EPSON
EXCEED YOUR VISION

管理員使用說明

NPD5493-00 TC

目錄

版權與商標

關於本手冊

標誌與符號. 5
插圖. 5
作業系統參考. 5
注意. 6

簡介

SSL/TLS 通訊. 7
通訊協定的控制. 7
IP 通訊加密和連線至身分驗證網路. 8
匯入和匯出掃描器設定值. 8

使用網路設定軟體

關於 Web Config. 9
存取 Web Config. 10
關於 EpsonNet Config. 11
使用 EpsonNet Config — Windows. 11
安裝 EpsonNet Config — Windows. 11
執行 EpsonNet Config - Windows. 11
解除安裝 EpsonNet Config - Windows. 11
使用 EpsonNet Config — Mac OS X. 12
安裝 EpsonNet Config — Mac OS X. 12
執行 EpsonNet Config - Mac OS X. 12
解除安裝 EpsonNet Config — Mac OS X. 12
Web Config 和 EpsonNet Config 功能比較. 12
其他網路軟體. 13
關於 Epson Device Admin. 13
關於 EpsonNet SetupManager. 13

在安全網路中使用掃描器

設定 SSL/TLS 通訊. 14
配置基本 SSL/TLS 設定. 14
配置掃描器的伺服器憑證. 15
通訊協定和服務的控制. 16
通訊協定的控制. 16
服務的控制. 16
設定 IPsec/IP Filtering. 17
關於 IPsec/IP Filtering. 17
配置 Default Policy. 17
配置 Group Policy. 19
IPsec/IP Filtering 的配置範例. 22
配置 IPsec/IP Filtering 的憑證. 23
使用 SNMPv3 通訊協定. 24
配置 SNMPv3. 24
將掃描器連接至 IEEE802.1X 網路. 26
配置 IEEE802.1X 網路. 26
配置 IEEE802.1X 的憑證. 27
使用數位憑證. 28
關於電子憑證. 28
取得並匯入 CA 簽署憑證. 29
刪除 CA 簽署憑證. 32
更新自我簽署憑證. 33
設定CA Certificate. 34

解決問題

解決問題的小祕訣. 36
使用網路軟體的問題. 36
無法存取 Web Config. 36
機型名稱及/或 IP 位址未顯示於 EpsonNet Config. 37
使用網路安全性功能的問題. 37
忘記預先共用金鑰. 37
無法使用 IPsec 通訊進行通訊. 37
突然無法進行通訊. 38
配置 IPsec/IP 篩選後無法連接. 39
在配置 IEEE802.1X 之後無法存取掃描器. 39
使用數位憑證的問題. 39
無法匯入 CA 簽署憑證. 39
無法更新自我簽署憑證. 40
無法建立 CSR. 40
顯示電子憑證相關警告. 41
意外刪除 CA 簽署憑證. 42
掃描問題. 43
無法執行 WSD 掃描. 43

附錄

使用電子郵件伺服器. 44
配置郵件伺服器. 44
檢查郵件伺服器連線. 46
發生事件時接收電子郵件通知. 48
關於電子郵件通知. 48
配置電子郵件通知. 48
配置系統管理員密碼. 48
配置通訊協定. 49

目錄

通訊協定設定項目. 50
匯出和匯入 Web Config 設定. 51
匯出設定. 51
匯入設定. 51
配置連接至掃描器的電腦. 52
將掃描器連接到網路. 52

版權與商標

關於本手冊

標誌與符號

> ⚠ 注意：
> 務必小心遵守以免身體受傷的說明。

> **重要事項：**
> 務必遵守以免損壞設備的說明。

附註：
包含有關掃描器操作的實用小秘訣及限制的說明。

相關資訊

➡ 按下此圖示可提供相關資訊。

插圖

❏ 螢幕擷取畫面與圖片的詳細資訊可能視機型而有不同，但操作說明皆相同。

❏ 螢幕擷取畫面取自 Windows 7。詳細資訊可能視作業系統版本而有不同。

❏ 螢幕擷取畫面中的部分功能表項目可能視機型而有不同。

作業系統參考

Windows

在本手冊中，「Windows 10」、「Windows 8.1」、「Windows 8」、「Windows 7」、「Windows Vista」、「Windows XP」、「Windows Server 2012 R2」、「Windows Server 2012」、「Windows Server 2008 R2」、「Windows Server 2008」、「Windows Server 2003 R2」及「Windows Server 2003」等專有名詞係指下列作業系統。此外，「Windows」泛指所有版本。

❏ 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 Vista® 作業系統

❏ Microsoft® Windows® XP 作業系統

❏ Microsoft® Windows® XP Professional x64 Edition 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
- ❏ Microsoft® Windows Server® 2008 作業系統
- ❏ Microsoft® Windows Server® 2003 R2 作業系統
- ❏ Microsoft® Windows Server® 2003 作業系統

Mac OS X

在本手冊中，「Mac OS X v10.11.x」係指 OS X El Capitan，「Mac OS X v10.10.x」係指 OS X Yosemite，「Mac OS X v10.9.x」係指 OS X Mavericks，且「Mac OS X v10.8.x」係指 OS X Mountain Lion。此外，「Mac OS X」係指「Mac OS X v10.11.x」、「Mac OS X v10.10.x」、「Mac OS X v10.9.x」、「Mac OS X v10.8.x」、「Mac OS X v10.7.x」及「Mac OS X v10.6.8」。

注意

- ❏ 禁止複製本手冊的資訊。
- ❏ 本手冊的所有資訊如有變更，恕不另行通知。
- ❏ 若在本手冊發現錯誤之處或對內容存有疑慮，請聯絡 Epson。
- ❏ 儘管有前述規定，Epson 不對使用本產品所導致之任何結果承擔任何責任。
- ❏ 因不當使用本產品及由第三方不當維修本產品所導致之任何故障，Epson 無須承擔任何責任。

簡介

本手冊是 Epson 掃描器的通用手冊，適合負責管理辦公室網路的系統管理員使用。系統管理員係指負責裝置配置以及用戶端、掃描器和電腦網路存取授權的人員。本手冊係提供系統管理員使用，詳細的程序可能視主題予以省略，相關專有名詞也可能未涵蓋於本手冊中。因此，閱讀者必須具備網路與電腦系統的相關知識。

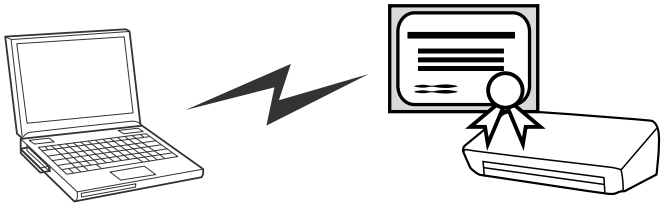
下列兩套軟體可以進行掃描器的進階網路配置：Web Config 和 EpsonNet Config。在本手冊中，各功能的配置說明基本上均來自 Web Config。如需 EpsonNet Config 的操作資訊，請參閱 EpsonNet Config 的說明文件或說明。作業系統功能表項目的描述是以 Windows 7 和 Mac OS X 10.10.x 為基礎。

附註：
若要配置系統管理功能，掃描器必須連上網路。如需將掃描器連上網路的詳細資訊，請參閱掃描器的說明文件或本手冊的附錄。

Epson 產品支援以下系統管理功能。可用的功能視產品而有所不同。(無法使用的功能不會顯示在掃描器的控制面板或軟體設定畫面中。)請參閱說明文件確認產品可用的功能。

SSL/TLS 通訊

您可透過 SSL/TLS (安全通訊端階層/傳輸層安全性) 通訊來設定掃描器的伺服器憑證，以及掃描器與電腦之間的加密通訊。使用此功能可防止詐騙攻擊，以及未經授權存取掃描器。



相關資訊

➡ 第14頁“設定 SSL/TLS 通訊”

通訊協定的控制

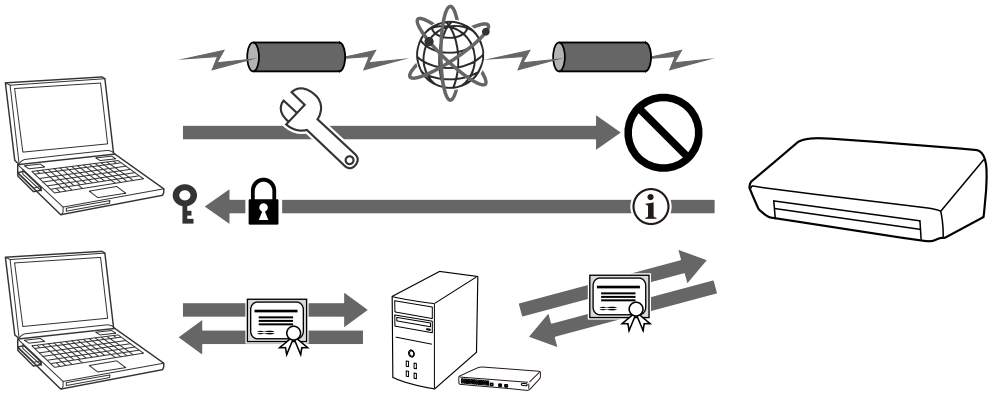
在掃描期間，掃描器會使用許多不同的通訊協定進行通訊。對單獨通訊協定新增權限或限制，即可控制該通訊協定，避免在意外操作時發生安全風險。

相關資訊

➡ 第16頁“通訊協定和服務的控制”
➡ 第49頁“配置通訊協定”

IP 通訊加密和連線至身分驗證網路

您可以加密通訊並控制掃描器的存取。若您想避免發生通訊攔截和資料篡改等狀況，請使用 [IPsec/IP Filtering] 或 SNMPv3 通訊協定。若您想驗證掃描器的存取，請使用 IEEE802.1X 功能。



相關資訊

➡ 第17頁“設定 IPsec/IP Filtering”

➡ 第24頁“使用 SNMPv3 通訊協定”

➡ 第26頁“將掃描器連接至 IEEE802.1X 網路”

匯入和匯出掃描器設定值

您可匯入和匯出掃描器設定值。若想將掃描器的設定值複製到另一台掃描器，或是替換掃描器時，即可使用此功能。

相關資訊

➡ 第51頁“匯出和匯入 Web Config 設定”

使用網路設定軟體

關於 Web Config

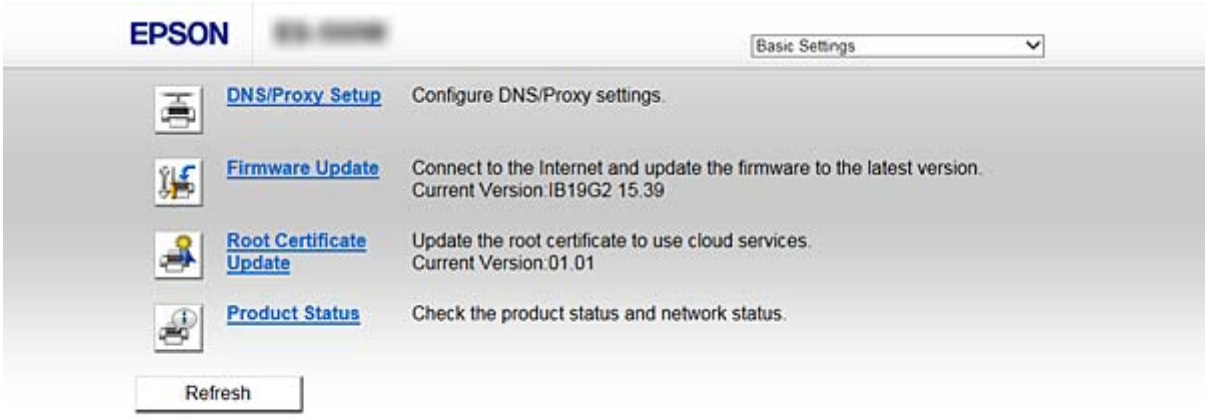
Web Config 是一種瀏覽器式的應用程式，可配置掃描器的設定。

若要存取 Web Config，您必須先將 IP 位址指派至掃描器。

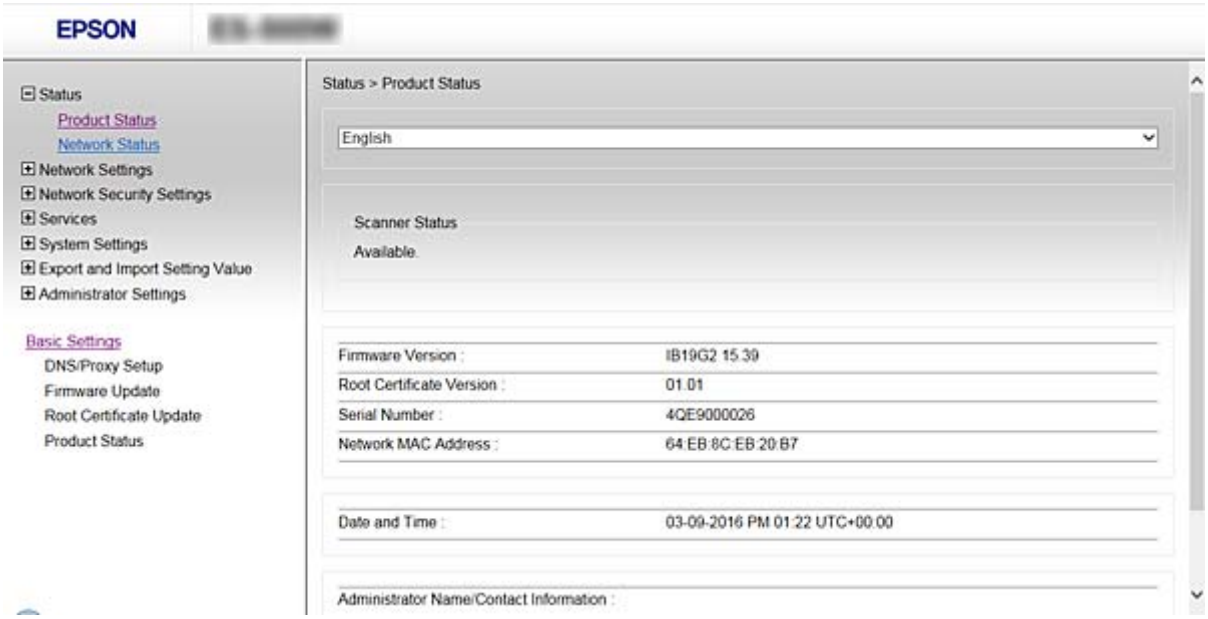
附註：
您可在掃描器配置系統管理員密碼，以鎖定設定。

設定頁面共有兩種，如下所示。

❏ [Basic Settings]
您可以配置掃描器的基本設定。



❏ [Advanced Settings]
您可以配置掃描器的進階設定。此頁面主要供管理員使用。



相關資訊

➡ 第12頁“Web Config 和 EpsonNet Config 功能比較”

