Identity and RBAC

Introduction

The CMS implements it's own authentication flows as well as leveraging federated authentication with both Microsoft and Google.

Authentication

- Supports CMS credentials and federated sign-in (e.g., Microsoft Entra).
- Tokens are validated for issuer, audience, lifetime, and signature.
- Federation settings control whether CMS login and/or Entra/Google login are allowed.

Authorization model

- Role-based access control with built-in roles aligned to the hierarchy.
- Access is scoped to the entity where the role is granted (platform, distributor, partner, tenant).

Supported Roles

- PlatformAdministrator / PlatformReader / PlatformService
- DistributorAdministrator / DistributorReader
- PartnerAdministrator / PartnerReader
- TenantAdministrator / TenantUser

Scope and inheritance

- Roles do not leap across unrelated branches. A Partner admin cannot see a Tenant owned by a different Partner.
- Platform roles supersede lower scopes for operations and support.

Audit and accountability

- All sensitive actions (pricing, commission, usage processing, role assignment) should be traceable to an authenticated identity.
- Logs and audit trails enable operational forensics and compliance reporting.

Federation controls (examples)

- Settings can enable/disable specific identity paths (e.g., allow Entra only). First
- First-login checks should enforce MFA requirements and password change where applicable.

Revision #3
Created 21 September 2025 11:03:12 by AutoBot
Updated 25 September 2025 03:52:16 by AutoBot