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

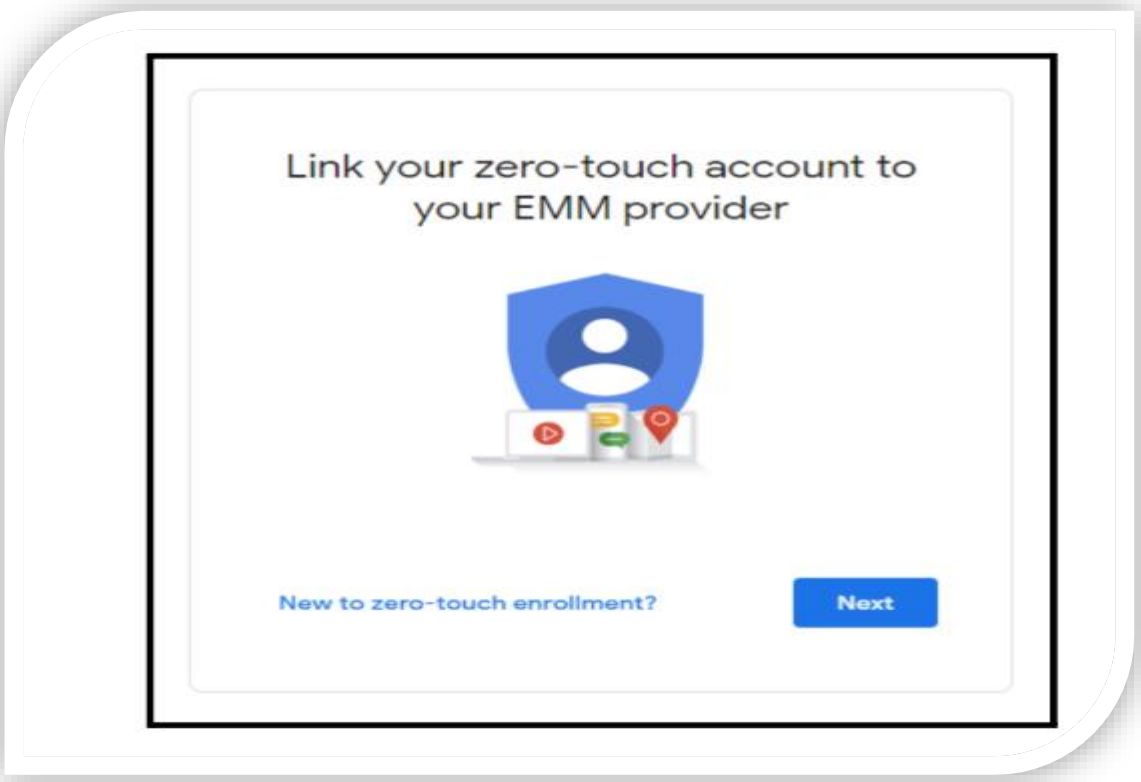
- *One time setup.*
- *Aids large-scale enterprise device rollout.*
- *Allows resellers to add devices to the portal, easing the enrollment process.*
- *Admins can set up the device with necessary apps and profiles and it gets applied automatically on device activation.*

