



桃園區網 eduroam
向上集中前置作業_學校端

2024.10.17 謝勝任

大綱

- 自建與向上集中 eduroam 架構&比較
- 如何取得學校端 Google LDAP 憑證&金鑰
- 填寫桃園區網 eduroam 向上集中申請單
- IOS載具連接方式
- Android 11以上版本 連接方式
- Windows 連接方式
- MAC 連接方式



自建與向上集中 eduroam 架構&比較

自建 eduroam 驗證伺服器架構

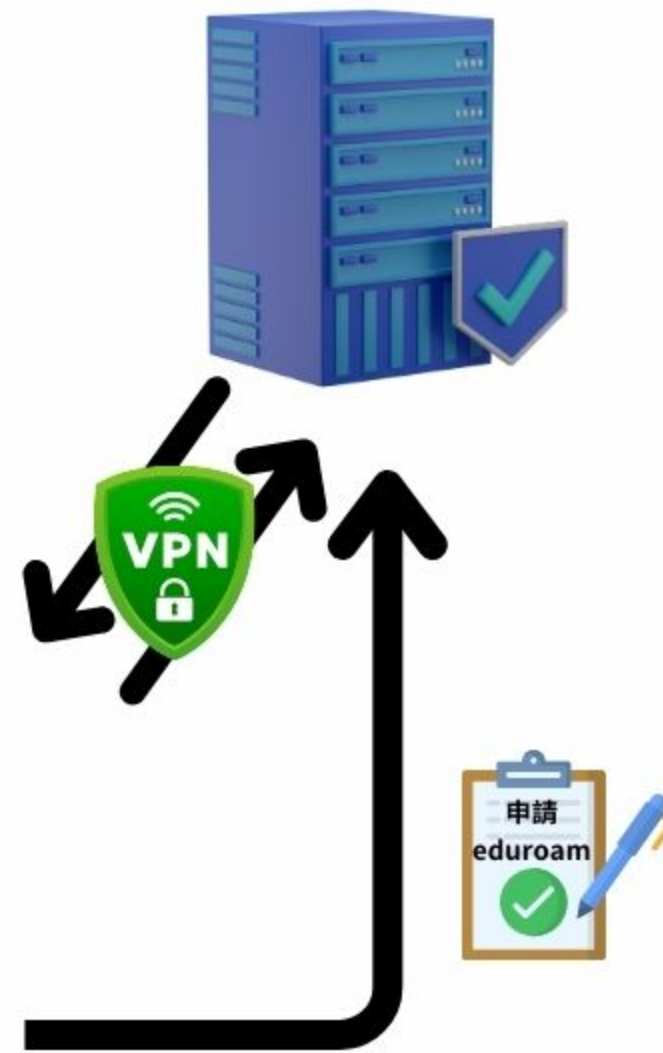
Google 建立LDAP
憑證&帳號認證



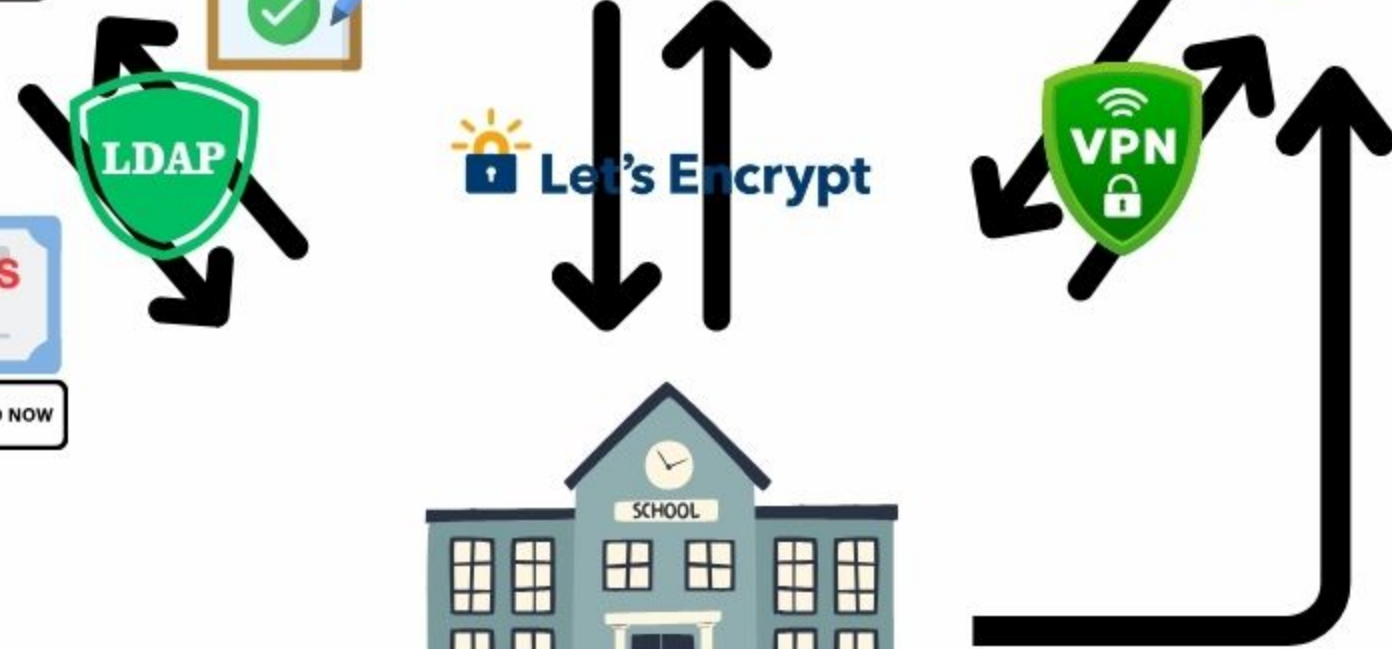
網域憑證認證
伺服器



漫遊中心
eduroam 伺服器

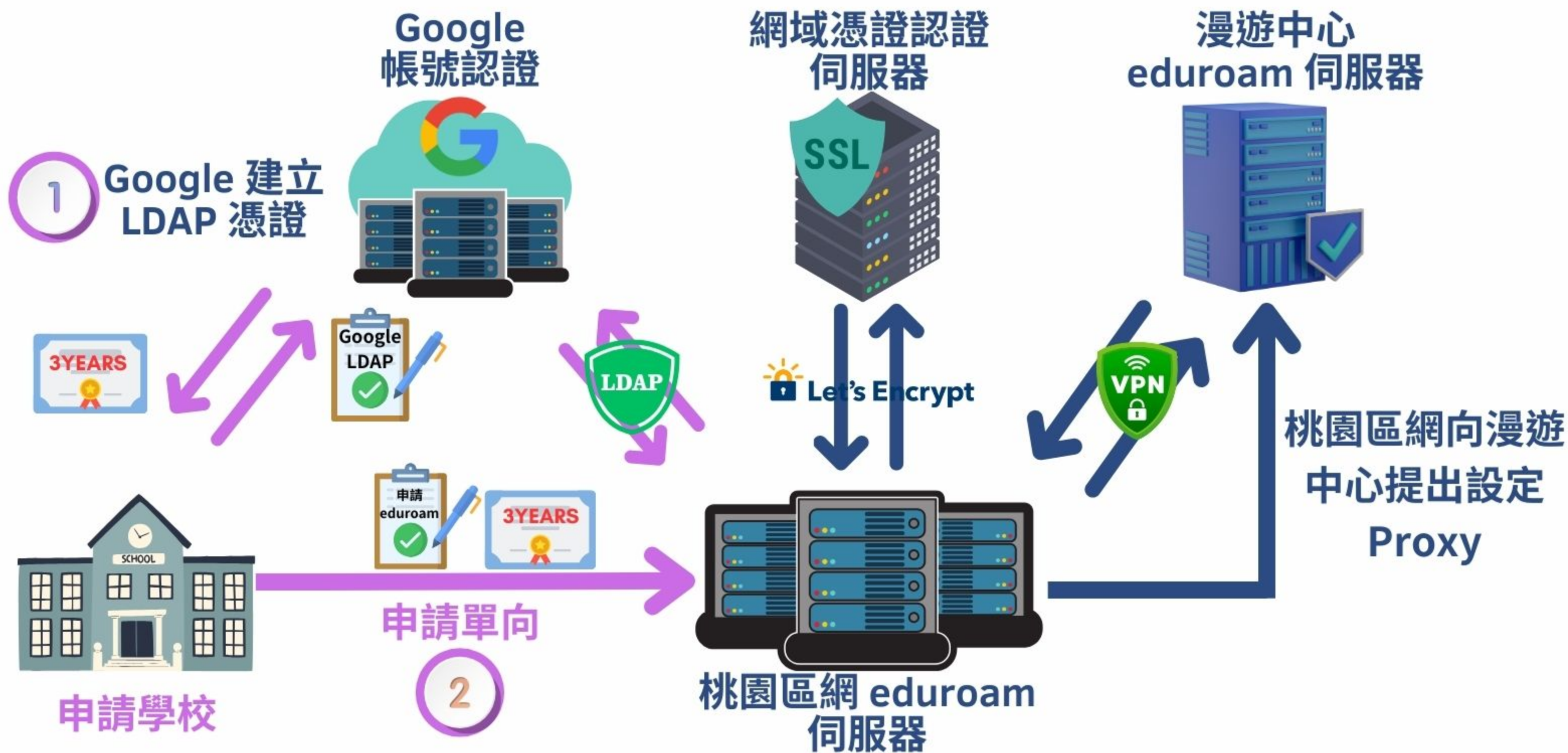


學校自建 eduroam
伺服器



桃園區網 eduroam 向上集中服務
申請單向???
申請雙向???

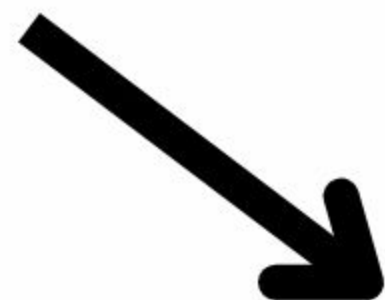
桃園區網 eduroam 向上集中架構(申請單向服務)



桃園區網 eduroam 向上集中架構(申請單向服務)



校內**無** eduroam SSID

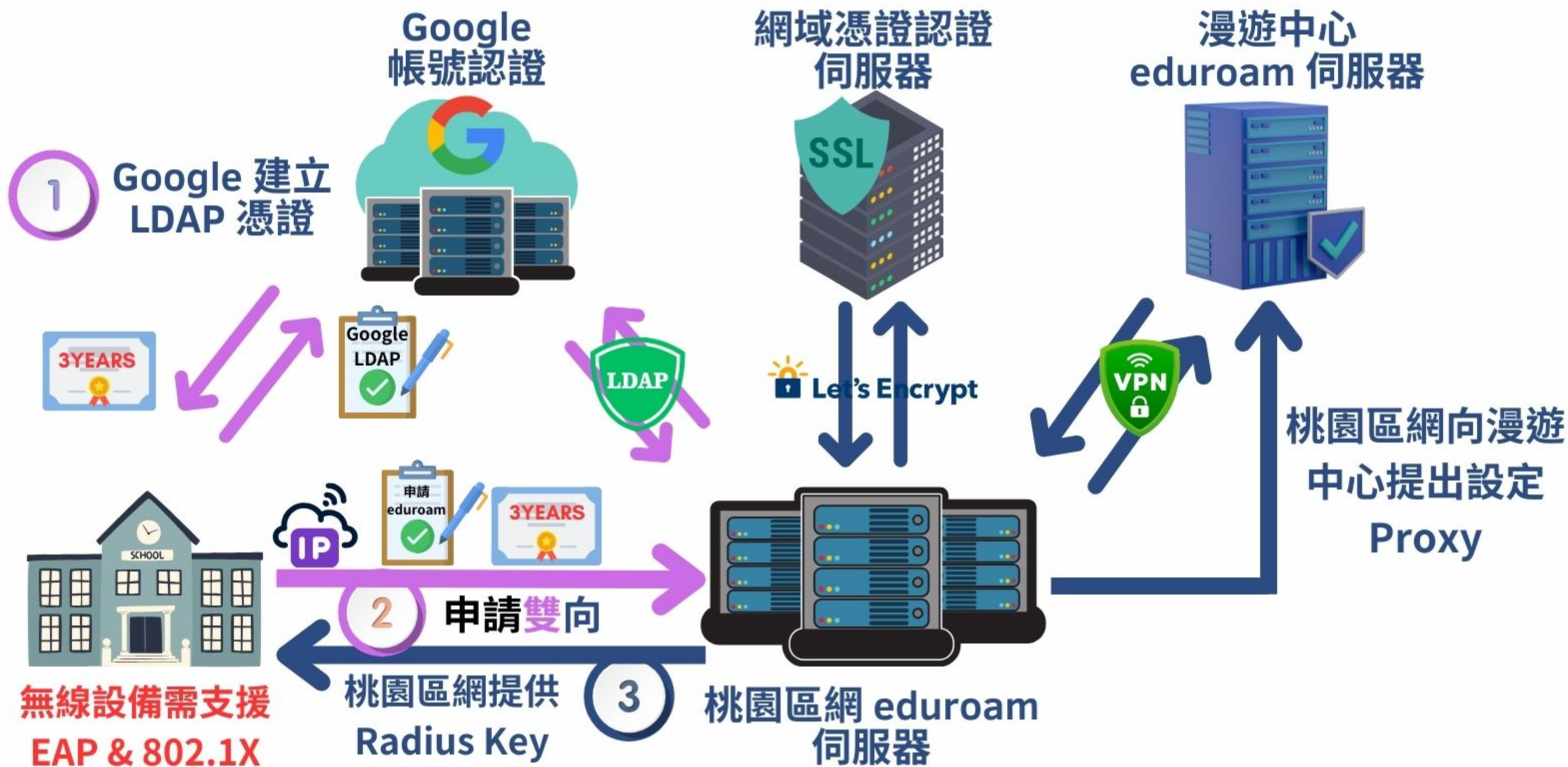


至它校時可使用學校
Google帳號
直連 eduroam SSID



它校**有** eduroam SSID
有申請向上集中服務或自建 eduroam

桃園區網 eduroam 向上集中架構(申請雙向服務)



桃園區網 eduroam 向上集中架構(申請雙向服務)

1. 可使用學校Google帳號直連
2. 它校來校時可直連eduroam



校內**有** eduroam SSID
有申請向上集中雙向服務



至它校時可使用學校
Google帳號
直連 eduroam SSID



它校**有** eduroam SSID
有申請向上集中服務或自建eduroam



自建 eduroam 與 向上集中 eduroam 比較

Search

項目	自建 eduroam 伺服器	向上集中 eduroam 伺服器
漫遊中心 OPEN VPN 憑證	自行申請	免申請 由桃園區網管理 
網域SSL憑證	自行申請	免申請 由桃園區網管理 
Google LDAP憑證	自行申請每三年更換	自行申請每三年更換
硬體維護	自行維護	由桃園區網維護 
安全性	佳	優 
需要Linux技術	進階	無
無線網路設備支援度	需支援EAP & 802.1X驗證，無法支援此驗證模式，僅可申請單向	

A person in a white shirt is handing a white sign to another person in a dark suit. The sign has the text "Google LDAP" written on it.

