Android Zero-touch Enrollment

Android Zero-touch Enrollment or Android Zero-touch Provisioning (ZTP) is a device enrollment method provided by Google that **streamlines** the enrollment and **easy deployment** of organization-owned Android devices in bulk.

Advantages of Zero-touch

- One time setup.
- Aids large-scale enterprise device rollout.
- Allows resellers to add devices to the portal, easing the enrollment process.
- Admins can set up the device with necessary apps and profiles and it gets applied automatically on device activation.

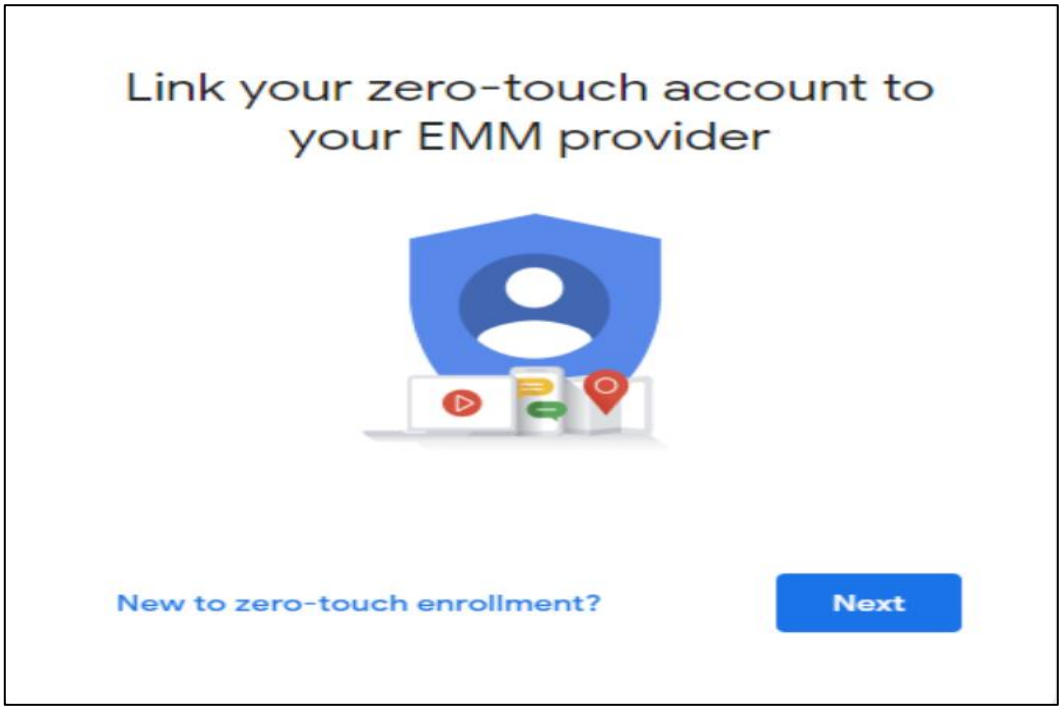
Pre-requisites for Zero-touch

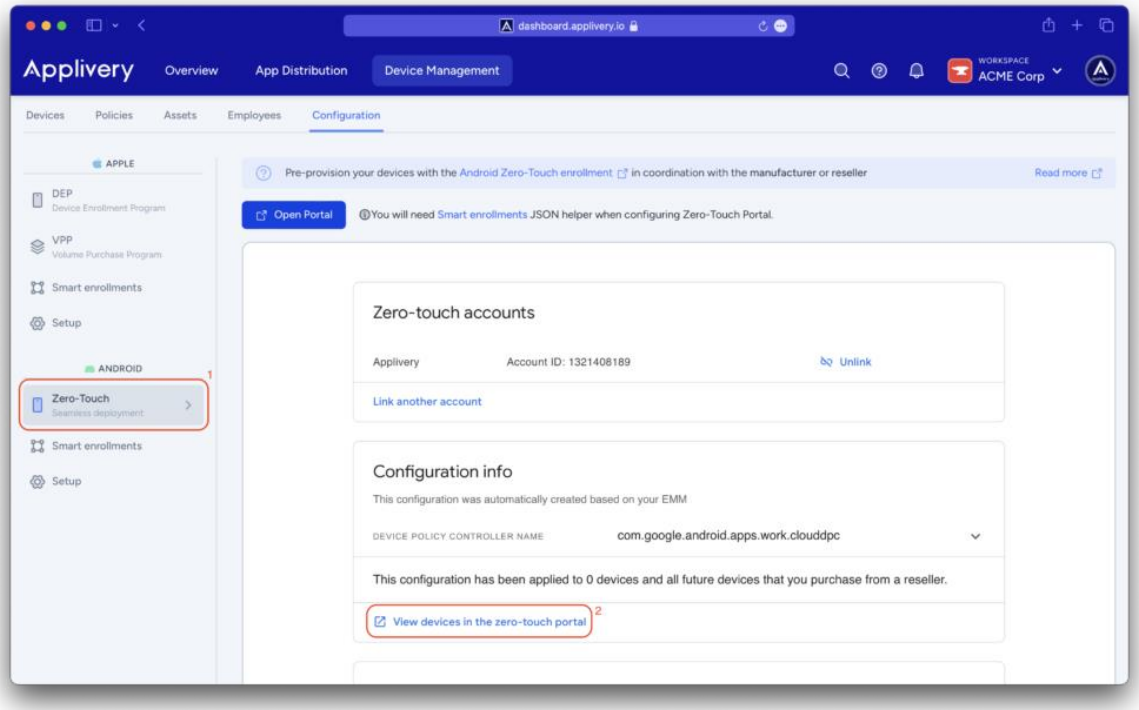
- Android Zero-touch **Enrollment is supported** for devices running Android 9.0 or later, purchased from specified reseller partners.
- You need a **Zero-touch portal account** which can be obtained by contacting your reseller.

Integrate Applivery with Zero-touch

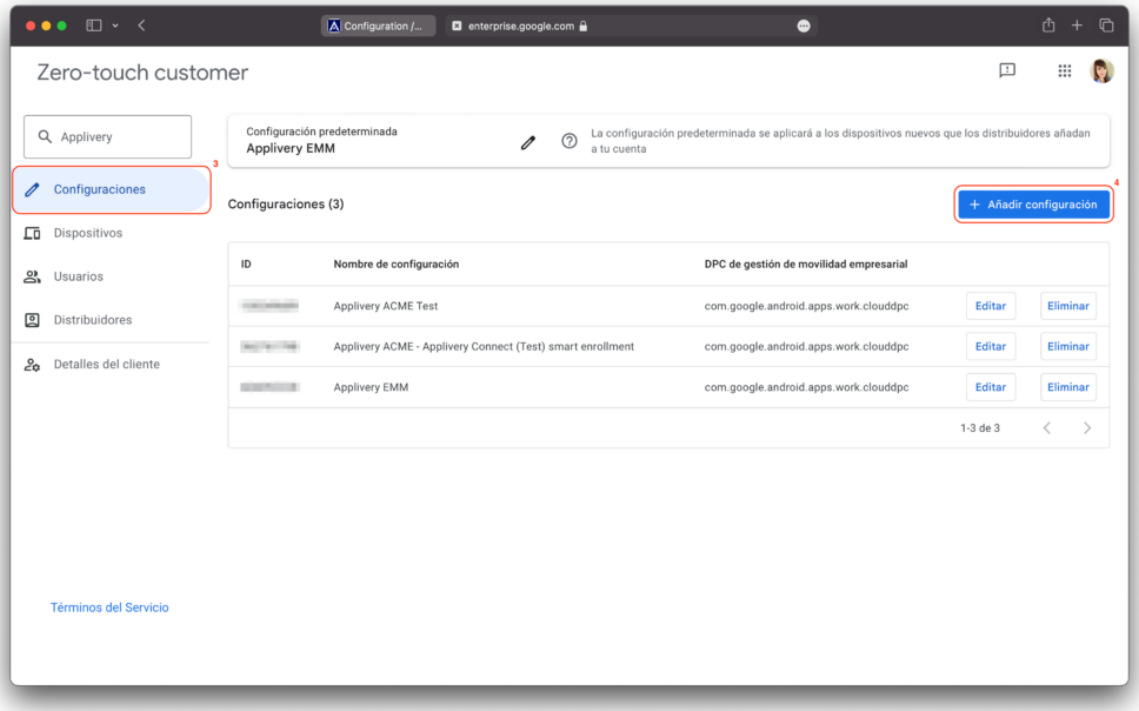
Once in the Applivery dashboard, head to Device Management > Configuration and select the **Android Zero-Touch (1)**.

