

Synoria Base

系統分析與設計規格書

權限管理 (IAM)

文件名稱	系統分析與設計規格書_SynoriaBase_權限管理.docx	版本	V 1.0
設計	—	日期	2026-09-24
系統	Synoria Base (Go 1.26 + Rust + React 18)	狀態	定稿

文件更新記錄

版本	日期	修改人	修改事項
1.0	2026-09-24	—	初版：權限管理功能區 10 支功能頁與共用機制

文件審核記錄

審核角色	姓名	日期	意見
需求方			
開發			
測試			

目錄

文件更新記錄	2
文件審核記錄	2
目錄.....	2
1 文件範圍	6
2 業務需求摘要	6
3 功能需求清單	7
4 系統架構與共用設定	7
4.1 系統架構.....	7
4.2 請求管線.....	8
4.3 授權決策 (PEP / PDP)	9
4.4 資料權限.....	10
4.5 回應格式與分頁.....	12
4.6 綁定的樂觀鎖	12
4.7 訊息顯示與錯誤碼	13
4.8 模組擴充契約	14

5 畫面與流程.....	15
5.1 登入 (Login)	15
5.1.1 頁面顯示邏輯.....	15
5.1.2 驗證邏輯.....	16
5.1.3 登入處理邏輯.....	16
5.1.4 登出	17
5.1.5 介面與訊息	17
5.2 個人設定 (Me)	17
5.2.1 個人資料.....	18
5.2.2 偏好設定.....	18
5.2.3 變更密碼.....	19
5.2.4 強制變更密碼.....	20
5.2.5 介面與訊息	20
5.3 使用者管理 (Users)	20
5.3.1 頁面顯示邏輯.....	21
5.3.2 查詢邏輯.....	22
5.3.3 新增使用者	22
5.3.4 編輯使用者	23
5.3.5 指派角色.....	24
5.3.6 重設密碼.....	25
5.3.7 批次啟用與停用	25
5.3.8 刪除使用者	26
5.3.9 匯入與匯出	26
5.3.10 介面清單	27
5.3.11 訊息一覽.....	27
5.4 部門管理 (Depts)	28
5.4.1 頁面顯示邏輯.....	28

5.4.2	新增部門.....	28
5.4.3	編輯部門.....	29
5.4.4	刪除部門.....	29
5.4.5	介面與訊息	29
5.5	角色管理 (Roles)	30
5.5.1	頁面顯示邏輯.....	30
5.5.2	新增與編輯	31
5.5.3	設定功能權限.....	32
5.5.4	設定選單可見性	33
5.5.5	設定資料範圍.....	34
5.5.6	並行修改.....	34
5.5.7	刪除與批次變更狀態.....	35
5.5.8	介面與訊息	35
5.6	權限管理 (Permissions)	36
5.6.1	頁面顯示邏輯.....	36
5.6.2	新增與編輯	36
5.6.3	刪除	37
5.6.4	權限目錄的來源	37
5.6.5	介面與訊息	37
5.7	選單管理 (Menus)	38
5.7.1	頁面顯示邏輯.....	38
5.7.2	新增與編輯	39
5.7.3	刪除	40
5.7.4	側欄選單的產生	40
5.7.5	介面與訊息	41
5.8	線上使用者 (Online Sessions)	41
5.8.1	頁面顯示邏輯與查詢.....	41

5.8.2	強制下線.....	42
5.8.3	介面與訊息	42
5.9	稽核紀錄 (Audit Logs)	42
5.9.1	事件類型.....	43
5.9.2	頁面顯示邏輯與查詢.....	43
5.9.3	變更明細.....	44
5.9.4	匯出與刪除	44
5.9.5	介面與訊息	45
5.10	登入日誌 (Login Log)	45
6	資料存取對象	46
7	業務規則與驗證	47
8	例外處理	49
9	使用者與權限	49
9.1	典型角色	49
9.2	權限鍵目錄	49
10	非功能需求	51

1 文件範圍

本文件描述 Synoria Base 後台「權限管理」功能區的系統分析與設計，供開發、測試與驗收使用。內容以畫面為單位展開：每個功能頁先呈現畫面，再依序說明頁面顯示邏輯、查詢邏輯、驗證邏輯與資料寫入邏輯，並標明所涉及的 API、權限鍵、資料表與對使用者顯示的訊息。

項目	內容
涵蓋	權限管理功能區的 10 支功能頁：登入、個人設定、使用者、部門、角色、權限、選單、線上使用者、稽核紀錄、登入日誌
涵蓋	上述頁面共用的機制：請求管線、授權決策 (PEP / PDP)、資料權限、回應格式、樂觀鎖、訊息與錯誤碼、模組擴充契約
不涵蓋	系統維運功能區 (參數設置、字典、行政區、檔案管理、通知公告、定時任務、背景任務、服務監控、前端錯誤、登入 IP 名單)，另行撰寫
不涵蓋	外部身分整合 (LDAP / AD / SAML / OIDC / MFA) 與多租戶
不涵蓋	部署與基礎設施 (高可用、WAF、監控告警)

文件中的畫面均為示意圖，依實際頁面版型與欄位重製，資料皆為虛構，用於標示欄位位置與狀態。

2 業務需求摘要

Synoria Base 是一套可重複使用的後台底座：任何業務系統 (CRM、ERP 等) 都能以它為基礎，直接取得身分驗證、授權、資料權限與稽核能力，把開發心力放在業務功能上。權限管理功能區是底座的核心，目標是讓「誰能做什麼、能看到哪些資料、做過什麼」都有明確且可驗證的答案。

需求	說明	對應功能
身分驗證	帳密登入、驗證碼、登入失敗鎖定、可撤銷的 session、強制變更密碼	登入、個人設定
帳號管理	建立與維護帳號、批次匯入匯出、重設密碼、指派角色與部門	使用者
組織與資料權限	維護部門樹；以角色設定資料可見範圍 (全部 / 自訂 / 本部門 / 本部門及以下 / 僅本人)	部門、角色
功能權限	以權限鍵定義每一個 API 動作，角色綁定權限鍵後，成員才能執行該動作	角色、權限
導覽治理	維護選單樹與頁面路由；選單可見性與功能權限分開設定	選單、角色
會話控管	檢視目前在線的連線，必要時強制下線	線上使用者
稽核	登入、授權拒絕與管理異動皆留紀錄，可依 request_id 追查整串請求並檢視欄位變更	稽核紀錄、登入日誌

整個功能區遵循四項設計原則：

- 後端是唯一的安全邊界。前端依權限隱藏按鈕只是為了使用體驗，每一支 API 仍由後端重新判定。
- 預設拒絕 (fail-closed)。未登記的路由、決策服務故障或逾時、授權資料不一致，一律拒絕。
- 功能權限與資料權限分開。權限鍵決定「能不能做」，資料範圍決定「能看到哪些資料列」。
- 可稽核。拒絕與異動都留下紀錄，並能區分「策略拒絕」與「系統故障造成的拒絕」。

3 功能需求清單

權限管理功能區的功能頁一覽。詳細規格見第 5 章對應小節。

編號	功能頁	路由	說明	章節
IAM-01	登入	/login	帳密登入，含驗證碼、失敗鎖定與 IP 限流	5.1
IAM-02	個人設定	/me/profile /me/preferences	個人資料、偏好設定與變更密碼	5.2
IAM-03	使用者	/system/users	帳號維護、匯入匯出、重設密碼、指派角色	5.3
IAM-04	部門	/system/depts	維護部門樹	5.4
IAM-05	角色	/system/roles	維護角色，設定功能權限、選單可見性與資料範圍	5.5
IAM-06	權限	/system/permissions	維護權限目錄	5.6
IAM-07	選單	/system/menus	維護選單樹、路由與所需權限	5.7
IAM-08	線上使用者	/system/online-sessions	檢視在線連線並強制下線	5.8
IAM-09	稽核紀錄	/system/audit	查詢、匯出稽核紀錄與檢視欄位變更	5.9
IAM-10	登入日誌	/system/login-log	檢視登入、登出與變更密碼事件	5.10

4 系統架構與共用設定

4.1 系統架構

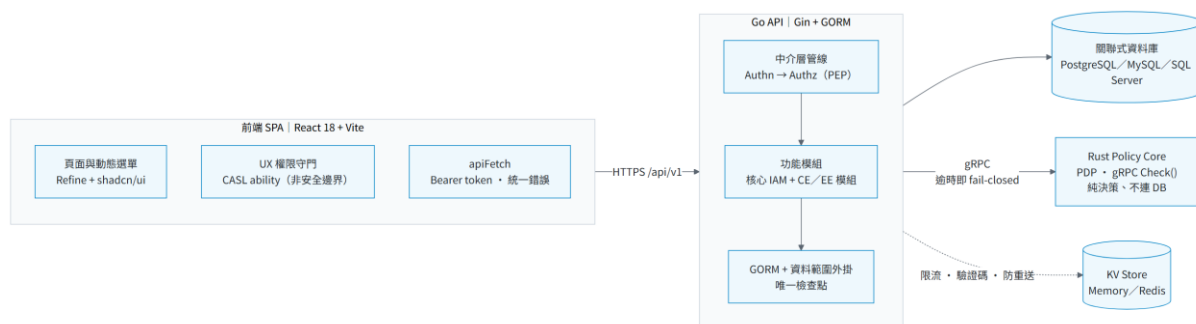


圖 4.1-1 系統架構與元件職責

元件	技術	職責
前端 SPA	React 18、Vite、Refine、shadcn/ui、TanStack Table、react-hook-form + zod、i18next	畫面、動態選單、表單驗證、UX 權限守門
API (PEP)	Go 1.26、Gin、GORM	HTTP 契約、身分驗證、授權執行、資料存取、稽核
Policy Core (PDP)	Rust、tonic gRPC	無狀態的授權決策，只回答允許或拒絕與原因
資料庫	PostgreSQL / MySQL / SQL Server	同一套 schema，以各方言的 migration 維護
KV Store	記憶體或 Redis	登入限流、失敗次數、驗證碼、防重送

決策 (PDP) 與執行 (PEP) 分成兩個服務。PDP 只做決策，不連資料庫，也不自行 fail-closed；逾時、無法連線等錯誤由 Go 端轉成型別化錯誤，再統一轉為拒絕。這樣的切分讓決策邏輯可以獨立測試與替換，也確保系統故障永遠不會被誤判為允許。

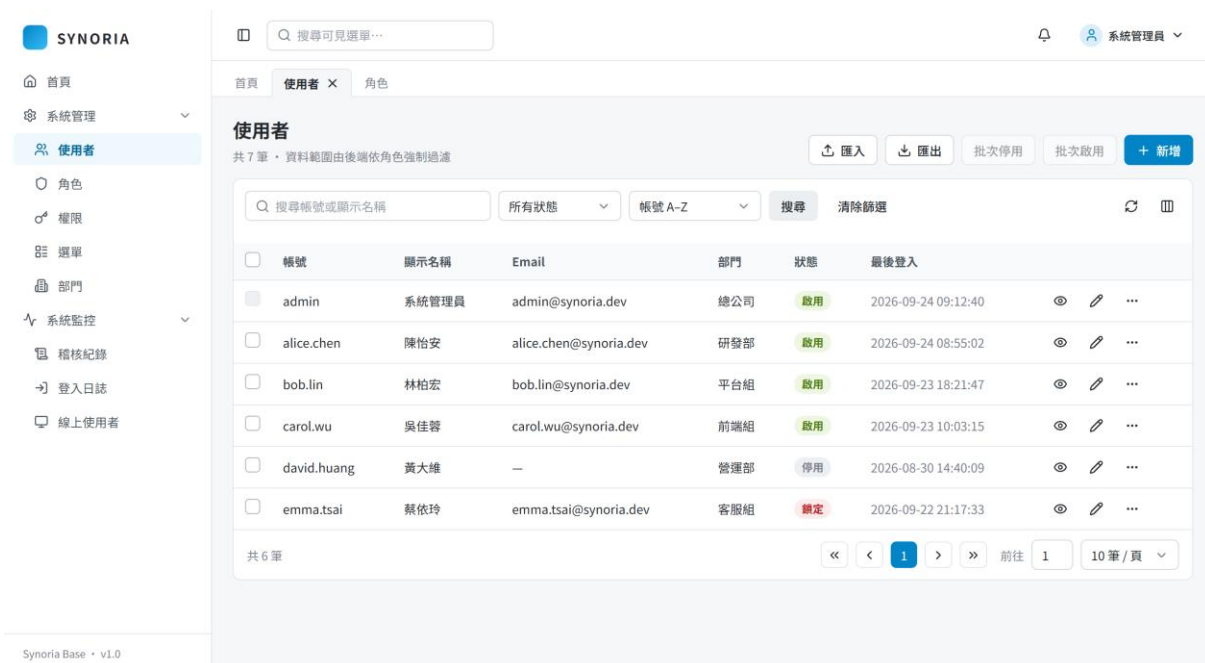


圖 4.1-2 後台外殼：側欄選單、頁籤列與內容區

登入後的頁面共用同一個外殼。側欄選單由後端依使用者的角色產生（見 5.7.4），頂部提供選單搜尋、通知與個人選單（個人資料、變更密碼、設定、登出），頁籤列保留已開啟的頁面。

