

Enterprise Mobile Device Management using Microsoft Intune and System Center 2012 R2 Configuration Manager



WorkshopPLUS

Strategic partnership addresses the specific needs within the customer environment in terms of Enterprise Mobile Device Management (MDM), organizational constraints and processes / operational infrastructure architectures and business solutions.

Target Audience:

Attendees of this course should be experienced users of System Center 2012 Configuration Manager. Ideally, they will have some background in Windows administration and network.

Overview

With the proliferation of mobile devices in the workplace, employees can, and do, work from just about anywhere. To stay productive, this mobile workforce demands consistent access to corporate resources and data from any location on any device. This trend has introduced significant challenges for IT administrators who want to enable enterprise mobility while ensuring that corporate resources are protected from unauthorized access.

Leveraging Microsoft Intune, you can deliver application and device management completely from the cloud, or on-premises through integration with System Center 2012 R2 Configuration Manager, all through a single management console.

Intune is included as part of the Microsoft Enterprise Mobility Suite, a cost-effective way to leverage the Microsoft enterprise mobility cloud services for all of your employees.

Key Features and Benefits

- Guidance about the Microsoft hybrid Mobile Management Solution
- Setup and Integration of Microsoft Intune and Configuration Manager
- Architectural Concepts
- Provisioning of all managed platforms (Microsoft Phone; Microsoft Windows, Apple iOS and Google Android)
- Hands-on training to deploy Software, Policies and Profiles to the devices

Best-Practice

Guidance:

Central management of mobile devices in the enterprise provides challenges to IT administrators. This WorkshopPLUS is designed to address these challenges and provides a central management solution.

Technical Highlights

Students will gain valuable insights from Microsoft Industry Experts on the challenges facing IT Mobile device management teams as they always have a need to keep up-to-date on new devices in the marketplace. This WorkshopPLUS will go into many best practices in the MDM space. Lab environment and exercises are used during the WorkshopPLUS, to help the students better understand how these technologies will work for them.

Prerequisites

This WorkshopPLUS will use virtualized Windows Phone devices to demo the functionality. If you want, you can bring a physical Windows Phone (version 8.0 or later); an iPhone / iPad (iOS version 7 or later) or an Android Phone / Tablet (version 4.4 or later). You are also required to create a Microsoft Account, an Apple ID, and a Google Account for this WorkshopPLUS upfront.

- How do I sign up for a Microsoft account?
<http://windows.microsoft.com/en-us/windows-live/sign-up-create-account-how>
- Create and start using an Apple ID:
<http://support.apple.com/en-us/HT203993>
- Create a Google Account
<https://support.google.com/accounts/answer/27441?hl=en>

Syllabus

Hardware

Requirements:

This WorkshopPLUS requires computers running Windows server 2012 R2 that supports Hyper-V and have at least 16 GB of RAM.

The Enterprise Mobile Device Management WorkshopPLUS of three days is designed to give the IT Administrators the technical ability to set up and maintain a mobile device infrastructure. Furthermore, we provide guidance in strengthening and securing their environment from the threats that employees and guests bring when they are allowed to use their own devices in a corporate IT environment.

Module 1: Introduction to MDM.

This module provides an overview, discusses the need of a mobile device management solution and the unique challenges introduced by MDM.

Module 2: Architecture.

This module provides an overview of the architecture of Microsoft's Device Management Solution and their components. It will also provide a brief view on how MDM integrates with Azure Active Directory, Intune and Office 365 Portals and Multi-Factor Authentication.

Module 3: Implementation.

This module covers the basics of signing up for Microsoft Intune Subscription service, usage of DirSync (Directory synchronization service), and how to set up integration between Microsoft Intune service and System Center 2012 R2 Configuration Manager.

Module 4: Provisioning

This module will cover the basics of enrolling different type of Mobile devices (Windows, Windows Phone, iOS, and Android) and configuring Hardware Inventory for mobile devices. It will also cover its functionality related to Selective and Full Wipe.

Module 5: Software Deployment

This module covers the app deployment to. It also includes Deep Link App deployment, supersedence as welmobile devicesl as side loading apps on mobile devices. This module also covers mobile application reporting.

Module 6 Policies.

This module covers several Policy Enforcement Scenarios using Extension and Compliance Settings. We will also look at OMA-URI settings and enforcements device lockdowns.

Module 7 Profiles.

This module provides in-depth knowledge on certificate deployment and distribution using a NDES infrastructure. We further look at the details of VPN, email and Wi-Fi Profile setup.

Module 8 Troubleshooting

This module explains the components and workflows on implementing the solution, and provides guidance on how to troubleshoot issues.