


# Manuale delle impostazioni IPsec



## Definizione delle note

Nella presente Guida dell'utente viene utilizzata la seguente icona:

|  |  |
|--|--|
|  Nota | Le note forniscono istruzioni da seguire in determinate situazioni o consigli sull'interazione tra le operazioni e le altre funzionalità dell'apparecchio. |
|--|--|

## Marchi commerciali

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

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

©2012 Brother Industries, Ltd. Tutti i diritti riservati.

# Sommario

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduzione</b>   | <b>1</b>  |
|          | Informazioni generali .....   | 1         |
|          | Configurazione mediante Gestione basata sul Web (browser Web) ..... | 2         |
| <b>2</b> | <b>Impostazioni IPsec</b>   | <b>5</b>  |
|          | Modello indirizzo .....   | 5         |
|          | Modello del servizio .....  | 7         |
|          | Modello servizio IPsec .....  | 7         |
|          | Imposta servizio .....  | 9         |
|          | Modello IPsec .....   | 11        |
| <b>A</b> | <b>Appendice A</b>  | <b>20</b> |
|          | Modelli dei servizi .....   | 20        |
|          | Tipo/Codice .....   | 21        |

## Informazioni generali

IPsec (Internet Protocol Security) è un protocollo di sicurezza che utilizza una funzione opzionale del protocollo IP (Internet Protocol) al fine di prevenire la manipolazione dei dati trasmessi come pacchetti IP e garantirne la riservatezza. IPsec esegue la crittografia dei dati trasmessi in rete, ad esempio i dati di stampa inviati dai computer a una stampante. Dal momento che i dati vengono crittografati a livello di rete, le applicazioni che utilizzano un protocollo di livello superiore impiegano IPsec anche se l'utente non è consapevole dell'utilizzo di questo protocollo.

IPsec supporta le seguenti funzioni:

### ■ Trasmissioni IPsec

In funzione delle condizioni di configurazione del protocollo IPsec, il computer collegato in rete invia e riceve i dati dal dispositivo specificato utilizzando IPsec. Quando i dispositivi iniziano a comunicare tramite IPsec, vengono innanzitutto scambiate le chiavi utilizzando il protocollo IKE (Internet Key Exchange), quindi i dati crittografati vengono trasmessi utilizzando le chiavi.

Inoltre, IPsec dispone di due modalità operative: la modalità Trasporto e la modalità Tunnel. La modalità Trasporto viene utilizzata principalmente per la comunicazione tra dispositivi e la modalità Tunnel viene utilizzata in ambienti quali le reti VPN (reti private virtuali).



### Nota

---

- Per le trasmissioni IPsec sono necessarie le seguenti condizioni:
    - Un computer in grado di comunicare tramite IPsec deve essere collegato alla rete.
    - La stampante o il dispositivo MFC deve essere configurato per la comunicazione tramite IPsec.
    - Il computer collegato alla stampante o al dispositivo MFC deve essere configurato per le connessioni IPsec.
  - Il protocollo IPsec non supporta la trasmissione circolare o la comunicazione multicast.
- 

### ■ Impostazioni IPsec

Impostazioni necessarie per le connessioni tramite IPsec. È possibile configurare queste impostazioni utilizzando la Gestione basata sul Web. (Vedere *Configurazione mediante Gestione basata sul Web (browser Web)* >> pagina 2.)



### Nota

---


Per configurare le impostazioni IPsec, è necessario che alla rete sia collegato un computer in grado di gestire un browser.

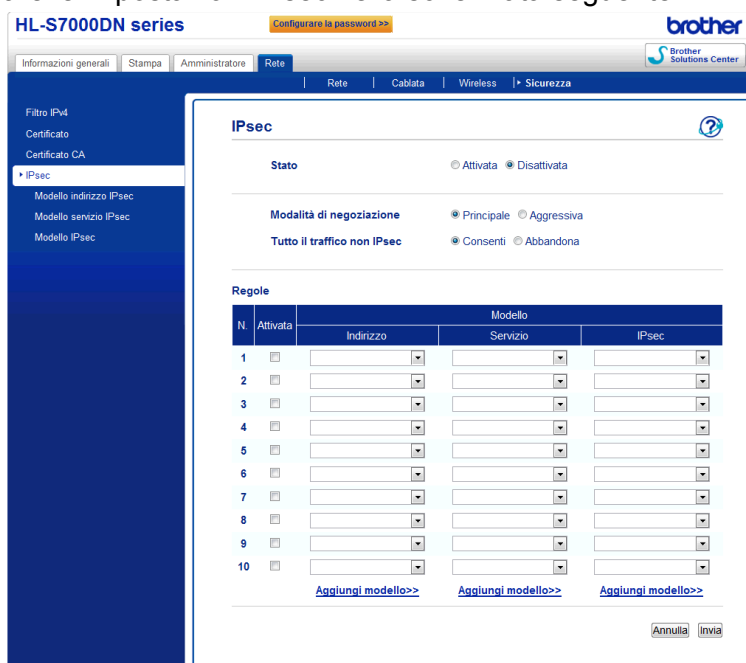
---

# Configurazione mediante Gestione basata sul Web (browser Web)

Per specificare le condizioni di connessione tramite IPsec, utilizzare la schermata delle impostazioni IPsec della Gestione basata sul Web.

Le condizioni di connessione IPsec comprendono tre tipi di **Modello**: **Indirizzo**, **Servizio** e **IPsec**; è possibile configurare fino a 10 condizioni di connessione.