4.2 請求管線

受保護的 API 依序通過下列中介層，任一層拒絕即回傳統一格式的錯誤，不會進入功能程式：

順序	中介層	職責	拒絕時
1	RequestID	沿用或產生 <code>X-Request-Id</code> ，寫入回應與稽核，用於串起整次請求	—
2	Authn	驗證 Bearer token 對應的 session 未撤銷、未過期；每次請求都自資料庫重新載入使用者狀態、角色、權限與自訂部門	401 AUTH-003 (session 無效) 401 AUTH-002 (帳號非啟用)
3	MustChangePassword	帳號被標記須變更密碼時，只放行變更密碼、取得身分與登出三支 API	403 AUTHZ-003
4	RateLimit	寫入類請求 (POST / PUT / PATCH / DELETE) 依使用者與路由限流，可由系統參數開關	429
5	AntiResubmit	3 秒內內容相同的請求視為重複送出，可由系統參數開關	409 DATA-003
6	Authz (PEP)	依路由的權限政策向 PDP 取得決策，並計算本次的資料範圍	403 / 500 / 503，見 4.3

由於每次請求都重新載入使用者資料，角色、權限或帳號狀態一經變更，下一次請求就會生效，不需要另外設計令牌版本或快取失效機制。強制變更密碼刻意回傳 403 而非 401，讓前端引導使用者變更密碼，而不是把人登出。

回應標頭：登入、建立使用者、匯入使用者、重設密碼、變更密碼等回應可能含憑證的路由，一律加上 `Cache-Control: no-store`，避免瀏覽器或代理伺服器快取。

4.3 授權決策 (PEP/PDP)

每一條路由在啟動時登記三種政策之一：公開、僅需登入、需權限鍵。啟動時系統會檢查所有路由都已分類，且每個權限鍵都存在於 `sys_permission`；任一不符即拒絕啟動，讓「忘了掛權限」在上線前就被擋下。

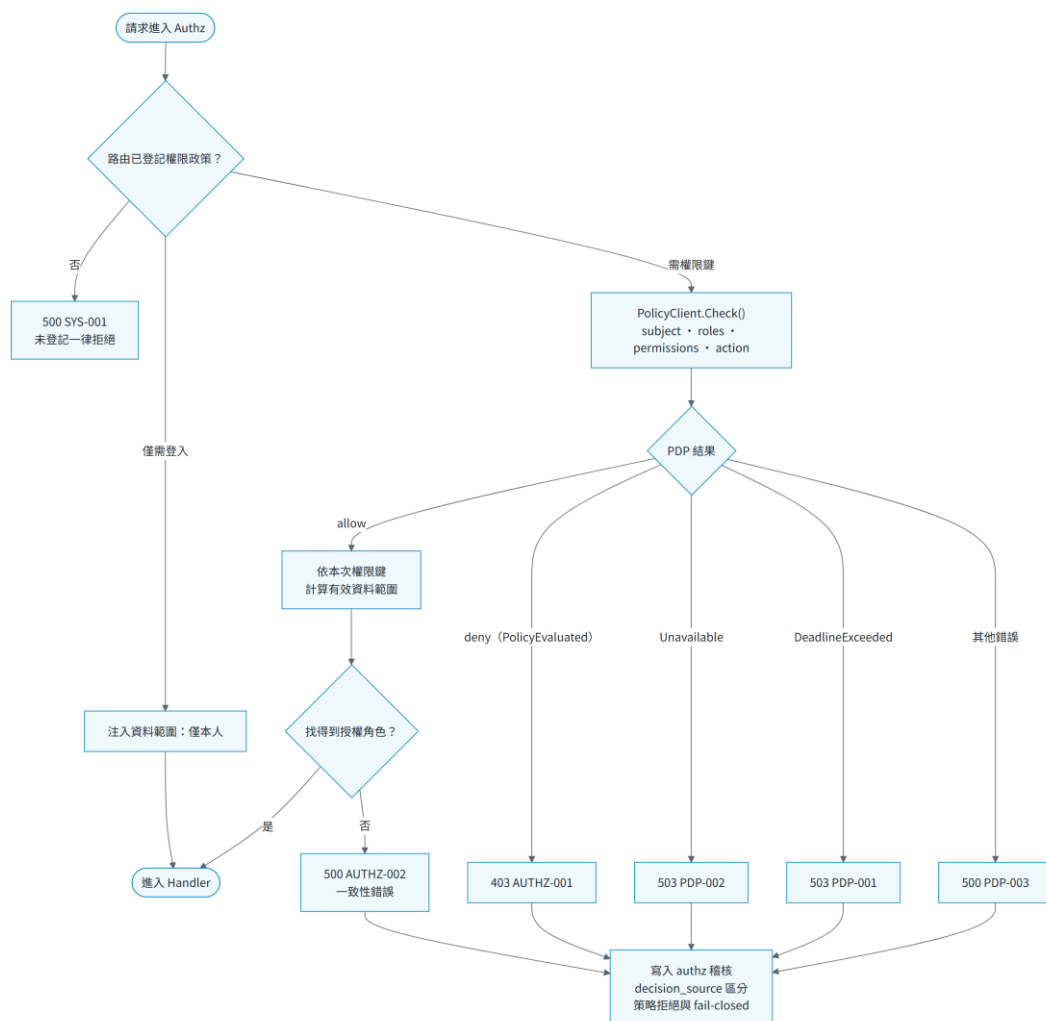


圖 4.3-1 授權決策流程

decision_source	情境	HTTP	原因碼
PolicyEvaluated	策略判定拒絕	403	AUTHZ-001
FailClosedUnavailable	PDP 無法連線	503	PDP-002
FailClosedTimeout	PDP 逾時 (預設 5 秒)	503	PDP-001
FailClosedInternalError	PDP 內部錯誤	500	PDP-003
FailClosedInternalError	PDP 允許，但找不到授予此權限鍵的角色	500	AUTHZ-002

PDP 的規則刻意保持簡單：持有 super role 者允許；請求的權限鍵在使用者的權限集合內則允許；其餘一律拒絕。所有拒絕與 fail-closed 都寫入 authz 稽核；允許不寫稽核，避免稽核量隨流量膨脹。

決策快取為選配功能，只快取策略判定的結果，不快取錯誤。快取鍵包含使用者、權限鍵，以及排序後的角色與權限集合，因此綁定一變更就會換成新的鍵，不會讀到舊的決策。

4.4 資料權限

資料權限決定使用者在清單與查詢中「看得到哪些資料列」，以角色為單位設定，共五個層級：

層級	名稱	過濾條件
1	全部	不過濾
2	自訂	部門在角色指定的自訂部門清單內 (sys_role_dept)
3	本部門	部門等於使用者所屬部門
4	本部門及以下	部門為使用者所屬部門或其子孫部門
5	僅本人	資料擁有者為使用者本人

有效範圍依「本次動作」計算 (action-aware)：只取授予本次權限鍵的角色，再取其中最寬的範圍；層級為自訂時，合併這些角色的自訂部門。持有 super role 者一律視為全部。

範例：使用者同時持有角色 A (user.read , 本部門) 與角色 B (report.read , 全部)。查詢使用者時只會得到本部門，B 的「全部」不會外溢到與它無關的動作。

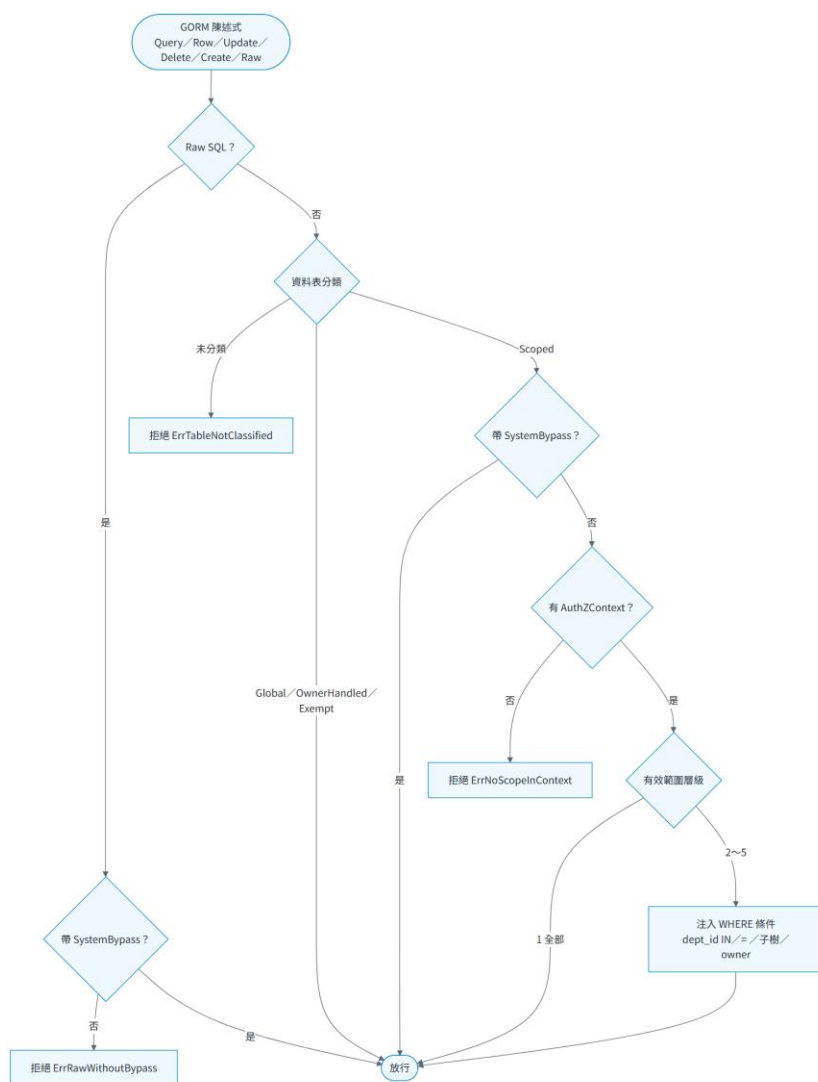


圖 4.4-1 資料範圍唯一檢查點

資料範圍由 GORM 外掛在所有 Query、Row、Update、Delete 陳述式執行前強制注入，是唯一的檢查點，功能模組不需要、也不應該自行拼接過濾條件。每張資料表必須先登記類別：

類別	行為	資料表
Scoped	依有效範圍注入條件	sys_user (部門欄 dept_id、擁有者欄 id)
OwnerHandled	由功能依擁有者自行過濾	sys_auth_session、sys_user_preference 等個人資料
Global	不過濾	角色、權限、選單、部門、綁定表、稽核等治理資料
Exempt	不過濾	schema_migrations

- 未登記的資料表、沒有授權內容的 Scoped 查詢，以及未標示系統旁路的原生 SQL，一律拒絕執行。
- 系統旁路 (migration、登入流程) 必須附上原因字串，缺少原因時程式直接中止。
- 範圍外的資料視同不存在，回傳 404 DATA-001，不透露資料是否存在。
- 資料範圍只負責「看得到哪些列」；寫入仍須先通過權限鍵授權。建立或搬移部門時，另由功能檢查目標部門是否在操作者的範圍內，不能以「讀不到」代替「不能改」。

4.5 回應格式與分頁

所有 API 回傳統一格式。成功時資料放在 data，清單另附 meta；失敗時回傳原因碼與訊息。每個回應都帶 request_id，可在稽核紀錄中查到同一次請求的所有事件。

```
成功: { "data": [ ... ], "meta": { "page": 1, "page_size": 20, "total": 57 }, "request_id": "3f2a9c1d..." }
失敗: { "error": { "code": "AUTHZ-001", "message": "...", }, "request_id": "a91c0e77..." }
```

參數	說明
page	頁碼，自 1 起算，預設 1
page_size	每頁筆數，預設 20、上限 100；不合法的值回到預設值，不視為錯誤
其他條件	依各功能頁定義，例如使用者清單的 q、status、sort、order

