Guida alle Funzioni di Sicurezza

Informazioni importanti per la sicurezza

- La password predefinita per gestire le impostazioni di questa macchina è riportata sul fondo della macchina e contrassegnata con "**Pwd:**". È consigliabile modificare immediatamente la password predefinita per proteggere la macchina da accessi non autorizzati.
- Quando si connette la macchina a una rete esterna, come ad esempio Internet, accertarsi che l'ambiente di rete sia protetto da un firewall separato o in altro modo, per evitare fughe di informazioni dovute a impostazioni inadeguate o all'accesso non autorizzato da parte di terzi malintenzionati.
- Se è disponibile un segnale nelle vicinanze, la rete LAN wireless consente di stabilire liberamente una connessione LAN. Tuttavia, se le impostazioni di sicurezza non sono configurate correttamente, il segnale potrebbe essere intercettato da terzi malintenzionati con le seguenti conseguenze:
  - Furto dei dati personali e delle informazioni riservate
  - Trasmissione inappropriata delle informazioni a terzi che si spacciano per individui specifici
  - Divulgazione dei contenuti delle comunicazioni trascritte che vengono intercettate

Informazioni correlate

- Rete

Configurare un certificato per la protezione del dispositivo

È necessario configurare un certificato per gestire in modo sicuro una macchina di rete mediante SSL/TLS. Per configurare un certificato è necessario utilizzare la Gestione basata sul Web.

- Panoramica delle funzioni del certificato di sicurezza
- Come creare e installare un certificato
- Creare un certificato autofirmato
- Creare una richiesta di firma certificato (CSR) e installare un certificato emesso da un'autorità di certificazione (CA)
- Importare ed esportare un certificato e una chiave privata
- Importare ed esportare un certificato CA

Panoramica delle funzioni del certificato di sicurezza

La macchina consente di utilizzare più certificati di sicurezza; questa caratteristica permette l'autenticazione e la comunicazione sicura con la macchina. Con la macchina è possibile utilizzare le seguenti funzionalità dei certificati di sicurezza:

Le funzioni, le opzioni e le impostazioni supportate potrebbero variare a seconda del modello.

- Comunicazione SSL/TLS
- Autenticazione IEEE 802.1x
- IPsec

La macchina supporta quanto segue:

- Certificato preinstallato

  Sull'apparecchio è preinstallato un certificato autofirmato. Questo certificato consente di utilizzare la comunicazione SSL/TLS senza che sia necessario creare o installare un certificato differente.

Il certificato autofirmato preinstallato protegge la comunicazione fino a un certo livello. Per una maggiore sicurezza è consigliabile utilizzare un certificato emesso da un'organizzazione affidabile.

- Certificato autofirmato

  Il server di stampa emette il proprio certificato. Se si usa questo certificato, è possibile utilizzare la comunicazione SSL/TLS senza che sia necessario creare o installare un certificato differente emesso da una CA.
- Certificato emesso da un'autorità di certificazione (CA)

  Per installare un certificato emesso da un'autorità di certificazione (CA) sono disponibili due metodi. 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 richiesta CSR (Certificates Signing Request) da questo server di stampa.
  - Quando si importa un certificato e una chiave privata.
- Certificato di un'Autorità di certificazione (CA)

  Per utilizzare un certificato CA che identifica l'autorità di certificazione e che possiede una sua chiave privata, è necessario importare tale certificato CA dall'autorità di certificazione stessa prima di configurare le funzioni di sicurezza di rete.

- Se si intende utilizzare le comunicazione SSL/TLS, è consigliabile rivolgersi innanzitutto all'amministratore di sistema.
- Quando si ripristinano le impostazioni 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 avere ripristinato le impostazioni del server di stampa, esportarli prima del ripristino e quindi reinstallarli.

Informazioni correlate

- Configurare un certificato per la protezione del dispositivo

Argomenti correlati:

- Configurare l'autenticazione IEEE 802.1x per la rete mediante Gestione basata sul Web (Browser Web)

Come creare e installare un certificato

Sono disponibili due opzioni per la scelta di un certificato di sicurezza: utilizzare un certificato autofirmato o utilizzare un certificato da un'autorità di certificazione (CA).