Google
LDAP

如何取得 Google LDAP 憑證 與 金鑰

Google LDAP 獲取憑證 & 金鑰五步驟

需使用 Google 最高管理員帳號登入

1

STEP

建立LDAP



2

STEP

設定存取權限



3

STEP

下載產生的憑證



4

STEP

啟用服務



5

STEP

建立存取憑證金鑰





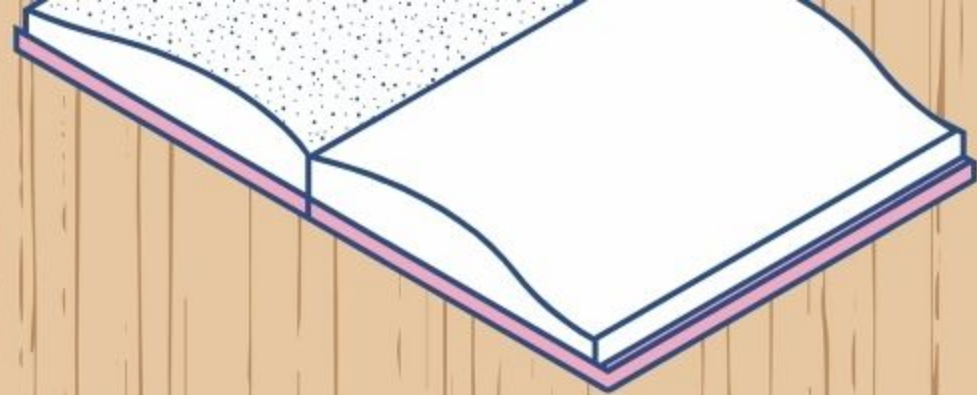
STEP 1

請先至Google控制台

- 左邊選單選擇「應用程式」
- 展開後選擇「LDAP」

PS.此動作需要Google最高管理員權限





建立 Google LDAP

- 右上點選「新增用戶端」
- 輸入「LDAP用戶端名稱」

PS.LDAP 用戶端名稱
只是辨識用途不影響認證



LDAP 用戶端名稱*

STEP 2

設定 Google LDAP 權限-驗證使用者憑證

驗證使用者憑證

- 可以選擇「整個網域」
- 也可以選擇單一機構或群組

PS.此權限代表指定的機構
或群組可以使用此 LDAP 認證

驗證使用者憑證

指定用戶端的存取層級以驗證使用者憑證。設定變更最多可能需要 24 小時才會生效。

- 整個網域 (lhvs.tyc.edu.tw)
- Selected organizational units, groups and excluded groups

驗證使用者憑證

指定用戶端的存取層級以驗證使用者憑證。設定變更最多可能需要 24 小時才會生效。

- 整個網域 (lhvs.tyc.edu.tw)
- Selected organizational units, groups and excluded groups

包含的機構單位

1 個機構單位 [編輯](#)

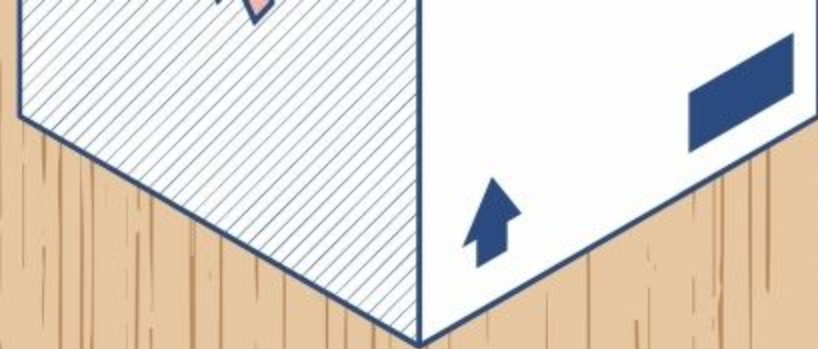
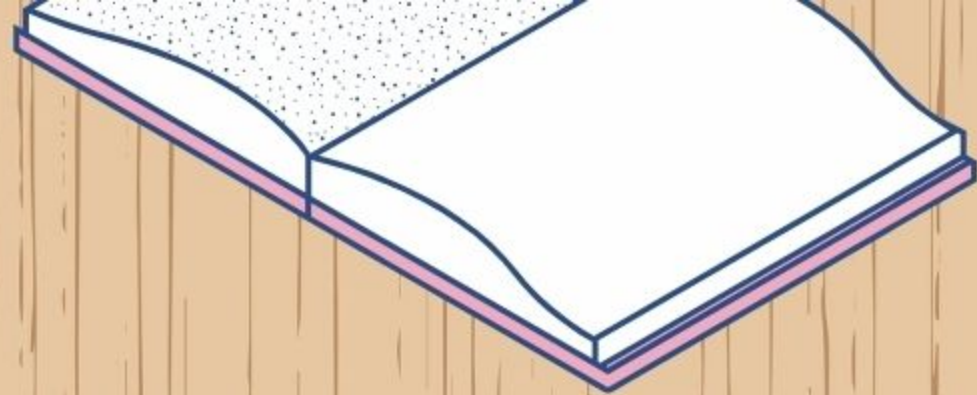
- 無存取權

已納入的群組

[新增](#)

已排除的群組

[新增](#)



設定 Google LDAP 權限-讀取使用者資訊

讀取使用者資訊

- 可以選擇「整個網域」
- 也可以選擇單一機構

PS.此權限代表允許指定的
機構單位可以讀取使用者屬性
必須與 驗證使用者憑證 權限對應

讀取使用者資訊

指定用戶端的存取層級以讀取使用者資訊。部分用戶端需要額外資訊才能驗證使用者。 ?

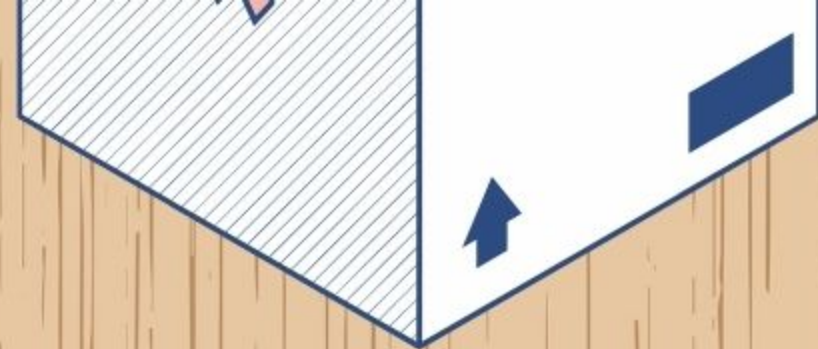
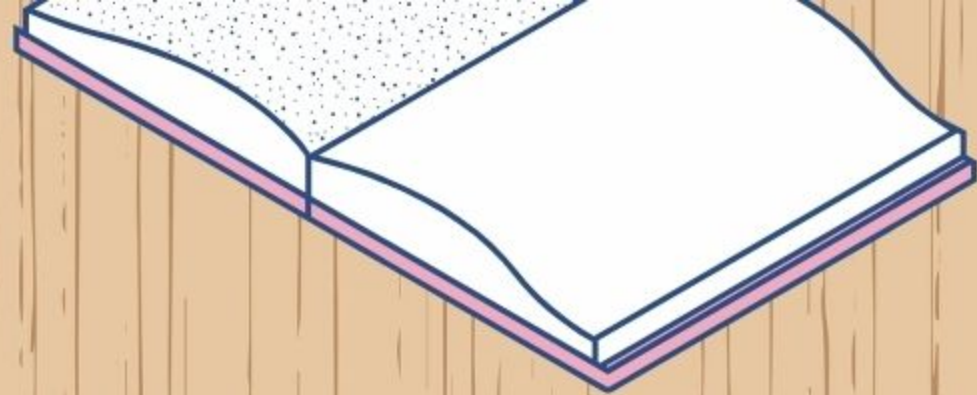
- 整個網域 (lhvs.tyc.edu.tw)
- Selected organizational units
- 無存取權

