Guida alle Funzioni di Sicurezza

Sommario

Introduzione

Definizioni delle note

Nella presente Guida dell'utente vengono utilizzati i seguenti simboli e convenzioni:

IMPORTANTE	IMPORTANTE indica una situazione potenzialmente pericolosa che, se non evitata, può causare danni alle cose o la perdita di funzionalità del prodotto.
NOTA	NOTA specifica l'ambiente operativo, le condizioni di installazione o speciali condizioni di utilizzo.
	Le icone dei suggerimenti segnalano suggerimenti utili e informazioni aggiuntive.
Grassetto	Lo stile grassetto identifica i pulsanti sul pannello dei comandi dell'apparecchio o nella schermata del computer.
Corsivo	Lo stile Italicized emphasizes un punto importante o rimanda a un argomento correlato.

Informazioni correlate

- Introduzione

Marchi

Adobe® e Reader® sono marchi o marchi registrati di Adobe Systems Incorporated negli Stati Uniti e/o in altri Paesi.

Ciascuna società il cui software è indicato nel presente manuale detiene un Contratto di License software specifico per i propri programmi proprietari.

Tutti i nomi commerciali e dei prodotti delle aziende citati nei prodotti Brother, i relativi documenti e qualsiasi altro materiale sono marchi o marchi registrati delle rispettive aziende.

Informazioni correlate

- Introduzione

Copyright

Informazioni correlate

- Introduzione

Prima di utilizzare le funzioni di sicurezza di rete

La macchina integra alcuni dei più recenti protocolli di sicurezza di rete e di crittografia attualmente disponibili. Queste funzioni di rete possono essere incluse nel piano generale di protezione della rete al fine di proteggere i dati e impedire l'accesso unauthorized alla macchina.

È consigliabile disattivare i protocolli FTP e TFTP. L'accesso alla macchina tramite questi protocolli non è protetto.

Informazioni correlate

- Introduzione
  - Disattivare i protocolli non necessari

Disattivare i protocolli non necessari

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. Deselezionare le caselle di controllo dei protocolli non necessari per disattivarle.
6. Fare clic su **Invia**.
7. Riavviare la macchina Brother per attivare la configurazione.

Informazioni correlate

- Prima di utilizzare le funzioni di sicurezza di rete

Sicurezza di rete

- Configurare un certificato per la protezione del dispositivo
- Utilizzare SSL/TLS
- Utilizzare SNMPv3
- Utilizzare IPsec
- Utilizzare l'autenticazione IEEE 802.1x per la 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 organization 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(Porta 443)** 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 unauthorized 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 sicurezza, utilizzare la modalità SNMPv3.
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 IPsec

Introduzione a IPsec

IPsec (Internet Protocol Security) è un protocollo di sicurezza che utilizza una funzione di protocollo Internet opzionale per impedire la manipolazione dei dati e garantire la riservatezza dei trasmessi come pacchetti IP. IPsec crittografa i dati trasmessi in rete, come i dati di stampa inviati dai computer a una stampante. Poiché i dati vengono crittografati a livello di rete, le applicazioni che utilizzano un protocollo di livello superiore sfruttano IPsec anche se l'utente non è a conoscenza del suo uso.

IPsec supporta le seguenti funzioni:

- Trasmissioni IPsec

  A seconda delle condizioni di impostazione IPsec, un computer connesso alla rete invia e riceve i dati da un dispositivo specificato mediante IPsec. Quando i dispositivi iniziano a comunicare tramite IPsec, si scambiano dapprima le chiavi utilizzando il sistema IKE (Internet Key Exchange), quindi i dati crittografati vengono trasmessi mediante le chiavi.

  Inoltre IPsec ha due modalità operative: la modalità Trasporto e la modalità Tunnel. La modalità Trasporto è utilizzata prevalentemente per la comunicazione tra dispositivi, mentre la modalità Tunnel è utilizzata in ambienti come i VPN (Virtual Private Network, reti private virtuali).

Per trasmissioni IPsec sono necessarie le seguenti condizioni:

- un computer in grado di comunicare utilizzando IPsec deve essere connesso alla rete.
- La macchina è configurata per la comunicazione IPsec.
- Il computer connesso alla macchina è configurato per le connessioni IPsec.

- Impostazioni IPsec

  Le impostazioni necessarie per le connessioni utilizzando IPsec. Queste impostazioni possono essere configurate utilizzando Gestione basata sul Web.

Per configurare le impostazioni IPsec, è necessario utilizzare il browser su un computer connesso alla rete.

Informazioni correlate

- Utilizzare IPsec

Configurare IPsec utilizzando Gestione basata sul Web

Le condizioni di connessione IPsec comprendono due **Modello** tipi: **Indirizzo** e **IPsec**. È possibile configurare fino a un massimo di 10 condizioni di connessione.

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** > **IPsec**.

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

5. Configurare le impostazioni.

Opzione	Descrizione
Stato	Abilitare o disabilitare IPsec.
Modalità di negoziazione	Selezionare **Modalità di negoziazione** per la fase 1 di IKE. IKE è un protocollo utilizzato per lo scambio di chiavi di crittografia per attuare una comunicazione crittografata con IPsec. In modalità **Principale**, la velocità di elaborazione è bassa, ma il livello di sicurezza è alto. Nella modalità **Aggressiva**, la velocità di elaborazione è maggiore rispetto alla modalità **Principale**, ma la sicurezza è inferiore.
Tutto il traffico non IPsec	Selezionare l'azione da eseguire per i pacchetti non IPsec. Se si usano i servizi Web, bisogna selezionare **Consenti** per **Tutto il traffico non IPsec**. Se si seleziona **Abbandona**, i servizi Web non possono essere utilizzati.
Bypass broadcast/multicast	Selezionare **Attivata** o **Disattivato**.
Bypass protocollo	Selezionare le caselle di controllo per l'opzione o le opzioni che si desiderano.
Regole	Selezionare la casella di controllo **Attivata** per attivare il modello. Quando si selezionano più caselle di controllo, in caso di conflitto tra le caselle di controllo selezionate viene data priorità alle caselle con i numeri minori. Fare clic sul corrispondente elenco a discesa per selezionare l'**Modello indirizzo** utilizzato per le condizioni di connessione IPsec. Per aggiungere un **Modello indirizzo**, fare clic su **Aggiungi modello**. Fare clic sul corrispondente elenco a discesa per selezionare l'**Modello IPsec** utilizzato per le condizioni di connessione IPsec. Per aggiungere un **Modello IPsec**, fare clic su **Aggiungi modello**.

6. Fare clic su **Invia**.

   Se è necessario riavviare la macchina per attivare le nuove impostazioni, viene visualizzata la schermata di conferma del riavvio.

Se il modello attivato nella tabella **Regole** contiene un elemento vuoto, verrà visualizzato un messaggio di errore. Confermare le scelte e fare clic nuovamente su **Invia**.

Informazioni correlate

- Utilizzare IPsec

Argomenti correlati:

- Configurare un certificato per la protezione del dispositivo

Configurare un modello Indirizzo IPsec utilizzando 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** > **Protezione** > **Modello indirizzo IPsec**.