Opzione 1

Certificato autofirmato

1. Creare un certificato autofirmato utilizzando Gestione basata sul Web.
2. Installare il certificato autofirmato sul computer.

Opzione 2

Certificato di una CA

1. Creare una richiesta di firma certificato (CSR) utilizzando Gestione basata sul Web.
2. Installare il certificato emesso dalla CA sulla macchina Brother mediante Gestione basata sul Web.
3. Installare il certificato sul computer.

Informazioni correlate

- Configurare un certificato per la protezione del dispositivo

Creare un certificato autofirmato

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

> La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato**.

> Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ≡.

5. Fare clic su **Crea certificato autofirmato**.
6. Immettere **Nome comune** e **Data valida**.
   - La lunghezza di **Nome comune** deve essere inferiore a 64 byte. Immettere un identificatore, ad esempio un indirizzo IP, un nome nodo o un nome 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.
7. Selezionare l'impostazione dall'elenco a discesa **Algoritmo a chiave pubblica**.
8. Selezionare l'impostazione dall'elenco a discesa **Algoritmo di Digest**.
9. Fare clic su **Invia**.

Informazioni correlate

- Configurare un certificato per la protezione del dispositivo

Creare una richiesta di firma certificato (CSR) e installare un certificato emesso da un'autorità di certificazione (CA)

Se si dispone già di un certificato emesso da un'autorità di certificazione (CA) affidabile, è possibile archiviare il certificato e la chiave privata sulla macchina e gestirla con le procedure di importazione ed esportazione. Se non si dispone di un certificato da una CA esterna affidabile, creare una richiesta di firma certificato (CSR), inviarla a una CA per l'autenticazione e installare il certificato restituito sulla macchina.

- Creare una richiesta di firma certificato (CSR)
- Installare un certificato nella macchina

Creare una richiesta di firma certificato (CSR)

Una richiesta di firma certificato (CSR) è una richiesta inviata a un'autorità di certificazione (CA) per autenticare le credenziali contenute all'interno del certificato.

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

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato**.

Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.

5. Fare clic su **Crea CSR**.
6. Digitare un **Nome comune** (obbligatorio) e aggiungere altre informazioni su **Organizzazione** (opzionale).

- Perché la CA possa confermare l'identità e attestarla a terzi, sono necessari i dettagli dell'azienda.
- La lunghezza di **Nome comune** deve essere inferiore a 64 byte. Immettere un identificatore, ad esempio un indirizzo IP, un nome nodo o un nome 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.
- Verrà visualizzato un avviso se si digita un nome diverso nell'URL rispetto al nome comune utilizzato per il certificato.
- La lunghezza di **Organizzazione**, **Unità organizzativa**, **Città** e **Provincia** deve essere inferiore a 64 byte.
- **Paese/Regione** deve essere un codice paese ISO 3166 di 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**.

7. Selezionare la macchina dall'elenco a discesa **Algoritmo a chiave pubblica**.
8. Selezionare la macchina dall'elenco a discesa **Algoritmo di Digest**.
9. Fare clic su **Invia**.

   La CSR viene visualizzata sullo schermo. Salvare la CSR come file o copiarlo e incollarlo su un modulo CSR online oferto da un'autorità di certificazione.
10. Fare clic su **Salva**.

- Attenersi alla politica della CA per il metodo con cui inviare una CSR alla CA.
- Se si utilizza Enterprise Root CA di Windows Server, è consigliabile utilizzare il Server Web per il modello di certificato per creare il certificato client in sicurezza. Se si crea un certificato client per un ambiente IEEE 802.1x con l'autenticazione EAP-TLS, si consiglia di utilizzare il modello di certificato Utente.

Informazioni correlate

- Creare una richiesta di firma certificato (CSR) e installare un certificato emesso da un'autorità di certificazione (CA)

Installare un certificato nella macchina

Quando si riceve un certificato da una Autorità di certificazione (CA), eseguire le seguenti procedure per installarlo nel server di stampa:

> È possibile installare nella macchina solo un certificato emesso con la richiesta di firma del certificato (CSR) della macchina. Se si desidera creare un'altra CSR, assicurarsi che il certificato sia installato prima di creare la nuova CSR. Creare un'altra CSR solo dopo aver installato il certificato nella macchina, altrimenti la CSR creata prima dell'installazione non sarà più valida.

