Mastering Modern Desktop and Mobile Device Administration with Microsoft EndPoint Manager (Intune)

0191 3778377
sales@ittrainingsolutions.co.uk
contact us to book

Duration : 3 days

Overview

The course takes learners on a journey through device management using Microsoft Endpoint Manager, formerly known as Intune. The course is a mixture of instructor lead training and hands on exercises when learners configure Microsoft Endpoint and enrol and manage Apple, Microsoft and Android devices.

Prerequisites

The course touches a number of technology areas including Active Directory, Cloud Services (SaaS), Windows, mobile device OSes, Application deployment, networking and Public Key Infrastructure. The course requires attendees to be technically competent with either Windows 10 or Windows Server 2016 and whereas the course does not require any detailed technical requirements it would be an advantage to have skills is some or all of those areas listed above.

Course Content

Introduction to endpoint management

The course starts by looking at the need in the modern information world for the need of a unified endpoint management solution.

Microsoft Endpoint Manager options and choosing a licensing solution

We'll then see where Endpoint Manager fits in to the Microsoft ecosphere and examine the different licensing options available.

Role Based Access Control

Once Endpoint Manger is enabled we'll look at how to build a robust support structure enabling fine grained control using Role Based Access Control (RBAC).

Hybrid environments

Next we'll look at using Endpoint Manager in a hybrid environment, exploring how Azure Active Directory and Active Directory Domain Services can be linked, how the co-management capabilities of Configuration Manager can concurrently manage Windows 10.

Device enrolment and management

After fully configuring Endpoint, we'll then look at how device management works. We start by enrolling devices in to Endpoint using automated options such as AutoPilot, Apple Business Manager and Google zero-touch. Ensuring devices meet corporate requirements with device compliance policies and finally we'll implement conditional access to ensure devices can only access services when they meet all corporate requirements.

Application deployment and control

Once we have devices enrolled and managed, we then take a look at deploying, configuring and protecting apps. We start by looking at how we can obtain apps from Microsoft's business store, Apple's App Store and Google Play store. We'll link Endpoint Manager to each store so that apps can be acquired at a corporate level and distributed to devices.

Once apps are installed we then look at how corporate data can be protected and managed using App Protection Policies. Finally we look at App configuration policies, allowing apps to be configured before they are first used.

Monitoring and reporting

Finally we take a look at the reporting tools built in to Endpoint manager to allow for dynamic monitoring of the health and activity of endpoint devices.

Course content liable to change without notice