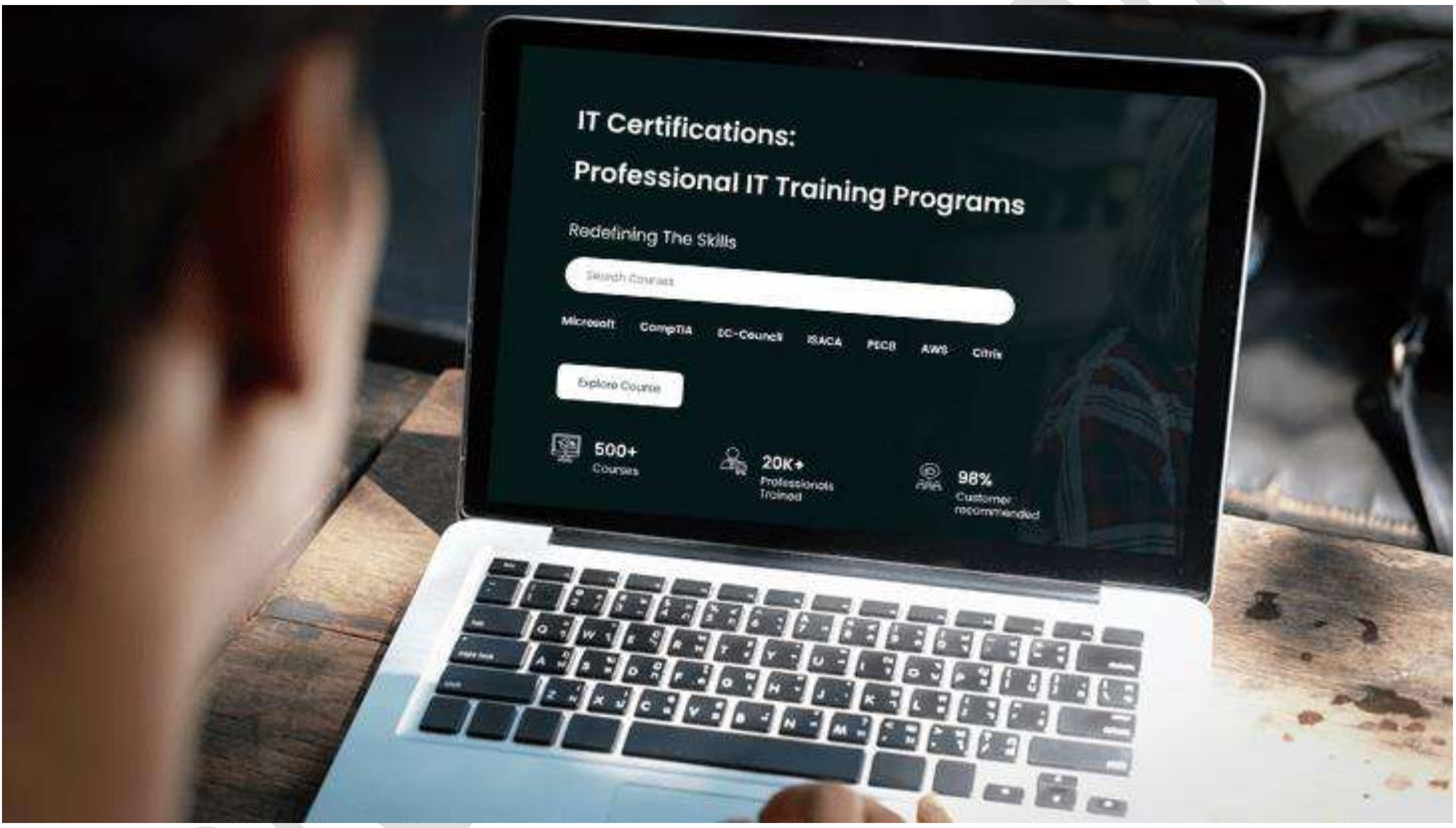
MICROTEK LEARNING | Redefining The Skills



55078: MOBILE DEVICE MANAGEMENT TRAINING

Duration: 2 Days

Course Description

This Mobile Device Management training is a two-day instructor-led training. It is intended for IT professionals responsible for developing a management strategy for mobile devices in the enterprise.

Many Microsoft technologies professionals will design a mobile device plan, configure mobile device management, and master connectivity and data security on these devices.

This course will cover devices running Windows, iOS and Android operating systems. Enterprises must allow users to access information from various devices with a minimum risk of losing that information.

The new tools performed as a part of Windows Server 2012 and Windows Server 2012 R2 and System Center will allow for a complete set of BYOD (bring your own device) enterprise policies.

This course is based on the objectives of 55078A.

Training Exclusives

- Live instructor-led interactive sessions with Microsoft Certified Trainers (MCT).
- Access to Microsoft Official Courseware (MOC).
- Real-time Virtual Lab Environment.
- Experience 24*7 Learner Support.
- Self-paced learning and flexible schedules.

Who should attend this course?

- This course is intended for IT professionals with experience with mobile devices and some versions of Windows client and server operating systems.
- Previous experience with management tools such as Microsoft System Center Configuration Manager would also be valuable but is not required.

What you will learn

- Understand the various types of mobile devices which may connect to the enterprise.
- Determine requirements for and connecting mobile devices via domain join, Workplace Join and VPNs.
- Create a mobile device management strategy.
- Configure a mobile device management infrastructure using Microsoft System Center products and Windows Server 2012 R2.
- Secure corporate data when in transit or on the devices with IPSec and BitLocker.
- Manage data security with Group Policy Objects (GPOs)
- Synchronize data across multiple mobile devices using Work Folders in Windows 8/Windows 8.1.
- Connecting to applications via Web Application Proxy.

