9.7.2 Mobile Device Management Facts

The use of mobile devices in the workplace has increased rapidly over the past few years. The management of these devices has become a big concern for system administrators.

Many organizations allow users to bring their own devices and use them for work-related purposes. This practice, known as bring your own device (BYOD) requires the organization to develop a set of policies to manage these devices, which allow the organization to ensure the mobile devices are secured and can be managed remotely. There are four main types of mobile device management solutions.

This lesson covers the following topics:

- Mobile device management (MDM).
- Mobile application management (MAM).
- Enterprise mobility management (EMM).
- Unified endpoint management (UEM).

Mobile Device Management

Mobile device management solutions allows IT administrators to remotely manage a mobile device even if it's a personally owned device being used for work-related purposes. MDM focuses on managing the device itself but not the applications or software.

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

Mobile application management 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:

- Install and uninstall apps remotely.
- Update apps as needed.
- Limit functionality in an app as needed.

Enterprise Mobility Management

Enterprise mobility management is the combination of MDM and MAM solutions in one package. These policies allow a system administrator to remotely manage a mobile device's hardware and applications.

As different brands and manufacturers of mobile devices came on the market, the ability to manage them all became more difficult. Enterprise mobility management solutions address this problem by being able to manage multiple types of devices in a single package.

Microsoft's Intune is one of the most popular EMM solutions. Intune is included with any Windows Enterprise agreement of at least 500 users and supports all types of devices. Intune is integrated into the organization's Azure Active Directory, which simplifies device management even more. Intune allows the system administrator to:

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

Unified Endpoint Management

The need to manage so many different devices has become an issue for organizations. Devices such as printers, workstations, servers, and others are managed in Active Directory. However, mobile devices need to be managed separately. A recent solution to this is unified endpoint management. UEM is the next step in device management. These solutions provide a single point for all types of devices, including:

- Workstations
- Printers
- Mobile devices
- IoT devices
- Wearable devices

UEM is the joining together of traditional device management and enterprise mobility management solutions.