EPSON
EXCEED YOUR VISION

# DS-790WN

# 管理員使用說明

適合目的的必要設定

網路設定

掃描的所需設定

基本安全性設定

進階安全設定

驗證設定

NPD6726-02 TC

# 著作權

未經 Seiko Epson Corporation 事先書面許可，禁止將本出版物的任何部分重製、儲存於檢索系統或以任何形式或方法傳送，不論係以電子、機械、複印、錄製或其他方式。使用本手冊所含之資訊無需擔負相關專利責任。亦無需擔負因使用本手冊資訊而導致之損害責任。本手冊內含的資訊僅設計供 Epson 產品之用。Epson 對於任何將此資訊應用於其他產品的作法概不負責。

若本產品購買人或第三方因意外使用、誤用或濫用本產品、未經授權而改裝、修理或變更本產品、或 (美國除外) 未嚴格遵守 Seiko Epson Corporation 操作與維護說明而發生損壞、損失或費用，則 Seiko Epson Corporation 與關係企業均不予負責。

如因使用非 Seiko Epson Corporation 指定之原廠產品或 Epson 認可之任何選購品或耗材而發生任何損壞或問題，Seiko Epson Corporation 與關係企業不予負責。

若因使用非 Seiko Epson Corporation 認可之任何界面連接線，致發生電子干擾而造成任何損壞，Seiko Epson Corporation 概不負責。

© 2022 Seiko Epson Corporation

本手冊的內容與本產品的規格若有變更，恕不另行通知。

# 商標

- ❏ EPSON、EPSON EXCEED YOUR VISION、EXCEED YOUR VISION 及其各自的標識乃 Seiko Epson 的註冊商標。
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa 和 PaSoRi 是 Sony Corporation 的註冊商標。
- ❏ MIFARE 是 NXP Semiconductor Corporation 的註冊商標。
- ❏ 一般注意事項：文中所用的其他產品名稱僅用於識別目的，且分別是其對應所有者的商標。Epson 放棄這些商標的所有權利。

# 目錄


## 著作權

## 商標

## 簡介

本文件內容. . . . . 7
使用本使用說明. . . . . 7
標記和符號. . . . . 7
本手冊使用的說明. . . . . 7
作業系統參考說明. . . . . 8

## 管理員密碼備註

管理員密碼備註. . . . . 10
初始管理員密碼. . . . . 10
需要管理員密碼的操作. . . . . 10
變更管理員密碼. . . . . 10
重設管理員密碼. . . . . 10

## 適合目的的必要設定

適合目的的必要設定. . . . . 12

## 網路設定

連接掃描器至網路. . . . . 15
在進行網路連線之前. . . . . 15
從控制面板連接至網路. . . . . 17
新增或更換電腦或裝置. . . . . 20
連接至已連接網路的掃描器. . . . . 20
直接連接智慧型裝置與掃描器 (Wi-Fi Direct). . 22
重新設定網路連線. . . . . 24
檢查網路連線狀態. . . . . 26
從控制台查看網路連線狀態. . . . . 26
網路規格. . . . . 27
Wi-Fi 規格. . . . . 27
乙太網路規格. . . . . 28
網路功能和 IPv4/IPv6. . . . . 29
安全性通訊協定. . . . . 29
掃描器使用的連接埠. . . . . 29
解決問題. . . . . 30
無法連接至網路. . . . . 30

## 掃描器設定軟體

Web Config. . . . . 35
在網頁瀏覽器上執行 Web Config. . . . . 35
在 Web Config 上執行 Windows. . . . . 36
Epson Device Admin. . . . . 36
設定範本. . . . . 36

## 掃描的所需設定

配置郵件伺服器. . . . . 41
郵件伺服器設定項目. . . . . 41
檢查郵件伺服器連線. . . . . 42
設定共用網路資料夾. . . . . 43
建立共用資料夾. . . . . 44
使聯絡人可用. . . . . 59
聯絡人配置比較. . . . . 60
使用 Web Config 將目的地登錄至聯絡人. . . . . 60
使用 Web Config 將目的地註冊為群組. . . . . 62
備份和匯入聯絡人. . . . . 63
使用工具匯出和批量登錄聯絡人. . . . . 63
LDAP 伺服器與使用者之間的合作. . . . . 65
使用 Document Capture Pro Server. . . . . 68
設定伺服器模式. . . . . 68
設定 AirPrint. . . . . 69
準備網路掃描時遇到的問題. . . . . 69
解決問題的提示. . . . . 69
無法存取 Web Config. . . . . 69

## 訂製控制面板顯示

登錄 預設. . . . . 72
預設 功能表選項. . . . . 73
編輯控制面板主畫面. . . . . 74
變更主畫面的 版面配置. . . . . 74
新增圖示. . . . . 75
移除圖示. . . . . 76
移動圖示. . . . . 77

## 基本安全性設定

產品安全功能介紹. . . . . 80
管理員設定. . . . . 80
配置管理員密碼. . . . . 80
對控制面板使用 鎖定設定. . . . . 81
從控制面板以管理員身份登入. . . . . 85
停用外部介面. . . . . 86
監控遠端掃描器. . . . . 86
檢查遠端掃描器資訊. . . . . 86

發生事件時接收電子郵件通知. . . . . .87
解決問題. . . . . 88
忘記您的管理員密碼. . . . . 88

## 進階安全設定

安全性設定與危險預防. . . . . 90
安全功能設定. . . . . .90
使用通訊協定控制. . . . . .90
通訊協定的控制. . . . . .91
可啟用或停用的通訊協定. . . . . 91
通訊協定設定項目. . . . . .91
使用數位憑證. . . . . .93
關於電子憑證. . . . . .93
組態 CA 簽署憑證. . . . . 94
更新自我簽署憑證. . . . . .97
組態 CA 憑證. . . . . .97
與掃描器之間的 SSL/TLS 通訊. . . . . .98
進行基本 SSL/TLS 設定. . . . . 98
配置掃描器的伺服器憑證. . . . . 99
使用 IPsec/IP 篩選加密的通訊. . . . . 99
關於 IPsec/IP 篩選. . . . . 99
配置預設原則. . . . . .99
配置群組原則. . . . . .103
IPsec/IP 篩選 的配置範例. . . . . .109
設定 IPsec/IP 篩選的證書. . . . . .110
將掃描器連接至 IEEE802.1X 網路. . . . . 110
配置 IEEE 802.1X 網路. . . . . 110
設定 IEEE 802.1X 的證書. . . . . 111
解決進階安全性的問題. . . . . 112
還原安全性設定. . . . . .112
使用網路安全性功能的問題. . . . . .112
使用數位憑證的問題. . . . . 114

## 驗證設定

關於 驗證設定. . . . . 119
適用於 驗證設定 的可用功能. . . . . .119
關於 驗證方法. . . . . 120
用於設定的軟體. . . . . .121
更新掃描器韌體. . . . . .121
連接和設定驗證裝置. . . . . 122
讀卡器相容清單. . . . . .122
連接驗證裝置. . . . . .124
驗證裝置設定. . . . . .125
登錄和設定資訊. . . . . .126
調定. . . . . 126
啟用驗證. . . . . 127
驗證設定. . . . . 127
登錄 使用者設定. . . . . .128
與 LDAP 伺服器 同步. . . . . .134
設定電子郵件伺服器. . . . . 138
設定 掃描至我的資料夾. . . . . .138
自訂單鍵功能. . . . . .140
使用 Epson Device Admin 的 工作歷史紀錄
報告. . . . . 141
可包含於報告內的項目. . . . . 141
從控制面板以管理員身份登入. . . . . .141
停用 驗證設定. . . . . 141
刪除 驗證設定 資訊 (回復至出廠預設值). . . . . .142
解決問題. . . . . 142
無法讀取驗證卡. . . . . .142

## 維護

清潔掃描器外部. . . . . .144
清潔掃描器內部. . . . . .144
更換滾輪組裝套件. . . . . 149
滾輪組裝套件代碼. . . . . 154
重設掃描次數. . . . . .154
省電. . . . . 154
搬運掃描器. . . . . .155
備份設定. . . . . 156
匯出設定. . . . . 156
匯入匯入設定. . . . . .156
回復至出廠預設值. . . . . 157
更新應用程式與韌體. . . . . 157
使用控制面板來更新掃描器韌體. . . . . .158
使用 Web Config 更新韌體. . . . . 158
在未連接至網際網路的情況下更新韌體. . . . 158

# 簡介

本文件內容. . . . . 7

使用本使用說明. . . . . 7

# 本文件內容

此文件為掃描器管理員提供下列資訊。

❏ 網路設定

❏ 準備掃描功能

❏ 啟用和管理安全設定

❏ 啟用和管理 驗證設定

❏ 執行每日維護

關於使用掃描器的標準方法，請參看 *進階使用說明*。

附註：
此文件說明 驗證設定 可提供單獨驗證，無需使用驗證伺服器。除本手冊內介紹的 驗證設定 以外，您還可以使用驗證伺服器建立驗證系統。若要建立系統，請使用 Document Capture Pro Server Authentication Edition（縮略名稱為 Document Capture Pro Server AE）。

如需進一步資訊，請洽詢當地的 Epson 公司。

# 使用本使用說明

## 標記和符號

> ⚠ 注意：
> 必須小心遵守此說明以避免受傷。

> **重要事項：**
> 必須遵守此說明以避免設備受損。

附註：
提供補充和參考資訊。

**相關資訊**

➡ 與相關章節之間的連結。

## 本手冊使用的說明

❏ 應用程式的螢幕截圖取自 Windows 10 或 macOS High Sierra。畫面上顯示的內容會隨著型號與情況而改變。

❏ 本手冊使用的圖示僅供參考。雖然這些圖示可能與您的實際產品略有不同，但操作方式均相同。

# 作業系統參考說明

Windows

在本手冊中，「Windows 10」、「Windows 8.1」、「Windows 8」、「Windows 7」、「Windows Server 2019」、「Windows Server 2016」、「Windows Server 2012 R2」、「Windows Server 2012」及「Windows Server 2008 R2」等詞語係指下列作業系統。此外，「Windows」泛指所有版本，「Windows Server」泛指「Windows Server 2019」、「Windows Server 2016」、「Windows Server 2012 R2」、Windows Server 2012」和「Windows Server 2008 R2」。

- ❏ Microsoft® Windows® 10 作業系統
- ❏ Microsoft® Windows® 8.1 作業系統
- ❏ Microsoft® Windows® 8 作業系統
- ❏ Microsoft® Windows® 7 作業系統
- ❏ Microsoft® Windows Server® 2019 作業系統
- ❏ Microsoft® Windows Server® 2016 作業系統
- ❏ Microsoft® Windows Server® 2012 R2 作業系統
- ❏ Microsoft® Windows Server® 2012 作業系統
- ❏ Microsoft® Windows Server® 2008 R2 作業系統

Mac OS

本手冊中，「Mac OS」用於泛指「macOS Big Sur」、「macOS Catalina」、「macOS Mojave」、「macOS High Sierra」、「macOS Sierra」、「OS X El Capitan」和「OS X Yosemite」。

# 管理員密碼備註

管理員密碼備註. . . . . 10

初始管理員密碼. . . . . 10

需要管理員密碼的操作. . . . . 10

變更管理員密碼. . . . . 10

重設管理員密碼. . . . . 10

# 管理員密碼備註

本裝置可讓您設定管理員密碼，以防止未經授權的第三方在裝置連接至網路時存取或變更儲存於裝置內的裝置設定或網路設定。

若您已設定管理員密碼，則需要在 Web Config 等配置軟體中變更設定時輸入該密碼。

掃描器上已設定初始管理員密碼，但您可以將其變更為任何密碼。

# 初始管理員密碼

初始管理員密碼隨產品背面附帶的標籤而不同。

如果背面附帶「PASSWORD」標籤，則輸入標籤上顯示的 8 位數字。

如果背面沒有附帶「PASSWORD」標籤，則輸入產品背面附帶標籤上的序列號以作為初始管理員密碼。

附註：
沒有預設使用者名稱。

# 需要管理員密碼的操作

如果您在以下操作過程中被提示輸入管理員密碼，請輸入產品上設定的管理員密碼。

- ❏ 在登入以進行 Web Config 的進階設定時
- ❏ 在操作已被管理員鎖定的控制面板的功能表時
- ❏ 在應用程式中變更裝置設定時
- ❏ 在更新裝置的韌體時
- ❏ 在變更或重設管理員密碼時

# 變更管理員密碼

您可以從產品控制面板或 Web Config 內進行變更。

當變更密碼時，新密碼必須是 8 至 20 個字元長度，且僅包含單字節字母數字字元和符號。

# 重設管理員密碼

您可以從產品的控制面板或在 Web Config 內將管理員密碼重設為初始設定。

如果您忘記密碼且無法將其重設為預設設定，則產品需要維修。聯絡您當地的經銷商。

# 適合目的的必要設定

適合目的的必要設定. . . . . .12

# 適合目的的必要設定

查看下列內容以進行適合目的的必要設定。

### 連接掃描器至網路

| 目的 | 所需設定 |
|---|---|
| 我希望連接掃描器至網路。 | 設定掃描器以進行網路掃描。<br>第15頁“連接掃描器至網路” |
| 我希望連接掃描器至一台新電腦。 | 在新電腦上為掃描器進行網路設定。<br>第20頁“新增或更換電腦或裝置” |

### 掃描設定

| 目的 | 所需設定 |
|---|---|
| 我希望透過電子郵件傳送掃描影像。<br>(掃描至電子郵件) | 1.設定您要連接的電子郵件伺服器。<br>第41頁“配置郵件伺服器”<br>2.在 [聯絡人] 內登錄接收者的電子郵件地址（選填）。透過登錄電子郵件地址，您無需在每次想要傳送內容時輸入它，只需從聯絡人中選取即可。<br>第59頁“使聯絡人可用” |
| 我希望儲存掃描影像至網路上的資料夾。<br>(掃描至網路資料夾/FTP) | 1.在您要儲存影像的網路上建立資料夾。<br>第43頁“設定共用網路資料夾”<br>2.登錄路徑至 [聯絡人] 內的資料夾（選填）。透過登錄資料夾路徑，您無需在每次想要傳送內容時輸入它，只需從聯絡人中選取即可。<br>第59頁“使聯絡人可用” |
| 我希望儲存掃描影像至雲端服務。<br>(掃描至雲端) | 設定 Epson Connect。如需關於設定的詳細資料，請參閱 Epson Connect 入口網站。<br>進行設定時，您需要準備連接的線上儲存服務使用者帳戶。<br>https://www.epsonconnect.com/<br>http://www.epsonconnect.eu（僅適用於歐洲） |

### 自定義控制面板顯示

| 目的 | 所需設定 |
|---|---|
| 我希望變更掃描器控制面板上顯示的項目。 | 設定 [預設] 或 [編輯主畫面]。您可以登錄您的最愛掃描設定至控制面板，並編輯顯示的項目。<br>第71頁“訂製控制面板顯示” |

### 設定基本安全功能

| 目的 | 所需設定 |
| --- | --- |
| 我希望防止除管理員以外的任何人變更掃描器設定。 | 為掃描器設定管理員密碼。<br>第80頁“管理員設定” |
| 我希望停用透過 USB 連接使用掃描器。 | 停用外部介面。<br>第86頁“停用外部介面” |

### 設定進階安全功能

| 目的 | 所需設定 |
| --- | --- |
| 我希望控制使用哪個協議。 | 啟用或停用協議。<br>第90頁“使用通訊協定控制” |
| 我希望加密通訊路徑。 | 1.設定您的數位憑證。<br>第93頁“使用數位憑證”<br>2.設定 SSL/TLS 通訊。<br>第98頁“與掃描器之間的 SSL/TLS 通訊” |
| 我要使用加密通訊 (IPsec)。<br>我希望能僅從特定電腦（IP 過濾）。 | 過濾流量的設定政策。<br>第99頁“使用 IPsec/IP 篩選加密的通訊” |
| 我希望在 IEEE802.1X 網路內使用掃描器。 | 為掃描器設定 IEEE802.1X。<br>第110頁“將掃描器連接至 IEEE802.1X 網路” |

### 將由掃描器驗證的設定功能

| 目的 | 所需設定 |
| --- | --- |
| 我希望啟用 驗證設定。 | 有關設定項目的更多資訊，請參閱 驗證設定 和 驗證方法 內的說明。<br>第119頁“關於 驗證設定”<br>第120頁“關於 驗證方法” |

### 使用伺服器驗證系統

透過 Document Capture Pro Server Authentication Edition（縮寫為 Document Capture Pro Server AE），您可以建立使用伺服器進行驗證的驗證系統。

如需進一步資訊，請洽詢當地的 Epson 公司。

# 網路設定

連接掃描器至網路. . . . . 15

新增或更換電腦或裝置. . . . . 20

檢查網路連線狀態. . . . . 26

網路規格. . . . . 27

解決問題. . . . . 30

# 連接掃描器至網路

本節說明如何使用掃描器控制面板連接掃描器至網路。

附註：
如果掃描器和電腦處於相同區段，還可以使用安裝程式進行連接。

❏ 從網站設定

存取以下網站，然後輸入產品名稱。前往 [設定]，然後開始設定。

http://epson.sn

❏ 使用軟體光碟片執行設定（僅限配有軟體光碟片的型號，以及配有光碟機的 Windows 電腦使用者）。

將軟體光碟片插入電腦，然後按照螢幕說明進行操作。

## 在進行網路連線之前

若要連接至網路，請先檢查連線方法和連線設定資訊。

### 收集連線設定相關資訊

準備必要的設定資訊以進行連接。請事先檢查下列資訊。

| 部分 | 項目 | 附註 |
|---|---|---|
| 裝置連線方法 | ❏ 乙太網路<br>❏ Wi-Fi | 決定如何將掃描器連線至網路。<br>若為有線 LAN，請連接至 LAN 交換機。<br>若為 Wi-Fi，連接至存取點的網路 (SSID)。 |
| LAN 連線資訊 | ❏ IP 位址<br>❏ 子網路遮罩<br>❏ 預設閘道 | 決定要指派給掃描器的 IP 位址。<br>當您指派靜態 IP 位址時，所有值均為必填資訊。<br>當您使用 DHCP 功能指派動態 IP 位址時，由於系統會自動設定，因此不需要此資訊。 |
| Wi-Fi 連線資訊 | ❏ SSID<br>❏ 密碼 | 這些是掃描器所連接之存取點的 SSID（網路名稱）和密碼。<br>若已設定了 MAC 位址篩選功能，請事先登錄掃描器的 MAC 位址，再登錄掃描器。<br>請參考下文以瞭解支援的標準。<br>第27頁“網路規格” |
| DNS 伺服器資訊 | ❏ 主 DNS 的 IP 位址<br>❏ 輔助 DNS 的 IP 位址 | 這些是指定 DNS 伺服器時的必要資訊。當系統具有冗餘配置且存在輔助 DNS 伺服器時，請設定輔助 DNS 的資訊。<br>若您處在小型組織中，且未設定 DNS 伺服器，則請設定路由器的 IP 位址。 |

| 部分 | 項目 | 附註 |
| --- | --- | --- |
| Proxy 伺服器資訊 | ❏ Proxy 伺服器名稱 | 當您的網路環境使用 Proxy 伺服器以從內部網路存取網際網路，且您使用掃描器直接存取網際網路的功能時，請設定此項。<br>掃描器可直接連接至網際網路以取得以下功能。<br>❏ Epson Connect 服務<br>❏ 其他公司的雲端服務<br>❏ 韌體更新<br>❏ 傳送掃描影像至 SharePoint(WebDAV) |
| 連接埠號碼資訊 | ❏ 要解除的連接埠號碼 | 檢查掃描器和電腦使用的連接埠號碼，如有必要，請釋放被防火牆封鎖的連接埠。<br>參考下列內容以查看被掃描器使用的連接埠編號。<br>第29頁“掃描器使用的連接埠” |

## IP 位址指派

下列是 IP 位址的指派類型。

**靜態 IP 位址：**

將預先確定的 IP 位址手動指派給掃描器 (主機)。

需要手動設定連接至網路的資訊 (子網路遮罩、預設閘道、DNS 伺服器等)。

即使關閉裝置，IP 位址也不會變動，因此，若要在無法變更 IP 位址的環境中管理裝置，或希望使用 IP 位址來管理裝置，此功能將非常實用。我們建議在許多電腦存取的掃描器、伺服器等上進行設定。另外，使用 IPsec/IP 篩選等安全功能時，請指派固定的 IP 位址，以免 IP 位址發生變動。

**使用 DHCP 功能 (動態 IP 位址) 自動指派：**

使用 DHCP 伺服器或路由器的 DHCP 功能，自動將 IP 位址指派給掃描器 (主機)。

連接至網路的資訊 (子網路遮罩、預設閘道、DNS 伺服器等) 會自動設定，因此您可輕鬆地將裝置連接至網路。

若裝置或路由器關閉，或根據 DHCP 伺服器設定，重新連接時 IP 位址可能會改變。

我們建議您管理 IP 位址以外的裝置，並使用可追蹤 IP 位址的通訊協定進行通訊。

附註：
使用 DHCP 的 IP 位址預留功能時，您可隨時為裝置指派相同的 IP 位址。

## DNS 伺服器與 Proxy 伺服器

DNS 伺服器具有與 IP 位址資訊相關聯的主機名稱、電子郵件地址的網域名稱等。

當電腦或掃描器執行 IP 通訊時，若另一方採用主機名稱、網域名稱等方式描述，則無法進行通訊。

查詢 DNS 伺服器以取得相關資訊，並獲取另一方的 IP 位址。此程序稱為名稱解析。

因此，電腦和掃描器等裝置可以使用 IP 位址進行通訊。

掃描器使用電子郵件功能或網際網路連線功能進行通訊時，必須執行名稱解析程序。

當您使用這些功能時，請進行 DNS 伺服器設定。

當您使用 DHCP 伺服器或路由器的 DHCP 功能指派掃描器的 IP 位址時，系統即會自動設定。

Proxy 伺服器放置在網路與網際網路之間的閘道處，且其可與電腦、掃描器及代表它們的網際網路（對方伺服器）通訊。對方伺服器只會與 Proxy 伺服器通訊。因此，IP 位址與連接埠號碼等掃描器資訊將無法被讀取，進而期望能提升安全性。

當您透過 Proxy 伺服器連接至網際網路時，請在掃描器上配置 Proxy 伺服器。

# 從控制面板連接至網路

使用掃描器的控制面板連接掃描器至網路。

## 指派 IP 位址

設定基本項目，如「主機位址」、子網路遮罩、預設閘道。

本節介紹設定靜態 IP 位址的步驟。

1. 開啟掃描器。
2. 在掃描器控制面板的主畫面上選取 [設定]。
3. 選取 [網路設定] > [進階] > [TCP/IP]。
4. 選取 [手動] 以 [取得 IP 位址]。

   使用路由器的 DHCP 功能自動設定 IP 位址時，請選取 [自動取得]。在此情況下，步驟 5 到 6 所提及的 [IP 位址]、[子網路遮罩] 及 [預設閘道] 也會自動設定，因此請前往步驟 7。
5. 輸入 IP 位址。

   若您選取 ◀ 和 ▶，焦點會移動至前一個區段或後一個區段（以句點分隔）。

   確認在上一個畫面反映的值。
6. 設定 [子網路遮罩] 與 [預設閘道]。

   確認在上一個畫面反映的值。

   > **重要事項：**
   > 如果 IP 位址、子網路遮罩 與 預設閘道 的組合錯誤，[開始設定] 會停用且無法繼續進行設定。請確認輸入內容正確無誤。
7. 輸入主 DNS 伺服器的 IP 位址。

   確認在上一個畫面反映的值。

   附註：
   當您選取 [自動取得]　作為 IP 位址指派設定時，可從 [手動]　或 [自動取得] 選取 DNS 伺服器設定。如果您無法自動取得 DNS 伺服器位址，請選取 [手動] 並輸入 DNS 伺服器位址。然後，直接輸入輔助 DNS 伺服器位址。如果您選取 [自動取得]，請前往步驟 9。
8. 輸入次 DNS 伺服器的 IP 位址。

   確認在上一個畫面反映的值。
9. 點選 [開始設定]。

### 設定 Proxy 伺服器

若以下兩個條件均成立，則設定 Proxy 伺服器。

❏ Proxy 伺服器專為網際網路連線而建立。

❏ 當使用掃描器直接連接至網際網路的功能時，如 Epson Connect 服務或其他公司的雲端服務。

1. 從主畫面選取 [設定]。
   在設定 IP 位址之後進行設定時，會顯示 [進階] 畫面。前往步驟 3。
2. 選取 [網路設定] > [進階]。
3. 選取 [Proxy 伺服器]。
4. 選取 [使用] 以 [Proxy 伺服器設定]。
5. 輸入 IPv4 或 FQDN 格式 Proxy 伺服器的位址。
   確認在上一個畫面反映的值。
6. 輸入 Proxy 伺服器的連接埠號碼。
   確認在上一個畫面反映的值。
7. 點選 [開始設定]。

## 連線至乙太網路

使用 LAN 連接線將掃描器連線至網路，然後檢查連線。

1. 使用 LAN 連接線連接掃描器與集線器（LAN 開關）。
2. 從主畫面選取 。
3. 選取 [路由器]。
4. 確認 連線狀態 和 IP 位址 設定準確無誤。
5. 點選 [關閉]。

## 連線至無線 LAN (Wi-Fi)

您可以多種方式將掃描器連接至無線 LAN (Wi-Fi)。選擇與您所使用環境及條件相符的連線方式。

如果您知道無線路由器的資訊，如 SSID 與密碼，可以手動設定。

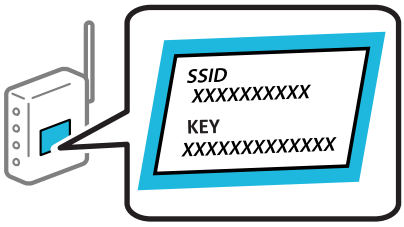
如果無線路由器支援 WPS，您也可以透過按鍵設定進行設定。

將掃描器連線至網路後，連線您希望使用的裝置（電腦、智慧型裝置、平板電腦等）至掃描器。

### 透過輸入 SSID 和密碼進行 Wi-Fi 設定

您可以從掃描器控制面板輸入連接至無線路由器所需的必要資訊而設定 Wi-Fi 網路。若要使用此方法進行設定，需要無線路由器的 SSID 和密碼。

附註：
如果在默認設置下使用無線路由器，則 SSID 和密碼在標籤上。如果您不知道 SSID 和密碼，請聯絡設定無線路由器的人員，或者參考無線路由器隨附的說明文件。




1. 在主畫面點選 。
2. 選取 [路由器]。
3. 點選 [開始設定]。

   若已設定網路連線，會顯示連線詳細資訊。點選 [變更至 Wi-Fi 連線。] 或 [變更設定] 以變更設定。
4. 選取 [Wi-Fi 設定嚮導]。
5. 依照畫面上的指示選取 SSID、輸入無線路由器密碼，並開始設定。

   如果您想要在設定完成後檢查掃描器的網路連線狀態，參閱下方相關資訊連結以了解詳細說明。

   附註：
   - ❏ 如果您不知道 SSID，看看是否寫在無線路由器的標籤上。如果在預設值下使用無線路由器，則使用寫在標籤上的 SSID。如果找不到任何資訊，請參閱無線路由器附帶的文件。
   - ❏ 密碼會區分大小寫。
   - ❏ 如果您不知道密碼，請檢查該資訊是否寫在無線路由器的標籤上。在標籤上，密碼可能書寫為「Network Key」、「Wireless Password」等。如果在預設值下使用無線路由器，則使用寫在標籤上的密碼。

**相關資訊**

➡ 第26頁“檢查網路連線狀態”

## 透過按鍵設定 (WPS) 進行 Wi-Fi 設定

您可以藉由按下無線路由器上的按鈕自動建立 Wi-Fi 網路。如果滿足以下條件，您就能使用這套方法設定。

❏ 無線路由器與 WPS (Wi-Fi Protected Setup) 相容。

❏ 目前的 Wi-Fi 連接是藉由按下無線路由器上的按鈕建立。

附註：
如果您找不到按鍵或正使用軟體設定，請參見無線路由器隨附的說明文件。

1. 在主畫面點選 。
2. 選取 [路由器]。

3. 點選 [開始設定]。

   若已設定網路連線，會顯示連線詳細資訊。點選 [變更至 Wi-Fi 連線。] 或 [變更設定] 以變更設定。

4. 選取 [按鍵模式設定 (WPS)]。

5. 依照畫面上的指示進行操作。

   如果您想要在設定完成後檢查掃描器的網路連線狀態，參閱下方相關資訊連結以了解詳細說明。

   附註：
   如果連線失敗，重新啟動無線路由器，將其移動到更靠近掃描器的位置，然後再次嘗試。

**相關資訊**

➡ 第26頁“檢查網路連線狀態”

### 透過 PIN 碼設定 (WPS) 進行 Wi-Fi 設定

您可以透過使用 PIN 碼自動連接至無線路由器。如果無線路由器具有 WPS (Wi-Fi Protected Setup) 功能，您可以使用此方法進行設定。使用電腦輸入 PIN 代碼到無線路由器。

1. 在主畫面點選 。

2. 選取 [路由器]。

3. 點選 [開始設定]。

   若已設定網路連線，會顯示連線詳細資訊。點選 [變更至 Wi-Fi 連線。] 或 [變更設定] 以變更設定。

4. 選取 [其他] > [PIN 碼設定 (WPS)]

5. 依照畫面上的指示進行操作。

   如果您想要在設定完成後檢查掃描器的網路連線狀態，參閱下方相關資訊連結以了解詳細說明。

   附註：
   有關輸入 PIN 碼的詳情，請參見無線路由器隨附的說明文件。

**相關資訊**

➡ 第26頁“檢查網路連線狀態”

# 新增或更換電腦或裝置

## 連接至已連接網路的掃描器

當掃描器已連接至網路時，您可透過網路將電腦或智慧型裝置連接至掃描器。

## 從第二台電腦使用網路掃描器

我們建議使用安裝程式將掃描器連線至電腦。您可以透過下列方法之一，執行安裝程式。

❏ 從網站設定
存取以下網站，然後輸入產品名稱。前往 [設定]，然後開始設定。
http://epson.sn

❏ 使用軟體光碟片執行設定（僅限配有軟體光碟片的型號，以及配有光碟機的 Windows 電腦使用者）。
將軟體光碟片插入電腦，然後依照畫面上的指示進行操作。

**選取掃描器**

遵循畫面上的指示直到顯示下一畫面，選取您要連接的掃描器名稱，然後點選 [下一步]。

依照畫面上的指示進行操作。

## 從智慧型裝置使用網路掃描器

您可以使用下列其中一種方法將掃描器連接到智慧型裝置。

**透過無線路由器連接**

將智慧型裝置連接到與掃描器相同的 Wi-Fi 網路 (SSID)。

如需詳細資訊，請參閱下列說明。

第24頁“進行智慧型裝置連接設定”

**透過 Wi-Fi Direct 連接**

將智慧型裝置無需無線路由器而直接連接至掃描器。

如需詳細資訊，請參閱下列說明。

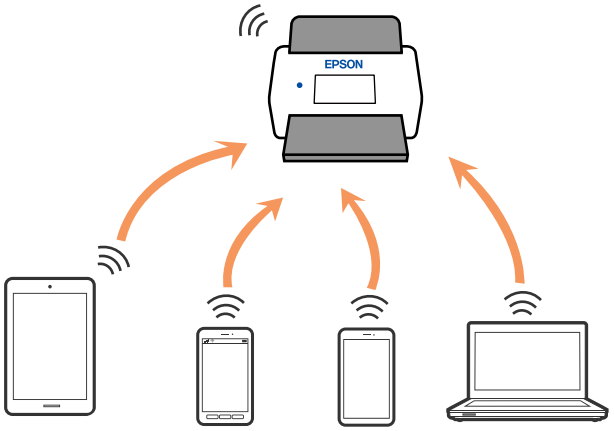
第22頁“直接連接智慧型裝置與掃描器 (Wi-Fi Direct)”

# 直接連接智慧型裝置與掃描器 (Wi-Fi Direct)

Wi-Fi Direct (Simple AP) 允許您將智慧型裝置直接連接至掃描器，無需無線路由器，並可從智慧型裝置進行掃描。

## 關於 Wi-Fi Direct

當您不是在家中或辦公室使用 Wi-Fi，或您想直接連接掃描器及電腦或智慧型裝置時，可使用此連線方法。掃描器在此模式下能作為無線路由器，您可直接將裝置連接至掃描器，而無需使用標準無線路由器。然而，直接連線至掃描器的裝置之間無法透過掃描器互相通訊。




掃描器可透過 Wi-Fi 或乙太網路和 Wi-Fi Direct (Simple AP) 連線模式同時連線。然而，若於掃描器透過 Wi-Fi Direct 連線時，在 Wi-Fi (Simple AP) 連線模式下開始網路連線，Wi-Fi 將會暫時中斷。

## 使用 Wi-Fi Direct 連接至智慧型裝置

此方法可不透過無線路由器，將掃描器直接連接到智慧型裝置。

1. 從主畫面選取 。
2. 選取 [Wi-Fi Direct]。
3. 選取 [開始設定]。
4. 在您的智慧型裝置上啟動 Epson Smart Panel。
5. 遵循 Epson Smart Panel 上顯示的說明連接至您的掃描器。
   當您的智慧型裝置連接至掃描器後，前往下一步。
6. 在掃描器控制面板上，選取 [完成]。

## 斷開 Wi-Fi Direct (Simple AP) 連線

有兩種方法可用於停用 Wi-Fi Direct (Simple AP) 連線；您可使用掃描器控制面板停用所有連線；或從電腦或智慧型裝置停用每個連線。

若要禁用所有連線，請選取 > [Wi-Fi Direct] > [開始設定] > [變更] > [刪除 Wi-Fi Direct]。

**重要事項：**

在 Wi-Fi Direct (Simple AP) 連接被禁用後，所有以 Wi-Fi Direct (Simple AP) 連接方式連接到掃描器的電腦和智慧型裝置將斷開連接。

附註：
如果您想斷開特定裝置的連線，請從裝置而非掃描器斷開連線。使用下述方法之一從裝置斷開 Wi-Fi Direct (Simple AP) 連線。

- ❏ 斷開至掃描器網路名稱 (SSID) 的 Wi-Fi 連線。
- ❏ 連接至另一網路名稱 (SSID)。

## 變更 SSID 等 Wi-Fi Direct (Simple AP) 設定

在啟用 Wi-Fi Direct (Simple AP) 連線後，您可從 > [Wi-Fi Direct] > [開始設定] > [變更] 變更設定，然後下列功能表項目隨即顯示。

### 變更網路名稱

將用於連接至掃描器的 Wi-Fi Direct (Simple AP) 網路名稱 (SSID) 變更為您的任意名稱。您可將網路名稱 (SSID) 設定為控制面板軟體鍵盤上顯示的 ASCII 字元。您可輸入最多 22 個字元。

變更網路名稱 (SSID) 時，所有連接的裝置將斷開連接。如果要重新連接裝置，請使用該網路名稱 (SSID)。

### 變更密碼

變更用於連接掃描器至您的任意值的 Wi-Fi Direct (Simple AP) 密碼。您可以使用控制面板上的軟體鍵盤所顯示的 ASCII 字元來設定密碼。可輸入 8 至 22 個字元。

變更密碼時，所有連接的裝置將斷開連接。若要重新連接裝置，請使用新密碼。

### 變更頻率範圍

變更用於連接至掃描器的 Wi-Fi Direct 頻率範圍。您可選取 2.4 GHz 或 5 GHz。

在變更頻率範圍時，所有連接的裝置將斷開連接。重新連接裝置。

請注意，當變更為 5 GHz 時，您無法從不支援 5 GHz 的裝置重新連接。

視您所在地區的不同，可能無法顯示此設定。

### 刪除 Wi-Fi Direct

停用掃描器的 Wi-Fi Direct (Simple AP) 設定。停用時，所有以 Wi-Fi Direct (Simple AP) 連線連接至掃描器的裝置均將中斷連線。

### 回復至出廠預設值

將所有 Wi-Fi Direct (Simple AP) 設定恢復為預設值。

儲存至掃描器的智慧型裝置 Wi-Fi Direct (Simple AP) 連線資訊被刪除。

附註：
您也可以從 Web Config 上的 [網路] 索引標籤 > [Wi-Fi Direct] 進行下列設定。

- ❏ 啟用或停用 Wi-Fi Direct (Simple AP)
- ❏ 變更網路名稱 (SSID)
- ❏ 變更密碼
- ❏ 變更頻率範圍
  視您所在地區的不同，可能無法顯示此設定。
- ❏ 恢復 Wi-Fi Direct (Simple AP) 設定

# 重新設定網路連線

本節說明在更換無線路由器或電腦時，如何設定網路連線及變更連線方式。

## 更換無線路由器時

更換無線路由器時，進行電腦或其他智慧型裝置與掃描器之間的連線設定。

如果您要變更您的網際網路服務提供商等，您需要進行這些設定。

### 進行電腦連接設定

我們建議使用安裝程式將掃描器連線至電腦。您可以透過下列方法之一，執行安裝程式。

- ❏ 從網站設定
  存取以下網站，然後輸入產品名稱。前往 [設定]，然後開始設定。
  http://epson.sn
- ❏ 使用軟體光碟片執行設定（僅限配有軟體光碟片的型號，以及配有光碟機的 Windows 電腦使用者）。
  將軟體光碟片插入電腦，然後依照畫面上的指示進行操作。

### 選取連線方法

依照畫面上的指示進行操作。在 [選擇操作] 畫面上，選取 [重新設定印表機連線。(適用於新的網路路由器或將 USB 變更為網路等情況)]，然後按下 [下一步]。

依照畫面上的指示完成設定。

如果無法連接，請查看下列內容以嘗試解決該問題。

第30頁“無法連接至網路”

