Integration with Azure AD / Google Workspace

Azure AD Integration

Azure Active Directory is a cloud-based identity and access management service by Microsoft.

�� Steps to Integrate:

1. **Join Windows Devices to Azure AD**
   - o Go to: Settings > Accounts > Access work or school
   - o Click **Connect** and provide Azure AD credentials.
2. **Automatic Enrollment with Intune**
   - o Azure Portal > **Devices > Enroll Devices**
   - o Configure **MDM auto-enrollment** for hybrid or Azure-only joined devices.
3. **Assign Roles and Groups**
   - o Portal > Azure AD > Groups
   - o Use dynamic or static device/user groups for role-based access.
4. **SSO (Single Sign-On) Configuration**
   - o Supports cloud apps like Salesforce, Zoom, Dropbox.
   - o Add apps in **Azure AD > Enterprise Applications**.

✅ Benefits

- · Centralized access control
- · Conditional access & MFA
- · Integrated app and device management via Intune

Google Workspace Integration

Google Workspace offers a cloud identity service similar to Azure AD.

⁄⁄ Steps to Integrate:

1. **Set up Google Workspace Admin Console**
   - admin.google.com > Devices > **Setup > Windows Device Management**
2. **Enable SAML-based SSO**
   - Security > Set up SSO with a third-party provider
   - Used for authenticating cloud applications
3. **Install Google Credential Provider for Windows (GCPW)**
   - Enables Windows sign-in using Google credentials
4. **Manage Apps using Chrome Enterprise Policies**
   - Policies set via Admin Console > Devices > Chrome > Apps & extensions

✅ Benefits

- · Centralized user control via Google accounts
- · Chromebook & browser-level policies
- · Application access and security enforcement

Administration Policy Configuration

Key Admin Policy Areas

⁄ Device Policies

· Password length, BitLocker enforcement, firewall rules

⁄ User Policies

· Login restrictions, session timeouts, multi-factor authentication (MFA)

Group Policies (for Windows via GPO or Intune):

- · Redirect Desktop/Documents to OneDrive
- · Disable Control Panel/Command Prompt
- · Set custom scripts (Logon/Startup)

🔒 Conditional Access Policies (Azure AD)

- · Block access if not on compliant device
- · Require MFA outside corporate network

🔒 Security Baselines

· Use Microsoft Intune's security baselines:

o Defender

o BitLocker

o Edge browser settings

Application Management

Application Deployment Tools

🔒🔒 Using Intune

1. Add App

o Intune > Apps > Add App (MSI, EXE, Win32 format)

2. Assign App

o Target specific device/user groups

3. Set Requirements

o OS version, free disk space, registry keys

4. Configure Detection Rules

o For uninstall or reinstall triggers

Using SCCM (ConfigMgr)

· Supports script-based, MSI, and EXE installs

· Use Application Model or Package Model

Using Google Admin Console

· Chrome Extensions/App deployment

· Android/iOS app control with managed Google Play

Common Use Cases

Task	Azure AD / Intune	Google Workspace
Auto-deploy Office 365	**Yes**	**Limited (via Chrome policies)**
Enforce BitLocker	**Yes (Security Baseline)**	**No**
Chromebook App Control	**N/A**	**Yes**
Sign-in with cloud ID	**Yes (Azure AD Join)**	**Yes (GCPW)**

Integrate Applivery with Zero-touch

What is Zero-touch Enrollment?

Android Zero-touch Enrollment (ZTE) is a feature by Google that helps companies set up and manage many Android devices at once. It is also called Zero-touch Provisioning (ZTP).

Zero-touch Enrollment is a method by Google to automatically set up company-owned Android devices in bulk—without manual steps.

Key Benefits:

- One-time setup by admin
- Ideal for large-scale deployment

- Resellers add devices to the portal
- Devices auto-configure on first power-on

How it works:

- Buy device from authorized reseller
- Reseller adds device to Zero-touch portal
- Admin assigns apps & settings
- User turns on device → setup auto-starts