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

5. Fare clic sul pulsante **Elimina** per eliminare un **Modello indirizzo**. Se un **Modello indirizzo** è in uso, non può essere eliminato.
6. Fare clic sul **Modello indirizzo** che si desidera creare. Viene visualizzato **Modello indirizzo IPsec**.
7. Configurare le impostazioni.

Opzione	Descrizione
Nome modello	Immettere un nome per il modello (massimo 16 caratteri).
Indirizzo IP locale	• **Indirizzo IP** Specificare l'indirizzo IP. Selezionare **Tutti gli indirizzi IPv4**, **Tutti gli indirizzi IPv6**, **Tutti gli indirizzi IPv6 locali**, o **Personalizzato** dall'elenco a discesa. Se si seleziona **Personalizzato** dall'elenco a discesa, immettere l'indirizzo IP (IPv4 o IPv6) nella casella di testo. • **Intervallo indirizzi IP** Nella casella di testo, immettere l'indirizzo IP iniziale e l'indirizzo IP finale dell'intervallo di indirizzi IP desiderato. Può verificarsi un errore se l'indirizzo IP iniziale e l'indirizzo IP finale non standardized agli standard IPv4 o IPv6 o se l'indirizzo IP finale è più piccolo di quello iniziale. • **Indirizzo IP / Prefisso** Specificare l'indirizzo IP utilizzando la notazione CIDR. Ad esempio: 192.168.1.1/24 Dato che il prefisso è specificato sotto forma di maschera di sottorete a 24 bit (255.255.255.0) per 192.168.1.1, gli indirizzi 192.168.1.### sono validi.
Indirizzo IP remoto	• **Qualsiasi** Se si seleziona **Qualsiasi**, tutti gli indirizzi IP sono attivati. • **Indirizzo IP** Digitare l'indirizzo IP specificato (IPv4 o IPv6) nella casella di testo. • **Intervallo indirizzi IP** Digitare il primo e l'ultimo indirizzo IP per l'intervallo di indirizzi IP. Può verificarsi un errore se il primo e l'ultimo indirizzo IP non

Opzione	Descrizione
	standardized agli standard IPv4 o IPv6 o se l'ultimo indirizzo IP è più piccolo del primo. • **Indirizzo IP / Prefisso** Specificare l'indirizzo IP utilizzando la notazione CIDR. Ad esempio: 192.168.1.1/24 Dato che il prefisso è specificato sotto forma di maschera di sottorete a 24 bit (255.255.255.0) per 192.168.1.1, gli indirizzi 192.168.1.### sono validi.

8. Fare clic su **Invia**.

Quando si modificano le impostazioni per il modello attualmente in uso, riavviare la macchina per attivare la configurazione.

Informazioni correlate

- Utilizzare IPsec

Configurare un modello IPsec utilizzando 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** > **Protezione** > **Modello IPsec**.

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

5. Fare clic sul pulsante **Elimina** per eliminare un **Modello IPsec**. Se un **Modello IPsec** è in uso, non può essere eliminato.
6. Fare clic sul **Modello IPsec** che si desidera creare. Viene visualizzata la schermata **Modello IPsec**. I campi per la configurazione differiscono in base alle impostazioni **Usa modello preimpostato** e **Scambio chiavi Internet (IKE)** selezionate.
7. Nel campo **Nome modello**, immettere un nome per il modello (fino a 16 caratteri).
8. Se è stato selezionato **Personalizzato** nell'elenco a discesa **Usa modello preimpostato**, selezionare le opzioni **Scambio chiavi Internet (IKE)** e modificare le impostazioni, se necessario.
9. Fare clic su **Invia**.

Informazioni correlate

- Utilizzare IPsec
  - Impostazioni IKEv1 per un modello IPsec
  - Impostazioni IKEv2 per un modello IPsec
  - Impostazioni manuali per il modello IPsec

Impostazioni IKEv1 per un modello IPsec

Opzione	Descrizione
Nome modello	Immettere un nome per il modello (massimo 16 caratteri).
Usa modello preimpostato	Selezionare **Personalizzato**, **Sicurezza elevata IKEv1** o **Sicurezza media IKEv1**. Gli elementi da impostare sono diversi a seconda del modello selezionato.
Scambio chiavi Internet (IKE)	IKE è un protocollo di comunicazione utilizzato per lo scambio di chiavi di crittografia per attuare una comunicazione crittografata con IPsec. Per attuare una comunicazione crittografata solo per una volta, l'algoritmo di crittografia necessario per IPsec è determinato e le chiavi di crittografia sono condivise. Per IKE, le chiavi di crittografia vengono scambiate utilizzando il metodo di scambio delle chiavi Diffie-Hellman, e la comunicazione crittografata limitata a IKE viene eseguita. Se è stato selezionato **Personalizzato** in **Usa modello preimpostato**, selezionare **IKEv1**.
Tipo di autenticazione	• **Gruppo Diffie-Hellman** Questo metodo di scambio chiavi consente di scambiare in modo sicuro chiavi segrete in una rete non protetta. Il metodo di scambio chiavi Diffie-Hellman utilizza un problema con un logaritmo discreto, e non la chiave segreta, per inviare e ricevere informazioni aperte generate utilizzando un numero casuale e la chiave segreta. Selezionare **Gruppo 1**, **Gruppo 2**, **Gruppo 5** o **Gruppo 14**. • **Crittografia** Selezionare **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. • **Hash** Selezionare **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. • **Durata associazione di protezione** Specificare la durata di associazione protezione di IKE. Immettere il tempo (secondi) e il numero di kilobyte (KB).
Sicurezza/Incapsulamento	• **Protocollo** Selezionare **ESP**, **AH** o **AH+ESP**. - ESP è un protocollo per attuare comunicazioni crittografate utilizzando IPsec. ESP esegue la crittografia sul carico utile (i contenuti comunicati) e aggiunge delle altre informazioni. Il pacchetto IP comprende l'intestazione e il carico crittografato, che segue l'intestazione. Oltre ai dati crittografati, il pacchetto IP include anche informazioni riguardanti il metodo di crittografia e la chiave di crittografia, i dati di autenticazione e altre informazioni. - AH è una parte del protocollo IPsec che autentica il mittente ed evita la manipolazione (assicura la completezza) dei dati. Nel pacchetto IP, i dati sono inseriti immediatamente dopo l'intestazione. Inoltre, i pacchetti includono valori cancelletto, calcolati utilizzando un'equazione dai contenuti comunicati, dalla chiave segreta e così via, al fine di evitare la falsificazione del mittente e la manipolazione dei dati. A differenza di ESP, i contenuti comunicati non sono crittografati, e i dati sono inviati e ricevuti come formato solo testo. • **Crittografia (Non disponibile per l'opzione AH.)** Selezionare **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**.

