoso.com. You have the devices shown in the following table.

Name	Platform
Devicel	Windows 1
Device 2	Windows 10
Devices	iOS
Device4	Ubuntu Linux

Which devices can be Azure AD joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area

Azure AD joined: | Device 1 and Dev»ce2 only
- **Device 1 only**
- **Device 1 and Device2 only**
- **Devicel and Device? only Devi cel. Device?, and Device? only Devicel, Device? Device?, and Device4**

Registered in contoso.com: | Devicel and Device? only ~
- **Devicel and Device? only**
- **Device? and Device? only**
- **Device? and Device4 only**
- **Device?. Device?, and Device4 only**
- **Devicel. Device?. Device?, and Device4**

Answer:

Explanation:

Answer Area

Azure AD joined: Devicel and Device? only

Registered in contoso.com: Devicel and Device? only

Question: 68

HOTSPOT

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

Name	Role
Admin 1 @>cont050.com	Secunty Administrator
Admin2@contoso.com	Cloud Device Administrator
Useri ©contoso.com	*None*

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator!	Network Configuration Operators
Administrators	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using user1@contoso.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	flies	No
Userl@contoso.com is a member of the local Administrators group on Computeri.		
Adminl@contoso.com can configure the firewall and Microsoft Defender on Cornputerl.		
Admin2@cgntpso,com an install software on Computer!.		

Answer:

Explanation:

Answer Area

Statements	flies	No
Userl @contoso.com is a member of the local Administrators group on Computeri.	O	*
Adminl@contoso.com can configure the firewall and Microsoft Defender on Cornputerl.	O	*
Admin2@contoso.com can install software on Computer!.	O	®

Question: 69

Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.

You enable Windows PowerShell remoting on the computers.

You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.

To which group should you add Admin1?

A. Access Control Assistance Operators
B. Remote Desktop Users
C. Power Users
D. Remote Management Users

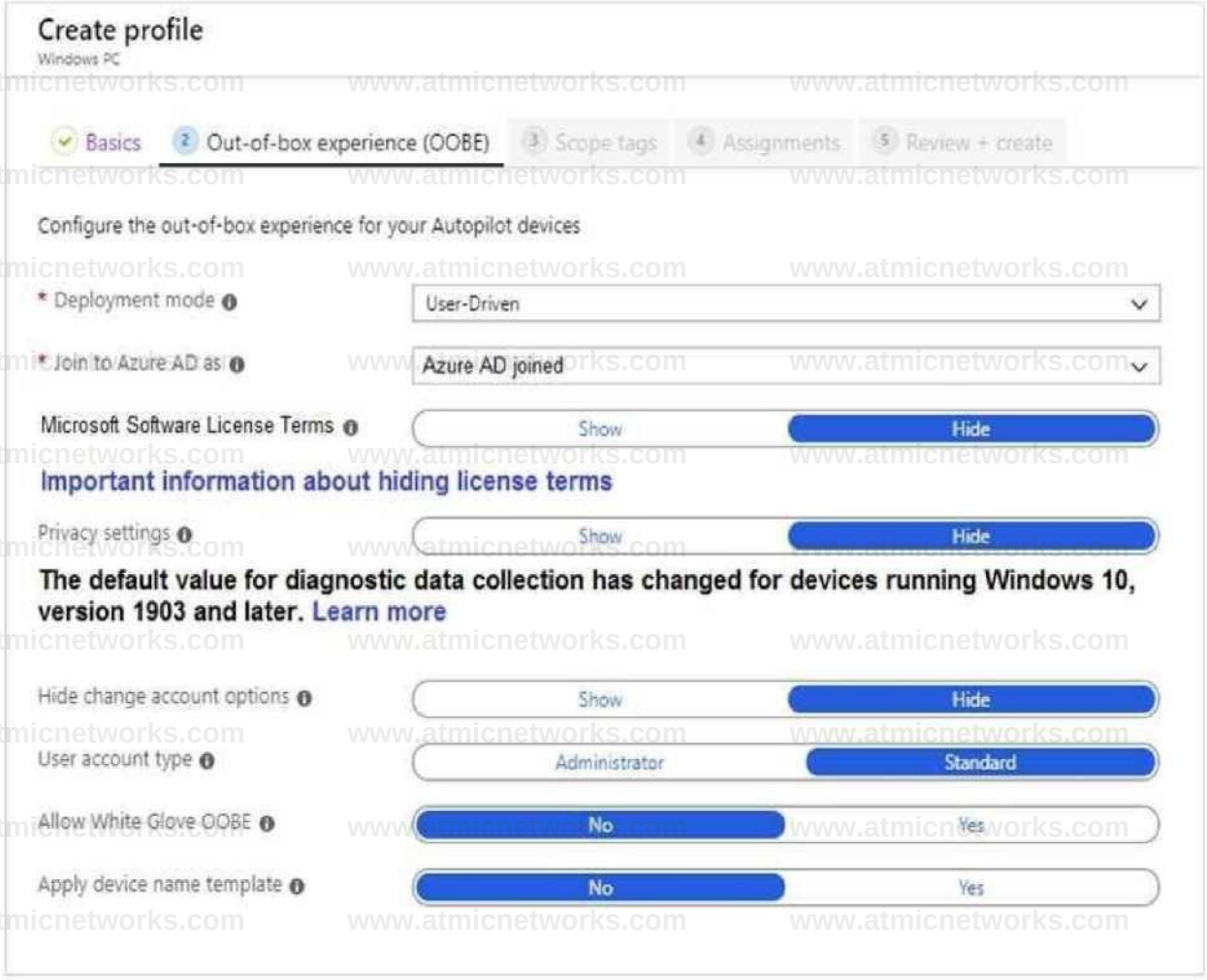
Answer: B

Explanation:

Question: 70

You have a Microsoft Intune subscription.

You are creating a Windows Autopilot deployment profile named Profile1 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.

Users who deploy a device by using Profile1 **[answer choice]**.

- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

Users can configure the **[answer choice]** during the deployment.

- computer name
- Cortana settings
- keyboard layout

Answer:

Explanation:

Users who deploy a device by using Profilel
[answer choice]

- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

Users can configure the [answer choice] during the deployment

- computer name
- Cortana settings
- keyboard layout

Question: 71

HOTSPOT

You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard.

You need to create a deployment share on Server1.

What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

On Serveri:

- Import the Deployment Image Servicing and Management (DISM) PowerShell module.
- Import the WindowsAutopilotIntune Windows PowerShell module.
- Install the Windows Assessment and Deployment Kit (Windows ADK).
- Install the Windows Deployment Services server role.

Add to the MDT deployment share:

- Windows 10 image and package only
- Windows 10 image and task sequence only
- Windows 10 image only
- Windows 10 image, task sequence, and package

Answer:

Explanation:

Box 1: Install the Windows Deployment Services role.

Install and initialize Windows Deployment Services (WDS)

On the server:

Open an elevated Windows PowerShell prompt and enter the following command:

Install-WindowsFeature -Name WDS -IncludeManagementTools

WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall"

WDSUTIL /Set-Server /AnswerClients:All

Box 2: Windows 10 image and task sequence only

Create the reference image task sequence

In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.

Reference: https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare- for-windows-deployment-with-mdt

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows- 10-reference-image

Question: 72

DRAG DROP

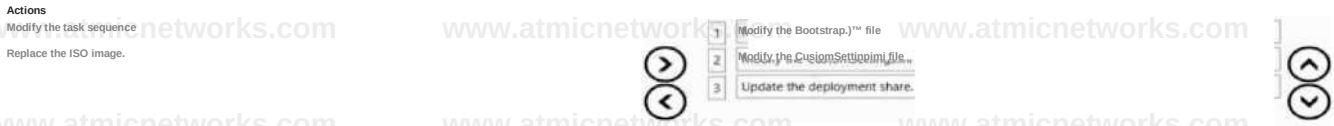
You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE_x64.Iso image and connect to MDT1. the welcome screen appears as shown In the following exhibit.

You need to prevent the welcome screen from appearing when the computers connect to MDT1. 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:



Box 1: Modify the Bootstrap.ini file.

Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:

SkipBDDWelcome=YES

Box 2: Modify the CustomSettings.ini file.

SkipBDDWelcome

Indicates whether the Welcome to Windows Deployment wizard page is skipped.

For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.

Box 3: Update the deployment share.

Reference: https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6- deployment-wizard-pages

Question: 75

HOTSPOT

Your network contains an Active Directory domain. The domain contains 1.000 computers that run Windows 11.

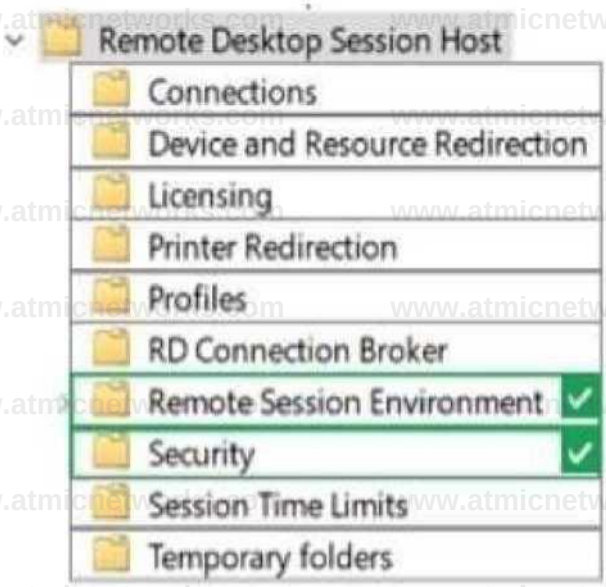
You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:

Prevent the sharing of clipboard contents.

- Ensure that users authenticate by using Network Level Authentication (NLA).

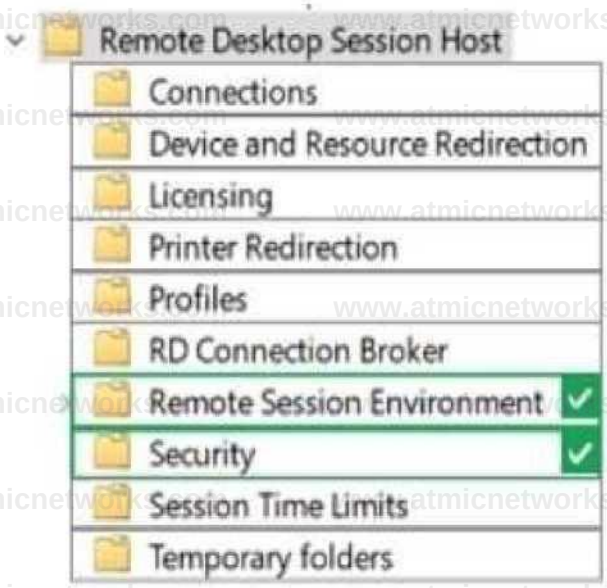
Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer are

a. NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 76

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device 1	64 bit version of Windows 10 Pro	Yes	No
Device?	32-bit version of Windows 10 Pro	No	Yes
DeviceB	64-bn version of Windows 10 Pro	No	Yes

You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11.

You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications. Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows Autopilot: | Pence! and Device3 only

None of the devices

Device! only

Device! and Device3 only

Device 1, Device2 and Device3

In-place upgrade: | Device! and Device3 only None of the devices Device! only

Device! and Device3 only

Device,. Device2. and Device3

Answer

Explanation:

Answer Area

Windows Autopilot Device! and Dev>ce3 only

In-place upgrade Device! and Device3 only

Question: 77

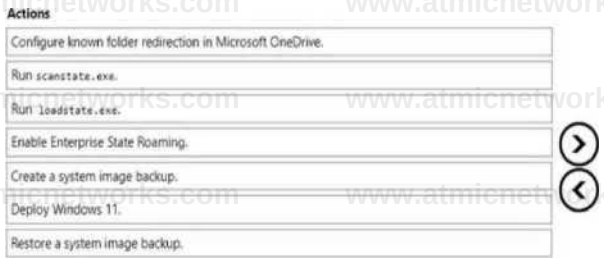
DRAG DROP

You have 100 computers that run Windows 10.

You plan to deploy Windows 11 to the computers by performing a wipe and load installation.

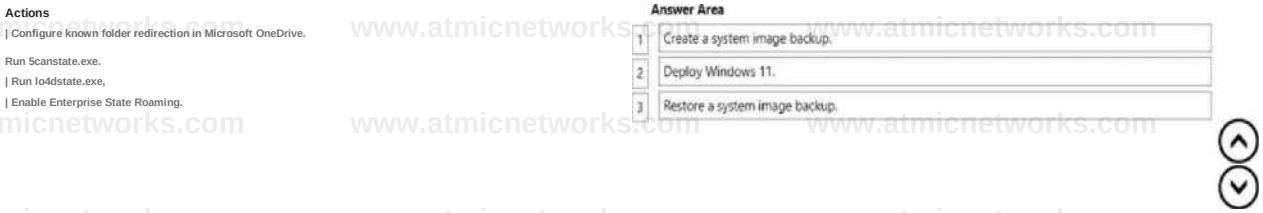
You need to recommend a method to retain the user settings and the user data.

Which three actions should you recommend be performed 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: 78

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

You use Microsoft Intune to manage devices.

You use Windows Autopilot to deploy Windows 11 to devices.

A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.

You need to ensure that when a deployment fails, the deployment logs can be collected.

What should you configure?

A. the automatic enrollment settings
B. the Windows Autopilot deployment profile
C. the enrollment status page (ESP) profile
D. the device configuration profile

Answer: B

Explanation:

Question: 79

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have a device named Device1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Deploy the Remote Help app to Device1.
B. Assign the Help Desk Operator role to User1.
C. Assign the Intune Administrator role to User1.
D. Assign a Microsoft 365 E5 license to User1.
E. Rerun device onboarding on Device1.
F. Assign the Remote Help add-on license to User1.

Answer: A, B, F

Explanation:

Question: 80

You have a Windows 11 capable device named Device1 that runs the 64-bit version of Windows 10 Enterprise and has Microsoft Office 2019 installed. You have the Windows 11 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

Which images can be used to perform an in-place upgrade of Device1?

A. image1 only
B. Image2only
C. Image1 and Image2

Answer: B

Explanation:

Question: 81

HOTSPOT

Your network contains an on-premises Active Directory Domain Services {AD DS) domain that syncs with an Azure AD tenant by using Azure AD Connect.

You use Microsoft Intune and Configuration Manager to manage devices.

You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:

- Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.
- Devices for The sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to The homes of the sales department users.
- Administrative effort must be minimized.

Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

Sales: | Windows Autopilot with automatic registration

Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

Marketing: Configuration Manager

Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

Answer:

Explanation:

Answer Area

Sales: Windows Autopilot with automatic regisiration

Marketing: Configuration Manager

Question: 82

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models. You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

A. Import an OS package.
B. Create a selection profile.
C. Add a Gather task to the task sequence.
D. Add a Validate task to the task sequence.

Answer: B

Explanation:

Question: 83

You have an on-premises server named Server! that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

A. Multipath I/O (MPIO)
B. Multipoint Connector
C. Windows Deployment Services (WDS)
D. Windows Server Update Services (WSUS)

Answer: C

Explanation:

Question: 84

Your company standardizes on Windows 10 Enterprise for all users.

Some users purchase their own computer from a retail store. The computers run Windows 10 Pro. You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps. The solution must meet the following requirements:

- Ensure that any applications installed by the users are retained.
- Minimize user intervention.

What is the best recommendation to achieve the goal?

More than one answer choice may achieve the goal.

Select the BEST answer.

A. Windows Autopilot
B. Microsoft Deployment Toolkit (MDT)
C. a Windows Configuration Designer provisioning package
D. Windows Deployment Services (WDS)

Answer: A

Explanation:

Question: 85

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 86

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 87

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 88

HOTSPOT
You have an Azure AD tenant that contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Enabled

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

You have a Conditional Access policy named CAPolicy1 that has the following settings:

- Assignments
  - o Users or workload identities: User 1. User1
  - o Cloud apps or actions: Office 365 Exchange Online
  - o Conditions: Device platforms: Windows, iOS
- Access controls
  - o Grant Require multi-factor authentication

You have a Conditional Access policy named CAPolicy2 that has the following settings: Assignments

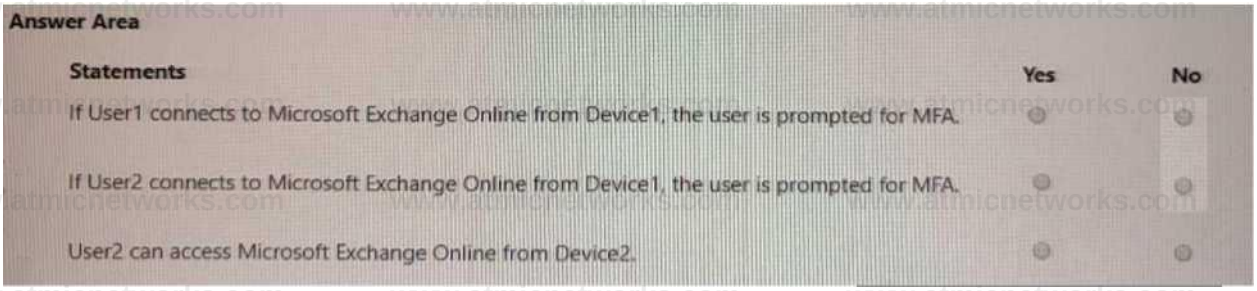
o Users or workload identities: Used, User2

o Cloud apps or actions: Office 365 Exch

o Conditions

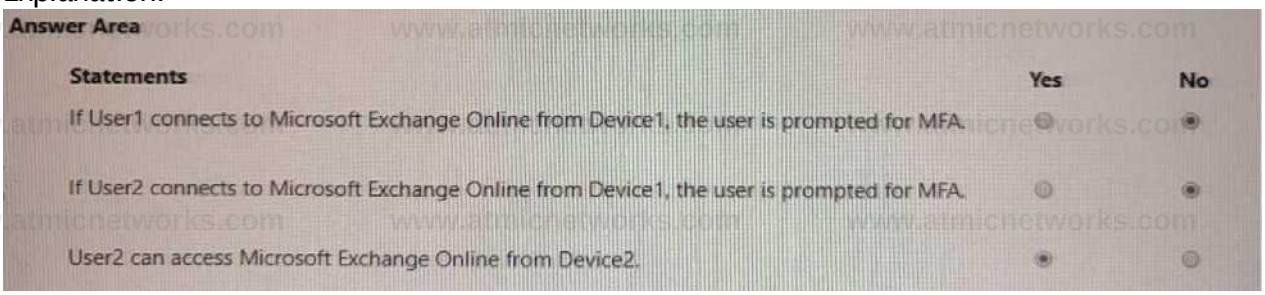
- Device platforms: Android, iOS
- Filter for devices
- Device matching the rule: Exclude filtered devices from policy
- Rule syntax: device. displayName- contains "1"
- Access controls
- Grant Block access

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



Answer:

Explanation:



Question: 89

HOTSPOT

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

Name	Platform
Devicel	Windows 10
Device?	iOS

You plan to enroll the devices in Microsoft Intune.

How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Devicel:

Evey 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Device2:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Answer:

Explanation:

Box 1: Every three minutes for 15 minutes, then every 15 minutes for two hours, and then around every eight hours

If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:

Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Platform	Frequency
iOS/iPadOS	Every 15 minutes for 1 hour, and then around every 8 hours
macOS	Every 15 minutes for 1 hour, and then around every 8 hours
Android	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 10/11 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 8.1	Every 5 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Box 2: Every 15 minutes for one hour, and then every eight hours
iOS/iPadOS: Every 15 minutes for 1 hour, and then around every 8 hours

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

Question: 90

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.

You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.

What should you do?

A. From the Microsoft Endpoint Manager admin center, create a configuration profile.
B. From the Microsoft Endpoint Manager admin center, create a security baseline.
C. Onboard the macOS devices to the Microsoft 365 compliance center.
D. Install Defender for Endpoint on the macOS devices.

Answer: D

Explanation:

Just install, and use Defender for Endpoint on Mac.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft- defender-endpoint-mac

Question: 91

HOTSPOT

You have the on-premises servers shown in the following table.

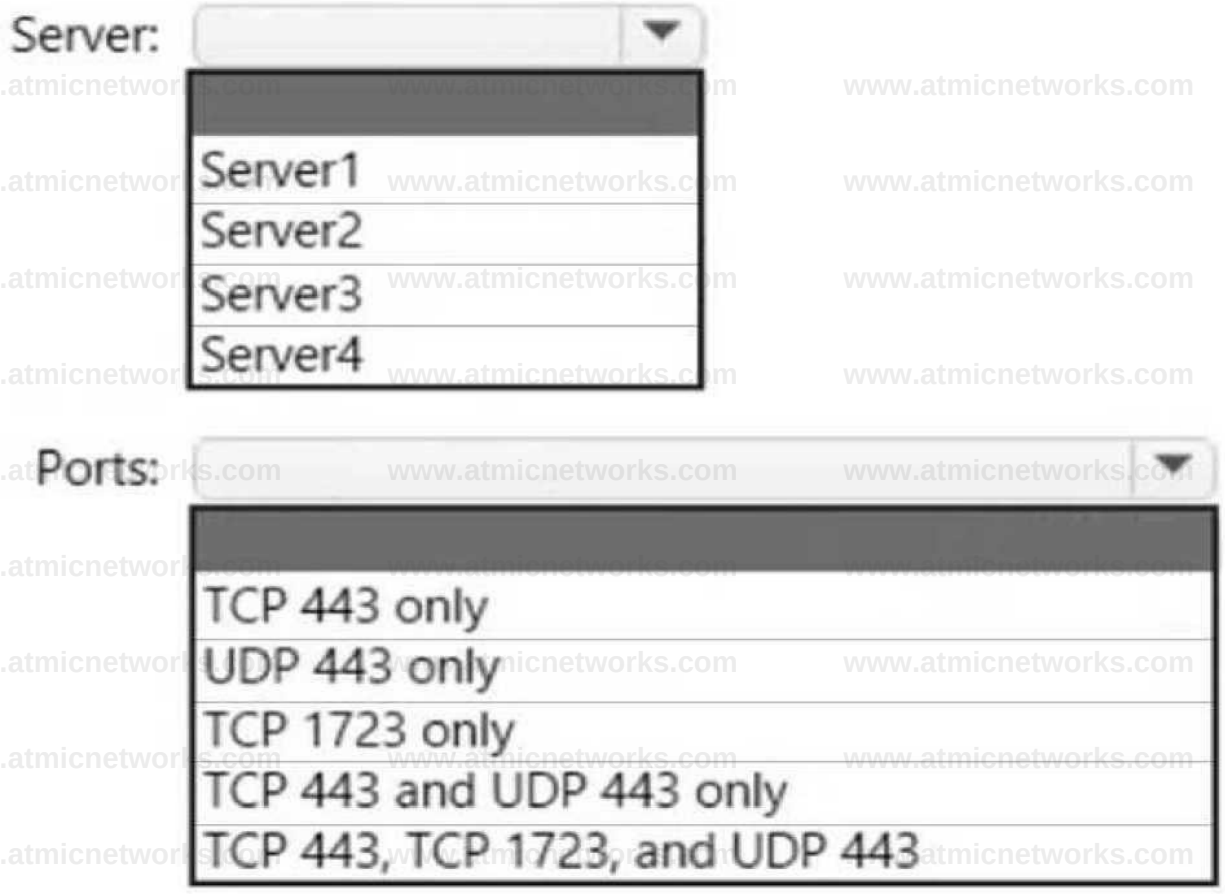
Name	Description
DC1	Domain controller that runs Windows Server 2022
Serveri	Standalone server that runs Windows Server 2022
Server2	Member server that runs Windows Server 2022 and has the Remote Access role installed
Server3	Member server that runs Windows Server 2019
Server4	Red Hat Enterprise Linux (RHEL) 8.4 server

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.

You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.

To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box 1: Server4

Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.

Box 2: TCP 443 and UDP 443 only

Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.

By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Saerver Configuration – Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.

Incorrect:

TCP 1723 is not used.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-overview

Question: 92

HOTSPOT

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
Useri	Groupl	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

MDM user scope: Group1
MAM user scope: Group2

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

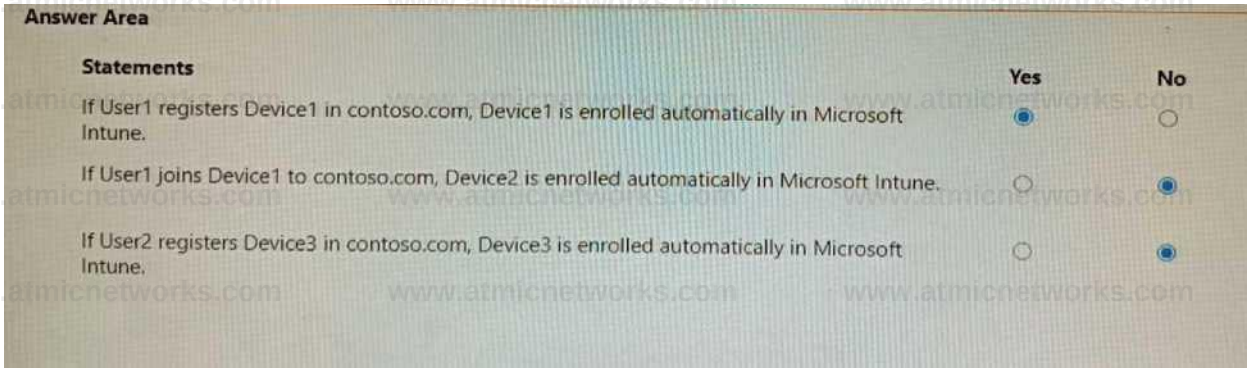
NOTE: Each correct selection is worth one point.

Answer Area

Statements	ye.
If Useri registers Device 1 in contoso.com, Device 1 is enrolled automatically in Microsoft Intune.	
If Useri joins Device 1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	
If User2 registers Device3 incontoso.com, Devices is enrolled automatically in Microsoft Intune.	

Answer:

Explanation:



Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll
https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/

Question: 93

Your company has devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

In Microsoft Endpoint Manager, you define the company's network as a location named Location1.

Which devices can use network location-based compliance policies?

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

Answer: E

Explanation:

Intune supported operating systems
Intune supports devices running the following operating systems (OS):

iOS
Android
Windows
macOS

Note: View the device compliance settings for the different device platforms:

Android device administrator
Android Enterprise
iOS
macOS
Windows Holographic for Business
Windows 8.1 and later
Windows 10/11

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

Question: 94

You use Microsoft Intune and Intune Data Warehouse.

You need to create a device inventory report that includes the data stored in the data warehouse.

What should you use to create the report?

A. the Azure portal app
B. Endpoint analytics
C. the Company Portal app
D. Microsoft Power BI

Answer: D

Explanation:

You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune

tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:

Devices
Enrollment
App protection policy
Compliance policy
Device configuration profiles
Software updates
Device inventory logs

Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.
Sign in to the Microsoft Endpoint Manager admin center.
Select Reports > Intune Data warehouse > Data warehouse.
Retrieve the custom feed URL from the reporting blade, for example:
https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api-version=v1.0
Open Power BI Desktop.
Choose File > Get Data. Select OData feed.
Choose Basic.
Type or paste the OData URL into the URL box.
Select OK.
If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials.
To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
Select Organizational account.
Type your username and password.
Select Sign In.
Select Connect.
Select Load.

Reference: https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

Question: 95

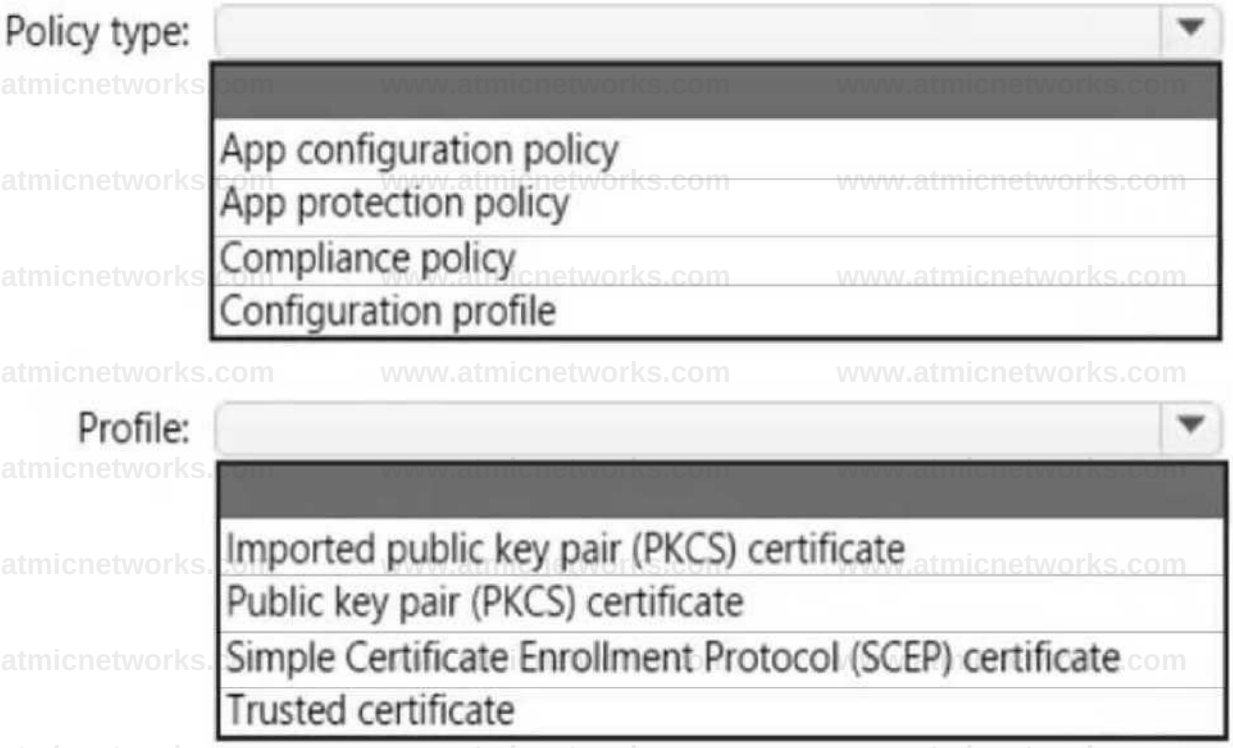
HOTSPOT

You have a Microsoft 365 tenant and an internal certification authority (CA).

You need to use Microsoft Intune to deploy the root CA certificate to managed devices.

Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box 1: Configuration profile
Create a trusted certificate profile.

Box 2: Trusted certificate
When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root

Question: 96

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

Name	Description
Groupl	Azure AD group that contains a user named Userl
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS devices. You assign CAPolicy1 to Group1.

You discover that User1 can still connect to Exchange Online from an iOS device.

You need to ensure that CAPolicy1 is enforced.

What should you do?

A. Configure a new terms of use (TOU).
B. Assign CAPolicy1 to Group2.
C. Enable CAPolicy1
D. Add a condition in CAPolicy1 to filter for devices.

Answer: B

Explanation:

Common signals that Conditional Access can take in to account when making a policy decision include the following signals:

* User or group membership
Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
* Device
Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
Use filters for devices to target policies to specific devices like privileged access workstations.
* Etc.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

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.

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.

Computer1 has apps that are compatible with Windows 10.

You need to perform a Windows 10 in-place upgrade on Computer1.

Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment share. You create a task sequence, and then you run the MDT deployment wizard on

Computer1.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 98

You have a Microsoft 365 E5 subscription that contains a group named Group1.

You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.

You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.

What should you configure?

A. Session access controls
B. an assignment that uses a User risk condition
C. an assignment that uses a Sign-in risk condition
D. Grant access controls

Answer: A

Explanation:

User sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.

Sign-in frequency control

Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.

Browse to Azure Active Directory > Security > Conditional Access.

Select New policy.

Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Choose all required conditions for customer's environment, including the target cloud apps.

Under Access controls > Session.

Select Sign-in frequency.

Choose Periodic reauthentication and enter a value of hours or days or select Every time.

Save your policy.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto- conditional-access-session-lifetime

Question: 99

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.

You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released.

What should you create?

A. a device configuration profile based on the Device features template
B. a device configuration profile based on the Device restrictions template
C. an update policy for iOS/iPadOS
D. an iOS app provisioning profile

Answer: C

Explanation:

Manage iOS/iPadOS software update policies in Intune, delay visibility of software updates.

When you use update policies for iOS, you might have need to delay visibility of an iOS software update.

Reasons to delay visibility include:

Prevent users from updating the OS manually

To deploy an older update while preventing users from installing a more recent one

To delay visibility, deploy a device restriction template that configures the following settings:

Defer software updates = Yes

This doesn't affect any scheduled updates. It represents days before software updates are visible to end users after release.

Delay default visibility of software updates = 1 to 90

90 days is the maximum delay that Apple supports.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/software-updates-ios

Question: 100

You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in

Microsoft Intune.

You plan to integrate Intune with Microsoft Defender for Endpoint.

You need to establish a service-to-service connection between Intune and Defender for Endpoint.

Which settings should you configure in the Microsoft Endpoint Manager admin center?

A. Connectors and tokens
B. Premium add-ons
C. Microsoft Tunnel Gateway
D. Tenant enrollment

Answer: A

Explanation:

Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure Right Now.

As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.

Reference: https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/

Question: 101

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Endpoint analytics.

You need to create baseline metrics.

What should you do first?

A. Create an Azure Monitor workbook.
B. Onboard 10 devices to Endpoint analytics.
C. Create a Log Analytics workspace.
D. Modify the Baseline regression threshold.

Answer: C

Explanation:

Onboarding from the Endpoint analytics portal is required for Intune managed devices.

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

Question: 102

DRAG DROP

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting 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.

Settings

Recuire Bit Locker.

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

Answer Area

Device1: Setting

Device2: Setting

Device3: Setting

Answer:

Explanation:

Box 1:

Device Compliance settings for Windows 10/11 in Intune

There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.

Note: Windows Health Attestation Service evaluation rules

Require BitLocker:

Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user dat

a. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.

Box 2: Prevent jailbroken devices from having corporate access

Device Compliance settings for iOS/iPadOS in Intune

There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.

Device Health

Jailbroken devices

Supported for iOS 8.0 and later

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Block - Mark rooted (jailbroken) devices as not compliant.

Box 3: Prevent rooted devices from having corporate access.

Device compliance settings for Android Enterprise in Intune

There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.

Device Health - for Personally-Owned Work Profile

Rooted devices

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Block - Mark rooted devices as not compliant.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create- windows
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios

Question: 103

HOTSPOT

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

You need to perform the following tasks for User1:

Set the Usage location to Canada.
Configure the Phone and Email authentication contact info for self-service password reset (SSPR).

Which two settings should you configure in the Azure Active Directory admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Manage

Question: 104

You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune.

You need to review the startup processes and how often each device restarts.

What should you use?

