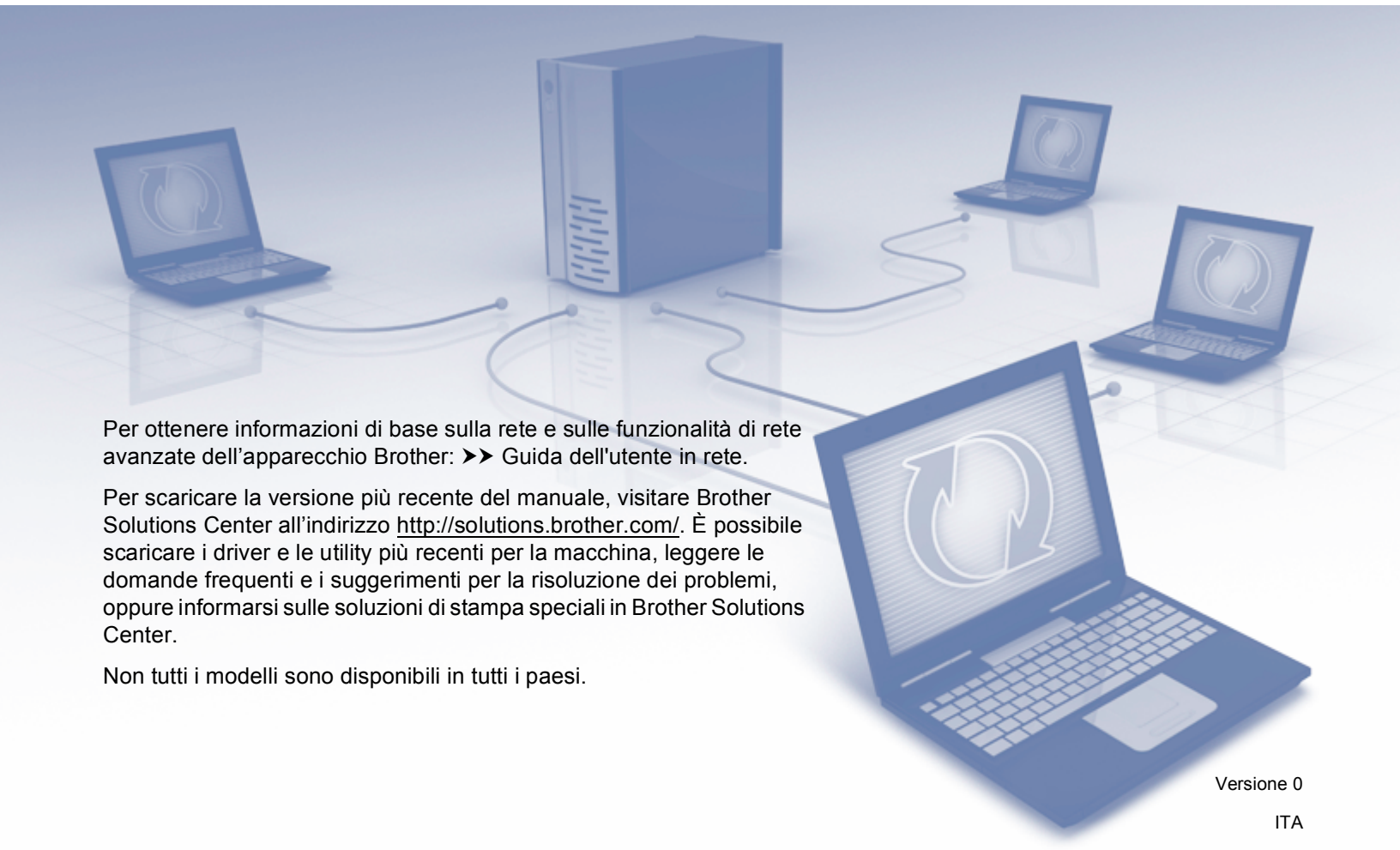
Guida SSL

(Secure Socket Layer)



Per ottenere informazioni di base sulla rete e sulle funzionalità di rete avanzate dell'apparecchio Brother: ➤➤ Guida dell'utente in rete.

Per scaricare la versione più recente del manuale, visitare Brother Solutions Center all'indirizzo http://solutions.brother.com/. È possibile scaricare i driver e le utility più recenti per la macchina, leggere le domande frequenti e i suggerimenti per la risoluzione dei problemi, oppure informarsi sulle soluzioni di stampa speciali in Brother Solutions Center.

Non tutti i modelli sono disponibili in tutti i paesi.

Versione 0

ITA

Modelli interessati

Il presente manuale dell'utente riguarda i seguenti modelli.

HL-5450DN(T)/5470DW(T)/6180DW(T)/S7000DN

DCP-8110DN/8150DN/8155DN/8250DN/MFC-8510DN/8710DW/8910DW/8950DW(T)

Definizione delle note

Nella presente Guida dell'utente vengono utilizzate le seguenti icone:

Nota	Le note spiegano come intervenire in determinate situazioni oppure offrono suggerimenti relativi all'utilizzo delle diverse funzioni della stampante.

Marchi

Il logo Brother è un marchio registrato di Brother Industries, Ltd.

Microsoft, Windows, Windows Server e Internet Explorer sono marchi commerciali registrati o marchi commerciali di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Windows Vista è un marchio commerciale registrato o un marchio commerciale di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Google Cloud Print è un marchio commerciale di Google Inc.

Tutte le società i cui programmi software sono citati nel presente manuale dispongono di un contratto di licenza software specifico per i rispettivi programmi prioritari.

Eventuali nomi commerciali e nomi di prodotto di altre società presenti sui prodotti Brother, i documenti ed eventuali altri materiali ad essi correlati sono marchi commerciali o marchi registrati delle rispettive società.

NOTA IMPORTANTE

- L’utilizzo di questo prodotto è approvato solo nel paese di acquisto. Non utilizzare questo prodotto al di fuori del paese di acquisto poiché potrebbe violare le norme relative alle telecomunicazioni senza fili di tale paese.
- Salvo diversamente specificato, in questo manuale si utilizzano schermate di MFC-8950DW(T).
- In questo documento Windows® XP rappresenta Windows® XP Professional, Windows® XP Professional x64 Edition e Windows® XP Home Edition.
- In questo documento Windows Server® 2003 rappresenta Windows Server® 2003 e Windows Server® 2003 x64 Edition.
- In questo documento Windows Server® 2008 rappresenta Windows Server® 2008 e Windows Server® 2008 R2.
- Windows Vista® in questo documento sta per tutte le edizioni di Windows Vista®.
- Windows® 7 in questo documento sta per tutte le edizioni di Windows® 7.
- Visitare Brother Solutions Center all’indirizzo http://solutions.brother.com/ e fare clic su Manuali nella pagina del proprio modello per scaricare gli altri manuali.

Sommario

1 Introduzione

Informazioni generali

Secure Socket Layer (SSL) è un metodo efficace per proteggere i dati inviati sulla rete locale o ad ampio raggio. Questo metodo consente di crittografare i dati inviati sulla rete (ad es., un processo di stampa), in modo da renderli illeggibili in caso di eventuali violazioni da parte di terzi.

Può essere configurato su reti wireless o cablate e utilizzato con altre forme di protezione, come le chiavi WPA™ e i firewall.

Breve storia di SSL

SSL fu originariamente creato per proteggere le informazioni sul traffico web, in particolare i dati inviati tra i browser web e i server. Ad esempio, quando si utilizza Internet Explorer® per i servizi di Internet Banking e nel browser web viene visualizzato https:// insieme a un piccolo lucchetto, si sta utilizzando SSL. Successivamente iniziò ad essere utilizzato con altre applicazioni come Telnet, stampanti e software FTP fino a diventare una soluzione universale per la sicurezza online. Attualmente la versione originaria del progetto è ancora utilizzata da molti rivenditori online e banche per la protezione dei dati sensibili come numeri di carte di credito, registrazioni dei clienti, ecc.

