

## 如何匯入政府總憑證管理中心第三代自簽憑證(GRCA3.cer)至系統中

網站申請內網 TLS 憑證(由 GCA 核發)並安裝後，用戶端須自行匯入 GRCA3.cer 至電腦中，其瀏覽器才能正常瀏覽網站，而不會跳出不信任的告警。匯入憑證步驟如下：

### 1. 下載政府憑證總管理中心第三代自簽憑證

請到 <https://grca.nat.gov.tw/repository/Certs/GRCA3.cer> 下載自簽憑證

或透過瀏覽政府憑證總管理中心網站(<https://grca.nat.gov.tw/>)的儲存庫區，進行憑證下載

---

以下的步驟 2 至步驟 6，用戶端視其電腦類型或配置方式，擇一使用即可

步驟 2：在 Windows 匯入政府憑證總管理中心第三代自簽憑證

步驟 3：在 macOS 匯入政府憑證總管理中心第三代自簽憑證

步驟 4：在 linux 匯入政府憑證總管理中心第三代自簽憑證

步驟 5：在瀏覽器中匯入政府憑證總管理中心第三代自簽憑證

步驟 6：使用 Active Directory 群組原則 (GPO) 派送政府憑證總管理中心第三代自簽憑證

---

### 2. 在 Windows 匯入政府憑證總管理中心第三代自簽憑證

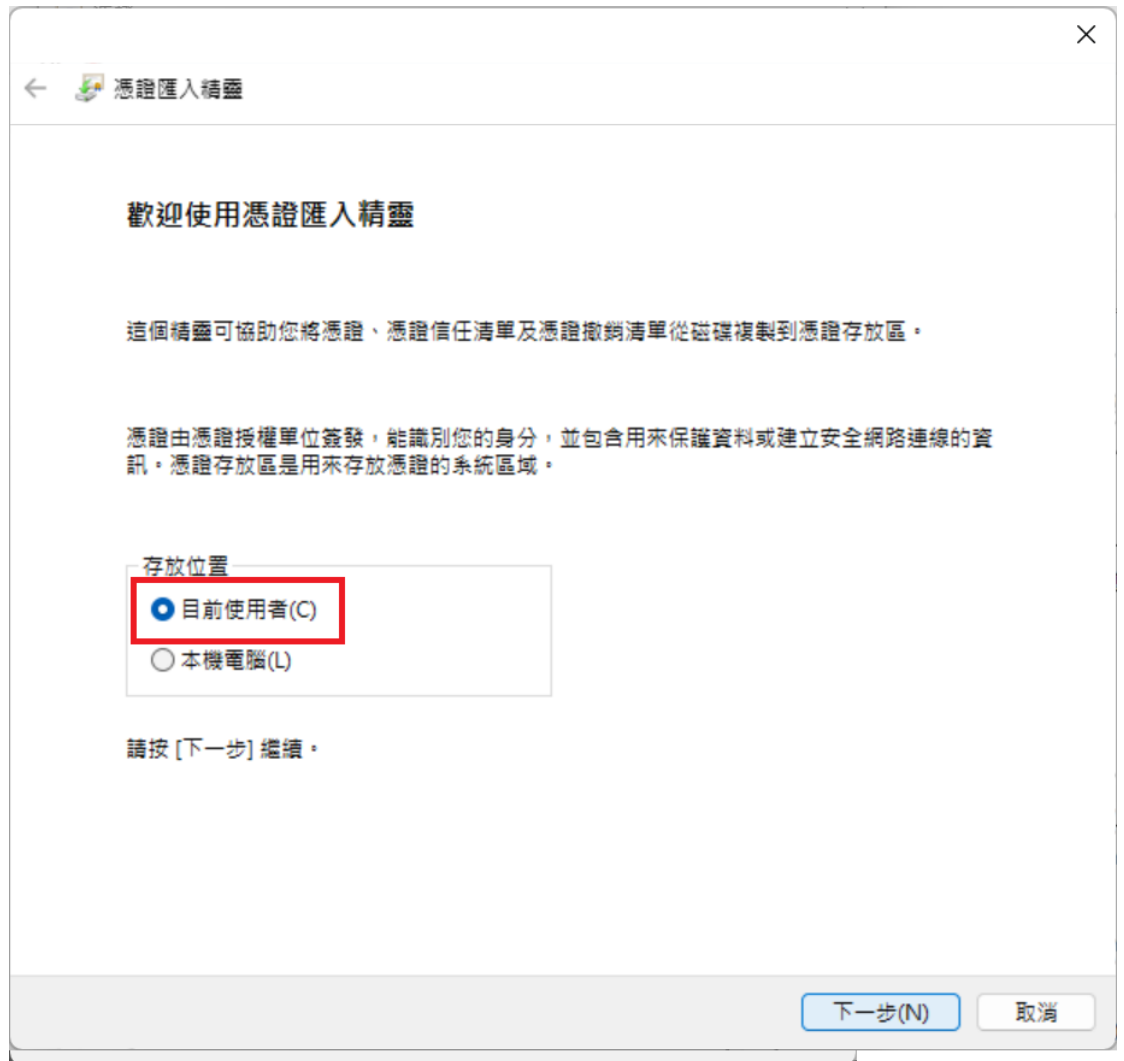
#### 方法 1：點擊憑證匯入

1. 點擊如上方連結下載之憑證，如 GRCA3.cer。

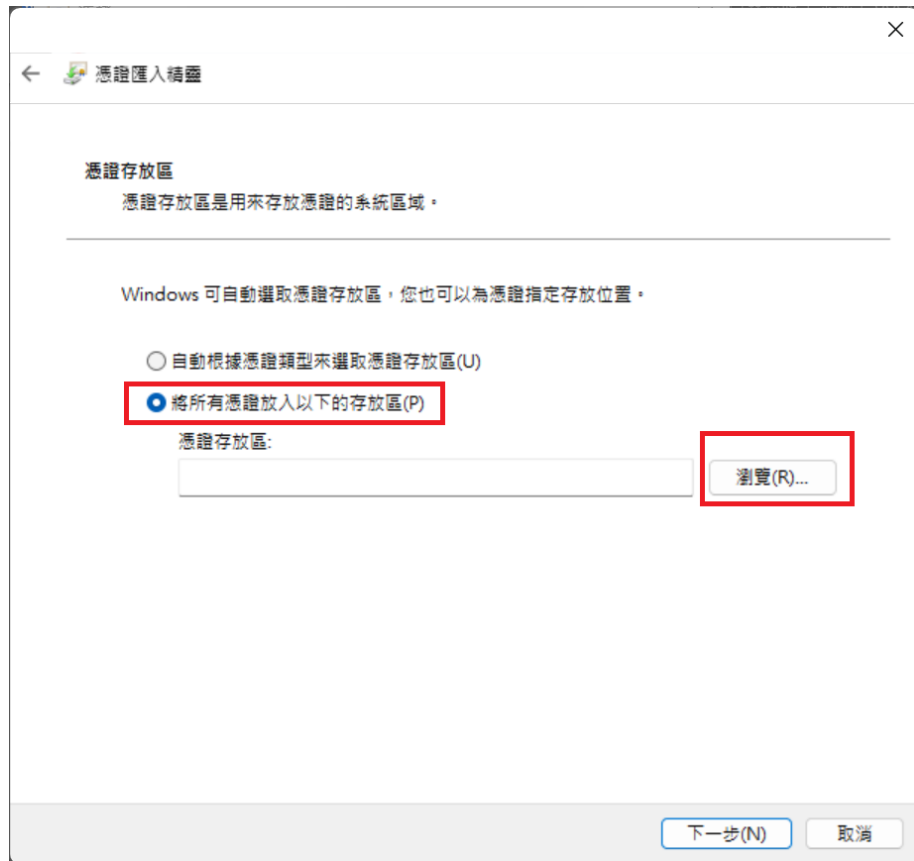


2. 匯入憑證：

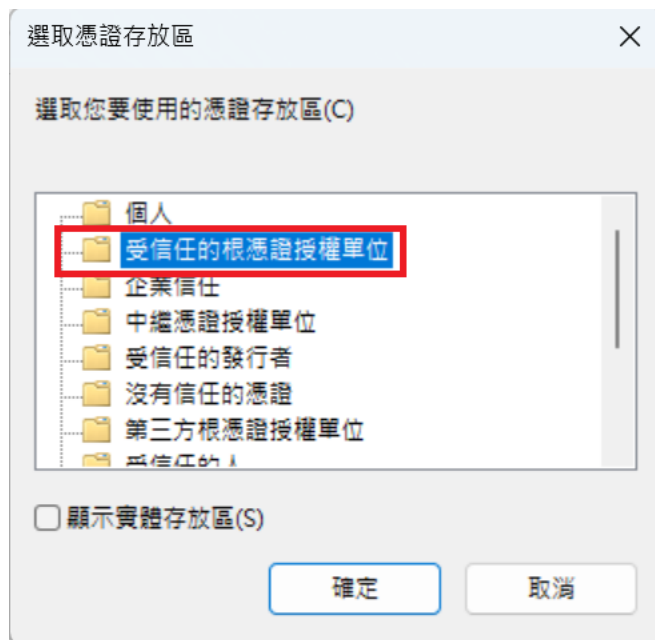
點擊安裝憑證



