MERAK • 零信任隱形網路防護平台

Merak
零信任隱形網路平台
操作手冊



使用者與管理員操作指南

版本 v1.3
Merak Agent 1.4.7
更新日期 2026-11-19

坤安科技
KUNANSEC

目錄

文件資訊

關於本手冊

名詞與架構說明

第一篇　使用者操作篇

1. 帳號啟用指南

2. 安裝 Merak Agent 與設備認證

3. 登入 Agentless Portal（免安裝 Agent）

第二篇　管理員操作篇

建立網路節點（Node）

4. 節點（Node）建置

功能管理

5. 新增成員

6. 匯入成員資料

7. 停用與刪除成員

8. 建立組織

9. 建立新應用程式

10. 設定 Agentless 存取

稽核日誌

11. 查詢與匯出日誌

系統管理

12. 建立與管理角色

13. 建立新管理員

附錄

附錄 A：常見問題彙整

附錄 B：設備認證狀態對照表

本手冊說明 Merak 隱形網路平台（ZTNA）平台從使用者帳號啟用、Agent 安裝與設備認證、成員與管理員管理、應用資源與節點建置，到角色權限設定的完整操作流程。

文件資訊

項目	內容
文件名稱	Merak Console 操作手冊
適用產品	Merak Zero Trust（ZTNA）
管理主控台	`https://console.merak.kunansec.com`
Agentless 入口（Portal）	`https://portal.merak.kunansec.com/login`
Merak Agent 版本	1.4.7
版本	v1.3

關於本手冊

本手冊分為兩篇：

- **第一篇　使用者操作篇**：提供給收到邀請信、需要啟用帳號並安裝 Merak Agent 使用的一般使用者（成員）。
- **第二篇　管理員操作篇**：提供給在 Merak Console 進行成員、應用程式、節點、角色與管理員管理的系統管理員。

請依你的角色，直接前往對應章節。所有管理操作皆於管理主控台 `https://console.merak.kunansec.com` 進行。

名詞與架構說明

Merak 平台中有幾個容易混淆的概念，先在此釐清：

名詞	說明	對應對象
成員（Member）	透過 Merak 存取應用程式的一般使用者。由管理員新增或匯入，指派群組與可存取的應用程式。	一般使用者
管理員（Admin）	可登入 Merak Console 進行後台管理的帳號。由管理員建立，指派角色以決定其後台權限。	後台管理者

名詞	說明	對應對象
群組（Group）	一組存取政策，指派給成員以決定其可套用的存取規則（如 RD、業務部）。	套用於成員
角色（Role）	一組後台操作權限（以「資源 × 動作」定義），指派給管理員。	套用於管理員
應用程式（Application）	受 Merak 保護、供成員存取的服務（如 ERP）。	存取標的
節點（Node）	部署於地端主機的元件，負責建立安全網路存取通道。	地端部署
Merak Agent	安裝於使用者電腦、用來登入與建立連線的用戶端程式。	使用者端

> 簡言之：成員搭配群組與應用程式（誰能存取什麼服務）；管理員搭配角色（誰能在後台做什麼操作）；節點是讓服務可被安全存取的地端基礎設施；Merak Agent 是使用者連線的入口。

第一篇　使用者操作篇

本篇提供給一般使用者（成員）：帳號啟用、安裝 Merak Agent 與設備認證。

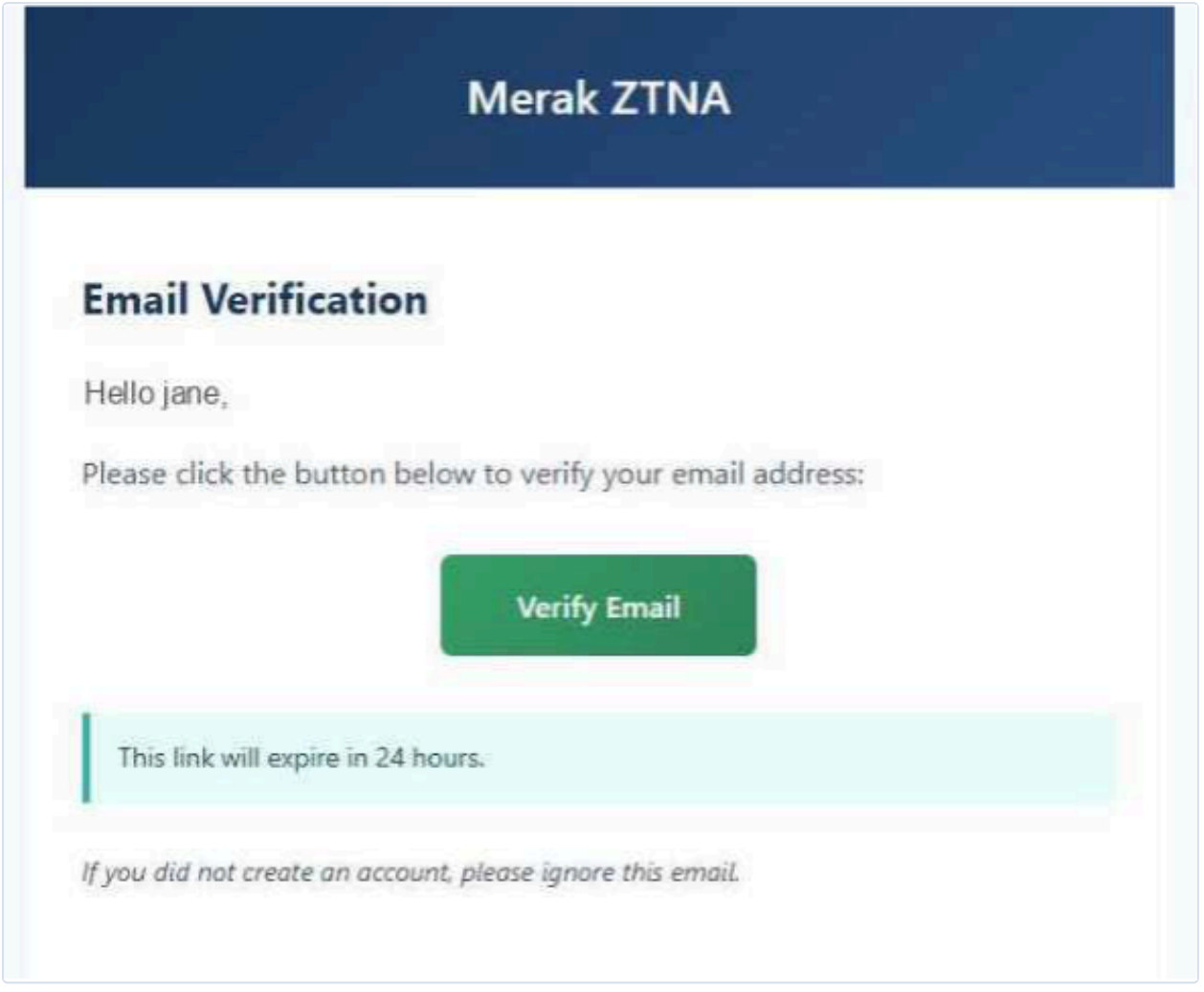
1. 帳號啟用指南

適用對象：收到 Merak ZTNA 邀請信的使用者。**需要準備**：可收信的電子郵件。

步驟 1　開啟邀請信

於信箱中找到主旨為「**Verify your Merak ZTNA email address**」的信件，點擊信中的驗證連結（**Verify Email**）。

- 若收件匣沒有，請檢查垃圾信匣。
- 信件寄件者為 `noreply@merak.kunansec.com`。



步驟 2　設定密碼

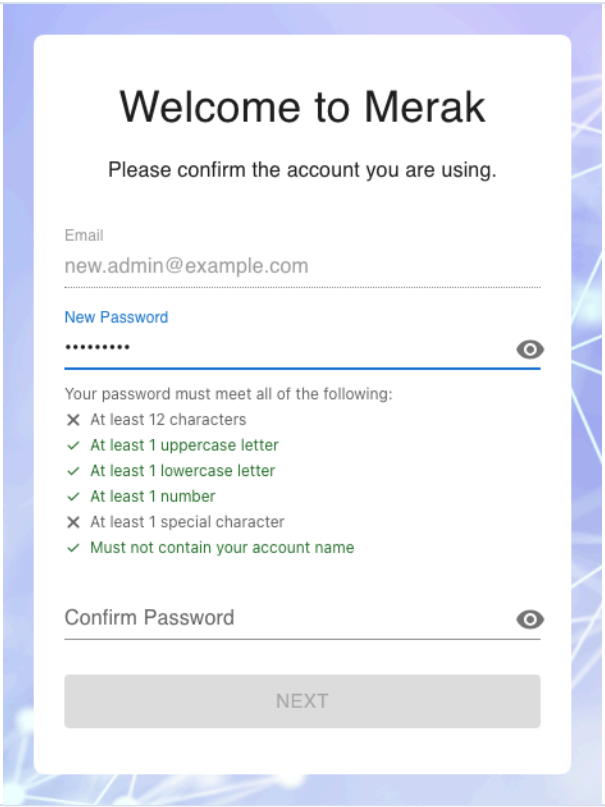
瀏覽器會開啟帳號啟用頁面，畫面上會顯示你的信箱與所屬組織名稱。依序填寫：

欄位	說明
新密碼	密碼必須同時符合以下全部條件（見下方）。
確認密碼	需與上方完全一致。

新密碼規則：

- 至少 12 個字元
- 至少 1 個大寫英文字母
- 至少 1 個小寫英文字母
- 至少 1 個數字
- 至少 1 個特殊符號
- 不可包含帳號名稱

填妥後點「**下一步**」。



步驟 3　確認啟用成功

出現「**帳號啟用成功**」畫面即完成。接著請開啟 **Merak Agent**，以此電子郵件與剛設定的密碼登入（安裝與登入步驟見〈2. 安裝 Merak Agent 與設備認證〉）。

> 【注意】啟用連結為一次性使用，完成後即失效；請勿轉發此連結給他人。

常見問題

狀況	處理方式
沒收到啟用信	檢查垃圾信匣；確認信箱正確；聯繫貴單位的 Merak 管理員重寄邀請。
點連結顯示「連結失效或已過期」	啟用連結有時效（24 小時），請聯繫管理員重寄。
兩次密碼不一致	重新輸入。
啟用成功但 Agent 登入失敗	確認帳號為信箱全名；確認 Agent 版本；仍失敗請聯繫管理員。
忘記密碼	於 Merak Agent 上點按「忘記密碼」進行重設。

2. 安裝 Merak Agent 與設備認證

適用對象：已完成帳號啟用的使用者（步驟 4 為管理員操作）。**用途**：在電腦端安裝 Merak Agent，完成設備註冊與認證，並啟動連線。

前置需求

安裝前請確認員工電腦符合下列條件。電腦只需要對外連得出去。

機器規格：

項目	需求
作業系統	Windows 10（2004 以上）或 Windows 11，64 位元
權限	安裝需本機系統管理員
防毒／EDR	放行 `Merak Agent.exe`、`merak-tunnel-service.exe`、`wintun.dll`

網路設定：

方向	來源 → 目的地	連接埠
出站	員工電腦 → `*.merak.kunansec.com`	TCP/443
出站	員工電腦 → 外部節點	TCP/3022

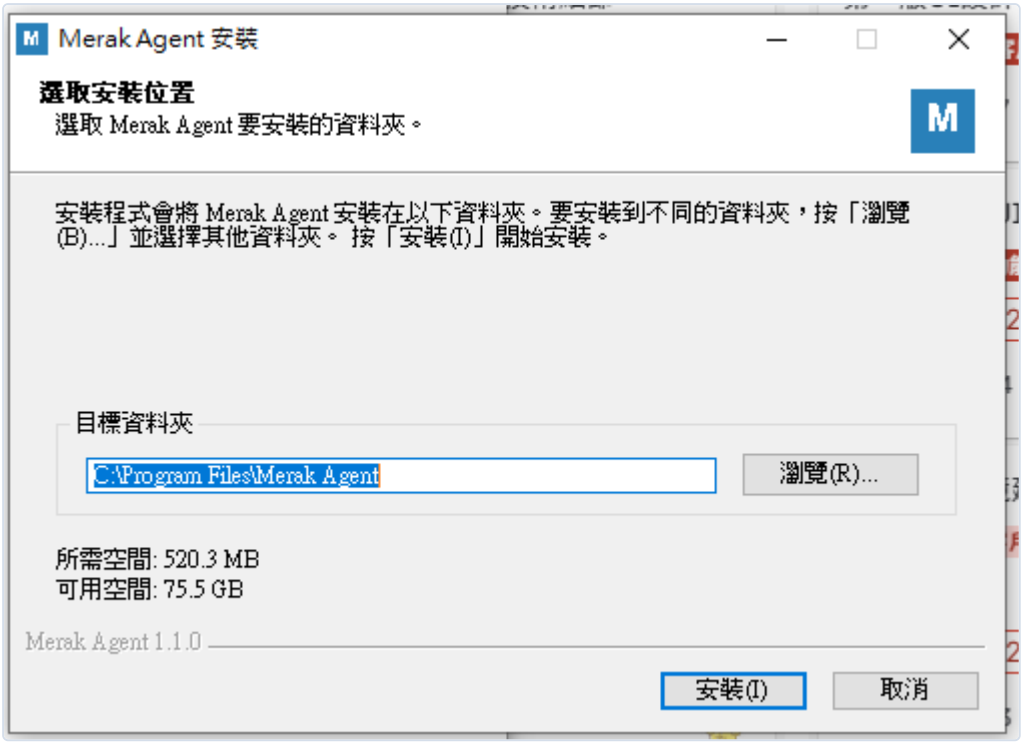
- 對外的 TCP 443 必須直接連線，不能經過 Proxy 伺服器，也不能做 HTTPS 內容檢查（SSL 解密）。員工電腦不需要任何 Inbound，在家或外出時也是同樣兩條規則。
- Agent 會使用 `100.64.0.0/10` 這段位址，請確認內網與其他 VPN 沒有用到。

步驟 1　安裝 Merak Agent

執行 Merak Agent 安裝程式後，依下列步驟完成安裝：

1. 進入「**選取安裝位置**」畫面，確認目標資料夾（預設為 `C:\Program Files\Merak Agent`）。如需變更，可點擊「**瀏覽(B)…**」選擇其他資料夾。
2. 確認所需空間與可用空間後，點擊「**安裝(I)**」開始安裝。
3. 安裝完成後進入「**即將完成安裝 Merak Agent**」畫面，確認已勾選「**☑ 執行 Merak Agent(R)**」（預設勾選）。
4. 點擊「**完成(F)**」關閉安裝程式並啟動 Merak Agent。