- 1 Avviare il browser Web.
- 2 Digitare "http://indirizzo IP dell'apparecchio/" nel browser (dove "indirizzo IP dell'apparecchio" corrisponde all'indirizzo IP dell'apparecchio).
  - Ad esempio:  
http://192.168.1.2/
- 3 Per impostazione predefinita non è richiesta alcuna password. Immettere la password, se è stata impostata, e premere .
- 4 Fare clic sulla scheda **Rete**.
- 5 Fare clic su **Sicurezza**.
- 6 Fare clic su **IPsec**.
- 7 È possibile configurare le impostazioni IPsec nella schermata seguente.



HL-S7000DN series Configurare la password >> **brother**  
 Brother Solutions Center

Informazioni generali | Stampa | Amministratore | Rete | Rete | Cablata | Wireless | Sicurezza

Filtro IPv4  
 Certificato  
 Certificato CA  
 IPsec  
 Modello indirizzo IPsec  
 Modello servizio IPsec  
 Modello IPsec

**IPsec** 

**Stato**  Attivata  Disattivata

**Modalità di negoziazione**  Principale  Aggressiva

**Tutto il traffico non IPsec**  Consenti  Abbandona

**Regole**

| N. | Attivata                 | Modello              |                      |                      |
|----|--------------------------|----------------------|----------------------|----------------------|
|    |                          | Indirizzo            | Servizio             | IPsec                |
| 1  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 2  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 3  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 4  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 5  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 6  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 7  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 8  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 9  | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 10 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

[Aggiungi modello>>](#) [Aggiungi modello>>](#) [Aggiungi modello>>](#)

## ■ Stato

Selezionare **Attivata** o **Disattivata** per l'opzione IPsec.

### ■ Modalità di negoziazione

Selezionare la modalità per la Fase 1 IKE.

- **Principale:** viene utilizzata la modalità principale.
- **Aggressiva:** viene utilizzata la modalità aggressiva.



#### Nota

Il protocollo IKE viene utilizzato per lo scambio di chiavi di crittografia allo scopo di effettuare una comunicazione crittografata utilizzando il protocollo IPsec.

Se si seleziona la modalità **Principale**, la velocità di elaborazione è inferiore ma la sicurezza è elevata. Se si seleziona la modalità **Aggressiva**, la velocità di elaborazione è maggiore rispetto alla modalità **Principale** ma il livello di sicurezza è inferiore.

### ■ Tutto il traffico non IPsec

Selezionare l'azione da effettuare per i pacchetti non IPsec.

- **Consenti:** viene consentita la ricezione di tutti i pacchetti.
- **Abbandona:** i pacchetti non IPsec vengono ignorati.



#### Nota

Quando si utilizzano i servizi Web, è necessario selezionare **Consenti** per **Tutto il traffico non IPsec**. Se si seleziona **Abbandona**, non è possibile utilizzare i servizi Web.

### ■ Regole

È possibile configurare un massimo di 10 condizioni di connessione IPsec (set di modelli).

### ■ Attivata

Quando si seleziona questa casella di controllo, viene attivato il set di modelli relativo al numero corrispondente.



#### Nota

Quando si selezionano più caselle di controllo, in caso di conflitto tra le impostazioni relative alle caselle selezionate viene data priorità ai numeri inferiori.

### ■ Modello - Indirizzo

Selezionare il **Modello indirizzo** utilizzato per le condizioni di connessione IPsec.

Per aggiungere un **Modello indirizzo**, fare clic su **Aggiungi modello**. (Vedere *Modello indirizzo* >> pagina 5.)

### ■ Modello - Servizio

Selezionare il **Modello servizio** utilizzato per le condizioni di connessione IPsec.

Per aggiungere un **Modello servizio**, fare clic su **Aggiungi modello**. (Vedere *Modello del servizio* >> pagina 7.)



### Nota

---

Se si desidera utilizzare DNS per la risoluzione dei nomi quando si adottano i modelli dei servizi 2, 3 e 4 riportati in *Appendice A*, è necessario configurare separatamente le impostazioni DNS.

---

#### ■ **Modello - IPsec**

Selezionare il **Modello IPsec** utilizzato per le condizioni di connessione IPsec.

Per aggiungere un **Modello IPsec**, fare clic su **Aggiungi modello**. (Vedere *Modello IPsec* >> pagina 11.)

#### ■ **Invia**

Fare clic su questo pulsante per registrare le impostazioni. Se è necessario riavviare il computer per modificare le impostazioni, quando si fa clic sul pulsante viene visualizzata la schermata di conferma del riavvio.



### Nota

---

Se si seleziona la casella di controllo **Attivata** e si fa clic su **Invia**, si verifica un errore nel caso in cui uno degli elementi del modello selezionato sia stato lasciato in bianco.

---

## Modello indirizzo

Specificare gli indirizzi IP che verranno utilizzati per le condizioni di connessione IPsec. È possibile utilizzare al massimo 10 voci per l'opzione **Modello indirizzo**.

