

# Microsoft 365 Mobility and Security

**1. Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error. You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You add your user account as a device enrollment manager.

Does this meet the goal?

A. Yes

B. No

**Answer(s): B**

---

**2. Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error. You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

A. Yes

B. No

**Answer(s): A**

---

**3. Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Endpoint Manager.

You successfully enroll Windows 10 devices in Endpoint Manager.

When you try to enroll an iOS device in Endpoint Manager, you get an error. You need to ensure that you can enroll the iOS device in Endpoint Manager.

Solution: You create an Apple Configurator enrollment profile.

Does this meet the goal?

A. Yes

B. No

**Answer(s): B**

---

**4. Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD). You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch). You configure pilot co-management. You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1. You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager. Solution: You create a device configuration profile from the Device Management admin center. Does this meet the goal?

A. Yes

B. No

**Answer(s): B**

---

**5. Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD). You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch). You configure pilot co-management. You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1. You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager. Solution: You add Device1 to an Active Directory group. Does this meet the goal?

A. Yes

B. No

**Answer(s): B**

---

**6. Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD). You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch). You configure pilot co-management. You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1. You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager. Solution: You unjoin Device1 from the Active Directory domain. Does this meet the goal?

A. Yes

B. No

Answer(s): B

7. HOTSPOT (Drag and Drop is not supported).

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

You use Microsoft Endpoint Configuration Manager for device management.

You have the Windows 10 devices shown in the following table.

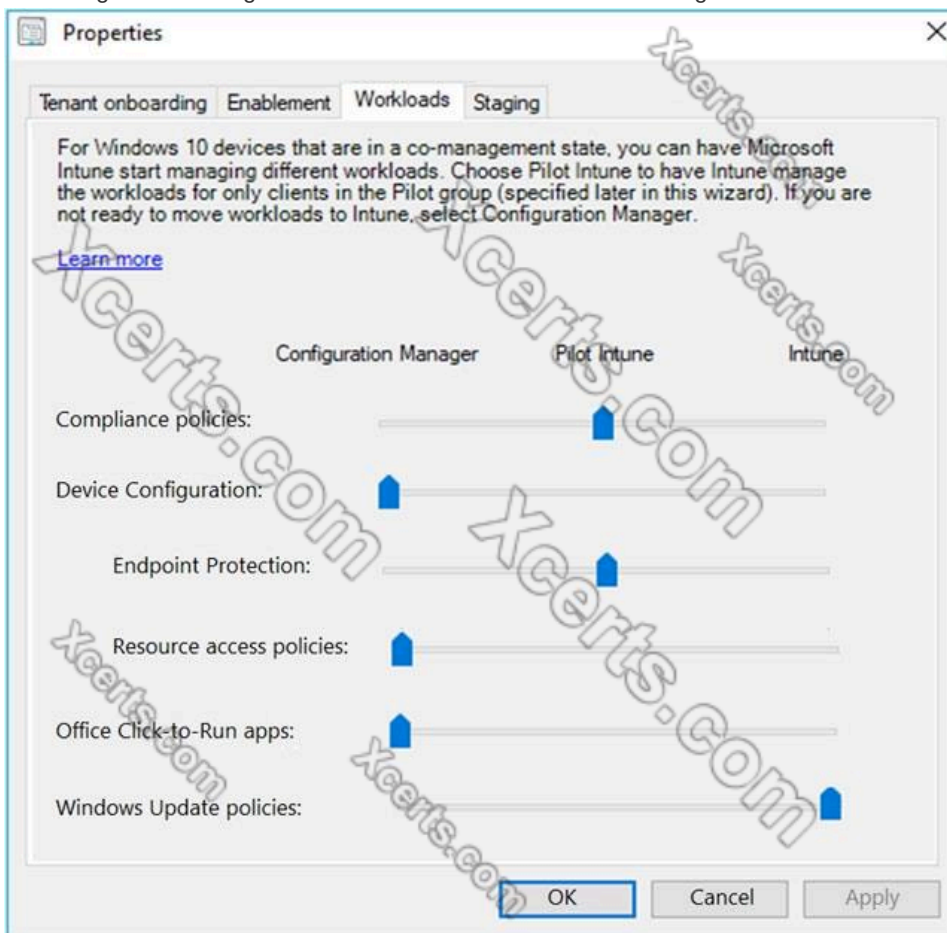
| Name    | Collection  |
|---------|-------------|
| Device1 | Collection1 |
| Device2 | Collection2 |

You configure Endpoint Configuration Manager co-management as follows:

Automatic enrollment in Intune: Pilot

Pilot collection for all workloads: Collection2

You configure co-management workloads 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.