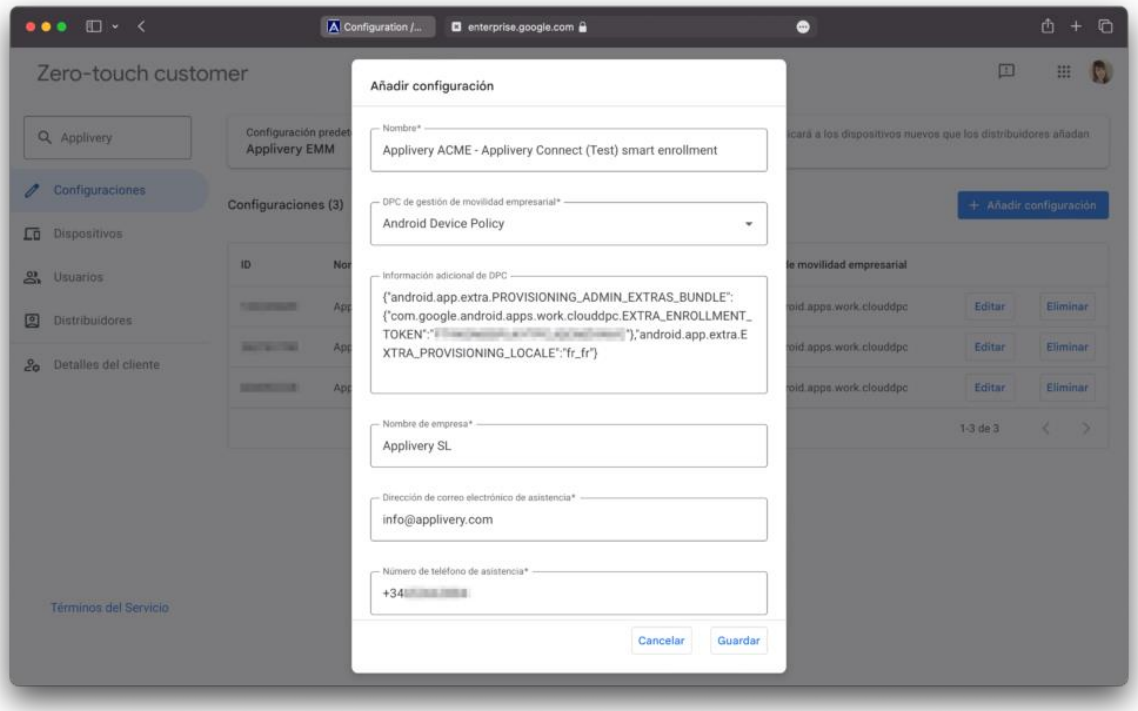
You will need to link your Zero-touch to Applivery and follow the on-screen steps. Once the **integration has been successfully** completed, you just need to click on **View devices in the zero-touch portal (2).**