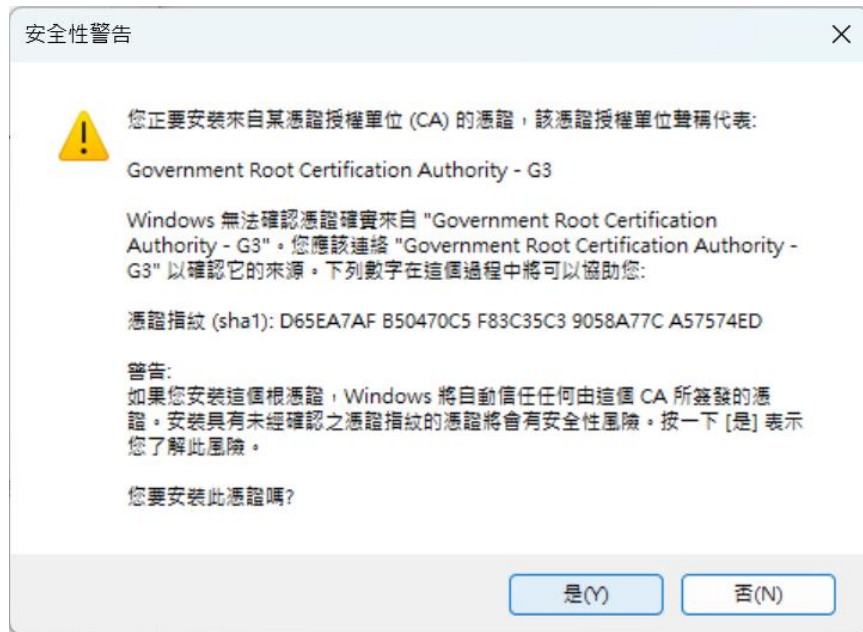
選擇「目前使用者」，按「下一步」。



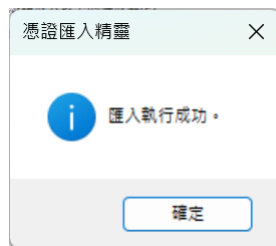
- 選擇「將所有憑證放入以下的存放區」→「瀏覽」



- 
- 選擇「受信任的根憑證授權單位」→「確定」→「下一步」



- 
- 系統詢問是否要選擇是安裝憑證授權單位，選擇「是」



- 
- 憑證匯入執行成功

備註：若是系統管理者幫用戶安裝，可在匯入憑證時改選「本機電腦」

## 方法 2：使用 PowerShell 指令

```
Import-Certificate -FilePath "C:\path\to\GRCA3.cer" -CertStoreLocation  
Cert:\LocalMachine\Root
```