存取 Web Config

在網路瀏覽器中輸入掃描器的 IP 位址。JavaScript 必須啟用。當透過 HTTPS 存取 Web Config 時，瀏覽器中將會顯示警告訊息，因為使用了儲存在掃描器中之自我簽署的憑證。

❏ 透過 HTTPS 存取

IPv4：https://<掃描器 IP 位址> (不加 < >)

IPv6：https://[掃描器 IP 位址]/ (加上 [ ])

❏ 透過 HTTP 存取

IPv4：http://<掃描器 IP 位址> (不加 < >)

IPv6：http://[掃描器 IP 位址]/ (加上 [ ])

附註：

❏ 範例

IPv4：

https://192.168.100.201/

http://192.168.100.201/

IPv6：

https://[2001:db8::1000:1]/

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

❏ 若掃描器名稱是以 DNS 伺服器登錄，您可使用掃描器名稱來取代掃描器的 IP 位址。

❏ 透過 HTTP 存取 Web Config 時，並非所有功能表皆會顯示。若要查看所有功能表，請透過 HTTPS 存取 Web Config。

❏ 您也可以從 EpsonNet Config 存取 Web Config。從掃描器清單畫面選擇掃描器，然後按下 [啟動瀏覽器]。

相關資訊

➡ 第12頁“Web Config 和 EpsonNet Config 功能比較”

➡ 第14頁“設定 SSL/TLS 通訊”

➡ 第28頁“使用數位憑證”

關於 EpsonNet Config

EpsonNet Config 可讓系統管理員配置掃描器的網路設定，如指派 IP 位址及變更連線模式。Windows 支援批次設定功能。如需詳細資訊，請參閱 EpsonNet Config 的說明文件或說明。

相關資訊

➡ 第12頁“Web Config 和 EpsonNet Config 功能比較”

使用 EpsonNet Config — Windows

安裝 EpsonNet Config — Windows

下載 EpsonNet Config，位址為 Epson 支援網站，然後按照畫面說明進行安裝。

執行 EpsonNet Config - Windows

選取 [所有程式] > [EpsonNet] > [EpsonNet Config Vxx] > [EpsonNet Config]。

附註：
若出現防火牆警示，請允許存取 EpsonNet Config。

相關資訊

➡ 第12頁“Web Config 和 EpsonNet Config 功能比較”

解除安裝 EpsonNet Config - Windows

選取[控制台] > [程式集] > [程式和功能] > [解除安裝程式] > [EpsonNet Config Vxx]，然後按一下[解除安裝]。

使用 EpsonNet Config — Mac OS X

安裝 EpsonNet Config — Mac OS X

下載 EpsonNet Config，位址為 Epson 支援網站，然後按照畫面說明進行安裝。

執行 EpsonNet Config - Mac OS X

選取 [前往]> [應用程式] > [Epson Software] > [EpsonNet] > [EpsonNet Config Vxx] > [EpsonNet Config]。

相關資訊

➡ 第12頁“Web Config 和 EpsonNet Config 功能比較”

解除安裝 EpsonNet Config — Mac OS X

使用 Uninstaller 解除安裝應用程式。您可使用 EPSON Software Updater 或從 Epson 支援網站下載 Uninstaller。

執行 Uninstaller 時，所有已安裝的 Epson 應用程式皆會顯示。選取 EpsonNet Config，然後依照螢幕上的指示操作。

附註：
若沒有 Uninstaller，請將 [應用程式]中的程式資料夾拖放至 Dock 中的垃圾桶圖示。

Web Config 和 EpsonNet Config 功能比較

下列兩套軟體可以進行掃描器的網路配置：Web Config 和 EpsonNet Config。

以下是本手冊涵蓋的功能及這兩套軟體的比較。

功能	Web Config	EpsonNet Config
配置 SSL/TLS 通訊	✓	✓
配置掃描器的伺服器憑證	✓	✓
配置 IPsec/IP 篩選	✓	✓
配置 SNMPv3 通訊協定	✓	—
將掃描器連接至 IEEE802.1X 網路 (乙太網路/Wi-Fi)	✓	✓
取得並匯入 CA 簽署憑證	✓	—
更新自我簽署憑證	✓	—
配置郵件伺服器	✓	✓
配置系統管理員密碼	✓	✓

功能	Web Config	EpsonNet Config
配置電子郵件通知	✓	—
針對多台掃描器進行批次設定	—	✓ (僅適用於 Windows)
匯入和匯出設定	✓	✓

相關資訊

➡ 第9頁“關於 Web Config”
➡ 第10頁“存取 Web Config”
➡ 第11頁“關於 EpsonNet Config”
➡ 第11頁“執行 EpsonNet Config - Windows”
➡ 第12頁“執行 EpsonNet Config - Mac OS X”
➡ 第14頁“配置基本 SSL/TLS 設定”
➡ 第15頁“配置掃描器的伺服器憑證”
➡ 第17頁“設定 IPsec/IP Filtering”
➡ 第24頁“使用 SNMPv3 通訊協定”
➡ 第26頁“將掃描器連接至 IEEE802.1X 網路”
➡ 第29頁“取得並匯入 CA 簽署憑證”
➡ 第33頁“更新自我簽署憑證”
➡ 第44頁“使用電子郵件伺服器”
➡ 第48頁“配置系統管理員密碼”
➡ 第48頁“配置電子郵件通知”
➡ 第51頁“匯出和匯入 Web Config 設定”

其他網路軟體

關於 Epson Device Admin

Epson Device Admin 是一款可讓您將裝置安裝至網路，然後設定和管理裝置的應用程式。您可建立包含設定項目的範本，再將其作為共用設定套用至其他裝置。您可將 Epson Device Admin 從 Epson 支援網站下載。如需詳細資訊，請參閱 Epson Device Admin 的說明文件或說明。

關於 EpsonNet SetupManager

EpsonNet SetupManager 是可建立掃描器簡易安裝套件的軟體，如安裝和配置掃描器驅動程式，以及安裝 Document Capture Pro。

此軟體允許系統管理員建立唯一的軟體套件，並在群組之間散發。

如需詳細資訊，請造訪您的區域 Epson 網站。

在安全網路中使用掃描器

此主題將會說明 Epson 產品支援的加密功能。可用的功能視機型而定。如需功能可用性的詳細資訊，請參閱掃描器的說明文件。

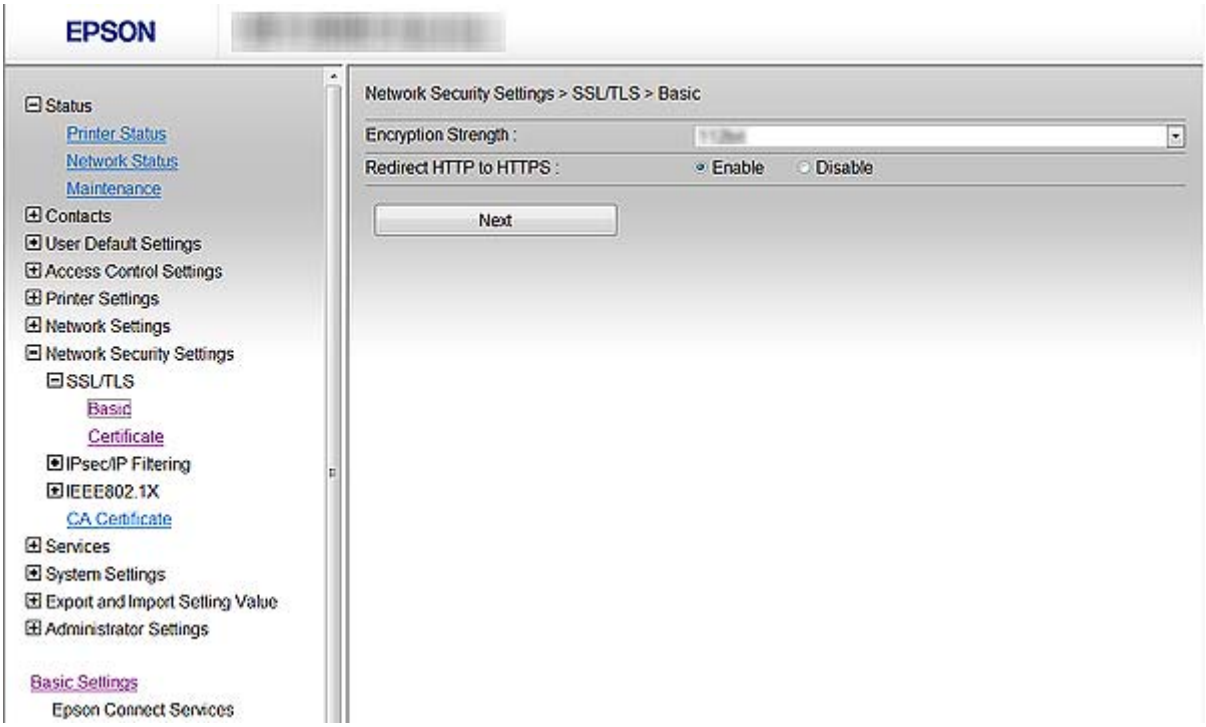
設定 SSL/TLS 通訊

配置基本 SSL/TLS 設定

若掃描器支援 HTTPS 伺服器功能，您可使用 SSL/TLS 通訊來加密通訊。您可使用 Web Config 配置及管理掃描器，同時確保安全性。

配置加密強度及重新導向功能。

1. 存取 Web Config，然後選擇 [Network Security Settings] > [SSL/TLS] > [Basic]。
2. 在各項目選擇數值。
   - ❏ [Encryption Strength]
     選擇加密強度等級。
   - ❏ [Redirect HTTP to HTTPS]
     存取 HTTP 時重新導向到 HTTPS。



3. 按下 [Next]。
   確認訊息會隨即顯示。

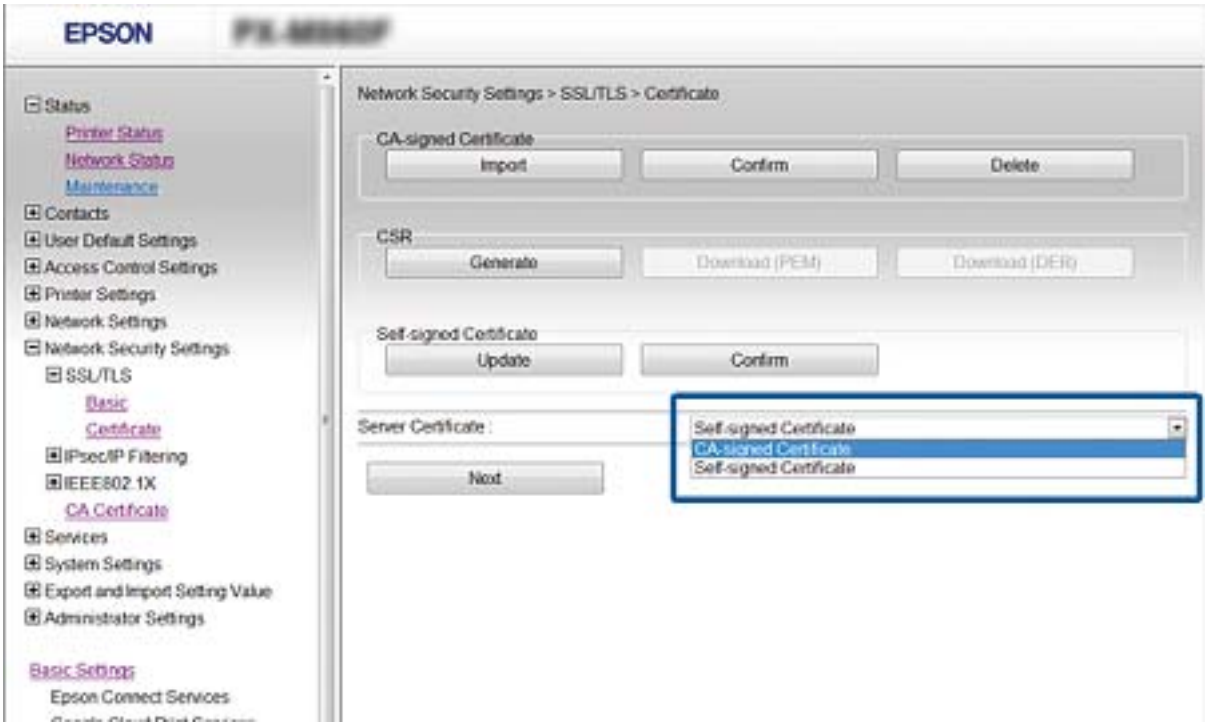
4. 按下 [OK]。
   掃描器會隨即更新。

相關資訊

➡ 第10頁“存取 Web Config”

配置掃描器的伺服器憑證

1. 存取 Web Config，然後選擇 [Network Security Settings] >[SSL/TLS]> [Certificate]。
2. 在 [Server Certificate] 上指定要使用的憑證。
   - ❏ [Self-signed Certificate]
     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-signed Certificate]
     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 [Next]。
   確認訊息會隨即顯示。
4. 按下 [OK]。
   掃描器會隨即更新。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第29頁“取得並匯入 CA 簽署憑證”

