安全功能指南

目錄

簡介

提示定義

本使用說明書使用以下符號和慣用標記：

重要事項	重要事項 表示潛在的危險狀況，若不加以避免，可能導致財產損失或產品功能喪失。
提醒	提醒特定作業環境、安裝條件或特殊使用條件。
	提示圖示用於指示有用的提示和補充資訊。
粗體	粗體字樣表示機器控制面板或電腦螢幕上顯示的按鍵/按鈕。
斜體	Italicized 字樣 emphasizes 應當注意的要點或提示您參考相關主題。

相關資訊

- 簡介

商標

Adobe® 和 Reader® 是 Adobe Systems 公司在美國和/或其他國家的註冊商標或商標。

本說明書中提及的軟體名稱都有一份軟體許可 License，此協定指明了其相應的所有者。

Brother 產品、相關說明書和任何其他材料中出現的任何公司的商標名稱、產品名稱都是其相應公司的商標或註冊商標。

相關資訊

- 簡介

版權

相關資訊

- 簡介

使用網路安全功能前

本機器採用目前最新的網路安全與加密通訊協定。這些網路功能可以整合到網路安全總計劃中，有助於保護資料並防止未經授權的使用者存取本機器。

建議停用 FTP 和 TFTP 通訊協定。使用這些通訊協定存取機器不安全。

相關資訊

- 簡介
  - 停用不必要的通訊協定

停用不必要的通訊協定

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Network (網路)** > **Protocol (通訊協定)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 取消勾選任何不必要通訊協定的核取方塊，以停用。
6. 按一下 **Submit (提交)**。
7. 重新啟動 Brother 機器以啟用設置。

相關資訊

- 使用網路安全功能前

網路安全

- 配置裝置安全憑證
- 使用 SSL/TLS
- 使用 SNMPv3
- 使用 IPsec
- 使用網路的 IEEE 802.1x 驗證

配置裝置安全憑證

必須設置憑證，以使用 SSL/TLS 安全地管理聯網的機器。必須使用網路管理來設置憑證。

- 安全憑證功能概述
- 如何建立和安裝憑證
- 建立自我簽署憑證
- 建立憑證簽署請求 (CSR) 和安裝憑證授權單位 (CA) 頒發的憑證
- 匯入和匯出憑證和私密金鑰
- 匯入和匯出 CA 憑證

安全憑證功能概述

本機器支援使用多個安全憑證，允許使用本機器進行安全驗證和通訊。本機器支援以下安全憑證功能：

支援的功能、選項或設定可能會因機器型號而有所不同。

- SSL/TLS 通訊
- IEEE 802.1x 驗證
- IPsec

本機器支援下列項目：

- 預先安裝的憑證

  本機器預先安裝有自我簽署憑證。透過該憑證，您無需建立或安裝其他憑證即可使用 SSL/TLS 通訊。

  預先安裝的自我簽署憑證可在一定程度上保護您的通訊。為了確保更加安全，建議您使用信任的 organization 發行的憑證。

- 自我簽署憑證

  此列印伺服器頒發它自身的憑證。使用此憑證時，您無需建立或安裝其他 CA 憑證即可輕鬆使用 SSL/TLS 通訊。

- 憑證授權單位 (CA) 頒發的憑證

  CA 憑證的安裝方法有兩種。如果您已擁有 CA 憑證或者您想使用信任的外部 CA 頒發的憑證：

  - 使用此列印伺服器的憑證簽署要求 (CSR) 時。
  - 匯入憑證和私密金鑰時。

- 憑證授權單位 (CA) 憑證

  若要使用可自行辨識 CA 並擁有其私密金鑰的 CA 憑證，配置網路安全功能之前，您必須匯入 CA 發行的 CA 憑證。

  - 如果您要使用 SSL/TLS 通訊，建議先聯絡您的系統管理員。
  - 將列印伺服器重置為預設出廠設定時，已安裝的憑證和私密金鑰將被刪除。如果您希望重置列印伺服器後保留相同的憑證和私密金鑰，重置前將它們匯出，然後重新安裝。

相關資訊

- 配置裝置安全憑證

相關主題:

- 使用網路管理 (網頁瀏覽器) 設置有線網路的 IEEE 802.1x 認證

如何建立和安裝憑證

選擇安全憑證時有兩種選項：使用自我簽署憑證或使用憑證授權單位 (CA) 頒發的憑證。

選項 1

自我簽署憑證

1. 使用網路基礎管理建立自我簽署憑證。
2. 在電腦上安裝自我簽署憑證。

選項 2

CA 憑證

1. 使用網路基礎管理建立憑證簽署請求 (CSR)。
2. 使用網路管理在 Brother 機器上安裝 CA 簽署的憑證。
3. 在電腦上安裝憑證。

相關資訊

- 配置裝置安全憑證

建立自我簽署憑證

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **Certificate (憑證)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 按一下 **Create Self-Signed Certificate (建立自我簽署憑證)**。
6. 輸入 **Common Name (一般名稱)** 和 **Valid Date (有效日期)**。
   - **Common Name (一般名稱)**的長度小於 64 位元組。輸入透過 SSL/TLS 通訊存取機器時使用的 IP 位址、節點名稱或網域名稱等識別碼。預設狀態下，將顯示節點名稱。
   - 如果您使用 IPPS 或 HTTPS 通訊協定，並在 URL 中輸入一個不同於自我簽署憑證的 **Common Name (一般名稱)**，將會顯示一個警告。
7. 從 **Public Key Algorithm (公開金鑰演算法)**下拉式選單中選擇您的設定。
8. 從 **Digest Algorithm (摘要演算法)**下拉式選單中選擇您的設定。
9. 按一下 **Submit (提交)**。

相關資訊

- 配置裝置安全憑證

建立憑證簽署請求 (CSR) 和安裝憑證授權單位 (CA) 頒發的憑證

如果您已擁有受信任的外部憑證授權單位 (CA) 頒發的憑證，您可透過匯入和匯出功能在機器上儲存憑證和私密金鑰並進行管理。如果您沒有受信任的外部 CA 頒發的憑證，請建立憑證簽署請求 (CSR)，將其發送至 CA 進行驗證，然後將返回的憑證安裝到機器上。

- 建立憑證簽署請求 (CSR)
- 在本機器上安裝憑證

建立憑證簽署請求 (CSR)

憑證簽署請求 (CSR) 是發送給憑證授權單位 (CA) 的請求，用於驗證該憑證包含的認證。

我們建議您建立 CSR 之前在電腦上安裝 CA 根憑證。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **Certificate (憑證)**。

如果左側導覽列沒有顯示，從☰啟動導覽。

5. 按一下 **Create CSR (建立 CSR)**。
6. 輸入 **Common Name (一般名稱)**(必要項)，並添加有關 **Organization (組織)** (可選項) 的其他資訊。

- 需要您公司的詳細資訊，以便 CA 可向外界確認您的身分和證明。
- **Common Name (一般名稱)**的長度小於 64 位元組。輸入透過 SSL/TLS 通訊存取機器時使用的 IP 位址、節點名稱或網域名稱等識別碼。預設狀態下，將顯示節點名稱。**Common Name (一般名稱)**為必要項。
- 如果您在 URL 中所輸入的一般名稱與憑證所用的一般名稱不同，將會顯示一個警告。
- **Organization (組織)**、**Organization Unit (組織單位)**、**City/Locality (城市/地區)**和 **State/Province (州/省)**的長度必須小於 64 位元組。
- **Country/Region (國家/地區)**應為兩位字元的 ISO 3166 國家代碼。
- 如果您要設置 X.509v3 憑證延伸，請勾選 **Configure extended partition (設定延伸磁碟分割)**核取方塊，然後選擇 **Auto (Register IPv4) (自動(註冊 IPv4))**或 **Manual (手動)**。

7. 從 **Public Key Algorithm (公開金鑰演算法)**下拉式選單中選擇您的設定。
8. 從 **Digest Algorithm (摘要演算法)**下拉式選單中選擇您的設定。
9. 按一下 **Submit (提交)**。
   螢幕上將顯示 CSR。將 CSR 儲存為檔案或將其複製和貼上為憑證授權單位提供的線上 CSR 格式。
10. 按一下 **存檔**。

- 請按照該方法有關的 CA 原則，將 CSR 發送給您的 CA。
- 如果您使用的是 Windows Server 的企業根 CA，我們建議您使用網頁伺服器作為憑證範本，以便安全建立用戶端憑證。如果您正在建立一個用於 IEEE 802.1x 環境與 EAP-TLS 驗證的用戶端憑證，我們建議您使用使用者作為憑證範本。

相關資訊

- 建立憑證簽署請求 (CSR) 和安裝憑證授權單位 (CA) 頒發的憑證

在本機器上安裝憑證

當您從憑證授權單位 (CA) 收到憑證時，請按照以下步驟將憑證安裝到列印伺服器上：

本機器上僅可安裝透過本機器的憑證簽署請求 (CSR) 頒發的憑證。當您要建立另一個 CSR 時，請確定新建 CSR 之前已安裝憑證。將憑證安裝到機器後建立另一個 CSR。否則，安裝新 CSR 之前建立的 CSR 將失效。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **Certificate (憑證)**。

   如果左側導覽列沒有顯示，從☰啟動導覽。
5. 按一下 **Install Certificate (安裝憑證)**。
6. 瀏覽至包含 CA 所頒發憑證的檔案，然後按一下 **Submit (提交)**。
   您的機器記憶體中將建立和儲存憑證。