- 1 Avviare il browser Web.
- 2 Digitare "http://indirizzo IP dell'apparecchio/" nel browser (dove "indirizzo IP dell'apparecchio" corrisponde all'indirizzo IP dell'apparecchio).
  - Ad esempio:  
http://192.168.1.2/
- 3 Per impostazione predefinita non è richiesta alcuna password. Immettere la password, se è stata impostata, e premere ➔.
- 4 Fare clic sulla scheda **Rete**.
- 5 Fare clic su **Sicurezza**.
- 6 Fare clic su **Modello indirizzo IPsec**.  
10 **Modelli indirizzo** vengono visualizzati. Se il **Modello indirizzo** non è stato configurato, viene visualizzato il messaggio **Non configurato**.
  - **Cancella**  
Fare clic su questo pulsante per eliminare il **Modello indirizzo** selezionato. Tuttavia, non è possibile eliminare il **Modello indirizzo** attualmente in uso.
- 7 Fare clic sul numero relativo al **Modello indirizzo** che si desidera creare. Specificare l'indirizzo IP che dovrà utilizzare IPsec nella schermata che segue, quindi creare il **Modello indirizzo IPsec**.



### ■ Nome modello

Immettere in questa casella un nome per il modello. (massimo 16 caratteri)

### ■ Indirizzo IP locale

Specificare le condizioni relative all'indirizzo IP del mittente.

#### • Indirizzo IP

Specificare l'indirizzo IP. Selezionare **Tutti gli indirizzi IPv4**, **Tutti gli indirizzi IPv6**, **Tutti gli indirizzi IPv6 locali** o **Personalizzato**.

Se si seleziona l'opzione **Personalizzato**, immettere nella casella di testo l'indirizzo IP specifico (IPv4 o IPv6).

#### • Intervallo indirizzi IP

Immettere l'indirizzo IP iniziale e finale dell'intervallo di indirizzi IP. Se l'indirizzo IP iniziale o finale non è conforme allo standard IPv4 o IPv6 oppure l'indirizzo IP finale è inferiore rispetto all'indirizzo iniziale, si verifica un errore.

#### • Indirizzo IP / Prefisso

Specificare l'indirizzo IP utilizzando un prefisso.

Ad esempio: 192.168.1.1/24

Dal momento che il prefisso è specificato sotto forma di subnet mask a 24 bit (255.255.255.0) per l'indirizzo 192.168.1.1, sono validi gli indirizzi 192.168.1.xx.

### ■ Indirizzo IP remoto

Specificare le condizioni relative all'indirizzo IP del destinatario.

#### • Qualsiasi

Quando si seleziona **Qualsiasi**, tutti gli indirizzi IP sono abilitati.

#### • Indirizzo IP

Immettere nella casella di testo l'indirizzo IP specifico (IPv4 o IPv6).

#### • Intervallo indirizzi IP

Immettere l'indirizzo IP iniziale e finale dell'intervallo di indirizzi IP. Se l'indirizzo IP iniziale o finale non è conforme allo standard IPv4 o IPv6 oppure l'indirizzo IP finale è inferiore rispetto all'indirizzo iniziale, si verifica un errore.

#### • Indirizzo IP / Prefisso

Specificare l'indirizzo IP utilizzando un prefisso.

Ad esempio: 192.168.1.1/24

Dal momento che il prefisso è specificato sotto forma di subnet mask a 24 bit (255.255.255.0) per l'indirizzo 192.168.1.1, sono validi gli indirizzi 192.168.1.xx.

### ■ Invia

Fare clic su questo pulsante per registrare le impostazioni.



### Nota

Quando si modificano le impostazioni del modello attualmente in uso, la schermata delle impostazioni IPsec della Gestione basata sul Web viene chiusa e riaperta.

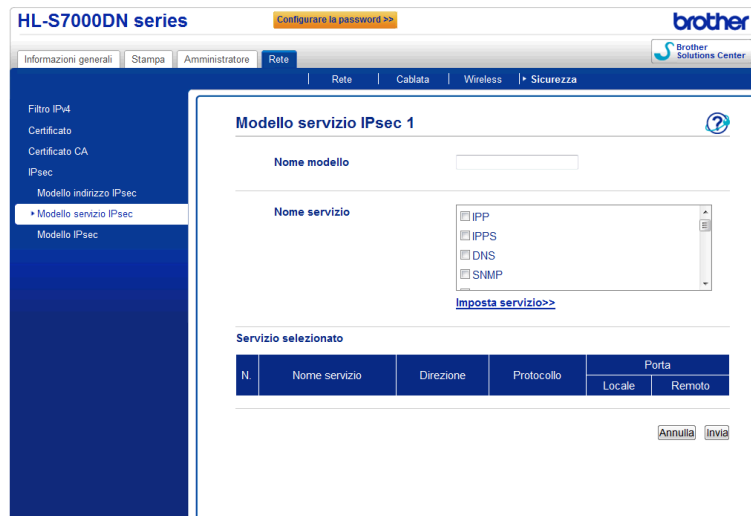
## Modello del servizio

### Modello servizio IPsec

Specificare il protocollo e il numero di porta da utilizzare per le connessioni IPsec. È possibile utilizzare al massimo 10 voci per l'opzione **Modello servizio**.

- 1 Avviare il browser Web.
- 2 Digitare "http://indirizzo IP dell'apparecchio/" nel browser (dove "indirizzo IP dell'apparecchio" corrisponde all'indirizzo IP dell'apparecchio).
  - Ad esempio:  
http://192.168.1.2/
- 3 Per impostazione predefinita non è richiesta alcuna password. Immettere la password, se è stata impostata, e premere ➔.
- 4 Fare clic sulla scheda **Rete**.
- 5 Fare clic su **Sicurezza**.
- 6 Fare clic su **Modello servizio IPsec**.  
10 **Modelli servizio** vengono visualizzati. Se il **Modello servizio** non è stato configurato, viene visualizzato il messaggio **Non configurato**.
  - **Cancella**  
Fare clic su questo pulsante per eliminare il **Modello servizio** selezionato. Tuttavia, non è possibile eliminare il **Modello servizio** attualmente in uso.

