

Course outline

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.

Lessons

- 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.

Lessons

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

Lab : Create the Mobile Device Management Infrastructure

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.

Lessons

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

Lab : Workplace Join Windows and iOS Devices

Lab : Work Folders

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.

Lessons

- Lesson 1: Web Application Proxy Overview
- Lesson 2: Installing the Web Application Proxy Role Service

- Lesson 3: Configuring the WAP and Publishing Applications

Lab : 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.

Lessons

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

Lab : Securing the MDM Infrastructure and Communications

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.

Lessons

- Lesson 1: Mobile Device Lifecycle Management
- Lesson 2: Configuring the SCCM Windows Intune Connector

- Lesson 3: Mobile Device Application Management

Lab : Managing Mobile Devices with SCCM and 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.