Microsoft Intune Device Management

Description:

Microsoft Intune is a cloud-based service in the enterprise mobility management (EMM) space that helps enable your workforce to be productive while keeping your corporate data protected. Similar to other Azure services, Microsoft Intune is available in the Azure portal. With Intune, you can:

- Manage the mobile devices and PCs your workforce uses to access company data.
- Manage the mobile apps your workforce uses.
- Protect your company information by helping to control the way your workforce accesses and shares it.

Course Duration:

3 days

Course Outline:

Module 1 - Definition of Microsoft Intune

1. What is Microsoft Intune?
2. Why Microsoft Intune?
3. Comparison between MDM for Office 3655 & Microsoft Intune

Module 2 - Configure Microsoft Intune

1. Setting up a Microsoft Intune account
2. Add Custom Domain
3. Add Intune Users
4. Activate Synchronized Users and Grant Licenses
5. Azure Active Directory Pass-through Authentication “PTA”

Module 3 - Organize Users & Devices in Microsoft Intune

1. Create Intune groups to organize users and devices.
2. Device Enrollment Manager
3. Assign Additional Administrators to manage Microsoft Intune
4. Role-Based administration control (RBAC) with Microsoft Intune

Module 4 - Set Mobile Devices Management (MDM) Authority.

1. Set Mobile Device Management Authority
2. Prepare for Mobile Device Management Authority “iOS”
3. Prepare for Mobile Device Management Authority “Android”
4. Manage your company’s terms and conditions for user access
5. Identify Devices Corporate-owned
6. Intune Company Portal Branding

Microsoft Intune Device Management

Module 5 – Protect Mobile Devices Using Microsoft Intune "MDM"

1. Device configuration
2. Compliance policies in Microsoft Intune
3. Conditional Access policies in Microsoft Intune
4. Reset passcodes when users are locked out of their devices
5. Bypass Activation Lock on Supervised iOS devices with Intune
6. Retire Devices and Remove Data

Module 6 - Deploy Applications Using Microsoft Intune.

1. Deploy Apps "Office ProPlus" to Windows 10 MDM using Intune
2. Deploy Apps to Mobile Devices in Microsoft Intune
3. Deploy App to Android Enterprise "Android for Work" Mobile Devices

Module 7 – Intune App Protection "Mobile Application Management"

1. iOS App Protection Policy
2. Android App Protection Policy
3. Enforce users to use Managed App on Mobile devices
4. Windows Information Protection (WIP) App Protection policy
5. App Configuration Policy
6. Protected Browser App on Mobile Devices
7. Monitor App Protection
8. App Selective Wipe
9. Wrap Android Apps with the Intune App Wrapping Tool for App protection policies
10. Wrap iOS Apps with the Intune App Wrapping Tool for App protection policies

Module 8 – Integrate between Intune & Other Products

1. Telecom expense management service in Intune
2. Integrate between Microsoft Intune & Windows Defender ATP
3. Integrate between Microsoft Intune & Lookout Mobile Threat Defense

Module 9 – Manage Windows 10 PCs Using Microsoft Intune

1. Enroll Windows 10 MDM
2. Manage Powershell Scripts Using Microsoft Intune
3. Deploy Application (EXE or MSI) on Windows 10 MDM
4. Manage Software Updates in Intune
5. Configure Remote Assistance
6. Protect Windows 10 MDM Using Microsoft Intune
7. Retire Devices and Remove Data

Microsoft Intune Device Management

Module 10 - Intune Reporting & Alerts.

1. Use the Intune Data Warehouse
2. Intune APIs in Microsoft Graph

Module 11 - Resource Access profile with Microsoft Intune.

1. Enable access to corporate email using email profiles
2. Help users connect to their work using VPN profiles
3. Help users connect to company networks using Wi-Fi profiles
4. Enable access to company resources using Certificate profiles

Module 12 – Intune Scenarios & End User Actions

1. Intune Business Scenarios
2. Enroll Mobile Devices Using Microsoft Intune