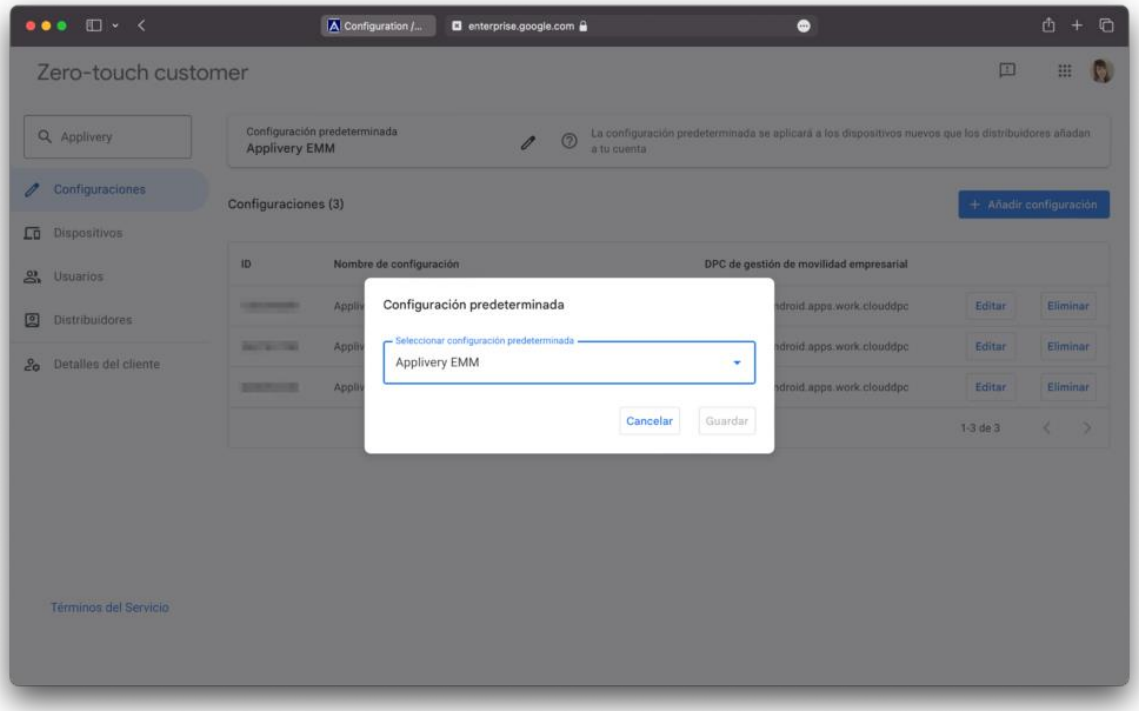


A new window will open in your browser, where you will find the **Configurations (3)** section. You can add a new configuration by simply clicking the **+ Add configuration (4)** button placed on the right side of the screen.



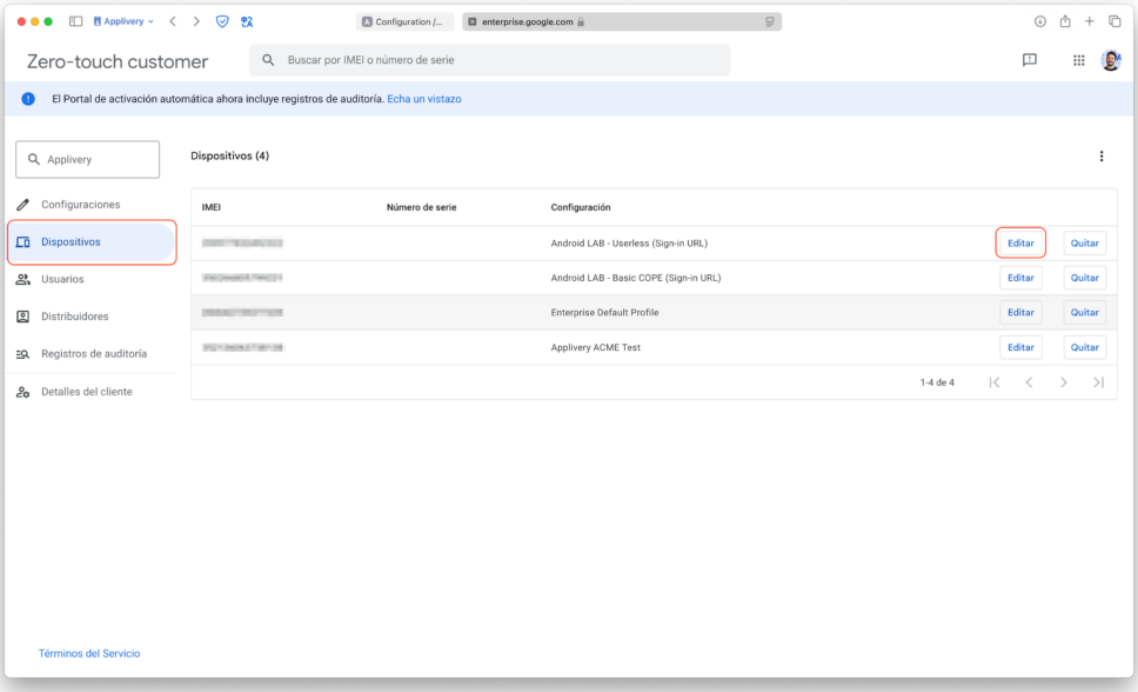


The last step in the portal is to associate the created configuration with the devices. To do that, just select the configuration, which is to be automatically applied to the added devices and click the **Save button.**