前端清單的每頁筆數可選 10 / 20 / 50 / 100，表格支援切換顯示欄位與緊密列高。部門與選單以樹狀一次載入，不分頁。

4.6 綁定的樂觀鎖

角色的功能權限、選單可見性與資料範圍三種綁定各有獨立的 revision。讀取綁定時一併取得 revision，儲存時帶回；後端在交易內鎖定角色列、比對 revision、遞增後再整組覆寫。兩位管理者同時編輯同一個角色時，後送出的一方會收到衝突，而不會默默蓋掉對方的修改。

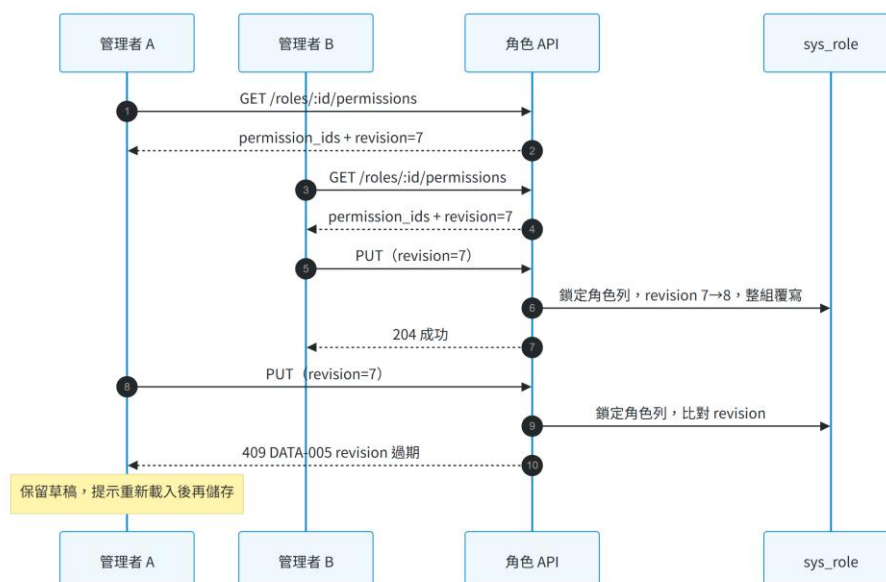


圖 4.6-1 兩位管理者同時編輯同一個角色

情況	HTTP	原因碼	畫面處理
未帶 revision	400	DATA-004	視為程式錯誤，顯示失敗提示
revision 格式錯誤	400	DATA-006	同上
revision 已過期	409	DATA-005	保留草稿，提示「捨棄草稿並重新載入」後再儲存

4.7 訊息顯示與錯誤碼

操作結果以畫面右上角的浮動提示呈現，分成功與失敗兩種樣式；表單欄位的驗證訊息直接顯示在欄位下方。前端依原因碼顯示在地化訊息，不直接把後端的技術訊息顯示給使用者。

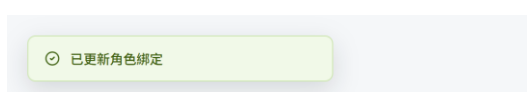


圖 4.7-1 成功提示

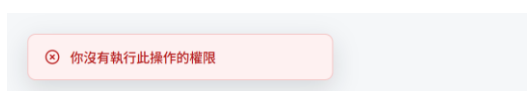


圖 4.7-2 失敗提示

原因碼	意義	典型 HTTP
AUTH-001	登入失敗（不揭露帳號是否存在）；也用於 IP 不允許、登入過於頻繁、驗證碼錯誤、舊密碼錯誤	401 / 403 / 429 / 400
AUTH-002	帳號停用、鎖定或達失敗上限	401
AUTH-003	session 過期、已撤銷或未提供	401
AUTHZ-001	權限不足	403
AUTHZ-002	授權一致性錯誤	500
AUTHZ-003	須先變更密碼	403
PDP-001 / PDP-002 / PDP-003	PDP 逾時 / 無法連線 / 內部錯誤	503 / 503 / 500
SESS-001	使用者主動登出（稽核用）	—
DATA-001	資料不存在或不在資料範圍內	404
DATA-002	唯一鍵衝突	409
DATA-003	完整性規則阻擋（受保護資料、最後一位超級管理員、刪除自己、重複送出等）	409
DATA-004 / DATA-005 / DATA-006	revision 缺少 / 過期 / 格式錯誤	400 / 409 / 400
AUDIT-001	稽核寫入失敗	500
SYS-001	欄位驗證失敗或系統內部錯誤	400 / 500

4.8 模組擴充契約

核心權限功能與其他功能模組使用同一套契約。下游系統在自己的程式中組合 Synoria Base 提供的模組與自有模組，即可取得相同的啟動檢查、授權與資料權限保護。

契約項目	說明
Key()	模組唯一鍵，同時作為 migration 紀錄的前綴
Migrations()	各資料庫方言的 migration 檔，在核心 migration 之後依模組順序執行
PermissionKeys()	模組宣告的權限鍵，啟動時寫入權限目錄
MenuSeed()	模組的選單項目（上層、類型、路由、頁面元件、所需權限、圖示、排序）
Wire() / RegisterRoutes()	注入資料庫、稽核、KV Store 等依賴，並以權限鍵登記路由
選用介面	DataScopeTables() 登記資料表類別；PermissionDescriptors() 提供權限說明；SeedData()；Start() / Stop()

- 啟動時驗證：模組鍵重複、權限鍵與核心或其他模組衝突、選單鍵使用核心保留字、資料表重複登記，任一成立即拒絕啟動。
- 模組路由經由同一個登記表，自動套用 4.3 的啟動檢查、PEP 與 4.4 的資料範圍。
- 前端以 registerPage(componentKey) 註冊頁面元件，選單的頁面元件欄位即對應到這個鍵。

5 畫面與流程

本章每一小節對應一支功能頁。各小節先呈現畫面，再依序說明頁面顯示邏輯、查詢邏輯，以及各項操作的顯示、驗證與寫入邏輯，最後列出介面與訊息。API 路由皆省略共同前綴 `/api/v1`。

5.1 登入 (Login)

提供帳密登入。登入成功後由伺服器建立 session 並回傳 token，之後的每一次請求都以此 token 識別身分。登入流程同時負責擋下暴力嘗試：IP 名單、IP 頻率限制、驗證碼與帳號失敗鎖定四道防線依序檢查。



圖 5.1-1 登入頁



圖 5.1-2 啟用驗證碼時的登入頁

5.1.1 頁面顯示邏輯

- 進入頁面時呼叫 `GET /auth/captcha`。系統參數 `sys.login.captcha_enabled` 關閉時不顯示驗證碼欄位；開啟時顯示一位數加減法的圖片題目，有效 5 分鐘，點圖片可換一題。
- 已登入的使用者進入 `/login` 時直接導回首頁。
- 送出期間按鈕顯示「登入中...」並停用，重複點擊不會重送。
- 離開頁面、切換分頁或登入狀態改變時，清除密碼與驗證碼欄位，不在畫面上殘留憑證。

5.1.2 驗證邏輯

欄位	必填	規則	未通過時
帳號	是	不可空白；含「@」時以 email 比對，否則以帳號比對	欄位下方提示「請輸入帳號」
密碼	是	不可空白	欄位下方提示「請輸入密碼」
驗證碼	啟用時	須與題目答案相符；每一題只能驗證一次，答錯即作廢	登入失敗並自動換新題

5.1.3 登入處理邏輯

依下列順序檢查，任一步未通過即拒絕，並寫入登入失敗的稽核：

1. **IP 名單**。來源 IP 不在允許清單或位於封鎖清單時，回傳 403 AUTH-001。
2. **IP 頻率限制**。同一 IP 每分鐘的嘗試次數超過 `sys.login.ip_rate_per_minute`（預設 60，設 0 為不限制）時，回傳 429 AUTH-001。成功的嘗試同樣計入。
3. **驗證碼**。啟用時檢查答案，錯誤回傳 401 AUTH-001。
4. **帳號鎖定**。以正規化後的帳號（去空白、轉小寫）計算失敗次數；達 `sys.login.max_retry`（預設 5）後鎖定 `sys.login.lock_minutes`（預設 10）分鐘，期間回傳 401 AUTH-002。
5. **帳號與密碼**。帳號不存在或密碼錯誤皆回傳 401 AUTH-001，並將失敗次數加一。密碼以 Argon2id 驗證；密碼正確時清除失敗次數。
6. **帳號狀態**。狀態不是「啟用」時回傳 401 AUTH-002。
7. **建立 session**。產生 32 位元組隨機 token，資料庫只保存其 SHA-256 雜湊；有效期限為 `auth.token_ttl`（預設 24 小時），不滑動延長。同時更新最後登入時間，並寫入登入成功的稽核。

不揭露帳號是否存在：帳號不存在時仍對一組假雜湊執行一次 Argon2id 運算，讓回應時間與密碼錯誤時一致；兩者也回傳相同的原因碼。畫面上所有登入失敗一律只顯示「登入失敗」，不區分原因。



圖 5.1-3 登入失敗

- 登入成功後，前端將 token 存於瀏覽器，之後以 `Authorization: Bearer` 標頭送出，並清除先前快取的權限資料後導向首頁。
- 回應中的 `force_password_change` 為真時，登入後直接開啟變更密碼對話框（見 5.2.4）。
- 所有登入嘗試（含失敗）都寫入 auth 稽核，記錄 IP、解析出的地理位置與 User-Agent，供登入日誌查詢。

5.1.4 登出

使用者從個人選單點「登出」時呼叫 `POST /auth/logout`，後端撤銷本次 session（寫入 `revoked_at`），並寫入原因碼為 `SESS-001` 的登出稽核。前端無論請求成功與否，都清除本機 token 與權限快取並導回登入頁。

5.1.5 介面與訊息

方法	路由	權限鍵	用途
GET	<code>/auth/captcha</code>	公開	取得驗證碼題目；未啟用時回傳 <code>enabled:false</code>
POST	<code>/auth/login</code>	公開	登入，回傳 token 與是否須變更密碼
POST	<code>/auth/logout</code>	僅需登入	撤銷本次 session
GET	<code>/auth/me</code>	僅需登入	取得身分、權限鍵、是否持有 <code>super role</code> 與選單樹

情境	訊息	呈現方式
未填帳號或密碼	請輸入帳號 / 請輸入密碼	欄位下方
任何登入失敗	登入失敗	表單內提示
session 失效後操作	（導回登入頁）	—

5.2 個人設定（Me）

每位登入者都能維護自己的顯示名稱、介面偏好與密碼。這些功能只需登入、不需權限鍵，由個人選單進入。

5.2.1 個人資料

個人資料

帳號
alice.chen

Email
alice.chen@synoria.dev

顯示名稱
陳怡安

儲存

權限鍵值
user.read user.create user.update user_role.bind dept.read role.read audit.read

圖 5.2-1 個人資料

- 帳號與 Email 為唯讀；顯示名稱可修改，去除前後空白後不可為空，儲存按鈕在空白時停用。
- 下方列出目前持有的權限鍵，方便使用者自行確認權限；持有 super role 者顯示「具備全部權限」。
- 儲存時呼叫 PUT /auth/me/profile，只更新 sys_user.display_name，並寫入管理稽核。

欄位	必填	規則	未通過時
顯示名稱	是	不可空白，最長 120 字元	欄位下方顯示驗證訊息，不送出

5.2.2 偏好設定

設定

外觀

主題配色 Clean

明暗模式 跟隨系統

主題設定儲存在此裝置。

地區與格式

日期格式 YYYY-MM-DD (系統設定值)

時間制 24 小時制

時區 Asia/Taipei

語言 繁體中文

儲存

圖 5.2-2 偏好設定

設定	儲存位置	說明
主題配色、明暗模式	瀏覽器本機	Synoria Blue / Clean / Classic ; 亮色 / 暗色 / 跟隨系統，切換後立即套用
日期格式、時間制、時區、語言	伺服器 sys_user_preference	跨裝置一致；選「系統設定值」時存空值，改用系統預設

偏好的解析順序為：使用者設定 → 系統參數 `sys.default.*` → 內建預設（語言為繁體中文）。後端只接受上述四個鍵與清單內的合法值，其他內容回傳 400 SYS-001。

5.2.3 變更密碼

圖 5.2-3 變更密碼（兩次新密碼不一致）

欄位	必填	規則	未通過時
目前密碼	是	不可空白	「請輸入目前密碼」
新密碼	是	至少 8 字元，且不得與目前密碼相同	「新密碼至少 8 字元」 / 「新密碼不得與目前密碼相同」
確認新密碼	是	須與新密碼相同	「請再次輸入新密碼」 / 「兩次新密碼不一致」

1. 後端以相同規則再檢查一次；目前密碼錯誤時回傳 400 AUTH-001，並寫入變更失敗的稽核。
2. 新密碼以 Argon2id 雜湊後寫入，同時清除「須變更密碼」標記。
3. 撤銷該使用者的其他 session，其他裝置需重新登入；本次 session 保持有效。步驟 2 與 3 於同一交易完成。
4. 寫入變更成功的稽核，回傳 204；前端重新取得身分資料並關閉對話框。