若要使用 SSL/TLS 通訊，電腦上必須安裝 CA 根憑證。請聯絡您的網路管理員。

相關資訊

- 建立憑證簽署請求 (CSR) 和安裝憑證授權單位 (CA) 頒發的憑證

匯入和匯出憑證和私密金鑰

可透過匯入和匯出功能在機器上儲存憑證和私密金鑰並進行管理。

- 匯入憑證和私密金鑰
- 匯出憑證和私密金鑰

匯入憑證和私密金鑰

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **Certificate (憑證)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 按一下 **Import Certificate and Private Key (匯入憑證和私密金鑰)**。
6. 瀏覽至您想匯入的檔案並選擇。
7. 如果檔案有加密，輸入密碼再按一下 **Submit (提交)**。

憑證和私密金鑰已匯入您的機器中。

相關資訊

- 匯入和匯出憑證和私密金鑰

匯出憑證和私密金鑰

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **Certificate (憑證)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 按一下與 **Export (匯出)** 一起顯示的 **Certificate List (憑證清單)**。
6. 如果您要加密檔案，請輸入密碼。
   如果密碼欄空白，輸出結果就不會加密。
7. 再輸入一次密碼加以確認，再按一下 **Submit (提交)**。
8. 按一下 **存檔**。

憑證和私密金鑰將匯出到您的電腦。

也可將憑證匯入您的電腦。

相關資訊

- 匯入和匯出憑證和私密金鑰

匯入和匯出 CA 憑證

您可以匯入、匯出 CA 憑證並將其儲存在 Brother 機器上。

- 匯入 CA 憑證
- 匯出 CA 憑證

匯入 CA 憑證

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **CA Certificate (CA 憑證)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 按一下 **Import CA Certificate (匯入 CA 憑證)**。
6. 瀏覽至您想匯入的檔案。
7. 按一下 **Submit (提交)**。

相關資訊

- 匯入和匯出 CA 憑證

匯出 CA 憑證

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **CA Certificate (CA 憑證)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 選擇要匯出的憑證，然後按一下 **Export (匯出)**。
6. 按一下 **Submit (提交)**。

相關資訊

- 匯入和匯出 CA 憑證

使用 SSL/TLS

- 使用 SSL/TLS 安全地管理網路機器
- 使用 SSL/TLS 安全列印文件
- 使用 SSL/TLS 安全發送或接收電子郵件

使用 SSL/TLS 安全地管理網路機器

為 SSL/TLS 和可用通訊協定設置憑證

使用 SSL/TLS 通訊之前，請先透過網路管理在您的機器上設置憑證。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Network (網路)** > **Protocol (通訊協定)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 按一下 **HTTP Server Settings (HTTP 伺服器設定)**。
6. 從 **Select the Certificate (選擇憑證)**下拉式選單中選擇您想設置的憑證。
7. 按一下 **Submit (提交)**。
8. 按一下 **Yes (是)**重新啟動您的列印伺服器。

相關資訊

- 使用 SSL/TLS 安全地管理網路機器

相關主題:

- 使用 SSL/TLS 安全列印文件

使用 SSL/TLS 存取網路管理

若要安全管理您的網路機器，必須使用帶有安全性通訊協定的管理工具程式。

- 若要使用 HTTPS 通訊協定，必須啟用機器上的 HTTPS。預設值為已啟用 HTTPS 通訊協定。
- 可使用網路管理螢幕變更 HTTPS 通訊協定設定。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 現在您可使用 HTTPS 存取機器。

相關資訊

- 使用 SSL/TLS 安全地管理網路機器

安裝自我簽署憑證 (Windows 管理員使用者)

- 以下步驟適用於 Microsoft Edge。如果您使用其他網頁瀏覽器，請參閱網頁瀏覽器附帶的說明書或線上說明，以取得如何安裝憑證的指示。
- 請確定您已使用網路管理建立了自我簽署憑證。

1. 在 **Microsoft Edge** 圖示上按一下滑鼠右鍵，再按一下**以系統管理員身分執行**。
   如果出現**使用者帳戶控制**螢幕，按一下**是**。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如果並非私人連線，請按一下**進階**按鍵，然後繼續前往網頁。
4. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
5. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **Certificate (憑證)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
6. 按一下 **Export (匯出)**。
7. 若要加密輸出檔案，請在 **Enter password (輸入密碼)**欄位中輸入密碼。如果 **Enter password (輸入密碼)**欄位留空，則不加密輸出檔案。
8. 在 **Retype password (重新輸入密碼)**欄位中再次輸入密碼，然後按一下 **Submit (提交)**。
9. 按一下開啟下載檔案。
10. 顯示**憑證匯入精靈**時，按一下**下一步**。
11. 按一下 **下一步**。
12. 如有需要，輸入密碼，然後按一下**下一步**。
13. 選擇**將所有憑證放入以下的存放區**，然後按一下**瀏覽...**。
14. 選擇**受信任的根憑證授權單位**，然後按一下**確定**。
15. 按一下 **下一步**。
16. 按一下 **完成**。
17. 如果憑證指紋碼正確，按一下**是**。
18. 按一下 **確定**。

相關資訊

- 使用 SSL/TLS 安全地管理網路機器

使用 SSL/TLS 安全列印文件

- 使用 IPPS 列印文件
- 為 SSL/TLS 和可用通訊協定設置憑證
- 配置裝置安全憑證

使用 IPPS 列印文件

若要以 IPP 通訊協定安全列印文件，使用 IPPS 通訊協定。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Network (網路)** > **Protocol (通訊協定)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 確認已勾選 **IPP** 核取方塊。

   如果您未勾選 **IPP** 核取方塊，勾選 **IPP** 核取方塊，然後按一下 **Submit (提交)**。
   重新啟動機器以啟用設置。
   待機器重新啟動後，返回機器網頁，輸入密碼，然後在左側導覽列中，按一下 **Network (網路)** > **Network (網路)** > **Protocol (通訊協定)**。
6. 按一下 **HTTP Server Settings (HTTP 伺服器設定)**。
7. 在 **HTTPS(連接埠 443)**區域中勾選 **IPP** 核取方塊，再按一下 **Submit (提交)**。
8. 重新啟動機器以啟用設置。

使用 IPPS 通訊無法避免 unauthorized 列印伺服器存取。

相關資訊

- 使用 SSL/TLS 安全列印文件

使用 SNMPv3

- 使用 SNMPv3 安全地管理網路機器

使用 SNMPv3 安全地管理網路機器

簡易網路管理通訊協定版本 3 (SNMPv3) 提供使用者驗證和資料加密，以安全管理網路裝置。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://Common Name」(「Common Name」是您為憑證指定的一般名稱，可能是 IP 位址、節點名稱或網域名稱)。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Network (網路)** > **Network (網路)** > **Protocol (通訊協定)**。

如果左側導覽列沒有顯示，從☰啟動導覽。

5. 確定 **SNMP** 設定已啟用，然後按一下 **Advanced Settings (進階設定)**。
6. 配置 SNMPv1/v2c 模式設定。

選項	說明
SNMP v1/v2c read-write access (SNMP v1/v2c 讀寫存取權限)	列印伺服器使用的是版本 1 和版本 2c 的 SNMP 通訊協定。您可在這個模式下使用本機器的所有應用程式。不過，此模式並不安全，因為此模式不驗證使用者，也不加密資料。
SNMP v1/v2c read-only access (SNMP v1/v2c 唯讀存取權)	列印伺服器使用的是唯讀存取 SNMP 通訊協定版本 1 和版本 2c。
Disabled (停用)	停用 SNMP 通訊協定版本 1 和版本 2c。 所有使用 SNMPv1/v2c 的應用程式都將受限。若要允許使用 SNMPv1/v2c 應用程式，請使用 **SNMP v1/v2c read-only access (SNMP v1/v2c 唯讀存取權)**或 **SNMP v1/v2c read-write access (SNMP v1/v2c 讀寫存取權限)**模式。

7. 配置 SNMPv3 模式設定。

選項	說明
Enabled (已啟用)	列印伺服器使用的是版本 3 的 SNMP 通訊協定。若要安全管理列印伺服器，請使用 SNMPv3 模式。
Disabled (停用)	停用 SNMP 通訊協定版本 3。 所有使用 SNMPv3 的應用程式都將受限。若要允許使用 SNMPv3 應用程式，請使用 SNMPv3 模式。

8. 按一下 **Submit (提交)**。

如果本機器顯示通訊協定設定選項，選擇所需選項。

9. 重新啟動機器以啟用設置。

相關資訊

- 使用 SNMPv3

使用 IPsec

IPsec 簡介

IPsec (網際網路通訊協定安全性) 是一種安全通訊協定，它使用選用的網際網路通訊協定功能來防止資料操控，並確保以 IP 封包形式傳送之資料的機密性。IPsec 對透過網路傳輸的資料進行加密，例如從電腦發送到印表機的列印資料。因為資料是在網路層被加密，所以使用更高級別通訊協定的應用程式也使用 IPsec，雖然使用者並未意識到它的使用。

IPsec 支援下列功能：

- IPsec 傳輸

  根據 IPsec 設定條件，連接到網路的電腦會使用 IPsec 將資料傳送到指定的裝置以及接收來自指定的裝置的資料。當裝置開始使用 IPsec 進行通訊時，先使用網際網路密碼交換 (IKE) 交換密碼，然後使用密碼傳輸加密的資料。

