EPSON
EXCEED YOUR VISION

管理員使用說明

NPD5668-02 TC

目錄

著作權

商標

關於本手冊

標誌與符號. 6
本手冊使用的說明. 6
作業系統參考說明. 6

簡介

手冊構成. 8
本指南所用術語定義. 8

準備

掃描器設定與管理流程. 10
網路環境範例. 11
　掃描器連線設定範例的簡介. 11
準備網路連線. 12
　收集連線設定相關資訊. 12
　掃描器規格. 12
　使用連接埠號碼. 12
　IP 位址指派類型. 13
　DNS 伺服器與代理伺服器. 13
　設定網路連線的方法. 13

連線

連線至網路. 15
　從控制面板連線至網路. 15
　使用安裝程式連線至網路. 18

功能設定

要設定的軟體. 21
　Web Config (裝置的網頁). 21
使用掃描功能. 23
　從電腦掃描. 23
　使用控制面板掃描. 24
執行系統設定. 27
　從控制面板執行系統設定. 27
　使用 Web Config 執行系統設定. 28

基本安全性設定

基本安全性功能簡介. 30
配置系統管理員密碼. 30
　從控制面板配置管理員密碼. 31
　使用 Web Config 配置管理員密碼. 31
使用管理員密碼鎖定的項目. 32
通訊協定的控制. 33
　可啟用或停用的通訊協定. 33
　通訊協定設定項目. 34

操作與管理設定

確認裝置資訊. 37
管理裝置 (Epson Device Admin). 37
發生事件時接收電子郵件通知. 38
　關於電子郵件通知. 38
　配置電子郵件通知. 38
　配置郵件伺服器. 39
　檢查郵件伺服器連線. 41
更新韌體. 43
　使用 Web Config 更新韌體. 43
　透過使用 Epson Firmware Updater 更新韌體. . 43
備份設定. 44
　匯出設定. 44
　匯入設定. 44

解決問題

解決問題的小祕訣. 46
查看伺服器與網路裝置的記錄. 46
初始化網路設定. 46
　從控制面板回復網路設定. 46
檢查裝置與電腦之間的通訊. 46
　使用 Ping 指令檢查連接 — Windows. 46
　使用 Ping 指令檢查連線 — Mac OS. 48
使用網路軟體的問題. 49
　無法存取 Web Config. 49
　機型名稱及/或 IP 位址未顯示於 EpsonNet Config. 50

附錄

網路軟體簡介. 51
　Epson Device Admin. 51
　EpsonNet Config. 51
　EpsonNet SetupManager. 52

使用 EpsonNet Config 指派 IP 位址. 52
使用批次設定指派 IP 位址. 52
將 IP 位址指派給每個裝置. 54
掃描器使用的連接埠. 56

適用於企業的進階安全性設定

安全性設定與危險預防. 57
安全性功能設定. 58
與掃描器之間的 SSL/TLS 通訊. 58
關於電子憑證. 58
取得並匯入 CA 簽署憑證. 58
刪除 CA 簽署憑證. 62
更新自我簽署憑證. 63
設定CA Certificate. 64
使用 IPsec/IP 篩選加密的通訊. 66
關於 IPsec/IP Filtering. 66
配置 Default Policy. 66
配置 Group Policy. 69
IPsec/IP Filtering 的配置範例. 74
配置 IPsec/IP Filtering 的憑證. 75
使用 SNMPv3 通訊協定. 76
關於 SNMPv3. 76
配置 SNMPv3. 76
將掃描器連接至 IEEE802.1X 網路. 78
配置 IEEE802.1X 網路. 78
配置 IEEE802.1X 的憑證. 80
解決進階安全性的問題. 81
還原安全性設定. 81
使用網路安全性功能的問題. 82
使用數位憑證的問題. 83

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。

©Seiko Epson Corporation 2019.

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® 係一註冊商標，EPSON EXCEED YOUR VISION 或 EXCEED YOUR VISION 亦為 Seiko Epson Corporation 之商標。
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ 一般注意事項：本手冊內的其他產品名稱僅供識別之用，且可能為其各自擁有者的商標。Epson 放棄這些商標的任何與全部權利。

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。

本手冊使用的說明

- ❏ 掃描器驅動程式的螢幕擷取畫面及 Epson Scan 2 (掃描器驅動程式) 畫面係從 Windows 10 或 OS X El Capitan 取得。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為範例。儘管各型號可能會有些微差異，操作方法均同。
- ❏ LCD 螢幕上的某些功能表項目會隨著型號與設定而改變。

作業系統參考說明

Windows

在本手冊中，「Windows 10」、「Windows 8.1」、「Windows 8」、「Windows 7」、「Windows Vista」、「Windows XP」、「Windows Server 2016」、「Windows Server 2012 R2」、「Windows Server 2012」、「Windows Server 2008 R2」、,「Windows Server 2008」、「Windows Server 2003 R2」和「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

關於本手冊

- ❏ 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
- ❏ 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

本手冊中，「Mac OS」泛指「macOS Sierra」、「OS X El Capitan」、「OS X Yosemite」、「OS X Mavericks」、「OS X Mountain Lion」、「Mac OS X v10.7.x」和「Mac OS X v10.6.8」。

簡介

手冊構成

本手冊適合負責將印表機或掃描器連線至網路的裝置管理員使用，其包含有關如何進行設定以使用功能的資訊。

如需功能使用情況的資訊，請參閱 *進階使用說明*。

準備

說明管理員的工作、如何設定裝置，及用於管理的軟體。

連線

說明如何將裝置連線至網路或電話線。同時說明網路環境，如針對裝置使用連接埠、DNS 與代理伺服器資訊。

功能設定

說明裝置每項功能的設定。

基本安全性設定

說明每種功能的設定，如列印、掃描與傳真。

操作與管理設定

說明開始使用裝置後的操作，如資訊檢查與維護。

解決問題

說明網路的設定初始化與疑難排解。

適用於企業的進階安全性設定

說明加強裝置安全性的設定方法，如使用 CA 憑證、SSL/TLS 通訊與 IPsec/IP 篩選。

根據機型而定，本章中的一些功能不受支援。

本指南所用術語定義

下列術語用於本指南。

管理員

負責在辦公室或組織安裝及設定裝置或網路的人員。對於小型組織，該名人員也可能同時負責裝置與網路管理。對於大型組織，管理員具有管理部門或分公司群組單位網路或裝置的權力，而網路管理員則負責組織外的通訊設定，如網際網路。

網路管理員

負責控制網路通訊的人員。此人員需要設定路由器、代理伺服器、DNS 伺服器以及郵件伺服器以控制透過網際網路或網路進行的通訊。

使用者

使用裝置 (如印表機或掃描器) 的人員。

Web Config (**裝置的網頁**)

內建於裝置中的 Web 伺服器。其名為 Web Config。您可以使用瀏覽器在其上查看及變更裝置狀態。

工具

用來設定或管理裝置之軟體 (如 Epson Device Admin、EpsonNet Config、EpsonNet SetupManager 等) 的總稱。

推送掃描

從裝置的控制面板進行掃描的泛稱。

ASCII (**美國訊息交換標準代碼**)

這是其中一種標準字元代碼。其定義了 128 個字元，包括字母字元 (a—z、A—Z)、阿拉伯數字 (0—9)、符號、空白字元以及控制字元。本指南中所提及的「ASCII」是指如下所列的 0x20—0x7E (十六進位數字)，並不牽涉控制字元。

SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* 空白字元。

Unicode (UTF-8)

這是一種國際標準代碼，涵蓋全球主要語言。本指南中所提及的「UTF-8」是指 UTF-8 格式的編碼字元。

準備

本章說明管理員的角色及進行設定前的準備。

掃描器設定與管理流程

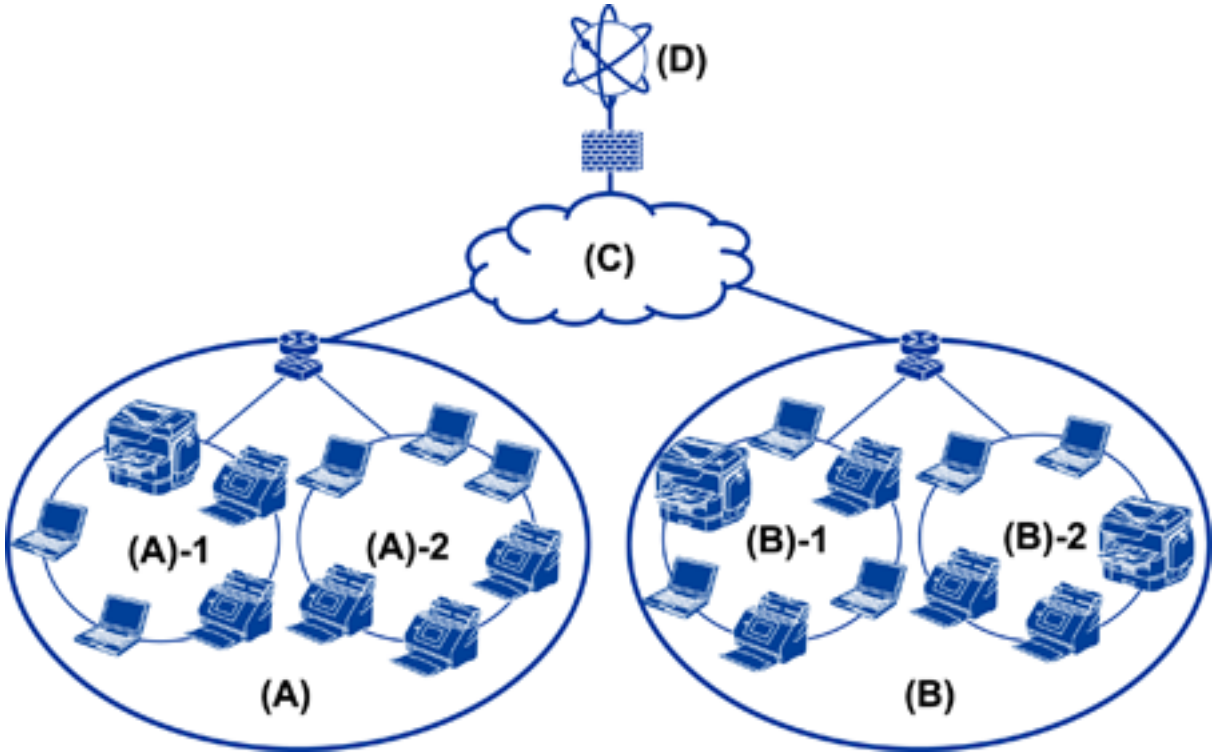
管理員可對掃描器進行網路連線設定、初始設定及維護，使其可供使用者使用。

1. 準備
   - ❏ 收集連線設定資訊
   - ❏ 決定連線方法
2. 連線
   - ❏ 從掃描器的控制面板連線網路
3. 設定功能
   - ❏ 掃描器驅動程式設定
   - ❏ 其他進階設定
4. 安全性設定
   - ❏ 管理員設定
   - ❏ SSL/TLS
   - ❏ 通訊協定控制
   - ❏ 進階安全性設定 (選項)
5. 操作與管理
   - ❏ 查看裝置狀態
   - ❏ 處理突發事件
   - ❏ 備份裝置設定