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

> La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato**.

> Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.

5. Fare clic su **Installa certificato**.
6. Cercare il file contenente il certificato emesso dalla CA e fare clic su **Invia**.

   Il certificato viene creato e salvato nella memoria della macchina.

Per utilizzare la comunicazione SSL/TLS, è necessario installare il certificato principale della CA nel computer. Rivolgersi all'amministratore di rete.

Informazioni correlate

- Creare una richiesta di firma certificato (CSR) e installare un certificato emesso da un'autorità di certificazione (CA)

Importare ed esportare un certificato e una chiave privata

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

- Importare un certificato e la chiave privata
- Esportare il certificato e la chiave privata

Importare un certificato e la chiave privata

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

> La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato**.

> Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.

5. Fare clic su **Importa certificato e chiave privata**.
6. Individuare e selezionare il file da importare.
7. Digitare la password se il file è crittografato e fare clic su **Invia**.

Il certificato e la chiave privata sono stati importati nella macchina.

Informazioni correlate

- Importare ed esportare un certificato e una chiave privata

Esportare il certificato e la chiave privata

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

> La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato**.

> Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.

5. Fare clic su **Esporta** mostrato con il **Elenco certificati**.
6. Immettere la password se si desidera crittografare il file.

   Se il campo della password viene lasciato in bianco, l'output non viene crittografato.
7. Immettere di nuovo la password per confermare e fare clic su **Invia**.
8. Fare clic su **Salva**.

Il certificato e la chiave privata sono stati esportati correttamente nel computer.

È anche possibile importare il certificato sul computer.

Informazioni correlate

- Importare ed esportare un certificato e una chiave privata

Importare ed esportare un certificato CA

È possibile importare, esportare e memorizzare i certificati CA nella macchina Brother.

- Importare un certificato CA
- Esportare un certificato CA

Importare un certificato CA

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato CA**.

Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ≡.

5. Fare clic su **Importa certificato CA**.
6. Cercare il file da importare.
7. Fare clic su **Invia**.

Informazioni correlate

- Importare ed esportare un certificato CA

Esportare un certificato CA

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

> La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato CA**.

> Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ≡.

5. Selezionare il certificato da esportare e fare clic su **Esporta**.
6. Fare clic su **Invia**.

Informazioni correlate

- Importare ed esportare un certificato CA

Utilizzare SSL/TLS

- Gestire in modo sicuro l’apparecchio di rete mediante SSL/TLS
- Stampa dei documenti in modo sicuro utilizzando SSL/TLS
- Inviare o ricevere in modo sicuro un messaggio e-mail utilizzando SSL/TLS

Gestire in modo sicuro l’apparecchio di rete mediante SSL/TLS

- Configurare un certificato per SSL/TLS e i protocolli disponibili
- Accedere a Gestione basata sul Web mediante SSL/TLS
- Installare il certificato autofirmato per gli utenti Windows come Amministratore
- Configurare un certificato per la protezione del dispositivo

Configurare un certificato per SSL/TLS e i protocolli disponibili

Prima di usare la comunicazione SSL/TLS è necessario configurare un certificato sulla macchina mediante Gestione basata sul Web.

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

   La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.
4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Rete** > **Protocollo**.

   Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.
5. Fare clic su **Impostazioni Server HTTP**.
6. Selezionare il certificato che si vuole configurare dall'elenco a discesa **Selezionare il certificato**.
7. Fare clic su **Invia**.
8. Fare clic su **SI** per riavviare il server di stampa.

Informazioni correlate

- Gestire in modo sicuro l'apparecchio di rete mediante SSL/TLS

Argomenti correlati:

- Stampa dei documenti in modo sicuro utilizzando SSL/TLS

Accedere a Gestione basata sul Web mediante SSL/TLS

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

- Per utilizzare il protocollo HTTPS, occorre attivare HTTPS sulla macchina. Il protocollo HTTPS è abilitato per impostazione predefinita.
- È possibile modificare le impostazioni del protocollo HTTPS utilizzando la schermata Gestione basata sul Web.

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. È ora possibile accedere alla macchina con HTTPS.

