AppConfig²

Product Overview: AppConfig

What is AppConfig?

AppConfig is the flagship product of the **AppConfig²** suite—a comprehensive SaaS platform for managing, configuring, testing, and securing Microsoft Entra ID applications that significantly reduces the need for multiple external tools.

It eliminates the dependency on combinations of Wireshark, Fiddler, Postman, Graph Explorer, token decoders, and PowerShell scripts by bringing essential functionality into one streamlined interface.

It combines traditional app registration tasks with advanced tools for authentication flow testing, claims customization, directory schema management, security risk analysis, and configuration backup — all through a consistent, Azure-aligned experience.

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, reducing time-to-value for Entra ID application deployments.

🔗 **Live Demo & More Info**: https://www.appconfig.eu

Why Use AppConfig?

- **Unified Management Experience** – Navigate applications, tools, actions, and documentation from a clean Sidebar layout that follows Azure design patterns. Configure and troubleshoot applications without switching between Entra portal, Graph Explorer, token decoders, and Postman collections.

- **Token & Claims Customization** – Modify both optional claims and claims mapping policies with visual previews of the resulting tokens. Test token customizations immediately without needing separate JWT debugging tools or complex authentication scripts.

- **Enhanced Security & Compliance** – Detect risky permission grants, validate claims mapping policies, and manage app-specific schema extensions directly, replacing manual security audits with integrated insights previously requiring specialized security tools.

- **Streamlined Troubleshooting** – Test and debug OIDC and OAuth flows in real-time without requiring Fiddler or Wireshark. Inspect tokens, decode assertions, and track authentication steps through integrated flow testers that provide immediate feedback without context switching.

- **Data-Driven Insights** – Use the embedded Graph Explorer functionality to query and manage Entra ID objects on the fly, from listing users and groups to editing application settings without writing complex custom PowerShell scripts.

- **Directory Schema Extensibility** – Create, manage and query directory schema extensions directly through an intuitive interface, eliminating the need for Graph API scripts while providing visibility into extension attributes across your tenant.

- **Data Protection & Recovery** – Save application settings locally using both manual and silent backups and revert quickly to known-good configurations when testing changes, providing functionality missing from the native Azure portal.

- **Governance Support** – Implement and manage Claims Mapping Policies and Directory Schema Extensions with a visual interface rather than complex JSON editing, ensuring consistent application of governance standards across your environment.

- **Application Lifecycle Management** – AppConfig includes tools for creating new applications, deleting existing ones, and restoring accidentally deleted apps, thus simplifying end-to-end management of application lifecycle.

By bringing together functionality that previously required multiple specialized tools, AppConfig delivers a more efficient, secure, and comprehensive application management experience that complements and extends the native capabilities of Microsoft Entra ID.

Key Features

Applications Management

✅ **Manage Redirect URIs** – Troubleshoot authentication flows by adding, editing or removing Redirect URIs across multiple platforms (Web, SPA). Easily add missing platform types to existing applications.

✅ **App Roles & API Permission Management** – Dynamically create, update, and manage app roles with fine-grained control. Assign roles to users and service principals. Add, remove, and consent to delegated or application permissions for Microsoft Graph and custom APIs directly from the UI.

✅ **Expose API Capabilities** – Configure custom APIs with defined permission scopes that other applications can request. Manage Application ID URIs, scope definitions, and user/admin consent requirements through an intuitive interface.

✅ **Provision Users and Assign App Roles** – Streamlined user provisioning workflow to assign users to applications with specific roles. Support for bulk user imports, real-time user lookup from Microsoft Entra ID, role assignments, and user deprovisioning without leaving the application.

✅ **Owner Management** – Easily add or remove application owners and manage administrative access to application registrations.

✅ **Customize Token Claims** – Configure both optional claims and claims mapping policies to customize tokens. Preview how custom claims appear in ID and access tokens, with support for all standard claim types.

✅ **Conditional Access Policy Insights** – View and understand which Conditional Access Policies apply to your applications. Analyze security requirements including MFA, device compliance, and location-based restrictions.

✅ **Test Authentication & Token Testing** – Generate tokens as "test users" directly within the application. Verify how different roles, scopes, and claims affect the resulting tokens with detailed token inspection.

✅ **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.

✅ **Schema Customization** – Define and manage application schemas with support for custom attributes. Integrate with Directory Extensions and Claims Mapping for complete identity customization.

Tools

✅ **Auth Flow Tester** – Validate **OIDC/OAuth2** flows:

- Authorization Code Flow
- Implicit Flow
- Hybrid Flow
- Client Credentials Flow
- Device Code (mock flow)

✅ **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.