- 7 Fare clic sul numero relativo al **Modello servizio** che si desidera creare. Selezionare nella schermata che segue i servizi che si desidera utilizzare per IPsec, quindi creare il **Modello servizio IPsec**. Inoltre, è possibile fare clic su **Imposta servizio** per creare servizi originali. (Vedere *Imposta servizio* >> pagina 9.)



■ **Nome modello**

Immettere in questa casella un nome per il modello. (massimo 16 caratteri)

■ **Nome servizio**

Vengono visualizzati i nomi dei servizi predefiniti e i nomi dei servizi creati in precedenza. Selezionare i servizi che si desidera aggiungere al modello.

■ **Imposta servizio**

Fare clic su **Imposta servizio** per configurare il modello mediante l'aggiunta di servizi. (Vedere *Imposta servizio* >> pagina 9.)

■ **Servizio selezionato**

Vengono visualizzate le informazioni sul servizio (**Nome servizio**, **Direzione**, **Protocollo** e **Porta**) selezionate per l'opzione **Nome servizio**.

**Nota**

- È possibile aggiungere contemporaneamente un massimo di 32 servizi.
- Per maggiori dettagli sui protocolli che è possibile specificare in **Modello servizio IPsec**, vedere l'*Appendice A*.

■ **Invia**

Fare clic su questo pulsante per registrare le impostazioni.

**Nota**

Quando si modificano le impostazioni del modello attualmente in uso, la schermata delle impostazioni IPsec della Gestione basata sul Web viene chiusa e riaperta.

## Imposta servizio

Creare un nuovo servizio.

- 1 Nella schermata **Modello servizio IPsec**, fare clic su **Imposta servizio**.  
60 **Nomi servizio** vengono visualizzati. Se il **Nome servizio** non è stato configurato, viene visualizzato il messaggio **Non configurato**.

- **Cancella**

Fare clic su questo pulsante per eliminare il **Nome servizio** selezionato. Tuttavia, non è possibile eliminare il **Nome servizio** attualmente in uso.

- **Modello servizio IPsec**

Fare clic su questo pulsante per tornare alla schermata **Modello servizio IPsec**.

- 2 Fare clic sul numero relativo al **Nome servizio** che si desidera creare. Selezionare nella schermata che segue i servizi che si desidera utilizzare per IPsec. Gli elementi che è possibile impostare variano in funzione del **Protocollo** selezionato.

(Protocollo:TUTTI)

The screenshot shows the Brother HL-S7000DN series web interface. The top navigation bar includes 'Informazioni generali', 'Stampa', 'Amministratore', and 'Rete'. The 'Rete' section is expanded to show 'Rete', 'Cablata', 'Wireless', and 'Sicurezza'. The left sidebar lists various settings: 'Filtro IPv4', 'Certificato', 'Certificato CA', 'IPsec', 'Modello indirizzo IPsec', 'Modello servizio IPsec', and 'Modello IPsec'. The main content area is titled 'Imposta servizio 1' and contains the following fields:

- Nome servizio**: A text input field.
- Direzione**: Radio buttons for 'Iniziatore', 'Risponditore', and 'Entrambi'.
- Protocollo**: A dropdown menu currently set to 'TUTTI'.
- Imposta servizio>>**: A link to save the configuration.
- Annulla** and **Invia**: Buttons at the bottom right.

(Protocollo:TCP o UDP)

(Protocollo: ICMP)

■ **Nome servizio**

Immettere in questa casella un nome per il servizio. (massimo 16 caratteri)

■ **Direzione**

Specificare la direzione della comunicazione. Selezionare **Iniziatore**, **Risponditore** o **Entrambi**.

■ **Protocollo**

Specificare il protocollo abilitato. Selezionare **TUTTI**, **TCP**, **UDP** o **ICMP**. Gli elementi che è possibile impostare variano in funzione del **Protocollo** selezionato.

- Se si seleziona **TCP** o **UDP**, registrare la **Porta locale/Porta remota**.
- Se si seleziona **ICMP**, registrare il **Tipo/Codice**.

 **Nota**

Il protocollo ICMP viene utilizzato per inviare messaggi di errore e messaggi di controllo IP. Questo protocollo viene utilizzato da computer e dispositivi di rete collegati mediante TCP/IP per le attività di conferma reciproca dello stato.

- **Porta locale/Porta remota** (Quando si seleziona **TCP** o **UDP** in **Protocollo**.)

Immettere il numero della porta locale. Se si seleziona l'opzione **Singola**, immettere un solo numero di porta. Se si seleziona l'opzione **Intervallo**, immettere il numero di porta iniziale, quindi il numero di porta finale. Se si desidera abilitare tutti i numeri di porta, selezionare **Intervallo** e immettere "1-65535" (senza virgolette).

- **ICMP(Locale)/ICMP(Remoto)** (Quando si seleziona **ICMP** in **Protocollo**.)

Configurare le impostazioni ICMP. Selezionare **Qualsiasi** oppure immettere il **Tipo/Codice**. Per maggiori dettagli su **Tipo/Codice**, vedere l'*Appendice A*.

- **Imposta servizio**

Fare clic su questo pulsante per tornare alla schermata **Imposta servizio**.

- **Invia**


Fare clic su questo pulsante per registrare le impostazioni.

