# 🔐 Access & System Control

## ✨ Module Overview

The **Access & System Control** module provides secure, granular permission management across the entire SaaS platform. It ensures that only authorized users can view or modify specific data, perform certain actions, or access designated sections of the platform. This module includes user roles, permission matrices, two-factor authentication, token scopes, feature toggles, and operational flags.

It is foundational to security, compliance, and operational isolation between tenants.

## 🔑 Key Features

### 1. 👤 Role-Based Access Control (RBAC)

* Define system roles: Superadmin, Brand Admin, Editor, Analyst, Support Agent, Reseller, etc.
* Create tenant-specific roles (e.g., “Marketing Head”)
* Assign permissions to:
  + Modules (e.g., Blog, Campaign, Inbox)
  + Actions (view, create, edit, delete, approve, publish)
  + Resource scopes (own, team, brand-wide)

**Tables:** - user\_roles - role\_permissions - role\_assignments

**Admin Panel:** /admin/access-roles

### 2. ✨ Feature Flags & Access Toggles

* Enable/disable modules per tenant
* Roll out new features via phased flags (Beta, Internal, GA)
* Hide UI sections if disabled
* Control usage of expensive modules (e.g., GPT, embeddings)

**Tables:** - feature\_flags - tenant\_feature\_overrides

**Admin Panel:** /admin/feature-control

### 3. 🚫 API Scope Control

* Limit API access by endpoint scope
* Define read-only vs write scopes
* Use OAuth token management for external integrations

**Tables:** - api\_tokens - token\_scopes

### 4. 🛋️ Operational Restrictions & Warnings

* Enforce action limits (e.g., max 10k emails per month)
* Auto-disable module if over quota
* Show warnings (e.g., nearing limit)
* Track excessive usage

**Tables:** - module\_usage\_limits - usage\_warnings

### 5. 🚪 Login & Access Security

* Multi-factor authentication (MFA) toggle per tenant
* Session logs (IP, device, timestamp)
* Login alerts (email)
* Rate-limit brute force attempts

**Tables:** - login\_attempts - active\_sessions - security\_policies

### 6. 📊 Access Audit & History

* Log every permission change
* Show who gave/revoked what access
* Track admin override history

**Tables:** - access\_logs - admin\_actions

### 7. 🔗 Integration Control

* Enable/disable 3rd party integrations per tenant
* OAuth token expiry monitor
* Reset access tokens manually

**Tables:** - integration\_status - oauth\_tokens

## ✅ Admin Panel Features

* Page: /admin/access
* Tabs:
  + [Roles]
  + [Permissions Matrix]
  + [Feature Flags]
  + [Integration Status]
  + [Access Logs]
* Per-role UI:
  + Role name + assigned users
  + Permissions toggles (CRUD)
  + Scope selectors (own/team/all)
  + Assign/unassign buttons
* Feature Flag Editor:
  + Toggle per module/feature
  + Notes per flag (e.g., beta reason)
  + Target tenants or all

## 🔧 Developer Notes

* Build as a reusable permission middleware (checkAccess(user, module, action))
* Use decorators or guards in APIs and frontend routes
* All modules must register their permission schema
* Implement fallback behavior if denied (redirect or hide UI)
* Use feature flags as config-based toggles in build pipeline

## ⚡ Use Cases

* Let “Editors” only publish blog posts but not touch campaigns
* Limit GPT usage for trial accounts
* Hide YouTube auto scripts unless on Pro plan
* Require MFA for enterprise brands
* Alert admin if unauthorized access attempts spike

## 🚀 Next Steps

* Connect this module to:
  + Superadmin Dashboard (overview)
  + Subscription Plan logic (module-level limits)
  + Usage Engine (warn if thresholds crossed)
  + Support System (permissions for agent)