9.7.6 Mobile Application Management Facts

Mobile application management (MAM) refers to the assortment of management features that lets a system administrator publish, push, configure, secure, monitor, and update mobile apps. The goal is to ensure users have the applications they need at all times while protecting the organization's data within the apps. This can be very challenging due to the wide variety of device platforms and application types. Intune is Microsoft's MAM solution in the Azure cloud.

This lesson covers the following topics:

- Mobile application management
- Intune application life cycle
- App deployment and update methods

Mobile Application Management

Microsoft app protection policies are rules that make sure the company's data is secure within an application. The user cannot move data or perform any action that is prohibited in a policy. Intune mobile device management (MDM) provides the app protection policies that enable MAM to protect devices and data. MAM also provides protection through MAM without enrollment (MAM-WE) in Intune MDM. The following table describes the two possible configurations.

Configuration Option	Description
Intune MDM + MAM	Manage apps using MAM and app protection policies on devices enrolled in Intune MDM. In an MDM + MAM implementation, administrators use the Intune console in the Azure portal.
MAM-WE	Manage apps using MAM and app protection policies but with devices enrolled with third-party enterprise mobility management (EMM) providers. Sensitive data can be managed on any device, including personal devices.

App protection can require a PIN to launch an application.

Intune Application Life Cycle

Each app in Intune goes through a life cycle. Intune provides a full range of tools to help manage apps during each phase. The following table describes these phases.

Phase	Description
Add	Add the apps you would like to manage and assign them in Intune. You can add the following app types: ▪ Apps from the Windows Store ▪ Apps that are line-of-business apps written in house ▪ Apps on the web ▪ Built-in apps
Deploy	

	Assign the app to users and/or devices you manage and monitor them on the Azure portal.
Configure	Update deployed apps with new versions using Intune.
Protect	Protect company data in deployed apps with conditional access to email and other corporate resources. Conditional access is based on the criteria you set in the app protection policies that lock down actions the users can perform on devices. Examples of locked-down actions include copying data and preventing app installation on rooted devices.
Retire	Remove apps that have reached end of life or become outdated and are no longer used.

App Deployment and Update Methods

The following table describes the three methods available to work with applications throughout their life cycle.

Method	Description
App catalog	An app catalog allows the 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.
Self-service portal	In a large organization, it is not feasible for the network administrator to manually push apps out to all users and groups for all devices. Therefore, a company can create a self-service portal using Intune that makes the distribution of apps easier for everyone.
Remote management	All app types, except for the line-of-business apps, automatically update as needed. Updates can be uploaded into Intune where they can be pushed out to users and updated within 24 hours. Administrators can push out updates for line-of-business apps through the company portal. When an employee leaves the organization, Intune allows the administrator to remotely remove apps and clear all data from the device without affecting the device itself.