 **Nota**

Quando si modificano le impostazioni del modello attualmente in uso, la schermata delle impostazioni IPsec della Gestione basata sul Web viene chiusa e riaperta.

## Modello IPsec

Configurare le impostazioni IKE/IPsec. È possibile utilizzare al massimo 10 voci per l'opzione **Modello IPsec**.

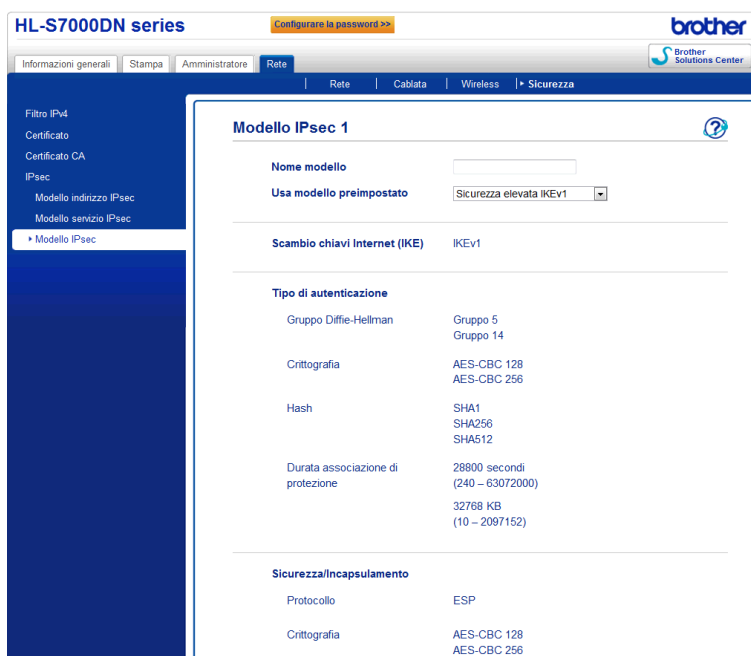
- 1 Avviare il browser Web.
- 2 Digitare "http://indirizzo IP dell'apparecchio/" nel browser (dove "indirizzo IP dell'apparecchio" corrisponde all'indirizzo IP dell'apparecchio).
  - Ad esempio:  
http://192.168.1.2/
- 3 Per impostazione predefinita non è richiesta alcuna password. Immettere la password, se è stata impostata, e premere .
- 4 Fare clic sulla scheda **Rete**.
- 5 Fare clic su **Sicurezza**.
- 6 Fare clic su **Modello IPsec**.  
10 **Modelli IPsec** vengono visualizzati. Se il **Modello IPsec** non è stato configurato, viene visualizzato il messaggio **Non configurato**.

■ **Cancella**

Fare clic su questo pulsante per eliminare il **Modello IPsec** selezionato. Tuttavia, non è possibile eliminare il **Modello IPsec** attualmente in uso.

- 7 Fare clic sul numero relativo al **Modello IPsec** che si desidera creare. Configurare le impostazioni IPsec nella schermata che segue, quindi creare il **Modello IPsec**. Gli elementi che è possibile impostare variano in funzione delle opzioni specificate per **Usa modello preimpostato** e **Scambio chiavi Internet (IKE)**.

**(IKE:Modello preimpostato)**



### (IKE:IKEv1)

**HL-S7000DN series** Configurare la password >> brother  
Brother Solutions Center

Informazioni generali | Stampa | Amministratore | Rete | Rete | Cablata | Wireless | Sicurezza

**Modello IPsec 1** ?

Nome modello

Usa modello preimpostato Personalizzato

Scambio chiavi Internet (IKE)  IKEv1  IKEv2  Manuale

**Tipo di autenticazione**

Gruppo Diffie-Hellman Gruppo 1

Crittografia DES

Hash MD5

Durata associazione di protezione 86600 secondi  
(240 – 63072000)  
32768 KB  
(10 – 2097152)

**Sicurezza/Incapsulamento**

Protocollo  ESP  AH

Crittografia DES

Hash MD5

Durata associazione di protezione 43200 secondi  
(120 – 4233600)

### (IKE:IKEv2)

**HL-S7000DN series** Configurare la password >> brother  
Brother Solutions Center

Informazioni generali | Stampa | Amministratore | Rete | Rete | Cablata | Wireless | Sicurezza

**Modello IPsec 1** ?

Nome modello

Usa modello preimpostato Personalizzato

Scambio chiavi Internet (IKE)  IKEv1  IKEv2  Manuale

**Tipo di autenticazione**

Gruppo Diffie-Hellman  Gruppo 1  Gruppo 2  Gruppo 5  Gruppo 14

Crittografia  DES  3DES  AES-CBC 128  AES-CBC 256

Hash  MD5  SHA1  SHA256  SHA512

Durata associazione di protezione 86600 secondi  
(240 – 63072000)  
32768 KB  
(10 – 2097152)

**Sicurezza/Incapsulamento**

Protocollo  ESP

Crittografia  DES  3DES  AES-CBC 128  AES-CBC 256

Hash  MD5  SHA1  SHA256  SHA512

■ **Nome modello**

Immettere in questa casella un nome per il modello. (massimo 16 caratteri)



### ■ Usa modello preimpostato

Selezionare **Personalizzato**, **Sicurezza elevata IKEv1**, **Sicurezza media IKEv1**, **Sicurezza elevata IKEv2** o **Sicurezza media IKEv2**. Gli elementi che è possibile impostare variano in funzione del modello selezionato.



