Planning for and Managing Devices in the Enterprise: Enterprise Mobility Suite (EMS) & On-Premises Tools

OD20398B; On-Demand, Video-based

Course Description

This course teaches IT professionals how to use the Enterprise Mobility Suite to manage devices, users, and data. In addition, this course teaches students how to use other technologies, such as Group Policy and other Windows Server–based technologies, to manage devices and secure data. Students will learn how to design and implement cloud-based and on-premises solutions for managing Windows-based, iOS, and Android devices, and they will learn how to provide secure and efficient access to data and applications.

Course Objectives

After completing this course, students will be able to:

- Use devices in the enterprise environment
- Describe AD DS features for device management
- Implement and administer Microsoft Azure Active Directory (Azure AD)
- Connect AD DS with Azure AD
- Plan and implement app support
- Manage devices in Microsoft Office 365
- Plan and implement Intune
- Use Intune to manage devices
- Use Intune to manage applications and Resource Access
- Plan and implement Microsoft Azure Rights Management (Azure RMS)
- Plan and implement Remote Access
- Plan and protect data
- Recover data and operating systems

Audience

This course is intended for IT professionals and consultants who plan, deploy, and manage devices and applications in medium to large organizations. A significant portion of this audience works in onpremises Active Directory Domain Services (AD DS) environments with both domain-joined and nondomain joined devices, for which they need to provide mobile device management and secure data access. Devices in

such environments typically run Windows 10, Windows 10 Mobile, iOS, and Android. They plan to extend on-premises AD DS to the cloud and they need to learn how to plan and implement Enterprise Mobility Suite.

Prerequisites

In addition to their professional experience, students who attend this training should already have the following technical knowledge:

- TCP/IP networking fundamentals
- Understanding of Domain Name System (DNS)
- Working knowledge of Active Directory principles
- Understanding of the public key infrastructure (PKI) fundamentals
- Understanding of cloud-based service concepts
- Windows Server 2012 R2 fundamentals, including Remote Desktop Services
- Experience with Windows 10
- Familiarity with Windows PowerShell
- Basic knowledge of mobile platforms

Course Outline

Module 1: Using devices in the enterprise environment

This is an overview module that introduces changes and challenges in today's typical workplace, and the solutions to address them. The intention of this module is to set the stage for later modules, and to introduce the Enterprise Mobility Suite.

Lessons

- Overview of devices in an enterprise
- Devices management features
- Overview of the Enterprise Mobility Suite

Lab: Planning for device management

- Selecting the appropriate products and technologies for device management
- Working with devices

After completing this module, students will be able to:

- Describe enterprise devices
- Describe device management features
- Describe Enterprise Mobility Suite

Module 2: Implementing and administering Azure AD

In this module students will learn how to manage devices in an on-premises Active Directory environment. They will learn about cloud identity, and the features that Azure AD provides. They also will learn about Azure AD offerings, how to create and manage an Azure AD tenant, and how claims-based authentication works.

Lessons

- Overview of AD DS
- Overview of Azure AD
- Creating and managing Azure AD
- Managing authentication in Azure AD

Lab: Working with Azure AD and providing access to claims-aware applications

- Managing Azure AD users and groups
- Joining a Windows 10 device to Azure AD
- Accessing cloud applications with SSO

After completing this module, students will be able to:

- Describe AD DS
- Describe Azure AD
- Create and manage Azure AD
- Manage authentication in Azure AD

Module 3: Connecting AD DS with Azure AD

In this module students will learn how to connect their on-premises AD DS with Azure AD. They will learn about Azure AD Connect, and how either to synchronize entire identities to Azure AD, including password hashes, or to establish federation with Azure AD.

Lessons

- Preparing AD DS for directory synchronization
- Implementing Azure AD Connect
- Planning and implementing federation

Lab: Synchronizing on-premises AD DS with Azure AD

- Implementing Azure AD Connect
- Verifying synchronization of new objects
- Implementing and using Azure AD Premium features

After completing this module, students will be able to:

- Prepare AD DS for directory synchronization
- Implement Azure AD Connect

- Plan and implement federation

Module 4: Managing devices in Office 365

In this module students will learn about Office 365 and its main features. The focus of this module is on device management by using mobile device management for Office 365.

Lessons

- Overview of Office 365
- MDM for Office 365

Lab: Managing devices in Office 365 (Part 1)

- Obtaining an Office 365 subscription
- Enabling MDM

Lab: Managing devices in Office 365 (Part 2)

- Configuring and testing mobile device management in Office 365

After completing this module, students will be able to:

- Describe Office 365
- Explain MDM for Office 365

Module 5: Planning and implementing Microsoft Intune

In this module students will learn how to plan for Microsoft Intune, how to deploy an Intune client, and how to perform basic Intune administration.

Lessons

- Planning for Intune
- Deploying Intune clients
- Basic Intune administration

Lab: Planning and implementing Intune

- Deploying Intune clients and linking computers to users
- Create Intune users
- Delegating Intune permissions
- Creating Intune groups

After completing this module, students will be able to:

- Plan for Intune
- Deploy Intune clients
- Describe basic Intune administration

Module 6: Managing devices by using Intune

In this module students will learn how to enroll and manage mobile devices with Intune, create, manage and deploy different types of Intune policies, and manage updates and Windows Defender by using Microsoft Intune.