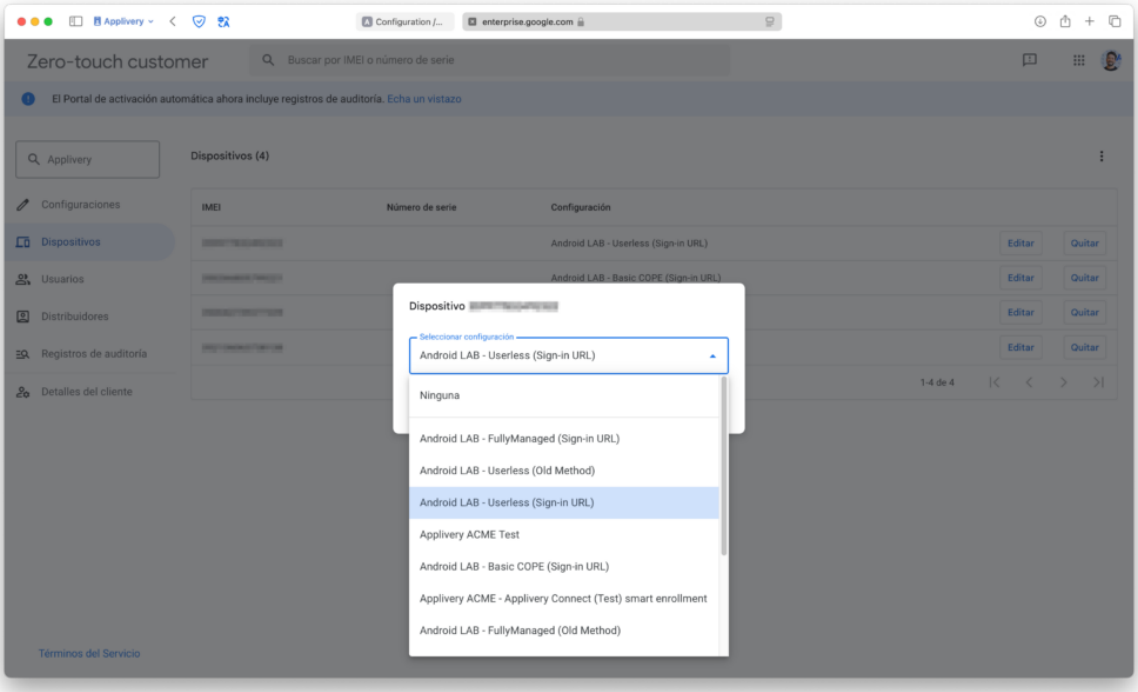


Adding the configuration to your devices

Once the configuration is created, **navigate** to the Devices section from the left-side menu. Here, you'll find a list of devices currently active with Zero-touch that need to be assigned a configuration. This ensures that **automatic enrollment** points to the correct configuration, allowing the device to enroll properly.



To assign a configuration, select **Edit on the desired device**. Then, **choose** the appropriate configuration from the drop-down menu.