A. Endpoint analytics
B. Intune Data Warehouse
C. Azure Monitor
D. Device Management

Answer: B

Explanation:

Question: 105

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

Name	Role
Admml	Application admin
Admin2	Cloud application admin
Admin3	Office apps admin
Admin4	Security admin

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization.

Which users can download the Office customization file from the admin center?

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

Answer: B

Explanation:

* Admin1

An application admin has full access to enterprise applications, applications registrations, and application proxy settings.

* Admin2

Mark your app as publisher verified.

In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.

* Admin3

Office Apps admin - Assign the Office Apps admin role to users who need to do the following:

- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health

Reference:

Office Apps admin - Assign the Office Apps admin role to users who need to do the following

https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified

Question: 106

HOTSPOT

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android devices named Policy1 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.

To apply Policy) to an Android device, you must **[answer choice] l**

install the Company Portal app on the device _____ install the Microsoft Authenticator app on the device onboard the device to Microsoft Defender for Endpoint onboard the device to the Microsoft 365 compliance center

When Policy 1 is assigned, the policy will apply to **[answer choice]. l**

users onty _____ devices only _____
users and devices

Answer:

Explanation:

Box 1: Install the Intune Company Portal app on the device

On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.

Bix 2: Devices only

For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.

Reference: https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipados-and-android-apps

Question: 107

You have a Microsoft 365 E5 subscription.

You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.

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

A. Apps. and then App protection policies
B. Apps. and then Monitor
C. Devices, and then Monitor
D. Reports, and the Device compliance

Answer: A

Explanation:

App report: You can search by platform and app, and then this report will provide two different app protection statuses that you can select before generating the report. The statuses can be Protected or Unprotected.

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

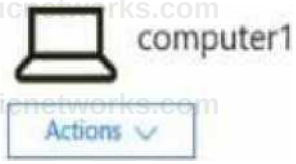
Question: 108

HOTSPOT

Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Name	Members
	Group 1	tag E Ovals dMO and OS In windows 10
	Groups	tag finals dew
3	Group?	Donate Equals *d*tua.coa
4	Group4	Domain Equals adatw».co« And OS In Windows 10
5	Groups	'J&ne starts with COT
Last	Ungrouped devices (default)	Mot *applicable*

You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.



Don¹ am aUatjm.com
OS Window! CW-bit (Budd 17T34)
Machine IP addresses >

What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Computed will be a member of: Groups only

Groups only
Group4 only Groups only Groups,
Group4, and Groups only

if you add me tag demo to Computer! Computer! will be a Group I only member of:

Group! only
Group2 only
Group! and Groups only
Group!. Groups, Groups, Group*. and Group?

Answer:

Explanation:

Answer Area

Computer! will be a member ot Groups only

it you add the tag demo to Computer!. Computer! will be a member of: Group! only

Question: 109

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.

You need to perform a Windows 10 in-place upgrade on Computer1.

Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 110

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

You are creating a compliance policy named Compliance1.

Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

A. Group3 and Group4 only
B. Group3, Group4, and Admin1 only
C. Group1, Group2, and Group3 only
D. Group1, Group2, Group3, and Group4 only
E. Group1, Group2, Group3, Group4, and Admin1

Answer: C

Explanation:

Reference:
https://www.ravenswoodtechnology.com/microsoft-intune-compliance-notifications/

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

Question: 111

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1 @contoso.com.

You join a Windows 10 device named Client1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

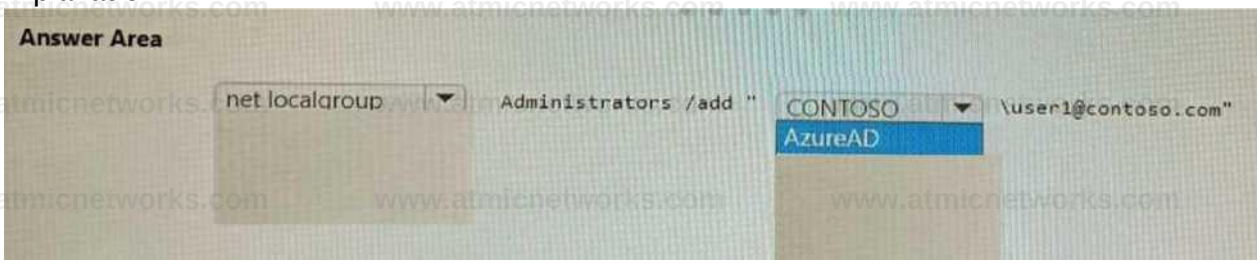
How should you complete the command? To answer, select the appropriate options in the answer

area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:



Question: 112

You have a Microsoft 365 subscription.
You need provide a user the ability to disable Security defaults and principle of least privilege.
Which role should you assign to the user?

A. Global Administrator
B. Conditional Access Administrator
C. Security Administrator
D. Intune Administrator

Answer: B

Explanation:

To enable or disable security defaults in your directory, sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.

Note: Conditional Access Administrator
Users with this role have the ability to manage Azure Active Directory Conditional Access settings.

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

Question: 113

HOTSPOT

In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 and later	Require	*Not applicable*	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

The Intune compliance policy settings are configured as shown in the following exhibit.

151 Save X Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as O

Answer Area

Compliant Not Compliant

Enhanced jailbreak detection Q

Enabled Disabled

Compliance status validity period (days) ⓘ

30

On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	Group2

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

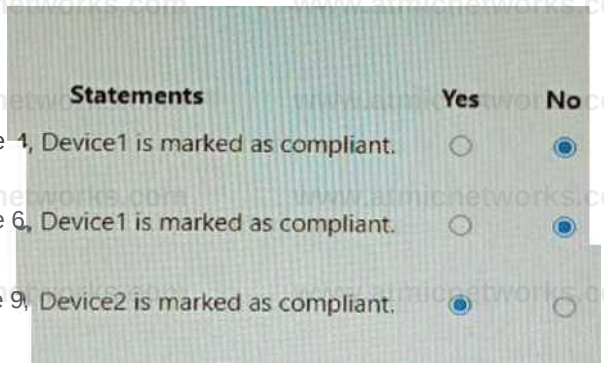
NOTE: Each correct selection is worth one

Statements	Yes	No
On June 4, Devicel is marked as compliant.		
On June 6, Devicel is marked as compliant.	O	( )
On June 9, Device2 is marked as compliant.	O	O

Answer:

Explanation:

Answer Area



Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO.
Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until june 10th.

Source:
Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.

When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.

This action is supported on all platforms supported by Intune.
https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

Question: 114

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices that run Windows 11.
User1 provides remote support for 75 devices in the marketing department.
You need to add User1 to the Remote Desktop Users group on each marketing department device.
What should you configure?

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

Answer: D

Explanation:

Question: 115

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to deploy and manage Windows devices.
You have 100 devices from users that left your company.
You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

A. Deploy a new configuration profile to the devices.
B. Perform a Windows Autopilot reset on the devices.
C. Perform an in-place upgrade on the devices.
D. Perform a clean installation of Windows 11 on the devices.

Answer: B

Explanation:

Question: 116

HOTSPOT

You create a Windows Autopilot deployment profile.

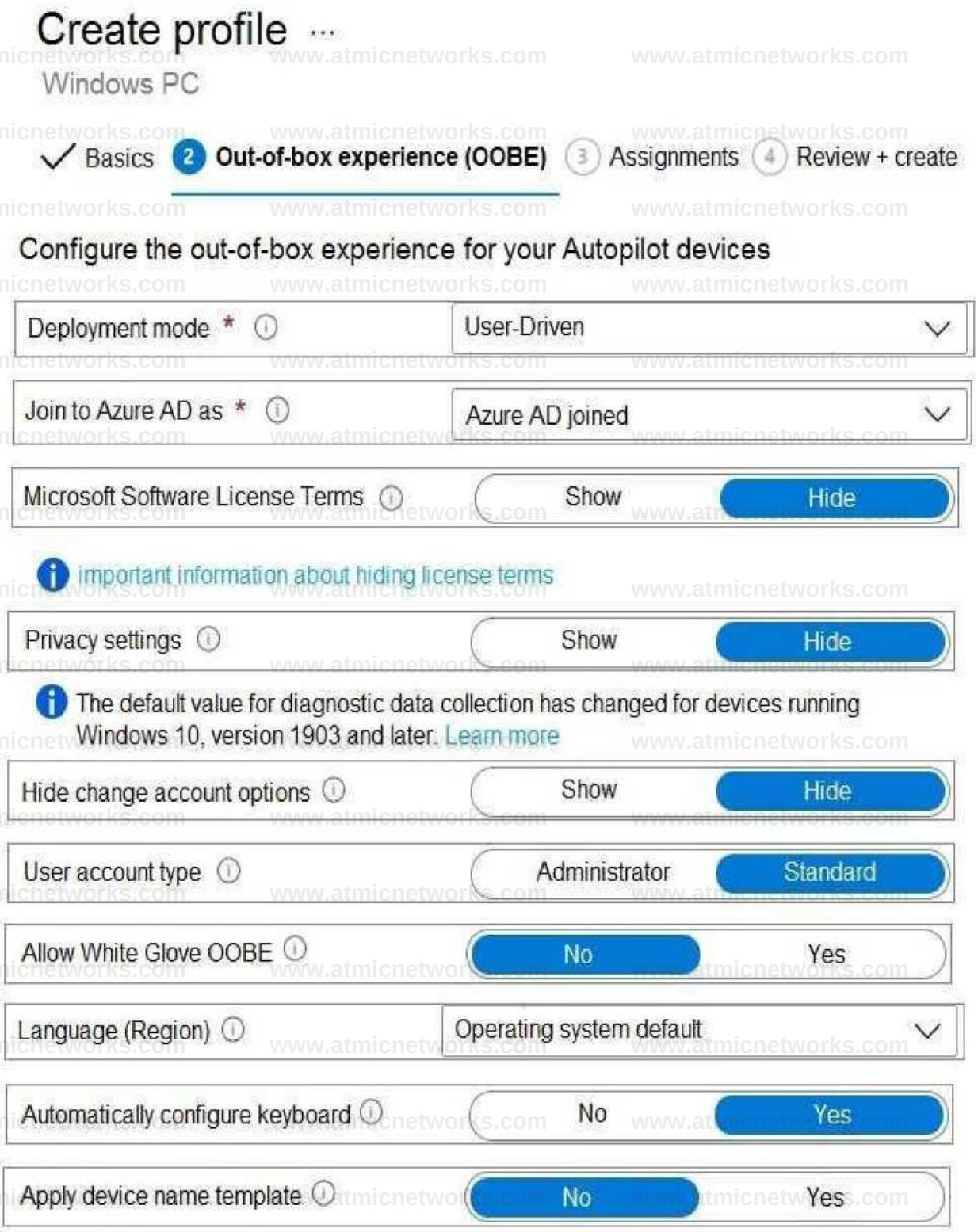
You need to configure the profile settings to meet the following requirements:

Automatically enroll new devices and provision system apps without requiring end-user authentication.
Include the hardware serial number in the computer name.

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

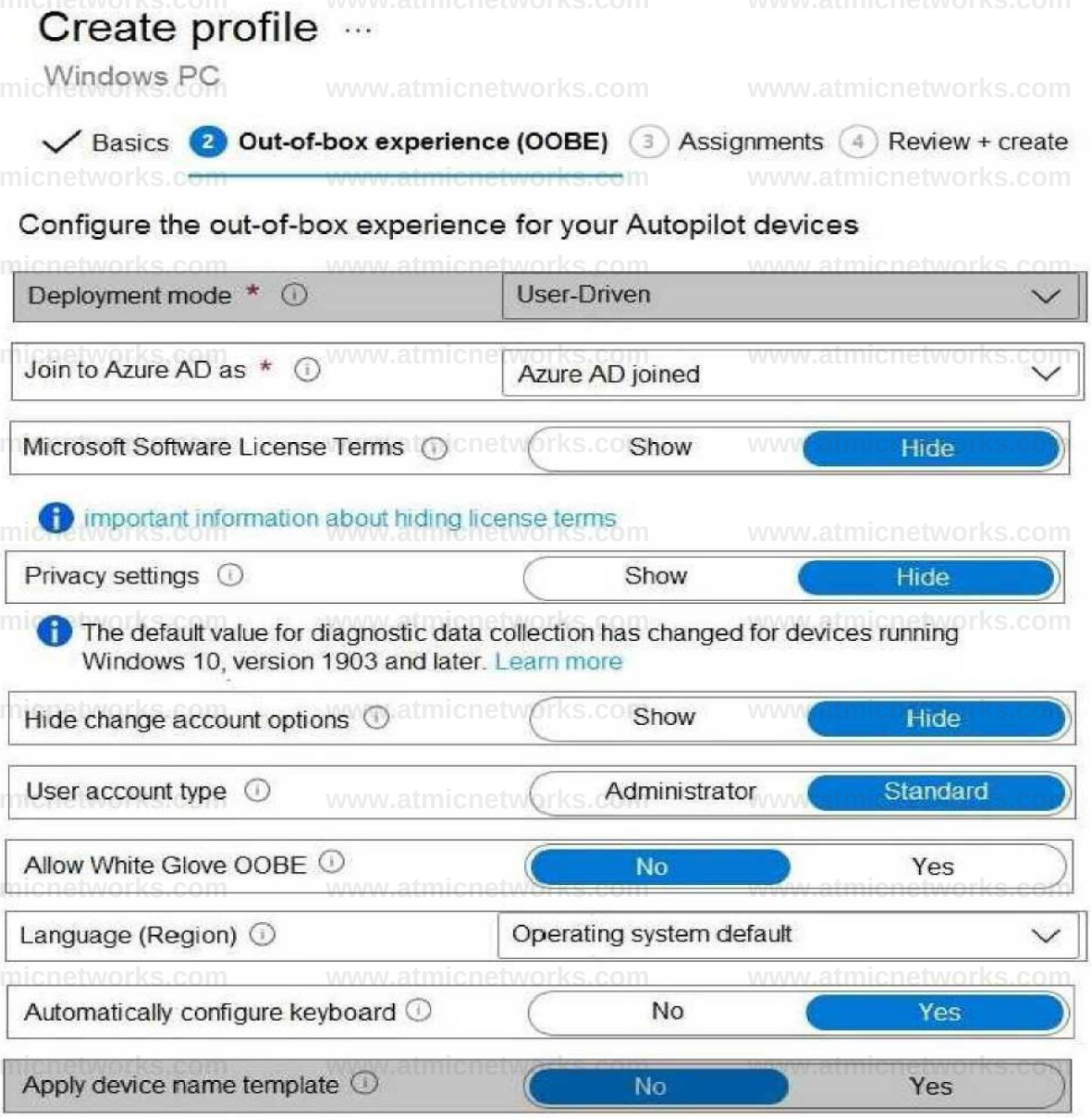
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/autopilot/profiles

Question: 117

You have a computer named Computer! that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.

What should you do on Computer1?

A. Turn on Reputation-based protection.
B. Enable Network Level Authentication (NLA).
C. Turn on Network Discovery.
D. Configure the Remote Desktop Configuration service.

Answer: B

Explanation:

Question: 118

You have a Hyper-V host that contains the virtual machines shown in the following table.

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

A. VM1 only
B. VM3only
C. VM1 and VM2 only
D. VM2 and VM3 only
E. VM1, VM2, and VM3

Answer: E

Explanation:

Question: 119

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You have the devices shown in the following table.

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

A. Device3 only
B. Device2 and Device3 only

C. Device 1 and Device2 only

D. Device1, Device2, and Device3

Answer: A

Explanation:

Question: 120

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Devicel	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

You add an Autopilot deployment profile as shown in the following exhibit.

Create profile

Windows PC

Basics O Out-of-box experience (OOBE) ^^ Assignments O Review

Summary

Basics

Name	Profilel
Description	—
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	No

Assignments

Included groups	Groupl
Excluded groups	Group2

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

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device 1	No	Joined	No
Device?	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.

Answer Area

Statements	Yes	No
If you reset Device1, the device will be deployed by using Autopilot.	○	○
If you reset Device2, the device will be deployed by using Autopilot.	○	○
If you restart Device3, the device will be deployed by using Autopilot.	○	○

Answer:

Explanation:

Answer Area

Statements	Yes	No
If you reset Devicel, the device will be deployed by using Autopilot,	O	®
If you reset Devices, the device will be deployed by using Autopilot.		®
If you restart Device3, the device will be deployed by using Autopilot.		

Question: 121

HOTSPOT

Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. Remote Desktop is enabled on Computer2.

The domain contains the user accounts shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.

Name	Members
Group1	ADATUM\User2 ADATUM\User3
Group2	ADATUM\User2
Group3	ADATUM\User3
Administrators	ADATUM\Domain Admins ADATUM\User3
Remote Desktop Users	Group1

The relevant user rights assignments for Computed are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	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
User! can establish a Remote Desktop session to Computed.		
User2 can establish a Remote Desktop session to Computers.		
User3 can establish a Remote Desktop session to Computers.		

Answer:

Explanation:

Question: 122

You have two computers named Computer1 and Computed that run Windows 10. Computed has Remote Desktop enabled.
From Computer1, you connect to Computer2 by using Remote Desktop Connection.
You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.
What should you do?

A. From Computer 2, configure the Remote Desktop settings.
B. From Windows Defender Firewall on Computer 1, allow Remote Desktop.
C. From Windows Defender Firewall on Computer 2, allow File and Printer Sharing.
D. From Computer1, configure the Remote Desktop Connection settings.

Answer: D

Explanation:

Question: 123

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

- Install Windows 11 Enterprise on each device.
- Install a Windows Installer (MSI) package named App1 on each device.
- Add a certificate named Certificate1 that is required by App1.
- Join each device to Azure AD.

Which three provisioning options can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. subscription activation
B. a custom Windows image
C. an in-place upgrade
D. Windows Autopilot
E. provisioning packages

Answer: B, D, E

Explanation:

Question: 124

DRAG DROP

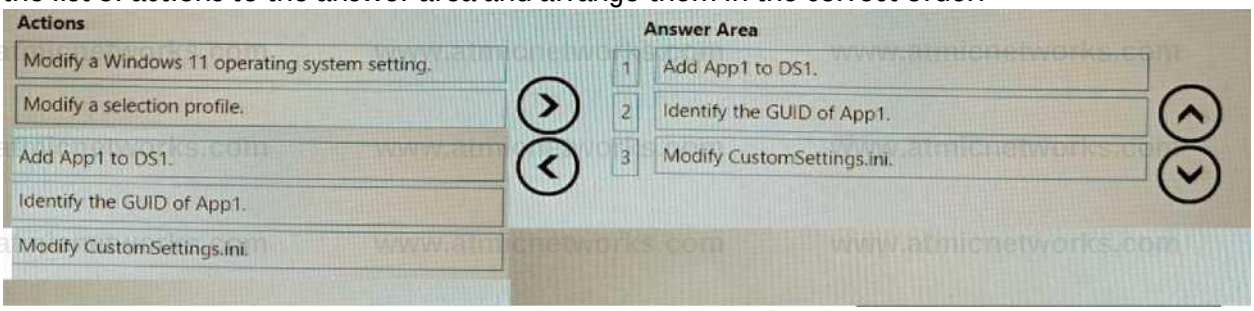
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

You import a Windows 11 image to DS1.

You have an executable installer for an application named App1.

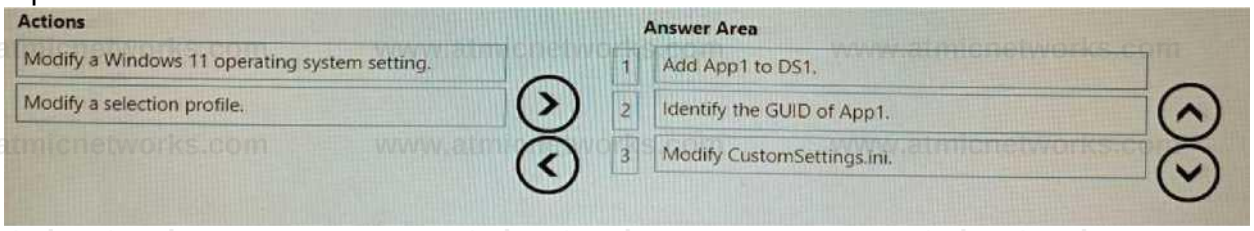
You need to ensure that App1 will be installed for all the task sequences that deploy the image.

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:



MDT is a tool that allows you to automate the deployment of Windows operating systems and applications. To install an application for all the task sequences that deploy a Windows 11 image, you need to perform the following three actions in sequence:

Add App1 to DS1. You can use the Deployment Workbench to import the executable installer of App1 to a folder in your deployment share. This will create an application entry with a unique GUID that identifies App11.
Identify the GUID of App1. You can find the GUID of App1 by opening the application properties in the Deployment Workbench and looking at the Application GUID field1. You can copy the GUID to use it later.
Modify CustomSettings.ini. You can edit the CustomSettings.ini file in your deployment share to specify which applications to install for each task sequence. You can use the Applications property to list the GUIDs of the applications you want to install, separated by commas1. For example, if you want to install App1 and another application with GUID {1234-5678-90AB-CDEF}, you can use this line:
Applications={GUID of App1},{1234-5678-90AB-CDEF}
These are the three actions you need to perform to ensure that App1 will be installed for all the task sequences that deploy the Windows 11 image from DS1. I hope this helps you.
If you want to learn more about MDT and how to deploy applications with it, you can check out these resources:
Get started with the Microsoft Deployment Toolkit (MDT) (Windows 10)
How to deploy applications with the Microsoft Deployment Toolkit

Question: 125

HOTSPOT
You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.

MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

You use Distributed File System (DFS) Replication to replicate images in a share named Production.
You configure the following settings in the Bootstrap.ini file.

```
[Settings]
Priority-DefaultGateway, Default
[DefaultGateway]
10.1.1.l«NewYork
10.5.5.l»London

[NewYork]
DeployRoot-\\MDTl\Production$

[NewYork]
DeployRoot-\\MDTl\Production$

[London]
DeployRoot=\\MDT2\Production$
KeyboardLocale=en-gb
[Default]
DeployRoot-\\HDT3\Production$
KeyboardLocale=en-us
```

You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

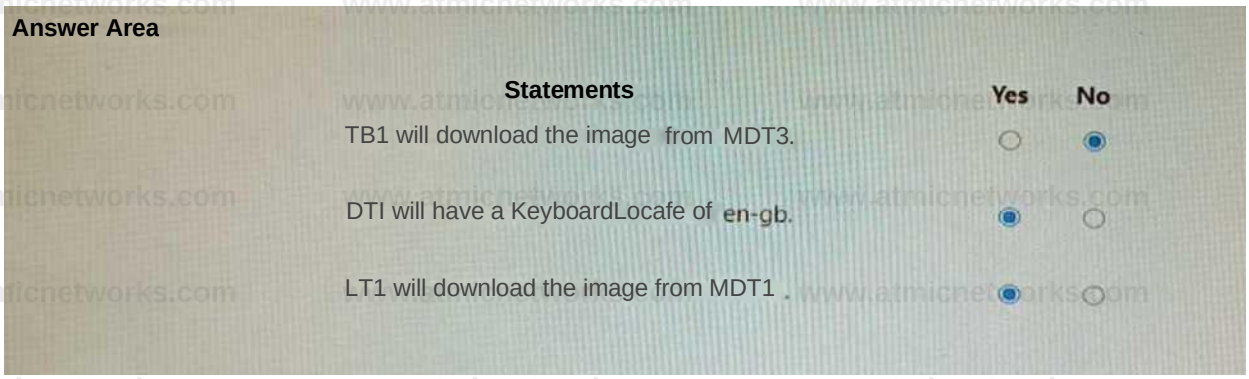
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
TB1 will download the innage from MDT3.	○	○
DTI will have a KeyboardLocale of en-gb.	○	○
LT1 will download the image from MDT1.	○	○

Answer:

Explanation:



Question: 126

HOTSPOT

You have the devices shown in the following table.

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Seryer1 during the migration.

Which command should you run on each device? To answer, select the appropriate options in the answer area.

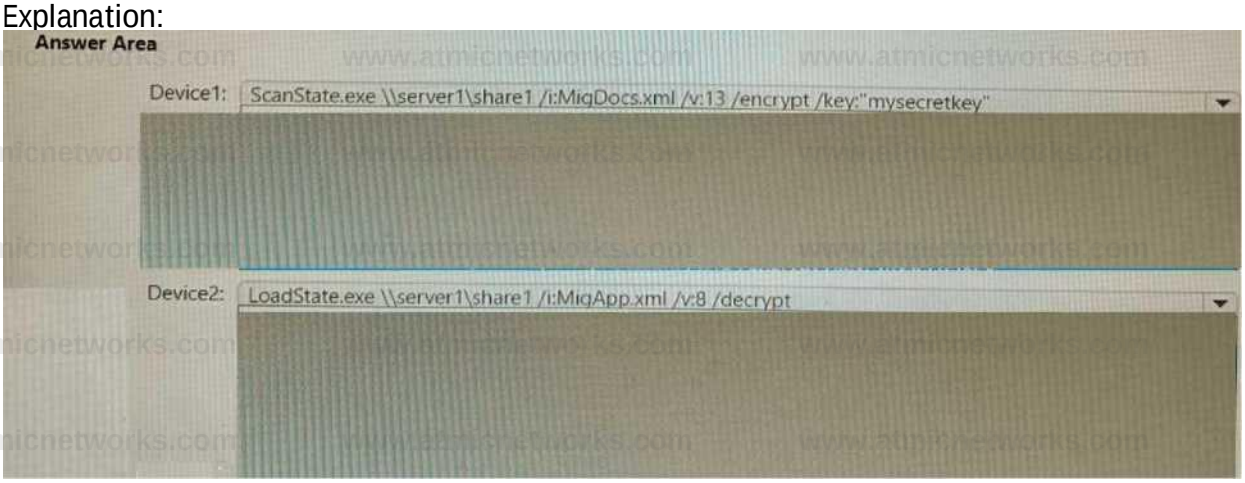
NOTE: Each correct selection is worth one point.

Answer Area

Devicel: ScanState.exe \\server1\$hare1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
LoadState.exe \\server1\sliare1 /i:MtgApp.xml /v:13 /decrypt /key:"mysecretkey"
Device2: LoadState.exe \\server1\share1 /LMigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 ZhMigPocs.xml /v:13 /decrypt /key: ntysecretkey
ScanState.exe \\server1\share1 /kMigApp.xml /config:Config.xml /v: 13 /encrypt /key:"mysecretkey"
ScanState.exe \\server1\share1 /i:MigApp.xml/config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xm| /v:13
Device2: LoadState.exe \\server1\share1 /i:MigApp,xml /v:8 /decrypt .....
| LoadState.exe Wseiver1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretkev"
LoadState.exe \\server1\share1 /cMigApp.xmi /v:8 /decrypt
LoadState.exe Wserver1\share1 /i:MigD©cs.xml /v:13 /decrypt /key: mysecretkey"
ScanState.exe \\server1\sharet /i:MigApp.xinl /config;Config.xml /v:13 /encrypt /key:'mysecretkey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
SeanStatoexe \Wprvbr-|\sJtare1 /i:lyfigDocs.xrrd/v:13 /encrypt /key: mysecretkey"

Answer:

Explanation:



Question: 127

You have a Microsoft 365 subscription.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to configure the Out-of-box experience (OOBE) settings. What should you create in the Microsoft Intune admin center?

A. an enrollment status page (ESP)
B. a deployment profile
C. a compliance policy
D. a PowerShell script
E. a configuration profile

Answer: B

Explanation:

Question: 128

You have an Azure AD tenant that contains the devices shown in the following table.
You purchase Windows 11 Enterprise E5 licenses.
Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

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

Answer: B

Explanation:

Question: 129

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You add apps to Intune as shown in the following table.

Name	App type
App1	Android store app
App2	Android line-of-business app
App3	Managed Google Play app

You need to create an app configuration policy named Policy1 for the Android Enterprise platform.
Which apps can you manage by using Policyl1?

A. App2 only
B. App3 only
C. App1 and App3 only
D. App2 and App3 only
E. App1, App2, and App3

Answer: D

Explanation:

Question: 130

HOTSPOT

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

Name	Member of
Userl	Groupl, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1.

All the users use Microsoft Excel.

From the Microsoft Endpoint Manager admin center, you create the policies shown in the following table.

Name	Type	Priority	Assigned to	Default file format for Excel
Policyl	Policies for Office apps	0	Groupl	OpenDocument Spreadsheet (*.ods)
Policy2	Policies for Office apps	1	Group2	Excel Binary Workbook (*.xlsb)

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
When Userl saves a new spreadsheet, the .ods format is used.	○	○
When User2 saves a new spreadsheet, the .xlsb format is used.	○	○
When User3 saves a new spreadsheet, the .xlsx format is used.	0	

Answer:

Explanation:

Box 1: No
User1 is member of Group1 and Group2.
Policy1 with priority 0 is assigned to Group1: default file format for Excel is.ods.
Policy2 with priority 1 is assigned to Group2: default file format for Excel is.xlsb.

Note: Key points to remember about policy order
Policies are assigned an order of priority.
Devices receive the first applied policy only.
You can change the order of priority for policies.
Default policies are given the lowest order of priority.

Box 2: Yes
User2 is member of Group2.
Group2 and Group3 are members of Group1.

Box 3: No
User3 is member of Group3.
Group2 and Group3 are members of Group1.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb- policy-order

Question: 131

You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune. You create an app configuration policy that contains the following settings:

- Device enrollment type: Managed devices
- Profile Type: All Profile Types
- Platform: Android Enterprise

Which two types of apps can be associated with the policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Built-in Android app
B. Managed Google Play store app

C. Web link
D. Android Enterprise system app
E. Android store app

Answer: B, D

Explanation:

Question: 132

You have a Microsoft 365 subscription that uses Microsoft Intune.
You need to ensure that you can deploy apps to Android Enterprise devices.
What should you do first?

A. Create a configuration profile.
B. Add a certificate connector.
C. Configure the Partner device management settings.
D. Link your managed Google Play account to Intune.

Answer: D

Explanation:

Question: 133

You have a Microsoft 365 subscription.
You have devices enrolled in Microsoft Intune as shown in the following table.
To which devices can you deploy apps by using Intune?

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

Answer: D

Explanation:

Question: 134

You have a Microsoft 365 tenant that uses Microsoft Intune.
You use the Company Portal app to access and install published apps to enrolled devices.
From the Microsoft Intune admin center, you add a Microsoft Store app.
Which two App information types are visible in the Company Portal?
NOTE: Each correct selection is worth one point.

A. Privacy URL

B. Information URL
C. Developer
D. Owner

Answer: A, B

Explanation:

A. Privacy URL

B. Information URL

Question: 135

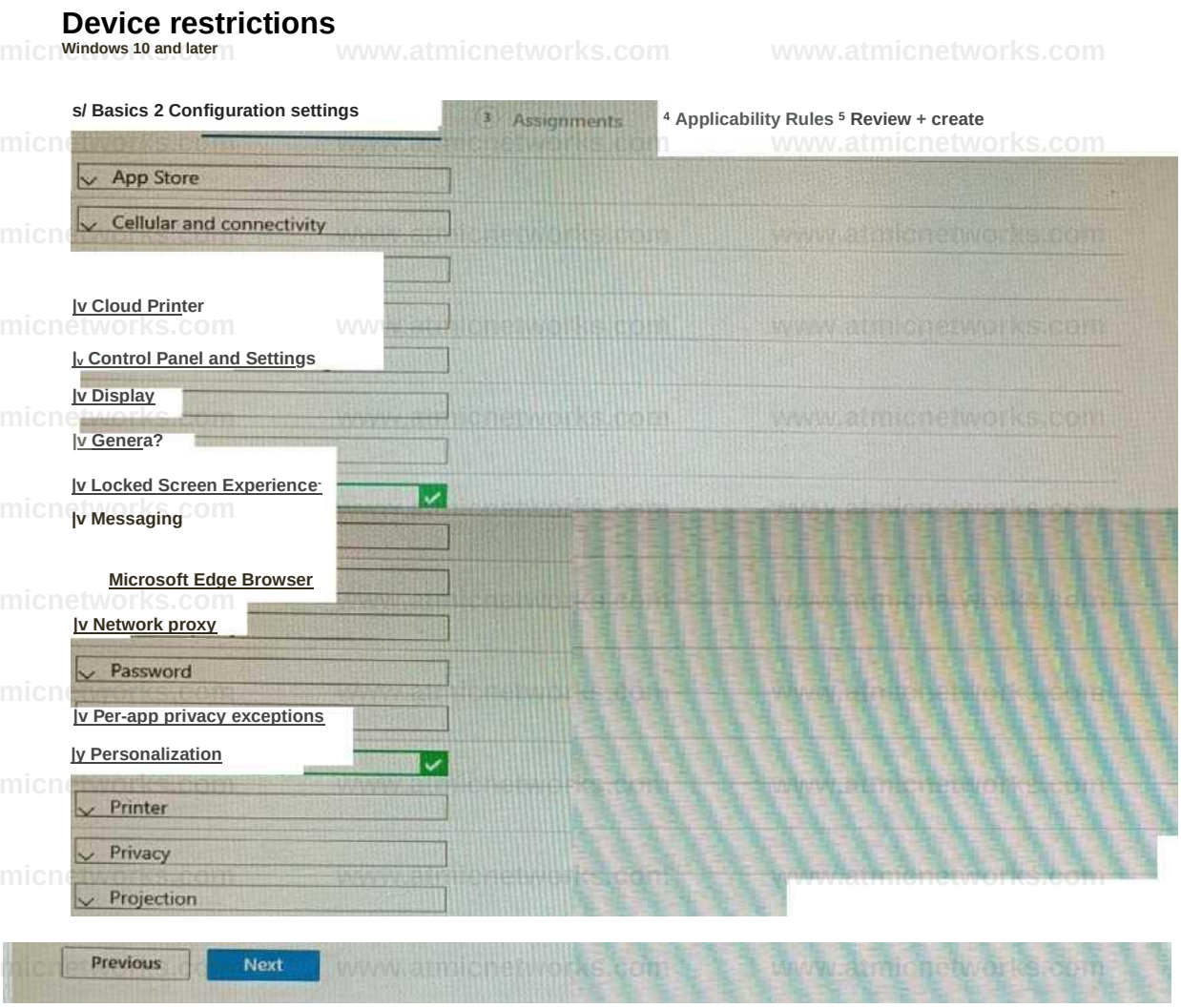
HOTSPOT

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.