Opzione	Descrizione
	• **Hash** Selezionare **Nessuno**, **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. **Nessuno** può essere selezionato solo quando è selezionato **ESP** per **Protocollo**. • **Durata associazione di protezione** Specificare la durata del SA IKE. Digitare il tempo (secondi) e il numero di kilobyte (KByte). • **Modalità di incapsulamento** Selezionare **Trasporto** o **Tunnel**. • **Indirizzo IP router remoto** Digitare l'indirizzo IP (IPv4 o IPv6) del router remoto. Inserire l'informazione solo quando è selezionata la modalità **Tunnel**. SA (Security Association) è un metodo di comunicazione crittografata utilizzando IPsec o IPv6 che permette lo scambio e la condivisione di informazioni, come il metodo e la chiave di crittografia, al fine di stabilire un canale di comunicazione sicuro prima dell'inizio della comunicazione. SA può inoltre riferirsi a un canale di comunicazione crittografata virtuale stabilito. Il SA utilizzato per IPsec stabilisce un metodo di crittografia, scambia le chiavi ed esegue un'autenticazione reciproca sulla base della procedura standard IKE (Internet Key Exchange, scambio chiavi internet). Inoltre, il SA viene periodicamente aggiornato.
Perfect Forward Secrecy (PFS)	PFS non trae le chiavi da chiavi usate in precedenza per crittografare i messaggi. Inoltre, se per crittografia di un messaggio si utilizza una chiave derivata da una chiave di livello superiore, la chiave di livello superiore non verrà utilizzata per generare altre chiavi. Inoltre, anche se una chiave viene compromessa, il danno sarà limitato solo ai messaggi crittografati utilizzando quella chiave. Selezionare **Attivata** o **Disattivato**.
Metodo di autenticazione	Selezionare il metodo di autenticazione. Selezionare **Chiave precondivisa** o **Certificati**.
Chiave precondivisa	Quando si applica la crittografia alla comunicazione, la chiave di crittografia viene scambiata e condivisa prima dell'operazione, utilizzando un altro canale. Se è stato selezionato **Chiave precondivisa** per **Metodo di autenticazione**, digitare la **Chiave precondivisa** (fino a 32 caratteri). • **Locale/Tipo di/ID** Selezionare il tipo di ID del mittente, quindi digitare l'ID. Selezionare **Indirizzo IPv4**, **Indirizzo IPv6**, **FQDN**, **Indirizzo e-mail**, o **Certificato** per il tipo. Se viene selezionato **Certificato**, digitare il nome comune del certificato nel campo **ID**. • **Remoto/Tipo di/ID** Selezionare il tipo di ID del destinatario, quindi digitare l'ID. Selezionare **Indirizzo IPv4**, **Indirizzo IPv6**, **FQDN**, **Indirizzo e-mail**, o **Certificato** per il tipo. Se viene selezionato **Certificato**, digitare il nome comune del certificato nel campo **ID**.
Certificato	Se è stato selezionato **Certificati** per **Metodo di autenticazione**, selezionare il certificato.

Opzione	Descrizione
	È possibile selezionare solo i certificati creati utilizzando la pagina **Certificato** della schermata di configurazione sicurezza di Gestione basata sul Web.

Informazioni correlate

- Configurare un modello IPsec utilizzando Gestione basata sul Web

Impostazioni IKEv2 per un modello IPsec

Opzione	Descrizione
Nome modello	Immettere un nome per il modello (massimo 16 caratteri).
Usa modello preimpostato	Selezionare **Personalizzato**, **Sicurezza elevata IKEv2** o **Sicurezza media IKEv2**. Gli elementi da impostare sono diversi a seconda del modello selezionato.
Scambio chiavi Internet (IKE)	IKE è un protocollo di comunicazione utilizzato per lo scambio di chiavi di crittografia per attuare una comunicazione crittografata con IPsec. Per attuare una comunicazione crittografata solo per una volta, l'algoritmo di crittografia necessario per IPsec è determinato e le chiavi di crittografia sono condivise. Per IKE, le chiavi di crittografia vengono scambiate utilizzando il metodo di scambio delle chiavi Diffie-Hellman, e la comunicazione crittografata limitata a IKE viene eseguita. Se è stato selezionato **Personalizzato** in **Usa modello preimpostato**, selezionare **IKEv2**.
Tipo di autenticazione	• **Gruppo Diffie-Hellman** Questo metodo di scambio chiavi consente di scambiare in modo sicuro chiavi segrete in una rete non protetta. Il metodo di scambio chiavi Diffie-Hellman utilizza un problema con un logaritmo discreto, e non la chiave segreta, per inviare e ricevere informazioni aperte generate utilizzando un numero casuale e la chiave segreta. Selezionare **Gruppo 1**, **Gruppo 2**, **Gruppo 5** o **Gruppo 14**. • **Crittografia** Selezionare **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. • **Hash** Selezionare **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. • **Durata associazione di protezione** Specificare la durata di associazione protezione di IKE. Immettere il tempo (secondi) e il numero di kilobyte (KB).
Sicurezza/Incapsulamento	• **Protocollo** Selezionare **ESP**. ESP è un protocollo per attuare comunicazioni crittografate utilizzando IPsec. ESP esegue la crittografia sul carico utile (i contenuti comunicati) e aggiunge delle altre informazioni. Il pacchetto IP comprende l'intestazione e il carico crittografato, che segue l'intestazione. Oltre ai dati crittografati, il pacchetto IP include anche informazioni riguardanti il metodo di crittografia e la chiave di crittografia, i dati di autenticazione e altre informazioni. • **Crittografia** Selezionare **DES**, **3DES**, **AES-CBC 128**, o **AES-CBC 256**. • **Hash** Selezionare **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. • **Durata associazione di protezione** Specificare la durata del SA IKE. Digitare il tempo (secondi) e il numero di kilobyte (KByte). • **Modalità di incapsulamento** Selezionare **Trasporto** o **Tunnel**.

Opzione	Descrizione
	• **Indirizzo IP router remoto** Digitare l'indirizzo IP (IPv4 o IPv6) del router remoto. Inserire l'informazione solo quando è selezionata la modalità **Tunnel**. SA (Security Association) è un metodo di comunicazione crittografata utilizzando IPsec o IPv6 che permette lo scambio e la condivisione di informazioni, come il metodo e la chiave di crittografia, al fine di stabilire un canale di comunicazione sicuro prima dell'inizio della comunicazione. SA può inoltre riferirsi a un canale di comunicazione crittografata virtuale stabilito. Il SA utilizzato per IPsec stabilisce un metodo di crittografia, scambia le chiavi ed esegue un'autenticazione reciproca sulla base della procedura standard IKE (Internet Key Exchange, scambio chiavi internet). Inoltre, il SA viene periodicamente aggiornato.
Perfect Forward Secrecy (PFS)	PFS non trae le chiavi da chiavi usate in precedenza per crittografare i messaggi. Inoltre, se per crittografia di un messaggio si utilizza una chiave derivata da una chiave di livello superiore, la chiave di livello superiore non verrà utilizzata per generare altre chiavi. Inoltre, anche se una chiave viene compromessa, il danno sarà limitato solo ai messaggi crittografati utilizzando quella chiave. Selezionare **Attivata** o **Disattivato**.
Metodo di autenticazione	Selezionare il metodo di autenticazione. Selezionare **Chiave precondivisa**, **Certificati**, **EAP - MD5** o **EAP - MS-CHAPv2**. Il protocollo di autenticazione EAP è un estensione del protocollo PPP. Utilizzando EAP con IEEE802.1x viene usata una chiave diversa per l'autenticazione utente a ogni sessione. Le seguenti impostazioni sono necessarie solo quando è selezionato **EAP - MD5** o **EAP - MS-CHAPv2** in **Metodo di autenticazione**: • **Modalità** Selezionare **Modalità server** o **Modalità client**. • **Certificato** Selezionare il certificato. • **Nome utente** Immettere il nome dell'utente (massimo 32 caratteri). • **Password** Immettere la password (massimo 32 caratteri). Per confermare la password è necessario immetterla due volte.
Chiave precondivisa	Quando si applica la crittografia alla comunicazione, la chiave di crittografia viene scambiata e condivisa prima dell'operazione, utilizzando un altro canale. Se è stato selezionato **Chiave precondivisa** per **Metodo di autenticazione**, digitare la **Chiave precondivisa** (fino a 32 caratteri). • **Locale/Tipo di/ID** Selezionare il tipo di ID del mittente, quindi digitare l'ID. Selezionare **Indirizzo IPv4**, **Indirizzo IPv6**, **FQDN**, **Indirizzo e-mail**, o **Certificato** per il tipo. Se viene selezionato **Certificato**, digitare il nome comune del certificato nel campo **ID**. • **Remoto/Tipo di/ID** Selezionare il tipo di ID del destinatario, quindi digitare l'ID. Selezionare **Indirizzo IPv4**, **Indirizzo IPv6**, **FQDN**, **Indirizzo e-mail**, o **Certificato** per il tipo.