Grazie ai suoi standard crittografici e protettivi estremamente elevati, SSL è considerato attendibile dalle banche di tutto il mondo.

I vantaggi di utilizzare SSL

Un vantaggio esclusivo dell'utilizzo di SSL su apparecchi Brother è quello di garantire stampe sicure su una rete IP impedendo agli utenti non autorizzati di leggere i dati inviati all'apparecchio. Il suo punto di forza è la possibilità di utilizzarlo per la stampa sicura di dati riservati. Ad esempio, nel caso di una grande società è probabile che la divisione risorse umane stampi buste paga in modo regolare. Senza crittografia, i dati contenuti nelle buste paga possono essere letti da altri utenti della rete. Con SSL, tuttavia, ogni tentativo di intercettazione dei dati avrà come risultato una pagina di codici illeggibili al posto della busta paga vera e propria.

Uso dei certificati per la sicurezza del dispositivo

La macchina Brother supporta l'uso di più certificati di protezione che consentono una gestione, un'autenticazione e una comunicazione sicura con la macchina. È possibile utilizzare le seguenti caratteristiche del certificato di protezione con la macchina. Quando si stampano documenti o si utilizza la Gestione basata sul Web (browser) in modo sicuro con SSL, è necessario installare il certificato sul proprio computer. Vedere *Installazione del certificato digitale* ➤➤ pagina 4.

- Comunicazione SSL/TLS
- Comunicazione SSL per SMTP/POP3

La macchina Brother supporta i seguenti certificati.

- Certificato preinstallato

  L'apparecchio dispone di un certificato preinstallato e autofirmato.

  Tramite questo certificato è possibile utilizzare facilmente la comunicazione SSL/TLS senza creare o installare un certificato. Se si desidera utilizzare la funzione Google Cloud Print™ disponibile sull'apparecchio, è possibile utilizzare questo certificato preinstallato per configurare le impostazioni di Google Cloud Print in modo sicuro. Per ulteriori informazioni su Google Cloud Print, visitare il Brother Solutions Center all'indirizzo http://solutions.brother.com/ e fare clic su Manuali nella pagina del proprio modello per scaricare Guida Google Cloud Print.

Nota

- La funzione Google Cloud Print non è disponibile per il modello HL-S7000DN.
- Il certificato preinstallato e autofirmato non è in grado di proteggere la comunicazione da attacchi informatici di tipo "spoofing". Per una maggiore sicurezza è consigliabile utilizzare un certificato emesso da un'organizzazione affidabile.

- Certificato autofirmato

  Il server di stampa rilascia un proprio certificato. Tramite questo certificato, è possibile utilizzare la comunicazione SSL/TLS senza ottenere un certificato da una CA. (Vedere *Creazione di un certificato autofirmato* ➤➤ pagina 6).

- Certificato di una CA

  Sono disponibili due metodi per installare un certificato rilasciato da una CA. Se già si dispone di un certificato da una CA o si desidera utilizzare un certificato da una CA esterna affidabile:

  - Quando si utilizza una CSR (Certificate Signing Request) da questo server di stampa. (Vedere *Creazione di una CSR (Certificate Signing Request)* ➤➤ pagina 7).
  - Quando si importano un certificato e una chiave privata. (Vedere *Importazione ed esportazione di un certificato e di una chiave privata* ➤➤ pagina 17).

■ Certificato CA

Se si utilizza un certificato CA che identifica la CA (Autorità di certificazione) stessa, è necessario importare un certificato CA dalla CA prima di eseguire la configurazione. (Vedere *Importazione ed esportazione di un certificato CA* ➤➤ pagina 18).

Nota

- Se si intende utilizzare la comunicazione SSL/TLS, è consigliabile contattare l'amministratore del sistema prima di procedere.
- Quando si ripristinano le impostazioni di fabbrica predefinite del server di stampa, il certificato e la chiave privata installati vengono eliminati. Se si desidera conservare lo stesso certificato e la stessa chiave privata dopo aver ripristinato le impostazioni del server di stampa, esportarli prima del ripristino e quindi reinstallarli. (Vedere *Come importare il certificato autofirmato, il certificato emesso da una CA e la chiave privata* ➤➤ pagina 17).

2 Certificato digitale per la comunicazione SSL

Installazione del certificato digitale

La stampa in rete protetta o la gestione protetta tramite la Gestione basata sul Web (browser) richiedono l'installazione di un certificato digitale sia sull'apparecchio che sul dispositivo che invia i dati all'apparecchio (ad esempio un computer). La macchina dispone di un'interfaccia preinstallata. Per configurare il certificato, l'utente deve accedere all'apparecchio da remoto tramite un browser web utilizzando il proprio indirizzo IP.

Nota

Si consiglia Windows® Internet Explorer® 7.0/8.0 o Firefox® 3.6 per Windows® e Safari 4.0/5.0 per Macintosh. Verificare inoltre che JavaScript e i cookie siano sempre attivati nel browser utilizzato. Se si utilizza un browser diverso, accertarsi che sia compatibile con HTTP 1.0 e HTTP 1.1.

1. Avviare il browser.
2. Digitare "http://indirizzo IP della macchina/" nel browser (dove per "indirizzo IP della macchina" si intende l'indirizzo IP della macchina o il nome del server di stampa).
   - Ad esempio: http://192.168.1.2/
3. Per impostazione predefinita non è richiesta alcuna password. Immettere la password, se è stata impostata, e premere  .
4. Fare clic su **Rete**.
5. Fare clic su **Sicurezza**.
6. Fare clic su **Certificato**.

7 È possibile configurare le impostazioni del certificato.
Per creare un certificato autofirmato utilizzando la Gestione basata sul Web, passare a *Creazione di un certificato autofirmato* ➤➤ pagina 6.
Per creare una CSR (Certificate Signing Request), passare a *Creazione di una CSR (Certificate Signing Request)* ➤➤ pagina 7.

1 Per creare e installare un certificato autofirmato

2 Per utilizzare un certificato da un'Autorità di certificazione (CA)

Nota

- Le funzioni in grigio e prive di collegamento non sono disponibili.
- Per ulteriori informazioni sulla configurazione, vedere il testo della Guida in Gestione basata sul Web.

Creazione di un certificato autofirmato

1. Fare clic su **Crea certificato autofirmato**.
2. Immettere **Nome comune** e **Data valida**.

Nota

- Il **Nome comune** non può superare i 64 caratteri di lunghezza. Immettere un identificatore, ad esempio un indirizzo IP, un nome di nodo o di dominio, da utilizzare per l'accesso alla macchina tramite la comunicazione SSL/TLS. Per impostazione predefinita è visualizzato il nome nodo.
- Viene visualizzato un avviso se si utilizza il protocollo IPPS o HTTPS e si immette un nome diverso nell'URL rispetto al **Nome comune** utilizzato per il certificato autofirmato.

3. È possibile scegliere le impostazioni **Algoritmo a chiave pubblica** e **Algoritmo di Digest** dall'elenco a discesa. Le impostazioni predefinite sono **RSA (2048 bit)** per **Algoritmo a chiave pubblica** e **SHA256** per **Algoritmo di Digest**.
4. Fare clic su **Invia**.
5. Il certificato autofirmato è stato creato e salvato correttamente nella memoria dell'apparecchio.