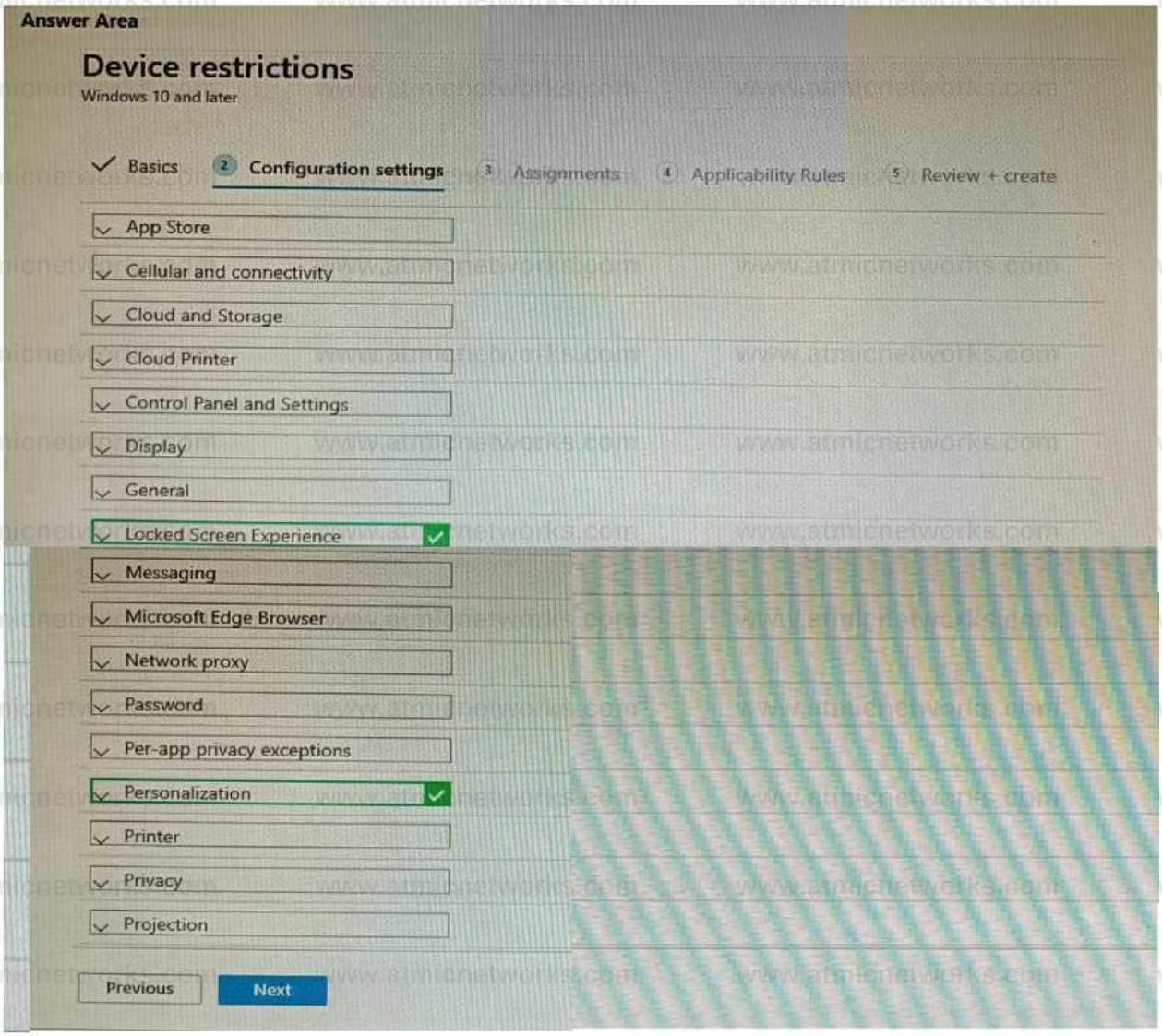
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:



Question: 136

You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to upgrade the computers to Windows 11 Enterprise. What should you configure in Intune?

A. a device compliance policy
B. a device cleanup rule
C. a device enrollment policy
D. a device configuration profile

Answer: D

Explanation:

Question: 137

You have computers that run Windows 10 and are managed by using Microsoft Intune.
Users store their files in a folder named D:\Folder1.
You need to ensure that only a trusted list of applications is granted write access to D:\Folder1.

What should you configure in the device configuration profile?

A. Microsoft Defender Exploit Guard
B. Microsoft Defender Application Guard
C. Microsoft Defender SmartScreen
D. Microsoft Defender Application Control

Answer: A

Explanation:

Question: 138

HOTSPOT

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You need to create Endpoint security policies to meet the following requirements:

Hide the Firewall & network protection area in the Windows Security app.
Disable the provisioning of Windows Hello for Business on the devices.

Which two policy types should you use? To answer, select the policies in the answer area.

NOTE: Each correct selection is worth one point.

Manage

Q Antivirus

Disk encryption

< Firewall

$ Endpoint detection and response

[T Attack surface reduction

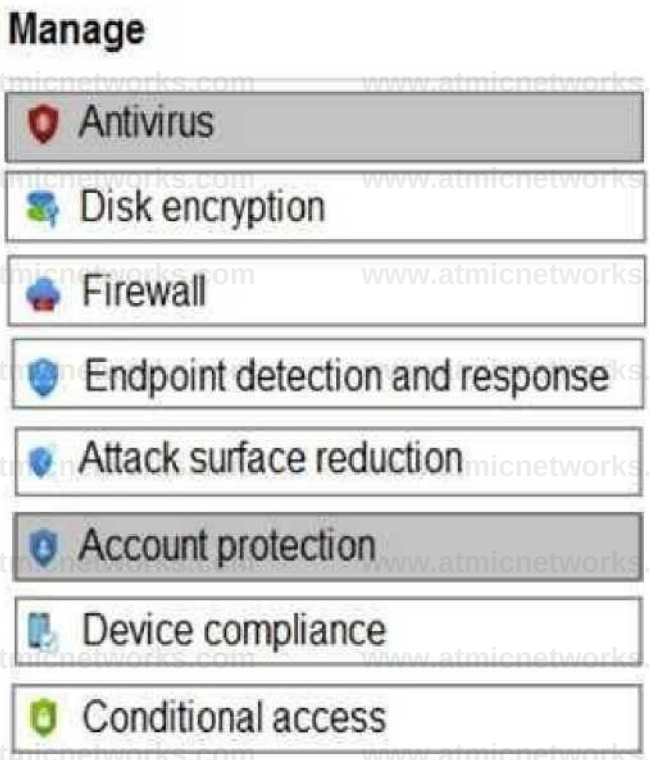
jo Account protection

I? Device compliance

0 Conditional access

Answer:

Explanation:



In the Antivirus policy settings, you can hide the Firewall and network protection area in the Windows Security app.

Windows Hello for Business settings are configured in Identity protection.

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows- settings

https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings

Question: 139

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune. Currently, Windows updates are downloaded without using Delivery Optimization. You need to configure the computers to use Delivery Optimization. What should you create in Intune?

A. a device compliance policy
B. a Windows 10 update ring
C. a device configuration profile
D. an app protection policy

Answer: C

Explanation:

Question: 140

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

You use Microsoft Intune to manage devices.

Auto-enrollment in Intune is configured.

You have 100 Windows 11 devices in a workgroup.

You need to connect the devices to the corporate wireless network and enroll 100 new Windows devices in Intune.

What should you use?

A. a provisioning package
B. a Group Policy Object (GPO)
C. mobile device management (MDM) automatic enrollment
D. a device configuration policy

Answer: C

Explanation:

Question: 141

HOTSPOT

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
q LON CL2	Yes	Windows	10.0.17763.615	Azure AD registered	User?	Microsoft Intune	Yes
q LON-CL4	Yes	Windows	10.0.17763.107	Azure AD joined	UserI	Microsoft Intune	Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Identified by Intune as a personal device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Answer:

Explanation:

Identified by Intune as a personal device: ▼

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device: ▼

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join

https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register

Question: 142

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

You use Microsoft Intune to manage devices. All devices are in the same time zone.

You create an update rings policy and assign the policy to all Windows devices.

On the November 1, you pause the update rings policy.

All devices remain online.
Without further modification to the policy, on which date will the devices next attempt to update?

A. December 1
B. December 6
C. November 15
D. November 22

Answer: C

Explanation:

Question: 143

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

All devices have Microsoft Edge installed.
From the Microsoft Intune admin center, you create a Microsoft
You need to apply Edge1 to all the supported devices.
To which devices should you apply Edge1?

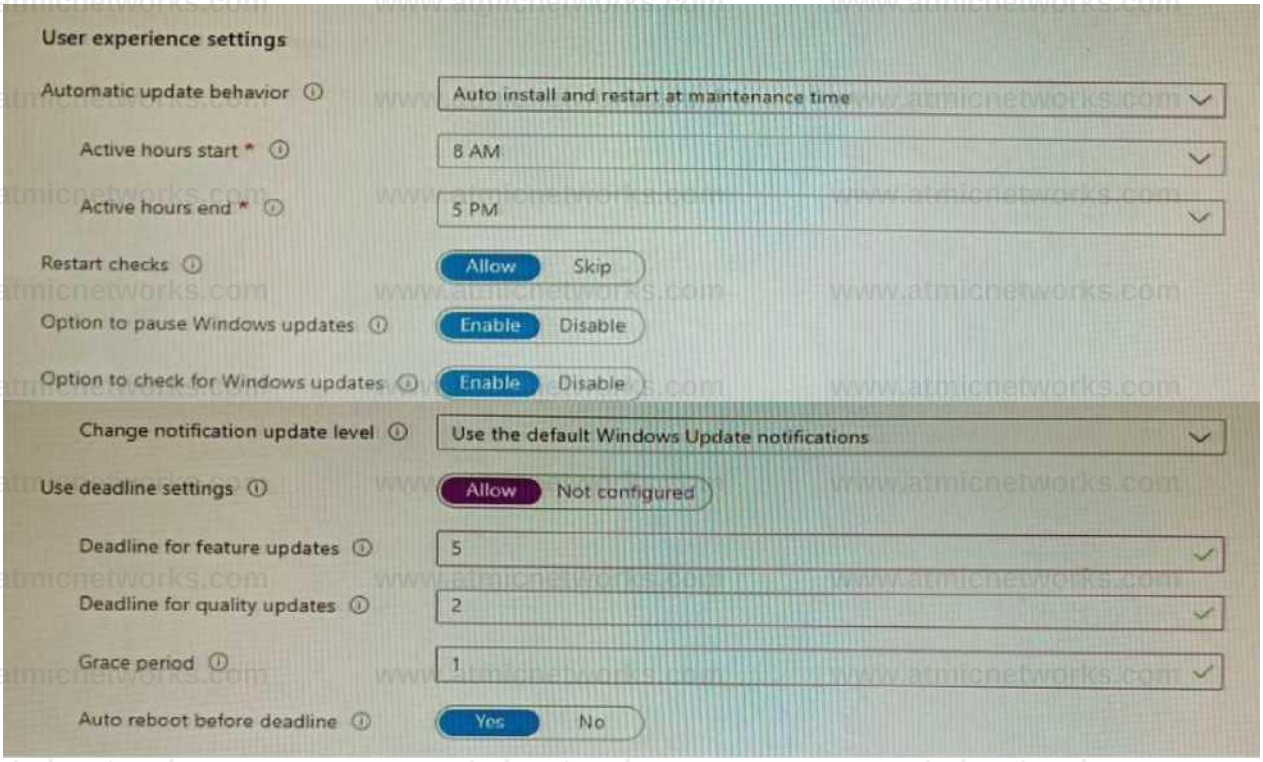
A. Device1 only
B. Device1 and Device2 only
C. Device1, Device2, and Device3 only
D. Device1, Device2, and Device4 only
E. Device1, Device2, Device3, and Device4

Answer: E

Explanation:

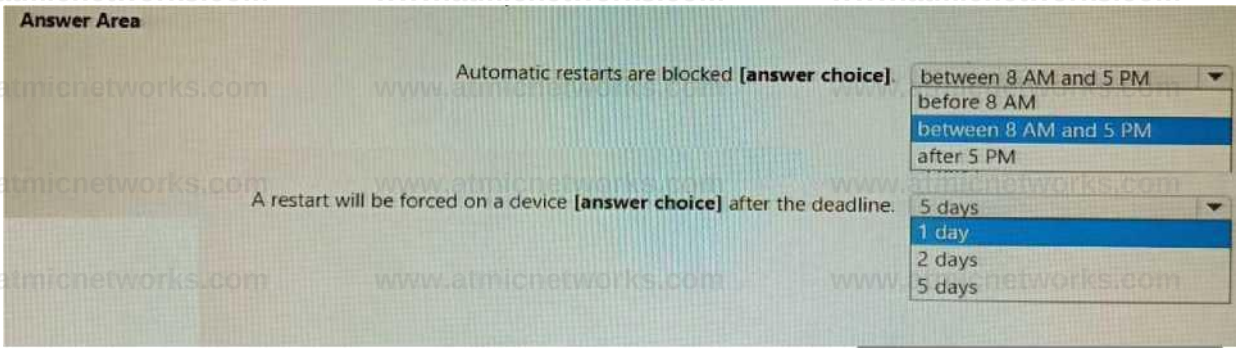
Question: 144

HOTSPOT
You have a Microsoft 365 subscription that uses Microsoft Intune.
You plan to manage Windows updates by using Intune.
You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.



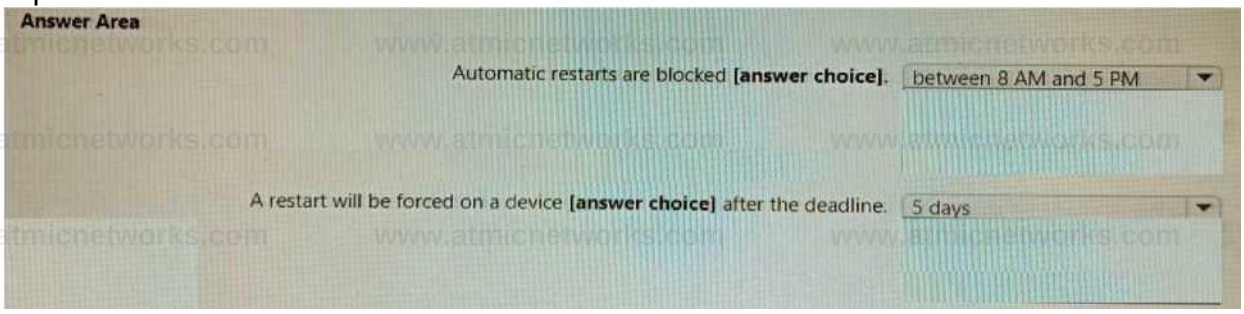
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 145

You have a Microsoft 365 tenant.

You have devices enrolled in Microsoft Intune.

You assign a conditional access policy named Policy1 to a group named Group1. Policy! restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.

You need to identify which noncompliant devices attempt to access OneDrive for Business. What

should you do?

A. From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.
B. From the Microsoft Intune admin center, review Device compliance report.
C. From the Microsoft Intune admin center, review the Noncompliant devices report.
D. From the Microsoft Intune admin center, review the Setting compliance report.

Answer: C

Explanation:

Question: 146

HOTSPOT

You use Microsoft Endpoint Manager to manage Windows 10 devices.

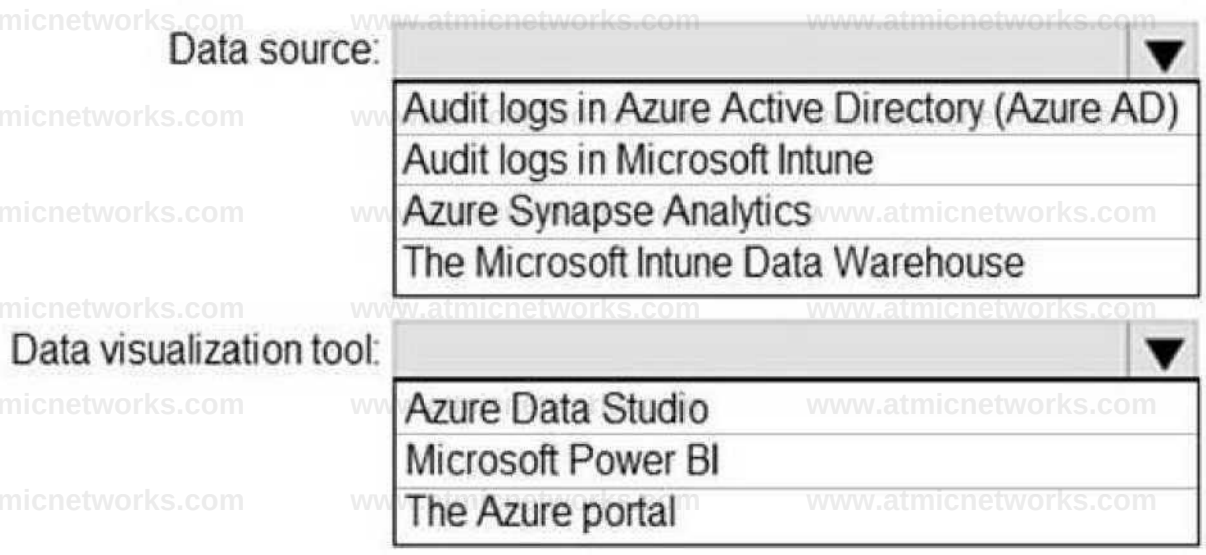
You are designing a reporting solution that will provide reports on the following:

Compliance policy trends
Trends in device and user enrolment
App and operating system version breakdowns of mobile devices

You need to recommend a data source and a data visualization tool for the design.

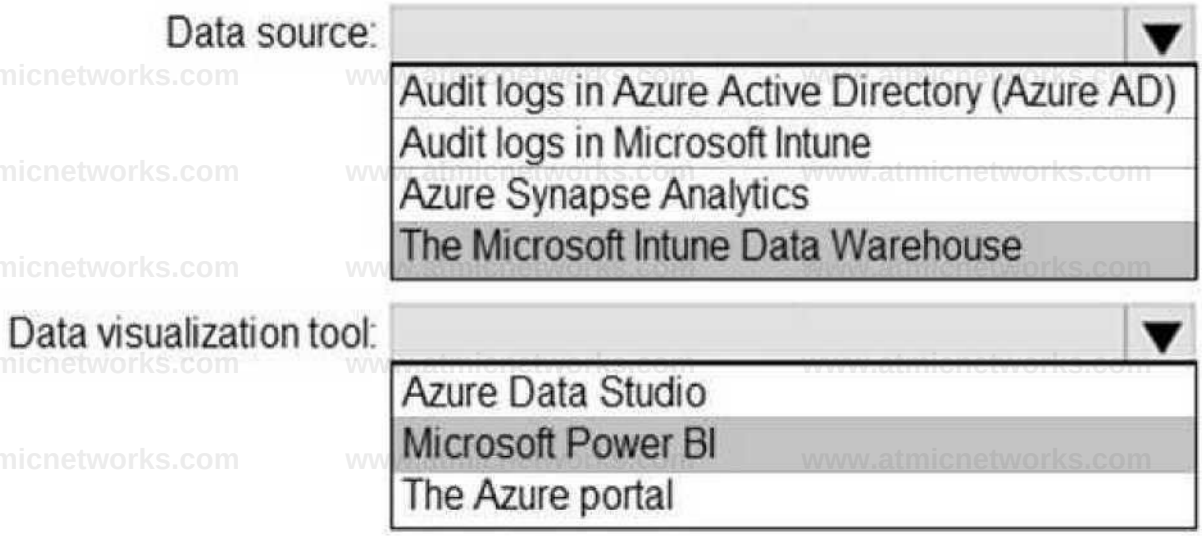
What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports

https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

Question: 147

Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10.

You implement hybrid Azure AD and Microsoft Intune.

You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune.

The solution must minimize administrative effort.

What should you use?

A. an Autodiscover address record
B. a Group Policy object (GPO)
C. an Autodiscover service connection point (SCP)
D. a Windows Autopilot deployment profile

Answer: D

Explanation:

Question: 148

HOTSPOT

You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.

Name	Member of
1 Computed	Group 1
I Computer?	Group1. Group?

Windows 10 update rings are defined in Intune as shown in the following table.

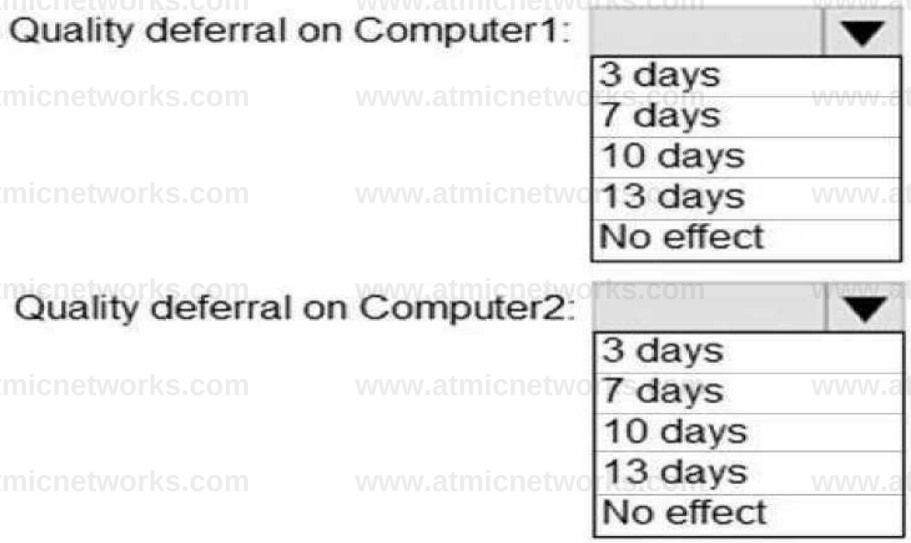
Name	Quality deferral (days)	Assigned
Ring I	3	Yes
Ring?	10	Yes

You assign the update rings as shown in the following table.

Name	Include	Exclude
Rmg1	Group 1	Group?
Ring?	Group?	Group 1

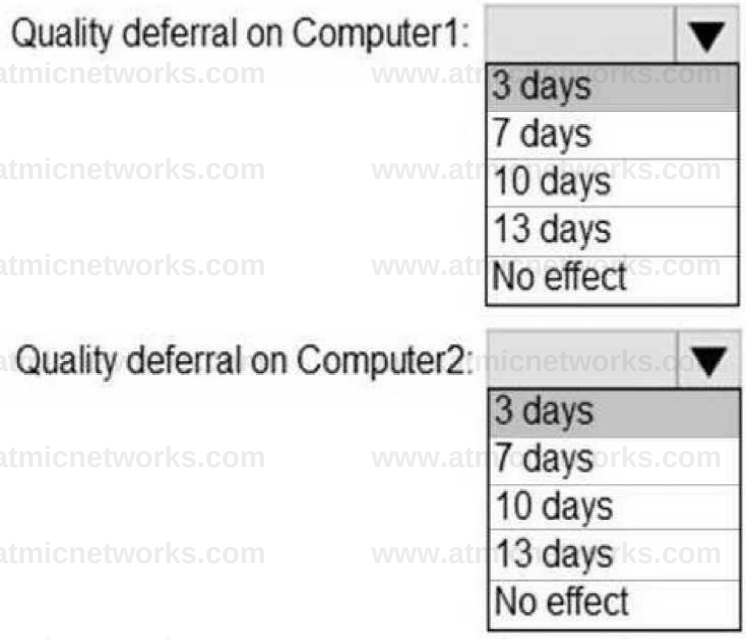
What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Computer1 and Computer2 are members of Group1. Ring1 is applied to Group1.

Note: The term "Exclude" is misleading. It means that the ring is not applied to that group, rather than that group being blocked.

Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-intune

https://allthingscloud.blog/configure-windows-update-business-using-microsoft-intune/

Question: 149

HOTSPOT

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to configure an Intune device configuration profile to meet the following requirements:

Prevent Microsoft Office applications from launching child processes.
Block users from transferring files over FTP.

Which two settings should you configure in Endpoint protection? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Endpoint protection

Windows 10 and later

x/ Basics O Configuration settings

v Microsoft Defender Appfication Guard

v Microsoft Defender firewall

v Microsoft Defender SmartScreen

v Windows Encryption

v Microsoft Defender Exploit Guard

x/ Microsoft Defender Application Control

v Microsoft Defender Credential Guard

v Microsoft Defender Security Center

v Local device security options

v Xbox services

Answer:

Explanation:

Answer Area

Reference:
https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

Question: 150

You have following types of devices enrolled in Microsoft Intune:

- Windows 10
- Android
- iOS

For which types of devices can you create VPN profiles in Microsoft Intune admin center?

A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and iOS only
D. Android and iOS only
E. Windows 10, Android, and iOS

Answer: E

Explanation:

Question: 151

You are creating a device configuration profile in Microsoft Intu
You need to configure specific OMA-URI settings in the profile. Which profile type template should you use?

A. Device restrictions (Windows 10 Team)
B. Identity protection
C. Custom
D. Device restrictions

Answer: C

Explanation:

Question: 152

HOTSPOT

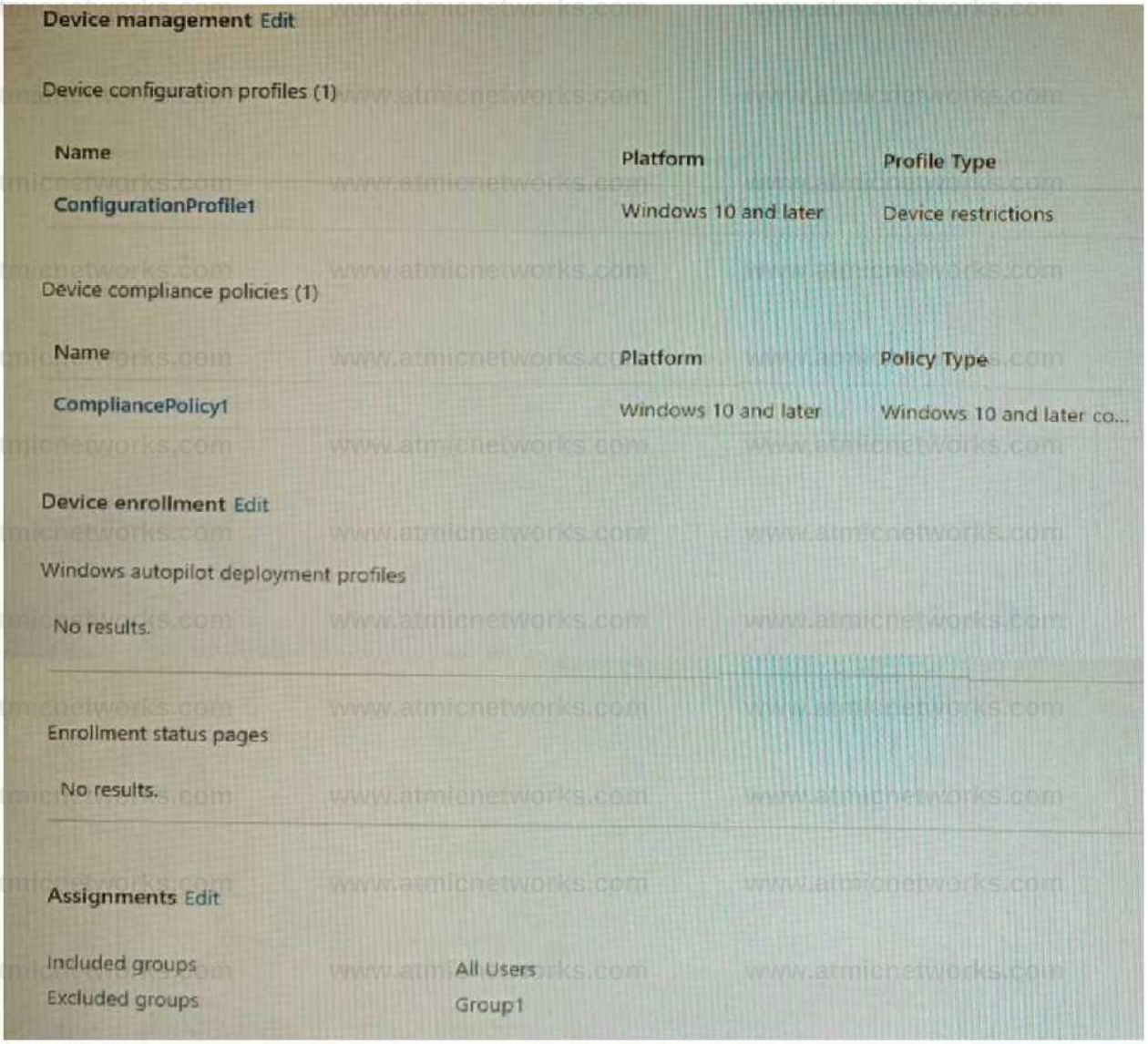
You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.

Name	Member of
Useri	Groupl
User2	*None*
User3	*None*

You create a policy set named Set1 as shown in the exhibit. (Click the Exhibit tab.) You enroll devices in Intune as shown in the following table.

Name	Operating system	User
Device 1	Windows 10	Useri
Device2	Windows 11	User2
Device3	Android	User3

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



Device management Edit

Device configuration profiles (1)

Name	Platform	Profile Type
ConfigurationProfile1	Windows 10 and later	Device restrictions

Device compliance policies (1)

Name	Platform	Policy Type
CompliancePolicy1	Windows 10 and later	Windows 10 and later co...

Device enrollment Edit

Windows autopilot deployment profiles

No results.

Enrollment status pages

No results.

Assignments Edit

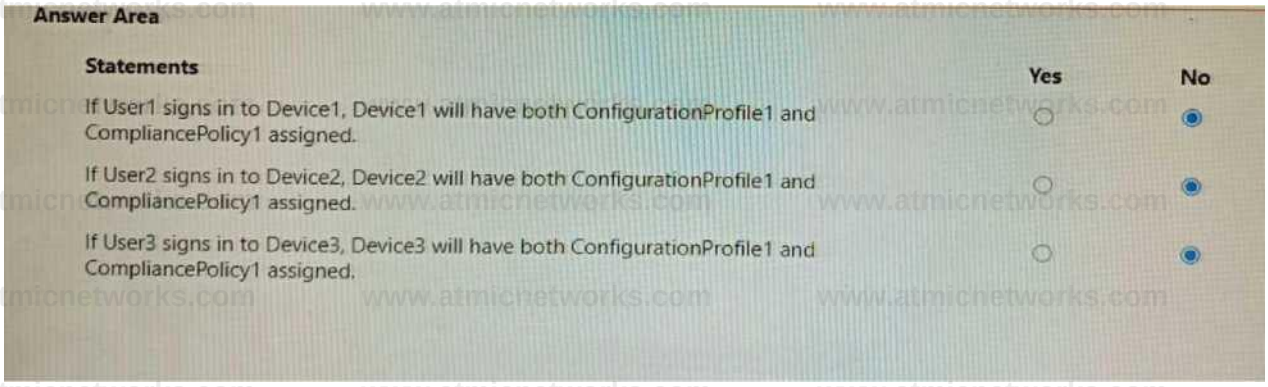
Included groups	All Users
Excluded groups	Group1

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○

Answer

Explanation:



Question: 153

HOTSPOT

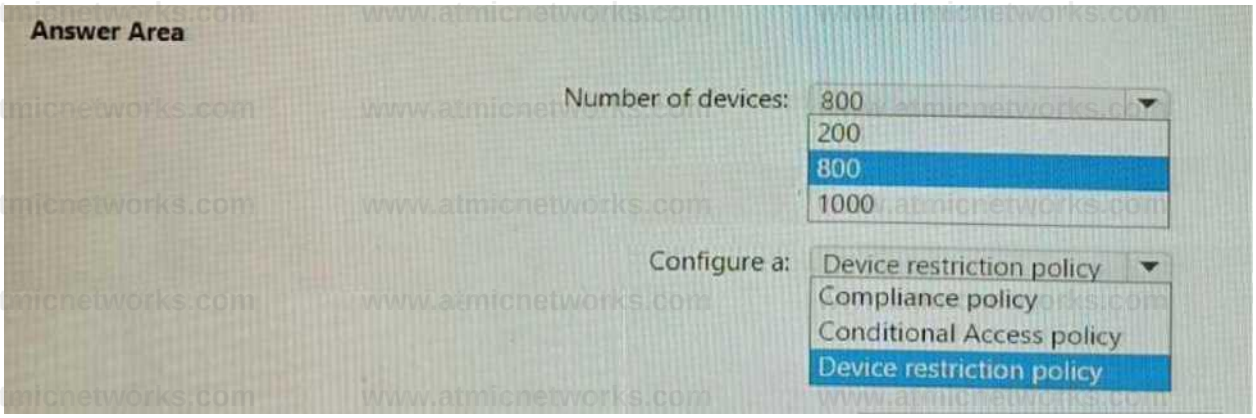
You have a Microsoft 365 subscription that contains 1,000 iOS devices. The devices are enrolled in Microsoft Intune as follows:

- Two hundred devices are enrolled by using the Intune Company Portal.
- Eight hundred devices are enrolled by using Apple Automated Device Enrollment (ADE).

You create an iOS/iPadOS software updates policy named Policy 1 that is configured to install iOS/iPadOS 15.5.

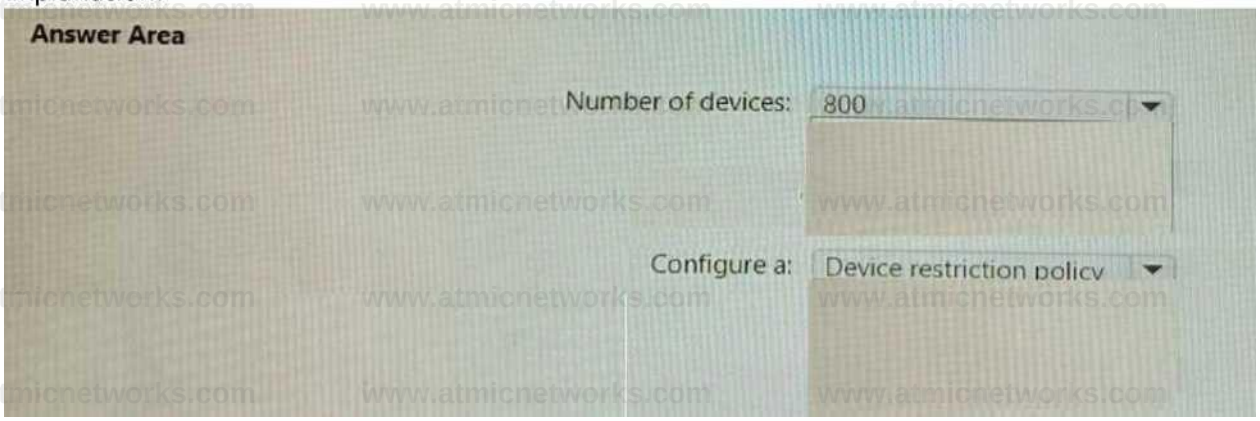
How many iOS devices will Policy1 update, and what should you configure to ensure that only iOS/iPadOS 15.5 is installed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Policy 1 will update 800 iOS devices that are enrolled by using Apple Automated Device Enrollment (ADE). This is because ADE devices are supervised devices that support software update policies in Intune1. Devices that are enrolled by using the Intune Company Portal are not supervised devices

and do not support software update policies2.