相關資訊

➡ 第10頁“準備”
➡ 第15頁“連線”
➡ 第21頁“功能設定”
➡ 第30頁“基本安全性設定”
➡ 第37頁“操作與管理設定”

網路環境範例



(A)：辦公室 1

❏ (A) — 1：LAN 1

❏ (A) — 2：LAN 2

(A)：辦公室 2

❏ (B) — 1：LAN 1

❏ (B) — 2：LAN 2

(C)：WAN

(D)：網際網路

掃描器連線設定範例的簡介

根據使用掃描器的方式，主要有兩種連線類型。透過集線器將掃描器連接到網路上的電腦。

❏ 伺服器/用戶端連線 (使用 Windows 伺服器、工作管理的掃描器)

❏ 點對點連線　(由用戶端電腦直接連線)

相關資訊

➡ 第12頁“伺服器/用戶端連線”

➡ 第12頁“點對點連線”

伺服器/用戶端連線

使用在伺服器上安裝的 Document Capture Pro Server 集中掃描器與工作管理。對於使用多部掃描器掃描特定格式之大量文件的工作而言，這最適合。

相關資訊

➡ 第8頁“本指南所用術語定義”

點對點連線

使用具有掃描器驅動程式 (如在用戶端電腦上安裝的 Epson Scan 2) 的個別掃描器。在用戶端電腦上安裝 Document Capture Pro (Document Capture) 可讓您在掃描器的個別用戶端電腦上執行工作。

相關資訊

➡ 第8頁“本指南所用術語定義”

準備網路連線

收集連線設定相關資訊

您必須擁有 IP 位址、閘道位址等才能進行網路連線。請事先檢查下列內容。

部分	項目	附註
裝置連線方法	❑ 乙太網路	使用 Category 5e 或更高等級的 STP (屏蔽雙絞線) 連接線進行乙太網路連線。
LAN 連線資訊	❑ IP 位址 ❑ 子網路遮罩 ❑ 預設閘道	如果您使用路由器的 DHCP 功能自動設定 IP 位址，則不需要檢查此資訊。
DNS 伺服器資訊	❑ 主 DNS 的 IP 位址 ❑ 輔助 DNS 的 IP 位址	如果您使用靜態 IP 位址作為 IP 位址，請配置 DNS 伺服器。 配置何時使用 DHCP 功能自動指派，及何時無法自動指派 DNS 伺服器。
代理伺服器資訊	❑ 代理伺服器名稱 ❑ 連接埠號碼	配置何時針對網際網路連線使用代理伺服器，及何時使用 Epson Connect 服務或韌體的自動更新功能。

掃描器規格

掃描器支援標準或連線模式的規格，請參閱 *進階使用說明*。

使用連接埠號碼

如需掃描器使用的連接埠號碼，請參閱「附錄」。

相關資訊

➡ 第56頁“掃描器使用的連接埠”

IP 位址指派類型

將 IP 位址指派給掃描器有兩種類型。

靜態 IP 位址：

將預先確定的專屬 IP 位址指派給掃描器。

此 IP 位址不會變更，即使關閉掃描器或路由器也不會變更，因此您可以透過 IP 位址管理裝置。

此類型適合管理許多掃描器的網路，如大型辦公室或學校。

由 DHCP 功能自動指派：

當支援 DHCP 功能的掃描器與路由器之間的通訊成功時，會自動指派正確的 IP 位址。

如果不方便變更特定裝置的 IP 位址，請事先保留 IP 位址，然後再予以指派。

DNS 伺服器與代理伺服器

如果您使用網際網路連線服務，請配置 DNS 伺服器。若未配置，則需要指定 IP 位址才能進行存取，因為您可能無法解析名稱。

代理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。對方伺服器只會與代理伺服器通訊。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。

您可以使用篩選功能來禁止存取特定 URL，因為代理伺服器能夠檢查通訊內容。

設定網路連線的方法

針對掃描器 IP 位址、子網路遮罩與預設閘道的連線設定，請以下列方式繼續。

使用控制面板：

針對每個掃描器，使用掃描器的控制面板配置設定。在配置掃描器的連線設定之後，連線至網路。

使用安裝程式：

如果使用安裝程式，會自動設定掃描器的網路與用戶端電腦。即使您對網路不是很瞭解，也可遵循安裝程式的指示進行設定。

使用工具：

從管理員電腦使用工具。您可以找到掃描器，然後設定掃描器，或建立 SYLK 檔案來對掃描器進行批次設定。您可以設定許多掃描器，但在設定之前，必須透過乙太網路纜線進行實體連接。因此，如果您可以建立乙太網路來進行設定，此為建議方法。

相關資訊

➡ 第15頁“從控制面板連線至網路”

準備

➡ 第18頁“使用安裝程式連線至網路”
➡ 第52頁“使用 EpsonNet Config 指派 IP 位址”

連線

本章說明將掃描器連線至網路的環境或程序。

連線至網路

從控制面板連線至網路

使用掃描器的控制面板將掃描器連線至網路。

有關掃描器控制面板的詳細資訊，請參閱 *進階使用說明*。

指派 IP 位址

設定基本項目，如 IP 位址、子網路遮罩 及 預設閘道。

1. 開啟掃描器。
2. 將畫面向掃描器控制面板的左側撥動，然後點選 [設定]。

3. 點選 [網路設定] > [變更設定]。
   如果項目未顯示，請向上撥動畫面以顯示項目。

4. 點選 [TCP/IP]。

5. 針對 [取得 IP 位址] 選取 [手動]。

附註：
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 6 到 7 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 8。

6. 點選 [IP 位址] 欄位，使用畫面上顯示的鍵盤輸入 IP 位址，然後點選 [確定]。

確認在上一個畫面反映的值。

7. 設定 [子網路遮罩] 與 [預設閘道]。

確認在上一個畫面反映的值。

附註：
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。

8. 點選 [DNS 伺服器] 的 [主要 DNS] 欄位，使用畫面上顯示的鍵盤輸入主 DNS 伺服器的 IP 位址，然後點選 [確定]。

   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 10。

9. 點選 [次要 DNS] 欄位，使用畫面上顯示的鍵盤輸入輔助 DNS 伺服器的 IP 位址，然後點選 [確定]。

   確認在上一個畫面反映的值。

10. 點選 [開始設定]。

11. 在確認畫面點選 [關閉]。

    如果不點選 [關閉]，在經過特定時間長度後，畫面會自動關閉。

連線至乙太網路

使用乙太網路連接線將掃描器連線至網路，然後檢查連線。

1. 使用乙太網路連接線連接掃描器與集線器 (L2 開關)。

   主畫面上的圖示會變更為 。

2. 在主畫面點選 。

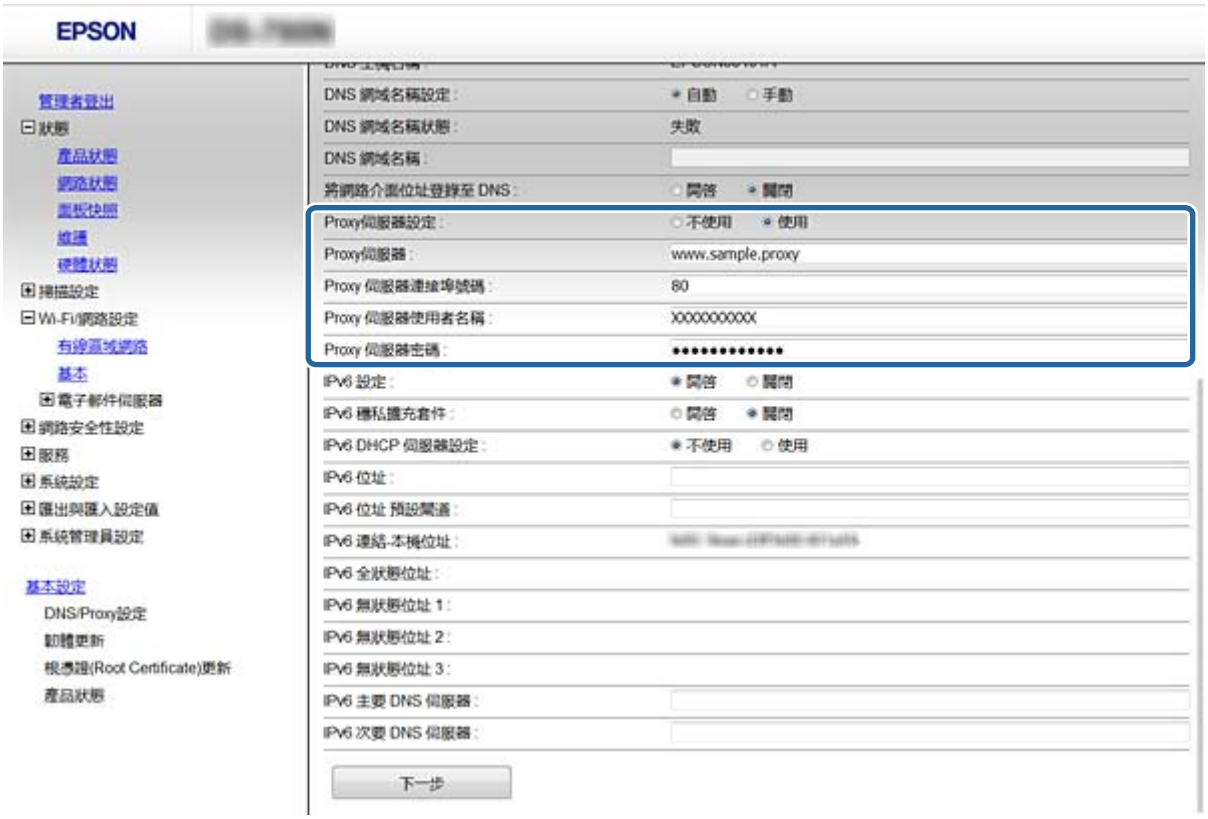
3. 向上撥動畫面，然後確定連線狀態與 IP 位址正確。

設定代理伺服器

代理伺服器無法在面板上設定。使用 Web Config 配置。

1. 存取 Web Config，然後選取 [Network Settings] > [Basic]。
2. 選取 [Proxy Server Setting] 中的 [Use]。
3. 在 [Proxy 伺服器] 中以 IPv4 位址或 FQDN 格式指定代理伺服器，然後在 [Proxy Server Port Number] 中輸入連接埠號碼。