5.2.4 強制變更密碼

管理者建立帳號或重設密碼後，帳號會被標記為「須變更密碼」。此時後端只放行變更密碼、取得身分與登出三支 API，其餘一律回傳 403 AUTHZ-003。前端在登入後直接開啟變更密碼對話框，首頁也顯示提示橫幅，完成變更後才恢復正常操作。



圖 5.2-4 須變更密碼的提示橫幅

5.2.5 介面與訊息

方法	路由	權限鍵	用途
PUT	/auth/me/profile	僅需登入	更新顯示名稱
GET	/me/preferences	僅需登入	取得個人偏好
PUT	/me/preferences	僅需登入	儲存個人偏好
PUT	/auth/password	僅需登入	變更自己的密碼

情境	訊息	呈現方式
儲存個人資料成功	已更新個人資料	浮動提示
儲存偏好成功	已儲存設定	浮動提示
變更密碼成功	密碼已變更	浮動提示
變更密碼失敗	變更失敗	對話框內提示

5.3 使用者管理（Users）

維護後台帳號：新增、編輯、啟用停用、刪除、指派角色、重設密碼，以及以 Excel 批次匯入匯出。清單受資料範圍限制，管理者只看得到、也只改得到自己範圍內的使用者。

使用者						
共 7 筆 · 資料範圍由後端依角色強制過濾						
搜尋帳號或顯示名稱 所有狀態 帳號 A-Z 搜尋 清除篩選 已選 2 筆						
☐ 帳號	顯示名稱	Email	部門	狀態	最後登入	
☐ admin	系統管理員	admin@synoria.dev	總公司	啟用	2026-09-24 09:12:40	☐ ☐ ☐
☐ alice.chen	陳怡安	alice.chen@synoria.dev	研發部	啟用	2026-09-24 08:55:02	☐ ☐ ☐
☒ bob.lin	林柏宏	bob.lin@synoria.dev	平台組	啟用	2026-09-23 18:21:47	☐ ☐ ☐
☒ carol.wu	吳佳蓉	carol.wu@synoria.dev	前端組	啟用	2026-09-23 10:03:15	☐ ☐ ☐
☐ david.huang	黃大維	—	營運部	停用	2026-08-30 14:40:09	☐ ☐ ☐
☐ emma.tsai	蔡依玲	emma.tsai@synoria.dev	客服組	鎖定	2026-09-22 21:17:33	☐ ☐ ☐
☐ frank.lee	李政勳	frank.lee@synoria.dev	財務部	啟用	—	☐ ☐ ☐
共 7 筆 << < 1 > >> 前往 1 10 筆 / 頁						

圖 5.3-1 使用者清單，選取兩筆後批次按鈕啟用

5.3.1 頁面顯示邏輯

- 查詢條件為關鍵字（帳號或顯示名稱，最長 200 字元）、狀態（所有狀態 / 啟用 / 停用）與排序（帳號 A-Z、帳號 Z-A、最新建立優先），預設為帳號 A-Z。條件保存在網址，重新整理或分享連結時保留。
- 工具列：新增（user.create）、匯入（user.create）、匯出（user.read）、批次停用與批次啟用（user.update）。批次按鈕在未選取資料時停用，選取後顯示「已選 n 筆」。
- 每一列的可用操作由後端依「權限鍵」與「目標帳號的保護狀態」共同計算後隨資料回傳，前端依此啟用或停用按鈕，不自行推算。
- 沒有 user.read 時不載入資料，顯示「你沒有檢視此頁的權限」。

欄位標題	資料欄位	顯示規則
（選取）	—	目標帳號不允許批次變更狀態時停用
帳號	username	—
顯示名稱	display_name	—
Email	email	非超級管理員檢視時遮罩，例如 a***e@synoria.dev；未填顯示「—」
部門	dept_id	以部門樹轉為名稱；沒有 dept.read 或找不到時顯示「—」
狀態	status	啟用（綠） / 停用（灰） / 鎖定（紅）
最後登入	last_login_at	依個人偏好的日期時間格式顯示
操作	—	查看、編輯、更多（指派角色、重設密碼、刪除）

可用操作	所需權限鍵	額外限制
編輯	user.update	目標持有 super role 時，操作者須為超級管理員
批次變更狀態	user.update	系統帳號不可；不可停用自己
刪除	user.delete	系統帳號不可；不可刪除自己
指派角色	user_role.bind 與 role.read	目標持有 super role 時，操作者須為超級管理員
重設密碼	user.password.reset	不可重設自己（請改用變更密碼）

5.3.2 查詢邏輯

1. 按下「搜尋」時送出 GET /users，參數為 q、status、sort、order 與分頁參數；後端驗證排序欄位只能是帳號、顯示名稱、建立時間或狀態。
2. 關鍵字以不分大小寫的包含比對同時查帳號與顯示名稱，並跳脫萬用字元。
3. 資料範圍外掛自動在計數與查詢兩段加入範圍條件，範圍外的帳號不會出現在清單與總筆數中。
4. 回傳前計算每一列的可用操作，並依檢視者身分遮罩 Email。密碼雜湊等欄位不得出現在回應中。

```
SELECT ... FROM sys_user
WHERE deleted_at IS NULL
  AND (LOWER(username) LIKE :q ESCAPE '!' OR LOWER(display_name) LIKE :q ESCAPE '!')
  AND status = :status          -- 有指定時才加入
  AND <資料範圍條件>          -- 由外掛注入，例如 dept_id IN (...)
ORDER BY :sort :order, id ASC
```

5.3.3 新增使用者

圖 5.3-2 新增使用者（臨時密碼長度不足）

欄位	必填	規則	未通過時
帳號	是	不可空白，最長 64 字元；不得與未刪除的帳號重複	重複時回傳「帳號或 Email 已存在」
顯示名稱	是	不可空白，最長 120 字元	欄位下方顯示驗證訊息
Email	否	須為合法格式；不得與未刪除的帳號重複	「email 格式錯誤」
臨時密碼	是	至少 12 字元	「密碼至少 12 字元」
部門	否	須在操作者的資料範圍內	回傳 403 AUTHZ-001

- 密碼以 Argon2id 雜湊後寫入 `sys_user`，狀態為啟用，並標記「須變更密碼」，使用者首次登入時必須更換。
- 角色不在此設定，建立後以「指派角色」另行指派（`user_role.bind` 與 `user.create` 分屬不同權限）。
- 寫入 `user.create` 管理稽核；部門超出範圍被擋下時也寫入失敗稽核。

5.3.4 編輯使用者

圖 5.3-3 編輯使用者

- 可修改顯示名稱、Email、部門與狀態；帳號與密碼不可在此修改。系統帳號不顯示狀態欄位，後端同樣拒絕變更系統帳號的狀態。
- Email 以遮罩值顯示時，未修改就不送出，避免遮罩值覆蓋真實資料。
- 部門選單只列出操作者資料範圍內的部門；使用者已有部門時不提供「未指派」選項。
- 不可停用或鎖定自己的帳號。

寫入流程於同一交易完成：

- 鎖定所有超級管理員列與目標使用者列，避免並行操作繞過下列檢查。
- 再次確認新部門在操作者的資料範圍內；目標持有 `super role` 時，確認操作者為現任超級管理員。
- 只更新有送出的欄位，並記錄 `updated_by`。

4. 重新計算啟用中的超級管理員人數，為 0 時整筆回滾，回傳 409 DATA-003。

成功後寫入 `user.update` 管理稽核，並將顯示名稱、Email、狀態、部門的變更前後值寫入 `sys_audit_change`，可在稽核紀錄的「變更明細」檢視。帳號停用或鎖定後，該帳號既有的 session 在下一次請求即被拒絕（401 AUTH-002）。

5.3.5 指派角色

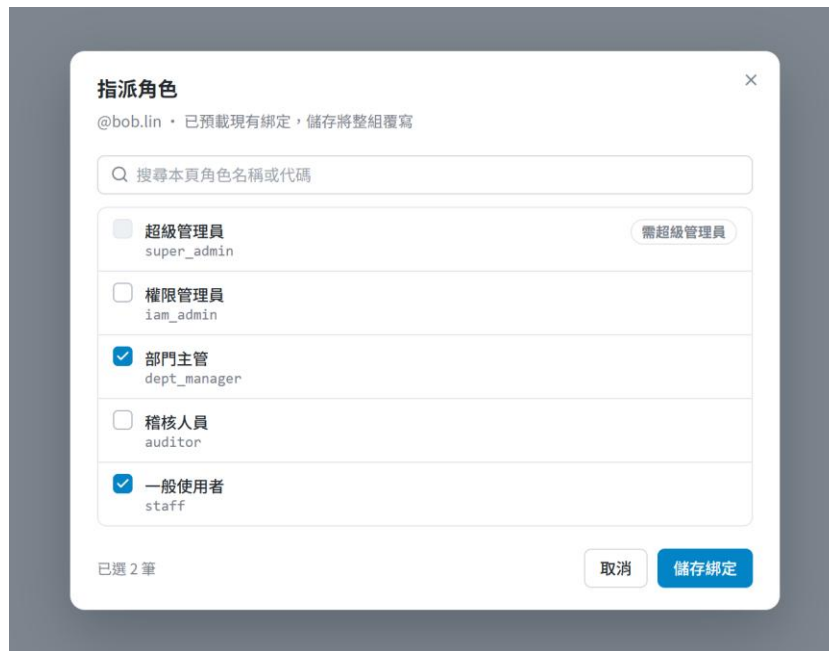


圖 5.3-4 指派角色

- 開啟時預載目前綁定（GET /users/:id/roles），勾選清單來自 GET /roles；儲存時整組覆寫。
- super role 與系統角色的指派或移除，只有現任超級管理員能執行；其他操作者看到這些選項為停用。
- 寫入於同一交易完成：鎖定使用者，刪除原有綁定後寫入新綁定，再確認至少保留一位超級管理員。
- 角色不存在時回傳 400 DATA-003；成功時寫入 `user_role.bind` 管理稽核。

5.3.6 重設密碼



圖 5.3-5 重設密碼：自動產生的臨時密碼只顯示一次

方式	說明
自動產生	由伺服器產生 16 字元高強度臨時密碼，只在本次回應中顯示一次，可複製；關閉對話框後即清除，無法再取回
手動指定	由管理者輸入臨時密碼（至少 12 字元）並再次確認

1. 不可重設自己的密碼；目標持有 `super role` 時，操作者須為超級管理員。
2. 於同一交易內鎖定目標、更新密碼雜湊，並標記「須變更密碼」。
3. 撤銷目標使用者的所有 `session`，對方所有裝置立即登出。
4. 寫入 `user.password.reset` 管理稽核（記錄方式與結果，不記錄密碼）。自動產生的密碼須先成功寫入「憑證交付」稽核才會回傳；稽核或撤銷 `session` 失敗時密碼仍已變更，但不交付憑證，提示管理者排除問題後重新重設。

5.3.7 批次啟用與停用

- 一次最多 200 筆。送出前後端先確認所有 `id` 都在操作者的資料範圍內，只要有一筆不在範圍內就整批拒絕，回傳 `404 DATA-001`，不透露是哪一筆。
- 於同一交易內逐筆鎖定：含系統帳號、含操作者自己，或含 `super role` 持有者而操作者不是超級管理員時，整批不執行。
- 更新後再確認至少保留一位啟用中的超級管理員；成功回傳異動筆數並寫入 `user.batch_status` 管理稽核。

5.3.8 刪除使用者



圖 5.3-6 刪除確認

- 採軟刪除（寫入 `deleted_at`）。已刪除帳號的帳號與 Email 可被新帳號重新使用。
- 不可刪除自己、系統帳號，或最後一位超級管理員；目標持有 `super role` 時，操作者須為超級管理員。
- 刪除後該帳號的 session 在下次請求即失效（`401 AUTH-003`）。

5.3.9 匯入與匯出



圖 5.3-7 匯入結果與一次性憑證下載

- **下載範本**：範本欄位由 `GET /users/import-template/schema` 提供（`username`、`display_name`、`email`、`status`），前端不寫死欄位。
- **匯入**：上傳 xlsx（上限 5 MiB），並選擇匯入的目標部門（須在操作者的資料範圍內）。每一列以與新增相同的規則驗證，逐列建立；成功的列產生臨時密碼並標記須變更密碼，失敗的列列出行號與原因，不影響其他列。
- **憑證交付**：產生的臨時密碼只能從本次回應下載一次（`temporary-credentials.txt`）；關閉對話框即丟棄。處理中或憑證尚未處理前，對話框不可用 Esc 或點背景關閉。
- **稽核**：寫入 `user.import`，結果為成功、部分成功或失敗，並附總筆數、成功與失敗筆數；不記錄個別資料內容。