Informazioni correlate

- Gestire in modo sicuro l'apparecchio di rete mediante SSL/TLS

Installare il certificato autofirmato per gli utenti Windows come Amministratore

- I passaggi seguenti si riferiscono a Microsoft Edge. Se si utilizza un browser web diverso, consultare la documentazione o la guida online del browser web per le istruzioni di installazione dei certificati.
- Verificare che il certificato autofirmato sia stato creato mediante Gestione basata sul Web.

1. Fare clic con il pulsante destro del mouse sull'icona **Microsoft Edge**, quindi fare clic su **Esegui come amministratore**.

   Se viene visualizzata la schermata **Controllo dell'account utente**, fare clic su **Sì**.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se la connessione non è privata, fare clic sul pulsante **Avanzato**, quindi accedere alla pagina web.
4. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

   La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.
5. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Protezione** > **Certificato**.

   Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ≡.
6. Fare clic su **Esporta**.
7. Per crittografare il file di output, immettere una password nel campo **Immetti password**. Se il campo **Immetti password** è vuoto, il file di output non sarà crittografato.
8. Digitare di nuovo la password nel campo **Ridigita password** e fare clic su **Invia**.
9. Fare clic sul file scaricato per aprirlo.
10. Quando viene visualizzato **Importazione guidata certificati**, fare clic su **Avanti**.
11. Fare clic su **Avanti**.
12. Se necessario, immettere una password, quindi fare clic su **Avanti**.
13. Selezionare **Colloca tutti i certificati nel seguente archivio** e quindi fare clic su **Sfoglia...**.
14. Selezionare **Autorità di certificazione radice attendibili**, quindi fare clic su **OK**.
15. Fare clic su **Avanti**.
16. Fare clic su **Fine**.
17. Fare clic su **Sì**, se l'identificazione personale è corretta.
18. Fare clic su **OK**.

Informazioni correlate

- Gestire in modo sicuro l'apparecchio di rete mediante SSL/TLS

Stampa dei documenti in modo sicuro utilizzando SSL/TLS

- Stampare i documenti mediante IPPS
- Configurare un certificato per SSL/TLS e i protocolli disponibili
- Configurare un certificato per la protezione del dispositivo

Stampare i documenti mediante IPPS

Per stampare i documenti in modo sicuro con il protocollo IPP, utilizzare il protocollo IPPS.

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

   La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.
4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Rete** > **Protocollo**.

   Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.
5. Controllare che la casella di controllo **IPP** sia selezionata.

   Se la casella di controllo **IPP**non è selezionata, selezionare la casella di controllo **IPP** e fare clic su **Invia**.

   Riavviare la macchina per attivare la configurazione.

   Dopo il riavvio della macchina, tornare alla pagina web della macchina, digitare la password e nella barra di spostamento di sinistra fare clic su **Rete** > **Rete** > **Protocollo**.
6. Fare clic su **Impostazioni Server HTTP**.
7. Selezionare la casella di controllo **HTTPS** nell'area **IPP**, quindi fare clic su **Invia**.
8. Riavviare la macchina per attivare la configurazione.

La comunicazione tramite IPPS non può impedire l'accesso non autorizzato al server di stampa.

Informazioni correlate

- Stampa dei documenti in modo sicuro utilizzando SSL/TLS

Utilizzare SNMPv3

- Gestione sicura della macchina in rete tramite SNMPv3

Gestione sicura della macchina in rete tramite SNMPv3

Il protocollo SNMPv3 (Simple Network Management Protocol versione 3) fornisce le funzioni di autenticazione utente e crittografia dei dati per gestire i dispositivi di rete in modo sicuro.

1. Avviare il browser Web.
2. Digitare “https://Nome comune” nella barra degli indirizzi del browser (dove “Nome comune” è il nome comune assegnato al certificato; può essere l’indirizzo IP, il nome del nodo o il nome di dominio).
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete** > **Rete** > **Protocollo**.

Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.

5. Verificare che l’impostazione **SNMP** sia attivata, quindi fare clic su **Impostazioni avanzate**.
6. Configurare le impostazioni della modalità SNMPv1/v2c.