Opzione	Descrizione
	Se viene selezionato **Certificato**, digitare il nome comune del certificato nel campo **ID**.
Certificato	Se è stato selezionato **Certificati** per **Metodo di autenticazione**, selezionare il certificato. È possibile selezionare solo i certificati creati utilizzando la pagina **Certificato** della schermata di configurazione sicurezza di Gestione basata sul Web.

Informazioni correlate

- Configurare un modello IPsec utilizzando Gestione basata sul Web

Impostazioni manuali per il modello IPsec

Opzione	Descrizione
Nome modello	Immettere un nome per il modello (massimo 16 caratteri).
Usa modello preimpostato	Selezionare **Personalizzato**.
Scambio chiavi Internet (IKE)	IKE è un protocollo di comunicazione utilizzato per lo scambio di chiavi di crittografia per attuare una comunicazione crittografata con IPsec. Per attuare una comunicazione crittografata solo per una volta, l'algoritmo di crittografia necessario per IPsec è determinato e le chiavi di crittografia sono condivise. Per IKE, le chiavi di crittografia vengono scambiate utilizzando il metodo di scambio delle chiavi Diffie-Hellman, e la comunicazione crittografata limitata a IKE viene eseguita. Selezionare **Manuale**.
Chiave di autenticazione (ESP, AH)	Digitare i valori **Ingresso/Uscita**. Queste impostazioni sono necessarie quando è selezionato **Personalizzato** per **Usa modello preimpostato**, **Manuale** per **Scambio chiavi Internet (IKE)**, e un'impostazione diversa da **Nessuno** è selezionata per **Hash** per la sezione **Sicurezza/ Incapsulamento**. Il numero di caratteri che è possibile impostare varia in base all'impostazione scelta per **Hash** nella sezione **Sicurezza/ Incapsulamento**. Se la lunghezza della chiave di autenticazione specificata è diversa dall'algoritmo hash selezionato, viene visualizzato un messaggio di errore. • **MD5**: 128 bit (16 byte) • **SHA1**: 160 bit (20 byte) • **SHA256**: 256 bit (32 byte) • **SHA384**: 384 bit (48 byte) • **SHA512**: 512 bit (64 byte) Se si specifica la chiave con codice ASCII, includere i caratteri tra virgolette doppie (").
Chiave di codifica (ESP)	Digitare i valori **Ingresso/Uscita**. Queste impostazioni sono necessarie quando è selezionato **Personalizzato** per **Usa modello preimpostato**, **Manuale** per **Scambio chiavi Internet (IKE)** e **ESP** per **Protocollo** in **Sicurezza/ Incapsulamento**. Il numero di caratteri che è possibile impostare varia in base all'impostazione scelta per **Crittografia** nella sezione **Sicurezza/Incapsulamento**. Se la lunghezza della chiave di codifica specificata è diversa dall'algoritmo di crittografia selezionato, viene visualizzato un messaggio di errore. • **DES**: 64 bit (8 byte) • **3DES**: 192 bit (24 byte) • **AES-CBC 128**: 128 bit (16 byte) • **AES-CBC 256**: 256 bit (32 byte) Se si specifica la chiave con codice ASCII, includere i caratteri tra virgolette doppie (").
SPI	Questi parametri vengono utilizzati per identificare le informazioni di sicurezza. Generalmente, un host ha più SA (Security Associations,

Opzione	Descrizione
	associazioni di sicurezza) per svariati tipi di comunicazione IPsec. Di conseguenza, è necessario identificare l'associazione di sicurezza applicabile quando viene ricevuto un pacchetto IPsec. Il parametro SPI, che identifica un'associazione di sicurezza, è incluso nell'AH (Authentication Header, intestazione di autenticazione) e nell'intestazione ESP (Encapsulating Security Payload). Queste impostazioni sono necessarie quando è selezionato **Personalizzato** per **Usa modello preimpostato**, e **Manuale** per **Scambio chiavi Internet (IKE)**. Immettere i valori **Ingresso/Uscita**. (3-10 caratteri)
Sicurezza/Incapsulamento	• **Protocollo** Selezionare **ESP** o **AH**. - ESP è un protocollo per attuare comunicazioni crittografate utilizzando IPsec. ESP esegue la crittografia sul carico utile (i contenuti comunicati) e aggiunge delle altre informazioni. Il pacchetto IP comprende l'intestazione e il carico crittografato, che segue l'intestazione. Oltre ai dati crittografati, il pacchetto IP include anche informazioni riguardanti il metodo di crittografia e la chiave di crittografia, i dati di autenticazione e altre informazioni. - AH è una parte del protocollo IPsec che autentica il mittente ed evita la manipolazione dei dati (assicura la completezza dei dati). Nel pacchetto IP, i dati sono inseriti immediatamente dopo l'intestazione. Inoltre, i pacchetti includono valori cancelletto, calcolati utilizzando un'equazione dai contenuti comunicati, dalla chiave segreta e così via, al fine di evitare la falsificazione del mittente e la manipolazione dei dati. A differenza di ESP, i contenuti comunicati non sono crittografati, e i dati sono inviati e ricevuti come formato solo testo. • **Crittografia (Non disponibile per l'opzione AH.)** Selezionare **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. • **Hash** Selezionare **Nessuno**, **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. **Nessuno** può essere selezionato solo quando è selezionato **ESP** per **Protocollo**. • **Durata associazione di protezione** Specificare la durata del SA IKE. Digitare il tempo (secondi) e il numero di kilobyte (KByte). • **Modalità di incapsulamento** Selezionare **Trasporto** o **Tunnel**. • **Indirizzo IP router remoto** Digitare l'indirizzo IP (IPv4 o IPv6) del router remoto. Inserire l'informazione solo quando è selezionata la modalità **Tunnel**. SA (Security Association) è un metodo di comunicazione crittografata utilizzando IPsec o IPv6 che permette lo scambio e la condivisione di informazioni, come il metodo e la chiave di crittografia, al fine di stabilire un canale di comunicazione sicuro prima dell'inizio della comunicazione. SA può inoltre riferirsi a un canale di comunicazione crittografata virtuale stabilito. Il SA utilizzato per IPsec stabilisce un metodo di crittografia, scambia le chiavi ed esegue un'autenticazione reciproca sulla base della procedura standard IKE (Internet Key Exchange, scambio chiavi internet). Inoltre, il SA viene periodicamente aggiornato.