To ensure that only iOS/iPadOS 15.5 is installed, you should configure a device restriction policy that restricts visibility of software updates. This will prevent users from manually updating the OS to a newer version than the one you specified in Policy 11. You can use the Deployment Workbench to create and assign a device restriction profile to your ADE devices3.

Question: 154

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure the Authentication methods.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 155

HOTSPOT

You have computers that run Windows 10 and are configured by using Windows AutoPilot.

A user performs the following tasks on a computer named Computer1:

Creates a VPN connection to the corporate network

Installs a Microsoft Store app named App1

Connects to a Wi-Fi network

You perform a Windows AutoPilot Reset on Computer1.

What will be the state of the computer when the user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The Wi-Fi connection will be:

- Removed
- Retained and the passphrase will be retained
- Retained but the passphrase will be reset

App1 will be:

- Reinstalled at sign-in
- Removed
- Retained

The VPN connection will be:

- Removed
- Retained and the credentials will be cached
- Retained but the credentials will be reset

Answer:

Explanation:

The Wi-Fi connection will be:

- Retained and the passphrase will be retained
- Retained but the passphrase will be reset

App1 will be:

- Reinstalled at sign-in
- Removed
- Retained

The VPN connection will be:

- Removed
- Retained and the credentials will be cached
- Retained but the credentials will be reset

Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot- reset

Question: 156

Your network contains an Active Directory domain named contoso.com. The domain contains two computers

named Computer! and Computer2 that run Windows 10. On Computer1, you need to run the Invoke-Command cmdlet to execute several PowerShell commands on Computed. What should you do first?

A. On Computed, run the Enable-PSRemoting cmdlet.
B. On Computed, add Computer! to the Remote Management Users group.
C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computed.
D. On Computer1, run the HcK-PSSession cmdlet.

Answer: C

Explanation:

Question: 157

You have an Azure AD tenant that contains the devices shown in the following table.

Name	Operating system	Azure AD join type
Device 1	Windows 11 Pro	Joined
Device?	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Dewce4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

A. Device 1 only
B. Device1 and Device2 only
C. Device1 and Device3 only
D. Device1, Device2. Device3, and Device4

Answer: C

Explanation:

Question: 158

You have 25 computers that run Windows 10 Pro.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.
What should you use?

A. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise
B. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise
C. Windows Autopilot
D. Subscription Activation

Answer: C

Explanation:

Question: 159

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments. From Deployment Workbench, you modify the WinPE settings and add PowerShell support. You need to generate a new set of WinPE boot image files that contain the updated settings. What should you do?

A. From the Deployment Shares node, update the deployment share.
B. From the Advanced Configuration node, create new media.
C. From the Packages node, import a new operating system package
D. From the Operating Systems node, import a new operating system.

Answer: A

Explanation:

Question: 160

You are replacing 100 company-owned Windows devices.

You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices. The solution must meet the following requirements:

- Back up the user state.
- Minimize administrative effort.

Which task sequence template should you use?

A. Standard Client Task Sequence
B. Standard Client Replace Task Sequence
C. Litetouch OEM Task Sequence
D. Sysprep and Capture

Answer: B

Explanation:

Question: 161

HOTSPOT

You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 11 deployment tasks.

MDT contains the operating system images shown in the following table.

Name	Description
Imagetwim	Custom-built Windows 11 imago that has preinstalled custom apps
image? wim	Custom built Windows 11 image without apps
Install.wim	Default Windows 11 image

You need to perform a Windows 11 in-place upgrade on several computers that run Windows 10.

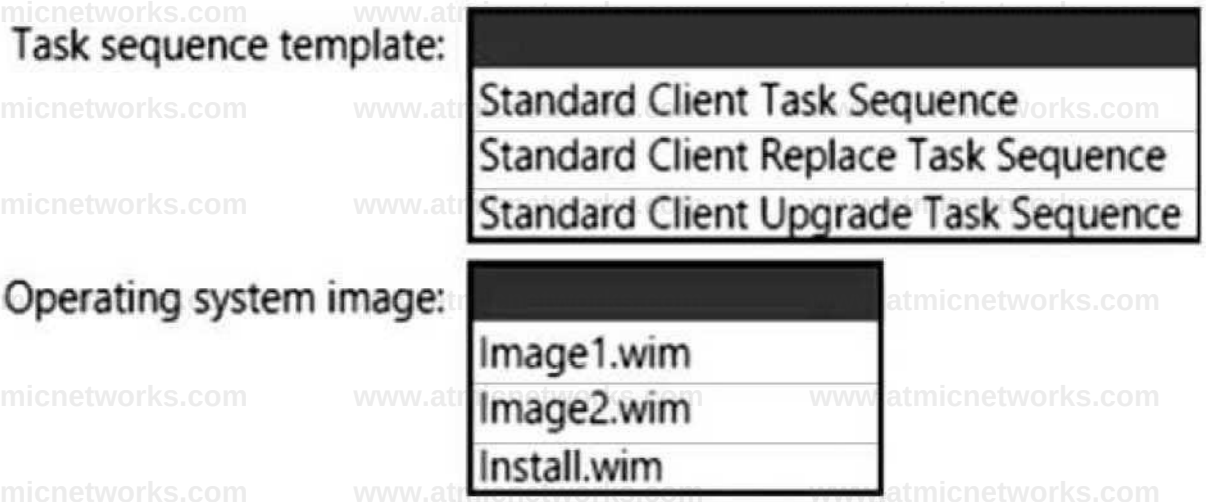
From the Deployment Workbench, you open the New Task Sequence Wizard.

You need to identify which task sequence template and which operating system image to use for the task

sequence. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box 1: Standard Client Upgrade Task Sequence

Use Template: Standard Client Upgrade Task Sequence

In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not plan to significantly change the device's configuration or applications. MDT includes an in-place upgrade task sequence template that makes the process really simple.

Box 2: Install.wim

In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. I

Reference: https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade- to-windows-10-with-the-microsoft-deployment-toolkit

Question: 162

Your network contains an Active Directory domain. The domain contains a computer named Computer! that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:

- For the WinRM service, set Startup type to Automatic.
- Create a listener that accepts requests from any IP address.
- Enable a firewall exception for WS-Management communications.

Which PowerShell cmdlet should you use?

A. Connect-WSMan

B. Enable-PSRemoting

C. Invoke-WSManAction

D. Enable-PSSessionConfiguration

Answer: B

Explanation:

Question: 163

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.

Name	Member of	On-premises sync
Userl	Groupl	Disabled
User?	Group?	Enabled

You assign Windows 10/11 Enterprise E5 licenses to Gtoup1 and Uset2.

You deploy the devices shown in the following table.

Name	Operating system	Joined to
Device 1	Windows 11 Pro	Azure AD
Device?	Windows 11 Pro	ADDS
DeviceS	Windows 10 Pro	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
If Useri signs in to Device! Devicel is upgraded to Windows 11 Enterprise automatically.		
If User? signs in to Device?, Device? is upgraded to Windows 11 Enterprise automatically.		
If User? signs in to Devices. Device3 is upgraded to Windows 11 Enterprise automatically.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
If Userl signs in to Device! Device! is upgraded to Windows 11 Enterprise automatically.		
If User? sign? in to Device?. Device? is upgraded to Windows 11 Enterprise automatically.		
If User? signs in to Devices. Device? is upgraded to Windows 11 Enterprise automatically.		

Question: 164

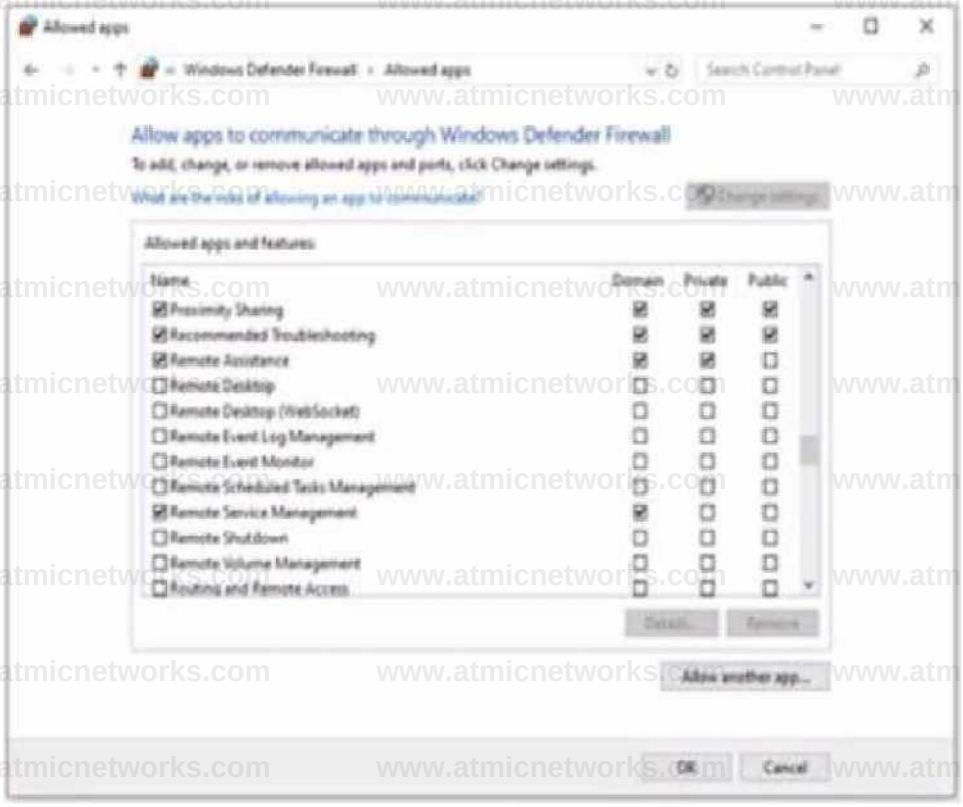
HOTSPOT

Your network contains an Active Directory domain named adatum.com, a workgroup, and computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of	Active Windows Defender Firewall profile
Cornputerl	Addlurn.com	Domain
Computer?	Adatum.com	Domain
Computer?	Workgroup	Public

The local Administrator accounts on Computed, Computed, and Computed have the same user name and password.

On Computed. Windows Defender Firewall is configured as shown in the following exhibit.



Status	Mame	Dis.pl ayharae
Stepped	RasAuto	Remote Access Auto Connection Manager
Running	RasMan	Remote Access Connection Manager
Stopped	Remote-Access	Routing and Remote Access
Stopped	RemoteRegistry	Remote Registry
Stopped	aetflilfcme	Retail Dw Service
Running	RmSvc	Radio Management Service
Running	RpcEptMapper	RPC Endpoint Mapper
Stopped	Rpc Locator	Remote Procedure Cell (RPC) locator
Running	RpcSs	Remote Procedure Call (RPC)

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 Computed, you can use Disk Management to manage Computeri remotely.		
From Computed, you can use Registry Editor to edit the registry of Computeri remotely, From Computers, you can use Performance Monitor to monitor the performance of Computeri.		

Answer:

Explanation:

Answer Area

Statements	Ves No
From Computer?. you can use Disk Management to manage Computeri remotely.	
From Computer?, you can use Registry Editor to edit the registry of Computeri remotely,	
From Computers, you can use Performance Monitor to monitor the performance of Computeri	

Question: 165

HOTSPOT

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

Name	Member of	License
User 1	Group1	*None*
User?	Groupl	Microsoft 365 E3
Useri	Group?	Microsoft 365 E5

Group2 has been assigned in the Enrollment Status Page.

You have the devices shown in the following table.

Name	Operating system	Department
Devicel	Windows 10 Pro	Marketing
Device?	Windows 11 Home	Research
Dev»ce3	Windows 10 Pro	Marketing

You capture and upload the hardware IDs of the devices in the marketing department.

You configure Windows Autopilot.

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 complete the Autopilot process on Devicel.		
User? can complete the Autopilot process on Devicel		
User3 can view device setup information during the enrollment phase of Devicel.		

Answer:

Explanation:

Answer Area Statements	Yes	No
Useri can complete the Autopilot process on Devicel.		
User2 can complete the Autopilot process on Devicel		
User3 can view device setup information during the enrollment phase ot Devicel.		

Question: 166

You have a Microsoft 365 subscription that contains a user named User1. User! is assigned a Windows 10/11 Enterprise E3 license. You use Microsoft Intune Suite to manage devices. User1 activates the following devices:

- Device1: Windows11 Enterprise
- Device2: Windows10 Enterprise
- Device3: Windows11 Enterprise

How many more devices can User1 activate?

A. 2
B. 3
C. 7
D. 8

Answer: A

Explanation:

Question: 167

DRAG DROP

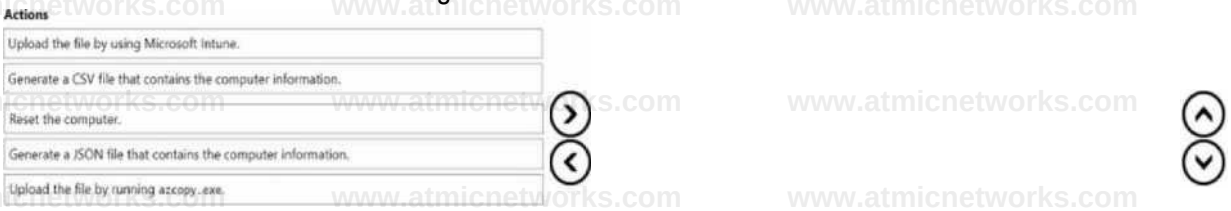
Your company has a computer named Computer1 that runs Windows 10.

Computed was used by a user who left the company.

You plan to repurpose Computer1 and assign the computer to a new user.

You need to redeploy Computer1 by using Windows Autopilot.

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:

To redeploy Computer1 by using Windows Autopilot, you need to perform the following three actions in sequence:

Generate a JSON file that contains the computer information. This file specifies the Autopilot profile to be applied during the deployment. You can use the Get-AutopilotProfilesForExistingDevices

PowerShell script to generate this file1.

Reset the computer. You can use the Windows Automatic Redeployment feature to trigger a reset from the login screen by pressing Ctrl + R and providing an administrator account2. Alternatively, you can use the Windows Autopilot Reset feature to remotely reset the device from Intune1.

Upload the file by running azcopy.exe. This step copies the JSON file to a blob storage account in Azure, where it can be accessed by the device during the deployment. You need to specify the storage account name, access key, and container name as parameters for azcopy.exe1.

Question: 168

You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 11.

You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 11 Enterprise to new computers. The computers have a single hard disk.

You need to modify the task sequence to create a system volume and a data volume.

Which phase should you modify in the task sequence?

A. Initialization
B. State Restore
C. Preinstall
D. Postinstall

Answer: C

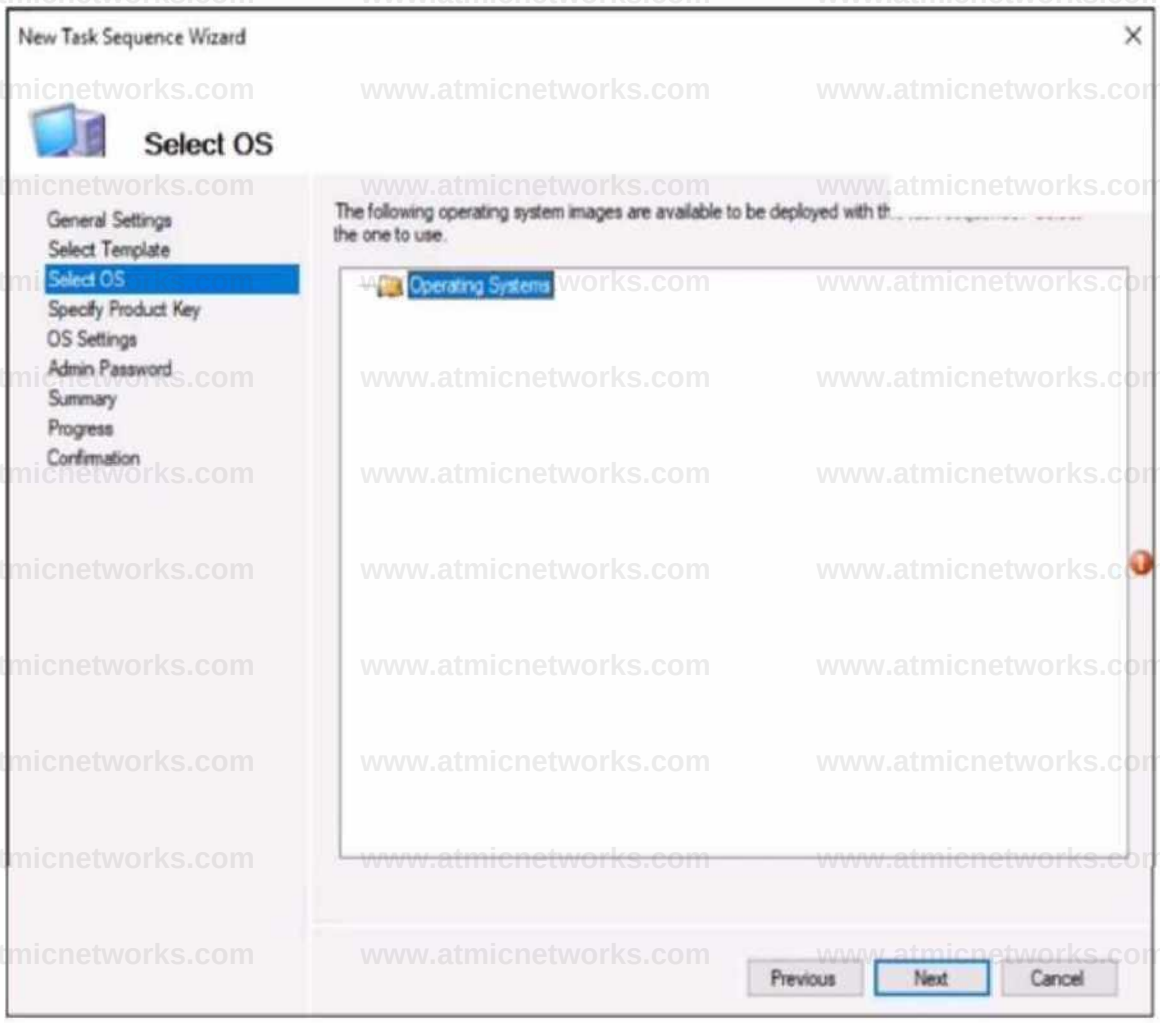
Explanation:

Question: 169

You have a Microsoft Deployment Toolkit (MDT) deployment share.

From the Deployment Workbench, you open the New Task Sequence Wizard and select the Standard Client Upgrade Task Sequence task sequence template.

You discover that there are no operating system images listed on the Select OS page as shown in the following exhibit.



You need to be able to select an operating system image to perform a Windows 11 in-place upgrade. What should you do?

A. Enable monitoring for the deployment share.
B. Import a full set of source files.
C. Import a custom image file.
D. Run the Update Deployment Share Wizard

Answer: D

Explanation:

Question: 170

Your company implements Azure AD, Microsoft 365, Microsoft Intune, and Azure Information Protection. The company's security policy states the following:

- Personal devices do not need to be enrolled in Intune.
- Users must authenticate by using a PIN before they can access corporate email data.
- Users can use their personal iOS and Android devices to access corporate cloud services.
- Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.

You need to configure a solution to enforce the security policy.

What should you create?

A. a device configuration profile from the Microsoft Intune admin center
B. a data loss prevention (DIP) policy from the Microsoft Purview compliance portal
C. an insider risk management policy from the Microsoft Purview compliance portal
D. an app protection policy from the Microsoft Intune admin center

Answer: B

Explanation:

Question: 171

You have a Microsoft 365 subscription that contains 500 Android Enterprise devices.
All the devices are enrolled in Microsoft Intune.
You need to deliver bookmarks to the Chrome browser on the devices
What should you create?

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

Answer: D

Explanation:

Question: 172

You have a Microsoft 365 E5 subscription and 100 computers that run Windows 10.
You need to deploy Microsoft Office Professional Plus 2019 to the computers by using Microsoft Office Deployment Tool (ODT).
What should you use to create a customization file for ODT?

A. the Microsoft 365 admin center
B. the Microsoft Intune admin center
C. the Microsoft Purview compliance portal
D. the Microsoft 365 Apps admin center

Answer: D

Explanation:

Question: 173

You have a Microsoft 365 subscription that contains 1.000 Windows 11 devices enrolled in Microsoft Intune. You plan to use Intune to deploy an application named App1 that contains multiple installation files.
What should you do first?

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.
B. Create an Android application package (APK).
C. Upload the contents of App1 to Intune.
D. Install the Microsoft Deployment Toolkit (MDT).

Answer: A

Explanation:

Question: 174

HOTSPOT

You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Groupl	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

You are deploying Microsoft 365 apps.

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

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Endpoint Manager admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

App Information Edit

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https //products.office com/en-us/explore-office-for-home https
Privacy URL	//privacy mic rosoft com/en-US/pnvac ystatement Microsoft
Developer	Microsoft
Owner	
Notes	
Logo	Office
	Teams, Word
Architecture	64-bit
Update channel	Current Channel
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License Teams on behalf of users	No
Install background service for Microsoft Search in Bing	No
Apps to be installed as part of the suite	1 language(s) selected

Assignments Edit

Group mode	Group
Xz Required	
(+,! Included	Groupl

Available for enrolled devices

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
LT 1 will have Microsoft Office 365 installed		
LT2 will have Microsoft Office 365 installed		
LT3 will have Microsoft Office 365 installed		

Answer:

Explanation:

Statements	Yes	No
LT1 will have Microsoft Office 365 installed	0	0
LT2 will have Microsoft Office 365 installed	0	0
LT3 will have Microsoft Office 365 installed	0	0

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

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

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

Question: 175

HOTSPOT

You have a Microsoft 365 subscription.

Users have iOS devices that are not enrolled in Microsoft 365 Device Management.

You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)

p protection po > Sett*

Create policy X

TptiM

* Platform

iOS

Target to all app types

Yes No

* App types

Apps on unmanaged devices

1 app selected

Review configured settings

Settings X

Data protection

Default settings configured

Default settings configured

Default settings configured

Scape i ex, 0 KopeW

wheeled

You need to configure the policy to meet the following requirements:

Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.

Require the users to use an alphanumeric passcode to access the Outlook app.

What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Prevent the users from using Outlook if the operating system version is less than 12.0.0:

- Access requirements
- Conditional launch
- Data protection
- Scope

Require the users to use an alphanumeric passcode to access Outlook:

- Access requirements
- Conditional launch
- Data protection
- Scope

Answer:

Explanation:

Prevent the users from using Outlook if the operating system version is less than 12.0.0: **Conditional launch**

Require the users to use an alphanumeric passcode to access Outlook: **Access requirements**

Reference:
https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios

Question: 176

HOTSPOT

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

You have the apps shown in the following exhibit.

By platform	App2	iOS line-of-business app	Yes
M Windows	App3	iOS line-ofrbusiness app	No
B iOS/iPadOS	Excel	Android store app	Yes
t macOS	Excel	iOS store app	Yes
Q Android	Managed Home Screen	Managed Google Play store app	Yes
Policy	Microsoft Authenticator	Managed Google Play store app	No
19 App protection policies	OneDnve	Android store app	No
ID App configuration policies	OneDrive	iOS store app	No

Use the drop-down menus to select the answer choice that completes each statement based upon the information presented in the graphic NOTE: Each correct selection is worth one point.

rwc*n awtoCOnh9M.1I ipc.-m tor (imwir choice) OS '.u^portod I;<M

1
2
3
4
5

loo cm onto coni-.u irwn poin-* . ¹ (MM*M chotco) Andi owl-iupoor1«d«or>t

I
2
3
4
5

Answer:

Explanation:

Answer Area

You can create configuration policies for [answer choice) iOS-supported apps. 4

You can create configuration policies for [answer choice] Android-supported apps. 3

Question: 177

You have a Microsoft 365 subscription. All devices run Windows 10.

You need to prevent users from enrolling the devices in the Windows Insider Program.

What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

A. a device restrictions device configuration profile
B. an app configuration policy
C. a Windows 10 and later security baseline
D. a custom device configuration profile
E. a Windows 10 and later update ring

Answer: A, E

Explanation:

Question: 178

You install a feature update on a computer that runs Windows 10. How many days do you have to roll back the update?

A. 5
B. 10
C. 14
D. 30

Answer: B

Explanation:

Question: 179

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.
You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup.
You need to ensure that you can use Log Analytics to query events from Computer1.
What should you do on Computer1?

A. Join Azure AD.
B. Configure Windows Defender Firewall
C. Create an event subscription.
D. Install the Azure Monitor Agent.

Answer: D

Explanation:

Question: 180

HOTSPOT

You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform
Device 1	Windows 10
Dev«ce2	macOS

In Microsoft Intune Endpoint security, you need to configure a disk encryption policy for each device.
Which encryption type should you use for each device, and which role-based access control (RBAQ role in Intune should you use to manage the encryption keys? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Question: 181

HOTSPOT

Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.

The company purchases an Azure subscription.

You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.

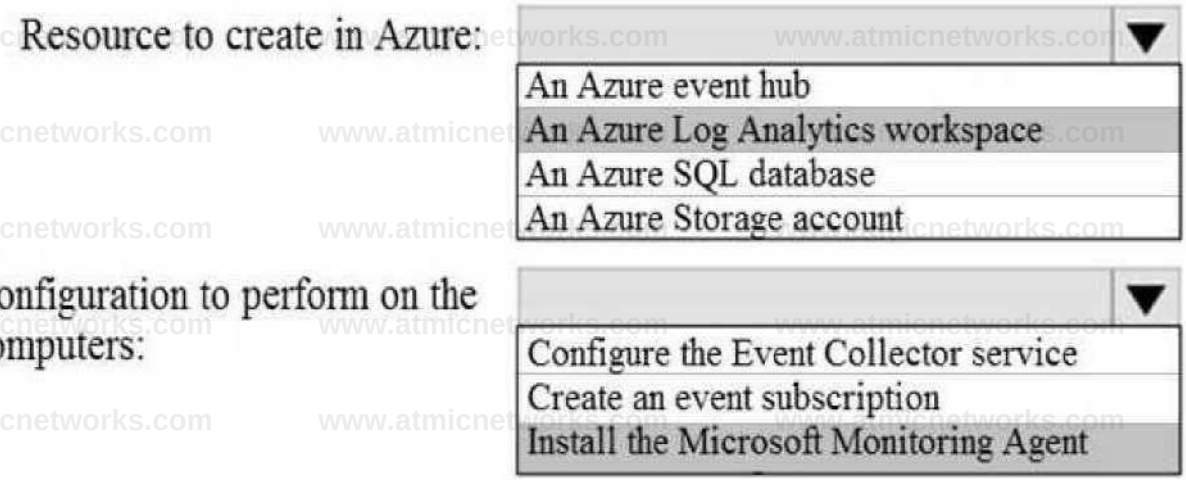
What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Resource to create in Azure:	An Azure event hub An Azure Log Analytics workspace An Azure SQL database An Azure Storage account
Configuration to perform on the computers:	Configure the Event Collector service Create an event subscription Install the Microsoft Monitoring Agent

Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent

Question: 182

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have an update ring named UpdateRingl that contains the following settings:

- Automatic update behavior: Auto install and restart at a scheduled time

- Automatic behavior frequency: First week of the month
- Scheduled install day: Tuesday
- Scheduled install time: 3 AM

From the Microsoft Intone admin center, you select Uninstall for the feature updates of UpdateRing1.

When will devices start to remove the feature updates?

A. when a user approves the uninstall
B. as soon as the policy is received
C. next Tuesday
D. the first Tuesday of the next month

Answer: C

Explanation:

Question: 183

You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.

You discover that Group Policy settings override the settings configured in Microsoft Intune policies.

You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings.

What should you do?

A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
B. From the Microsoft Intune admin center, create a custom device profile.
C. From the Microsoft Intune admin center, create an Administrative Templates device profile.
D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

Answer: C

Explanation:

Question: 184

HOTSPOT

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8,9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.

Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

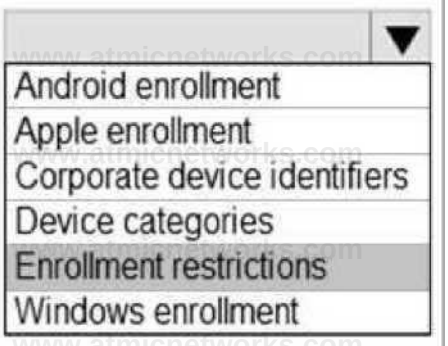
Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

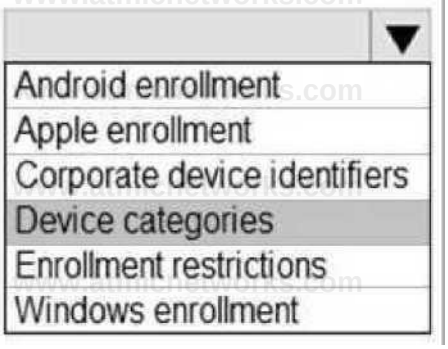
Answer:

Explanation:

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:



Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:



Reference:

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

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

Question: 185

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

You use Microsoft Intune to manage devices.

You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.

What should you configure?

A. the Azure Monitor agent
B. a device compliance policy
C. a Conditional Access policy
D. an Intune data collection policy

Answer: D

Explanation:

Question: 186

HOTSPOT

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

Devices are enrolled in Intune as shown in the following table.

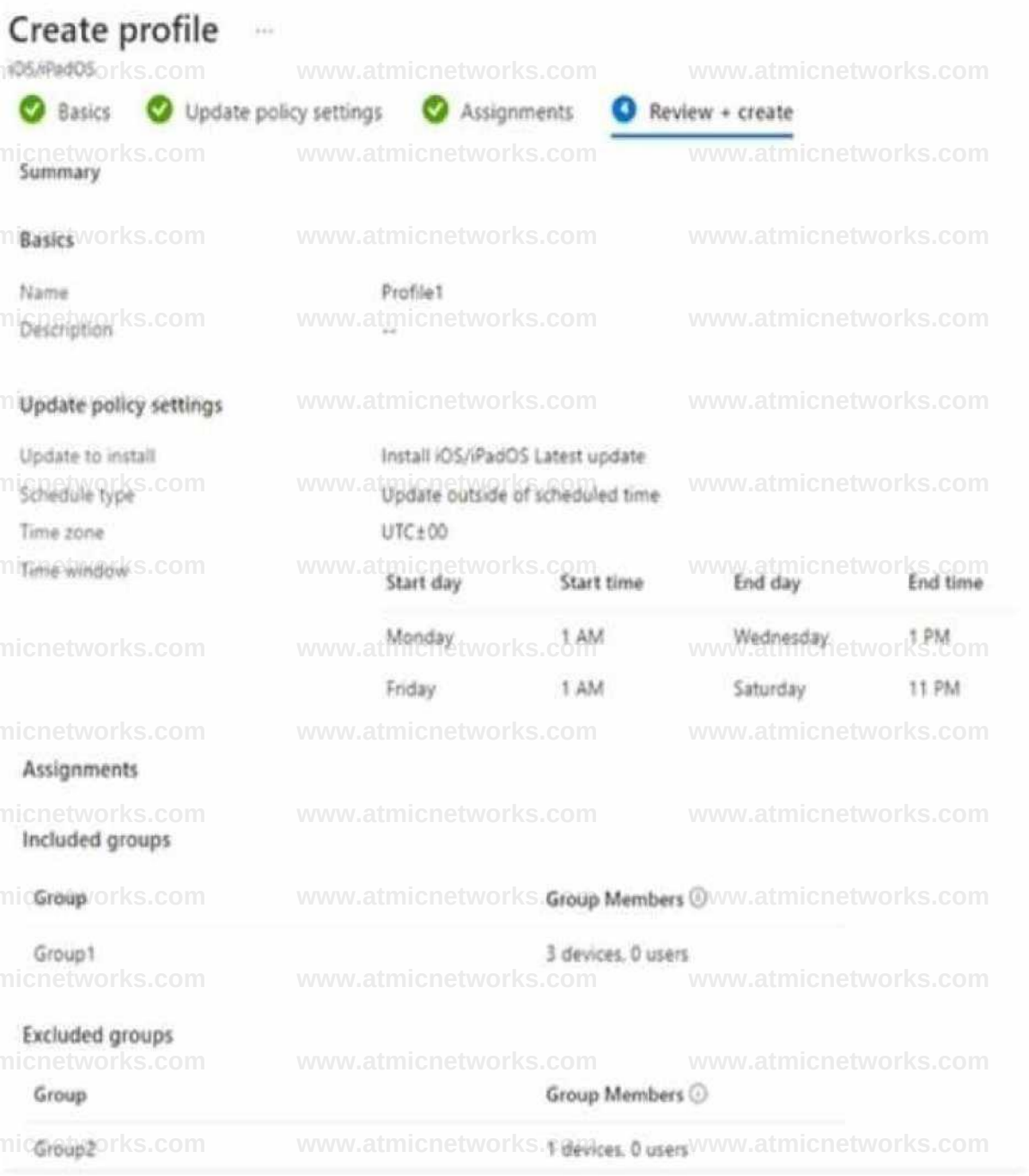
Name	Platform	Enrolled by using
Devicel	iOS	Apple Automated Device Enrollment (ADE)

Device?	iPadOS	Apple Automated Device Enrollment (ADE)
De, ?:J	iPadOS	The Company Portal app

The devices are the members of groups as shown in the following table.

Name	Members
Group!	Device!. Device?. Device?
Group?	Device?

You create an JOS/iPadOS update profile 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
If an iOS update becomes available on Tuesday at 5 AM. the update is installed on Devicel automatically on Wednesday.		
If an iPadOS update becomes available on Thursday at 2 AM. the update is installed on Device? automatically on Thursday.		
If an iPadOS update becomes available on Friday at 10 PM. the update is installed on Device? automatically on Sunday.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
If an iOS update become* available on Tuesday at 5 AM. the update is installed on Devicel automatically on Wednesday.		
If an iPadOS update becomes available on Thursday at 2 AM. the update is installed on Device? automatically on Thursday.		

Question: 187

You have a Microsoft Intune deployment that contains the resources shown in the following table.

Name	Type	Platform
Complyl	Device compliance policy	Windows 10 and later
Comply?	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	*Not applicable*
Conti	Device configuration profile	Windows 10 and later
Oflicel	Office app policy	*Not applicable*

You create a policy set named Set1 and add Comply1 to Set1.

Which additional resources can you add to Set1?

A. Conf1 only
B. Comply2 only
C. Comply2 and Conf1 only
D. CA1. Conf1. and Office 1 only
E. Comply2. CA1, Conf1. and Office1

Answer: B

Explanation:

Question: 188

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

A. Microsoft Defender for Endpoint Power 81 app
B. Microsoft Secure Score
C. Endpoint Analytics
D. Microsoft 365 Defender portal

Answer: B

Explanation:

Question: 189

DRAG DROP

You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).