安裝資訊	內容
Agent 版本	Merak Agent 1.4.7
預設安裝路徑	`C:\Program Files\Merak Agent`

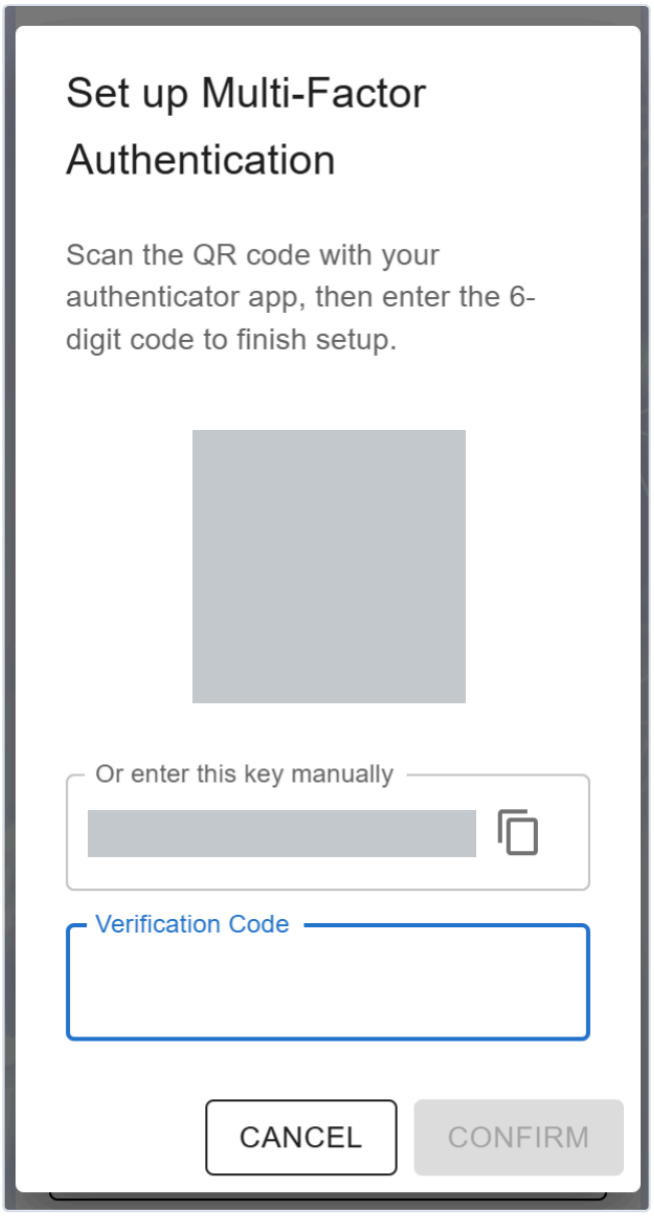


步驟 2　登入 Merak Agent

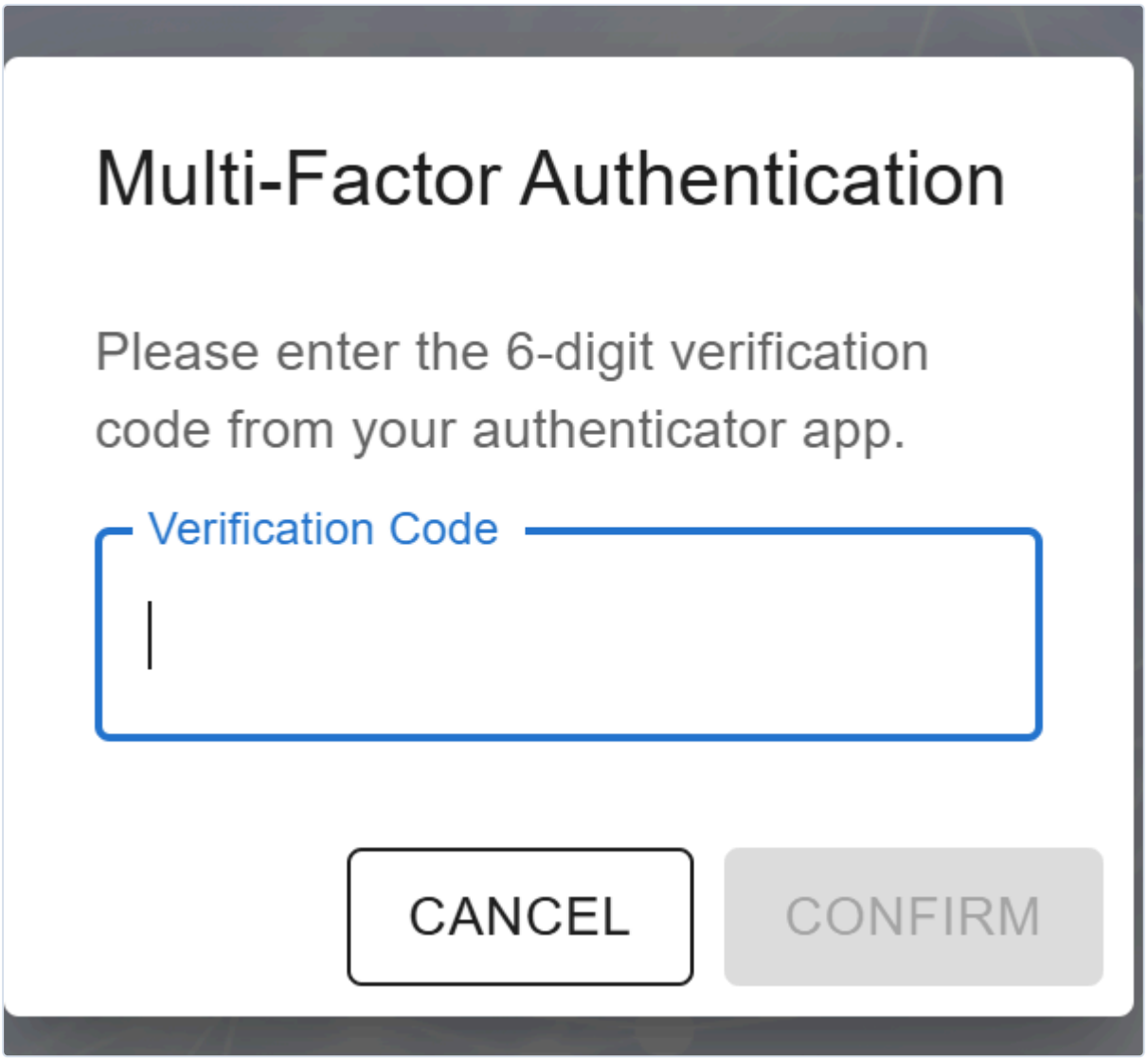
啟動 Merak Agent 後進入登入畫面：

1. 於「**Email**」欄位輸入使用者註冊的電子信箱。
2. 於「**Password**」欄位輸入密碼（可點擊欄位右側的眼睛圖示，切換密碼顯示／隱藏）。
3. 點擊「**LOGIN**」按鈕完成登入。若忘記密碼，可點擊「**FORGOT PASSWORD**」進行密碼重設。
4. 點「LOGIN」後需完成 MFA（多因素驗證）。首次登入與日後登入的畫面不同，詳見下方。

首次登入——綁定 MFA：出現「Set up Multi-Factor Authentication」視窗，使用驗證器 App（支援 Google Authenticator 與 Microsoft Authenticator）掃描 QR Code；或點「Or enter this key manually」的金鑰手動輸入。接著輸入 App 顯示的 6 位數驗證碼，點「CONFIRM」完成綁定。綁定完成後會接續跳至設備註冊（步驟 3）與管理員批准（步驟 4）。



日後登入（首次綁定 MFA 後的每次登入）——輸入驗證碼：出現「Multi-Factor Authentication」視窗，輸入驗證器 App 顯示的 6 位數驗證碼，點「CONFIRM」完成登入（點「CANCEL」可取消）。如下圖：



步驟 3　送出設備註冊請求

> 本步驟（設備註冊）僅於**首次登入**時出現，且在完成上方 MFA 綁定後才會進入。

首次登入後，Agent 主畫面會顯示設備狀態為未註冊：

1. 確認畫面顯示「**Hi [使用者姓名]!**」歡迎訊息。
2. 點擊下方藍色「**REQUEST REGISTER**」按鈕送出設備註冊請求。

送出後畫面狀態會更新為：`Status` 從 **Unregistered** 變更為 **Auditing（審核中）**；下方按鈕顯示「**DURING THE AUDIT**」（灰色，不可點擊）。此時須等待管理員至 Merak 主控台批准設備註冊。



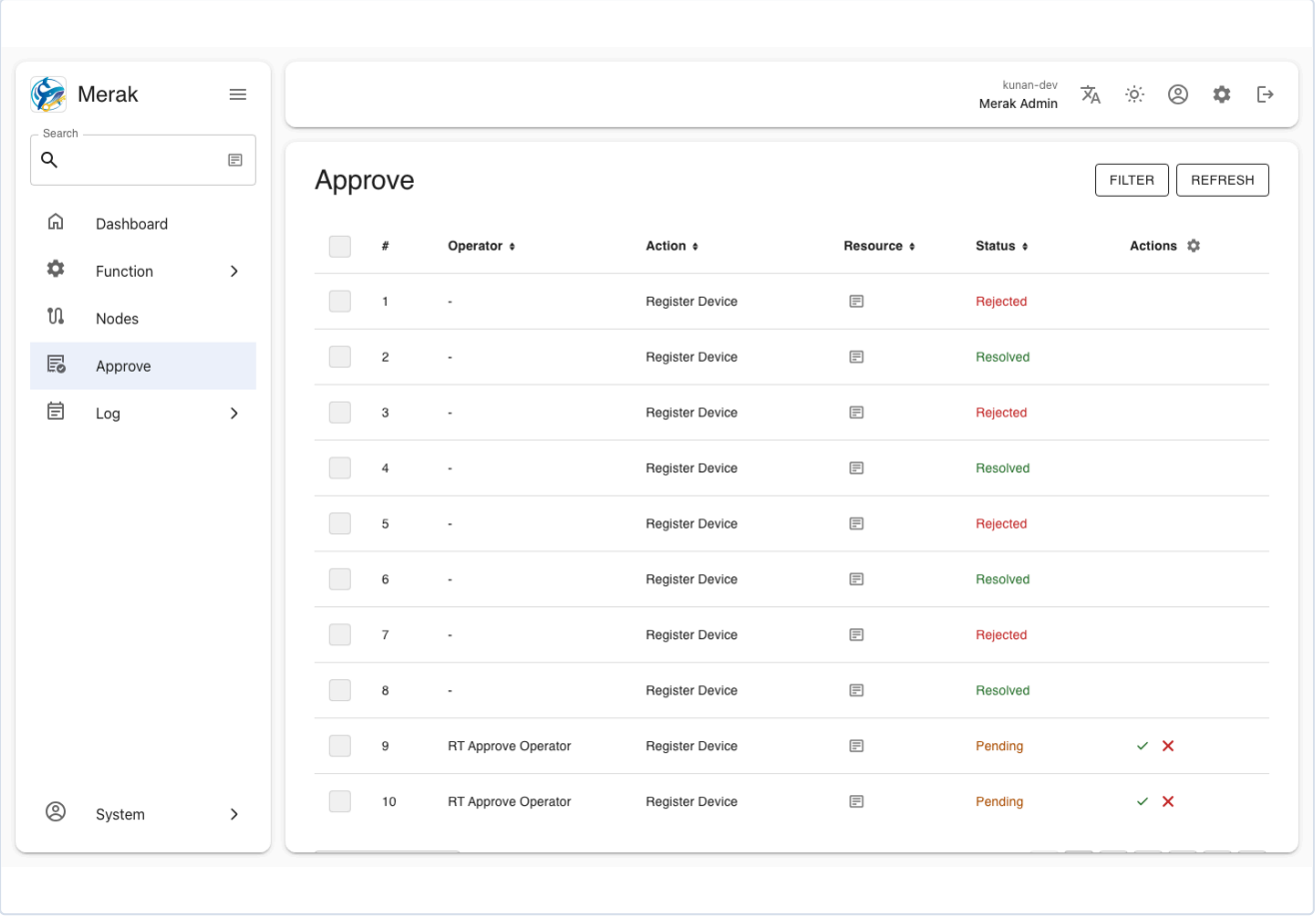
步驟 4　管理員至主控台批准（管理員操作）

當使用者送出註冊請求後，管理員須登入 Merak 主控台執行批准：

1. 登入 Merak 主控台後，點擊左側選單「**批准**」進入審批頁面。
2. 於審批列表中找到該使用者的「**Register Device**」請求（狀態欄顯示「**待審批**」，橘色）。
3. 點擊操作欄的「**綠色勾勾（✓）**」圖示進行核准；若要拒絕，可點擊「**紅色叉叉（×）**」。
4. 系統彈出「核准」確認對話框「**您確定要核准嗎？**」，點擊藍色「**確認**」按鈕完成批准（要取消可點「取消」）。
5. 核准後狀態欄將從「待審批」變更為「**已解決**」（綠色）。

審批頁面欄位說明：

欄位	說明
#	序號
操作者	送出請求的使用者
動作	請求類型（例如：Register Device）
資源	請求對應的資源資訊
狀態	待審批／已解決
建立時間	請求送出時間
更新時間	最後處理時間
操作	核准（✓）／拒絕（×）按鈕



步驟 5　使用者啟動連線

管理員批准後，使用者端 Agent 畫面會自動更新：

- 設備狀態變更為「**Status：Not connected**」（未連線）。
- 中央電源圖示變為深色（已啟用，可點擊）。
- 下方按鈕變更為藍色「**START**」。

點擊「**START**」按鈕或中央電源圖示啟動連線。成功連線後，畫面狀態會更新為：`Last Login Time` 顯示本次連線時間（例如 `2026/5/20 上午 11:42:07`）、`Status` 變更為 **Connected（已連線）**、中央電源圖示變為綠色、下方按鈕變更為橘色「**CLOSE**」。

如需中斷連線，可點擊橘色「**CLOSE**」按鈕。

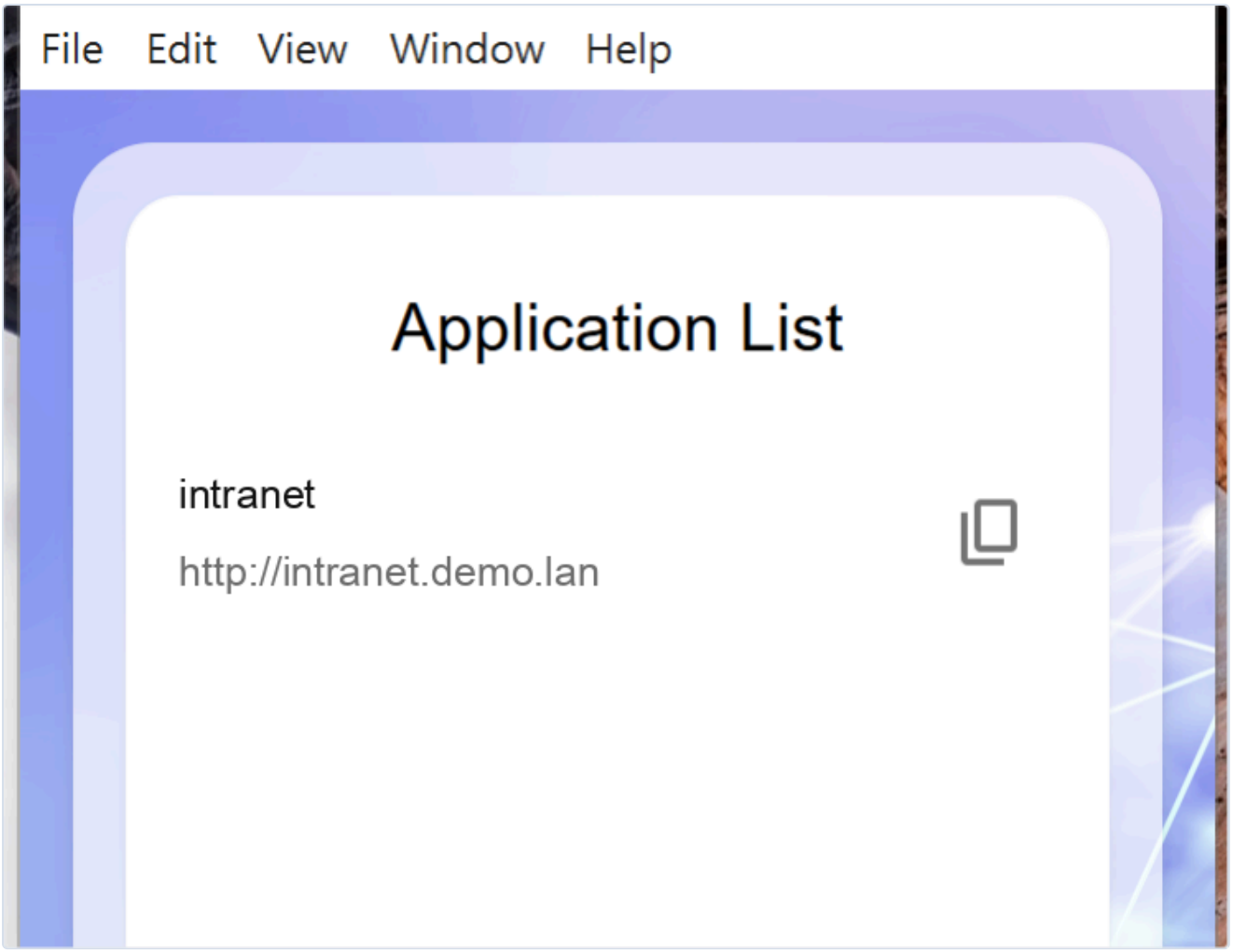
> 設備各狀態的意義與對應動作，另見〈附錄 B：設備認證狀態對照表〉。



步驟 6　查看並連線至授權的應用程式

登入後，可查看自己被授權的服務並取得連線網址：

1. 點「**Menu**」。
2. 點「**PROFILE**」。
3. 於「**Application List**」中可看到你被授權的服務（例如：`intranet`，`http://intranet.demo.lan`）。
4. 點該服務右側的「**複製**」圖示，將網址貼到瀏覽器即可連線。



3. 登入 Agentless Portal（免安裝 Agent）

適用對象：已被授權 Agentless 存取的使用者。**用途**：不安裝 Merak Agent，直接用瀏覽器經 Portal 登入，開啟你有權限的 Agentless 服務。

步驟 1　開啟 Portal 登入頁

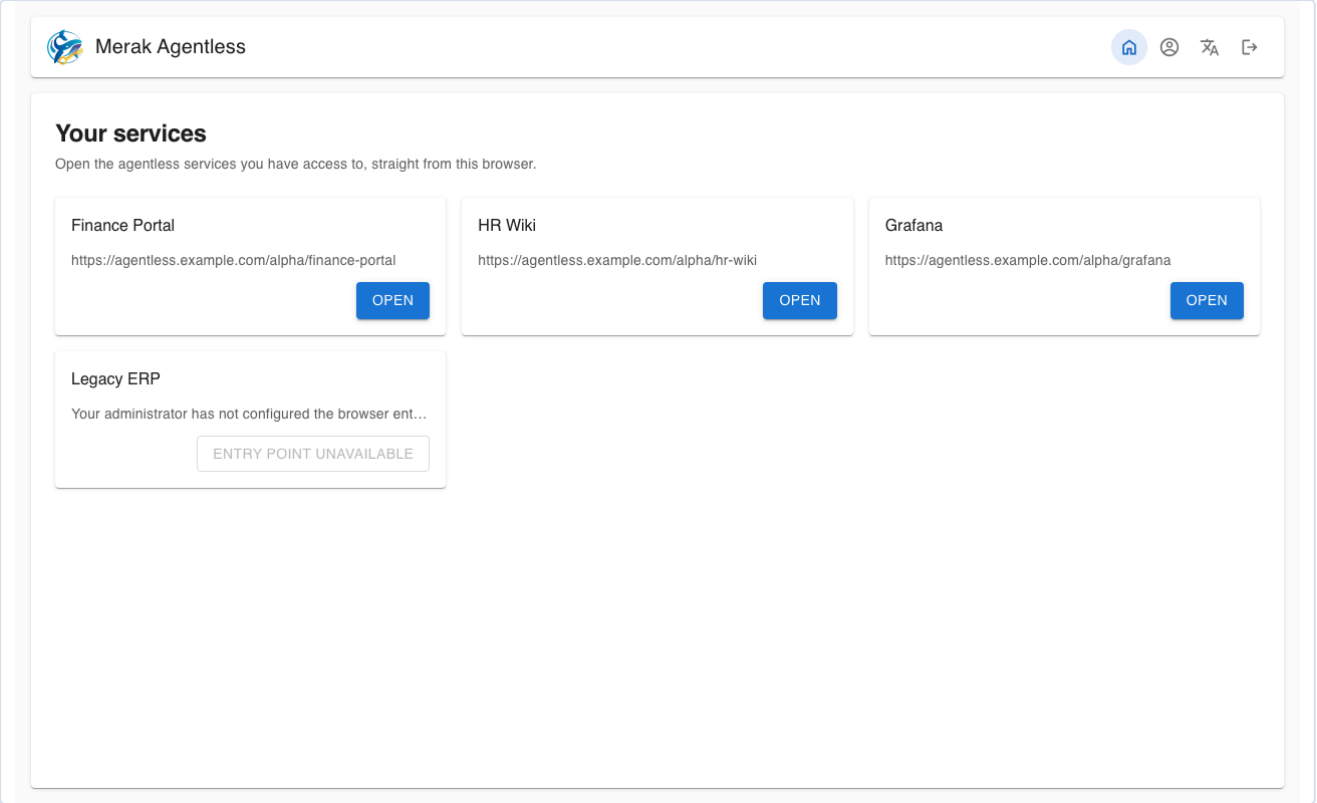
於瀏覽器開啟 Agentless 入口網址：`https://portal.merak.kunansec.com/login`。

步驟 2　登入

輸入帳號、密碼，並完成 MFA 驗證（多因素驗證，與 Merak Agent 登入相同；支援 Google Authenticator 與 Microsoft Authenticator）。

步驟 3　開啟服務

登入後會進入「**您的服務**」頁面，列出你有權限的 Agentless 服務。於目標服務卡片（例如：`intranet`，`https://portal.merak.kunansec.com/agentless/kunan/intranet`）點「**開啟**」，即可用瀏覽器直接連線。