Informazioni correlate

- Configurare un modello IPsec utilizzando Gestione basata sul Web

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 unauthorized. 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 tunneled.

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

Autenticazione utente

- Utilizzare l'autenticazione Active Directory
- Utilizzare l'autenticazione LDAP
- Utilizzo del Blocco funzioni sicurezza 3.0

Utilizzare l'autenticazione Active Directory

- Introduzione all’autenticazione Active Directory
- Configurare l’autenticazione Active Directory utilizzando Gestione basata sul Web
- Effettuare l’accesso per modificare le impostazioni della macchina utilizzando il pannello dei comandi della macchina (autenticazione Active Directory)

Introduzione all’autenticazione Active Directory

L'autenticazione Active Directory limita l'uso della macchina. Se è abilitata l’autenticazione Active Directory, il pannello di controllo della macchina viene bloccato. Non è possibile modificare le impostazioni della macchina fin quando l’utente non inserisce l’ID utente e la password.

L’autenticazione Active Directory offre le seguenti funzioni:

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

- Archiviazione dei dati di stampa in entrata
- Archiviazione dei dati fax in entrata
- Ricezione dell’indirizzo e-mail dal server Active Directory in base all’ID utente quando si inviano i dati acquisiti a un server e-mail.

  Per utilizzare questa funzione, selezionare l'opzione **Sì** per l'impostazione **Ottieni indirizzo e-mail** e il metodo di autenticazione **LDAP + kerberos** o **LDAP + NTLMv2**. Il proprio indirizzo e-mail sarà impostato come mittente quando la macchina invia i dati acquisiti a un server e-mail o come destinatario se si desidera inviare i dati acquisiti al proprio indirizzo e-mail.

Quando l’autenticazione Active Directory è attivata, la macchina archivia tutti i dati fax in entrata. Dopo aver effettuato l’accesso, la macchina stampa i dati fax archiviati.

È possibile modificare le impostazioni dell'autenticazione Active Directory mediante Gestione basata sul Web.

Informazioni correlate

- Utilizzare l'autenticazione Active Directory

Configurare l’autenticazione Active Directory utilizzando Gestione basata sul Web

L’autenticazione Active Directory supporta l’autenticazione Kerberos e NTLMv2. Per l’autenticazione è necessario configurare il protocollo SNTP (server di riferimento orario di rete) e il server DNS.

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 **Amministratore** > **Funzione limitazione utente** o **Gestione limitazioni**.

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

5. Selezionare **Autenticazione Active Directory**.
6. Fare clic su **Invia**.
7. Fare clic su **Autenticazione Active Directory**.
8. Configurare le seguenti impostazioni:

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

Opzione	Descrizione
Dati RX Fax di storage	Selezionare questa opzione per archiviare i dati fax in entrata. È possibile stampare tutti i dati fax in entrata dopo aver effettuato l’accesso alla macchina.
Memorizza ID utente	Selezionare questa opzione per salvare l’ID utente.
Indirizzo server Active Directory	Digitare l’indirizzo IP o il nome del server Active Directory (ad esempio: ad.example.com).
Nome dominio Active Directory	Immettere il nome dominio della Active Directory.
Protocollo e metodo di autenticazione	Selezionare il protocollo e il metodo di autenticazione.
SSL/TLS	Selezionare l’opzione **SSL/TLS**.
Porta server LDAP	Digitare il numero della porta per collegare il server Active Directory tramite LDAP (disponibile solo per il metodo di autenticazione **LDAP + kerberos** o **LDAP + NTLMv2**).
Cartella principale di ricerca LDAP	Digitare la radice di ricerca LDAP (disponibile solo per metodo di autenticazione **LDAP + kerberos** o **LDAP + NTLMv2**).

Opzione	Descrizione
Ottieni indirizzo e-mail	Selezionare questa opzione per ottenere l'indirizzo e-mail dell'utente collegato dal server Active Directory. (disponibile solo per il metodo di autenticazione **LDAP + kerberos** o **LDAP + NTLMv2**)
Ottieni directory home utente	Selezionare questa opzione per ottenere la directory Home come destinazione di scansione su rete. (disponibile solo per il metodo di autenticazione **LDAP + kerberos** o **LDAP + NTLMv2**)

9. Fare clic su **Invia**.

Informazioni correlate

- Utilizzare l'autenticazione Active Directory

Effettuare l’accesso per modificare le impostazioni della macchina utilizzando il pannello dei comandi della macchina (autenticazione Active Directory)

Quando l’autenticazione Active Directory è abilitata, il pannello dei comandi della macchina sarà bloccato fin quando non vengono immessi l’ID utente e la password dal pannello dei comandi della macchina.

1. Per effettuare l'accesso, immettere l'ID utente e la password dal pannello di controllo della macchina.
2. Se l'autenticazione avviene correttamente, il pannello di controllo della macchina viene sbloccato.

Informazioni correlate

- Utilizzare l'autenticazione Active Directory

Utilizzare l'autenticazione LDAP

- Introduzione all’autenticazione LDAP
- Configurare l’autenticazione LDAP utilizzando Gestione basata sul Web
- Effettuare l’accesso per modificare le impostazioni della macchina utilizzando il pannello dei comandi della macchina (autenticazione LDAP)

Introduzione all’autenticazione LDAP

L'autenticazione LDAP limita l'uso della macchina. Se è abilitata l’autenticazione LDAP, il pannello di controllo della macchina viene bloccato. Non è possibile modificare le impostazioni della macchina fin quando l’utente non inserisce l’ID utente e la password.

L’autenticazione LDAP offre le funzioni seguenti:

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

- Archiviazione dei dati di stampa in entrata
- Archiviazione dei dati fax in entrata
- Ricezione dell’indirizzo e-mail dal server LDAP in base all’ID utente quando si inviano i dati acquisiti a un server e-mail.

  Per utilizzare questa funzione, selezionare l'opzione **Sì** per l'impostazione **Ottieni indirizzo e-mail**. Il proprio indirizzo e-mail sarà impostato come mittente quando la macchina invia i dati acquisiti a un server e-mail o come destinatario se si desidera inviare i dati acquisiti al proprio indirizzo e-mail.

Quando l’autenticazione LDAP è attivata, la macchina archivia tutti i dati fax in entrata. Dopo aver effettuato l’accesso, la macchina stampa i dati fax archiviati.

È possibile modificare le impostazioni dell'autenticazione LDAP mediante Gestione basata sul Web.

Informazioni correlate

- Utilizzare l'autenticazione LDAP

Configurare l’autenticazione LDAP utilizzando 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 **Amministratore** > **Funzione limitazione utente** o **Gestione limitazioni**.

