

# Product Overview: AppConfig<sup>2</sup>

Last updated: 27.04.2025

## What is AppConfig<sup>2</sup>?

AppConfig<sup>2</sup> is a unified workspace for managing, configuring, testing, and securing Microsoft Entra™ ID applications.

It combines traditional app registration tasks with advanced tools for authentication flow testing, security risk analysis, claims customization, directory schema management, and configuration backup — all within a single streamlined interface.

Developers, IT administrators, security engineers, and L2/L3 support teams can streamline their work by eliminating the guesswork and manual scripting typically associated with application management.

 **Live Demo & More Info:** [appconfig.app](https://appconfig.app)

---

## Why Use AppConfig<sup>2</sup>?

- **Unified Management Experience** – Navigate applications, tools, actions, and documentation from a clean Sidebar layout. Configure and troubleshoot apps with minimal friction.
- **Enhanced Security & Compliance** – Detect risky permission grants, validate claims mapping policies, and manage app-specific schema extensions directly.
- **Streamlined Troubleshooting** – Test and debug **OIDC, OAuth, SAML** flows in real time. Inspect tokens, decode assertions, and track authentication steps through integrated **flow testers**.
- **Data-Driven Insights** – Use the **integrated Graph Explorer** to query and manage Entra ID objects on the fly, from listing users and groups to editing application settings.
- **Flexible Customization** - Edit application manifests safely, manage claims and token settings, and assign custom app roles and permissions.

- **Data Protection & Recovery** – Save app settings locally using both **manual** and **silent** backups and revert quickly to known-good configurations when testing new changes.
- **Governance Support** – Implement and manage Claims Mapping Policies and Directory Schema Extensions without complex scripting or additional consoles

## Key Features

### Applications Management

- ✓ **Manage Redirect URIs** – Troubleshoot authorization issues by adding or removing URIs (for both SPA and Web platforms).
- ✓ **Application Role & API Permission Management** – Dynamically create or update app roles. Link them to your Entra ID applications and manage assignments. Add and remove delegated or application permissions. Grant admin consent for Microsoft Graph and custom APIs directly from the UI.
- ✓ **Provision Users and Assign App Roles** – Assign users to an app with the correct roles, remove users, and handle role-based access without leaving AppConfig<sup>2</sup>.
- ✓ **Owner Management** – Easily add or remove application owners. Resolve user details from Microsoft Graph in real time.
- ✓ **Customize Token Claims** – Modify optional and custom claims and test them right away. Validate how additional claims appear in ID tokens or access tokens.
- ✓ **“Authenticate As” & Impersonation** – Generate tokens as a “test user” directly in AppConfig<sup>2</sup>. Quickly verify how different roles or scopes affect the resulting tokens.