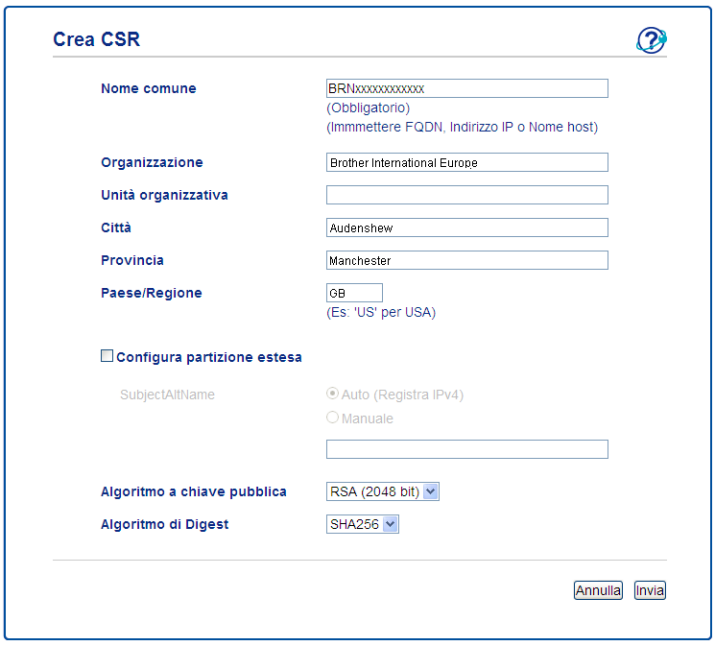
Creazione di una CSR (Certificate Signing Request)

Una CSR (Certificate Signing Request) è una richiesta inviata a una CA per autenticare le credenziali contenute nel certificato.

Nota

È consigliabile installare il certificato principale della CA nel computer prima di creare la CSR.

1. Fare clic su **Crea CSR**.
2. Immettere un **Nome comune** e i propri dati, ad esempio **Organizzazione**.
   Vengono richiesti i dati aziendali affinché la CA possa confermare l'identità del richiedente e attestarlo all'esterno.



Nota

- Il **Nome comune** non può superare i 64 caratteri di lunghezza. Immettere un identificatore, ad esempio un indirizzo IP, un nome di nodo o di dominio, da utilizzare per l'accesso alla macchina tramite la comunicazione SSL/TLS. Per impostazione predefinita è visualizzato il nome nodo. Il **Nome comune** è obbligatorio.
- Viene visualizzato un avviso se si immette un nome diverso nell'URL rispetto al Nome comune utilizzato per il certificato.
- **Organizzazione**, **Unità organizzativa**, **Città** e **Provincia** non possono superare i 64 caratteri di lunghezza.
- Il **Paese/Regione** deve essere rappresentato da un codice paese ISO 3166 composto da due caratteri.
- Se si sta configurando l'estensione del certificato X.509v3, selezionare la casella di controllo **Configura partizione estesa**, quindi selezionare **Auto (Registra IPv4)** o **Manuale**.

3 È possibile scegliere le impostazioni **Algoritmo a chiave pubblica** e **Algoritmo di Digest** dall'elenco a discesa. Le impostazioni predefinite sono **RSA (2048 bit)** per **Algoritmo a chiave pubblica** e **SHA256** per **Algoritmo di Digest**.

4 Fare clic su **Invia**. Viene visualizzata la schermata seguente.

5 Dopo qualche istante viene prodotto il certificato, che può essere salvato in un file di piccole dimensioni o copiato e incollato direttamente nel modulo CSR online emesso da un'Autorità di certificazione. Fare clic su **Salva** per salvare il file CSR sul proprio computer.

Nota

Attenersi alla politica della CA per il metodo con cui inviare una CSR alla CA.

6 La CSR è stata creata. Per informazioni su come installare il certificato sul proprio apparecchio, passare a *Come installare il certificato nella macchina* ➤➤ pagina 9.

Come installare il certificato nella macchina

Quando si riceve il certificato da una CA, eseguire le seguenti procedure per installarlo nel server di stampa.

Nota

È possibile installare solo un certificato emesso con la CSR di questa macchina. Se si desidera creare un altro CSR, assicurarsi che il certificato sia installato prima di procedere alla creazione. Creare un altro CSR dopo aver installato il certificato nella macchina. Diversamente il CSR creato prima dell'installazione non sarà più valido.

1. Fare clic su **Installa certificato** nella pagina **Certificato**.

2. Specificare il file del certificato emesso da una CA e fare clic su **Invia**.

3. Il certificato è stato creato e salvato correttamente nella memoria dell'apparecchio.
Per utilizzare la comunicazione SSL/TLS, è necessario installare il certificato principale della CA nel computer. Contattare l'amministratore della rete per informazioni sull'installazione.
La configurazione del certificato digitale è stata completata. Se si desidera inviare o ricevere una e-mail utilizzando SSL, consultare *Invio o Ricezione (per i modelli DCP e MFC) di e-mail in sicurezza* ➤➤ pagina 25 per le fasi di configurazione necessarie.

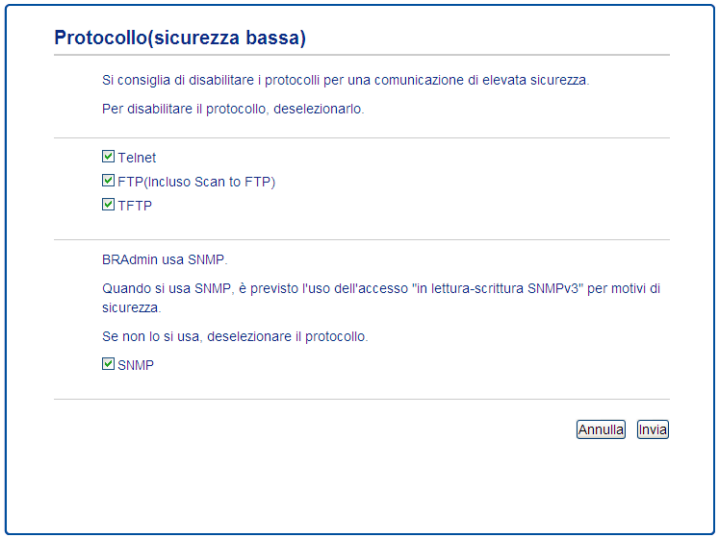
Scelta del certificato

Dopo aver installato il certificato, seguire i passaggi sotto riportati per scegliere il certificato che si desidera utilizzare.

1. Fare clic su **Rete**.
2. Fare clic su **Protocollo**.
3. Fare clic su **Impostazioni Server HTTP** e scegliere il certificato dall'elenco a discesa **Selezionare il certificato**.

Nota

- Se appare la seguente finestra di dialogo, Brother consiglia di disabilitare i protocolli Telnet, FTP e TFTP e la gestione di rete con versioni precedenti di BRAdmin Professional (2.8 o precedente) per proteggere le comunicazioni. In caso contrario, l'autenticazione dell'utente non sarà sicura.



- Per i modelli DCP e MFC:

  Se si disattiva il protocollo FTP, anche la funzione Scansione su FTP viene disattivata.

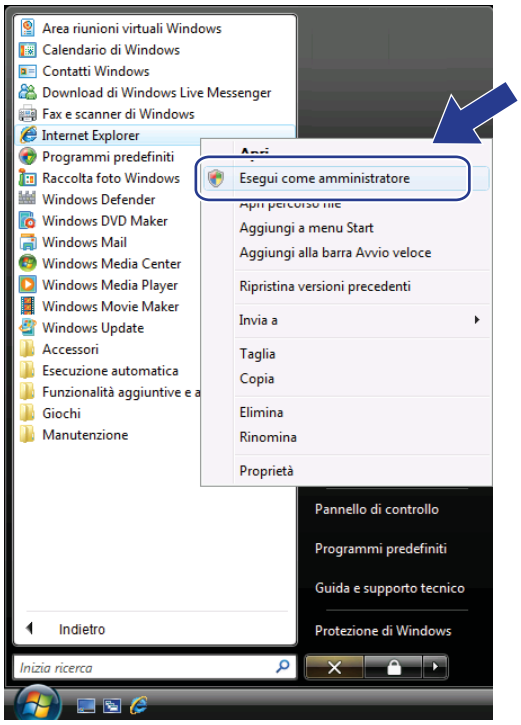
4. Fare clic su **Invia**.