   針對需要驗證的代理伺服器，輸入「代理伺服器驗證使用者名稱」與「代理伺服器驗證密碼」。
4. 按下 [下一步] 鍵。



5. 確認設定，然後按下 [設定]。

相關資訊

➡ 第22頁“存取 Web Config”

使用安裝程式連線至網路

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，直到顯示下列畫面，然後選取將掃描器連線至電腦的連線方法。

❏ Windows
選取連線類型，然後按下 [下一步]。

連線

❏ Mac OS

選取連線類型。

依照畫面上的指示進行操作。已安裝必要的軟體。

功能設定

本章說明要使用裝置各項功能而需要先行進行的設定。

要設定的軟體

此主題會說明使用 Web Config 從管理員的電腦進行設定的程序。

Web Config (裝置的網頁)

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。

存取 Web Config

在網頁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://192.0.2.111/

http://192.0.2.111/

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。

相關資訊

➡ 第58頁“與掃描器之間的 SSL/TLS 通訊”
➡ 第58頁“關於電子憑證”

使用掃描功能

根據您使用掃描器的方式，安裝下列軟體並使用軟體進行設定。

❏ 從電腦掃描

❏ 使用 Web Config 確認網路掃描服務的有效性 (原廠出貨時為有效)。

❏ 在您的電腦安裝 Epson Scan 2 並設定 IP 位址

❏ 使用工作掃描時，安裝 Document Capture Pro (Document Capture) 並設定工作設定。

❏ 從操作面板掃描

❏ 當使用 Document Capture Pro 或 Document Capture Pro Server　時：

安裝 Document Capture Pro 或 Document Capture Pro Server

DCP 設定 (伺服器模式、用戶端模式)。

❏ 使用 WSD 通訊協定時：

在 Web Config 或操作面板上確認 WSD 的有效性 (原廠出貨時為有效)

其他裝置設定 (Windows 電腦)。

從電腦掃描

安裝軟體，並檢查啟用網路掃描服務，來透過網路從電腦掃描。

相關資訊

➡ 第23頁“要安裝的軟體”
➡ 第24頁“啟用網路掃描”

要安裝的軟體

❏ Epson Scan 2

此為掃描器驅動程式。如果您從電腦使用裝置，請在每個用戶端電腦上安裝驅動程式。若已安裝 Document Capture Pro/Document Capture，您可以執行指派給裝置按鍵的操作。

使用 EpsonNet SetupManager，印表機驅動程式也可以一起以套件方式發佈。

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

在用戶端電腦上予以安裝。您可以從電腦及掃描器的操作面板使用安裝於網路的 Document Capture Pro/Document Capture 呼叫及執行登錄於電腦的工作。

您也可以透過網路從電腦掃描。掃描時需要 Epson Scan 2。

相關資訊

➡ 第52頁“EpsonNet SetupManager”

設定 Epson Scan 2 掃描器的 IP 位址

指定掃描器的 IP 位址，使掃描器能夠在網路上使用。

1. 從 [開始] > [所有程式] > [EPSON] > [Epson Scan 2] 啟動 [Epson Scan 2 Utility]。
   若已登錄另一部掃描器，請前往步驟 2。
   若未登錄，請前往步驟 4。
2. 在 [掃描器] 上按下 ▼。
3. 按下 [設定]。
4. 按下 [啟用編輯]，然後按下 [新增]。
5. 從 [機型] 選取掃描器型號名稱。
6. 從 [搜尋網路] 的 [位址] 中選取要使用之掃描器的 IP 位址。
   按下  並按下  來更新清單。如果您找不到掃描器的 IP 位址，請選取 [輸入位址] 並輸入 IP 位址。
7. 按下 [新增]。
8. 按下 [確定]。

啟用網路掃描

當透過網路從用戶端電腦掃描時，您可以設定網路掃描服務。會啟用預設設定。

1. 存取 Web Config 並選取 [Services] > [Network Scan]。
2. 確保已選取 [EPSON Scan] 的 [Enable scanning]。
   若其已選取，則表示此工作已完成。關閉 Web Config。
   若其已清除，請予以選取並前往下一步。
3. 按下 [下一步]。
4. 按下 [確定]。
   網路會重新連線，然後會啟用設定。

相關資訊

➡ 第22頁“存取 Web Config”

使用控制面板掃描

使用掃描器控制面板掃描至資料夾功能與掃描至郵件功能，以及將掃描結果傳送至郵件、資料夾等，可透過從電腦執行工作來進行。

當傳送掃描結果時，請使用 Document Capture Pro Server 或 Document Capture Pro 設定工作。

有關設定及設定工作的詳細資訊，請參閱 Document Capture Pro Server 或 Document Capture Pro 的文件或說明。

相關資訊

➡ 第25頁“Document Capture Pro Server/Document Capture Pro 設定”

➡ 第26頁“伺服器與資料夾的設定”

要在電腦上安裝的軟體

❏ Document Capture Pro Server

這是 Document Capture Pro 的伺服器版本。在 Windows 伺服器上安裝。伺服器可集中管理多部裝置及多個工作。工作可從多部掃描器同時執行。

透過使用經認證版本的 Document Capture Pro Server，您可以管理工作及掃描連結至使用者與群組的歷史紀錄。

有關 Document Capture Pro Server 的詳細資訊，請聯絡當地的 Epson 公司。

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

就像從電腦掃描一樣，您可以從控制面板中呼叫登錄於電腦的工作並予以執行。您無法同時從多部掃描器執行電腦工作。

Document Capture Pro Server/Document Capture Pro 設定

從掃描器的操作面板進行使用掃描功能的設定。

1. 存取 Web Config，然後選取 [Services] > [Document Capture Pro]。
2. 選取 [操作模式]。

   ❏ Server Mode：

   在使用 Document Capture Pro Server 時選取它。

   ❏ Client Mode：

   當您選取在網路中的每一部用戶端電腦上安裝之 Document Capture Pro (Document Capture) 的工作設定而不指定電腦時，請設定此項。
3. 根據所選模式設定下列項目。

   ❏ Server Mode：

   在 [Server Address] 中，指定安裝 Document Capture Pro Server 所在的伺服器。它可為 2 至 252 個字元的 IPv4、IPv6、主機名稱或 FQDN 格式。在 FQDN 格式中，可以使用 US-ASCII 字母、數字、字母與連字號 (字首與字尾除外)。

   ❏ Client Mode：

   指定 [Group Settings] 以使用從 Document Capture Pro (Document Capture) 中指定的掃描器群組。
4. 按下 [設定]。

相關資訊

➡ 第22頁“存取 Web Config”

伺服器與資料夾的設定

Document Capture Pro 與 Document Capture Pro Server 可將掃描的資料儲存到伺服器或用戶端電腦一次，並使用傳送功能來執行掃描至資料夾功能與掃描至郵件功能。

您需要授權與資訊才能從安裝 Document Capture Pro、Document Capture Pro Server 的電腦上傳送至電腦或雲端服務。

請參考以下說明，準備您將使用之功能的資訊。

您可以使用 Document Capture Pro 或 Document Capture Pro Server 進行這些功能的設定。有關設定的詳細資訊，請參閱 Document Capture Pro Server 或 Document Capture Pro 的說明文件或說明。

名稱	設定	要求
掃描至網路資料夾 (SMB)	建立並設定共用儲存資料夾	建立儲存資料夾之電腦的管理使用者帳戶。
	掃描至網路資料夾的目的地 (SMB)	用來登入具有儲存資料夾之電腦的使用者名稱與密碼，以及更新儲存資料夾的權限。
掃描至網路資料夾 (FTP)	FTP 伺服器登入的設定	FTP 伺服器的登入資訊以及更新儲存資料夾的權限。
掃描至電子郵件	電子郵件伺服器的設定	電子郵件伺服器資訊的設定
掃描至 Document Capture Pro (使用 Document Capture Pro Server 時)	登入雲端服務的設定	網際網路連線環境 登錄雲端服務的帳戶

使用 WSD 掃描 (僅限 Windows)

如果電腦使用 Windows Vista 或更新版本，您可以使用 WSD 掃描。

當可以使用 WSD 通訊協定時，[電腦 (WSD)] 功能表將會顯示在掃描器控制面板上。

1. 存取 Web Config，然後選取 [Services] > [Protocol]。
2. 確認在 [WSD Settings] 中已核取 [Enable WSD]。
   若已核取，即表示您的工作已完成，且您可以關閉 Web Config。
   若未核取，請予以核取並繼續下一步。
3. 按下 [下一步] 鍵。
4. 確認設定並按下 [設定]。