  另外，IPsec 有兩種操作模式：傳輸模式和通道模式。傳輸模式主要用於裝置之間的通訊，通道模式則用於虛擬私人網路 (VPN) 等環境中。

對於 IPsec 傳輸，下列條件為必要條件：

- 使用 IPsec 進行通訊的電腦已連接到網路。
- 機器已配置為可進行 IPsec 通訊。
- 連接至機器的電腦已配置為使用 IPsec 連線。

- IPsec 設定

  使用 IPsec 建立連線所需的設定。這些設定可以使用「網路基本管理」進行配置。

若要配置 IPsec 設定，必須使用連接到網路的電腦上的瀏覽器。

相關資訊

- 使用 IPsec

使用網路基本管理配置 IPsec

IPsec 連接條件由兩種 **Template (模板)** 類型組成：**Address (位址)** 和 **IPsec**。您最多可以配置 10 個連接條件。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **IPsec**。

   如果左側導覽列沒有顯示，從☰啓動導覽。

5. 設置設定。

選項	說明
Status (狀態)	啟用或停用 IPsec。
Negotiation Mode (交涉模式)	針對 IKE 階段 1 選擇 **Negotiation Mode (交涉模式)**。IKE 通訊協定用於交換加密金鑰，以便使用 IPsec 進行加密通訊。 在 **Main (主要)**模式下，處理速度慢，但安全性高。在 **Aggressive (加強)**模式下，處理速度比 **Main (主要)**模式快，但安全性較低。
All Non-IPsec Traffic (所有非 IPsec 流量)	選擇針對非 IPsec 封包要採取的措施。 使用 Web 服務時，必須將 **All Non-IPsec Traffic (所有非 IPsec 流量)** 選擇為 **Allow (允許)**。如果您選擇 **Drop (丟棄)**，Web 服務將無法使用。
Broadcast/Multicast Bypass (廣播/多播旁路)	選擇 **Enabled (已啟用)**或 **Disabled (停用)**。
Protocol Bypass (通訊協定旁路)	勾選所需的一個或多個選項的核取方塊。
Rules (規則)	勾選 **Enabled (已啟用)**核取方塊以啟用範本。勾選多個核取方塊時，如果所勾選核取方塊之間的設定相互衝突，則編號較小的核取方塊具有優先權。 按一下相應的下拉式選單以選擇用於 IPsec 連接條件的 **Address Template (位址模板)**。若要新增 **Address Template (位址模板)**，按一下 **Add Template (新增模板)**。 按一下相應的下拉式選單以選擇用於 IPsec 連接條件的 **IPsec Template (IPsec 模板)**。若要新增 **IPsec Template (IPsec 模板)**，按一下 **Add Template (新增模板)**。

6. 按一下 **Submit (提交)**。
   如果必須重新啟動機器以啟用新設定，重新啟動確認螢幕將會顯示。
   如果您在 **Rules (規則)**表中啟用的範本有空白項，將會顯示錯誤訊息。確認選擇並再次按一下 **Submit (提交)**。

相關資訊

- 使用 IPsec

相關主題:

- 配置裝置安全憑證

使用網路基本管理配置 IPsec 位址範本

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **IPsec Address Template (IPsec 位址模板)**。

   如果左側導覽列沒有顯示，從☰啟動導覽。
5. 按一下 **Delete (刪除)**按鍵刪除 **Address Template (位址模板)**。如果 **Address Template (位址模板)**正在使用中，則無法刪除。
6. 按一下您想建立的 **Address Template (位址模板)**。**IPsec Address Template (IPsec 位址模板)**將會顯示。
7. 設置設定。

選項	說明
Template Name (模板名稱)	鍵入範本的名稱 (最多 16 個字元)。
Local IP Address (本機 IP 位址)	• **IP Address (IP 位址)** 指定 IP 位址。從下拉式選單中選擇 **ALL IPv4 Address (所有 IPv4 位址)**、**ALL IPv6 Address (所有 IPv6 位址)**、**ALL Link Local IPv6 (所有連結本機 IPv6)** 或 **Custom (自訂)**。 如果從下拉式選單中選擇 **Custom (自訂)**，在文字方塊中輸入 IP 位址 (IPv4 或 IPv6)。 • **IP Address Range (IP 位址範圍)** 在文字方塊中輸入該 IP 位址範圍的起始 IP 位址和結束 IP 位址。如果起始和結束 IP 位址未 standardized 為 IPv4 或 IPv6，或結束 IP 位址小於起始位址，將發生錯誤。 • **IP Address / Prefix (IP 位址/首碼)** 使用 CIDR 表示法指定 IP 位址。 例如：192.168.1.1/24 因為對於 192.168.1.1，字首以 24 位元子網路遮罩 (255.255.255.0) 的形式指定，所以位址 192.168.1.### 有效。
Remote IP Address (遙距 IP 位址)	• **Any (任意)** 如果您選擇 **Any (任意)**，所有 IP 位址均被啟用。 • **IP Address (IP 位址)** 在文字方塊中輸入指定的 IP 位址 (IPv4 或 IPv6)。 • **IP Address Range (IP 位址範圍)** 輸入該 IP 位址範圍的第一個和最後一個 IP 位址。如果第一個和最後一個 IP 位址未 standardized 為 IPv4 或 IPv6，或最後一個 IP 位址小於第一個位址，將發生錯誤。 • **IP Address / Prefix (IP 位址/首碼)** 使用 CIDR 表示法指定 IP 位址。 例如：192.168.1.1/24 因為對於 192.168.1.1，字首以 24 位元子網路遮罩 (255.255.255.0) 的形式指定，所以位址 192.168.1.### 有效。

8. 按一下 **Submit (提交)**。

當您變更目前使用中的範本的設定時，重新啟動機器以啟用設置。

相關資訊

- 使用 IPsec

使用網路基本管理配置 IPsec 範本

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Network (網路)** > **Security (安全性)** > **IPsec Template (IPsec 模板)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 按一下 **Delete (刪除)**按鍵刪除 **IPsec Template (IPsec 模板)**。如果 **IPsec Template (IPsec 模板)**正在使用中，則無法刪除。
6. 按一下您想建立的 **IPsec Template (IPsec 模板)**。**IPsec Template (IPsec 模板)**螢幕將會顯示。設置欄位會因選擇的 **Use Prefixed Template (使用帶首碼的模板)**和 **Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))**設定而有所不同。
7. 在 **Template Name (模板名稱)**欄位中，輸入範本的名稱 (最 多 16 位字元)。
8. 如果在 **Use Prefixed Template (使用帶首碼的模板)**下拉式選單中選擇 **Custom (自訂)**，選擇 **Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))**選項，然後變更設定 (如有需要)。
9. 按一下 **Submit (提交)**。

相關資訊

- 使用 IPsec
  - IPsec 範本的 IKEv1 設定
  - IPsec 範本的 IKEv2 設定
  - IPsec 範本的手動設定

IPsec 範本的 IKEv1 設定

選項	說明
Template Name (模板名稱)	輸入範本的名稱 (最多 16 位字元)。
Use Prefixed Template (使用帶首碼的模板)	選擇 **Custom (自訂)**、**IKEv1 High Security (IKEv1 高安全性)**或 **IKEv1 Medium Security (IKEv1 中安全性)**。設定項目視乎所選範本而有所不同。
Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))	IKE 通訊協定用於交換加密金鑰，以便使用 IPsec 進行加密通訊。為了僅在該時間執行加密通訊，將確定 IPsec 所需的加密演算法並共用加密金鑰。對於 IKE，將使用 Diffie-Hellman 密碼交換方法交換加密金鑰，且執行被限制為 IKE 的加密通訊。 如果在 **Use Prefixed Template (使用帶首碼的模板)**中選擇了 **Custom (自訂)**，請選擇 **IKEv1**。
Authentication Type (驗證類型)	• **Diffie-Hellman Group (Diffie-Hellman 群組)** 此密碼交換方法允許秘密密碼透過不受保護的網路進行安全交換。Diffie-Hellman 密碼交換方法使用離散對數問題 (而非秘密密碼) 發送和接收使用隨機數字和秘密密碼生成的資訊。 選擇 **Group1 (群組 1)**、**Group2 (群組 2)**、**Group5 (群組 5)** 或 **Group14 (群組 14)**。 • **Encryption (加密)** 選擇 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **Hash (雜湊)** 選擇 **MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 • **SA Lifetime (SA 存留期)** 指定 IKE SA 的存留期。 輸入時間 (秒數) 和千位元組數 (KB)。
Encapsulating Security (封裝安全性)	• **Protocol (通訊協定)** 選擇 **ESP**、**AH** 或 **AH+ESP**。 - ESP 是使用 IPsec 執行加密通訊的通訊協定。ESP 對裝載 (通訊內容) 進行加密並新增其他資訊。IP 封包由標題及其後的加密裝載組成。除了加密資料，IP 封包還包含加密方式和加密金鑰、驗證資料等相關資訊。 - AH 是 IPsec 通訊協定的一部分，用於驗證發送方並阻止操控資料 (確保資料的完整性)。在 IP 封包中，資料緊接在標題後面。此外，封包中還包含使用方程式從通訊內容、秘密金鑰等計算得出的雜湊值，以防止竄改發送方和操控資料。與 ESP 不同，此通訊協定不對通訊內容進行加密，而將資料作為普通文字進行發送和接收。 • **Encryption (加密) (不適用於 AH 選項。)** 選擇 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **Hash (雜湊)** 選擇 **None (無)**、**MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 僅當在 **Protocol (通訊協定)**中選擇了 **ESP** 時，才可以選擇 **None (無)**。 • **SA Lifetime (SA 存留期)** 指定 IKE SA 的存留期。 輸入時間 (秒數) 和千位元組數 (KB)。 • **Encapsulation Mode (封裝模式)** 選擇 **Transport (傳輸)**或 **Tunnel (隧道)**。