Installazione del certificato autofirmato o del certificato preinstallato per gli utenti di Windows Vista®, Windows® 7 e Windows Server® 2008 con diritti di amministratore

Nota

- Le seguenti procedure si riferiscono a Windows® Internet Explorer®. Se si utilizza un altro browser, seguire il testo della Guida del browser stesso.
- Per installare il certificato autofirmato o preinstallato, è necessario disporre dei diritti di amministratore.

1. Fare clic sul pulsante e selezionare **Tutti i programmi**.
2. Fare clic con il pulsante destro del mouse su **Internet Explorer**, quindi fare clic su **Esegui come amministratore**.



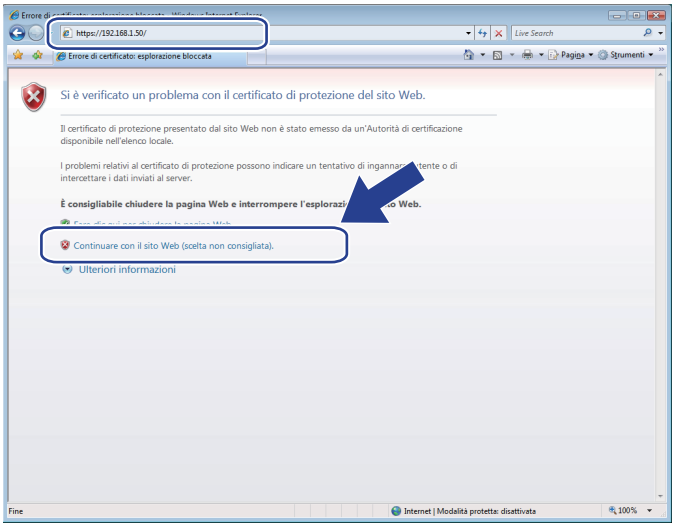
Nota

Se viene visualizzata la schermata **Controllo dell'account utente**,

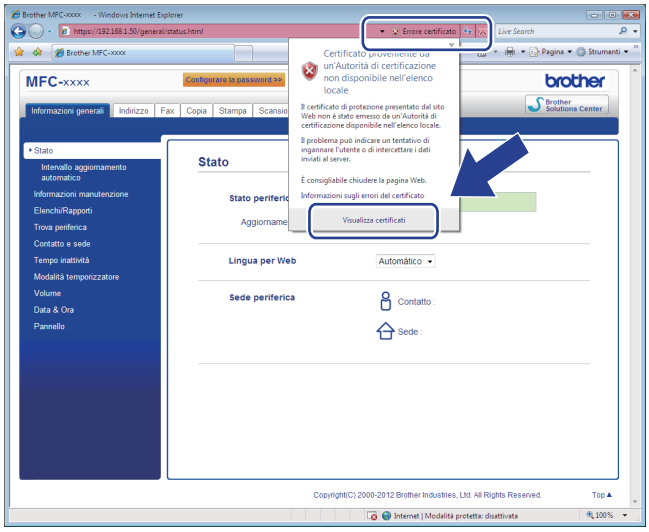
(Windows Vista®) Fare clic su **Continua (Consenti)**.

(Windows® 7) Fare clic su **Sì**.

3 Digitare “https://indirizzo IP della macchina/” nel browser per accedere alla macchina (dove “indirizzo IP della macchina” è l’indirizzo IP della macchina o il nome di nodo assegnato al certificato).
Quindi, fare clic su **Continuare con il sito Web (scelta non consigliata)**.

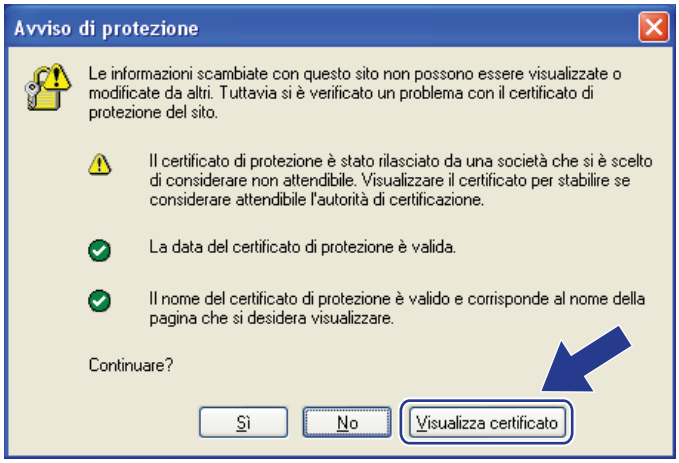


4 Fare clic su **Errore certificato** e quindi su **Visualizza certificati**. Per ulteriori istruzioni, seguire i passaggi dal punto ❹ nella sezione *Installazione del certificato autofirmato o del certificato preinstallato per gli utenti di Windows® XP e Windows Server® 2003* ➤➤ pagina 14.

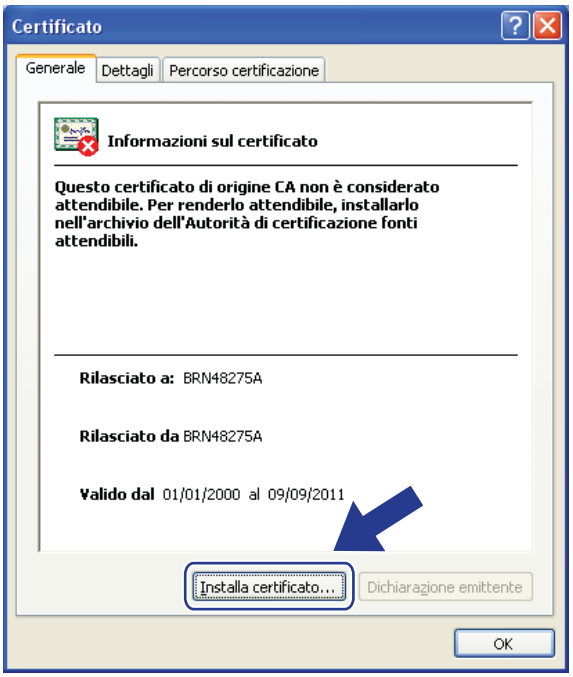


Installazione del certificato autofirmato o del certificato preinstallato per gli utenti di Windows® XP e Windows Server® 2003

1. Avviare il browser.
2. Digitare “https://indirizzo IP della macchina/” nel browser per accedere alla macchina (dove “indirizzo IP della macchina” è l’indirizzo IP o il nome di nodo assegnato al certificato).
3. Quando viene visualizzata la finestra di dialogo dell’avviso di protezione, effettuare una delle seguenti operazioni:
   - Fare clic su **Continuare con il sito Web (scelta non consigliata)**. Fare clic su **Errore certificato** e quindi su **Visualizza certificati**.
   - Quando viene visualizzata la seguente finestra di dialogo, fare clic su **Visualizza certificato**.

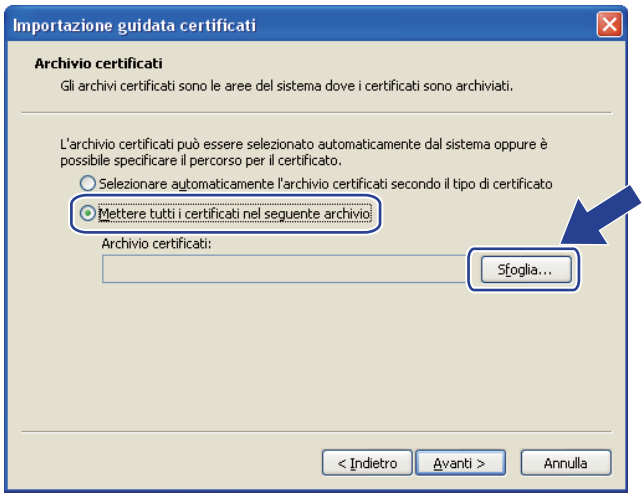


4. Fare clic su **Installa certificato...** dalla scheda **Generale**.

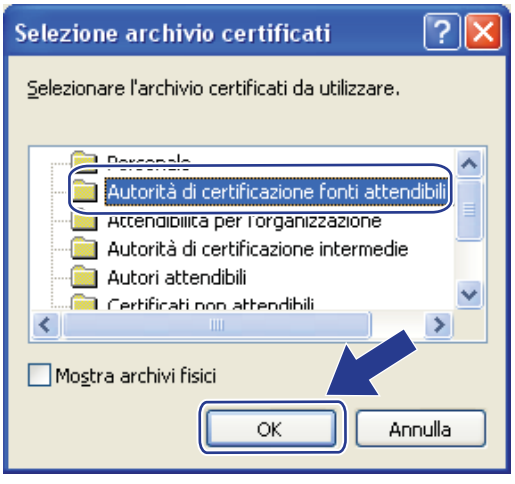


5 Quando viene visualizzato **Importazione guidata certificati**, fare clic su **Avanti**.

6 È necessario specificare una posizione per installare il certificato. È consigliabile scegliere **Mettere tutti i certificati nel seguente archivio** e poi fare clic su **Sfoglia...**.



