

Config Server 部署

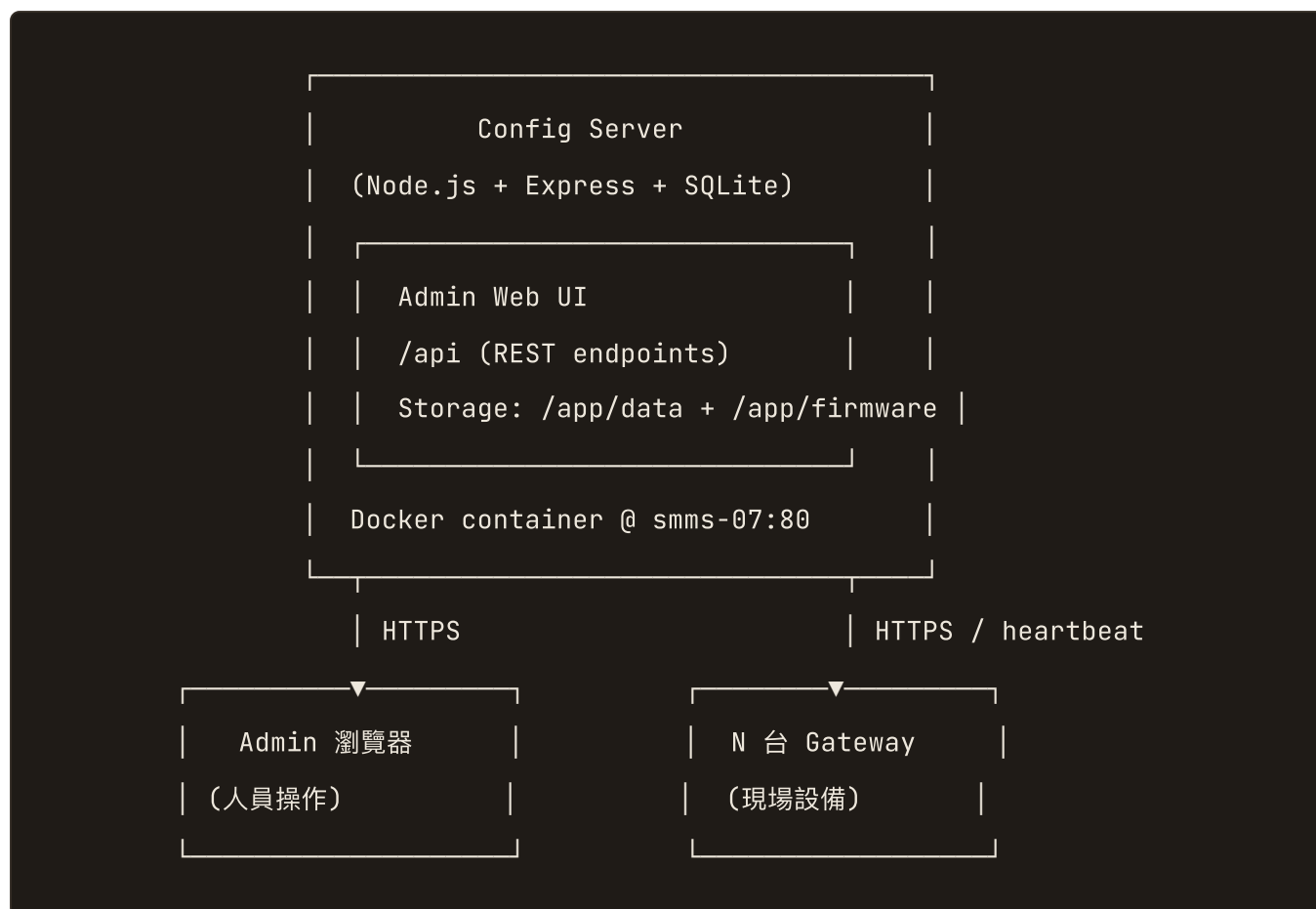
更新於 Wed May 06 2026 08:00:00 GMT+0800 (台北標準時間)

適用版本: config-server v1.x (與韌體 v5.9.63 同步)

適用對象: 系統管理員、後端維運、SaaS 平台管理者

雲端 Config Server 是管理多台 MES I/O Gateway 的中央後台，提供設備清冊、授權發放、韌體倉庫、設定備份、遠端 OTA 等功能。本手冊涵蓋日常 admin 操作與部署維護。