頁面右上角可切換語言、查看帳戶，或點「登出」結束。管理員如何為應用程式開啟 Agentless 並授權成員，見〈10. 設定 Agentless 存取〉。

第二篇　管理員操作篇

本篇提供給系統管理員：成員管理（新增、匯入、停用與刪除）、應用資源與節點（建立應用、Agentless、節點）、權限與管理員（角色、建立管理員）。

建立網路節點（Node）

部署與管理 Merak 地端節點（Node）。

4. 節點（Node）建置

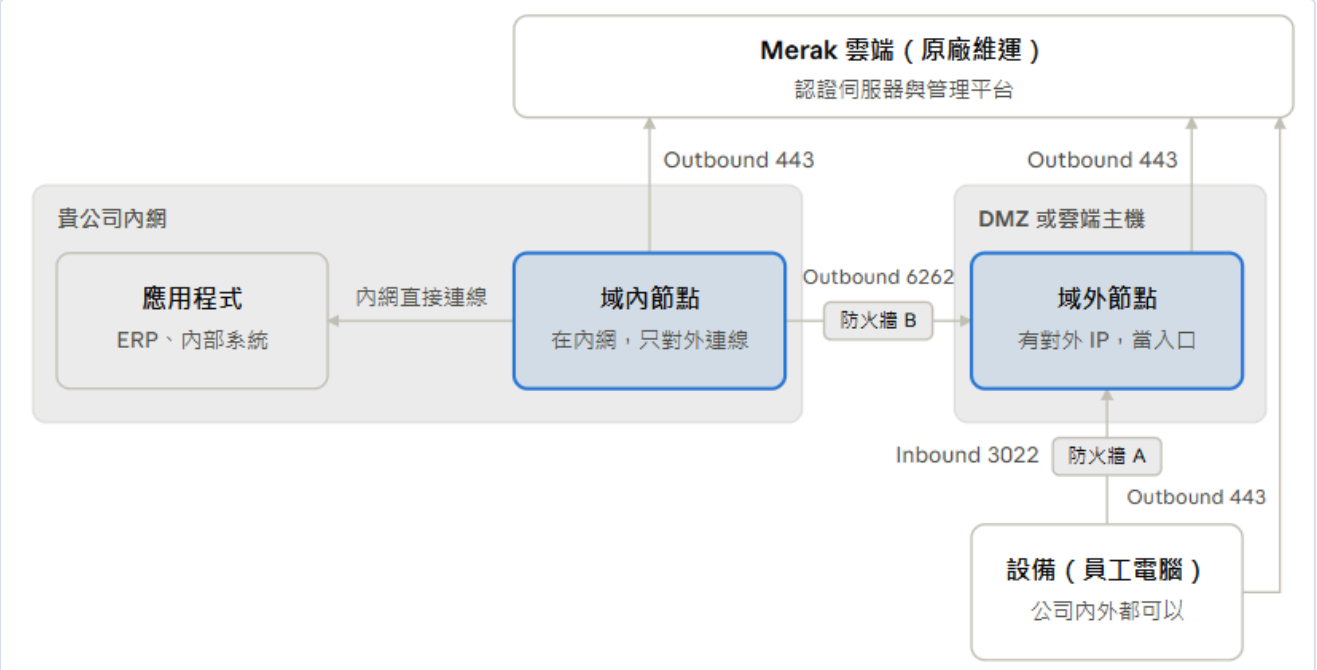
適用對象：具管理員權限者、負責地端部署的人員。**用途**：在管理介面中新增節點，並完成安裝腳本的下載與部署。

概覽

節點（Node）是 Merak Zero Trust 平台的地端/雲端部署元件，負責在目標主機上建立安全的網路存取通道。

建置位置建議

標準架構為兩台節點：放在 DMZ 或雲端、有對外 IP 的「外部節點」，以及放在內網的「內部節點」。員工電腦（設備）先連到外部節點，外部節點再透過內部節點把連線帶進內網的應用程式。整個過程只有外部節點需要開放對內連線，內網防火牆不用改。



節點	放置位置	作用	Console「路由器角色」
外部節點	DMZ 或雲端主機，需固定對外 IP（或網域名稱）	使用者連線的入口；設備與內部節點都連到它	純入口

節點	放置位置	作用	Console「路由器角色」
內部節點	內網，固定內網 IP 即可	只主動對外連線，負責連到內網的應用程式；防火牆不用開任何對內連線	可承載服務

架構重點：

- 所有使用者與節點都須經 Merak Auth Server 驗證，採 MFA 與 TLS 1.3 雙向憑證。
- 使用者只看得到被授權的服務。例如 ERP 與 RD 位於同一網段，廠商 B 只被授權 ERP，就無法掃描或探測到 RD。

前置需求

安裝前請準備下列機器與防火牆設定。表中 Inbound 指對內連線（別人連進來），Outbound 指對外連線（自己連出去）。

機器規格（最小）：

機器	數量	規格
外部節點	1 台	Ubuntu Server 24.04 LTS 以上版本（64 位元）、2 核心／4 GB 記憶體／20 GB 磁碟、root 權限；需固定對外 IP（或網域名稱）
內部節點	1 台	同上，固定內網 IP 即可

外部節點主機防火牆規則：

方向	來源	目的地	連接埠
Inbound	設備（員工電腦）	外部節點	TCP 3022
Inbound	內部節點	外部節點	TCP 6262
Outbound	外部節點	`*.merak.kunansec.com`	TCP 443

內部節點主機防火牆規則（不需要任何 Inbound）：

方向	來源	目的地	連接埠
Outbound	內部節點	外部節點	TCP 6262
Outbound	內部節點	`*.merak.kunansec.com`	TCP 443
Outbound	內部節點	各應用程式	應用程式本身的連接埠

- 外部節點若放在防火牆後方、使用內部 IP（例如 DMZ），請在防火牆設定 Port Forwarding，將對外 IP 的 TCP 3022 與 6262 轉到外部節點。

- 對外的 TCP 443 必須直接連線，不能經過 Proxy 伺服器，也不能做 HTTPS 內容檢查（SSL 解密）。
- 安裝時須填寫「主機」，即外部節點的對外 IP 或網域名稱（對應 Console 節點頁的「主機」欄位），之後無法修改。
- 有購買 Merak Agentless 的客戶，外部節點還要再開放 Inbound TCP 443。

> 【重要提醒】安裝腳本內含 enrollment JWT，僅提供一次下載機會，請務必妥善保存。若遺失，需重新產生 JWT。

兩台防火牆的設定

若貴公司有兩台防火牆：防火牆 A 位於網際網路與外部節點之間，防火牆 B 位於外部節點（DMZ）與內網之間，請依下表設定。每台防火牆的 Inbound／Outbound 以它保護的那一側為準；表中沒列的一律不開。

防火牆 A（保護 DMZ；Inbound＝網際網路 → DMZ，Outbound＝DMZ → 網際網路）：

方向	來源	目的地	連接埠	說明
Inbound	任何來源（設備可能在公司外）	外部節點	TCP 3022	設備的連線入口
Outbound	外部節點	`*.merak.kunansec.com`	TCP 443	連 Merak 雲端
Outbound	內部節點、公司內的設備	`*.merak.kunansec.com`	TCP 443	內網的流量經防火牆 B 後再從這裡出去
NAT	對外 IP 的 3022、6262	外部節點的內部 IP	同連接埠	外部節點使用內部 IP 時要設 Port Forwarding

防火牆 B（保護內網；Inbound＝DMZ → 內網，Outbound＝內網 → DMZ 或網際網路）：

方向	來源	目的地	連接埠	說明
Outbound	內部節點	外部節點	TCP 6262	內部節點主動連出
Outbound	公司內的設備	外部節點	TCP 3022	如果公司內的員工電腦也是連外部節點
Outbound	內部節點、設備	`*.merak.kunansec.com`	TCP 443	連 Merak 雲端，會再經過防火牆 A
Inbound	（無）	（無）	（無）	不用開任何 Inbound，這正是使用兩台節點的目的

> 【重要提醒】「主機」位址：內部節點與公司內的設備，都是用外部節點的「主機」位址連線。很多防火牆不允許從內網連自己的對外 IP（沒有 NAT Loopback），建議二選一：

- 建議做法：「主機」填網域名稱，內部 DNS 把它解析成外部節點的 DMZ 內部 IP（Split DNS）。這樣內網的連線只經過防火牆 B，防火牆 A 不必開 TCP 6262。
- 或者在防火牆 A 開啟 NAT Loopback，讓內網也能連到對外 IP。

硬體規格建議

每台節點為一台 VM，依尖峰每秒流量選擇級距。下表為初步建議值，實際依導入評估調整。

尖峰每秒流量	CPU	記憶體	硬碟	網路卡
100 Mbps	4 核	8 GB	50 GB SSD	1 Gbps
300 Mbps	6 核	12 GB	100 GB SSD	1 Gbps
500 Mbps	8 核	12 GB	100 GB SSD	1 Gbps
1 Gbps	12 核	16 GB	200 GB SSD	10 Gbps
1.5 Gbps	16 核	24 GB	200 GB SSD	10 Gbps
2 Gbps	20 核	24 GB	200 GB SSD	10 Gbps
2.5 Gbps	24 核	32 GB	200 GB SSD	10 Gbps
3 Gbps	28 核	32 GB	200 GB SSD	10 Gbps

【提示】表中流量是尖峰時段的每秒流量（Mbps、Gbps），不是檔案大小或每月總用量。

選擇級距的方式：

- 估算尖峰時段的每秒流量，對照上表選擇不低於該流量的級距。
- 有加購抗量子加密模組時，選高一級（加密較耗 CPU）。
- 若資安規定要求對外（使用者從網際網路連入）與對內（連到公司內部系統）的網路分開，節點主機需準備兩張網路卡，一張接外、一張接內；不需分開時，一張即可。
- 500 Mbps 以上建議另備一台備援。

步驟 1　進入節點管理頁面

1. 登入 Merak 管理介面。
2. 點擊左側導覽列的「**節點**」。

畫面將顯示節點列表，包含以下欄位：

欄位	說明
名稱	節點的自訂名稱
主機	節點所在主機位址

欄位	說明
狀態	節點目前的連線狀態
部署狀態	節點的部署進度（如：等待佈署）
建立時間	節點建立的日期
建立者	建立該節點的帳號 ID
更新時間	最後更新日期
操作	可進行編輯或刪除



步驟 2　新增節點

1. 點擊右上角「**新增節點**」按鈕。
2. 在彈出的「新增節點」視窗中，填入**節點名稱**（必填）。
3. 點擊「**建立**」。

> 【提示】節點建立後將部署為地端節點，可下載 `install.sh` 於目標主機執行安裝。



步驟 3　下載安裝腳本

建立成功後，系統將顯示安裝資訊頁面：

1. 確認頁面上顯示的**過期時間**（JWT 有效期限）。
2. 點擊「**下載 INSTALL.SH**」，將安裝腳本儲存至本機。
3. 確認下載完成後，點擊「**完成**」。

> 【注意事項】安裝腳本內含 enrollment JWT，僅能下載一次，請立即妥善保存；若 JWT 已過期或需要重新安裝，請點擊「重新產生 JWT」取得新的安裝腳本；支援 Ubuntu Server 24.04 LTS 以上版本。



步驟 4　於目標主機執行安裝

將下載好的 `install.sh` 上傳至目標主機並執行。流程為：

1. 上傳安裝腳本至目標主機。

```
scp install.sh <user>@<host-ip>:/home/<user>/
```

2. 連線至目標主機。

```
ssh <user>@<host-ip>
```

3. 賦予執行權限。

```
chmod +x install.sh
```

4. 執行安裝腳本。

```
sudo ./install.sh
```

5. 等待安裝完成。

安裝腳本將自動完成以下程序：下載並安裝必要套件、註冊節點至 Merak 控制器（使用內含的 enrollment JWT）、啟動節點服務。安裝成功後，終端機將顯示安裝完成訊息。

步驟 5　確認節點狀態

1. 回到 Merak 管理介面，點擊左側「**節點**」頁面。
2. 確認剛建立的節點狀態已更新為「**線上**」。

若狀態仍顯示「等待佈署」或「無資料」，請確認：安裝腳本是否已成功執行、目標主機是否可正常連線至外部網路、JWT 是否在有效期限內。

常見問題

問題	可能原因	處理方式
安裝腳本執行後立即中止	作業系統不支援	確認目標主機為 Ubuntu Server 24.04 LTS 以上版本。
JWT 已過期	下載後未即時安裝	回到節點頁面，點選該節點詳情，點擊右上角「重新產生 JWT」。
節點狀態持續顯示「等待佈署」	網路不通或安裝失敗	確認主機網路連線，並重新執行安裝腳本。
忘記下載 install.sh	僅提供一次下載	回到節點頁面，點擊「下載安裝包」重新下載。
需刪除節點	—	於該節點的操作點選「刪除」。

功能管理

成員與應用程式的日常管理（建立組織、成員新增/匯入/停用刪除、建立應用程式、設定 Agentless）。

5. 新增成員

適用對象：具管理員權限者。**用途**：讓新同仁或外部協作者能登入 Merak，並指定其所屬群組與可存取的應用程式。

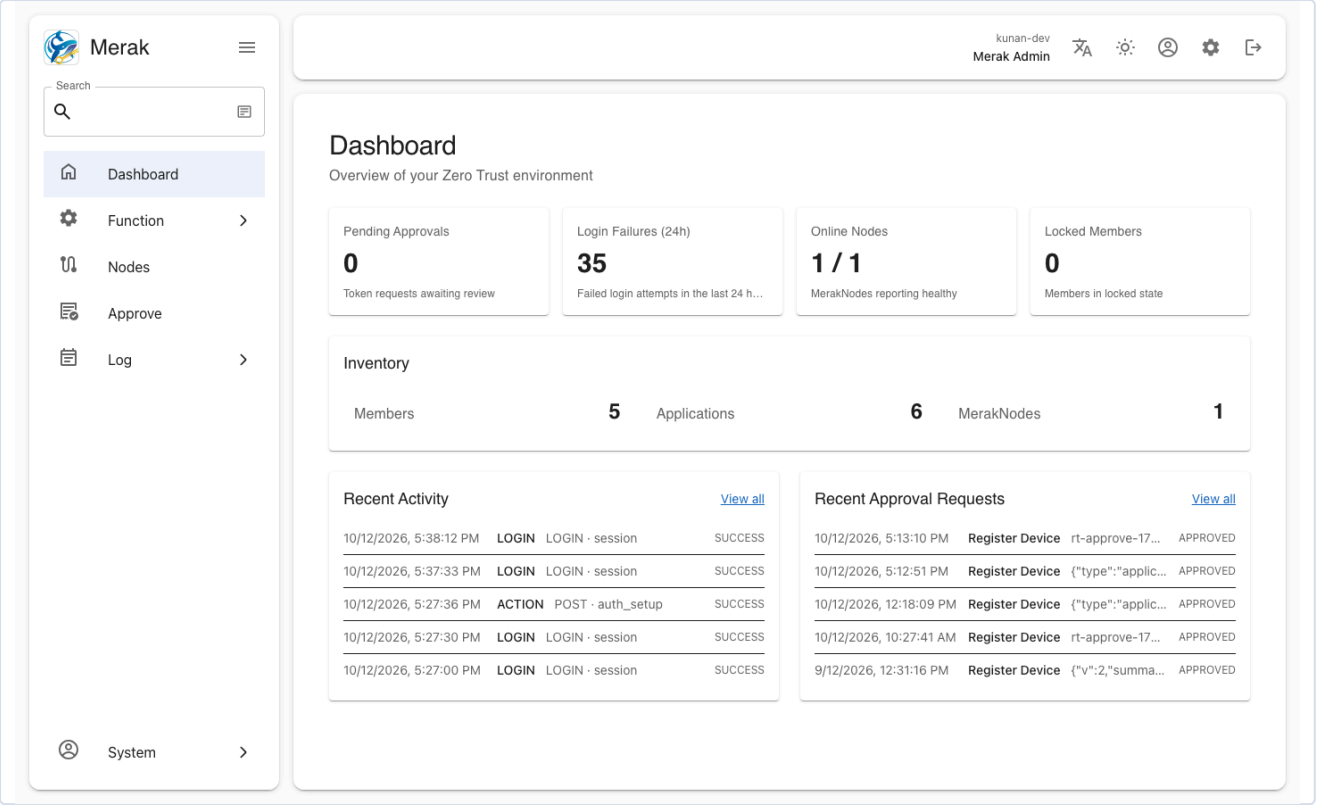
前置需求

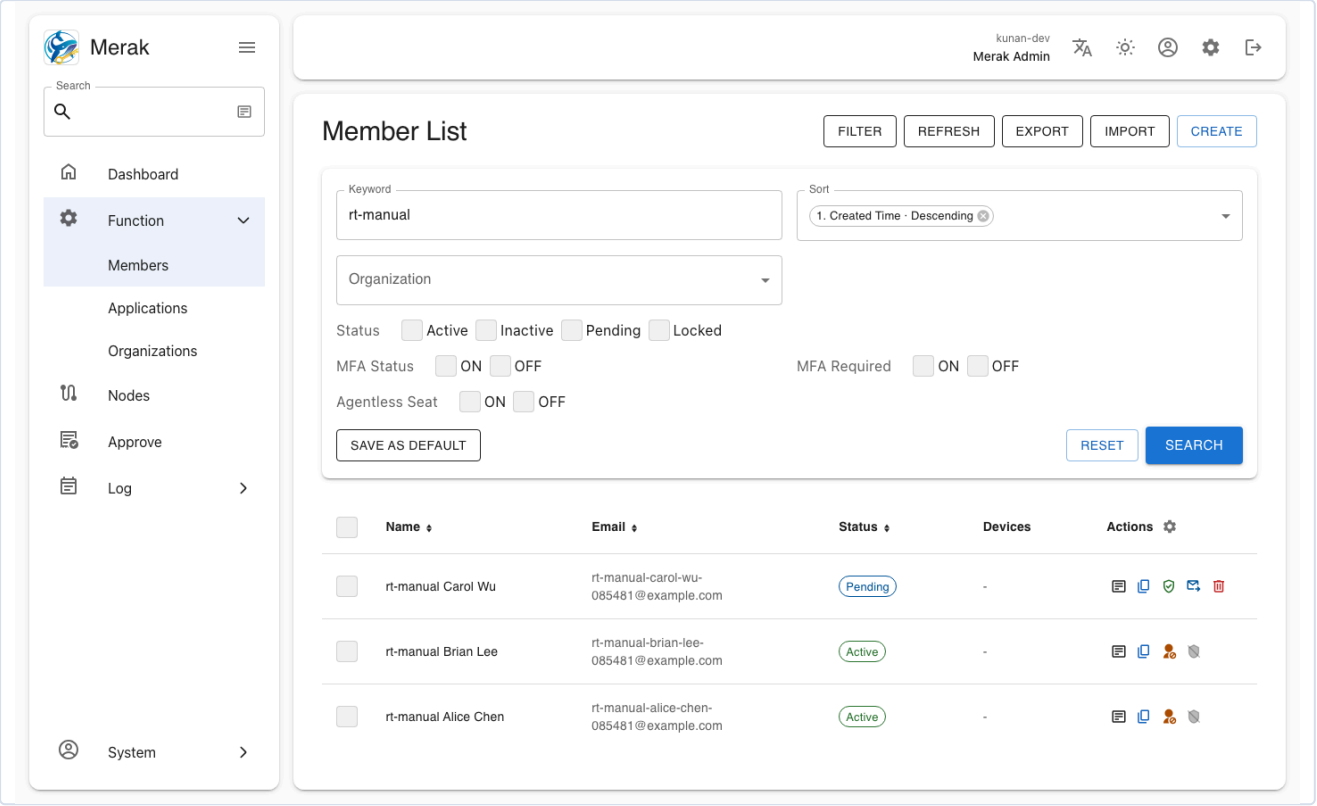
- 執行者需具備管理員權限。
- 對方的電子郵件信箱（邀請信將寄至此信箱）。
- 欲指派的群組已建立（如 RD、業務部）。
- 欲授權的應用程式已完成發佈（如 ERP）。