### 進行智慧型裝置連接設定

當您將掃描器和智慧型裝置連接到同一個 Wi-Fi 網路 (SSID) 時，可從智慧型裝置使用掃描器。若要透過智慧型裝置使用掃描器，請存取以下網站，然後輸入產品名稱。前往 [設定]，然後開始設定。

http://epson.sn

使用您想連線至掃描器的智慧型裝置訪問以下網站。

## 變更電腦時

變更電腦時，進行電腦與掃描器之間的連線設定。

### 進行電腦連接設定

我們建議使用安裝程式以連線掃描器至電腦。您可以使用下列方法之一執行安裝程式。

❏ 從網站設定
存取以下網站，然後輸入產品名稱。前往 [設定]，然後開始設定。
http://epson.sn

❏ 使用軟體光碟片執行設定 (僅限配有軟體光碟片的型號，以及配有光碟機的 Windows 電腦使用者)。
將軟體光碟片插入電腦，然後按照螢幕說明進行操作。

依照畫面上的指示進行操作。

## 變更與電腦的連線方法

本節說明在電腦與掃描器已連接時，如何變更連線方法。

### 將網路連線從乙太網變更為 Wi-Fi

從掃描器控制面板將乙太網連線變更為 Wi-Fi。變更連線的方法基本與 Wi-Fi 連線設定相同。

#### 相關資訊

➡ 第18頁“連線至無線 LAN (Wi-Fi)”

### 將網路連線從 Wi-Fi 變更為乙太網

遵循下列步驟從 Wi-Fi 連線變更為乙太網連線。

1. 從主畫面選取 [設定]。
2. 選取 [網路設定] > [有線區域網路設定]。
3. 依照畫面上的指示進行操作。

### 從 USB 變更為網路連線

透過不同的連線方法使用安裝程式和重新設定。

❏ 從網站設定
存取以下網站，然後輸入產品名稱。前往 [設定]，然後開始設定。
http://epson.sn

❏ 使用軟體光碟片執行設定（僅限配有軟體光碟片的型號，以及配有光碟機的 Windows 電腦使用者）。
將軟體光碟片插入電腦，然後依照畫面上的指示進行操作。

**選取變更連線方法**

依照畫面上的指示進行操作。在 [選擇操作] 畫面上，選取 [重新設定印表機連線。(適用於新的網路路由器或將 USB 變更為網路等情況)]，然後按下 [下一步]。

選取您要使用的網路連線，[透過無線網路 (Wi-Fi) 連接] 或 [透過有線區域網路 (乙太網路) 連線]，然後點選 [下一步]。

依照畫面上的指示完成設定。

# 檢查網路連線狀態

您可透過下列方式檢查網路連線狀態。

## 從控制台查看網路連線狀態

您可以使用掃描器控制面板上的網路圖示或網路資訊檢查網路連接狀態。

### 使用網路圖示檢查網路連線狀態

您可使用掃描器主畫面的網路圖示檢查網路連線狀態以及無線電波的強度。

| | | |
|---|---|---|
| | 顯示網路連線狀態。<br>選取此圖示可查看並變更目前設定。此為下列功能表的捷徑。<br>[設定] > [網路設定] > [Wi-Fi 設定] | |
| | | 掃描器未連線至無線 (Wi-Fi) 網路。 |
| | | 掃描器正在搜尋 SSID、未設定 IP 位址或無線 (Wi-Fi) 網路存在問題。 |
| | | 掃描器連線至無線 (Wi-Fi) 網路。<br>格數表示連線的訊號強度。格數越多，表示連線越穩定。 |
| | | 掃描器未連線至處於 Wi-Fi Direct (Simple AP) 模式下的無線 (Wi-Fi) 網路。 |
| | | 掃描器已連線至處於 Wi-Fi Direct (Simple AP) 模式下的無線 (Wi-Fi) 網路。 |
| | | 掃描器未連線至有線網路 (乙太網路) 或未設定。 |
| | | 掃描器已連線至有線網路 (乙太網路)。 |

## 從控制面板顯示詳細網路資訊

當掃描器連接至網路後，您也可以選取您想要查看的網路功能表，以查看其他與網路相關的資訊。

1. 從主畫面選取 [設定]。
2. 選取 [網路設定] > [網路狀態]。
3. 若要查看資訊，請選取您希望查看的功能表。
   - ❏ 有線區域網路/Wi-Fi狀態
     顯示乙太網路或 Wi-Fi 連線的網路資訊（裝置名稱、連線、訊號強度等）。
   - ❏ Wi-Fi Direct 狀態
     顯示 Wi-Fi Direct 是啟用還是停用，以及 SSID 連線的 Wi-Fi Direct、密碼等資訊。
   - ❏ 電子郵件伺服器狀態
     顯示電子郵件伺服器的網路資訊。

# 網路規格

## Wi-Fi 規格

請參閱下表以了解 Wi-Fi 規格。

| | |
|---|---|
| 下面列示以外的國家或地區 | 表 A |
| 澳洲<br>紐西蘭<br>台灣<br>韓國 | 表 B |

表 A

| | |
|---|---|
| 標準 | IEEE 802.11b/g/n[*1] |
| 頻率範圍 | 2.4 GHz |
| 最大傳輸無線電頻率功率 | 2,400—2,483.5 MHz：20 dBm (EIRP) |
| 通道 | 1/2/3/4/5/6/7/8/9/10/11/12/13 |
| 連線模式 | 架構、Wi-Fi Direct (Simple AP)[*2][*3] |
| 安全協議[*4] | WEP (64/128bit)、WPA2-PSK (AES)[*5]、WPA3-SAE (AES)、WPA2/WPA3-Enterprise |

*1 僅適用於 HT20。

*2 不支援 IEEE 802.11b。

*3 Infrastructure 和 Wi-Fi Direct 模式或乙太網連線可同時使用。

*4 Wi-Fi Direct 僅支援 WPA2-PSK (AES)。

*5 與 WPA2 標準相容並支援 WPA/WPA2 個人版。

表 B

| | | | |
|---|---|---|---|
| 標準 | IEEE 802.11a/b/g/n*1/ac | | |
| 頻率範圍 | IEEE 802.11b/g/n：2.4 GHz、IEEE 802.11a/n/ac：5 GHz | | |
| 通道 | Wi-Fi | 2.4 GHz | 1/2/3/4/5/6/7/8/9/10/11/12*2/13*2 |
| | | 5 GHz*3 | W52 (36/40/44/48)，<br>W53 (52/56/60/64)，<br>W56 (100/104/108/112/116/120/124/128/132/136/140/144)，<br>W58 (149/153/157/161/165) |
| | Wi-Fi Direct | 2.4 GHz | 1/2/3/4/5/6/7/8/9/10/11/12*2/13*2 |
| | | 5 GHz*3 | W52 (36/40/44/48)<br>W58 (149/153/157/161/165) |
| 連線模式 | Infrastructure、Wi-Fi Direct (Simple AP)*4、*5 | | |
| 安全協議*6 | WEP (64/128bit)、WPA2-PSK (AES)*7、WPA3-SAE (AES)、WPA2/WPA3-Enterprise | | |

*1 僅適用於 HT20。

*2 不適用於台灣。

*3 這些通道的可用性及透過這些通道在戶外是否可在戶外透過這些通道使用本產品隨地點而不同。若需更多資訊，請參閱 http://support.epson.net/wifi5ghz/

*4 不支援 IEEE 802.11b。

*5 Infrastructure 和 Wi-Fi Direct 模式或乙太網連線可同時使用。

*6 Wi-Fi Direct 僅支援 WPA2-PSK (AES)。

*7 與 WPA2 標準相容並支援 WPA/WPA2 個人版。

# 乙太網路規格

| | |
|---|---|
| 標準 | IEEE802.3i (10BASE-T)*1<br>IEEE802.3u (100BASE-TX)*1<br>IEEE802.3ab (1000BASE-T)*1<br>IEEE802.3az (Energy Efficient Ethernet)*2 |
| 連線方式 | 自動、10 Mbps 全雙工、10 Mbps 半雙工、100 Mbps 全雙工、100 Mbps 半雙工 |
| 接頭 | RJ-45 |

*1 為防止無線電干擾的危險，請使用 Category 5e 或更高等級的 STP (屏蔽雙絞線) 連接線。

*2 連接的裝置應符合 IEEE802.3az 標準。

# 網路功能和 IPv4/IPv6

| 功能 | 支援 |
|---|---|
| Epson Scan 2 | IPv4、IPv6 |
| Document Capture Pro/Document Capture | IPv4 |
| Document Capture Pro Server | IPv4、IPv6 |

# 安全性通訊協定

| | |
|---|---|
| IEEE802.1X* | |
| IPsec/IP 篩選 | |
| SSL/TLS | HTTPS 伺服器/用戶端 |
| SMTPS (STARTTLS、SSL/TLS) | |
| SNMPv3 | |

* 您必須使用符合 IEEE802.1X 的連線裝置。

# 掃描器使用的連接埠

掃描器會使用下列連接埠。這些連接埠應可在必要時由管理員允許使其可用。

**當傳送人（用戶端）是掃描器時**

| 使用 | 目的地（伺服器） | 協議 | 連接埠編號 |
|---|---|---|---|
| 檔案傳送（從掃描器使用掃描至網路資料夾時） | FTP/FTPS 伺服器 | FTP/FTPS (TCP) | 20 |
| | | | 21 |
| | 檔案伺服器 | SMB (TCP) | 445 |
| | | NetBIOS (UDP) | 137 |
| | | | 138 |
| | | NetBIOS (TCP) | 139 |
| | WebDAV 伺服器 | Protocol HTTP (TCP) | 80 |
| | | Protocol HTTPS(TCP) | 443 |
| 電郵傳送（從掃描器使用掃描至郵件時） | SMTP 伺服器 | SMTP (TCP) | 25 |
| | | SMTP SSL/TLS (TCP) | 465 |
| | | SMTP STARTTLS (TCP) | 587 |
| SMTP 連線之前的 POP（從掃描器使用掃描至郵件時） | POP 伺服器 | POP3 (TCP) | 110 |

| 使用 | 目的地（伺服器） | 協議 | 連接埠編號 |
|---|---|---|---|
| 使用 Epson Connect 時 | Epson Connect 伺服器 | HTTPS | 443 |
| | | XMPP | 5222 |
| 收集使用者資訊（從掃描器使用連絡人） | LDAP 伺服器 | LDAP (TCP) | 389 |
| | | LDAP SSL/TLS (TCP) | 636 |
| | | LDAP STARTTLS (TCP) | 389 |
| 收集使用者資訊時的使用者授（從掃描器使用連絡人時）<br>從掃描器使用掃描至網路資料夾 (SMB) 時的使用者授權 | KDC 伺服器 | Kerberos | 88 |
| 控制 WSD | 用戶端電腦 | WSD (TCP) | 5357 |
| 從應用程式推送掃描時搜尋電腦 | 用戶端電腦 | 網路推送掃描發現 | 2968 |

**當傳送人（用戶端）是用戶端電腦時**

| 使用 | 目的地（伺服器） | 協議 | 連接埠編號 |
|---|---|---|---|
| 從應用程式 (如 EpsonNet Config) 與掃描器驅動程式探索掃描器。 | 掃描器 | ENPC (UDP) | 3289 |
| 從應用程式 (如 EpsonNet Config) 與掃描器驅動程式收集並設定 MIB 資訊。 | 掃描器 | SNMP (UDP) | 161 |
| 搜尋 WSD 掃描器 | 掃描器 | WS-Discovery (UDP) | 3702 |
| 轉寄來自應用程式的掃描資料 | 掃描器 | 網路掃描 (TCP) | 1865 |
| 從應用程式推送掃描時收集工作資訊 | 掃描器 | 網路推送掃描 | 2968 |
| Web Config | 掃描器 | HTTP (TCP) | 80 |
| | | HTTPS (TCP) | 443 |

# 解決問題

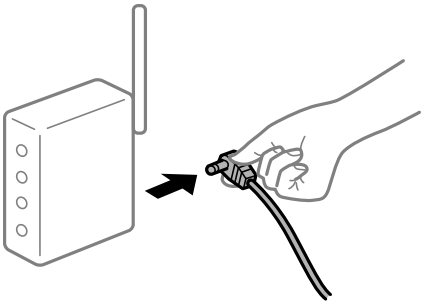
## 無法連接至網路

原因可能是下列問題之一。

## 網路裝置的 Wi-Fi 連線存在錯誤。

### 解決方法

關閉您要連線到網路的裝置。等待 10 秒鐘左右，然後按照以下次序打開裝置：無線路由器、電腦或智慧型裝置，然後是掃描器。將掃描器和電腦或智慧型裝置移近無線路由器，以改善無線電通信，然後再次嘗試進行網路設定。



## 裝置由於距離太遠而無法收到無線路由器的訊號。

### 解決方法

將電腦或智慧型裝置和掃描器更靠近無線路由器後，關閉無線路由器，然後再次將其開啟。

## 變更無線路由器時，設置與新路由器不匹配。

### 解決方法

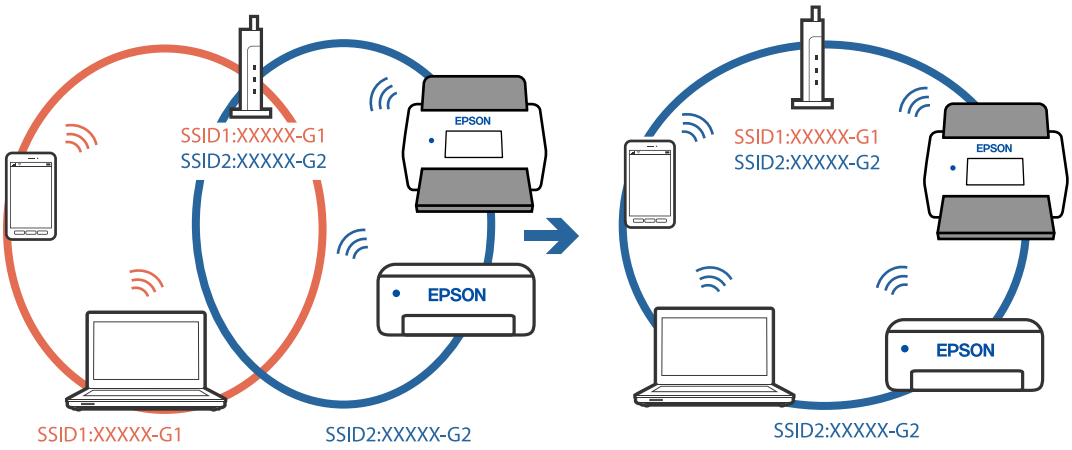
再次進行連線設定，使其與新無線路由器匹配。

## 從電腦或智慧型裝置與電腦連接的 SSID 不相同。

### 解決方法

當您同時使用多個無線路由器或無線路由器擁有多個 SSID，並且裝置連接至不同 SSID 時，您無法連接至無線路由器。

將電腦或智慧型裝置連線至與掃描器相同的 SSID。



## 無線路由器提供 Privacy Separator（隱私區分）可用。

### 解決方法

大部分無線路由器具有 Privacy Separator（隱私區分）功能，可阻止所連接裝置間的通訊。如果在掃描器和電腦或智慧型裝置連線至相同網路後仍無法通訊，請停用無線路由器上的 Privacy Separator（隱私區分）。詳細資訊，請參考無線路由器隨附的手冊。

## IP 位址指派有誤。

### 解決方法

如果指派給掃描器的 IP 位址是 169.254.XXX.XXX，且子網路遮罩為 255.255.0.0，表示可能未正確指派 IP 位址。

在掃描器控制面板上選取 [設定] > [網路設定] > [進階] > [TCP/IP 設定]，然後檢查 IP 位址及指派給掃描器的子網路遮罩。

請重新啟動無線路由器或重設掃描器的網路設定。

## 電腦上的網路設定存在問題。

### 解決方法

試著在您的電腦上存取任意網站，檢查您的電腦的網路設定是否正確。如果無法存取任何網站，則電腦出了問題。

檢查電腦的網路連線。詳情請參見電腦提供的文件。

## 掃描器使用支援 IEEE 802.3az（節能高效乙太網）的裝置透過乙太網進行連接。

### 解決方法

使用支援 IEEE 802.3az（節能高效乙太網）的裝置透過乙太網路連接掃描器時，依據您使用的集線器或路由器，可能出現下列問題。

- ❏ 連線變得不穩定，掃描器反復連接和斷開連接。
- ❏ 無法連接至掃描器。
- ❏ 通訊速度變慢。

依照下面的步驟為掃描器停用 IEEE 802.3az，然後進行連接。

1. 取下連接到電腦和掃描器的乙太網路線纜。
2. 如果已為電腦啟用 IEEE 802.3az，則將其停用。

   詳情請參見電腦提供的文件。
3. 使用乙太網路線纜直接連接電腦和掃描器。
4. 在掃描器上，檢查網路設定。

   選取 [設定] > [網路設定] > [網路狀態] > [有線區域網路/Wi-Fi狀態]。
5. 檢查掃描器的 IP 位址。
6. 在電腦上，存取 Web Config。

   啟動網頁瀏覽器，然後輸入掃描器的 IP 位址。

   第35頁“在網頁瀏覽器上執行 Web Config”

7. 選取 [網路] 索引標籤 > [有線區域網路]。
8. 選取 [關閉] 以 [IEEE 802.3az]。
9. 按下 [下一步]。
10. 按下 [確定]。
11. 取下連接到電腦和掃描器的乙太網路線纜。
12. 如果已在步驟 2 中為電腦停用 IEEE 802.3az，則將其啟用。
13. 將您在步驟 1 中取下的乙太網路線纜連接到電腦和掃描器。

如果問題依然發生，則可能是掃描器以外的其他裝置導致了此問題。

## 掃描器已關閉。

### 解決方法

確保掃描器已啟動。

此外，等到狀態燈號停止閃爍，表示掃描器已就緒，可執行掃描。

# 掃描器設定軟體

Web Config. . . . . 35

Epson Device Admin. . . . . .36

# Web Config

Web Config 是可在電腦上的 Microsoft Edge、Safari 等網頁瀏覽器中執行的應用程式。您可確認掃描器狀態，或變更網路服務與掃描器設定。由於掃描器直接從網路存取和操作，因此適合每次設定一台掃描器。若要使用 Web Config，請將電腦連接至與掃描器相同的網路。

支援以下瀏覽器。使用最新版本。

Microsoft Edge、Windows Internet Explorer、Firefox、Chrome、Safari

附註：
您可能會在使用此裝置時被提示輸入管理員密碼。請參閱下列內容以了解關於管理員密碼的詳細資訊。

第10頁“管理員密碼備註”

**相關資訊**

➡ 第69頁“無法存取 Web Config”

## 在網頁瀏覽器上執行 Web Config

1. 檢查掃描器的 IP 位址。

   選取掃描器控制面板上的 [設定] > [網路設定] > [網路狀態]。然後選擇活躍連線方式（[有線區域網路/Wi-Fi狀態] 或 [Wi-Fi Direct 狀態]）以確認掃描器的 IP 位址。

2. 從電腦或智慧型裝置啟動網頁瀏覽器，然後輸入掃描器的 IP 位址。

   格式：

   IPv4: http://掃描器的 IP 位址/

   IPv6: http://[掃描器的 IP 位址]/

   範例：

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   附註：
   由於掃描器在存取 HTTPS 時使用自我簽名證書，當您啟動 Web Config 時，瀏覽器上會顯示一條警告；這並不表示發生了問題，可安全地忽略。

3. 以管理員身份登入以變更掃描器設定。

   點按畫面最右側的 [登入]。輸入 [使用者名稱] 與 [目前密碼]，然後按下 [確定]。

   附註：
   ❏ 下列內容提供 Web Config 管理員資訊的初始值。
   · 使用者名稱：無（空白）
   · 密碼：視乎產品背面附帶的標籤而定。
   如果背面附帶「PASSWORD」標籤，則輸入標籤上顯示的 8 位數字。
   如果背面沒有附帶「PASSWORD」標籤，則輸入產品背面附帶標籤上的序列號以作為初始管理員密碼。
   ❏ 如果畫面最右側顯示 [登出]，表明您已經以管理員身份登入。
   ❏ 您將在大約 20 分鐘無活動後被自動登出。

## 在 Web Config 上執行 Windows

當使用 WSD 將電腦連線至掃描器時，請遵循下列步驟以執行 Web Config。

1. 開啟電腦上的掃描器清單。
   - ❏ Windows 10
     按下開始鍵，然後選取 [Windows 系統] > [控制台] > [硬體和音效]中的[檢視裝置和印表機]。
   - ❏ Windows 8.1/Windows 8
     選取[桌面] > [設定] > [控制台] > [硬體和音效] (或[硬體]) 中的[檢視裝置和印表機]。
   - ❏ Windows 7
     按下開始鍵，選取[控制台] > [硬體和音效]中的[檢視裝置和印表機]。
2. 在掃描器上按右鍵，然後選取[內容]。
3. 選取 [Web 服務]索引標籤並按一下 URL。
   由於掃描器在存取 HTTPS 時使用自我簽名證書，當您啟動 Web Config 時，瀏覽器上會顯示一條警告；這並不表示發生了問題，可安全地忽略。
   附註：
   - ❏ 下列內容提供 Web Config 管理員資訊的初始值。
     · 使用者名稱：無（空白）
     · 密碼：視乎產品背面附帶的標籤而定。
     如果背面附帶「PASSWORD」標籤，則輸入標籤上顯示的 8 位數字。
     如果背面沒有附帶「PASSWORD」標籤，則輸入產品背面附帶標籤上的序列號以作為初始管理員密碼。
   - ❏ 如果畫面最右側顯示 [登出]，表明您已經以管理員身份登入。
   - ❏ 您將在大約 20 分鐘無活動後被自動登出。

# Epson Device Admin

Epson Device Admin 是一款多功能應用程式，可讓您管理網路上的裝置。

您可以使用組態範本套用統一設定至網路上的多個掃描器，使其適合安裝和管理多個掃描器。

您可從 Epson 支援網站下載 Epson Device Admin。關於如何使用此應用程式的詳細資訊，請參閱 Epson Device Admin 文件或說明。

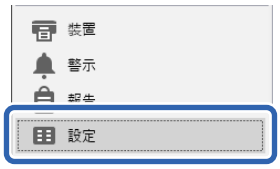
## 設定範本

### 建立設定範本

建立新的設定範本。

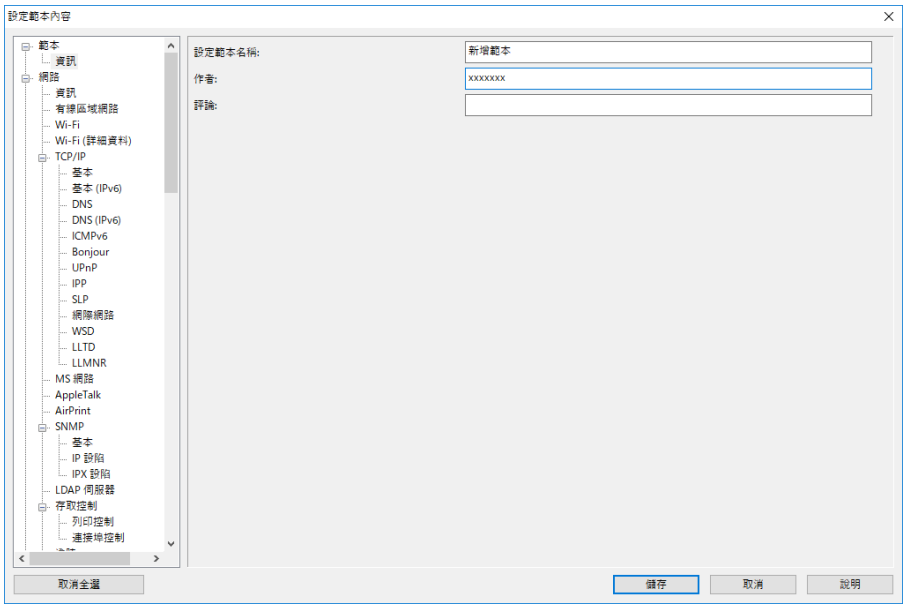
1. 啟動 Epson Device Admin。

2. 在側欄工作功能表中選取 [設定]。




3. 在功能區選單上選取 [新增]。

4. 設定各個項目。




| 項目 | 說明 |
|---|---|
| 設定範本名稱 | 設定範本的名稱。<br>最多輸入 1024 個 Unicode (UTF-8) 字元。 |
| 作者 | 範本建立者的資訊。<br>最多輸入 1024 個 Unicode (UTF-8) 字元。 |
| 評論 | 輸入任意資訊。<br>最多輸入 1024 個 Unicode (UTF-8) 字元。 |

5. 從左側選取您要設定的項目。

附註：
按下左側的選單項目，以切換至各個畫面。切換熒幕時設定的值會保留，但取消畫面時不會保留。完成所有設定後，點選 [儲存]。

## 套用設定範本

套用儲存的設定範本至掃描器。已套用在範本中選擇的項目。如果目標掃描器沒有相應的功能，則不會套用。

附註：
如果已為掃描器設定管理員密碼，請提前組態密碼。

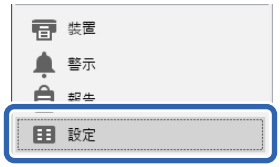
1.在裝置清單畫面的面板式功能表內，選取 [選項] > [密碼管理]。

2.選擇 [啟用自動密碼管理]，然後按下 [密碼管理]。

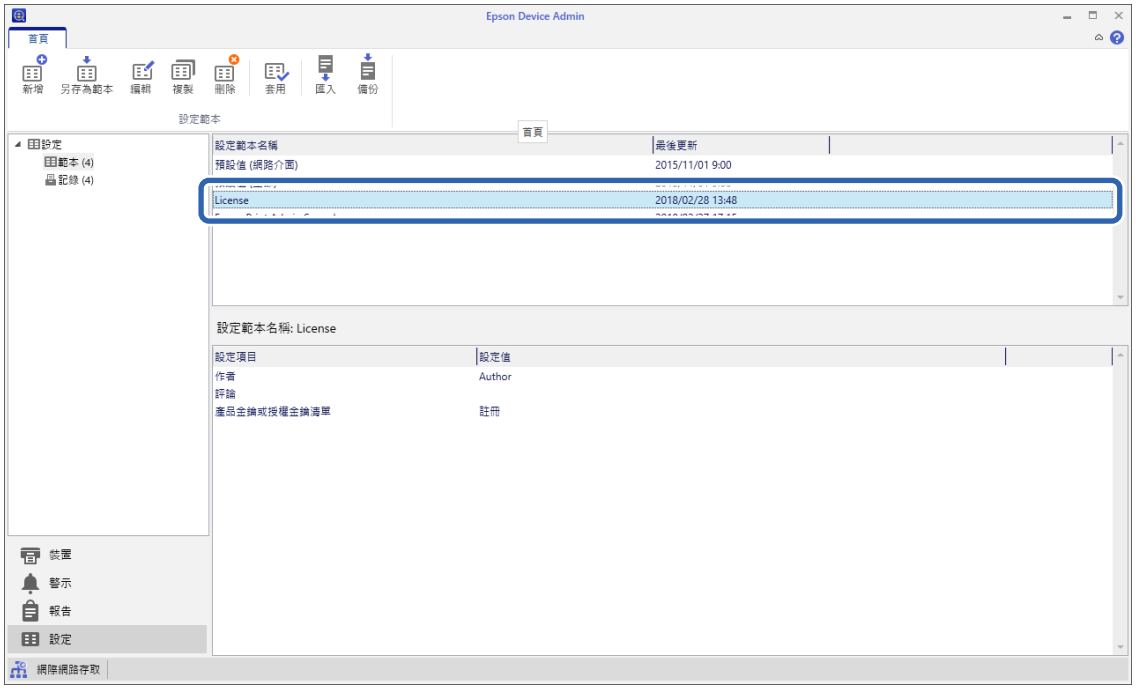
3.選取相應的掃描器，然後按下 [編輯]。

4.設定密碼，然後按下 [確定]。

1. 在側欄工作功能表中選取 [設定]。




2. 從 [設定範本名稱] 選取您要套用的設定範本。




3. 在功能區選單上按下 [套用]。

   裝置選擇畫面會隨即顯示。

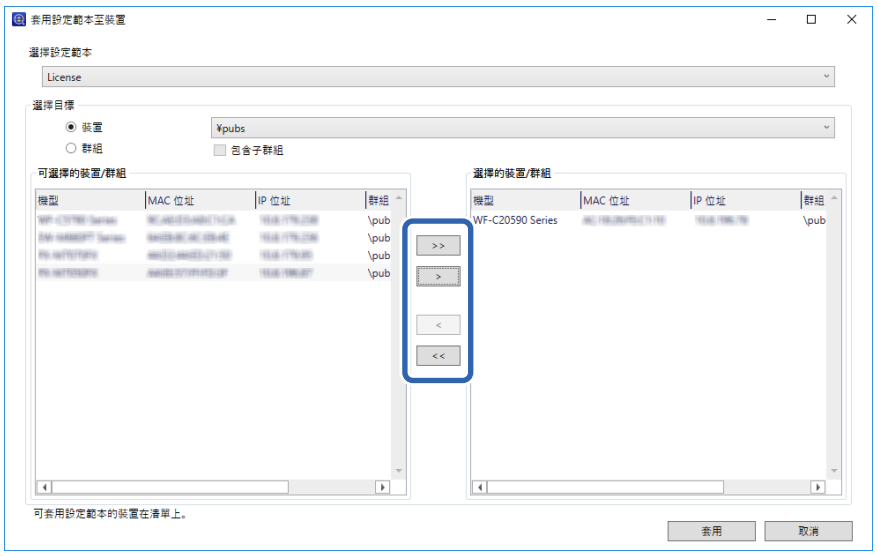
4. 選取您要套用的設定範本。

   附註：

   ❏ 當您從下拉式選單選取 [裝置] 及含有裝置的群組時，各裝置會隨即顯示。

   ❏ 當您選取 [群組] 時，群組會隨即顯示。選取 [包含子群組] 以自動選取所選群組中的子群組。

5. 移動您要套用範本的裝置或群組至 [選擇的裝置/群組]。




6. 按下 [套用]。

   要套用之設定範本的確認畫面會隨即顯示。

7. 按下 [確定] 以套用設定範本。

8. 顯示登錄完成的通知訊息時，按下 [確定]。

9. 按下 [詳細資訊] 並查看資訊。

   所套用之項目上顯示 時，表示套用已成功完成。

10. 按下 [關閉]。

# 掃描的所需設定

配置郵件伺服器. . . . . 41

設定共用網路資料夾. . . . . .43

使聯絡人可用. . . . . 59

使用 Document Capture Pro Server. . . . . .68

設定 AirPrint. . . . . 69

準備網路掃描時遇到的問題. . . . . 69

# 配置郵件伺服器

從 Web Config 中設定郵件伺服器。

若可透過設定郵件伺服器讓掃描器傳送電子郵件，即可進行以下操作。

❏ 使用電子郵件傳輸掃描結果

❏ 接收來自掃描器的電子郵件通知

進行設定前請檢查以下內容。

❏ 掃描器連接至可以存取郵件伺服器的網路。

❏ 若電腦使用與掃描器相同的郵件伺服器，以電子郵件傳送其設定資訊。

附註：

❏ 在網際網路上使用郵件伺服器時，請確認提供者或網站的設定資訊。

❏ 您也可從掃描器的控制面板設定郵件伺服器。存取方式如下。
[設定] > [網路設定] > [進階] > [電子郵件伺服器] > [伺服器設定]

1. 存取 Web Config 並選取 [網路] 索引標籤 > [電子郵件伺服器] > [基本]。
2. 在各項目輸入數值。
3. 選取 [確定]。
   您所選取的設定會顯示。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 郵件伺服器設定項目

| 項目 | 設定與說明 | |
|---|---|---|
| 驗證方法 | 指定掃描器存取郵件伺服器的驗證方式。 | |
| | 關閉 | 與郵件伺服器進行通訊時驗證功能會停用。 |
| | SMTP驗證 | 需要郵件伺服器支援 SMTP 驗證。 |
| | 以POP驗證取代SMTP | 選取此方式時，請配置 POP3 伺服器。 |
| 已驗證帳戶 | 若您選擇 [SMTP驗證] 或 [以POP驗證取代SMTP] 作為 [驗證方法]，則請輸入已驗證的帳戶名稱（0 至 255 個字元、ASCII 格式 (0x20—0x7E)）。 | |
| 已驗證密碼 | 若您選取 [SMTP驗證] 或 [以POP驗證取代SMTP] 作為 [驗證方法]，則請輸入已驗證的密碼（0 至 20 個字元、ASCII 格式 (0x20—0x7E)）。 | |
| 寄件者的電子郵件位址 | 輸入寄件者的電子郵件地址。輸入介於 0 和 255 個之間的 ASCII (0x20—0x7E) 字元，不包括：( ) < > [ ] ; ¥。句點「.」不可當作第一個字元。 | |
| SMTP伺服器位址 | 輸入 0 至 255 個字元，可以使用 A—Z a—z 0—9 .-。您可以使用 IPv4 或 FQDN 格式。 | |
| SMTP伺服器連接埠號碼 | 輸入介於 1 至 65535 的數字。 | |

| 項目 | 設定與說明 | |
|---|---|---|
| 安全連線 | 指定電子郵件伺服器的安全連線方法。 | |
| | 無 | 若您在 [驗證方法] 中選取了 [以POP驗證取代SMTP]，連線方法則會設定為 [無]。 |
| | SSL/TLS | 此功能在 [驗證方法] 設定為 [關閉] 或 [SMTP驗證] 時即可使用。 |
| | STARTTLS | 此功能在 [驗證方法] 設定為 [關閉] 或 [SMTP驗證] 時即可使用。 |
| 憑證驗證 | 若啟用此功能，憑證即可發揮效力。建議設定為 [開啓]。 | |
| POP3伺服器位址 | 若您選擇 [以POP驗證取代SMTP] 作為 [驗證方法]，則請輸入 POP3 伺服器地址 0 至 255 個字元之間，可使用 A—Z a—z 0—9 .-。您可以使用 IPv4 或 FQDN 格式。 | |
| POP3伺服器連接埠號碼 | 若您選取 [以POP驗證取代SMTP] 作為 [驗證方法]，則請輸入 1 至 65535 個字元之間的數字。 | |

# 檢查郵件伺服器連線

您可執行連線檢查來檢查與郵件伺服器的連線。

1. 存取 Web Config 並選取 [網路] 索引標籤 > [電子郵件伺服器] > [連線測試]。
2. 選取 [開始]。

   即開始電子郵件伺服器的連線測試。完成測試後，會顯示檢查報告。

   附註：
   您也可從掃描器的控制面板檢查與郵件伺服器的連線。存取方式如下。

   [設定] > [網路設定] > [進階] > [電子郵件伺服器] > [連線檢查]

## 郵件伺服器連線測試參考

| 訊息 | 原因 |
|---|---|
| 連線測試成功。 | 成功建立與伺服器的連線時會顯示此訊息。 |
| SMTP 伺服器通訊錯誤。請檢查下列內容。- 網路設定 | 以下情況會顯示訊息<br>❏ 掃描器未連接網路<br>❏ SMTP 伺服器停機<br>❏ 進行通訊時網路斷線<br>❏ 接收到不完整的資料 |
| POP3 伺服器通訊錯誤。請檢查下列內容。- 網路設定 | 以下情況會顯示訊息<br>❏ 掃描器未連接網路<br>❏ POP3 伺服器停機<br>❏ 進行通訊時網路斷線<br>❏ 接收到不完整的資料 |

| 訊息 | 原因 |
| --- | --- |
| 連線至 SMTP 伺服器時發生錯誤。請檢查下列內容。- SMTP 伺服器位址- DNS 伺服器 | 以下情況會顯示訊息<br>❏ 與 DNS 伺服器的連線失敗<br>❏ SMTP 伺服器的名稱解析失敗 |
| 連線至 POP3 伺服器時發生錯誤。請檢查下列內容。- POP3 伺服器位址- DNS 伺服器 | 以下情況會顯示訊息<br>❏ 與 DNS 伺服器的連線失敗<br>❏ POP3 伺服器的名稱解決方案失敗 |
| SMTP 伺服器驗證錯誤。請檢查下列內容。- 驗證方法- 已驗證的帳戶- 已驗證的密碼 | SMTP 伺服器驗證失敗時，會顯示此訊息。 |
| POP3 伺服器驗證錯誤。請檢查下列內容。- 驗證方法- 已驗證的帳戶- 已驗證的密碼 | POP3 伺服器驗證失敗時，會顯示此訊息。 |
| 不支援的通訊方法。請檢查下列內容。- SMTP 伺服器位址- SMTP 伺服器連接埠號碼 | 嘗試用不支援的通訊協定進行通訊時，會顯示此訊息。 |
| 連線至 SMTP 伺服器失敗。請將 安全連線 變更為 無。 | 伺服器與用戶端之間發生 SMTP 不相符的情況，或伺服器不支援 SMTP 安全連線 (SSL 連線) 時，會顯示此訊息。 |
| 連線至 SMTP 伺服器失敗。請將 安全連線 變更為 SSL/TLS。 | 伺服器與用戶端之間發生 SMTP 不相符的情況，或伺服器要求使用 SSL/TLS 進行 SMTP 安全連線時，會顯示此訊息。 |
| 連線至 SMTP 伺服器失敗。請將 安全連線 變更為 STARTTLS。 | 伺服器與用戶端之間發生 SMTP 不相符的情況，或伺服器要求使用 STARTTLS 進行 SMTP 安全連線時，會顯示此訊息。 |
| 不信任的連線。請檢查下列內容。- 日期與時間 | 掃描器的日期與時間設定不正確，或憑證過期時，會顯示此訊息。 |
| 不信任的連線。請檢查下列內容。- CA 憑證 | 若掃描器沒有對應伺服器的根憑證，或 CA 憑證 並未匯入，則會顯示此訊息。 |
| 不安全的連線。 | 若取得的憑證已經毀損，則會顯示此訊息。 |
| SMTP 伺服器驗證失敗。請將驗證方法變更為 SMTP-AUTH。 | 伺服器和用戶端之間的驗證方法不相符時，會顯示此訊息。伺服器支援 SMTP 驗證。 |
| SMTP 伺服器驗證失敗。請將驗證方法變更為 POP before SMTP。 | 伺服器和用戶端之間的驗證方法不相符時，會顯示此訊息。伺服器不支援 SMTP驗證。 |
| 寄件者的電子郵件位址不正確。請變更為您電子郵件服務的電子郵件位址。 | 指定的寄件者電子郵件地址不正確時，會顯示此訊息。 |
| 程序未完成前，您無法存取產品。 | 掃描器忙碌時會顯示此訊息。 |

# 設定共用網路資料夾

設定共用網路資料夾以儲存掃描影像。

儲存檔案至資料夾時，掃描器作為該資料夾在其上建立之電腦使用者登入。

# 建立共用資料夾

**相關資訊**

➡ 第44頁“在建立共用資料夾之前”
➡ 第44頁“檢查網路設定檔”
➡ 第44頁“共用資料夾的建立位置和安全範例”
➡ 第56頁“新增允許存取的群組或使用者”