Pre-requisites for Zero-touch

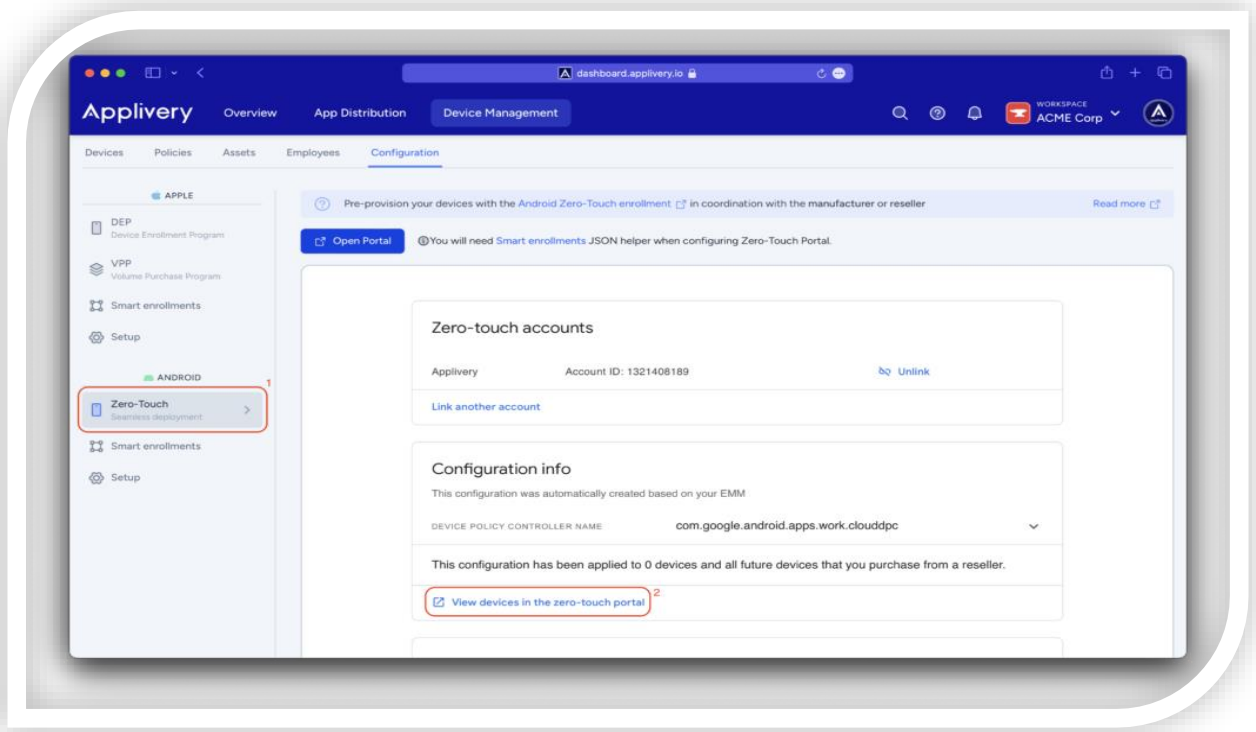
- *Android Zero-touch Enrollment is supported for devices running Android 9.0 or later, purchased from **specified reseller partners**.*
- *You need a Zero-touch portal account which can be obtained by contacting your reseller.*

Integrate Applivery with Zero-touch

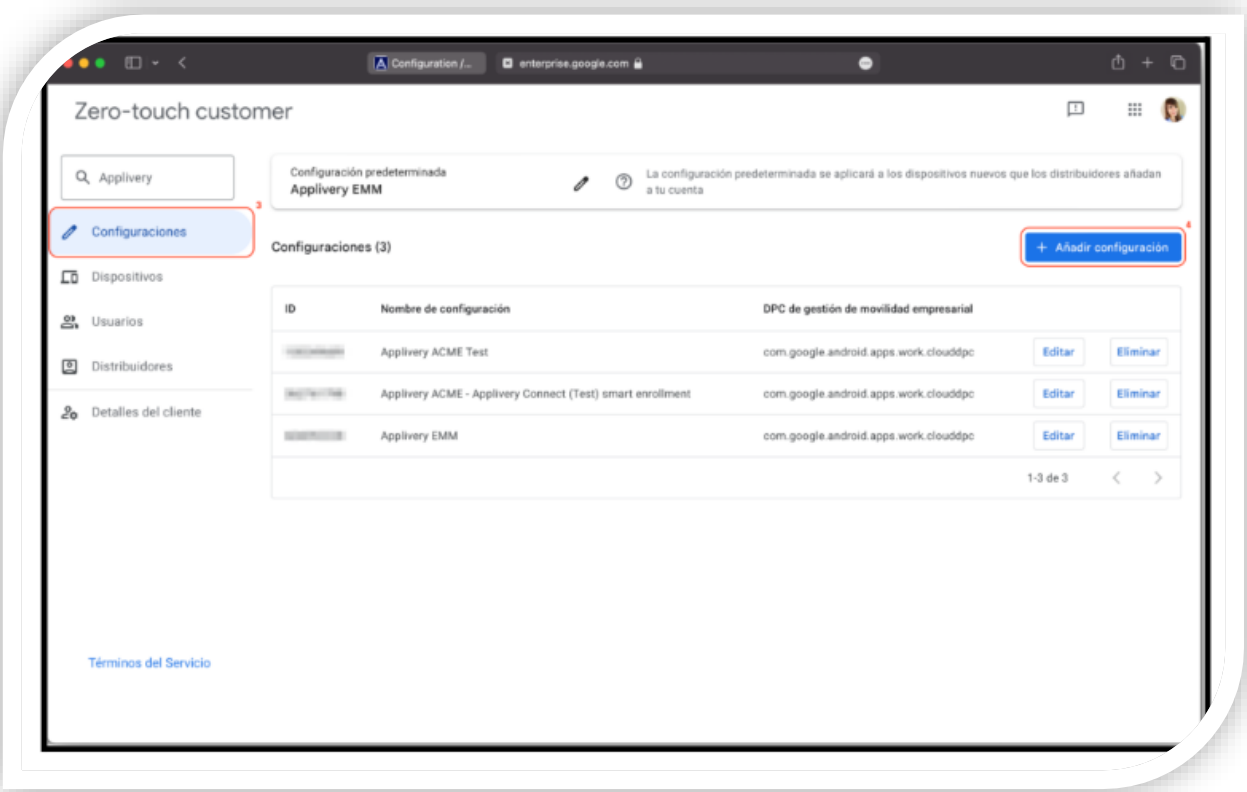
1. *Once in the **Applivery dashboard**, head to **Device Management > Configuration** and select the **Android Zero-Touch** section. You will need to link your Zero-touch to Applivery and follow the on-screen steps.*

