Microsoft Intune Training Model

1. Introduction to Microsoft Intune

1. What is Microsoft Intune?
2. Overview of mobile device management (MDM) and mobile application management (MAM).
3. Cloud-based solution for device security, app management, and compliance enforcement.
4. Integration with Azure Active Directory (Azure AD), Microsoft 365, and other Microsoft services.
5. Intune Benefits: Security, scalability, compliance.
6. Key use cases: Device provisioning, security enforcement, app management, and reporting.
7. Intune Service Architecture
8. Intune components and integration with Microsoft 365.
9. Data residency and compliance.
10. Role-Based Access Control (RBAC)
11. Advanced RBAC configuration.
12. Custom roles and delegation.

---

2. Getting Started with Intune

1. Setting Up Microsoft Intune
2. Signing up for Microsoft Intune.
3. Accessing the Intune portal (Microsoft Endpoint Manager admin centre).
4. Initial configuration: Linking with Azure AD, assigning licenses, and setting up the basic environment.
5. Intune Interface Overview
6. Navigation: Admin centre dashboard, device management, app deployment, and policies.
7. Key components: Devices, Apps, Endpoint security, Configuration profiles, Reports, and Groups.

---

3. Managing Devices with Intune

1. Device Enrolment
2. Methods of enrolling devices (Auto Enrolment, Apple DEP, Android Enterprise, Windows Autopilot, etc.).
3. Device enrolment flows and steps for iOS, Android, and Windows devices.
4. Conditional access during enrolment.
5. Device Configuration Profiles
6. Creating and deploying configuration profiles (Wi-Fi, VPN, email settings).
7. Configuring security settings, such as passwords, encryption, and restrictions.
8. Managing device settings for different OS platforms (iOS, Android, Windows).
9. Device Compliance Policies
10. What is a compliance policy?
11. Creating and deploying compliance policies to enforce security standards (e.g., PIN, encryption, OS version).
12. Monitoring compliance status and acting on non-compliant devices.
13. Managing Device Groups
14. Creating device groups (based on OS, location, or department).
15. Assigning policies, apps, and configuration profiles to device groups.

Microsoft Intune Training Model

4. Managing Applications with Intune

1. App Deployment
2. Types of apps supported: Store apps, line-of-business (LOB) apps, web apps, and public apps.
3. Adding and assigning apps to devices or users.
4. Configuring app protection policies.
5. App Configuration
6. Configuring app settings for iOS, Android, and Windows apps.
7. Using Managed Google Play and App Store for app management.
8. App Protection Policies
9. Creating app protection policies for securing data in mobile apps (MAM without enrolment).
10. Protecting corporate data with features like encryption, access control, and data sharing restrictions.

---

5. Security with Intune

1. Endpoint Security Policies
2. Managing BitLocker and File Vault.
3. Creating and deploying antivirus, firewall, and other endpoint security policies.
4. Managing and monitoring security profiles for devices (e.g., anti-malware, firewall, attack surface reduction).
5. Integration with Microsoft Defender.
6. What is conditional access and how does it work? Setting up conditional access policies to control access to corporate resources based on user/device state.
7. Blocking or granting access based on compliance, location, or user risk.
8. Understanding security baselines for Android, iOS, and Windows.
9. Implementing and customizing security baselines to meet organizational needs.

---

6. Monitoring and Reporting

1. Monitoring Device Status
2. Using the Intune portal to track device status, including enrolment, compliance, and health.
3. Device lifecycle: From enrolment to decommissioning.
4. Reporting and Analytics
5. Overview of Intune reporting capabilities: Device reports, app deployment status, compliance policies.
6. Exporting and customizing reports for auditing and troubleshooting.
7. Troubleshooting
8. Troubleshooting device enrolment, compliance issues, and app deployment failures.
9. Using the Intune Troubleshoot and Diagnostics tool for resolving issues.
10. Common issues and how to resolve them (e.g., device not enrolling, compliance errors).

---

7. Advanced Intune Features

1. Windows Autopilot
2. Overview of Windows Autopilot for provisioning new devices.
3. Creating profiles for Autopilot deployment and setting up a zero-touch provisioning experience.
4. Advanced Threat Protection (ATP)
5. Integration with Microsoft Defender ATP.
6. Creating policies to defend against malware and other threats.
7. Intune for Education
8. Managing and configuring Intune for schools.
9. Special configurations for K-12 environments, including simplified deployment and management tools.

---

8. Best Practices and Tips

1. Best Practices for Device Management
2. Structuring and organizing device groups.
3. Maintaining security with least privilege principles.
4. Routine monitoring and reporting for compliance.
5. Troubleshooting Tips
6. Using the diagnostic tools and logs.
7. How to handle common device issues (e.g., apps not installing, devices failing to meet compliance).
8. Common Pitfalls and How to Avoid Them
9. Mistakes to avoid during policy creation and deployment.
10. Ensuring the correct configurations are set to avoid conflicts between policies.

---

9. Conclusion

1. Recap and Key Takeaways
2. Understanding the end-to-end device lifecycle management.
3. Emphasizing security, compliance, and effective app management.
4. Importance of ongoing monitoring and troubleshooting.
5. Next Steps
6. Encourage deeper learning and certification (Microsoft Certified: Endpoint Administrator Associate).
7. Link to further documentation, communities, and forums for advanced learning.