7 Selezionare **Autorità di certificazione fonti attendibili** e quindi fare clic su **OK**.

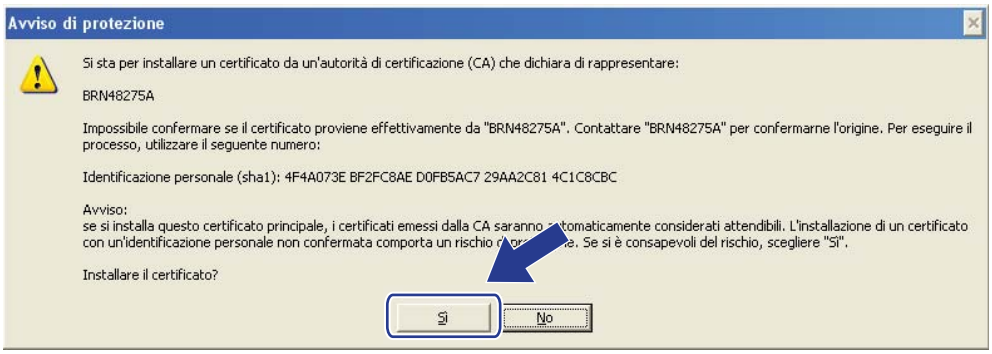


8 Fare clic su **Avanti**.

9 Nella schermata successiva, fare clic su **Fine**.

10 Viene richiesta l'installazione del certificato.
Eseguire una delle seguenti operazioni:

- Se si installa il certificato autofirmato, confermare l'identificazione personale e poi fare clic su **Sì**.
- Se si installa il certificato preinstallato, fare clic su **Sì**.



Nota

- Per il certificato autofirmato, l'identificazione personale è stampata nel rapporto di configurazione di rete.

  Per informazioni sulla stampa della configurazione di rete, vedere *Stampa della pagina Impostazioni stampante (Per HL-5450DN(T))* ➤➤ pagina 29 o *Stampa del rapporto di configurazione di rete (Per gli altri modelli)* ➤➤ pagina 29.
- Per il certificato preinstallato, l'identificazione personale è stampata nel rapporto di configurazione di rete.

11 Fare clic su **OK**.

12 Il certificato autofirmato o il certificato preinstallato è ora installato sul computer e la comunicazione SSL/TLS è disponibile.

Ripetere la stessa procedura in ogni computer da cui si desidera stampare in modo sicuro. Una volta installato, tuttavia, questi passaggi non dovranno essere ripetuti salvo modifiche al certificato.

Importazione ed esportazione di un certificato e di una chiave privata

È possibile archiviare il certificato e la chiave privata sulla macchina e gestirli con le procedure di importazione ed esportazione.

Come importare il certificato autofirmato, il certificato emesso da una CA e la chiave privata

1. Fare clic su **Importa certificato e chiave privata** nella pagina **Certificato**.
2. Specificare il file da importare.
3. Immettere la password se il file è crittografato e fare clic su **Invia**.
4. Il certificato e la chiave privata sono stati importati correttamente nella macchina.

Come esportare il certificato autofirmato, il certificato emesso da una CA e la chiave privata

1. Fare clic su **Esporta** visualizzato con **Elenco certificati** nella pagina **Certificato**.
2. Immettere una password se si desidera crittografare il file.

Nota

Se il campo della password viene lasciato in bianco, l'output non viene crittografato.

3. Immettere di nuovo la password per confermare e fare clic su **Invia**.
4. Specificare la posizione in cui salvare il file.
5. Il certificato e la chiave privata sono stati esportati correttamente nel computer.

Importazione ed esportazione di un certificato CA

È possibile memorizzare un certificato CA sull'apparecchio con le procedure di importazione ed esportazione.

Importazione di un certificato CA

1. Fare clic su **Certificato CA** nella pagina **Sicurezza**.
2. Fare clic su **Importa certificato CA** e scegliere il certificato. Fare clic su **Invia**.

Esportazione di un certificato CA

1. Fare clic su **Certificato CA** nella pagina **Sicurezza**.
2. Scegliere il certificato da esportare e fare clic su **Esporta**. Fare clic su **Invia**.
3. Fare clic su **Salva** e scegliere la cartella di destinazione.
4. Scegliere la destinazione in cui salvare il certificato esportato, quindi salvare il certificato.

Gestione di più certificati

La funzione per certificati multipli consente di gestire ogni certificato installato utilizzando la Gestione basata sul Web. Dopo l'installazione dei certificati è possibile visualizzare quali certificati sono installati dalla pagina **Certificato** e quindi visualizzare il contenuto, eliminare o esportare il certificato. Per informazioni su come accedere alla pagina **Certificato**, vedere *Installazione del certificato digitale* ➤➤ pagina 4.

■ Per i modelli di stampante

L'apparecchio Brother consente di archiviare fino a tre certificati autofirmati o fino a tre certificati emessi da una CA. È possibile utilizzare i certificati memorizzati per l'impiego del protocollo HTTPS/IPPS o l'autenticazione IEEE 802.1x.

■ Per i modelli DCP e MFC

L'apparecchio Brother consente di memorizzare fino a quattro certificati autofirmati o fino a quattro certificati emessi da una CA. È possibile utilizzare i certificati memorizzati per l'impiego del protocollo HTTPS/IPPS, l'autenticazione IEEE 802.1x o un PDF firmato.

È inoltre possibile memorizzare fino a quattro o sei (HL-S7000DN) certificati CA per l'uso dell'autenticazione IEEE 802.1x e di SSL per SMTP/POP3.

Si consiglia di memorizzare un certificato in meno e di mantenere l'ultimo libero per gestire la scadenza dei certificati. Ad esempio, se si desidera memorizzare un certificato CA, memorizzare tre certificati e lasciarne uno di riserva. In caso di nuova emissione di un certificato (ad esempio in seguito a scadenza), è possibile importare un nuovo certificato nel backup ed eliminare il certificato scaduto senza causare errori di configurazione.

Nota

- Quando si utilizzano HTTPS/IPPS, IEEE 802.1x o un PDF firmato (per i modelli DCP e MFC), è necessario scegliere il certificato da utilizzare.
- Quando si utilizzano le comunicazioni SSL per SMTP/POP3 (per i modelli DCP e MFC), non è necessario scegliere il certificato. Il certificato richiesto viene selezionato automaticamente.

3 Gestione della macchina di rete in sicurezza con SSL/TLS

Per gestire in modo sicuro la macchina di rete, è necessario utilizzare le utilità di gestione con i protocolli di protezione.

Gestione protetta tramite Gestione basata sul Web (browser)

È consigliabile utilizzare il protocollo HTTPS per la gestione protetta. Per utilizzare questi protocolli sono necessarie le seguenti impostazioni della macchina.

Nota

- Il protocollo HTTPS è abilitato per impostazione predefinita.