通訊協定和服務的控制

您可透過多種途徑和通訊協定進行掃描，並可透過連網電腦 (未指定數量) 進行網路掃描。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

配置通訊協定配置。

1. 存取 Web Config，然後選擇 [Services] > [Protocol]。
2. 配置各個項目。
3. 按下 [Next]。
4. 按下 [OK]

   設定即會套用到掃描器。

可啟用或停用的通訊協定

通訊協定	說明
Bonjour Settings	您可指定是否要使用 Bonjour。Bonjour 用於搜尋裝置、掃描等等。
SLP Settings	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 Settings	您可啟用或停用 WSD 功能。啟用後，您可新增 WSD 裝置或從 WSD 連接埠進行掃描。
LLTD Settings	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 Settings	您可啟用或停用 LLMNR 功能。啟用此功能後，即便無法使用 NetBIOS，也不需要 DNS 就可使用名稱解析。
SNMPv1/v2c Settings	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。

服務的控制

啟用或停用服務，如網路掃描。

1. 存取 Web Config，然後選擇 [Services]。
2. 啟用或停用項目。

   可配置的項目會隨著掃描器而有所不同。
3. 按下 [Next]。
4. 按下 [OK]。

可啟用或停用的服務

服務	描述
Network Scan	您可指定是否使用 Network Scan。啟用此功能後，可透過連網電腦使用掃描功能。
AP mode	您可指定是否啟用 AP mode。啟用此功能後，則可透過 AP mode 進行裝置連線。

設定 IPsec/IP Filtering

關於 IPsec/IP Filtering

若掃描器支援 IPsec/IP 篩選，您可依據 IP 位址、服務及連接埠篩選流量。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。

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。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。

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。

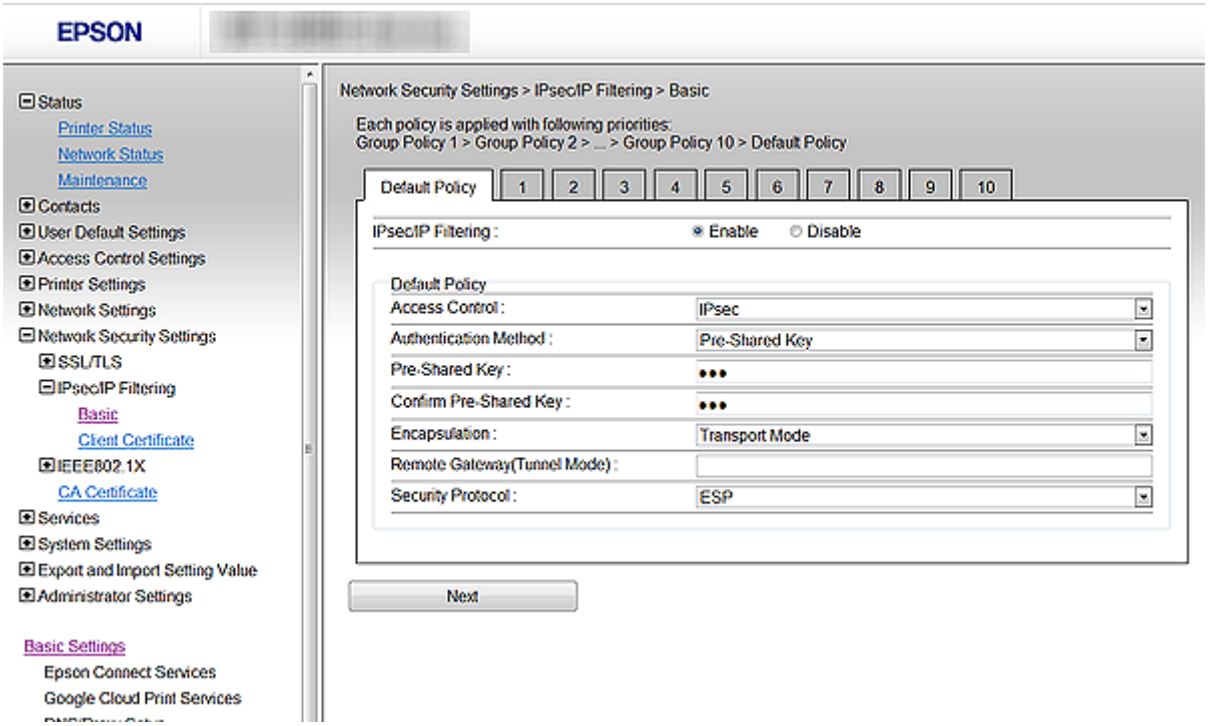
配置 Default Policy

1. 存取 Web Config，然後選擇 [Network Security Settings] > [IPsec/IP Filtering] > [Basic]。
2. 在各項目輸入數值。
3. 按下 [Next]。
   確認訊息會隨即顯示。
4. 按下 [OK]。
   掃描器會隨即更新。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第18頁“Default Policy 設定項目”

Default Policy 設定項目



項目	設定與說明	
IPsec/IP Filtering	您可啟用或停用 IPsec/IP 篩選功能。	
Access Control	配置 IP 封包流量的控制方式。	
	Permit Access	選擇此選項會允許已配置的 IP 封包通過。
	Refuse Access	選擇此選項會拒絕已配置的 IP 封包通過。
	IPsec	選擇此選項會允許已配置的 IPsec 封包通過。
Authentication Method	若選擇 [Certificate]，您必須事先取得並匯入 CA 簽署憑證。	
Pre-Shared Key	若在 [Pre-Shared Key] 選擇 [Authentication Method]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。	
Confirm Pre-Shared Key	輸入您配置用於確認的金鑰。	
Encapsulation	若在 [IPsec] 選擇 [Access Control]，您必須配置封裝模式。	
	Transport Mode	若只在相同 LAN 上使用掃描器，請選擇此選項。第 4 層以上的 IP 封包會經過加密。
	Tunnel Mode	若您在具有網際網路功能的網路 (如 IPsec-VPN) 上使用掃描器，請選擇此選項。IP 封包的標頭及資料會經過加密。
Remote Gateway(Tunnel Mode)	若在 [Tunnel Mode] 選擇 [Encapsulation]，請輸入介於 1 和 39 個字元之間的閘道位址。	

項目	設定與說明	
Security Protocol	若在 [Access Control] 選擇 [IPsec]，請選擇一個選項。	
	ESP	選擇此選項可確保驗證和資料的完整性，並加密資料。
	AH	選擇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。

相關資訊

➡ 第17頁“配置 Default Policy”

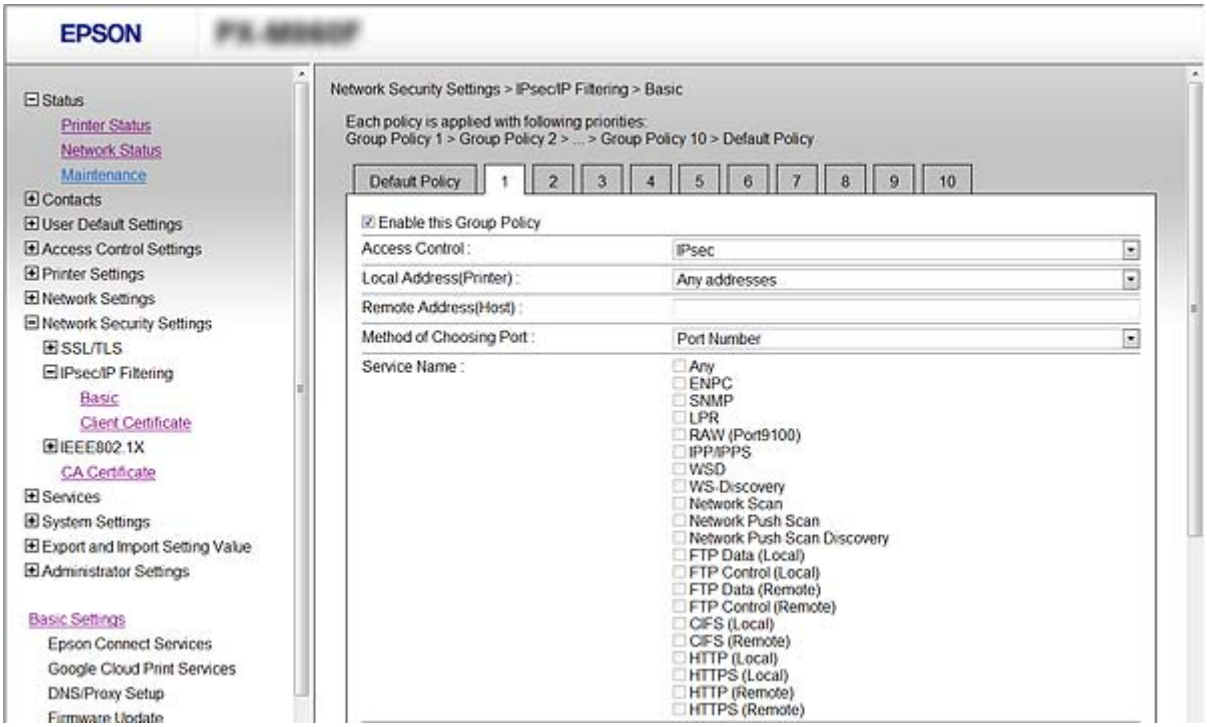
配置 Group Policy

1. 存取 Web Config，然後選擇 [Network Security Settings] > [IPsec/IP Filtering] > [Basic]。
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 [Next]。
   確認訊息會隨即顯示。
5. 按下 [OK]。
   掃描器會隨即更新。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第20頁“Group Policy 設定項目”

Group Policy 設定項目



項目	設定與說明	
Enable this Group Policy	您可啟用或停用群組原則。	
Access Control	配置 IP 封包流量的控制方式。	
	Permit Access	選擇此選項會允許已配置的 IP 封包通過。
	Refuse Access	選擇此選項會拒絕已配置的 IP 封包通過。
	IPsec	選擇此選項會允許已配置的 IPsec 封包通過。
Local Address (Scanner)	選擇與您的網路環境相符的 IPv4 地址或 IPv6 地址。若 IP 地址為自動指派，則可選擇 [Use auto-obtained IPv4 address]。	
Remote Address(Host)	輸入裝置的 IP 位址以控制存取。IP 位址必須介於 0 和 43 個字元之間。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。	
Method of Choosing Port	選擇指定連接埠的方式。	
Service Name	若在 [Method of Choosing Port] 選擇 [Service Name]，請選擇一個選項。	

項目	設定與說明	
Transport Protocol	若在 [Port Number] 選擇 [Method of Choosing Port]，您必須配置封裝模式。	
	Any Protocol	選擇此選項可控制所有通訊協定類型。
	TCP	選擇此選項可控制單點傳播的資料。
	UDP	選擇此選項可控制廣播及多點傳播的資料。
	ICMPv4	選擇此選項可控制 Ping 命令。
Local Port	若您在 [Method of Choosing Port] 選擇 [Port Number]，且在 [Transport Protocol] 選擇 [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。	
Remote Port	若您在 [Method of Choosing Port] 選擇 [Port Number]，且在 [Transport Protocol] 選擇 [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。	
Authentication Method	若在 [Access Control] 選擇 [IPsec]，請選擇一個選項。已使用憑證與預設原則一樣。	
Pre-Shared Key	若在 [Pre-Shared Key] 選擇 [Authentication Method]，請輸入介於 1 和 127 個字元之間的預先共用金鑰。	
Confirm Pre-Shared Key	輸入您配置用於確認的金鑰。	
Encapsulation	若在 [IPsec] 選擇 [Access Control]，您必須配置封裝模式。	
	Transport Mode	若只在相同 LAN 上使用掃描器，請選擇此選項。第 4 層以上的 IP 封包會經過加密。
	Tunnel Mode	若您在具有網際網路功能的網路 (如 IPsec-VPN) 上使用掃描器，請選擇此選項。IP 封包的標頭及資料會經過加密。
Remote Gateway(Tunnel Mode)	若在 [Tunnel Mode] 選擇 [Encapsulation]，請輸入介於 1 和 39 個字元之間的閘道位址。	
Security Protocol	若在 [Access Control] 選擇 [IPsec]，請選擇一個選項。	
	ESP	選擇此選項可確保驗證和資料的完整性，並加密資料。
	AH	選擇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。

相關資訊

➡ 第19頁“配置 Group Policy”
➡ 第22頁“在 Group Policy 上結合 Local Address (Scanner) 和 Remote Address(Host)”
➡ 第22頁“集團政策服務名稱參考”

在 Group Policy 上結合 Local Address (Scanner) 和 Remote Address(Host)

		Local Address (Scanner) 的設定		
		IPv4	IPv6*2	Any addresses*3
Remote Address(Host) 的設定	IPv4*1	✓	—	✓
	IPv6*1, *2	—	✓	✓
	空白	✓	✓	✓

*1 若針對 [Access Control] 選擇 [IPsec]，您無法指定前綴長度。

*2 若針對 [Access Control] 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。

集團政策服務名稱參考

附註：
無法使用的服務將會顯示，但無法選擇。

服務名稱	通訊協定類型	本機連接埠編號	遠端連接埠編號	受控功能
Any	—	—	—	所有服務
ENPC	UDP	3289	任一連接埠	從 EpsonNet Config 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 EpsonNet Config 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	從 WSD 中搜尋掃描器
Network Scan	TCP	1865	任一連接埠	轉寄來自 Document Capture Pro 的掃描資料
HTTP (Local)	TCP	80	任一連接埠	HTTP(S) 伺服器 (轉寄 Web Config 和 WSD 的資料)
HTTPS (Local)	TCP	443	任一連接埠	
HTTP (Remote)	TCP	任一連接埠	80	HTTP(S) 用戶端 (韌體更新和根認證更新之間的通訊)
HTTPS (Remote)	TCP	任一連接埠	443	