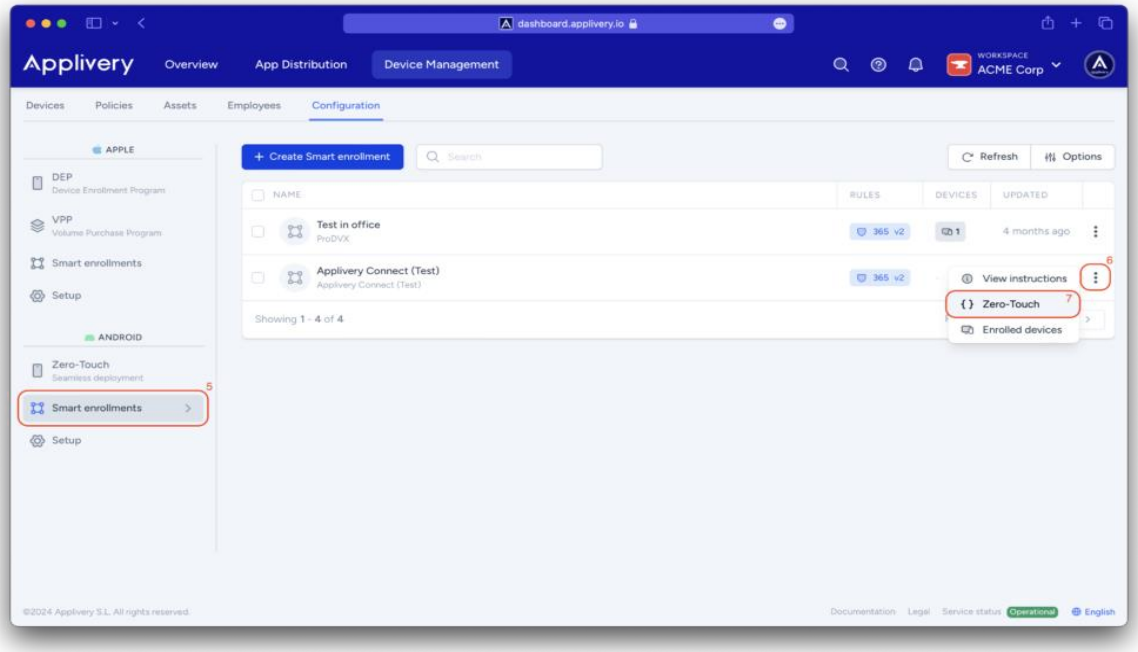


From this point on, the device will **automatically enroll** in Applivery after a factory reset, requiring no additional action.

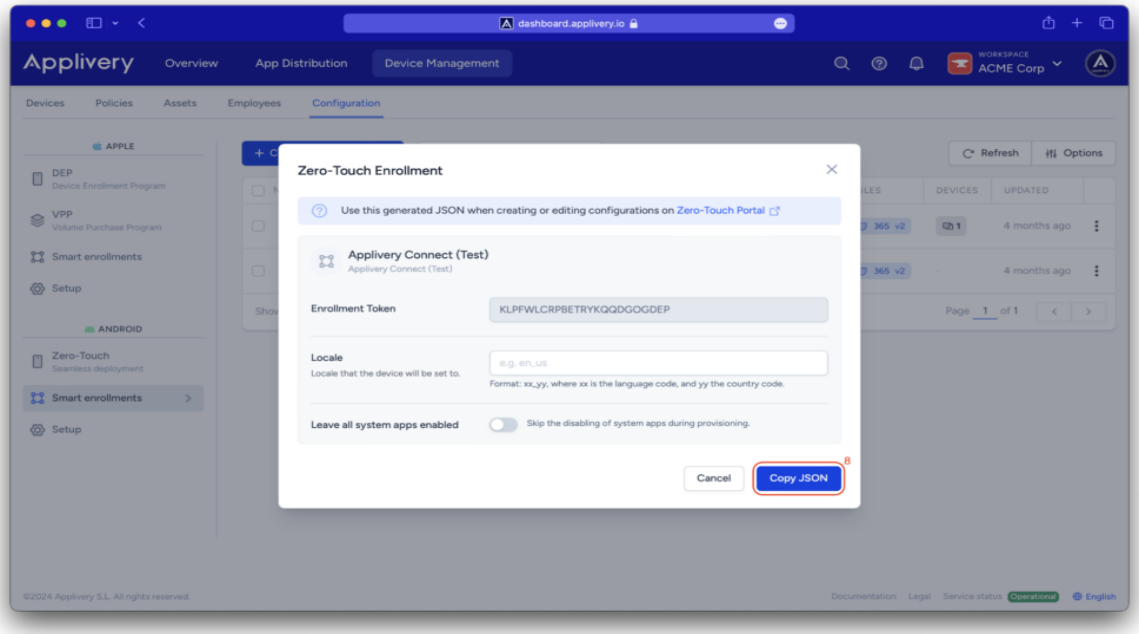
Obtain the JSON for the DCP extras field

Once in the Applivery dashboard, navigate to Device Management > Configuration and select the **Android Smart enrollments (5).**

Then, click on the **vertical dots (6)** located at the end of the smart enrollment you wish to configure within the Zero-touch portal and select **Zero-Touch (7).**



A modal view will appear, allowing you to input additional **configurations and copy (8)** the necessary JSON for the DPC extras.