1. Go to Applivery Dashboard

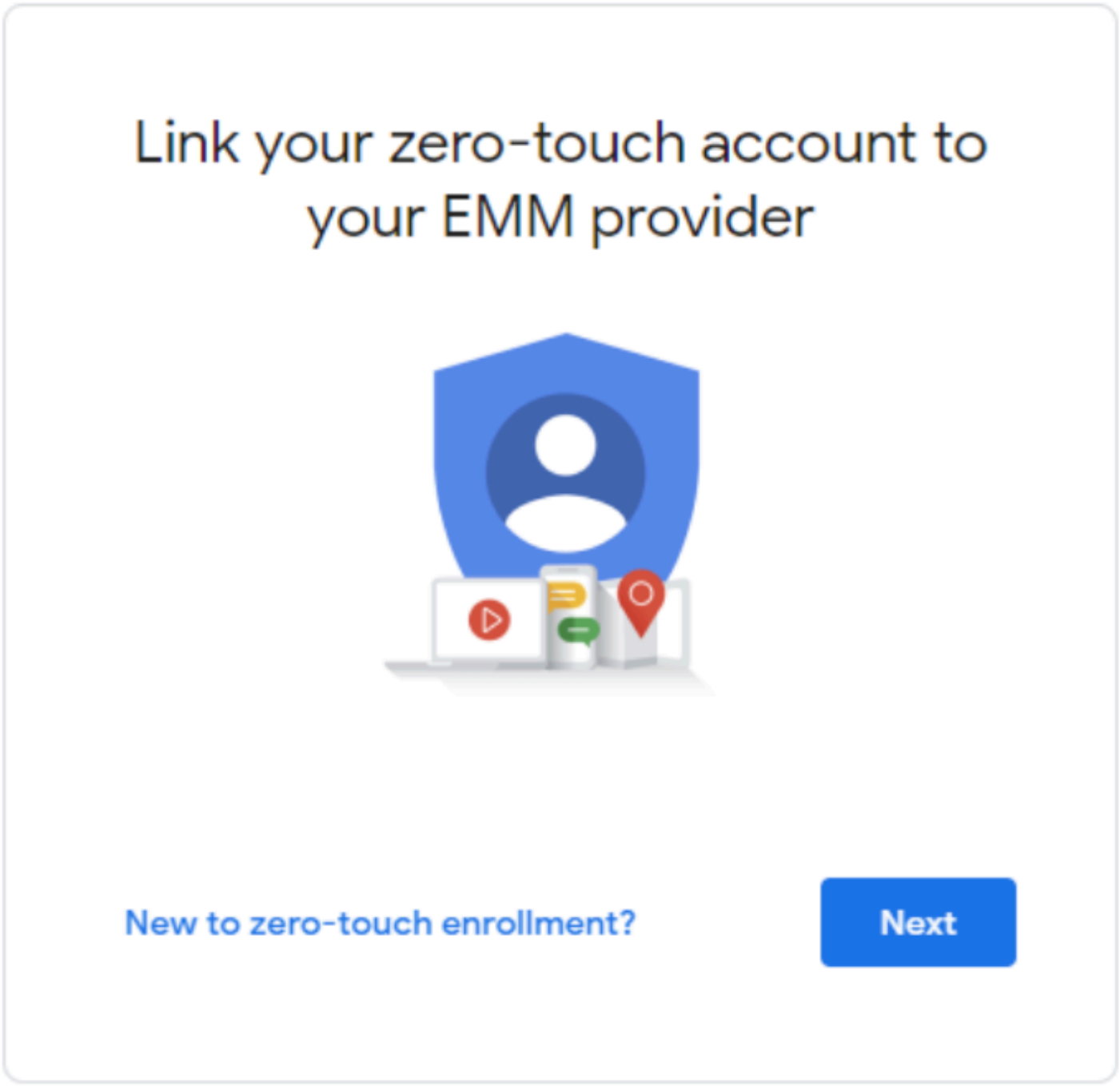
Navigate to:

Device Management > Configuration > Android Zero-touch

Link your Zero-touch account *to Applivery*

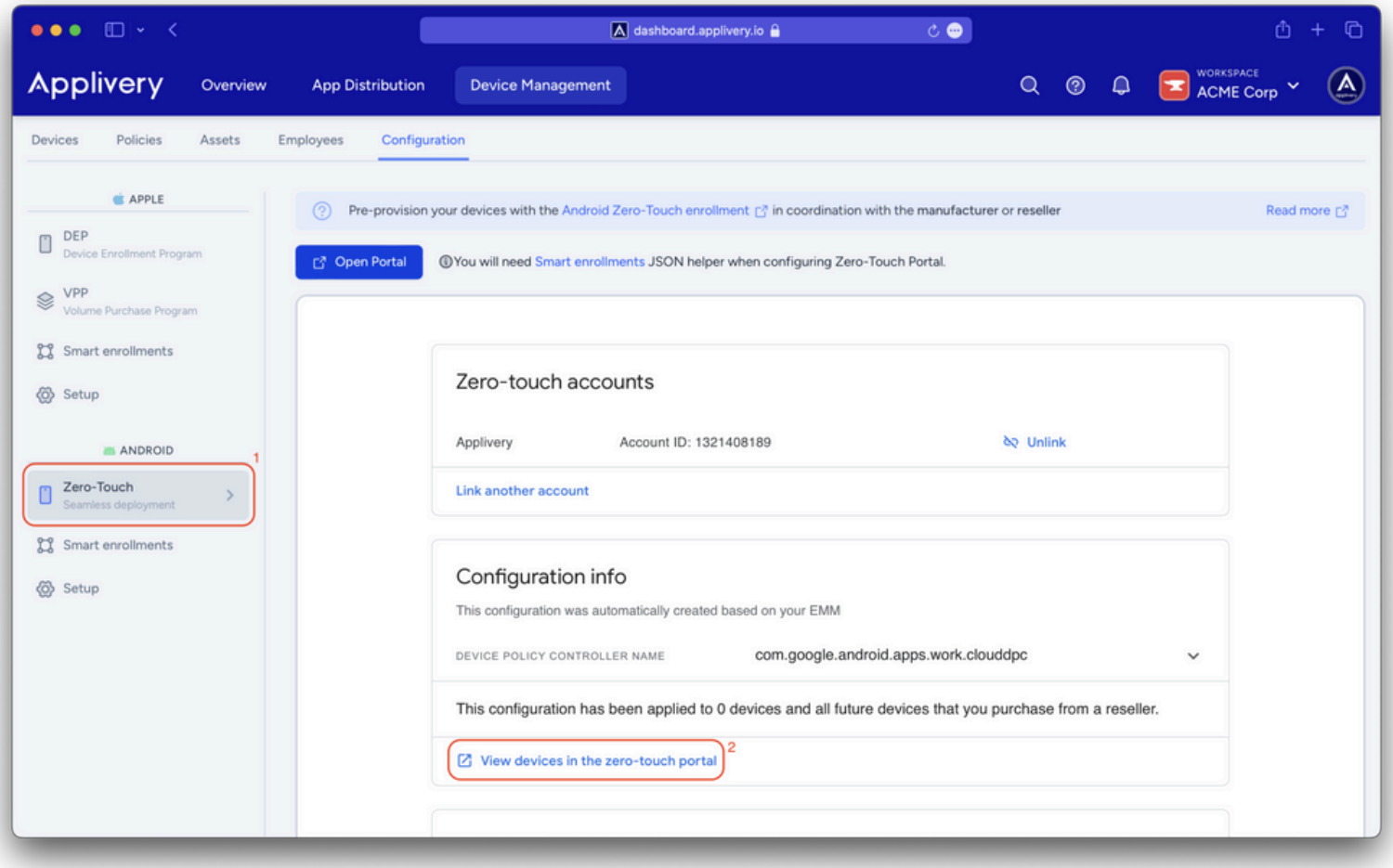
Follow the on-screen instructions to complete the setup