IPsec/IP Filtering 的配置範例

僅接收 IPsec 封包

此範例僅用來配置預設原則。

[Default Policy]：

❏ [IPsec/IP Filtering]: [Enable]

❏ [Access Control]: [IPsec]

❏ [Authentication Method]: [Pre-Shared Key]

❏ [Pre-Shared Key]：最多輸入 127 個字元。

[Group Policy]：

請勿配置。

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。

[Default Policy]：

❏ [IPsec/IP Filtering]: [Enable]

❏ [Access Control]: [Refuse Access]

[Group Policy]：

❏ [Enable this Group Policy]：勾選方塊。

❏ [Access Control]: [Permit Access]

❏ [Remote Address(Host)]：用戶端的 IP 位址

❏ [Method of Choosing Port]: [Service Name]

❏ [Service Name]：勾選 [ENPC], [SNMP], [HTTP (Local)], [HTTPS (Local)] 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。

[Default Policy]：

❏ [IPsec/IP Filtering]: [Enable]

❏ [Access Control]:[Refuse Access]

[Group Policy]：

❏ [Enable this Group Policy]：勾選方塊。

❏ [Access Control]: [Permit Access]

❏ [Remote Address(Host)]：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。

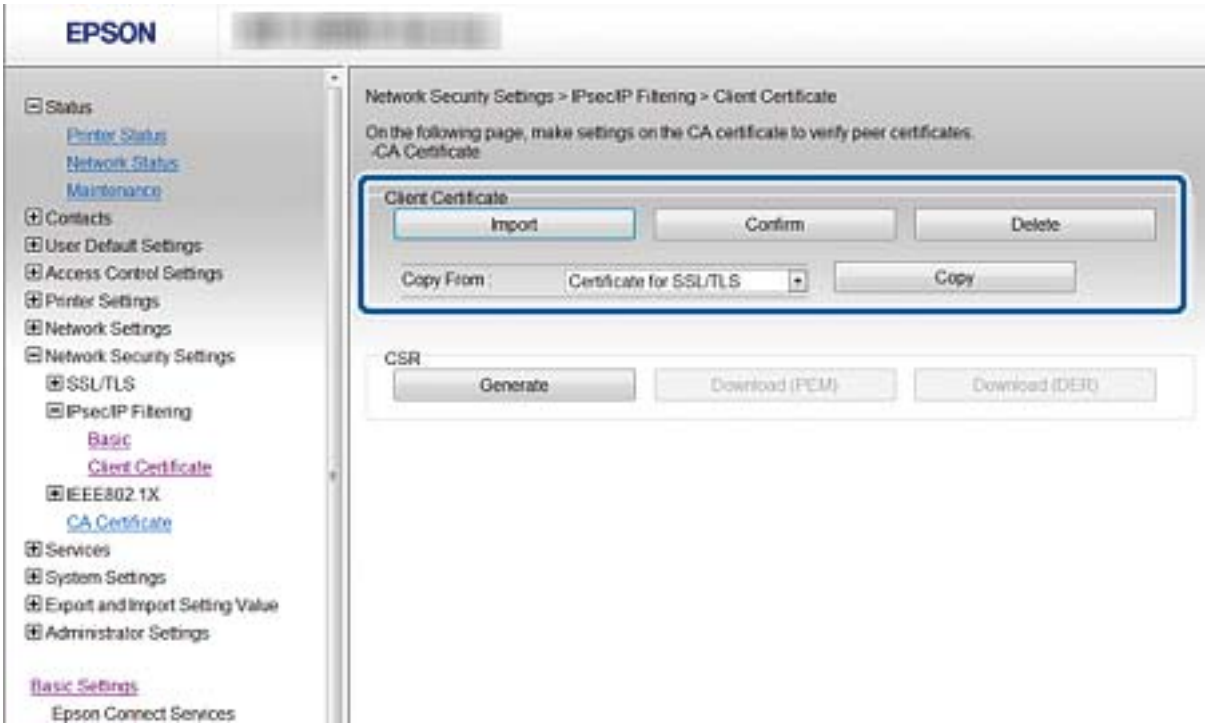
配置 IPsec/IP Filtering 的憑證

配置用戶端憑證，進行 IPsec/IP 過濾。若您要配置憑證授權，請前往 [CA Certificate]。

1. 存取 Web Config，然後選擇 [Network Security Settings] > [IPsec/IP Filtering] > [Client Certificate]。

2. 在 [Client Certificate] 中匯入憑證。

   若您已經匯入由憑證授權單位所核發的 IEEE802.1X 或 SSL/TLS 憑證，則可複製憑證並用於 IPsec/IP 過濾。若要複製，請在 [Copy From] 中選擇憑證，然後按下 [Copy]。



相關資訊

➡ 第10頁“存取 Web Config”

➡ 第29頁“取得並匯入 CA 簽署憑證”

使用 SNMPv3 通訊協定

配置 SNMPv3

若掃描器支援 SNMPv3 通訊協定，則您可監視和控制掃描器的存取。

1. 存取 Web Config，然後選擇 [Services] > [Protocol]。
2. 在 [SNMPv3 Settings] 的各項目輸入數值。
3. 按下 [Next]。

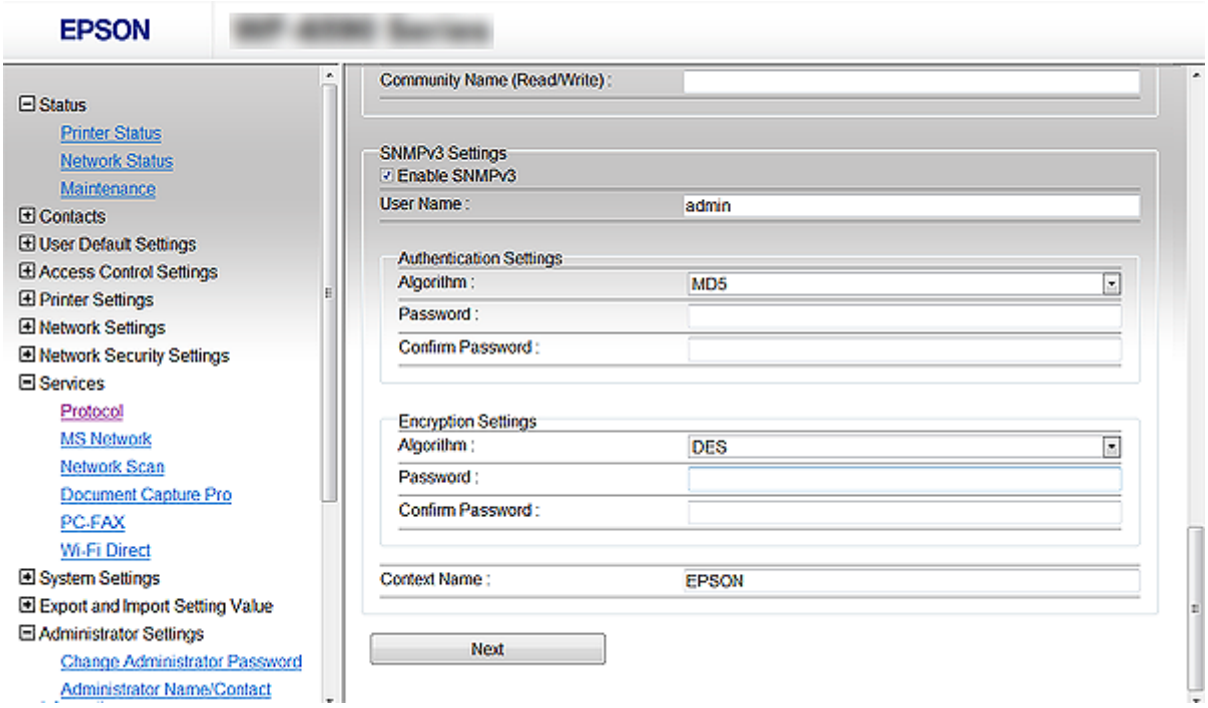
   確認訊息會隨即顯示。
4. 按下 [OK]。

   掃描器會隨即更新。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第25頁“SNMPv3 設定項目”

SNMPv3 設定項目



項目	設定與說明
Enable SNMPv3	勾選檢查盒時，SNMPv3 會啟用。
User Name	輸入 1 至 32 個 1 位元組字元。
Authentication Settings	
Algorithm	選取驗證的演算法。
Password	輸入 8 至 32 個 ASCII (0x20-0x7E) 字元。
Confirm Password	輸入您設定的密碼進行確認。
Encryption Settings	
Algorithm	選取加密的演算法。
Password	輸入 8 至 32 個 ASCII (0x20-0x7E) 字元。
Confirm Password	輸入您設定的密碼進行確認。
Context Name	輸入 1 至 32 個 1 位元組字元。

相關資訊

➡ 第24頁“配置 SNMPv3”

將掃描器連接至 IEEE802.1X 網路

配置 IEEE802.1X 網路

若掃描器支援 IEEE802.1X，您可使用與 RADIUS 伺服器及集線器進行網路驗證的掃描器作為驗證器。

1. 存取 Web Config，然後選擇 [Network Security Settings] > [IEEE802.1X] > [Basic]。
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 Setup]，並選擇或輸入 SSID。
3. 按下 [Next]。
   確認訊息會隨即顯示。
4. 按下 [OK]。
   掃描器會隨即更新。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第26頁“IEEE802.1X 網路設定項目”
➡ 第39頁“在配置 IEEE802.1X 之後無法存取掃描器”

IEEE802.1X 網路設定項目

項目	設定與說明
IEEE802.1X (Wi-Fi)	畫面會顯示 IEEE802.1X 的連線狀態 (Wi-Fi)。
Connection Method	目前網路的連線方式會顯示。

項目	設定與說明	
EAP Type	選擇用於掃描器與 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。
User ID	配置要用於 RADIUS 伺服器驗證的 ID。 輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。	
Password	配置驗證掃描器的密碼。 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。	
Confirm Password	輸入您配置用於確認的密碼。	
Server ID	您可配置要與指定 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。 輸入 0 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。	
Certificate Validation	不論驗證方法為何，您都可設定憑證效力。在 [CA Certificate] 中匯入憑證。	
Anonymous Name	若在 [PEAP-TLS] 選擇 [PEAP/MSCHAPv2] 或 [Authentication Method]，則您可配置匿名名稱來取代 PEAP 驗證之階段 1 的使用者 ID。 輸入 0 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。	
Encryption Strength	您可選擇下列其中一項。	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

相關資訊

➡ 第26頁“配置 IEEE802.1X 網路”

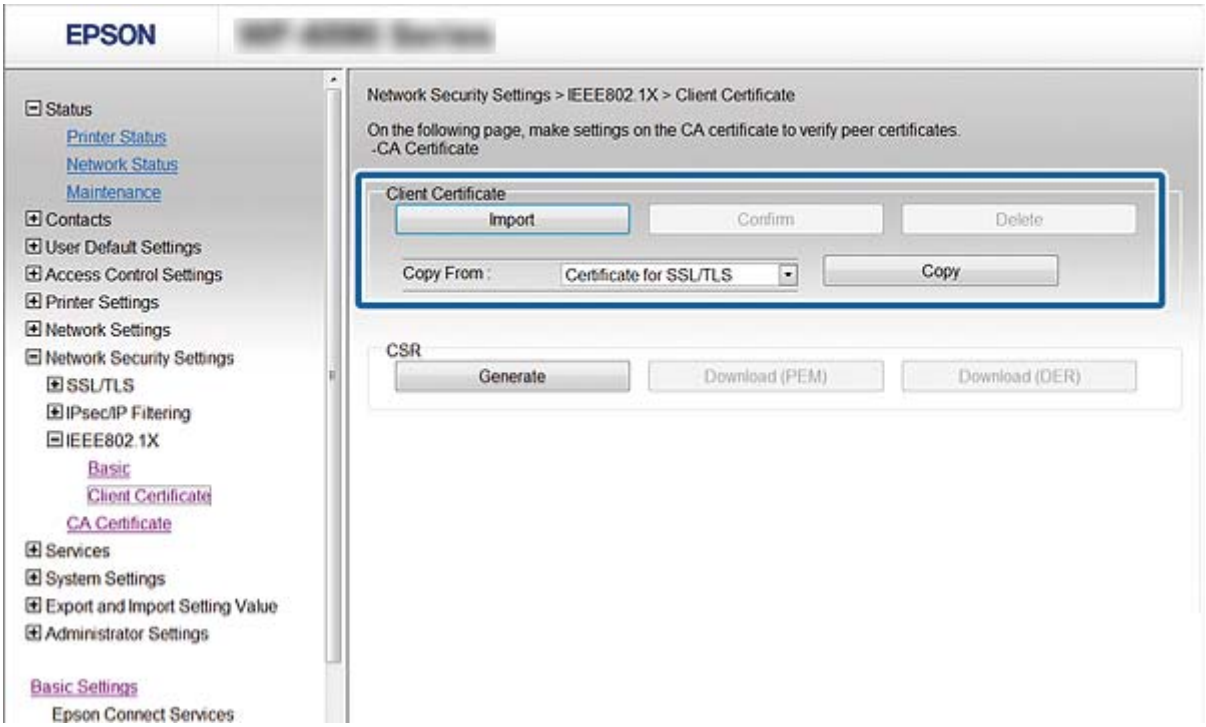
配置 IEEE802.1X 的憑證

配置 IEEE802.1X 的用戶端憑證。若您要配置憑證授權單位的憑證，請前往 [CA Certificate]。

1. 存取 Web Config，然後選擇 [Network Security Settings] > [IEEE802.1X] > [Client Certificate]。

2. 在 [Client Certificate] 中輸入憑證。

   若憑證是由憑證授權單位核發，則可複製該憑證。若要複製，請在 [Copy From] 中選擇憑證，然後按下 [Copy]。



相關資訊

➡ 第10頁“存取 Web Config”

➡ 第29頁“取得並匯入 CA 簽署憑證”

