MDM with Intune (standalone)

Course Outline

Module 1: Plan for Microsoft Intune
In this module, students will learn how to plan for Microsoft Intune, device management, identity and device management strategies and concludes with signing up for an Intune trial tenant.

- Plan Licensing and product requirements and capabilities
- Mobile device management strategy cloud vs hybrid
- Identity strategy – Users / Groups
- Physical device considerations BYOD / CYOD
- Use of the Intune Portals
- License assignment

Module 2: Compliance
Module 2 is all about device compliance. Compliance policies help protect company data; you need to ensure that any devices used to access company data comply with the rules you define. The rules could include using an 8 digit PIN to access a device and ensuring all data is encrypted when stored on a device.

- Compliance in Intune
- Create a compliance policy
- Using multiple compliance policies

Module 3: Configuration
Module 3 discusses configuration of devices in Intune. Configuration policies, conditional access, exchange active sync and corporate device enrollment.

- Configuration in Intune
- Android
- Android for Work
- iOS
- Mac OS X
- Windows
- Software
- Computer Management
- Common device settings

Module 4: Managing Applications and Updates
Module 4 discusses mobile application management without enrollment on iOS and Android devices. In addition it covers the ability to sideload and deeplink apps and the use of the Intune Software publisher.

Module 5: Enrolling Devices, Alerts, Troubleshooting and Reporting
Module 5 discusses enrolling mobile devices, the Intune alerts categories and capabilities. Reporting is covered in depth and general troubleshooting hints and tips.

• Alerts overview
• Device alerts
• Policy alerts
• Service alerts
• Reporting
• Troubleshooting

Module 6: Monitoring and Reporting
Module 6 discusses monitoring and reporting using Microsoft Intune.

Module 7: Intune as Part of the Enterprise Mobility and Security Product Suite
Module 7 discusses Microsoft Intune as part of the Enterprise Mobility and Security suite of products.
• Azure Active Directory
• Azure Information Protection
• Microsoft Cloud App Security
• Microsoft Advanced Threat Analytics
• Microsoft Identity Manager

Lab: Implementing Microsoft Intune
In this hands-on lab, you will:
1. Sign up for an Office 365 (O365) E5 free trial and a Microsoft Enterprise Mobility and Security (EMS) E5 trial. The EMS trial includes Microsoft Intune. You will use these two trials to complete all the labs in this course. Having created the free trial tenant, you will then explore the portals used to manage them, add users and allocate licenses and finally configure company branding for your tenant.
2. Configure compliance policies for a variety of device platforms using the Azure Portal. This will involve enabling device health, security and operating system settings. To enable this, you will first create Azure AD groups for the devices.
3. Create device configuration profiles, conditional access policies and exchange active sync conditional access connections.
4. Create Intune App Protection (MAM-WE) Policies and evaluate their effectiveness
5. Test the Exchange online conditional access policy.
6. Enrolling an iOS, Windows and Android device into Intune management using various methods