> 若群組尚未建立，請先參考〈8. 建立組織〉；若應用程式尚未建立，請先參考〈9. 建立新應用程式〉。

步驟 1　進入成員管理頁

登入 `https://console.merak.kunansec.com/`，於左側選單點選「**成員**」，再點右上角「**建立**」。



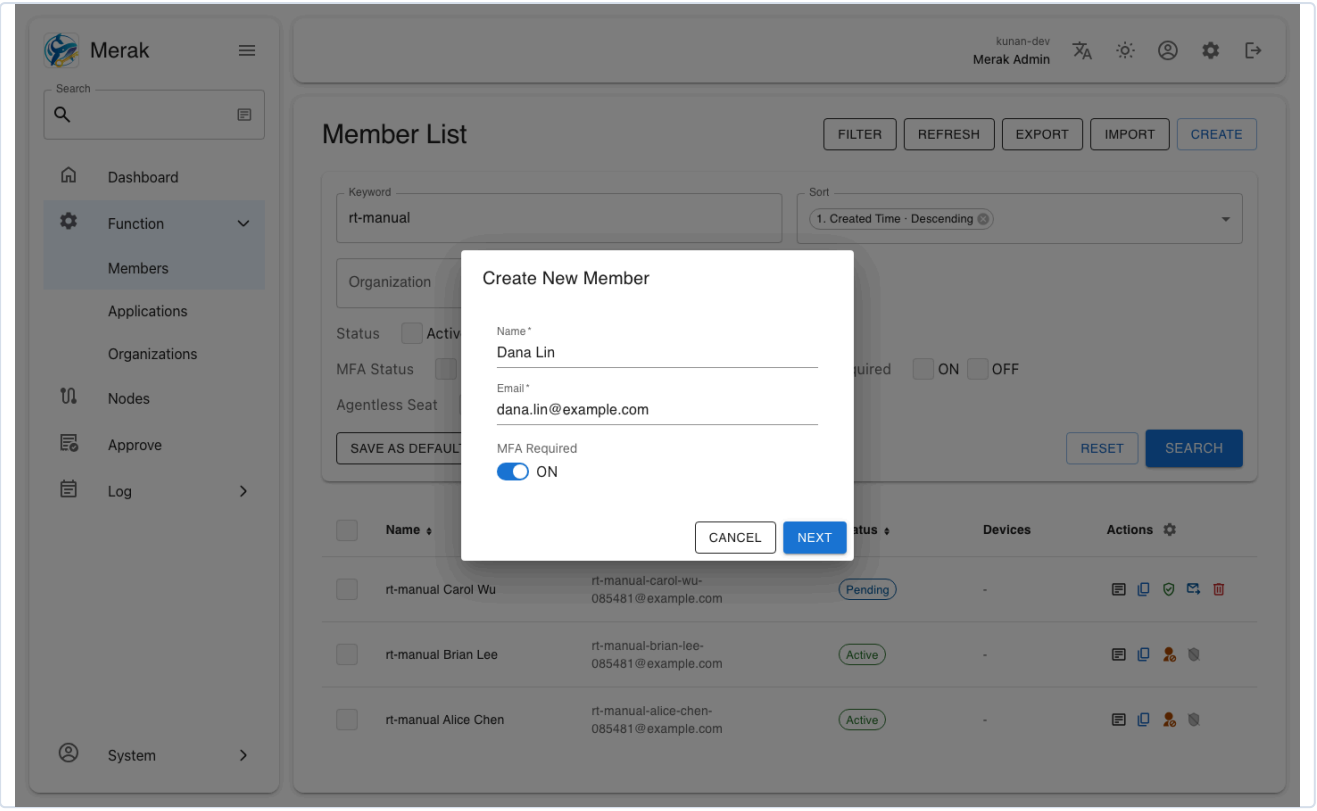


步驟 2　填寫基本資料

欄位	必填	說明
Nickname	是	成員在 Console 中的顯示名稱。建議統一格式（如「姓名-部門」），方便日後搜尋與稽核。

欄位	必填	說明
Email	是	邀請信與登入帳號。

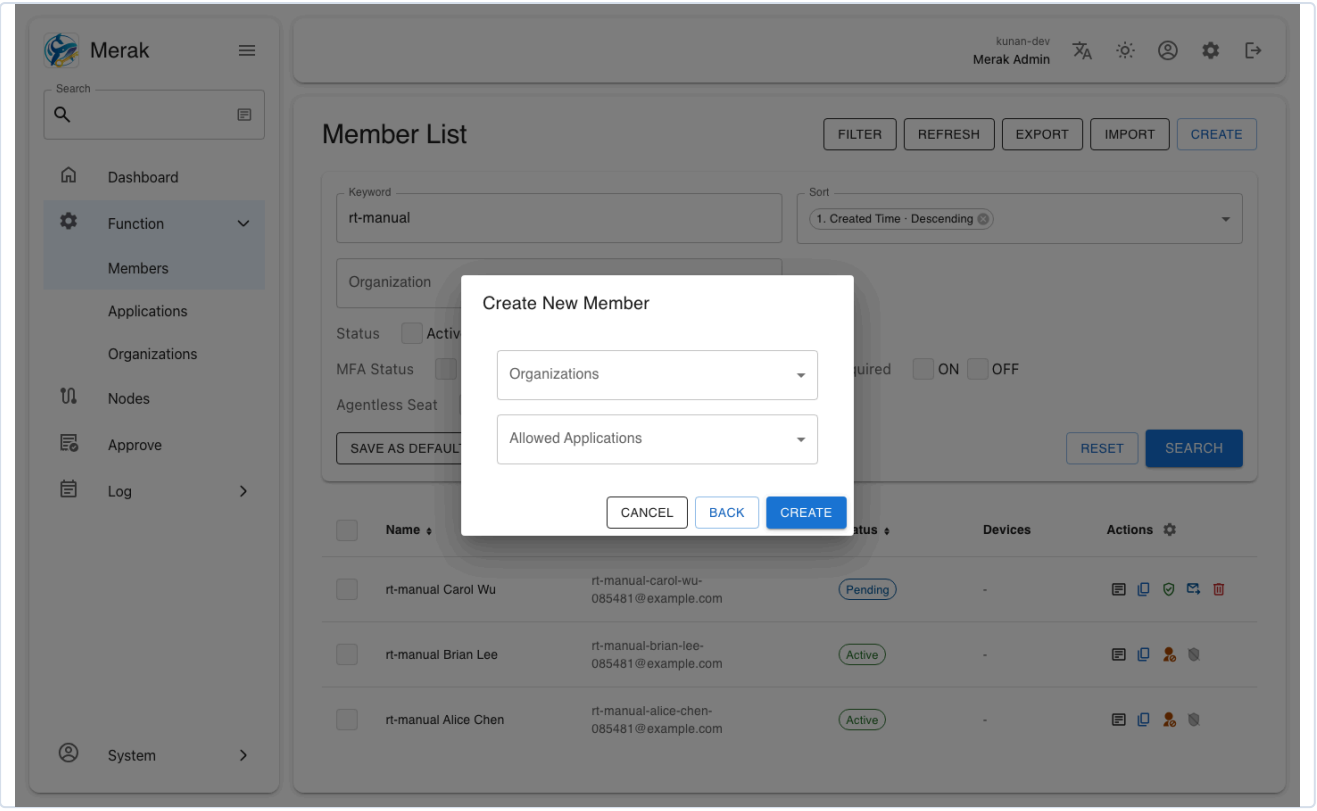
填妥後點「**下一步**」。



步驟 3　指派群組

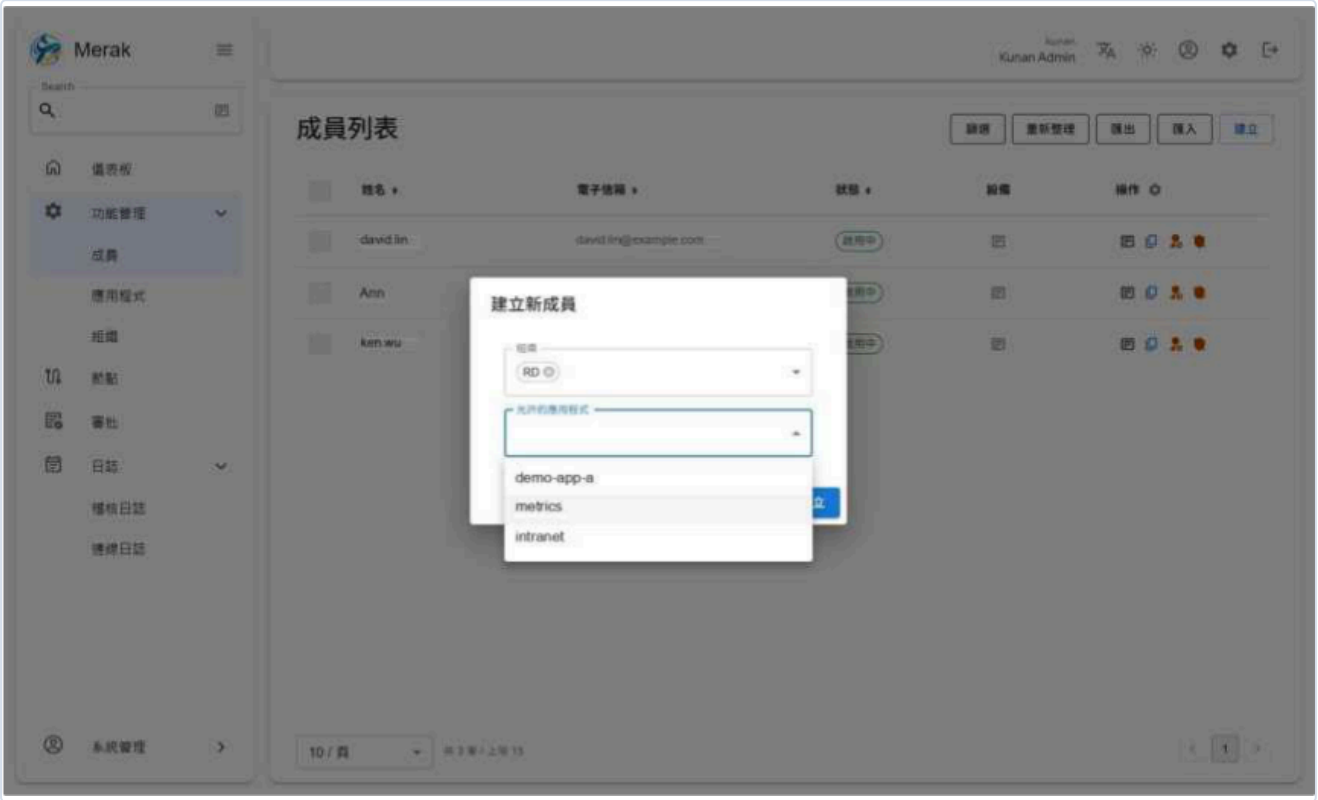
於群組選單中選擇該成員所屬群組（範例：`RD`），完成後進入下一步。群組決定成員套用哪些存取政策。

備註：同一成員可加入多個群組。



步驟 4　授權應用程式

勾選該成員可存取的應用程式（範例：`ERP`），完成後進入下一步。此處只會列出已發佈的應用程式；若清單中找不到目標應用，表示該應用尚未發佈或不在你的管理範圍內。



步驟 5　建立並完成

確認摘要內容無誤後點「**建立**」，再點「**完成**」關閉視窗。成員將出現在成員列表中，狀態為「**待啟用**」。

後續流程：

1. 系統寄出邀請信至該成員信箱。
2. 成員點擊信中連結完成密碼設定與 MFA 綁定後，即可登入（參見〈1. 帳號啟用指南〉、〈2. 安裝 Merak Agent 與設備認證〉）。

常見問題

狀況	處理方式
成員未收到邀請信	請對方檢查垃圾信匣；確認信箱拼寫；於成員列表重寄邀請。
信箱重複	該信箱已存在於此組織，無法新增重複信箱，請至成員列表搜尋既有帳號並調整其權限。

6. 匯入成員資料

適用對象：具管理員權限者。**用途**：以檔案批次匯入多筆成員資料至 Merak Console。

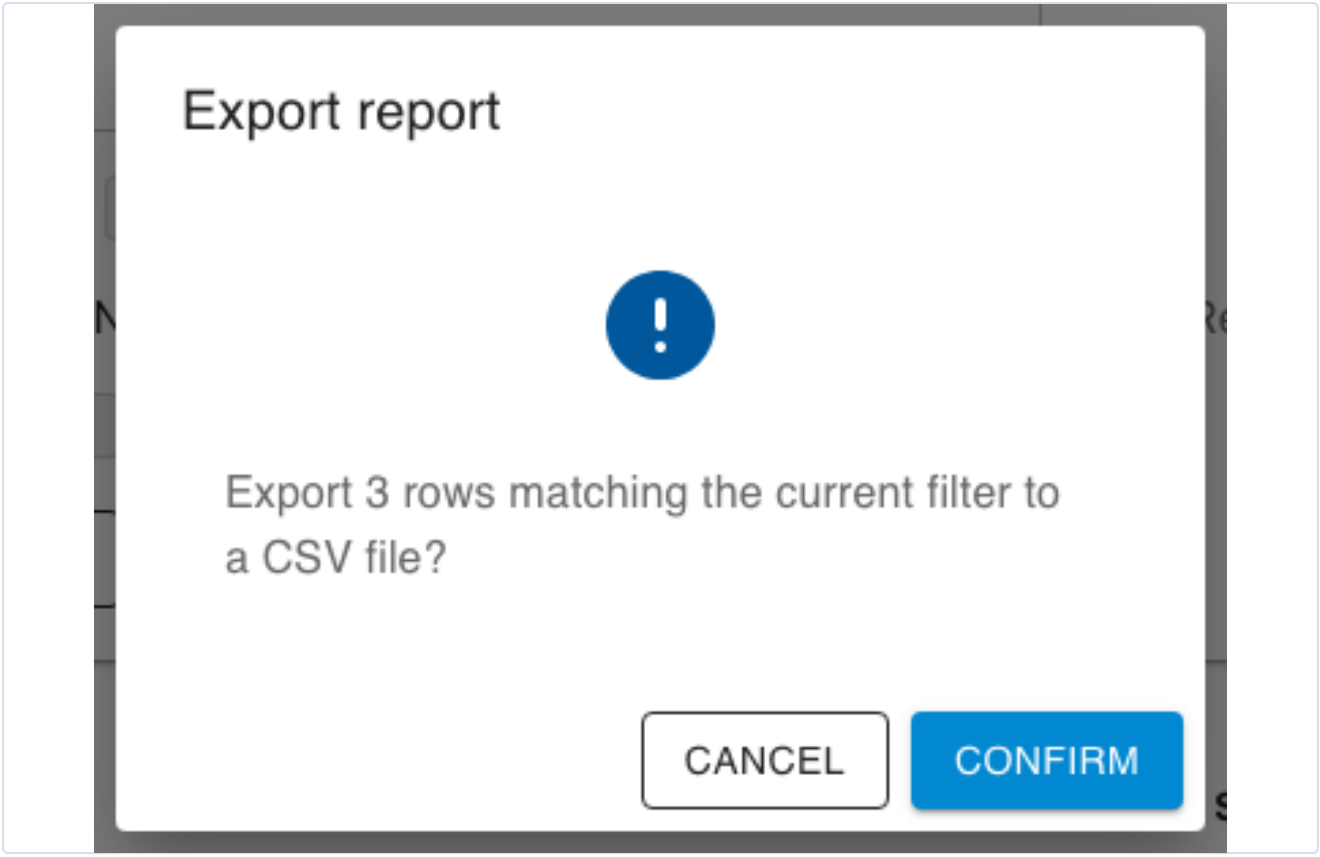
> 【提示】建議：正式匯入前，可先用「匯出」取得現有成員資料作為欄位範本，依相同格式（姓名、電子郵件、描述）填寫後再匯入。

