

01 使用者

Web 登入與密碼

從韌體 **5.9.47** 起，MES Gateway 的 Web 介面 (`http://<DUT-IP>/`) 強制需要登入。出廠時內建兩組預設帳號：**管理員** 與 **唯讀**，使用者首次登入後**請立刻更改 Token**。

01

預設帳號

韌體首次啟動 (或執行恢復原廠後第一次開機) 會自動建立兩組 Token：

角色	預設 Token	權限	說明
 管理員 (admin)	<code>change-me-admin</code>	<code>PERM_ADMIN</code> (2)	全部功能：編輯設定、規則、I/O 控制、OTA 更新等
 唯讀 (viewer)	<code>change-me-viewer</code>	<code>PERM_READONLY</code> (0)	只能查看 Dashboard / Config / Rules / Devices / Settings；所有寫入按鈕被 disable

 **必改：**上線前第一件事就是改掉這兩組預設值，否則任何同網段的人都能用 `change-me-admin` 完全控制設備。

02

登入步驟

1. 打開瀏覽器，輸入設備 IP (如 `http://192.168.51.77/`)
2. 第一次開或之前登出後，畫面中央會跳出  **登入 MES Gateway Modal**
3. 從下拉選擇 **權限級別**：
 - 「 管理員 (admin, 全部功能)」
 - 「 唯讀 (viewer, 只能查看)」
4. 在「Token 值」欄位輸入對應 token：
 - 出廠預設：`change-me-admin` 或 `change-me-viewer`
 - 自訂後請輸入新值
5. 按「登入」

登入成功後 Token 會存於瀏覽器的 `localStorage` (key 為 `opta_token`)，下次開同一個瀏覽器**不會再跳 modal**。

03

登出 + 帳戶 Badge

右上**管理區** (Header 最右側, 5.9.48+) 有三件式：

元素	說明
 語系切換器	自動 /  繁中 /  EN
 admin /  viewer 角色 badge	顯示目前登入身份；admin 紅點、viewer 眼睛圖示
 登出	點擊清除 localStorage + 頁面 reload + login modal 重新跳出

5.9.47 把登出放在側邊欄底部; **5.9.48 起改放右上 header** (更顯眼、與 user badge 一起)

04

修改預設 Token (必須做)

透過 API 改

```
BASH
# 改 admin token (index 0)
curl -X POST http://192.168.51.77/api/tokens \
  -H "Authorization: Bearer change-me-admin" \
  -H "Content-Type: application/json" \
  -d '{"index":0,"value":"<your-new-strong-admin-token>","permission":2,"name":"'

# 改 viewer token (index 1)
curl -X POST http://192.168.51.77/api/tokens \
  -H "Authorization: Bearer change-me-admin" \
  -H "Content-Type: application/json" \
  -d '{"index":1,"value":"<your-new-strong-viewer-token>","permission":0,"name":"'

# 確認
curl -H "Authorization: Bearer <your-new-strong-admin-token>" \
  http://192.168.51.77/api/tokens
```

Token 字元規則: 4 ~ 31 字元, 建議 16 字元以上隨機字串 (如 `openssl rand -hex 16`)

透過 Web UI 改 (規劃中)

Settings → **使用者管理** 區塊 (admin only) — 待 sprint-28 補上 UI (FR-A5-25 follow-up)。

權限級別說明

韌體層 `TokenManager.h` 定義三級：

級別	數 值	限制
<code>PERM_READONLY</code>	0	只能 GET，所有 POST/DELETE/PUT 回 401
<code>PERM_CONTROL</code>	1	可 I/O 控制 (POST <code>/api/io/do</code>) 但不能改 config/rules (保留中，目前 boot 不會 seed)
<code>PERM_ADMIN</code>	2	全部功能

實作層：`tokenManager.hasPermission(actual, required)` 用 `actual >= required` 比較，所以 admin 可以做 readonly 的事，但 viewer 不能做 admin 的事。

目前並非所有 endpoint 都有 `checkAuth()` 檢查 (部分留作後續強化) — 但已上 auth 的高敏感路徑 (license reset、tcpio clear、rules clear、tokens 管理) 都正確擋住。

新增其他 Token

最多可有 4 組 token (`MAX_TOKENS=4` in `TokenManager.h`)。例如新增一組 control 等級 token 給機器人 / 自動化測試：

```
curl -X POST http://192.168.51.77/api/tokens \
  -H "Authorization: Bearer <your-admin-token>" \
  -H "Content-Type: application/json" \
  -d '{"value":"automation-bot-token","permission":1,"name":"playwright"}'
```

不帶 `index` 就是「新增到末尾」；slot 滿 (4 組) 時回 409。

07

刪除 Token

```
curl -X DELETE -H "Authorization: Bearer <your-admin-token>" \
  "http://192.168.51.77/api/tokens?index=2"
```

防呆：不能刪除最後一個 ADMIN token (避免設備永遠無法管理)。回 400 `Cannot delete (out of range or last admin)`。

08

API endpoint 一覽

Method	Path	權限	說明
GET	<code>/api/tokens</code>	ADMIN	列所有 token (value 顯示前 4 + <code>****</code> + 後 4)
POST	<code>/api/tokens</code>	ADMIN	新增 / 更新 token, body: <code>{value, permission, name, enabled, index?}</code>
DELETE	<code>/api/tokens?index=N</code>	ADMIN	刪除 token (防最後一個 admin)

常見問題

Q1: 我忘記 admin token 了怎麼辦？

走「恢復原廠」流程 (Settings → 維護操作 → 恢復原廠) — 設備會回到出廠 baseline，重啟後 token 自動 reseed 為 `change-me-admin` / `change-me-viewer`。

Q2: Token 是明文傳輸嗎？

是。韌體 HTTP server 不支援 TLS，所以 `Authorization: Bearer xxx` 在區網中是明文。建議：

- 設備放在受控網段
- 不要把 admin token 寫進公開腳本
- 高敏感場景考慮在前面加 reverse proxy (如 nginx) 走 HTTPS (5.9.47 韌體可外連 cloud HTTPS，但本地 server 仍是 HTTP)

Q3: Playwright 測試怎麼帶 token？

```
const ADMIN_AUTH = { headers: { Authorization: 'Bearer <your-admin-token>' } };
const res = await request.get('/api/system', ADMIN_AUTH);
```

JS

或用 `BASE_URL=http://...` + `localStorage.setItem('opta_token', '<token>')` 在 `page.goto` 前注入。

出貨清理

出貨清理流程**不會 reset token** (避免客戶重啟後找不到帳號)。出貨前 SOP 必須：

1. 確認 admin / viewer token 已被改為客戶指定值 (或讓客戶第一次登入後自己改)
2. 把預設 token `change-me-admin` / `change-me-viewer` 列入 SOP「上線後立即更換」清單
3. 文件交付時包含本檔 (`guide-web-login.md`)

若想出貨時 reset token 為預設, 可呼叫 `tokenManager.seedDefaults()` (內部 API, 目前無對外 endpoint, 可在 sprint-28 補 `POST /api/admin/tokens/reset`)

11

相關文件

- `src/TokenManager.h` / `src/TokenManager.cpp` — 韌體實作
- `src/ApiHandlers_Logic.cpp` `handleGetTokens` / `handlePostToken` / `handleDeleteToken` — API 實作
- `web/src/index.html` `#loginModal` — Login UI
- `web/src/app.js` `_apiToken` / `submitLogin()` / `logout()` — 認證邏輯