✅ **Directory Extensions Management** – Create and manage custom extension attributes for Entra ID objects. Discover existing extensions, including those synchronized from Entra Connect, and apply them to users and applications.

✅ **Security Analyzer** – Comprehensive security analysis including permissions, configurations, and security posture assessment.

✅ **Attack Surface Analyzer** - Advanced attack surface analysis from an adversary's perspective. Identify potential attack vectors, vulnerabilities, and exposure points in Entra ID applications.

✅ **Claims Mapping Policy Tool** – Create, edit, and assign claims mapping policies to service principals in a guided way, without complex Powershell or Graph syntax
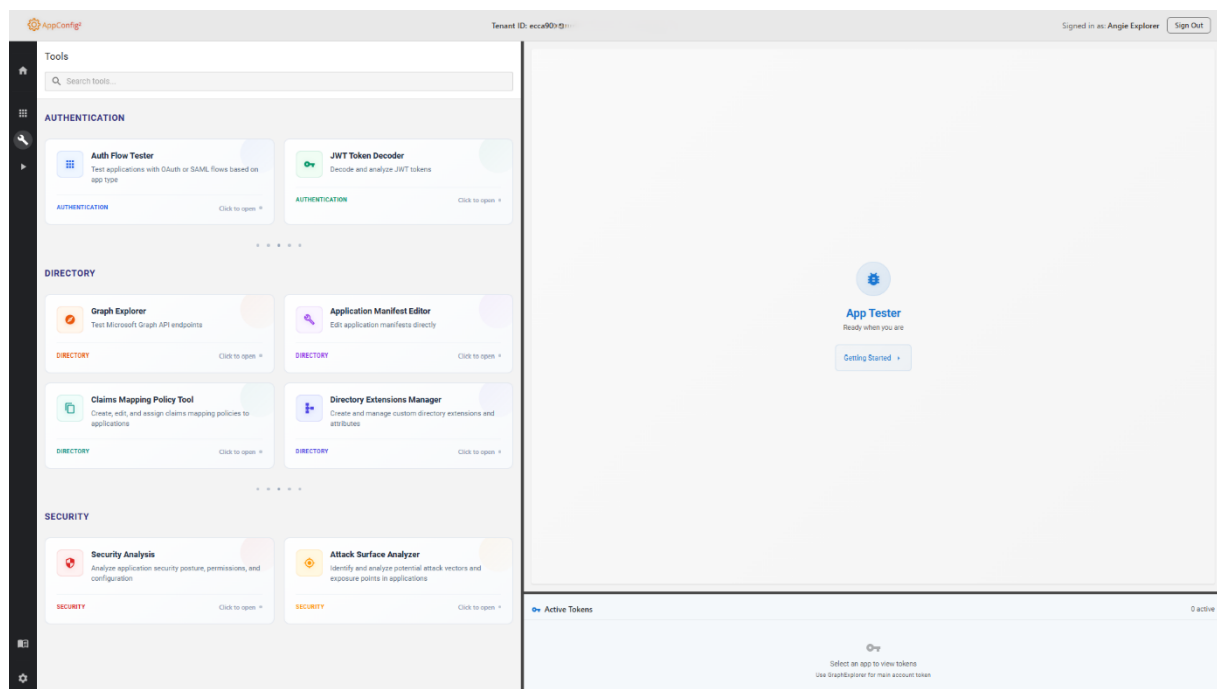
Actions

✅ **Register & Modify Applications** – Easily spin up new Entra ID app registrations or update existing ones. Manage sign-in audiences, credentials, and supported account types.

✅ **Delete Application** - Permanently removes an application registration from Entra ID with comprehensive safety measures.

✅ **Restore Deleted Applications** - Restores accidentally deleted applications within 30 days or permanently clean up expired deletions

✅ **Backup & Restore** – Comprehensively back up all applications in your tenant.