選項	說明
	• **Remote Router IP-Address (遙距路由器 IP 位址)** 輸入遠端路由器的 IP 位址 (IPv4 或 IPv6)。僅當選擇了 **Tunnel (隧道)**模式時，輸入此資訊。 SA (安全性關聯) 是一種使用 IPsec 或 IPv6 的加密通訊方法，用於交換和共用加密方式和加密金鑰等資訊，以便在開始通訊前建立一個安全的通訊頻道。SA 還可能指已建立的虛擬加密通訊通道。用於 IPsec 的 SA 依照 IKE (網際網路密碼交換) 標準步驟建立加密方式、交換密碼和執行相互驗證。此外，SA 還會定期更新。
Perfect Forward Secrecy (PFS) (完整轉寄密碼(PFS))	PFS 不會從用於對訊息進行加密的先前密碼衍生密碼。此外，如果用於對訊息進行加密的密碼是從父密碼衍生的，則該父密碼不用於衍生其他密碼。因此，即使密碼被洩漏，損壞也僅限於使用該密碼加密的訊息。 選擇 **Enabled (已啟用)**或 **Disabled (停用)**。
Authentication Method (驗證方法)	選擇驗證方法。選擇 **Pre-Shared Key (預先共用金鑰)**或 **Certificates (憑證)**。
Pre-Shared Key (預先共用金鑰)	對通訊進行加密時，事先將使用其他頻道交換和共用加密金鑰。 如果選擇了 **Pre-Shared Key (預先共用金鑰)**作為 **Authentication Method (驗證方法)**，輸入 **Pre-Shared Key (預先共用金鑰)** (最多 32 位字元)。 • **Local/ID Type/ID (本機/ID 類型/ID)** 選擇發送方的 ID 類型，然後輸入 ID。 從類型中選擇 **IPv4 Address (IPv4 位址)**、**IPv6 Address (IPv6 位址)**、**FQDN**、**E-mail Address (電子郵件地址)**或 **Certificate (憑證)**。 如果選擇了 **Certificate (憑證)**，在 **ID** 欄位中輸入憑證的一般名稱。 • **Remote/ID Type/ID (遠端/ID 類型/ID)** 選擇接收方的 ID 類型，然後輸入 ID。 從類型中選擇 **IPv4 Address (IPv4 位址)**、**IPv6 Address (IPv6 位址)**、**FQDN**、**E-mail Address (電子郵件地址)**或 **Certificate (憑證)**。 如果選擇了 **Certificate (憑證)**，在 **ID** 欄位中輸入憑證的一般名稱。
Certificate (憑證)	如果選擇了 **Certificates (憑證)**作為 **Authentication Method (驗證方法)**，選擇憑證。 您只能選擇使用網路管理的安全設置螢幕中的 **Certificate (憑證)**頁面建立的憑證。

相關資訊

- 使用網路基本管理配置 IPsec 範本

IPsec 範本的 IKEv2 設定

選項	說明
Template Name (模板名稱)	輸入範本的名稱 (最多 16 位字元)。
Use Prefixed Template (使用帶首碼的模板)	選擇 **Custom (自訂)**、**IKEv2 High Security (IKEv2 高安全性)**或 **IKEv2 Medium Security (IKEv2 中安全性)**。設定項目視乎所選範本而有所不同。
Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))	IKE 通訊協定用於交換加密金鑰，以便使用 IPsec 進行加密通訊。為了僅在該時間執行加密通訊，將確定 IPsec 所需的加密演算法並共用加密金鑰。對於 IKE，將使用 Diffie-Hellman 密碼交換方法交換加密金鑰，且執行被限制為 IKE 的加密通訊。 如果在 **Use Prefixed Template (使用帶首碼的模板)**中選擇了 **Custom (自訂)**，請選擇 **IKEv2**。
Authentication Type (驗證類型)	• **Diffie-Hellman Group (Diffie-Hellman 群組)** 此密碼交換方法允許秘密密碼透過不受保護的網路進行安全交換。Diffie-Hellman 密碼交換方法使用離散對數問題 (而非秘密密碼) 發送和接收使用隨機數字和秘密密碼生成的資訊。 選擇 **Group1 (群組 1)**、**Group2 (群組 2)**、**Group5 (群組 5)** 或 **Group14 (群組 14)**。 • **Encryption (加密)** 選擇 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **Hash (雜湊)** 選擇 **MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 • **SA Lifetime (SA 存留期)** 指定 IKE SA 的存留期。 輸入時間 (秒數) 和千位元組數 (KB)。
Encapsulating Security (封裝安全性)	• **Protocol (通訊協定)** 選擇 **ESP**。 ESP 是使用 IPsec 執行加密通訊的通訊協定。ESP 對裝載 (通訊內容) 進行加密並新增其他資訊。IP 封包由標題及其後的加密裝載組成。除了加密資料，IP 封包還包含加密方式和加密金鑰、驗證資料等相關資訊。 • **Encryption (加密)** 選擇 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **Hash (雜湊)** 選擇 **MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 • **SA Lifetime (SA 存留期)** 指定 IKE SA 的存留期。 輸入時間 (秒數) 和千位元組數 (KB)。 • **Encapsulation Mode (封裝模式)** 選擇 **Transport (傳輸)**或 **Tunnel (隧道)**。 • **Remote Router IP-Address (遙距路由器 IP 位址)** 輸入遠端路由器的 IP 位址 (IPv4 或 IPv6)。僅當選擇了 **Tunnel (隧道)**模式時，輸入此資訊。 SA (安全性關聯) 是一種使用 IPsec 或 IPv6 的加密通訊方法，用於交換和共用加密方式和加密金鑰等資訊，以便在開始通訊前建立一個安全的通訊頻道。SA 還可能指已建立的虛擬加密通訊通道。用於 IPsec 的 SA 依照 IKE (網際網路密碼交換) 標準步驟建立加密方式、交換密碼和執行相互驗證。此外，SA 還會定期更新。

選項	說明
Perfect Forward Secrecy (PFS) (完整轉寄密碼(PFS))	PFS 不會從用於對訊息進行加密的先前密碼衍生密碼。此外，如果用於對訊息進行加密的密碼是從父密碼衍生的，則該父密碼不用於衍生其他密碼。因此，即使密碼被洩漏，損壞也僅限於使用該密碼加密的訊息。 選擇 **Enabled (已啟用)**或 **Disabled (停用)**。
Authentication Method (驗證方法)	選擇驗證方法。選擇 **Pre-Shared Key (預先共用金鑰)**、**Certificates (憑證)**、**EAP - MD5** 或 **EAP - MS-CHAPv2**。 EAP 驗證通訊協定是 PPP 的延伸。透過使用 EAP 和 IEEE802.1x，各工作階段的使用者認證使用不同的金鑰。 僅當在 **Authentication Method (驗證方法)**中選擇了 **EAP - MD5** 或 **EAP - MS-CHAPv2** 時，以下設定為必要項： • **Mode (模式)** 選擇 **Server-Mode (伺服器模式)**或 **Client-Mode (用戶端模式)**。 • **Certificate (憑證)** 選擇憑證。 • **User Name (使用者名稱)** 鍵入使用者名稱 (最多 32 個字元)。 • **Password (密碼)** 輸入密碼 (最多 32 個字元)。密碼必須輸入兩次以進行確認。
Pre-Shared Key (預先共用金鑰)	對通訊進行加密時，事先將使用其他頻道交換和共用加密金鑰。 如果選擇了 **Pre-Shared Key (預先共用金鑰)**作為 **Authentication Method (驗證方法)**，輸入 **Pre-Shared Key (預先共用金鑰)** (最多 32 位字元)。 • **Local/ID Type/ID (本機/ID 類型/ID)** 選擇發送方的 ID 類型，然後輸入 ID。 從類型中選擇 **IPv4 Address (IPv4 位址)**、**IPv6 Address (IPv6 位址)**、**FQDN**、**E-mail Address (電子郵件地址)**或 **Certificate (憑證)**。 如果選擇了 **Certificate (憑證)**，在 **ID** 欄位中輸入憑證的一般名稱。 • **Remote/ID Type/ID (遠端/ID 類型/ID)** 選擇接收方的 ID 類型，然後輸入 ID。 從類型中選擇 **IPv4 Address (IPv4 位址)**、**IPv6 Address (IPv6 位址)**、**FQDN**、**E-mail Address (電子郵件地址)**或 **Certificate (憑證)**。 如果選擇了 **Certificate (憑證)**，在 **ID** 欄位中輸入憑證的一般名稱。
Certificate (憑證)	如果選擇了 **Certificates (憑證)**作為 **Authentication Method (驗證方法)**，選擇憑證。 您只能選擇使用網路管理的安全設置螢幕中的 **Certificate (憑證)**頁面建立的憑證。

