

Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/26/2022 9:57:50 am • Time spent: 02:21

Score: 70%

Passing Score: 80%



▼ Question 1: ✓ Correct

Which of the following mobile device management (MDM) solutions is hardware-agnostic and supports many different brands of mobile devices?

- MAM
- UEM
- MDM
- EMM

EXPLANATION

Enterprise mobility management (EMM) is the combination of MDM and MAM solutions in one package. EMM solutions are able to manage multiple brands and types of mobile devices in a single package.

Mobile application management (MAM) solutions focus on managing the applications on a mobile device, but do not manage the device itself.

Mobile device management (MDM) solutions allow IT administrators to remotely manage a mobile device even if it's a personally owned device used for work-related purposes.

Unified endpoint management (UEM) is the next step in device management. These solutions provide a single point for all types of devices.

REFERENCES

-  9.7.2 Mobile Device Management Facts

q_mdm_emm_secp7.question.fex

▼ Question 2: Correct

Mobile application management (MAM) provides the ability to do which of the following?

- Control data access.
- Manage mobile devices.
- Comply with security policies.
-  Remotely install and uninstall apps.

EXPLANATION

Mobile application management (MAM) solutions focus on managing the applications on a mobile device but not the device itself. Licensed applications or custom-designed apps fall under MAM policies.

Mobile application management provides the ability to:

- Remotely install and uninstall apps.
- Update apps as needed.
- Limit functionality in an app as needed.

Microsoft Intune allows the system administrator to:

- Manage mobile devices
- Manage mobile apps
- Control data access
- Comply with security policies

REFERENCES

-  9.7.2 Mobile Device Management Facts

q_mdm_mam_secp7.question.fex

▼ Question 3: Incorrect

What is the minimum number of users needed in a Windows Enterprise agreement for Intune to be included?

 100 500 No minimum 1,000**EXPLANATION**

Intune is included with any Windows Enterprise agreement of at least 500 users and supports all types of devices.

REFERENCES 9.7.2 Mobile Device Management Facts[q_mdm_manage_secp7.question.fex](#)

▼ Question 4: Correct

Mobile device management (MDM) provides the ability to do which of the following?

-   **Track the device.**
- Remotely install apps.
- Control data access.
- Update apps as needed.

EXPLANATION

Mobile device management (MDM) solutions allow IT administrators to remotely manage a mobile device even if it's a personally owned device being used for work-related purposes.

Mobile device management provides the ability to:

- Track the device.
- Push apps and updates (this is also known as provisioning the device).
- Manage security settings, such as lock screens, passwords, etc.
- Remotely wipe the device in case it is lost or stolen.

Mobile application management provides the ability to remotely install and uninstall apps.

Microsoft Intune allows the system administrator to:

- Manage mobile devices
- Manage mobile apps
- Control data access
- Comply with security policies

REFERENCES

-  9.7.2 Mobile Device Management Facts

q_mdm_mdm_secp7.question.fex

▼ Question 5: Incorrect

Which of the following mobile device management (MDM) solutions allows an organization to manage all devices, including printers, workstations, and even IoT devices?

- MDM
-  UEM
- EMM
- MAM

EXPLANATION

Unified endpoint management (UEM) is the next step in device management. These solutions provide a single point for all types of devices. This includes workstations, printers, mobile devices, IoT devices, and wearable devices.

Mobile application management (MAM) solutions focus on managing the applications on a mobile device, but not on managing the device itself.

Mobile device management (MDM) solutions allows IT administrators to remotely manage a mobile device even if it's a personally owned device being used for work-related purposes.

Enterprise mobility management (EMM) is the combination of MDM and MAM solutions in one package.

REFERENCES

-  9.7.2 Mobile Device Management Facts

q_mdm_uem_secp7.question.fex

▼ Question 6: Correct

Which of the following is the first phase of the Microsoft Intune application life cycle?

- Configure
- Protect
-  Add
- Deploy

EXPLANATION

The first phase of the Microsoft Intune application life cycle is to add the apps that are to be managed and assigned in Intune.

Deploy is the second phase.

Configure is the third phase.

Protect is the fourth phase.

REFERENCES

-  9.7.6 Mobile Application Management Facts

q_mam_add_secp7.question.fex

▼ Question 7: Correct

Which of the following app deployment and update methods can be configured to make available to specific users and groups only the apps that they have rights to access?

- BYOD
- Self-service portal
- Remote management
-  App catalog

EXPLANATION

An app catalog allows an organization to define the apps that a user can and cannot use. Apps can be assigned to specific users and devices via groups to facilitate management. The catalog is configured to make available to specific users and groups only the apps that they have rights to access. An app can also be blacklisted so no user can use it to access company resources.

A company can create a self-service portal using Intune that makes the distribution of apps easier for everyone.

With remote management, all app types (except for line-of-business apps) automatically update as needed.

Bring Your Own Device (BYOD) is a policy that allows a user to use their personal device for business purposes.

REFERENCES

-  9.7.6 Mobile Application Management Facts

q_mam_catalog_secp7.question.fex

▼ Question 8: Incorrect

In which phase of the Microsoft Intune application life cycle would you assign an app to users and/or devices you manage and monitor them on the Azure portal?

- Configure
-  Deploy
- Add
- Protect

EXPLANATION

During the Deploy phase, apps are assigned to users and devices and then monitored on the Azure portal.

The Configure phase is when apps are updated using Intune.

Add is the first phase. This is when apps are added to Intune to be managed.

Protect is the fourth phase. This is the phase in which company data is protected.

REFERENCES

-  9.7.6 Mobile Application Management Facts

q_mam_deploy_secp7.question.fex

▼ Question 9: Correct

Which of the following app deployment and update methods allows updates to be uploaded onto Intune where they can be pushed out to users within 24 hours?

- App catalog
-  Remote management
- Self-service portal
- BYOD

EXPLANATION

With remote management, all app types (except for line-of-business apps) automatically update as needed. Updates can be uploaded onto Intune where they can be pushed out to users within 24 hours.

A company can create a self-service portal using Intune. This makes the distribution of apps easier for everyone.

Bring Your Own Device (BYOD) is a policy that allows a user to use their personal device for business purposes.

An app catalog allows an organization to define the apps that a user can and cannot use.

REFERENCES

-  9.7.6 Mobile Application Management Facts

q_mam_remote_01_secp7.question.fex

▼ Question 10:  Correct

Which of the following app deployment and update methods allows an administrator to remove apps and clear all data from a device without affecting the device itself?

- BYOD
- Self-service portal
- App catalog
-  Remote management

EXPLANATION

With remote management, when an employee leaves an organization, an administrator can remotely remove apps and clear all data from a device without affecting the device itself.

A company can create a self-service portal using Intune that makes the distribution of apps easier for everyone.

Bring Your Own Device (BYOD) is a policy that allows a user to use their personal device for business purposes.

An app catalog allows the organization to define the apps that a user can and cannot use.

REFERENCES

-  9.7.6 Mobile Application Management Facts

q_mam_remote_02_secp7.question.fex