- **匯出**：依目前的查詢條件與排序匯出資料範圍內的使用者（上限 100,000 筆），欄位為帳號、顯示名稱、Email、狀態，並寫入 `user.export` 稽核。匯出失敗時顯示失敗提示。

5.3.10 介面清單

方法	路由	權限鍵	用途
GET	/users	user.read	使用者清單與總筆數
GET	/users/:id	user.read	單筆使用者
POST	/users	user.create	新增使用者
PUT	/users/:id	user.update	編輯使用者
PUT	/users/batch-status	user.update	批次啟用或停用
DELETE	/users/:id	user.delete	刪除使用者（軟刪除）
GET	/users/:id/roles	user.read	目前的角色綁定
PUT	/users/:id/roles	user_role.bind	整組覆寫角色綁定
POST	/users/:id/password-reset	user.password.reset	重設密碼
GET	/users/import-template /users/import-template/schema	user.create	匯入範本與欄位定義
POST	/users/import	user.create	匯入使用者
GET	/users/export	user.read	匯出使用者

5.3.11 訊息一覽

情境	訊息	呈現方式
新增成功 / 更新成功 / 刪除成功	已新增使用者 / 已更新使用者 / 已刪除使用者	浮動提示，並重新整理表格
帳號或 Email 重複	帳號或 Email 已存在	浮動提示
部門超出資料範圍	所選部門不在你的資料範圍內	浮動提示
刪除或停用最後一位超級管理員	至少須保留一位啟用中的超級管理員	浮動提示
刪除自己	不能刪除自己的帳號	浮動提示
批次含受保護帳號	選取項目包含受保護的帳號，未套用任何變更	浮動提示
重設密碼成功（自動）	已產生臨時密碼，該使用者所有登入已登出，下次登入須變更密碼	對話框內提示
重設後憑證未交付	密碼已變更，但撤銷工作階段或必要交付稽核失敗，因此未交付憑證。排除失敗原因後請執行新的重設。	對話框內提示
匯入完成	共 n 筆 · 成功 n · 失敗 n	對話框內，失敗列另列行號與原因

5.4 部門管理 (Depts)

維護組織的部門樹。部門是資料權限的範圍基準：使用者掛在部門下，角色的資料範圍再以部門決定可見資料。

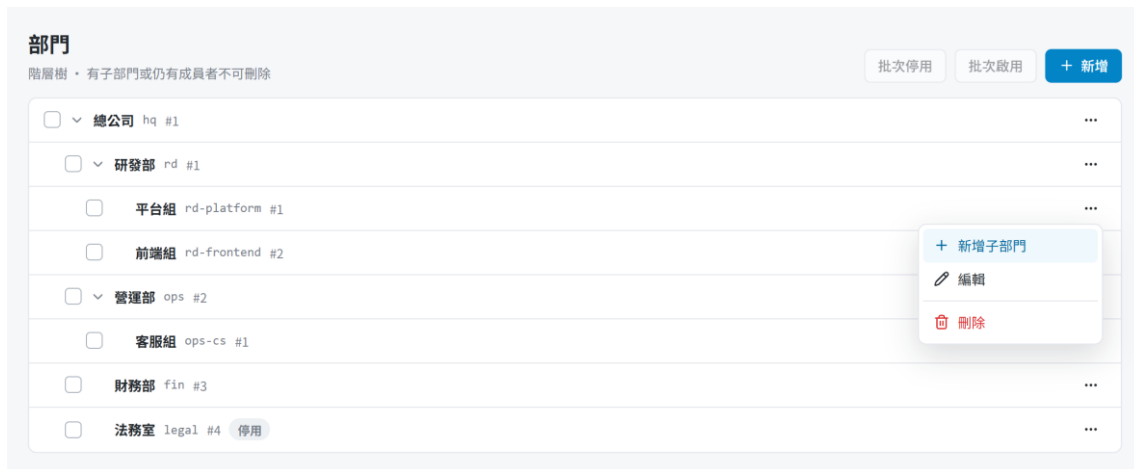


圖 5.4-1 部門樹與列操作選單

5.4.1 頁面顯示邏輯

- 以 GET /depts/tree 一次載入所有未刪除的部門並組成樹，依排序、部門代碼遞增排列，預設全部展開。
- 每列顯示部門名稱、部門代碼、排序與停用標記；列操作為新增子部門、編輯、刪除，依 dept.create、dept.update、dept.delete 顯示。
- 工具列的新增用於建立根層級部門；批次停用與批次啟用需 dept.update。
- 部門樹屬於治理資料，不套用資料範圍，擁有 dept.read 即可看到完整的樹。

5.4.2 新增部門



圖 5.4-2 新增子部門

欄位	必填	規則	未通過時
部門代碼	是	不可空白，最長 100 字元；不得與未刪除的部門重複	重複時回傳「部門代碼已存在」
部門名稱	是	不可空白，最長 120 字元	欄位下方顯示驗證訊息
排序	否	非負整數，預設 0	欄位下方顯示驗證訊息

新增子部門時，上層部門必須存在；新部門的祖先路徑（ancestors）為上層的祖先路徑再加上上層 id，供「本部門及以下」範圍以前綴比對查詢子孫部門。成功後寫入 `dept.create` 管理稽核。

5.4.3 編輯部門

- 可修改部門名稱（不可空白）、排序與狀態；部門代碼不可變更。
- 搬移上層只允許葉節點（沒有子部門的部門），且不可以自己為上層。因為只有葉節點能搬移，部門樹不可能形成循環，其他部門的祖先路徑也不需要重算。畫面不提供搬移，由 API 支援。
- 停用部門不會連帶停用子部門或使用者，也不影響登入。

5.4.4 刪除部門

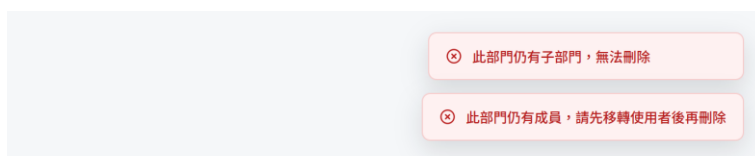


圖 5.4-3 刪除被阻擋

- 仍有子部門時不可刪除，回傳 409 DATA-003。
- 仍有使用者掛在此部門時不可刪除，須先將使用者移到其他部門。
- 通過檢查後採軟刪除，寫入 `dept.delete` 管理稽核；被阻擋時也寫入失敗稽核。

5.4.5 介面與訊息

方法	路由	權限鍵	用途
GET	/depts/tree	dept.read	部門樹
POST	/depts	dept.create	新增部門
PUT	/depts/:id	dept.update	編輯部門（含搬移上層）
PUT	/depts/batch-status	dept.update	批次啟用或停用
DELETE	/depts/:id	dept.delete	刪除部門（軟刪除）

情境	訊息	呈現方式
新增 / 更新 / 刪除成功	已新增部門 / 已更新部門 / 已刪除部門	浮動提示
部門代碼重複	部門代碼已存在	浮動提示
有子部門	此部門仍有子部門，無法刪除	浮動提示
仍有成員	此部門仍有成員，請先移轉使用者後再刪除	浮動提示
搬移有子部門的部門	有子部門的部門不能搬移	浮動提示

5.5 角色管理（Roles）

角色是權限的載體，分別承載三件事：**功能權限**（能呼叫哪些 API）、**選單可見性**（側欄看得到哪些頁面）與**資料範圍**（看得到哪些資料列）。三者各自設定、各自有權限鍵與 revision，勾選選單不會授予任何功能權限。



圖 5.5-1 角色清單與「更多」選單

5.5.1 頁面顯示邏輯

- 清單依 role_key 遞增排序並分頁；欄位為 role_key、角色名稱、排序、資料範圍，以及「超管」「系統」標記。
- 列操作：查看、編輯、更多（設定功能權限、設定選單可見性、設定資料範圍、刪除）。每一項依後端回傳的可用操作決定是否啟用，並同時要求開啟對話框所需的讀取權限（例如設定功能權限需 permission.read，設定選單可見性需 menu.read，設定資料範圍需 dept.read）。
- 受保護角色無法操作時，對話框顯示原因說明，而不是只把按鈕變灰。

判定（依序）	結果
目標為系統角色或 super role，且動作為變更狀態或刪除	不可操作：此內建角色設定不可修改
目標為 super role，且動作為設定功能權限、選單或資料範圍	不可操作：super role 天生具備全部權限、選單與資料範圍，綁定資料不影響實際能力
目標為系統角色或 super role，操作者不是超級管理員	不可操作：只有超級管理員可以修改此受保護角色
操作者不是超級管理員，也沒有對應權限鍵	不可操作：你沒有修改此設定的權限
其他	可操作

5.5.2 新增與編輯

新增角色

功能權限、選單可見性與資料範圍可在建立後設定

role_key *

角色名稱 *

說明 (選填)

資料範圍

排序

圖 5.5-2 新增角色

欄位	必填	規則	未通過時
role_key	是（新增）	不可空白，最長 100 字元；不得與未刪除的角色重複；建立後不可變更	重複時回傳「角色代碼已存在」
角色名稱	是	不可空白，最長 120 字元	「必填」
說明	否	—	—
資料範圍	是（新增）	1~5，預設 3（本部門）；不得寬於操作者自身的範圍	回傳 403 AUTHZ-001
排序	否	非負整數	「必須為非負整數」
狀態	是（編輯）	啟用或停用；受保護角色不可變更	—

- `is_super_role` 與 `is_system` 不開放由介面設定，只由系統初始化建立（`super role` 必定同時是系統角色）。
- 編輯只修改名稱、說明、排序與狀態；資料範圍請使用「設定資料範圍」。所有變更都在交易內先鎖定角色列、再依 5.5.1 的規則判定。



圖 5.5-3 受保護角色：欄位唯讀並說明原因

5.5.3 設定功能權限



圖 5.5-4 設定功能權限

- 開啟時同時載入權限目錄（每頁 100 筆）與目前綁定及其 revision；每個權限鍵下方顯示「程式定義用途」與「管理員描述」，讓指派者清楚知道勾選的後果。
- 儲存時送出勾選的權限 id 與 revision，後端整組覆寫 `sys_role_permission`（見 4.6）。

- **防止越權授予**：非超級管理員只能勾選自己持有的權限鍵，送出的清單含有自己沒有的權限時整筆拒絕，回傳 403 AUTHZ-001。
- 變更於下一次請求起對該角色的所有成員生效；寫入 `role_permission.bind` 管理稽核。

5.5.4 設定選單可見性



圖 5.5-5 設定選單可見性

- 以樹狀列出所有選單；勾選或取消一個節點時，其子孫節點一併勾選或取消。
- 已綁定但選單已刪除的項目顯示為「無法取得的既有選單」，可明確取消綁定。
- 儲存時整組覆寫 `sys_role_menu`。選單綁定只影響側欄是否顯示，不授予任何 API 能力；側欄最終還會濾掉使用者沒有所需權限的選單（見 5.7.4）。

5.5.5 設定資料範圍

設定資料範圍

人資專員 · 自訂時須選部門 (整組覆寫)

範圍層級 2 · 自訂

自訂部門

- ☐ 總公司
- ☒ 研發部
- ☐ 平台組
- ☐ 前端組
- ☒ 營運部
- ☒ 客服組
- ☐ 財務部

取消 套用

圖 5.5-6 設定資料範圍：自訂時勾選部門

- 選擇範圍層級 1 ~ 5；選「自訂」時必須至少勾選一個部門，否則「套用」按鈕停用。
- 儲存時送出層級、部門 id (非自訂時為空) 與 revision；後端更新 `sys_role.data_scope`，並整組覆寫 `sys_role_dept`。
- 非超級管理員設定的範圍不得寬於自己在 `role.data_scope.set` 下的有效範圍。
- 寫入 `role.data_scope.set` 管理稽核。

5.5.6 並行修改

設定功能權限

部門主管 · 已預載現有綁定，儲存將整組覆寫

伺服器上的綁定已變更，已保留你的草稿。請捨棄草稿並重新載入目前綁定後再儲存。

捨棄草稿並重新載入

- ☒ **user.read**
程式定義用途：檢視使用者清單與明細
- ☒ **user.update**
程式定義用途：修改使用者資料與狀態
- ☒ **user.delete**
程式定義用途：刪除使用者 (軟刪除)

已選 13 筆

取消 儲存綁定

圖 5.5-7 綁定已被他人修改

儲存時 revision 已過期 (409 DATA-005)，對話框保留使用者的勾選草稿、停用儲存按鈕，並提供「捨棄草稿並重新載入」。管理者重新載入最新綁定後再決定如何修改，避免在不知情的情況下覆蓋他人的變更。