步驟 1　開啟成員管理頁

於瀏覽器導航至 `https://console.merak.kunansec.com/member`。

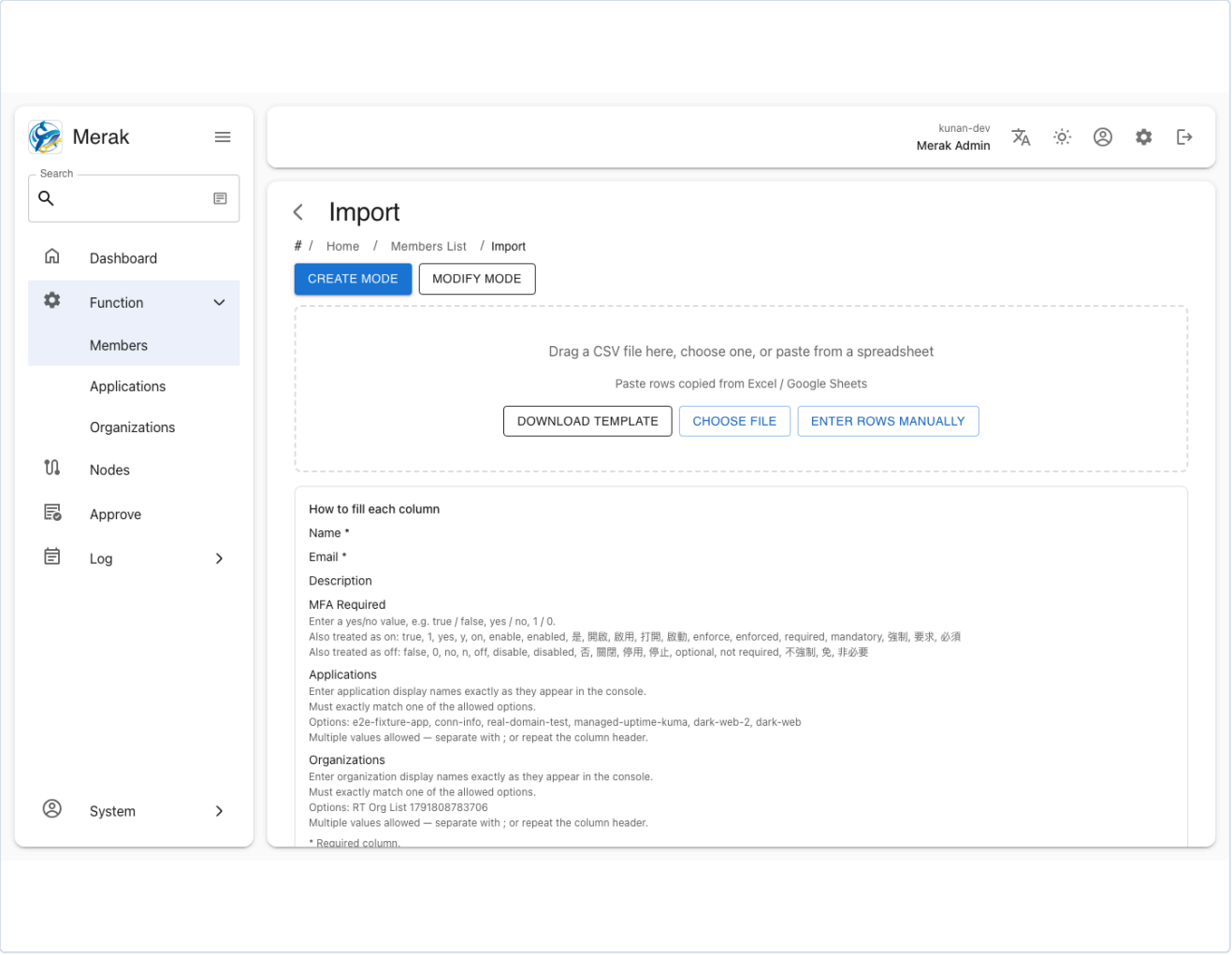
步驟 2　（選用）匯出範本

1. 點擊「**匯出**」。
2. 於確認視窗點擊「**確認**」，下載現有成員資料檔。
3. 依檔案欄位（**姓名**、**電子郵件**、**描述**）整理要匯入的成員清單。



步驟 3　開始匯入並選擇檔案

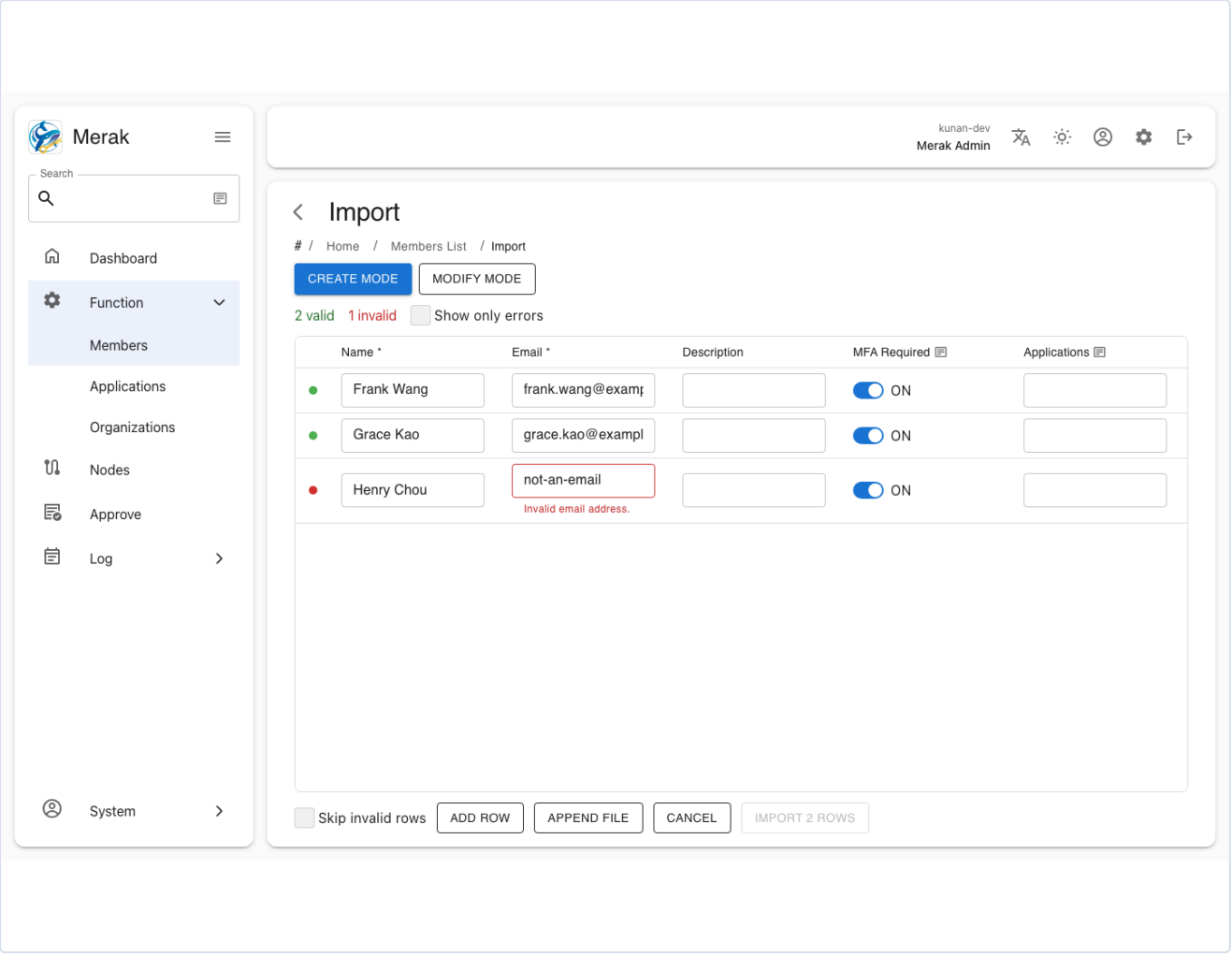
1. 點擊「**匯入**」。
2. 點擊「**選擇檔案**」，選取已填好成員資料的檔案。

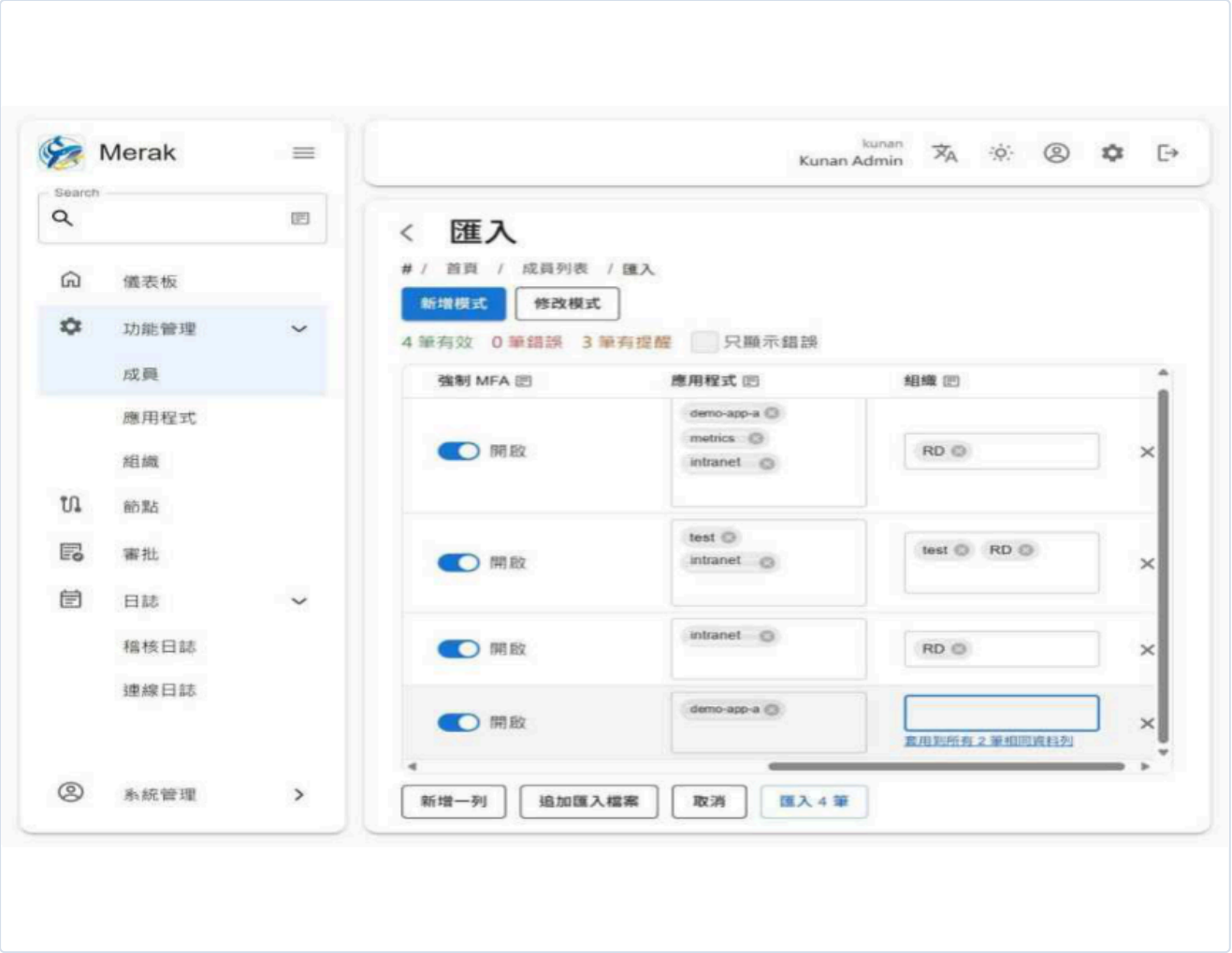


步驟 4　設定匯入對應項目

為匯入的成員指定對應設定：

項目	說明	範例
組織	選擇成員所屬組織	`demo-app-a`
應用程式	選擇要授權的應用程式	`RD`
環境	選擇對應環境	`test`
MFA	是否強制開啟 MFA	開／關


Merak
Search
Dashboard
Function
Members
Applications
Organizations
Nodes
Approve
Log
System
kunan-dev
Merak Admin
Import
/ Home / Members List / Import
CREATE MODE
MODIFY MODE
2 valid
1 invalid
Show only errors
Name *
Email *
Description
MFA Required
Applications
Frank Wang
frank.wang@exam
ON
Grace Kao
grace.kao@exampl
ON
Henry Chou
not-an-email
Invalid email address.
ON
Skip invalid rows
ADD ROW
APPEND FILE
CANCEL
IMPORT 2 ROWS



步驟 5　確認匯入清單

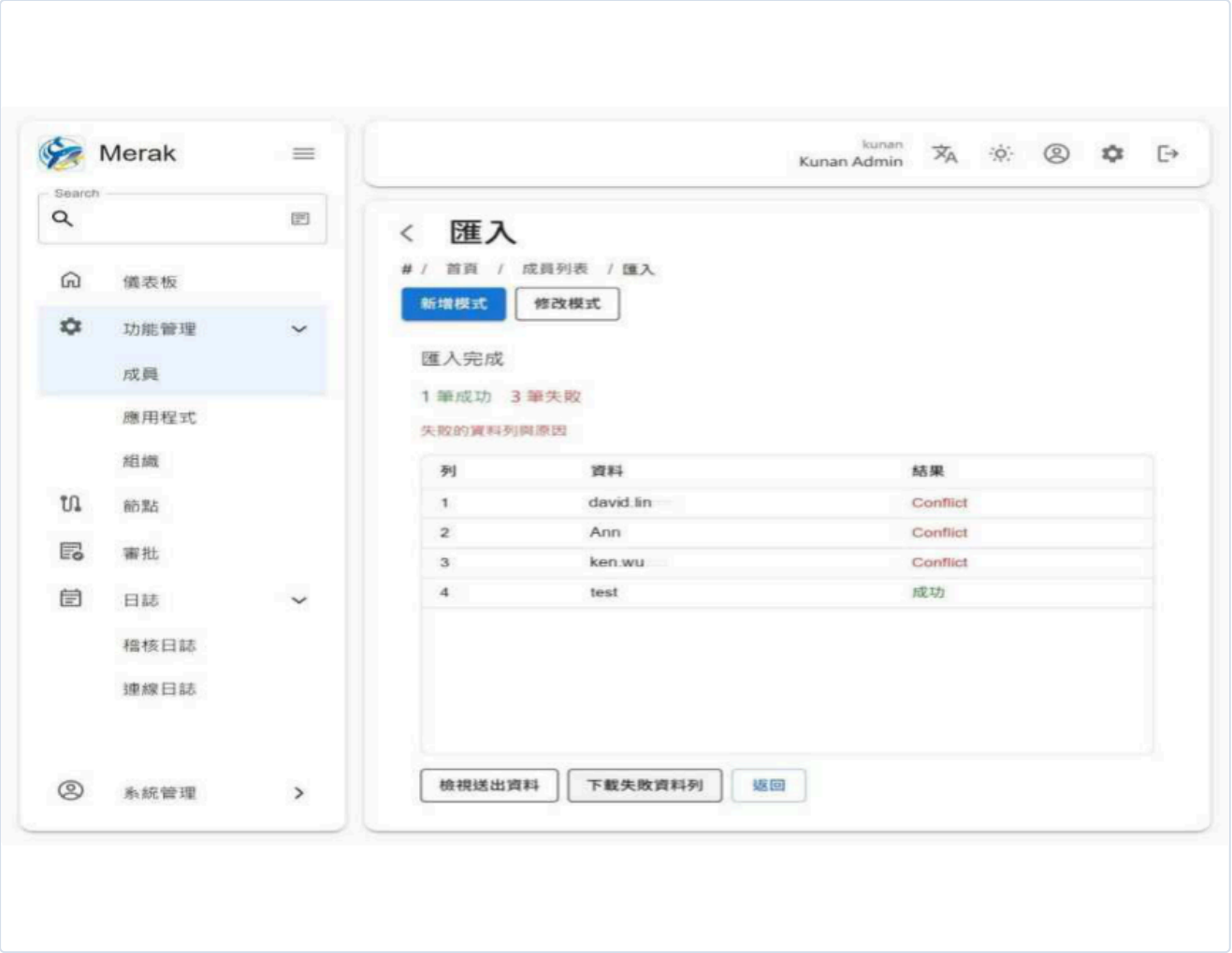
檢視系統帶出的成員清單，確認欲匯入的資料無誤。如需一次匯入多個檔案，點擊「**追加匯入檔案**」加入其他檔案。

步驟 6　執行匯入

點擊「**匯入 N 筆**」（N 為系統偵測到的筆數，如「匯入 4 筆」）執行匯入。

步驟 7　處理失敗資料（如有）

若有匯入失敗的資料列，點擊「**下載失敗資料列**」取得錯誤明細，修正後可重新匯入。



步驟 8　完成

點擊「**返回**」離開，結束匯入流程。

7. 停用與刪除成員

適用對象：具管理員權限者。**用途**：將成員帳號失效（停用），或自組織中永久刪除。

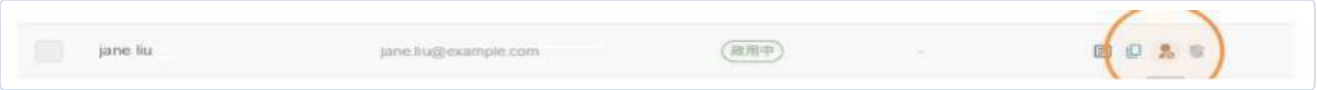
> 【請注意】刪除成員為不可逆操作。建議先「停用（失效）」觀察，確認無誤後再執行刪除。