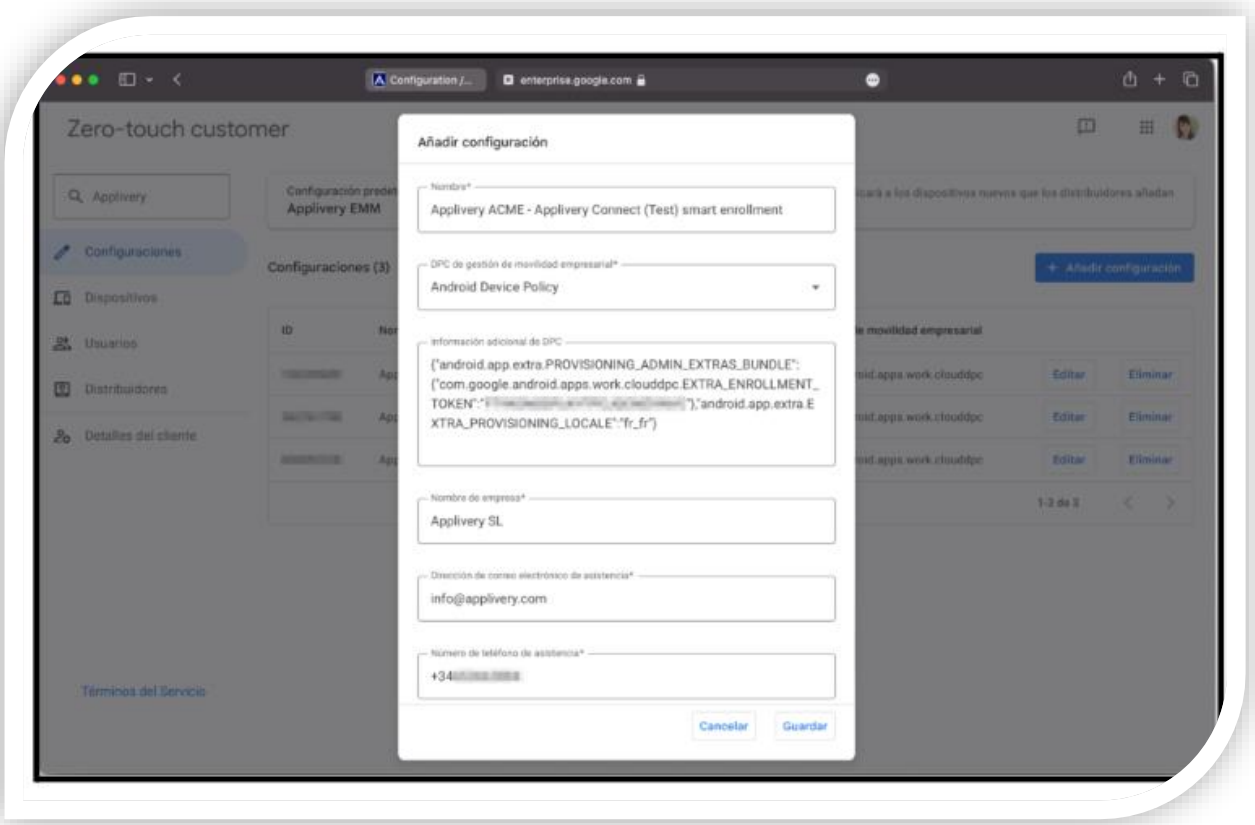


2. *Once the integration has been successfully completed, you just need to click on **View devices in the zero-touch portal**.*