1. 系統定位與架構



核心責任：

- **設備管理**：認領、清冊、刪除、解除授權
- **授權**：License 簽發、撤銷、續期
- **韌體倉庫**：上傳 .bin、版本歷史、發起遠端 OTA
- **設定備份**：每台 Gateway 上傳的 config.json 快照保存(含 diff 比對)
- **MQTT bridge (選用)**：把現場 IO 資料中繼到上層系統

2. 部署環境

2.1 生產環境（已部署）

項目	值
主機	<code>smms-07</code> (10.0.0.9)
Docker container	<code>opta-config-server</code>
對外 URL	<code>https://config.metasource.tw</code> (透過反向 proxy + Let's Encrypt)
內網 URL	<code>http://10.0.0.9</code>
Image registry	<code>smmsregistry.azurecr.io/kc-opta-config-server:latest</code>
資料持久化	Docker volumes: <code>opta-data</code> (SQLite + backups)、 <code>opta-firmware</code> (.bin 倉庫)

2.2 開發環境

```
cd config-server
npm install
npm start # listen on :3000
```

預設 admin token: `admin-token` (生產環境應在 docker compose 設 `DEVICE_TOKEN=...`)

03

3. Admin 登入

打開 `http://10.0.0.9` 或 `https://config.metasource.tw`，會跳出登入框。

Admin 帳號 (v2.2.4+)：

- `admin@localhost` (cloud 用)、`local@localhost` (local 用)
- 初始密碼：`DEFAULT_ADMIN_PASSWORD` env 沒設 → docker log 印一次 random; 有設 → 那個值 (`.env.example` 預設 `smmsadmin`)
- 第一次登入後請走右上角  **改密碼** button (或 `POST /api/auth/password`) 改成強密碼

設備用 **API Token** (向下相容, 跟 admin 登入無關): env `DEVICE_TOKEN`, 預設 `admin-token` (生產環境必改強隨機字串)。

登入後右上角顯示角色徽章 +  改密碼 + 登出 button。

04

4. 主要頁面

頁面	用途
 設備 (Devices)	看所有 heartbeat 過的 Gateway, 刪除、解除授權
 授權 (Licenses)	簽發 / 撤銷 / 續期 License
 韌體 (Firmware)	上傳 .bin、看 changelog、部署到指定設備
 備份 (Backups)	看每台設備的 config 歷史快照、diff 比對

05

5. 設備管理 (Devices)

5.1 設備如何出現在清冊?

Gateway 啟用 Config Server 後, 每 30 秒送一次 heartbeat 到雲端, 雲端會自動建立或更新清冊 (WI-098 BUG-3)。無需手動 **claim**。

5.2 設備卡片資訊

每張設備卡片顯示：

- UID (H7 的 96-bit unique ID)
- 設備名稱 (用戶自訂)
- 狀態： online (最近 60s 有 heartbeat) /  offline
- 韌體版本
- 最後 heartbeat 時間
- 待派發 OTA (若有)

5.3 操作

動作	場景	注意
 部署 韌體	從韌體頁的「  部署」按鈕觸發，設備下次 heartbeat 自動取得	OTA 失敗會 fallback 到 DFU
 刪除 設備	設備永久退役、UID 衝突	不會清掉設備本機的 config，只是雲端清冊移除
 解除 授權	License 撤銷，下次 heartbeat 設備會收到並停用授權功能	Gateway 停用後僅可進入 AP 重新認領

大量設備清理：列表上方有「 清理離線 24h+ 設備」批次操作。

6. 授權管理 (Licenses)

6.1 授權狀態

狀態	意義
unseen	License 已產生但未被任何設備啟用
pending	設備首次連線，等 admin 核准
active	已核准，設備可正常運作
deactivated	被 admin 解除授權，設備進入限制模式
expired	已過期

6.2 操作

- 核准 (Approve): 把 unseen / pending → active
- 解除授權 (Deactivate): active → deactivated，設備下次 heartbeat 收到並停用控制功能
- 拒絕 (Reject): 把 unseen / pending 標記為拒絕
- 刪除 (Delete): 永久刪除 License 記錄 (任何狀態都可，含確認 modal)