#### Nota

Il modello predefinito varia in funzione dell'opzione (Principale o Aggressiva) selezionata come Modalità di negoziazione nella schermata delle impostazioni IPsec. Per maggiori dettagli sulla schermata delle impostazioni IPsec, vedere *Configurazione mediante Gestione basata sul Web (browser Web)*

➤➤ pagina 2.

### ■ Scambio chiavi Internet (IKE)

IKE è un protocollo di comunicazione utilizzato per lo scambio di chiavi di crittografia allo scopo di effettuare una comunicazione crittografata utilizzando il protocollo IPsec. Per poter eseguire una comunicazione crittografata unicamente per la sessione in corso, viene determinato l'algoritmo di crittografia necessario per IPsec e vengono condivise le chiavi di crittografia. Per il protocollo IKE, le chiavi di crittografia vengono scambiate mediante il metodo di scambio chiavi Diffie-Hellman, quindi viene portata a termine la comunicazione crittografata limitatamente al protocollo IKE.

Se si seleziona **Personalizzato** in **Usa modello preimpostato**, selezionare l'opzione **IKEv1**, **IKEv2** o **Manuale**.

Se si seleziona un'impostazione diversa da **Personalizzato**, viene visualizzato il tipo di autenticazione selezionato in **Usa modello preimpostato**.

### ■ Tipo di autenticazione

Consente di configurare l'autenticazione e la crittografia IKE.

#### • Gruppo Diffie-Hellman

Questo metodo di scambio chiavi consente di scambiare le chiavi in modo sicuro attraverso una rete non protetta. Il metodo di scambio chiavi Diffie-Hellman utilizza un problema di logaritmi discreti (e non la chiave segreta) per inviare e ricevere informazioni aperte generate utilizzando un numero casuale e la chiave segreta.

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **IKEv1** o **IKEv2** in **IKE**) Selezionare **Gruppo 1**, **Gruppo 2**, **Gruppo 5** o **Gruppo 14**. Se si sceglie **IKEv2**, è possibile effettuare selezioni multiple.

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **Manuale** in **IKE**) Il gruppo non viene visualizzato.

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) Il suddetto gruppo abilitato viene visualizzato.

#### • Crittografia

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **IKEv1** o **IKEv2** in **IKE**) Selezionare **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. Se si sceglie **IKEv2**, è possibile effettuare selezioni multiple.

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **Manuale** in **IKE**) La crittografia non viene visualizzata.

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) La suddetta crittografia abilitata viene visualizzata.

- **Hash**

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **IKEv1** o **IKEv2** in **IKE**) Selezionare **MD5**, **SHA1**, **SHA256** o **SHA512**. Se si sceglie **IKEv2**, è possibile effettuare selezioni multiple.

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **Manuale** in **IKE**) L'algoritmo di hash non viene visualizzato.

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) Il suddetto algoritmo di hash abilitato viene visualizzato.

- **Durata associazione di protezione**

Specificare la durata della IKE SA.

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **IKEv1** o **IKEv2** in **IKE**) Immettere il tempo (secondi) e il numero di kilobyte (KByte).

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **Manuale** in **IKE**) Le informazioni sulla durata della SA non vengono visualizzate.

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) Il tempo (secondi) e il numero di kilobyte (KByte) vengono visualizzati.

## ■ Sicurezza/Incapsulamento

- **Protocollo**

(Se si seleziona **Personalizzato** in **Usa modello preimpostato**) Selezionare **ESP** o **AH**. Se si seleziona **IKEv2** in **IKE**, è possibile selezionare soltanto **ESP**.

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) Il suddetto protocollo abilitato viene visualizzato.



### Nota

- Il protocollo ESP consente di eseguire una comunicazione crittografata utilizzando IPsec. ESP crittografa il payload (o carico utile, ovvero i contenuti oggetto della comunicazione) e aggiunge ulteriori informazioni. Il pacchetto IP è costituito dall'header e dal carico utile, che segue l'header. Oltre ai dati crittografati, il pacchetto IP contiene anche informazioni relative al metodo di crittografia e alla chiave di crittografia, ai dati di autenticazione e così via.
- L'header di autenticazione (AH) è la parte del protocollo IPsec che esegue l'autenticazione del mittente e previene la manipolazione dei dati (garantisce l'integrità dei dati). Nel pacchetto IP, i dati vengono inseriti immediatamente dopo l'header. Inoltre, i pacchetti comprendono i valori hash, che vengono calcolati utilizzando un'equazione a partire dai contenuti oggetto della comunicazione, dalla chiave segreta e così via, allo scopo di prevenire la falsificazione del mittente e la manipolazione dei dati. A differenza di quanto avviene con il protocollo ESP, i contenuti oggetto della comunicazione non sono crittografati e i dati vengono inviati e ricevuti come testo.

- **Crittografia**

(Se si seleziona **Personalizzato** in **Usa modello preimpostato**) Selezionare **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. È possibile selezionare la crittografia solo quando si seleziona **ESP** in **Protocollo**. Se si sceglie **IKEv2** in **IKE**, è possibile effettuare selezioni multiple.

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) La suddetta crittografia abilitata viene visualizzata.

- **Hash**

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **IKEv1** o **Manuale** in **IKE**) Selezionare **Nessuno**, **MD5**, **SHA1**, **SHA256** o **SHA512**. È possibile selezionare **Nessuno** solo quando si seleziona **ESP** in **Protocollo**.