  È possibile cambiare le impostazioni del protocollo HTTPS e il certificato da utilizzare nella schermata Gestione basata sul Web facendo clic su **Rete**, **Protocollo** e quindi su **Impostazioni Server HTTP**.
- È inoltre necessario installare sul proprio computer il certificato già installato sull'apparecchio. Consultare *Installazione del certificato autofirmato o del certificato preinstallato per gli utenti di Windows Vista®, Windows® 7 e Windows Server® 2008 con diritti di amministratore* ➤➤ pagina 12 o *Installazione del certificato autofirmato o del certificato preinstallato per gli utenti di Windows® XP e Windows Server® 2003* ➤➤ pagina 14.

1. Avviare il browser.
2. Digitare "https://indirizzo IP macchina/" nel browser. (Se si utilizza il certificato creato, digitare "https://nome comune/" nel browser. La voce "nome comune" rappresenta il nome comune assegnato al certificato, ad esempio un indirizzo IP, un nome di nodo o un nome di dominio. Per l'assegnazione di un nome comune per il certificato, vedere *Uso dei certificati per la sicurezza del dispositivo* ➤➤ pagina 2.)

   ■ Ad esempio:

   https://192.168.1.2/ (se il nome comune corrisponde all'indirizzo IP della macchina)
3. Per impostazione predefinita non è richiesta alcuna password. Immettere la password, se è stata impostata, e premere  .

4 Stampa dei documenti in sicurezza con SSL

Stampa dei documenti in sicurezza con IPPS per Windows®

È consigliabile utilizzare il protocollo IPPS per la gestione protetta. Per utilizzare il protocollo IPPS, sono necessarie le seguenti impostazioni della macchina.

Nota

- La comunicazione tramite IPPS non può impedire l'accesso non autorizzato al server di stampa.
- È inoltre necessario installare sul proprio computer il certificato già installato sull'apparecchio. Consultare *Installazione del certificato autofirmato o del certificato preinstallato per gli utenti di Windows Vista®, Windows® 7 e Windows Server® 2008 con diritti di amministratore* ➤➤ pagina 12 o *Installazione del certificato autofirmato o del certificato preinstallato per gli utenti di Windows® XP e Windows Server® 2003* ➤➤ pagina 14.
- È necessario attivare il protocollo IPPS. L'impostazione predefinita è abilitata. È possibile cambiare le impostazioni del protocollo IPPS e il certificato da utilizzare nella schermata Gestione basata sul Web facendo clic su **Rete**, **Protocollo** e quindi su **Impostazioni Server HTTP**.

Windows® XP e Windows Server® 2003

1. Fare clic su **Start**, quindi scegliere **Stampanti e fax**.
2. Fare clic su **Aggiungi stampante** per avviare **Installazione guidata stampante**.
3. Quando viene visualizzata la schermata **Installazione guidata stampante**, fare clic su **Avanti**.
4. Scegliere **Stampante di rete o stampante collegata a un altro computer**.
5. Fare clic su **Avanti**.
6. Scegliere **Connetti ad una stampante in Internet o della rete domestica o aziendale** e immettere nell'URL il seguente indirizzo:
   "https://indirizzo IP dell'apparecchio/" (dove "indirizzo IP dell'apparecchio" è l'indirizzo IP dell'apparecchio o il nome del nodo.)

Nota

- È importante utilizzare “https://” e non “http://”, altrimenti la stampa su IPP non sarà sicura.
- Se il file host sul computer è stato modificato o si sta utilizzando un Domain Name System (DNS), è possibile immettere anche il nome DNS del server di stampa. Poiché il server di stampa supporta i nomi TCP/IP e NetBIOS, è possibile immettere anche il nome NetBIOS del server di stampa. Il nome NetBIOS può essere visualizzato nel rapporto di configurazione di rete. (Per informazioni sulla stampa del rapporto di configurazione di rete, vedere *Stampa della pagina Impostazioni stampante (Per HL-5450DN(T))* ➤➤ pagina 29 o *Stampa del rapporto di configurazione di rete (Per gli altri modelli)* ➤➤ pagina 29.) Il nome NetBIOS assegnato corrisponde ai primi 15 caratteri del nome del nodo e per impostazione predefinita è riportato come “BRNxxxxxxxxxxxx” per una rete cablata o “BRWxxxxxxxxxxxx” per una rete senza fili. (“xxxxxxxxxxxx” è l'indirizzo MAC o l'indirizzo Ethernet della macchina).

7 Facendo clic su **Avanti**, Windows® XP e Windows Server® 2003 si connettono all’URL specificato.

- Se il driver della stampante è già stato installato:

  Viene visualizzata la schermata di selezione della stampante nel **Installazione guidata stampante**.

  Andare al passo ⓫.

- Se il driver della stampante NON è stato installato:

  Uno dei vantaggi derivanti dall’impiego del protocollo di stampa IPP è la sua capacità di stabilire il nome del modello della stampante quando si comunica con essa. Dopo aver stabilito correttamente la comunicazione, il nome del modello della stampante viene visualizzato automaticamente. Questo significa che non è necessario comunicare a Windows® XP e Windows Server® 2003 il tipo di driver della stampante utilizzato.

  Andare al passo ❽.

Nota

Se il driver della stampante che si vuole installare non dispone di un certificato digitale, viene visualizzato un messaggio di avvertimento. Fare clic su **Continua** per continuare l’installazione.

8 Fare clic su **Disco driver**. Viene quindi richiesto di inserire il disco del driver.

9 Fare clic su **Sfoglia** e scegliere il driver della stampante Brother appropriato contenuto nel CD-ROM o nella condivisione di rete.
Fare clic su **OK**.

10 Fare clic su **OK**.

11 Scegliere la macchina e fare clic su **OK**.

12 Selezionare **Sì** se si desidera utilizzare l’apparecchio come stampante predefinita. Fare clic su **Avanti**.

13 Selezionare **Fine**; a questo punto l’apparecchio è configurato ed è quindi possibile avviare la stampa. Per verificare la connessione della stampante, stampare una pagina di prova.

Windows Vista®, Windows® 7 e Windows Server® 2008

1. (Windows Vista®)
   Fare clic sul pulsante , **Pannello di controllo**, **Hardware e suoni**, quindi su **Stampanti**.
   (Windows® 7)
   Fare clic sul pulsante e selezionare **Dispositivi e stampanti**.
   (Windows Server® 2008)
   Fare clic su **Start**, **Pannello di controllo**, **Hardware e suoni**, quindi su **Stampanti**.
2. Fare clic su **Aggiungi stampante**.
3. Scegliere **Aggiungi stampante di rete, wireless o Bluetooth**.
4. Fare clic su **La stampante desiderata non é nell'elenco**.
5. Scegliere **Seleziona in base al nome una stampante condivisa** e immettere nell'URL il seguente indirizzo: "https://indirizzo IP dell'apparecchio/ipp" (dove "indirizzo IP dell'apparecchio" è l'indirizzo IP dell'apparecchio o il nome del nodo.)

Nota

- È importante utilizzare "https://" e non "http://", altrimenti la stampa su IPP non sarà sicura.
- Se il file host sul computer è stato modificato o si sta utilizzando un Domain Name System (DNS), è possibile immettere anche il nome DNS del server di stampa. Poiché il server di stampa supporta i nomi TCP/IP e NetBIOS, è possibile immettere anche il nome NetBIOS del server di stampa. Il nome NetBIOS può essere visualizzato nel rapporto di configurazione di rete. (Per informazioni sulla stampa del rapporto di configurazione di rete, vedere *Stampa della pagina Impostazioni stampante (Per HL-5450DN(T))* ➤➤ pagina 29 o *Stampa del rapporto di configurazione di rete (Per gli altri modelli)* ➤➤ pagina 29.) Il nome NetBIOS assegnato corrisponde ai primi 15 caratteri del nome del nodo e per impostazione predefinita è riportato come "BRNxxxxxxxxxxxx" per una rete cablata o "BRWxxxxxxxxxxxx" per una rete senza fili. ("xxxxxxxxxxxx" è l'indirizzo MAC o l'indirizzo Ethernet della macchina).