執行系統設定

從控制面板執行系統設定

設定螢幕亮度

設定 LCD 螢幕亮度。

1. 在主畫面點選 [設定]。
2. 點選 [通用設定] > [LCD 亮度]。
3. 點選  或  來調整亮度。
   您可從 1 至 9 調整。
4. 點選 [確定]。

設定聲音

設定面板操作聲音與錯誤聲音。

1. 在主畫面點選 [設定]。
2. 點選 [通用設定] > [音效設定]。
3. 視需要設定下列項目。
   - ❏ 操作聲音
     設定操作面板的操作聲音音量。
   - ❏ 錯誤聲音
     設定錯誤聲音音量。
4. 點選 [確定]。

相關資訊

➡ 第22頁“存取 Web Config”

偵測原稿多張進紙

決定功能以偵測要掃描之文件的多張進紙，並於發生多張進紙時停止掃描。

若要掃描被認定為多張進紙的原稿，如信封或貼有貼紙的紙張，請將其設定為關閉。

附註：
它也可以從 Web Config 或 Epson Scan 2 中設定。

1. 在主畫面點選 [設定]。

2. 點選 [外部掃描設定] > [超音波多頁進紙偵測]。
3. 點選 [超音波多頁進紙偵測] 以將其開啟或關閉。
4. 點選 [關閉]。

設定低速模式

設定以低速掃描，以便在掃描如紙條等薄文件時不會發生夾紙。

1. 在主畫面點選 [設定]。
2. 點選 [外部掃描設定] > [慢]。
3. 點選 [慢] 以將其開啟或關閉。
4. 點選 [關閉]。

使用 Web Config 執行系統設定

停用期間的省電設定

可為掃描器的停用期間進行省電設定。請根據您的使用環境設定時間。

附註：
您也可在掃描器的控制面板上進行省電設定。

1. 存取 Web Config，然後選取 [系統設定] > [Power Saving]。
2. 輸入 [Sleep Timer] 的時間，在發生停用時切換至省電模式。
3. 針對 [Power Off Timer] 選取關閉時間。
4. 按下 [確定]。

相關資訊

➡ 第22頁“存取 Web Config”

設定控制面板

設定掃描器的控制面板。您可依照下列方式設定。

1. 存取 Web Config，然後選取 [系統設定] > [Control Panel]。
2. 視需要設定下列項目。

   ❏ Language
   在控制面板上選取顯示語言。

❏ Panel Lock

如果選取 [ON]，當您執行需要管理員權限的操作時，必須輸入管理員密碼。如果未設定管理員密碼，面板鎖會停用。

❏ Operation Timeout

如果選取 [ON]，則當您以管理員身分登入時，會將您自動登出，並會在一段時間沒有任何活動之後回到初始畫面。

您可以設定 10 秒到 240 分鐘 (以秒為單位) 之間的時間。

3. 按下 [確定]。

相關資訊

➡ 第22頁“存取 Web Config”

設定外部界面的限制

您可從電腦限制 USB 連線。將其設定為限制用網路以外的方式掃描。

1. 存取 Web Config，然後選取 [系統設定] > [External Interface]。
2. 選取 [Enable] 或 [Disable]。

   若要限制，請選取 [Disable]。
3. 點選 [確定]。

與時間伺服器同步日期與時間

如果您使用 CA 憑證，可以防止發生時間問題。

1. 存取 Web Config，然後選取 [系統設定] > [Date and Time] > [Time Server]。
2. 針對 [Use Time Server] 選取 [Use]。
3. 針對 [Time Server Address] 輸入時間伺服器位址。

   您可以使用 IPv4、IPv6 或 FQDN 格式。輸入不超過 252 個字元。如果您未指定此項目，請將其保留空白。
4. 輸入 [Update Interval (min)]。

   您最多可以設定 10,800 分鐘 (以分鐘為單位)。
5. 按下 [確定]。

   附註：
   您可在 [Time Server Status] 中確認時間伺服器的連線狀態。

相關資訊

➡ 第22頁“存取 Web Config”

基本安全性設定

本章說明不需要特殊環境的基本安全性設定。

基本安全性功能簡介

我們將介紹 Epson 裝置的基本安全性功能。

功能名稱	功能類型	設定內容	防止目標
設定管理員密碼	鎖定與系統相關的設定，如網路與 USB 連線設定，以便除了管理員以外無人能夠變更它。	管理員可設定裝置的密碼。 可從 Web Config、控制面板、Epson Device Admin 與 EpsonNet Config 的任何位置配置或更新。	防止非法讀取及變更儲存在裝置中的資訊，如 ID、密碼、網路設定及聯絡人。此外，也可大範圍降低安全風險，如洩漏網路環境或安全性原則的資訊。
SSL/TLS 通訊	當從裝置存取網際網路上的 Epson 伺服器時，如使用電腦透過瀏覽器或韌體更新來通訊，通訊內容會受到 SSL/TLS 通訊加密。	取得 CA 簽署憑證，然後將其匯入至掃描器。	透過 CA 簽署憑證清除裝置的識別碼，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，且其會防止洩漏列印資料與設定資訊的內容。
控制協定	可控制用於在裝置與電腦之間通訊的協定，並啟用/停用功能。	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。

相關資訊

➡ 第21頁“關於 Web Config”
➡ 第51頁“EpsonNet Config”
➡ 第51頁“Epson Device Admin”
➡ 第30頁“配置系統管理員密碼”
➡ 第33頁“通訊協定的控制”

配置系統管理員密碼

在設定管理員密碼時，除管理員之外的使用者將無法變更系統管理的設定。您可使用 Web Config、掃描器的控制面板或軟體 (Epson Device Admin 或 EpsonNet Config) 設定及變更管理員密碼。使用軟體時，請參閱各軟體的說明文件。

相關資訊

➡ 第31頁“從控制面板配置管理員密碼”
➡ 第31頁“使用 Web Config 配置管理員密碼”
➡ 第51頁“EpsonNet Config”
➡ 第51頁“Epson Device Admin”

從控制面板配置管理員密碼

您可從掃描器的控制面板設定管理員密碼。

1. 在主畫面點選 [設定]。
2. 點選 [系統管理] > [管理員設定]。
   如果項目未顯示，請向上撥動畫面以顯示項目。
3. 點選 [管理員密碼] > [登錄]。
4. 輸入新密碼，然後點選 [確定]。
5. 重新輸入密碼，然後點選 [確定]。
6. 在確認畫面點選 [確定]。
   管理員設定畫面即會顯示。
7. 點選 [鎖定設定]，然後點選確認畫面的 [確定]。
   鎖定設定 設定為 [開啟]，當您操作鎖定的功能表項目時，將需要管理員密碼。

附註：

- ❏ 如果您將 [設定] > [通用設定] > [操作逾時] 設定為 [開啟]，則在控制面板處於停用狀態一段時間之後，掃描器會將您登出。
- ❏ 當您在 [管理員密碼] 畫面選取 [變更] 或 [重設] 並輸入管理員密碼時，您可以變更或刪除管理員密碼。

使用 Web Config 配置管理員密碼

您可使用 Web Config 設定管理員密碼。

1. 存取 Web Config，然後選取 [Administrator Settings] > [Change Administrator Authentication Information]。

2. 將密碼輸入至 [New Password] 和 [Confirm New Password]。必要時，請輸入使用者名稱。
   若要變更為新密碼，請輸入目前的密碼。

3. 選取 [確定]。

   附註：
   - ❏ 若要設定或變更鎖定的功能表項目，請按下 [Administrator Login]，然後輸入管理員密碼。
   - ❏ 若要刪除管理員密碼，請按下 [Administrator Settings] > [Delete Administrator Authentication Information]，然後輸入管理員密碼。

相關資訊

➡ 第22頁“存取 Web Config”

使用管理員密碼鎖定的項目

管理員擁有對裝置所有功能進行設定及變更的權限。

此外，如果您為裝置設定了管理員密碼，您可將其鎖定，使您無法變更與裝置管理相關的項目。

管理員可以控制的項目如下所列。

項目	描述
掃描器設定	設定多張進紙偵測與低速模式。
乙太網路連線設定	變更裝置名稱與 IP 位址、DNS 伺服器或代理伺服器的設定，以及網路連線相關設定變更。
使用者服務設定	用來控制通訊協定、網路掃描與 Document Capture Pro 服務的設定。

項目	描述
電子郵件伺服器設定	與裝置直接通訊之電子郵件伺服器的設定。
安全性設定	網路安全性設定，如 SSL/TLS 通訊、IPsec/IP 篩選與 IEEE802.1X。
根憑證更新	Document Capture Pro Server 驗證與從 Web Config 進行韌體更新所需的根憑證更新。
韌體更新	檢查並更新裝置韌體。
時間、計時器設定	睡眠轉換模式、自動關機、日期/時間、非操作計時器、與計時器相關的其他設定。
回復至預設值	要重設為出廠設定之掃描器的設定。
管理員設定	管理員鎖定或管理員密碼的設定。
已認證裝置設定	驗證裝置的 ID 設定。當在支援驗證裝置的驗證系統上使用掃描器時設定。

通訊協定的控制

您可透過多種途徑和通訊協定進行掃描。您也可以從未指定數量的網路電腦中使用網路掃描。例如，允許僅使用指定途徑與通訊協定來掃描。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。

配置通訊協定配置。

1. 存取 Web Config，然後選取 [Services] > [Protocol]。
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22頁“存取 Web Config”
➡ 第33頁“可啟用或停用的通訊協定”
➡ 第34頁“通訊協定設定項目”

可啟用或停用的通訊協定

通訊協定	描述
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 可用於 Epson Scan 2 並進行 EpsonNet Config. 中的網路搜尋。
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。

通訊協定	描述
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。
SNMPv3 Settings	您可指定是否啟用 SNMPv3。這可用來設定加密裝置、監控等。

相關資訊

➡ 第33頁 “通訊協定的控制”

➡ 第34頁 “通訊協定設定項目”

通訊協定設定項目

項目	設定值與描述
Bonjour Settings	
Use Bonjour	選取此項目，透過 Bonjour 搜尋或使用裝置。
Bonjour Name	顯示 Bonjour 名稱。
Bonjour Service Name	您可以顯示及設定 Bonjour 服務名稱。
Location	顯示 Bonjour 位置名稱。
SLP Settings	