### 3. 在 macOS 匯入政府憑證總管理中心第三代自簽憑證

1. 打開「鑰匙圈存取 (Keychain Access)」 (Cmd + Space 搜尋)。
2. 點擊「系統」鑰匙圈（需要管理員權限）。
3. 匯入憑證：
  - 點擊「檔案」→「匯入項目」，選擇 GRCA3.cer 檔案。

#### 4. 信任憑證：

- 雙擊新增的憑證，在「信任 (Trust)」選項中，將「使用此憑證時」設為「始終信任 (Always Trust)」。

---

#### 4. 在 Linux 匯入政府憑證總管理中心第三代自簽憑證

對於 Debian/Ubuntu，使用指令：

```
sudo cp GRCA3.cer /usr/local/share/ca-certificates/
```

```
sudo update-ca-certificates
```

對於 RHEL/CentOS，使用指令：

```
sudo cp GRCA3.cer /etc/pki/ca-trust/source/anchors/
```

```
sudo update-ca-trust
```

---

#### 5. 在瀏覽器中匯入政府憑證總管理中心第三代自簽憑證

##### Google Chrome / Edge

1. 打開設定 (chrome://settings/ 或 edge://settings/)。
2. 搜尋「憑證」→ 點擊「管理憑證 (Manage Certificates)」。
3. 選擇「受信任的根憑證授權機構」→ 點擊「匯入」，選擇 GRCA3.cer 檔案。

##### Firefox

1. 打開 **Firefox** 設定 (about:preferences)。
  2. 搜尋「憑證」→ 點擊「檢視憑證」。
  3. 在「憑證機構」分頁中，點擊「匯入」。
  4. 選擇 GRCA3.cer 檔案，並勾選「信任此 CA 來辨識網站」。
-

## 6. 使用 **Active Directory** 群組原則 (GPO) 派送政府憑證總管理中心第三代自簽憑證

### 步驟 1：準備憑證

1. 取得 **GRCA3.cer** 憑證
  2. 將憑證存放於共享資料夾 (可選)
    - 如果需要讓多台電腦存取憑證，建議將其存放於網路共享資料夾，如：`\\server\shared\certs\GRCA3.cer`
    - 確保 AD 使用者有權限存取該檔案。
- 

### 步驟 2：建立並部署 GPO

1. 打開「群組原則管理」 (**Group Policy Management**)
  - 在 **Windows Server** 上，按 Win + R，輸入 `gpmc.msc`，按 Enter。
2. 建立新的 **GPO**
  - 在「網域」(Domain) 下，右鍵點擊「群組原則物件 (**Group Policy Objects**)」→「新增」。
  - 命名為 `Deploy-Certificate`，點擊「確定」。
3. 編輯 **GPO**
  - 右鍵點擊剛建立的 GPO (`Deploy-Certificate`)，選擇「編輯」。
4. 配置憑證至受信任的根憑證授權機構
  - 在 GPO 編輯器中，展開：  
電腦設定 → 原則 → Windows 設定 → 安全性設定 → 公用金鑰原則 (Public Key Policies) → 受信任的根憑證授權機構 (Trusted Root Certification Authorities)
    - 右鍵「受信任的根憑證授權機構」，選擇「匯入」。
    - 選擇 `GRCA3.cer` 憑證檔案，完成匯入。

## 5. 將 GPO 連結至適用的 OU (組織單位)

- 在「群組原則管理」，找到適用的「組織單位 (OU)」(如 Computers 或 Users)。
  - 右鍵點擊 OU，選擇「連結現有 GPO」，選擇 Deploy-Certificate。
- 

## 步驟 3：強制更新 GPO

### 1. 在伺服器端

- 開啟命令提示字元 (CMD) 或 PowerShell，輸入：

```
gpupdate /force
```

- 確保 GPO 已套用。

### 2. 在用戶端電腦

- 讓用戶重新登入，或執行：

```
gpupdate /force
```

- 檢查是否成功安裝：
  - certmgr.msc → 受信任的根憑證授權機構 → 憑證
  - 確認有 Government Root Certification Authority - G3 存在

