Concepts

- Identity and RBAC
- Multi-Tenant Commercial Model
- Pricing, SKUs and Meters
- Regions and Usage

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.

Multi-Tenant Commercial Model

Purpose

This page explains the CMS hierarchy and how ownership, visibility, and billing flow across Distributors, Partners, Tenants, and Subscriptions. It also clarifies the role of platform administrators.

Roles in the hierarchy

- Platform Administrators: Operate and configure the system. Own global settings, branding, pricing frameworks, commission frameworks, and region/usage processing.
- Distributors: Top commercial tier beneath the platform. Own one or more partners. See aggregate usage, billing, and
- commission outcomes across their partner network.
  Partners: Customer-facing organizations that onboard and manage tenants. Can inherit or define their own commission structures.
- Tenants: Consuming organizations (end customers or internal business units). Own subscriptions and users.
  Subscriptions: The unit of consumption and billing within a tenant. Usage, rating, and invoicing are calculated at this level.

Ownership and visibility

- Distributors can see all Partner, Tenant, and Subscription activity under their umbrella.
  Partners can see their Tenants and Subscriptions.
  Tenants can see only their own Subscriptions and users.
  Subscriptions are strictly tenant-scoped; they never cross tenants.
  All layers are visible to Platform Administrators for governance and support.

Delegation and access control

- Administration is delegated by layer. Distributors manage partners; partners manage tenants; tenants manage their own subscriptions and users.
- This reduces cross-team friction and aligns access with commercial responsibility.

Data boundaries

- Billing and usage roll up from Subscriptions to Tenants, then to Partners, and finally to Distributors.
- Commission calculation operates on these roll-ups; partner/distributor payouts are tied to actual consumption for the period.

Typical journeys

1. Service-provider sales: Distributor onboards a new Partner → Partner onboards a Tenant → Platform Admin (or Partner) creates a Subscription → Tenant users begin consuming services → Usage flows to billing → Commissions are calculated and attributed upstream.
2. Enterprise IT “internal reseller”: Central IT acts as Distributor; divisional IT acts as Partner; departments are Tenants; projects/business lines are Subscriptions.

Out of scope for this model

- Native Azure resource provider internals (Compute/Storage/Network specifics) are not modeled here. The CMS focuses on commercial hierarchy, delegation, usage processing, pricing, and billing.

Pricing, SKUs and Meters

Purpose

Defines how the CMS models chargeable items (SKUs), how prices are set (flat or tiered), how credits/discounts apply, and how this connects to commissions.

Core concepts

- SKU: A metered service or unit that can be priced (for example: VM vCPU-hour, managed disk GB-hour, static IP per hour).
- Price: The monetary rate attached to a SKU. Can be flat or tiered.
- Thresholds: Quantity breakpoints where a rate changes (tiered pricing).
- Adjustments: Bulk increases or decreases by percentage or absolute values, applied across selected SKUs.
- Credits and discounts: Monetary or quantity-based reductions that may apply at tenant, subscription, or resource scope.

Scoping and precedence

- Pricing selection and credits respect scope. In practice:
- Tenant-scoped pricing/credits override region defaults when configured.
- Subscription-scoped pricing/credits can further customize for a specific workload.
- Resource-level credits (when supported) apply last for fine-grained cases.

When no custom scope is present, region defaults are used.

Currency and FX

- Billing can run in a selected display currency.
- FX conversion applies at report time or during rating, depending on configuration.
- Historical FX rates should be preserved to ensure reproducibility of past invoices.

Operational guidance

- After changing prices or thresholds, re-rate affected periods or trigger targeted usage reprocessing, so billing reflects new prices where policy allows.
- Price comparison tools and cloning workflows help align price sheets across regions or offers.

Commission linkage

- Commission rates are defined at the Partner or Distributor level.
- Monthly billing aggregates by partner/distributor scope; commissions are calculated from those aggregates and stored for downstream reporting and payout.

Regions and Usage

Purpose

Explains how regions (stamps) are represented and how usage flows from collection to rating and billing, including offline scenarios.

Regions (stamps)

- A Region represents a source of usage.
- Each Region has the endpoints/credentials required for usage collection and health checks.
- Multiple Regions can be operated concurrently; billing can aggregate across regions.
- Offline and disconnected operations
- The CMS is designed to support disconnected environments.
- Usage and rating can proceed without continuous internet access when inputs are available.

Usage processing pipeline

1. Collection: Pull raw usage records for a Region and time range.
2. Mapping: Normalize and map records to Subscriptions and SKUs.
3. Aggregation: Group by resource/meter and billing period with quantity roll-ups.
4. Rating: Apply prices, thresholds, credits, and currency rules.
5. Output: Persist rated usage and expose summaries for invoicing, analytics, and commissions.