Opzione	Descrizione
SNMP v1/v2c accesso lettura-scrittura	Il server di stampa utilizza la versione 1 e la versione 2c del protocollo SNMP. È possibile utilizzare tutte le applicazioni della macchina in questa modalità. Tuttavia, la modalità non è sicura finché l’utente non viene autenticato e i dati non vengono crittografati.
Accesso sola lettura SNMP v1/v2c	Il server di stampa utilizza l’accesso in sola lettura della versione 1 e la versione 2c del protocollo SNMP.
Disattivato	Disattivare la versione 1 e la versione 2c del protocollo SNMP. Tutte le applicazioni che utilizzando SNMPv1/v2c saranno limitate. Per consentire l'uso delle applicazioni SNMPv1/v2c, utilizzare la modalità **Accesso sola lettura SNMP v1/v2c** o **SNMP v1/v2c accesso lettura-scrittura**.

7. Configurare le impostazioni della modalità SNMPv3.

Opzione	Descrizione
Attivata	Il server di stampa utilizza la versione 3 del protocollo SNMP. Per gestire il server di stampa in modo sicuro, utilizzare la modalità SNMPv3, quindi configurare le impostazioni.
Disattivato	Disattivare la versione 3 del protocollo SNMP. Tutte le applicazioni che utilizzando SNMPv3 saranno limitate. Per consentire l'uso delle applicazioni SNMPv3, utilizzare la modalità SNMPv3.

8. Fare clic su **Invia**.

Se la macchina visualizza le opzioni di impostazione del protocollo, selezionare le opzioni desiderate.

9. Riavviare la macchina per attivare la configurazione.

Informazioni correlate

- Utilizzare SNMPv3

Utilizzare l'autenticazione IEEE 802.1x per la rete

- Cos’è l’autenticazione IEEE 802.1x?
- Configurare l'autenticazione IEEE 802.1x per la rete mediante Gestione basata sul Web (Browser Web)
- Metodi di autenticazione IEEE 802.1x

Cos'è l'autenticazione IEEE 802.1x?

IEEE 802.1x è uno standard IEEE che impedisce l'accesso da parte di dispositivi di rete non autorizzati. La macchina Brother invia una richiesta di autenticazione a un server RADIUS (server di autenticazione) attraverso il punto di accesso o hub. Dopo che la richiesta è stata verificata dal server RADIUS, la macchina ottiene l'accesso alla rete.

Informazioni correlate

- Utilizzare l'autenticazione IEEE 802.1x per la rete

Configurare l'autenticazione IEEE 802.1x per la rete mediante Gestione basata sul Web (Browser Web)

- Se si configura la macchina utilizzando l'autenticazione EAP-TLS, è necessario installare il certificato per client emesso da un'autorità di certificazione (CA) prima di iniziare la configurazione. Per informazioni relative al certificato per client, rivolgersi all'amministratore di rete. Se è stato installato più di un certificato, è consigliabile annotare il nome del certificato che si intende utilizzare.
- Prima di poter verificare il certificato del server, è necessario importare il certificato CA emesso dall'autorità di certificazione che ha firmato il certificato del server. Rivolgersi all'amministratore di rete o al fornitore di servizi Internet (ISP) per verificare se è necessario importare un certificato CA.

È possibile configurare l'autenticazione IEEE 802.1x anche mediante la configurazione guidata wireless dal pannello dei comandi (rete wireless).

1. Avviare il browser Web.
2. Digitare "https://indirizzo IP della macchina" nella barra degli indirizzi del browser (dove "indirizzo IP della macchina" è l'indirizzo IP della macchina in uso).

   Ad esempio:

   https://192.168.1.2

   L'indirizzo IP della macchina è indicato nel rapporto di configurazione della rete.
3. Se richiesto, digitare la password nel campo **Accesso**, quindi fare clic su **Accesso**.

La password predefinita per gestire le impostazioni di questa macchina è riportata sul retro o sulla base della macchina e contrassegnata con "**Pwd**". Modificare la password predefinita seguendo le istruzioni a schermo quando si accede per la prima volta.

4. Nella barra di spostamento di sinistra, fare clic su **Rete**.

Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ≡.

5. Effettuare una delle seguenti operazioni:
   - Per la rete cablata

     Fare clic su **Cablata** > **autenticazione 802.1x**.
   - Per la rete wireless

     Fare clic su **Wireless** > **Wireless (Aziendale)**.
6. Configurare le impostazioni di autenticazione IEEE 802.1x.