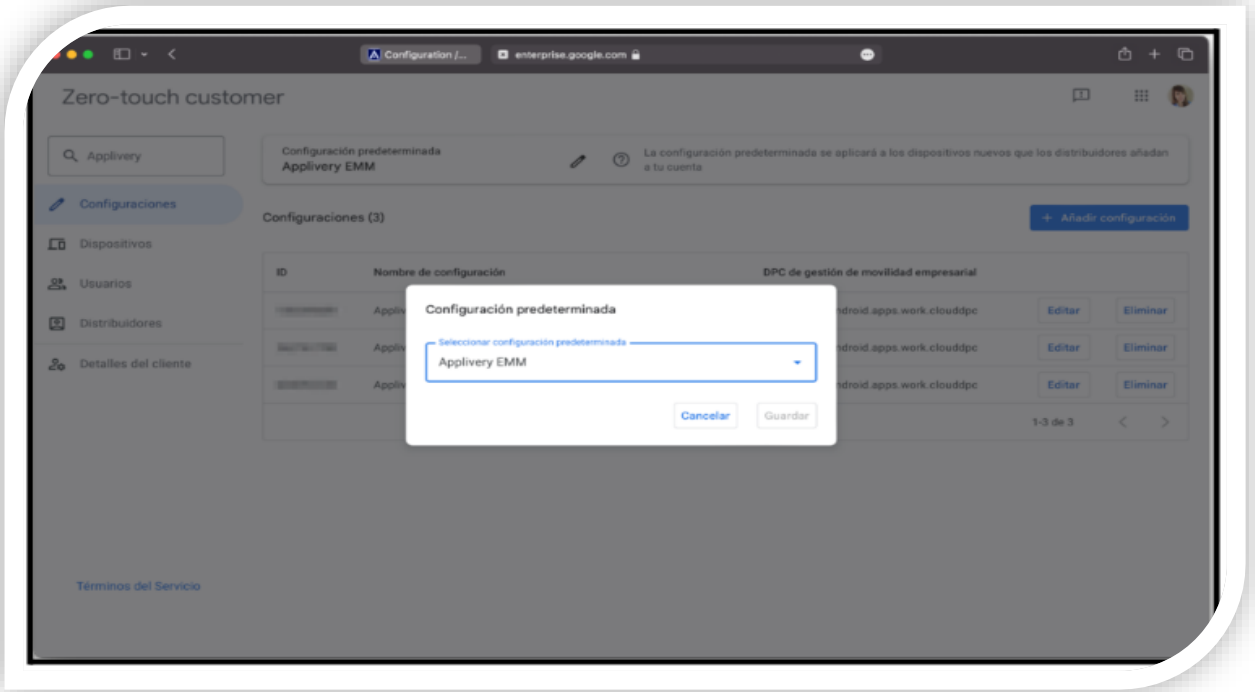


3. *A new window will open in your browser, where you will find the **Configurations** section.*
4. *You can add a new configuration by simply clicking the **+Add Configuration** button placed on the right side of the screen.*