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

5. Selezionare **Autenticazione LDAP**.
6. Fare clic su **Invia**.
7. Fare clic sul menu **Autenticazione LDAP**.
8. Configurare le seguenti impostazioni:

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

Opzione	Descrizione
Dati RX Fax di storage	Selezionare questa opzione per archiviare i dati fax in entrata. È possibile stampare tutti i dati fax in entrata dopo aver effettuato l’accesso alla macchina.
Memorizza ID utente	Selezionare questa opzione per salvare l’ID utente.
Indirizzo server LDAP	Digitare l’indirizzo IP o il nome del server LDAP (ad esempio: ldap.example.com).
SSL/TLS	Selezionare l'opzione **SSL/TLS** per utilizzare LDAP su SSL/TLS.
Porta server LDAP	Immettere il numero di porta del server LDAP.
Cartella principale di ricerca LDAP	Digitare la directory radice di ricerca LDAP.
Attributo nome (Chiave di ricerca)	Immettere l'attributo che si desidera utilizzare come chiave di ricerca.
Ottieni indirizzo e-mail	Selezionare questa opzione per ottenere l'indirizzo e-mail dell'utente collegato dal server LDAP.
Ottieni directory home utente	Selezionare questa opzione per ottenere la directory Home come destinazione di scansione su rete.

9. Fare clic su **Invia**.

Informazioni correlate

- Utilizzare l'autenticazione LDAP

Effettuare l’accesso per modificare le impostazioni della macchina utilizzando il pannello dei comandi della macchina (autenticazione LDAP)

Quando l’autenticazione LDAP è abilitata, il pannello dei comandi della macchina sarà bloccato fin quando non vengono immessi l’ID utente e la password dal pannello dei comandi della macchina.

1. Per effettuare l'accesso, immettere l'ID utente e la password dal pannello di controllo della macchina.
2. Se l'autenticazione avviene correttamente, il pannello di controllo della macchina viene sbloccato.

Informazioni correlate

- Utilizzare l'autenticazione LDAP

Utilizzo del Blocco funzioni sicurezza 3.0

Blocco funzioni sicurezza 3.0 consente di aumentare la sicurezza attraverso la limitazione delle funzioni disponibili nella macchina.

Prima dell'utilizzo di Secure Function Lock 3.0

Utilizzare Blocco funzioni sicurezza per configurare le password, impostare un limite di pagine specifico per ciascun utente e concedere l'accesso ad alcune o a tutte le funzioni elencate.

È possibile configurare e modificare le seguenti impostazioni di Blocco funzioni sicurezza 3.0 mediante Gestione basata sul Web:

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

- **Stampa**
- **Copia**
- **Scansione**
- **Fax**
- **Supporto**
- **Web Connect**
- **App**
- **Limiti di pagina**
- **Contatore pagine**
- **ID scheda (ID NFC)**

Modelli LCD touchscreen:

Quando Blocco funzioni sicurezza è attivo, la macchina passa automaticamente alla modalità pubblica e alcune funzioni della macchina risultano accessibili solo agli utenti authorized. Per accedere alle funzioni della macchina con restrizioni, premere , selezionare il proprio nome utente e immettere la password.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Configurare Secure Function Lock 3.0 utilizzando 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 **Amministratore** > **Funzione limitazione utente** o **Gestione limitazioni**.

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

5. Selezionare **Blocco funzione protezione**.
6. Fare clic su **Invia**.
7. Fare clic sul menu **Funzioni limitate**.
8. Configurare le impostazioni per gestire le restrizioni per utente o per gruppo.
9. Fare clic su **Invia**.
10. Fare clic sul menu **Elenco utenti**.
11. Configurare l'elenco utenti.
12. Fare clic su **Invia**.

È anche possibile modificare le impostazioni di blocco dell'elenco utenti nel menu **Blocco funzione protezione**.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Eseguire la scansione utilizzando Secure Function Lock 3.0

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

Impostazione delle limitazioni alla scansione (per gli amministratori)

Blocco funzioni sicurezza 3.0 consente all'amministratore di limitare gli utenti autorizzati a eseguire la scansione. Quando la funzione di scansione è impostata su No per l'opzione utenti pubblici, solo gli utenti per i quali è selezionata la casella di controllo **Scansione** possono eseguire la scansione.

Uso della funzione di scansione (per gli utenti con restrizioni)

- Per eseguire la scansione dal pannello di controllo della macchina:

  Gli utenti con restrizioni devono immettere le proprie password nel pannello dei comandi della macchina per accedere alla modalità di scansione.
- Per eseguire la scansione da un computer:

  Gli utenti con restrizioni devono immettere le proprie password nel pannello dei comandi della macchina prima di eseguire la scansione dal computer. Se sul pannello dei comandi della macchina non vengono immesse le password, sul computer dell'utente viene visualizzato un messaggio di errore.

Se la macchina supporta l'autenticazione con scheda IC, gli utenti limitati possono accedere alla modalità di scansione anche toccando il simbolo NFC sul pannello dei comandi della macchina con le proprie schede IC registrate.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Configurare la modalità pubblica per Secure Function Lock 3.0

Utilizzare la schermata Secure Function Lock per impostare la modalità pubblica, che consente di limitare le funzioni disponibili agli utenti pubblici. Gli utenti pubblici non devono immettere una password per accedere alle funzioni rese disponibili tramite le impostazioni della modalità pubblica.

La modalità pubblica comprende i lavori di stampa inviati tramite Brother iPrint&Scan e Brother Mobile Connect.

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 **Amministratore** > **Funzione limitazione utente** o **Gestione limitazioni**.

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

5. Selezionare **Blocco funzione protezione**.
6. Fare clic su **Invia**.
7. Fare clic sul menu **Funzioni limitate**.
8. Nella riga **Modalità pubblica**, selezionare una casella di controllo per consentire l'uso della funzione elencata oppure deselezionare la casella per limitare la funzione stessa.
9. Fare clic su **Invia**.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Configurare le impostazioni della schermata Home personale utilizzando Gestione basata sul Web

L'amministratore può specificare quali schede possono visualizzare gli utenti nelle rispettive schermate Home personali. Queste schede forniscono un accesso rapido alle scelte rapide favorite degli utenti, i quali possono scegliere di assegnarle alle loro schede della schermata Home personale dal pannello di controllo della macchina.

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

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 **Amministratore** > **Funzione limitazione utente** o **Gestione limitazioni**.

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

5. Selezionare **Blocco funzione protezione**.
6. Nel campo **Impostazioni scheda**, selezionare **Personale** per i nomi delle schede da utilizzare come schermata Home personale.
7. Fare clic su **Invia**.
8. Fare clic sul menu **Funzioni limitate**.
9. Configurare le impostazioni per gestire le restrizioni per utente o per gruppo.
10. Fare clic su **Invia**.
11. Fare clic sul menu **Elenco utenti**.
12. Configurare l'elenco utenti.
13. Selezionare **Elenco utenti/funzioni limitate** per ogni utente dall'elenco a discesa.
14. Selezionare il nome della scheda dall'elenco a discesa **Schermata iniziale** per ogni utente.
15. Fare clic su **Invia**.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Altre funzionalità di Secure Function Lock 3.0

Configurare le seguenti funzionalità nella schermata Secure Function Lock:

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

Ripristino di tutti i contat.