Hot Area:

Answer Area

| Statements   | Yes                   | No                    |
|--|-----------------------|-----------------------|
| Microsoft Intune manages the compliance policies for Device1.          | <input type="radio"/> | <input type="radio"/> |
| Configuration Manager manages the Windows Update policies for Device1. | <input type="radio"/> | <input type="radio"/> |
| Microsoft Intune manages Endpoint Protection for Device2.              | <input type="radio"/> | <input type="radio"/> |

A. See Explanation section for answer.

Answer(s): A

8. HOTSPOT (Drag and Drop is not supported).

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

| Name    | Platform   | Member of      |
|---------|------------|----------------|
| Device1 | Windows 10 | Group1         |
| Device2 | Android    | Group2, Group3 |
| Device3 | Windows 10 | Group2, Group3 |

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

| Name    | Platform             | Assigned |
|---------|----------------------|----------|
| Policy1 | Windows 10 and later | Yes      |
| Policy2 | Android              | No       |
| Policy3 | Windows 10 and later | Yes      |

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

| Name    | Include | Exclude |
|---------|---------|---------|
| Policy1 | Group3  | None    |
| Policy2 | Group2  | 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.

Hot Area:

Answer Area

| Statements                  | Yes                   | No                    |
|-----------------------------|-----------------------|-----------------------|
| Policy1 applies to Device3. | <input type="radio"/> | <input type="radio"/> |
| Policy2 applies to Device2. | <input type="radio"/> | <input type="radio"/> |

A. See Explanation section for answer.

Answer(s): A

9. You have Windows 10 Pro devices that are joined to an Active Directory domain. You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Endpoint Manager enrollment

B. Microsoft Azure Active Directory (Azure AD)

C. smartcards

D. TPM-enabled devices

Answer(s): A B

10. You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the

device is enrolled in Microsoft Endpoint Manager automatically.  
 What should you configure?

- A. Enrollment restrictions from the Endpoint Manager admin center
- B. device enrollment managers from the Endpoint Manager admin center
- C. MAM User scope from the Azure Active Directory admin center
- D. MDM User scope from the Azure Active Directory admin center

Answer(s): D

11. HOTSPOT (Drag and Drop is not supported).

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

| Name  | Member of      |
|-------|----------------|
| User1 | Group1         |
| User2 | Group1, Group2 |
| User3 | None           |

The device type restrictions in Endpoint Manager are configured as shown in the following table.

| Priority | Name      | Allowed platform            | Assigned to |
|----------|-----------|-----------------------------|-------------|
| 1        | Policy1   | Android, iOS, Windows (MDM) | None        |
| 2        | Policy2   | Windows (MDM)               | Group2      |
| 3        | Policy3   | Android, iOS                | Group1      |
| Default  | All users | Android, Windows (MDM)      | All users   |

You add User3 as a device enrollment manager in Endpoint Manager.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| Statements  | Yes                   | No                    |
|---|-----------------------|-----------------------|
| User1 can enroll Windows devices in Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |
| User2 can enroll Android devices in Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |
| User3 can enroll iOS devices in Endpoint Manager.     | <input type="radio"/> | <input type="radio"/> |

A. See Explanation section for answer.

Answer(s): A

12. HOTSPOT (Drag and Drop is not supported).

You create two device compliance policies for Android devices as shown in the following table.

| Policy  | Configuration   | Action                            | Assigned to |
|---------|---|-----------------------------------|-------------|
| Policy1 | Require encryption of the data storage on the device. | Mark as noncompliant immediately. | Group1      |
| Policy2 | Require Google Play services.                         | Mark as noncompliant immediately. | Group2      |

You have the Android devices shown in the following table.

| Name     | User  | Configuration                                    |
|----------|-------|--|
| Android1 | User1 | Not encrypted                                    |
| Android2 | User2 | Google Play services not configured              |
| Android3 | User3 | Not encrypted<br>Google Play services configured |

The users belong to the groups shown in the following table.

| User  | Group          |
|-------|----------------|
| User1 | Group1         |
| User2 | Group1, Group2 |
| User3 | Group2         |

The users enroll their device in Microsoft Endpoint Manager.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| Statements                        | Yes                   | No                    |
|-----------------------------------|-----------------------|-----------------------|
| The device of User1 is compliant. | <input type="radio"/> | <input type="radio"/> |
| The device of User2 is compliant. | <input type="radio"/> | <input type="radio"/> |
| The device of User3 is compliant. | <input type="radio"/> | <input type="radio"/> |

A. See Explanation section for answer.

**Answer(s):** A

**13. HOTSPOT** (Drag and Drop is not supported).

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Quality updates:

Feature updates:

A. See Explanation section for answer.

**Answer(s):** A

14. Your company uses Microsoft Endpoint Configuration Manager and Microsoft Endpoint Manager to co-manage devices. Which two actions can be performed only from Endpoint Manager? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Deploy applications to Windows 10 devices.