5.5.7 刪除與批次變更狀態

- 刪除採軟刪除；系統角色與 super role 不可刪除。仍有使用者持有此角色時不可刪除，須先解除指派。
- 批次啟用停用一次最多 200 筆，依 id 排序逐筆鎖定並檢查規則，任一筆不允許則整批不執行。
- 停用或刪除的角色在下一次請求起不再提供任何權限、選單與資料範圍。

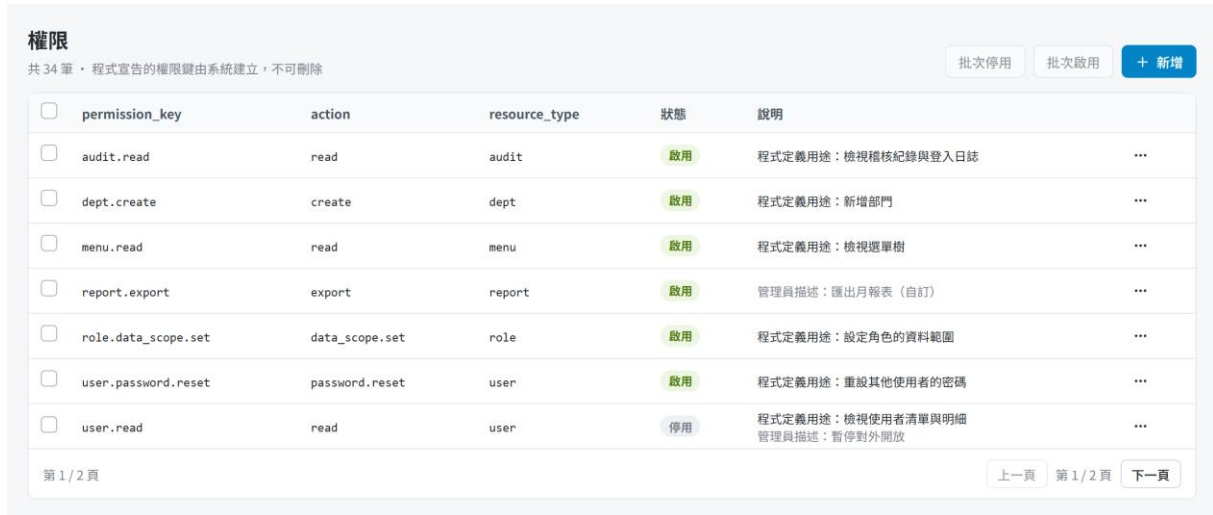
5.5.8 介面與訊息

方法	路由	權限鍵	用途
GET	/roles	role.read	角色清單 (含每列可用操作與 revision)
GET	/roles/:id	role.read	單筆角色
POST	/roles	role.create	新增角色
PUT	/roles/:id	role.update	編輯角色
PUT	/roles/batch-status	role.update	批次啟用或停用
DELETE	/roles/:id	role.delete	刪除角色 (軟刪除)
GET / PUT	/roles/:id/permissions	role.read / role_permission.bind	讀取 / 覆寫功能權限
GET / PUT	/roles/:id/menus	role.read / role_menu.bind	讀取 / 覆寫選單可見性
GET / PUT	/roles/:id/data-scope	role.read / role.data_scope.set	讀取 / 設定資料範圍

情境	訊息	呈現方式
新增 / 更新 / 刪除成功	已新增角色 / 已更新角色 / 已刪除角色	浮動提示
綁定儲存成功	已更新綁定	浮動提示
資料範圍設定成功	已設定資料範圍	浮動提示
角色代碼重複	角色代碼已存在	浮動提示
綁定已被他人修改	伺服器上的綁定已變更，已保留你的草稿。 請捨棄草稿並重新載入目前綁定後再儲存。	對話框內提示
勾選了自己沒有的權限	不能授予你自己沒有的權限	浮動提示
角色仍有成員	此角色仍有使用者持有，請先解除指派	浮動提示
批次含受保護角色	未套用任何變更。選取項目包含不允許修改的角色。	浮動提示

5.6 權限管理 (Permissions)

維護權限目錄。每一個權限鍵對應一類 API 動作，格式為 `<resource>.<action>`，例如 `user.read`。絕大多數權限鍵由程式宣告、啟動時自動建立；本頁主要用於檢視、補充說明、停用，以及為下游業務建立自訂權限。



The screenshot shows a web interface for managing permissions. At the top, there's a title '權限' (Permissions) and a subtitle '共 34 筆 · 程式宣告的權限鍵由系統建立，不可刪除' (Total 34 items · Permission keys declared by the program are built by the system and cannot be deleted). On the right, there are buttons for '批次停用' (Batch Disable), '批次啟用' (Batch Enable), and '+ 新增' (Add). Below this is a table with columns: 'permission_key', 'action', 'resource_type', '狀態' (Status), and '說明' (Description). The table lists several permissions, most with a status of '啟用' (Enabled) in green, and one 'user.read' with a status of '停用' (Disabled) in grey. Each row has a checkbox on the left and a three-dot menu on the right. At the bottom, there's a pagination bar showing '第 1 / 2 頁' and buttons for '上一頁' (Previous), '第 1 / 2 頁', and '下一頁' (Next).

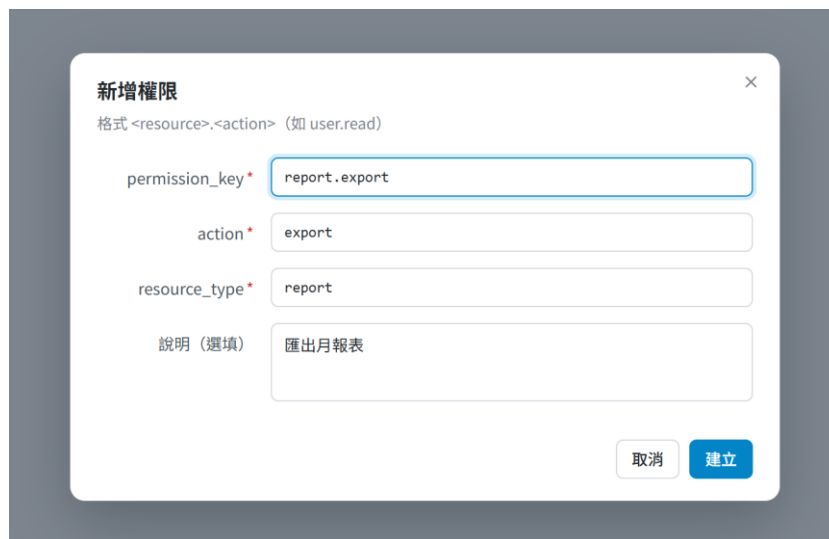
☐	permission_key	action	resource_type	狀態	說明	
☐	audit.read	read	audit	啟用	程式定義用途：檢視稽核紀錄與登入日誌	...
☐	dept.create	create	dept	啟用	程式定義用途：新增部門	...
☐	menu.read	read	menu	啟用	程式定義用途：檢視選單樹	...
☐	report.export	export	report	啟用	管理員描述：匯出月報表（自訂）	...
☐	role.data_scope.set	data_scope.set	role	啟用	程式定義用途：設定角色的資料範圍	...
☐	user.password.reset	password.reset	user	啟用	程式定義用途：重設其他使用者的密碼	...
☐	user.read	read	user	停用	程式定義用途：檢視使用者清單與明細 管理員描述：暫停對外開放	...

圖 5.6-1 權限清單

5.6.1 頁面顯示邏輯

- 清單依 `permission_key` 遞增排序，每頁 20 筆，包含已停用的權限。
- 欄位為 `permission_key`、`action`、`resource_type`、狀態（啟用 / 停用）與說明。說明分兩行：
「程式定義用途」來自程式宣告，不存於資料庫；「管理員描述」為管理者自行填寫的備註。
- 列操作為編輯（`permission.update`）與刪除（`permission.delete`）；工具列為新增與批次啟用停用。

5.6.2 新增與編輯



The screenshot shows a modal form titled '新增權限' (Add Permission) with a close button (X). Below the title is a subtitle '格式 <resource>.<action> (如 user.read)' (Format <resource>.<action> (e.g., user.read)). The form has four input fields: 'permission_key *' with the value 'report.export', 'action *' with the value 'export', 'resource_type *' with the value 'report', and '說明 (選填)' (Optional Description) with the value '匯出月報表'. At the bottom right, there are two buttons: '取消' (Cancel) and '建立' (Create).

圖 5.6-2 新增自訂權限

欄位	必填	規則	未通過時
permission_key	是 (新增)	格式為 <resource>.<action>，最長 160 字元；不得與未刪除的權限重複；建立後不可變更	格式錯誤或重複時回傳對應訊息
action	是	不可空白，最長 80 字元	「必填」
resource_type	是	不可空白，最長 80 字元	「必填」
說明	否	管理員描述	—
狀態	是 (編輯)	啟用或停用	—

停用的影響：停用的權限會立即從所有使用者的權限集合中移除（載入使用者時只取啟用的權限），等同對全體成員收回該能力。停用程式宣告的權限前，畫面應提示可能導致既有角色無法使用對應功能。

5.6.3 刪除

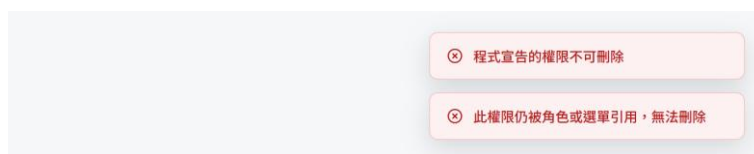


圖 5.6-3 刪除被阻擋

1. 程式宣告的權限不可刪除，回傳 409 DATA-003。
2. 仍被任何角色綁定，或被任何未刪除選單設為「所需權限」時不可刪除，回傳 409 DATA-003。
3. 通過檢查後採軟刪除。硬刪除僅超級管理員可透過 API 執行，並於交易內再次確認沒有任何引用。

5.6.4 權限目錄的來源

核心權限鍵與各模組宣告的權限鍵在啟動時合併成權限目錄：先驗證跨模組沒有重複、說明只描述自己宣告的鍵，再只補建資料庫中不存在的權限，不覆寫管理者修改過的狀態與描述，也不復活已被軟刪除的權限。路由使用的權限鍵若不存在於資料庫，系統拒絕啟動（見 4.3）。

5.6.5 介面與訊息

方法	路由	權限鍵	用途
GET	/permissions	permission.read	權限清單（附程式定義用途）
POST	/permissions	permission.create	新增自訂權限
PUT	/permissions/:id	permission.update	編輯權限
PUT	/permissions/batch-status	permission.update	批次啟用或停用
DELETE	/permissions/:id	permission.delete	刪除權限

情境	訊息	呈現方式
新增 / 更新 / 刪除成功	已新增權限 / 已更新權限 / 已刪除權限	浮動提示
權限鍵重複	權限鍵已存在	浮動提示
刪除程式宣告的權限	程式宣告的權限不可刪除	浮動提示
權限仍被引用	此權限仍被角色或選單引用，無法刪除	浮動提示

5.7 選單管理（Menus）

維護側欄選單樹與頁面路由。選單分為三種類型：目錄（M）用於分組；選單（C）是一個頁面，須有路由與頁面元件；按鈕（F）代表頁面內的操作點。每個選單可設定「所需權限」，沒有該權限的使用者即使角色綁定了這個選單也看不到。