## 在建立共用資料夾之前

在建立共用資料夾之前，請檢查以下內容。

❏ 掃描器連接至可存取將要建立共用資料夾之電腦的網路。

❏ 將要建立共用資料夾的電腦名稱中不包括多位元組字元。

**重要事項：**

當電腦名稱中包含多位元組字元時，將檔案儲存至共用資料夾的作業可能會失敗。

在這種情況下，請變更為名稱中不包含多位元組字元的電腦，或變更電腦名稱。

變更電腦名稱時，請務必事先與管理員確認，因為這可能會影響到某些設定，如電腦管理、資源存取等。

## 檢查網路設定檔

在要建立共用資料夾的電腦上，檢查是否可使用資料夾共用功能。

1. 以具有管理員權限的使用者帳戶登入將要建立共用資料夾的電腦。
2. 選取[控制台] > [網路和網際網路] > [網路和共用中心]。
3. 按下[變更進階共用設定]，然後針對顯示的網路設定檔中具有[（目前的設定檔）]的設定檔按下 。
4. 檢查[檔案及印表機共用]上是否選取 [開啟檔案及印表機共用]。
   若已選取，按下[取消]並關閉視窗。
   變更設定時，請按下[儲存變更]並關閉視窗。

## 共用資料夾的建立位置和安全範例

視乎共用資料夾的建立位置，其安全性和便利性會有所不同。

若要從掃描器或其他電腦上操作共用資料夾，您需具備下列讀取和變更資料夾的權限。

❏ [共用]索引標籤 > [進階共用] > [權限]
此標籤控制共用資料夾的網路存取權限。

❏ [安全]索引標籤的存取權限
此標籤控制共用資料夾的網路存取權限與本機存取權限。

針對建立在桌面上的共用資料夾，當您將其權限設為[所有人]時，作為建立共用資料夾的範例，所有可存取電腦的使用者均被允許存取該資料夾。

但桌面（資料夾）處於使用者資料夾的控制下，未獲授權的使用者將無法存取，因此使用者資料夾的安全設定將會傳遞給該資料夾。允許存取[安全]索引標籤的使用者（本案例中為登入的使用者和管理員）可以操作資料夾。

請參閱下文以建立適當的位置。

本範例說明建立「scan_folder」資料夾的情況。

**相關資訊**

➡ 第45頁“檔案伺服器的配置範例”
➡ 第51頁“個人電腦的配置範例”

## 檔案伺服器的配置範例

此說明是在共用電腦上的磁碟根目錄下建立共用資料夾的範例，如下列情況下的檔案伺服器。

存取可控制的使用者（如，擁有相同電腦網域並要建立共用資料夾的使用者）可以存取共用資料夾。

若允許任何使用者讀寫電腦上的共用資料夾（如檔案伺服器和共用電腦），請設定此配置。

❏ 建立共用資料夾的地方：磁碟根目錄

❏ 資料夾路徑：C:\scan_folder

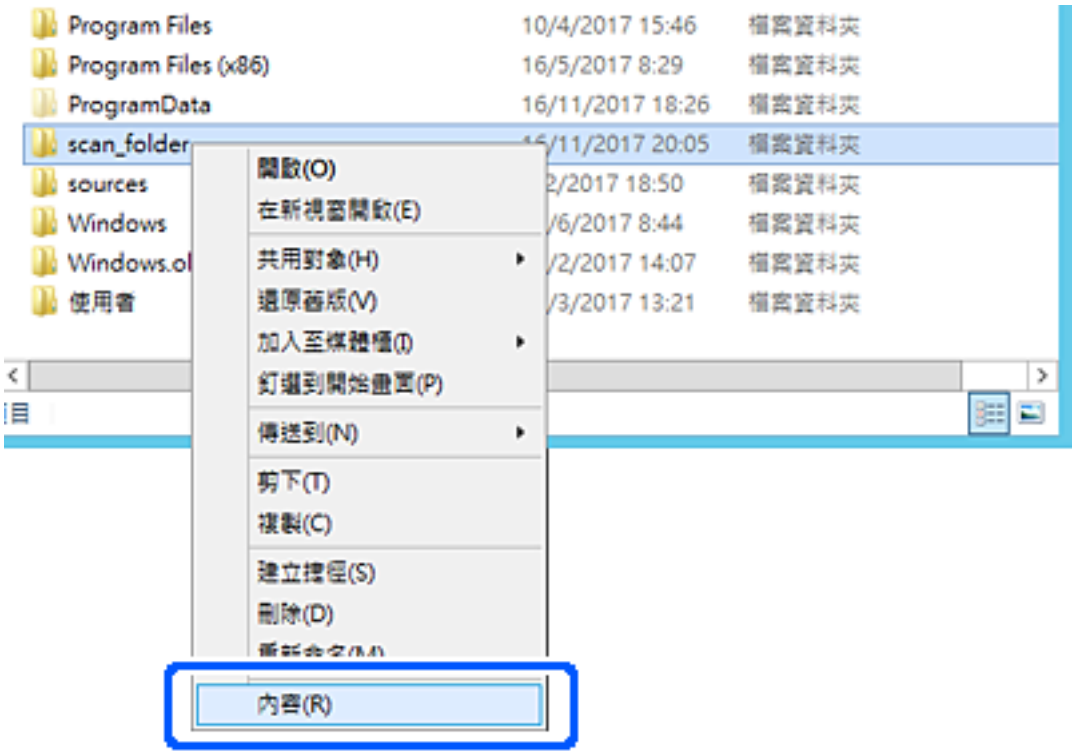
❏ 透過網路存取權限（共用權限）：所有人

❏ 檔案系統的存取權限（安全）：已驗證的使用者

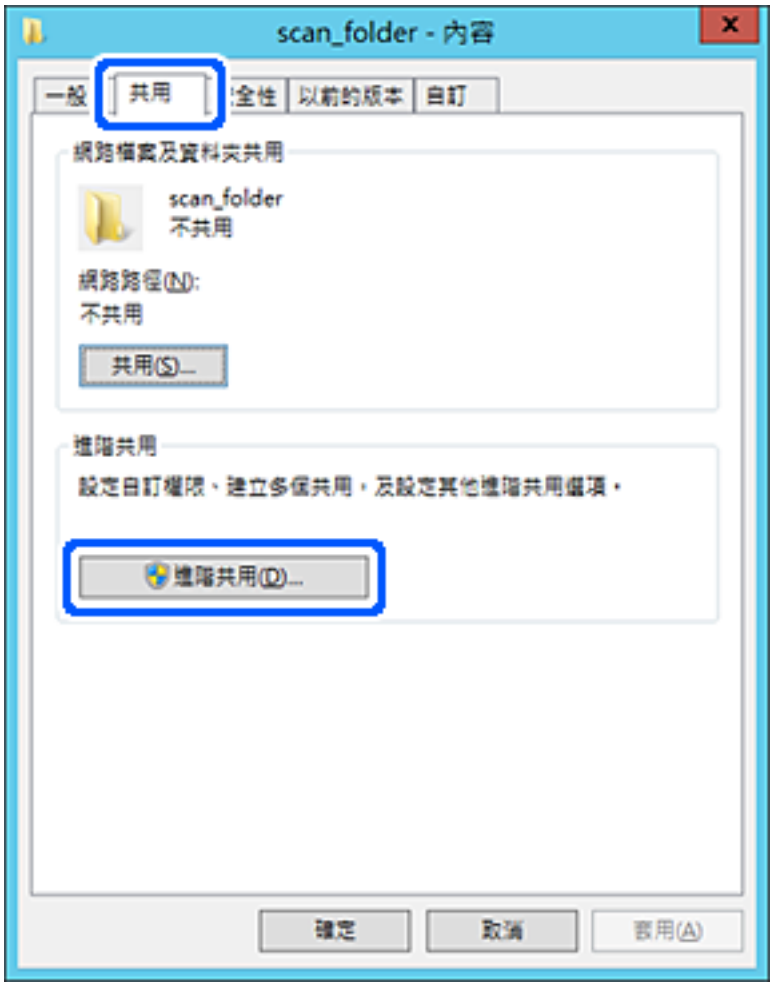
1. 以具有管理員權限的使用者帳戶登入將要建立共用資料夾的電腦。
2. 啟動瀏覽器。
3. 在磁碟根目錄上建立資料夾，然後將其命名為「scan_folder」。

   針對資料夾名稱，輸入 1 至 12 個字母數字字元。若超過資料夾名稱的字元限制，則可能無法在各種環境中正常存取。

4. 在資料夾上按下滑鼠右鍵，然後選取[內容]。

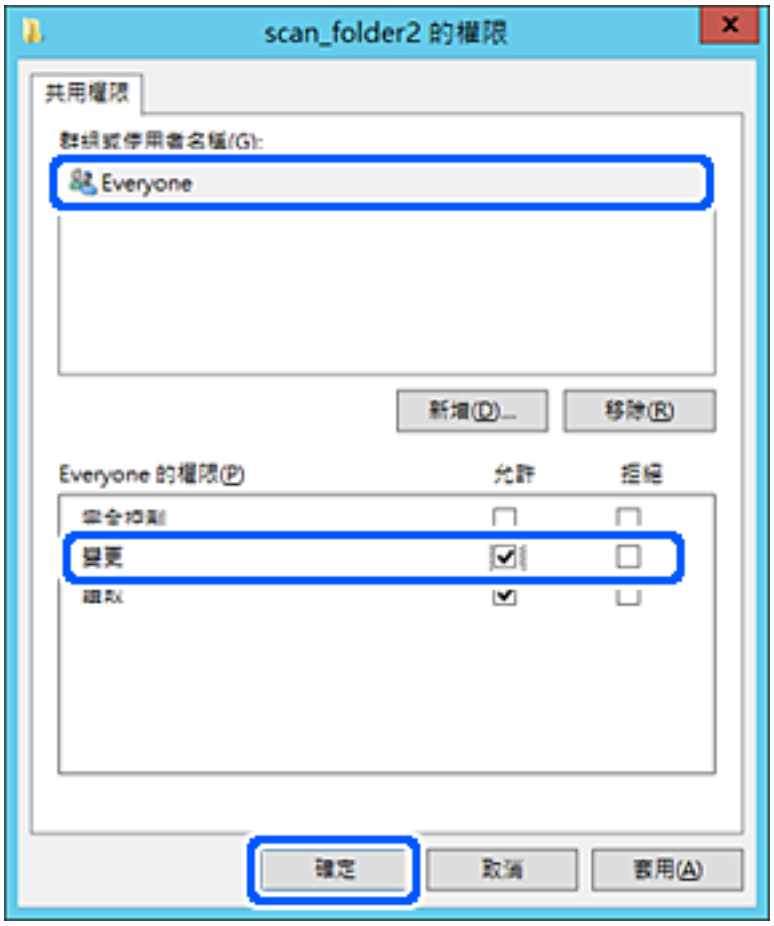


5. 點選 [共用] 索引標籤上的 [進階共用]。



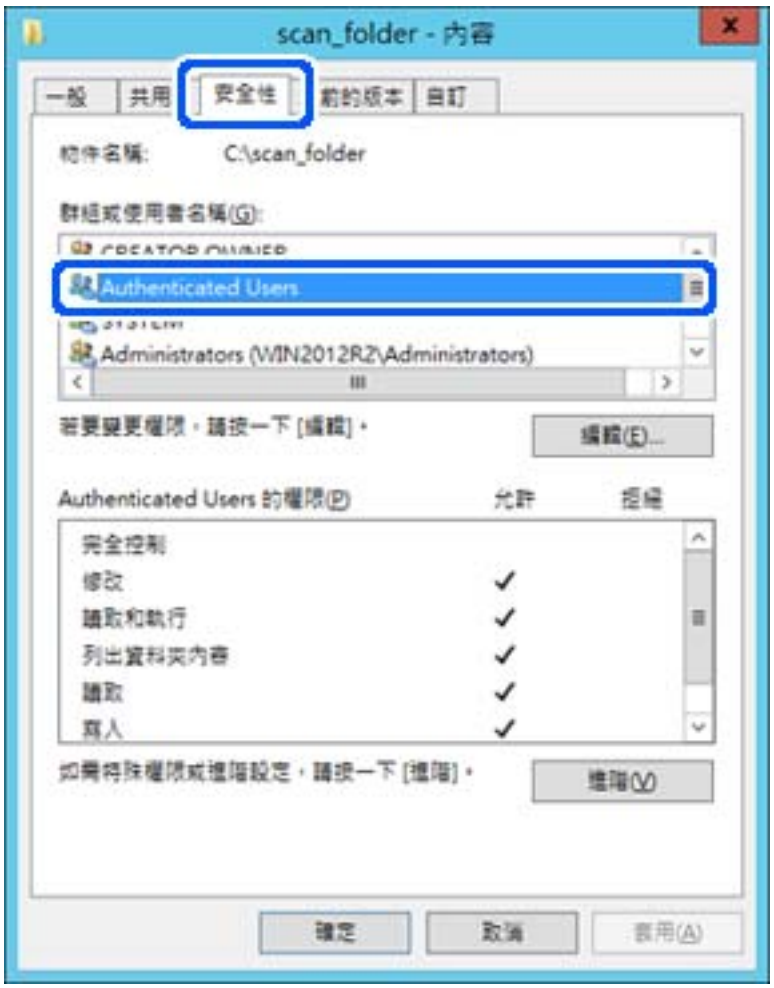
6. 選取[共用此資料夾]，然後按下[權限]。

7. 選取[群組或使用者名稱]的[所有人]群組，選取[變更]上的[允許]，然後按下 [OK]。



8. 按下 [OK]。

9. 選取[安全]索引標籤，然後在[群組或使用者名稱]上選取[已驗證的使用者]。

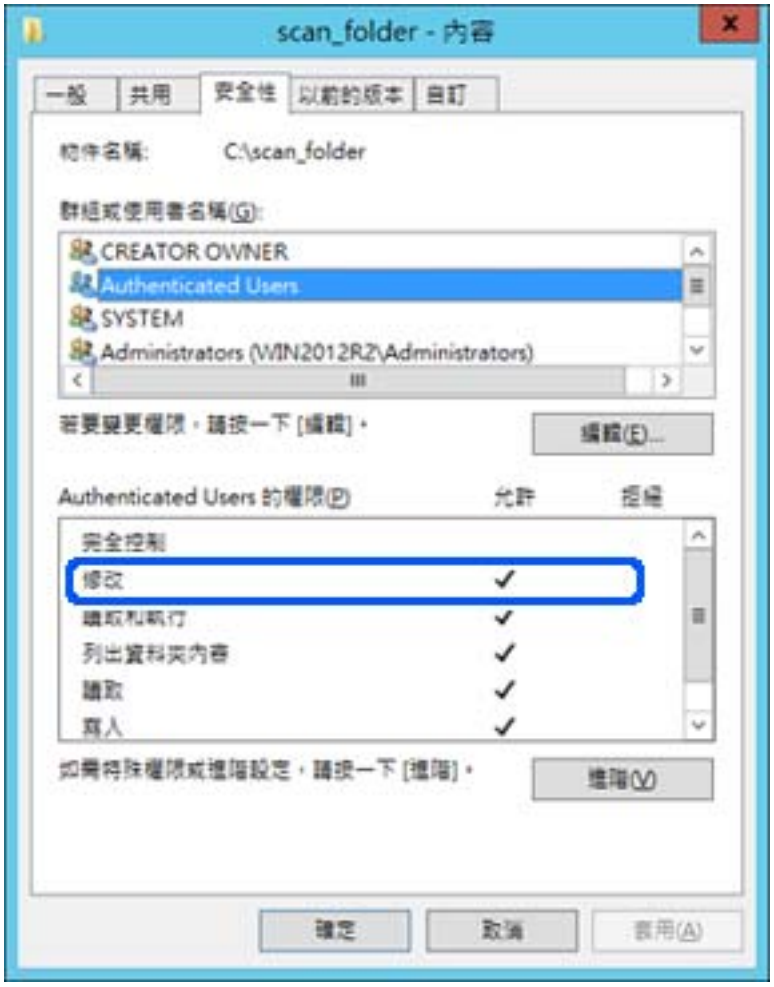



「已驗證的使用者」是包含所有可登入網域或電腦之使用者的特殊群組。僅在根資料夾下方建立資料夾時才會顯示此群組。

若未顯示，您可以按下[編輯]來新增權限。詳細資料，請參考「相關資訊」。

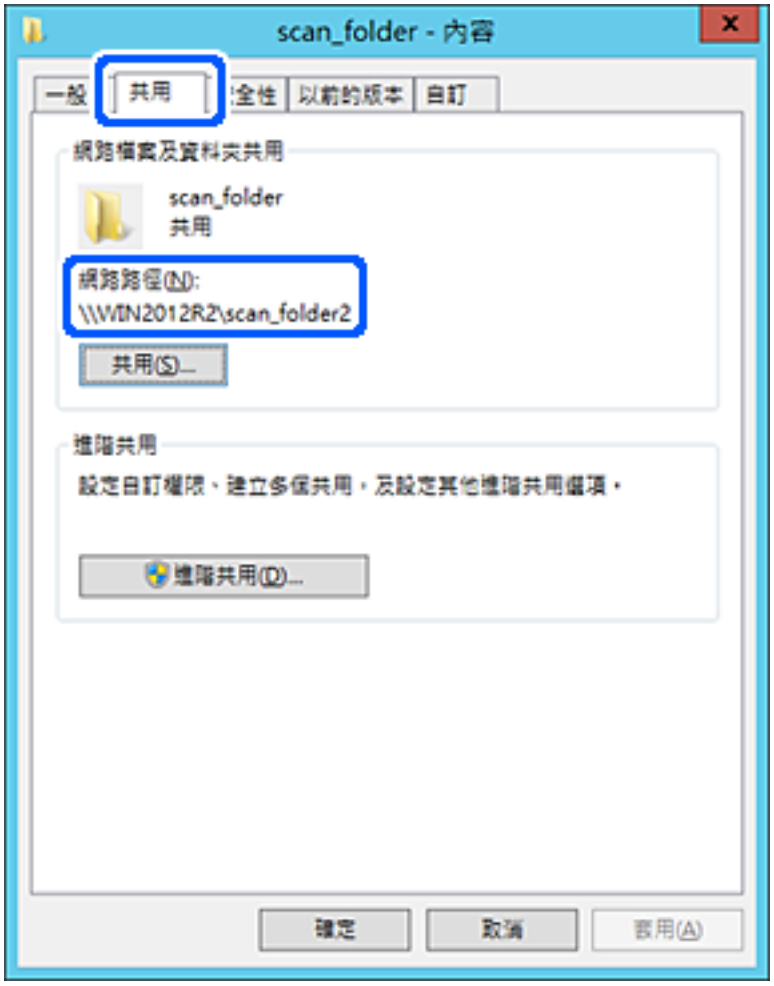
10. 檢查是否在[已驗證的使用者權限]中選取了[修改]上的[允許]。

    若未選取，請選取[已驗證的使用者]，按下[編輯]，在[已驗證的使用者權限]中選取[修改]上的[允許]，然後再按下 [OK]。



11. 選取[共用]索引標籤。

會顯示共用資料夾的網路路徑。在登錄至掃描器的聯絡人時會使用此資訊。請將此資訊寫下來。




12. 按下 [OK]或[關閉]關閉畫面。

檢查是否可透過同一個網域中的電腦寫入或讀取共用資料夾上的檔案。

**相關資訊**

➡ 第56頁“新增允許存取的群組或使用者”
➡ 第60頁“使用 Web Config 將目的地登錄至聯絡人”

### 個人電腦的配置範例

此說明是在目前已登入電腦之使用者的桌面上，建立共用資料夾的範例。

登入電腦並具有管理員權限的使用者，可以存取使用者資料夾下的桌面資料夾和文件資料夾。

若您不允許讀取和寫入其他使用者到個人電腦上的共用資料夾，請設定此配置。

❏ 用於建立共用資料夾的位置：桌面

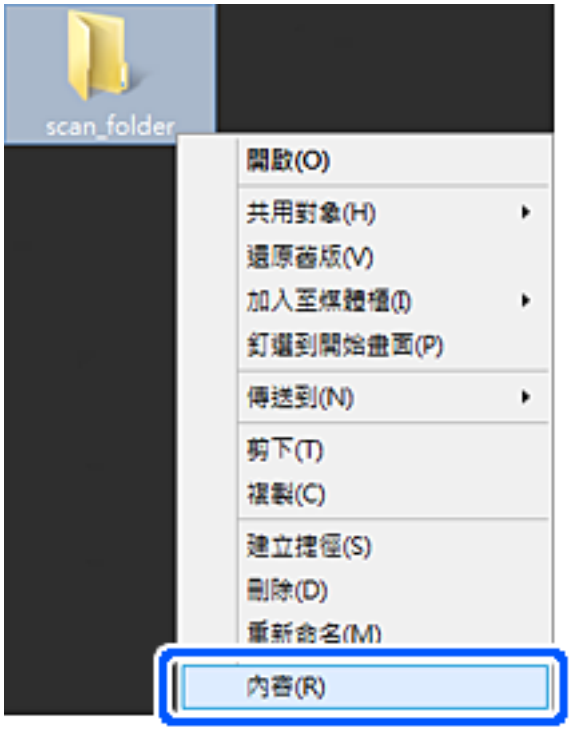
❏ 資料夾路徑：C:\Users\xxxx\Desktop\scan_folder

❏ 透過網路存取權限（共用權限）：所有人

❏ 檔案系統存取權限（安全性）：請勿新增，或新增使用者/群組名稱以允許存取

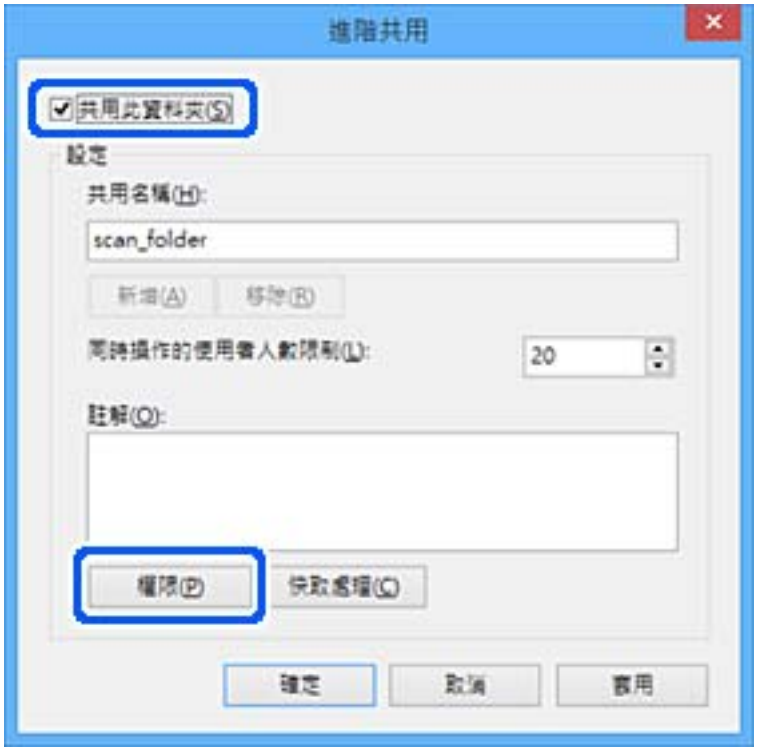
1. 以具有管理員權限的使用者帳戶登入將要建立共用資料夾的電腦。
2. 啟動瀏覽器。
3. 在桌面上建立資料夾，然後將其命名為「scan_folder」。

   針對資料夾名稱，輸入 1 至 12 個字母數字字元。若超過資料夾名稱的字元限制，則可能無法在各種環境中正常存取。
4. 在資料夾上按下滑鼠右鍵，然後選取[內容]。



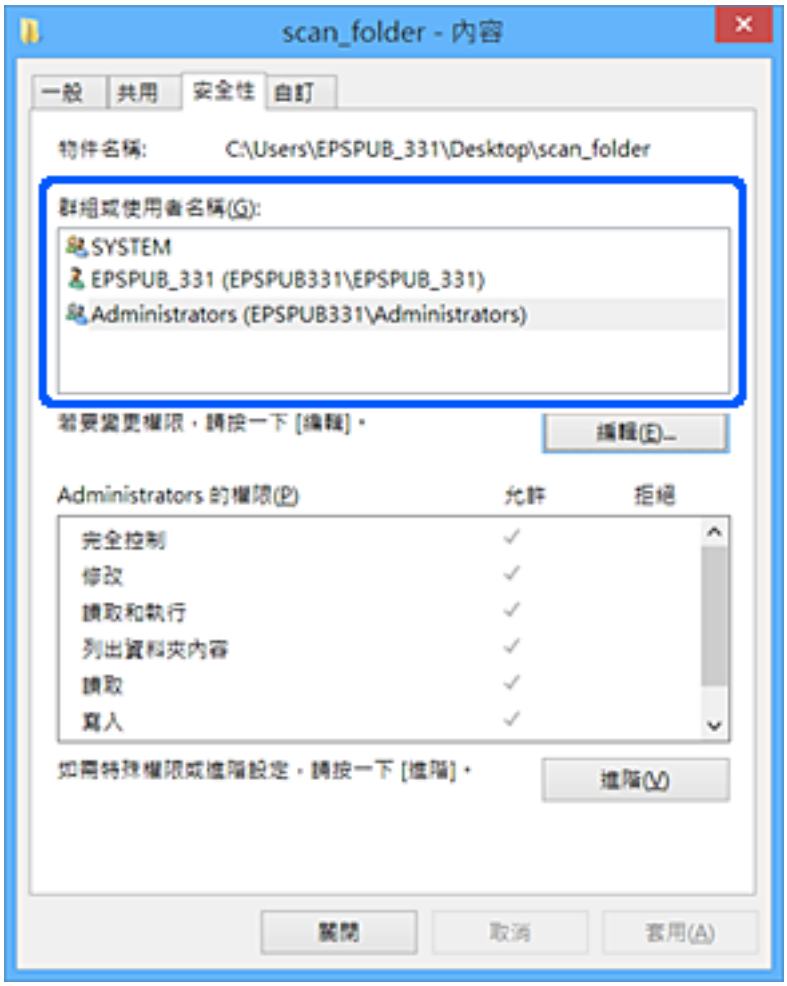
5. 點選 [共用] 索引標籤上的 [進階共用]。

6. 選取[共用此資料夾]，然後按下[權限]。




7. 選取[群組或使用者名稱]的[所有人]群組，選取[變更]上的[允許]，然後按下 [OK]。

8. 按下 [OK]。
9. 選取[安全]索引標籤。
10. 檢查[群組或使用者名稱]中的群組或使用者。
    此處顯示的群組或使用者可以存取共用資料夾。
    在這種情況下，登入此電腦的使用者和管理員可以存取共用資料夾。
    如有必要，請新增存取權限。您可以按下[編輯]來新增權限。詳細資料，請參考「相關資訊」。



11. 選取[共用]索引標籤。

    會顯示共用資料夾的網路路徑。在登錄至掃描器的聯絡人時會使用此資訊。請將此資訊寫下來。

12. 按下 [OK]或[關閉]關閉畫面。

    從使用者或群組具有存取權限的電腦上檢查是否可在共用資料夾上寫入或讀取檔案。

**相關資訊**

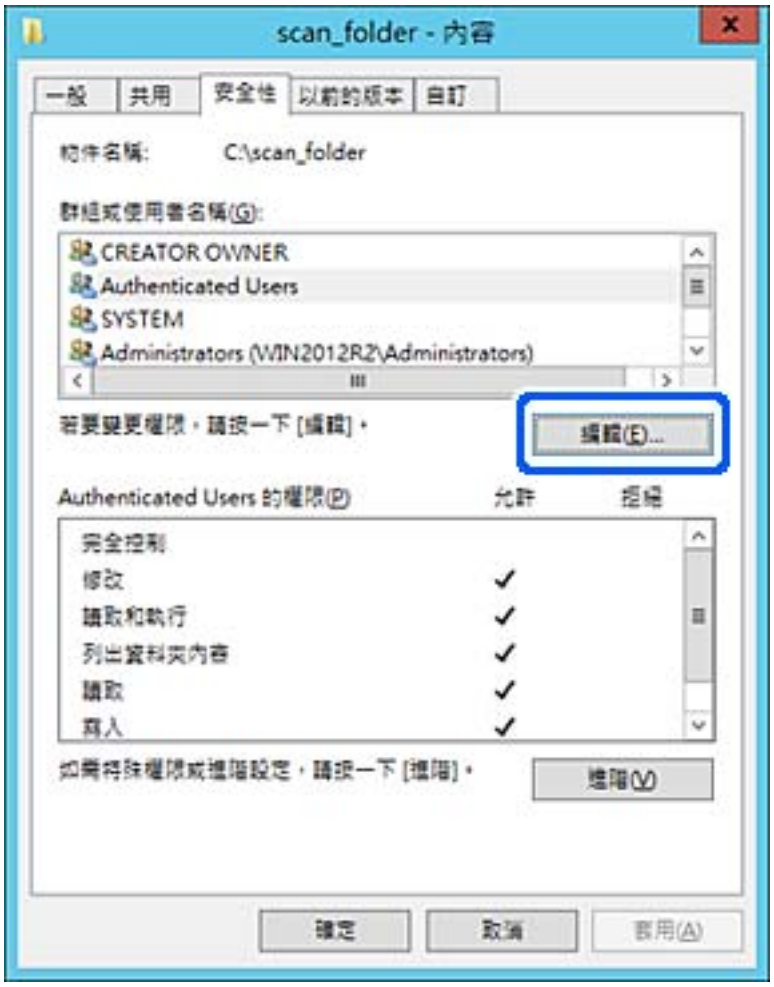
➡ 第56頁“新增允許存取的群組或使用者”
➡ 第60頁“使用 Web Config 將目的地登錄至聯絡人”

## 新增允許存取的群組或使用者

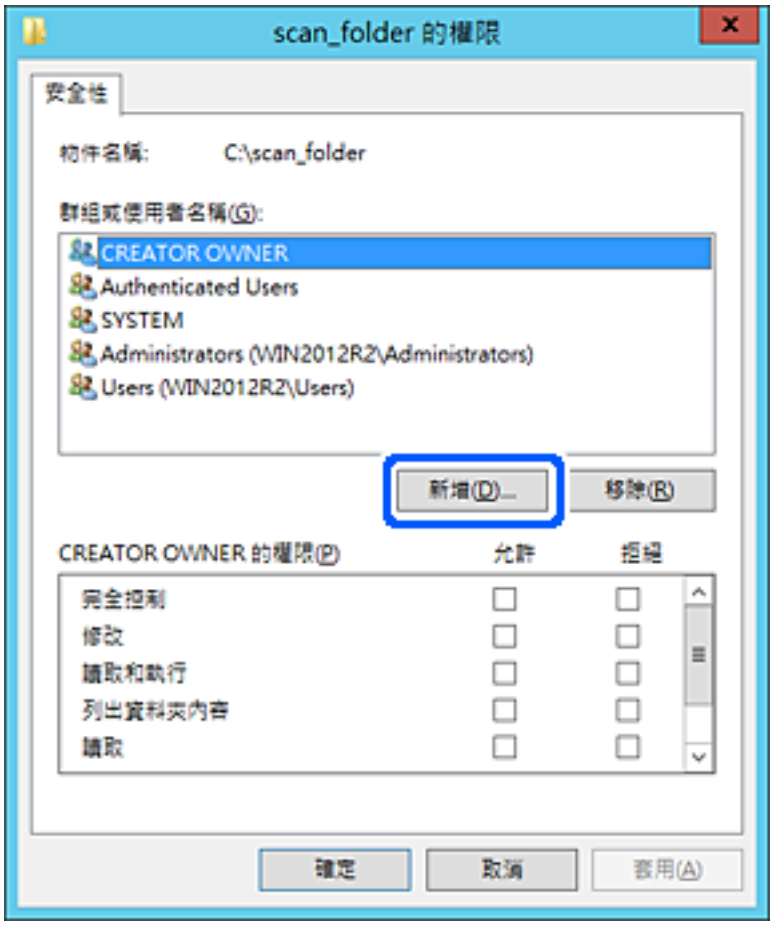
您可以新增允許存取的群組或使用者。

1. 在資料夾上按下滑鼠右鍵並選取[屬性]。
2. 選取[安全]索引標籤。

3. 按下[編輯]。


scan_folder - 內容
一般
共用
安全性
以前的版本
自訂
物件名稱:
C:\scan_folder
群組或使用者名稱(G):
CREATOR OWNER
Authenticated Users
SYSTEM
Administrators (WIN2012R2\Administrators)
若要變更權限，請按一下 [編輯]。
編輯(E)...
Authenticated Users 的權限(P)
允許
拒絕
完全控制
修改
讀取和執行
列出資料夾內容
讀取
寫入
如需特殊權限或進階設定，請按一下 [進階]。
進階(V)
確定
取消
套用(A)

4. 按下[群組或使用者名稱]下方的[新增]。



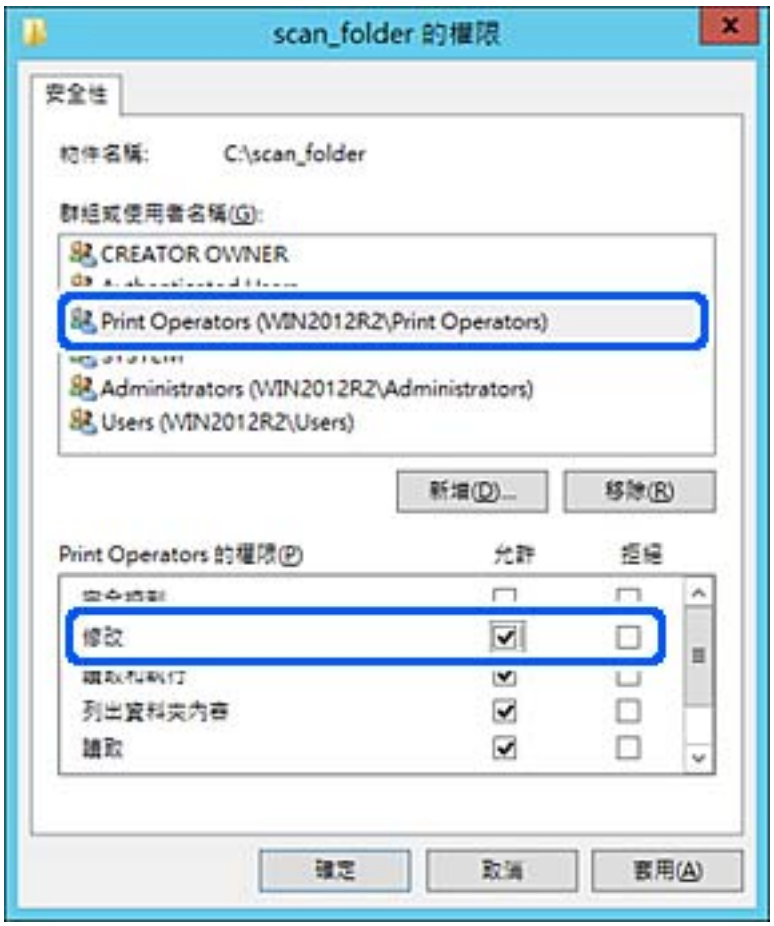

5. 輸入您要允許存取的群組或使用者名稱，然後按下[檢查名稱]。

   該名稱上會加上底線。

   附註：
   如果您不知道群組或使用者的完整名稱，請輸入部分名稱，然後按下[檢查名稱]。系統會列出與部分名稱相符的群組名稱或使用者名稱，然後即可從清單中選取完整名稱。

   若只有一個名稱符合，則[輸入要選取的對象名稱]中即會顯示含有底線的完整名稱。

6. 按下[確定]。
7. 在「權限」畫面中，選取已輸入[群組或使用者名稱]的使用者名稱，允許[修改]，然後按下[確定]。




8. 按下[確定]或[關閉]關閉畫面。
   從使用者或群組具有存取權限的電腦上檢查是否可在共用資料夾上寫入或讀取檔案。

# 使聯絡人可用

在掃描器聯絡人清單中登錄目的地，可讓您在掃描時輕鬆輸入目的地。

您可在聯絡人清單中登錄下列類型的目的地。您總共可登錄最多 300 個條目。

附註：
您還可使用 LDAP 伺服器（LDAP 搜尋）輸入目的地。

| | |
|---|---|
| 電子郵件 | 電子郵件目的地。<br>您需要提前進行電子郵件伺服器設定。 |
| 網路資料夾 | 掃描資料目的地。<br>您需要提前準備網路資料夾。 |

**相關資訊**

➡ 第65頁“LDAP 伺服器與使用者之間的合作”

## 聯絡人配置比較

有三種工具可以配置掃描器的聯絡人：Web Config、Epson Device Admin 及印表機的控制面板。這三種工具的差異如下表所列。

| 功能 | Web Config* | Epson Device Admin | 掃描器的控制面板 |
|---|---|---|---|
| 登錄目的地 | ✓ | ✓ | ✓ |
| 編輯目的地 | ✓ | ✓ | ✓ |
| 新增群組 | ✓ | ✓ | ✓ |
| 編輯群組 | ✓ | ✓ | ✓ |
| 刪除目的地或群組 | ✓ | ✓ | ✓ |
| 刪除所有目的地 | ✓ | ✓ | — |
| 匯入檔案 | ✓ | ✓ | — |
| 匯出至檔案 | ✓ | ✓ | — |

* 以管理員身份登入以進行設定。

## 使用 Web Config 將目的地登錄至聯絡人

附註：
您也可從掃描器的控制面板登錄聯絡人。

1. 存取 Web Config 並選取 [掃描] 索引標籤 > [聯絡人]。
2. 選取您想要註冊的號碼，然後按下 [編輯]。
3. 輸入 [名稱] 和 [索引字]。
4. 在 [類型] 選項選取目的地類型。