You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

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	Answer Area
Obtain the root certificate.	
From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.	
From the Enterprise CA, configure certificate managers.	
From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.	
From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.	

Answer:

Explanation:

Obtain the root certificate.

From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.

From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

Question: 190

HOTSPOT

Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active Directory (Azure AD).

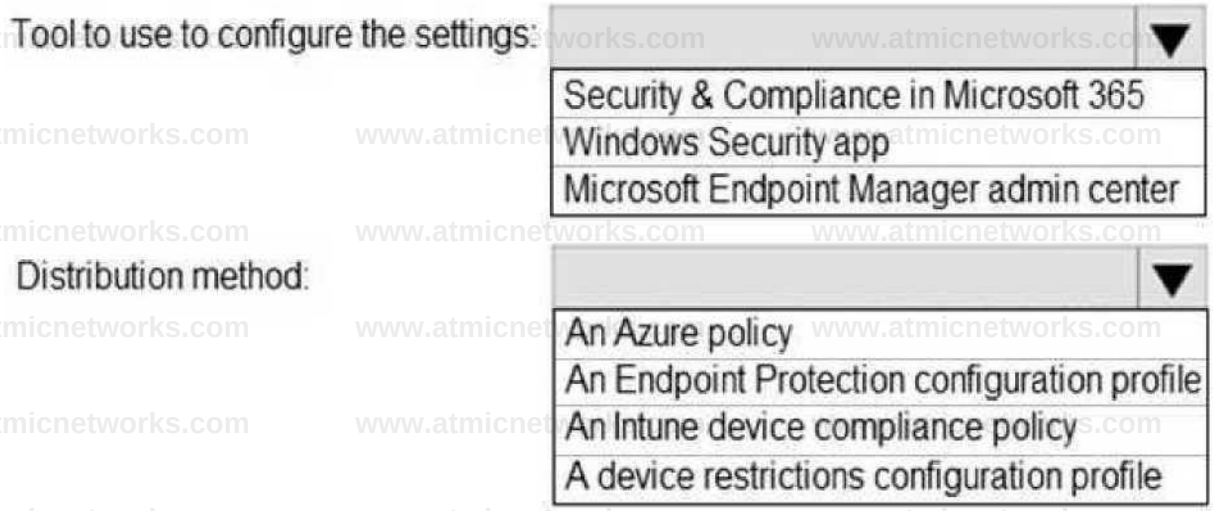
There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.

You plan to implement Microsoft Defender Exploit Guard.

You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.

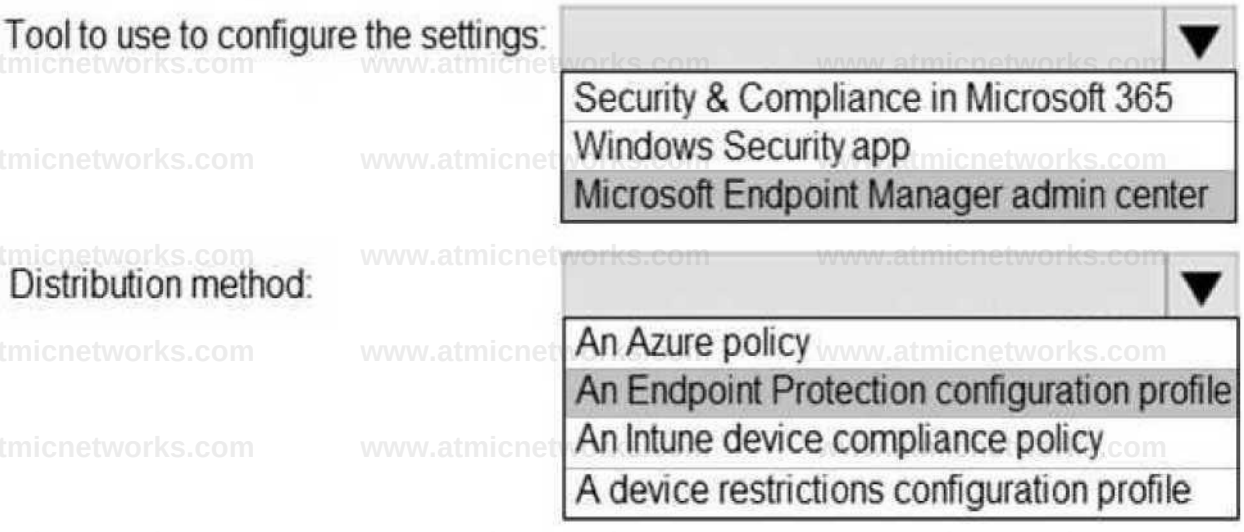
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/import-export-exploit-protection-emet-xml#manage-or-deploy-a-configuration

https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

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

Question: 191

Your company uses Microsoft Intune.

More than 500 Android and iOS devices are enrolled in the Intune tenant.

You plan to deploy new Intune policies. Different policies will apply depending on the version of Android or iOS installed on the device.

You need to ensure that the policies can target the devices based on their version of Android or iOS. What should you configure first?

A. groups that have dynamic membership rules in Azure AD
B. Device categories in Intune
C. Corporate device identifiers in Intune
D. Device settings in Azure AD

Answer: B

Explanation:

Question: 192

DRAG DROP

You have SOO Windows 10 devices enrolled in Microsoft Intune.

You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASlR)

You need to configure a Windows 10 device that will be used to create a template file.

Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings. Each protection area 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.

Protection areas

| Account protection |

App & browser control I

Device security

Virus & threat protection

Answer Area

pp.

Mandatory ASIR:

Answer:

Explanation:

Exploit protection is a feature that helps protect against malware that uses exploits to infect devices and spread.

Exploit protection consists of many mitigations that can be applied to either the operating system or individual apps1.

To configure a Windows 10 device that will be used to create a template file for Exploit protection, you need to configure the following protection areas on the device in the Windows Security app: DEP: Device security. Data Execution Prevention (DEP) is a mitigation that prevents code from running in memory regions marked as non-executable. You can enable DEP system-wide or for specific apps in the Device security section of the Windows Security app1.

Mandatory ASLR: App & browser control. Force randomization for images (Mandatory ASLR) is a mitigation that randomizes the location of executable images in memory, making it harder for attackers to predict where to inject code. You can enable Mandatory ASLR system-wide or for specific apps in the App & browser control section of the Windows Security app1.

Question: 193

You have an Azure AD tenant named contoso.com.
You have a workgroup computer named Computer! that runs Windows 11.
You need to add Computer1 to contoso.com.
What should you use?

A. dsreecmd.exe
B. Computer Management
C. netdom.exe
D. the Settings app

Answer: A

Explanation:

Question: 194

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage Windows 11 devices.
You need to implement passwordless authentication that requires users to use number matching
Which authentication method should you use?

A. Microsoft Authenticator
B. voice calls
C. FI002 security keys
D. text messages

Answer: A

Explanation:

Question: 195

You use a Microsoft Intune subscription to manage iOS devices.
You configure a device compliance policy that blocks jailbroken iOS devices.
You need to enable Enhanced jailbreak detection.
What should you configure?

A. the Compliance policy settings
B. the device compliance policy
C. a network location
D. a configuration profile

Answer: D

Explanation:

Question: 197
HOTSPOT

You have a Microsoft Intune subscription that has the following device compliance policy settings:

Mark devices with no compliance policy assigned as: Compliant
Compliance status validity period (days): 14

On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Devicel	Enabled	Off	Tag1	Groupl
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:

Name: Policy1
Platform: Windows 10 and later
Require BitLocker: Require
Mark device noncompliant: 5 days after noncompliance
Scope (Tags): Tag1

Name: Policy2
Platform: Windows 10 and later
Firewall: Require
Mark device noncompliant: Immediately

Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

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

On January 7,	Devicel is marked as compliant	O	O
On January 8,	Devicel is marked as compliant.	O	O
On January 8,	Device2 is marked as compliant	O	O

Answer:

Explanation:

Statements	Yes	No
On January 7, Devicel is marked as compliant.	O	|O|
On January 8, Devicel is marked as compliant	O	O
On January8, Device2 is marked as compliant	O	O

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No

For the same reason as Box1.

Box 3: Yes

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply. The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

Question: 198

HOTSPOT

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have computers that run Windows 11 as shown in the following table.

Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computed	Joined	Enrolled	Disabled	Enabled
Computer?	Registered	Enrolled	Enabled	Enabled
Computer 3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.

Name	Members
Groupl	Computer 1. Computer?
Group?	Computers _____

You create and assign the compliance policies shown in the following table.

Name	Configuration	Action for noncompliance	Assignment
Pohcyl	Require Bitlocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Groupl
Policy?	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group?

The next day, you review the compliance status of the computers.
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
The compliance status of Computeri is In grace period-		
Ilie compliance status of Computer? is Compliant.		
Tire compliance status of Computers is Not compliant		

Answer:

Explanation:

Answer Area Statements	Yes	No
The compliance status of Computeri is In grace period.	Tire compliance status of Computer? is Compliant.	
Tire compliance status of Computer! is Not compliant		

Question: 199

You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune.
You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

A. an app configuration policy
B. a security baseline
C. an app protection policy
D. an iOS app provisioning profile

Answer: C

Explanation:

An app protection policy is a set of rules that controls how data is accessed and handled by managed apps on mobile devices. App protection policies can prevent the printing of corporate data from managed apps on iOS

devices by using the Restrict cut, copy, and paste with other apps setting. This setting can be configured to block printing from the iOS share menu. An app configuration policy is used to customize the behavior of a managed app, such as specifying a VPN profile or a web link. A security baseline is a collection of recommended security settings for Windows 10 devices that are managed by Intune. An iOS app provisioning profile is a file that contains information about the app's identity, entitlements, and distribution method

Question: 200

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

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

In the Microsoft Intune admin center, you are creating a Microsoft 365 Apps app named App1. To which objects can you assign App1?

A. Group3 and Group4 only
B. Admin1, Group3, and Group4 only
C. Group1, Group3, and Group4 only
D. Group1, Group2, Group3, and Group4 only
E. Admin1, Group1. Group2, Group3, andGroup4

Answer: C

Explanation:

In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using

device groups. In this scenario, the objects shown in the table are as follows:
Admin1 is an individual user account that belongs to the Global administrators role group.
Group1 is a user group that contains 100 users.
Group2 is a device group that contains 50 devices.
Group3 is a user group that contains 200 users.
Group4 is a device group that contains 150 devices.
Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment. Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

Question: 201

You have a Hyper-V host. The host contains virtual machines that run Windows 10 as shown in following table.

Name	Generation	Virtual TPM	Virtual processors	Memory
VM1	1	No	4	16 GB
VM2	2	Yes	2	4 GB
VM3	2	Yes		8 GB

Which virtual machines can be upgraded to Windows 11?

A. VM1 only
B. VM2 only
C. VM2 and VM3 only
D. VM1.VM2. andVM3

Answer: C

Explanation:

Windows 11 has certain hardware requirements that must be met in order to upgrade from Windows 10. Some of these requirements are as follows:

A processor with at least 1 GHz clock speed and 2 cores.

A system firmware that supports UEFI and Secure Boot.

A Trusted Platform Module (TPM) version 2.0 or higher.

At least 4 GB of system memory (RAM).

At least 64 GB of storage space.

In this scenario, the virtual machines that run Windows 10 have the following specifications:

VM1 is a generation 1 virtual machine with no virtual TPM, 4 virtual processors, and 16 GB of memory.

VM2 is a generation 2 virtual machine with a virtual TPM, 2 virtual processors, and 4 GB of memory.

VM3 is a generation 2 virtual machine with a virtual TPM, 1 virtual processor, and 8 GB of memory.

VM1 cannot be upgraded to Windows 11 because it does not have a virtual TPM and it is not a generation 2 virtual machine. Generation 1 virtual machines do not support UEFI and Secure Boot, which are required for Windows 11. VM2 and VM3 can be upgraded to Windows 11 because they have a virtual TPM and they are generation 2 virtual machines. They also meet the minimum requirements for processor speed, cores, memory, and storage space.

Question: 202

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User! uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

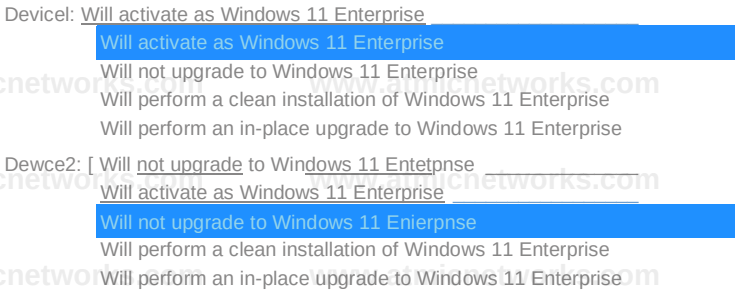
In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1.

You need to identify what will occur when User1 next signs in to the devices.

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

NOTE: Each correct selection is worth one point.

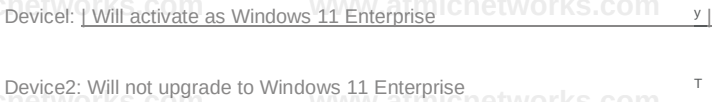
Answer Area



Answer:

Explanation:

Answer Area



Device2: Will not upgrade to Windows 11 Enterprise

Device 1:

Will activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 1 has Windows 11 Pro, so it meets the requirement. When User1 signs in to Device 1 with their Azure AD account, the device will automatically activate as Windows 11 Enterprise without changing the edition.

Will not activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 2 has Windows 10 Home, so it does not meet the requirement. When User1 signs in to Device 2 with their Azure AD account, the device will not activate as Windows 11 Enterprise by subscription.

Question: 204

DRAG DROP

You have a Microsoft 365 subscription that uses Microsoft Intune.

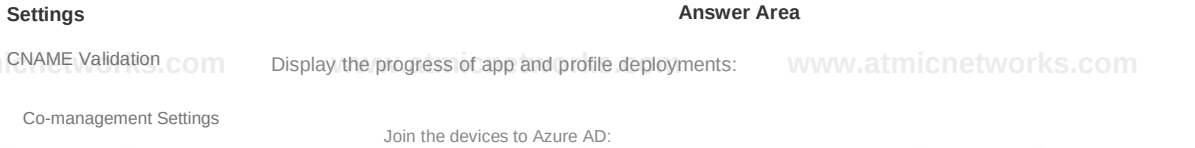
You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to meet the following requirements during device provisioning:

- Display the progress of app and profile deployments.
- Join the devices to Azure AD.

What should you configure to meet each requirement? To answer drag the appropriate settings to the correct requirements. Each setting 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.



Deployment Profiles

Enrollment notifications

Enrollment Status Page

Answer:

Explanation:

Question: 205

Your company has a Remote Desktop Gateway (RD Gateway).

You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.

You need to configure a Remote Desktop connection to connect through the gateway.

Which setting should you configure?

A. Connect from anywhere
B. Server authentication
C. Connection settings
D. Local devices and resources

Answer: A

Explanation:

To connect to a remote server through the RD Gateway, you need to configure the Connect from anywhere setting in the Remote Desktop Connection client. This setting allows you to specify the domain name and port of the RD Gateway server, as well as the authentication method. The other settings are not related to the RD Gateway connection. Reference: Configure Remote Desktop Connection Settings for Remote Desktop Gateway

Question: 206

DRAG DROP

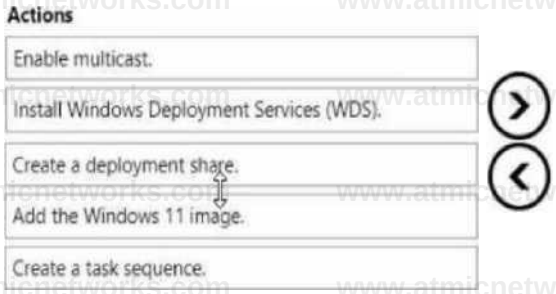
Your network contains an Active Directory domain.

You install the Microsoft Deployment Toolkit (MDT) on a server.

You have a custom image of Windows 11.

You need to deploy the image to 100 devices by using MDT.

Which three actions should you perform in sequence? To answer, move answer area and arrange them in the correct order.



Answer:

Explanation:

To deploy the Windows 11 image to 100 devices by using MDT, you should perform the following three actions in sequence:

Install Windows Deployment Services (WDS) on the server. WDS is a role that enables you to deploy Windows operating systems over the network by using PXE boot and multicast technologies. You need to install WDS before you can enable multicast and configure the boot images for MDT. You can install WDS by using the Server Manager or PowerShell1.

Create a deployment share on the server. A deployment share is a folder that contains the MDT files, scripts, applications, drivers, operating systems, and task sequences that you use to deploy Windows. You need to create a deployment share by using the MDT Deployment Workbench2.

Add the Windows 11 image and create a task sequence in the deployment share. An image is a file that contains a snapshot of a Windows installation. A task sequence is a set of steps that MDT executes to install Windows and configure the settings. You need to add the Windows 11 image by importing it from a source folder or a WIM file, and create a task sequence by using a template or customizing your own3.

These are the basic steps to prepare for deploying Windows 11 with MDT. For more details and guidance, you can refer to the web search results I found for you by using search_web("deploy Windows 11 image with MDT").

Question: 207

You have the Microsoft Deployment Toolkit (MDT) installed.

You install and customize Windows 11 on a reference computer

You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.

Which command should you run before you capture the image?

A. dism
B. wpeinit
C. sysprep
D. bcdedit

Answer: C

Explanation:

To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the sysprep command with the /generalize option. This option removes all unique system information from the Windows installation, such as the computer name, security identifier (SID), and driver cache. The other commands are not used for this purpose. Reference: Sysprep (Generalize) a Windows installation

Question: 208

Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer? that run Windows 10.
You install Windows Admin Center on Computer1.
You need to manage Computer2 from Computer1 by using Windows Admin Center.
What should you do on Computed?

A. Update the TrustedHosts list
B. Run the Enable-PSRemoting cmdlet
C. Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.
D. Add an inbound Microsoft Defender Firewall rule.

Answer: B

Explanation:

To manage a remote computer from Windows Admin Center, you need to enable PowerShell remoting on the remote computer. You can do this by running the Enable-PSRemoting cmdlet, which configures the WinRM service, creates a listener, and allows inbound firewall rules for PowerShell remoting. The other options are not sufficient or necessary for this task. Reference: Installation and configuration for Windows Remote Management

Question: 209

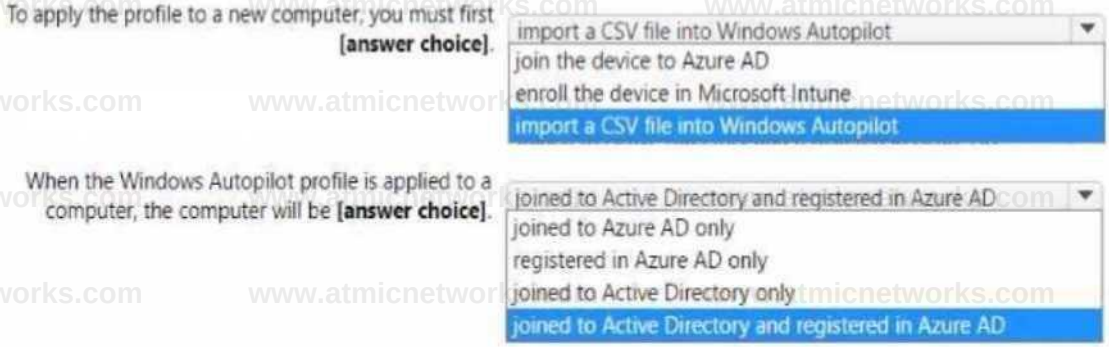
HOTSPOT

You have a hybrid Azure AD tenant.
You configure a Windows Autopilot deployment profile 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



Answer:

Explanation:

Answer Area

To apply the profile to a new computer, you must first [answer choice] — import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be **[answer choice]** — joined to Active Directory and registered in Azure AD

Question: 210

HOTSPOT

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

You use Microsoft Intune to manage devices.

You plan to create Windows 11 device builds for the marketing and research departments The solution must meet the following requirements:

- Marketing department devices must support Windows Update for Business.

- Research department devices must have support for feature update versions for up to 36 months from release.

What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

Marketing: Windows 11 Pro ˅

Windows 11 Enterprise

Windows 11 Pro for Workstations

Research: | Windows 11 Enterprise ˅

Windows 11 Pro

Windows 11 Pro for Workstations

Answer:

Explanation:

Answer Area

Marketing: Windows 11 Pro

Research: Windows 11 Enterprise

Question: 211

You have an Azure AD tenant named contoso.com.

You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

Name	Memory	TPM
Device1	16 GB	None
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

A. Device2 only
B. Device3 only
C. Device2 and Devnce3 only
D. Device 1, Device2, and Device3

Answer: C

Explanation:

Windows Autopilot self-deploying mode requires devices that have a firmware-embedded activation key for

Windows 10 Pro or Windows 11 Pro. This feature allows devices to automatically activate Windows Enterprise edition using the subscription license assigned to the user. Device1 does not have a firmware-embedded activation key, so it cannot use self-deploying mode. Device2 and Device3 have firmware-embedded activation keys for Windows 10 Pro, so they can use selfdeploying mode. Reference: Windows Autopilot self-deploying mode (Public Preview), Deploy Windows Enterprise licenses

Question: 212

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft 365 subscription

You plan to use Windows Autopilot to deploy new Windows devices.

You plan to create a deployment profile.

You need to ensure that The deployment meets the following requirements:

- Devices must be joined to AD DS regardless of their current working location.
- Users in the marketing department must have a line-of-business (LOB) app installed during the deployment.

The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Devices must be joined to AD DS regardless of their current working location: nstall the Intune connector foi Acti cj-cc: . Deploy Always On VPN.

Install the Intune connector for Active Directory.
Modify the Autopilot deployment profile
E lit' ■- l o-n -i ■ -i rem sen ni in mt me

The marketing department users must have an LOB app installed dunng the deployment t Modify the Autopilot deployment motile Modify the Autopilot deployment profile
Creates Microsoft Intune app deployment
Create a device configuration profile in Intune

Answer:

Explanation:

Answer Area

Devices must be joined to AD DS regardless of their current working location: I Install the Intune connector for Active Directory.

The marketing department users must have an LOB app installed dunng the deployment Modify the Autopilot deployment profile.

Question: 213

You have 200 computers that run Windows 10 and are joined to an Active Directory domain.
You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable the Allow Remote Shell access setting.
B. Enable the Allow remote server management through WinRM setting.
C. Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.
D. Enable the Windows Defender Firewall: Allow inbound Remote Desktop exceptions setting.
E. Set the Startup Type of the Remote Registry service to Automatic
F. Enable the Windows Defender Firewall: Allow inbound remote administration exception setting.

Answer: B, C, F

Explanation:

To enable WinRM on domain computers using Group Policy, you need to perform the following actions:
Enable the Allow remote server management through WinRM setting under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service.
This setting allows you to specify the IP address ranges that can connect to the WinRM service.
Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic under Computer Configuration > Preferences > Control Panel Settings > Services. This setting ensures that the WinRM service starts automatically on the computers.
Enable the Windows Defender Firewall: Allow inbound remote administration exception setting under Computer Configuration > Policies > Security Settings > Windows Firewall and Advanced Security > Windows Firewall and

Advanced Security > Inbound Rules. This setting creates a firewall rule that allows incoming TCP connections on port 5985 for WinRM. Reference: How to Enable WinRM via Group Policy, Installation and configuration for Windows Remote Management

Question: 214

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices.
You purchase a Microsoft 365 E5 subscription.
You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.
Which upgrade method should you use?

A. Windows Autopilot
B. a Microsoft Deployment Toolkit (MDT) lite-touch deployment
C. Subscription Activation
D. an in-place upgrade by using Windows installation media

Answer: C

Explanation:

Subscription Activation is a feature that allows you to upgrade from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise without needing a product key or reinstallation. You just need to assign a subscription license (such as Microsoft 365 E5) to the user in Azure AD, and then sign in to the device with that user account. The device will automatically activate Windows Enterprise edition using the firmware-embedded activation key for Windows Pro edition. This method minimizes administrative effort and simplifies the upgrade process. Reference: Windows subscription activation, Deploy Windows Enterprise licenses

Question: 215

HOTSPOT
You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.

Name	Platform	IPaddress
Devicel	Windows	192.168.1035
Device?	Android	[10.10.10.40
Devices	Android	192.168.10.10

The devices are members of a group named Group1.
In Intune, you create a device compliance location that has the following configurations:

- Name: Network1
- IPv4 range: 192.168.0.0/16

In Intune. you create a device compliance policy for the Android platform. The policy has the following configurations:

- Name: Policy1
- Device health: Rooted devices: Block
- Locations: Location: Network1
- Mark device noncompliant: Immediately

- Assigned: Group1

The Intune device compliance policy has the following configurations:

- Mark devices with no compliance policy assigned as: Compliant
- Enhanced jailbreak detection: Enabled
- Compliance status validity period (days): 20

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
Devicel is marked as compliant.	O	O
Device2 is marked as compliant.	O	
Devices is marked as compliant.	0	O

Answer:

Explanation:

Device1 is marked as compliant. = No Device2 is marked as compliant. = Yes Device3 is marked as compliant. = No

Device1 is marked as noncompliant because it is rooted and the device compliance policy Policy1 blocks rooted devices under the Device health setting1.

Device2 is marked as compliant because it is not rooted and it is within the network location Network1 that is specified in the device compliance policy Policy11.

Device3 is marked as noncompliant because it is outside the network location Network1 that is specified in the device compliance policy Policy11. The device compliance location setting requires devices to be in a specific network range to be compliant2.

Question: 216

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

- Ensure that you can manage the personal devices by using Microsoft Intune.
- Ensure that users can access company data seamlessly from their personal devices.
- Ensure that users can only sign in to their personal devices by using their personal account

What should you use to add the devices to Azure AD?

A. Azure AD registered
B. hybrid Azure AD join
C. AD joined

Answer: A

Explanation:

To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD

registered devices are devices that are connected to your organization's resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.

The other options are not suitable for this scenario because:

Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both onpremises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories2.

AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources3.

Reference: What are Azure AD registered devices?, What are hybrid Azure AD joined devices?, What is an Active Directory domain join?

Question: 217

HOTSPOT

You have a Microsoft 365 subscription.

All computers are enrolled in Microsoft Intune.

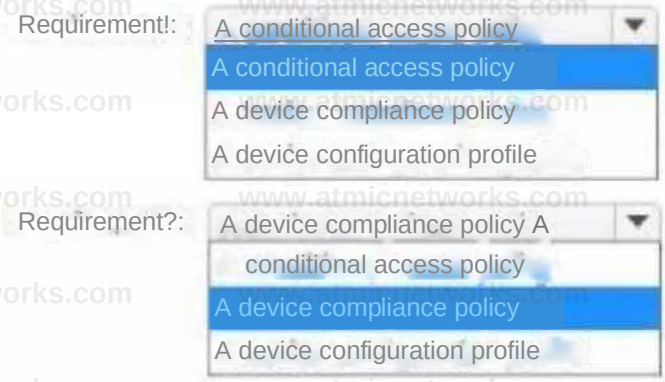
You have business requirements for securing your Windows 11 environment as shown in the following table.

Requirement	Detail
Requirement1	Ensure that Microsoft Exchange Online can be accessed from known locations only.
Requirement2	Lock a device that has a high Microsoft Defender for Endpoint risk score.

What should you implement to meet each requirement? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

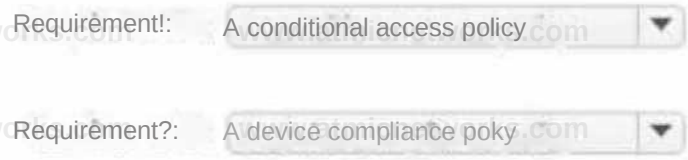
Answer



Answer:

Explanation:

Answer



Question: 218

HOTSPOT

You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to assign roles in Intune to meet the following requirements:

- The members of Group1 must manage Intune roles and assignments.
- The members of Group2 must assign existing apps and policies to users and devices.

The solution must follow the principle of least privilege.

Which role should you assign to each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Groupl: Intune Service Administrator
Help Desk Operator Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

Group2: Policy and Profile Manager Help Desk Operator
Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

Answer:

Explanation:

To assign roles in Intune to meet the requirements, you should assign the following roles to each group:

Group1: Intune Role Administrator Group2: Help Desk Operator

The Intune Role Administrator role is the only Intune role that can manage custom Intune roles and add assignments for built-in Intune roles1. This role meets the requirement for Group1 to manage Intune roles and assignments.

The Help Desk Operator role can perform remote tasks on users and devices, and can assign applications or policies to users or devices1. This role meets the requirement for Group2 to assign existing apps and policies to users and devices.

Question: 219

HOTSPOT

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

Name	Platform	Encryption	Secure Boot	Member of
Devicel	Windows 10	Yes	No	Group
Device?	Windows 10	No	Yes	Group?
Devices	Android	No	Nor *applicable*	GroupS

Intune includes the device compliance policies shown in the following table.

Name	Platform	Encryption	Secure Boot
Policy 1	Windows 10	Not configured	Not configured
Policy?	Windows 10	Not configured	Required
Policy^	Windows 10	Required	Required
Policy4	Android	Not configured	*Not applicable*

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group1
Policy2	Group1, Group2
Policy3	Group3
Policy4	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 ^
Devicel is marked as compliant	
Device? is marked as compliant	
Devices is marked as compliant	

Answer:

Explanation:

Device1 is marked as compliant = No Device2 is marked as compliant = Yes Device3 is marked as compliant = No

Device1 is marked as noncompliant because it does not meet the minimum OS version requirement of Policy1, which is 11.0.0. Device1 has an OS version of 10.0.0, which is lower than the required version1.

Device2 is marked as compliant because it meets all the requirements of Policy2, which are: minimum OS version of 10.0.0, password required, and encryption enabled. Device2 has an OS version of 11.0.0, a password set, and encryption enabled1.

Device3 is marked as noncompliant because it does not meet the encryption requirement of Policy3, which is enabled. Device3 has encryption disabled1.

Question: 220

HOTSPOT

You have an Azure AD tenant named contoso.com that contains a user named Used. User! has a user principal name (UPN) of user1@contoso.com.

You join a Windows 11 device named Client 1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

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

net kxalgroup * [net accounts	Administrators /add ' ^CONTOSO	\userl^contoso.co«"
	AzureAD	

net localqroup

l net user UPN

Answer:

Explanation:
net localgroup Administrators /add “AzureAD\user1@contoso.com”

This command will add the Azure AD user with the UPN of user1@contoso.com to the local Administrators group of the device1. You need to use the AzureAD prefix and double backslashes to specify the user’s domain2. You also need to enclose the user’s name in quotation marks if it contains special characters like @1.
You can run this command from an elevated command prompt on Client1, or remotely by using PowerShell or other tools1. You can also use the Intune Role Administrator role or the Additional local administrators on all Azure AD joined devices setting to manage the local administrators group on Azure AD joined devices34.

Question: 221

HOTSPOT
You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft intune as shown in the following table.

Name	Platform	Member of	Description
Devicel	Windows 11	Group 1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Groups	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.
Intune has the device compliance policies shown in the following table.

Name	Platform	Setting	Applied to
Compliance!	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	GroupS

The Compliance policy settings are configured as shown in the exhibit. (Click the Exhibit tab.) You create the following Conditional Access policy:

Compliance policies | Compliance policy settings

These settings configure the way the compliance service treats devices Each device evaluates these as a 'Built-in Device Compliance Policy' which is reflected in device mentoring

Maric devices with no compliance policy assigned as Compliant

Enhanced jailbreak detection Q Disabled

Compliance status validity period (days) Q 30

- Name: Policy1
- Assignments

o Users and groups: User1

o Cloud apps or actions: Office 365 SharePoint Online

- Access controls

o Grant Require device to be marked as compliant

- 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 Microsoft SharePoint Online from Devicel by using Microsoft Edge.		
User! can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.		
User! can access Microsoft SharePoint Online from Devices by using Microsoft Edge.	O	

Answer:

Explanation:

Answer Area

Statemenu	Yes	No
User 1 can access Microsoft SharePoint Online from Devicel by using Microsoft Edge.	O	#
Useri can access Microsoft SharePoint Online from Device? by using Microsoft Edge	•	
Useri can access Microsoft SharePoint Online from Devices by using Microsoft Edge.	O	•

Question: 222

You have an Azure AD tenant named contoso.com.
You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com. What should you configure?

A. Windows Autopilot
B. provisioning packages for Windows
C. Security defaults in Azure AD
D. Device settings in Azure AD

Answer: D

Explanation:

To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users. By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected1.

The other options are not relevant for this scenario because:

Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune. It does not control the local administrator role of the users who join the devices2.

Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users3.

Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role4.

Reference: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security defaults?

Question: 223

You have an Azure subscription.

You have an on-premises Windows 11 device named Device 1.

You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription.

To what should you associate DCR1 ?

A. Azure Network Watcher
B. Device1
C. a Log Analytics workspace
D. a Monitored Object

Answer: B

Explanation:

To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it. A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1. To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2. You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.

The other options are not correct for this scenario because:

Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources. It is not related to data collection rules or Azure Monitor4.

A Log Analytics workspace is a destination where you can send the data collected by a data collection rule. It is not an entity that you can associate a DCR with5.

A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules. Reference: Data collection rules in Azure Monitor, Configure data collection for Azure Monitor Agent, Use Azure Policy to install Azure Monitor Agent and associate with a DCR, What is Azure Network Watcher?, Log Analytics workspaces in Azure Monitor

Question: 224

You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.

You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enroll the devices in Microsoft Intune by using the Intune Company Portal.
B. Create a compliance policy.
C. Enroll the devices in Microsoft Intune by using Apple Business Manager.
D. Create an iOS app provisioning profile.
E. Create a device configuration profile.

Answer: C, E

Explanation:

To deploy a specific iOS update to the unmanaged iPad devices, you need to perform the following actions:

Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to create device groups and assign roles and permissions12.

Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices34.

The other options are not correct for this scenario because:

Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune. However, this method requires user interaction and consent, and does not enroll the devices as supervised devices5. Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings. However, a compliance policy does not deploy or manage software updates on the devices6.

Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune. However, an iOS app provisioning profile does not affect the software updates on the devices7.

Reference: What is Apple Business Manager?, Enroll iOS/iPadOS devices in Intune, Manage iOS/iPadOS software update policies in Intune, Software updates planning guide and scenarios for supervised iOS/iPadOS devices in

Microsoft Intune, Enroll your personal device in Intune, Device compliance policies in Microsoft Intune, Add an iOS app provisioning profile with Microsoft Intune

Question: 225

HOTSPOT

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

You use Microsoft Intune to manage devices.