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



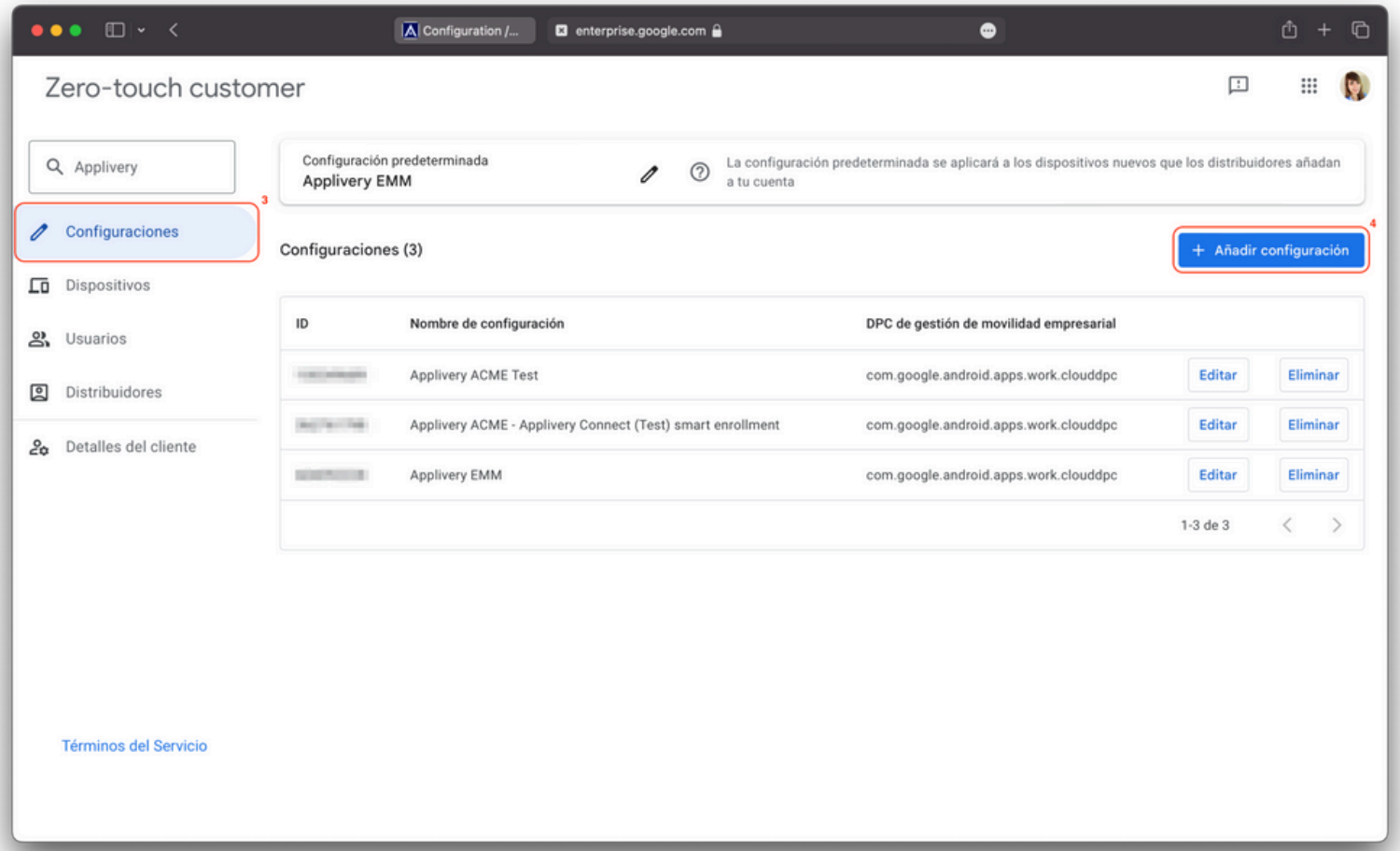
Once the integration has been successfully completed,