Prerequisites

- Basic understanding of TCP/IP and networking concepts.
- Basic Windows and Active Directory knowledge.
- Basic understanding of security concepts such as authentication and authorization.
- Basic experience with a mobile device and mobile operating system.
- Basic understanding of device management fundamentals.

Curriculum

Module 1: Overview of Mobile Device Management

In the past organizations either provided laptops or smart phones approved by the IT department and or allowed users to connect from their Windows based computers using options such as VPNs or Remote Desktop Gateways. These options still exist and remain common. However, the incredible growth of mobile devices from various vendors creates a need for managing access to data and applications from these devices. Organizations must determine the best methods for doing so in a secure manner.

- Lesson 1: What is Mobile Device Management?
- Lesson 2: Overview of Device Management Options

After completing this module, students will be able to:

- Understand the basics of mobile device management
- Gain a high level overview of Microsoft Mobile Device Management tools

Module 2: Mobile Device Management Strategy and Infrastructure

Every organization has unique needs for connecting mobile devices to the corporate network to increase user productivity. Based on the principle of People-centric IT (PCIT) a mobile device strategy can be created to meet those needs. Once the strategy has been determined then it's time to created the infrastructure.

- Lesson 1: Planning for a Mobile Device Management Strategy
- Lesson 2: Designing a Mobile Device Management Infrastructure with Windows Server 2012 R2

Lab1: Create the Mobile Device Management Infrastructure

- Exercise 1: Prepare Active Directory.
- Exercise 2: Prepare the Certification Authority.
- Exercise 3: Prepare Active Directory Federation Services (ADFS).

After completing this module, students will be able to:

- Create a mobile device management (MDM) strategy.
- Design a mobile device management infrastructure based on Windows Server 2012 R2 technologies.

Module 3: Workplace Join and Work Folders

Allowing device connectivity is important, but more important is managing that connectivity. Workplace Join allows a way to track and control which devices can connect. Once connected users will need access to data, no matter the device. That data must be current and consistent without users manually copying files. Work Folders creates this ability.

- Lesson 1: Workplace Join for Mobile Devices
- Lesson 2: Work Folders

Lab1: Workplace Join Windows and iOS Devices

- Exercise 1: Prepare the Workplace Join Infrastructure.
- Exercise 2: Workplace Join an iOS Device.
- Exercise 3: Workplace Join a Windows Device.

Lab2: Work Folders

- Exercise 1: Create the Work Folders Infrastructure.
- Exercise 2: Install Work Folders on Devices.

After completing this module, students will be able to:

- Set up the requirements for Workplace Join.
- Workplace Join devices to Active Directory.
- Create the Work Folders infrastructure.
- Test Work Folders on devices. Resolve common application compatibility issues

Module 4: Web Application Proxy

In the previous module we learned how to connect non-domain devices to Active Directory for management and policies with Workplace Join. In addition we showed how to synchronize data between multiple devices using Work Folders. However almost always data will be used in some type of application, therefore a part of our MDM (Mobile Device Management) strategy must include accessing those applications from devices. This is the responsibility of Web Application Proxy.

- Lesson 1: Web Application Proxy Overview
- Lesson 2: Installing the Web Application Proxy Role Service
- Lesson 3: Configuring the WAP and Publishing Applications

Lab1: Web Application Proxy

- Exercise 1: Prepare the web application (website) on the SCCM virtual machine.
- Exercise 2: Prepare the certificates.
- Exercise 3: Install Web Application Proxy.
- Exercise 4: Publish the application in Web Application Proxy.

After completing this module, students will be able to:

- Understand the features and benefits of Web Application Proxy (WAP).
- Install and configure WAP.
- Publish and connect to applications using WAP.

Module 5: Mobile Device Management Security

One of the primary responsibilities of any IT professional is security. Physical security, network security and data security are critical. In this module we will look at how mobile devices affect security plans not just for BYOD, but also for the entire network infrastructure.

- Lesson 1: Overview of Enterprise and Mobile Device Management Security
- Lesson 2: Hardening the Mobile Device Management Infrastructure

Lab1: Securing the MDM Infrastructure and Communications

- Exercise 1: Secure Accounts Used by MDM.
- Exercise 2: Use Bitlocker to Encrypt a Client System.
- Exercise 3: Configure IPSec.

After completing this module, students will be able to:

- Understand security in the enterprise.
- See how previously discussed MDM technologies are secured.
- Harden the security infrastructure for mobile devices.

Module 6: Mobile Device Lifecycle and Application Management

In this module we will discover the process of managing mobile devices throughout their lifecycles. Technologies including the Microsoft Exchange Connector, System Center Configuration Manager and Windows InTune can be used for these purposes. We will also see how applications can be managed for mobile devices.

- Lesson 1: Mobile Device Lifecycle Management
- Lesson 2: Configuring the SCCM Windows InTune Connector
- Lesson 3: Mobile Device Application Management

Lab1: Managing Mobile Devices with SCCM and Windows InTune

- Exercise 1: Create the Microsoft and Windows InTune Accounts.
- Exercise 2: Connect Windows InTune and Active Directory.
- Exercise 3: Configure Windows InTune to be managed by Configuration Manager.
- Exercise 4: Enroll an External Device in Windows InTune.

After completing this module, students will be able to:

- Understand the Microsoft Exchange Connector.
- Connect System Center Configuration Manager to Windows InTune.
- Manage applications for mobile devices.

For any query Contact Us – Microtek Learning