相關資訊

- 使用網路基本管理配置 IPsec 範本

IPsec 範本的手動設定

選項	說明
Template Name (模板名稱)	輸入範本的名稱 (最多 16 位字元)。
Use Prefixed Template (使用帶首碼的模板)	選擇 **Custom (自訂)**。
Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))	IKE 通訊協定用於交換加密金鑰，以便使用 IPsec 進行加密通訊。為了僅在該時間執行加密通訊，將確定 IPsec 所需的加密演算法並共用加密金鑰。對於 IKE，將使用 Diffie-Hellman 密碼交換方法交換加密金鑰，且執行被限制為 IKE 的加密通訊。 選擇 **Manual (手動)**。
Authentication Key (ESP, AH) (驗證金鑰 (ESP、AH))	輸入 **In/Out (輸入/輸出)**值。 在 **Encapsulating Security (封裝安全性)**部分中，當 **Use Prefixed Template (使用帶首碼的模板)**選擇為 **Custom (自訂)**、**Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))** 選擇為 **Manual (手動)**、**Hash (雜湊)**選擇為除 **None (無)**之外的設定時，這些設定為必要項。 視乎您在 **Encapsulating Security (封裝安全性)**部分中選擇的 **Hash (雜湊)**設定，可設定的字元數會有所不同。 如果所指定的驗證金鑰長度不同於所選擇的雜湊演算法，將會發生錯誤。 • **MD5**：128 位元 (16 位元組) • **SHA1**：160 位元 (20 位元組) • **SHA256**：256 位元 (32 位元組) • **SHA384**：384 位元 (48 位元組) • **SHA512**：512 位元 (64 位元組) 當您使用 ASCII 碼指定金鑰時，請將字元括在雙引號 (") 中。
Code key (ESP) (代碼金鑰(ESP))	輸入 **In/Out (輸入/輸出)**值。 在 **Encapsulating Security (封裝安全性)**中，當 **Use Prefixed Template (使用帶首碼的模板)**選擇為 **Custom (自訂)**、**Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))** 選擇為 **Manual (手動)**、**Protocol (通訊協定)**選擇為 **ESP** 時，這些設定為必要項。 視乎您在 **Encapsulating Security (封裝安全性)**部分中選擇的 **Encryption (加密)**設定，可設定的字元數會有所不同。 如果所指定的代碼金鑰長度不同於所選擇的雜湊演算法，將會發生錯誤。 • **DES**：64 位元 (8 位元組) • **3DES**：192 位元 (24 位元組) • **AES-CBC 128**：128 位元 (16 位元組) • **AES-CBC 256**：256 位元 (32 位元組) 當您使用 ASCII 碼指定金鑰時，請將字元括在雙引號 (") 中。
SPI	這些參數用來識別安全性資訊。一般而言，主機具有多種 IPsec 通訊類型的多個安全性關聯 (SA)。因此，當接收到 IPsec 封包時，必須識別適用的 SA。識別 SA 的 SPI 參數包括在驗證標頭 (AH) 和封裝安全內容 (ESP) 標頭中。 當 **Use Prefixed Template (使用帶首碼的模板)**選擇為 **Custom (自訂)**、**Internet Key Exchange (IKE) (互聯網金鑰交換(IKE))** 選擇為 **Manual (手動)**時，這些設定為必要項。 輸入 **In/Out (輸入/輸出)**值。(3 ~ 10 位字元)
Encapsulating Security (封裝安全性)	• **Protocol (通訊協定)** 選擇 **ESP** 或 **AH**。

選項	說明
	- ESP 是使用 IPsec 執行加密通訊的通訊協定。ESP 對裝載 (通訊內容) 進行加密並新增其他資訊。IP 封包由標題及其後的加密裝載組成。除了加密資料，IP 封包還包含加密方式和加密金鑰、驗證資料等相關資訊。 - AH 是 IPsec 通訊協定的一部分，用於驗證發送方並阻止操控資料 (確保資料的完整性)。在 IP 封包中，資料緊接在標題後面。此外，封包中還包含使用方程式從通訊內容、秘密金鑰等計算得出的雜湊值，以防止竄改發送方和操控資料。與 ESP 不同，此通訊協定不對通訊內容進行加密，而將資料作為普通文字進行發送和接收。 • **Encryption (加密) (不適用於 AH 選項。)** 選擇 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **Hash (雜湊)** 選擇 **None (無)**、**MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 僅當在 **Protocol (通訊協定)**中選擇了 **ESP** 時，才可以選擇 **None (無)**。 • **SA Lifetime (SA 存留期)** 指定 IKE SA 的存留期。 輸入時間 (秒數) 和千位元組數 (KB)。 • **Encapsulation Mode (封裝模式)** 選擇 **Transport (傳輸)**或 **Tunnel (隧道)**。 • **Remote Router IP-Address (遙距路由器 IP 位址)** 輸入遠端路由器的 IP 位址 (IPv4 或 IPv6)。僅當選擇了 **Tunnel (隧道)**模式時，輸入此資訊。 SA (安全性關聯) 是一種使用 IPsec 或 IPv6 的加密通訊方法，用於交換和共用加密方式和加密金鑰等資訊，以便在開始通訊前建立一個安全的通訊頻道。SA 還可能指已建立的虛擬加密通訊通道。用於 IPsec 的 SA 依照 IKE (網際網路密碼交換) 標準步驟建立加密方式、交換密碼和執行相互驗證。此外，SA 還會定期更新。

相關資訊

- 使用網路基本管理配置 IPsec 範本

使用網路的 IEEE 802.1x 驗證

- 什麼是 IEEE 802.1x 認證？
- 使用網路管理 (網頁瀏覽器) 設置有線網路的 IEEE 802.1x 認證
- IEEE 802.1x 驗證方法

什麼是 IEEE 802.1x 認證？

IEEE 802.1x 是 IEEE 標準，可限制 unauthorized 網路裝置進行存取。透過您的存取點或集線器，Brother 機器會發送一個驗證要求給 RADIUS 伺服器 (驗證伺服器)。RADIUS 伺服器驗證過要求後，您的機器才能存取網路。

相關資訊

- 使用網路的 IEEE 802.1x 驗證

使用網路管理 (網頁瀏覽器) 設置有線網路的 IEEE 802.1x 認證

- 如果您採用 EAP-TLS 認證方法來設置機器，開始設置之前，您必須安裝 CA 所頒發的用戶端憑證。如需用戶端憑證的資訊，請聯絡您的網路管理員。如果您安裝有多個憑證，我們建議您寫下您想使用的憑證名稱。
- 驗證伺服器憑證之前，您必須匯入負責簽署伺服器憑證的 CA 所頒發的 CA 憑證。請聯絡您的網路管理員或網際網路服務供應商 (ISP) 確認是否需要匯入 CA 憑證。

您也可從控制面板使用無線安裝精靈設置 IEEE 802.1x 驗證 (無線網路)。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Network (網路)**。

如果左側導覽列沒有顯示，從☰啓動導覽。

5. 執行下列其中一項操作：
   - 對於有線網路
     按一下 **Wired (有線)** > **Wired 802.1x Authentication (有線 802.1x 驗證)**。
   - 對於無線網路
     按一下 **Wireless (無線)** > **Wireless (Enterprise) (無線網絡(企業))**。
6. 設置 IEEE 802.1x 驗證方法。

- 若要為有線網路啟用 IEEE 802.1x 驗證，請在 **Enabled (已啟用)**頁面將 **Wired 802.1x status (有線 802.1x 狀態)**選擇為 **Wired 802.1x Authentication (有線 802.1x 驗證)**。
- 如果使用 **EAP-TLS** 驗證，必須從 **Client Certificate (用戶端憑證)** 下拉式選單選擇已安裝的用戶端憑證 (與憑證名稱一併顯示)。
- 如果您選擇 **EAP-FAST**、**PEAP**、**EAP-TTLS** 或 **EAP-TLS** 驗證，從 **Server Certificate Verification (伺服器憑證驗證)**下拉式選單中選擇驗證方法。事先將簽署伺服器憑證的 CA 所頒發的 CA 憑證匯入機器，以使用該憑證驗證伺服器憑證。

從 **Server Certificate Verification (伺服器憑證驗證)**下拉式選單中選擇下列其中一種驗證方法：

選項	說明
No Verification (無驗證)	永遠信任伺服器憑證。不執行驗證。
CA Cert. (CA 憑證)	使用簽署伺服器憑證的 CA 所頒發的 CA 憑證檢查伺服器憑證的 CA 可靠性的驗證方法。
CA Cert. + ServerID (CA 憑證 + 伺服器 ID)	除了檢查伺服器憑證的 CA 可靠性，還檢查伺服器憑證的一般名稱值的驗證方法[1]。

1 一般名稱驗證會將伺服器憑證的一般名稱與設置給 **Server ID (伺服器 ID)**的字元字串比較。在使用此方法之前，請聯絡系統管理員，瞭解伺服器憑證的一般名稱，然後設置 **Server ID (伺服器 ID)**。

7. 設置完成後，按一下 **Submit (提交)**。

   對於有線網路：設置完成後，將機器連接到支援 IEEE 802.1x 的網路。經過幾分鐘後，列印網路設置報告來檢查 **<Wired IEEE 802.1x>** 狀態。

選項	說明
Success	已啟用有線 IEEE 802.1x 功能且認證成功。
Failed (失敗)	已啟用有線 IEEE 802.1x 功能，但是認證失敗。
Off	有線 IEEE 802.1x 功能不可用。

相關資訊

- 使用網路的 IEEE 802.1x 驗證

相關主題:

- 安全憑證功能概述
- 配置裝置安全憑證

IEEE 802.1x 驗證方法

EAP-FAST

可延伸驗證通訊協定 - 透過安全通道進行的彈性驗證 (EAP-FAST) 由 Cisco Systems, Inc. 開發，此通訊協定利用使用者 ID 和密碼進行驗證，並以對稱密碼演算法達成 tunneled 驗證程序。

Brother 機器支援以下內部驗證方法：

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (有線網路)

可延伸認證通訊協定 - 第五代訊息摘要演算法 (EAP-MD5) 利用使用者 ID 和密碼進行挑戰-回應認證。

PEAP

受保護的可延伸驗證通訊協定 (PEAP) 是由 Cisco Systems, Inc.、Microsoft Corporation 和 RSA Security 共同開發的一個 EAP 方法版本。PEAP 會在用戶端和驗證伺服器之間建立加密的安全通訊端層 (SSL)/傳送層安全性 (TLS) 通道，供發送使用者 ID 和密碼之用。PEAP 可在伺服器和用戶端之間進行雙向認證。