使用數位憑證

關於電子憑證

❏ 憑證由 CA 簽署

由 CA (憑證授權單位) 簽署的憑證必須從憑證授權單位取得。您可透過 CA 簽署憑證確保通訊安全。您可將 CA 簽署憑證用於各種安全性功能。

❏ CA 憑證

CA 憑證表示第三方已經驗證伺服器的身分識別。這是信任網路安全性機制的重要關鍵。您必須取得 CA 所核發的 CA 憑證進行伺服器驗證。

❏ 自我簽署憑證

自我簽署憑證是由掃描器核發並自行簽署的憑證。這種憑證並不可靠，也無法避免詐騙攻擊。若將此憑證用於 SSL/TLS 憑證，瀏覽器可能會顯示安全性警示。您只能將此憑證用於 SSL/TLS 通訊。

相關資訊

➡ 第12頁“Web Config 和 EpsonNet Config 功能比較”

➡ 第29頁“取得並匯入 CA 簽署憑證”
➡ 第32頁“刪除 CA 簽署憑證”
➡ 第33頁“更新自我簽署憑證”

取得並匯入 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，然後選擇 [Network Security Settings]。接著選擇 [SSL/TLS] > [Certificate] 或 [IPsec/IP Filtering] > [Client Certificate] 或 [IEEE802.1X] > [Client Certificate]。
2. 按下 [Generate] 的 [CSR]。

   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 [OK]。

   完成訊息會隨即顯示。
5. 選擇 [Network Security Settings]。接著選擇 [SSL/TLS] > [Certificate] 或 [IPsec/IP Filtering] > [Client Certificate] 或 [IEEE802.1X] > [Client Certificate]。
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-signed Certificate。
7. 將 CSR 傳送至憑證授權單位，並取得 CA-signed Certificate。

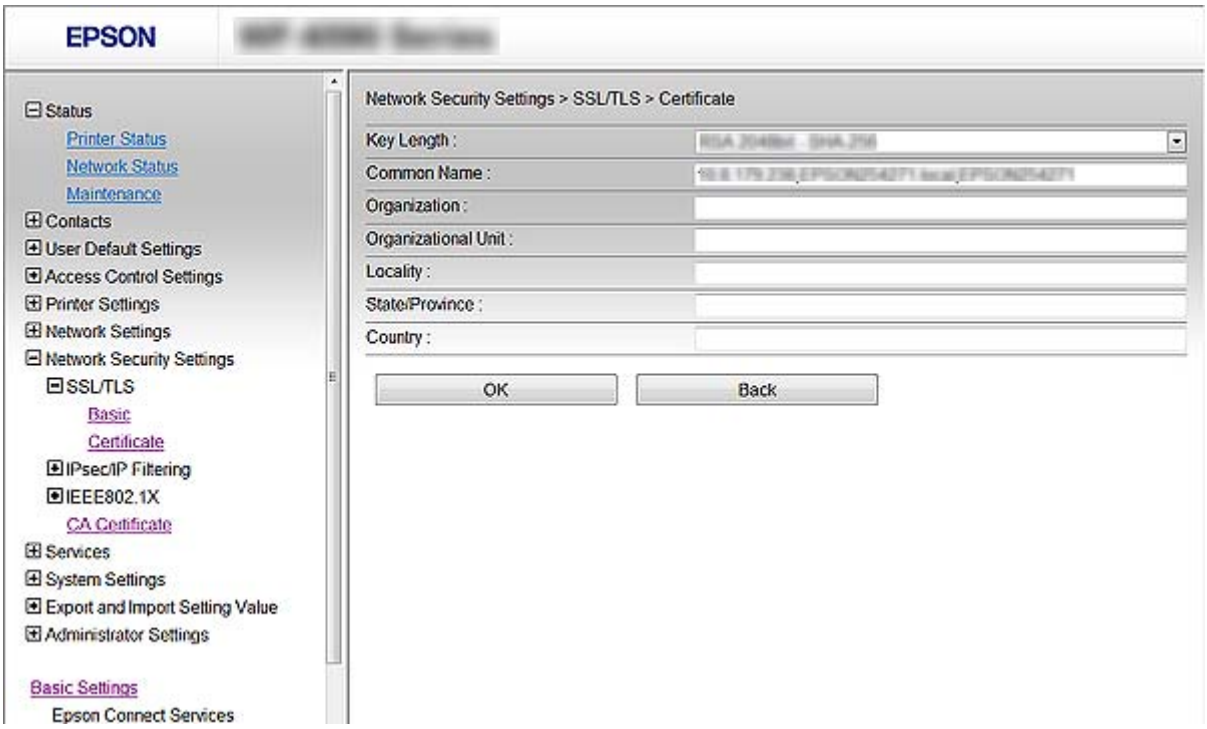
   請遵守各憑證授權單位的傳送方式及表單規定。
8. 將已核發的 CA-signed Certificate 儲存至與掃描器相連接的電腦。

   將憑證儲存至目的地的同時，CA-signed Certificate 的取得程序隨即完成。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第30頁“CSR 設定項目”
➡ 第30頁“匯入 CA 簽署憑證”

CSR 設定項目



項目	設定與說明
Key Length	選取 CSR 的金鑰長度。
Common Name	您可輸入 1 至 128 個字元。若這是 IP 位址，則必須為靜態 IP 位址。 範例： 存取 Web Config 的網址：https://10.152.12.225 一般名稱：10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	您可輸入 0 至 64 個 ASCII (0x20-0x7E) 字元。您可使用逗號分隔辨別名稱。
Country	輸入 ISO-3166 所指定的兩位數國碼。

相關資訊

➡ 第29頁“取得 CA 簽署憑證”

匯入 CA 簽署憑證

重要事項：

❏ 確定已正確設定掃描器的日期與時間。

❏ 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，然後選擇 [Network Security Settings]。接著選擇 [SSL/TLS] > [Certificate] 或 [IPsec/IP Filtering] > [Client Certificate] 或 [IEEE802.1X] > [Client Certificate]。

2. 按下 [Import]。

   憑證匯入頁面會隨即開啟。

3. 在各項目輸入數值。

   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
     - ❏ [Private Key]：由於掃描器含有私密金鑰，因此請勿進行配置。
     - ❏ [Password]：請勿配置。
     - ❏ [CA Certificate 1]/[CA Certificate 2]：選擇性
   - ❏ 從電腦取得的 PEM/DER 格式憑證
     - ❏ [Private Key]：您必須進行設定。
     - ❏ [Password]：請勿配置。
     - ❏ [CA Certificate 1]/[CA Certificate 2]：選擇性
   - ❏ 從電腦取得的 PKCS#12 格式憑證
     - ❏ [Private Key]：請勿配置。
     - ❏ [Password]：選擇性
     - ❏ [CA Certificate 1]/[CA Certificate 2]：請勿配置。

4. 按下 [OK]。

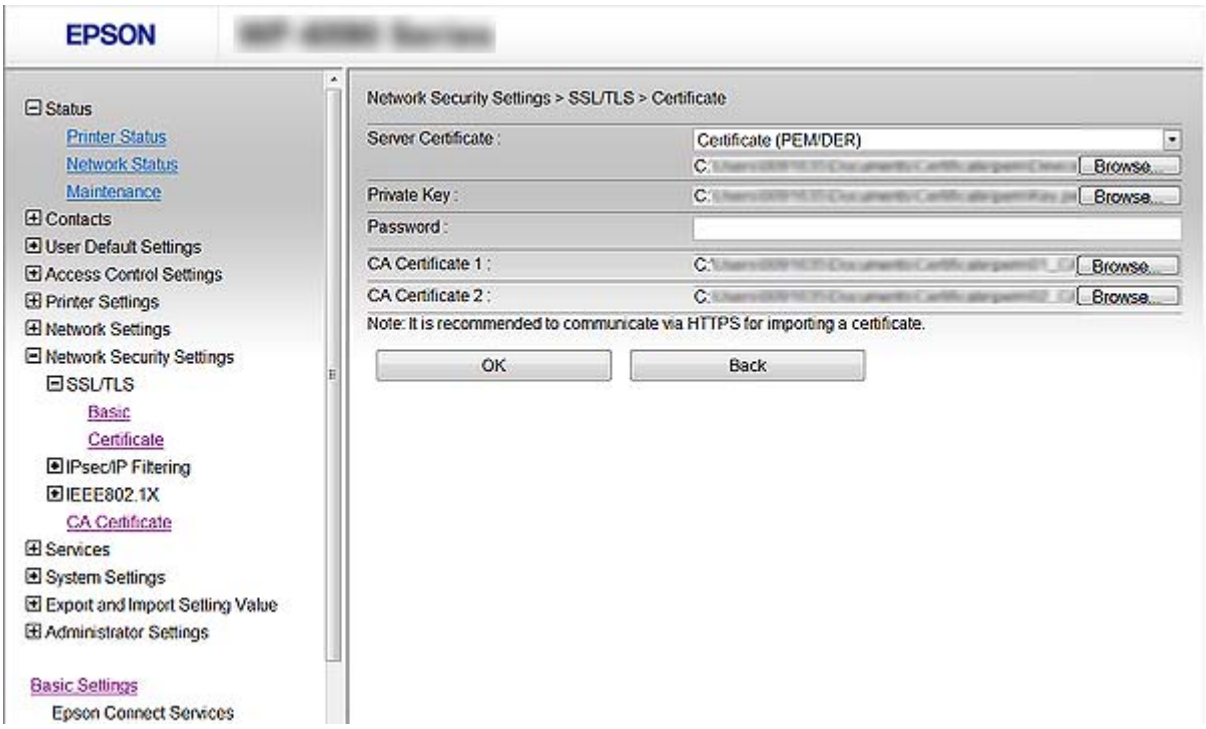
   完成訊息會隨即顯示。

附註：
按下 [Confirm] 確認憑證資訊。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第32頁“CA 簽署憑證匯入設定項目”

CA 簽署憑證匯入設定項目



項目	設定與說明
Server Certificate或Client Certificate	選取憑證的格式。
Private Key	若使用電腦建立的 CSR 取得 PEM/DER 格式的憑證，請指定符合憑證的私密金鑰檔案。
Password	輸入密碼以加密私密金鑰。
CA Certificate 1	若憑證的格式為 [Certificate (PEM/DER)]，請匯入核發伺服器憑證之憑證授權單位的憑證。視需要指定檔案。
CA Certificate 2	若憑證的格式為 [Certificate (PEM/DER)]，請匯入核發 [CA Certificate 1] 之憑證授權單位的憑證。視需要指定檔案。

相關資訊

➡ 第30頁“匯入 CA 簽署憑證”

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，然後選擇 [Network Security Settings]。接著選擇 [SSL/TLS] > [Certificate] 或 [IPsec/IP Filtering] > [Client Certificate] 或 [IEEE802.1X] > [Client Certificate]。

2. 按下 [Delete]。

   確認訊息會隨即顯示。

3. 按下 [OK]。

相關資訊

➡ 第10頁“存取 Web Config”