- Per abilitare l'autenticazione IEEE 802.1x per le reti cablate, selezionare **Attivata** per **Stato 802.1x cablato** nella pagina **autenticazione 802.1x**.
- Se si utilizza l'autenticazione **EAP-TLS** è necessario selezionare il certificato client installato (indicato dal nome del certificato) per la verifica dall'elenco a discesa **Certificato client**.
- Selezionando l'autenticazione **EAP-FAST**, **PEAP**, **EAP-TTLS** o **EAP-TLS**, scegliere il metodo di verifica dall'elenco a discesa **Verifica certificato server**. Verificare il certificato del server utilizzando il certificato CA importato in precedenza nella macchina ed emesso dalla CA che ha firmato il certificato del server.

Scegliere uno dei seguenti metodi di verifica dall'elenco a discesa **Verifica certificato server**:

Opzione	Descrizione
Nessuna verifica	Il certificato del server è essere attendibile. La verifica non viene eseguita.

Opzione	Descrizione
Cert. CA	Il metodo di verifica per controllare l'affidabilità della CA del certificato del server, utilizzando il certificato CA emesso dalla CA che ha firmato il certificato del server.
Cert. CA + ID server	Il metodo di verifica per controllare il valore del nome comune [1] del certificato del server, oltre che l'affidabilità della CA del certificato del server.

7. Al termine della configurazione, fare clic su **Invia**.

   Per le reti cablate: dopo la configurazione, connettere la macchina alla rete con supporto IEEE 802.1x. Dopo qualche minuto, stampare il rapporto di configurazione di rete per verificare lo stato <**Wired IEEE 802.1x**>.

Opzione	Descrizione
Success	La funzione IEEE 802.1x cablata è abilitata e l'autenticazione è riuscita.
Failed	La funzione IEEE 802.1x cablata è abilitata, ma l'autenticazione non è riuscita.
Off	La funzione IEEE 802.1x cablata non è disponibile.

Informazioni correlate

- Utilizzare l'autenticazione IEEE 802.1x per la rete

Argomenti correlati:

- Panoramica delle funzioni del certificato di sicurezza
- Configurare un certificato per la protezione del dispositivo

1 La verifica del nome comune confronta il nome comune del certificato del server con la stringa di caratteri configurata per il **ID server**. Prima di utilizzare questo metodo, contattare l'amministratore del sistema per conoscere il nome comune del certificato del server, quindi configurare il valore **ID server**.

Metodi di autenticazione IEEE 802.1x

EAP-FAST

EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secured Tunnelling) è stato sviluppato da Cisco Systems, Inc. che utilizza un ID utente e una password per eseguire l'autenticazione, e algoritmi a chiave simmetrica per effettuare il processo di autenticazione con il tunnel.

La macchina Brother supporta i seguenti metodi di autenticazione interna:

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

EAP-MD5 (rete cablata)

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) utilizza un ID utente e una password per l'autenticazione In attesa/Risposta.

PEAP

Il protocollo PEAP (Protected Extensible Authentication Protocol) è una versione del metodo EAP sviluppata da Cisco Systems, Inc., Microsoft Corporation e RSA Security. PEAP crea un tunnel SSL (Secure Sockets Layer)/TLS (Transport Layer Security) crittografato tra un client e un server di autenticazione per l'invio di un ID utente e di una password. PEAP consente l'autenticazione reciproca tra server e client.

La macchina Brother supporta i seguenti metodi di autenticazione interna:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) è stato sviluppato da Funk Software e Certicom. Analogamente a PEAP, EAP-TTLS crea un tunnel SSL crittografato tra un client e un server di autenticazione, per l'invio di un ID utente e di una password. EAP-TTLS consente l'autenticazione reciproca tra server e client.

La macchina Brother supporta i seguenti metodi di autenticazione interna:

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

EAP-TLS

EAP-TLS (Extensible Authentication Protocol Transport Layer Security) richiede l'autenticazione mediante certificato digitale sia sul client sia sul server di autenticazione.

Informazioni correlate

- Utilizzare l'autenticazione IEEE 802.1x per la rete