you just need to click on **View devices in the zero-touch portal**

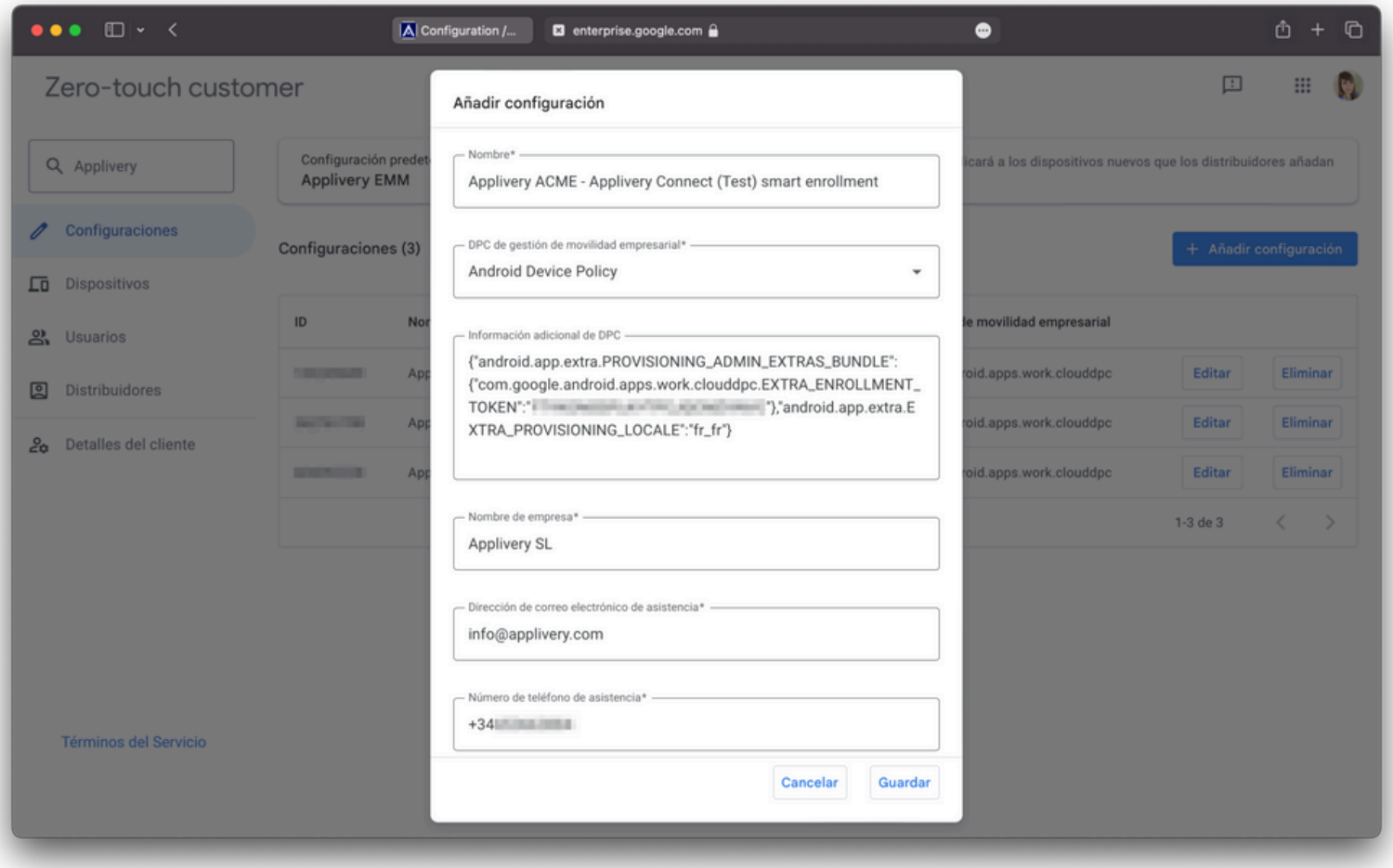


A new window will open in your browser, where you will find the **Configurations** section.

You can add a new configuration by simply clicking the + Add configuration button placed on the right side of the screen.