   附註：
   完成註冊後，您無法變更 [類型] 選項。若想變更類型，請刪除目的地並重新註冊。
5. 在各項目輸入數值，然後按下 [套用]。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 目的地設定項目

| 項目 | 設定與說明 |
|---|---|
| 一般設定 | |
| 名稱 | 以 Unicode (UTF-16) 格式輸入顯示在聯絡人中的名稱，長度不得超過 30 個字元。如果您未指定此項目，請將其保留空白。 |
| 索引字 | 輸入採用 30 個或以內 Unicode (UTF-16) 格式字元的名稱以在掃描器控制面板上搜尋聯絡人。如果您未指定此項目，請將其保留空白。 |
| 類型 | 選取要註冊的位址類型。 |
| 指定至常用 | 選取此項可將註冊的位址設定為常用位址。<br>若設定為常用位址，該位址會顯示在掃描的最上層畫面，您可指定目的地而不顯示聯絡人。 |
| 電子郵件 | |
| 電子郵件位址 | 輸入 1 至 255 個字元 (可以使用 A—Z a—z 0—9 ! # $ % & ' * + - ./ = ? ^ _ { \| } ~ @)。 |
| 網路資料夾(SMB) | |
| 儲存至 | \\「資料夾路徑」<br>以 Unicode (UTF-16) 格式輸入目標資料夾的所在位置，長度為 1 到 253 個字元，「\\」不算在內。<br>輸入資料夾內容畫面上顯示的網路路徑。請參閱下列內容以了解關於設定網路路徑的詳細資訊。<br>第51頁“個人電腦的配置範例” |
| 使用者名稱 | 以 Unicode (UTF-16) 格式輸入用來存取網路資料夾的使用者名稱，長度不得超過 30 個字元。但請避免使用控制字元 (0x00 至 0x1F、0x7F)。 |
| 密碼 | 輸入密碼 (0 至 20 個字元、Unicode 格式 (UTF-16)) 以存取網路資料夾。但請避免使用控制字元 (0x00 至 0x1F、0x7F)。 |
| FTP | |
| 安全連線 | 依據 FTP 伺服器支援的檔案傳送協議選取 FTP 或 FTPS。選取 [FTPS] 以允許掃描器在有安全措施情況下通訊。 |
| 儲存至 | 以 Unicode (UTF-16) 格式輸入 1 到 253 個字元的伺服器名稱，「ftp://」或「ftps://」不算在內。 |
| 使用者名稱 | 以 Unicode (UTF-16) 格式輸入用來存取 FTP 伺服器的使用者名稱，長度不得超過 30 個字元。但請避免使用控制字元 (0x00 至 0x1F、0x7F)。若伺服器允許匿名連線，則請輸入 Anonymous 和 FTP 等使用者名稱。如果您未指定此項目，請將其保留空白。 |
| 密碼 | 輸入密碼 (0 至 20 個字元、Unicode 格式 (UTF-16)) 以存取 FTP 伺服器。但請避免使用控制字元 (0x00 至 0x1F、0x7F)。如果您未指定此項目，請將其保留空白。 |
| 連線模式 | 從功能表選取連線模式。若掃描器與 FTP 伺服器之間有設定防火牆，請選取 [被動模式]。 |
| 連接埠編號 | 輸入 FTP 伺服器連接埠號碼 (1 至 65535 之間的數字)。 |

| 項目 | 設定與說明 |
|---|---|
| 憑證驗證 | FTP 伺服器在此啟用後進行驗證。只有當針對 [安全連線] 選取 [FTPS] 時，此項才可用。<br>若要設定，需要將 CA 憑證 匯入掃描器。 |
| SharePoint(WebDAV)* | |
| 安全連線 | 依據伺服器支援的檔案傳送協議選取 HTTP 或 HTTPS。選取 [HTTPS] 以允許掃描器在有安全措施情況下通訊。 |
| 儲存至 | 以 Unicode (UTF-16) 格式輸入 1 到 253 個字元的伺服器名稱，「http://」或「https://」不算在內。 |
| 使用者名稱 | 以 Unicode (UTF-16) 格式輸入用來存取伺服器的使用者名稱，長度不得超過 30 個字元。但請避免使用控制字元 (0x00 至 0x1F、0x7F)。如果您未指定此項目，請將其保留空白。 |
| 密碼 | 輸入密碼 (0 至 20 個字元、Unicode 格式 (UTF-16)) 以存取伺服器。但請避免使用控制字元 (0x00 至 0x1F、0x7F)。如果您未指定此項目，請將其保留空白。 |
| 憑證驗證 | 伺服器在此啟用後進行驗證。只有當針對 [安全連線] 選取 [HTTPS] 時，此項才可用。<br>若要設定，需要將 CA 憑證 匯入掃描器。 |
| Proxy伺服器 | 選取是否使用代理伺服器。 |

* SharePoint Online 在從掃描器控制面板掃描至網路資料夾時不受支援。

如果您要儲存掃描影像至 SharePoint Online，請在安裝 SharePoint Online Connector 後使用 Document Capture Pro。請參閱 Document Capture Pro 手冊以瞭解詳細資訊。

https://support.epson.net/dcp/

# 使用 Web Config 將目的地註冊為群組

若目的地類型設為 [電子郵件]，您可將目的地註冊為群組。

1. 存取 Web Config 並選取 [掃描] 索引標籤 > [聯絡人]。
2. 選取您想要註冊的號碼，然後按下 [編輯]。
3. 從 [類型] 選取群組。
4. 按下 [群組的聯絡人] 的 [選擇]。
   可用的目的地會隨即顯示。
5. 選取您要註冊至群組的目的地，然後按下 [選擇]。
6. 輸入 [名稱] 和 [索引字]。
7. 選取是否將註冊的群組指派給常用群組。
   **附註：**
   目的地可以註冊至多個群組。
8. 按下 [套用]。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

# 備份和匯入聯絡人

您可以使用 Web Config 或其他工具來備份和匯入聯絡人。

若使用 Web Config，您可以匯出包含聯絡人的掃描器設定來備份聯絡人。由於匯出為二進位檔案，所以匯出的檔案無法進行編輯。

將掃描器設定匯入掃描器時，系統將會覆寫聯絡人資訊。

若為 Epson Device Admin，您僅可從裝置的屬性畫面上匯出聯絡人。另外，若您不匯出有關安全的項目，您可以編輯匯出的聯絡人並將其匯入，這樣可儲存為 SYLK 檔案或 CSV 檔案。

## 使用 Web Config 匯入聯絡人

如果您有一台可備份連絡人且與此掃描器相容的掃描器，您可匯入備份檔案而輕鬆登錄連絡人。

附註：
若需有關如何備份掃描器連絡人的指南，請參閱掃描器附帶的手冊。

請依照下列步驟匯入連絡人至此掃描器。

1. 存取 Web Config，選取 [裝置管理] 索引標籤 > [匯出與匯入設定值] > [匯入]。
2. 選取您在 [檔案] 中建立的備份檔案、輸入密碼，然後點按 [下一步]。
3. 選取 [聯絡人] 核取方塊，然後點按 [下一步]。

## 使用 Web Config 將聯絡人備份

聯絡人資料可能因掃描器故障而遺失。每次更新資料時，建議您做好備份工作。Epson 對於任何資料遺失、備份或復原資料及/或設定概不負責，即使是在保固期內。

您可以使用 Web Config 將儲存在掃描器中的聯絡人資料備份至電腦。

1. 存取 Web Config，然後選取 [裝置管理] 索引標籤 > [匯出與匯入設定值] > [匯出]。
2. 選取 [掃描] 類別下的 [聯絡人] 核取方塊。
3. 輸入密碼以加密匯出檔案。

   您需要密碼才可匯出檔案。若您不想要加密檔案，則請留白。
4. 按下 [匯出]。

# 使用工具匯出和批量登錄聯絡人

如果您使用 Epson Device Admin，則只需備份聯絡人並編輯匯出檔案，然後立即進行登錄。

如果您只想備份聯絡人，或在更換掃描器時，想要從舊聯絡人轉移到新聯絡人，則此功能十分實用。

## 匯出聯絡人

將聯絡人資訊儲存至檔案。

您可以使用試算表應用程式或文字編輯器來編輯以 SYLK 格式或 csv 格式儲存的檔案。您可以在刪除或新增資訊後立即登錄。

您可以使用密碼以二進位格式儲存安全項目資訊，包括密碼和個人資訊等。您無法編輯檔案。這可以用作安全項目等資訊的備份檔案。

1. 啟動 Epson Device Admin。
2. 在側欄工作功能表中選取 [裝置]。
3. 從裝置清單中選取要配置的裝置。
4. 按下功能區功能表 [首頁] 索引標籤上的 [裝置設定]。
   若已設定管理員密碼，請輸入密碼並按下 [確定]。
5. 按下 [常用] > [聯絡人]。
6. 從 [匯出] > [匯出項目] 中選取匯出格式。
   - ❏ 所有項目
     匯出加密的二進位檔案。若要包括密碼和個人資訊等安全項目，請選取此功能。您無法編輯檔案。如果您選取，您必須設定密碼。按下 [設定] 並設定 8 至 63 個 ASCII 字元的密碼。匯入二進位檔案時，您需要輸入密碼。
   - ❏ 安全資訊以外的項目
     匯出 SYLK 格式或 csv 格式檔案。若要編輯匯出檔案的資訊，請選取此功能。
7. 按下 [匯出]。
8. 指定儲存檔案的位置，選取檔案類型，然後按下 [儲存]。
   完成訊息會隨即顯示。
9. 按下 [確定]。
   檢查檔案是否已儲存在指定位置。

## 匯入聯絡人

從檔案匯入聯絡人資訊。

您可以匯入以 SYLK 格式或 csv 格式儲存的檔案，或包含安全項目的備份二進位檔案。

1. 啟動 Epson Device Admin。
2. 在側欄工作功能表中選取 [裝置]。
3. 從裝置清單中選取要配置的裝置。
4. 按下功能區功能表 [首頁] 索引標籤上的 [裝置設定]。
   若已設定管理員密碼，請輸入密碼並按下 [確定]。

5. 按下 [常用] > [聯絡人]。
6. 在 [匯入] 上按下 [瀏覽]。
7. 選取您想要匯入的檔案，然後按下 [開啟]。
   當您選取二進位檔案時，請在 [密碼] 中輸入您在匯出檔案時設定的密碼。
8. 按下 [匯入]。
   隨即顯示確認畫面。
9. 按下 [確定]。
   顯示驗證結果。
   - ❏ 編輯載入的資訊
     當您想單獨編輯資訊時按下。
   - ❏ 載入更多檔案
     當您想匯入多個檔案時按下。
10. 按下 [匯入]，然後在匯入完成畫面上按下 [確定]。
    返回裝置的屬性畫面。
11. 按下 [傳輸]。
12. 在確認訊息上按下 [確定]。
    設定即會傳送到掃描器。
13. 在傳送完成畫面上，按下 [確定]。
    掃描器的資訊已更新。
    從 Web Config 或掃描器控制面板開啟聯絡人，然後檢查聯絡人是否已更新。

# LDAP 伺服器與使用者之間的合作

與 LDAP 伺服器搭配使用時，您可以將已登錄至 LDAP 伺服器的地址資訊作為電子郵件目的地。

## 設定 LDAP 伺服器

若要使用 LDAP 伺服器資訊，請在掃描器上登錄。

1. 存取 Web Config 並選取 [網路] 索引標籤 > [LDAP 伺服器] > [基本]。
2. 在各項目輸入數值。
3. 選取 [確定]。
   您所選取的設定會顯示。

## LDAP 伺服器設定項目

| 項目 | 設定與說明 |
|---|---|
| 使用 LDAP 伺服器 | 選取 [使用] 或 [不使用]。 |
| LDAP 伺服器位址 | 輸入 LDAP 伺服器的位址。輸入 1 至 255 個字元的 IPv4、IPv6 或 FQDN 格式。對於 FQDN 格式，您可使用 ASCII (0x20—0x7E) 英數字元及「-」（位址的開頭及結束除外）。 |
| LDAP 伺服器連接埠號碼 | 輸入 LDAP 伺服器連接埠號碼（1 至 65535 之間的數字）。 |
| 安全連線 | 指定掃描器存取 LDAP 伺服器的驗證方式。 |
| 憑證驗證 | 啟用此項後，系統將驗證 LDAP 伺服器的憑證。建議設定為 [開啓]。<br>若要設定，需要將 [CA 憑證] 匯入掃描器。 |
| 搜尋逾時 (秒) | 設定逾時前搜尋時間長度（5 至 300 之間的數字）。 |
| 驗證方法 | 選取下列其中一種方式。<br>如果您選取 [Kerberos 驗證]，請選取 [Kerberos 設定] 來針對 Kerberos 進行設定。<br>若要執行 Kerberos 驗證，需具備以下環境。<br>❏ 掃描器和 DNS 伺服器可以進行通訊。<br>❏ 掃描器、KDC 伺服器和驗證所需的伺服器（LDAP 伺服器、SMTP 伺服器、檔案伺服器）的時間均同步。<br>❏ 將服務伺服器指派為 IP 位址時，服務伺服器的 FQDN 即會登錄在 DNS 伺服器反向對應區域中。 |
| 要使用的 Kerberos 領域 | 如果您針對 [驗證方法] 選取 [Kerberos 驗證]，請選取要使用的 Kerberos 範圍。 |
| 管理員 DN / 使用者名稱 | 以 Unicode (UTF-8) 格式輸入 LDAP 伺服器的使用者名稱，長度不得超過 128 個字元。您無法使用控制字元，如 0x00—0x1F 和 0x7F。在選取 [匿名驗證] 作為 [驗證方法] 時，不會使用此設定。如果您未指定此項目，請將其保留空白。 |
| 密碼 | 以 Unicode (UTF-8) 格式輸入 LDAP 伺服器驗證的密碼，長度不得超過 128 個字元。您無法使用控制字元，如 0x00—0x1F 和 0x7F。在選取 [匿名驗證] 作為 [驗證方法] 時，不會使用此設定。如果您未指定此項目，請將其保留空白。 |

## Kerberos 設定

如果您針對 [LDAP 伺服器] > [基本] 的 [驗證方法] 選取 [Kerberos 驗證]，請從 [網路] 索引標籤 > [Kerberos 設定] 中進行下列 Kerberos 設定。針對 Kerberos 設定，您最多可以登錄 10 項設定。

| 項目 | 設定與說明 |
|---|---|
| 領域 (網域) | 輸入不超過 255 個 ASCII (0x20—0x7E) 字元的 Kerberos 驗證範圍。如果您未登錄此項目，請將其保留空白。 |
| KDC 位址 | 輸入 Kerberos 驗證伺服器的位址。輸入不超過 255 個 IPv4、IPv6 或 FQDN 格式的字元。如果您未登錄此項目，請將其保留空白。 |
| 連接埠號碼 (Kerberos) | 輸入 Kerberos 伺服器連接埠號碼（1 至 65535 之間的數字）。 |

## 進行 LDAP 伺服器搜尋設定

在設定搜尋設定時，您可以使用已登錄至 LDAP 伺服器的電子郵件地址。

1. 存取 Web Config 並選取 [網路] 索引標籤 > [LDAP 伺服器] > [搜尋設定]。
2. 在各項目輸入數值。
3. 按下 [確定] 顯示設定結果。
   您所選取的設定會顯示。

### LDAP 伺服器搜尋設定項目

| 項目 | 設定與說明 |
|---|---|
| 搜尋基礎 (辨別名稱) | 若要搜尋任意網域，請指定 LDAP 伺服器的網域名稱。輸入 0 至 128 個 Unicode (UTF-8) 字元。若不搜尋任意屬性，請保留空白。<br>本機伺服器目錄的範例：dc=server、dc=local |
| 搜尋項目數量 | 指定搜尋項目的數量，範圍介於 5 至 500。指定的搜尋項目數量會暫時儲存並顯示。即使搜尋項目的數量超過指定數量且出現錯誤訊息，仍可完成搜尋。 |
| 使用者名稱屬性 | 指定搜尋使用者名稱時要顯示的屬性名稱。輸入 1 至 255 個 Unicode (UTF-8) 字元。第一個字元必須是 a—z 或 A—Z。<br>範例：cn、uid |
| 使用者名稱顯示屬性 | 指定要顯示為使用者名稱的屬性名稱。輸入 0 至 255 個 Unicode (UTF-8) 字元。第一個字元必須是 a—z 或 A—Z。<br>範例：cn、sn |
| 電子郵件屬性 | 指定搜尋電子郵件地址時要顯示的屬性名稱。使用 A—Z、a—z、0—9 及 - 輸入 1 至 255 個字元。第一個字元必須是 a—z 或 A—Z。<br>範例：mail |
| 自訂屬性 1 - 自訂屬性 4 | 您可指定要搜尋的其他任意屬性。輸入 0 至 255 個 Unicode (UTF-8) 字元。第一個字元必須是 a—z 或 A—Z。若不想搜尋任意屬性，請保留空白。<br>範例：o、ou |

## 檢查 LDAP 伺服器連線

使用 [LDAP 伺服器] > [搜尋設定] 上所設定的參數對 LDAP 伺服器執行連線測試。

1. 存取 Web Config 並選取 [網路] 索引標籤 > [LDAP 伺服器] > [連線測試]。
2. 選取 [開始]。
   連線測試會隨即啟動。完成測試後，會顯示檢查報告。

### LDAP 伺服器連線測試參考

| 訊息 | 說明 |
|---|---|
| 連線測試成功。 | 成功建立與伺服器的連線時會顯示此訊息。 |
| 連線測試失敗。<br>檢查設定。 | 下列原因會顯示此訊息：<br>❏ LDAP 伺服器位址或連接埠號碼不正確。<br>❏ 發生逾時。<br>❏ 已選取 [不使用] 作為 [使用 LDAP 伺服器]。<br>❏ 如果已選取 [Kerberos 驗證] 作為 [驗證方法]，如 [領域 (網域)], [KDC 位址] 與 [連接埠號碼 (Kerberos)] 等設定不正確。 |
| 連線測試失敗。<br>在您的產品或伺服器上檢查日期與時間。 | 由於掃描器與 LDAP 伺服器的時間設定不一致而導致連線失敗時，會顯示此訊息。 |
| 驗證失敗。<br>檢查設定。 | 下列原因會顯示此訊息：<br>❏ [使用者名稱] 及/或 [密碼] 不正確。<br>❏ 如果已選取 [Kerberos 驗證] 作為 [驗證方法]，可能未配置時間/日期。 |
| 程序未完成前，您無法存取產品。 | 掃描器忙碌時會顯示此訊息。 |

# 使用 Document Capture Pro Server

透過使用 Document Capture Pro Server，您可以管理從掃描器控制面板執行之掃描結果的排序方法、儲存格式與轉寄目的地。您可以從掃描器的控制面板呼叫並執行之前在伺服器上登錄的工作。

將它安裝在伺服器電腦上。

若需有關 Document Capture Pro Server, 的更多資訊，請聯絡當地 Epson 辦事處。

## 設定伺服器模式

若要使用 Document Capture Pro Server，請依照下列方式設定。

1. 存取 Web Config 並選取 [掃描] 索引標籤 > [Document Capture Pro]。
2. 選取 [伺服器模式] 以 [模式]。
3. 針對 [伺服器位址] 輸入已安裝 Document Capture Pro Server 之伺服器的位址。

   輸入 2 至 255 個字元的 IPv4、IPv6、主機名稱或 FQDN 格式。對於 FQDN 格式，您可使用 ASCII (0x20—0x7E) 英數字元及「-」（位址的開頭及結束除外）。
4. 按下 [確定]。

   網路會重新連線，然後會啟用設定。

# 設定 AirPrint

存取 Web Config，選取 [網路] 索引標籤，然後選取 [AirPrint設定]。

| 項目 | 說明 |
|---|---|
| Bonjour服務名稱 | 使用 ASCII 文字 (0x20—0x7E) 及最多 41 個字元輸入 Bonjour 服務名稱。 |
| Bonjour位置 | 使用 Unicode (UTF-8) 文字及最多 127 個字節輸入掃描器位置描述。 |
| Wide-Area Bonjour | 設定是否使用寬面 Bonjour。若使用，您必須在 DNS 伺服器上登錄掃描器，才能在區段上搜尋掃描器。 |
| 啟用AirPrint | Bonjour 和 AirPrint（掃描服務）被啟用。 |

# 準備網路掃描時遇到的問題

## 解決問題的提示

❏ 檢查錯誤訊息

發生故障時，首先檢查掃描器控制面板或驅動程式畫面上是否有任何訊息。若您已設定在發生事件時寄送通知電子郵件，即可及時瞭解相關狀態。

❏ 檢查通訊狀態

使用 ping 和 ipconfig 等命令，檢查伺服器電腦或用戶端電腦的通訊狀態。

❏ 連線測試

若要檢查掃描器和郵件伺服器之間的連線，請使用掃描器的連線測試功能。此外，請檢查從用戶端電腦到伺服器的連線以檢查通訊狀態。

❏ 初始化設定

若設定和通訊狀態沒有問題，則也許可停用或初始化掃描器的網路設定，然後重新設定來解決問題。

### 無法存取 Web Config

#### IP 位址未指派給掃描器。

**解決方法**

有效的 IP 位址未指派給掃描器。使用掃描器的控制面板配置 IP 位址。您可以從掃描器的控制面板確認目前設定資訊。

#### 網路瀏覽器不支援 SSL/TLS 的加密強度。

**解決方法**

SSL/TLS 擁有 加密長度。您可使用職員批量加密的網路瀏覽器開啟 Web Config，如下所示。檢查您是否在使用受支援的瀏覽器。

❏ 80 bit：AES256/AES128/3DES

❏ 112 bit：AES256/AES128/3DES

❏ 128 bit：AES256/AES128

❏ 192 bit：AES256

❏ 256 bit：AES256

## CA 簽署憑證 已過期。

### 解決方法

如果證書的過期日期存在問題，當使用 SSL/TLS 通訊 (https) 連接至 Web Config 時顯示「正式已過期」。如果該訊息在其過期日期之前顯示，請確定掃描器的日期已正確組態。

## 憑證的通用名稱和掃描器不一致。

### 解決方法

若憑證的通用名稱和掃描器不一致，則在使用 SSL/TLS 通訊 (https) 存取 Web Config 時，系統將會顯示「安全性憑證的名稱不一致...」訊息。此狀況是因為下面的 IP 位址不一致所致。

❏ 將掃描器的 IP 位址輸入用於建立 自我簽署憑證 或 CSR 的通用名稱

❏ 執行 Web Config 時將 IP 位址輸入網頁瀏覽器

對於 自我簽署憑證，更新證書。

若為 CA 簽署憑證，則請再次取得掃描器的憑證。

## 本機位址的代理伺服器設定未設定至網路瀏覽器。

### 解決方法

當掃描器設定為使用代理伺服器時，組態網路瀏覽器不透過代理伺服器連接至本機位址。

❏ Windows：

選取 [控制台] > [網路和網際網路] > [網際網路選項] > [連線] > [LAN 設定] > [代理伺服器]，然後組態為不對 LAN（本機位址）使用代理伺服器。

❏ Mac OS：

選取 [系統偏好] > [網路] > [進階] > [代理]，然後為 [這些主機和域名的繞過代理設定]登錄本機位址。

範例：

192.168.1.*：本機位址 192.168.1.XXX、子網路遮罩 255.255.255.0

192.168.*.*：本機位址 192.168.XXX.XXX、子網路遮罩 255.255.0.0

## DHCP 在電腦設定中被禁用。

### 解決方法

如果用於自動獲取 IP 位址的 DHCP 在電腦上被禁用，您無法存取 Web Config。啟用 DHCP。

Windows 10 範例：

開啟控制台，然後按下 [網路和網際網路] > [網路和共用中心] > [變更介面卡設定]。開啟您所用連線的屬性畫面，然後開啟 [網際網路協議版本 4 (TCP/IPv4)] 或 [網際網路協議版本 6 (TCP/IPv6)] 的屬性畫面。在顯示的畫面上檢查是否已啟用[自動獲取 IP 位址]。

# 訂製控制面板顯示

登錄 預設. . . . . 72

編輯控制面板主畫面. . . . . .74

# 登錄 預設

您可以將頻繁使用的掃描設定登錄為 [預設]。最多可登錄 48 個預先設定。

附註：

- ❏ 您可在啟動掃描畫面上選取 ☆ 以登錄當前設定。
- ❏ 您也可在 Web Config 內登錄 [預設]。
  選取 [掃描] 索引標籤 > [預設]。
- ❏ 如果在登錄時選取 [掃描至電腦]，您可以將建立的工作在 Document Capture Pro 內登錄為 [預設]。這僅在透過網路連接的電腦上可用。預先在 Document Capture Pro 內登錄工作。
- ❏ 如果已啟用驗證功能，僅管理員可登錄 [預設]。

1. 在掃描器控制面板的主畫面上選取 [預設]。

2. 選取 ⊕。

3. 選取您要用於登錄預先設定的功能表。

4. 設定各項目，然後選取 ☆+。

附註：
當選取 [掃描至電腦] 時，選取已安裝 Document Capture Pro 的電腦，然後選取登錄的工作。這僅在透過網路連接的電腦上可用。

5. 進行預先設定。

- ❏ [名稱]：設定名稱。
- ❏ [設定圖示]：設定要顯示的圖示影像和顏色。
- ❏ [快速傳送設定]：選取預先設定後無需確認就立刻啟動掃描。

  使用 Document Capture Pro Server 時，即使已設定軟體在掃描前確認工作，掃描器預先設定上的 [快速傳送設定] 會優先於軟體使用。
- ❏ [內容]：檢查掃描設定。

6. 選取 [OK]。

## 預設 功能表選項

您可在每個預設中選取 > 以變更該預設的設定。

變更名稱：

變更預設名稱。

變更圖示：

變更預設圖示影像和顏色。

快速傳送設定：

選取預設設定後無需確認就立刻啟動掃描。

變更位置：

變更預設顯示順序。

刪除：

刪除預設。

新增或移除首頁上的圖示：

新增或刪除主畫面預設圖示。

確認詳細資料：

檢視預設設定。可透過選取 [使用此設定] 載入預設。

# 編輯控制面板主畫面

您可以在掃描器控制面板上選取 [設定] > [編輯主畫面] 以訂製主畫面。

- 版面配置：變更功能表圖示顯示方式。
  第74頁“變更主畫面的 版面配置”
- 新增圖示：新增圖示至您進行的 [預設] 設定，或還原已從畫面刪除的圖示。
  第75頁“新增圖示”
- 移除圖示：刪除首頁上的圖示。
  第76頁“移除圖示”
- 移動圖示：變更圖示顯示順序。
  第77頁“移動圖示”
- 還原預設圖示顯示：還原主畫面預設顯示設定。
- 背景圖案：變更主畫面的桌布色彩。

## 變更主畫面的 版面配置

1. 選取掃描器控制面板上的 [設定] > [編輯主畫面] > [版面配置]。

2. 選取 [行列] 或 [矩陣]。

[行列]：

[矩陣]：

3. 選取 以回到並檢查主畫面。

## 新增圖示

1. 選取掃描器控制面板上的 [設定] > [編輯主畫面] > [新增圖示]。
2. 選取 [功能] 或 [預設]。
   - ❏ 功能：顯示主畫面所示的預設功能。

❏ 預設：顯示登錄的預設。

3. 選取您要新增至主畫面的項目。

4. 選取您要向其新增項目的空白處。

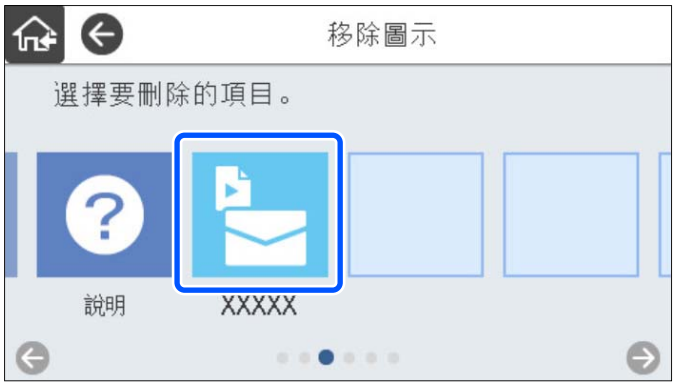
   如果您要新增多個副本，請重複步驟 3 至 4。

5. 選取 以回到並檢查主畫面。

## 移除圖示

1. 選取掃描器控制面板上的 [設定] > [編輯主畫面] > [移除圖示]。

2. 選取您要刪除的圖示。




3. 選取 [是] 完成操作。
   如果您要刪除多個圖示，請重複步驟 2 至 3。

4. 選取 以回到並檢查主畫面。

## 移動圖示

1. 選取掃描器控制面板上的 [設定] > [編輯主畫面] > [移動圖示]。

2. 選取您要移動的圖示。

3. 選取目的地幀。

   如果已在目的地框內設定另一圖示，該圖示將被取代。

4. 選取 以回到並檢查主畫面。

# 基本安全性設定

產品安全功能介紹. . . . . 80

管理員設定. . . . . 80

停用外部介面. . . . . 86

監控遠端掃描器. . . . . 86

解決問題. . . . . 88

# 產品安全功能介紹

本節介紹 Epson 裝置的安全功能。

| 功能名稱 | 功能類型 | 設定內容 | 防止內容 |
|---|---|---|---|
| 管理員密碼設定 | 鎖定系統設定，例如網路或 USB 連線設定。 | 管理員設定裝置的密碼。<br>您可從 Web Config 與掃描器控制面板設定或變更。 | 防止非法讀取和變更儲存於裝置上的資訊，例如 ID、密碼、網路設定和連絡人等。還可減少許多安全風險，例如網路環境或安全政策資訊洩露。 |
| 外部介面設定 | 控制連接至裝置的介面。 | 啟用或停用電腦的 USB 連線。 | 電腦的 USB 連線：透過禁止不經由網路的掃描防止未獲授權的使用裝置。 |

**相關資訊**

➡ 第80頁“配置管理員密碼”
➡ 第86頁“停用外部介面”

# 管理員設定

## 配置管理員密碼

設定管理員密碼時，您可以防止使用者變更系統管理設定。預設值在購買時設定。視需要變更它們。

附註：
下列內容提供管理員資訊的預設值。

- ❏ 使用者名稱（僅用於 Web Config）：無（空白）
- ❏ 密碼：取決於產品背面附帶的標籤。
  如果背面附帶「PASSWORD」標籤，則輸入標籤上顯示的 8 位數字。
  如果背面沒有附帶「PASSWORD」標籤，則輸入產品背面附帶標籤上的序列號以作為初始管理員密碼。

您可以使用 Web Config、掃描器控制面板或 Epson Device Admin 變更管理員密碼。當使用 Epson Device Admin 時，請參閱 Epson Device Admin 指南或說明。

### 使用 Web Config 變更管理員密碼

在 Web Config 中變更管理員密碼。

1. 存取 Web Config 並選取 [產品安全性] 索引標籤 > [變更系統管理員密碼]。
2. 在 [目前密碼]、[使用者名稱]、[新密碼] 和 [確認新密碼] 中輸入必要的資訊。
   新密碼必須是 8 至 20 個字元長度，且僅包含單字節字母數字字元和符號。

附註：
下列內容提供管理員資訊的預設值。

- ❏ 使用者名稱：無（空白）
- ❏ 密碼：取決於產品背面附帶的標籤。
  如果背面附帶「PASSWORD」標籤，則輸入標籤上顯示的 8 位數字。
  如果背面沒有附帶「PASSWORD」標籤，則輸入產品背面附帶標籤上的序列號以作為初始管理員密碼。

**重要事項：**
請務必記住您設定的管理員密碼。如果您忘記您的密碼，您將無法重置它，並將需要尋求維修人員的協助。

3. 選取 [確定]。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 從控制面板變更管理員密碼

您可從掃描器的控制面板變更管理員密碼。

1. 選取掃描器控制面板上的 [設定]。
2. 選取 [系統管理] > [管理員設定]。
3. 選取 [管理員密碼] > [變更]。
4. 輸入您的當前密碼。

   附註：
   購買時的初始管理員密碼（預設）隨產品背面附帶的標籤而不同。
   如果背面附帶「PASSWORD」標籤，則輸入標籤上顯示的 8 位數字。
   如果背面沒有附帶「PASSWORD」標籤，則輸入產品背面附帶標籤上的序列號以作為初始管理員密碼。
5. 輸入新密碼。

   新密碼必須是 8 至 20 個字元長度，且僅包含單字節字母數字字元和符號。

   **重要事項：**
   請務必記住您設定的管理員密碼。如果您忘記您的密碼，您將無法重置它，並將需要尋求維修人員的協助。
6. 再次輸入新密碼用於確認。

完成訊息會隨即顯示。

# 對控制面板使用 鎖定設定

您可以使用 鎖定設定 鎖定控制面板以防止使用者變更關於系統設定的項目。

附註：
如果啟用掃描器上的 驗證設定，鎖定設定 也將為控制面板啟用。當 驗證設定 啟用時，控制面板無法鎖定。

即使停用 驗證設定，鎖定設定 依然保持啟用狀態。如果要將起停用，可以從控制面板或 Web Config 進行設定。

## 從控制面板設定 鎖定設定

1. 如果要在一旦啟用後取消 [鎖定設定]，點選首頁畫面右上角的 ，以管理員身份登入。

   在 [鎖定設定] 停用後不顯示。若要啟用此設定，請前往下一步。

2. 選取 [設定]。
3. 選取 [系統管理] > [管理員設定]。
4. 為 [鎖定設定] 選取 [開啟] 或 [關閉]。

## 從 Web Config 設定 鎖定設定

1. 選取 [裝置管理] 索引標籤 > [控制面板]。
2. 選取 [開啟] 或 [關閉] 作為 [面板鎖定]。
3. 按下 [確定]。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 設定 功能表上的 鎖定設定 項目

這是控制面板上 [設定] 功能表內被 鎖定設定 鎖定的項目清單。

✓：待鎖定。

-：不會鎖定。

| 設定 功能表 | 鎖定設定 |
|---|---|
| 基本設定 | - |

| 設定 功能表 | | 鎖定設定 |
|---|---|---|
| | LCD 亮度 | - |
| | 音效 | - |
| | 睡眠模式定時器 | ✓ |
| | 電源關閉計時器 | ✓ |
| | 日期/時間設定 | ✓ |
| | 語言設定/Language | ✓/-* |
| | 鍵盤<br>（視乎您的區域，該功能可能不可用。） | - |
| | 操作逾時 | ✓ |
| | 透過 USB 的 PC 連線 | ✓ |
| | 直接開機 | ✓ |
| 掃描器設定 | | - |
| | 慢速模式 | - |
| | 多張進紙停止時間 | ✓ |
| | DFDS 功能 | - |
| | 紙張保護 | ✓ |
| | 髒污偵測 | ✓ |
| | 超音波多頁進紙偵測 | ✓ |
| | 自動進紙模式逾時 | ✓ |
| | 確認收件人 | ✓ |
| 編輯主畫面 | | ✓ |
| | 版面配置 | ✓ |
| | 新增圖示 | ✓ |
| | 移除圖示 | ✓ |
| | 移動圖示 | ✓ |
| | 還原預設圖示顯示 | ✓ |
| | 背景圖案 | ✓ |
| 使用者設定 | | ✓ |
| | 網路資料夾/FTP | ✓ |
| | 電子郵件 | ✓ |
| | 雲端 | ✓ |
| | USB 隨身碟 | ✓ |

| 設定 功能表 | | 鎖定設定 |
|---|---|---|
| 網路設定 | | ✓ |
| | Wi-Fi 設定 | ✓ |
| | 有線區域網路設定 | ✓ |
| | 網路狀態 | ✓ |
| | 進階 | ✓ |
| 網路服務設定 | | ✓ |
| | Epson Connect 服務 | ✓ |
| Document Capture Pro | | - |
| | 變更設定 | ✓ |
| 聯絡人管理員 | | - |
| | 登記/刪除 | ✓/-* |
| | 常用 | - |
| | 檢視選項 | - |
| | 搜尋選項 | - |
| 系統管理 | | ✓ |
| | 聯絡人管理員 | ✓ |
| | 管理員設定 | ✓ |
| | 限制 | ✓ |
| | 密碼加密 | ✓ |
| | 顧客調查 | ✓ |
| | WSD 設定 | ✓ |
| | 回復至出廠預設值 | ✓ |
| | 韌體更新 | ✓ |
| 裝置資訊 | | - |

| 設定 功能表 | | | 鎖定設定 |
|---|---|---|---|
| | 序號 | | - |
| | 目前版本 | | - |
| | 總掃描次數 | | - |
| | 單面掃描次數 | | - |
| | 雙面掃描次數 | | - |
| | 掃描專用護套掃描次數 | | - |
| | 更換滾輪後的掃描次數 | | - |
| | 定期清潔後的掃描次數 | | - |
| | 重設掃描次數 | | ✓ |
| 掃描器維護 | | | - |
| | 滾輪清潔 | | - |
| | 維護滾輪更換 | | - |
| | | 重設掃描次數 | ✓ |
| | | 更換方式 | - |
| | 定期清潔 | | - |
| | | 重設掃描次數 | ✓ |
| | | 如何清潔 | - |
| | 工作平台清潔 | | - |
| 滾輪更換警示設定 | | | ✓ |
| | 計數警示設定 | | ✓ |
| 定期清理警示設定 | | | ✓ |
| | 警告警示設定 | | ✓ |
| | 計數警示設定 | | ✓ |

* 您可以設定是否允許在 [系統管理] > [限制] 內進行變更。

# 從控制面板以管理員身份登入

您可以使用下列任一方式從掃描器的控制面板以管理員身份登入。

1. 點選畫面最右側的 。
   - ❏ 當 驗證設定 啟用後，圖示會顯示在 [歡迎使用] 畫面上（驗證待機畫面）。
   - ❏ 當 驗證設定 停用後，圖示會顯示在主畫面上。
2. 當確認畫面顯示時，點選 [是]。

3. 輸入管理員的密碼。

   登入完成訊息隨即顯示，然後控制面板上的主畫面顯示。

若要登出，點選畫面最右側的 。

# 停用外部介面

您可停用連接裝置至掃描器的介面。進行限制設定以限制透過網路以外的掃描。

附註：
您也可在掃描器的控制面板上進行限制設定。

透過 USB 的 PC 連線：[設定] > [基本設定] > [透過 USB 的 PC 連線]