✅ **View Application Lifecycle** - Track and visualize applications' lifecycle from creation to retirement.
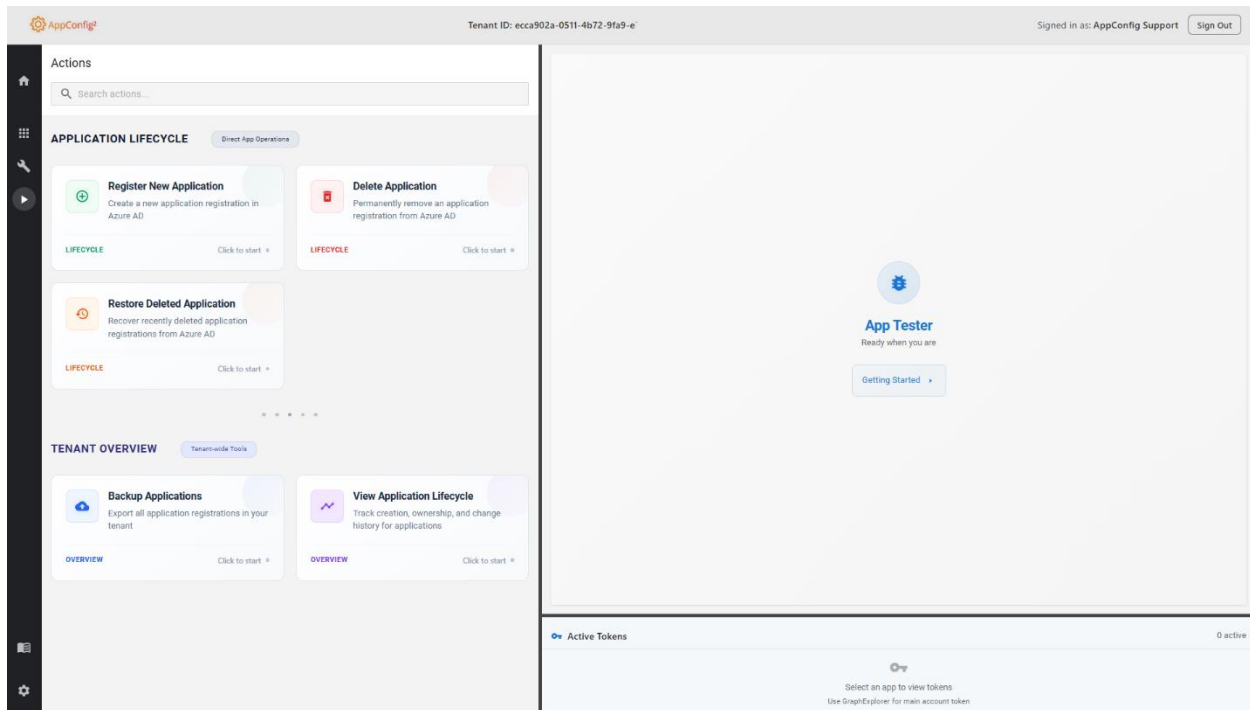
Split Panel Workspace

✅ 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, appId, owner, redirect URI or tenant type. 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.
4. **Analyze Tokens & Grant Consent** – Decode access tokens and validate authentication responses. Review or change delegated and application permissions.
5. **Restore & Secure** – Capture a backup prior to major changes. Restore from local files or revert to a stored backup if needed.

Who Should Use AppConfig²?

👨‍💻 **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 is built for professionals managing identity and authentication systems within Microsoft Entra ID environments.*

Appendix: Architecture Overview

AppConfig is built as a modern, cloud-native SaaS solution leveraging Microsoft Azure's enterprise-grade infrastructure. The architecture is designed for scalability, security, and performance while providing intuitive user experience.

Core Architecture Principles

✅ Serverless-First: Built on Azure Static Web Apps and Azure Functions for automatic scaling

✅ Microsoft-Native: Deep integration with Microsoft Graph API and Entra ID

✅ Enterprise-Ready: Designed for multi-tenant usage with enterprise security standards

✅ Global Performance: Worldwide content delivery through Azure CDN

Technology Stack

➢ **Frontend**: React with TypeScript, hosted on Azure Static Web Apps

➢ **Backend**: Node.js Azure Functions providing serverless API endpoints

➢ **Authentication/Authorization**: Entra ID OAuth 2.0/OIDC

➢ **APIs**: Direct Microsoft Graph API integration for app registration management

➢ **Distribution**: Global CDN for worldwide performance optimization

Key Architectural Benefits

Real-Time Performance

- Direct Microsoft Graph API integration eliminates backend proxy latency

- Azure Static Web Apps provide instant global distribution

- Serverless functions scale automatically based on demand

Enterprise Security

- Native Entra ID authentication with multi-tenant support

- End-to-end HTTPS/TLS encryption for all communications

- Built on Microsoft's enterprise security standards and compliance frameworks

High Availability & Scalability

- 99.9% SLA through Azure infrastructure

- Automatic scaling from individual users to enterprise-wide deployments

- Global redundancy with automatic failover capabilities

Integration Capabilities

➢ Azure Marketplace: Seamless subscription management and billing

➢ Microsoft Graph: Full CRUD operations on Entra ID app registrations

➢ CI/CD Pipelines: API endpoints for automated configuration management

➢ Enterprise Tools: Integration-ready architecture for existing DevOps workflows

---