6. Quando si sceglie **Avanti**, Windows Vista® e Windows Server® 2008 si connettono all'URL specificato.
   - Se il driver della stampante è già stato installato:

     Viene visualizzata la schermata di selezione della stampante nell'Installazione guidata stampante. Fare clic su **OK**.

     Se l'apposito driver della stampante è già installato sul computer, Windows Vista® e Windows Server® 2008 lo utilizzano automaticamente. In questo caso viene richiesto di specificare se si desidera rendere la stampante predefinita, quindi l'Installazione guidata del driver viene completata. A questo punto è possibile avviare la stampa.

     Andare al passo ⓫.

■ Se il driver della stampante NON è stato installato:

Uno dei vantaggi derivanti dall'impiego del protocollo di stampa IPP è la sua capacità di stabilire il nome del modello della stampante quando si comunica con essa. Dopo aver stabilito correttamente la comunicazione, il nome del modello della stampante viene visualizzato automaticamente. Questo significa che non è necessario comunicare a Windows Vista® e Windows Server® 2008 il tipo di driver della stampante utilizzato.

Andare al passo ❼.

7. Se l'apparecchio non è nell'elenco delle stampanti supportate, fare clic su **Disco driver**. Viene quindi richiesto di inserire il disco del driver.

8. Fare clic su **Sfoglia** e scegliere il driver della stampante Brother appropriato contenuto nel CD-ROM o nella condivisione di rete. Fare clic su **Apri**.

9. Fare clic su **OK**.

10. Specificare il nome del modello dell'apparecchio. Fare clic su **OK**.

Nota

- Quando viene visualizzata la schermata controllo dell'account utente, fare clic su **Continua**.
- Se il driver della stampante che si vuole installare non dispone di un certificato digitale, viene visualizzato un messaggio di avvertimento. Fare clic su **Installa il software del driver** per continuare l'installazione. L'**Installazione guidata stampante** viene quindi completata.

11. Viene visualizzata la schermata di **Digitare il nome di una stampante** nella configurazione guidata di **Aggiungi stampante**. Selezionare la casella di controllo **Imposta come stampante predefinita** se si desidera utilizzare l'apparecchio come stampante predefinita, quindi fare clic su **Avanti**.

12. Per verificare la connessione della stampante, fare clic su **Stampa pagina di prova**, quindi su **Fine**. A questo punto l'apparecchio è configurato ed è quindi possibile avviare la stampa.

5 Invio o Ricezione (per i modelli DCP e MFC) di e-mail in sicurezza

Configurazione mediante Gestione basata sul Web (browser Web)

È possibile configurare l'invio sicuro di e-mail con l'autenticazione utente o l'invio e la ricezione di e-mail (per i modelli DCP e MFC) utilizzando SSL/TLS nella schermata Gestione basata sul Web.

1. Avviare il browser.
2. Digitare "http://indirizzo IP della macchina/" nel browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina).
   - Ad esempio:

     http://192.168.1.2/
3. Per impostazione predefinita non è richiesta alcuna password. Immettere la password, se è stata impostata, e premere  .
4. Fare clic su **Rete**.
5. Fare clic su **Protocollo**.
6. Fare clic su **Impostazione avanzata** di **POP3/SMTP** e assicurarsi che lo stato di **POP3/SMTP** sia **Attivata**.
7. È possibile configurare le impostazioni **POP3/SMTP** in questa pagina.

Nota

- Per ulteriori informazioni, vedere il testo della Guida in Gestione basata sul Web.
- È anche possibile confermare se le impostazioni e-mail sono corrette dopo la configurazione inviando una e-mail di prova.
- Se non si conoscono le impostazioni del server POP3/SMTP, rivolgersi all'amministratore di sistema o all'ISP (provider di servizi Internet) per i dettagli.

8. Dopo la configurazione, fare clic su **Invia**. Vengono visualizzate la schermata **Test configurazione invio posta elettronica** o **Test configurazione invio/ricezione posta elettronica**.
9. Seguire le istruzioni sullo schermo se si desidera verificare le impostazioni correnti.

Invio o Ricezione (per i modelli DCP e MFC) di e-mail in sicurezza con SSL/TLS

L'apparecchio supporta i metodi SSL/TLS per l'invio o la ricezione (per i modelli DCP e MFC) di e-mail attraverso un server di posta che richiede la comunicazione SSL/TLS protetta. Per inviare o ricevere e-mail attraverso un server di posta elettronica che utilizza la comunicazione SSL/TLS è necessario configurare correttamente SMTP su SSL/TLS o POP3 su SSL/TLS.

Verifica del certificato del server

- Se si sceglie SSL o TLS per **SMTP su SSL/TLS** o **POP3 su SSL/TLS**, la casella di controllo **Verificare il certificato server** viene automaticamente selezionata per verificare il certificato del server.
  - Prima di verificare il certificato del server è necessario importare il certificato CA emesso dalla CA che ha firmato il certificato del server. Rivolgersi all'amministratore della rete o al provider di servizi Internet per sapere se è necessario importare un certificato CA. Per l'importazione del certificato, vedere *Importazione ed esportazione di un certificato CA* ➤➤ pagina 18.
  - Se non è necessario verificare il certificato del server, deselezionare **Verificare il certificato server**.

Numero di porta

- Se si sceglie SSL o TLS, il valore **Porta SMTP** o **Porta POP3** viene modificato in base al protocollo. Se si desidera cambiare manualmente il numero della porta, immettere tale numero dopo aver scelto **SMTP su SSL/TLS** o **POP3 su SSL/TLS**.
- È necessario configurare il metodo di comunicazione POP3/SMTP in base al server di posta. Per i dettagli sulle impostazioni del server di posta rivolgersi all'amministratore di rete o all'ISP (provider di servizi Internet). Nella maggior parte dei casi, i servizi di posta sul Web protetti richiedono le seguenti impostazioni:
  - **SMTP**
    - **Porta SMTP**: 587
    - **Metodo di autenticazione del server SMTP**: SMTP-AUTH
    - **SMTP su SSL/TLS**: TLS
  - **POP3**
    - **Porta POP3**: 995
    - **POP3 su SSL/TLS**: SSL

6 Risoluzione dei problemi

Informazioni generali

In questo capitolo è spiegato come risolvere i problemi di rete tipici che si possono verificare durante l'utilizzo della macchina Brother. Se dopo aver letto il capitolo non è ancora possibile risolvere il problema, visitare il Brother Solutions Center all'indirizzo: (http://solutions.brother.com/).

Visitare il Brother Solutions Center all'indirizzo (http://solutions.brother.com/) e fare clic su Manuali nella pagina del proprio modello per scaricare gli altri manuali.

Identificazione del problema

Prima di leggere questo capitolo, assicurarsi che le seguenti voci siano configurate.

Controllare innanzi tutto quanto segue:
Il cavo di alimentazione è collegato correttamente e la macchina Brother è accesa.
Tutti gli imballaggi protettivi sono stati rimossi dalla macchina.
Le cartucce toner e il gruppo tamburo o cartucce d'inchiostro (HL-S7000DN) sono installati correttamente.
I coperchi anteriore e posteriore sono chiusi.
Nel vassoio carta è stata inserita correttamente della carta.
La macchina è stata connessa correttamente alla rete.

Visitare la pagina della soluzione negli elenchi di seguito

- Non è possibile stampare il documento su Internet con IPPS.

  Vedere *Non è possibile stampare il documento su Internet con IPPS.* ➤➤ pagina 28.
- Desidero controllare che i dispositivi di rete funzionino correttamente.

  Vedere *Desidero controllare che i dispositivi di rete funzionino correttamente.* ➤➤ pagina 28.

Non è possibile stampare il documento su Internet con IPPS.

