

Topic 1, Case Study Contoso, Ltd.

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

image1

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

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

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

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.

Group1 and Group2 have a Membership type of Assigned.

Devices -

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

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	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	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration -
Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

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 ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30

✓

The Automatic Enrollment 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: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

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

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum 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 AD joined.

Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -

Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

Administrative effort must be minimized.

Q1

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: B

Q2

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 Area

Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	☐	☐
If User1 sets the desktop background to blue on Device2, when User1 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.	☐	☐

Answer:

Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	☒	☐
If User1 sets the desktop background to blue on Device2, when User1 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.	☐	☒

Q3

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

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>

Q4

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 Device2? To answer select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Answer Area

Device1:	1 2 3 4 5
Device2:	1 2 3 4 5

Answer:

Device1:

	▼
1	
2	
3	
4	
5	

Device2:

	▼
1	
2	
3	
4	
5	

Q5
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

User1:

No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

User2:

No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

Answer:

User1:	No devices Device4 and Device5 only Device1, Device2 and Device3 only Device1, Device2, Device3, Device4, and Device5
User2:	No devices Device4 and Device5 only Device1, Device2 and Device3 only Device1, Device2, Device3, Device4, and Device5

Reference:

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

Q6

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

Reference:

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

Q7
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
Device1 is marked as compliant.	☐	☐
Device4 is marked as compliant.	☐	☐
Device5 is marked as compliant.	☐	☐

Answer:

Statements	Yes	No
Device1 is marked as compliant.	☒	☐
Device4 is marked as compliant.	☐	☒
Device5 is marked as compliant.	☒	☐

Q8
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
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	☐	☐
User2 can remove D:\Folder1 from the list of protected folders on Device2.	☐	☐
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	☐	☐

Answer:

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	☐	☒
User2 can remove D:\Folder1 from the list of protected folders on Device2.	☒	☐
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	☐	☒

Q9

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

Reference:

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

Q10

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