Brother 機器支援以下內部驗證方法：

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

可延伸認證通訊協定 - 通道傳送層安全性 (EAP-TTLS) 由 Funk Software 和 Certicom 共同開發。EAP-TTLS 會在用戶端和認證伺服器之間建立一個類似於 PEAP 的加密 SSL 通道，供發送使用者 ID 和密碼之用。EAP-TTLS 可在伺服器和用戶端之間進行雙向認證。

Brother 機器支援以下內部驗證方法：

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

可延伸認證通訊協定 - 傳送層安全性 (EAP-TLS) 需要在用戶端和認證伺服器認證數位憑證。

相關資訊

- 使用網路的 IEEE 802.1x 驗證

使用者驗證

- 使用 Active Directory 驗證
- 使用 LDAP 驗證
- 使用安全功能鎖定 3.0

使用 Active Directory 驗證

- Active Directory 驗證簡介
- 使用網路管理設置 Active Directory 驗證
- 使用機器的控制面板登入以變更機器設定 (Active Directory 驗證)

Active Directory 驗證簡介

Active Directory 驗證可限制機器的使用。如果 Active Directory 驗證已啟用，機器的控制面板將被鎖定。您必須輸入使用者 ID 和密碼後，方能變更機器設定。

Active Directory 驗證提供以下功能：

支援的功能、選項或設定可能會因機器型號而有所不同。

- 儲存傳入列印資料
- 儲存傳入傳真資料
- 發送掃描資料到電郵伺服器時，視乎使用者 ID 從 Active Directory 伺服器獲取電子郵件地址。

  若要使用此功能，將 **Get Mail Address (獲取郵件地址)**設定選擇為 **On (開)**選項，並選擇 **LDAP + kerberos** 或 **LDAP + NTLMv2** 驗證方法。機器發送掃描資料到電郵伺服器時，您的電子郵件地址將被設定為發送方；如果想發送掃描資料到您的電子郵件地址，則您的電子郵件地址將被設定為接收方。

Active Directory 驗證已啟用時，機器會儲存所有傳入傳真資料。您登入後，機器將列印儲存的傳真資料。

您可以使用網路型管理工具變更 Active Directory 驗證設定。

相關資訊

- 使用 Active Directory 驗證

使用網路管理設置 Active Directory 驗證

Active Directory 驗證支援 Kerberos 驗證和 NTLMv2 驗證。您必須配置 SNTP 通訊協定 (網路時間伺服器) 和 DNS 伺服器才能進行認證。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Administrator (管理員)**>**User Restriction Function (使用者限制功能)**或 **Restriction Management (限制管理)**。

如果左側導覽列沒有顯示，從☰啟動導覽。

5. 選擇 **Active Directory Authentication (Active Directory 驗證)**。
6. 按一下 **Submit (提交)**。
7. 按一下 **Active Directory Authentication (Active Directory 驗證)**。
8. 配置下列設定：

支援的功能、選項或設定可能會因機器型號而有所不同。

選項	說明
Storage Fax RX Data (儲存傳真接收資料)	選擇此選項可儲存傳入傳真資料。登入機器後，您可以列印所有傳入傳真資料。
Remember User ID (記住用戶 ID)	選擇此選項可儲存您的使用者 ID。
Active Directory Server Address (Active Directory 伺服器位址)	輸入 Active Directory 伺服器的 IP 位址或伺服器名稱 (例如：ad.example.com)。
Active Directory Domain Name (Active Directory 網域名稱)	輸入 Active Directory 網域名稱。
Protocol & Authentication Method (通訊協定和驗證方法)	選擇通訊協定和驗證方法。
SSL/TLS	選擇 **SSL/TLS** 選項。
LDAP Server Port (LDAP 伺服器連接埠)	輸入連接埠號碼以透過 LDAP 連接 Active Directory 伺服器 (僅適用於 **LDAP + kerberos** 或 **LDAP + NTLMv2** 驗證方法)。
LDAP Search Root (LDAP 搜尋根目錄)	輸入 LDAP 搜尋根目錄 (僅適用於 **LDAP + kerberos** 或 **LDAP + NTLMv2** 驗證方法)。
Get Mail Address (獲取郵件地址)	選擇此選項可從 Active Directory 伺服器獲取已登入使用者的電子郵件地址。 (僅適用於 **LDAP + kerberos** 或 **LDAP + NTLMv2** 驗證方法)
Get User's Home Directory (獲取用戶的主目錄)	選擇此選項可獲取作為掃描到網路目標的主目錄。 (僅適用於 **LDAP + kerberos** 或 **LDAP + NTLMv2** 驗證方法)

9. 按一下 **Submit (提交)**。

相關資訊

- 使用 Active Directory 驗證

使用機器的控制面板登入以變更機器設定 (Active Directory 驗證)

Active Directory 驗證啟用時，機器的控制面板將被鎖定，直到您在機器的控制面板上輸入您的使用者 ID 和密碼。

1. 在機器的控制面板上輸入您的使用者 ID 和登入密碼。
2. 驗證成功時，機器的控制面板解除鎖定。

相關資訊

- 使用 Active Directory 驗證

使用 LDAP 驗證

- LDAP 驗證簡介
- 使用網路管理設置 LDAP 驗證
- 使用機器的控制面板登入以變更機器設定 (LDAP 驗證)

LDAP 驗證簡介

LDAP 驗證可限制機器的使用。如果 LDAP 驗證已啟用，機器的控制面板將被鎖定。您必須輸入使用者 ID 和密碼後，方能變更機器設定。

LDAP 驗證提供以下功能：

支援的功能、選項或設定可能會因機器型號而有所不同。

- 儲存傳入列印資料
- 儲存傳入傳真資料
- 發送掃描資料到電郵伺服器時，視乎使用者 ID 從 LDAP 伺服器獲取電子郵件地址。

  若要使用此功能，將 **Get Mail Address (獲取郵件地址)**設定選擇為 **On (開)**選項。機器發送掃描資料到電郵伺服器時，您的電子郵件地址將被設定為發送方；如果想發送掃描資料到您的電子郵件地址，則您的電子郵件地址將被設定為接收方。

LDAP 驗證已啟用時，機器會儲存所有傳入傳真資料。您登入後，機器將列印儲存的傳真資料。

您可以使用網路型管理工具變更 LDAP 驗證設定。

相關資訊

- 使用 LDAP 驗證

使用網路管理設置 LDAP 驗證

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Administrator (管理員)**>**User Restriction Function (使用者限制功能)**或 **Restriction Management (限制管理)**。

如果左側導覽列沒有顯示，從☰啓動導覽。

5. 選擇 **LDAP Authentication (LDAP 驗證)**。
6. 按一下 **Submit (提交)**。
7. 按一下 **LDAP Authentication (LDAP 驗證)**選單。
8. 配置下列設定：

支援的功能、選項或設定可能會因機器型號而有所不同。

選項	說明
Storage Fax RX Data (儲存傳真接收資料)	選擇此選項可儲存傳入傳真資料。登入機器後，您可以列印所有傳入傳真資料。
Remember User ID (記住用戶 ID)	選擇此選項可儲存您的使用者 ID。
LDAP Server Address (LDAP 伺服器位址)	輸入 LDAP 伺服器的 IP 位址或伺服器名稱 (例如：ldap.example.com)。
SSL/TLS	選擇 **SSL/TLS** 選項以使用 LDAP over SSL/TLS。
LDAP Server Port (LDAP 伺服器連接埠)	鍵入 LDAP 伺服器連接埠編號。
LDAP Search Root (LDAP 搜尋根目錄)	輸入 LDAP 搜尋根目錄。
Attribute of Name (Search Key) (名稱屬性 (搜尋金鑰))	鍵入要用作搜尋金鑰的屬性。
Get Mail Address (獲取郵件地址)	選擇此選項可從 LDAP 伺服器取得已登入使用者的電子郵件地址。
Get User's Home Directory (獲取用戶的主目錄)	選擇此選項可獲取作為掃描到網路目標的主目錄。

9. 按一下 **Submit (提交)**。

相關資訊

- 使用 LDAP 驗證

使用機器的控制面板登入以變更機器設定 (LDAP 驗證)

LDAP 驗證啟用時，機器的控制面板將被鎖定，直到您在機器的控制面板上輸入您的使用者 ID 和密碼。

1. 在機器的控制面板上輸入您的使用者 ID 和登入密碼。
2. 驗證成功時，機器的控制面板解除鎖定。

相關資訊

- 使用 LDAP 驗證

使用安全功能鎖定 3.0

安全功能鎖 3.0 限制機器上的可用功能以提高安全性。

- 使用安全功能鎖 3.0 前
- 使用網路管理來配置安全功能鎖定 3.0
- 使用安全功能鎖 3.0 進行掃描
- 配置安全功能鎖 3.0 的公用模式
- 使用網路管理設置個人首頁畫面設定
- 其他安全功能鎖 3.0 功能
- 使用機器的控制面板註冊新 IC 卡
- 註冊外部 IC 卡讀卡器

使用安全功能鎖 3.0 前

使用安全功能鎖可配置密碼、設定指定使用者頁數限制、授權使用以下列出的部分或全部功能。
您可使用網路管理來配置和變更安全功能鎖 3.0 的以下設定：

支援的功能、選項或設定可能會因機器型號而有所不同。

- **Print (列印)**
- **Copy (複印)**
- **Scan (掃描)**
- **傳真**
- **媒體**
- **Web Connect (網路連接)**
- **Apps (應用程式)**
- **Page Limits (頁面限制)**
- **Page Counters (頁碼計數器)**
- **Card ID (NFC ID) (卡片 ID(NFC ID))**