Lessons

- Working with Microsoft Intune policies
- Mobile device management
- Managing updates and Windows Defender

Lab: Using Microsoft Intune policies to manage devices

- Configuring Azure AD with automatic mobile device management enrollment
- Working with Microsoft Intune policies

Lab: Managing updates and Windows Defender

- Managing updates by using Intune
- Managing Windows Defender by using Intune

After completing this module, students will be able to:

- Work with Intune policies
- Describe mobile device management
- Manage updates and Windows Defender

Module 7: Using Microsoft Intune to manage applications and resource access

In this module students will learn how to manage application deployments by using Microsoft Intune. They will also learn how to deploy settings, such as VPN profiles, Wi-Fi profiles and certificates to Intune clients.

Lessons

- Application lifecycle management
- Application deployment process
- Managing access to company resources

Lab: Using Intune to deploy and monitor applications

- Using Intune to deploy and monitor applications

Lab: Using Intune to manage resource access

- Configuring certificate deployment in Intune
- Configuring conditional access policies

After completing this module, students will be able to:

- Describe application lifecycle management
- Describe the application deployment process
- Manage access to company resources

Module 8: Planning and implementing Azure RMS

In this module students will learn how to plan and implement Azure Rights Management to protect digital content. They also will learn which applications can integrate with Azure Rights Management, and how to use Azure Rights Management with Office 365 in an on-premises infrastructure.

Lessons

- Overview of Azure RMS
- Implementing Azure RMS

Lab: Using Azure RMS to protect documents and data

- Protecting documents with Azure RMS
- Using FCI with Azure RMS

After completing this module, students will be able to:

- Describe Azure RMS
- Implement Azure RMS

Module 9: Planning and implementing app support

In this module students will learn how they can mitigate compatibility issues between applications on the same device, and between the application and the operating system. They also will learn about RemoteApp and Azure RemoteApp programs, which enable you to run Windows apps on any device with the Remote Desktop Protocol (RDP) client.

Lessons

- Planning and implementing application compatibility options
- Publishing and using RemoteApp programs
- Publishing and using Azure RemoteApp

Lab: Publishing and using RemoteApp and Azure RemoteApp

- Publishing and accessing RemoteApp programs
- Publishing and accessing Azure RemoteApp programs

After completing this module, students will be able to:

- Plan and implement application compatibility options
- Publish and use RemoteApp programs
- Publish and use Azure RemoteApp

Module 10: Planning and implementing remote access

In this module students will learn how to provide remote access from devices to a company network. They also will learn how to provide access to company infrastructure servers, data in work folders, and data that is stored in the cloud.

Lessons

- Overview of remote access solutions
- Implementing remote infrastructure access
- Planning and implementing Work Folders
- Implementing cloud data access
- Planning and implementing mobility options

Lab: Configuring and using VPN and Work Folders

- Configuring a VPN server and a VPN client
- Configuring and using Work Folders

Lab: Using Offline Files and OneDrive

- Configuring and using Offline Files
- Synchronize settings between Windows 10 devices
- Configuring and using OneDrive

After completing this module, students will be able to:

- Describe remote access solutions
- Implement remote infrastructure access
- Plan and implement Work Folders
- Plan and implement cloud data access
- Plan and implement mobility options

Module 11: Planning and implementing Dynamic Access Control and auditing

In this module students will learn how to implement Dynamic Access Control, and how to configure and

use advanced auditing.

Lessons

- Planning and implementing Dynamic Access Control
- Planning and deploying advanced audit policies

Lab: Implementing secure data access

- Preparing for Dynamic Access Control deployment
- Implementing Dynamic Access Control
- Validating and remediating Dynamic Access Control
- Using advanced audit policies

After completing this module, students will be able to:

- Plan and implement Dynamic Access Control
- Implement Dynamic Access Control
- Plan and deploy advanced audit policies

Module 12: Planning and protecting data

In this module students will learn how to protect data on a device by using encryption or BitLocker. They will also learn about Enterprise Data Protection and how data can be remotely wiped if a device is lost or stolen.

Lessons

- Planning and implementing encryption
- Planning and implementing BitLocker
- Protecting data on devices

Lab: Protecting data by using encryption and BitLocker

- Encrypting and recovering access to encrypted files
- Using BitLocker to protect data

After completing this module, students will be able to:

- Plan and implement encryption
- Plan and implement BitLocker
- Protect data on the device

Module 13: Recovering data and operating systems

In this module students will learn how to plan and implement file recovery and device recovery of Windows 10 devices. They also will learn how to update a Windows 10 device, and learn about

Windows Branch.

Lessons

- Planning and implementing file recovery
- Planning and implementing device recovery
- Planning and implementing updates

Lab: Implementing file recovery and device recovery

- Using File History to recover files
- Using Previous Versions to recover files
- Recovering a device with a restore point
- Using the advanced startup options to recover a device

After completing this module, students will be able to:

- Plan and implement file recovery
- Plan and implement device recovery
- Plan and implement updates