步驟 1　開啟成員管理頁

於瀏覽器導航至 `https://console.merak.kunansec.com/member`。

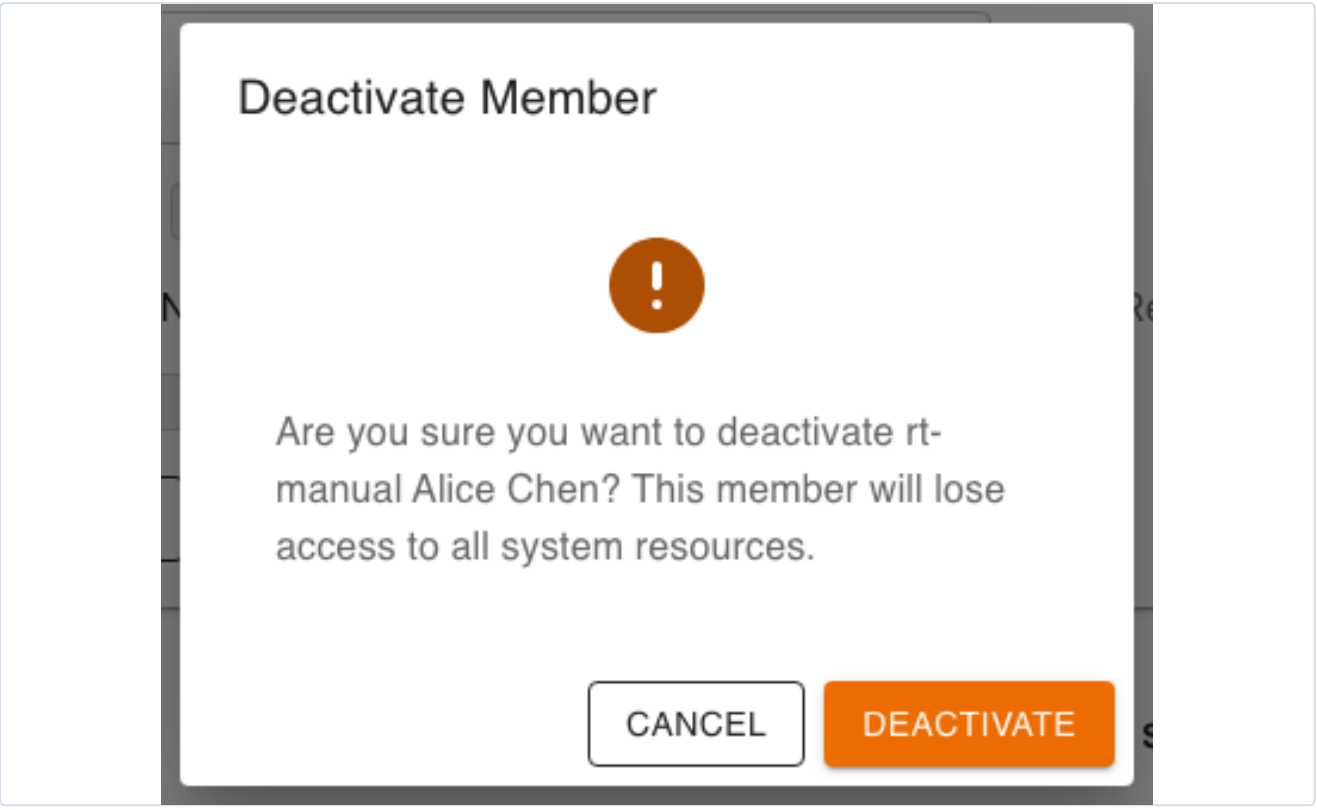
步驟 2　選擇欲處理的成員

在成員清單中找到目標成員，點擊該列的操作選項。



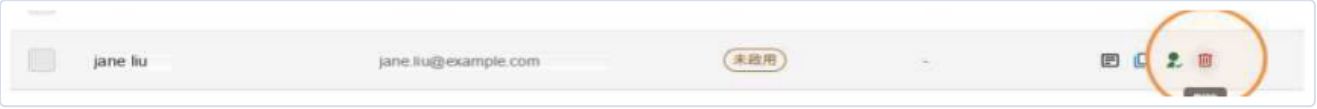
步驟 3　停用（失效）成員

點擊「**失效**」，將該成員帳號停用。停用後該成員將無法登入。



步驟 4　（如需刪除）開啟刪除選項

於已停用的成員上再次點擊操作選項。



步驟 5　刪除成員

點擊「**刪除**」，將該成員自組織中永久移除。

8. 建立組織

適用對象：具管理員權限者。**用途**：建立組織，並指定群組成員與可存取的應用程式。

步驟 1　開啟成員管理頁

於瀏覽器導航至 `https://console.merak.kunansec.com/member`。

步驟 2　新增組織

點選「**組織**」，再點「**新增**」。

步驟 3　填寫名稱

於「**名稱 ***」欄位輸入群組名稱（必填，例如：`RD`），填妥後點「**下一步**」。

步驟 4　選擇成員

選擇要加入此群組的成員（範例：Ann ），完成後進入下一步。

步驟 5　授權應用程式

選擇此群組可存取的應用程式（範例：`intranet` 、 `metrics` ），完成後進入下一步。

步驟 6　建立並完成

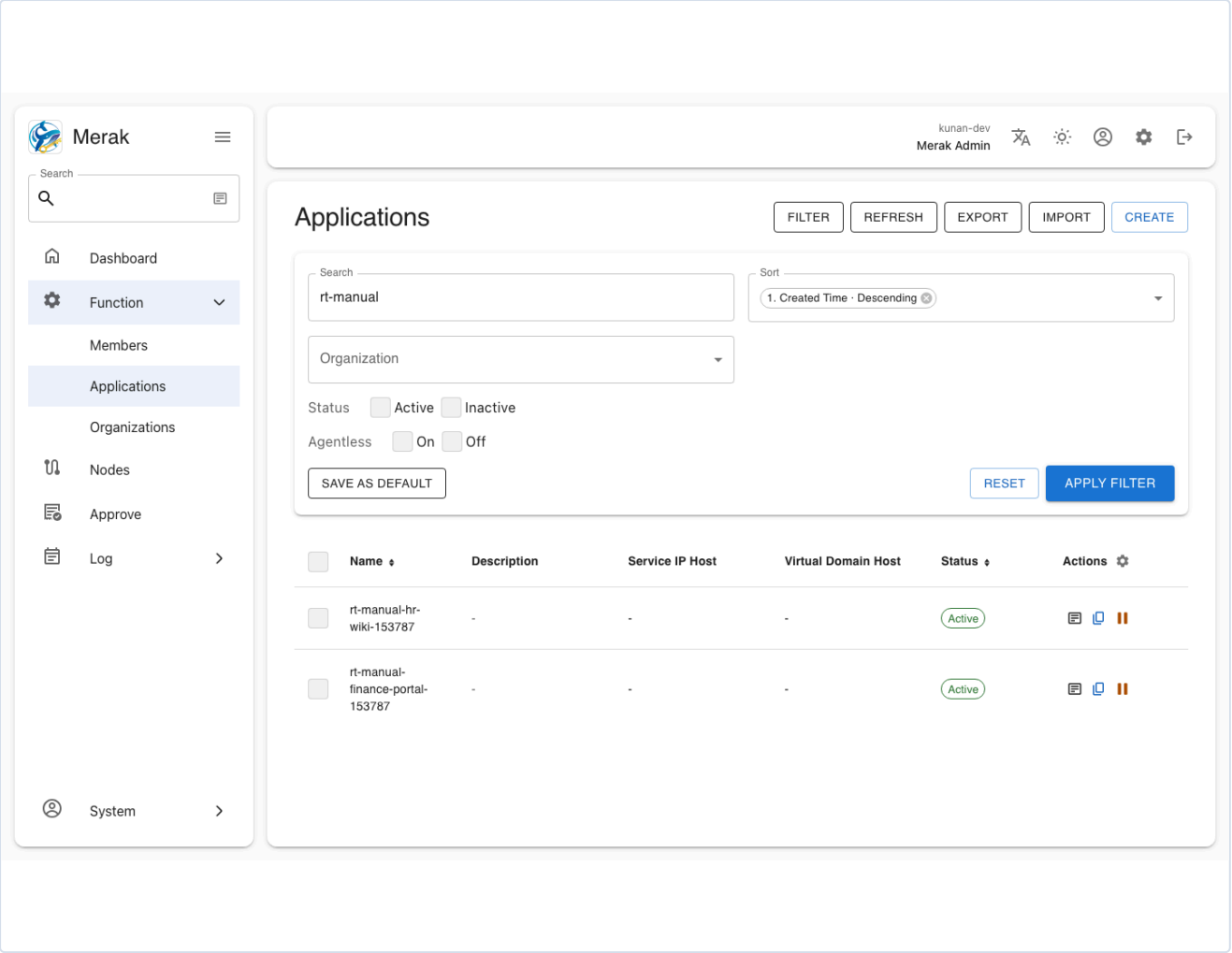
確認設定無誤後點「**建立**」，再點「**完成**」關閉視窗。

9. 建立新應用程式

適用對象：具管理員權限者。**用途**：在 Merak Console 中新增一個應用程式，並設定服務主機與授權對象。

步驟 1　開啟應用程式管理頁

於瀏覽器導航至 `https://console.merak.kunansec.com/application` 。



步驟 2　新增應用程式

點擊「**建立**」按鈕。

步驟 3　填寫基本資訊

欄位	說明
應用程式名稱 *	必填。輸入此應用程式的名稱。
描述	選填。輸入應用程式用途說明。

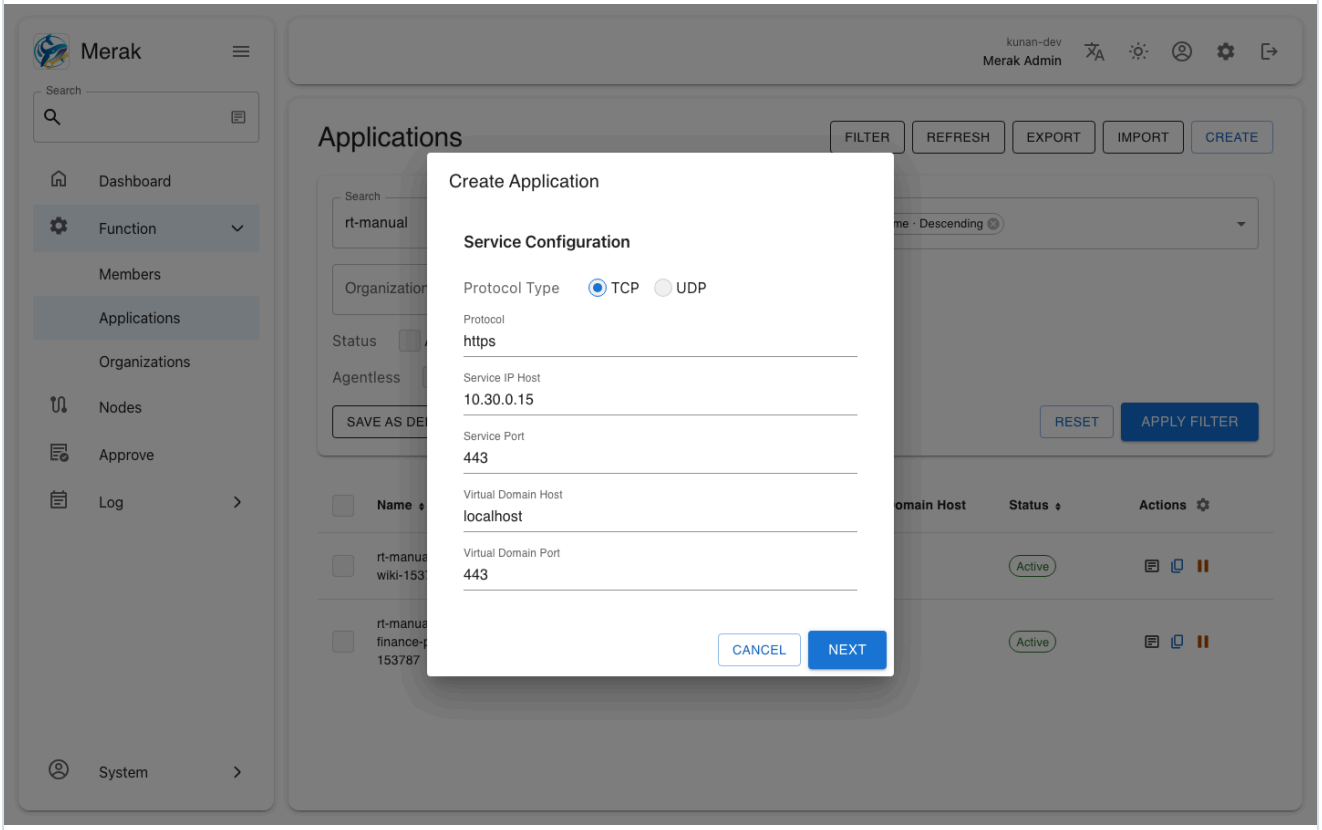
填妥後點「**下一步**」。

步驟 4　設定服務主機

1. 點擊「**服務 IP 主機**」欄位，輸入該應用程式對應的服務 IP 主機。
2. 填寫「**虛擬 DNS**」，例如：`test.web`，port `443`。

> 【注意】盡量避免使用一般的 DNS 命名方式（例如 `google.com`）。建議採用「**服務名稱 + 公司縮寫**」的命名方式。

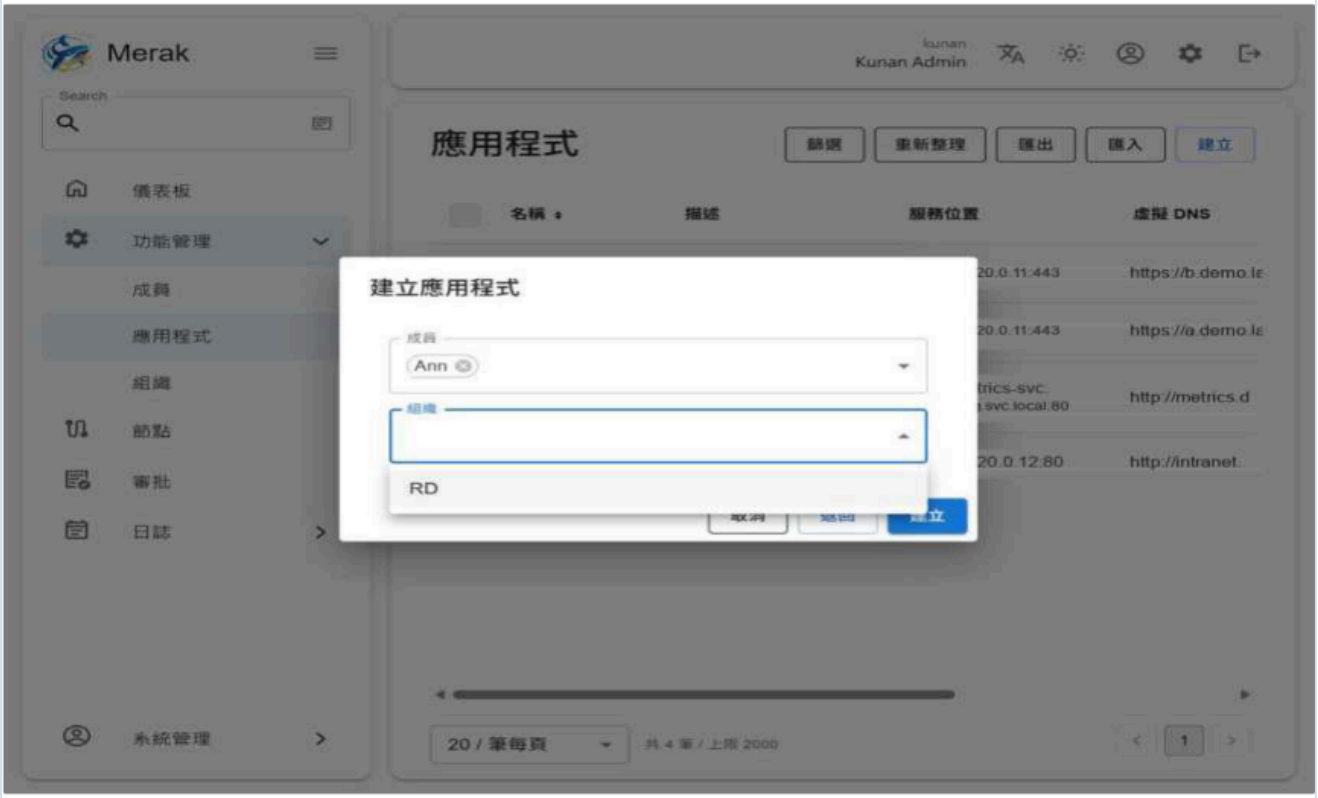
填妥後點「**下一步**」。



步驟 5　指定授權對象

選擇可存取此應用程式的**使用者**與**角色／群組**：

- 於清單中點選要授權的使用者（例如：`Ann`）。
- 選擇對應的角色／群組（例如：`RD`）。



步驟 6　建立並完成

1. 確認以上設定無誤後，點擊「**建立**」。
2. 出現完成畫面後，點擊「**完成**」，結束新增流程。

10. 設定 Agentless 存取

適用對象：具管理員權限者。**用途**：為指定應用程式開啟 **Agentless**，讓使用者**免安裝 Merak Agent**、直接用瀏覽器經入口網址存取該應用；並授權可使用的成員。

> 【提示】什麼是 Agentless？Agentless 透過指定的虛擬網域（網域／服務位址／服務埠）提供存取，使用者可直接用瀏覽器連線、免安裝客戶端程式。

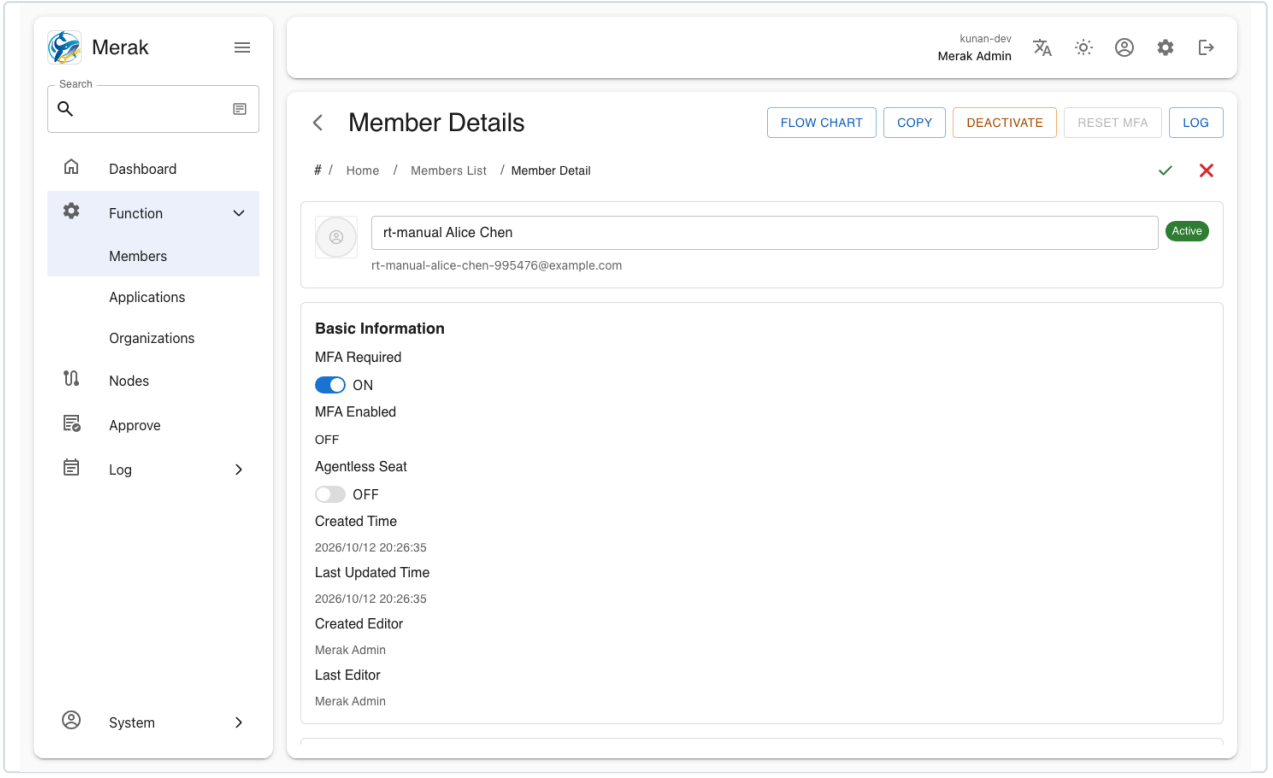
前置需求

- 目標應用程式已建立，並已設定好「虛擬 DNS」與「虛擬 DNS 埠」（參見〈9. 建立新應用程式〉）。
- 欲授權的成員，已於其「成員詳情頁」開啟「Agentless 存取」。未開通者在授權清單中會被鎖住、無法勾選（開通步驟見下方〈事前準備〉）。