詳見 WI-109 / WI-110 / WI-111 規格。

07

7. 韌體倉庫 (Firmware)

v5.9.59 起改成 card 排版 (WI-115d)：

```

| ★ Latest |
| v5.9.63 檔案 mes-gateway-v5.9.63-... | 大小 745 KB |
|          時間 2026/5/6 | SHA-256 fdedbbc8... |
|          部署 |
| ▶ v5.9.63 - 重大瘦身! 移除 dead code... |

```

```

| v5.9.62 ... |

```

7.1 上傳韌體

兩種方式：

1. **拖放區**：直接把 `.bin` 拖到頁面上方的 drop zone
2. **表單**：填版本號 + 選檔案 + 按「 上傳」

強制要求 (WI-114)：

- 必須夾帶 changelog (可在 release 腳本中用 `--changelog "..."` 帶入)
- changelog 至少 10 字元
- 透過 `X-Firmware-ChangeLog-B64` header 上傳 (base64 編碼, 支援多行 + 中文)

release 腳本 (建議方式)：

```
python3 scripts/release_firmware.py --upload http://10.0.0.9 \
--changelog "v5.9.x - 修補 ABC + 改善 DEF"
```

BASH

7.2 部署到設備

點某個版本卡片的「 部署」按鈕 → 選目標設備 → 確認。設備下次 heartbeat 取得指令, 用戶在 Gateway Web UI「設定 → OTA」按「 更新」開始下載。

⚠ **OTA size 限制** (v5.9.63 起) : binary > 770KB 時 Gateway 端 `/api/ota/trigger` 會回 413, 須改用 USB DFU 升級。Cloud admin UI 不會擋 (依設備行為), 但用戶會看到 toast 錯誤。

7.3 刪除韌體

- 點某個版本卡片的「」→ 確認 modal
- 若該版本正在派發給設備 (in-flight OTA), 會回 409 + 錯誤訊息「該版本正在派發給 N 台設備, 請先取消 OTA」

7.4 下載 .bin

點「」直接下載, 方便離線 USB DFU 燒錄。

08

8. 設定備份 (Backups)

每次 Gateway config.json 變動 (且啟用「每次設定儲存後自動推送」), 會推送一份快照到雲端。

8.1 看快照歷史

設備卡片點「 看備份」→ 列出所有快照, 每筆顯示:

- 時間戳
- 設定 CRC (hash)
- 變更摘要 (與前一版的 diff, 欄位級別)

8.2 還原

選某筆快照 → 點「 還原到此版本」→ 雲端會把該版本當作 pending config, 設備下次 heartbeat 拉回。

設定還原會覆蓋現場設定。執行前請通知現場人員。

09

9. 部署 / 升級流程

9.1 開發機 → 推送到生產

```
cd config-server
# 1. 打包 source (排除 node_modules 等)
tar -czf source.tar.gz --exclude=node_modules --exclude=.git --exclude=data .

# 2. SCP + SSH build + run (已包成 expect script)
expect upload_and_build.exp
```

BASH

`upload_and_build.exp` 做的事：

1. SCP `source.tar.gz` 到 `smms-07`
2. SSH 上去解壓
3. `docker build` 重 build image
4. `docker stop / rm / run` 換 container (用 `;` 串接 + `__DEPLOY_DONE__` sentinel 避免 race)
5. 確認 container `Up X seconds`

9.2 升級後 smoke test

```
curl -s -o /dev/null -w "Cloud HTTP %{http_code}\n" http://10.0.0.9/
curl -s -m 5 -H "Authorization: Bearer admin-token" http://10.0.0.9/api/firmware
curl -s -m 5 -H "Authorization: Bearer admin-token" http://10.0.0.9/api/devices
```

BASH

9.3 Volume 持久化

Volume	內容	何時備份
<code>opta-data</code>	SQLite (devices, licenses, backups history)	每週、重大設定變更前
<code>opta-firmware</code>	.bin 倉庫 + .json manifests	上傳新版本後

備份指令範例：

```
BASH
ssh smmsadmin@10.0.0.9 'sudo docker run --rm -v opta-data:/data -v $(pwd):/backu
```

10

10. 反向 Proxy + HTTPS

對外 `config.metasource.tw` 由前端 nginx 反向 proxy 到 `127.0.0.1:80`，由 Let's Encrypt 簽發憑證。Gateway 透過 RTC fallback 機制 (WI-100) 解決 H7 開機時間不準導致的 cert 驗證失敗。