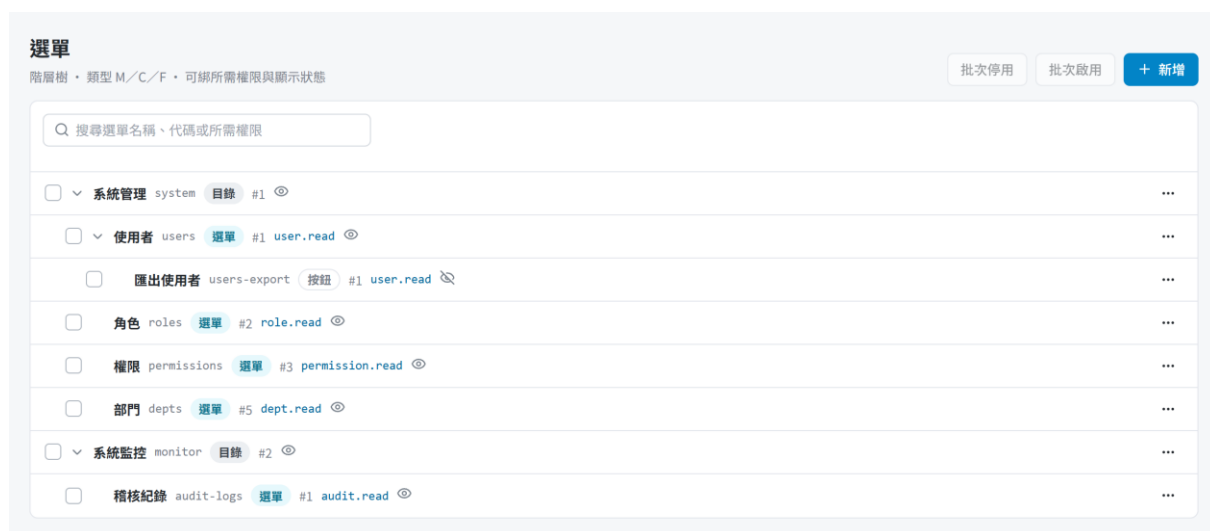


圖 5.7-1 選單樹

5.7.1 頁面顯示邏輯

- 以 GET /menus/tree 載入所有未刪除的選單（含隱藏與停用），依排序、選單代碼遞增排列；上層不存在的節點視為根節點。
- 每列顯示標題、選單代碼、類型、排序、所需權限與是否顯示；搜尋框同時比對標題、代碼與所需權限，符合的節點保留其上層路徑，搜尋時全部展開。
- 列操作為新增子選單、編輯、刪除，依 menu.create、menu.update、menu.delete 顯示。

5.7.2 新增與編輯

新增子選單

上層：系統管理

menu_key *

reports

標題 *

報表中心

類型

選單 (C)

route_path *

/system/reports

頁面元件 *

system/reports

圖示

ScrollText

排序

6

所需權限 (選填)

report.read · 檢視報表

選單可見性與功能權限分開設定；勾選選單不會授予功能權限。

☒ 在選單中顯示 (visible)

取消

建立

圖 5.7-2 新增頁面型選單

欄位	必填	規則	未通過時
menu_key	是 (新增)	不可空白，最長 120 字元；不得與未刪除的選單重複，且不可使用核心保留的代碼；建立後不可變更	重複時回傳「選單代碼已存在」
標題	是	不可空白，最長 120 字元	「必填」
類型	是	M、C、F 其中之一；畫面預設選 C	—
route_path	C 時必填	最長 255 字元	「頁面型選單必須填寫路由路徑」
頁面元件	C 時必填	只能選擇前端已註冊的頁面元件	「頁面型選單必須選擇頁面元件」
圖示	否	只能選擇側欄支援的圖示	—
排序	否	非負整數	欄位下方顯示驗證訊息
所需權限	否	須為權限目錄中存在的權限鍵	「所需權限不存在」
在選單中顯示	—	預設勾選	—

頁面型的必填規則前後端各檢查一次。頁面元件下拉的選項由前端自動掃描已註冊的頁面產生；資料庫中存有、但此版本沒有的元件，以「此版本沒有這個頁面元件」標示，避免建立點不進去的選單。編輯時可修改上述欄位與狀態，選單代碼與上層不可變更。

5.7.3 刪除

- 仍有子選單時不可刪除，回傳 409 DATA-003；確認文案為「有子選單時後端會擋下」。
- 通過檢查後採軟刪除；角色對此選單的既有綁定保留，在角色的選單設定中顯示為「無法取得的既有選單」，可明確取消。
- 硬刪除僅超級管理員可透過 API 執行，且須先解除所有角色綁定。

5.7.4 側欄選單的產生

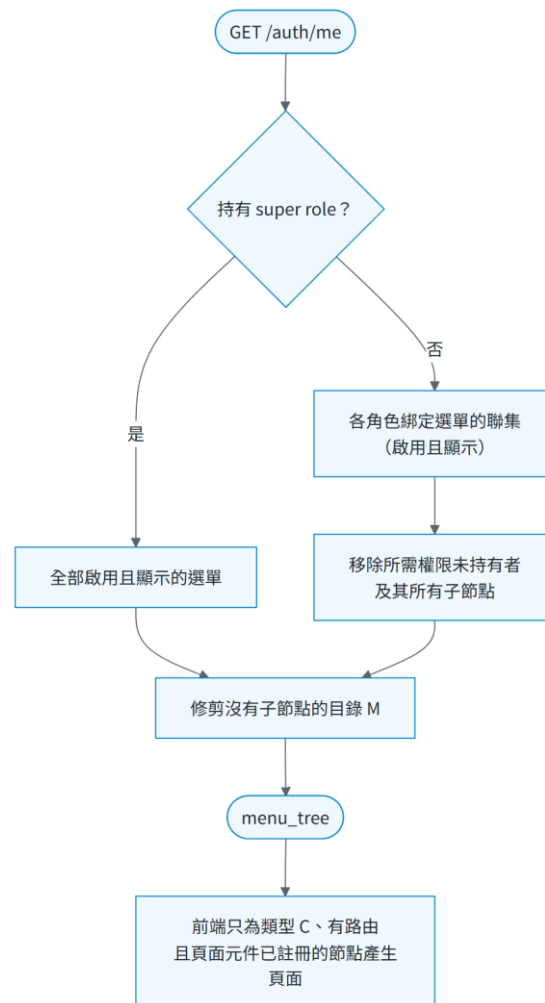


圖 5.7-3 由 /auth/me 產生側欄選單

1. 持有 super role 者取得所有啟用且顯示的選單。
2. 其他使用者取得各角色綁定選單的聯集，只保留啟用且顯示者。
3. 移除所需權限未持有的選單，連同其所有子節點。
4. 修剪已沒有子節點的目錄。
5. 前端只為類型為 C、有路由且頁面元件已註冊的節點產生路由，其餘節點只作為分組。

5.7.5 介面與訊息

方法	路由	權限鍵	用途
GET	/menus/tree	menu.read	選單樹
POST	/menus	menu.create	新增選單
PUT	/menus/:id	menu.update	編輯選單
PUT	/menus/batch-status	menu.update	批次啟用或停用
DELETE	/menus/:id	menu.delete	刪除選單

情境	訊息	呈現方式
新增 / 更新 / 刪除成功	已新增選單 / 已更新選單 / 已刪除選單	浮動提示
選單代碼重複	選單代碼已存在	浮動提示
仍有子選單	此選單仍有子選單，無法刪除	浮動提示
所需權限不存在	所需權限不存在	浮動提示

5.8 線上使用者（Online Sessions）

檢視目前有效的登入連線，必要時強制下線，例如帳號疑似外洩或人員離職時立即切斷對方的存取。

線上使用者				
共 4 個活躍連線 · 強制下線會立即失效該連線的 token（自己的當前連線不可下線）				
使用者	IP	位置	登入時間	User-Agent
系統管理員 @admin 目前連線	10.0.12.8	臺灣 臺北市	2026-09-24 09:12:40	Chrome 140 / Windows
陳怡安 @alice.chen	10.0.14.22	臺灣 新北市	2026-09-24 08:55:02	Edge 140 / Windows
林柏宏 @bob.lin	172.16.3.41	臺灣 臺中市	2026-09-23 18:21:47	Firefox 142 / macOS
林柏宏 @bob.lin	172.16.3.57	臺灣 臺中市	2026-09-23 09:02:11	Safari 18 / iOS
第 1 / 1 頁				
上一頁 第 1 / 1 頁 下一頁				

圖 5.8-1 線上使用者

5.8.1 頁面顯示邏輯與查詢

- GET /online-sessions 列出未撤銷且未過期的 session，依登入時間由新到舊排列，每頁 20 筆。
- 欄位為使用者（顯示名稱與帳號）、IP、位置（依 IP 解析）、登入時間與 User-Agent；操作者自己目前使用的連線標示「目前連線」。
- token 雜湊不會出現在回應中；是否為目前連線由後端比對後以布林值回傳。
- 沒有 session.revoke 時不顯示操作欄。

5.8.2 強制下線



圖 5.8-2 強制下線確認

- 1. 不可對自己目前的連線執行，按鈕停用；後端同樣拒絕，回傳 409 DATA-003，並提示改用登出。
- 2. 對超級管理員的連線強制下線時，操作者須為超級管理員。
- 3. 將該 session 寫入撤銷時間；對方的下一個請求即回傳 401 AUTH-003 並被導回登入頁。
- 4. 寫入 session.revoke 管理稽核，記錄被下線的使用者。

5.8.3 介面與訊息

方法	路由	權限鍵	用途
GET	/online-sessions	session.read	有效連線清單
DELETE	/online-sessions/:id	session.revoke	強制下線

情境	訊息	呈現方式
強制下線成功	已強制下線	浮動提示，並重新整理表格
連線已結束	此連線已結束或不存在	浮動提示
對自己的連線操作	不能讓目前的連線下線，請使用登出	浮動提示

5.9 稽核紀錄（Audit Logs）

稽核紀錄是治理證據：登入、授權拒絕與所有管理異動都寫入 sys_audit_log，並以 request_id 串起同一次請求的所有事件。本頁提供查詢、欄位變更明細與匯出。

稽核紀錄

共 1,284 筆 · 治理證據

🗑 批次刪除

📄 匯出

查詢

操作者

事件類型

資源類型

動作

使用者 UUID

全部

role

結果

起

訖

套用篩選

清除

全部

2026-09-24 00:00

2026-09-25 00:00

☐	時間	類型	動作	結果	資源	request_id	訊息／原因碼	
☐	2026-09-24 09:31:05	management	role_permission.bind	success	role_permission:7c1e09a2	3f2a9c1d8e4b...	-	變更
☐	2026-09-24 09:28:44	authz	user.delete	failure	-	a91c0e77b2d5...	AUTHZ-001	
☐	2026-09-24 09:20:13	management	user.update	success	user:5d0b44e1	c07d31aa9f60...	-	變更
☐	2026-09-24 09:12:40	auth	login	success	-	e4b8f2c60a17...	-	
☐	2026-09-24 09:05:57	authz	role.update	failure	-	1b6f3d9e05ca...	PDP-001	
☐	2026-09-24 08:55:02	auth	login	failure	-	f93a0b2e7d14...	AUTH-001	

第 1 / 65 頁

上一頁

第 1 / 65 頁

下一頁

圖 5.9-1 稽核紀錄與篩選條件

5.9.1 事件類型

event_type	寫入時機	典型 action
auth	登入（成功與失敗）、登出、變更密碼	login、logout、password.change
authz	授權拒絕與 fail-closed；允許不寫入	被拒絕的權限鍵，例如 user.delete
management	所有管理異動	user.update、role_permission.bind、session.revoke 等

所有紀錄都包含事件類型、動作、結果、request_id、IP 與 User-Agent；其餘欄位依事件類型記錄：

event_type	另外記錄的欄位
auth	操作者（帳號不存在時為空）、原因碼、IP 解析出的位置
authz	操作者、被拒絕的權限鍵、決策（deny）、decision_source、原因碼
management	操作者、資源類型與 id、原因碼（失敗時）；需要時附事件摘要（metadata）

事件摘要不得包含明文憑證、未清理的輸入或可重建業務資料的內容。

5.9.2 頁面顯示邏輯與查詢

- 快查：貼上 request_id 查詢整串請求；點清單中的 request_id 也會以此值篩選並清除其他條件。
- 篩選條件為操作者（使用者 UUID）、事件類型、資源類型、動作、結果與起訖時間；按「套用篩選」才生效並回到第 1 頁。起訖為左閉右開區間。
- 清單依時間由新到舊排列，每頁 20 筆；時間依個人偏好格式顯示。管理類事件提供「變更」連結。
- 稽核資料不套用資料範圍：稽核人員需要看到完整證據。擁有 audit.read 即可查詢全部。

欄位	必填	規則	未通過時
操作者	否	須為 UUID	欄位下方提示「請輸入有效的使用者 UUID」
起 / 訖	否	日期時間，起不得晚於訖	欄位下方顯示驗證訊息

5.9.3 變更明細



圖 5.9-2 變更明細

以 `request_id` 查詢 `sys_audit_change`，列出該次操作每個欄位的變更前後值。密碼、密碼雜湊、`token` 等敏感欄位永不記錄。

5.9.4 匯出與刪除



圖 5.9-3 刪除稽核紀錄確認

- **匯出：**依目前套用的篩選條件匯出 `xlsx` (上限 200,000 筆)，欄位為時間、事件類型、動作、結果、操作者、IP、位置、原因碼、訊息、`request_id`。匯出本身寫入稽核；失敗時顯示失敗提示。
- **刪除：**需 `audit.delete`，一次最多 200 筆，執行前必須確認。刪除的筆數與範圍另寫一筆管理稽核，使刪除證據這件事本身也留有證據。

5.9.5 介面與訊息

方法	路由	權限鍵	用途
GET	/audit-logs	audit.read	稽核清單
GET	/audit-logs/export	audit.read	匯出稽核
GET	/audit-changes?request_id=	audit.read	欄位變更明細
POST	/audit-logs/batch-delete	audit.delete	批次刪除稽核