- 整個網域 (lhvs.tyc.edu.tw)
- Selected organizational units

包含的機構單位 - 從「驗證使用者憑證」面板複製

1 個機構單位 編輯

- 無存取權



設定 Google LDAP 權限-讀取群組資訊

讀取群組資訊

- 預設是「關閉」
- 都設定完成後請點「新增LDAP用戶端」

PS.此權限代表允許讀取群組屬性

讀取群組資訊

用戶端可讀取群組資訊。部分用戶端需要額外資訊才能驗證使用者



新增LDAP用戶端





STEP 3 下載 Google LDAP 憑證

- 點選「下載憑證」
- 並將憑證提供給桃園區網

PS.此憑證從產生起**3年內有效**
3年後必須自行重新產生
並重新提供給桃園區網更新

接下來，將您的用戶端連上 LDAP 服務

1. 下載產生的憑證 (產生過程可能需要幾分鐘)。

不想立即執行這項作業嗎？您隨時可以透過用戶端的詳細資料頁面產生並下載憑證。

Google_2027_09_13_27785

到期日：2027年9月13日

[↓ 下載憑證](#)



2. 將憑證上傳到 LDAP 用戶端並設定應用程式。您可能要有 LDAP 存取憑證才能進行設定。[瞭解詳情](#)



STEP4 啟用 Google LDAP 服務

- 下載憑證完成後請點「繼續前往用戶端詳細資料」
- 點選「服務狀態」
- 點選「為所有人啟用」
- 點選右下角「儲存」




繼續前往用戶端詳細資料

服務狀態

關閉

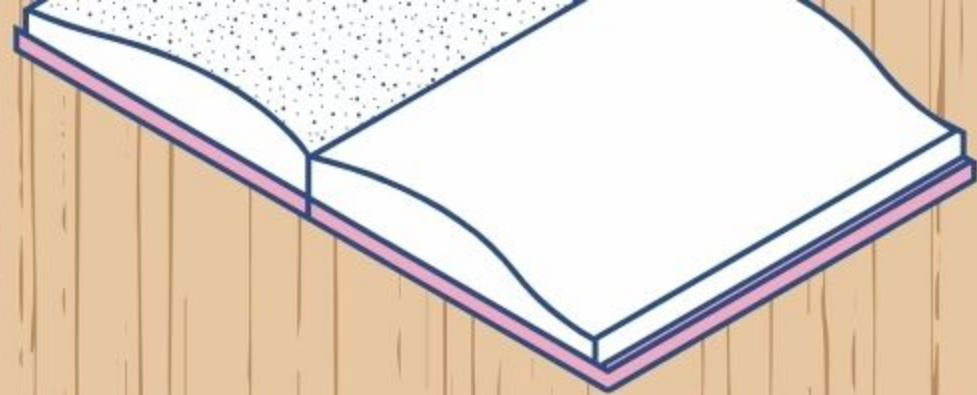
為所有人啟用

為所有人關閉

 大部分的變更會在幾分鐘內生效。瞭解詳情



儲存



STEP5 建立存取憑證金鑰

- 點選「驗證」區塊
- 點選「產生新憑證」

驗證



憑證

這個 LDAP 用戶端已經與 1 個憑證建立關聯

存取憑證

這個 LDAP 用戶端已經與 0 個存取憑證建立關聯



這個 LDAP 用戶端沒有任何存取憑證。

產生新憑證



建立存取憑證金鑰

- 產生存取憑證
- 請將此「使用者名稱」、「密碼」提供給桃園區網
- 此密碼請在此畫面複製留存，**關閉後將無法再次查看密碼**

PS. **此密碼請勿外流**

「TEST」的存取憑證

使用下列憑證設定這個用戶端的 LDAP 服務存取權：

使用者名稱

CluelessGo

密碼

rTFnd4HDbFyhH4q7yehgNb57

按一下即可複製密碼



為了安全起見，管理控制台不會儲存及顯示這組密碼。如果日後需要重新設定這個用戶端，請產生新憑證。

關閉

重新產生存取憑證

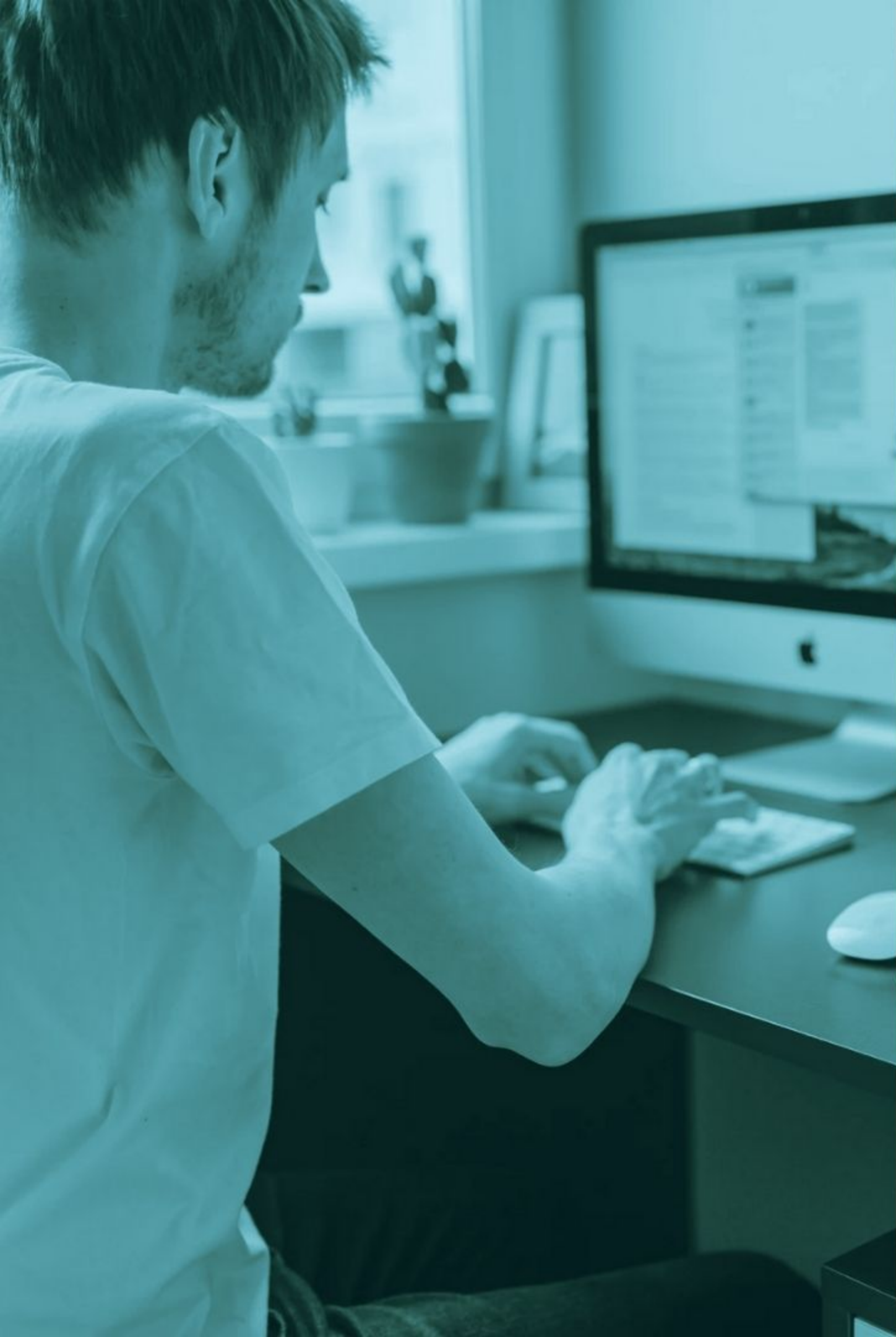
- 年限到期 可點選右上角「產生新憑證」，即可取得新的三年憑證檔案

驗證 ^

憑證
產生憑證以驗證這個用戶端的 LDAP 服務。 ?