項目	設定值與描述
Enable SLP	選取此項目啟用 SLP 功能。其用於 Epson Scan 2 與 EpsonNet Config 中的網路探索。
WSD Settings	
Enable WSD	選取此項目啟用透過 WSD 新增裝置功能，並從 WSD 連接埠進行列印與掃描。
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	
Enable LLTD	選取此項目啟用 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 Settings	
Enable SNMPv1/v2c	選取以啟用 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。選取 [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。
SNMPv3 Settings	
Enable SNMPv3	若核取此方塊，SNMPv3 會啟用。
User Name	使用 1 位元輸入 1 至 32 個字元。
Authentication Settings	
Algorithm	選取驗證 SNMPv3 的演算法。
Password	輸入驗證 SNMPv3 的密碼。 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。
Confirm Password	輸入您配置用於確認的密碼。
Encryption Settings	
Algorithm	選取加密 SNMPv3. 的演算法
Password	輸入加密 SNMPv3 的密碼。 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。

項目	設定值與描述
Confirm Password	輸入您配置用於確認的密碼。
Context Name	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。

相關資訊

➡ 第33頁“通訊協定的控制”

➡ 第33頁“可啟用或停用的通訊協定”

操作與管理設定

本章說明與裝置日常操作和管理相關的項目。

確認裝置資訊

您可使用 Web Config 從 [狀態] 中查看操作裝置的下列資訊。

❏ 產品狀態

查看語言、狀態、產品型號、MAC 位址等。

❏ Network Status

查看網路連線狀態、IP 位址、DNS 伺服器等資訊。

❏ Panel Snapshot

顯示裝置控制面板上所顯示之螢幕影像的快照。

❏ Maintenance

檢查開始日期、掃描資訊等。

❏ Hardware Status

檢查掃描器的狀態。

相關資訊

➡ 第22頁“存取 Web Config”

管理裝置 (Epson Device Admin)

您可以使用 Epson Device Admin 管理並操作許多裝置。Epson Device Admin 允許您管理位於不同網路中的裝置。下文概述主要的管理功能。

如需關於功能及使用軟體的詳細資訊，請參閱 Epson Device Admin 的說明文件或說明。

❏ 找到裝置

您可以找到網路中的裝置，然後將其登錄至清單。如果 Epson 裝置 (如印表機與掃描器) 連線至與管理員電腦相同的網路區段，您可以找到它們，即使並未為其指派 IP 位址也是如此。

您也可以找到透過 USB 連接線連線至網路中電腦的裝置。您需要在電腦上安裝 Epson Device USB Agent。

❏ 設定裝置

您可建立包含設定項目 (如網路界面與紙張來源) 的範本，再將其作為共用設定套用至其他裝置。當它連線至網路時，您可以在尚未指派 IP 位址的裝置上指派 IP 位址。

❏ 監控裝置

您可以定期取得網路上裝置的狀態與詳細資訊。您也可以監控透過 USB 連接線連線至網路中電腦的裝置，以及已登錄至裝置清單之其他公司的裝置。若要監控透過 USB 連接線連線的裝置，您需要安裝 Epson Device USB Agent。

❏ 管理警示

您可以監控關於裝置與耗材狀態的警示。系統會根據設定的條件，自動將通知電子郵件傳送至管理員。

❏ 管理報告

您可以在系統累積裝置使用情況與耗材相關資料時建立定期報告。然後，您可以儲存這些建立的報告，並透過電子郵件傳送。

相關資訊

➡ 第51頁“Epson Device Admin”

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。

必須將郵件伺服器配置為使用此功能。

相關資訊

➡ 第39頁“配置郵件伺服器”

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 [確定]。

相關資訊

➡ 第22頁“存取 Web Config”
➡ 第39頁“配置郵件伺服器”

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 [確定]。
   您所選擇的設定會顯示。

相關資訊

➡ 第22頁“存取 Web Config”
➡ 第40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。	

項目	設定與說明	
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。
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39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22頁“存取 Web Config”
➡ 第41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

訊息	說明
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
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。

訊息	說明
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41頁“檢查郵件伺服器連線”

更新韌體

使用 Web Config 更新韌體

使用 Web Config 更新韌體。裝置必須連線至網際網路。

1. 存取 Web Config，然後選取 [Basic Settings] > [Firmware Update]。
2. 按下 [Start]。

   即會開始韌體確認，如果存在更新的韌體，會顯示韌體資訊。
3. 按下 [Start]，然後依照畫面上的指示進行操作。

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。如需詳細資訊，請參閱 Epson Device Admin 的指南或說明。

相關資訊

➡ 第22頁“存取 Web Config”
➡ 第51頁“Epson Device Admin”

透過使用 Epson Firmware Updater 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。

1. 存取 Epson 網站並下載韌體。
2. 使用 USB 纜線將包含下載韌體的電腦連接至裝置。
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。

備份設定

您可匯出 Web Config 中的設定項目，以將這些項目複製到其他掃描器。

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。

相關資訊

➡ 第22頁“存取 Web Config”

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 [下一步]。
4. 選擇您想要匯入的設定，然後按下 [下一步]。
5. 按下 [確定]。

設定即會套用到掃描器。

相關資訊

➡ 第22頁“存取 Web Config”

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

提供有關使用掃描器、維護和解決問題的說明。

查看伺服器與網路裝置的記錄

如果網路連線有問題，可以透過確認郵件伺服器、LDAP 伺服器等的記錄、使用系統設備記錄與命令 (例如路由器) 的網路記錄檢查狀態，來找出原因。

初始化網路設定

從控制面板回復網路設定

您可以將所有的網路設定回復至預設值。

1. 在主畫面點選 [設定]。
2. 點選 [系統管理] > [回復至出廠預設值] > [網路設定]。
3. 查看訊息，然後點選 [是]。
4. 顯示完成訊息後，點選 [關閉]。

   如果不點選 [關閉]，在經過特定時間長度後，畫面會自動關閉。

檢查裝置與電腦之間的通訊

使用 Ping 指令檢查連接 — Windows

您可以使用 Ping 指令來確保電腦是否連接至掃描器。請遵循下列步驟，使用 Ping 指令檢查連接。

1. 檢查您想要檢查的掃描器 IP 連接位址。

   您可以使用 Epson Scan 2 檢查該位址。

2. 顯示電腦指令提示畫面。

   ❏ Windows 10

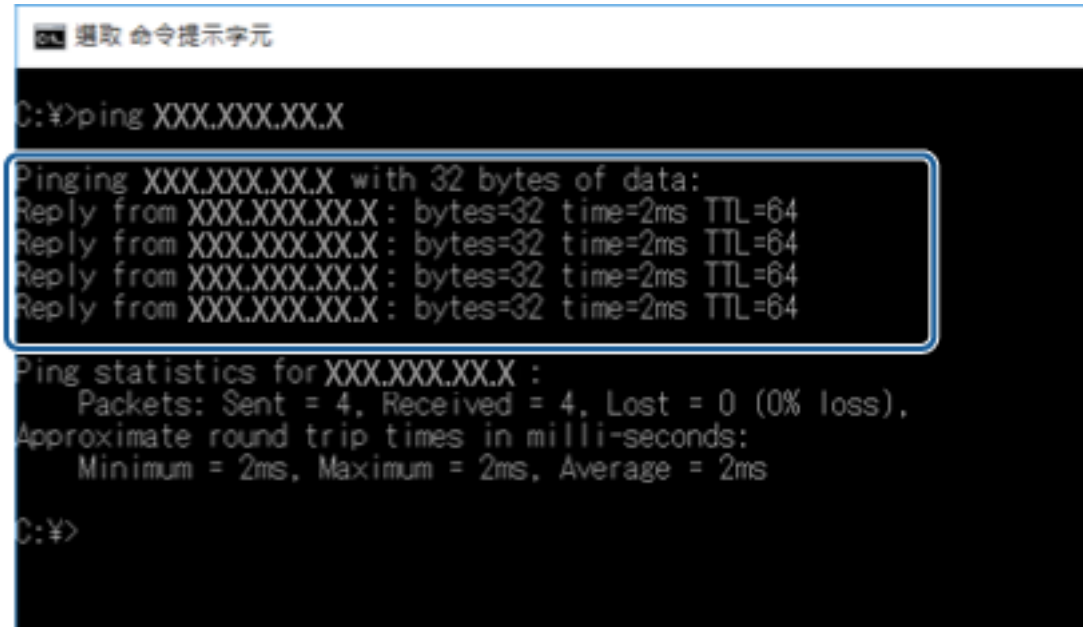
   在開始鍵上按滑鼠右鍵或按住，然後選擇[命令提示字元]。

❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
顯示應用程式畫面，然後選擇[命令提示字元]。

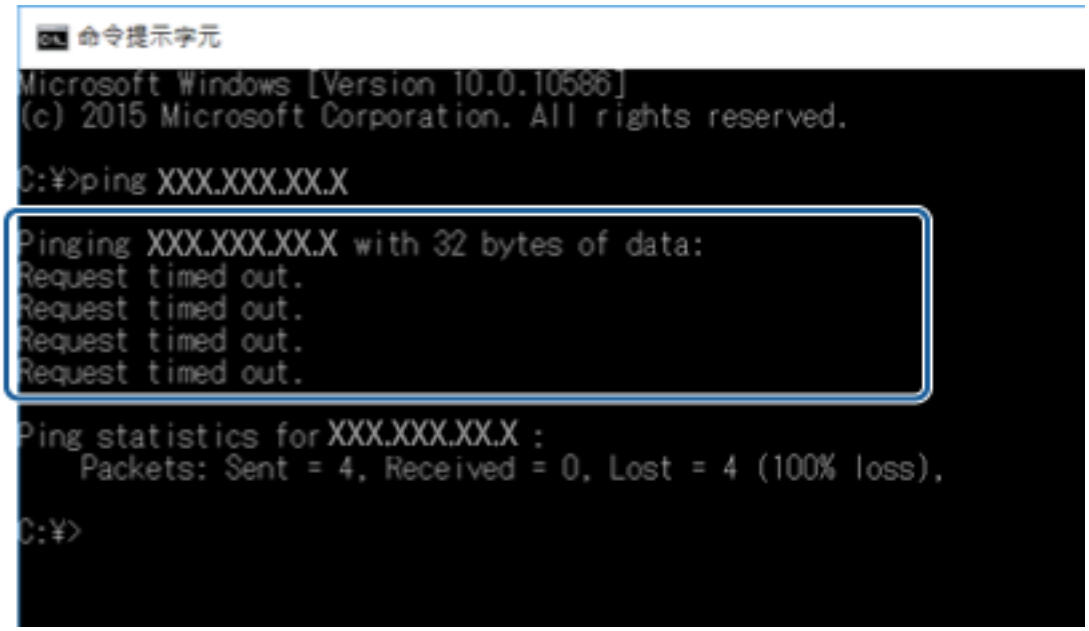
❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 或更舊版本
按下開始鍵，選擇[程式集]或[程式] > [附屬應用程式] > [命令提示字元]。