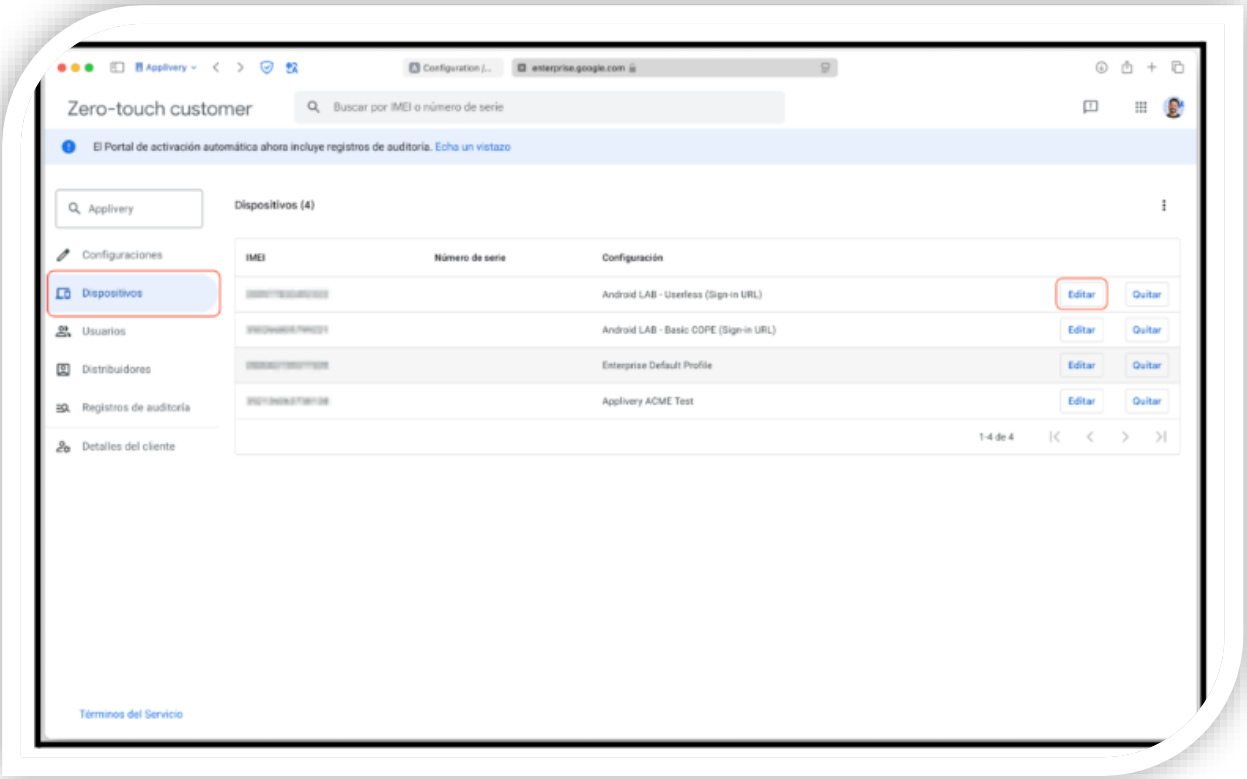


5. *The last step in the portal is to associate the created configuration with the devices. To do that, just select the configuration, which is to be automatically applied to the added devices and click the* ***Save*** *button.*

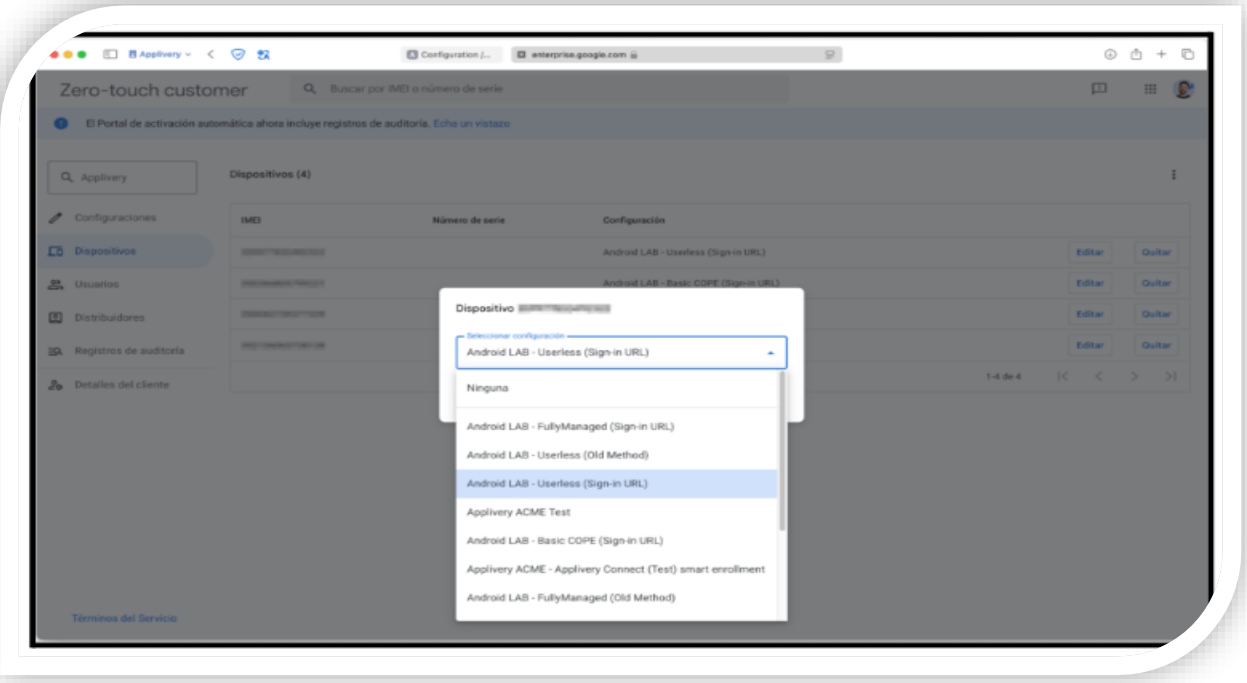


Adding the configuration to your devices

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.