1. 存取 Web Config 並選取 [產品安全性] 索引標籤 > [外部介面]。
2. 在要設定的功能上選取 [關閉]。

   在要取消控制時選取 [開啓]。

   透過 USB 的 PC 連線

   您可限制透過電腦使用 USB 連線。如果您想限制它，請選取 [關閉]。
3. 按下 [確定]。
4. 檢查已停用的連接埠是否不可用。

   透過 USB 的 PC 連線

   如果驅動程式已安裝在電腦上

   使用 USB 纜線將掃描器連接至電腦，然後確認掃描器不會掃描。

   如果驅動程式尚未安裝在電腦上

   Windows：

   開啟裝置管理員並保持開啟，使用 USB 連接線將掃描器連接至電腦，然後確認裝置管理員的顯示內容保持不變。

   Mac OS：

   使用 USB 纜線將掃描器連接至電腦，然後確認您無法從[印表機與掃描器]新增掃描器。

相關資訊

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

# 監控遠端掃描器

## 檢查遠端掃描器資訊

您可使用 Web Config 從 [狀態] 檢查運作掃描器的下列資訊。

❏ 產品狀態
檢查狀態、雲服務、產品編號、MAC 位址等。

❏ 網路狀態
檢查網路連接狀態、IP 位址、DNS 伺服器等資訊。

❏ 使用狀態
檢查掃描首日、掃描次數等。

❏ 硬體狀態
檢查掃描器每項功能的狀態。

❏ 面板快照
顯示掃描器控制面板所示畫面的螢幕截圖。

# 發生事件時接收電子郵件通知

## 關於電子郵件通知

這是一項通知功能，可在發生掃描停止和掃描器錯誤等事件時，將電子郵件傳送至指定的地址。
您最多可以登錄五個目的地，並為每個目的地設定通知設定。
若要使用此功能，您需在設定通知之前先設定郵件伺服器。

**相關資訊**

➡ 第41頁“配置郵件伺服器”

## 配置電子郵件通知

使用 Web Config 配置電子郵件通知。

1. 存取 Web Config 並選取 [裝置管理] 索引標籤 > [電子郵件通知]。
2. 設定電子郵件通知的主旨。
   從兩個下拉式功能表中選取顯示在主旨上的內容。
   ❏ [主旨] 旁會顯示所選取的內容。
   ❏ 左右兩側不可設定相同的內容。
   ❏ 當 [位置] 中的字元數超過 32 個位元組時，將省略超過 32 個位元組的字元。
3. 輸入要傳送通知電子郵件的電子郵件地址。
   使用 A—Z a—z 0—9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @ 並可輸入 1 至 255 個的字元。
4. 選取電子郵件通知的語言。
5. 針對您想要接收通知的事件選取相關的核取方塊。
   [通知設定] 的數量連結至 [電子郵件位址設定] 的目的地數量。
   範例：

如果您想要在管理員密碼變更時向 [電子郵件位址設定] 中設為編號 1 的電子郵件地址傳送通知，請選取 [系統管理員密碼已變更] 列中第 [1] 欄的核取方塊。

6. 按下 [確定]。

   確認電子郵件通知將會經由引發事件傳送。

   範例：管理員密碼已變更。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

**電郵通知項目**

| 項目 | 設定與說明 |
|---|---|
| 系統管理員密碼已變更 | 在管理員密碼已變更時通知。 |
| 掃描器錯誤 | 在發生掃描器錯誤時通知。 |
| Wi-Fi 故障 | 在發生無線 LAN 介面錯誤時通知。 |

# 解決問題

## 忘記您的管理員密碼

您需要客服人員的協助。聯絡您當地的經銷商。

附註：
下列內容提供 Web Config 管理員的初始值。

- 使用者名稱：無（空白）
- 密碼：取決於產品背面附帶的標籤。
  如果背面附帶「PASSWORD」標籤，則輸入標籤上顯示的 8 位數字。
  如果背面沒有附帶「PASSWORD」標籤，則輸入產品背面附帶標籤上的序列號以作為初始管理員密碼。

如果您恢復管理員密碼，它將被重設為購買時的初始值。

# 進階安全設定

安全性設定與危險預防. . . . . .90

使用通訊協定控制. . . . . 90

使用數位憑證. . . . . 93

與掃描器之間的 SSL/TLS 通訊. . . . . 98

使用 IPsec/IP 篩選加密的通訊. . . . . .99

將掃描器連接至 IEEE802.1X 網路. . . . . .110

解決進階安全性的問題. . . . . .112

# 安全性設定與危險預防

當掃描器連線至網路時，您可從遠端位置予以存取。此外，還可以多人共用掃描器，這在改善操作效率與便利性方面很有用。但是，非法存取、非法使用與篡改資料等方面的風險會增加。如果您在可存取網際網路的環境中使用掃描器，風險會更高。

針對沒有外部存取保護的掃描器，可從網際網路讀取儲存在掃描器中的列印工作記錄。

為了避免此風險，Epson 掃描器提供了多種安全性技術。

請根據已使用客戶環境資訊建立的環境條件，視需要設定掃描器。

| 名稱 | 功能類型 | 設定內容 | 防止內容 |
|---|---|---|---|
| 控制協定 | 控制要用於掃描器與電腦間通訊的通訊協定與服務，且其可啟用及停用這些功能。 | 已單獨允許或禁止套用至功能的通訊協定或服務。 | 防止使用者使用不必要的功能，進而降低可能因意外操作發生的安全風險。 |
| SSL/TLS 通訊 | 從掃描器存取網際網路中的 Epson 伺服器時，會使用 SSL/TLS 通訊加密通訊內容，如透過網頁瀏覽器與電腦通訊、使用 Epson Connect 及更新韌體。 | 取得 CA 簽署憑證，然後將其匯入至掃描器。 | 透過 CA 簽署憑證清除掃描器的識別碼，可防止模擬與未經授權的存取。此外，會保護 SSL/TLS 的通訊內容，且其會防止洩漏掃描資料與設定資訊的內容。 |
| IPsec/IP 篩選 | 您可設定允許切斷來自特定用戶端或屬於特定類型的資料。由於 IPsec 透過 IP 封包單元（加密與驗證）保護資料，因此，您可以安全地通訊不安全的通訊協定。 | 建立基本原則與個別原則來設定可存取掃描器的用戶端或資料類型。 | 保護掃描器免遭未經授權存取、篡改及攔截通訊資料。 |
| IEEE 802.1X | 僅允許經過認證的使用者連接至網路。僅允許許可的使用者使用掃描器。 | RADIUS 伺服器（驗證伺服器）的驗證設定。 | 保護掃描器免遭未經授權存取與使用。 |

**相關資訊**


➡ 第90頁 “使用通訊協定控制”
➡ 第98頁 “與掃描器之間的 SSL/TLS 通訊”
➡ 第99頁 “使用 IPsec/IP 篩選加密的通訊”
➡ 第110頁 “將掃描器連接至 IEEE802.1X 網路”


## 安全功能設定

當設定 IPsec/IP 篩選或 IEEE 802.1X 時，建議您使用 SSL/TLS 存取 Web Config 以通訊設定資訊，從而降低安全風險，例如篡改或攔截。

確保您在設定 IPsec/IP 篩選或 IEEE 802.1X 之前設定管理員密碼。

# 使用通訊協定控制

您可透過多種途徑和通訊協定進行掃描。此外，您還可以從未指定數量的網路電腦中使用網路掃描。

您可限制由指定途徑所進行的掃描作業，或者控制可用的功能，藉此降低意外安全風險。

# 通訊協定的控制

配置掃描器支援的協議設定。

1. 存取 Web Config，然後選取 [網路安全性] tab > [通訊協定]。
2. 配置各個項目。
3. 按下 [下一步]。
4. 按下 [確定]。
   設定即會套用到掃描器。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

# 可啟用或停用的通訊協定

| 協議 | 描述 |
|---|---|
| Bonjour 設定 | 您可指定是否要使用 Bonjour。Bonjour 用於搜尋裝置、掃描等等。 |
| SLP 設定 | 您可啟用或停用 SLP 功能。SLP 可用來進行 EpsonNet Config 中的推送掃描以及網路搜尋。 |
| WSD 設定 | 您可啟用或停用 WSD 功能。啟用後，您可新增 WSD 裝置並從 WSD 連接埠進行掃描。 |
| LLTD 設定 | 您可啟用或停用 LLTD 功能。啟用此功能後，會顯示在 Windows 網路圖中。 |
| LLMNR 設定 | 您可啟用或停用 LLMNR 功能。啟用此功能後，即便無法使用 DNS.，也不需要 NetBIOS 就可使用名稱解析功能 |
| SNMPv1/v2c 設定 | 您可指定是否啟用 SNMPv1/v2c。此功能可進行裝置設定、監控等作業。 |
| SNMPv3 設定 | 您可指定是否啟用 SNMPv3。這可用來設定加密裝置、監控等。 |

# 通訊協定設定項目

Bonjour 設定

| 項目 | 設定值與描述 |
|---|---|
| 使用 Bonjour | 選取此項目，透過 Bonjour 搜尋或使用裝置。 |
| Bonjour 名稱 | 顯示 Bonjour 名稱。 |
| Bonjour服務名稱 | 顯示 Bonjour 服務名稱。 |
| 位置 | 顯示 Bonjour 位置名稱。 |
| Wide-Area Bonjour | 設定是否使用 Wide-Area Bonjour。 |

SLP 設定

| 項目 | 設定值與描述 |
| --- | --- |
| 啟用 SLP | 選取此項目啟用 SLP 功能。<br>此項目會在 EpsonNet Config 中使用，如網路搜尋功能。 |

WSD 設定

| 項目 | 設定值與描述 |
| --- | --- |
| 啟用 WSD | 選取此項目啟用透過 WSD 新增裝置功能，並從 WSD 連接埠進行掃描。 |
| 掃描逾時 (秒) | 輸入 WSD 掃描工作的通訊逾時值（3 至 3,600 秒）。 |
| 裝置名稱 | 顯示 WSD 裝置名稱。 |
| 位置 | 顯示 WSD 位置名稱。 |

LLTD 設定

| 項目 | 設定值與描述 |
| --- | --- |
| 啟用 LLTD | 選取此項目啟用 LLTD。掃描器會顯示在 Windows 網路圖中。 |
| 裝置名稱 | 顯示 LLTD 裝置名稱。 |

LLMNR 設定

| 項目 | 設定值與描述 |
| --- | --- |
| 啟用 LLMNR | 選取此項目啟用 LLMNR。即便無法使用 DNS，也不需要 NetBIOS 就可使用名稱解析功能。 |

SNMPv1/v2c 設定

| 項目 | 設定值與描述 |
| --- | --- |
| 啟用 SNMPv1/v2c | 選取以啟用 SNMPv1/v2c。 |
| 存取權限 | 啟用 SNMPv1/v2c 後，設定存取授權。選取 [唯讀] 或 [讀/寫]。 |
| 社群名稱 (唯讀) | 輸入 0 至 32 個 ASCII（0x20 至 0x7E）字元。 |
| 社群名稱 (讀取/寫入) | 輸入 0 至 32 個 ASCII（0x20 至 0x7E）字元。 |

SNMPv3 設定

| 項目 | 設定值與描述 |
| --- | --- |
| 啟用 SNMPv3 | 若核取此方塊，SNMPv3 會啟用。 |
| 使用者名稱 | 使用 1 位元輸入 1 至 32 個字元。 |
| 驗證設定 | |

| 項目 | | 設定值與描述 |
|---|---|---|
| | 演算法 | 選取驗證 SNMPv3 的演算法。 |
| | 密碼 | 輸入驗證 SNMPv3 的密碼。<br>最多輸入 8 至 32 個 ASCII (0x20—0x7E) 字元。如果您未指定此項目，請將其保留空白。 |
| | 確認密碼 | 輸入您配置用於確認的密碼。 |
| 加密設定 | | |
| | 演算法 | 選取加密 SNMPv3 的演算法。 |
| | 密碼 | 輸入加密 SNMPv3 的密碼。<br>最多輸入 8 至 32 個 ASCII (0x20—0x7E) 字元。如果您未指定此項目，請將其保留空白。 |
| | 確認密碼 | 輸入您配置用於確認的密碼。 |
| 內容名稱 | | 輸入不超過 32 個 Unicode (UTF-8) 字元。如果您未指定此項目，請將其保留空白。可以輸入的字元數因語言而異。 |

# 使用數位憑證

## 關於電子憑證

❏ CA 簽署憑證

這是由 CA（憑證授權）簽署的憑證。您可取得憑證以套用於憑證授權。此憑證可證明掃描器的存在並用於 SSL/TLS 通訊，以確保資料通訊的安全。

用於 SSL/TLS 通訊時，可作為伺服器憑證。

若憑證設定為 IPsec/IP 篩選或 IEEE 802.1X 通訊時，則可作為客戶端憑證。

❏ CA 憑證

這是 CA 簽署憑證 鏈中的憑證，也稱為中級 CA 憑證。存取另一方伺服器或 Web Config 時，網頁瀏覽器會使用憑證來驗證掃描器憑證的路徑。

若為 CA 憑證，請設定何時驗證從掃描器存取伺服器憑證的路徑。若為掃描器，請設定為驗證 SSL/TLS 連接的 CA 簽署憑證 路徑。

您可以從核發 CA 憑證的憑證授權中取得掃描器的 CA 憑證。

另外，您可以從核發其他伺服器的 CA 簽署憑證 憑證授權中，取得用於驗證另一方伺服器的 CA 憑證。

❏ 自我簽署憑證

這是掃描器自行簽署和發行的憑證。亦稱為根憑證。由於核發者自行證明，所以此憑證並不可靠且無法防止模擬。

在進行安全設定，以及執行無 CA 簽署憑證 的簡單 SSL/TLS 通訊時才使用此憑證。

如果您將此憑證用於 SSL/TLS 通訊，由於該憑證未在網頁瀏覽器上登錄，因此網頁瀏覽器上可能會顯示安全警報。您只能將 自我簽署憑證 用於 SSL/TLS 通訊。

**相關資訊**

➡ 第94頁“組態 CA 簽署憑證”

➡ 第97頁“更新自我簽署憑證”
➡ 第97頁“組態 CA 憑證”

# 組態 CA 簽署憑證

## 取得 CA 簽署憑證

若要取得 CA 簽署憑證，請建立 CSR (憑證簽署要求) 並套用至憑證授權單位。您可使用 Web Config 及電腦建立 CSR。

請依照下列步驟使用 Web Config 建立 CSR 並取得 CA 簽署憑證。使用 Web Config 建立 CSR 時，憑證為 PEM/DER 格式。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤。接著選取 [SSL/TLS] > [憑證] 或 [IPsec/IP 篩選] > [用戶端憑證] 或 [IEEE802.1X] > [用戶端憑證]。

   無論選擇哪項，您均可獲得相同的憑證並將其共同使用。

2. 按下 [CSR] 的 [產生]。

   CSR 建立頁面會隨即開啟。

3. 在各項目輸入數值。

   附註：
   可用的金鑰長度及縮寫視憑證授權單位而定。根據各憑證授權單位的規定建立要求。

4. 按下 [確定]。

   完成訊息會隨即顯示。

5. 選取 [網路安全性] 索引標籤。接著選取 [SSL/TLS] > [憑證] 或 [IPsec/IP 篩選] > [用戶端憑證] 或 [IEEE802.1X] > [用戶端憑證]。

6. 根據各憑證授權單位的指定格式，按下 [CSR] 的其中一個下載鍵，將 CSR 下載至電腦。

   **重要事項：**
   請勿再次產生 CSR。否則可能無法匯入已核發的 CA 簽署憑證。

7. 將 CSR 傳送至憑證授權單位，並取得 CA 簽署憑證。

   請遵守各憑證授權單位的傳送方式及表單規定。

8. 將已核發的 CA 簽署憑證 儲存至與掃描器相連接的電腦。

   將憑證儲存至目的地的同時，CA 簽署憑證 的取得程序隨即完成。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

### CSR 設定項目

| 項目 | 設定與說明 |
|---|---|
| 金鑰長度 | 選取 CSR 的金鑰長度。 |
| 一般名稱 | 您可輸入 1 至 128 個的字元。若這是 IP 位址，則必須為靜態 IP 位址。您可以輸入 1 至 5 個 IPv4 位址、IPv6 位址、主機名稱、FQDN，並使用逗號分隔。<br>第一個元素會儲存至通用名稱，其他元素則會儲存在憑證主旨的別名欄位。<br>範例：<br>掃描器的 IP 位址：192.0.2.123，掃描器名稱：EPSONA1B2C3<br>一般名稱：EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123 |
| 組織/ 組織單位/ 位置/ 州/省 | 您最多可輸入 0 至 64 個 ASCII (0x20—0x7E) 字元。您可使用逗號分隔辨別名稱。 |
| 國家 | 輸入 ISO-3166 所指定的兩位數國碼。 |
| 寄件者的電子郵件位址 | 您可為郵件伺服器設定輸入傳送者的電子郵件地址。為 [網路] 索引標籤 > [電子郵件伺服器] > [基本] 輸入與 [寄件者的電子郵件位址] 相同的電子郵件地址。 |

## 匯入 CA 簽署憑證

將取得的 CA 簽署憑證 匯入到掃描器。

**重要事項：**

❏ 確保已正確設定掃描器的日期與時間。憑證可能無效。

❏ 若取得的憑證使用從 Web Config 建立的 CSR，您可匯入憑證一次。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤。接著選取 [SSL/TLS] > [憑證] 或 [IPsec/IP 篩選] > [用戶端憑證] 或 [IEEE802.1X] > [用戶端憑證]。

2. 按下 [匯入]

   憑證匯入頁面會隨即開啟。

3. 在各項目輸入數值。驗證存取掃描器的網頁瀏覽器上的憑證路徑時，請設定 [CA 憑證 1] 和 [CA 憑證 2]。

   根據 CSR 的建立位置及憑證的檔案格式，必要的設定可能會有所不同。根據下列說明輸入必要項目的值。

   ❏ 從 Web Config 取得的 PEM/DER 格式憑證

      ❏ [私密金鑰]：由於掃描器含有私密金鑰，因此請勿進行配置。

      ❏ [密碼]：不配置。

      ❏ [CA 憑證 1]/[CA 憑證 2]：選購

   ❏ 從電腦取得的 PEM/DER 格式憑證

      ❏ [私密金鑰]：您必須進行設定。

      ❏ [密碼]：不配置。

      ❏ [CA 憑證 1]/[CA 憑證 2]：選購

❏ 從電腦取得的 PKCS#12 格式憑證

❏ [私密金鑰]：不配置。

❏ [密碼]：選購

❏ [CA 憑證 1]/[CA 憑證 2]：不配置。

4. 按下 [確定]。

完成訊息會隨即顯示。

附註：
按下 [確認] 確認憑證資訊。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

### CA 簽名證書匯入設定項目

| 項目 | 設定與說明 |
|---|---|
| 伺服器憑證 或 用戶端憑證 | 選取證書格式。<br>對於 SSL/TLS 連線，伺服器憑證 會顯示。<br>對於 IPsec/IP 篩選或 IEEE 802.1X，用戶端憑證 會顯示。 |
| 私密金鑰 | 如果您透過使用從電腦建立的 CSR 而獲取 PEM/DER 格式的證書，請指定與證書相符的私有密鑰檔案。 |
| 密碼 | 如果檔案格式為 [有私密金鑰的憑證 (PKCS#12)]，請輸入密碼以為您在獲取證書時設定的私有密鑰加密。 |
| CA 憑證 1 | 如果您的證書格式是 [憑證 (PEM/DER)]，匯入簽發用作伺服器證書之 CA 簽署憑證 的證書機構的證書。視需要指定檔案。 |
| CA 憑證 2 | 如果您的證書格式是 [憑證 (PEM/DER)]，匯入簽發 CA 憑證 1 的證書機構的證書。視需要指定檔案。 |

## 刪除 CA 簽署憑證

當憑證過期或不再需要使用加密連線時，您可刪除已匯入的憑證。

**重要事項：**
若取得的憑證使用從 Web Config 建立的 CSR，您無法重新匯入已刪除的憑證。在此情況下，請建立 CSR 並重新取得憑證。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤。接著選取 [SSL/TLS] > [憑證] 或 [IPsec/IP 篩選] > [用戶端憑證] 或 [IEEE802.1X] > [用戶端憑證]。

2. 按下 [刪除]。

3. 在顯示的訊息中，確認您是否要刪除憑證。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 更新自我簽署憑證

由於 自我簽署憑證 是由掃描器所核發，因此您可以在其過期或所述內容變更時進行更新。

1. 存取 Web Config 並選取 [網路安全性] tab > [SSL/TLS] > [憑證]。
2. 按下 [更新]。
3. 輸入 [一般名稱]。

   您最多可以輸入 5 個 IPv4 位址、IPv6 位址、主機名稱、1 至 128 個字元的 FQDN 並使用逗號分隔。第一個參數會儲存至通用名稱，其他參數則會儲存在憑證主旨的別名欄位。

   範例：

   掃描器的 IP 位址：192.0.2.123，掃描器名稱：EPSONA1B2C3

   一般名稱：EPSONA1B2C3、EPSONA1B2C3.local、192.0.2.123
4. 指定憑證的有效期間。
5. 按下 [下一步]。

   確認訊息會隨即顯示。
6. 按下 [確定]。

   掃描器會隨即更新。

附註：
您可以從 [網路安全性] 索引標籤 > [SSL/TLS] > [憑證] > [自我簽署憑證] 檢查憑證資訊，並按下 [確認]。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 組態 CA 憑證

設定 CA 憑證 時，您可以針對掃描器要存取的伺服器，驗證其 CA 憑證的路徑。這可防止模擬。

您可以從核發 CA 簽署憑證 的憑證授權中取得 CA 憑證。

### 匯入 CA 憑證

將 CA 憑證 匯入掃描器。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤 > [CA 憑證]。
2. 按下 [匯入]。
3. 指定您想要匯入的 CA 憑證。

4. 按下 [確定]。

匯入完成後，您可返回 [CA 憑證] 畫面，即會顯示匯入的 CA 憑證。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 刪除 CA 憑證

您可以刪除匯入的 CA 憑證。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤 > [CA 憑證]。
2. 按下您想要刪除的 CA 憑證 旁的 [刪除]。
3. 在顯示的訊息中確認您想要刪除的證書。
4. 按下 [按下 [重新啟動網路] 以套用設定。]，然後檢查已刪除的 CA 證書是否未列示在已更新的畫面上。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

# 與掃描器之間的 SSL/TLS 通訊

若伺服器憑證使用與掃描器之間的 SSL/TLS (安全通訊端階層/傳輸層安全性) 通訊進行設定，您可以加密電腦之間的通訊路徑。如果您要防止遠端存取及未經授權的存取，請執行此操作。

## 進行基本 SSL/TLS 設定

如果掃描器支援 HTTPS 伺服器功能，您可以使用 SSL/TLS 通訊來加密通訊。您可以使用 Web Config 設定和管理掃描器，同時確保安全性。

設定加密強度和重定向功能。

1. 存取 Web Config，並選取 [網路安全性] 索引標籤 > [SSL/TLS] > [基本]。
2. 為每個項目選取一個值。
   - ❏ 加密長度
     選取加密強度級別。
   - ❏ 將 HTTP 重新導向至 HTTPS
     當 HTTP 被存取時重定向至 HTTPS。
3. 按下 [下一步]。
   確認訊息隨即顯示。

4. 按下 [確定]。
   掃描器被更新。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 配置掃描器的伺服器憑證

1. 存取 Web Config 並選取 [網路安全性] 索引標籤 > [SSL/TLS] > [憑證]。
2. 在 [伺服器憑證] 上指定要使用的憑證。
   - ❏ 自我簽署憑證
     自我簽署憑證已經由掃描器產生。若沒有取得 CA 簽署憑證，請選擇此選項。
   - ❏ CA 簽署憑證
     若您事先取得並匯入 CA 簽署憑證，則您可指定此選項。
3. 按下 [下一步]。
   確認訊息會隨即顯示。
4. 按下 [確定]。
   掃描器會隨即更新。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”
➡ 第94頁“組態 CA 簽署憑證”
➡ 第97頁“組態 CA 憑證”

# 使用 IPsec/IP 篩選加密的通訊

## 關於 IPsec/IP 篩選

您可使用 IPsec/IP 篩選功能，根據 IP 位址、服務和連接埠篩選流量。結合篩選功能，您可配置掃描器接受或封鎖指定的用戶端及資料。此外，您可使用 IPsec 改善安全性層級。

附註：
執行 Windows Vista (或以後版本) 或 Windows Server 2008 (或以後版本) 的電腦支援 IPsec。

## 配置預設原則

若要篩選流量，請配置預設原則。預設原則會套用至連線至掃描器的每個使用者或群組。若要更精細地控制使用者及使用者群組，請配置群組原則。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤 > [IPsec/IP 篩選] > [基本]。

2. 在各項目輸入數值。
3. 按下 [下一步]。
   確認訊息會隨即顯示。
4. 按下 [確定]。
   掃描器會隨即更新。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 預設原則 設定項目

[預設原則]

| 項目 | 設定與說明 |
|---|---|
| IPsec/IP 篩選 | 您可啟用或停用 IPsec/IP 篩選功能。 |

❏ [存取控制]
配置 IP 封包流量的控制方式。

| 項目 | 設定與說明 |
|---|---|
| 允許存取 | 選取此選項會允許已配置的 IP 封包通過。 |
| 拒絕存取 | 選取此選項會拒絕已配置的 IP 封包通過。 |
| IPsec | 選取此選項會允許已配置的 IPsec 封包通過。 |

❏ [IKE 版本]

選取 [IKEv1] 或 [IKEv2] 作為 [IKE 版本]。請根據與掃描器連接的裝置選取二者之一。

❏ IKEv1

若選取 [IKEv1] 作為 [IKE 版本]，會顯示下列項目。

| 項目 | 設定與說明 |
|---|---|
| 驗證方法 | 若選取 [憑證]，您必須事先取得並匯入 CA 簽署憑證。 |
| 預先共用金鑰 | 若針對 [驗證方法] 選取 [預先共用金鑰]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。 |
| 確認預先共用金鑰 | 輸入您配置用於確認的金鑰。 |

❏ IKEv2

若選取 [IKEv2] 作為 [IKE 版本]，會顯示下列項目。

| 項目 | | 設定與說明 |
|---|---|---|
| 本機 | 驗證方法 | 若選取 [憑證]，您必須事先取得並匯入 CA 簽署憑證。 |
| | ID 類型 | 如果您針對 [驗證方法] 選取 [預先共用金鑰]，請選取掃描器的 ID 類型。 |
| | ID | 輸入與 ID 類型相符的掃描器 ID。<br>不得使用「@」、「#」與「=」作為第一個字元。<br>[識別名稱]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「=」。<br>[IP位址]：輸入 IPv4 或 IPv6 格式。<br>[FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。<br>[電子郵件位址]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「@」。<br>[金鑰 ID]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。 |
| | 預先共用金鑰 | 若針對 [驗證方法] 選取 [預先共用金鑰]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。 |
| | 確認預先共用金鑰 | 輸入您配置用於確認的金鑰。 |

| 項目 | | 設定與說明 |
|---|---|---|
| 遠端 | 驗證方法 | 若選取 [憑證]，您必須事先取得並匯入 CA 簽署憑證。 |
| | ID 類型 | 如果您針對 [驗證方法] 選取 [預先共用金鑰]，請選取您要驗證之裝置的 ID 類型。 |
| | ID | 輸入與 ID 類型相符的掃描器 ID。<br>不得使用「@」、「#」與「=」作為第一個字元。<br>[識別名稱]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「=」。<br>[IP位址]：輸入 IPv4 或 IPv6 格式。<br>[FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。<br>[電子郵件位址]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「@」。<br>[金鑰 ID]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。 |
| | 預先共用金鑰 | 若針對 [驗證方法] 選取 [預先共用金鑰]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。 |
| | 確認預先共用金鑰 | 輸入您配置用於確認的金鑰。 |

❏ [封裝]

若針對 [存取控制] 選取 [IPsec]，您必須配置封裝模式。

| 項目 | 設定與說明 |
|---|---|
| 傳輸模式 | 若只在相同 LAN 上使用掃描器，請選取此選項。第 4 層以上的 IP 封包會經過加密。 |
| 通道模式 | 若您在具有網際網路功能的網路（如 IPsec-VPN）上使用掃描器，請選取此選項。IP 封包的標頭及資料會經過加密。<br>[遠端閘道 (通道模式)]：若針對 [封裝] 選取 [通道模式]，請輸入介於 1 和 39 個字元之間的閘道位址。 |

❏ [安全通訊協定]

若針對 [存取控制] 選取 [IPsec]，請選取一個選項。

| 項目 | 設定與說明 |
|---|---|
| ESP | 選取此選項可確保驗證和資料的完整性，並加密資料。 |
| AH | 選取此選項可確保驗證和資料的完整性。即使加密資料遭禁止，您也可以使用 IPsec。 |

❏ [演算法設定]

建議您針對所有設定選取 [任何] 或針對每個設定選取 [任何] 以外的項目。如果您針對部分設定選取 [任何] 並針對其他設定選取 [任何] 以外的項目，根據您要驗證的其他裝置而定，裝置可能無法通訊。

| 項目 | | 設定與說明 |
|---|---|---|
| IKE | 加密 | 選取 IKE 的加密演算法。<br>項目根據 IKE 版本而有所不同。 |
| | 驗證 | 選取 IKE 的驗證演算法。 |
| | 金鑰交換 | 選取 IKE 的金鑰交換演算法。<br>項目根據 IKE 版本而有所不同。 |
| ESP | 加密 | 選取 ESP 的加密演算法。<br>只有當針對 [安全通訊協定] 選取 [ESP] 時，此項才可用。 |
| | 驗證 | 選取 ESP 的驗證演算法。<br>只有當針對 [安全通訊協定] 選取 [ESP] 時，此項才可用。 |
| AH | 驗證 | 選取 AH 的加密演算法。<br>只有當針對 [安全通訊協定] 選取 [AH] 時，此項才可用。 |

# 配置群組原則

群組原則是套用至使用者或使用者群組的一或多條規則。掃描器會控制符合已配置原則的 IP 封包。IP 封包會依照群組原則 1 至 10、預設原則的順序進行驗證。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤 > [IPsec/IP 篩選] > [基本]。
2. 按下您要配置的編號索引標籤。
3. 在各項目輸入數值。
4. 按下 [下一步]。
   確認訊息會隨即顯示。
5. 按下 [確定]。
   掃描器會隨即更新。

## 群組原則 設定項目

| 項目 | 設定與說明 |
|---|---|
| 啟用此群組原則 | 您可啟用或停用群組原則。 |

[存取控制]

配置 IP 封包流量的控制方式。

| 項目 | 設定與說明 |
|---|---|
| 允許存取 | 選取此選項會允許已配置的 IP 封包通過。 |
| 拒絕存取 | 選取此選項會拒絕已配置的 IP 封包通過。 |
| IPsec | 選取此選項會允許已配置的 IPsec 封包通過。 |

[本機位址 (掃描器)]

選取與您的網路環境相符的 IPv4 位址或 IPv6 位址。若 IP 位址為自動指派，則可選取 [使用自動取得的 IPv4 位址]。

**附註：**
若 IPv6 位址是自動指派，可能無法取得連線。配置靜態 IPv6 位址。

[遠端位址 (主機)]

輸入裝置的 IP 位址以控制存取。IP 位址不得超過 43 個字元。若沒有輸入 IP 位址，所有位址會受到控制。

**附註：**
若 IP 位址是自動指派 (例如由 DHCP 指派)，可能無法取得連線。配置靜態 IP 位址。

[選擇連接埠方法]

選取指定連接埠的方式。

❏ 服務名稱

若針對 [選擇連接埠方法] 選取 [服務名稱]，請選取一個選項。

❏ 傳輸通訊協定

若針對 [選擇連接埠方法] 選取 [連接埠編號]，您必須配置封裝模式。

| 項目 | 設定與說明 |
|---|---|
| 任何通訊協定 | 選取此選項可控制所有通訊協定類型。 |
| TCP | 選取此選項可控制單點傳播的資料。 |
| UDP | 選取此選項可控制廣播及多點傳播的資料。 |
| ICMPv4 | 選取此選項可控制 Ping 命令。 |

❏ 本機連接埠

若針對 [選擇連接埠方法] 選取 [連接埠編號]，且針對 [傳輸通訊協定] 選取 [TCP] 或 [UDP]，請輸入連接埠號碼來控制接收封包，並以逗號分隔。您最多可輸入 10 個連接埠號碼。

範例：20、80、119、5220

若沒有輸入連接埠號碼，所有連接埠會受到控制。

❏ 遠端連接埠

若針對 [選擇連接埠方法] 選取 [連接埠編號]，且針對 [傳輸通訊協定] 選取 [TCP] 或 [UDP]，請輸入連接埠號碼來控制傳送封包，並以逗號分隔。您最多可輸入 10 個連接埠號碼。

範例：25、80、143、5220

若沒有輸入連接埠號碼，所有連接埠會受到控制。

[IKE 版本]

選取 [IKEv1] 或 [IKEv2] 作為 [IKE 版本]。請根據與掃描器連接的裝置選取二者之一。

❏ IKEv1

若選取 [IKEv1] 作為 [IKE 版本]，會顯示下列項目。

| 項目 | 設定與說明 |
| --- | --- |
| 驗證方法 | 若針對 [存取控制] 選取 [IPsec]，請選取一個選項。已使用憑證與預設原則一樣。 |
| 預先共用金鑰 | 若針對 [驗證方法] 選取 [預先共用金鑰]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。 |
| 確認預先共用金鑰 | 輸入您配置用於確認的金鑰。 |

❏ IKEv2

若選取 [IKEv2] 作為 [IKE 版本]，會顯示下列項目。

| 項目 | | 設定與說明 |
|---|---|---|
| 本機 | 驗證方法 | 若針對 [存取控制] 選取 [IPsec]，請選取一個選項。已使用憑證與預設原則一樣。 |
| | ID 類型 | 如果您針對 [驗證方法] 選取 [預先共用金鑰]，請選取掃描器的 ID 類型。 |
| | ID | 輸入與 ID 類型相符的掃描器 ID。<br>不得使用「@」、「#」與「=」作為第一個字元。<br>[識別名稱]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「=」。<br>[IP位址]：輸入 IPv4 或 IPv6 格式。<br>[FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。<br>[電子郵件位址]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「@」。<br>[金鑰 ID]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。 |
| | 預先共用金鑰 | 若針對 [驗證方法] 選取 [預先共用金鑰]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。 |
| | 確認預先共用金鑰 | 輸入您配置用於確認的金鑰。 |
| 遠端 | 驗證方法 | 若針對 [存取控制] 選取 [IPsec]，請選取一個選項。已使用憑證與預設原則一樣。 |
| | ID 類型 | 如果您針對 [驗證方法] 選取 [預先共用金鑰]，請選取您要驗證之裝置的 ID 類型。 |
| | ID | 輸入與 ID 類型相符的掃描器 ID。<br>不得使用「@」、「#」與「=」作為第一個字元。<br>[識別名稱]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「=」。<br>[IP位址]：輸入 IPv4 或 IPv6 格式。<br>[FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。<br>[電子郵件位址]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。您需要包括「@」。<br>[金鑰 ID]：輸入 1 至 255 個 1 位元組的 ASCII（0x20 至 0x7E）字元。 |
| | 預先共用金鑰 | 若針對 [驗證方法] 選取 [預先共用金鑰]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。 |
| | 確認預先共用金鑰 | 輸入您配置用於確認的金鑰。 |

[封裝]

若針對 [存取控制] 選取 [IPsec]，您必須配置封裝模式。

| 項目 | 設定與說明 |
|---|---|
| 傳輸模式 | 若只在相同 LAN 上使用掃描器，請選取此選項。第 4 層以上的 IP 封包會經過加密。 |

| 項目 | 設定與說明 |
|---|---|
| 通道模式 | 若您在具有網際網路功能的網路（如 IPsec-VPN）上使用掃描器，請選取此選項。IP 封包的標頭及資料會經過加密。<br>[遠端閘道 (通道模式)]：若針對 [封裝] 選取 [通道模式]，請輸入介於 1 和 39 個字元之間的閘道位址。 |

[安全通訊協定]

若針對 [存取控制] 選取 [IPsec]，請選取一個選項。

| 項目 | 設定與說明 |
|---|---|
| ESP | 選取此選項可確保驗證和資料的完整性，並加密資料。 |
| AH | 選取此選項可確保驗證和資料的完整性。即使加密資料遭禁止，您也可以使用 IPsec。 |

[演算法設定]

建議您針對所有設定選取 [任何] 或針對每個設定選取 [任何] 以外的項目。如果您針對部分設定選取 [任何] 並針對其他設定選取 [任何] 以外的項目，根據您要驗證的其他裝置而定，裝置可能無法通訊。

| 項目 | | 設定與說明 |
|---|---|---|
| IKE | 加密 | 選取 IKE 的加密演算法。<br>項目根據 IKE 版本而有所不同。 |
| | 驗證 | 選取 IKE 的驗證演算法。 |
| | 金鑰交換 | 選取 IKE 的金鑰交換演算法。<br>項目根據 IKE 版本而有所不同。 |
| ESP | 加密 | 選取 ESP 的加密演算法。<br>只有當針對 [安全通訊協定] 選取 [ESP] 時，此項才可用。 |
| | 驗證 | 選取 ESP 的驗證演算法。<br>只有當針對 [安全通訊協定] 選取 [ESP] 時，此項才可用。 |
| AH | 驗證 | 選取 AH 的加密演算法。<br>只有當針對 [安全通訊協定] 選取 [AH] 時，此項才可用。 |

## 在 群組原則 上結合 本機位址 (掃描器) 和 遠端位址 (主機)

| | | 本機位址 (掃描器) 的設定 | | |
|---|---|---|---|---|
| | | IPv4 | IPv6*2 | 任何位址*3 |
| 遠端位址 (主機) 的設定 | IPv4*1 | ✓ | — | ✓ |
| | IPv6*1, *2 | — | ✓ | ✓ |
| | 空白 | ✓ | ✓ | ✓ |