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **IKEv2** in **IKE**) Selezionare **MD5**, **SHA1**, **SHA256** o **SHA512**. È possibile effettuare selezioni multiple.

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) Il suddetto tipo di algoritmo di hash abilitato viene visualizzato.

- **Durata associazione di protezione**

Specificare la durata della IKE SA.

(Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **IKEv1** o **IKEv2** in **IKE**) Immettere il tempo (secondi) e il numero di kilobyte (KByte).

(Se si seleziona un'impostazione diversa da **Personalizzato** in **Usa modello preimpostato**) Il tempo (secondi) e il numero di kilobyte (KByte) vengono visualizzati.

- **Modalità di incapsulamento**

Selezionare **Trasporto** o **Tunnel**.

- **Indirizzo IP router remoto**

Specificare l'indirizzo IP (IPv4 o IPv6) della destinazione della connessione. Immettere tale dato solo quando si seleziona la modalità **Tunnel**.



### Nota

Il metodo SA (Security Association) è un metodo di comunicazione crittografata tramite IPsec o IPv6 che consente di scambiare e condividere dati quali il metodo di crittografia e la chiave di crittografia al fine di stabilire un canale di comunicazione sicuro prima che venga avviata la comunicazione. La dicitura SA può inoltre fare riferimento a un canale di comunicazione crittografato virtuale che è stato stabilito. La SA utilizzata per IPsec stabilisce il metodo di crittografia, esegue lo scambio delle chiavi ed effettua l'autenticazione reciproca in base alla procedura IKE (Internet Key Exchange) standard. Inoltre, la SA viene aggiornata periodicamente.

- **Perfect Forward Secrecy (PFS)**

Il protocollo PFS non ricava le chiavi da quelle utilizzate in precedenza per crittografare i messaggi. Inoltre, se una chiave utilizzata per crittografare un messaggio è stata ricavata da una chiave padre, che non viene utilizzata per ricavare altre chiavi. Pertanto, anche se una chiave dovesse risultare compromessa, i danni sarebbero limitati solo ai messaggi crittografati utilizzando quella chiave.

Selezionare **Attivata** o **Disattivata**. Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **Manuale** in **IKE**, le informazioni PFS non vengono visualizzate.

- **Metodo di autenticazione**

Selezionare il metodo di autenticazione. Selezionare **Chiave precondivisa**, **Certificati**, **EAP - MD5** o **EAP - MS-CHAPv2**.

È possibile selezionare **EAP - MD5** e **EAP - MS-CHAPv2** solo quando si seleziona **IKEv2** in **IKE**. Se si seleziona **Personalizzato** in **Usa modello preimpostato** e **Manuale** in **IKE**, le informazioni relative al metodo di autenticazione non vengono visualizzate.

### ■ Chiave precondivisa

Quando la comunicazione viene crittografata, la chiave di crittografia viene scambiata e condivisa anticipatamente utilizzando un altro canale.

Se si seleziona **Chiave precondivisa** in **Metodo di autenticazione**, immettere la **Chiave precondivisa**. (massimo 32 caratteri)

#### • Locale Tipo di ID/ID

Selezionare il tipo di ID del mittente e immettere l'ID.

Selezionare **Indirizzo IPv4**, **Indirizzo IPv6**, **FQDN**, **Indirizzo e-mail** o **Certificato** come tipo.

Se si seleziona **Certificato**, immettere il nome comune del certificato in **ID**.

#### • Remoto Tipo di ID/ID

Selezionare il tipo di ID del destinatario e immettere l'ID.

Selezionare **Indirizzo IPv4**, **Indirizzo IPv6**, **FQDN**, **Indirizzo e-mail** o **Certificato** come tipo.

Se si seleziona **Certificato**, immettere il nome comune del certificato in **ID**.

### ■ Certificati

Se si seleziona **Certificati** in **Metodo di autenticazione**, selezionare il certificato.



### Nota

È possibile selezionare solo i certificati creati utilizzando la pagina **Certificato** delle funzioni di sicurezza della Gestione basata sul Web. Per maggiori dettagli, vedere la Guida dell'utente in rete: Uso dei certificati per la sicurezza del dispositivo.

### ■ EAP

EAP è un protocollo di autenticazione che costituisce un'estensione di PPP. Se si utilizza il protocollo EAP unitamente a IEEE802.1x, viene utilizzata una chiave differente per l'autenticazione utente e per ciascuna sessione.

Le seguenti impostazioni sono necessarie solo quando si seleziona **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 utente. (massimo 32 caratteri)

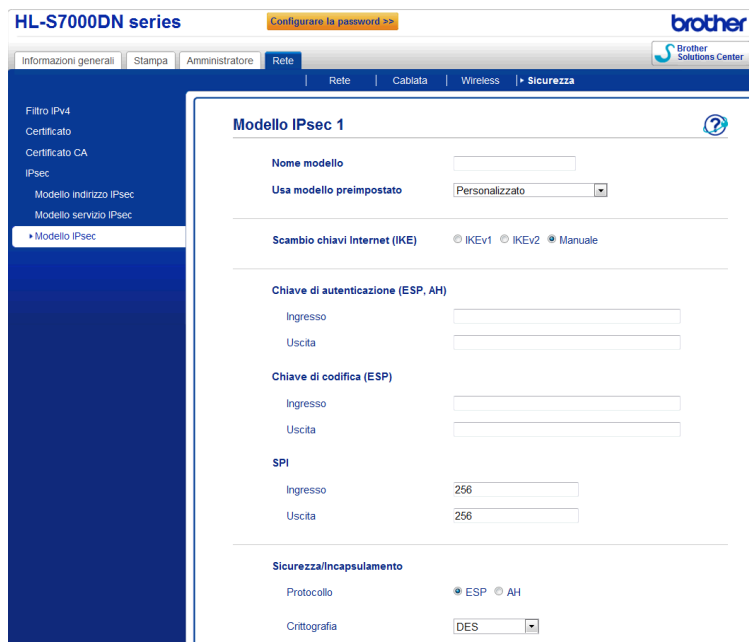
#### • Password

Immettere la password. È necessario immettere due volte la password per conferma. (massimo 32 caratteri)

- **Certificato>>**

Fare clic su questo pulsante per passare alla schermata di impostazione del certificato.