Fare clic su **Ripristino di tutti i contat.** nella colonna **Contatore pagine** per azzerare il contatore delle pagine.

Esporta in file CSV

Fare clic su **Esporta in file CSV** per esportare come file CSV il contatore delle pagine corrente e l'ultimo contatore, incluse le informazioni relative a **Elenco utenti/funzioni limitate**.

ID scheda (ID NFC)

Fare clic sul menu **Elenco utenti** quindi digitare l'ID della scheda utente nel campo **ID scheda (ID NFC)**. Per l'autenticazione, è possibile utilizzare la scheda IC.

Output

Quando l'unità Mailbox è installata sulla macchina, selezionare il vassoio di uscita per ogni utente dall'elenco a discesa.

Ultima registrazione contatore

Fare clic su **Ultima registrazione contatore** se si desidera che l'apparecchio conservi il conteggio delle pagine una volta azzerato il contatore.

Reimpostazione automatica contatore

Fare clic su **Reimpostazione automatica contatore** per configurare l'intervallo di tempo tra un azzeramento del contatore delle pagine e il successivo azzeramento. Selezionare un intervallo giornaliero, settimanale o mensile.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Registrare una nuova scheda IC utilizzando il pannello dei comandi della macchina

È possibile registrare schede a circuito integrato (schede IC) nella macchina.

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

1. Toccare il simbolo NFC (Near-Field Communication) sul pannello dei comandi della macchina con una scheda di circuito integrato (scheda IC) registrata.
2. Premere il proprio ID utente sul display LCD.
3. Premere il pulsante Registra scheda.
4. Mettere a contatto una nuova scheda IC con il simbolo NFC.

   Il numero della nuova scheda IC viene registrato nella macchina.
5. Premere il pulsante OK.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Registrare un lettore di carte IC esterno

Quando si collega un lettore di schede IC (circuito integrato) esterno, utilizzare Gestione basata sul Web per registrarlo. La macchina supporta i lettori di carte IC esterni supportati dal driver di classe HID.

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 **Amministratore** > **Lettore card esterno**.

   Se la barra di spostamento di sinistra non è visibile, avviare l'esplorazione da ☰.
5. Immettere le informazioni necessarie, quindi fare clic su **Invia**.
6. Riavviare la macchina Brother per attivare la configurazione.
7. Collegare il lettore di schede alla macchina.
8. Per utilizzare l'autenticazione con scheda, mettere a contatto la scheda con il lettore di schede.

Informazioni correlate

- Utilizzo del Blocco funzioni sicurezza 3.0

Inviare o ricevere messaggi e-mail in modo sicuro

Configurare l'invio e la ricezione di e-mail utilizzando Gestione basata sul Web

- La ricezione e-mail è disponibile solo per alcuni modelli.
- È consigliabile utilizzare Gestione basata sul Web per configurare l'invio e-mail in modo sicuro tramite l'autenticazione utente oppure l'invio e la ricezione e-mail mediante SSL/TLS (solo modelli supportati).

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. Nel campo **Client POP3/IMAP4/SMTP**, fare clic su **Impostazioni avanzate** e verificare che lo stato dell'opzione **Client POP3/IMAP4/SMTP** corrisponda a **Attivata**.

- I protocolli disponibili potrebbero variare a seconda della macchina.
- Se viene visualizzata la schermata di selezione **Metodo di autenticazione**, selezionare il metodo di autenticazione e seguire le istruzioni a schermo.

6. Configurare le impostazioni **Client POP3/IMAP4/SMTP**.
   - Al termine della configurazione, verificare che le impostazioni e-mail siano corrette inviando un messaggio e-mail di prova.
   - Se non si conoscono le impostazioni del server POP3/IMAP4/SMTP, rivolgersi all'amministratore di rete o all'ISP (provider di servizi Internet).
7. Al termine, fare clic su **Invia**.

   Viene visualizzata la finestra di dialogo **Prova configurazione invio/ricezione e-mail**.
8. Seguire le istruzioni visualizzate nella finestra di dialogo per verificare le impostazioni correnti.

Informazioni correlate

- Inviare o ricevere messaggi e-mail in modo sicuro

Argomenti correlati:

- Inviare o ricevere in modo sicuro un messaggio e-mail utilizzando SSL/TLS

Inviare un messaggio e-mail con l’autenticazione utente

La macchina invia e-mail tramite un server e-mail che richiede l'autenticazione utente. Tale metodo impedisce agli utenti unauthorized di accedere al server e-mail.

È possibile inviare notifiche e-mail, rapporti e-mail e I-Fax (disponibile solo per alcuni modelli) mediante l'autenticazione utente.

- I protocolli disponibili potrebbero variare a seconda della macchina.
- È consigliabile utilizzare Gestione basata sul Web per configurare l'autenticazione SMTP.

Impostazioni del server e-mail

È necessario configurare il metodo di autenticazione SMTP della macchina in modo che corrisponda al metodo utilizzato dal server e-mail. Per i dettagli sulle impostazioni del server e-mail, rivolgersi all’amministratore di rete o al fornitore di servizi Internet (ISP).

Per attivare l'autenticazione del server SMTP mediante Gestione basata sul Web, selezionare il metodo di autenticazione in **Metodo autenticazione server** nella schermata **Client POP3/IMAP4/SMTP**.

Informazioni correlate

- Inviare o ricevere messaggi e-mail in modo sicuro

Inviare o ricevere in modo sicuro un messaggio e-mail utilizzando SSL/TLS

La macchina supporta i metodi di comunicazione SSL/TLS. Per utilizzare un server e-mail che utilizza la comunicazione SSL/TLS, è necessario configurare le impostazioni seguenti.

- La ricezione e-mail è disponibile solo per alcuni modelli.
- È consigliabile utilizzare Gestione basata sul Web per configurare SSL/TLS.

Verificare il certificato del server

Nella sezione **SSL/TLS**, se si seleziona **SSL** o **TLS**, la casella di controllo **Verificare il certificato server** viene selezionata automaticamente.

- 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.
- Se non è necessario verificare il certificato del server, deselezionare la casella di controllo **Verificare il certificato server**.

Numero della porta

Se si sceglie **SSL** o **TLS**, il valore **Porta** viene modificato in modo da corrispondere al protocollo prescelto. Per modificare il numero di porta manualmente, digitare il numero della porta dopo avere selezionato le impostazioni **SSL/TLS**.

È necessario configurare il metodo di comunicazione della macchina in modo che corrisponda al metodo utilizzato dal server e-mail. Per i dettagli sulle impostazioni del server e-mail, rivolgersi all'amministratore di rete o all'ISP.

Nella maggior parte dei casi, i servizi di posta sul Web protetti richiedono le seguenti impostazioni:

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

SMTP	**Porta**	587
	Metodo autenticazione server	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Porta**	995
	SSL/TLS	**SSL**
IMAP4	**Porta**	993
	SSL/TLS	**SSL**

Informazioni correlate

- Inviare o ricevere messaggi e-mail in modo sicuro

Argomenti correlati:

- Configurare l'invio e la ricezione di e-mail utilizzando Gestione basata sul Web
- Configurare un certificato per la protezione del dispositivo

Memorizzazione del registro di stampa in rete

Panoramica della memorizzazione del registro di stampa in rete

La funzione di memorizzazione del registro di stampa in rete consente di salvare il file di registro della stampa dalla macchina a un server di rete mediante il protocollo CIFS (Common Internet File System). È possibile registrare l'ID, il tipo di processo di stampa, il nome del processo, il nome utente, la data, l'ora e il numero di pagine stampate per ogni processo di stampa. CIFS è un protocollo che viene eseguito su TCP/IP per consentire ai computer in rete di condividere i file su rete intranet o su Internet.