憑證名稱 ↑	到期日	SHA-256 指紋	
Google_2027_09_13_28313	2027年9月13日	C11ED634 7DC08718 63217583 2DCAAD8D F8DE97DA 8B2C53D2 0472352D F33C2AA2	  





**填寫桃園區網
eduroam 向上集中申請單**

桃園區網 eduroam 向上集中申請單



桃園區網漫遊向上集中資訊網

TYRC Roaming Upstream Centralized Information Network.



Home



主機服務



漫遊主機



漫遊統計



各校驗證



連線測試



向上集中申請

申請單取得方式

1.與桃園區網索取檔案

2.使用線上申請

<https://eduroam.tyc.edu.tw>



桃園區網 eduroam 向上集中申請單

本申請單填寫完成後請 Email: tanet_ncu@ncu.edu.tw 或寄送桃園區網中心

申請人	王大明	申請日期	2024年 10 月 14 日
申請學校	六和高中	學校電話	034204999
電子郵件	xxx@mail.xxxx.tyc.edu.tw		
服務類型	<p>壹、請擇一勾選</p> <p><input type="checkbox"/> 申請單向無線漫遊 eduroam 向上集中服務。 (限校內無意願建置 eduroam SSID 勾選)註1</p> <p><input checked="" type="checkbox"/> 申請雙向無線漫遊 eduroam 向上集中服務。 (限校內有意願建置 eduroam SSID 勾選)註2</p> <p>(以下簡稱無線漫遊)(勾選申請代表同意以下服務條款)</p> <p>允許無線漫遊 Google 網域(至多3個)請由下方表格填寫 (申請單雙向向上集中服務均需要填寫)註3</p> <p>無線網路設備流出介面實體 IP 請由下方表格填寫 (申請雙向向上集中服務才需要填寫)註4</p> <p>桃園區網中心無線漫遊向上集中服務條款如下:</p> <p>一、桃園區網中心提供之無線漫遊向上集中服務,其所涉及系統可用性與資料完整性與機密性及權利義務關係,依本服務條款之規定辦理。</p> <p>二、執行期間,桃園區網中心依中心資訊安全規定善盡管理責任,確保該硬體與服務之運作正常。</p> <p>三、轄下連線單位需使用 Google 帳號認證,此服務需要提供 Google 串接憑證至桃園區網中心無線漫遊向上集中伺服器。</p> <p>四、Google 串接憑證效期為三年,請自行在效期到期前提供新申請之 Google 串接憑證至桃園區網中心進行更換,如效期逾期將無法提供無線漫遊認證。</p> <p>五、如 Google 網域有異動,請主動通知桃園區網中心,並重新提供 Google 串接憑證。</p> <p>六、此申請需提供一至兩位有 Google 管理權之人員,作為後續技術聯繫,申請雙向向上集中服務者需有防火牆管理權。</p>		

本申請單填寫完成後請 Email: tanet_ncu@ncu.edu.tw 或寄送桃園區網中心

七、申請雙向向上集中服務之學校如流出介面實體 IP 有異動,請主動通知桃園區網中心變更 IP。
八、服務均依雙方的資安規定進行相關防護措施,以保持系統持續營運,並確保伺服器安全與防止資安事件之發生。倘有資安事件發生,雙方得進行中斷服務,以防事件擴大。
九、雙方將依各自的資訊安全規定善盡管理責任,但不保證或擔保任何經由本服務不會遭受損毀、遺失或移除。
十、因連線載具種類眾多,如有無法連線無線漫遊之載具,請務必先行使用其他載具進行無線漫遊連線交叉測試。
十一、如需終止此服務,請聯繫桃園區網中心進行終止申請。
十二、本申請單如有未盡事宜,依桃園區網中心公告為主。
註1:申請單向向上集中服務之學校,在校內無 eduroam SSID 可連線,至有建置 eduroam SSID 之學校可使用校內之 Google 帳號連線 eduroam SSID
註2:
1. 校內無線網路設備均需支援802.1X 驗證服務,需自行建置或委由專業廠商協助建置驗證服務之 eduroam SSID。
2. 建置驗證服務之 eduroam SSID,需有 Radius Key,請向桃園區網取得。
3. 申請雙向向上集中服務之學校,在校內外皆可連線至 eduroam SSID,他校人員至貴校也能使用他校之 Google 帳號直接連線至 eduroam SSID。
註3:申請單雙向向上集中服務之學校,需提供連線 eduroam SSID 時需輸入之 [帳號@Google 網域],可由 Google 管理控制台→網域內查看,最多提供三組網域做申請。
註4:申請雙向向上集中服務之學校,需提供無線網路設備流出外網之實體 IP,校內防火牆需開放流入,流出外網之實體 IP 可由校內防火牆查看。

本申請單填寫完成後請 Email: tanet_ncu@ncu.edu.tw 或寄送桃園區網中心

申請網域1	mail.xxxx.tyc.edu.tw		
申請網域2			
申請網域3			
介面實體 IP	210.99.99.99		
資訊聯絡人一	王大明	連絡電話	034204999
		EMAIL	xxx@mail.xxxx.tyc.edu.tw
資訊聯絡人二	張三豐	連絡電話	034204999
		EMAIL	zzz@mail.xxxx.tyc.edu.tw
申請人/資訊組長核章		申請單位主管核章	
以下欄位由桃園區網中心填寫(申請單位請勿填寫)			
確認完成	<input type="checkbox"/> 已完成。 <input type="checkbox"/> 未完成。原因: _____ 日期時間: 年 月 日		
區網承辦人	組長	主任	



桃園區網 eduroam 向上集中申請單

=====申請**單向**服務=====

- 申請此服務需提供「Google網域、串接憑證、金鑰」
- 此服務需提供一至兩位資訊人員需**具有Google管理權**的聯繫方式
- Google串接憑證效期為三年
三年到期前請自行提供新憑證
至桃園區網中心更換
- 需提供一組帳號供向上集中伺服器
做驗證

=====申請**雙向**服務=====

- 申請此服務需提供「Google網域、串接憑證、金鑰、
介面IP」
- 此服務需提供一至兩位資訊人員需**具有Google及防火牆管理權**的聯繫
方式Google串接憑證效期為三年，
三年到期前請自行提供新憑證至桃
園區網中心更換
- 需提供一組帳號供向上集中伺服器
做驗證