觸控式液晶螢幕型號：
安全功能鎖啟用時，機器自動進入公用模式，機器的部分功能限制為 authorized 使用者。若要存取受限制的機器功能，按  ，選擇您的使用者名稱，然後輸入您的密碼。

相關資訊

- 使用安全功能鎖定 3.0

使用網路管理來配置安全功能鎖定 3.0

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Administrator (管理員)**>**User Restriction Function (使用者限制功能)**或 **Restriction Management (限制管理)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 選擇 **Secure Function Lock (安全功能鎖定)**。
6. 按一下 **Submit (提交)**。
7. 按一下 **Restricted Functions (受限功能)**選單。
8. 配置用於管理每個使用者或每個群組的限制的設定。
9. 按一下 **Submit (提交)**。
10. 按一下 **User List (用戶清單)**選單。
11. 配置使用者清單。
12. 按一下 **Submit (提交)**。

    您也可在 **Secure Function Lock (安全功能鎖定)**選單中變更使用者清單鎖定設定。

相關資訊

- 使用安全功能鎖定 3.0

使用安全功能鎖 3.0 進行掃描

支援的功能、選項或設定可能會因機器型號而有所不同。

設定掃描限制 (適用於管理員)

安全功能鎖 3.0 允許管理員限制使用者進行掃描的權限。掃描功能的公共使用者設定設為關時，只有 **Scan (掃描)** 已勾選核取方塊的使用者能夠掃描。

使用掃描功能 (適用於受限使用者)

- 若要透過機器控制面板進行掃描：

  受限使用者必須在機器控制面板上輸入自己的密碼以存取掃描模式。
- 若要透過電腦進行掃描：

  透過電腦掃描前，受限使用者必須在機器控制面板上輸入自己的密碼。否則，使用者電腦上將顯示一條錯誤訊息。

如果本機器支援 IC 卡驗證，受限使用者還可將已註冊的 IC 卡接觸到機器控制面板的 NFC 標識上，以存取掃描模式。

相關資訊

- 使用安全功能鎖定 3.0

配置安全功能鎖 3.0 的公用模式

使用安全功能鎖螢幕設定公用模式，以限制公用使用者可使用的功能。公用使用者無需輸入密碼即可使用公用模式設定所允許的功能。

公用模式包括透過 Brother iPrint&Scan 和 Brother Mobile Connect 發送的列印工作。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。

   例如：

   https://192.168.1.2

   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Administrator (管理員)**>**User Restriction Function (使用者限制功能)**或 **Restriction Management (限制管理)**。

如果左側導覽列沒有顯示，從☰啓動導覽。

5. 選擇 **Secure Function Lock (安全功能鎖定)**。
6. 按一下 **Submit (提交)**。
7. 按一下 **Restricted Functions (受限功能)**選單。
8. 在 **Public Mode (公用模式)**行中，勾選一個核取方塊以允許所列出的功能，或者取消勾選一個核取方塊以限制所列出的功能。
9. 按一下 **Submit (提交)**。

相關資訊

- 使用安全功能鎖定 3.0

使用網路管理設置個人首頁畫面設定

作為管理員，您可以指定使用者可以在其個人首頁畫面上檢視哪些標籤。這些標籤可快速存取使用者 favorite 的捷徑，使用者可以從機器的控制面板將捷徑指派給其個人首頁畫面。

支援的功能、選項或設定可能會因機器型號而有所不同。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Administrator (管理員)**>**User Restriction Function (使用者限制功能)**或 **Restriction Management (限制管理)**。

如果左側導覽列沒有顯示，從☰啓動導覽。

5. 選擇 **Secure Function Lock (安全功能鎖定)**。
6. 在 **Tab Settings (標籤設定)**欄位中，選擇 **Personal (個人)**作為您要用作個人首頁畫面的標籤名稱。
7. 按一下 **Submit (提交)**。
8. 按一下 **Restricted Functions (受限功能)**選單。
9. 配置用於管理每個使用者或群組的限制的設定。
10. 按一下 **Submit (提交)**。
11. 按一下 **User List (用戶清單)**選單。
12. 配置使用者清單。
13. 從下拉式選單中為各使用者選擇 **User List / Restricted Functions (用戶清單/受限功能)**。
14. 從 **Home Screen (主畫面)**下拉式選單中為各使用者選擇標籤名稱。
15. 按一下 **Submit (提交)**。

相關資訊

- 使用安全功能鎖定 3.0

其他安全功能鎖 3.0 功能

在安全功能鎖螢幕上配置以下功能：

支援的功能、選項或設定可能會因機器型號而有所不同。

All Counter Reset (計數器重設)

在 **Page Counters (頁碼計數器)**欄位中按一下 **All Counter Reset (計數器重設)**，以重置頁碼計數器。

Export to CSV file (匯出至 CSV 檔案)

按一下 **Export to CSV file (匯出至 CSV 檔案)**，將包括 **User List / Restricted Functions (用戶清單/受限功能)** 資訊在內的目前和最後一頁的頁碼計數器記錄匯出為 CSV 檔案。

Card ID (NFC ID) (卡片 ID(NFC ID))

按一下 **User List (用戶清單)**選單，然後在 **Card ID (NFC ID) (卡片 ID(NFC ID))**欄位中輸入使用者的卡片 ID。您可以使用 IC 卡進行認證。

Output (輸出)

將分頁器組件安裝到機器上時，從下拉式選單中為各使用者選擇出紙匣。

Last Counter Record (最後一筆計數器記錄)

如果您希望機器在重置計數器後仍保留頁數，按一下 **Last Counter Record (最後一筆計數器記錄)**。

Counter Auto Reset (計數器自動重設)

按一下 **Counter Auto Reset (計數器自動重設)**設置所需的重置頁碼計數器的時間間隔。選擇每天、每週或每月。

相關資訊

- 使用安全功能鎖定 3.0

使用機器的控制面板註冊新 IC 卡

可在機器上註冊積體電路卡 (IC 卡)。

支援的功能、選項或設定可能會因機器型號而有所不同。

1. 用已註冊積體電路卡 (IC 卡) 接觸機器控制面板上的近距離通訊 (NFC) 符號。
2. 將使用者 ID 接觸到液晶螢幕上。
3. 按註冊卡按鍵。
4. 將新 IC 卡接觸到 NFC 標識上。
   新 IC 卡的號碼隨即註冊至機器。
5. 按確定按鍵。

相關資訊

- 使用安全功能鎖定 3.0

註冊外部 IC 卡讀卡器

連接外部 IC (積體電路) 卡讀卡器時，請使用 Web Based Management 註冊讀卡器。本機器可使用支援 HID 類別驅動程式的外部 IC 卡讀卡器。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

   用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。
4. 在左側導覽列中，按一下 **Administrator (管理員)** > **External Card Reader (外部讀卡機)**。

   如果左側導覽列沒有顯示，從☰啓動導覽。
5. 輸入必要的資訊，然後按一下 **Submit (提交)**。
6. 重新啟動 Brother 機器以啟用設置。
7. 將讀卡器連接至本機器。
8. 使用卡驗證時，將卡接觸到讀卡器上。

相關資訊

- 使用安全功能鎖定 3.0

安全地發送或接收電子郵件

- 使用網路管理設置電子郵件發送或接收
- 發送需要使用者認證的電子郵件
- 使用 SSL/TLS 安全發送或接收電子郵件

使用網路管理設置電子郵件發送或接收

- 接收電郵僅適用於某些型號。
- 我們建議使用網路管理配置需要使用者認證的加密電子郵件發送或使用 SSL/TLS 的電子郵件發送和接收 (僅限受支援的型號)。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Network (網路)** > **Network (網路)** > **Protocol (通訊協定)**。

如果左側導覽列沒有顯示，從☰啓動導覽。

5. 在 **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 用戶端)**欄位中，按一下 **Advanced Settings (進階設定)**並確保 **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 用戶端)**的狀態為 **Enabled (已啟用)**。

- 視乎機器，可用的通訊協定可能會有所不同。
- 如果顯示 **Authentication Method (驗證方法)**選項螢幕，選擇驗證方法，然後遵循螢幕上的說明執行操作。

6. 設置 **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 用戶端)**設定。
   - 配置完成後，透過發送測試電子郵件確認電子郵件設定是否正確。
   - 如果您不知道 POP3/IMAP4/SMTP 伺服器的設定，請聯絡您的網路管理員或網際網路服務供應商 (ISP)。
7. 完成後，按一下 **Submit (提交)**。
   Test Send/Receive E-mail Configuration (測試發送/接收電子郵件設定)對話方塊將會顯示。
8. 遵循對話方塊中的說明測試目前的設定。

相關資訊

- 安全地發送或接收電子郵件

相關主題:

- 使用 SSL/TLS 安全發送或接收電子郵件

發送需要使用者認證的電子郵件

本機器透過需要使用者驗證的電郵伺服器發送電子郵件。這種方法可防止 unauthorized 使用者存取電子郵件伺服器。

可透過使用者驗證發送電子郵件通知、電子郵件報告和 I-Fax (僅適用於某些型號)。

- 視乎機器，可用的通訊協定可能會有所不同。
- 我們建議您使用網路管理配置 SMTP 認證。

電郵伺服器設定

您必須設置機器的 SMTP 驗證方法，以符合電郵伺服器所使用的方法。有關電郵伺服器設定的詳細資訊，請聯絡網路管理員或網際網路供應商 (ISP)。

若要使用網路管理啟用 SMTP 伺服器認證，在 **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 用戶端)** 畫面中的 **Server Authentication Method (伺服器驗證方法)**下選擇驗證方法。