Le seguenti funzioni di stampa sono registrate nel registro di stampa:

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

- Processi di stampa dal computer
- Stampa USB diretta
- Copia
- Fax ricevuto
- Web Connect Print

- La funzione di memorizzazione del registro di stampa in rete supporta l'autenticazione Kerberos e l'autenticazione NTLMv2. È necessario configurare il protocollo SNTP (server di riferimento ora di rete), oppure è necessario impostare correttamente la data, l'ora e il fuso orario per l'autenticazione sul pannello di controllo.
- È possibile impostare il tipo di file su TXT o CSV per la memorizzazione di un file sul server.

Informazioni correlate

- Memorizzazione del registro di stampa in rete

Configurare le impostazioni di memorizzazione del registro di stampa in rete tramite 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 **Amministratore** > **Salva registro di stampa in rete**.

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

5. Nel campo **Stampa registro**, fare clic su **Sì**.
6. Configurare le seguenti impostazioni:

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

Opzione	Descrizione
Percorso della cartella di rete	Digitare la cartella di destinazione in cui archiviare il registro di stampa sul server CIFS (ad esempio: \\ComputerName\SharedFolder).
Nome file	Digitare il nome file da utilizzare per il registro di stampa (fino a 32 caratteri).
Tipo file	Selezionare l'opzione **TXT** o **CSV** per il tipo di file del registro di stampa.
Origine ora per il registro	Selezionare il riferimento orario per il registro di stampa.
Metodo di autenticazione	Selezionare il metodo di autenticazione richiesto per l'accesso al server CIFS: **Auto**, **Kerberos** o **NTLMv2**. Kerberos è un protocollo di autenticazione che consente ai dispositivi o agli individui di dimostrare con sicurezza la propria identità ai server di rete utilizzando un punto di accesso singolo. NTLMv2 è il metodo di autenticazione utilizzato da Windows per l'accesso ai server. • **Auto**: se si seleziona **Auto**, NTLMv2 verrà utilizzato per il metodo di autenticazione. • **Kerberos**: Selezionare l'opzione **Kerberos** per utilizzare solo l'autenticazione Kerberos. • **NTLMv2**: Selezionare l'opzione **NTLMv2** per utilizzare solo l'autenticazione NTLMv2. • Per l'autenticazione **Kerberos** e **NTLMv2** è inoltre necessario configurare le impostazioni **Data/Ora** o il protocollo SNTP (server di riferimento orario di rete) e il server DNS. • È possibile configurare le impostazioni di data e ora anche dal pannello di controllo della macchina.

Opzione	Descrizione
Nome utente	Digitare il nome utente per l'autenticazione (fino a 96 caratteri). Se il nome utente appartiene a un dominio, immettere il nome utente seguendo una delle seguenti convenzioni: utente@dominio o dominio \utente.
Password	Digitare la password per l'autenticazione (fino a 32 caratteri).
Indirizzo server Kerberos (se necessario)	Digitare l'indirizzo host Key Distribution Center (KDC) (ad esempio: kerberos.example.com; fino a 64 caratteri) o l'indirizzo IP (ad esempio: 192.168.56.189).
Impostazione rilevazione errori	Scegliere l'azione da intraprendere se il registro di stampa non può essere archiviato sul server a causa di un errore di rete.

7. Nel campo **Stato connessione**, verificare l'ultimo stato di registro.

È anche possibile verificare lo stato si errore sull'LCD della macchina.

8. Fare clic su **Invia** per visualizzare la pagina **Log Stampa di prova in rete**.

   Per verificare le impostazioni, fare clic su **SI** e passare al punto successivo.

   Per saltare il test, fare clic su **No**. Le impostazioni verranno inviate automaticamente.
9. La macchina esegue il test delle impostazioni.
10. Se le impostazioni vengono accettate, sulla schermata viene visualizzato **Test OK**.

    Se viene visualizzato **Errore test**, selezionare tutte le impostazioni e fare clic su **Invia** per visualizzare nuovamente la pagina di test.

Informazioni correlate

- Memorizzazione del registro di stampa in rete

Utilizzare l'impostazione di rilevamento degli errori della memorizzazione del registro di stampa in rete

Utilizzare l'impostazione di rilevamento degli errori per determinare l'azione da intraprendere quando il registro di stampa non può essere archiviato sul server a causa di un errore di rete.

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 **Amministratore** > **Salva registro di stampa in rete**.

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

5. Nella sezione **Impostazione rilevazione errori**, selezionare l'opzione **Annulla stampa** o **Ignora regis. e stampa**.

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

Opzione	Descrizione
Annulla stampa	Se si seleziona l'opzione **Annulla stampa**, i processi di stampa vengono canceled nel caso in cui il registro di stampa non possa essere memorizzato sul server. Anche se si seleziona l'opzione **Annulla stampa**, la macchina stampa il fax ricevuto.

Ignora regis. e stampa	Se si seleziona l'opzione **Ignora regis. e stampa**, la macchina stampa la documentazione anche nel caso in cui il registro di stampa non possa essere memorizzato sul server.
	
	Se la funzione di memorizzazione del registro di stampa è stata ripristinata, il registro di stampa viene registrato come indicato di seguito:
	
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	
	a. Se alla fine della stampa non è possibile memorizzare il registro di stampa, il numero di pagine stampante non sarà registrato.
	b. Se il registro di stampa non può essere memorizzato all'inizio e alla fine della stampa, il registro di stampa del processo non viene registrato. Quando la funzione viene ripristinata, l'errore è indicato nel registro di stampa.

6. Fare clic su **Invia** per visualizzare la pagina **Log Stampa di prova in rete**.

   Per verificare le impostazioni, fare clic su **SI** e passare al punto successivo.

Per saltare il test, fare clic su **No**. Le impostazioni verranno inviate automaticamente.

7. La macchina esegue il test delle impostazioni.
8. Se le impostazioni vengono accettate, sulla schermata viene visualizzato **Test OK**.

   Se viene visualizzato **Errore test**, selezionare tutte le impostazioni e fare clic su **Invia** per visualizzare nuovamente la pagina di test.

Informazioni correlate

- Memorizzazione del registro di stampa in rete

Utilizzare la memorizzazione del registro di stampa in rete con Secure Function Lock 3.0

Se Blocco funzioni sicurezza 3.0 è attivo, i nomi degli utenti registrati per le funzioni di copia, ricezione fax, stampa Web Connect Print e stampa diretta USB sono registrati nel rapporto di memorizzazione del registro di stampa in rete. Se l'autenticazione Active Directory è attiva, il nome utente viene registrato nel rapporto di memorizzazione del registro di stampa in rete:

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

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

Informazioni correlate

- Memorizzazione del registro di stampa in rete

brother

Brother Earth

www.brotherearth.com

ITA
Versione 0