## Tools

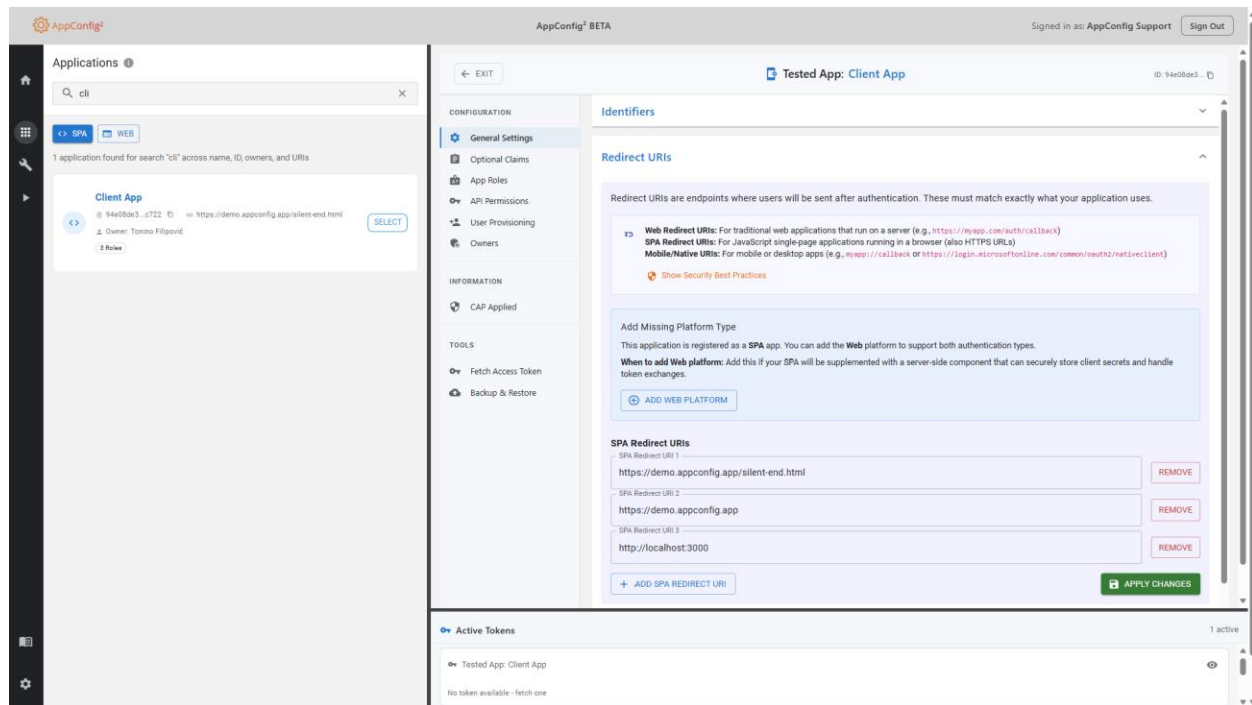
- ✓ **Auth Flow Tester** – Validate **OIDC/OAuth2** flows:
  - Authorization Code Flow
  - Implicit
  - Hybrid
  - Client Credentials
  - Device Code (mock flow)
- ✓ **SAML Tester** – Capture and decode SAML assertions from SP-initiated flows.
- ✓ **JWT Token Decoder** – Inspect OIDC/OAuth2 (JWT) tokens in real time.
- ✓ **Graph Explorer** – Send GET, POST, PATCH, or DELETE requests to the Microsoft Graph API to retrieve or modify Entra ID objects.
- ✓ **Manifest Editor** – Edit, validate, and safely update app manifests.
- ✓ **Schema Extensions Tool** – View, create, and manage directory extension attributes.
- ✓ **Permission Analyzer** – Detect high-risk permissions and calculate app-specific security scores.
- ✓ **Claims Mapping Policy Tool** – Create, edit, and assign claims mapping policies to service principals in a guided way, without complex Powershell or Graph syntax

## Actions

- ✓ **Register & Modify Applications** – Easily spin up new Entra ID app registrations or update existing ones. Manage sign-in audiences, branding, and supported account types.
- ✓ **Backup & Restore Configurations** – Perform manual backups to JSON, plus **silent local backups** stored in your browser. Revert to a previous version of the app registration in one click.