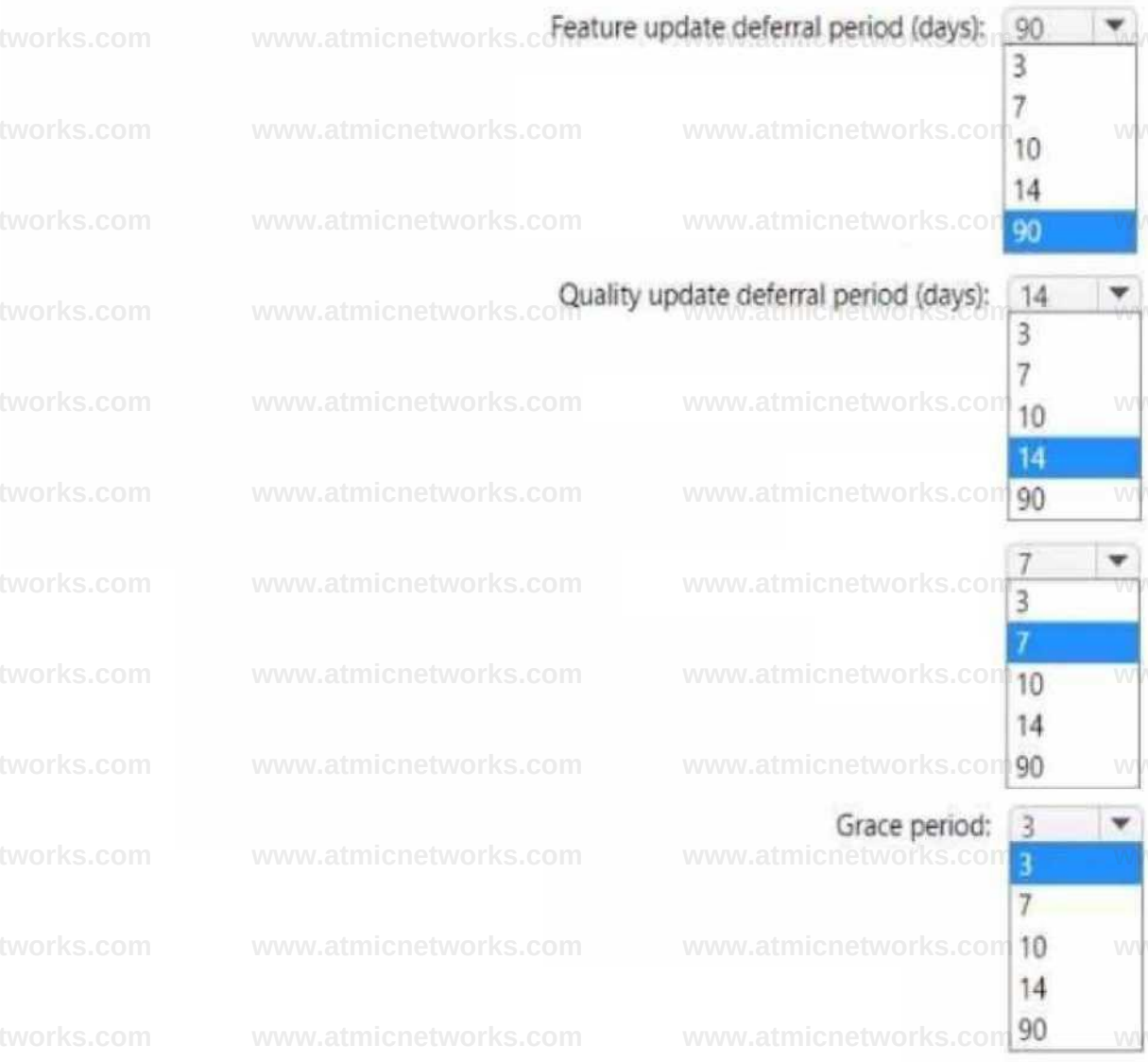
You need to configure an update ring that meets the following requirements:

- Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.
- The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.
- Devices must restart automatically three days after an update is installed.

How should you configure the update ring? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Feature update deferral period (days): 90

Quality update deferral penod (days): 14

Deadline for feature updates: 7

Grace penod: 3

Question: 226

You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

A. 30 days
B. 60 days
C. 90 days
D. 365 days

Answer: B

Explanation:

The Device compliance trends report shows the number of devices that are compliant, noncompliant, and not evaluated over time. The report displays trend data for the last 60 days by default, but you can change the time range to view data for the last 7, 14, or 30 days as well. The report does not show data for more than 60 days.
Reference: [Device compliance trends report]

Question: 227

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.
You plan to manage Microsoft Defender Antivirus on the computers.
You need to prevent users from disabling Microsoft Defender Antivirus,
What should you do?

A. From the Microsoft Intune admin center, create a security baseline.
B. From the Microsoft 365 Defender portal, enable tamper protection.
C. From the Microsoft Intune admin center, create an account protectionpolicy.
D. From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.

Answer: B

Explanation:

Tamper protection is a feature of Microsoft Defender Antivirus that prevents users or malicious software from disabling or modifying the antivirus settings. Tamper protection can be enabled from the Microsoft 365 Defender portal for devices that are Azure AD joined and enrolled in Microsoft Intune. This will prevent users from turning off Microsoft Defender Antivirus or changing its configuration through Windows Security, PowerShell, Registry, or Group Policy. Reference: [Enable tamper protection]

Question: 228

HOTSPOT

You have 1,000 computers that run Windows 10 and are members of an Active Directory domain.

You need to capture the event togs from the computers to Azure.

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

NOTE: Each correct selection is worth one point.

Answer Area

Azure service to provision: Log Analytics
An Azure Storage account
Azure Cosmos DB
Azure SQL Database

Action to perform on the computers: Install the Azure Monitor Agent
install the Azure Monitor Agent
Enroll in Microsoft Intune
Register to Azure AD

Answer:

Explanation:

Answer Area

Azure service to provision: Log Analytics

Action to perform on the computers: Install ihe Azure Monitor Agent

Question: 229

You have a computer named Computed that has Windows 10 installed.

You create a Windows PowerShell script named config.psl.

You need to ensure that config.psl runs after feature updates are installed on Computer5.

Which file should you modify on Computer5?

A. LiteTouch.wsf
B. SetupConfig.ini
C. Unattendb*
D. Unattend.xml

Answer: B

Explanation:

SetupConfig.ini is a file that can be used to customize the behavior of Windows Setup during feature updates. You can use this file to specify commands or scripts that run before or after the installation process. To run a PowerShell script after a feature update, you can use the PostOOBE parameter in SetupConfig.ini and specify the path to the script file. Reference: [SetupConfig.ini reference]

Question: 230

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices. You need to create Intune configuration profiles to perform the following actions on the devices:

- Deploy a custom Start layout.
- Rename the local Administrator account.

Which profile type template should you use for each action? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area

Deploy a custom Stan layout Device restncton

I Delivery optimization

Endpoint protection

Identity protection

Rename the local Administrator account: Identity protection

Device restriction

Endpoint protection

Answer:

Explanation:

Answer Area

Deploy a custom Start layout Device restnction

Rename the local Administrator account Identity protection

Question: 231

HOTSPOT

You have a Microsoft 365 subscription.

You plan to enable Microsoft Intune enrollment for the following types of devices:

- Existing Windows 11 devices managed by using Configuration Manager
- Personal iOS devices

The solution must minimize user disruption.

Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 11 devices managed by using Configuration Manager Windows Autopilot Co-management User enrollment

Windows Autopilot

Personal iOS devices; | Automated Device Enrollment (ADE) | Apple Configurator

Automated Device Enrollment (ADE)

[User enrollment

Answer:

Explanation:

Answer Area

Windows 11 devices managed by using Configuration Manager | Windows Autopilot '

Personal iOS devices: Automated Device Enrollment (ADE)

Question: 232

You have a Windows 10 device named Device! that is joined to Active Directory and enrolled in Microsoft Intune.
Device1 is managed by using Group Policy and Intune.
You need to ensure that the Intune settings override the Group Policy settings.
What should you configure?

A. a device configuration profile
B. a device compliance policy
C. an MDM Security Baseline profile
D. a Group Policy Object (GPO)

Answer: A

Explanation:

A device configuration profile is a collection of settings that can be applied to devices enrolled in Microsoft Intune. You can use device configuration profiles to manage Windows 10 devices that are joined to Active Directory and enrolled in Intune. To ensure that the Intune settings override the Group Policy settings, you need to enable the policy CSP setting called MDMWinsOverGP in the device configuration profile. This setting will give precedence to the MDM policy over any conflicting Group Policy settings.
Reference: [Use policy CSP settings to create custom device configuration profiles]

Question: 233

HOTSPOT

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the

following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- MDM user scope: Group1
- MAM user scope: 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	Yes	No
Userl can enroll Devicel in intune by using automatic enrollment.		
Useri can enroll Device? in Intune by using automatic enrollment.		
User2 can enroll Devicel in Intune by using automatic enrollment		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Userl can enroll Devicel in intune by using automatic enrollment		
Userl can enroll Device? in Intune by using automatic enrollment.		
User? can enroll Devicel in Intune by using automatic enrollment.		

Question: 234

HOTSPOT

You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.)

Home > Endpoint security > MOM Security Baseline >

Create profile

Block Office applications from injecting code into other processes ©	Disable v
Block Office applications from creating executable content ©	Audit mode v
Block all Office applications from creating child processes ©	Audit mode ^
Block Win32 API calls from Office macro G	Disable v
Block execution of potentially obfuscated scripts (js/vbs/ps) 0	Disable v

You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR tab.)

Home > Endpoint security > ASR Endpoint security >

Edit profile

Attack Surface Reduction Rules

Block credential stealing from the Windows Audit mode local security authority subsystem (bass.exe) O

Block Adobe Reader from creating child Audit mode processes ©

Block Office applications from injecting | Audit mode code into other processes ©

Block Office applications from creating | Audit mode executable content ©

You plan to deploy both profiles to devices enrolled in Microsoft Intune. You need to identify how the following settings will be configured on the devices:

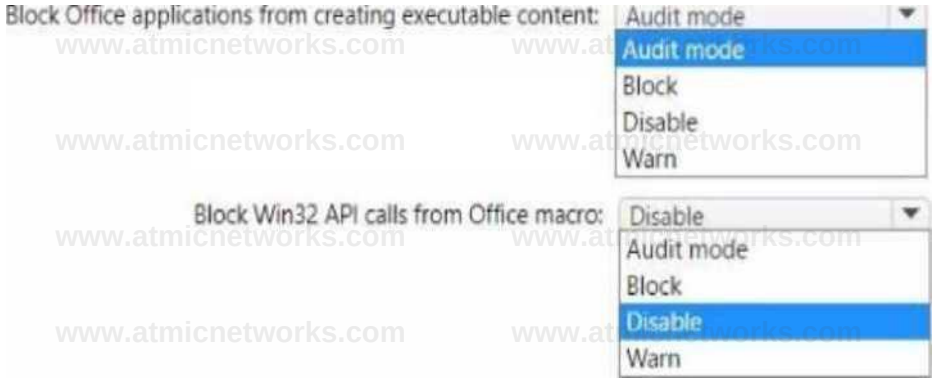
- Block Office applications from creating executable content
- Block Win32 API calls from Office macro

Currently, the settings are disabled locally on each device.

What are the effective settings on the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Block Office applications from creating executable content: [Audit mode

Block Win32 API calls from Office macro: Disable

Question: 235

DRAG DROP

You have an on-premises Active Directory domain that syncs to Azure AD tenant.

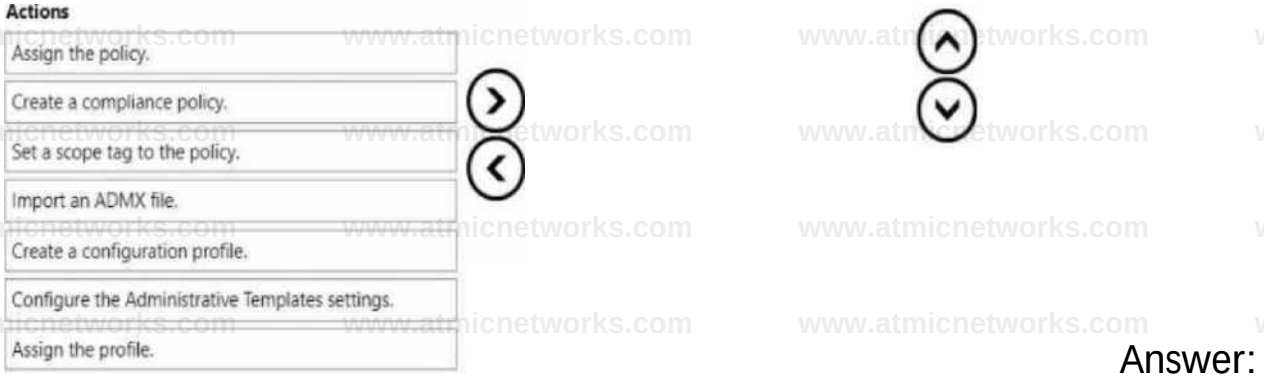
The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune.

The Microsoft Office settings on the computers are configured by using an Group Policy Object (GPO).

You need to migrate the GPO to Intune.

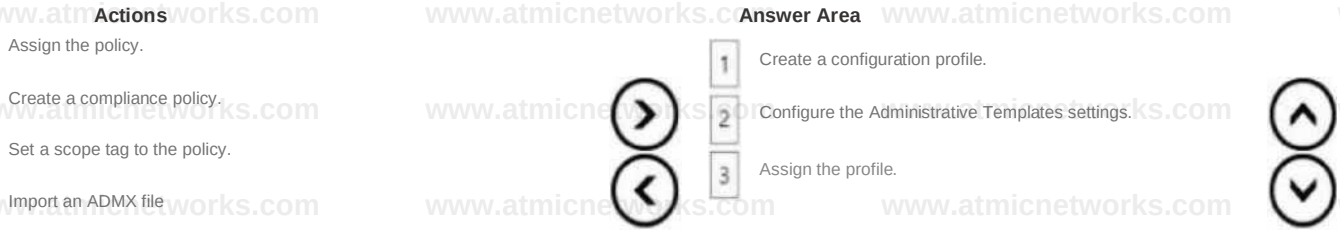
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer Area



Answer:

Explanation:



Question: 236

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains 100 client computers that run Windows 10.

Currently, your company does NOT have a deployment infrastructure.

The company purchases Windows 11 licenses through a volume licensing agreement.

You need to recommend how to upgrade the computers to Windows 11. The solution must minimize licensing costs.

What should you include in the recommendation?

A. Microsoft Deployment Toolkit (MDT)
B. Configuration Manager
C. subscription activation
D. Windows Autopilot

Answer: A

Explanation:

Question: 237

You have a Microsoft Intune subscription associated to an Azure AD tenant named contoso.com. Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com.

You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment process. The solution must minimize the number of changes.

Which DNS records do you need?

A. three CNAME records
B. one CNAME record only
C. three TXT records
D. one TXT record only

Answer: A

Explanation:

Question: 238

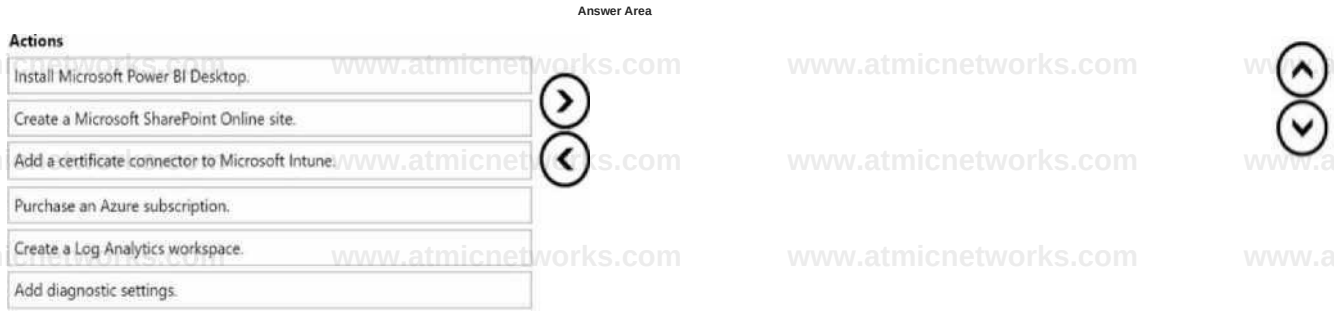
DRAG DROP

Your company has a Microsoft 365 E5 tenant.

All the devices of the company are enrolled in Microsoft Intune.

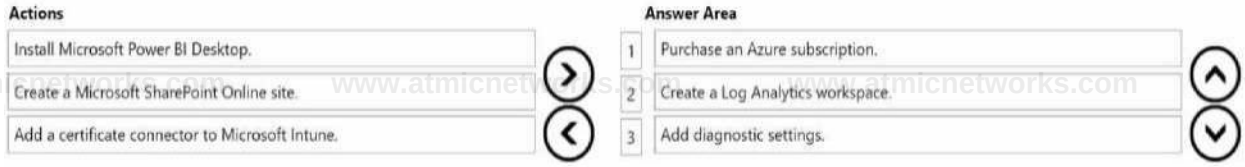
You need to create advanced reports by using custom queries and visualizations from raw Microsoft Intune data.

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: 239

You manage 1,000 computers that run Windows 10. All the computers are enrolled in Microsoft Intune. You manage the servicing channel settings of the computers by using Intune.

You need to review the servicing status of a computer.

What should you do?

A. From Software updates, view the Per update ring deployment state.
B. From Software updates, view the audit logs.
C. From Device configuration - Profiles, view the device status.
D. From Device compliance, view the device compliance.

Answer: A

Explanation:

Question: 240

You have a workgroup computer named Client1 that runs Windows 11 and connects to a public network.

You need to enable PowerShell remoting on Client1. The solution must ensure that PowerShell remoting connections are accepted from the local subnet only.

Which PowerShell command should you run?

A. Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
B. Set-PSSessionConfiguration -AccessMode Local
C. Enable-PSRemoting -Force
D. Enable-PSRemoting -SkipNetworkProfileCheck

Answer: D

Explanation:

Question: 241

HOTSPOT

You have a Microsoft 365 subscription.

You need to enable passwordless authentication for all users. The solution must meet the following requirements:

- Users in the research department cannot use mobile devices and must authenticate from unmanaged Linux devices by using an alternative method.
- To access services, users in the sales department must authenticate by using their mobile phone.
- Administrative effort must be minimized.

Which authentication method should you use for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sales: | Windows Hello for Business ▼

FIDO2 security keys
Microsoft Authenticator
Temporary Access Pass
Windows Hello for Business

Research: [Temporary Access Pass ▼

FIDO2 security keys
Microsoft Authenticator
lemporary Access Pass |
Windows Hello for Business

Answer:

Explanation:

Answer Area

Sales: Windows Hello for Business

Research: Temporary Access Pass

Question: 242

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

Name	Platform
Devicel	Windows
Device?	Android
Device?	iOS
Device4	macOS

For which devices can you manage updates by using intune?

A. Devic1I only
B. Device1 and Oevice2 only
C. Device 1 and Device3 only
D. Device 1. Device3, and Device4 only

E. Device 1. Device2, Device3, and Device4

Answer: D

Explanation:

Question: 243

You have a Microsoft 365 subscription that has Windows 365 Enterprise licenses.

You plan to use a custom Windows 11 image as a template for Cloud PCs.

You have a Hyper-V virtual machine that runs Windows 11 and has the following configurations:

- Name: VM1
- Disk size: 64 GB
- Disk format: VHDX
- Disk type: Fixed size
- Generation: Generation 2

You need to ensure that you can use VM1 as a source for the custom image. What should you do on VM1 first?

A. Change the disk type to Dynamically expanding
B. Change the disk format to the VHD
C. Change the generation to Generation 1.
D. Increase the disk size.

Answer: B

Explanation:

Question: 244

DRAG DROP

Your on-premises network contains an Active Directory Domain Services (AD DS) domain.

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains five virtual machines and is NOT connected to the on-premises network.

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

You purchase Windows 365 Enterprise licenses.

You need to deploy Cloud PC. The solution must meet the following requirements:

- All users must be able to access their Cloud PC at any time without any restrictions.
- The users must be able to connect to the virtual machines on VNet1.

How should you configure the provisioning policy for Windows 365? To answer, drag the appropriate options to the correct settings.
Each option 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: 245

You have a Microsoft 365 subscription that contains a user named User1.
You use Microsoft in tune to manage devices that run Windows 11.
You need to remove User1 from the local Administrators group on all enrolled devices. The solution must minimize administrative effort.
What should you configure?

A. a device compliance policy
B. an app configuration policy
C. an account protection policy

Answer: C

Explanation:

Question: 246

You have a Microsoft 365 subscription that includes Microsoft Intune.
You need to deploy a custom app to Android devices. The app uses the APK file format. Which type of app should you select for the deployment?

A. built-in
B. Android store
C. Managed Google Play
D. line-of-business (LOB)
E. web link

Answer: D

Explanation:

Question: 247

You have a Microsoft 365 ES subscription.
You use Microsoft Intune to manage all devices.
You need to prepare a Win32 app named Appl.exe for deployment.
What should you do first?

A. From the Microsoft Intune admin center, create an app configuration policy.
B. Change App1.exe to the INIUNEW1N format.
C. From the Microsoft 365 Apps admin center, create a deployment configuration
D. Upload App1 exe to Azure Blob Storage.

Answer: B

Explanation:

Question: 248

HOTSPOT
You have a Microsoft 36S subscription, use Microsoft Intune. and have the users shown in the following table.

Name	Member of
User1	Group1
User2	None
User3	None

You create a policy set named Set1 as shown in the exhibit. (Click the Exhibit tab.)

Device management lit

Device configuration profiles (I)

Name	Platform	Profile Type
ConfigurationProlHel	Windows 10 and later	Device restrictions

Device compliance potties (1)

Name	Platform	Policy Type
Compliant ePolicyl	Windows 10 and later	Windows 10 and later co

Device enrollment Edit

Wmdowt autopilot deployment profile!

NO result!

Enrolment status pages

No resets

Assignments Edit

Included groups	Al Users
Excluded groups	6roup 1

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

Name	Operating system	User
Device 1	Windows 10	User'
Device2	Windows 11	User 2
Device 5	Android	User}

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

Answer Area

Statements	Yes	No
If Useri signs in to Devicel. Devicel will have both ConfigurationProfilel and CompliancePolicyl assigned.	O	O
If User? signs in to Device?. Device? will have both ConfigurationProfilel and CompliancePolicyl assigned.		
If User) signs in Io Device?. Device? will have both ConfigurationProfilel and CompliancePolicyl assigned.	0	

Answer:

Explanation:

Answer Area

Statements	Yes	No
If Useri signs in to Devicel. Devicel will have both ConfigurationProfilel and CompliancePolicyl assigned.	O	9
If User? signs in to Device?. Device? will have both ConfigurationProfilel and CompliancePolicyl assigned.	*	
If User? signs in to Device?. Device? will have both ConfigurationProfilel and CompliancePolicyl assigned.	0	*

Question: 249

HOTSPOT

Your network contains an Active Directory domain.

The domain contains four computer named Computer 1. Computet2. Computed, and Computer4 that run Windows 10. Vou perform the following actions:

- On Computer1, you install Windows Admin Center and configure Windows Defender Firewall to allow incoming communication over TCP pons 80.443. and 6516.
- On Computed, you run the Enable-PS Remoting cmdlet.
- On Computer 3, you configure Windows Defender firewall to allow Windows Remote Management (WinRM) traffic
- On Computer4, you run the winrm quickconfig command.

You need to manage the computers remotely by using Windows Admin Center.

From which computers can you connect to Windows Admin Center, and which computers can you manage by using Windows Admin Center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Explanation:

Answer:

Answer Area

Connect from: Computeri only

Manage: Computeri, Computed, Computer}, and Computer^

Question: 250

You have the Windows 10 devices shown in the following table.

Name	Operating system	Edition
Device!	64-b4 version of Windows 10	Home
Dev»ce2	32*b*t version of Windows 10	Pro
Device 3	64-bit version of Windows 10	Enterprise
Dewe4	64-bit version of Windows 10	Pro

You plan to upgrade the devices to Windows 11 Enterprise.
On which devices can you perform a direct in-place upgrade to Windows 11 Enterprise?

A. Device3 only
B. Device 3 and Device 4 only
C. Device2. Device3. and Devtce4 only
D. Device1. Device3, and Devtce4 only
E. Device1, Device2. Device3. and Devke4 only

Answer: A

Explanation:

https://learn.microsoft.com/en-us/windows/deployment/upgrade/windows-upgrade-paths https://learn.microsoft.com/en-us/windows/deployment/upgrade/windows-edition-upgrades

Question: 251

You have a Microsoft Deployment Toolkit (MDT) deployment shore.
You plan to deploy Windows 11 by using the Standard Client Task Sequence template.
You need to modify the task sequence to perform the following actions:

- Format disks to support Unified Extensible Firmware Interface (UEFI).
- Create a recovery partition.

Which phase of the Task sequence should you modify?

A. Preinstall
B. Install
C. Initialization
D. Post Install

Answer: A

Explanation:

Question: 252

You have a Microsoft 365 subscription that includes Microsoft Intune.
You have 500 corporate-owned Android devices enrolled as fully managed devices.
You need to prepare an app named App1 for deployment to the 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 the Intune Company Portal, download Appl.

B. Create an OEMConfig profile.
C. From the Managed Google Play Store, approve App1.
D. Sync App1 with Intune.

Answer: C, D

Explanation:

https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work

Question: 253

You ate implementing Microsoft Intune Suite.
You enroll devices in Intune as shown in the following table.

Name	Platform
Device 1	Windows 11
Device?	Windows 10
Device3	Android
Devicd	iOS

The performance of which devices can be analyzed by using Endpoint analytics?

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

Answer: B

Explanation:

https://learn.microsoft.com/en-us/mem/analytics/overview#bkmk_prereq

Question: 254

You have a Microsoft 365 subscription. The subscription contains 500 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to manage the deployment of monthly security updates. The solution must meet the following requirements:

- Updates must be deployed to a group of test computers for quality assurance.
- Updates must be deployed automatically 15 days after the quality assurance testing.

What should you create in the Microsoft Intune admin center?

A. a device Configuration profile
B. an update ring
C. a feature update policy
D. a security baseline

Answer: B

Explanation:

Question: 258

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

You use Microsoft Intune to manage Windows 11 devices.

You create a new policy set named Set and add five device configuration profiles for Windows 10 and later.

You create a device compliance policy named Policy1.

You need to ensure that when users are assigned the device configuration profiles in Set1, they are always assigned Policy1 also.

What should you configure?

A. the assignments of Policy1
B. the Policy1 configurations
C. the assignments of Set1
D. the Set1 configurations

Answer: D

Explanation:

You can include the following management objects in a policy set:
Apps
App configuration policies
App protection policies
Device configuration profiles
Device compliance policies
Windows autopilot deployment profiles
Enrollment status page
Settings catalog policies

Question: 259

HOTSPOT

You have a Microsoft 365 tenant that uses Microsoft Intune.

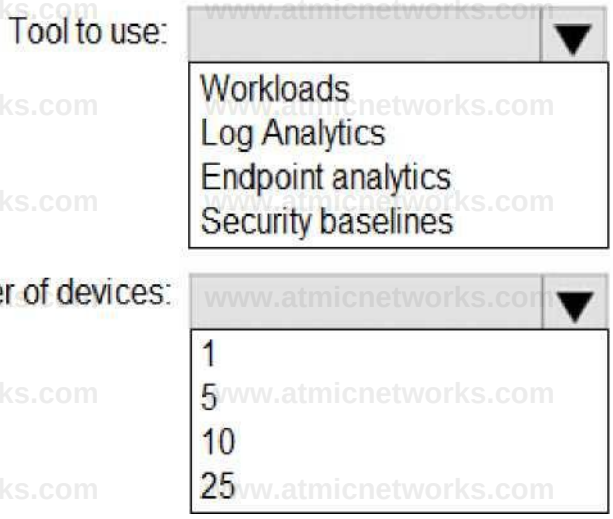
From the Microsoft Intune admin center, you plan to create a baseline to monitor the Startup score and the App reliability score of enrolled Windows 10 devices.

You need to identify which tool to use to create the baseline and the minimum number of devices required to create 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 Area



Answer:

Explanation:

Endpoint Analytics
Minimum 10 devices

(Ref: https://learn.microsoft.com/en-us/mem/analytics/startup-performance#bkmk_report:~:text=The%20table%20only%20lists%20processes%20that%20affect%20a%20minimum%20of%2010%20devices%20in%20your%20tenant.)

Question: 260

You have the devices shown in the following table.

Name	Operating system	Domain member
Device1	Windows 11 Enterprise	No
Device2	Windows 10 Pro	Yes
Device3	Android	No
Device4	Mac OS X	No

You plan to implement Microsoft Defender for Endpoint.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint.

What should you identify?

A. Device1 only

B. Device2 only

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

Answer: D

Explanation:

Here is the list of Windows versions. Win10 and Win11 supported. The sentence "(standalone or as part of other Microsoft 365 plans)" excludes the domain needs.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum- requirements?view=o365-worldwide

Here is the link for Android. No information about the specific version therefore it is supported. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender- endpoint-android?view=o365-worldwide

Here is the link for MacOS
System requirements: 14 (Sonoma), 13 (Ventura), 12 (Monterey). MAC OS X is older therefore unsupported.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender- endpoint-mac?view=o365-worldwide

Question: 261

HOTSPOT -

You have a Microsoft 365 subscription. The subscription contains 1,000 computers that run Windows 11 and are enrolled in Microsoft Intune.

You plan to create a compliance policy that has the following options enabled:

- Require Secure Boot to be enabled on the device.
- Require the device to be at or under the machine risk score.

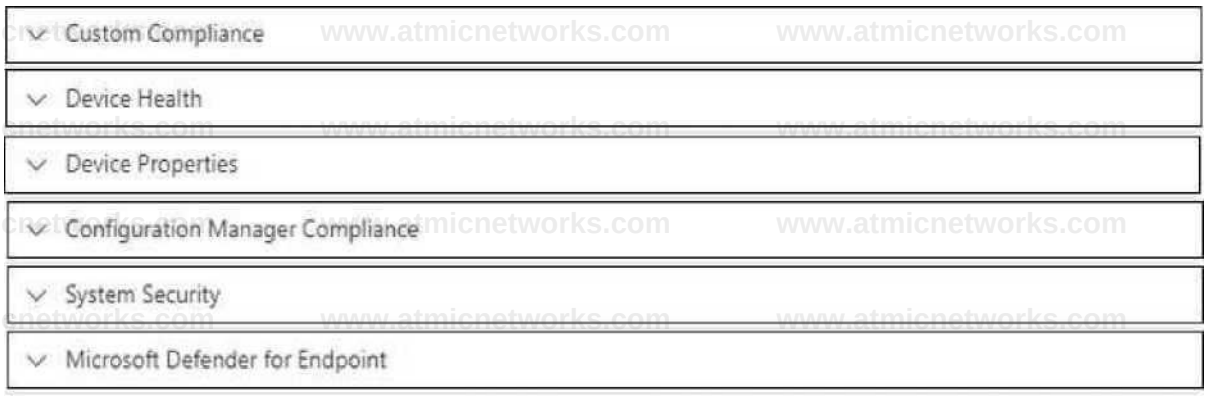
Which two Compliance settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 10/11 compliance policy

O Basics 0 Compliance settings



Answer:

Explanation:

Device health
https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status
Microsoft Defender for Endpoint
https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows#microsoft-defender-for-endpoint

Question: 262

You have a Microsoft 365 subscription.

You use app protection policies to protect corporate data on Android devices.

You need to ensure that any user connecting from an Android device can only access the corporate data if they connect from an app that supports mobile application management (MAM).

What should you configure?

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

Answer: B

Explanation:

https://learn.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune#:~:text=Microsoft%20Intune%20app%20protection%20policies%20work%20with%20Microsoft%20Entra%20Conditional%20Access%20to%20help%20protect%20your%20organizational%20data%20on%20devices%20your%20employees%20use.

Question: 263

DRAG DROP

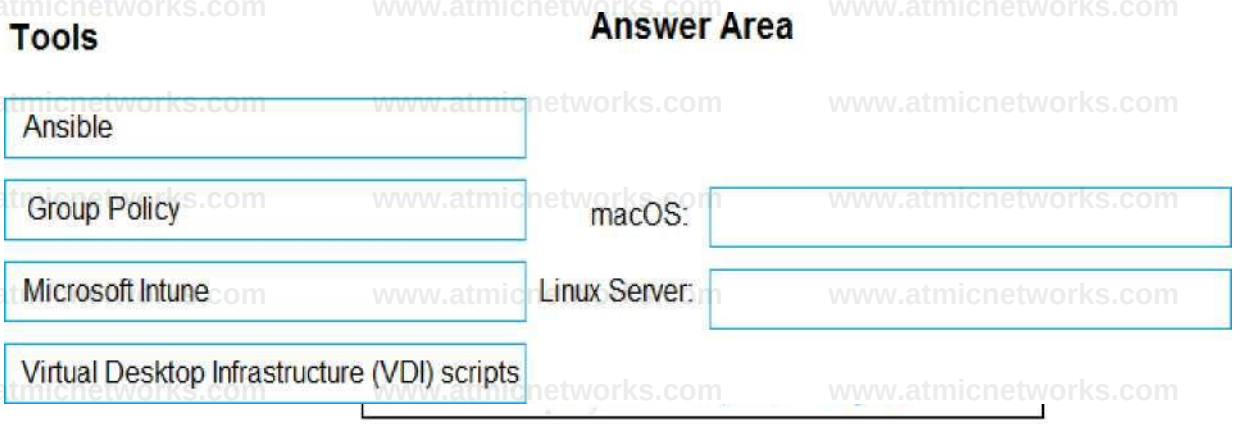
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You plan to onboard the following types of devices to Defender for Endpoint:

- macOS
- Linux Server

What should you use to onboard each device? To answer, drag the appropriate tools to the correct device types. Each tool 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:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/linux-install-with-ansible?view=o365-worldwide https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac?view=o365-worldwide

Question: 265

DRAG DROP

You have an on-premises Active Directory domain that syncs to Azure AD tenant.

The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune.

The Microsoft Office settings on the computers are configured by using a Group Policy Object (GPO).

You need to migrate the GPO to Intune.

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

Assign the policy.

Create a compliance policy.

Set a scope tag to the

Import an ADMX file.

Create a configuration profile.

Configure the Administrative

Assign the profile.

Answer Area

Answer:

Explanation:

Answer Area

1. Create a configuration profile.
2. Configure the Administrative Templates settings.
3. Assign the profile.

https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows

Question: 266

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

- Ensure that you can manage the personal devices by using Microsoft Intune.
- Ensure that users can access company data seamlessly from their personal devices.
- Ensure that users can only sign in to their personal devices by using their personal account.