B. Deploy VPN profiles to iOS devices.

C. Deploy VPN profiles to Windows 10 devices.

D. Publish applications to Android devices.

**Answer(s):** B D

---

15. HOTSPOT (Drag and Drop is not supported).

Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).

You have Windows 10 and Windows 8.1 devices.

You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

First action to perform:

|   |
|---|
| ▼   |
| Enroll the devices in Microsoft Intune.                     |
| Configure device compliance in Microsoft Intune.            |
| Create a Microsoft Azure Log Analytics workspace.           |
| Add an alias (CNAME) record to the DNS zone of contoso.com. |

Second action to perform:

|  |
|--|
| ▼  |
| Configure all the devices to have a commercial ID.                   |
| Configure software inventory in Configuration Manager.               |
| Configure all the devices to join the Windows Insider Program.       |
| Configure and restart the Windows Update service on all the devices. |

A. See Explanation section for answer.

**Answer(s):** A

---

16. You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You have a Microsoft 365 subscription.

You need to ensure that administrators can manage the configuration settings for all the Windows 10 devices in your organization.

What should you configure?

A. the Enrollment restrictions

B. the mobile device management (MDM) authority

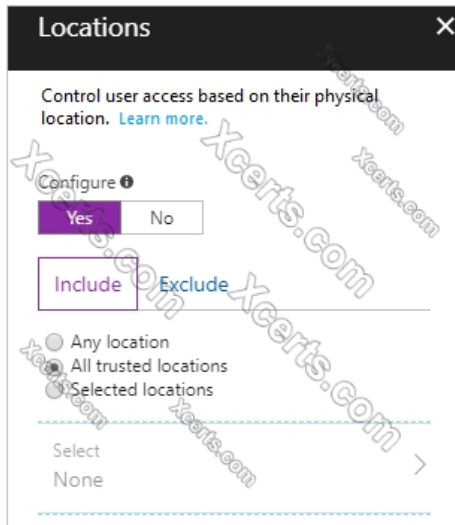
C. the Exchange on-premises access settings

D. the Windows enrollment settings

Answer(s): B

---

17. You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)



The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

You need to ensure that the members of the Security reader group can sign in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

What should you do?

A. From the conditional access policy, configure the device state.

B. From the Azure Active Directory admin center, create a custom control.

C. From the Endpoint Manager admin center, create a device compliance policy.

D. From the Azure Active Directory admin center, create a named location.

Answer(s): D

---

18. You have computers that run Windows 10 Enterprise and are joined to the domain. You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.

You need to prevent Windows from being updated for the next 30 days.



Which two Group Policy settings should you configure? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. Select when Quality Updates are received
- B. Select when Preview Builds and Feature Updates are received
- C. Turn off auto-restart for updates during active hours
- D. Manage preview builds
- E. Automatic updates detection frequency

Answer(s): A B

19. HOTSPOT (Drag and Drop is not supported).

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

| Name    | Platform   | BitLocker Drive Encryption (BitLocker) | Member of      |
|---------|------------|--|----------------|
| Device1 | Windows 10 | Disabled                               | Group1, Group2 |
| Device2 | Windows 10 | Disabled                               | Group2, Group3 |
| Device3 | Windows 10 | Disabled                               | Group3         |

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

| Name    | Require BitLocker | Mark noncompliant after (days) | Assigned |
|---------|-------------------|--------------------------------|----------|
| Policy1 | Require           | 5                              | No       |
| Policy2 | Require           | 10                             | Yes      |
| Policy3 | Non configured    | 15                             | Yes      |

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

| Name    | Assigned to |
|---------|-------------|
| Policy2 | Group2      |
| Policy3 | Group3      |

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

| Statements                                       | Yes                   | No                    |
|--|-----------------------|-----------------------|
| Device1 is marked as noncompliant after 10 days. | <input type="radio"/> | <input type="radio"/> |
| Device2 is marked as noncompliant after 10 days. | <input type="radio"/> | <input type="radio"/> |
| Device3 is marked as noncompliant after 15 days. | <input type="radio"/> | <input type="radio"/> |

A. See Explanation section for answer.

Answer(s): A

20. You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.

Which role should you assign to the user?

A. Cloud application administrator

B. Application administrator

C. Global administrator

D. Service administrator

**Answer(s): C**

---