Microsoft

Enterprise Mobile Device Management Using Microsoft Intune and Configuration Manager

Workshop*PLUS*

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 WorkshopPLUS should be experienced users of Microsoft System Center 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 they 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.

Using Microsoft Intune, you can deliver application and device management completely from the cloud, or on-premises through integration with Microsoft System Center 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.

Current version of the WorkshopPLUS supports **System Center Configuration Manager CB 1702.**

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 (Windows 10, Microsoft Windows, Apple iOS and Google Android)
- Hands-on training on deploying 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 industry experts on Microsoft 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 Workshop*PLUS* will go into many best practices in the MDM space.
The lab environment and exercises are used during the Workshop*PLUS*, to help the students better understand how these technologies will work for them.

Prerequisites

This Workshop*PLUS* will require customers to bring their own devices to demonstrate the MDM functionalities. You are also required to create a Microsoft account, an Apple ID, and a Google Account for this Workshop*PLUS* 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

Microsoft

Syllabus

IT Requirements:
This WorkshopPLUS requires computers running Windows server 2012 R2 or higher that supports Hyper-V. These computers should 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 and Architecture
This module provides an overview of MDM, and discusses the need of a mobile device management solution and the unique challenges introduced by MDM. This module also provides an overview of the architecture of Device Management Solution and its components. It will also provide a brief overview on how MDM integrates with Microsoft Azure Active Directory, Intune and Office 365 Portals and Azure Multi-Factor Authentication.

Module 2: Conditional Access & Device Enrollment
This module covers how to enforce conditional access on devices to ensure company polices are applied before a device can access a company's data.
This module covers the basics of enrolling different types of mobile devices (Windows, Windows 10 Mobile, iOS, Android and Android for work).

Module 3: Application Management
This module covers the app deployment to mobile devices. It also includes Deep Link App deployment, supersedence, as well as side loading apps on mobile devices. This module also covers mobile application reporting.

Module 4: Mobile Application Management (MAM) & Windows Information Protection (WIP)
This module covers enforcing MAM and WIP policies to help protect a company's data.

Module 5: Windows Store for Business (WSfB)
This module covers integration of WSfB with Configuration Manager and deploying apps using WSfB.

Module 6: Profiles Management
This module provides in-depth knowledge on certificate deployment and distribution by using a Network Device Enrollment Service (NDES) infrastructure. It also covers the details of certificate setup for virtual private network (VPN) and Wi-Fi profiles.

Module 7: Wipe Functionalities and Reports
This module covers the selective wipe, full wipe, remote lock, and passcode reset features that help in protecting a company's assets when a device is lost or stolen. It also covers the built-in reports available for Mobile Device Management in Configuration Manager.

Module 8: App Protection & CA without Enrollment
This module covers the App Protection and Conditional access App Protection for devices without enrolling the device into Intune or Configuration manager. Covers policies for iOS, Android and Window 10 platforms. Also covers deploying apps to un-enrolled devices

Module 9: On-premises MDM
This module covers the overview of offline MDM solution with Configuration Manager and Intune for customers who restricts storing any data to the cloud. This module covers how to support Windows 10 devices with on-premises solution with Hybrid Intune.

Microsoft