Create Integration with Azure AD/Google Workspace & Administration Policy Configuration & Application Management

Integration with Azure AD/Google Workspace

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.

Key aspects of integration:

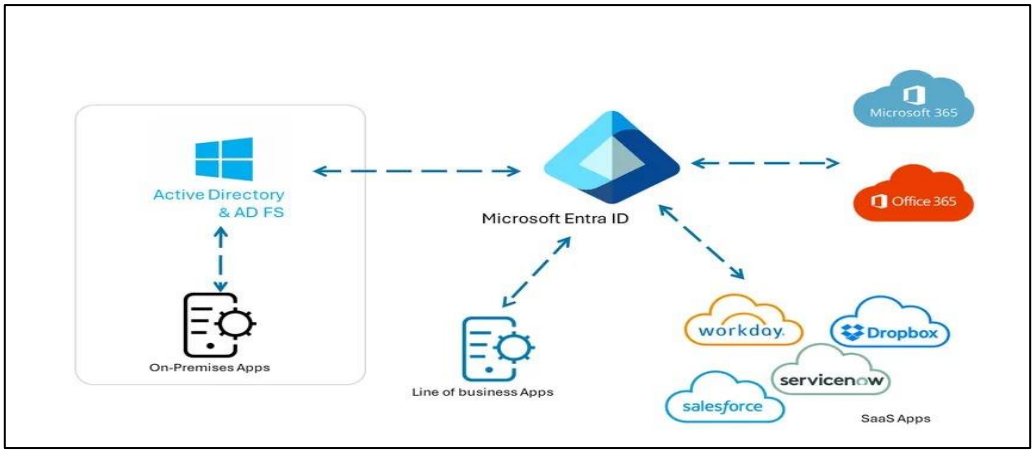
- **Single Sign-On (SSO):** Enables users to access both Azure AD-managed and Google Workspace-managed resources with a single set of credentials, improving user experience and streamlining access.
- **User Provisioning:** Automates the creation and management of user accounts in both Azure AD and Google Workspace, ensuring consistency and reducing manual administration.
- **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.
- **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.

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.
- **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.

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.
2. **Configure SSO:** Set up SSO between Azure AD and Google Workspace, potentially using SAML or other protocols.
3. **Enable user provisioning:** Configure automatic user provisioning to synchronize users and groups between Azure AD and Google Workspace.
4. **Connect your EMM to Google Play:** If using Intune, connect it to Managed Google Play for Android device management.
5. **Configure policies and application access:** Define policies and manage application access for both Azure AD and Google Workspace resources.



Policy Configuration and Application management

In Enterprise Mobility Management (EMM), policy configuration and application management are **crucial for securing and controlling access to corporate data and resources on mobile devices**.

Policy Configuration:

- **Purpose:** EMM policies define rules and restrictions for devices, users, and applications to maintain security and compliance.
- **Device policies:** Control access to corporate resources, enforce password requirements, manage device settings (like Wi-Fi and VPN), and enable remote actions like device lock or wipe.
- **Application policies:** Control how corporate apps are used, including data access, sharing restrictions, and permissions.
- **User policies:** Define user roles, access levels, and authentication requirements.
- **Implementation:** EMM platforms offer tools and interfaces for IT admins to create, configure, and deploy policies. This often involves selecting pre-defined policies or creating custom ones.
- **Example:** An EMM policy might restrict users from downloading specific apps, require strong passwords, or prevent data from being copied to personal storage.

Application Management:

- **Purpose:** EMM solutions allow for the distribution, management, and control of applications on corporate devices.
- **Application deployment:** EMMs can deploy apps to devices, either directly or through app stores, and manage app updates.
- **App configuration:** EMMs can push pre-configured settings to apps, ensuring consistent behavior and reducing user setup time.
- **Application security:** EMMs can enforce security policies on apps, including data encryption, access restrictions, and protection against malware.
- **App wrapping:** Some EMMs can wrap apps with security features, providing enhanced control and protection without requiring changes to the app itself.
- **Implementation:** EMMs offer tools for discovering, deploying, and managing apps. This may involve integration with app stores or internal app catalogs.
- **Example:** An EMM can distribute a secure email client, pre-configure it with the user's email account, and enforce policies that prevent saving attachments to personal storage.