設備端的 ISRG Root X1 cert 已內建在 firmware (`src/Cert.h`)。

11

11. API 端點速查

完整定義見 `docs/api/api-config-server.md`。常用：

Method	Path	用途
GET	<code>/api/devices</code>	設備清單
DELETE	<code>/api/admin/devices/:id</code>	刪除設備 (WI-110)
GET	<code>/api/firmware</code>	韌體列表 + changelog
POST	<code>/api/firmware/upload</code>	上傳 .bin (含 X-Firmware-Version + X-Firmware-Changelog-B64)
DELETE	<code>/api/admin/firmware/:filename</code>	刪除韌體 (WI-110)
POST	<code>/api/firmware/deploy/:deviceId</code>	派發 OTA
GET	<code>/api/firmware/download/:filename</code>	下載 bin
GET	<code>/api/licenses</code>	License 列表
POST	<code>/api/licenses/:id/approve</code>	核准
POST	<code>/api/licenses/:id/deactivate</code>	解除授權 (WI-110)
POST	<code>/api/licenses/:id/reject</code>	拒絕
DELETE	<code>/api/licenses/:id</code>	刪除
GET	<code>/api/snapshots/:deviceId</code>	設定備份歷史
POST	<code>/api/heartbeat</code>	Gateway 上傳 heartbeat (無需 admin token, 憑 license)

所有 admin 端點需 `Authorization: Bearer <admin-token>`。Gateway 自身的 heartbeat 用 `Authorization: Bearer <license-id>` (WI-098 + WI-065 中介層)。

12. 常見問題

12.1 設備在清冊上但 status 永遠 offline

可能原因：

- Gateway 端 Config Server URL 錯誤 / 未啟用「雲端 Server」
- Gateway 端網路斷線 (檢查 sysConn 狀態)
- License 已 deactivated (heartbeat 會被 reject)

排查：用 SSH 進 smms-07 看 docker logs：

```
ssh smmsadmin@10.0.0.9 'sudo docker logs --tail 100 opta-config-server'
```

BASH

找對應 UID 的 heartbeat 紀錄。

12.2 上傳韌體失敗

最常見：changelog 太短 (< 10 字元) → 回 400 + "Changelog too short". 修正後重 upload。

12.3 OTA 部署後設備一直在 pending

設備可能：

- heartbeat 還沒拉到 (30s 間隔)
- 用戶還沒在 Gateway Web UI 按「更新」(OTA-V2 是 user-triggered, 不是 push)
- 韌體 binary > 770KB → Gateway 端 OTA guard 回 413, 需改 USB DFU

12.4 Cloud UI 上的 firmware card 沒看到 changelog

舊版上傳的韌體 (WI-114 之前) 沒帶 changelog, 會顯示 (legacy: ...)。新版必填, 從 release_firmware.py 上傳會強制夾帶。

12.5 想砍掉某個 firmware 但 in-flight OTA

回 409 時，先在「設備」頁找到等待 OTA 的設備 → 取消 OTA → 再回韌體頁刪。

13

13. 維護清單

頻率	項目
每週	備份 <code>opta-data</code> volume + <code>opta-firmware</code> volume
每月	Docker image 重 pull / 升級基底
每季	清理 > 6 個月離線設備
每年	Let's Encrypt cert 自動續期確認 (certbot)

14

14. 相關文件

- `docs/guides/guide-config-server-cloud-deployment.md` — 從零部署到 Azure / 自架
- `docs/guides/guide-config-server-backup.md` — 備份還原 SOP
- `docs/api/api-config-server.md` — 完整 API 規格
- `docs/sprints/cards/sprint-27/wi-110-cloud-admin-p0-endpoints.md` — admin endpoints 設計
- `docs/sprints/cards/sprint-27/wi-111-cloud-admin-ui-buttons.md` — UI 按鈕設計
- `docs/sprints/cards/sprint-27/wi-114-firmware-changelog-system.md` — changelog 強制夾帶機制
- `docs/sprints/cards/sprint-27/wi-115-firmware-login-password-rename.md` — 帳號 / 密碼系統

若 Cloud Server 行為與本手冊不一致，請以 git log + 現行 source code 為準，並回頭修訂本手冊。