Integrating Enterprise Mobility Management (EMM) with Azure AD and Google Workspace involves ***connecting your chosen EMM solution (like Microsoft Intune, Google Workspace's built-in EMM, or a third-party solution) with both Azure AD and Google Workspace to manage devices and applications****. This typically involves configuring single sign-on (SSO) and potentially user provisioning, allowing for consistent authentication and access control across both platforms. [1, 2, 3, 4, 5, 6]*

Key aspects of integration:

- ***Single Sign-On (SSO):*** *Enables users to access both Azure AD-managed and Google Workspace-managed resources with a single set of credentials, improving user experience and streamlining access. [7, 7, 8, 8, 9, 9, 10, 11]*
- ***User Provisioning:*** *Automates the creation and management of user accounts in both Azure AD and Google Workspace, ensuring consistency and reducing manual administration. [12, 12, 13, 13, 14, 15, 16]*
- ***Device Management:*** *Allows you to manage devices (including mobile devices and computers) enrolled in your EMM solution and enforce policies across both Azure AD and Google Workspace environments. [17, 17, 18, 18, 19]*
- ***Application Management:*** *Provides control over which applications users can access, potentially through both Azure AD's app gallery and Google Workspace's managed Google Play store. [20, 20, 21, 21, 22, 23]*

Common integration scenarios:

- ***Microsoft Intune with Google Workspace:*** *Intune can be connected to Managed Google Play to manage Android devices and applications, while also integrating with Azure AD for user authentication and SSO. [17, 17, 18, 18]*
- ***Google Workspace as the primary identity provider:*** *In some cases, Google Workspace can be used as the primary identity provider for users accessing Azure AD resources, potentially through federation or SSO configurations. [8, 8, 24, 24, 25, 26]*

Steps for integration:

1. ***Choose an EMM solution:*** *Decide whether to use Microsoft Intune, Google Workspace's built-in EMM, or a third-party EMM solution. [17, 17, 18, 18, 27, 27]*
2. ***Configure SSO:*** *Set up SSO between Azure AD and Google Workspace, potentially using SAML or other protocols. [7, 7, 8, 8, 9, 9, 28, 29]*
3. ***Enable user provisioning:*** *Configure automatic user provisioning to synchronize users and groups between Azure AD and Google Workspace. [12, 12, 21, 21, 30, 31, 32]*
4. ***Connect your EMM to Google Play:*** *If using Intune, connect it to Managed Google*

Play for Android device management. [17, 17, 18, 18]

5. ***Configure policies and application access:*** *Define policies and manage application access for both Azure AD and Google Workspace resources. [20, 27, 33, 34]*

Considerations:

- ***Choose the right EMM solution:*** *The best EMM solution depends on your specific needs and infrastructure. [21, 21, 35, 35, 36]*
- ***Plan your integration carefully:*** *Thorough planning is crucial to ensure a smooth and secure integration process.*
- ***Test thoroughly:*** *Before deploying to production, test the integration thoroughly to identify and resolve any potential issues. [21, 21, 35, 35, 37]*
- ***Consider security implications:*** *Ensure that your integration adheres to security best practices and that you have appropriate security measures in place. [24, 24, 35, 35, 38]*