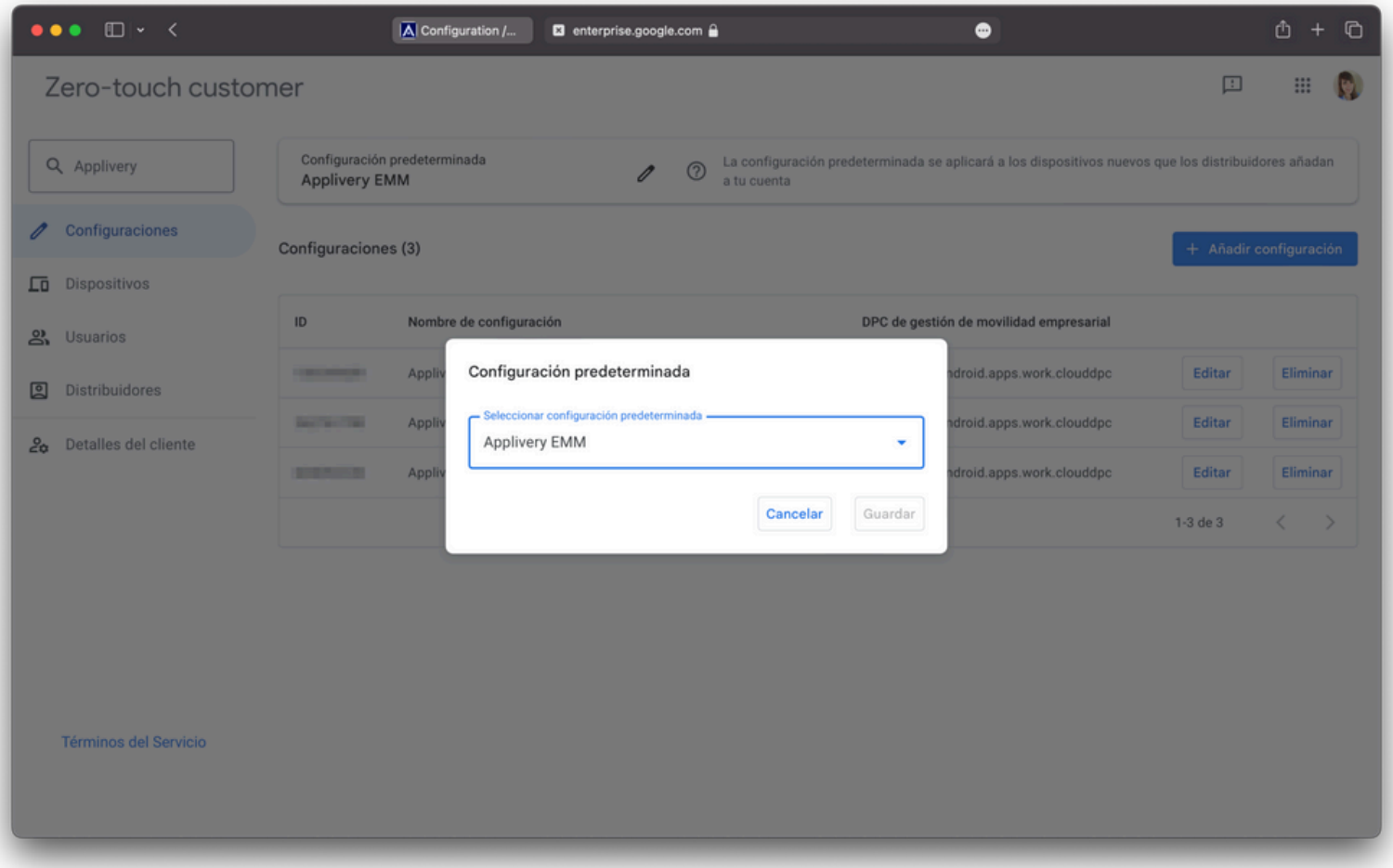


Note : **At this stage, you need to provide a name for the configuration and fill in the required fields. Pay close attention when selecting Android Device Policy in the corresponding DPC field. Additionally, you can learn how to obtain the JSON for the DPC extras field here.**