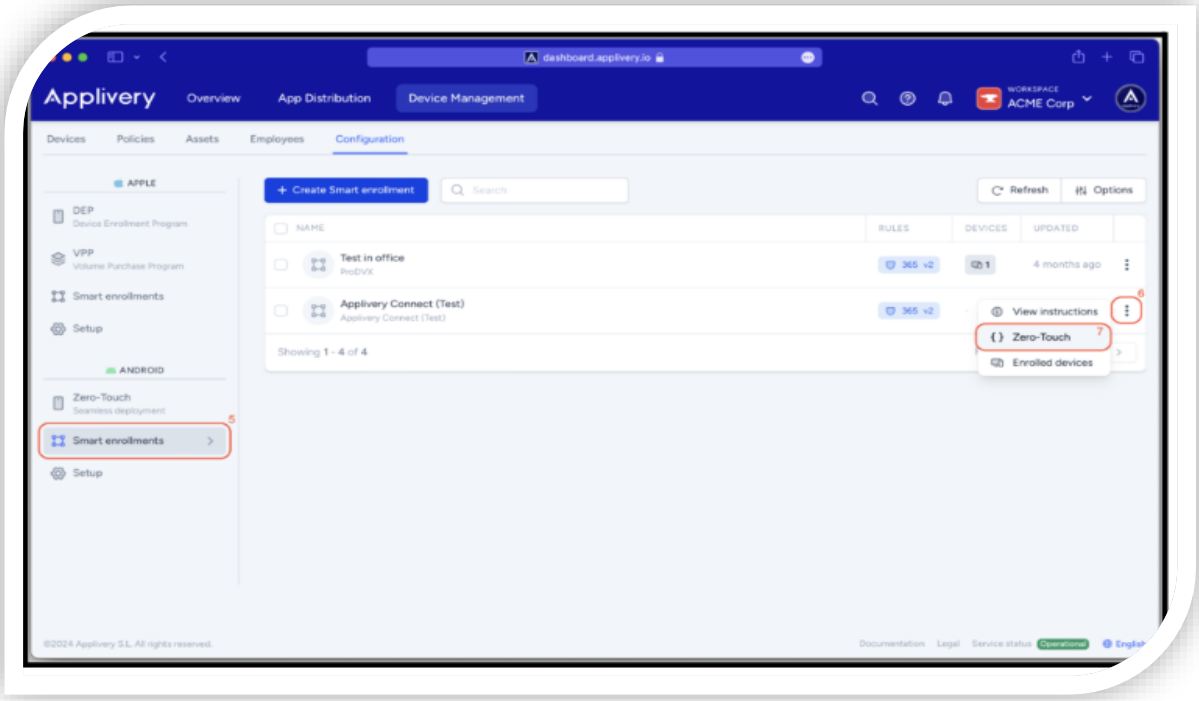


To assign a configuration, select **Edit** on the desired device. Then, choose the appropriate configuration from the drop-down menu.