IOS連接方式





IOS連接 eduroam

- 點選 eduroam SSID
- 輸入「使用者名稱」、「密碼」

PS.使用者名稱輸入Google帳號@後之網域，必須是申請向上集中之網域



8:11    96

輸入「eduroam」的密碼

取消 輸入密碼 加入

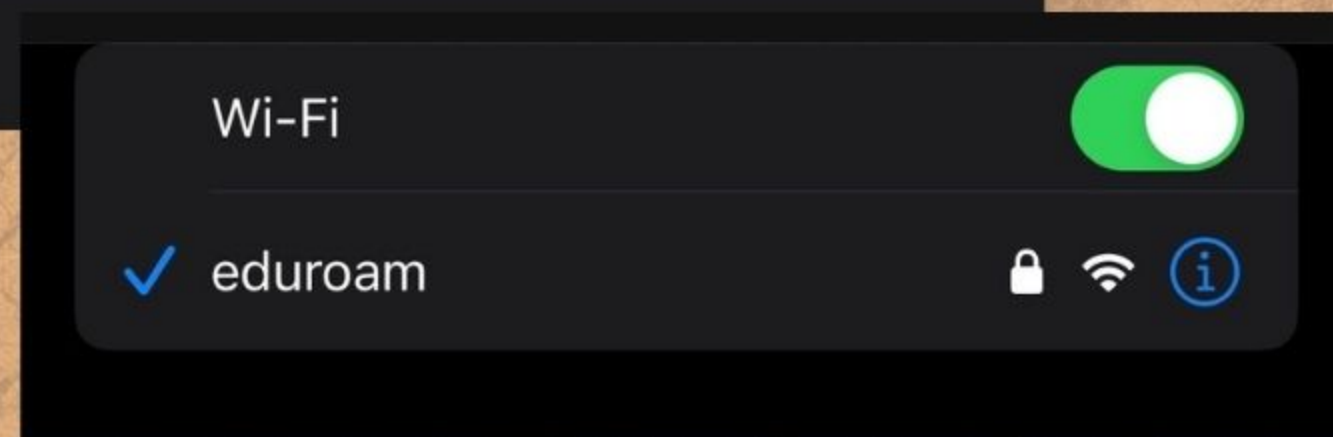
使用者名稱

密碼

IOS連接 eduroam

- 跳出憑證需要信任訊息
- 確認憑證為 `eduroam.tyc.edu.tw`
- 即可放心點選右上角「信任」
- 信任完成後即連線成功

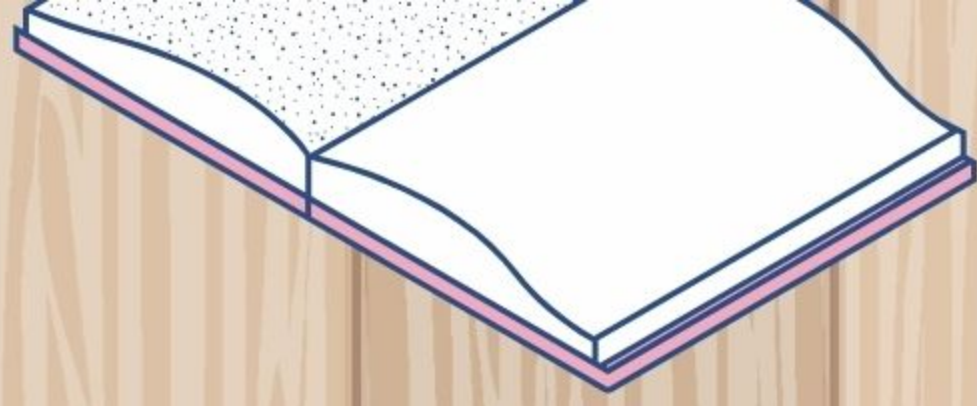
**PS.資安原則，請再三確認憑證資訊
網域為`eduroam.tyc.edu.tw`，或者點
選下方「更多詳細資訊」查看憑證內容**





Android連接方式





Android 11 以上版本連接 eduroam

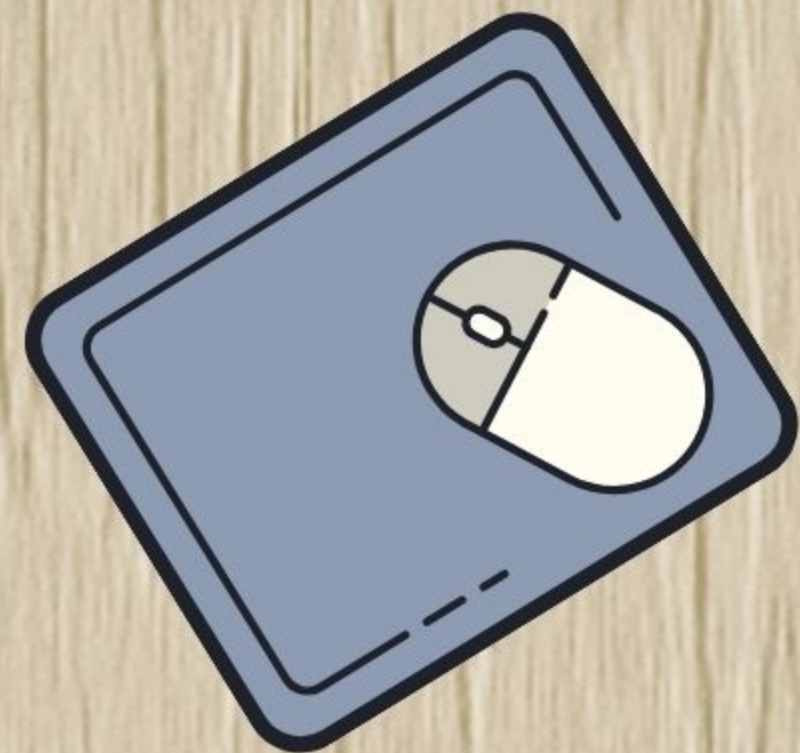
- EAP方法請選擇「PEAP」
- 階段2驗證請選擇「GTC」
- CA驗證請選擇「使用系統憑證」
- 最低傳輸層版本請選擇「TLSV1.2」
- 線上憑證狀態請選擇「要求取得憑證狀態」
- 網域請輸入「eduroam.tyc.edu.tw」
- 身分請輸入「學校端Google帳號」
- 匿名身分請「空白」
- 密碼請輸入「學校端Google密碼」
- 連線時如彈出憑證是否信任請選擇「信任」

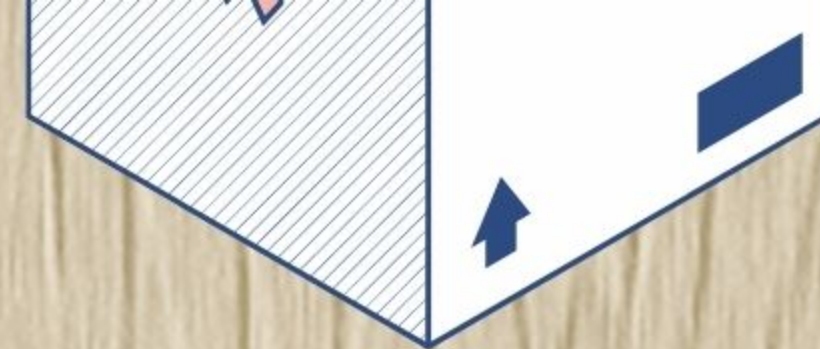
The screenshot shows the eduroam configuration interface on an Android device. The settings are as follows:

- eduroam
- EAP 方法: PEAP
- 階段 2 驗證: GTC
- CA 憑證: 使用系統憑證
- 最低傳輸層安全標準版本: TLS v1.2
- 線上憑證狀態: 要求取得憑證狀態
- 網域: eduroam.tyc.edu.tw
- 身分: sam@g.lhvs.tyc.edu.tw
- 匿名身分: (blank)
- 密碼: (blank)