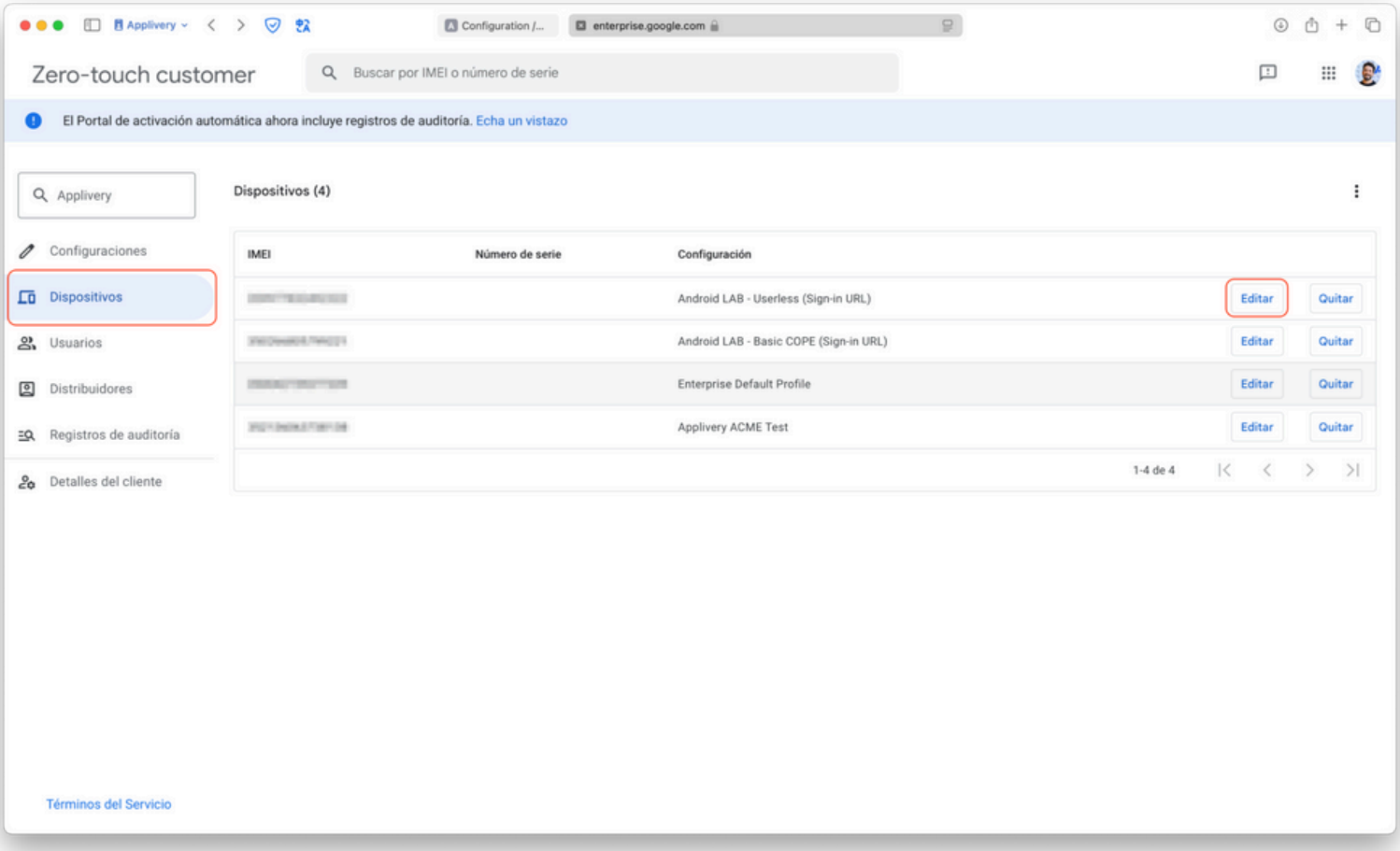
The last step in the portal is to associate the created configuration with the devices.

To do that, just select the configuration, which is to be automatically applied to the added devices and click the Save button.



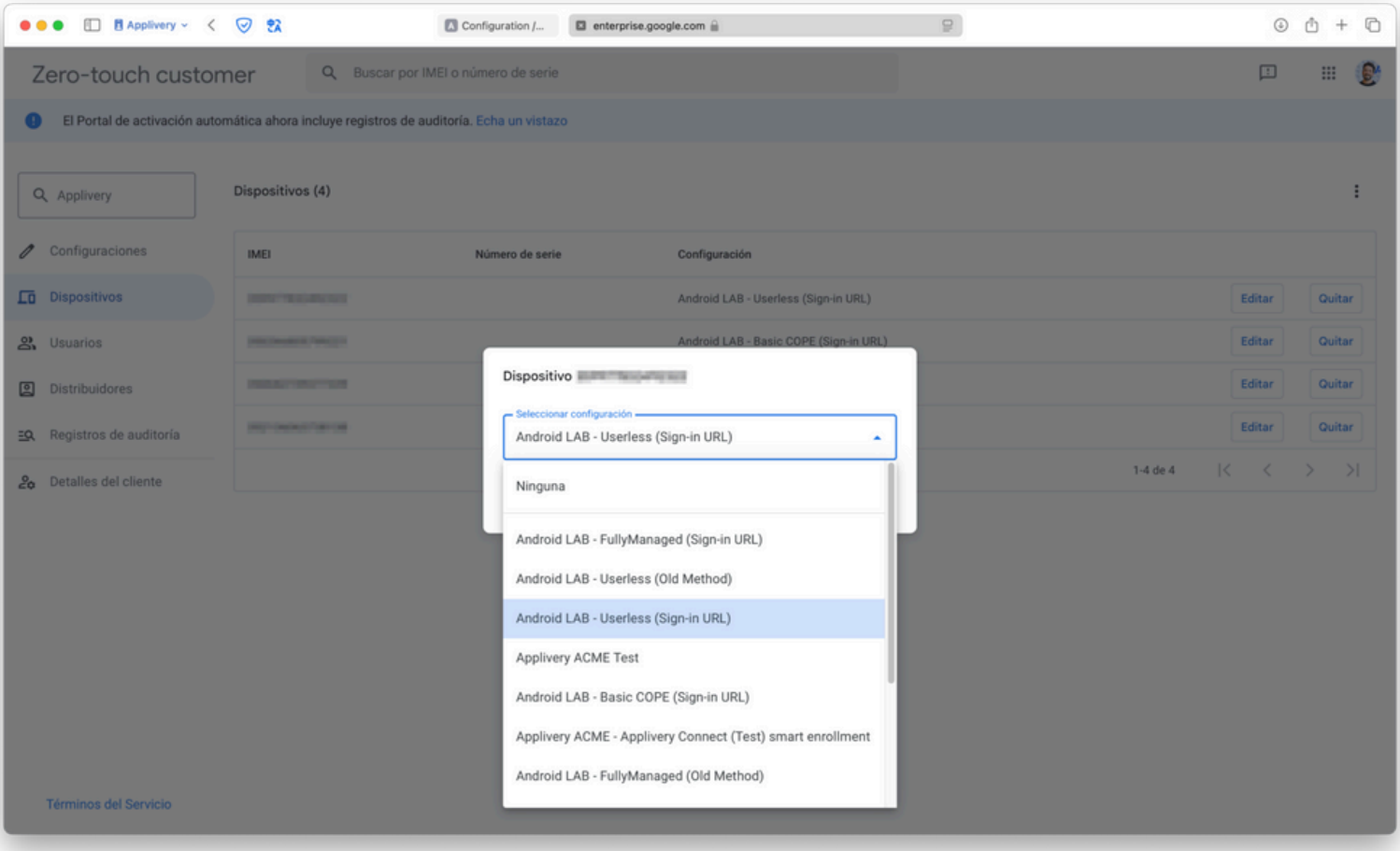
Adding the configuration to your devices