*1 若針對 [存取控制] 選擇 [IPsec]，您無法指定前綴長度。

*2 若針對 [存取控制] 選擇 [IPsec]，則您可選擇連結本地地址 (fe80::)，但群組政策將會停用。

*3 除了 IPv6 連結本地地址。

### 相關資訊

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 群組原則服務名稱參考

附註：
無法使用的服務將會顯示，但無法選取。

| 服務名稱 | 通訊協定類型 | 本機連接埠號碼 | 遠端連接埠號碼 | 受控功能 |
|---|---|---|---|---|
| 任何 | — | — | — | 所有服務 |
| ENPC | UDP | 3289 | 任一連接埠 | 從 Epson Device Admin 和掃描器驅動程式等應用程式中搜尋掃描器 |
| SNMP | UDP | 161 | 任一連接埠 | 從 Epson Device Admin 和 Epson 掃描器驅動程式等應用程式中，獲取並配置 MIB |
| WSD | TCP | 任一連接埠 | 5357 | 控制 WSD |
| WS-Discovery | UDP | 3702 | 任一連接埠 | 搜尋 WSD 掃描器 |
| Network Scan | TCP | 1865 | 任一連接埠 | 轉寄來自 Document Capture Pro 的掃描資料 |
| Network Push Scan | TCP | 任一連接埠 | 2968 | 從 Document Capture Pro 獲取推送掃描的工作資訊 |
| Network Push Scan Discovery | UDP | 2968 | 任一連接埠 | 從掃描器中搜尋電腦 |
| FTP 資料 (遠端) | TCP | 任一連接埠 | 20 | FTP 客戶端（轉寄掃描資料）<br>但這僅可控制使用遠端連接埠號碼 20 的 FTP 伺服器。 |
| FTP 控制 (遠端) | TCP | 任一連接埠 | 21 | FTP 客戶端（控制轉寄掃描資料） |
| CIFS (遠端) | TCP | 任一連接埠 | 445 | CIFS 客戶端（轉寄掃描資料至資料夾） |
| NetBIOS Name Service (遠端) | UDP | 任一連接埠 | 137 | CIFS 客戶端（轉寄掃描資料至資料夾） |
| NetBIOS Datagram Service (遠端) | UDP | 任一連接埠 | 138 | |
| NetBIOS Session Service (遠端) | TCP | 任一連接埠 | 139 | |
| HTTP (本機) | TCP | 80 | 任一連接埠 | HTTP(S) 伺服器（轉寄 Web Config 和 WSD 的資料） |
| HTTPS (本機) | TCP | 443 | 任一連接埠 | |

| 服務名稱 | 通訊協定類型 | 本機連接埠號碼 | 遠端連接埠號碼 | 受控功能 |
|---|---|---|---|---|
| HTTP (遠端) | TCP | 任一連接埠 | 80 | HTTP(S) 客戶端（更新韌體和根憑證） |
| HTTPS (遠端) | TCP | 任一連接埠 | 443 | |

# IPsec/IP 篩選 的配置範例

**僅接收 IPsec 封包**

此範例僅用來配置預設原則。

[預設原則]：

❏ [IPsec/IP 篩選]: [開啓]

❏ [存取控制]: [IPsec]

❏ [驗證方法]: [預先共用金鑰]

❏ [預先共用金鑰]：最多輸入 127 個字元。

[群組原則]：不配置。

**接收掃描資料和掃描器設定**

此範例允許從指定的服務進行掃描資料和掃描器配置的通訊。

[預設原則]：

❏ [IPsec/IP 篩選]: [開啓]

❏ [存取控制]: [拒絕存取]

[群組原則]：

❏ [啟用此群組原則]：勾選方塊。

❏ [存取控制]: [允許存取]

❏ [遠端位址 (主機)]：用戶端的 IP 位址

❏ [選擇連接埠方法]: [服務名稱]

❏ [服務名稱]：勾選 [ENPC], [SNMP], [HTTP (本機)], [HTTPS (本機)] 和 [Network Scan] 方塊。

**僅從指定的 IP 位址接收存取**

此範例允許指定的 IP 位址存取掃描器。

[預設原則]：

❏ [IPsec/IP 篩選]: [開啓]

❏ [存取控制]:[拒絕存取]

[群組原則]：

❏ [啟用此群組原則]：勾選方塊。

❏ [存取控制]: [允許存取]

❏ [遠端位址 (主機)]：系統管理員用戶端的 IP 位址

附註：
不論原則配置為何，用戶端將可存取及配置掃描器。

## 設定 IPsec/IP 篩選的證書

設定 IPsec/IP 篩選的客戶端證書。當您設定它時，您可將證書用作 IPsec/IP 篩選的驗證方式。如果您想要配置證書機構，請前往 [CA 憑證]。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤 > [IPsec/IP 篩選] > [用戶端憑證]。
2. 在 [用戶端憑證] 中匯入證書。

   如果您已匯入證書機構發佈的證書，您可複製該證書，並將其用於 IPsec/IP 篩選。若要複製，請從 [複製來源] 選取該證書，然後按下 [複印]。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”
➡ 第94頁“組態 CA 簽署憑證”
➡ 第97頁“組態 CA 憑證”

# 將掃描器連接至 IEEE802.1X 網路

## 配置 IEEE 802.1X 網路

將 IEEE 802.1X 設定至掃描器時，您可以在連接至 RADIUS 伺服器、具有驗證功能的 LAN 交換機或存取點的網路上使用。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤 > [IEEE802.1X] > [基本]。
2. 在各項目輸入數值。

   若要在 Wi-Fi 網路上使用掃描器，請按下 [Wi-Fi設定]，並選取或輸入 SSID。

   附註：
   您可以在乙太網路和 Wi-Fi 網路之間共享設定。
3. 按下 [下一步]。

   確認訊息會隨即顯示。
4. 按下 [確定]。

   掃描器會隨即更新。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## IEEE 802.1X 網路設定項目

| 項目 | 設定與說明 | |
|---|---|---|
| IEEE802.1X (有線網路) | 您可啟用或停用頁面中的設定值 ([IEEE802.1X] > [基本]) 以符合 IEEE802.1X (有線 LAN)。 | |
| IEEE802.1X (Wi-Fi) | 畫面會顯示 IEEE802.1X 的連線狀態 (Wi-Fi)。 | |
| 連線方式 | 目前網路的連線方式會顯示。 | |
| EAP 類型 | 選取用於掃描器與 RADIUS 伺服器之間的驗證方式選項。 | |
| | EAP-TLS | 您必須取得並匯入 CA 簽署憑證。 |
| | PEAP-TLS | |
| | PEAP/MSCHAPv2 | 您必須配置密碼。 |
| | EAP-TTLS | |
| 使用者 ID | 配置要用於 RADIUS 伺服器驗證的 ID。<br>輸入 1 至 128 個 1 位元組的 ASCII（0x20 至 0x7E）字元。 | |
| 密碼 | 配置驗證掃描器的密碼。<br>輸入 1 至 128 個 1 位元組的 ASCII（0x20 至 0x7E）字元。若您使用 Windows 伺服器作為 RADIUS 伺服器，則可輸入最多 127 個字元。 | |
| 確認密碼 | 輸入您配置用於確認的密碼。 | |
| 伺服器 ID | 您可配置使用指定 RADIUS 伺服器進行驗證的伺服器 ID。驗證器會針對從 RADIUS 伺服器傳送的伺服器憑證，驗證其 subject/subjectAltName 欄位是否包含伺服器 ID。<br>輸入 0 至 128 個 1 位元組的 ASCII（0x20 至 0x7E）字元。 | |
| 憑證驗證 | 不論驗證方法為何，您都可設定憑證效力。在 [CA 憑證] 中匯入憑證。 | |
| 匿名名稱 | 若針對 [EAP 類型] 選取 [PEAP-TLS] 或 [PEAP/MSCHAPv2]，則您可配置匿名名稱來取代 PEAP 驗證階段 1 的使用者 ID。<br>輸入 0 至 128 個 1 位元組的 ASCII（0x20 至 0x7E）字元。 | |
| 加密長度 | 您可選取下列其中一項。 | |
| | 高 | AES256/3DES |
| | 中 | AES256/3DES/AES128/RC4 |

# 設定 IEEE 802.1X 的證書

設定 IEEE802.1X 的客戶端證書。當您設定它時，您可以使用 [EAP-TLS] 和 [PEAP-TLS] 作為 IEEE 802.1X 的認證方式。如果您想要設定認證機構證書，請前往 [CA 憑證]。

1. 存取 Web Config，然後選取 [網路安全性] 索引標籤 > [IEEE802.1X] > [用戶端憑證]。
2. 在 [用戶端憑證] 中輸入證書。

   如果您已匯入證書機構發佈的證書，您可複製該證書，並將其用於 IEEE802.1X。若要複製，請從 [複製來源] 選取該證書，然後按下 [複印]。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

# 解決進階安全性的問題

## 還原安全性設定

當您建立高度安全環境（如 IPsec/IP 篩選）時，可能會因為錯誤設定或者裝置或伺服器故障而無法與裝置通訊。如果遇到這種情況，請還原安全性設定以針對裝置再次進行設定，或允許您暫時使用。

### 使用 Web Config 停用安全功能

您可使用 Web Config 停用 IPsec/IP 篩選。

1. 存取 Web Config 並選取 [網路安全性] 索引標籤 > [IPsec/IP 篩選] > [基本]。
2. 停用 [IPsec/IP 篩選]。

## 使用網路安全性功能的問題

### 忘記預先共用金鑰

**重新配置預先共用金鑰。**

若要變更金鑰，請存取 Web Config，然後選取 [網路安全性] 索引標籤 > [IPsec/IP 篩選] > [基本] > [預設原則] 或 [群組原則]。

當您變更預先共用金鑰時，請為電腦配置預先共用金鑰。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”
➡ 第99頁“使用 IPsec/IP 篩選加密的通訊”

### 無法使用 IPsec 通訊進行通訊

**指定掃描器或電腦不支援的演算法。**

掃描器支援以下演算法。檢查電腦的設定。

| 加密方式 | 演算法 |
|---|---|
| IKE 加密演算法 | AES-CBC-128、AES-CBC-192、AES-CBC-256、AES-GCM-128*、AES-GCM-192*、AES-GCM-256*、3DES |
| IKE 驗證演算法 | SHA-1、SHA-256、SHA-384、SHA-512、MD5 |

| 加密方式 | 演算法 |
| --- | --- |
| IKE 金鑰交換演算法 | DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30* |
| ESP 加密演算法 | AES-CBC-128、AES-CBC-192、AES-CBC-256、AES-GCM-128、AES-GCM-192、AES-GCM-256、3DES |
| ESP 驗證演算法 | SHA-1、SHA-256、SHA-384、SHA-512、MD5 |
| AH 驗證演算法 | SHA-1、SHA-256、SHA-384、SHA-512、MD5 |

* 僅適用於 IKEv2

**相關資訊**

➡ 第99頁“使用 IPsec/IP 篩選加密的通訊”

## 突然無法進行通訊

**掃描器的 IP 位址已變更或無法使用。**

當 群組原則 中所登錄的本機位址的 IP 位址已變更或無法使用時，將無法執行 IPsec 通訊。使用掃描器的控制面板停用 IPsec。

如果 DHCP 過期、重新啟動、IPv6 位址過期或尚未取得，則可能找不到針對掃描器之 Web Config（[網路安全性] 索引標籤 > [IPsec/IP 篩選] > [基本] > [群組原則] > [本機位址 (掃描器)]）登錄的 IP 位址。

使用靜態 IP 位址。

**電腦的 IP 位址已變更或無法使用。**

當 群組原則 中所登錄的遠端位址的 IP 位址已變更或無法使用時，將無法執行 IPsec 通訊。

使用掃描器的控制面板停用 IPsec。

如果 DHCP 過期、重新啟動、IPv6 位址過期或尚未取得，則可能找不到針對掃描器之 Web Config（[網路安全性] 索引標籤 > [IPsec/IP 篩選] > [基本] > [群組原則] > [遠端位址 (主機)]）登錄的 IP 位址。

使用靜態 IP 位址。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”
➡ 第99頁“使用 IPsec/IP 篩選加密的通訊”

## 配置 IPsec/IP 篩選後無法連線

**IPsec/IP 篩選的設定不正確。**

在掃描器的控制面板上停用 IPsec/IP 篩選。連接掃描器與電腦，然後再次進行 IPsec/IP 篩選設定。

相關資訊

➡ 第99頁“使用 IPsec/IP 篩選加密的通訊”

### 在配置 IEEE 802.1X 之後無法存取掃描器

IEEE 802.1X 的設定不正確。

從掃描器控制面板停用 IEEE 802.1X 與 Wi-Fi。連接掃描器與電腦，然後再次配置 IEEE 802.1X。

連接掃描器與電腦，然後再次配置 IEEE 802.1X。

相關資訊

➡ 第110頁“配置 IEEE 802.1X 網路”

## 使用數位憑證的問題

### 無法匯入 CA 簽署憑證

CA 簽署憑證 和 CSR 上的資訊不相符。

若 CA 簽署憑證 與 CSR 沒有相同的資訊，則無法匯入 CSR。檢查以下項目：

❏ 是否嘗試將憑證匯入至不具有相同資訊的裝置中？
檢查 CSR 的資訊，然後將憑證匯入至具有相同資訊的裝置中。

❏ 是否在將 CSR 傳送至憑證授權單位後，覆寫了已儲存至掃描器的 CSR？
請使用 CSR 重新取得 CA 簽署憑證。

CA 簽署憑證 超過 5 KB。

您無法匯入超過 5KB 的 CA 簽署憑證。

憑證匯入密碼不正確。

輸入正確的密碼。若忘記密碼，您無法匯入憑證。重新取得 CA 簽署憑證。

相關資訊

➡ 第95頁“匯入 CA 簽署憑證”

### 無法更新自我簽署憑證

尚未輸入 一般名稱。

您必須輸入 [一般名稱]。

在 一般名稱 中輸入了不支援的字元。

在 IPv4、IPv6、主機名稱或 FQDN 格式輸入 1 至 128 個 ASCII (0x20—0x7E) 字元。

**在通用名稱中包括逗號或空格。**

若輸入逗號，[一般名稱] 會從該處分成一半。若只有在逗號之前或之後輸入一個空格，則會發生錯誤。

**相關資訊**

➡ 第97頁“更新自我簽署憑證”

## 無法建立 CSR

**尚未輸入 一般名稱。**

您必須輸入 [一般名稱]。

**在 一般名稱、組織、組織單位、位置 和 州/省 中輸入了不支援的字元。**

在 IPv4、IPv6、主機名稱或 FQDN 格式輸入 ASCII (0x20—0x7E) 字元。

**在 一般名稱 中包括逗號或空格。**

若輸入逗號，[一般名稱] 會從該處分成一半。若只有在逗號之前或之後輸入一個空格，則會發生錯誤。

**相關資訊**

➡ 第94頁“取得 CA 簽署憑證”

## 顯示電子憑證相關警告

| 訊息 | 原因/解決方法 |
|---|---|
| 輸入伺服器憑證。 | 原因：<br>您沒有選擇要匯入的憑證。<br>解決方法：<br>選擇檔案並按下 [匯入]。 |
| 未輸入 CA 憑證 1。 | 原因：<br>CA 憑證 1 未輸入，僅輸入 CA 憑證 2。<br>解決方法：<br>先匯入 CA 憑證 1。 |
| 下列為無效值。 | 原因：<br>檔案路徑及/或密碼包含不支援的字元。<br>解決方法：<br>確定針對項目輸入正確的字元。 |
| 無效的日期與時間。 | 原因：<br>尚未設定掃描器的日期與時間。<br>解決方法：<br>使用 Web Config 或 EpsonNet Config 設定日期與時間。 |

| 訊息 | 原因/解決方法 |
|---|---|
| 無效的密碼。 | 原因：<br>為 CA 憑證所設定的密碼與輸入的密碼不一致。<br>解決方法：<br>輸入正確的密碼。 |
| 無效的檔案。 | 原因：<br>您沒有匯入 X509 格式的憑證檔案。<br>解決方法：<br>確定您選擇由信任的憑證授權單位所核發的正確憑證。 |
| | 原因：<br>您匯入的檔案太大。檔案大小上限為 5 KB。<br>解決方法：<br>若選擇正確的檔案，則憑證可能已損毀或是偽造的。 |
| | 原因：<br>憑證中包含的鏈結無效。<br>解決方法：<br>如需憑證的詳細資訊，請參閱憑證授權單位的網站。 |
| 無法使用含有三張以上 CA 憑證的伺服器憑證。 | 原因：<br>PKCS#12 格式的憑證檔案包含 3 個以上的 CA 憑證。<br>解決方法：<br>從 PKCS#12 格式轉換成 PEM 格式時匯入每個憑證，或匯入最多含有 2 個 CA 憑證的 PKCS#12 格式憑證檔案。 |
| 憑證已過期。請檢查憑證是否有效，或檢查產品上的日期與時間。 | 原因：<br>憑證過期。<br>解決方法：<br>❏ 若憑證過期，請取得並匯入新的憑證。<br>❏ 若憑證沒有過期，請確定已正確設定掃描器的日期與時間。 |
| 需要私密金鑰。 | 原因：<br>憑證沒有已配對的私密金鑰。<br>解決方法：<br>❏ 若憑證為 PEM/DER 格式並使用電腦從 CSR 取得，請指定私密金鑰檔案。<br>❏ 若憑證為 PKCS#12 格式並使用電腦從 CSR 取得，請指定包含私密金鑰的檔案。 |
| | 原因：<br>您已重新匯入使用 Web Config 從 CSR 取得的 PEM/DER 憑證。<br>解決方法：<br>若憑證為 PEM/DER 格式並使用 Web Config 從 CSR 取得，則您只能匯入一次。 |

| 訊息 | 原因/解決方法 |
| --- | --- |
| 安裝失敗。 | 原因：<br>由於掃描器與電腦之間的通訊失敗，或檔案因為一些錯誤而無法讀取，導致無法完成配置。<br>解決方法：<br>檢查指定的檔案及通訊後，重新匯入檔案。 |

相關資訊

➡ 第93頁“關於電子憑證”

## 意外刪除 CA 簽署憑證

沒有 CA 簽署憑證的備份檔案。

若有保留備份檔案，請重新匯入憑證。

若使用從 Web Config 建立的 CSR 取得憑證，您無法重新匯入已刪除的憑證。建立 CSR 並取得新憑證。

相關資訊

➡ 第95頁“匯入 CA 簽署憑證”
➡ 第96頁“刪除 CA 簽署憑證”

# 驗證設定

關於 驗證設定. . . . . 119

關於 驗證方法. . . . . 120

用於設定的軟體. . . . . 121

更新掃描器韌體. . . . . 121

連接和設定驗證裝置. . . . . 122

登錄和設定資訊. . . . . 126

使用 Epson Device Admin 的 工作歷史紀錄 報告. . . . . 141

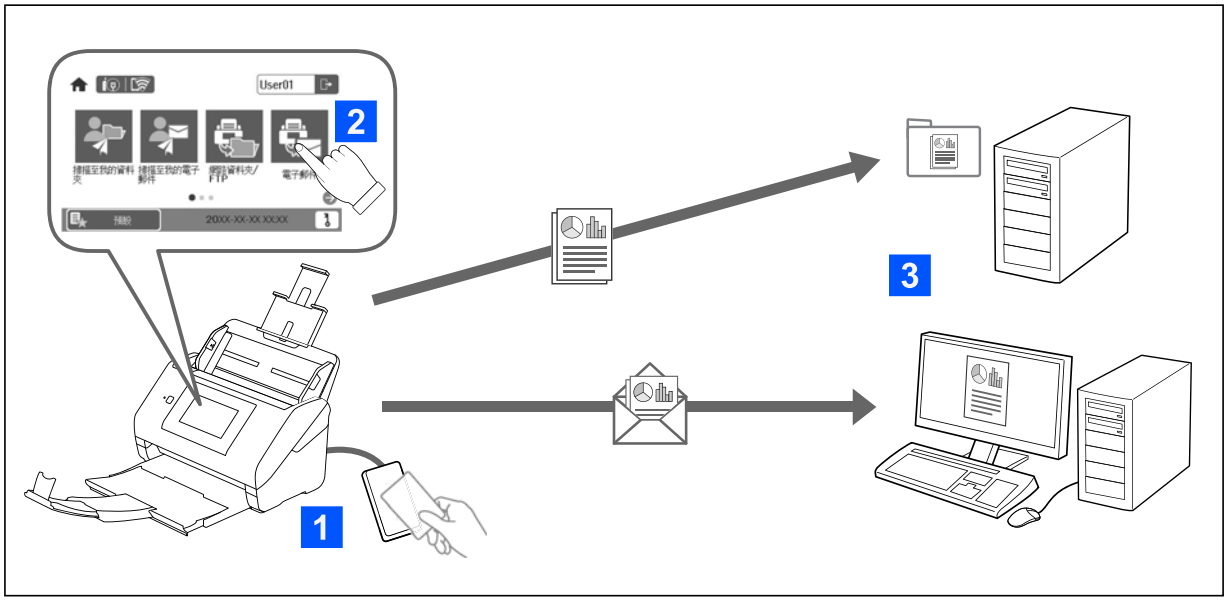
從控制面板以管理員身份登入. . . . . 141

停用 驗證設定. . . . . 141

刪除 驗證設定 資訊 (回復至出廠預設值). . . . . 142

解決問題. . . . . 142

# 關於 驗證設定




當 驗證設定 啟用後，需要使用者驗證才能啟動掃描。您可以設定每位使用者可以使用的掃描方法，並防止意外操作。

您可以指定已驗證使用者的電子郵件地址作為掃描目的地 (掃描至我的電子郵件)，或儲存每位使用者的資料至個人資料夾 (掃描至我的資料夾)。您還可以指定其他掃描方法。

附註：

- ❏ 當 驗證設定 啟用後，您無法從電腦或智慧型裝置進行掃描。
- ❏ 除本手冊內介紹的 驗證設定 以外，您還可以使用驗證伺服器建立驗證系統。若要建立系統，請使用 Document Capture Pro Server Authentication Edition（縮略名稱為 Document Capture Pro Server AE）。如需進一步資訊，請洽詢當地的 Epson 公司。

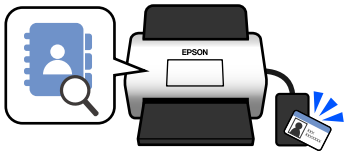
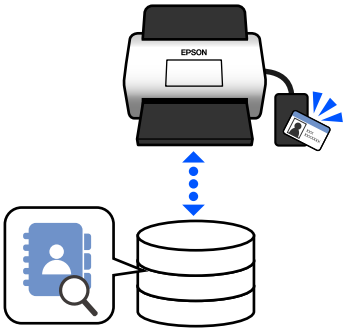
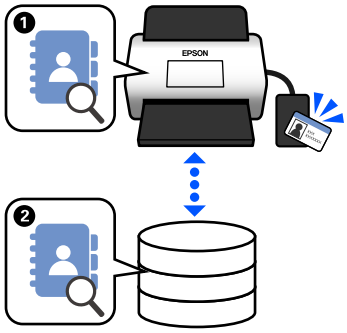
## 適用於 驗證設定 的可用功能

| 控制面板上的掃描功能 | 驗證設定 | |
|---|---|---|
| | 啟用時 | 禁用時 |
| **掃描至我的資料夾**<br>儲存影像至指派給經驗證使用者的資料夾。 | ✓ | - |
| **掃描至我的電子郵件**<br>儲存影像至指派給經驗證使用者的電子郵件地址。 | ✓ | - |
| **掃描至網路資料夾/FTP**<br>儲存影像至網路上的資料夾。 | ✓ | ✓ |
| **掃描至電腦**<br>使用在 Document Capture Pro (Windows)/Document Capture (Mac OS) 內建立的工作儲存影像至連接的電腦。<br>* 當 驗證設定 啟用後，您僅可以使用登錄於 [預設] 內的工作。 | ✓* | ✓ |

| 控制面板上的掃描功能 | 驗證設定 | |
|---|---|---|
| | 啟用時 | 禁用時 |
| **掃描至電子郵件**<br>傳送影像至您設定的電子郵件地址。 | ✓ | ✓ |
| **掃描至雲端**<br>傳送影像至您設定的雲服務。 | ✓ | ✓ |
| **掃描至 USB 隨身碟**<br>儲存影像至連接到掃描器的 USB 驅動。這僅在認證裝置連接至掃描器時可用。 | ✓ | ✓ |
| **掃描至 WSD**<br>使用 WSD 功能儲存影像至連接的電腦。 | - | ✓ |
| **預設**<br>您可以登錄最多 48 個預設掃描功能。<br>您可以分配最多五個 預設 給登錄於 本機 DB 內的使用者。分配的 預設 僅可由該使用者使用。未分配給任何使用者的 預設 可由所有使用者使用。 | ✓ | ✓ |

# 關於 驗證方法

此掃描器可使用下列方法提供驗證，無需建立驗證伺服器。

| | 本機 DB | LDAP | 本機 DB 和 LDAP |
|---|---|---|---|
| 使用者資訊位置 | **掃描器記憶體**<br>此驗證方法檢查登錄至掃描器的使用者資訊，並將其與使用掃描功能的使用者進行對比。 | LDAP 伺服器*<br>該驗證方法檢查與掃描器同步之 LDAP 伺服器的使用者資訊。由於最多 300 條來自 LDAP 伺服器的使用者資訊可以作為緩存暫時儲存於掃描器內，如果 LDAP 伺服器宕機，可以使用緩存執行驗證。<br>* 提供可與 LDAP 通訊之目錄服務的伺服器。 | **掃描器記憶體和 LDAP 伺服器**<br>首先檢查登錄於掃描器內的使用者資訊 (❶)，如果沒有匹配項，對照 LDAP 伺服器檢查使用者資訊 (❷)。 |
| |  |  |  |
| 已登錄使用者的數目 | 50（掃描器記憶體） | 無限（LDAP 伺服器） | 50（掃描器記憶體）<br>無限（LDAP 伺服器） |

| | 本機 DB | LDAP | 本機 DB 和 LDAP |
|---|---|---|---|
| 掃描器記憶體緩存 | - | 300 | 最大 300<br>（其中的 50 個緩存插槽與 本機 DB 內的 使用者設定 共用） |
| 登入方法 | 您可使用下列任一方法。<br>❏ 握住驗證卡或輸入 [使用者 ID] 和 [密碼]<br>❏ 握住驗證卡或輸入 [識別碼]<br>❏ 輸入 [使用者 ID] 和 [密碼]<br>❏ 輸入 [使用者 ID]<br>❏ 輸入 [識別碼] | | |
| 「掃描至」功能的限制 | 為每位使用者單獨設定 | 所有 LDAP 使用者設定相同 | 本機 DB 使用者：單獨設定<br>LDAP 使用者：所有使用者設定相同 |
| 分配 預設至使用者 | 每位使用者最多 5 個 | -<br>（無法單獨設定） | 本機 DB 使用者：每位使用者最多 5 個<br>LDAP 使用者：- |

# 用於設定的軟體

使用 Web Config 或 Epson Device Admin 進行設定。

❏ 使用 Web Config 時，您可僅使用網路瀏覽器設定掃描器。
第35頁“Web Config”

❏ 使用 Epson Device Admin 時，您可以使用設定範本一次設定多個掃描器。
第36頁“Epson Device Admin”

# 更新掃描器韌體

啟用 驗證設定 前，更新掃描器韌體至最新版本。預先連接掃描器至網際網路。

**重要事項：**
更新時請勿關閉電腦或掃描器。

從 Web Config 進行設定時：

選取 [裝置管理] 索引標籤 > [韌體更新]，然後遵循螢幕上的操作說明清潔印字頭。

從 Epson Device Admin 進行設定時：

選取裝置清單畫面上的 [首頁] > [韌體] > [更新]，然後遵循螢幕上的操作說明清潔印字頭。

附註：
如果已安裝最新版韌體，則無需更新。

# 連接和設定驗證裝置

如果要連接和使用驗證裝置，例如 IC 讀卡器，首先應設定該裝置。如果不使用驗證裝置，則無須執行此操作。

**相關資訊**

➡ 第124頁“連接驗證裝置”
➡ 第125頁“驗證裝置設定”

## 讀卡器相容清單

此清單不保證清單內讀卡器的操作。

是：支援（ID 資訊可使用標準讀卡器設定讀取。）

否：不相容

| 製造商 | 型號 | 型號編碼 | 驗證卡 | | | | | | | 模式 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | HID Global | DMZ | MIFARE | | FeliCa™ | | IEC/ ISO14443 (Type B) Compliance | |
| | | | iClass | EM4002 | Classic | Ultralight | Standard | Lite/ Lite-S | | |
| RF IDEAS | pcProx Plus | RDR-80081AKU | 是 | 是*1 | 是*1 | 是*1 | 否 | 否 | 否 | 鍵盤 |
| RF IDEAS | pcProx | RDR-7081BKU | 是*1 | 否 | 是 | 是 | 否 | 否 | 否 | 鍵盤 |
| RF IDEAS | pcProx | RDR-7581AKU | 是 | 否 | 是*1 | 是*1 | 否 | 否 | 否 | 鍵盤 |
| ELATEC | TWN3 MIFARE | T3DT-MB2BEL T3DT-MB2WEL | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 鍵盤 |
| ELATEC | TWN3 MIFARE NFC | T3DT-FB2BEL T3DT-FB2WEL | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 鍵盤 |

| 製造商 | 型號 | 型號編碼 | 驗證卡 | | | | | | | 模式 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | HID Global | DMZ | MIFARE | | FeliCa™ | | IEC/ ISO14443 (Type B) Compliance | |
| | | | iClass | EM4002 | Classic | Ultralight | Standard | Lite/ Lite-S | | |
| ELATEC | TWN4 MULTITECH | T4DT-FB2BEL-PI T4DT-FB2WEL-PI | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 鍵盤 |
| ELATEC | TWN4 MultiTech 2 BLE-PI | T4LK-FB4BLZ-PI | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 鍵盤 |
| ELATEC | TWN4 Slim | T4QC-FC3B7 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 鍵盤 |
| HID Global | OMNIKEY 5427 | OMNIKEY5427CK OMNIKEY5427CK gen2 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 鍵盤[*1] |
| ACS | ACR122U | ACR122U | 否 | 否 | 是[*2] | 是[*2] | 是 | 否 | 是[*2] | PC/SC |
| ACS | ACR1252 | ACR1252 | 否 | 否 | 是[*2] | 是[*2] | 是 | 是 | 是[*2] | PC/SC |
| Sony | PaSoRi | RC-S330/S | 否 | 否 | 是[*2] | 是[*2] | 是[*2] | 是[*2] | 是[*2] | PaSoRi |
| Sony | PaSoRi | RC-S380/P RC-S380/S | 否 | 否 | 是[*2] | 是[*2] | 是[*2] | 是[*2] | 是[*2] | PaSoRi |
| DMZ | Leitor RFID Universal | DMZ008 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 鍵盤 |
| DMZ | Leitor RFID Multi-125 | DMZ087 | 否 | 是 | 否 | 否 | 否 | 否 | 否 | 鍵盤 |
| DMZ | Leitor RFID Mifare | DMZ088 | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 鍵盤 |

| 製造商 | 型號 | 型號編碼 | 驗證卡 | | | | | | | 模式 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | HID Global | DMZ | MIFARE | | FeliCa™ | | IEC/ ISO14443 (Type B) Compliance | |
| | | | iClass | EM4002 | Classic | Ultralight | Standard | Lite/ Lite-S | | |
| DMZ | Biometric & RFID Reader | DMZ073 | 否 | 是 | 否 | 否 | 否 | 否 | 否 | 鍵盤 |
| inepro | SCR708 | SCR708 | 是*1 | 是*1 | 是*1 | 是*1 | 是*1 | 是*1 | 是*1 | 鍵盤 |
| Y Soft | YU03088 001 | MU0388 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 鍵盤 |
| Cartadis | TCM3 Cartadis MiFare Card Reader | ZTCM3-MIFARE | 否 | 否 | 是 | 是 | 否 | 否 | 是 | 鍵盤 |
| MICI Network Co., Ltd. | EM & Mifare Card Reader | mCR-600 | 否 | 否 | 是 | 是 | 否 | 否 | 是 | 鍵盤 |
| NT-ware | MiCard MultiTech4-PI | T4DT-FB4WUF-PI | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 鍵盤 |
| NT-ware | MiCard Plus-2-V2 | RDR-80081AGU-NT2-20 | 是*1 | 是*1 | 是*1 | 是*1 | 否 | 否 | 否 | 鍵盤 |
| NT-ware | MiCard V3 Multi | MiCard V3 Multi | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 鍵盤 |

*1 您需要使用讀卡器製造商提供的專用軟體變更讀卡器的設定。

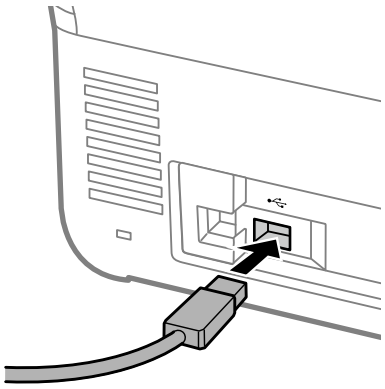
*2 如果您需要透過組態產品設定來使用卡內特定區域內的資料而非標準 ID 卡作為驗證 ID，請聯絡您的 Epson 合作夥伴或本地代表以獲取關於設定產品的更多資訊。

# 連接驗證裝置

**重要事項：**

當您連接驗證裝置至多個掃描器時，請使用具有相同機型編號的產品。

連接讀卡器的 USB 線纜至掃描器上的外部界面 USB 連接埠。



## 驗證裝置的操作檢查

您可以從掃描器控制面板檢查驗證裝置的連接狀態和驗證卡識別。

如果您選取 [設定] > [裝置資訊] > [驗證裝置狀態]，將顯示資訊。

# 驗證裝置設定

設定接收自驗證卡之驗證資訊的讀取格式。

可為驗證裝置設定以下讀取方式。

❏ 讀取驗證卡的特定區域，例如員工編號或個人 ID。

❏ 使用除 UID 以外的驗證卡資訊（序號等驗證卡資訊。）
可以使用工具生成操作參數。詳情請洽詢經銷商。

附註：
使用不同製造商提供的驗證卡：

使用 UID 取得卡片資訊（序號等卡片 ID 資訊）時，可以搭配使用不同類型的驗證卡。使用其他卡片資訊時，則無法搭配使用。

從 Web Config 進行設定時：

選取 [裝置管理] 索引標籤 > [讀卡機]。

從 Epson Device Admin 進行設定時：

從設定範本中選取 [管理員設定] > [驗證設定] > [讀卡機]。

| 項目 | 說明 |
|---|---|
| Vendor ID | 使用 4 個字母數字字元，設定驗證裝置的供應商 ID，限制使用 0000 至 FFFF。如果不想限制，則設定為 0000。 |
| Product ID | 使用 4 個字母數字字元，設定驗證裝置的產品 ID，限制使用 0000 至 FFFF。如果不想限制，則設定為 0000。 |
| 操作參數 | 設定驗證裝置的運作參數為 0 至 8,192 個字元。可用 A—Z、a—z、0—9、+、/、=、空白和換行。 |
| 讀卡機 | 選擇驗證裝置的轉換格式。您可以檢查格式細節。查看項目描述內提供的連結。 |

| 項目 | 說明 |
|---|---|
| 驗證卡 ID 儲存格式 | 選擇 ID 卡之驗證資訊的轉換格式。您可以檢查格式細節。查看項目描述內提供的連結。 |
| 設定卡片 ID 範圍 | 啟用讀取位置規格。 |
| 文字開始位置 | 指定用於讀取 ID 資訊的文字開始位置。可指定 1 至 4096 個。 |
| 字元數量 | 指定從 ID 資訊開始位置讀取的字符數。可指定 1 至 4096 個。 |

# 登錄和設定資訊

## 調定

視乎所用 驗證方法 和掃描方式，進行必要設定。

**重要事項：**

開始設定前，請檢查掃描器的時間設定是否正確。

如果時間設定有誤，會顯示「授權已過期」錯誤訊息，這可能導致設定掃描器失敗。此外，為了使用 SSL/TLS 通訊或 IPsec 等安全功能，也必須設定正確的時間。您可以下述方式設定時間。

❏ Web Config：[裝置管理] 索引標籤 > [日期與時間] > [日期與時間]。

❏ 掃描器控制面板：[設定] > [基本設定] > [日期/時間設定]。

| 設定 | 本機 DB | LDAP | 本機 DB 和 LDAP |
|---|---|---|---|
| **啟用驗證**<br>進行驗證設定前，需要啟用驗證。<br>第127頁“啟用驗證” | ✓ | ✓ | ✓ |
| **驗證設定**<br>設定 驗證方法 和如何驗證使用者。<br>第127頁“驗證設定” | ✓ | ✓ | ✓ |
| **登錄 使用者設定**<br>為每位使用者登錄設定。您還可以使用 CSV 檔案大量登錄使用者。<br>第128頁“登錄 使用者設定” | ✓ | — | ✓ |
| **與 LDAP 伺服器 同步**<br>進行 LDAP 伺服器同步設定。<br>第134頁“與 LDAP 伺服器 同步” | — | ✓ | ✓ |
| **設定 電子郵件伺服器**<br>進行電子郵件伺服器設定。在使用需要電子郵件伺服器設定的功能（例如 掃描至我的電子郵件）時使用此項。<br>第138頁“設定電子郵件伺服器” | ✓ | ✓ | ✓ |

| 設定 | 本機 DB | LDAP | 本機 DB 和 LDAP |
|---|---|---|---|
| 設定 掃描至我的資料夾<br>設定目的地資料夾。在使用 掃描至我的資料夾 功能時設定此項。<br>第138頁“設定 掃描至我的資料夾” | ✓ | ✓ | ✓ |
| 自訂單鍵功能<br>在變更掃描器控制面板上顯示的項目時設定此項。您可以僅在控制面板上顯示需要的圖示，或變更圖示順序。<br>第140頁“自訂單鍵功能” | ✓ | ✓ | ✓ |

## 啟用驗證

進行驗證設定前，需要啟用驗證。

從 Web Config 進行設定時：

從 [產品安全性] 索引標籤 > [基本] > [驗證] 選取 [開啟 (裝置/LDAP 伺服器)]。

從 Epson Device Admin 進行設定時：

在設定範本上，從 [管理員設定] > [驗證設定] > [基本] > [驗證] 選取 [開啟 (裝置/LDAP 伺服器)]。

附註：
如果啟用掃描器上的 驗證設定，鎖定設定 也將為控制面板啟用。當 驗證設定 啟用時，控制面板無法鎖定。

即使停用 驗證設定，鎖定設定 依然保持啟用狀態。如果要將起停用，可以從控制面板或 Web Config 進行設定。

### 相關資訊

➡ 第82頁“從控制面板設定 鎖定設定”
➡ 第82頁“從 Web Config 設定 鎖定設定”