Domanda	Soluzione
Non è possibile comunicare con l'apparecchio Brother utilizzando le comunicazioni SSL.	■ Ottenere un certificato valido e installarlo di nuovo sull'apparecchio e sul computer. ■ Assicurarsi che le impostazioni della porta dell'apparecchio siano corrette. È possibile confermare le impostazioni della porta dell'apparecchio nella schermata Gestione basata sul Web facendo clic su **Rete**, **Protocollo** e quindi su **Impostazioni Server HTTP**.

Desidero controllare che i dispositivi di rete funzionino correttamente.

Domanda	Soluzione
L'apparecchio Brother è acceso?	Assicurarsi di aver confermato tutte le istruzioni in *Controllare innanzi tutto quanto segue:* ➤➤ pagina 27.
Dove è possibile trovare le impostazioni di rete della macchina Brother, ad esempio l'indirizzo IP?	Stampare il rapporto di configurazione di rete. Consultare *Stampa della pagina Impostazioni stampante (Per HL-5450DN(T))* ➤➤ pagina 29 o *Stampa del rapporto di configurazione di rete (Per gli altri modelli)* ➤➤ pagina 29.

Stampa della pagina Impostazioni stampante (Per HL-5450DN(T))

Nota

Nome nodo: il nome del nodo viene visualizzato nel rapporto di configurazione di rete. Il nome del nodo predefinito è “BRNxxxxxxxxxxxx”. (“xxxxxxxxxxxx” è l'indirizzo MAC o l'indirizzo Ethernet della macchina).

La Pagina Impostazioni stampante stampa un rapporto che elenca le impostazioni attuali della stampante, comprese le impostazioni del server di stampa di rete.

Si può stampare la pagina Impostazioni stampante utilizzando il pulsante **Go** dell’apparecchio.

1. Assicurarsi che il coperchio anteriore sia chiuso e che il cavo di alimentazione sia inserito nella presa.
2. Accendere la macchina e attendere che entri nella modalità Ready.
3. Premere tre volte **Go** entro 2 secondi. L’apparecchio stampa la pagina Impostazioni stampante attuale.

Stampa del rapporto di configurazione di rete (Per gli altri modelli)

Nota

Nome nodo: il nome del nodo viene visualizzato nel rapporto di configurazione di rete. Il nome del nodo predefinito è “BRNxxxxxxxxxxxx” per una rete cablata o “BRWxxxxxxxxxxxx” per una rete senza fili. (“xxxxxxxxxxxx” è l'indirizzo MAC o l'indirizzo Ethernet della macchina).

Il rapporto di configurazione di rete elenca la configurazione della rete corrente, comprese le impostazioni del server di stampa di rete.

Per HL-5470DW(T) e HL-6180DW(T)

1. Premere ▲ o ▼ per selezionare `Info. macchina`.
   Premere **OK**.
2. Premere ▲ o ▼ per selezionare `Stampa Imp.Rete`.
   Premere **OK**.

Per DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW e MFC-8910DW

1. Premere **Menu**.
2. (Per i modelli MFC) Premere ▲ o ▼ per selezionare `Stamp rapporto`.
   (Per i modelli DCP) Premere ▲ o ▼ per selezionare `Info. macchina`.
   Premere **OK**.
3. Premere ▲ o ▼ per selezionare `Config.Rete`.
   Premere **OK**.
4. Premere **Inizio**.

Per DCP-8250DN e MFC-8950DW(T)

1. Premere `Menu`.
2. Premere ▲ o ▼ per visualizzare `Stamp.rapporto`, quindi premere `Stamp.rapporto`.
3. Premere `Config.Rete`.
4. Premere **Inizio**.

Per HL-S7000DN

1. Premere **Menu**.
2. Premere ▲ o ▼ per selezionare `Info. macchina`.
   Premere **OK**.
3. Premere ▲ o ▼ per selezionare `Stampa Imp.Rete`.
   Premere **OK**.

Nota

Se **IP Address** nel rapporto di configurazione di rete indica **0.0.0.0**, attendere un minuto e riprovare.

Terminologia e nozioni di rete

Informazioni tecniche SSL

Secure Socket Layer (SSL) è un metodo di protezione dei dati a livello trasporto inviati sulla rete locale o ad ampio raggio utilizzando l'Internet Printing Protocol (IPP) per impedirne le lettura da parte di utenti non autorizzati.

A tale scopo si utilizzano protocolli di autenticazione sotto forma di chiavi digitali, classificabili in 2 tipologie:

- Chiave pubblica: nota a chiunque stia stampando.
- Chiave privata: nota solo all'apparecchio utilizzato per decriptare i pacchetti e renderli di nuovo leggibili dall'apparecchio stesso.

La chiave pubblica utilizza la crittografia a 1.024bit o a 2.048bit ed è contenuta all'interno di un certificato digitale. Questi certificati possono essere autofirmati o approvati da un'Autorità di certificazione (CA).

Esistono tre tipi di chiavi: private, pubbliche e condivise.

La chiave privata, nota solo all'apparecchio, è associata alla chiave pubblica ma non è contenuta all'interno del certificato digitale del client (mittente). Quando l'utente stabilisce la connessione per la prima volta, l'apparecchio invia la chiave pubblica con il certificato. Il PC client presume che la chiave pubblica provenga dall'apparecchio con il certificato. Il client genera la chiave condivisa e la codifica con la chiave pubblica, per poi inviarla all'apparecchio. L'apparecchio codifica la chiave condivisa con la chiave privata. A questo punto l'apparecchio e il client utilizzano la chiave condivisa in modo sicuro, e viene stabilita la connessione sicura per il trasferimento dei dati di stampa.

I dati di stampa vengono codificati e decodificati con la chiave condivisa.

SSL non impedisce agli utenti non autorizzati di accedere ai pacchetti, ma si limita a renderli illeggibili senza la chiave privata, che è nota soltanto all'apparecchio.

Con un'adeguata configurazione, il metodo SSL può essere configurato su reti wireless o cablate e utilizzato con altre forme di protezione come le chiavi WPA e i firewall.

Terminologia di rete

- Secure Socket Layer (SSL)

  Il protocollo di sicurezza per le comunicazioni esegue la crittografia dei dati per salvaguardarli da eventuali minacce.

- Internet Printing Protocol (IPP)

  IPP è un protocollo di stampa standard utilizzato per la gestione e l'amministrazione dei processi di stampa. Può essere utilizzato sia a livello locale che globale, per consentire a chiunque in qualsiasi angolo del mondo di stampare sullo stesso apparecchio.

- IPPS

  La versione del protocollo di stampa in base al quale Internet Printing Protocol (IPP Versione 1.0) utilizza SSL.

- HTTPS

  La versione del protocollo Internet in base al quale Hyper Text Transfer Protocol (HTTP) utilizza SSL.

- CA (Autorità di certificazione)

  Una CA è un'ente che rilascia certificati digitali (soprattutto certificati X.509) e che garantisce l'associazione tra gli elementi di dati in un certificato.

- CSR (Certificate Signing Request)

  Una CSR è un messaggio inviato da un richiedente a una CA per richiedere il rilascio di un certificato. La CSR contiene informazioni che identificano il richiedente, la chiave pubblica generata dal richiedente e la firma digitale dello stesso.

- Certificato

  Un certificato è costituito dalle informazioni che associano una chiave pubblica a un'identità. Il certificato può essere utilizzato per verificare che una chiave pubblica appartenga a un individuo. Il formato è definito dallo standard x.509.

- Sistema crittografico a chiave pubblica

  Un sistema crittografico a chiave pubblica è un ramo della moderna crittografia in cui gli algoritmi impiegano una coppia di chiavi (una chiave pubblica e una chiave privata) e utilizzano un componente diverso della coppia per i diversi passaggi dell'algoritmo.

- Sistema crittografico a chiave condivisa

  Un sistema crittografico a chiave condivisa è un ramo della crittografia in cui gli algoritmi utilizzano la stessa chiave per due diversi passaggi dell'algoritmo (ad esempio crittografia e decrittografia).