

**MICROSOFT ENDPOINT CONFIGURATION
MANAGER
COURSE BROCHURE**

Overview

This course provides the necessary knowledge to effectively Deploy, Configure, Manage and Administrate **Microsoft Endpoint Configuration Manager**. Learners will receive hands-on training on Microsoft Endpoint Manager which helps to deliver the modern workplace and modern management to keep your data secure, in the cloud and on-premises. Endpoint Manager includes the services and tools you use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot.

Course Objectives

In this Course, you will learn:

- Installation and Configuration of Microsoft Endpoint Manager
- Verify Your Domain Name with Azure AD Tenant
- Install Azure AD Connect and Sync On-Premises Object to Azure AD
- Enable Co-Management-Publish-Devices to Admin Center
- Windows 10 device - AutoJoin to Hybrid
- Configure Azure Cloud services for use with Configuration Manager
- Azure AD Domain Join and Enroll the device in (MEM) Microsoft Endpoint Manager
- Enroll Byod / Standalone Windows 10 Devices to Endpoint Manager
- Compliance policies to set rules for devices you manage
- Deploy APPS in Microsoft Endpoint Manager - Windows , iOS / Android
- Deploy LOB - Line of Business Applications in Microsoft Endpoint Manager
- Deploy WIN32 Apps - Prepare / Convert Win32 app content for upload
- Configuration Profiles - Automate the settings from Microsoft EndPoint Manager
- Configure Android Enrollment Settings in MEM - For BYOD Devices
- Configure and Enroll Android Devices - Personally-Owned with a work profile (BYOD)
- BYOD - Retire, Remote Lock and Reset Passcode
- Enrollment - Android Enterprise Corporate-Owned with a work profile (COPE)
- Microsoft Endpoint Manager - End user Device - Experience
- Enrollment Configuration - COBO- Corporate owned, Fully managed User Devices
- Deploy App to Android Devices as Available mode
- Configure Apple Enrollment - Apple MDM Push Certificate
- Push Apps to iOS Devices
- Enroll your macOS Device - Admin Center and EndUser Experience
- Deploy Applications to MAC Devices
- Microsoft Endpoint Manager Admin center - Device clean-up rules
- Windows 10 Autopilot for User Driven Mode - Complete Building Blocks Overview
- Adding Devices to Windows Autopilot Profile as Target
- Conditional Access with Endpoint Manager Admin center
- Application Protection policy
- Tenant Administration - Tenant Details, Service Health And Message Center
- Microsoft Endpoint Manager - Tenant Administration