3. 輸入「ping xxx.xxx.xxx.xxx」，然後按下確認 (Enter) 鍵。
輸入掃描器的 IP 位址 xxx.xxx.xxx.xxx。

4. 檢查通訊狀態。
如果掃描器和電腦正在通訊，將顯示以下訊息。



如果掃描器和電腦未在通訊，將顯示以下訊息。

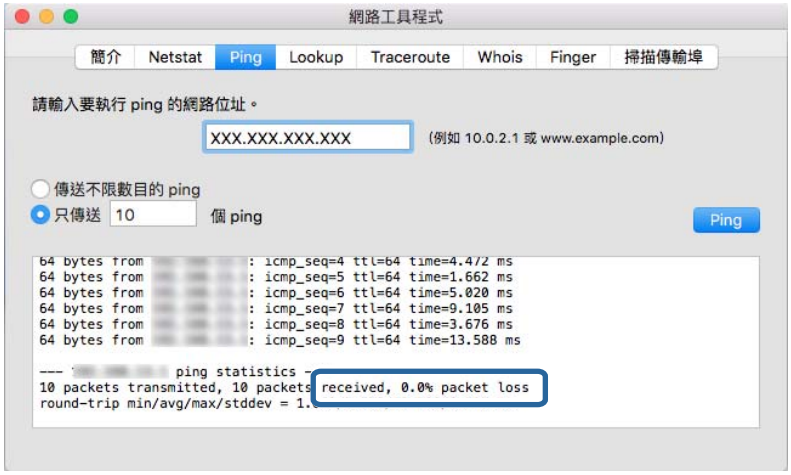


使用 Ping 指令檢查連線 — Mac OS

您可以使用 Ping 指令來確保電腦連線至掃描器。請遵循下列步驟，使用 Ping 指令檢查連線。

1. 檢查您想要檢查的掃描器連線 IP 位址。
   您可以使用 Epson Scan 2 檢查該位址。
2. 執行網路公用程式。
   在 [Spotlight] 中輸入「網路公用程式」。
3. 按下 [Ping] 索引標籤，輸入您在步驟 1 檢查的 IP 位址，然後按下 [Ping]。

4. 檢查通訊狀態。
   如果掃描器和電腦正在通訊，將顯示以下訊息。



如果掃描器和電腦未在通訊，將顯示以下訊息。

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 Epson Device Admin 或 EpsonNet Config 配置 IP 位址。

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：

選取[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：

選取[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22頁“存取 Web Config”

➡ 第15頁“指派 IP 位址”

➡ 第52頁“使用 EpsonNet Config 指派 IP 位址”

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 [Tools] > [Options] > [Timeout]，然後增加 [Communication Error] 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51頁“執行 EpsonNet Config — Windows”

➡ 第52頁“執行 EpsonNet Config — Mac OS”

附錄

網路軟體簡介

下文描述配置及管理裝置的軟體。

Epson Device Admin

Epson Device Admin 是一款可讓您將裝置安裝至網路，然後配置和管理裝置的應用程式。您可以獲取如狀態與耗材的裝置詳細資訊、傳送警示通知，及建立裝置使用情況報告。您也可以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。

執行 Epson Device Admin (僅適用於 Windows)

選取[所有程式] > [EPSON] > [Epson Device Admin] > [Epson Device Admin]。

附註：
若出現防火牆警示，請允許存取 Epson Device Admin。

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。

執行 EpsonNet Config — Windows

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

附註：
若出現防火牆警示，請允許存取 EpsonNet Config。

執行 EpsonNet Config — Mac OS

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

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。

使用 EpsonNet Config 指派 IP 位址

您可使用 EpsonNet Config 將 IP 位址指派給掃描器。EpsonNet Config 可讓您將 IP 位址指派給在使用乙太網路連接線連線之後尚未獲得指派的掃描器。

使用批次設定指派 IP 位址

建立批次設定的檔案

您可使用 MAC 位址與機型名稱作為金鑰，建立用來設定 IP 位址的新 SYLK 檔案。

1. 開啟試算表應用程式 (如 Microsoft Excel) 或文字編輯器。
2. 在第一列輸入「Info_MACAddress」、「Info_ModelName」與「TCPIP_IPAddress」作為設定項目名稱。

   輸入下列文字字串的設定項目。為了區分大寫/小寫以及雙位元組/單位元組字元，如果只有一個字元不同，也不會辨識項目。

   如下所述輸入設定項目名稱；否則 EpsonNet Config 無法辨識設定項目。

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. 輸入每個網路界面的 MAC 位址、機型名稱以及 IP 位址。

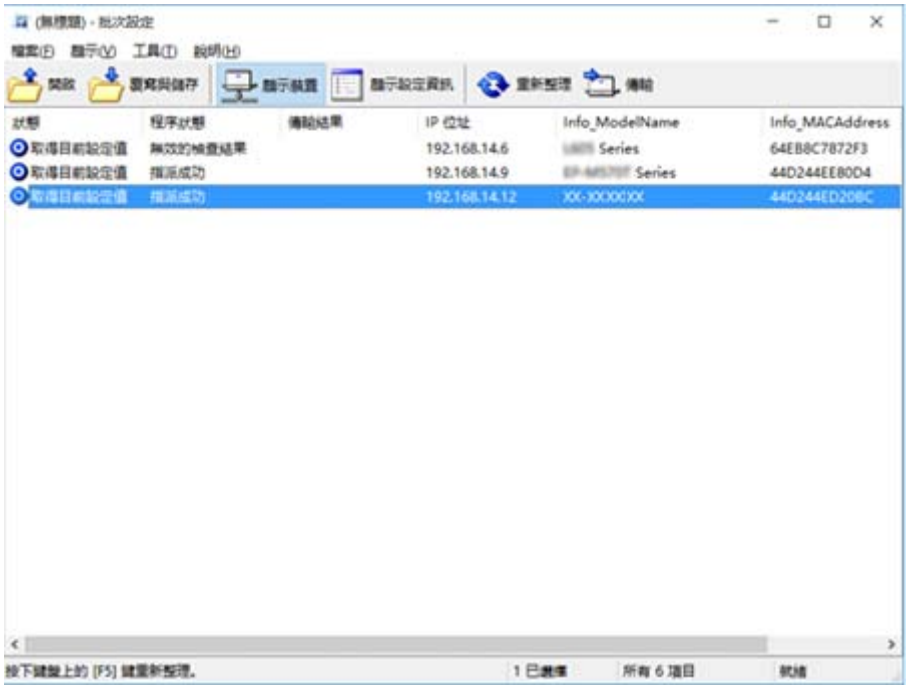
Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. 輸入名稱並儲存為 SYLK 檔案 (*.slk)。

使用配置檔案進行批次設定

在配置檔案 (SYLK 檔案) 中一次指派多個 IP 位址。您需要先建立配置檔案再進行指派。

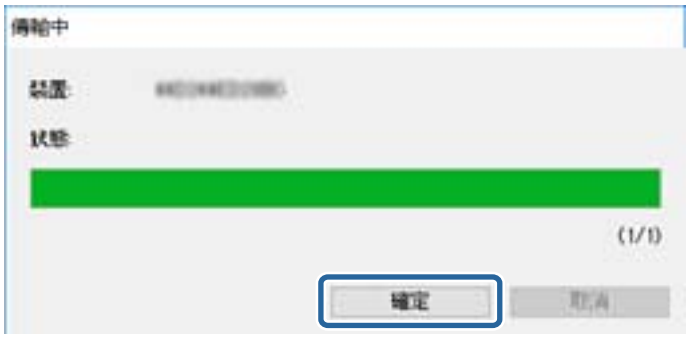
1. 使用乙太網路連接線將所有裝置連線至網路。
2. 開啟掃描器。
3. 啟動 EpsonNet Config。
   網路上掃描器的清單即會顯示。此清單可能需要一段時間才會顯示。
4. 按下 [Tools] > [Batch Settings]。
5. 按下 [Open]。
6. 在檔案選取畫面上，選取包含設定的 SYLK 檔案 (*.slk)，然後按下 [Open]。
7. 選取您要針對其執行批次設定且 [Status] 欄設定為 [Unassigned]、[Process Status] 設定為 [Assign Successful] 的裝置。
   當進行多重選取時，請按下 Ctrl 或 Shift 鍵同時按下或拖曳滑鼠。



8. 按下 [Transmit]。
9. 當顯示密碼輸入畫面時，請輸入密碼，然後按下 [OK]。
   傳輸設定。

> **重要事項：**
> 會將資訊傳輸至網路界面，直到進度表完成為止。請勿關閉裝置或無線配接器，且勿將任何資料傳送至裝置。

10. 在 [Transmitting Settings] 畫面中，按下 [OK]。



11. 查看您設定之裝置的狀態。

    針對顯示  或  的裝置，檢查設定檔案的內容，或裝置是否已正常重新啟動。

圖示	Status	Process Status	說明
	Setup Complete	Setup Successful	設定已正常完成。
	Setup Complete	Rebooting	傳輸資訊後，每個裝置都必須重新啟動才能啟用設定。會執行檢查以判斷在重新啟動之後是否可以連線至裝置。
	Setup Complete	Reboot Failed	在傳輸設定後，無法確認裝置。檢查裝置是否開啟，或是否已正常重新啟動。
	Setup Complete	Searching	搜尋設定檔案中指示的裝置。*
	Setup Complete	Search Failed	無法檢查已設定的裝置。檢查裝置是否開啟，或是否已正常重新啟動。*