What should you use to add the devices to Azure AD?

A. Azure AD registered Most Voted
B. hybrid Azure AD join
C. Azure AD joined

Answer: A

Explanation:

zure AD registered devices meet all your requirements:

Microsoft Intune management: Azure AD registered devices can be managed by Microsoft Intune, allowing you to configure policies, apply security settings, and distribute apps.
Seamless data access: Users can access company data through approved mobile apps using their personal accounts. Conditional Access policies can ensure secure access while respecting their personal device ownership.
Personal account sign-in: Users can only sign in to their devices using their personal accounts, as Azure AD registered devices don't join the domain and don't require work or school credentials.

Azure AD joined and hybrid Azure AD join wouldn't be suitable choices in this case:

Azure AD joined devices are domain-joined, requiring users to sign in with work or school credentials, violating your requirement for personal accounts.
Hybrid Azure AD join combines on-premises Active Directory with Azure AD, adding complexity and not aligning with your need for purely personal device management.

Question: 267

DRAG DROP -

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune.

You need to create Endpoint security policies to enforce the following requirements:

- Computers that run macOS must have FileVault enabled.
- Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.
- Computers that run Windows 10 must have Microsoft Defender Application Control enabled.

Which Endpoint security feature should you use for each requirement? 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.

Features

Account protection

Attack surface reduction (ASR)

Disk encryption

Endpoint detection and response (EDR)

Answer Area

Computers that run macOS must have FileVault enabled:

Computers that run Windows 10 must have Microsoft Defender Application Control enabled:

Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled:

Answer

Explanation:

Answer Area

Computers that run macOS must have FileVault enabled: Disk encryption

Computers that run Windows 10 must have Microsoft Defender Application Control enabled: Attack surface reduction (ASR)

Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled: Account protection

Disk Encryption

ASR - Ref https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy#:~:text=Application%20control%20%2D%20Application,Constrained%20Language%20Mode.

Account Protection - Ref https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/configure?tabs=intune#:~:text=You%20can%20also%20configure%20Credential%20Guard%20by%20using%20an%20account%20protection%20profile%20in%20endpoint%20security.

Question: 268

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

Name	Member of
Device1	Group1
Device2	Group1
Device3	Group1

The devices are managed by using Microsoft Intune.

You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the device security settings match the settings specified in the policy.
You discover that devices that are not members of Group1 are shown as Compliant.

You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not compliant.

What should you do from the Microsoft Intune admin center?

A. From Device compliance, configure the Compliance policy settings.
B. From Endpoint security, configure the Conditional access settings.
C. From Tenant administration, modify the Diagnostic settings.
D. From Policy1, modify the actions for noncompliance.

Answer: A

Explanation:

https://learn.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#:~:text=Device%20compliance%20%3E%20Compliance%20policy%20settings

Question: 269

You have a Microsoft 365 subscription that includes Microsoft Intune.

You plan to use Windows Autopilot to deploy Windows 11 devices.

You need to meet the following requirements during Autopilot provisioning:

- Display the app and profile configuration progress.
- Block users from using the devices until all apps and profiles are installed

What should you configure?

A. an app configuration policy
B. an app protection policy
C. an enrollment device platform restriction
D. an enrollment status page

Answer: D

Explanation:

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

Question: 270

You need to assign the same deployment profile to all the computers that are configured by using Windows Autopilot.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create an Azure AD group that has dynamic membership rules and uses the ZTDID tag.

B. Create an Azure AD group that has dynamic membership rules and uses the operatingSystem tag.
C. Assign a Windows Autopilot deployment profile to a group.
D. Join the computers to Azure AD.
E. Create a Group Policy object (GPO) that is linked to a domain.
F. Join the computers to an on-premises Active Directory domain.

Answer: AC

Explanation:

Ref: https://learn.microsoft.com/en-us/autopilot/enrollment-autopilot#:~:text=To%20create%20a%20group%20that%20includes%20all%20of%20your%20Autopilot%20devices%2C%20enter%3A%20(device.devicePhysicalIDs%20%2Dany%20(_%20%2DstartsWith%20%22%5BZTDid%5D%22))

Question: 271

HOTSPOT

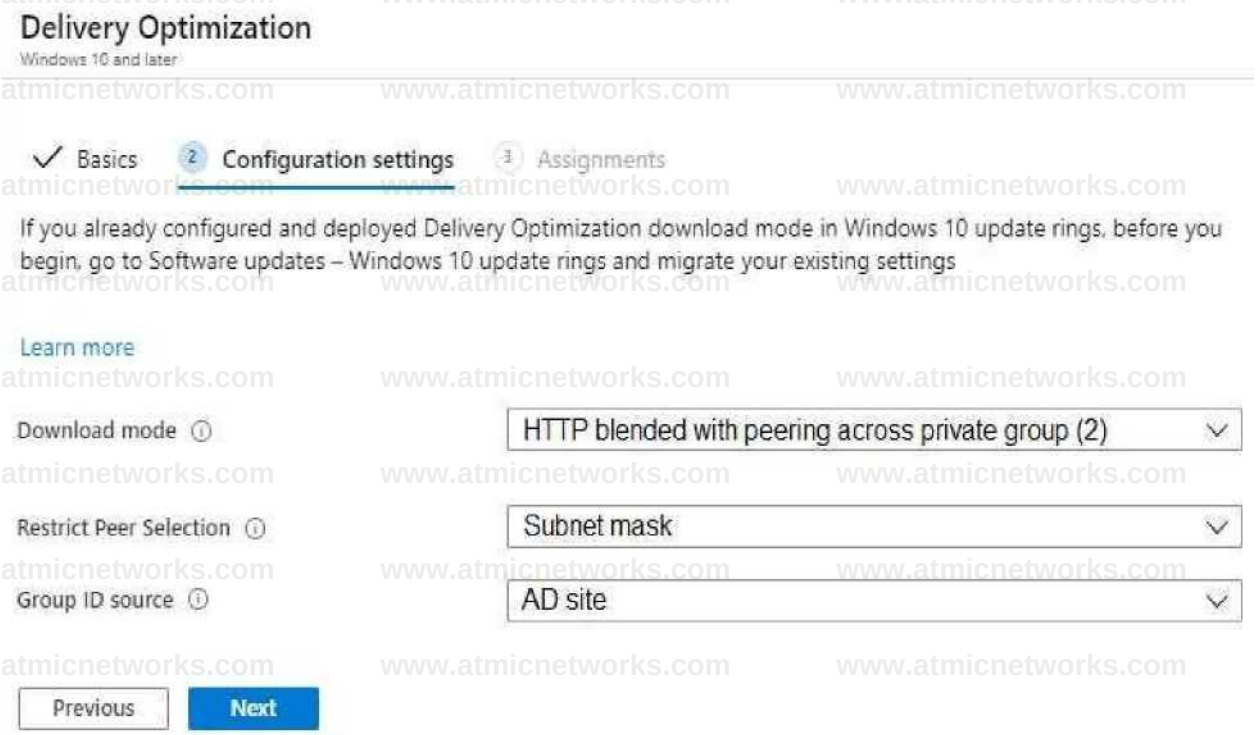
Your network contains an on-premises Active Directory domain that contains the locations shown in the following table.

Name	Internal IP address	Public Network Address Translation (NAT) IP address	Active Directory site
Location 1	10.10.0.0/16	131.10715.0/24	Sitel
Location2	10.20.0.0/16	131.107.16.0/24	Sitel
Locations	172.16.0.0/16	131.107.196.0/24	Site2

In Microsoft Intune, you enroll the Windows 10 devices shown in the following table.

Name	IP address
Device1	10.10.0.50
Device2	10.20.1.150
Device3	10.10.1.155
Device4	172.16.0.30

You have a Delivery Optimization device configuration profile applied to all the devices. The profile is configured as shown in the following exhibit.



From which devices can Device1 and Device2 get updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- Can get updates from Device3 only.
- Cannot get updates from any device.
- Can get updates from Device1 and Device3 only.
- Can get updates from Device1, Device3, and Device4.

Device2:

- Can get updates from Device3 only.
- Cannot get updates from any device.
- Can get updates from Device1 and Device3 only.
- Can get updates from Device1, Device3, and Device4.

Answer:

Explanation:

Device 1: only from Device 3

Device 2: cannot get updates from any device

Question: 272

HOTSPOT

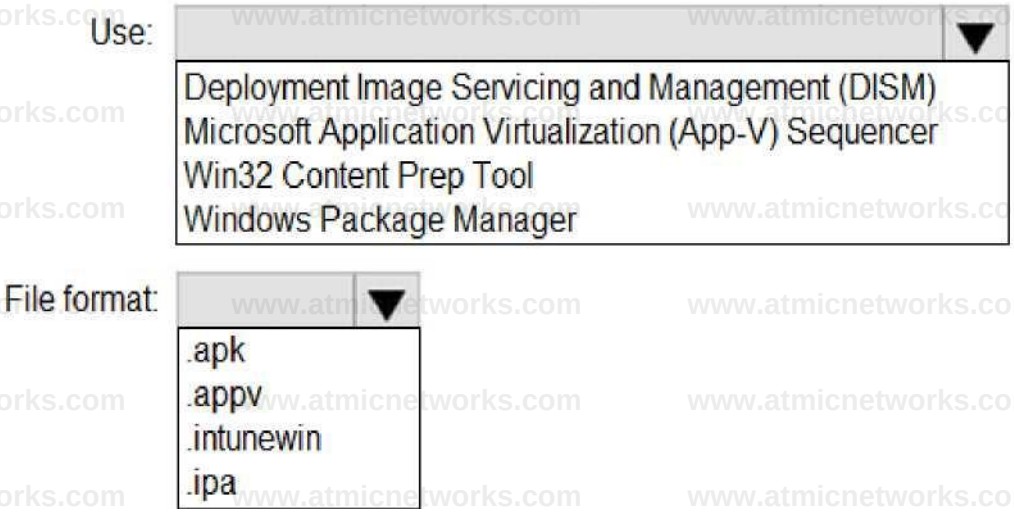
You have a Microsoft 365 E5 subscription that contains a computer named Computer1 that runs Windows 11. Computer1 is enrolled in Microsoft Intune.

You need to deploy an app named App1 to Computer1. The App1 installation will use multiple files.

What should you use to package App1, and which file format will be used? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

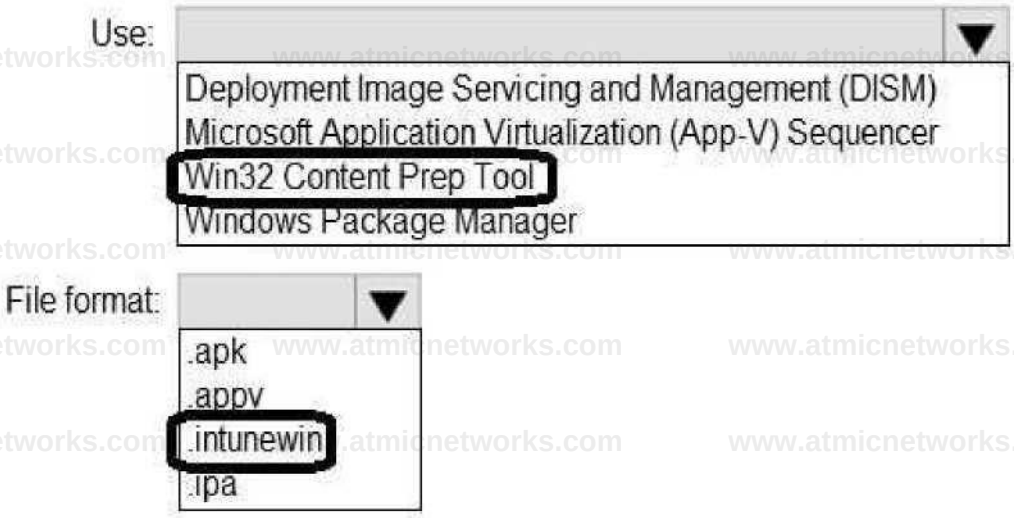
Answer Area



Answer:

Explanation:

Answer Area



"The Microsoft Win32 Content Prep Tool zips all files and subfolders when it creates the .intunewin file. Be sure to keep the Microsoft Win32 Content Prep Tool separate from the installer files and folders, so that you don't include the tool or other unnecessary files and folders in your .intunewin file."

Question: 273

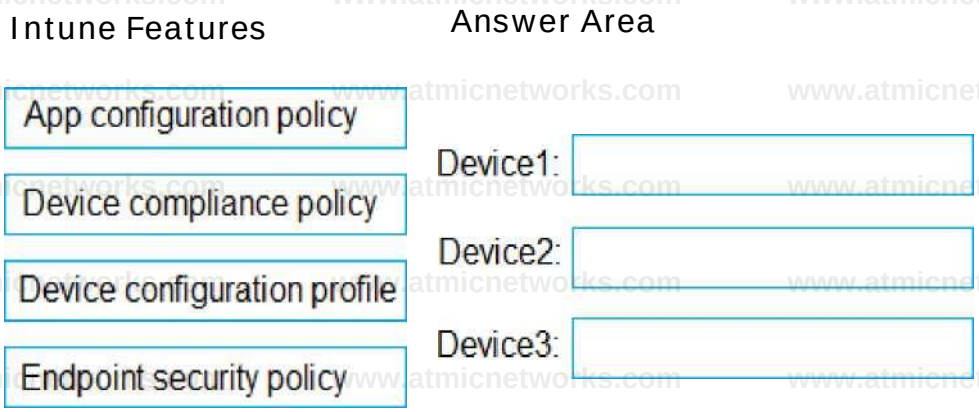
DRAG DROP

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

You need to configure the Microsoft Edge settings for each device.

What should you use? To answer, drag the appropriate Intune features to the correct devices. 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.



Answer:

Explanation:

Answer Area

Devicel: Device configuration profile

Device2: App configuration policy

Device3: App configuration policy

Windows: https://learn.microsoft.com/en-us/deployedge/configure-edge-with-intune#:~:text=You%20can%20configure%20Microsoft%20Edge%20policies%20and%20settings%20by%20adding%20a%20device%20configuration%20profile%20to%20Microsoft%20Intune.

Android: https://developer.android.com/work/managed-configurations

Apple: https://developer.apple.com/library/archive/samplecode/sc2279/Introduction/Intro.html

Question: 274

Your network contains an Active Directory domain named contoso.com. The domain contains 25 computers that run Windows 11.

You have a Microsoft 365 subscription

You have an Azure AD tenant that syncs with contoso.com.

You configure hybrid Azure AD join and discover that some of the computers have a registered state of Pending.

You need to ensure that the computers complete the join successfully.

What should you ensure?

A. that Windows is activated on all the computers
B. that the users of the computers are assigned Microsoft 365 licenses
C. that each computer has a line of sight to a domain controller
D. that the computers contain the latest quality updates

Answer: C

Explanation:

https://learn.microsoft.com/en-us/entra/identity/devices/hybrid-join-plan

Question: 275

HOTSPOT

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

Name	RAM	Storage	TPM version
Device1	14 GB	256 GB	1.2
Device2	4 GB	64 GB	2.0
Device3	8 GB	128 GB	2.0

All the devices will be reimaged and licensed by using subscription activation.

The devices are assigned to the users shown in the following table.

Name	Device	License
User1	Device1	Microsoft 365 E5
User2	Device2	Microsoft 365 E3
User3	Device3	Office 365 E5, Enterprise Mobility + Security E5

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
Devicel can be upgraded to Windows 11 and activated.	O	O
Device2 requires additional hardware before it can be upgraded to Windows 11.0		O
User3 requires an additional license to activate Windows 11 on Device3. O		O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Devicel can be upgraded to Windows 11 and activated	O	
Device? requires additional hardware before it can be upgraded to Windows 110 p		
User3 requires an additional license to activate Windows 11 on Device3		O

Question: 276

DRAG DROP

You have a Microsoft Deployment Toolkit (MDT) deployment share that has a path of D:\MDTShare.

You need to add a feature pack to the boot image.

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

Modify the Windows PE properties of the deployment share.

Modify the General properties of the deployment share.

Update the deployment share.

Answer Area

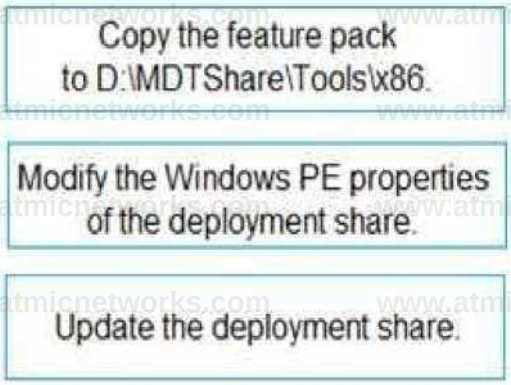
Copy the feature pack to D:\MDTShare\Tools\x86.

Copy the feature pack to D:\MDTShare\Packages.

Answer:

Explanation:

Answer Area



Step 1: Copy the feature pack to D:\MDTShare\Tools\x86
Add a feature pack, DaRT 10 (part of MDOP 2015), to the boot images.

1. Copy the CAB files to the deployment share: MDTShare\Tools\x86
2. In the Deployment Workbench, right-click the MDTShare deployment share and select Properties.

Step 2: Modify the Windows PE properties of the deployment share

3. On the Windows PE tab, in the Platform drop-down list, make sure x86 is selected.
4. On the Features sub tab, select the Microsoft Diagnostics and Recovery Toolkit (DaRT) checkbox.

Step 3: Update the deployment share
Like the MDT Build Lab deployment share, the MDT Production deployment share needs to be updated after it has been configured. This is the process during which the Windows PE boot images are created.

Question: 277

You have an Azure AD tenant named contoso.com.

You plan to purchase 25 computers that run Windows 11. You plan to deliver the computers directly to users.

You need to ensure that during the out-of-box experience (OBE), users are prompted to sign in, and then the computers are configured to use Microsoft Intune.

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a provisioning package
B. automatic enrollment
C. an unattend.xml answer file
D. a Windows Autopilot deployment profile for self-deploying mode
E. a Windows Autopilot deployment profile for user-driven mode

Answer: BE

Explanation:

Self-deploying mode doesn't presently associate a user with the device (since no user ID or password is specified as part of the process).

Ref: https://learn.microsoft.com/en-us/autopilot/self-deploying#:~:text=Self%2Ddeploying%20mode%20doesn%27t%20presently%20associate%20a%20user%20with%20the%20device%20(since%20no%20user%20ID%20or%20password%20is%20specified%20as%20part%20of%20the%20process).

Windows Autopilot user-driven mode
Ref: https://learn.microsoft.com/en-us/autopilot/user-driven#:~:text=Specify%20your%20e%2Dmail%20address%20and%20password%20for%20your%20organization%20account.

Question: 278

Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 10. Users in the finance department use the computers.

You have a computer named Computer1 that runs Windows 10.

From Computer1, you plan to run a script that executes Windows PowerShell commands on the finance department computers.

You need to ensure that you can run the PowerShell commands on the finance department computers from Computer.

What should you do on the finance department computers?

A. From Windows PowerShell, run the Enable-MMAgent cmdlet.
B. From the local Group Policy, enable the Allow Remote Shell Access setting.
C. From Windows PowerShell, run the Enable-PSRemoting cmdlet.
D. From the local Group Policy, enable the Turn on Script Execution setting.

Answer: C

Explanation:

Enable-PSRemoting is specifically designed to enable remote PowerShell access. This cmdlet configures the necessary settings on the target computers to allow remote PowerShell connections. The other options are not directly related to enabling remote PowerShell: Enable-MMAgent is used for managing mobile devices. The "Allow Remote Shell Access" group policy setting is primarily for enabling remote access for command prompt (cmd.exe), not PowerShell. The "Turn on Script Execution" group policy setting controls whether scripts can run locally on a computer, but it doesn't enable remote PowerShell access. By running Enable-PSRemoting on the finance department computers, you'll ensure that they are ready to receive and execute PowerShell commands from Computer1.

Question: 279

HOTSPOT

You manage a Microsoft Deployment Toolkit (MDT) deployment share named DS1. DS1 contains an Out-of-Box Drivers folder named Windows 11 x64 that has subfolders in the format of {make name}\{model name}.

You need to modify a deployment task sequence to ensure that all the drivers in the folder that match the make and model of the computers are installed without using PnP detection or selection profiles.

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

NOTE: Each correct selection is worth one point.

Answer Area

Phase that you must modify in the deployment task sequence:

- Install Preinstall
- Validation

Task that you must use to specify which folder contains the drivers:

- Gather
- Inject Drivers
- Set Task Sequence Variable
- Validate

Answer:

Explanation:

Preinstall
Set Task Sequence Variable

Question: 280
HOTSPOT

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android device named Policy1 as shown in the following exhibit.

Home Apps

Create policy

O Basics 0 Apps) Data (*J Access requirements

Choose how you want to apply this policy to apps on different devices. Then add at least one app.

Target to apps on all device types 0 — No / Yes

Device types Q — Unmanaged

Target policy to — All Apps

0 Well continue to add managed apps to your policy as they become avaiable in Intune View a st of apps that v.-ill be targeted

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

To apply Policy1 to an Android device, you must
- install the Company Portal app on the device
- install the Microsoft Authenticator app on the device
- onboard the device to Microsoft Defender for Endpoint
- onboard the device to the Microsoft Purview compliance portal

When Policy1 is assigned, the policy will apply to
- users only
- devices only
- users and devices

Answer:

Explanation:

Box 1: Install the Company portal

Box 2: Users Only

https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policies#target-app- protection-policies-based-on-device-management-state:~:text=Because%20Intune%20app%20protection%20policies%20target%20a%20user%27s%20identity%2C%20the%20protection%20settings%20for%20a%20user%20can%20apply%20to%20both%20enrolled%20(MDM%20managed)%20and%20nonenrolled%20devices%20(no%20MDM).

Question: 281

You have a Windows 10 device named Computer1 enrolled in Microsoft Intune.

You need to configure Computer1 as a public workstation that will run a single customer-facing, fullscreen application.

Which configuration profile type template should you use in Microsoft Intune admin center?

A. Shared multi-user device
B. Device restrictions
C. Kiosk
D. Endpoint protection

Answer: C

Explanation:

Question: 282

You plan to deploy Windows 11 Pro to 200 new computers by using the Microsoft Deployment Toolkit (MDT) and Windows Deployment Services (WDS).

The company has a Volume Licensing Agreement and uses a product key to activate Windows 11.

You need to ensure that the new computers will be configured to have the correct product key during the installation.

What should you configure?

A. an MDT task sequence
B. the Device settings in Azure AD
C. a WDS boot image
D. a Windows Autopilot deployment profile

Answer: A

Explanation:

https://learn.microsoft.com/en-us/answers/questions/856939/how-to-place-windows-product-key- in-the-rules-on-t#:~:text=You%20may%20set%20the%20Product%20Key%20per%20Task%20Sequence%20in%20customsettings.ini

Question: 283

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. Vou configure Intune to send log data to Log Analytics. You need to review events involving devices that fail to enroll in Intune.

What should you monitor?

A. operational logs

B. audit logs
C. the Intune Device log
D. device compliance organizational logs

Answer: C

Explanation:

Question: 284

You have a Microsoft 365 subscription.

You use Microsoft Intune to manage Windows 11 devices.

You need to implement Windows Local Administrator Password Solution (Windows LAPS). What should you configure?

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

Answer: C

Explanation:

Question: 285

You have a Microsoft 365 subscription that includes Microsoft Intune. The subscription contains corporate-owned, fully managed Android Enterprise devices.

You plan to deploy a configuration profile that will have a device restrictions profile type named Profile1. Profile1 will assign maintenance windows for system updates.

What should you configure from the Configuration settings for Profile1?

A. Device experience
B. General
C. Connectivity
D. Power Settings

Answer: A

Explanation:

Question: 286

HOTSPOT

You have a Microsoft 365 subscription.

You have 25 Microsoft Surface Hub devices that you plan to manage by using Microsoft Intune.

You need to configure the devices to meet the following requirements:

- Enable Windows Hello for Business.
- Configure Microsoft Defender SmartScreen to block users from running unverified files.

Which profile type template should you use for each requirement? To answer, select the appropriate

options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

Windows Hollo fa Business: Identity protection
Device restrictions
Device restrictions (Windows 10 Team)
Endpoint protection
Identity protection
i Microsoft Defender for Endpant (Desktop devices running Windows 10 or later)

Microsoft Defender SmartScreen: Endpoint protection
l Windows health monitoring
Device restrictions (Windows 10 Team)
Endpant protection
identity protection
[Microsoft Defender for Endpoint (Desktop devices tunning Windows 10 a later)

Answer:

Explanation:

Answer Area

Windows Hello fa Business: Identity protection

Microsoft Defender SmartScreen: Endpant protection

Question: 287

HOTSPOT

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage Windows 365 Cloud PC devices.

You need to deploy a Windows 365 Security Baseline to the Cloud PC devices. The solution must meet the following requirements:

- Block data execution prevention.
- Enable virtualization-based security (V8S) and Secure Boot.

What should you configure for the Windows 365 Security Baseline profile? To answer, select the appropriate options in the answer area.

Answer Area

To block data execution prevention: Microsoft Defender File Explore!
Microsoft Defender
Microsoft Edge

To enable VBS: Device Guard
Device Guard
Microsoft Defender
System

Answer:

Explanation:

Answer Area

To block data execution prevention: Microsoft Defender ”

To enable VBS' Device Guard *

Question: 288

HOTSPOT

You have a Microsoft 365 subscription.

You use Microsoft Intune to manage devices.

You need to assess device performance during startup and identify any device models that take longer than average to start.

What should you use to assess the device performance, 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

Use | Endpoint analytics
Compliance policies
Device diagnostics
I Endpoint analytics

In portal Microsoft Intune admin center T
Microsoft 365 Apps admin center Microsoft Entra admin center
Microsoft Intune admin center

Answer:

Explanation:

Answer Area

Question: 289

You have a Microsoft 365 subscription that includes Microsoft Intune.

You create a new Android app protection policy named Policy1 that prevents screen captures in all Microsoft apps. You discover that an unmanaged email client installed on Android devices can still capture screens You need to ensure that users can only use Microsoft apps to access email. What should you do?

A. Create a Conditional Access policy.
B. Create a compliance policy.
C. Modify the Data protection settings of Policy1.
D. Modify the assignments of Policy1.

Answer: D

Explanation:

Question: 290

You have a Microsoft 365 E5 subscription. All Windows devices are enrolled in Microsoft Intune.

You need to create an app protection policy named Policy1 and apply Policy1 to the devices. What can you protect by using Policy1?

A. Microsoft Outlook
B. Microsoft OneDrive
C. Microsoft Teams
D. Microsoft Edge

Answer: D

Explanation:

Question: 291

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage all Windows 11 devices.

You create an attack surface reduction (ASR) policy named Profile1 based on the Attack Surface Reduction Rules profile and assign Profile! to all the devices.

A user reports that an Adobe Reader plug-in is now blocked.

You need to ensure that the plug-in is unblocked.

What should you do?

A. Create an Endpoint Privilege Management policy and assign the policy to all the devices.
B. Add a scope tag to Profile1.
C. Configure ASR Only Per Rule Exclusions in Profile1.
D. Create a device compliance policy and assign the policy to all the devices.

Answer: C

Explanation:

Question: 293

Your company has a Microsoft 365 subscription.

All the users in the finance department own personal devices that run iOS or Android. All the devices are enrolled in Microsoft Intune.

The finance department adds new users each month.

The company develops a mobile application named App1 for the finance department users.

You need to ensure that only the finance department users can download Appl.

What should you do first?

A. Register App1 in Microsoft Entra.

B. Add App1 to the vendor stores for iOS and Android applications.

C. Add App1 to a Microsoft Deployment Toolkit (MDT) deployment share.

D. Add App1 to Intune.

Answer: D

Explanation:

Question: 295

You have a Microsoft 365 E5 subscription.

All devices are enrolled in Microsoft Intune.

You need to ensure that devices that have NOT checked in for 30 days are deleted from intune.

What should you configure from the Microsoft Intune admin center?

A. a device limit restriction

B. automatic enrollment

C. a device clean-up rule

D. a configuration profile

Answer: C

Explanation:

Question: 296

You have a Microsoft 365 E5 subscription. All devices are enrolled in Microsoft Intune.

You create a Conditional Access policy named Policy! that requires multifactor authentication (MFA).

You need to ensure that Policy1 only applies to devices marked as noncompliant. Which settings of Policy1 should you configure?

A. Device platforms under Conditions

B. Filter for devices under Conditions

C. Target resources

D. Grant

E. Session

Answer: B

Explanation:

Question: 297

HOTSPOT

Your on-premises network contains an Active Directory domain named contoso.com. The domain contains a user account named Admin1 and the resources shown in the following table.

Name	Type
Serveri	Computer object
0U1	Organizational unit (OU)

You have a Microsoft 365 E5 subscription.

You have a Microsoft Entra tenant that syncs with contoso.com.

Admin! plans to use Windows Autopilot to deploy 10X3 Windows 11 devices. The deployment must meet the following requirements:

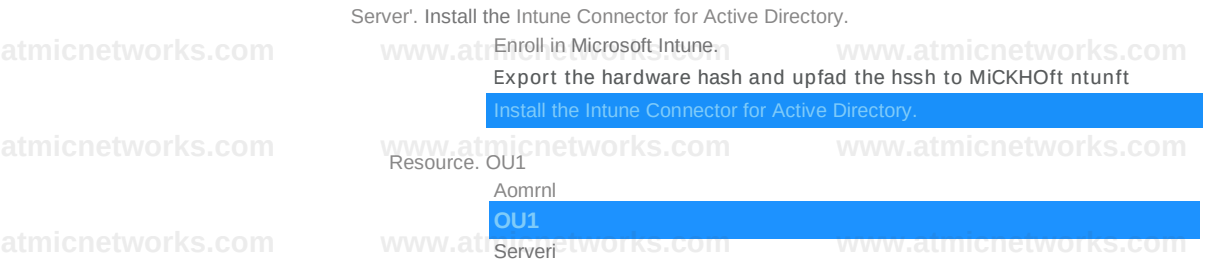
- The devices must be Microsoft Entra hybrid joined during the deployment.
- Computer objects must be created in 0U1.

You need to configure Server1 and Active Directory delegation to support the deployment.

How should you configure Server1, and on which resource should you configure delegated permissions? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Serveri: Install the intune Connector for Active Directory. ’

Resource: 0U1 ’

Question: 298

You have 200 computers that run Windows 10. The computers are joined to Microsoft Entra and enrolled in Microsoft Intune. You need to enable self-service password reset on the sign-in screen. Which settings should you configure from the Microsoft Intune admin center?

A. Conditional access

B. Device compliance

C. Device configuration

D. Device enrollment

Answer: C

Question: 300

HOTSPOT

You have a Microsoft 365 E5 subscription. All devices are enrolled in Microsoft Intune.

You have a device group named Group1 that contains five Windows 11 devices.

You need to ensure that the devices in Group1 automatically receive new Windows 11 builds before the builds are released to the public.

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

NOTE: Each correct selection is worth one point.

Answer Area

Profile type: Update rings for Windows 10 and later
Feature updates for Windows 10 and later
Quality updates for Windows 10 and later

| Windows insider - Release Preview

Answer:

Explanation:

Answer Area

Profile type:

Prerelease channel: Dev Channel
[Beta Channel

Update rings for Windows 10 and later

Prerelease channel Dev Channel

Question: 301

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Intune.

You purchase 50 Windows devices.

You configure automatic enrollment to Intune for Microsoft Entra joined devices.

You need to use a provisioning package to join the devices to Microsoft Entra.

What should you use to create the provisioning package, and what is the maximum amount of time you can use the package for bulk enrollment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Use: Windows Configuration Designer

Maximum amount of time: 180 days

Question: 302

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Intune. The subscription contains a Microsoft Entra tenant that syncs with an on-premises Active Directory Domain Services (AD DS) domain. The tenant has Windows Local Administrator Password Solution (Windows LAPS) enabled.

You have the Windows devices shown in the following table.

Name	Join type	Enrolled in Intune
Device!	Joined to the AD DS domain	Yes
Device?	Microsoft Entra hybrid joined	Yes
De vice J	Microsoft Entra joined	No

You have an Endpoint security policy that is configured as shown in the following table.

Setting	Value
Name	Policy!
Platform	Windows 10 and later
Profile	Local admin password solution (Windows LAPS)
Backup Directory	Backup the password to Azure AD only
Password Age Days	30
Assignments	Include: All devices

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
The local administrator password of Devicel will be reset every 30 days.	I 1	O
The local administrator password of Devices will be recoverable from Microsoft Entra ID.	Ci	
The local administrator password of Devices will be reset every 30 days,	O	0

Answer:

Explanation:

Answer Area

Statements	Yes	No
The local administrator password of Devicel will be reset every 30 days.	•	
The local administrator password of Devices will be recoverable from Microsoft Entra ID.	•	
The local administrator password of Devices will be reset every 30 days.		®

Question: 303

HOTSPOT

You have a Microsoft 365 subscription that includes Microsoft Intune and Microsoft Defender for Endpoint.

Users have devices that run Windows 11.

You deploy a connection from Defender for Endpoint to Intune.

You need to ensure that when a device is enrolled in Intune, the device is onboarded automatically to Defender for Endpoint

What should you configure, 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

Configure: An endpoint detection and response (EDR) profile '

| An account protection profile

An endpoint detection and response (EDR) profile

| An onboarding package for Microsoft Defender

In portal: | Microsoft Intune admin center * (

Microsoft Defender portal

Microsoft Entra admin center

Microsoft Intune admin center

Answer:

Explanation:

Answer Area

Configure: An endpoint detection and response (EDR) profile

In portal; Microsoft Intune admin center •

Question: 304

You have a Microsoft 365 subscription and use Microsoft Intune Suite.

The subscription contains devices enrolled in Intune as shown in the following table.

Name	Platform	Join type
Devicel	Windows 10	Microsoft Entra joined
Device?	Windows 11	Microsoft Entra registered
Devices	iOS	Microsoft Entra registered
Deviced	Android	Microsoft Entra registered

Which devices support Device query?

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

Answer: C

Explanation:

Question: 305

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Intune Suite. You manage the following types of devices;

- Windows 11
- Android

- iOS

You need to implement Microsoft Tunnel for Mobile Application Management (MAM) to provide the devices with access to on-premises company apps.

What should you deploy first, and which device types can use Tunnel for MAM? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Deploy: Microsoft Tunnel Gateway
- Intune Connector for Active Directory
- Microsoft Entra application proxy
- Microsoft Tunnel Gateway
- The Microsoft Authenticator app

Device types | Android and iOS only *
- Windows 11 only
- Windows 11 and Android only
- Windows 11 and iOS only
- Android and iOS only
- Windows 11. Android, and iOS

Answer:

Explanation:

Answer Area

Deploy Microsoft Tunnel Gateway

Device types Android and iOS only

Question: 306

HOTSPOT

You have a Microsoft 365 E5 subscription that includes Microsoft Intune. The subscription contains a

group named Group! Group1 contains devices enrolled in Intune.

