



安全功能指南

重要的安全性資訊

- 用於管理本機器之設定的預設密碼位於機器底部並且標有 "Pwd:"。建議立即變更預設密碼，防止機器遭到未經授權存取。
- 將本機器連接至網際網路等外部網路時，請確保您的網路環境受到單獨的防火牆或其他方式保護，以防止因設定不充分或惡意第三方未經授權存取而導致資訊洩露。
- 如果附近有訊號，無線區域網路可讓您自由連接至區域網路。但是，如果未正確設置安全設定，則訊號可能被惡意第三方攔截，從而可能導致：
 - 竊取個人或機密資訊
 - 資訊被不正當地傳輸至冒充指定個人的各方
 - 傳播被攔截的轉譯通訊內容



相關資訊

- [網路](#)
-

設置裝置安全憑證

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、選項和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，建議您使用信任的組織發行的憑證。

- 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

- [設置裝置安全憑證](#)

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

- [設置裝置安全憑證](#)

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 ☰ 啟動導覽。

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

- [設置裝置安全憑證](#)

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 ☰ 啟動導覽。

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 ☰ 啟動導覽。

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 ☰ 啟動導覽。

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 ☰ 啟動導覽。

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 存取網路管理
- 安裝自我簽署憑證 (Windows 管理員使用者)
- 設置裝置安全憑證

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 ☰ 啟動導覽。

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 ☰ 啟動導覽。

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
- 設置裝置安全憑證

使用 IPPS 列印文件

若要透過 IPP 通訊協定安全地列印文件，請使用 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 ☰ 啟動導覽。

5. 確認已勾選 **IPP** 核取方塊。



如果未勾選 **IPP** 核取方塊，請勾選 **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，返回到機器網頁，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 **IPP** 區域中勾選 **HTTPS** 核取方塊，然後按一下 **Submit (提交)**。
8. 重新啟動機器以啟用設置。

使用 IPPS 進行通訊時，無法避免未經授權的列印伺服器存取。



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，以安全地管理網路裝置。

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. 確保已啟用 **SNMP** 設定，然後按一下 **Advanced Settings (進階設定)**。
6. 設置 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。您可在此模式下使用本機器的所有應用程式。不過，此模式並不安全，因為此模式並不會驗證使用者，也不會將資料加密。
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. 設置 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。若要安全地管理列印伺服器，請使用 SNMPv3 模式並設置設定。
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，請選取所需選項。

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，可限制未經授權的網路裝置進行存取。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)。

- 啟動網頁瀏覽器。
- 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。
- 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。

- 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 ☰ 啟動導覽。

- 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))**。
- 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	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](#)
- [設置裝置安全憑證](#)

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通道驗證程序。

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](#)