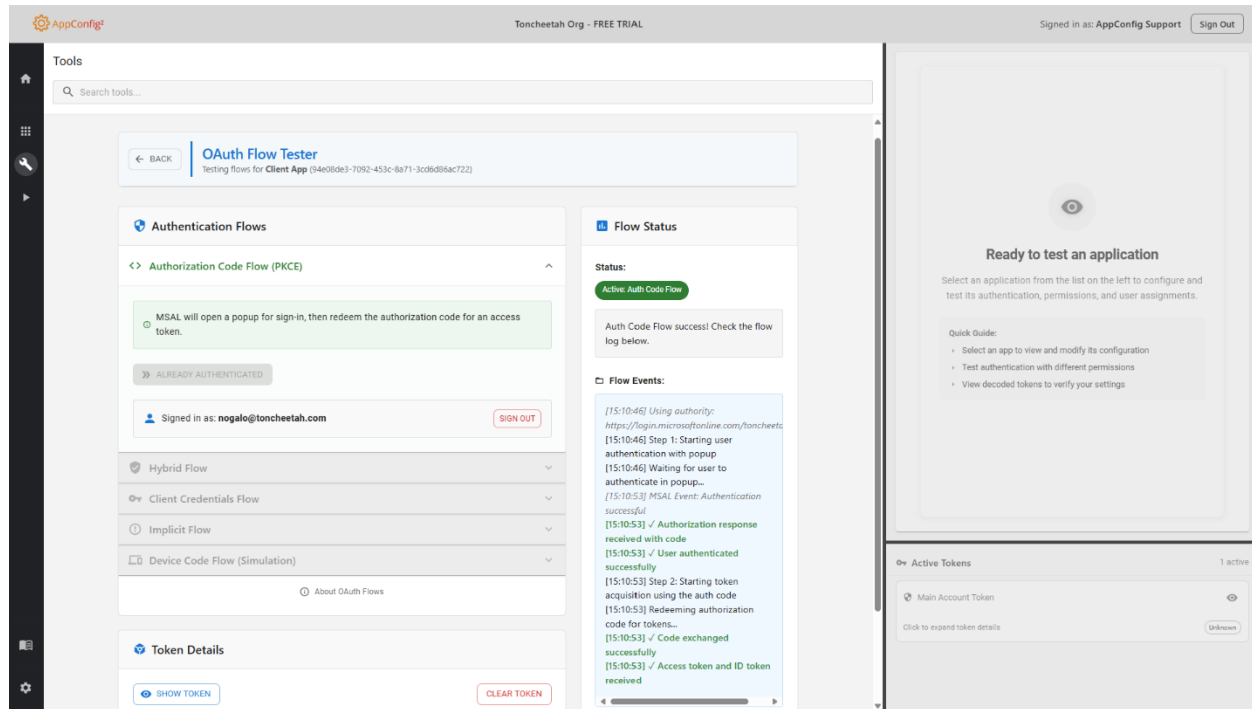
## Split Panel Workspace

- ✓ Manage apps and tools side-by-side with testing and decoded token panels.
- ✓ Control visibility of panels (App Content, App Tester, Token Viewer) for a customizable workflow.





## How It Works


1. **Sign in** using your Microsoft Entra ID administrator account (with the relevant permissions).
2. **Browse Applications** – Filter by type (SPA or Web) or search by app name, appld, owner or RedirectURI. Click on an application to open its details.
3. **Modify & Test Configurations** – Update redirect URIs, add or remove custom claims, configure roles, and assign users. Use the **Auth Flow Tester** to validate sign-in OIDC/OAuth flows or the integrated **SAML Tester** for SAML flows.
4. **Analyze Tokens & Grant Consent** – Decode access tokens and validate authentication responses. Review or change delegated and application permissions.
5. **Restore & Secure** – Capture a **silent** or **manual** backup prior to major changes. Restore from local files or revert to a stored backup if needed.





## Who Should Use AppConfig<sup>2</sup>?

 **Developers** – Debug authentication flows, test custom claims, and iterate on app registration settings without repeated visits to the Azure portal.

 **Security Engineers** – Confirm compliance with best practices, check for missing admin consents, and review assigned roles or user access.

 **IT Administrators** – Handle day-to-day Entra ID application management, user provisioning, and platform configuration in one place.

 **L3 Support Teams** – Diagnose and resolve login, token, or permission issues efficiently—no specialized scripts required.

 *AppConfig<sup>2</sup> is built for professionals managing identity and authentication systems within Microsoft Entra ID environments.*

## Try AppConfig<sup>2</sup> Today!

1. **Live Demo:** See it in action at [appconfig.app](https://appconfig.app).

2. **Contact Us:** For enterprise pricing or integrations, reach us at [support@appconfig.app](mailto:support@appconfig.app).
3. **Get Started:** Onboard your Entra ID environment and start configuring, testing, and securing your apps with ease!

---

© 2025 AppConfig<sup>2</sup>. All rights reserved.

*Microsoft Entra <sup>TM</sup> ID and Azure AD are trademarks of Microsoft Corporation.*