## 驗證設定

設定 驗證方法 和如何驗證使用者。

從 Web Config 進行設定時：

選取 [產品安全性] 索引標籤 > [驗證設定]。

從 Epson Device Admin 進行設定時：

從設定範本中選取 [管理員設定] > [驗證設定] > [驗證設定]。

| 項目 | 說明 |
|---|---|
| 驗證方法 | 選取 驗證方法。<br>❏ 本機 DB<br>使用登錄至掃描器的 使用者設定 進行驗證。必須將使用者登錄至掃描器。<br>❏ LDAP<br>使用與掃描器同步的 LDAP 伺服器上的使用者資訊進行驗證。您需要提前進行 LDAP 伺服器設定。<br>❏ 本機 DB 和 LDAP<br>使用登錄至掃描器的使用者資訊，或登錄至與掃描器同步的 LDAP 伺服器的使用者資訊進行驗證。需要將使用者登錄至掃描器，並設定 LDAP 伺服器。 |
| 如何驗證使用者 | 選取如何驗證使用者。<br>❏ 卡片或使用者 ID 和密碼<br>使用驗證卡驗證使用者。亦可透過使用者 ID 和密碼進行驗證。<br>❏ 使用者 ID 和密碼<br>透過使用者 ID 和密碼驗證使用者。<br>選取此功能後，不可使用驗證卡進行驗證。<br>❏ 使用者 ID<br>僅透過使用者 ID 驗證使用者。無須設定密碼。<br>❏ 卡片或識別碼<br>使用驗證卡驗證使用者。亦可使用 識別碼。<br>❏ 識別碼<br>僅適用 ID 編碼驗證使用者。 |
| 允許使用者登錄驗證卡 | 如果要允許使用者將驗證卡登錄至系統，請啟用它。<br>如果為 [驗證方法] 選取 [LDAP]，則無法設定它。<br>關於使用者如何登錄其驗證卡的更多資訊，請參閱 *進階使用說明* 內的「登錄驗證卡」。 |
| 識別碼的最小位數 | 為 ID 編號選取最少位數。 |
| LDAP 驗證使用者的快取 | 使用 LDAP 伺服器驗證時，您可以設定是否要將快取用於使用者資訊。 |
| 在 SMTP 驗證中使用使用者資訊 | 將使用者 ID 與密碼用於驗置時，您可以設定是否要將使用者資訊用於 SMTP 驗證。系統會使用上一次登入的使用者 ID 與密碼。 |
| LDAP 驗證使用者的限制 | 如果使用 LDAP，可設定使用者能使用的功能。 |

# 登錄 使用者設定

登錄用於使用者驗證的 使用者設定。您可使用下列任一方法進行登錄。

❏ 逐一登錄 使用者設定 (Web Config)

❏ 使用 CSV 檔案整批登錄多個 使用者設定 (Web Config)

❏ 使用設定範本整批登錄 使用者設定 至多個掃描器 (Epson Device Admin)

**相關資訊**

➡ 第129頁“單獨登錄 使用者設定 (Web Config)”
➡ 第130頁“使用 CSV 檔案登錄多個 使用者設定 (Web Config)”
➡ 第132頁“整批登錄 使用者設定 至多個掃描器 (Epson Device Admin)”

## 單獨登錄 使用者設定 (Web Config)

存取 Web Config 並選取 [產品安全性] 索引標籤 > [使用者設定] > [新增]，然後輸入 使用者設定。

| 項目 | 說明 |
|---|---|
| 使用者 ID | 輸入您希望用於驗證的使用者 ID，是可用 Unicode (UTF-8) 表示的 1 至 83 個字節。<br>使用者 ID 不分大小寫，您可以使用大寫或小寫字母登入。 |
| 使用者名稱顯示 | 輸入掃描器控制面板上顯示的使用者名稱，是可以 Unicode (UTF-16) 表示的 32 個字元。您可將此留白。 |
| 密碼 | 輸入您希望用於驗證的密碼，為 32 個 ASCII 格式字元。密碼會區分大小寫。<br>如果為 [如何驗證使用者] 選取 [使用者 ID]，則將此留白。 |
| 驗證卡 ID | 輸入 116 個 ASCII 格式的驗證卡 ID。您可將此留白。<br>如果為 [驗證設定] 允許 [允許使用者登錄驗證卡]，則將體現使用者登錄的結果。 |
| 識別碼 | 當在 [驗證設定] > [如何驗證使用者] 中選取 [卡片或識別碼] 或 [識別碼] 時，會顯示此項目。<br>輸入在 [驗證設定] > [識別碼的最小位數] 中設定的數值之間的某個數字，最多 8 位數。 |
| 自動產生 | 當在 [驗證設定] > [如何驗證使用者] 中選取 [卡片或識別碼] 或 [識別碼] 時，會顯示此項目。<br>按下以自動生成與您在 [識別碼的最小位數] 內所選數位相同的 ID 編號。 |
| 部門 | 輸入可識別使用者的 40 個 Unicode (UTF-16) 格式字元的部門名稱等。<br>您可將此留白。 |
| 電子郵件位址 | 輸入 200 個 ASCII 格式字元的使用者電子郵件地址。這被用作 [掃描至我的電子郵件] 的目的地。<br>您可將此留白。 |
| 掃描至我的資料夾 | 在 [掃描至我的資料夾] > [設定類型] 內選取 [個別] 時，單獨輸入儲存目的地。有關設定項目的更多資訊，請參閱以下說明。<br>第138頁“設定 掃描至我的資料夾” |
| 限制 | 您可以限制每位使用者可使用的功能。選取您允許使用的功能。 |

| 項目 | 說明 |
|---|---|
| 預設 | 您可以從掃描器登錄的 預設 中，設定最多五項僅供所選使用者適用的預設值。<br>❏ 已分配給任何使用者的 預設 僅可由該使用者使用。未分配給任何使用者的 預設 可由所有使用者使用。<br>❏ 如果使用者僅有一個 預設 可用，它將在驗證後自動載入。如果多個 預設 可用，驗證後會顯示 預設 清單。<br>❏ 您無法建立或顯示使用 [限制] 內所限制功能的 預設。 |

## 使用 CSV 檔案登錄多個 使用者設定 (Web Config)

在 CSV 檔案中為每位使用者輸入設定，並整批登錄他們。

### 建立 CSV 檔案

建立要匯入 使用者設定 的 CSV 檔案。

附註：
如果預先登錄一個或多個 使用者設定，然後匯出格式化檔案（CSV 檔案），可以使用登錄的設定作為參考來輸入設定項目。

1. 存取 Web Config 並選取 [產品安全性] 索引標籤 > [使用者設定]。
2. 按下 [匯出]。
3. 為 [檔案格式] 選取檔案格式。

   參閱以下內容進行選取。

| 項目 | 說明 |
|---|---|
| CSV UTF-16 (Tab 鍵分隔) | 使用 Microsoft Excel 編輯檔案時進行選取。<br>每個參數均以「[ ]」（括號）括住。在「[ ]」中輸入參數。<br>更新檔案時，建議覆寫檔案。如果新儲存檔案，請為檔案格式選取 Unicode 文字 (*.txt)。 |
| CSV UTF-8 (逗號分隔) | 使用 文字編輯器或巨集而非 Microsoft Excel 編輯檔案時進行選取。 |
| CSV UTF-8 (分號分隔) | |

4. 按下 [匯出]。
5. 在試算表應用程式（例如 Microsoft Excel）或文字編輯器中編輯和儲存此 CSV 檔案。

> **重要事項：**
> 編輯檔案時，請勿變更編碼和標題資訊。

## CSV 檔案設定項目

| 項目 | 設定與說明 |
|---|---|
| UserID | 輸入要使用驗證的使用者 ID，為 1 至 83 個 Unicode 格式位元組。 |
| UserName | 輸入掃描器控制面板上顯示的使用者名稱，為 32 個 Unicode 格式字元。您可將此留白。 |
| Password | 輸入使用驗證所需的密碼，為 32 個 ASCII 格式字元。匯入時，可以將此設為密碼，而不是 [EncPassword]。<br>如果為 [如何驗證使用者] 選取 [使用者 ID]，則將此留白。<br>匯出時，必須將此留白。 |
| AuthenticationCardID | 設定驗證卡的讀取結果。如果在 [驗證設定] 內允許 [允許使用者登錄驗證卡]，則將體現使用者登錄的結果。<br>輸入 116 個以內的 ASCII 格式字元。您可將此留白。 |
| IDNumber | 當在 [驗證設定] > [如何驗證使用者] 中選取 [卡片或識別碼] 或 [識別碼] 時，會顯示此項目。<br>輸入在 [驗證設定] > [識別碼的最小位數] 中設定的數值之間的某個數字，最多 8 位數。<br>ID 編碼不可重複。若有重複，您會在匯入檔案時收到該錯誤提示。留白時，系統會自動指派一個編號。 |
| Department | 輸入任意部門名稱以區分使用者。<br>輸入 Unicode 格式 40 個字元以內的值。您可將此留白。 |
| MailAddress | 為使用者設定電子郵件位址。這被用作 [掃描至我的電子郵件] 的目的地。<br>您可以使用 A-Z、a-z、0-9、!#’%&’*+-./=?^_{|}~@。輸入不超過 200 個字元。不得使用「,」（逗號）作為第一個字元。您可將此留白。 |
| FolderProtocol | 設定 掃描至我的資料夾 功能類型。<br>網路資料夾/FTP (SMB)：0，FTP：1 |
| FolderPath | 設定 掃描至我的資料夾 功能的儲存目的地。 |
| FolderUserName | 設定 掃描至我的資料夾 功能的使用者名稱。 |
| FolderPassword | 設定 32 個 ASCII 字元以內的密碼，以驗證 掃描至我的資料夾 功能的目的地資料夾。<br>匯入時，可以將此設為密碼，而不是 [EncPassword]。匯出時，必須將此留白。 |
| FtpPassive | 選取 [FTP] 作為 掃描至我的資料夾 功能的 [類型] 時，設定 FTP 伺服器的連線模式。<br>主動模式：0，被動模式：1 |
| FtpPort | 選取 [FTP] 作為 掃描至我的資料夾 功能的 [類型] 時，設定將已掃描資料傳送至 FTP 伺服器的連接埠號碼，範圍介於 0 至 65535 之間。 |
| ScanToMemory | 設定 掃描至 USB 隨身碟 的限制。<br>不允許：0，允許：1 |
| ScanToMail | 設定 掃描至電子郵件 的限制。<br>僅在 [掃描至電子郵件] 已啟用時才可設定 [掃描至我的電子郵件]。<br>不允許：0，允許：1 |

| 項目 | 設定與說明 |
|---|---|
| ScanToFolder | 設定 掃描至網路資料夾/FTP 的限制。<br>僅在 [掃描至網路資料夾/FTP] 已啟用時才可設定 [掃描至我的資料夾]。<br>不允許：0，允許：1 |
| ScanToCloud | 設定 掃描至雲端 的限制。<br>不允許：0，允許：1 |
| ScanToComputer | 設定 掃描至電腦 的限制。<br>不允許：0，允許：1 |
| PresetIndex | 設定要和使用者建立關聯的 預設。您最多可以設定五個 預設 登錄編號，並以逗號區隔。 |
| EncPassword | 匯出使用者設定時，為 [Password] 設定的參數會被加密，相應的值採用 BASE64 進行編碼並被匯出。<br>為 [Password] 匯入新密碼時，此值被忽略。<br>如果 [Password] 為空白，此值將被使用，密碼保持與匯出前相同。 |
| EncFolderPassword | 匯出時，為 [FolderPassword] 設定的參數會被加密，相應的值採用 BASE64 進行編碼並被匯出。<br>為 [FolderPassword] 匯入新密碼時，此值被忽略。<br>如果 [FolderPassword] 為空白，此值將被使用，密碼保持與匯出前相同。 |

### 匯入 CSV 檔案

1. 存取 Web Config 並選取 [產品安全性] 索引標籤 > [使用者設定]。
2. 按下 [匯入]。
3. 選擇您要匯入的檔案。
4. 按下 [匯入]。
5. 檢查顯示的資訊後，按下 [確定]。

## 整批登錄 使用者設定 至多個掃描器 (Epson Device Admin)

您可以使用 LDAP 伺服器或 CSV/ENE 檔案整批登錄 本機 DB 內使用的 使用者設定。

附註：
ENE 檔案是 Epson 提供的二進制檔案，可加密和儲存 [聯絡人] 資訊，例如個人資訊和 使用者設定。可從 Epson Device Admin 將其匯出並設定密碼。如果您要從備份檔案匯入 使用者設定，它十分有用。

### 從 CSV/ENE 檔案匯入

1. 從設定範本中選取 [管理員設定] > [驗證設定] > [使用者設定]。
2. 按下 [匯入]。

3. 從 [匯入來源] 中選取 [CSV 或 ENE 檔案]。
4. 按下 [瀏覽]。

   檔案選取畫面會隨即顯示。
5. 選擇您要匯入的工作檔案以將其開啟。
6. 選取匯入方法。

   ❏ 覆寫與新增：如果存在相同的使用者 ID，則複寫；如果不存在，則新增 ID。

   ❏ 全部取代：使用要匯入的使用者設定替換所有內容。
7. 按下 [匯入]。

   設定確認畫面會隨即顯示。
8. 按下 [確定]。

   顯示驗證結果。

   附註：

   ❏ 如果匯入的使用者設定數量超過可以匯入的數量，會有一條訊息提示刪除一些使用者設定。匯入前刪除任何過量的使用者設定。

   ❏ 匯入前選取要刪除的使用者設定，然後按下 [刪除]。
9. 按下 [匯入]。

   使用者設定匯入設定範本。

### 從檔案或 LDAP 伺服器匯入

1. 從設定範本中選取 [管理員設定] > [驗證設定] > [使用者設定]。
2. 按下 [匯入]。
3. 從 [匯入來源] 中選取 [LDAP]。
4. 按下 [設定]。

   [LDAP 伺服器] 設定會隨即顯示。

   附註：

   此 LDAP 伺服器設定用於從 LDAP 伺服器匯入使用者設定。匯入的（複製的）使用者設定透過使用掃描器自行驗證使用者。

   另外，當選取 [LDAP] 或 [本機資料庫和 LDAP] 作為驗證方式時，使用者透過與 LDAP 伺服器通訊進行驗證。
5. 設定每個項目。

   從 LDAP 伺服器匯入使用者設定時，除了 LDAP 設定之外，您也可以組態下列設定。

   對於其他項目，請參考「相關資訊」。

| 項目 | | 說明 |
|---|---|---|
| LDAP 伺服器設定 | LDAP 伺服器類型 | 允許您選取 LDAP 伺服器的類型。 |

| 項目 | | | 說明 |
|---|---|---|---|
| 搜尋設定 | 搜尋篩選條件 | | 您可以設定用於 LDAP 搜尋篩選器的文字。選取 [自訂] 以編輯搜尋文字。 |
| | 選項 | 類型 | 您可以設定 [掃描至我的資料夾] 的儲存目的地類型。 |
| | | 連線模式 | 當 [類型] 設定為 [FTP] 時，您可以設定 FTP 連接模式。 |
| | | 連接埠號 | 當 [類型] 設定為 [FTP] 時，您可以設定要使用的連接埠編號。 |

6. 視需要按下 [連線測試] 執行連線測試。
   從 LDAP 伺服器擷取和顯示 10 個使用者設定。
7. 按下 [確定]。
8. 選取匯入方法。
   - ❏ 覆寫與新增：如果存在相同的使用者 ID，則複寫；如果不存在，則新增 ID。
   - ❏ 全部取代：使用要匯入的使用者設定替換所有內容。
9. 按下 [匯入]。
   設定確認畫面會隨即顯示。
10. 按下 [確定]。
    顯示驗證結果。
11. 按下 [匯入]。
    使用者設定匯入設定範本。

**相關資訊**

➡ 第135頁 “配置 LDAP 伺服器”
➡ 第136頁 “進行 LDAP 伺服器搜尋設定”

# 與 LDAP 伺服器 同步

為掃描器進行 LDAP 伺服器 設定。

視需要對主伺服器和次伺服器進行設定。

附註：
[LDAP 伺服器] 設定與 [聯絡人] 共用。

## 可用服務

以下為支援的目錄服務。

| 服務名稱 | 版本 |
|---|---|
| Active Directory | Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 |
| OpenLDAP | Ver.2.3, Ver.2.4 |

## 配置 LDAP 伺服器

若要使用 LDAP 伺服器，您必須配置 LDAP 伺服器。

**在從 Web Config 進行設定時：**

選取 [網路] 索引標籤 > [LDAP 伺服器] > [基本 (主要伺服器)] 或 [基本 (次要伺服器)]。

如果您選取 [Kerberos 驗證] 作為 [驗證方法]，請選取 [網路] > [Kerberos 設定] 以進行 Kerberos 設定。

**在從 Epson Device Admin 進行設定時：**

從配置範本中選取 [網路] > [LDAP 伺服器] > [伺服器設定 (主要伺服器)] 或 [伺服器設定 (次要伺服器)]。

如果您選取 [Kerberos 驗證] 作為 [驗證方法]，請選取 [網路] — [加密] > [Kerberos 設定] 以進行 Kerberos 設定。

| 項目 | 設定與說明 |
|---|---|
| 使用 LDAP 伺服器 | 選取 [使用] 或 [不使用]。 |
| LDAP 伺服器位址 | 輸入 LDAP 伺服器位址。輸入 1 至 255 個字元的 IPv4、IPv6 或 FQDN 格式。對於 FQDN 格式，除位址開頭和結尾外，您可使用 ASCII (0x20—0x7E) 英數字元及連字符。 |
| LDAP 伺服器連接埠號碼 (連接埠號) | 輸入 LDAP 伺服器連接埠號碼 (1 至 65535 之間的數字)。 |
| 安全連線 | 指定掃描器存取 LDAP 伺服器的驗證方式。<br>若您選取 [無]，則通訊未加密。我們建議將此設定為 [無] 以外的其他內容。 |
| 憑證驗證 | LDAP 伺服器的證書在此啟用後被驗證。我們建議將此設定為 [開啓]。<br>若要設定，需要將 [CA 憑證] 匯入掃描器。 |
| 搜尋逾時 (秒) | 設定逾時發生前的搜尋時間長度，介於 5 至 300 秒之間。 |
| 驗證方法 | 選擇驗證方法。<br>當您選取 [簡易驗證] 時，我們建議設定 [安全連線] 為 [無] 以外的其他內容。<br>如果您選取 [Kerberos 驗證]，請預先為 Kerberos 進行設定。<br>若要執行 Kerberos 驗證，需具備以下環境。<br>❏ 掃描器和 DNS 伺服器可以進行通訊。<br>❏ 掃描器、KDC 伺服器和驗證所需的伺服器（LDAP 伺服器、SMTP 伺服器、檔案伺服器）的時間均同步。<br>❏ 將服務伺服器指派為 IP 位址時，服務伺服器的 FQDN 即會登錄在 DNS 伺服器反向對應區域中。 |
| 要使用的 Kerberos 領域 | 如果您針對 [驗證方法] 選取 [Kerberos 驗證]，請選取要使用的 Kerberos 範圍。 |
| 管理員 DN / 使用者名稱 | 以 Unicode (UTF-8) 格式輸入 LDAP 伺服器的使用者名稱，長度不得超過 128 個字元。您無法使用控制字元，如 0x00 至 0x1F 和 0x7F。在選取 [匿名驗證] 作為 [驗證方法] 時，不會使用此設定。如果您不想指定此項目，請將其保留空白。 |

| 項目 | 設定與說明 |
|---|---|
| 密碼 | 以 Unicode (UTF-8) 格式輸入 LDAP 伺服器驗證的密碼，長度不得超過 128 個字元。您無法使用控制字元，如 0x00 至 0x1F 和 0x7F。在選取 [匿名驗證] 作為 [驗證方法] 時，不會使用此設定。如果您不想指定此項目，請將其保留空白。 |

### Kerberos 設定

如果您選取 [Kerberos 驗證] 作為 [驗證方法]，則需進行 Kerberos 設定。您最多可登錄 10 組 Kerberos 設定。

**從 Web Config 進行設定時：**

選取 [網路] 索引標籤 > [Kerberos 設定]。

**從 Epson Device Admin 進行設定時：**

從設定範本中選取 [網路] > [加密] > [Kerberos 設定]。

| 項目 | 設定與說明 |
|---|---|
| 領域 (網域) | 輸入不超過 255 個 ASCII (0x20—0x7E) 字元的 Kerberos 驗證範圍。如果您不想登錄此項目，請將其保留空白。 |
| KDC 位址 | 輸入 Kerberos 驗證伺服器的位址。輸入不超過 255 個 IPv4、IPv6 或 FQDN 格式的字元。如果您不想登錄此項目，請將其保留空白。 |
| 連接埠號碼 (Kerberos) | 輸入 Kerberos 伺服器連接埠號碼（1 至 65535 之間的數字）。 |

## 進行 LDAP 伺服器搜尋設定

設定使用者設定的搜尋屬性。

**從 Web Config 進行設定時：**

選取 [網路] 索引標籤 > [LDAP 伺服器] > [搜尋設定 (驗證)]。

**從 Epson Device Admin 進行設定時：**

從設定範本中選取 [管理員設定] > [驗證設定] > [LDAP 伺服器] > [搜尋設定 (驗證)]。

| 項目 | 設定與說明 |
|---|---|
| 搜尋基礎 (辨別名稱) | 從 LDAP 伺服器搜尋使用者資訊時，指定開始位置。輸入 0 至 128 個 Unicode (UTF-8) 字元。若不搜尋任意屬性，請保留空白。<br>本機伺服器目錄的範例：dc=server、dc=local |
| 使用者 ID 屬性 | 指定搜尋 ID 編碼時要顯示的屬性名稱。最多輸入 1 至 255 個 ASCII 字元。第一個字元必須是 a—z 或 A—Z。<br>範例：cn、uid |
| 使用者名稱顯示屬性 | 指定要顯示為使用者名稱的屬性名稱。最多輸入 0 至 255 個 ASCII 字元。第一個字元必須是 a—z 或 A—Z。您可將此留為空白。<br>範例：cn、name |
| 驗證卡 ID 屬性 | 指定要顯示為驗證卡 ID 的屬性名稱。最多輸入 0 至 255 個 ASCII 字元。第一個字元必須是 a—z 或 A—Z。您可將此留為空白。<br>範例：cn、sn |

| 項目 | 設定與說明 |
|---|---|
| ID 號碼屬性 | 指定搜尋 ID 編碼時要顯示的屬性名稱。最多輸入 1 至 255 個 ASCII 字元。第一個字元必須是 a—z 或 A—Z。<br>範例：cn、id |
| 部門屬性 | 指定要顯示為部門名稱的屬性名稱。最多輸入 0 至 255 個 ASCII 字元。第一個字元必須是 a—z 或 A—Z。您可將此留為空白。<br>範例：ou、ou-cl |
| 電子郵件屬性 | 指定搜尋電子郵件地址時要顯示的屬性名稱。最多輸入 1 至 255 個 ASCII 字元。第一個字元必須是 a—z 或 A—Z。<br>範例：mail |
| 儲存至屬性 | 指定指向 掃描至我的資料夾 目的地的屬性名稱。最多輸入 0 至 255 個 ASCII 字元。<br>例如：homeDirectory |

## 檢查 LDAP 伺服器連線

使用 [LDAP 伺服器] > [搜尋設定] 上所設定的參數對 LDAP 伺服器執行連線測試。

1. 存取 Web Config 並選取 [網路] 索引標籤 > [LDAP 伺服器] > [連線測試]。
2. 選取 [開始]。
   連線測試會隨即啟動。完成測試後，會顯示檢查報告。

### LDAP 伺服器連線測試參考

| 訊息 | 說明 |
|---|---|
| 連線測試成功。 | 成功建立與伺服器的連線時會顯示此訊息。 |
| 連線測試失敗。<br>檢查設定。 | 下列原因會顯示此訊息：<br>❏ LDAP 伺服器位址或連接埠號碼不正確。<br>❏ 發生逾時。<br>❏ 已選取 [不使用] 作為 [使用 LDAP 伺服器]。<br>❏ 如果已選取 [Kerberos 驗證] 作為 [驗證方法]，如 [領域 (網域)], [KDC 位址] 與 [連接埠號碼 (Kerberos)] 等設定不正確。 |
| 連線測試失敗。<br>在您的產品或伺服器上檢查日期與時間。 | 由於掃描器與 LDAP 伺服器的時間設定不一致而導致連線失敗時，會顯示此訊息。 |
| 驗證失敗。<br>檢查設定。 | 下列原因會顯示此訊息：<br>❏ [使用者名稱] 及/或 [密碼] 不正確。<br>❏ 如果已選取 [Kerberos 驗證] 作為 [驗證方法]，可能未配置時間/日期。 |
| 程序未完成前，您無法存取產品。 | 掃描器忙碌時會顯示此訊息。 |

# 設定電子郵件伺服器

當您使用 [掃描至我的電子郵件] 時，設定電子郵件伺服器。

附註：
僅在 [掃描至電子郵件] 已啟用時才可設定 [掃描至我的電子郵件]。

**從 Web Config 進行設定時：**

選取 [網路] 索引標籤 > [電子郵件伺服器] > [基本]。

**從 Epson Device Admin 進行設定時：**

從設定範本中選取 [常用] > [電子郵件伺服器] > [郵件伺服器設定]。

| 項目 | 設定與說明 | |
|---|---|---|
| 驗證方法 | 指定掃描器存取郵件伺服器的驗證方式。 | |
| | 關閉 | 與郵件伺服器進行通訊時驗證功能會停用。 |
| | SMTP驗證 | 電子郵件伺服器需支援 SMTP 驗證。 |
| | 以POP驗證取代SMTP | 當您選取此項目時，請設定 POP3 伺服器。 |
| 已驗證帳戶 | 如果您選取 [SMTP驗證] 或 [以POP驗證取代SMTP] 作為 [驗證方法]，請輸入驗證的帳戶名稱。輸入 0 至 255 個 ASCII (0x20—0x7E) 字元。 | |
| 已驗證密碼 | 如果您選取 [SMTP驗證] 或 [以POP驗證取代SMTP] 作為 [驗證方法]，請輸入驗證的密碼。輸入 0 至 20 個 ASCII (0x20—0x7E) 字元。 | |
| 寄件者的電子郵件位址 | 輸入寄件者的電子郵件地址。輸入介於 0 和 255 個之間的 ASCII (0x20—0x7E) 字元，不包括 : ( ) < > [ ] ; ¥。句點「.」不可當作第一個字元。 | |
| SMTP伺服器位址 | 輸入 0 至 255 個字元，可以使用 A—Z a—z 0—9 .-。您可以使用 IPv4 或 FQDN 格式。 | |
| SMTP伺服器連接埠號碼 | 輸入介於 1 至 65535 的數字。 | |
| 安全連線 | 指定電子郵件伺服器的安全連線方法。 | |
| | 無 | 若您在 [驗證方法] 中選取了 [以POP驗證取代SMTP]，連線方法則會設定為 [無]。 |
| | SSL/TLS | 此功能在 [驗證方法] 設定為 [關閉] 或 [SMTP驗證] 時即可使用。 |
| | STARTTLS | 此功能在 [驗證方法] 設定為 [關閉] 或 [SMTP驗證] 時即可使用。 |
| 憑證驗證 | 若啟用此功能，憑證即被驗證。推薦將此設定為 [開啓]。 | |
| POP3伺服器位址 | 如果您選取 [以POP驗證取代SMTP] 作為 [驗證方法]，請輸入 POP3 伺服器地址。您可以輸入 0 至 255 個字元，可以使用 A—Z a—z 0—9。您可以使用 IPv4 或 FQDN 格式。 | |
| POP3伺服器連接埠號碼 | 如果您選取 [以POP驗證取代SMTP] 作為 [驗證方法]，請指定連接埠編號。輸入介於 1 至 65535 的數字。 | |

# 設定 掃描至我的資料夾

儲存影像至指派給每位使用者的資料夾。您可設定以下項目作為專用資料夾。

附註：
僅在 [掃描至網路資料夾/FTP] 已啟用時才可設定 [掃描至我的資料夾]。

| 儲存至設定 | 驗證方法 | 資料夾路徑設定位置 |
|---|---|---|
| 為整個 驗證設定 指定一個網路資料夾，以使用使用者 ID 名稱在指定資料夾下自動建立個人資料夾。 | ❏ 本機 DB<br>❏ LDAP<br>❏ 本機 DB 和 LDAP | 掃描器（掃描至我的資料夾 設定） |
| 單獨指派不同的網路資料夾給每位使用者。 | 本機 DB | 掃描器（使用者設定） |
| | LDAP | LDAP 屬性 |
| | 本機 DB 和 LDAP | 掃描器（使用者設定）或 LDAP 屬性 |

從 Web Config 進行設定時：

選取 [產品安全性] 索引標籤 > [掃描至網路資料夾/FTP]。

從 Epson Device Admin 進行設定時：

從設定範本中選取 [管理員設定] > [驗證設定] > [掃描至網路資料夾/FTP] > [掃描至我的資料夾]。

| 項目 | | 說明 |
|---|---|---|
| 儲存至設定 | 設定類型 | ❏ [共用]：<br>在 [儲存至] 中指定的資料夾路徑或 URL 下，自動建立根據使用者 ID 命名的資料夾，並將掃描影像儲存到此資料夾。<br>❏ [個別]：<br>針對每位使用者的掃描結果，設定儲存目的地。<br>本機 DB 使用者可以在使用者設定內設定。<br>LDAP 使用者使用從 LDAP 伺服器搜尋屬性擷取的儲存位置。 |
| | 類型 | 依據掃描輸出目的地選取傳送協議。<br>對於網路資料夾：[網路資料夾(SMB)]<br>對於 FTP 伺服器：[FTP] |
| | 儲存至 | 指定輸出路徑的路徑或 URL。<br>輸入 160 個以內的 Unicode (UTF-16) 字元。 |
| | 連線模式 | 在 [類型] 中選取 [FTP] 時設定。<br>選取 FTP 伺服器的連線模式。 |
| | 連接埠編號 | 在 [類型] 中選取 [FTP] 時設定。<br>輸入將掃描資料傳送至 FTP 伺服器的連接埠號碼，範圍介於 0 與 65535 之間。 |

| 項目 | | 說明 |
|---|---|---|
| 驗證設定 | 設定類型 | 當您在 [儲存至設定] 中選取 [個別] 作為 [設定類型] 時設定。<br>設定「使用者名稱」和「密碼」以存取資料夾。<br>❏ [共用]：<br>對所有使用者使用通用 [使用者名稱] 和 [密碼]。<br>❏ [個別]：<br>對於 本機 DB 使用者，在 [使用者設定] 內單獨設定 [使用者名稱] 和 [密碼]。LDAP 使用者無法單獨設定。由此項設定的 [使用者名稱] 和 [密碼] 在一批使用。 |
| | 使用者名稱 | 輸入用於存取掃描輸出目的地資料夾的使用者名稱。<br>輸入 30 個以內的 Unicode (UTF-16) 字元。當您使用 [共用] 或 LDAP 伺服器時設定此項。 |
| | 密碼 | 輸入 [使用者名稱] 對應的密碼。<br>輸入 20 個以內的 Unicode (UTF-16) 字元。當您使用 [共用] 或 LDAP 伺服器時設定此項。 |

## 禁止變更 掃描至網路資料夾/FTP 的目的地

| 項目 | 說明 |
|---|---|
| 禁止手動輸入目的地 | 啟用後，使用者無法變更預設目的地。 |

# 自訂單鍵功能

透過編輯主畫面上用於控制面板的圖示配置，您可只顯示所需的圖示。

**從 Web Config 進行設定時：**

選取 [產品安全性] 索引標籤 > [自訂單鍵功能]。

**從 Epson Device Admin 進行設定時：**

從設定範本中選取 [管理員設定] > [驗證設定] > [自訂單鍵功能]。

**附註：**
在下列情況下，指定功能的圖示不會顯示於主畫面。

❏ 選取因 [限制] 而不允許使用的功能時。

❏ 登入使用者的電子郵件地址未登錄時。(掃描至我的電子郵件)

❏ 目的地資料夾未設定時。(掃描至我的資料夾)

| 項目 | 說明 |
|---|---|
| 每個畫面的功能上限 | 選取要在控制面板上顯示的圖示配置。影像會根據所選配置而改變。 |
| 畫面 | 選擇页面數目。 |
| 編號 | 選擇要為每個編號位置顯示的功能。 |

# 使用 Epson Device Admin 的 工作歷史紀錄 報告

您可使用 Epson Device Admin 為每個群組和每個使用者建立 工作歷史紀錄 報告。您可以儲存最多 3,000 條使用記錄至掃描器。您透過指定期間或設定定期排程的方式建立報告。

若要將 工作歷史紀錄 輸出為報告，請從裝置列表畫面上的功能區選單中選取 [選項] > [Epson Print Admin Serverless/驗證 設定] > [管理 Epson Print Admin Serverless/驗證 相容裝置]。

關於如何建立使用者報告的詳細資訊，請參閱 Epson Device Admin 文件。

## 可包含於報告內的項目

您可以在使用者報告內輸出下列項目。

日期/工作 ID/操作/使用者 ID/部門/結果/結果詳細資訊/掃描：目的地類型/掃描：目的地/掃描：紙張大小/掃描：雙面/掃描：彩色/掃描：頁面/裝置：機型/裝置：IP 位址/裝置：序號/裝置：部門/裝置：位置/裝置：備註/裝置：附註

# 從控制面板以管理員身份登入

您可以使用下列任一方式從掃描器的控制面板以管理員身份登入。

1. 點選畫面最右側的 。
   - ❏ 當 驗證設定 啟用後，圖示會顯示在 [歡迎使用] 畫面上（驗證待機畫面）。
   - ❏ 當 驗證設定 停用後，圖示會顯示在主畫面上。
2. 當確認畫面顯示時，點選 [是]。
3. 輸入管理員的密碼。

   登入完成訊息隨即顯示，然後控制面板上的主畫面顯示。

若要登出，點選畫面最右側的 。

# 停用 驗證設定

您可使用 Web Config 停用 驗證設定。

附註：
儘管 驗證設定 被停用，登錄至掃描器的 使用者設定 將被儲存。可以透過復原掃描器至預設設定將它們刪除。

1. 存取 Web Config。
2. 選取 [產品安全性] 索引標籤 > [基本] > [驗證]。
3. 選取 [關閉]。
4. 按下 [下一步]。
5. 按下 [確定]。

附註：
即使停用 驗證設定，鎖定設定 依然保持啟用狀態。如果要將起停用，可以從控制面板或 Web Config 進行設定。

**相關資訊**

➡ 第82頁“從控制面板設定 鎖定設定”
➡ 第82頁“從 Web Config 設定 鎖定設定”

# 刪除 驗證設定 資訊 (回復至出廠預設值)

若要刪除 驗證設定 資訊（讀卡機、驗證方法、使用者設定 等等），復原所有掃描器設定至購買時的預設設定。

在控制面板上選取 [設定] > [系統管理] > [回復至出廠預設值] > [所有設定]。

**重要事項：**
所有聯絡人和其他網路設定都將被刪除。刪除的設定無法復原。

# 解決問題

## 無法讀取驗證卡

檢查下列內容。

❏ 請確認驗證裝置是否與掃描器正確連接。
連接驗證裝置至掃描器背部的外部界面 USB 連接埠。

❏ 確認驗證裝置和驗證卡是否受支援。

# 維護

清潔掃描器外部. . . . . 144

清潔掃描器內部. . . . . 144

更換滾輪組裝套件. . . . . .149

重設掃描次數. . . . . 154

省電. . . . . .154

搬運掃描器. . . . . 155

備份設定. . . . . 156

回復至出廠預設值. . . . . .157

更新應用程式與韌體. . . . . .157

# 清潔掃描器外部

用乾布或沾有溫和清潔劑和水的濕布擦拭外殼上的污漬。

**重要事項：**

- ❏ 切勿使用酒精、稀釋劑或任何腐蝕性溶劑清潔掃描器。否則可能出現變形或變色。
- ❏ 請勿讓水進入本產品內部。否則將導致發生故障。
- ❏ 切勿打開掃描器外殼。

1. 按下 ⏻ 鍵以關閉掃描器。
2. 拔下掃描器上的 AC 變壓器。
3. 使用沾有溫和清潔劑和水的濕布清潔外殼。

   **附註：**
   使用柔軟的乾布擦拭觸控式螢幕。

# 清潔掃描器內部

在使用一段時間的掃描器後，掃描器內部的滾輪或玻璃零件上的紙屑和室內灰塵，可能會造成進紙問題或掃描影像的品質問題。每掃描 5,000 次，對掃描器內部執行清潔。

您可以在控制面板或 Epson Scan 2 Utility 中檢查最新的掃描次數。

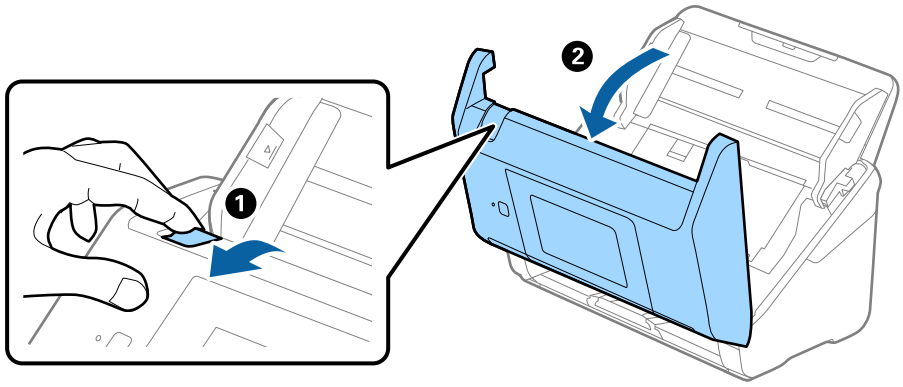
如果表面上沾染了難以去除的物質，請使用 Epson 原廠清潔套件來去除污漬。在清潔布上使用少量清潔劑，以清除污漬。