    * 僅限顯示設定資訊時。

相關資訊

➡ 第51頁 “執行 EpsonNet Config — Windows”
➡ 第52頁 “執行 EpsonNet Config — Mac OS”

將 IP 位址指派給每個裝置

可使用 EpsonNet Config 將 IP 位址指派給掃描器。

1. 開啟掃描器。
2. 使用乙太網路連接線將掃描器連線至網路。

3. 啟動 EpsonNet Config。

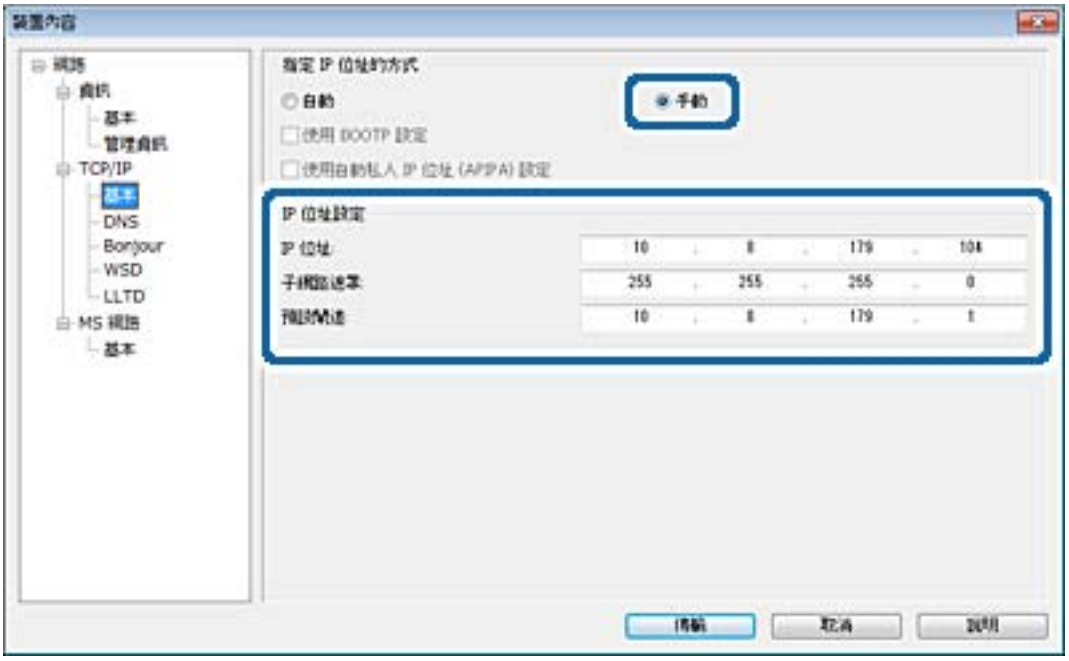
   網路上掃描器的清單即會顯示。此清單可能需要一段時間才會顯示。

4. 按兩下您要指派至的掃描器。

   附註：
   如果已連線相同機型的多個掃描器，可使用 MAC 位址識別掃描器。

5. 選取 [Network] > [TCP/IP] > [Basic]。

6. 輸入 [IP Address]、[Subnet Mask] 及 [Default Gateway] 的位址。



   附註：
   在將掃描器連線至安全網路時，請輸入靜態位址。

7. 按下 [Transmit]。

   確認傳送資訊的畫面即會顯示。

8. 按下 [OK]。

   傳送完成畫面即會顯示。

   附註：
   資訊會傳送至裝置，然後「配置成功完成。」訊息即會顯示。請勿關閉裝置，且勿將任何資料傳送至服務。

9. 按下 [OK]。

相關資訊

➡ 第51頁“執行 EpsonNet Config — Windows”
➡ 第52頁“執行 EpsonNet Config — Mac OS”

掃描器使用的連接埠

掃描器會使用下列連接埠。根據需要，網路管理員應允許這些連接埠變為可用。

傳送者 (用戶端)	使用	目的地 (伺服器)	通訊協定	連接埠號碼
掃描器	電子郵件傳送 (電子郵件通知)	SMTP 伺服器	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	在 SMTP 連線之前使用 POP (電子郵件通知)	POP 伺服器	POP3 (TCP)	110
	控制 WSD	用戶端電腦	WSD (TCP)	5357
	從 Document Capture Pro 推送掃描時搜尋電腦	用戶端電腦	網路推送掃描探索	2968
	從 Document Capture Pro 推送掃描時收集工作資訊	用戶端電腦	網路推送掃描	2968
用戶端電腦	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 Document Capture Pro 的掃描資料	掃描器	網路掃描 (TCP)	1865

適用於企業的進階安全性設定

在本章中，我們將介紹進階安全性功能。

安全性設定與危險預防

當裝置連線至網路時，您可從遠端位置予以存取。此外，還可以多人共用裝置，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裝置，風險會更高。

為了避免此風險，Epson 裝置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，視需要設定裝置。

名稱	功能類型	設定內容	防止目標
SSL/TLS 通訊	電腦與裝置的通訊路徑使用 SSL/TLS 通訊加密。透過瀏覽器進行內容通訊是受到保護的。	為伺服器設定 CA 憑證，其為裝置的 CA (憑證授權單位) 簽署憑證。	防止將設定資訊與傳輸的資料內容從電腦洩漏至掃描器。在網際網路上從裝置存取 Epson 伺服器也可使用韌體更新等保護。
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掃描通訊協定。	建立基本原則與個別原則來設定可存取裝置的用戶端或資料類型。	保護裝置免遭未經授權存取、篡改及攔截通訊資料。
SNMPv3	已新增功能，如在網路中監控連線的裝置、要控制之 SNMP 通訊協定的資料完整性、加密、使用者驗證等。	啟用 SNMPv3，然後設定驗證與加密方法。	確保透過網路在狀態監控下機密地變更設定。
IEEE802.1X	僅允許通過驗證的使用者連線至乙太網路。僅允許許可的使用者使用裝置。	RADIUS 伺服器 (驗證伺服器) 的驗證設定。	保護裝置免遭未經授權存取與使用。
讀取身分證件	您可透過延期連線之驗證裝置的身分證件來使用裝置。您可以限制每位使用者與裝置獲取記錄，並限制每位使用者與群組使用裝置與可用的功能。	將驗證裝置連接至裝置，然後在驗證系統中設定使用者的資訊。	防止對裝置進行未經授權的使用及詐騙攻擊。

相關資訊

➡ 第58頁“與掃描器之間的 SSL/TLS 通訊”
➡ 第66頁“使用 IPsec/IP 篩選加密的通訊”
➡ 第76頁“使用 SNMPv3 通訊協定”
➡ 第78頁“將掃描器連接至 IEEE802.1X 網路”

安全性功能設定

設定 IPsec/IP 篩選或 IEEE802.1X 時，建議您存取 Web Config，使用 SSL/TLS 來傳遞設定資訊，以降低如篡改或攔截等安全風險。

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。

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58頁“取得並匯入 CA 簽署憑證”

➡ 第62頁“刪除 CA 簽署憑證”

➡ 第63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 [確定]。

   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22頁“存取 Web Config”
➡ 第60頁“CSR 設定項目”
➡ 第60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 個的字元。若這是 IP 位址，則必須為靜態 IP 位址。 範例： 存取 Web Config 的　URL：https://10.152.12.225 一般名稱：10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	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。
Country	輸入 ISO-3166 所指定的兩位數國碼。

相關資訊

➡ 第58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 [確定]。

   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22頁“存取 Web Config”
➡ 第62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60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，然後選取 [Network Security Settings]。接著選取 [SSL/TLS] > [Certificate] 或 [IPsec/IP Filtering] > [Client Certificate] 或 [IEEE802.1X] > [Client Certificate]。
2. 按下 [Delete]。
3. 在顯示的訊息中，確認您是否要刪除憑證。

相關資訊

➡ 第22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，然後選取 [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 [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：
按下 [Confirm] 確認憑證資訊。

相關資訊

➡ 第22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 [確定]。

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

相關資訊

➡ 第22頁“存取 Web Config”

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。

相關資訊

➡ 第22頁“存取 Web Config”

使用 IPsec/IP 篩選加密的通訊

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 [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22頁“存取 Web Config”
➡ 第67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	選取此選項會允許已配置的 IP 封包通過。
	Refuse Access	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 Version	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 Version]，會顯示下列項目。	
	Authentication Method	若選取 [Certificate]，您必須事先取得並匯入 CA 簽署憑證。
	Pre-Shared Key	若針對 [Authentication Method] 選取 [Pre-Shared Key]，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。
IKEv2	若選取 [IKEv2] 作為 [IKE Version]，會顯示下列項目。	