事前準備：開通成員的 Agentless 存取

授權前，須先在成員詳情頁開啟「Agentless 席次」，並確認該成員已被授權存取目標服務，才能為他新增 Agentless 應用程式。

1. 於瀏覽器導航至 `https://console.merak.kunansec.com/member`。
2. 在成員列表中，點目標成員操作欄的第一個圖示，進入「成員詳情」頁。
3. 點右上角的「編輯（鉛筆）」圖示。
4. 於「基本資訊」區塊，將「**Agentless 席次**」開關切換為 ON。

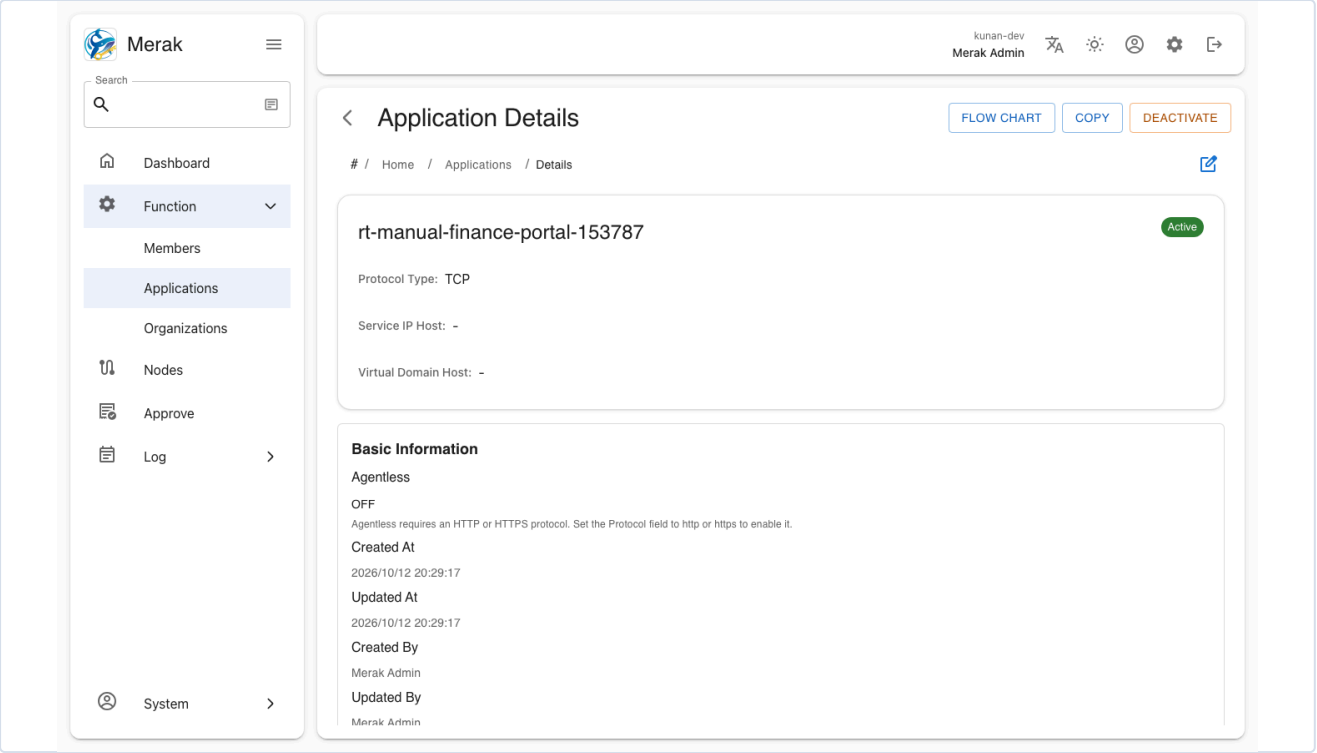


5. 點右上角的**綠色勾勾（儲存）**。
6. 確認「**允許的應用程式**」區塊已列出要開放的服務（例如：`intranet`）。若沒有，請先為該成員授權應用程式（參見〈5. 新增成員〉步驟 4）。
7. 向下捲動至「**Agentless 應用程式**」區塊，點右側的「⋮」圖示（編輯 Agentless 應用程式），開啟「管理 Agentless 應用程式」視窗。
8. 視窗中若顯示「此成員尚未綁定任何 Agentless 應用程式」，點「**編輯**」新增。

> 【注意】成員須先被授權存取該服務（出現在「允許的應用程式」中），才能新增該服務的 Agentless 存取。

步驟 1　開啟應用程式詳情

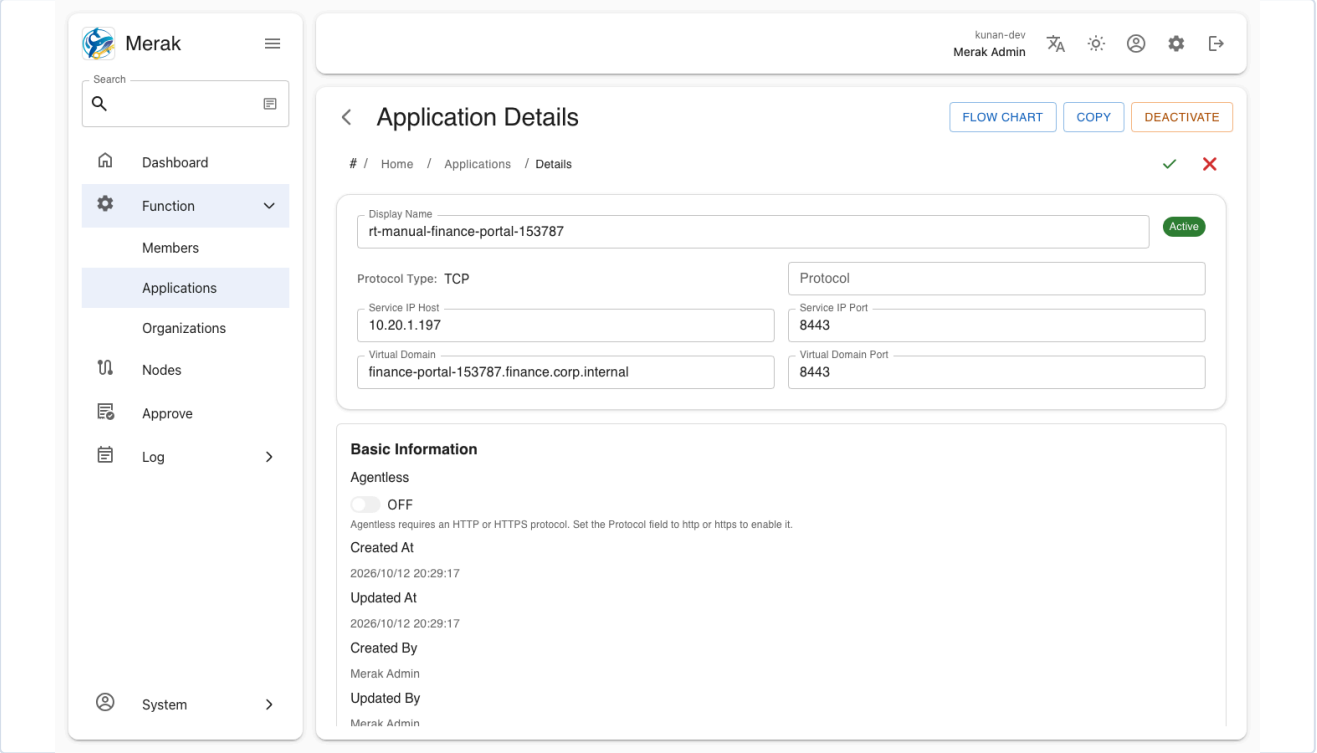
於主控台左側「**應用程式**」清單點選目標應用，進入「**應用程式詳情**」。畫面會顯示該應用的綁定設定與 Agentless 區塊。



步驟 2　開啟 Agentless

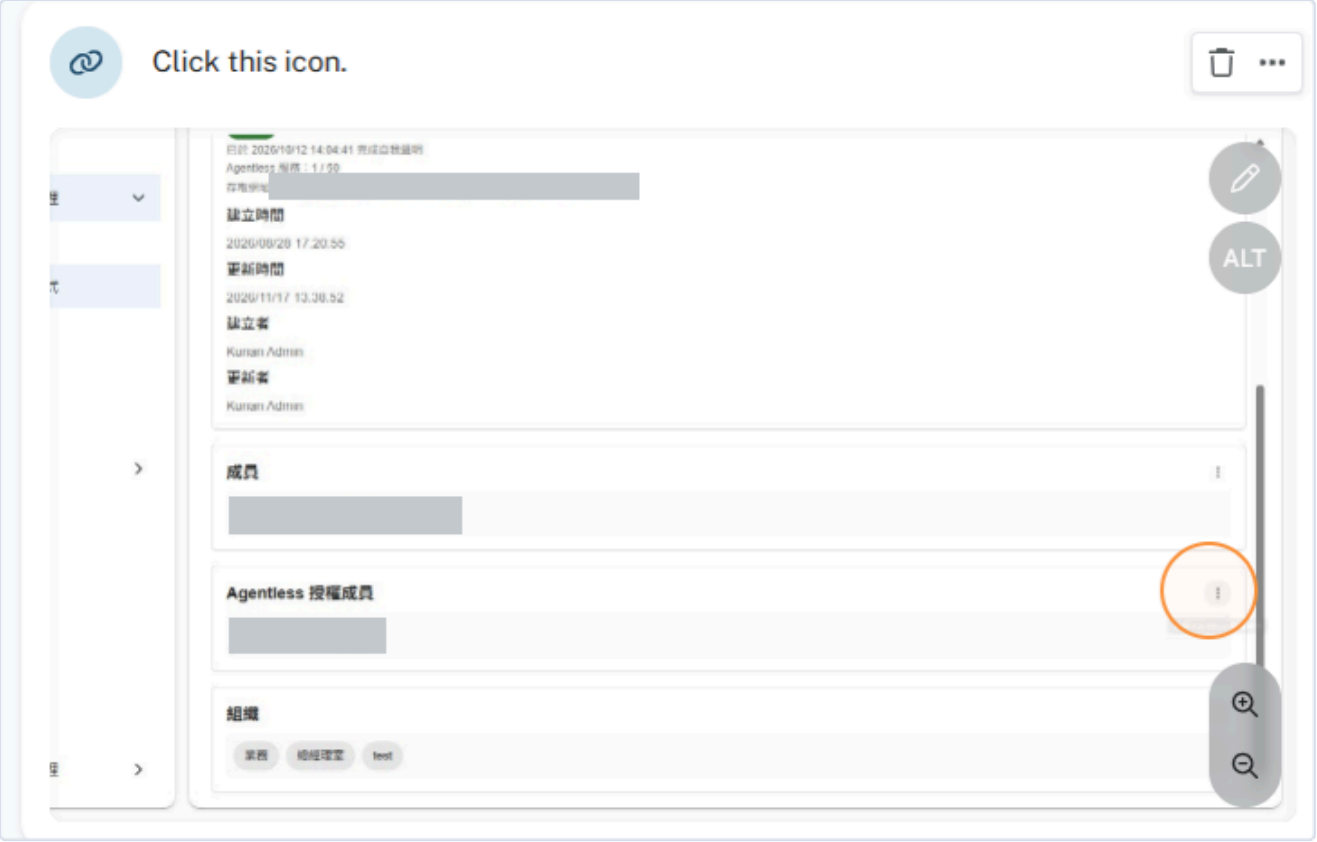
1. 點右上角的「編輯（鉛筆）」圖示進入編輯模式。
2. 於「**基本資訊**」區塊，將 **Agentless** 開關切換為 **ON**。
3. 點右上角的「綠色勾勾（儲存）」完成設定。

> 開啟後，「**存取網域**」即為使用者免安裝 Agent、直接用瀏覽器登入使用的入口網址。



步驟 3　開啟授權成員管理

向下捲動至「**Agentless 授權成員**」區塊，點該區塊右側的「⋮」圖示，開啟「**管理 Agentless 存取權**」視窗。



步驟 4　進入編輯

於「**管理 Agentless 存取權**」視窗點「**編輯**」。

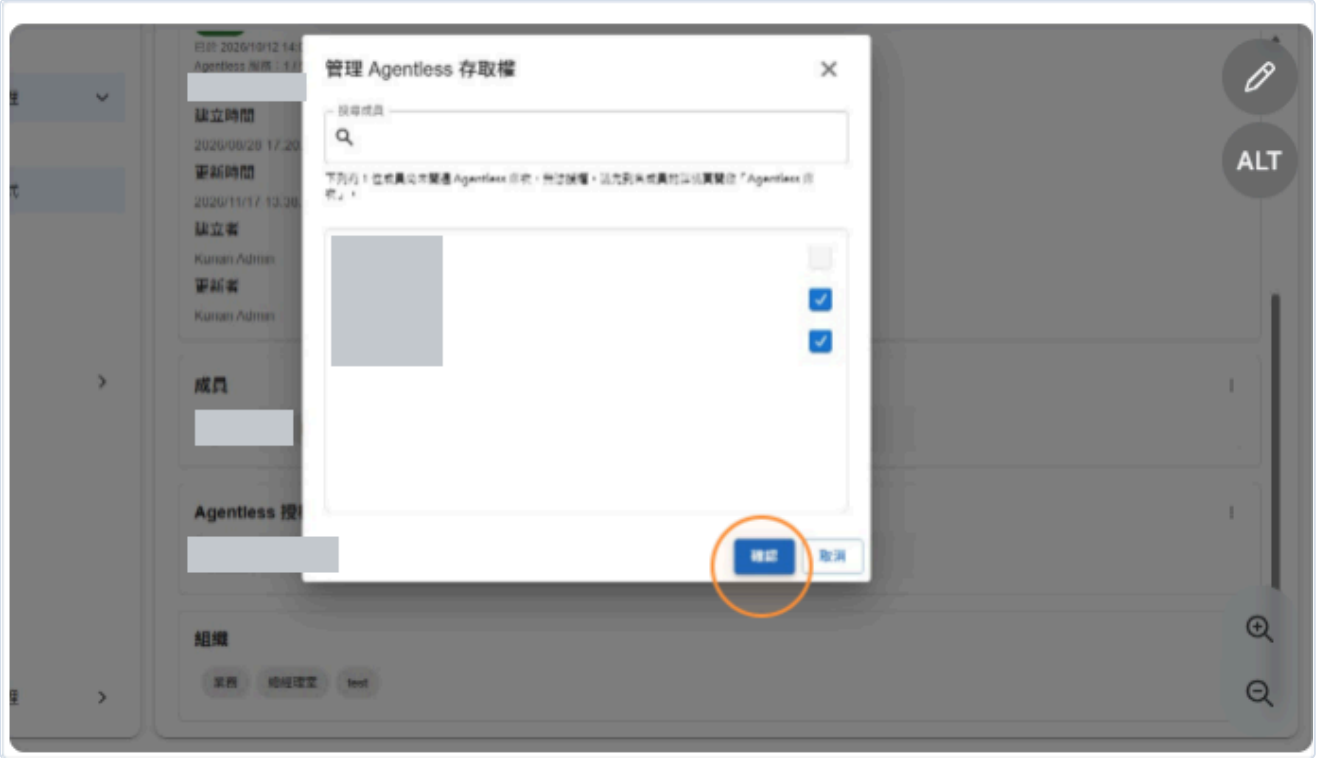
步驟 5　勾選要授權的成員

勾選要開放 Agentless 存取的成員。

> 【注意】尚未開通「Agentless 存取」的成員會被鎖住、**無法勾選**。視窗上方會提示「下方列 N 位成員尚未開通 Agentless 存取，無法授權，請先到成員的詳情頁開啟『Agentless 存取』」。請先到該成員的詳情頁開啟後，再回到此處授權。

步驟 6　確認

點「**確認**」儲存授權。被授權的成員即會出現在「**Agentless 授權成員**」清單中。



使用者端

被授權的成員，直接用瀏覽器開啟該應用的「**存取網域**」（入口網址）登入使用即可，**無需安裝 Merak Agent**。

稽核日誌

查詢與匯出成員的連線紀錄，以及後台操作的稽核紀錄。

11. 查詢與匯出日誌

適用對象：具管理員權限者。**用途**：查詢成員存取應用程式的連線紀錄，以及後台的登入與操作紀錄，並匯出成 CSV 檔案。

Merak Console 左側「**日誌**」選單下有兩種日誌：

日誌	記錄內容
連線日誌	成員何時、用哪個裝置連到哪個應用程式
稽核日誌	誰在何時做了什麼操作，例如登入、建立組織、修改成員

A. 查看連線日誌

步驟 1　開啟連線日誌——於瀏覽器導航至 `https://console.merak.kunansec.com/connection-log`，或點左側「日誌」→「連線日誌」。列表欄位包含：建立時間、結束時間、成員、裝置、應用程式。

步驟 2　查看單筆明細——點該筆紀錄「操作」欄的「檢視詳情」圖示，開啟「連線詳情」視窗，可看到連線時長、建立／結束時間、成員、裝置、應用程式、用戶端 IP 與路由路徑。看完點「**關閉**」。

步驟 3　匯出——點右上角「**匯出**」，視窗會顯示「要將符合目前篩選的 N 筆資料匯出成 CSV 檔案嗎？」。點「**確認**」下載；不匯出則點「取消」。

B. 查詢稽核日誌

步驟 1　開啟稽核日誌——點左側「日誌」→「**稽核日誌**」。列表欄位包含：建立時間、操作者、標題、內容、身分（如管理員、系統）。

步驟 2　開啟篩選——點右上角「**篩選**」，展開查詢條件。

步驟 3　設定條件——依需要填寫或選擇條件，例如於「類型」選「操作」。可用的條件如下，設定後點「**搜尋**」；點「重設」可清除條件，點「存為預設」可保留常用條件。