**重要事項：**

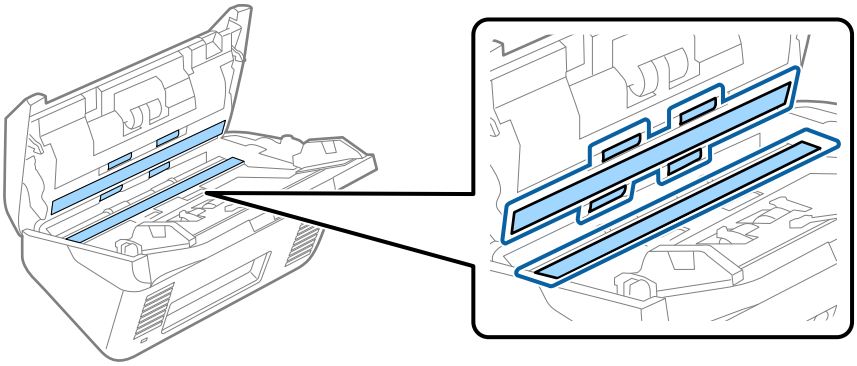
- ❏ 切勿使用酒精、稀釋劑或任何腐蝕性溶劑清潔掃描器。否則可能出現變形或變色。
- ❏ 切勿在掃描器上噴灑任何液體或潤滑劑。設備或電路損壞可能導致出現運行異常。
- ❏ 切勿打開掃描器外殼。

1. 按下 ⏻ 鍵以關閉掃描器。
2. 拔下掃描器上的 AC 變壓器。

3. 拉開控制桿，打開掃描器護蓋。



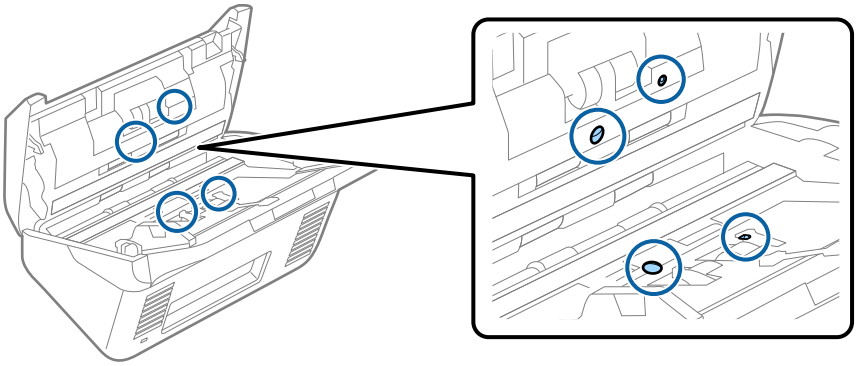

4. 使用軟布或 Epson 原廠清潔套件，擦淨掃描器護蓋底部內側的塑膠滾輪和玻璃表面上的污漬。



**重要事項：**

- ❏ 請勿大力按壓玻璃表面。
- ❏ 請勿使用刷子或硬質工具。玻璃上的劃痕可能影響掃描品質。
- ❏ 請勿在玻璃表面直接噴塗清潔劑。

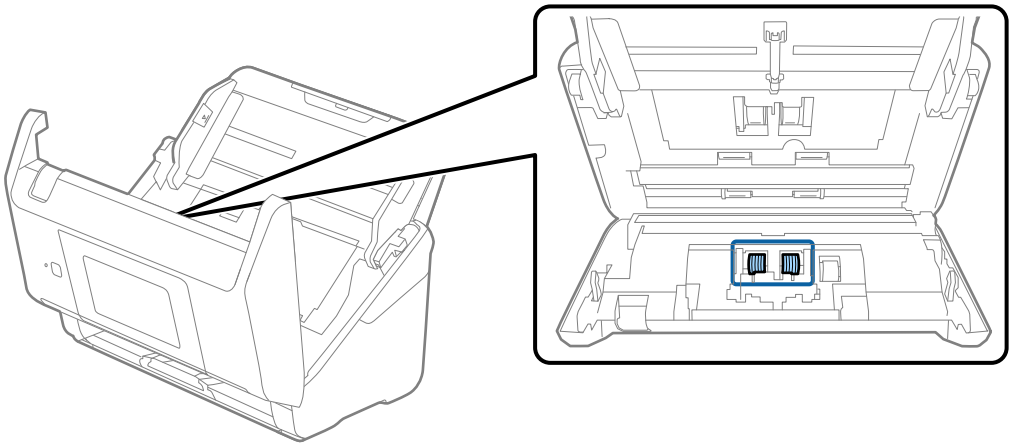
5. 使用棉花棒擦淨感應器上的污漬。



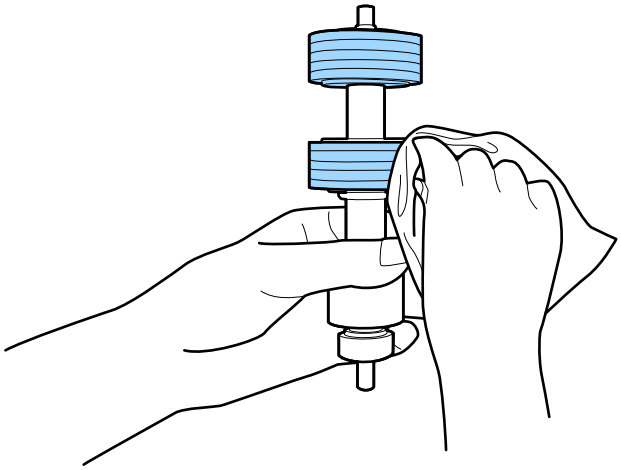
**重要事項：**

請勿在棉花棒上使用清潔劑之類的液體。

6. 打開護蓋，然後取出分紙滾輪。
   詳細資訊，請參考「更換滾輪組裝套件」。

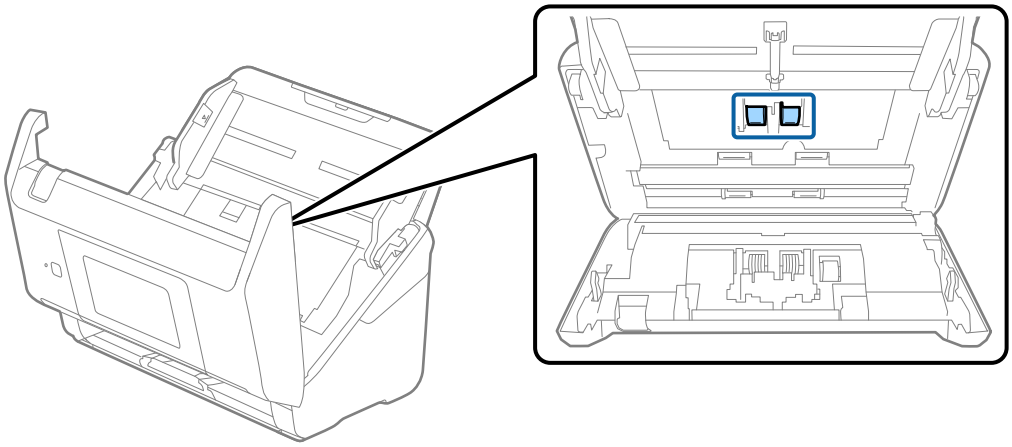


7. 使用 Epson 原廠清潔套件或沾濕的軟布擦除分紙滾輪上的灰塵。

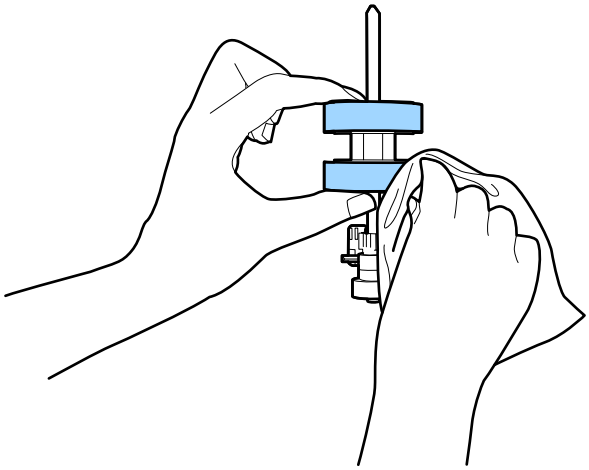


**重要事項：**
只能使用 Epson 原廠清潔套件或微濕的軟布清潔滾輪。使用乾軟布可能會導致滾輪表面損壞。

8. 打開護蓋，然後取出取紙滾輪。
   詳細資訊，請參考「更換滾輪組裝套件」。



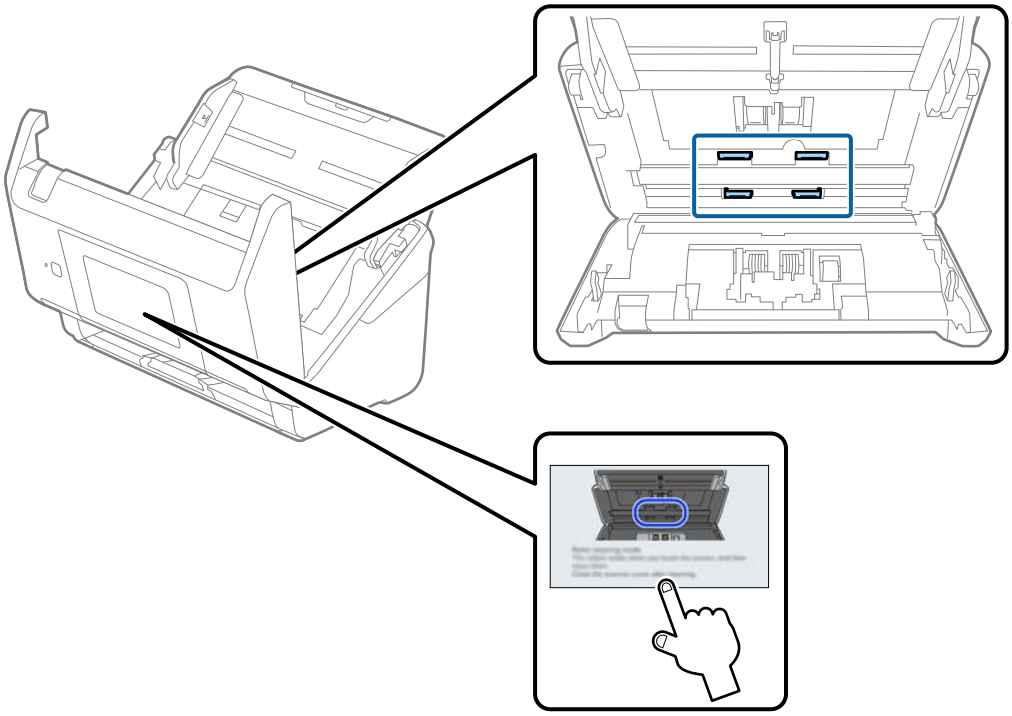
9. 使用 Epson 原廠清潔套件或沾濕的軟抹擦除取紙滾輪上的灰塵。



> **重要事項：**
> 只能使用 Epson 原廠清潔套件或微濕的軟布清潔滾輪。使用乾軟布可能會導致滾輪表面損壞。

10. 闔上掃描器護蓋。
11. 插入 AC 變壓器，然後開啟掃描器電源。
12. 從主畫面選取 [掃描器維護]。
13. 在 [掃描器維護] 畫面中，選取 [滾輪清潔]。
14. 拉開控制桿，打開掃描器護蓋。
    掃描器進入滾輪清潔模式。

15. 點選 LCD 上的任意位置，緩慢滾動底部的滾輪。使用 Epson 原廠清潔套件或沾水的軟布擦拭滾輪表面。重複此動作，直到滾輪清潔為止。



> **注意：**
> 操作滾輪時請小心，不要讓手或頭髮卡入機械裝置中。否則可能導致受傷。

16. 闔上掃描器護蓋。

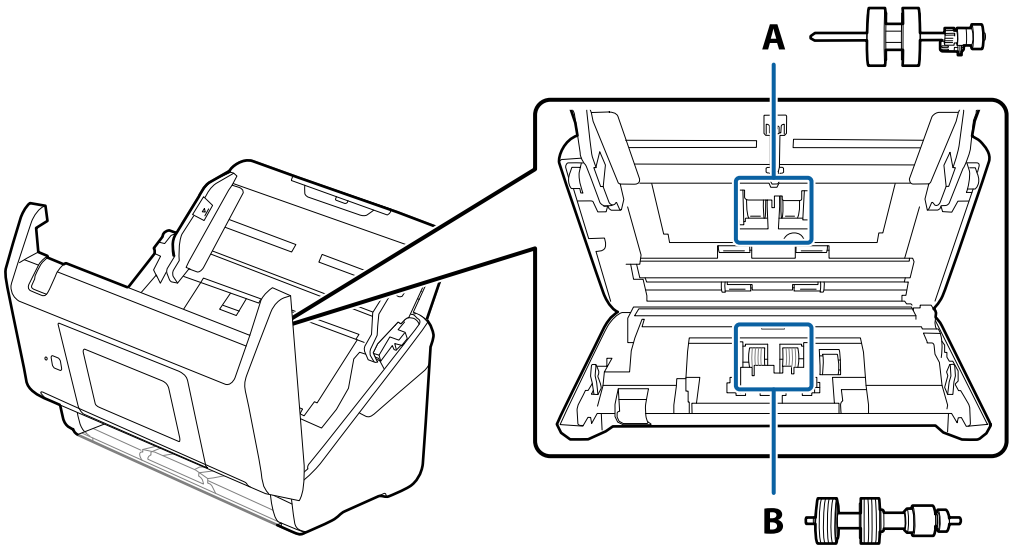
    掃描器退出滾輪清潔模式。

**相關資訊**

➡ 第149頁“更換滾輪組裝套件”

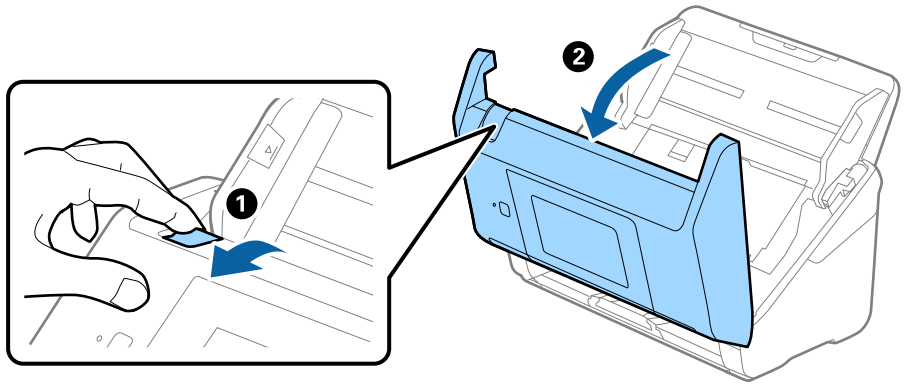
# 更換滾輪組裝套件

當掃描次數超出滾輪的使用壽命時，需要更換滾輪組裝套件（取紙滾輪和分紙滾輪）。當控制面板或電腦畫面上顯示更換訊息時，請依照以下步驟執行更換。

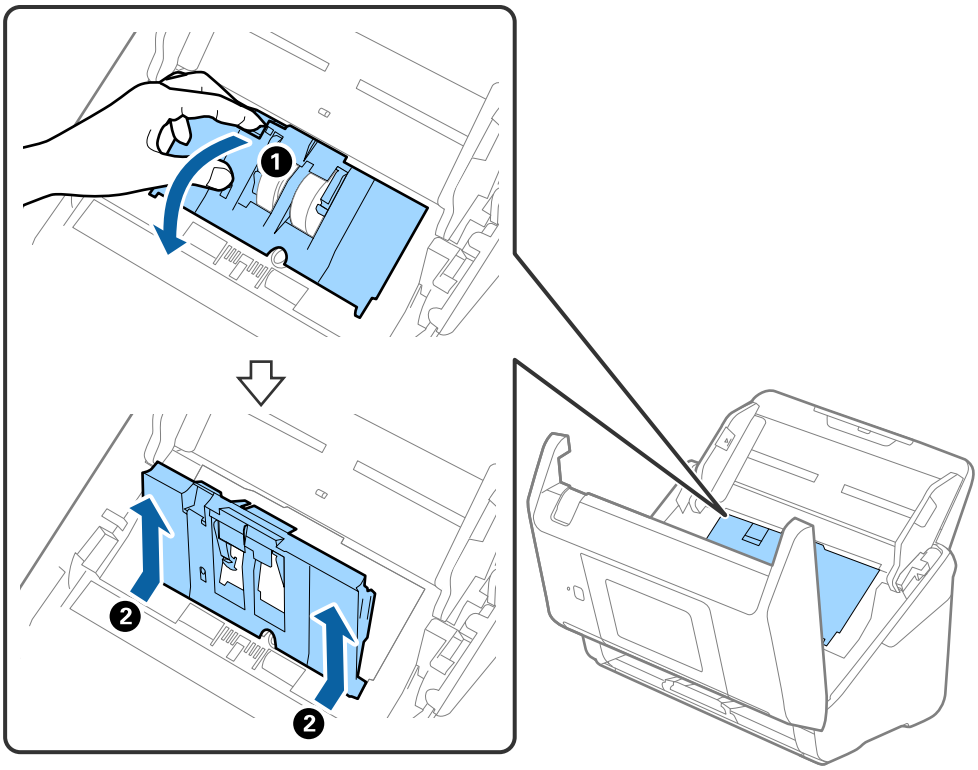



A：取紙滾輪，B：分紙滾輪

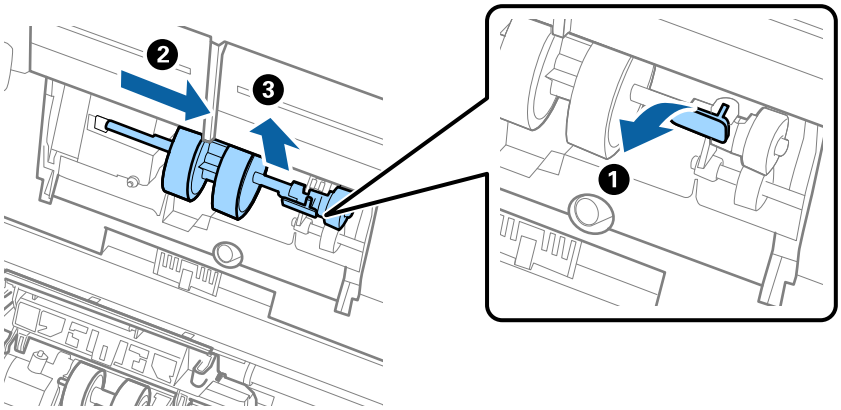
1. 按下 ⏻ 鍵以關閉掃描器。
2. 拔下掃描器上的 AC 變壓器。
3. 拉開控制桿，打開掃描器護蓋。



4. 打開取紙滾輪護蓋，然後滑動並取出護蓋。



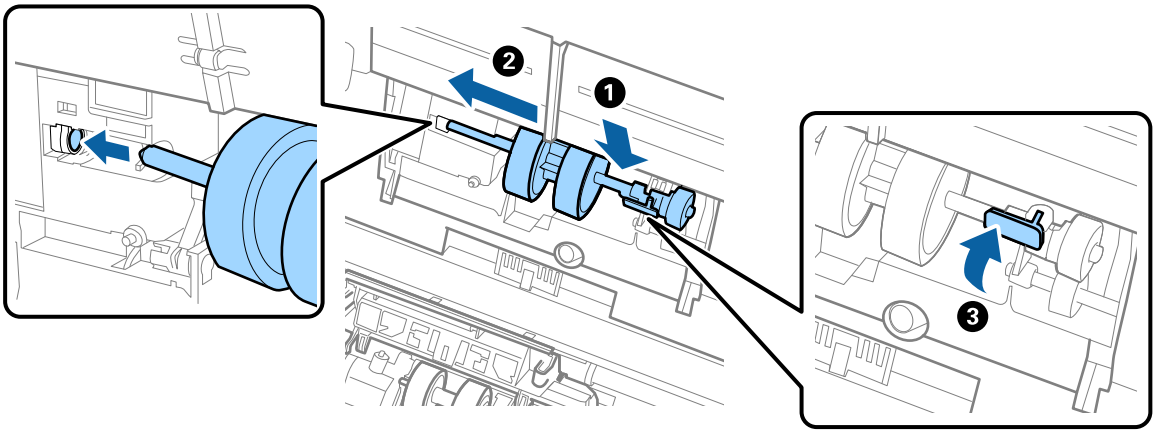
5. 拉下滾輪轉軸上的固定裝置，然後滑動並取出先前安裝的進紙滾輪。



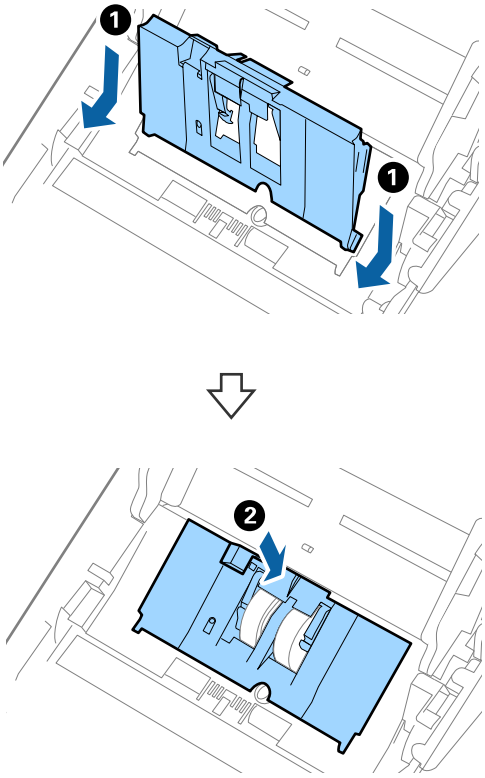
**重要事項：**

請勿用蠻力拉出取紙滾輪。否則可能損壞掃描器內側。

6. 按住固定裝置的同時，將新的取紙滾輪滑至左側，並插入掃描器的凹槽內。按下固定裝置以將其固定。

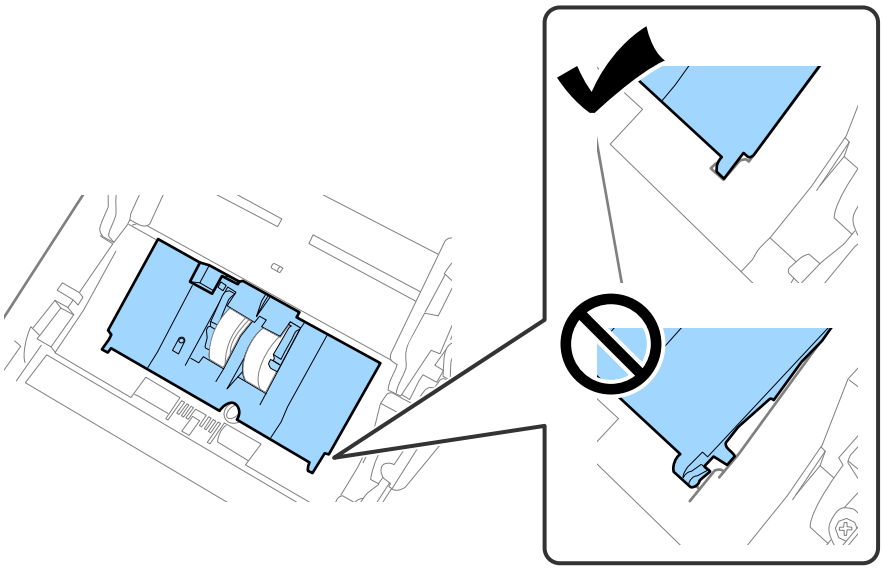



7. 將取紙滾輪護蓋邊緣放入溝槽中並滑動。闔緊護蓋。

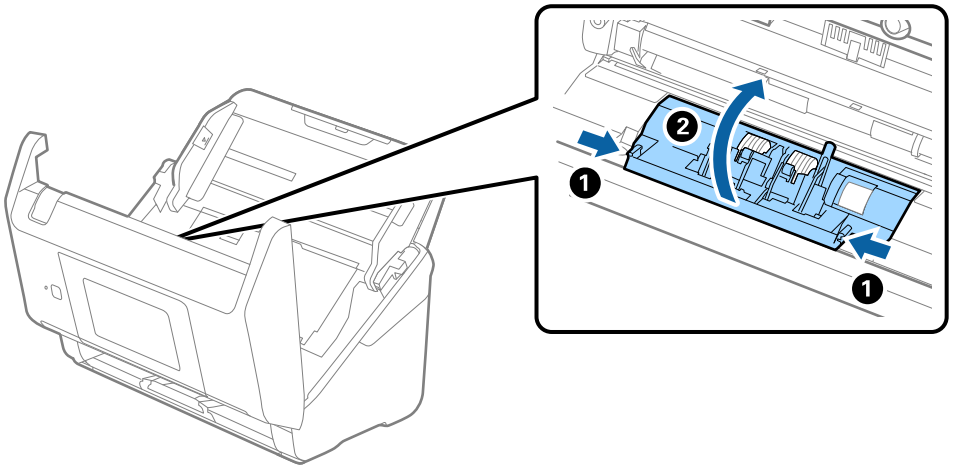


**重要事項：**

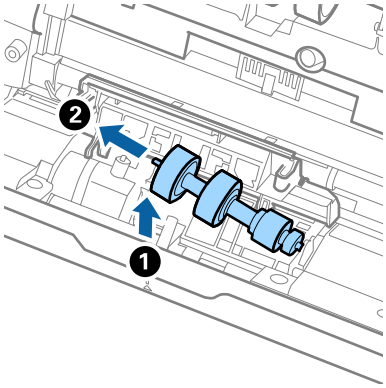
- ❏ 確定取紙滾輪護蓋已正確闔上。
- ❏ 如果護蓋無法闔上，請確保取紙滾輪已正確安裝。
- ❏ 如果其處於抬起位置，請勿安裝護蓋。



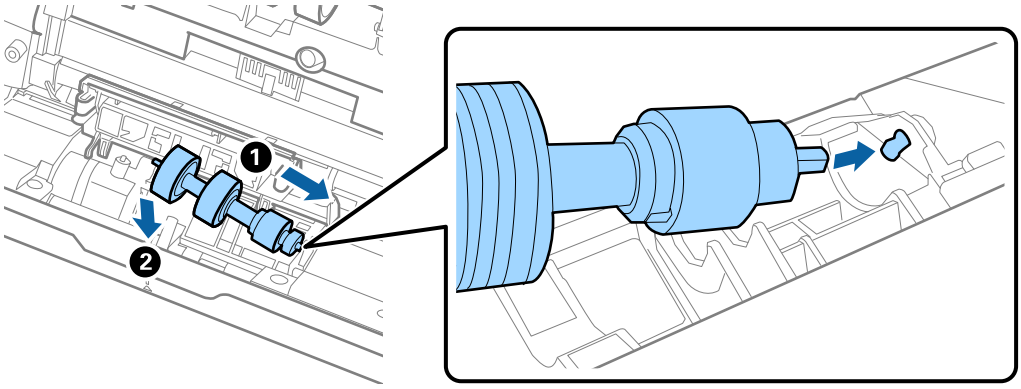
8. 按住分紙滾輪護蓋兩端的卡榫即可打開護蓋。



9. 抬起分紙滾輪的左側，然後滑動並取出先前安裝的分紙滾輪。



10. 將新的分紙滾輪轉軸插入右側的凹槽，然後放下滾輪。



11. 闔上分紙滾輪護蓋。

> **重要事項：**
> 如果護蓋很難蓋上，請確定分紙滾輪安裝正確。

12. 闔上掃描器護蓋。

13. 插入 AC 變壓器，然後開啟掃描器電源。

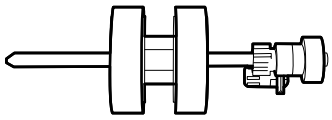
14. 在控制面板上重設掃描次數。

附註：
棄置取紙滾輪和分紙滾輪時，請遵守當地主管機關的規定及法規。請勿自行拆解。

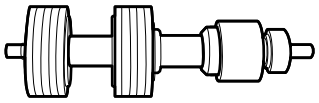
## 滾輪組裝套件代碼

當掃描次數超過使用壽命時，應更換零件 (取紙滾輪和分紙滾輪)。您可以在控制面板或 Epson Scan 2 Utility 中檢查最新的掃描次數。

**A**



**B**



A：取紙滾輪，B：分紙滾輪

| 零件名稱 | 代碼 | 壽命週期 |
|---|---|---|
| 滾輪組裝套件 | B12B819671<br>B12B819681 (僅限印度) | 200,000* |

* 此數字是透過連續使用 Epson 測試原稿樣張掃描所取得，且僅供更換週期參考。更換週期可能會因不同的紙張種類而異，如可能產生大量紙屑或表面較粗糙的紙，將縮短生命週期。

# 重設掃描次數

更換輥組裝套件後重置掃描次數。

1. 從主畫面選取 [設定] > [裝置資訊] > [重設掃描次數] > [更換滾輪後的掃描次數]。
2. 點選 [是]。

**相關資訊**

➡ 第149頁 “更換滾輪組裝套件”

# 省電

當掃描器未執行操作時，您可以透過睡眠模式或自動關機模式來省電。您可以設定掃描器進入睡眠模式和自動關機前的時間週期。提高任何數值都會影響印表機的能源效率。請在進行任何變更前考慮環境。

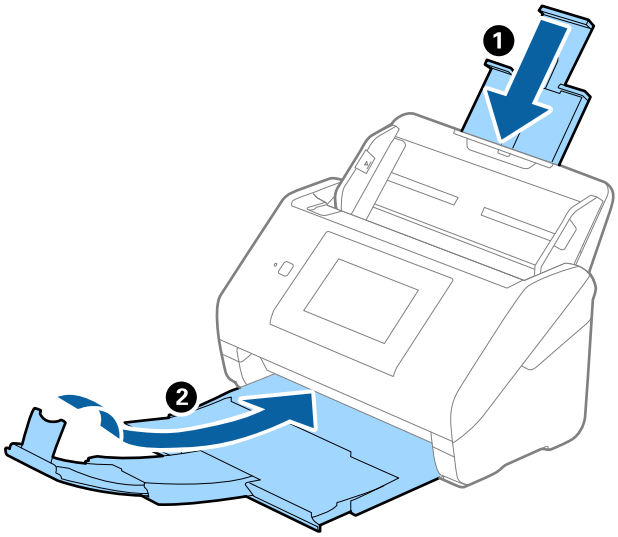
1. 從主畫面選取 [設定]。
2. 選取 [基本設定]。
3. 選取 [電源關閉設定]，然後進行設定。

   **附註：**
   可用功能可能隨購買地點而不同。

# 搬運掃描器

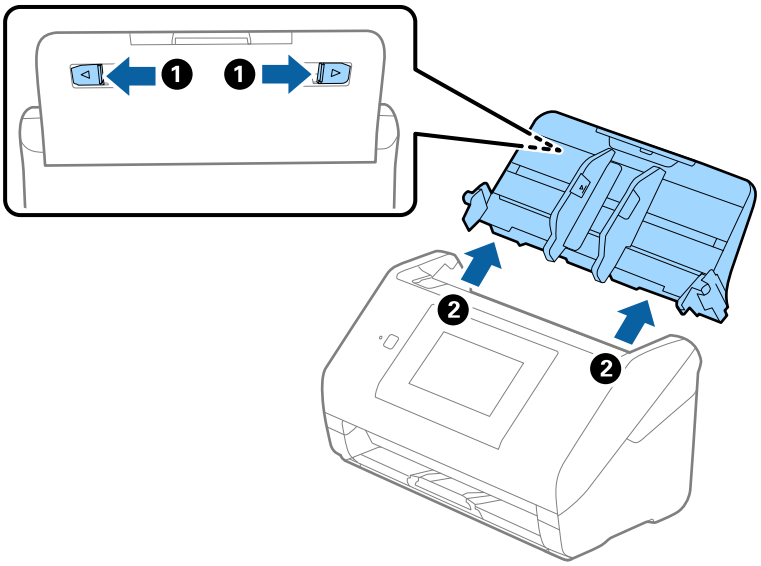
當您需要搬運掃描器以移動或進行維修時，請遵循以下步驟包裝掃描器。

1. 按下 ⏻ 鍵以關閉掃描器。
2. 拔下 AC 變壓器。
3. 拔下連接線與裝置。
4. 闔上延伸進紙托盤和出紙托盤。




> **重要事項：**
> 務必妥善闔上出紙托盤；否則在搬運過程中可能會受到損壞。

5. 移除進紙托盤。



6. 裝上掃描器隨附的包裝材料，然後將其重新裝入原包裝箱或堅固的箱子內。

# 備份設定

您可以將從 Web Config 設定的設定值匯出至檔案。您可以將其用於備份聯絡人、設定值、更換掃描器等。

由於匯出為二進位檔案，所以匯出的檔案無法進行編輯。

## 匯出設定

匯出掃描器的設定。

1. 存取 Web Config，然後選取 [裝置管理] 索引標籤 > [匯出與匯入設定值] > [匯出]。
2. 選取您要匯出的設定值。

   選取您要匯出的設定值。若您選取父系類別，子類別也會選取。但是，無法選取在相同網路中重複 (如 IP 位址等) 而導致錯誤的子類別。
3. 輸入密碼以加密匯出檔案。

   您需要密碼才可匯出檔案。若您不想要加密檔案，則請留白。
4. 按下 [匯出]。

   **重要事項：**

   若您要匯出掃描器的網路設定，如裝置名稱和 IPv6 位址，請選取 [啟用以選取裝置的個別設定]，然後選取更多項目。選取的數值僅限用於替換掃描器。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 匯入匯入設定

將匯出的 Web Config 檔案匯入到掃描器。

**重要事項：**

當匯入包含掃描器名稱或 IP 位址等單獨資訊的值時，確保同一網路上不存在同一名稱的 IP 位址。

1. 存取 Web Config，然後選取 [裝置管理] 索引標籤 > [匯出與匯入設定值] > [匯入]。
2. 選取匯出檔，然後輸入加密密碼。
3. 按下 [下一步]。
4. 選取您想要匯入的設定，然後按下 [下一步]。
5. 按下 [確定]。

設定將套用至掃描器。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

# 回復至出廠預設值

在控制面板上，選取 [設定] > [系統管理] > [回復至出廠預設值]，然後選取您希望復原至其預設設定的項目。

❏ 網路設定：將網路相關設定還原為其初始狀態。

❏ 網路設定以外的所有設定：將其他設定還原為其初始狀態，網路相關設定除外。

❏ 所有設定：將所有設定還原為其購買時的初始狀態。

**重要事項：**

如果您選取並執行 [所有設定]，登錄至掃描器的所有設定資料將被刪除，包括聯絡人和驗證使用者設定在內。刪除的設定無法復原。

# 更新應用程式與韌體

您可以透過更新應用程式和韌體，解決部分問題和改進或添加某些功能。請確定使用最新版本的應用程式與韌體。

**重要事項：**

❏ 更新時請勿關閉電腦或掃描器。

**附註：**
當掃描器可連接至網際網路時，即可從 Web Config 更新韌體。選取 [裝置管理] 索引標籤 > [韌體更新]，檢查顯示的訊息，然後點按 [開始]。

1. 確保掃描器已與電腦連線，且電腦已連線至網際網路。
2. 啟動 EPSON Software Updater，並更新應用程式或韌體。

   **附註：**
   不支援 Windows Server 作業系統。

   ❏ Windows 10

   按下開始鍵，然後選取 [Epson Software] > [EPSON Software Updater]。

   ❏ Windows 8.1/Windows 8

   請在搜尋快速鍵中輸入應用程式名稱，然後選取顯示的圖示。

   ❏ Windows 7

   按下開始鍵，然後選取[所有程式]或[程式集] > [Epson Software] > [EPSON Software Updater]。

   ❏ Mac OS

   選擇 [尋找工具] > [前往] > [應用程式] > [Epson Software] > [EPSON Software Updater]。

附註：
若在清單中找不到要更新的應用程式，則無法使用 EPSON Software Updater 進行更新。請在當地的 Epson 網站上檢查最新版本的應用程式。

http://www.epson.com

## 使用控制面板來更新掃描器韌體

若掃描器可以連線至網際網路，可以使用控制面板來更新掃描器韌體。您也可以將掃描器設定為定期檢查韌體更新，並在有更新時通知您。

1. 從主畫面選取 [設定]。
2. 選取 [系統管理] > [韌體更新] > [更新]。

   附註：
   選取 [通知] > [開啟]，將掃描器設定為定期檢查是否有韌體更新。
3. 查看畫面上顯示的訊息並開始搜尋可用的更新。
4. 如果 LCD 螢幕上顯示的訊息通知您有可用的更新，按照螢幕上的指示開始更新。

   **重要事項：**
   - ❏ 在更新完畢之前，不要關閉掃描器或拔掉電源，否則掃描器可能會出故障。
   - ❏ 如果韌體更新沒有完成或不成功，掃描器將無法正常啟動，並且在下次打開掃描器時，LCD 螢幕上會顯示「Recovery Mode」。在這種情況下，必須用電腦進行再次更新。使用 USB 纜線連接掃描器至電腦。如果掃描器上顯示「Recovery Mode」，將無法透過網路連線更新韌體。從電腦上存取您本地的 Epson 網站，然後下載最新的掃描器韌體。後面的步驟見網站上的說明。

## 使用 Web Config 更新韌體

當掃描器可連接至網際網路時，即可從 Web Config 更新韌體。

1. 存取 Web Config 並選取 [裝置管理] 索引標籤 > [韌體更新]。
2. 按下 [開始]，然後依照螢幕上的指示操作。

   即會開始韌體確認，如果存在更新的韌體，會顯示韌體資訊。

附註：
您也可以使用 Epson Device Admin 更新韌體。您可以目視確認裝置清單中的韌體資訊。當您想更新多個裝置的韌體時，這很有用。詳細資訊，請參考 Epson Device Admin 的指南或說明。

**相關資訊**

➡ 第35頁“在網頁瀏覽器上執行 Web Config”

## 在未連接至網際網路的情況下更新韌體

您可以在電腦上，從 Epson 網站下載裝置的韌體，然後透過 USB 纜線連接裝置與電腦以更新韌體。如果您無法透過網路更新，請嘗試此方法。

附註：
更新前，確定您的電腦上已安裝掃描器驅動程式 Epson Scan 2。如果未安裝 Epson Scan 2，則再次將其安裝。

1. 請查看 Epson 網站以瞭解最新韌體更新版本。
   http://www.epson.com
   - ❏ 如果存在適用於您的掃描器的韌體，請將其下載並前往下一步。
   - ❏ 如果網站上沒有韌體資訊，表明您已經在使用最新版韌體。
2. 使用 USB 連接線將包含下載韌體的電腦連接至掃描器。
3. 按兩下下載的 .exe 檔案。
   Epson Firmware Updater 會隨即啟動。
4. 依照畫面上的指示進行操作。