更新自我簽署憑證

若掃描器支援 HTTPS 伺服器功能，您可更新自我簽署憑證。使用自我簽署憑證存取 Web Config 時，會顯示警告訊息。

暫時使用自我簽署憑證，直到取得並匯入 CA 簽署憑證。

1. 存取 Web Config，然後選擇 [Network Security Settings] > [SSL/TLS] > [Certificate]。

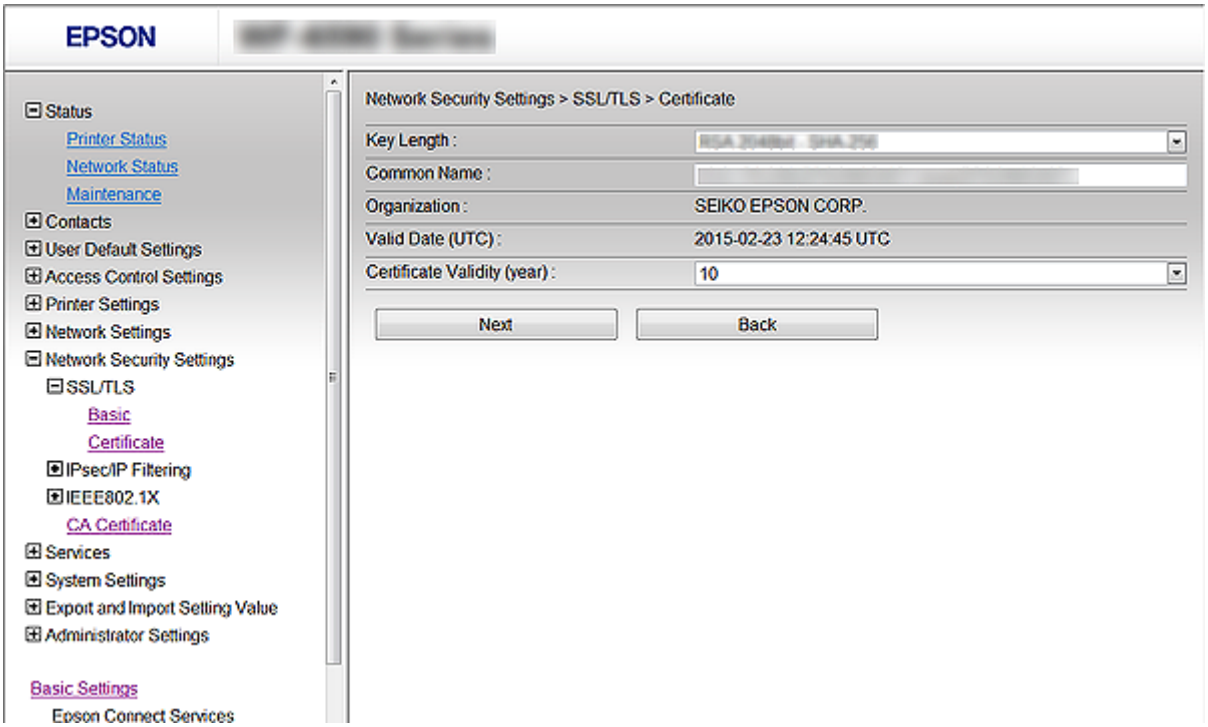
2. 按下 [Update]。

3. 輸入 [Common Name]。

   輸入 IP 位址或識別碼，如掃描器的 FQDN 名稱。您可輸入 1 至 128 個的字元。

   附註：
   您可使用逗號分隔辨別名稱 (CN)。

4. 指定憑證的有效期間。



5. 按下 [Next]。

   確認訊息會隨即顯示。

6. 按下 [OK]。

   掃描器會隨即更新。

附註：
按下 [Confirm] 確認憑證資訊。

相關資訊

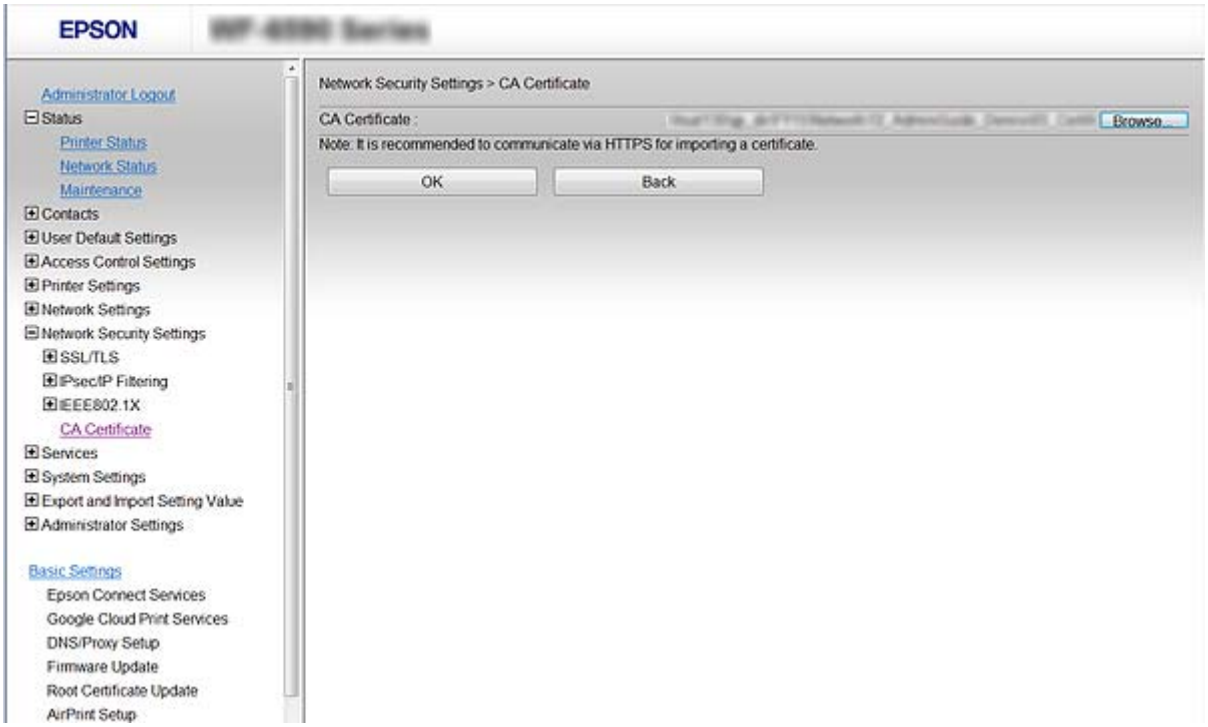
➡ 第10頁“存取 Web Config”

設定CA Certificate

您可匯入、顯示、刪除CA Certificate。

匯入 CA Certificate

1. 存取 Web Config，然後選擇 [Network Security Settings] > [CA Certificate]。
2. 按下 [Import]。
3. 指定您想要匯入的 CA Certificate。



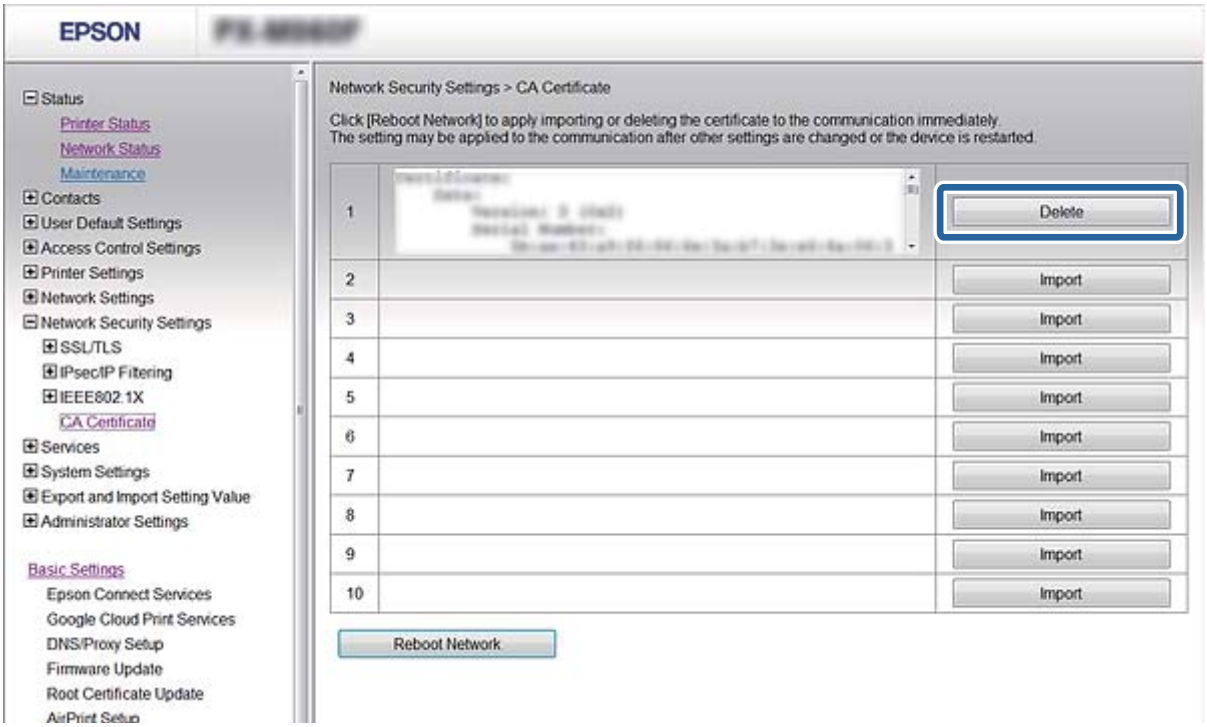
4. 按下 [OK]。

匯入完成後，您可返回 [CA Certificate] 畫面，即會顯示匯入的 CA Certificate。

刪除 CA Certificate

您可刪除匯入的 CA Certificate。

1. 存取 Web Config，然後選擇 [Network Security Settings] > [CA Certificate]。
2. 在您要刪除的 CA Certificate 旁邊，按下 [Delete]。



3. 在顯示的訊息中，確認您是否要刪除憑證。

重新啟動網路

匯入或刪除 CA Certificate 後，請重新啟動網路讓變更生效。

1. 存取 Web Config，然後選擇 [Network Security Settings] > [CA Certificate]。
2. 按下 [Reboot Network]。
3. 確認訊息然後繼續操作。

解決問題

解決問題的小祕訣

您可在下列手冊中找到更多資訊。

❏ 進階使用說明 (PDF 手冊)

提供有關使用掃描器、維護和解決問題的說明。

使用網路軟體的問題

無法存取 Web Config

掃描器的 IP 位址是否正確配置？

使用 EpsonNet Config 或 EPSON Scan 2 配置 IP 位址。您可以使用網路狀態表或從掃描器的控制面板確認目前設定資訊。

您的瀏覽器是否支援適用於 SSL/TLS 的 Encryption Strength 批量加密功能？

適用於 SSL/TLS 的 Encryption Strength 批量加密功能如下所述。Web Config 僅可在支援下列批量加密功能的瀏覽器中進行存取。檢查瀏覽器的加密支援。

❏ 80 位元：AES256/AES128/3DES

❏ 112 位元：AES256/AES128/3DES

❏ 128 位元：AES256/AES128

❏ 192 位元：AES256

❏ 256 位元：AES256

使用 SSL 通訊 (https) 存取 Web Config 時出現「過期」訊息。

若憑證過期，請重新取得憑證。若訊息在到期日之前顯示，請確認有正確配置掃描器的日期。

使用 SSL 通訊 (https) 存取 Web Config 時出現「安全性憑證的名稱不一致· · · 」訊息。

針對 [Common Name] 所輸入用以建立自我簽署憑證或 CSR 的掃描器 IP 位址不符合輸入至瀏覽器中的位址。請重新取得並匯入憑證，或變更掃描器名稱。

掃描器目前透過 Proxy 伺服器存取。

若掃描器目前使用 Proxy 伺服器，您必須配置瀏覽器的 Proxy 設定。

❏ Windows：

選擇[控制台] > [網路和網際網路] > [網際網路選項] > [連線] > [區域網路設定] > [Proxy 伺服器]，然後配置本機位址不使用 Proxy 伺服器。

❏ Mac OS X：

選擇[系統偏好設定] > [網路] > [進階] > [代理伺服器]，然後在[忽略這些主機與網域的代理伺服器設定]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

相關資訊

➡ 第10頁“存取 Web Config”

機型名稱及/或 IP 位址未顯示於 EpsonNet Config

當顯示 Windows 安全性畫面或防火牆畫面時，是否選取 [Block]、[Cancel] 或 [Shut down]？

若選取 [封鎖]、[取消]或 [關閉]，IP 位址和機型名稱將不會顯示在 EpsonNet Config 或 EpsonNet Setup 上。

若要修正此問題，請使用 Windows 防火牆及市售安全防護軟體將 EpsonNet Config 登錄為例外。若您有使用防毒或安全防護軟體，請先將其關閉，再嘗試使用 EpsonNet Config。

通訊錯誤逾時設定的時間是否太短？

執行 EpsonNet Config 並選取 [工具] > [選項] > [逾時]，然後增加 [通訊錯誤] 設定的時間長度。請注意，這麼做可能導致 EpsonNet Config 的執行速度變慢。

相關資訊

➡ 第11頁“執行 EpsonNet Config - Windows”

➡ 第12頁“執行 EpsonNet Config - Mac OS X”

使用網路安全性功能的問題

忘記預先共用金鑰

使用 Web Config 重新配置金鑰。

若要變更金鑰，請存取 Web Config，然後選擇 [Network Security Settings] > [IPsec/IP Filtering] > [Basic] > [Default Policy] 或 [Group Policy]。

無法使用 IPsec 通訊進行通訊

電腦設定是否使用不支援的演算法？

掃描器支援以下演算法。

加密方式	演算法
一致性演算法	AES-CBC 128
	AES-CBC 192
	AES-CBC 256
	3DES-CBC
	DES-CBC
雜湊演算法	SHA-1
	SHA2-256
	SHA2-384
	SHA2-512
	MD5
金鑰相容演算法	Diffie-Hellman Group2
	Diffie-Hellman Group1*、Diffie-Hellman Group14*、Elliptic Curve Diffie-Hellman P-256* 及 Elliptic Curve Diffie-Hellman P-384*

* 可用方式視機型而定。

相關資訊

➡ 第17頁“設定 IPsec/IP Filtering”

突然無法進行通訊

憑證中是否發生錯誤？

若掃描器的電源長時間未供電，則掃描器的日期和時間設定可能不正確。

當掃描器使用 IPsec/IP 篩選或 IEEE802.1X 進行連接時，若掃描器的日期和時間與憑證的有效期之間出現時間延遲，系統即會指示錯誤。因為掃描器識別出該憑證無法使用。如需有關掃描器錯誤指示器的詳細資料，請參閱掃描器的 *進階使用說明*。

您可以校正掃描器的日期和時間設定來解決此問題。使用 USB 纜線連接掃描器和電腦，開啟掃描器，然後使用 EPSON Scan 2 透過 USB 進行掃描。掃描器與電腦同步，其日期和時間設定將會進行校正。掃描器指示正常狀態。

若無法解決問題，請使用掃描器的控制面板來還原所有網路設定。連接掃描器和電腦，再次進行網路設定，然後進行客戶端認證、IPsec/IP 篩選或 IEEE802.1X 的設定。

掃描器的 IP 位址是否無效或已變更？

從另一台電腦 (如系統管理員的電腦) 上使用 EpsonNet Config 或 EPSON Device Admin 透過其 MAC 位址來存取掃描器。您可在掃描器上所粘的標籤上找到 MAC 位址。

可存取時，請使用 EpsonNet Config 或 EPSON Device Admin 來變更掃描器的 IP 位址。使用靜態 IP 位址。

若無法存取，請使用掃描器的控制面板來還原所有網路設定。連接掃描器和電腦，然後再次進行網路設定。設定掃描器的 IP 位址時，請使用靜態 IP 位址。

電腦的 IP 位址是否無效或已變更？

從另一台電腦 (如系統管理員的電腦) 上使用 EpsonNet Config 或 EPSON Device Admin 根據其 MAC 位址來存取掃描器。您可在掃描器上所貼的標籤上找到 MAC 位址。

可存取時，請使用 EpsonNet Config 或 EPSON Device Admin 來變更電腦的 IP 位址。使用靜態 IP 位址。

若無法存取，請使用掃描器的控制面板來還原所有網路設定。連接掃描器和電腦，然後再次進行網路設定。設定電腦的 IP 位址時，請使用靜態 IP 位址。

相關資訊

➡ 第17頁“設定 IPsec/IP Filtering”

配置 IPsec/IP 篩選後無法連接

設定值可能不正確。

從另一台電腦 (如系統管理員的電腦) 上使用 EpsonNet Config 或 EPSON Device Admin 根據其 MAC 位址來存取掃描器。您可在掃描器上所貼的標籤上找到 MAC 位址。