相關資訊

- 安全地發送或接收電子郵件

使用 SSL/TLS 安全發送或接收電子郵件

機器支援 SSL/TLS 通訊方法。若要使用採用 SSL/TLS 通訊的電郵伺服器，必須配置以下設定。

- 接收電郵僅適用於某些型號。
- 我們建議使用網路管理配置 SSL/TLS。

驗證伺服器憑證

在 **SSL/TLS** 選項下，如果您選擇 **SSL** 或 **TLS**，將自動勾選 **Verify Server Certificate (驗證伺服器憑證)**核取方塊。

- 驗證伺服器憑證之前，您必須匯入負責簽署伺服器憑證的 CA 所頒發的 CA 憑證。請聯絡您的網路管理員或網際網路服務供應商 (ISP) 確認是否需要匯入 CA 憑證。
- 如果您無需驗證伺服器憑證，請取消勾選 **Verify Server Certificate (驗證伺服器憑證)**核取方塊。

連接埠編號

如果您選擇 **SSL** 或 **TLS**，則 **Port (連接埠)** 值將變更以與通訊協定相匹配。若要手動變更連接埠編號，選擇 **SSL/TLS** 設定後，輸入連接埠編號。

您必須設置機器的通訊方法，以符合電郵伺服器所使用的方法。如需詳細的電郵伺服器設定資訊，請聯絡您的網路管理員或 ISP。

在大多數情況下，安全的網路郵件服務需要下列設定：

支援的功能、選項或設定可能會因機器型號而有所不同。

SMTP	**Port (連接埠)**	587
	Server Authentication Method (伺服器驗證方法)	**SMTP-AUTH (SMTP-認證)**
	SSL/TLS	**TLS**
POP3	**Port (連接埠)**	995
	SSL/TLS	**SSL**
IMAP4	**Port (連接埠)**	993
	SSL/TLS	**SSL**

相關資訊

- 安全地發送或接收電子郵件

相關主題:

- 使用網路管理設置電子郵件發送或接收
- 配置裝置安全憑證

儲存列印記錄至網路

將列印記錄儲存到網路概述

透過將列印記錄儲存到網路功能，您可以使用公用網際網路檔案系統 (CIFS) 通訊協定將機器的列印記錄檔案儲存至網路伺服器。您可記錄每一個列印工作的 ID、列印工作類型、工作名稱、使用者名稱、日期、時間和已列印頁數。CIFS 是 TCP/IP 上執行的通訊協定，讓網路上的電腦可以在內部網路或網際網路上共用檔案。

列印記錄記下的列印功能如下：

支援的功能、選項或設定可能會因機器型號而有所不同。

- 從電腦列印工作
- USB 直接列印
- 複印
- 接收的傳真
- Web Connect 列印

- 將列印記錄儲存到網路功能支援 Kerberos 驗證和 NTLMv2 驗證。必須配置 SNTP 通訊協定 (網路時間伺服器)，或在控制面板上正確設定日期、時間和時區，才能進行驗證。
- 將檔案儲存到伺服器時，您可將檔案類型設為 TXT 或 CSV。

相關資訊

- 儲存列印記錄至網路

使用網路管理配置「將列印記錄儲存到網路」設定

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Administrator (管理員)** > **Store Print Log to Network (將列印記錄儲存到網絡)**。

如果左側導覽列沒有顯示，從☰啟動導覽。

5. 在 **Print Log (列印記錄)**欄位中，按一下 **On (開)**。
6. 配置下列設定：

支援的功能、選項或設定可能會因機器型號而有所不同。

選項	說明
Network Folder Path (網絡資料夾路徑)	輸入 CIFS 伺服器上用來儲存列印記錄的目標資料夾 (例如：\\ComputerName\SharedFolder)。
File Name (檔案名稱)	輸入您想使用的列印記錄檔名稱，最多 32 位字元。
File Type (檔案類型)	選擇 **TXT** 或 **CSV** 選項作為列印記錄檔案類型。
Time Source for Log (記錄的時間源)	選擇列印記錄的時間來源。
Auth. Method (驗證方法)	選擇存取 CIFS 伺服器所需的驗證方法：**Auto (自動)**、**Kerberos** 或 **NTLMv2**。Kerberos 是一種在網路伺服器上使用單一登入方法讓裝置或個人安全驗證身分的通訊協定。NTLMv2 是 Windows 登入伺服器採用的認證方法。 • **Auto (自動)**：如果選擇 **Auto (自動)**，將使用 NTLMv2 驗證方法。 • **Kerberos**：選擇 **Kerberos** 選項，僅使用 Kerberos 驗證。 • **NTLMv2**：選擇 **NTLMv2** 選項，僅使用 NTLMv2 驗證。 • 採用 **Kerberos** 和 **NTLMv2** 驗證時，還必須設置 **Date&Time (日期和時間)**設定或 SNTP 通訊協定 (網路時間伺服器) 和 DNS 伺服器。 • 您也可透過機器控制面板來配置日期和時間設定。
Username (用戶名稱)	輸入使用者名稱進行認證 (最多 96 位字元)。 如果使用者名稱為網域的一部分，請利用下列其中一種形式輸入使用者名稱：user@domain or domain\user。
Password (密碼)	輸入密碼進行認證 (最多 32 位字元)。
Kerberos Server Address (Kerberos 伺服器位址) (如有需要)	輸入金鑰發佈中心 (KDC) 主機位址 (例如：kerberos.example.com；最多 64 位字元) 或 IP 位址 (例如：192.168.56.189)。

選項	說明
Error Detection Setting (錯誤偵測設定)	選擇網路發生錯誤無法將列印記錄儲存到伺服器時應採取的動作。

7. 在 **Connection Status (連線狀態)**欄位中，確認最近一筆記錄狀態。

也可在機器液晶螢幕上確認錯誤狀態。

8. 按一下 **Submit (提交)**顯示 **Test Print Log to Network (網絡列印記錄測試)**頁面。
   若要測試您的設定，請按一下 **Yes (是)**，然後轉到下一步驟。
   若要跳過測試，請按一下 **No (否)**。您的設定將自動送出。
9. 機器將測試您的設定。
10. 如果接受您的設定，螢幕上會顯示 **Test OK (測試成功)**。
    如果出現 **Test Error (測試錯誤)**，請檢查所有設定，然後按一下 **Submit (提交)**再次顯示測試頁面。

相關資訊

- 儲存列印記錄至網路

使用將列印記錄儲存到網路功能的錯誤偵測設定

使用錯誤偵測設定來確定因網路發生錯誤而無法將列印記錄儲存到伺服器時要採取的動作。

1. 啟動網頁瀏覽器。
2. 在瀏覽器的位址列中輸入「https://machine's IP address」(「machine's IP address」為本機器的 IP 位址)。
   例如：
   https://192.168.1.2
   本機器的 IP 位址可在網路設置報告中找到。
3. 如有需要，在 **Login (登入)**欄位中輸入密碼，然後按一下 **Login (登入)**。

用於管理本機器之設定的預設密碼位於機器背面或底座並且標有「**Pwd**」。首次登入時，遵循螢幕上的說明變更預設密碼。

4. 在左側導覽列中，按一下 **Administrator (管理員)** > **Store Print Log to Network (將列印記錄儲存到網絡)**。

如果左側導覽列沒有顯示，從☰啓動導覽。

5. 在 **Error Detection Setting (錯誤偵測設定)** 部分，選擇 **Cancel Print (取消列印)** 或 **Ignore Log & Print (忽略記錄並列印)** 選項。

支援的功能、選項或設定可能會因機器型號而有所不同。

選項	說明
Cancel Print (取消列印)	如果您選擇 **Cancel Print (取消列印)**選項，無法將列印記錄儲存到伺服器時會 canceled 列印工作。 即使您選擇 **Cancel Print (取消列印)** 選項，機器也會列印接收的傳真。

Ignore Log & Print (忽略記錄並列印)	如果您選擇 **Ignore Log & Print (忽略記錄並列印)** 選項，即使列印記錄無法儲存到伺服器，機器還是會列印文件。
	列印記錄儲存功能恢復後，列印記錄會以下列原則記錄：
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	a. 列印結束後若無法儲存列印記錄，將不會記錄已列印頁數。
	b. 開始和結束列印時若無法儲存列印記錄，將不會記錄該工作的列印記錄。該功能恢復時，列印記錄中會反映該錯誤。

6. 按一下 **Submit (提交)**顯示 **Test Print Log to Network (網絡列印記錄測試)**頁面。
   若要測試您的設定，請按一下 **Yes (是)**，然後轉到下一步驟。
   若要跳過測試，請按一下 **No (否)**。您的設定將自動送出。
7. 機器將測試您的設定。
8. 如果接受您的設定，螢幕上會顯示 **Test OK (測試成功)**。
   如果出現 **Test Error (測試錯誤)**，請檢查所有設定，然後按一下 **Submit (提交)**再次顯示測試頁面。

相關資訊

- 儲存列印記錄至網路

透過安全功能鎖 3.0 使用將列印記錄儲存到網路功能

安全功能鎖 3.0 啟動時，在儲存列印記錄至網路的報告中將記錄複印、傳真接收、Web Connect 列印和 USB 直接列印等功能的註冊使用者名稱。Active Directory 驗證啟用時，在儲存列印記錄至網路的報告中將記錄使用者名稱：

支援的功能、選項或設定可能會因機器型號而有所不同。

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

相關資訊

- 儲存列印記錄至網路

brother

Brother Earth

www.brotherearth.com

TCHN
版本 0