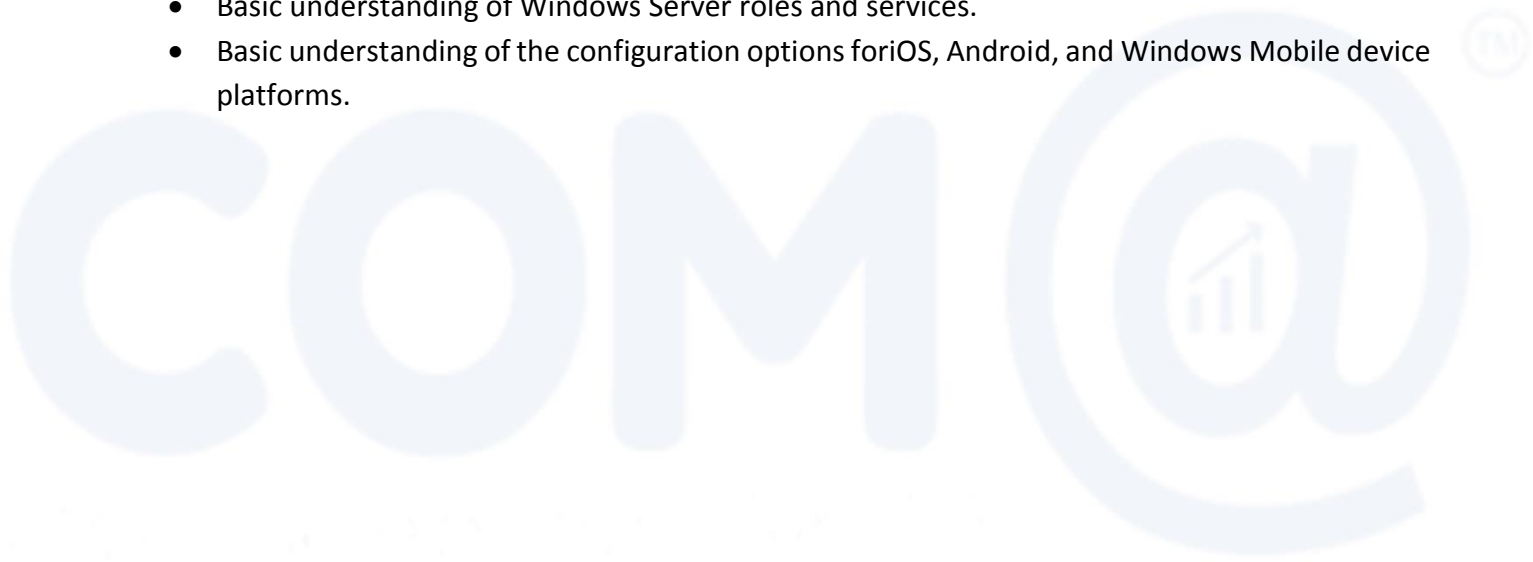
Audience Profile

- This course is for experienced information technology (IT) professionals, typically described as Enterprise Desktop Administrators (EDAs). These EDAs deploy, manage, and maintain PCs, devices, and applications across medium, large, and enterprise organizations. A significant portion of this audience uses, or intends to use, the latest release of Configuration Manager to manage and deploy PCs, devices, and applications.

Prerequisites

Before attending this course, students must have :

- Networking fundamentals, including common networking protocols, topologies, hardware, media, routing, switching, and addressing.
- Active Directory Domain Services (AD DS) principles and fundamentals of AD DS management.
- Installation, configuration, and troubleshooting for Windows-based personal computers.
- Basic understanding of Windows Server roles and services.
- Basic understanding of the configuration options for iOS, Android, and Windows Mobile device platforms.



Course Content:

- Installation and Configuration of Microsoft Endpoint Manager
- Verify Your Domain Name with Azure AD Tenant
- Install Azure AD Connect and Sync On-Premises Object to Azure AD
- Enable Co-Management-Publish-Devices to Admin Center
- Windows 10 device - AutoJoin to Hybrid
- Configure Azure Cloud services for use with Configuration Manager
- Azure AD Domain Join and Enroll the device in (MEM) Microsoft Endpoint Manager
- Enroll Byod / Standalone Windows 10 Devices to Endpoint Manager
- Compliance policies to set rules for devices you manage
- Deploy APPS in Microsoft Endpoint Manager - Windows , iOS / Android
- Deploy LOB - Line of Business Applications in Microsoft Endpoint Manager
- Deploy WIN32 Apps - Prepare / Convert Win32 app content for upload
- Configuration Profiles - Automate the settings from Microsoft EndPoint Manager
- Configure Android Enrollment Settings in MEM - For BYOD Devices
- Configure and Enroll Android Devices - Personally-Owned with a work profile (BYOD)
- BYOD - Retire, Remote Lock and Reset Passcode
- Enrollment - Android Enterprise Corporate-Owned with a work profile (COPE)
- Microsoft Endpoint Manager - End user Device - Experience
- Enrollment Configuration - COBO- Corporate owned, Fully managed User Devices
- Deploy App to Android Devices as Available mode
- Configure Apple Enrollment - Apple MDM Push Certificate
- Push Apps to iOS Devices
- Enroll your macOS Device - Admin Center and EndUser Experience
- Deploy Applications to MAC Devices
- Microsoft Endpoint Manager Admin center - Device clean-up rules
- Windows 10 Autopilot for User Driven Mode - Complete Building Blocks Overview
- Adding Devices to Windows Autopilot Profile as Target
- Conditional Access with Endpoint Manager Admin center
- Application Protection policy
- Tenant Administration - Tenant Details, Service Health and Message Center
- Microsoft Endpoint Manager - Tenant Administration



Our Students Testimonials

CONTACT US

Mobile : +91 9940068251 / 58251

Mail : ramesh@cometcompuserve.com / ilanchezhian@cometcompuserve.com