可存取時，請使用 EpsonNet Config 或 EPSON Device Admin 來進行 IPsec/IP 篩選設定。

若無法存取，請使用掃描器的控制面板來還原所有網路設定。連接掃描器和電腦，再次進行網路設定，然後進行 IPsec/IP 篩選設定。

相關資訊

➡ 第17頁“設定 IPsec/IP Filtering”

在配置 IEEE802.1X 之後無法存取掃描器

設定可能不正確。

使用掃描器的控制面板來還原所有網路設定。連接掃描器和電腦，再次進行網路設定，然後配置 IEEE802.1X。

相關資訊

➡ 第26頁“配置 IEEE802.1X 網路”

使用數位憑證的問題

無法匯入 CA 簽署憑證

CA 簽署憑證與 CSR 上的資訊是否相符？

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 簽署憑證是否超過 5 KB？

您無法匯入超過 5 KB 的 CA 簽署憑證。

憑證匯入密碼是否正確？

若忘記密碼，您無法匯入憑證。

相關資訊

➡ 第30頁“匯入 CA 簽署憑證”

無法更新自我簽署憑證

是否已經輸入 Common Name？

您必須輸入 [Common Name]。

是否在 Common Name 輸入了不支援的字元？例如，日文並不支援。

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

是否在 Common Name 中加入逗號或空格？

若輸入逗號， [Common Name] 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33頁“更新自我簽署憑證”

無法建立 CSR

是否已經輸入 Common Name？

您必須輸入 [Common Name]。

是否在 Common Name, Organization, Organizational Unit, Locality, State/Province 輸入了不支援的字元？例如，日文並不支援。

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

是否在 Common Name 中加入逗號或空格？

若輸入逗號， [Common Name] 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29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
Enter a Server Certificate.	原因： 您沒有選擇要匯入的憑證。 解決方法： 選擇檔案並按下 [Import]。
CA Certificate 1 is not entered.	原因： CA 憑證 1 未輸入，僅輸入 CA 憑證 2。 解決方法： 先匯入 CA 憑證 1。
Invalid value below.	原因： 檔案路徑及/或密碼包含不支援的字元。 解決方法： 確定針對項目輸入正確的字元。
Invalid date and time.	原因： 尚未設定掃描器的日期與時間。 解決方法： 使用 Web Config 或 EpsonNet Config 設定日期與時間。
Invalid password.	原因： 為 CA 憑證所設定的密碼與輸入的密碼不一致。 解決方法： 輸入正確的密碼。
Invalid file.	原因： 您沒有匯入 X509 格式的憑證檔案。 解決方法： 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： 您匯入的檔案太大。檔案大小上限為 5 KB。 解決方法： 若選擇正確的檔案，則憑證可能已損毀或是偽造的。
	原因： 憑證中包含的鏈結無效。 解決方法： 如需憑證的詳細資訊，請參閱憑證授權單位的網站。

訊息	原因/解決方法
Cannot use the Server Certificates that include more than three CA certificates.	原因： PKCS#12 格式的憑證檔案包含 3 個以上的 CA 憑證。 解決方法： 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。
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	原因： 憑證過期。 解決方法： ❏ 若憑證過期，請取得並匯入新的憑證。 ❏ 若憑證沒有過期，請確定已正確設定掃描器的日期與時間。
Private key is required.	原因： 憑證沒有已配對的私密金鑰。 解決方法： ❏ 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。 ❏ 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： 您已重新匯入使用 Web Config 從 CSR 取得的 PEM/DER 憑證。 解決方法： 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。
Setup failed.	原因： 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。 解決方法： 檢查指定的檔案及通訊後，重新匯入檔案。

相關資訊

➡ 第28頁“關於電子憑證”

意外刪除 CA 簽署憑證

是否保留憑證的備份檔案？

若有保留備份檔案，請重新匯入憑證。

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。建立 CSR 並取得新憑證。

相關資訊

➡ 第32頁“刪除 CA 簽署憑證”

掃描問題

無法執行 WSD 掃描

WSD 連接埠是否遭封鎖？

如果防火牆封鎖了 WSD 通訊，您無法進行掃描。務必確保電腦上的 WSD 連接埠 (連接埠：5357) 可以使用。

附錄

使用電子郵件伺服器

若要使用電子郵件功能，如使用 Epson Scan 2 或 Document Capture Pro 的掃描轉寄功能，則需配置電子郵件伺服器。

配置郵件伺服器

進行配置前，請檢查以下項目。

❏ 掃描器已經連接網路。

❏ 電腦的電子郵件伺服器資訊。

1. 存取 Web Config，然後選擇 [Network Settings] > [Email Server] > [Basic]。
2. 在各項目輸入數值。
3. 選擇 [OK]。

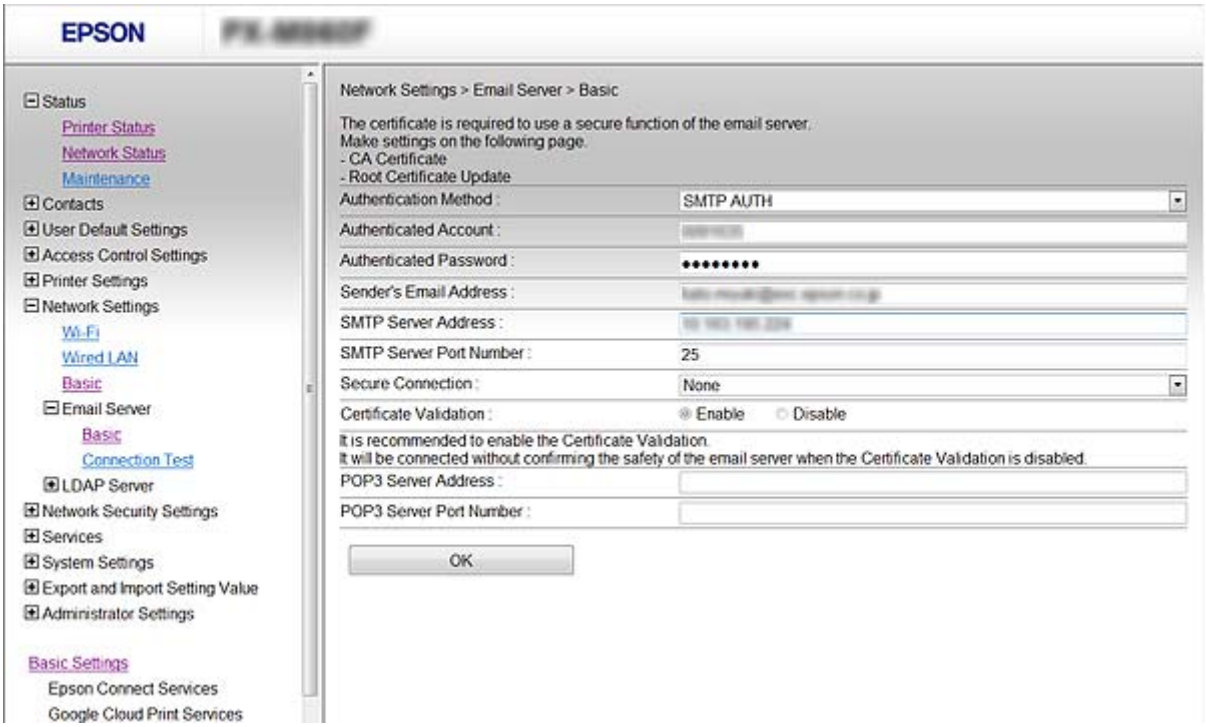
   您所選擇的設定會顯示。

相關資訊

➡ 第10頁“存取 Web Config”

➡ 第45頁“郵件伺服器設定項目”

郵件伺服器設定項目



項目	設定與說明	
Authentication Method	指定掃描器存取郵件伺服器的驗證方式。	
	Off	與郵件伺服器進行通訊時驗證功能會停用。
	SMTP AUTH	需要郵件伺服器支援 SMTP 驗證。
	POP before SMTP	選擇此方式時，請配置 POP3 伺服器。
Authenticated Account	若您選擇 [SMTP AUTH] 或 [POP before SMTP] 作為 [Authentication Method]，則請輸入已驗證的帳戶名稱 (0 至 255 個字元、ASCII 格式 (0x20—0x7E))。	
Authenticated Password	若您選擇 [SMTP AUTH] 或 [POP before SMTP] 作為 [Authentication Method]，則請輸入已驗證的密碼 (0 至 20 個字元之間，可使用 A—Z a—z 0—9 !# $ % & ' * + - ./ = ?^ _ { | } ~ @)。	
Sender's Email Address	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 Server Address	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 Server Port Number	輸入介於 1 至 65535 的數字。	
Secure Connection	指定電子郵件伺服器的安全連線方法。	
	None	若您在 [POP before SMTP] 中選擇了 [Authentication Method]，連線方法則會設定為 [None]。
	SSL/TLS	此功能在 [Authentication Method] 設定為 [Off] 或 [SMTP AUTH] 時即可使用。
	STARTTLS	此功能在 [Authentication Method] 設定為 [Off] 或 [SMTP AUTH] 時即可使用。

項目	設定與說明
Certificate Validation	若啟用此功能，憑證即可發揮效力。建議設定為 [Enable]。
POP3 Server Address	若您選擇 [POP before SMTP] 作為 [Authentication Method]，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 Server Port Number	若您選擇 [POP before SMTP] 作為 [Authentication Method]，則請輸入 1 至 65535 個字元之間的數字。

相關資訊

➡ 第44頁“配置郵件伺服器”

檢查郵件伺服器連線

1. 存取 Web Config，然後選擇 [Network Settings] > [Email Server] > [Connection Test]。
2. 選擇 [Start]。

   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。

相關資訊

➡ 第10頁“存取 Web Config”
➡ 第46頁“郵件伺服器連線測試參考”

郵件伺服器連線測試參考

訊息	說明
Connection test was successful.	成功建立與伺服器的連線時會顯示此訊息。
SMTP server communication error. Check the following. - Network Settings	以下情況會顯示訊息 ❏ 掃描器未連接網路 ❏ SMTP 伺服器停機 ❏ 進行通訊時網路斷線 ❏ 接收到不完整的資料
POP3 server communication error. Check the following. - Network Settings	以下情況會顯示訊息 ❏ 掃描器未連接網路 ❏ POP3 伺服器停機 ❏ 進行通訊時網路斷線 ❏ 接收到不完整的資料
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	以下情況會顯示訊息 ❏ 與 DNS 伺服器的連線失敗 ❏ SMTP 伺服器的名稱解析失敗

訊息	說明
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	以下情況會顯示訊息 ❏ 與 DNS 伺服器的連線失敗 ❏ POP3 伺服器的名稱解析失敗
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	SMTP 伺服器驗證失敗時，會顯示此訊息。
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	POP3 伺服器驗證失敗時，會顯示此訊息。
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	嘗試用不支援的通訊協定進行通訊時，會顯示此訊息。
Connection to SMTP server failed. Change Secure Connection to None.	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。
Connection to SMTP server failed. Change Secure Connection to 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。
Connection to SMTP server failed. Change Secure Connection to 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。
The connection is untrusted. Check the following. - Date and Time	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。
The connection is untrusted. Check the following. - CA Certificate	若掃描器沒有對應伺服器的根憑證，或 CA Certificate 並未匯入，則會顯示此訊息。
The connection is not secured.	若取得的憑證已經毀損，則會顯示此訊息。
SMTP server authentication failed. Change Authentication Method to 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 AUTH。
SMTP server authentication failed. Change Authentication Method to 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 AUTH。
Sender's Email Address is incorrect. Change to the email address for your email service.	指定的寄件者電子郵件地址不正確時，會顯示此訊息。
Cannot access the product until processing is complete.	掃描器忙碌時會顯示此訊息。

相關資訊

➡ 第46頁 “檢查郵件伺服器連線”

發生事件時接收電子郵件通知

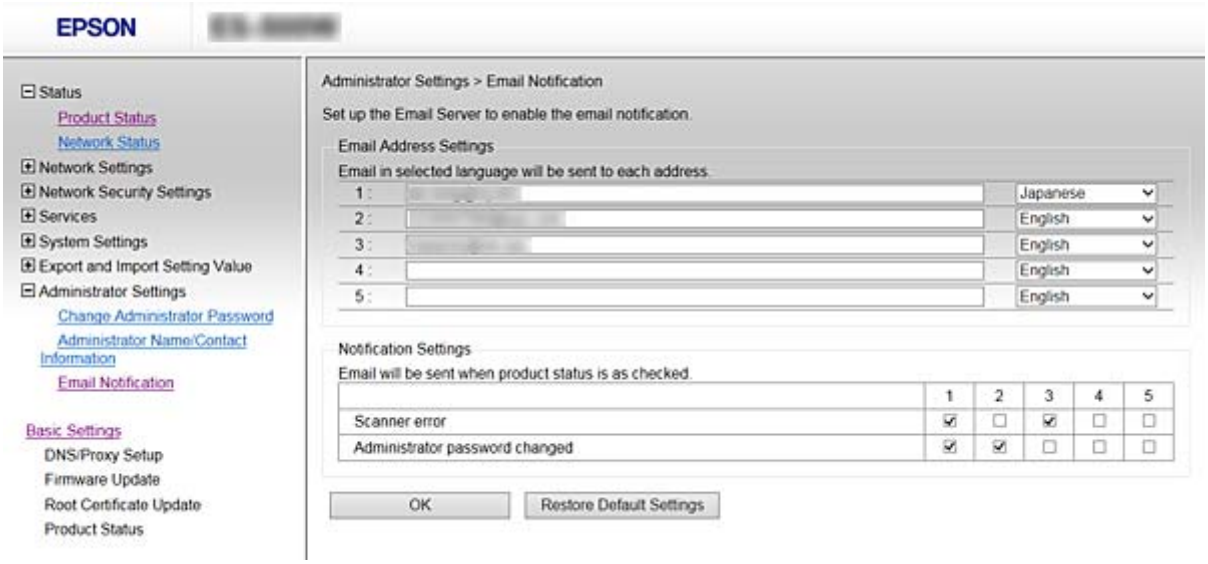
關於電子郵件通知

您可以使用此功能在事件發生時透過電子郵件接收警示訊息。您最多可註冊 5 個電子郵件地址，並選擇您希望收到通知的事件。

配置電子郵件通知

若要使用此功能，您必須配置郵件伺服器。

1. 存取 Web Config，然後選擇 [Administrator Settings] > [Email Notification]。
2. 輸入您要用於接收電子郵件通知的電子郵件地址。
3. 選擇電子郵件通知的語言。
4. 勾選您要接收的通知方塊。