條件	說明
類型	登入、操作、錯誤
狀態、動作、資源類型	下拉選單
起始時間、結束時間	查詢的時間區間

條件	說明
IP 位址、Request ID、資源 ID、狀態碼、路徑	輸入關鍵字

步驟 4　匯出——點右上角「**匯出**」，系統會匯出符合目前篩選條件的資料。在確認視窗點「**確認**」下載 CSV；不匯出則點「取消」。

> 【提示】匯出的筆數以目前的篩選條件為準。要匯出特定期間或特定類型的紀錄，請先設好篩選再匯出。

系統管理

角色權限與管理員帳號管理。

12. 建立與管理角色

適用對象：具管理員權限者。**用途**：在 Merak Console 中建立角色、設定權限，或刪除既有角色。

> 【提示】角色（Role）定義一組權限，可指派給管理員（參見〈13. 建立新管理員〉）。

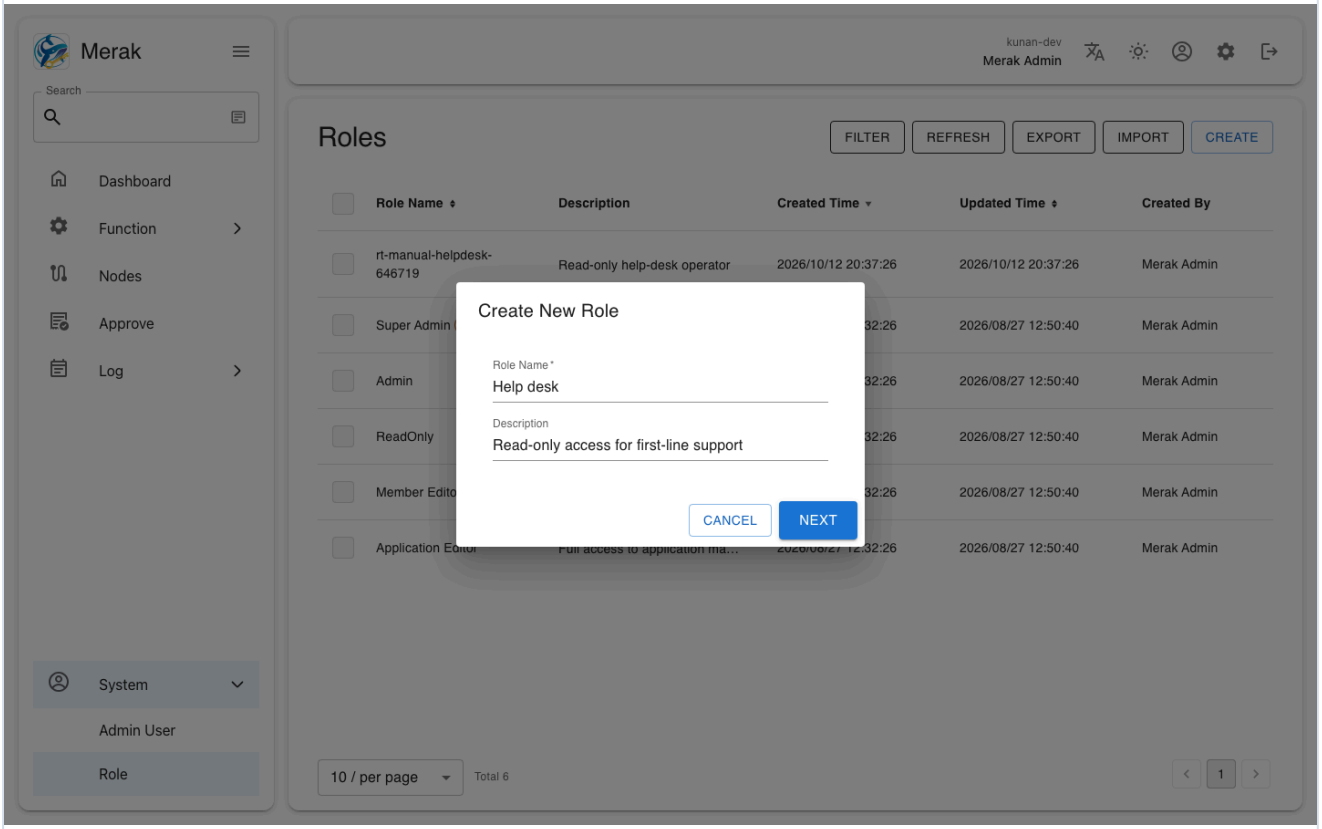
A. 建立新角色

步驟 1　開啟角色管理頁——於瀏覽器導航至 `https://console.merak.kunansec.com/role`。

步驟 2　新增角色——點擊「**建立**」。

步驟 3　填寫角色基本資訊

欄位	說明
角色名稱 *	必填。輸入角色名稱（例如：`test rule`）。
描述	選填。輸入角色用途說明。

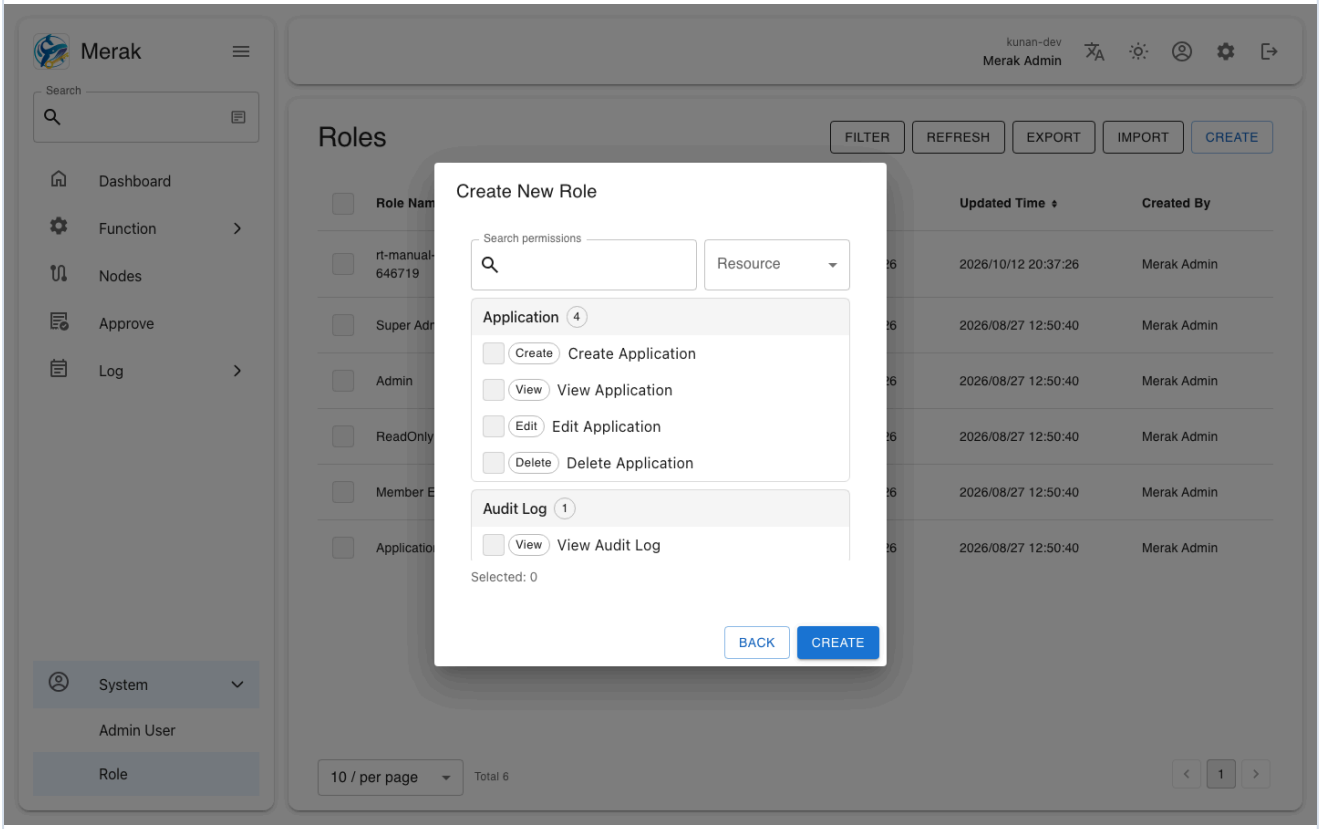


填妥後點「**下一步**」。

步驟 4　設定權限——為此角色勾選各項資源的權限。權限以「資源 × 動作」方式設定，常見動作包含檢視、編輯、建立等。可設定的資源與權限如下：

資源	可設定的權限
應用程式	檢視應用程式、編輯應用程式
稽核日誌	檢視稽核日誌
設備	檢視設備、編輯設備
授權	檢視授權、編輯授權
成員	檢視成員、編輯成員
Merak 節點	檢視節點、編輯節點
組織	新增／建立組織
權限	檢視權限

資源	可設定的權限
角色	檢視角色、編輯角色
租戶	檢視租戶
Token 申請	檢視 Token 申請、編輯 Token 申請
管理員	檢視管理員、編輯管理員



步驟 5　建立並完成——確認權限設定無誤後點「**建立**」，再於完成畫面點「**完成**」。

B. 刪除角色

步驟 1　開啟角色管理頁——於 `https://console.merak.kunansec.com/role` 找到欲刪除的角色。

步驟 2　選取角色——勾選目標角色（例如：`test rule`），可點「**檢視選取（1）**」確認已選取的項目。

步驟 3　刪除——點擊「**刪除**」，再於確認視窗點「**確認**」完成刪除。

13. 建立新管理員

適用對象：具管理員權限者。**用途**：在 Merak Console 中新增一個管理員帳號並指派角色。

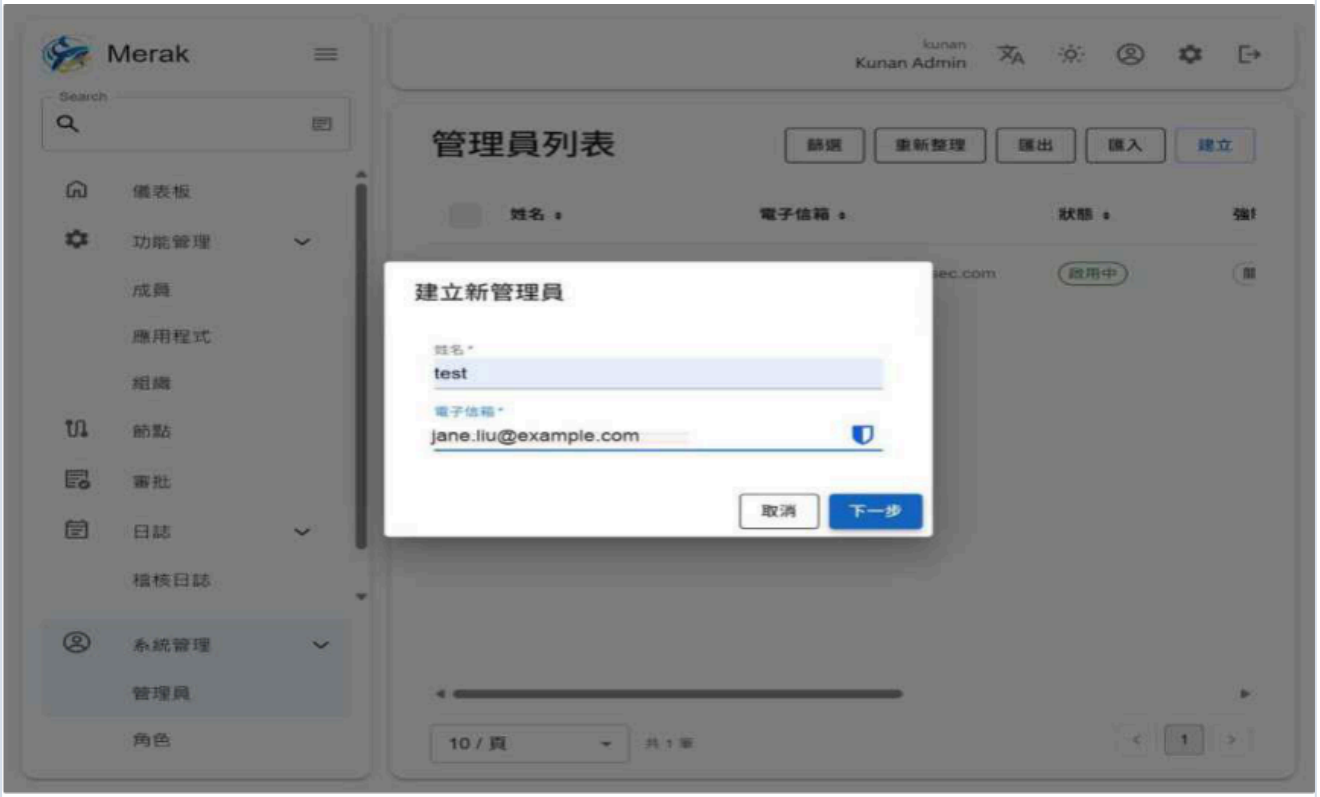
> 【提示】建立完成後，新管理員會以「待處理」狀態列於清單，並收到啟用邀請信（參見〈1. 帳號啟用指南〉）。

步驟 1　開啟系統管理頁

進入系統管理頁面。

步驟 2　填寫管理員基本資訊

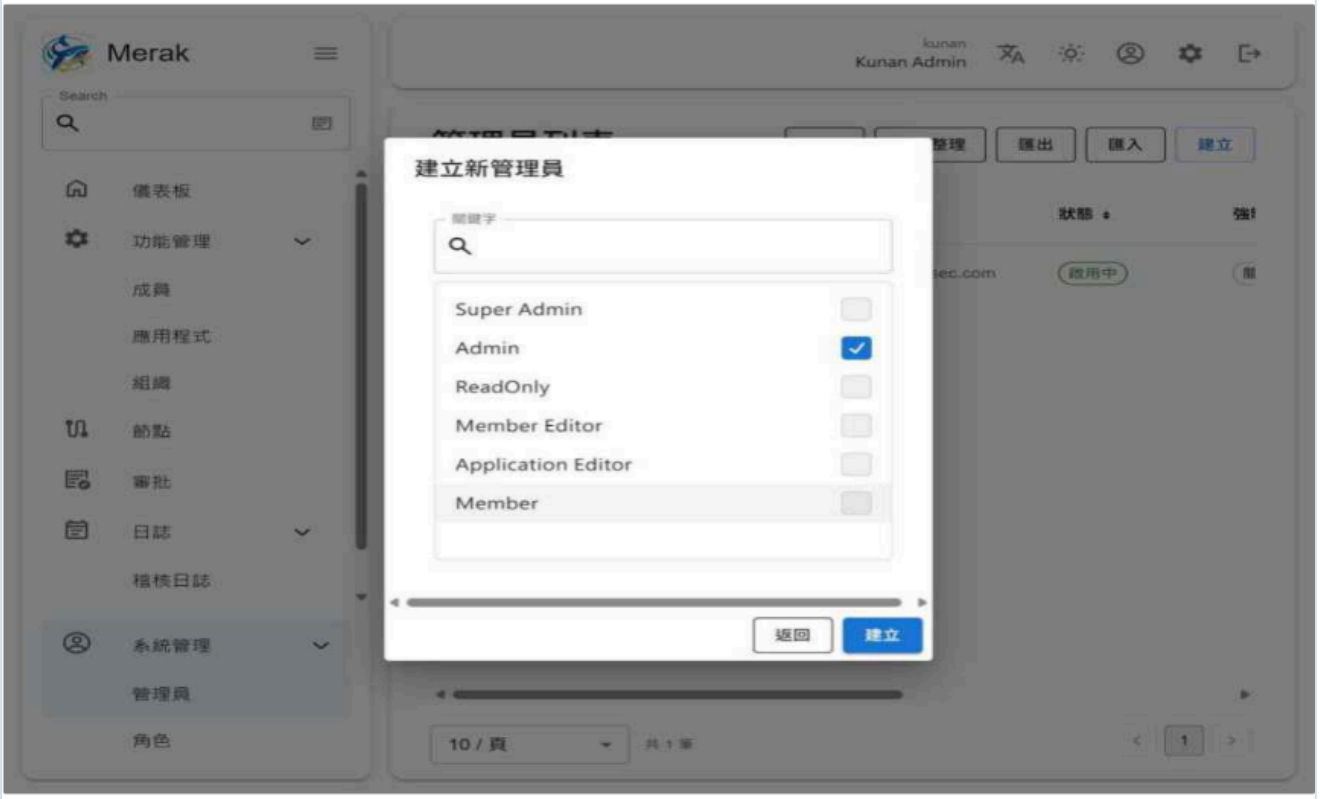
欄位	說明
姓名 *	必填。輸入使用者姓名。
電子信箱 *	必填。輸入使用者電子郵件（例如：`sample@your-company.com`）。此信箱將作為登入帳號並用於接收啟用邀請信。



填妥後點「**下一步**」。

步驟 3　指派角色

選擇要指派給此管理員的角色，例如「**Admin**」。



步驟 4　建立並完成

1. 確認設定無誤後，點擊「**建立**」。
2. 出現完成畫面後，點擊「**完成**」，結束新增流程。

步驟 5　確認結果

回到清單，可看到新建立的帳號，狀態為「**待處理**」，並顯示 MFA（多因素驗證）設定欄位。待使用者完成啟用後，狀態即會更新。

附錄

常見問題彙整與設備認證狀態對照。

附錄 A：常見問題彙整

使用者（帳號啟用與 Agent）

狀況	處理方式
沒收到啟用信	檢查垃圾信匣；確認信箱正確；聯繫管理員重寄邀請。
連結失效或已過期	啟用連結時效為 24 小時，請聯繫管理員重寄。
兩次密碼不一致	重新輸入。
Agent 登入失敗	確認帳號為信箱全名；確認 Agent 版本；仍失敗請聯繫管理員。
忘記密碼	於 Merak Agent 上點按「FORGOT PASSWORD／忘記密碼」重設。
送出註冊後一直停在 Auditing	設備註冊需管理員於主控台「批准」頁面核准，請聯繫管理員。

管理員（成員管理）

狀況	處理方式
成員未收到邀請信	對方檢查垃圾信匣；確認信箱拼寫；於成員列表重寄邀請。
信箱重複	該信箱已存在於組織，請搜尋既有帳號並調整權限。

管理員（節點）

問題	處理方式
安裝後立即中止	確認為 Ubuntu Server 24.04 LTS 以上版本。
JWT 過期	於節點詳情點「重新產生 JWT」。
狀態停在「等待佈署」	確認網路連線並重新執行安裝腳本。
忘記下載 install.sh	於節點頁面點「下載安裝包」重新下載。

附錄 B：設備認證狀態對照表

Status 狀態	中文說明	對應動作
Unregistered	未註冊	需點擊「REQUEST REGISTER」送出註冊請求。
Auditing	審核中	等待管理員批准。
Not connected	未連線	已批准，可點擊「START」啟動連線。
Connected	已連線	連線中，可點擊「CLOSE」中斷連線。