You deploy Remote Help in Intune.

You need to configure Remote Help to only allow support administrators to join Remote Help sessions from the devices in Group1.

Which type of Microsoft Entra object should you create, and which type of policy should you configure7 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra object [A service principal
- A service principal

An app registration
An enterprise application

Policy — Conditional Access
Compliance

Conditional Access
Endpoint Privilege Management

devices

Answer:

Explanation:

Answer Area

Microsoft Entra object — A service principal

&

Policy — Conditional Access

Question: 307

You have a Microsoft 365 E5 subscription that contains devices enrolled in Microsoft Intune.

You plan to use Device query to provide on-demand information about the state of the devices. The solution must minimize costs. What should you do first?

A. Onboard the devices to Endpoint analytics.
B. Purchase the Intune Advanced Analytics add-on.
C. Use the Collect diagnostics remote action.
D. Purchase the Intune Suite add-on.

Answer: A

Explanation:

Question: 308

You have a Microsoft Entra tenant named contoso.com that contains a Windows 11 device named Device1 and a user named User1 User! registers Device1 in contoso.com.

Which capability is available to Device1 after registering in contoso.com.

A. authenticating to cloud resources by using single sign-on (SSO)
B. enforcing software updates
C. enforcing hard drive encryption
D. enforcing compliance policies

Answer: A

Explanation:

Question: 309

HOTSPOT

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

Name	Platform	Join type
Devicel	Windows 11	Microsoft Entra joined
Device?	Windows 11	Microsoft Entra registered
DeviceB	iOS	Microsoft Entra registered

You need to create two dynamic device groups named Group1 and Group2. The solution must meet the following requirements:

- Group1 must contain Device1 and Device2 only.
- Group2 must contain Device1 and Device3 only.

Which device membership rule should you configure for each group? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

Group): (devicedisplayName -eq "Devicel"! and (device.displayName eq "Device2")

(device deviceTrustType -eq 'AzureAD')

(device displayName -eq "Devicel") and (device displayName -eq 'Device?") (device displayName -startsWith "Device") and (device deviceOSType -eq 'Windows)

Group? [device deviceTrustType -eq AzureAD") or (device deviceOSType -eq "iPhone'J (device.deviceOSType eq "iPhone') and (device.deviceOSType eq "Windows") (device deviceOSType eq " Phone") or (device.deviceOSType eq "Windows")

(device deviceTrustType -eq "AzureAD") or (device deviceOSType -eq "iPhone")

Answer:

Explanation:

Answer Area

Groupl (device.displayName -eq "Devicel") and (devicedisplayName eq "Device2")

Group?. (device deviceTrustType -eq 'AzureAD") or (device.deviceOSType -eq "iPhone")

Question: 310

You have a Microsoft 365 E5 subscription.

You need to create a dynamic device group that will contain any device that has the word Marketing in its name. Which device membership rule should you use?

A. (device.displayName -in "'Marketing'")
B. (device.displayName -contains "'Marketing'")
C. (device.displayName -in "Marketing")
D. (device.displayName -contains "Marketing")

Answer: D

Explanation:

Question: 311

DRAG DROP

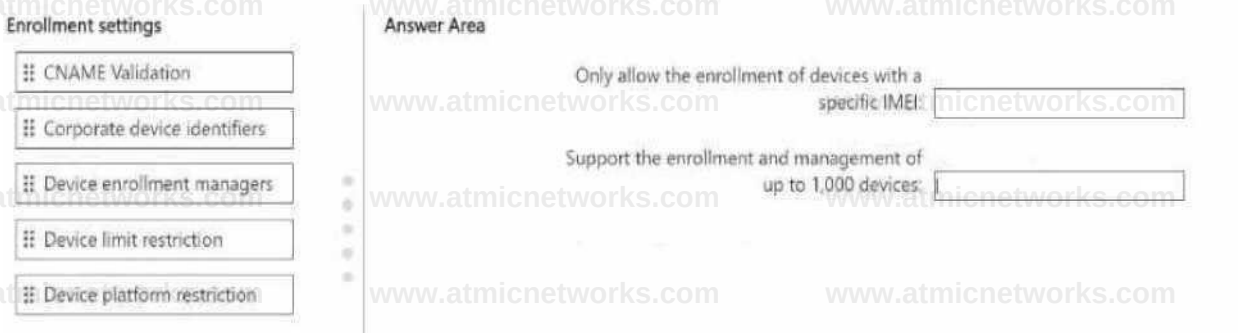
You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Intune. You need to meet the following requirements:

- Only allow the enrollment of devices that have a specific international mobile equipment identifier (IMEI).
- Support the enrollment and management of up to 1,000 devices

Which enrollment setting should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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.

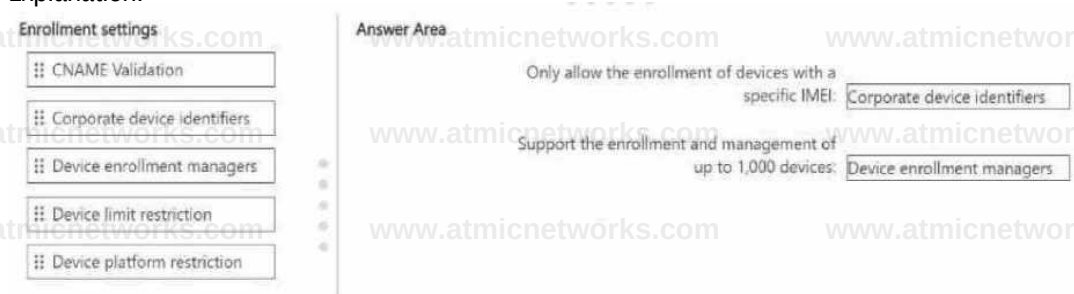
NOTE: Each correct selection is worth one point.



devices

Answer:

Explanation:



Question: 312

You have a Microsoft 365 E5 subscription that contains a group named Group1. You need to ensure that only the members of Group1 can join devices to the Microsoft Entra tenant. What should you configure in the Microsoft Entra admin center?

A. Enterprise State Roaming
B. Mobility
C. Device settings
D. User settings

Answer: C

Explanation:

Question: 313

HOTSPOT

You have a hybrid environment that contains a Microsoft Entra tenant and an on-premises Active Directory Domain Services (AD DS) domain. The environment contains the devices shown in the following table.

Name	Platform	Domain status
Device!	Windows 11	Workgroup
DeviceZ	iOS	*Not applicable*

Which Microsoft Entra join type can each device use? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

Device! Microsoft Entra registered. Microsoft Entra lomed, or Microsoft Entra hybrid lomed | Microsoft Entrajoined only Microsoft Entra registered only
Microsoft Entra hybrid joined only
I Microsoft Entra joined or Microsoft Entra registered only
Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

DeviteJ. Microsoft Entra registered only

*

[Microsoft Entra joined only

Microsoft Entra registered only
Microsoft Entra hybrid joined only
Microsoft Entra joined or Microsoft Entra registered only
Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

Answer:

Explanation:

Answer Area

Devicel Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

Device2 Microsoft Entra registered only

Question: 314

You have a Microsoft 365 subscription.

You use Microsoft Intune to manage all devices.

Users have iOS devices with Microsoft apps installed.

You need to prevent users from cutting, copying, and pasting data between Microsoft Excel and other apps installed on the devices.

What should you configure'

A. an iOS app provisioning profile
B. policies for Microsoft Office apps
C. an app configuration policy
D. an app protection policy

Answer: D.

Explanation:

Question: 315

HOTSPOT

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

Name	Member of	Join type
Devicel	Groupl, Group2	Microsoft Entra joined
Device2	Group2	Microsoft Entra joined
DeviceS	Groupl, Group2	Microsoft Entra hybrid joined

You create an Endpoint Privilege Management (EPM) elevation settings policy named ElevationSettmgsl that has the following settings:

- Endpoint Privilege Management: Enabled

o Default elevation response: Require user confirmation

o Validation: Business justification

- Assignments: Group1 Each device contains a file named File1.exe that can be run only by an administrator.

You create an EPM elevation rules policy named ElevattonRules1 that has the following settings:

- Rule name: Rule1

o Elevation type: Automatic

o File name: Filel.exe

o File hash: <Filel.exe hash>

- Assignments: Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select

NOTE: Each correct selection is worth one point.

Answer Area Statements	Yes	No
A user on Devicel must provide a business justification to run File1.exe A user on Device^ can run Filel exe	O	O
A user on Devices can run Filel exe without providing a business justification		

Answer:

Explanation:

Answer Area Statements	Yes	No
A user on Devicel must provide a business justification to run Filel exe	®	
A user on Devke2 can run Filel .exe	■	$
A user on Devices can runFile1.exe without providing a business justification	0	#

Question: 316

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune

You create a user named User1.

You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.

Solution: From the Microsoft Entra admin center, you assign the Helpdesk Administrator role to User1.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Question: 317

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.

You create a user named Userl.

You need to ensure that User1 can rotate Bitlocker recovery keys by using Intune.

Solution: From the Microsoft Intune admin center, you assign the Help Desk Operator role to User1. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Question: 318

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.

You create a user named User1.

You need to ensure that User1 can rotate Bitlocker recovery keys by using Intune.

Solution: From the Microsoft Intune admin center, you assign the Endpoint Security Manager role to User1.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Question: 319

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

Name	Platform	Join type	Microsoft Intune
Devicel	Windows 11	Microsoft Entra joined	Enrolled
Device2	Windows 11	Microsoft Entra joined	Not enrolled
DeviceS	Windows 11	Microsoft Entra registered	Enrolled
Device4	Android	Microsoft Entra registered	Enrolled

On which devices can you implement Endpoint Privilege Management (EPM)?

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

Answer: C

Explanation:

Question: 320

You have a Microsoft 365 subscription that includes Microsoft Intune. The subscription contains Windows 11 devices enrolled in Intune. The subscription contains three groups named Department Department2. and Department3.

You need to deploy Microsoft 365 Apps to the Windows 11 devices. The solution must meet the following requirements:

- Users in Department1 and Department2 must receive the full Microsoft 365 Apps suite, including Microsoft Project and Visio.
- Users in Department3 must receive the full Microsoft 365 Apps suite, including Microsoft Project, but without Visio.
- All other users must receive the full Microsoft 365 Apps suite without Microsoft Project or Visio. What is

the minimum number of deployments you should create?

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

Answer: C

Explanation:

Question: 321

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

Name	Platform	Join type
Devicel	Windows 11	Microsoft Entra registered
Device2	Windows 11	Microsoft Entra joined
Device3	Android	Microsoft Entra registered
Device4	iOS	Microsoft Entra registered

All the devices are enrolled in Microsoft Intune and have Microsoft 365 Apps for enterprise installed On which devices can you use the Cloud Policy service for Microsoft 365 to manage Microsoft 365 Apps for enterprise?

A. Device2 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: B

Explanation:

Question: 322

HOTSPOT

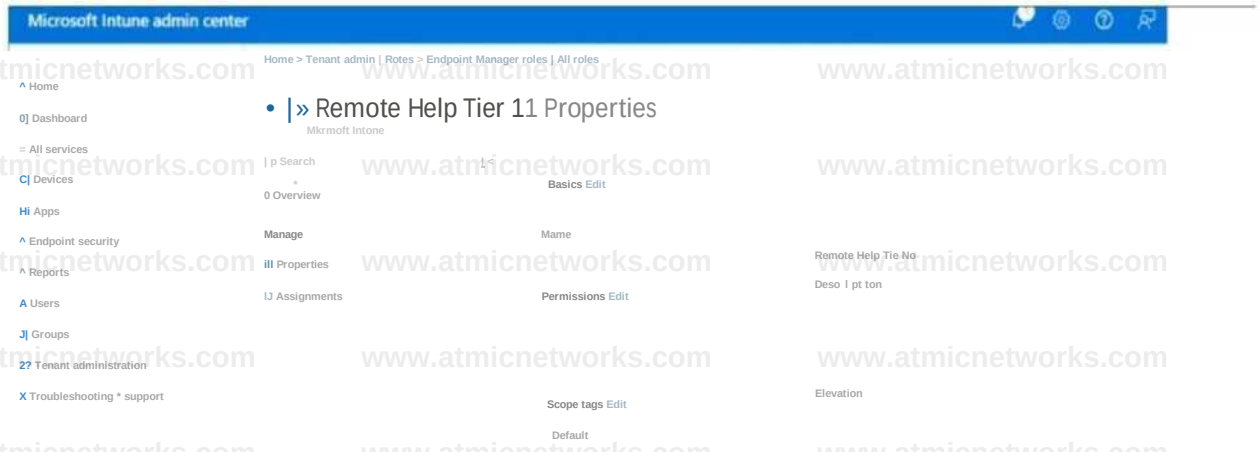
You have a Microsoft 365 E5 subscription that contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Devicel	Windows 11
Device2	iOS
DeviceS	Android

The subscription contains the users shown in the following table

Name	Role	Role type
Adminl	Help Desk Operator	Built-in role
Admin2	Remote Help fieri	Custom Intune role

The Remote Help Tier1 role is configured 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.

Statements	Yes	No
Admin 1 can take full control of Device?	Q	
Admin? can take full control of Devicel.	0	
Admin? can take unattended control of Device?		

Answer:

Explanation:

Statements	Yes	No
Admin 1 can take full control of Device?	0	•
Admin? can take full control of Devicel		
Admin? can take unattended control of Device?		*

Question: 323

HOTSPOT

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Cloud Device Administrator
Admin3	Directory Writer
User1	*None*

The tenant contains a standalone workgroup computer named Computer1 that runs Window 11.

Computer1 contains the local users shown in the following table.

Name	Member of
UserA	Administrators
UserB	Power Users
UserC	Device Owners
UserD	Users

Computer1 needs to be joined to contoso.com.

Which local users can join Computer1 to contoso.com, and the Microsoft Entra credentials of which user can be used? To answer,
select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Local users UserA only
UserA only
UserA or UserB only
UserA or UserC only UserA, UserB, or UserC only UserA, UserB, UserC, or UserD

Credentials of Admin! or Admin? only i Admin! only
Admin! or Admin? only
Admin! or AdminS only
Admin!. Admin?, or Admm3 only
Adminl, Admin?, Admin3, or Useri

Answer:

Explanation:

Question: 324
HOTSPOT

You have a Microsoft Entra tenant named contoso.com.

You manage devices by using Microsoft Intune. Automatic Intune enrollment is disabled.

Users report that they must enter the mobile device management (MDM) server address during device enrollment.

To reduce user interaction during device enrollment, you plan to create the following CNAME DNS hostname records:

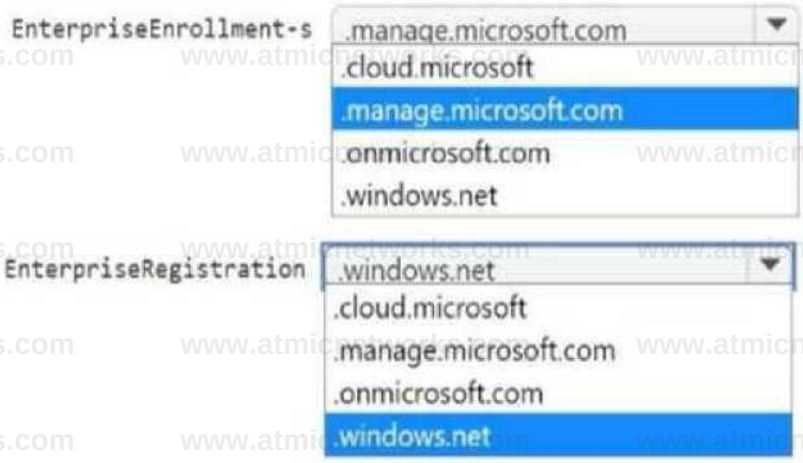
EnterpriseEnrollment.contoso.com

EnterpriseRegistration.contoso.com

You need to configure a fully qualified domain name (FQDN) for each CNAME record to redirect enrollment requests to the Intune servers.

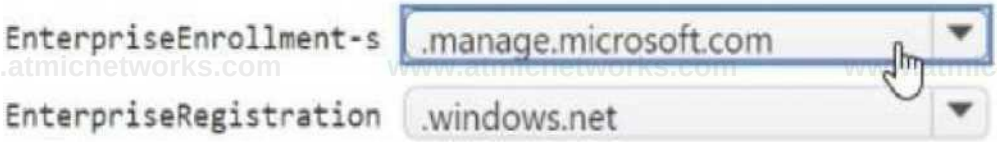
How should you configure each FQDN? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



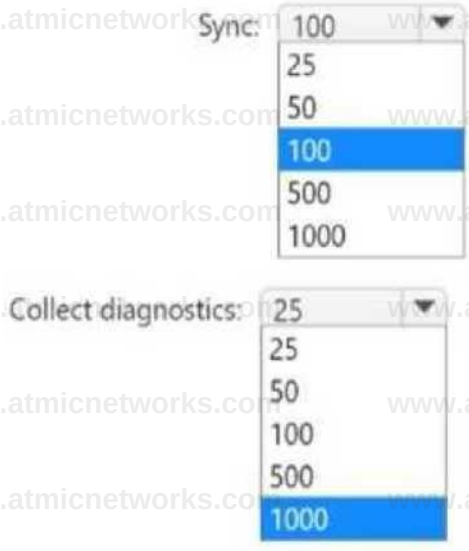
Question: 325
HOTSPOT

You have a Microsoft 365 subscription that contains 5,000 Windows devices enrolled in Microsoft Intune.

You plan to use the Sync and Collect diagnostics bulk device actions.

What is the maximum number of devices you can include in each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Question: 326

You have a Microsoft 365 E5 subscription and use Microsoft Intune.

You need to use a Sync bulk device action on all corporate-owned Windows devices.

What is the maximum number of devices you can include the action?

A. 25

B. 50

C. 100

D. 500

E. 1000

Answer: C

Explanation:

Question: 327

You have a Microsoft 365 E5 subscription and use Microsoft Intune Suite.

You plan to use Intune to run remediation script packages.

What should you do first in the Microsoft Intune admin center?

A. Enable Windows diagnostic data in processor configuration.

B. Upload a Windows enterprise certificate.

C. Enable Windows license verification.

D. Configure the Derived Credential settings.

Answer: A

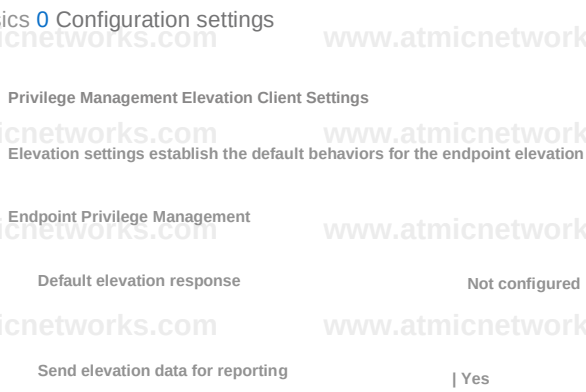
Explanation:

Question: 328

HOTSPOT

You have a Microsoft 365 subscription and use Microsoft Intune.

You have the Endpoint Privilege Management (EPM) elevation settings policy shown in the following exhibit.



No EPM elevation rules policies are configured.

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.

Software installations will [answer choice] require user confirmation be denied.
require support approval

[Answer choice] will be reported. Only diagnostic data
All diagnostic data and elevations
No diagnostic data or elevations

Answer:

Explanation:

Software installations will [answer choice][1] require user confirmation.

[Answer choice] will be reported. Only diagnostic data

Question: 329

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage all devices.

You need to prepare a Win32 app named App1.exe for deployment.

What should you do first?

A. Upload App1 exe to Azure Blob Storage.

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

C. From the Microsoft 365 Apps admin center, create a deployment configuration.

D. Package App1.exe in the INTUNEWIN format.

Answer: D

Explanation:

Question: 330

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain.

You have a Microsoft 365 E5 subscription that includes Microsoft Intune and syncs with the AD DS domain.

Windows Local Administrator Password Solution (Windows LAPS) is enabled in Microsoft Entra ID.

The subscription has the custom roles shown in the following table.

Name	Permission
Role1	microsoft.directory/deviceLocalCredentials/password/read
Role2	microsoft.directory/deviceLocalCredentials/standard/read
Role3	microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/deviceLocalCredentials/password/read

Microsoft Entra contains the users shown in the following table.

Name	Built-in role	Assigned custom roles
Userl	Helpdesk Administrator	Rolel
User2	Security Reader	Role2
User3	*None*	Role3

You have the devices shown in the following table.

Name	Domain Join Type
Devicel	Joined to AD DS
Device?	Microsoft Entra hybrid joined
Device?	Microsoft Entra joined

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 use Microsoft Entra to read the local administrator password of Device!.		
User? can use Microsoft Entra to read the local administrator password of Device?		
UserJ can use Microsoft Entra to read the local administrator password of Devices.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can use Microsoft Entra to read the local administrator password of Devicel	O	•
User? can use Microsoft Entra to read the local administrator password of Device?	0	•
User 3 can use Microsoft Entra to read the local administrator password of Device}.	•	

Question: 332

You have a Microsoft 365 E5 subscription.

You need to use Device query to gather information about all the devices that are managed by using Microsoft Intune.

What should you do first?

A. Onboard the devices to Microsoft Defender for Endpoint.

B. Onboard the devices to Endpoint analytics.

C. Enable Windows license verification.

D. Create a compliance policy for all the devices.

Answer: B

Explanation:

Question: 333

You have a Microsoft 365 E5 subscription.

All Windows devices are enrolled in Microsoft Intune.

You need to deploy the Remote Help app to all the devices.

The solution must minimize administrative effort.

Which type of app should you deploy?

A. Windows app (Win32)

B. Microsoft Store

C. line-of-business (LOB)

D. Microsoft 365

Answer: A

Explanation:

Question: 334

DRAG DROP

You have a Microsoft 365 subscription that contains the following devices enrolled in Microsoft Intune:

- A corporate-owned Windows device named Device1
- A personally-owned Android device named Device2

You need to use a remote action on each device.

The solution must meet the following requirements:

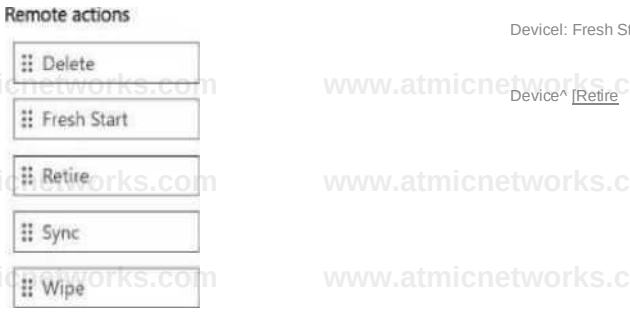
- Repurpose Device1 by returning the device to the factory default settings.
- Remove only corporate data from Device2 and remove the device from Intune when the device checks in.

Which remote action should you use on each device? To answer, drag the appropriate remote actions to the correct devices. Each remote 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:

Explanation:



Question: 335

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two devices named Device1 and Device2.

You manage the devices by using Microsoft Intune.

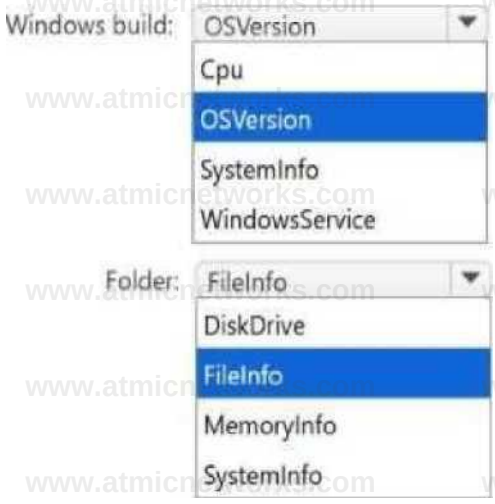
You need to use Device query to meet the following requirements:

- Identify the Windows build on a device.
- Validate whether a folder exists on the C drive of a device.

Which table should you target for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Windows build: OSVersion

Folder: Fileinfo

Question: 336

You have a Microsoft 365 subscription that contains Windows 11 devices enrolled in Microsoft Intune.

You need to use Device query to identify whether a critical security patch was installed on a device.

Which table should you target?

A. Fileinfo

B. OsVersion

C. WindowsQfe

D. SystemInfo

E. WindowsRegistry

Answer: C

Explanation:

Question: 337

DRAG DROP

You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com. The subscription contains a user named User1 and a new Windows 11 device named Device1.

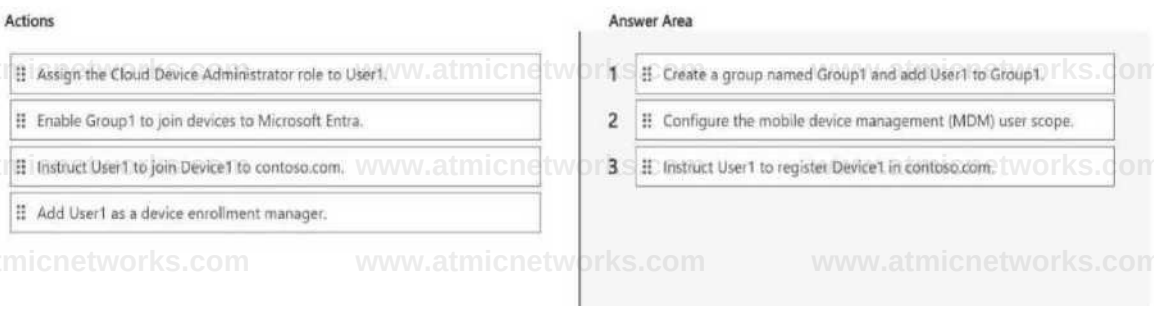
User1 must enroll Device1 in Microsoft Intune automatically.

You need to ensure that all other users cannot use automatic enrollment.

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: 338

You have a Microsoft 365 E5 subscription.

You need to enroll Android Enterprise devices in Microsoft Intune by using zero-touch enrollment.

What should you do first?

A. From the zero-touch enrollment portal, create a zero-touch configuration.

B. From the Microsoft Intune admin center, configure enrollment restrictions.

C. From the Microsoft Intune admin center, create a zero-touch configuration.

D. From the Microsoft Intune admin center, link a Managed Google Play account.

Answer: D

Explanation:

Question: 339

You have a Microsoft Entra tenant named contoso.com that contains a group named Contoso Help Desk.

You need to ensure that Contoso Help Desk is added to the local Administrators group whenever a Windows device is joined to contoso.com.

What should you do?

A. Configure the Enterprise State Roaming settings.

B. Assign the Microsoft Entra Joined Device Local Administrator role to Contoso Help Desk.

C. Enable Microsoft Entra Local Administrator Password Solution (LAPS) for contoso.com.

D. Assign the Cloud Device Administrator role to Contoso Help Desk.

Answer: B

Explanation:

Question: 340

HOTSPOT

You have a Microsoft Entra tenant.

You are creating a dynamic device group named Group1.

Group1 will include only Windows devices that are Microsoft Entra registered.

How should you configure the dynamic membership rule for Group1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

(device.deviceOSType -eq "Windows") and

Answer:

Explanation:

Answer Area

```
(device.deviceOSType -eq " Windows") and devtce.deviceTiustType ’ -eq "Workplace" ^ )
```

Question: 341

HOTSPOT

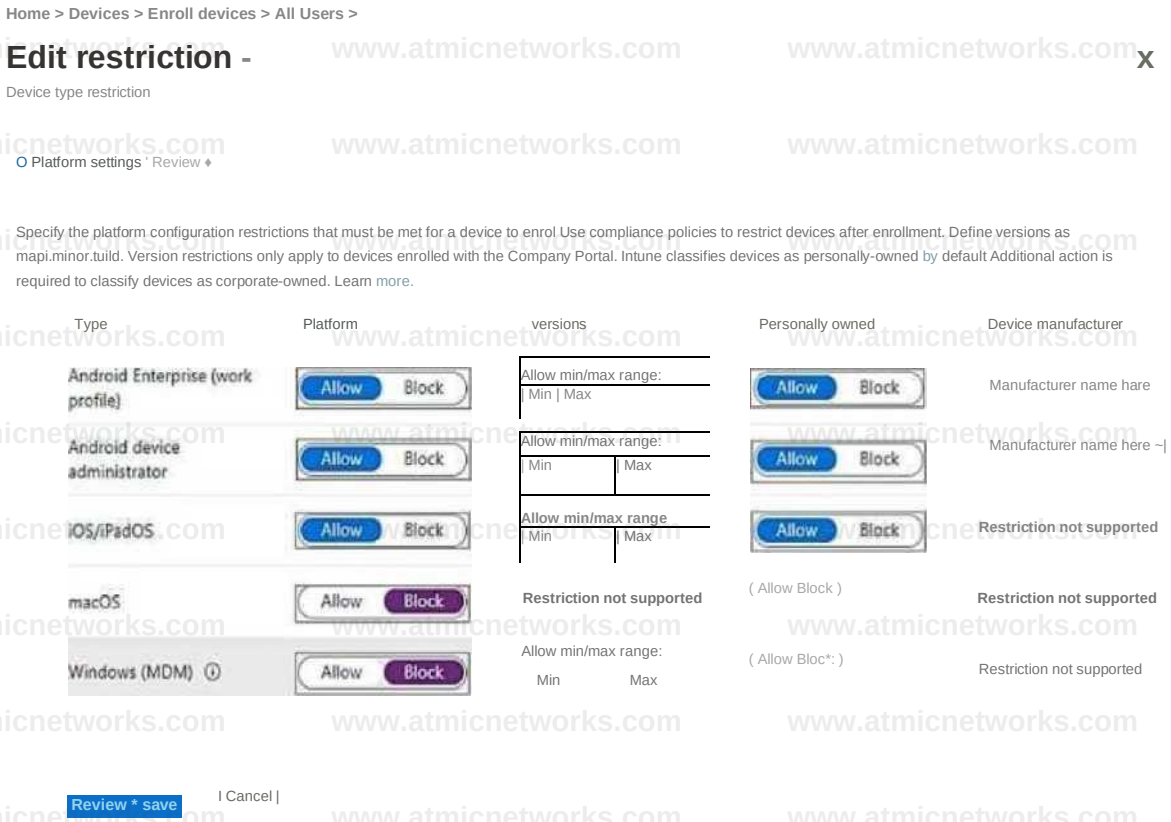
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to ensure that users can only enroll devices that meet the following requirements:

- Android devices that support the use of work profiles.
- iOS devices that run iOS 16.0 or later.

Which two restrictions should you modify? To answer, select the restrictions in the answer area.

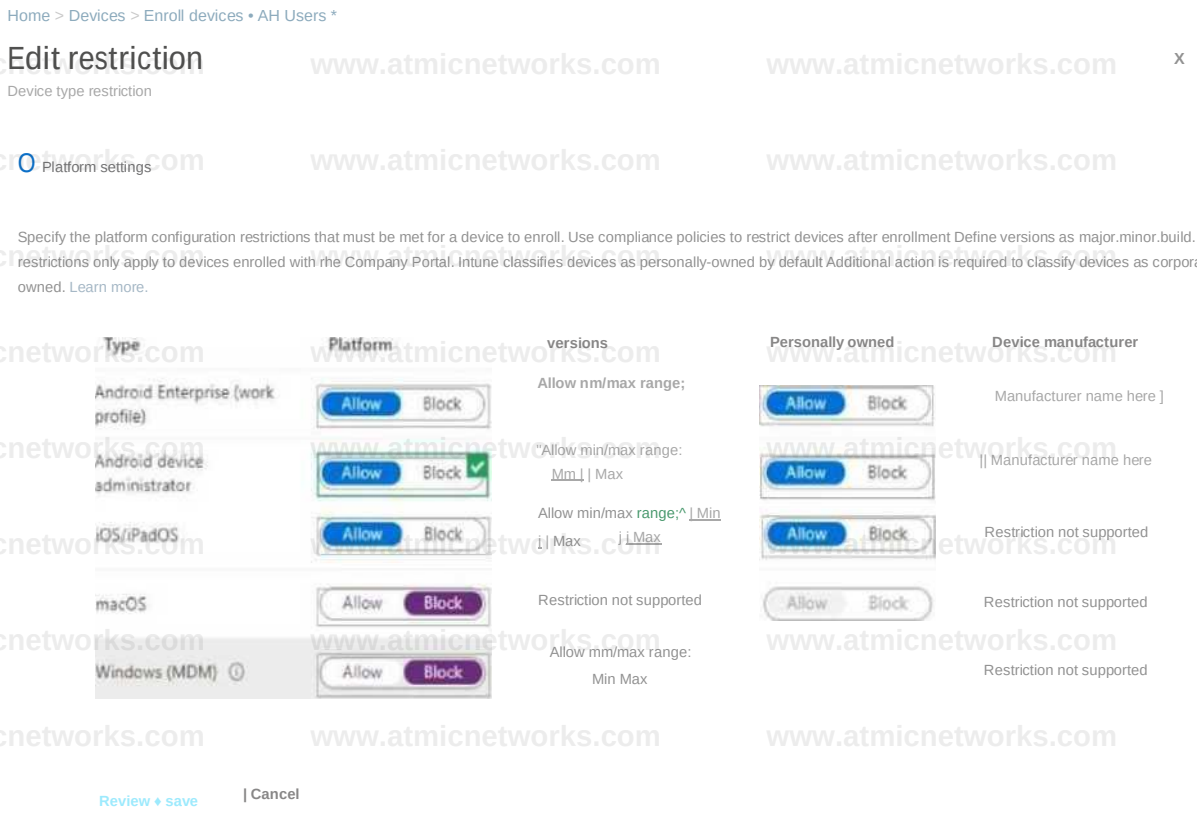
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area



Question: 342

You have a Microsoft 365 subscription that contains a user named User1 and 500 Windows devices enrolled in Microsoft Intune.

You configure an attack surface reduction {ASR) rule and enable the rule in Warn mode.

User1 downloads a file named file1.exe. When User1 attempts to run file1.exe he receives a prompt that the content has been blocked. The user unblocks the content.

How much time will pass until the user is prompted next to unblock the content?

A. 10 minutes

B. one hour

C. 24 hours

D. one week

Answer: C

Explanation:

Question: 343

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 Entra tenant named contoso.com.

You purchase an Android device named Device1.

You need to register Device1 in contoso.com.

Solution; You use the Microsoft Intune Company Portal app.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 344

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 Entra tenant named contoso.com.

You purchase an Android device named Devtce1.

You need to register Devtce1 in contoso.com.

Solution; You use the Google Chrome app.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 345

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 Entra tenant named contoso.com.

You purchase an Android device named Device1.

You need to register Device1 in contoso.com.

Solution; You use the Microsoft Authenticator app.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 346

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. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.

You create a user named User1.

You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.

Solution: From the Microsoft Entra admin center, you assign the Cloud Device Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Answer: B