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.

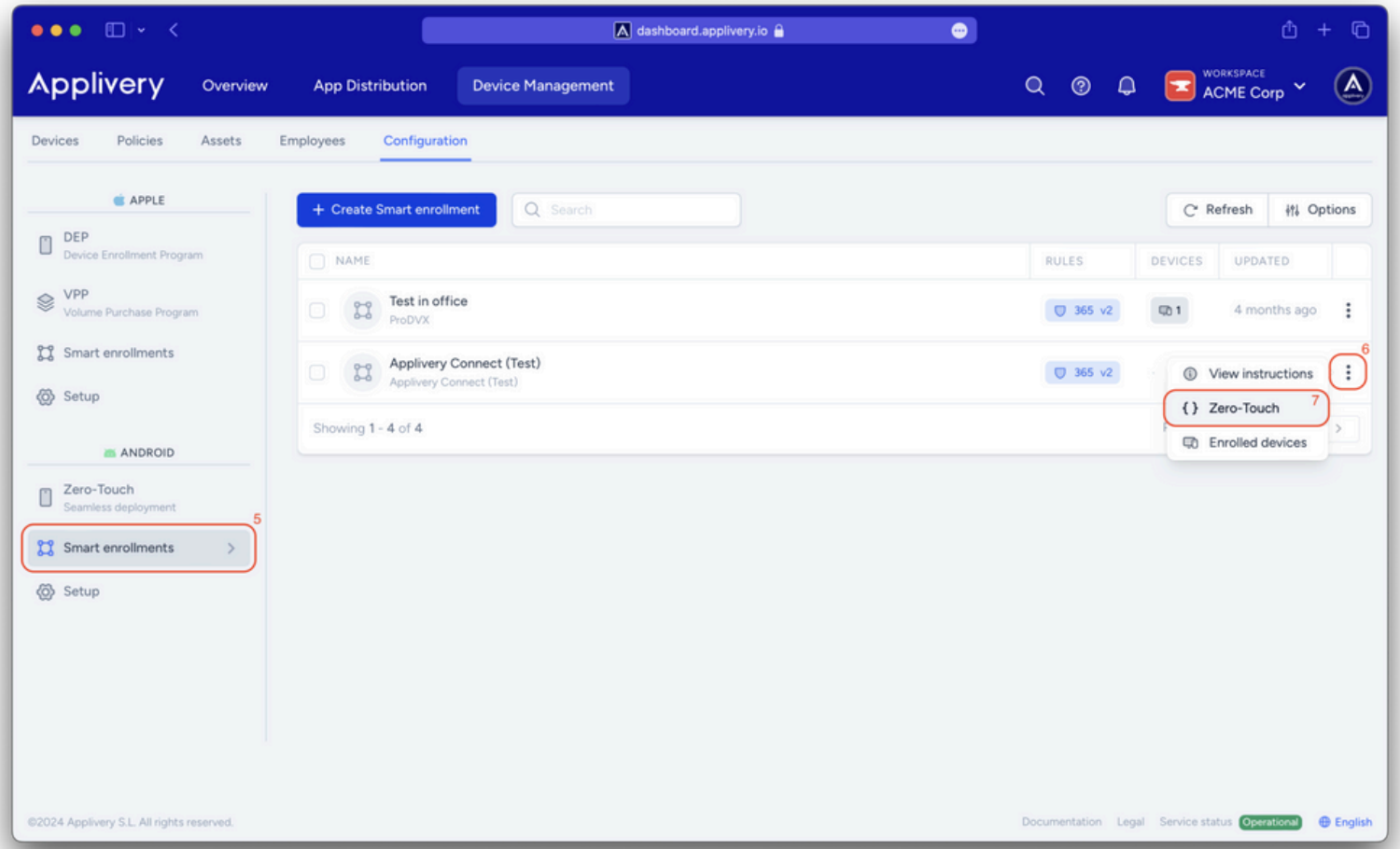


From this point on, the device will automatically enroll in Applivery after a factory reset, requiring no additional action.