情境	訊息	呈現方式
刪除成功	已刪除	浮動提示
無符合資料	沒有符合的紀錄	表格內空狀態
沒有欄位變更	沒有欄位變更紀錄	對話框內空狀態
匯出失敗	匯出失敗，請稍後再試	浮動提示

5.10 登入日誌（Login Log）

帳號異常時最先查看的頁面。資料來源是稽核紀錄中事件類型為 `auth` 的事件，因此與稽核紀錄共用 `audit.read`，不另設權限。

登入日誌					
共 412 筆，帳號異常時先看這裡的登入 IP 與位置					
使用者 UUID 全部結果 查詢					
時間	動作	結果	IP	位置	User-Agent
2026-09-24 09:12:40	login	成功	10.0.12.8	臺灣 臺北市	Chrome 140 / Windows
2026-09-24 08:57:19	password.change	成功	10.0.14.22	臺灣 新北市	Edge 140 / Windows
2026-09-24 08:55:02	login	失敗	10.0.14.22	臺灣 新北市	Edge 140 / Windows
2026-09-23 18:40:03	logout	成功	172.16.3.41	臺灣 臺中市	Firefox 142 / macOS
2026-09-23 18:21:47	login	成功	172.16.3.41	臺灣 臺中市	Firefox 142 / macOS
第 1 / 21 頁 上一頁 第 1 / 21 頁 下一頁					

圖 5.10-1 登入日誌

- 以固定條件 `event_type=auth` 呼叫 `GET /audit-logs`，可再依操作者與結果（成功 / 失敗）篩選，每頁 20 筆。
- 欄位為時間、動作（登入、登出、變更密碼）、結果、IP、位置與 User-Agent。
- 帳號不存在的登入失敗沒有操作者，只能以時間與 IP 追查；搭配 5.1.3 的失敗鎖定與 IP 限流判斷是否為暴力嘗試。

6 資料存取對象

本章彙整權限管理功能區所存取的資料表，供建置環境與權限盤點時參考。所有主鍵皆為應用程式產生的 UUID；多數資料表具備建立與更新時間、建立者與更新者欄位，並以 `deleted_at` 軟刪除，唯一鍵只在未刪除的資料間成立。PostgreSQL、MySQL 與 SQL Server 使用同一套結構，由各方言的 migration 維護。

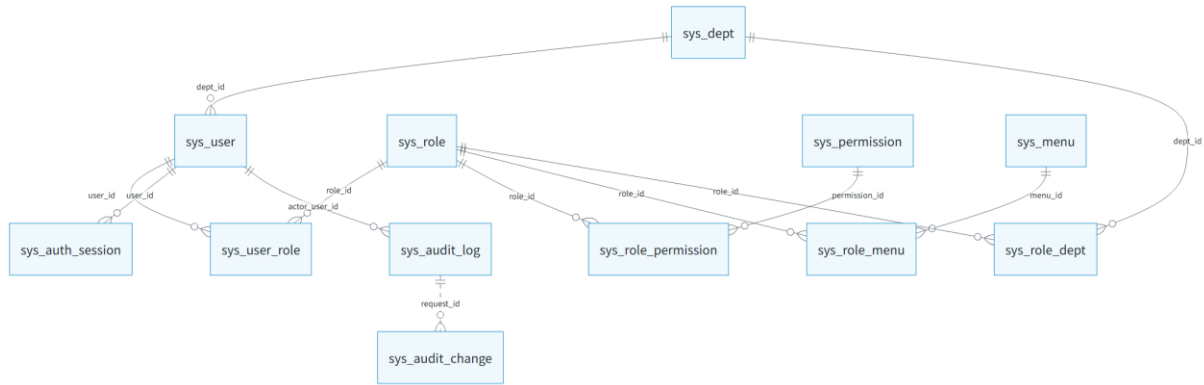


圖 6-1 資料表關聯

資料表	用途	關鍵欄位與限制	章節
sys_user	使用者帳號	username、email 唯一；status (active / disabled / locked)；dept_id；force_password_change；is_system	5.3
sys_dept	部門樹	parent_id 自我參照；ancestors 祖先路徑；dept_key 唯一	5.4
sys_role	角色	role_key 唯一；data_scope 1~5；is_super_role 必為 is_system；三個 revision	5.5
sys_permission	權限目錄	permission_key 唯一；action、resource_type、status	5.6
sys_menu	選單樹	parent_id 自我參照；menu_key 唯一；menu_type 限 M / C / F；required_permission_key	5.7
sys_user_role	使用者與角色	主鍵 (使用者, 角色)；記錄指派者與時間	5.3
sys_role_permission	角色與權限	主鍵 (角色, 權限)；權限端不連鎖刪除	5.5
sys_role_menu	角色與選單	主鍵 (角色, 選單)；選單端不連鎖刪除	5.5
sys_role_dept	自訂資料範圍	主鍵 (角色, 部門)；只在 data_scope=2 時使用	5.5
sys_auth_session	登入 session	token_hash 唯一 (SHA-256)；expires_at、revoked_at；只撤銷不修改	5.1、5.8
sys_user_preference	個人偏好	主鍵為使用者；prefs 為 JSON	5.2
sys_audit_log	稽核紀錄	只新增不修改；event_type、decision_source、reason_code、request_id、metadata	5.9、5.10
sys_audit_change	欄位變更明細	request_id、欄位、變更前後值；不記錄敏感欄位	5.9

7 業務規則與驗證

編號	規則	適用
BR-01	後端是唯一的安全邊界；前端的權限判斷只影響畫面呈現，每一支 API 都由後端重新授權。	全區
BR-02	每條路由必須登記為公開、僅需登入或需權限鍵；未登記或權限鍵不存在時系統拒絕啟動。	全區
BR-03	無法取得明確的允許決策時一律拒絕 (PDP 故障、逾時、授權資料不一致)。	全區

編號	規則	適用
BR-04	資料範圍由唯一檢查點強制注入；範圍外的資料視同不存在。	全區
BR-05	有效資料範圍依本次權限鍵計算，只取授予該權限鍵的角色中最寬的範圍。	全區
BR-06	前端阻擋的條件，後端必須重複檢查一次。	全區
BR-07	系統必須至少保留一位啟用中的超級管理員；任何會讓人數歸零的操作整筆回滾。	使用者、角色
BR-08	只有超級管理員能管理持有 super role 的帳號，以及指派或移除 super role 與系統角色。	使用者
BR-09	不可刪除、停用或重設自己的帳號；自己的密碼以「變更密碼」處理。	使用者
BR-10	非超級管理員不能授予自己沒有的權限，設定的資料範圍也不能寬於自己的範圍。	角色
BR-11	選單可見性與功能權限分開；綁定選單不授予任何 API 能力。	角色、選單
BR-12	角色綁定以 revision 樂觀鎖保護，過期時不得覆寫。	角色
BR-13	有子節點的部門與選單不可刪除；仍有成員的部門、仍有持有者的角色、仍被引用的權限不可刪除。	部門、角色、權限、選單
BR-14	程式宣告的權限不可刪除；系統角色與 super role 不可刪除或停用。	角色、權限
BR-15	新建或重設密碼的帳號必須在下次登入時變更密碼，變更前只能使用變更密碼、取得身分與登出。	登入、使用者
BR-16	密碼只保存 Argon2id 雜湊；token 只保存 SHA-256 雜湊；臨時密碼只交付一次。	登入、使用者
BR-17	重設密碼撤銷目標的所有 session；變更自己的密碼撤銷其他 session。	使用者、個人設定
BR-18	登入失敗一律回傳相同訊息，不揭露帳號是否存在。	登入
BR-19	拒絕與異動都寫入稽核，並能區分策略拒絕與系統故障。	全區

8 例外處理

情境	處理方式
輸入參數無法解析	回傳 400 與可理解的訊息，不讓解析錯誤直接向外拋出
session 過期或已撤銷	回傳 401；前端清除本機 token 並導回登入頁
權限不足	回傳 403；前端顯示提示但不登出使用者
PDP 無法連線、逾時或內部錯誤	fail-closed 拒絕，回傳 503 / 500，稽核標記 decision_source
資料不存在或不在資料範圍	回傳 404 DATA-001，兩者不區分
唯一鍵衝突	回傳 409 DATA-002，提示對應欄位
並行修改綁定	回傳 409 DATA-005，保留草稿並提示重新載入
系統或資料庫錯誤	記錄伺服器端日誌，回應只帶原因碼與 request_id，不洩漏 SQL、連線資訊或例外內容
稽核寫入失敗	一般管理稽核記錄錯誤後不中斷請求；臨時憑證的交付稽核失敗時不交付憑證
查無資料	回傳空集合與總筆數 0，前端顯示空狀態，不視為錯誤

9 使用者與權限

9.1 典型角色

角色	資料範圍	典型權限
超級管理員 (super_admin)	全部	系統角色，天生具備全部權限與選單；不可刪除或停用
權限管理員	全部	使用者、角色、權限、選單、部門的讀寫與綁定
部門主管	本部門及以下	user.read、user.update、user_role.bind、dept.read
稽核人員	全部	audit.read、session.read；不授予任何寫入類權限
一般使用者	僅本人	依業務模組授權

9.2 權限鍵目錄

以下為權限管理功能區使用的權限鍵，皆由程式宣告，不可刪除。說明即畫面上的「程式定義用途」。

權限鍵	說明
user.read	檢視使用者帳號；僅限資料範圍內的部門
user.create	建立使用者帳號，含初始密碼與所屬部門；角色另由 user_role.bind 指派
user.update	修改使用者的名稱、部門、狀態等欄位
user.delete	刪除使用者帳號；系統帳號與最後一位超級管理員受保護
user_role.bind	調整使用者持有的角色，決定其可用權限

權限鍵	說明
user.password.reset	代使用者重設密碼；可由伺服器產生臨時密碼或自行指定，兩者都要求對方於首次登入時更換
role.read	檢視角色及其綁定摘要
role.create	建立角色
role.update	修改角色的名稱、描述與排序；受保護角色的識別欄位不可變更
role.delete	刪除角色；系統角色受保護
role_permission.bind	調整角色的功能權限，直接決定其成員能執行哪些操作
role_menu.bind	調整角色可見的選單；只影響可見度，不授予操作能力
role.data_scope.set	設定角色的資料範圍，決定其成員能看到哪些部門的資料
permission.read / create / update / delete	檢視權限目錄 / 建立自訂權限鍵 / 修改描述與狀態 / 刪除自訂權限
menu.read / create / update / delete	檢視選單樹 / 建立選單 / 修改標題、路由與所需權限 / 刪除選單
dept.read / create / update / delete	檢視部門樹 / 建立部門 / 修改名稱、上層與排序 / 刪除部門
audit.read	查詢稽核紀錄與登入日誌，包含操作者與變更前後值
audit.delete	刪除稽核紀錄
session.read / session.revoke	檢視線上連線 / 強制下線

- 每個 API 都必須以權限鍵保護，或明確標示為公開、僅需登入；未標示者系統拒絕啟動。
- 寫入類權限與讀取類權限分開，唯讀角色只授予 .read 權限。
- 操作者身分一律由後端自 session 取得，不由前端傳入。

10 非功能需求

面向	要求
安全	密碼以 Argon2id 雜湊 (t=3、m=64 MiB、p=4、16 位元組 salt) 並以常數時間比對；token 為 32 位元組隨機值，只保存 SHA-256；所有 SQL 參數化；含憑證的回應禁止快取；回應與錯誤訊息不得洩漏密碼、token、SQL 或例外內容；前端部署加上 CSP、HSTS 與 X-Frame-Options
Session	預設有效 24 小時，不滑動延長；登出、重設密碼、變更密碼與強制下線立即生效
防濫用	登入 IP 名單、IP 每分鐘嘗試上限、驗證碼、帳號失敗鎖定；寫入類 API 限流與防重送可由系統參數開關
可稽核	登入、授權拒絕與管理異動皆留下含操作者、時間、對象、IP 與 request_id 的紀錄；欄位變更記錄前後值
效能	清單一律伺服器端分頁 (每頁上限 100)；授權決策可選擇性快取；PDP 呼叫逾時 5 秒
相容性	資料庫支援 PostgreSQL、MySQL 與 SQL Server，同一套結構以各方言 migration 維護
可擴充	業務模組透過模組契約加入 migration、權限鍵、選單與路由，自動套用相同的授權與資料權限保護
在地化	介面預設繁體中文並支援英文；使用者可設定日期格式、時間制與時區
可維運	每個回應帶 request_id；提供健康檢查與就緒檢查端點；PDP 或資料庫不可用時回傳明確錯誤而非停滯