Windows 10/11 連接方式



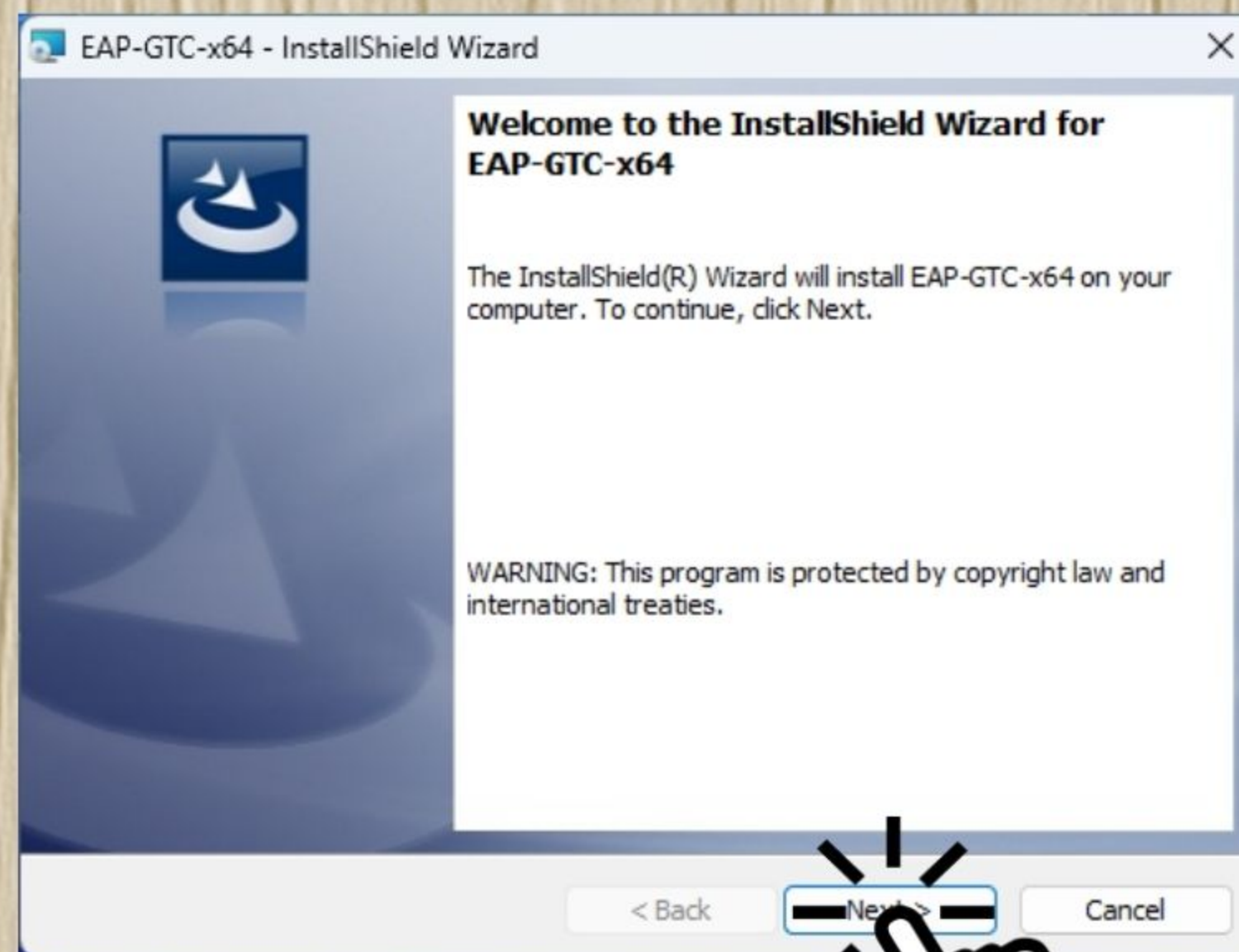


Windows 10/11 連接 eduroam 方式

- 下載 EAP-GTC 壓縮包
- 解壓縮 執行「EAP-GTC-x64(x86).msi」
- 安裝 EAP-GTC 套件
- 點選「Next」至安裝完成
- 重新啟動電腦

[https://eduroam.tyc.edu.tw/
eduroam_win_x64.rar](https://eduroam.tyc.edu.tw/eduroam_win_x64.rar)

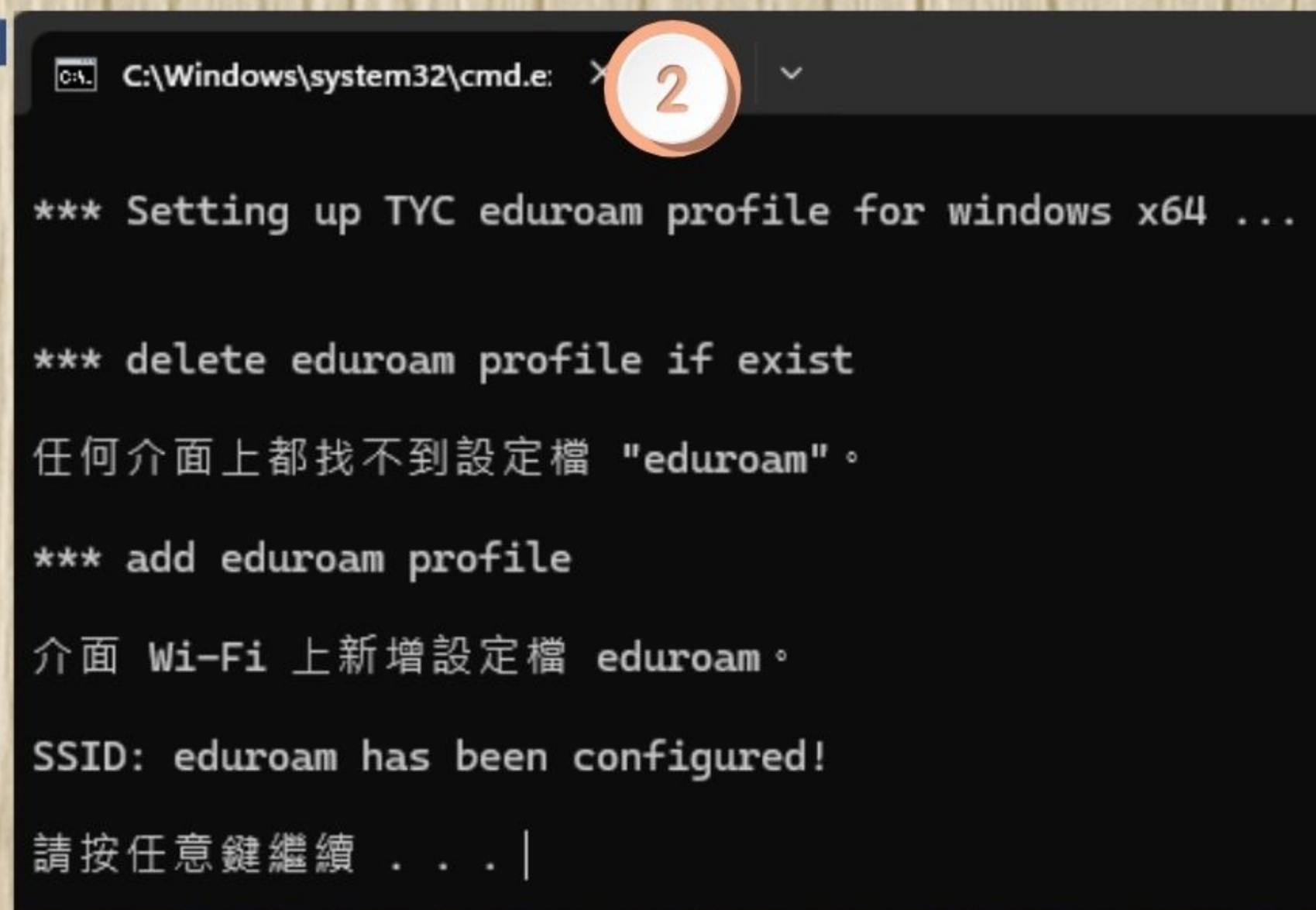
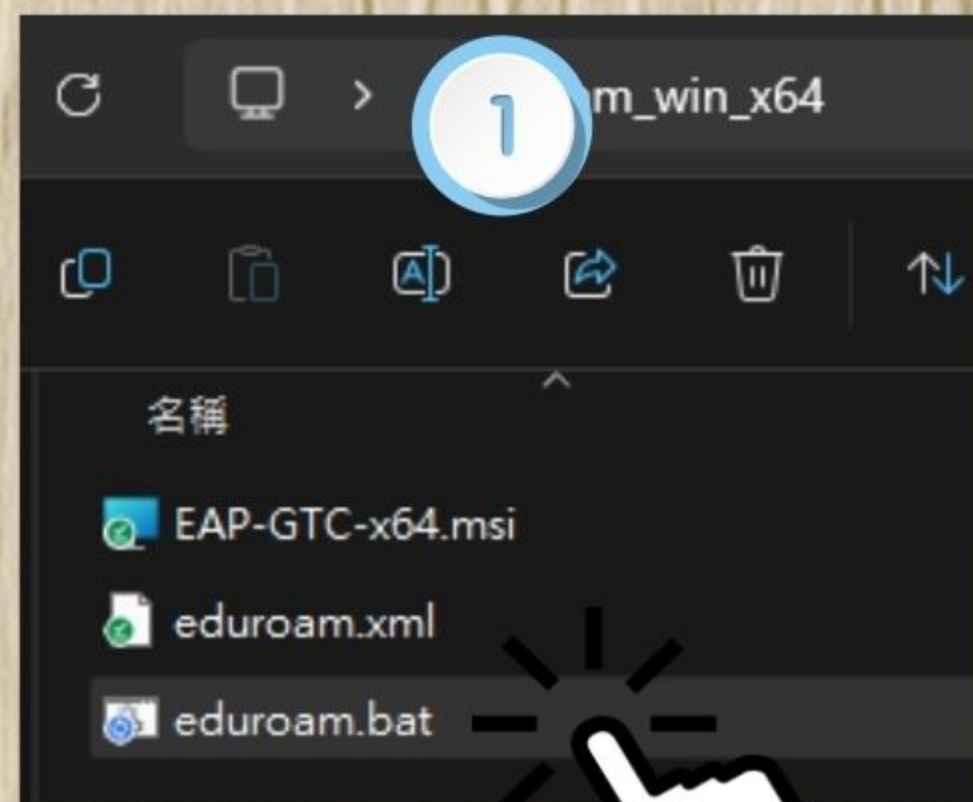
EAP-GTC 壓縮包