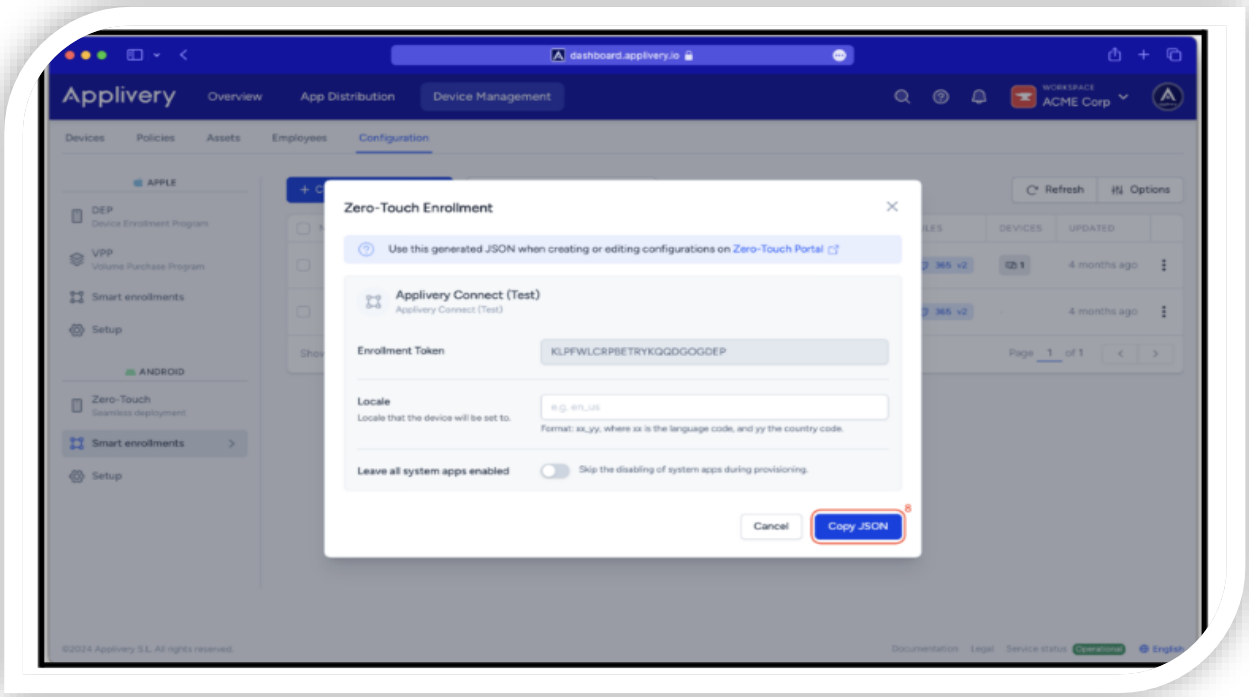


Obtain the JSON for the DCP extras field

1. *Once in the **Applivery dashboard**, navigate to **Device Management > Configuration** and select the **Android Smart enrollments** section.*
2. *Then, click on the vertical dots located at the end of the smart enrollment you wish to configure within the Zero-touch portal and select **Zero-Touch**.*

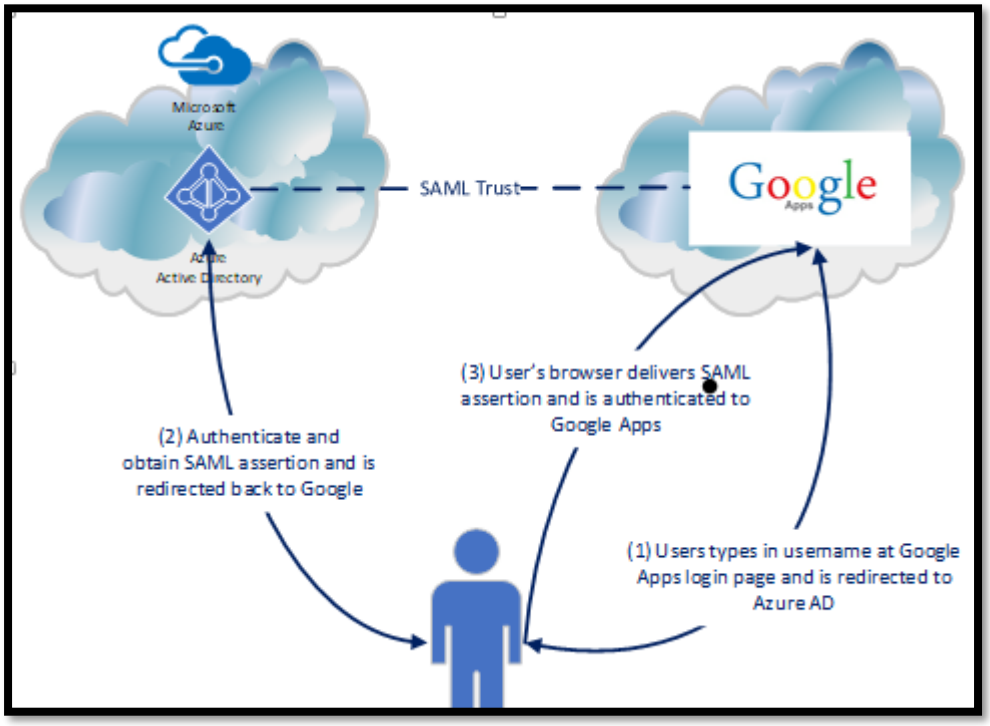


3. *A modal view will appear, allowing you to input additional configurations and copy the necessary JSON for the DPC extras.*



Integration with Azure AD/Google Workspace

Integrating an Enterprise Mobility Management (EMM) solution (like Intune or Google Workspace EMM) with Azure AD and Google Workspace enables centralized management of users, devices, and apps across both platforms. The integration involves:



Key Features:

1. *Single Sign-On (SSO): Users access resources with one set of credentials.*

2. *User Provisioning: Automates user account creation and sync between Azure AD and Google Workspace.*

3. *Device Management: Enforces policies and manages enrolled devices.*

4. *App Management: Controls app access via Azure AD and Google Play.*

Common integration Scenarios:

- ***Microsoft Intune with Google Workspace:*** *Intune manages Android devices via Google Play, and integrates with Azure AD for SSO.*

- ***Google Workspace as the primary identity provider:*** *Google Workspace may act as the identity provider for Azure AD access.*

Integration Steps:

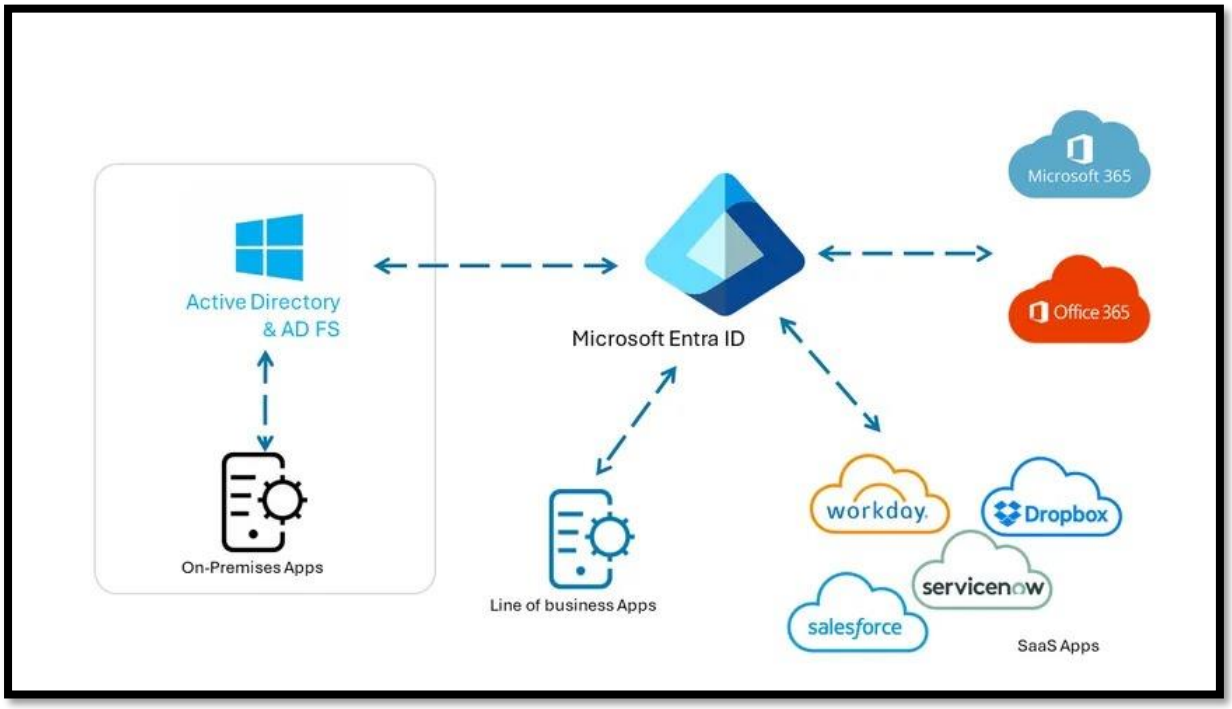
1. ***Choose an EMM solution:*** *Decide whether to use Microsoft Intune, Google Workspace's built-in EMM, or a third-party EMM solution.*
2. ***Configure SSO:*** *Set up SSO between Azure AD and Google Workspace, potentially using SAML or other protocols.*
3. ***Enable user provisioning:*** *Configure 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.*

Considerations:

- ***Choose the right EMM solution:*** *The best EMM solution depends on your specific needs and infrastructure.*
- ***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.*
- ***Consider security implications:*** *Ensure that your integration adheres to security best practices and that you have appropriate security measures in place.*



Administration Policy Configuration & 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.*

Relationship between Policy Configuration and Application Management:

- ***Integrated Approach:*** *EMM policy configuration and application management are closely linked. Policies often dictate how applications are managed and used.*
- ***Example:*** *A policy might restrict the use of specific apps to only managed devices, or enforce data loss prevention (DLP) policies on certain applications.*

Benefits: *By combining policy configuration and application management, EMMs provide a comprehensive solution for securing and controlling corporate data and resources on mobile devices.*