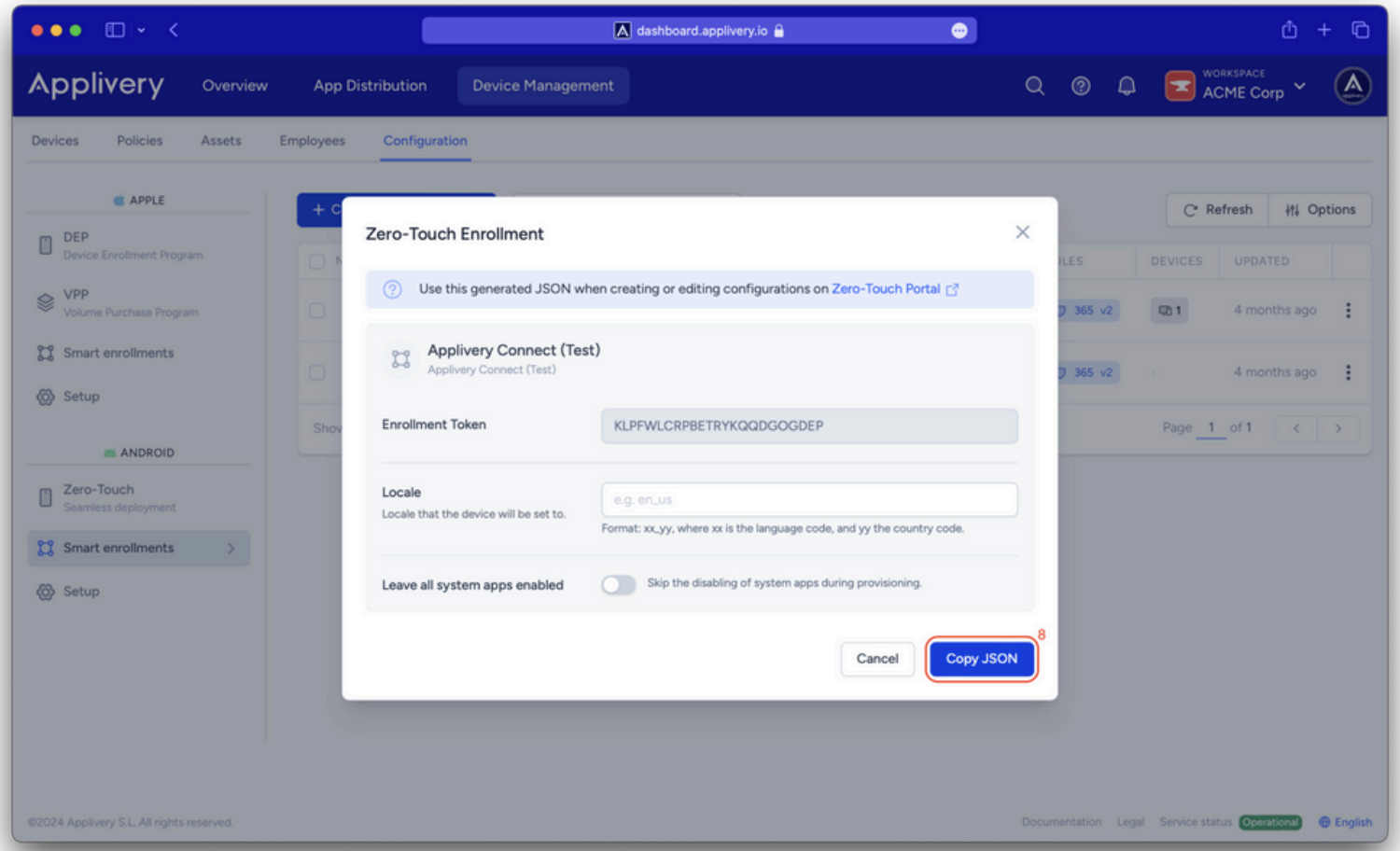
Obtain the JSON for the DCP extras field

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

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** .



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


dashboard.applivery.io
Applivery
Overview
App Distribution
Device Management
WORKSPACE
ACME Corp
Devices
Policies
Assets
Employees
Configuration
APPLE
DEP
Device Enrollment Program
VPP
Volume Purchase Program
Smart enrollments
Setup
ANDROID
Zero-Touch
Seamless deployment
Smart enrollments
Setup
Refresh
Options
DEVICES
UPDATED
4 months ago
4 months ago
Page 1 of 1
Zero-Touch Enrollment
Use this generated JSON when creating or editing configurations on Zero-Touch Portal
Applivery Connect (Test)
Applivery Connect (Test)
Enrollment Token
KLPFWLCRPBETRYKQQDGOGDEP
Locale
Locale that the device will be set to.
e.g. en_us
Format: xx_yy, where xx is the language code, and yy the country code.
Leave all system apps enabled
Skip the disabling of system apps during provisioning.
Cancel
Copy JSON
8
©2024 Applivery S.L. All rights reserved.
Documentation
Legal
Service status
Operational
English