項目	設定與說明	
Local	Authentication Method	若選取 [Certificate]，您必須事先取得並匯入 CA 簽署憑證。
	ID Type	選取掃描器的 ID 類型。
	ID	輸入與 ID 類型相符的掃描器 ID。 不得使用「@」、「#」與「=」作為第一個字元。 [Distinguished Name]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「=」。 [IP Address]：輸入 IPv4 或 IPv6 格式。 [FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。 [Email Address]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「@」。 [Key ID]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。
	Pre-Shared Key	若針對 [Authentication Method] 選取 [Pre-Shared Key]，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。
Remote	Authentication Method	若選取 [Certificate]，您必須事先取得並匯入 CA 簽署憑證。
	ID Type	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。 不得使用「@」、「#」與「=」作為第一個字元。 [Distinguished Name]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「=」。 [IP Address]：輸入 IPv4 或 IPv6 格式。 [FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。 [Email Address]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「@」。 [Key ID]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。
	Pre-Shared Key	若針對 [Authentication Method] 選取 [Pre-Shared Key]，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	若針對 [Access Control] 選取 [IPsec]，您必須配置封裝模式。	
	Transport Mode	若只在相同 LAN 上使用掃描器，請選取此選項。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，請選取此選項。IP 封包的標頭及資料會經過加密。
Remote Gateway(Tunnel Mode)	若針對 [Encapsulation] 選取 [Tunnel Mode]，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 [Access Control] 為 [IPsec]，選取一個選項。	
	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。
Algorithm Settings		
IKE	Encryption	選取 IKE 的加密演算法。 項目根據 IKE 版本而有所不同。
	Authentication	選取 IKE 的驗證演算法。
	Key Exchange	選取 IKE 的金鑰交換演算法。 項目根據 IKE 版本而有所不同。
ESP	Encryption	選取 ESP 的加密演算法。 只有當針對 [Security Protocol] 選取 [ESP] 時，此項才可用。
	Authentication	選取 ESP 的驗證演算法。 只有當針對 [Security Protocol] 選取 [ESP] 時，此項才可用。
AH	Authentication	選取 AH 的加密演算法。 只有當針對 [Security Protocol] 選取 [AH] 時，此項才可用。

相關資訊

➡ 第66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 [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。

相關資訊

➡ 第22頁“存取 Web Config”
➡ 第70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	選取此選項會允許已配置的 IP 封包通過。
	Refuse Access	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。
Local Address (Scanner)	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 [Use auto-obtained IPv4 address]。	
Remote Address(Host)	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。	
Method of Choosing Port	選取指定連接埠的方式。	
Service Name	若針對 [Method of Choosing Port] 選取 [Service Name]，請選取一個選項。	

項目	設定與說明	
Transport Protocol	若針對 [Method of Choosing Port] 選取 [Port Number]，您必須配置封裝模式。	
	Any Protocol	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。
Local Port	若針對 [Method of Choosing Port] 選取 [Port Number]，且針對 [Transport Protocol] 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。	
Remote Port	若針對 [Method of Choosing Port] 選取 [Port Number]，且針對 [Transport Protocol] 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 Version	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 Version]，會顯示下列項目。	
	Authentication Method	若針對 [Access Control] 選取 [IPsec]，請選取一個選項。已使用憑證與預設原則一樣。
	Pre-Shared Key	若針對 [Authentication Method] 選取 [Pre-Shared Key]，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。
IKEv2	若選取 [IKEv2] 作為 [IKE Version]，會顯示下列項目。	

項目	設定與說明	
Local	Authentication Method	若針對 [Access Control] 選取 [IPsec]，請選取一個選項。已使用憑證與預設原則一樣。
	ID Type	選取掃描器的 ID 類型。
	ID	輸入與 ID 類型相符的掃描器 ID。 不得使用「@」、「#」與「=」作為第一個字元。 [Distinguished Name]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「=」。 [IP Address]：輸入 IPv4 或 IPv6 格式。 [FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。 [Email Address]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「@」。 [Key ID]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。
	Pre-Shared Key	若針對 [Authentication Method] 選取 [Pre-Shared Key]，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。
Remote	Authentication Method	若針對 [Access Control] 選取 [IPsec]，請選取一個選項。已使用憑證與預設原則一樣。
	ID Type	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。 不得使用「@」、「#」與「=」作為第一個字元。 [Distinguished Name]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「=」。 [IP Address]：輸入 IPv4 或 IPv6 格式。 [FQDN]：使用 A—Z、a—z、0—9、「-」及句點 (.) 輸入 1 至 255 個字元的組合。 [Email Address]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。您需要包括「@」。 [Key ID]：輸入 1 至 128 個 1 位元組的 ASCII (0x20 至 0x7E) 字元。
	Pre-Shared Key	若針對 [Authentication Method] 選取 [Pre-Shared Key]，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	若針對 [Access Control] 選取 [IPsec]，您必須配置封裝模式。	
	Transport Mode	若只在相同 LAN 上使用掃描器，請選取此選項。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，請選取此選項。IP 封包的標頭及資料會經過加密。
Remote Gateway(Tunnel Mode)	若針對 [Encapsulation] 選取 [Tunnel Mode]，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	若針對 [Access Control] 選取 [IPsec]，請選取一個選項。	
	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。
Algorithm Settings		
IKE	Encryption	選取 IKE 的加密演算法。 項目根據 IKE 版本而有所不同。
	Authentication	選取 IKE 的驗證演算法。
	Key Exchange	選取 IKE 的金鑰交換演算法。 項目根據 IKE 版本而有所不同。
ESP	Encryption	選取 ESP 的加密演算法。 只有當針對 [Security Protocol] 選取 [ESP] 時，此項才可用。
	Authentication	選取 ESP 的驗證演算法。 只有當針對 [Security Protocol] 選取 [ESP] 時，此項才可用。
AH	Authentication	選取 AH 的驗證演算法。 只有當針對 [Security Protocol] 選取 [AH] 時，此項才可用。

相關資訊

➡ 第69頁 “配置 Group Policy”
➡ 第73頁 “在 Group Policy 上結合 Local Address (Scanner) 和 Remote Address(Host)”
➡ 第74頁 “群組原則服務名稱參考”

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。

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
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
Network Push Scan Discovery	UDP	2968	任一連接埠	從掃描器中搜尋電腦。
Network Push Scan	TCP	任一連接埠	2968	從 Document Capture Pro 或 Document Capture 獲取推送掃描的作業資訊
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 (韌體更新和根憑證更新之間的通訊)
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。

使用 Epson Scan 2 與掃描器設定接受掃描

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], [Network Scan], [HTTP (Local)] 和 [HTTPS (Local)] 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22頁 “存取 Web Config”

➡ 第58頁 “取得並匯入 CA 簽署憑證”

使用 SNMPv3 通訊協定

關於 SNMPv3

SNMP 是一個通訊協定，可進行監控與控制，以收集連線至網路之裝置的資訊。SNMPv3 是已強化的管理安全性功能版本。

使用 SNMPv3 時，可驗證及加密 SNMP 通訊 (封包) 的狀態監控與設定變更，以保護 SNMP 通訊 (封包) 免於網路風險，如竊聽電話、模擬以及篡改。

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 [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22頁 “存取 Web Config”
➡ 第77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。

項目	設定與說明
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76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，然後選取 [Network Security Settings] > [IEEE802.1X] > [Basic]。
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22頁“存取 Web Config”
➡ 第79頁“IEEE802.1X 網路設定項目”
➡ 第83頁“在配置 IEEE802.1X 之後無法存取印表機或掃描器”

IEEE802.1X 網路設定項目

項目	設定與說明	
IEEE802.1X (Wired LAN)	您可啟用或停用頁面中的設定值 ([IEEE802.1X] > [Basic]) 以符合 IEEE802.1X (有線 LAN)。	
EAP Type	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。
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。	

項目	設定與說明	
Anonymous Name	若針對 [Authentication Method] 選取 [PEAP-TLS] 或 [PEAP/MSCHAPv2]，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	您可選取下列其中一項。	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

相關資訊

➡ 第78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22頁“存取 Web Config”

➡ 第58頁“取得並匯入 CA 簽署憑證”

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 篩選或 IEEE802.1X) 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。

使用控制面板停用安全性功能

您可以使用掃描器的控制面板停用 IPsec/IP 篩選或 IEEE802.1X。

1. 點選 [設定] > [網路設定]。
2. 點選 [變更設定]。
3. 點選要停用的項目。
   - ❏ [IPsec/IP 篩選]
   - ❏ [IEEE802.1X]
4. 顯示完成訊息後，點選 [繼續]。

使用 Web Config 還原安全性功能

針對 IEEE802.1X，可能無法在網路上辨識裝置。此時請使用掃描器的控制面板停用該功能。

針對 IPsec/IP 篩選，如果您從電腦存取裝置，可停用該功能。

使用 Web Config 停用 IPsec/IP 篩選

1. 存取 Web Config，然後選取 [Network Security Settings] > [IPsec/IP Filtering] > [Basic]。
2. 在 [Default Policy] 中，選取 [IPsec/IP Filtering] 的 [Disable]。
3. 按下 [下一步]，然後針對所有群組原則清除 [Enable this Group Policy]。
4. 按下 [確定]。

相關資訊

➡ 第22頁“存取 Web Config”

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，然後選取 [Network Security Settings] > [IPsec/IP Filtering] > [Basic] > [Default Policy] 或 [Group Policy]。

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22頁“存取 Web Config”

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
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
IKE 金鑰交換演算法	DH 群組 1、DH 群組 2、DH 群組 5、DH 群組 14、DH 群組 15、DH 群組 16、DH 群組 17、DH 群組 18、DH 群組 19、DH 群組 20、DH 群組 21、DH 群組 22、DH 群組 23、DH 群組 24、DH 群組 25、DH 群組 26、DH 群組 27*、DH 群組 28*、DH 群組 29*、DH 群組 30*
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66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 位址是否無效或已變更？

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 IPv6 位址，則可能找不到針對掃描器之 Web Config ([Network Security Settings] > [IPsec/IP Filtering] > [Basic] > [Group Policy] > [Local Address (Scanner)]) 登錄的 IP 位址。

使用靜態 IP 位址。

電腦的 IP 位址是否無效或已變更？

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 IPv6 位址，則可能找不到針對掃描器之 Web Config ([Network Security Settings] > [IPsec/IP Filtering] > [Basic] > [Group Policy] > [Remote Address(Host)]) 登錄的 IP 位址。

使用靜態 IP 位址。

相關資訊

➡ 第22頁“存取 Web Config”
➡ 第66頁“使用 IPsec/IP 篩選加密的通訊”

配置 IPsec/IP 篩選後無法連線

設定值可能不正確。

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66頁“使用 IPsec/IP 篩選加密的通訊”

在配置 IEEE802.1X 之後無法存取印表機或掃描器

設定可能不正確。

從掃描器控制面板停用 IEEE802.1X。連接掃描器與電腦，然後再次配置 IEEE802.1X。

相關資訊

➡ 第78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60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63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58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58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62頁“刪除 CA 簽署憑證”

➡ 第60頁“匯入 CA 簽署憑證”