5. 按下 [OK]。

相關資訊

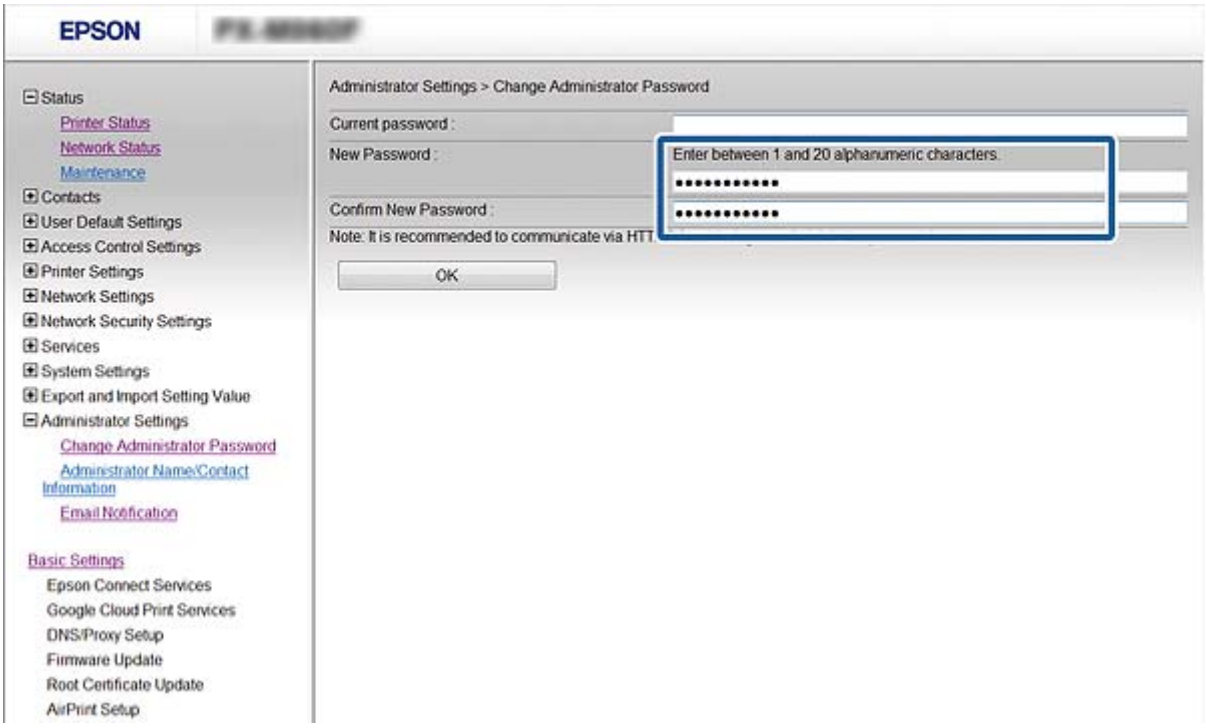
➡ 第10頁“存取 Web Config”
➡ 第44頁“使用電子郵件伺服器”

配置系統管理員密碼

設定系統管理員密碼時，用戶端將無法變更設定。

1. 存取 Web Config，然後選擇 [Administrator Settings] > [Change Administrator Password]。

2. 將密碼輸入至 [New Password] 和 [Confirm New Password]。
   若要變更為新密碼，請輸入目前的密碼。



3. 選擇 [OK]。
   附註：
   Web Config 和 EpsonNet Config 的系統管理員密碼皆相同。
   若忘記系統管理員密碼，請聯絡 Epson 授權服務中心。如需聯絡資訊，請參閱掃描器的說明文件。

相關資訊

➡ 第10頁“存取 Web Config”

配置通訊協定

您可啟用或停用受到控制的通訊協定。

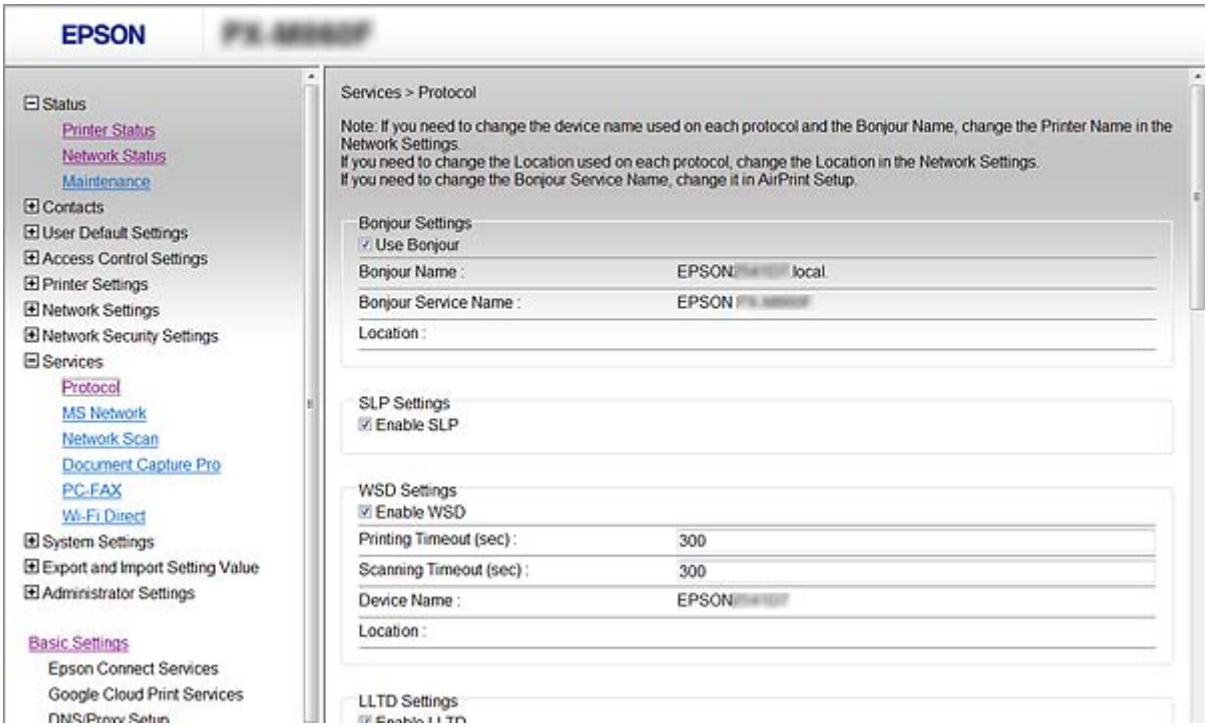
附註：
若您要使用 SNMPv3 通訊協定，請參閱 [使用 SNMPv3 通訊協定]。

1. 存取 Web Config，然後選擇 [Services] > [Protocol]。
2. 配置各個項目。
3. 按下 [Next]。
4. 按下 [OK]。
   設定即會套用到掃描器。

相關資訊

➡ 第24頁“使用 SNMPv3 通訊協定”

通訊協定設定項目



項目	設定值與描述
Bonjour Settings	
Use Bonjour	選擇此項目，透過 Bonjour 搜尋或使用裝置。
Bonjour Name	顯示 Bonjour 名稱。
Bonjour Service Name	顯示 Bonjour 服務名稱。
Location	顯示 Bonjour 位置名稱。
SLP Settings	
Enable SLP	選擇此項目啟用 SLP 功能。此項目會搭配 EpsonNet Config 中的推送掃描功能和網路搜尋功能使用。
WSD Settings	
Enable WSD	選擇此項目啟用透過 WSD 新增裝置功能，並從 WSD 連接埠進行掃描。
Scanning Timeout (sec)	輸入 WSD 掃描工作的通訊逾時值 (3 至 3,600 秒)。
Device Name	顯示 WSD 裝置名稱。
Location	顯示 WSD 位置名稱。
LLTD Settings	

項目	設定值與描述
Enable LLTD	選擇此項目啟用 LLTD。掃描器會顯示在 Windows 網路圖中。
Device Name	顯示 LLTD 裝置名稱。
LLMNR Settings	
Enable LLMNR	選擇此項目啟用 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 Settings	
Enable SNMPv1/v2c	選擇以啟用 SNMPv1/v2c。僅會顯示支援 SNMPv3 的掃描器。
Access Authority	啟用 SNMPv1/v2c 後，設定存取授權。選擇 [Read Only] 或 [Read/Write]。
Community Name (Read Only)	輸入 0 至 32 個 ASCII (0x20 至 0x7E) 字元。
Community Name (Read/Write)	輸入 0 至 32 個 ASCII (0x20 至 0x7E) 字元。

匯出和匯入 Web Config 設定

您可匯出 Web Config 設定並且複製到另一部掃描器。

匯出設定

匯出掃描器的各項設定。

1. 存取 Web Config，然後選擇 [Export and Import Setting Value] > [Export]。
2. 選擇您要匯出的設定值。

   選擇您要匯出的設定值。若您選擇父系類別，子類別也會選擇。但是，無法選擇在相同網路中重複 (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 [Export]。

> **重要事項：**
>
> 若您要匯出掃描器的網路設定，如掃描器名稱和 IP 位址，請選擇 [Enable to select the individual settings of device]，然後選擇更多項目。選擇的數值僅限用於替換掃描器。

匯入設定

將匯出的 Web Config 檔案匯入到掃描器。

重要事項：

匯入含有個別資訊 (如掃描器名稱或 IP 位址) 的設定值時，請確保同一個網路內不得出現一樣的 IP 位址。若 IP 位址重複，掃描器則無法使用設定值。

1. 存取 Web Config，然後選擇 [Export and Import Setting Value] > [Import]。
2. 選擇匯出檔，然後輸入加密密碼。
3. 按下 [Next]。
4. 選擇您想要匯入的設定，然後按下 [Next]。
5. 按下 [OK]。

設定即會套用到掃描器。

配置連接至掃描器的電腦

將掃描器連接到網路

您需要在電腦上安裝掃描器驅動程式 (EPSON Scan 2)，才可在網路中使用掃描器。

1. 安裝 EPSON Scan 2。

   從以下網站下載軟體，然後進行安裝。

   http://epson.sn > [其他軟體]

2. 開啟 EPSON Scan 2。

   ❏ Windows 10

   按一下開始鍵，然後選取[所有應用程式] > [EPSON] > [EPSON Scan 2] > [EPSON Scan 2]。

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   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/Windows Vista/Windows XP/Windows Server 2008 R2/Windows Server 2008/Windows Server 2003 R2/Windows Server 2003

   按下啟動鍵，選取[所有程式]或[程式] > [EPSON] > [Epson Scan 2] > [Epson Scan 2]。

   ❏ Mac OS X

   按一下[前往] > [應用程式] > [Epson Software] > [Epson Scan 2]。

   掃描器設定 畫面在您首次開啟 EPSON Scan 2 時會顯示。若顯示 EPSON Scan 2 畫面，請選取 [設定] (位於 [掃描器] 內)。

3. 如果禁用 [新增] 和 [刪除]，則按下 [啟用編輯]，然後允許使用者賬戶控制視窗上的變更。

   附註：
   狀態和操作視乎作業系統和登入使用者的權限而不同。對於 Mac OS X，按下按鍵圖示，並輸入管理員的使用者名稱和密碼，即可進行編輯。

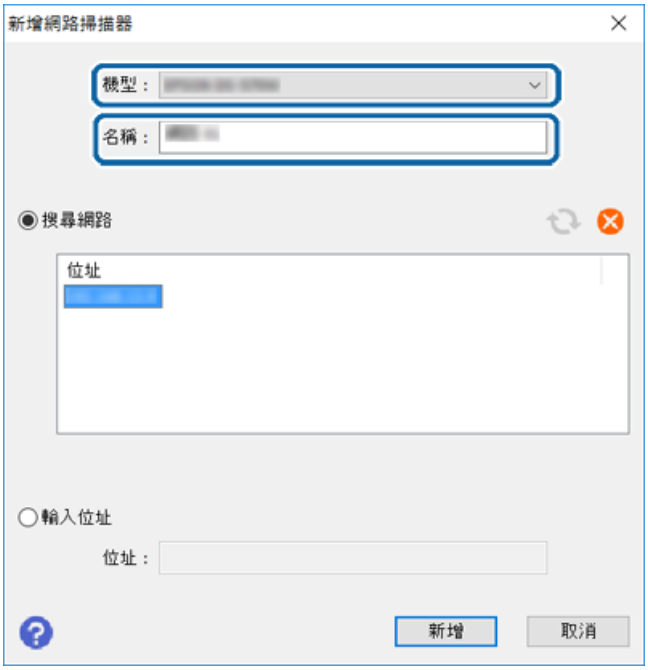
4. 按一下 [新增]。

   新增網路掃描器 畫面即會顯示。

   附註：
   對於 Mac OS X，按下 +。

5. 從 [機型] 中選取您希望使用的掃描器。

6. 在 [名稱] 中輸入掃描器的註冊名稱。



7. 按一下掃描器的 IP 位址，然後按一下 [新增]。

   重要事項：
   您無法搜尋路由器上不同網路區段中的掃描器。選取 [輸入位址] 以直接輸入 IP 位址。

8. 按下 [確定] (位於 掃描器設定 畫面)。

   EPSON Scan 2 畫面會顯示，您可測試掃描。