Windows 10/11 連接 eduroam 方式

- 重新啟動電腦後執行「eduroam.bat」
- 會自動建立eduroam連接設定檔



Windows 10/11 連接 eduroam 方式

- 設定檔建立完成後
- 可開始連接eduroam SSID
- 連接時會彈出登入視窗
- 輸入「User name」、
「Password」 點下方OK驗
證完成後即可連網

**PS.User name輸入Google帳號
@後之網域，必須是申請向上集
中之網域**



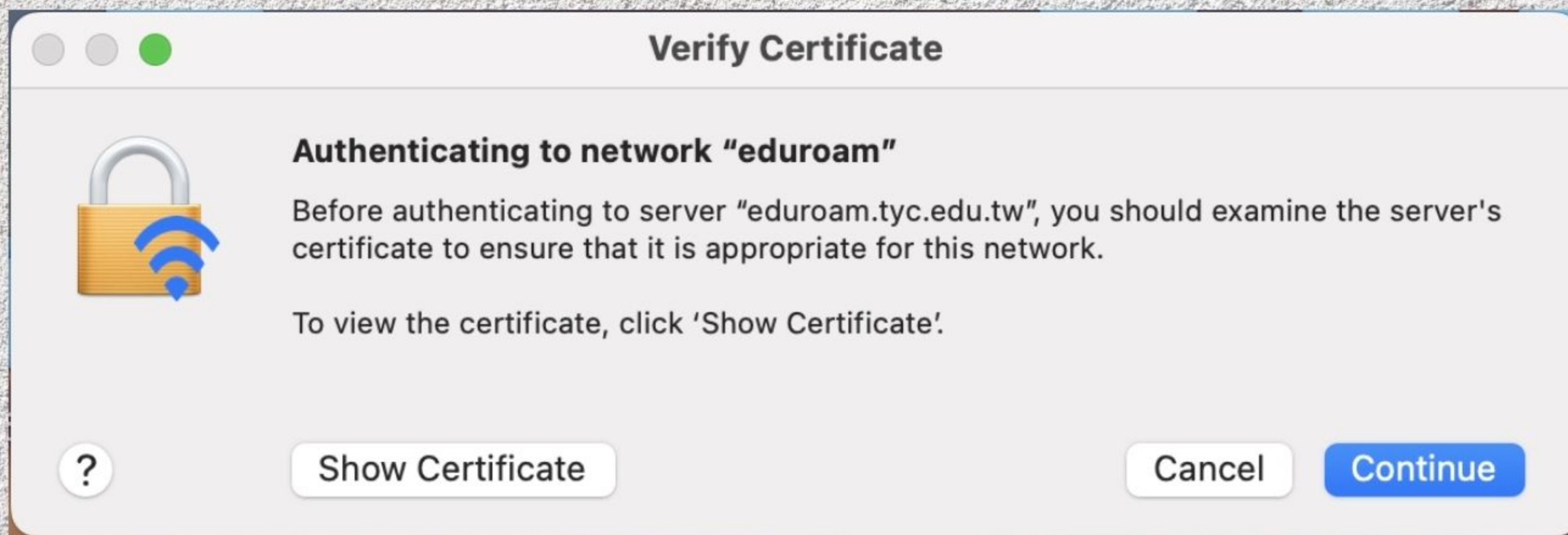
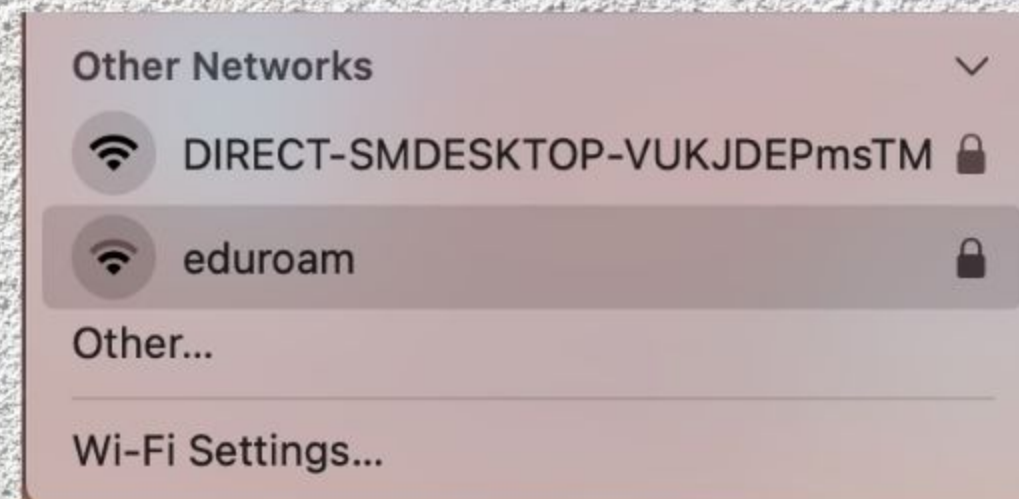


Mac連接方式



MAC 連接方式

- 點選 eduroam 進行連線
- 彈出憑證請求 請點選 Continue 繼續
會需要填入密碼或要求指紋





MAC 連接方式

- 輸入學校的 Google 帳號
- 輸入學校的 Google 密碼
- 按下OK進行連線，驗證完成即可使用漫遊上網

Enter a name and password for network "eduroam"

Account Name:

Password:

Remember this information





Thank You