**(IKE:Manuale)**



- **Chiave di autenticazione (ESP, AH)**

Specificare la chiave da utilizzare per l'autenticazione. Immettere i valori di **Ingresso/Uscita**.

Queste impostazioni sono necessarie quando si seleziona **Personalizzato** in **Usa modello preimpostato**, **Manuale** in **IKE** e si sceglie un'impostazione diversa da **Nessuno** in **Hash** in **Sicurezza/Incapsulamento**.

 **Nota**

Il numero di caratteri che è possibile impostare varia in funzione dell'impostazione selezionata in Hash in Sicurezza/Incapsulamento.

Se la lunghezza della chiave di autenticazione specificata è diversa dall'algoritmo di hash selezionato, si verifica un errore.

- **MD5**: 128 bit (16 byte)
- **SHA1**: 160 bit (20 byte)
- **SHA256**: 256 bit (32 byte)
- **SHA512**: 512 bit (64 byte)

Quando si specifica la chiave in codice ASCII, immettere i caratteri tra virgolette.

- **Chiave di codifica (ESP)**

Specificare la chiave da utilizzare per la crittografia. Immettere i valori di **Ingresso/Uscita**.

Queste impostazioni sono necessarie quando si seleziona **Personalizzato** in **Usa modello preimpostato, Manuale** in **IKE** e si sceglie **ESP** in **Protocollo** in **Sicurezza/Incapsulamento**.

#### **Nota**

Il numero di caratteri che è possibile impostare varia in funzione dell'impostazione selezionata in Crittografia in Sicurezza/Incapsulamento.

Se la lunghezza della chiave di codifica specificata è diversa dall'algoritmo di crittografia selezionato, si verifica un 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)

Quando si specifica la chiave in codice ASCII, immettere i caratteri tra virgolette.

#### ■ **SPI**

Questi parametri si utilizzano per identificare le informazioni di sicurezza. In genere, un host dispone di più SA (Security Association) per i vari tipi di comunicazione IPsec. Pertanto, è necessario identificare la SA valida nel momento in cui viene ricevuto un pacchetto IPsec. Il parametro SPI, che identifica la SA, è incluso nell'header di autenticazione (AH) e nell'header ESP (Encapsulating Security Payload).

Queste impostazioni sono necessarie quando si seleziona **Personalizzato** in **Usa modello preimpostato e Manuale** in **IKE**.

Immettere i valori di **Ingresso/Uscita**. (3-10 caratteri)

#### ■ **Invia**

Fare clic su questo pulsante per registrare le impostazioni.

#### **Nota**

Quando si modificano le impostazioni del modello attualmente in uso, la schermata delle impostazioni IPsec della Gestione basata sul Web viene chiusa e riaperta.

## Modelli dei servizi

È possibile utilizzare i seguenti servizi selezionando i rispettivi modelli.

### 1 Tutti i servizi

Per tutti i protocolli viene utilizzato IPsec.

### 2 Servizi di stampa

| Nome del servizio | Protocollo | Porta locale | Porta remota |
|-------------------|------------|--------------|--------------|
| IPP               | TCP        | 631          | Qualsiasi    |
| IPPS              | TCP        | 443          | Qualsiasi    |
| FTP (controllo)   | TCP        | 21           | Qualsiasi    |
| FTP (dati)        | TCP        | 20           | Qualsiasi    |
| P9100             | TCP        | 9100         | Qualsiasi    |
| Servizi Web       | TCP        | 80           | Qualsiasi    |
| LPD               | TCP        | 515          | Qualsiasi    |

### 3 Servizi di gestione

| Nome del servizio   | Protocollo | Porta locale | Porta remota |
|---------------------|------------|--------------|--------------|
| SNMP                | UDP        | 161          | Qualsiasi    |
| Telnet              | TCP        | 23           | Qualsiasi    |
| HTTP                | TCP        | 80           | Qualsiasi    |
| HTTPS               | TCP        | 443          | Qualsiasi    |
| Impostazione remota | TCP        | 54922        | Qualsiasi    |

### 4 Servizi stampante/MFC <sup>1</sup>

| Nome del servizio | Protocollo | Porta locale | Porta remota |
|-------------------|------------|--------------|--------------|
| CIFS              | TCP        | Qualsiasi    | 445          |
| SMB               | TCP        | Qualsiasi    | 139          |
| LDAP              | TCP        | Qualsiasi    | 389          |
| SMTP              | TCP        | Qualsiasi    | 25           |
| POP3              | TCP        | Qualsiasi    | 110          |
| SNTP              | UDP        | Qualsiasi    | 123          |
| Scansione rete    | TCP        | 54921        | Qualsiasi    |
| PC-FAX            | TCP        | 54923        | Qualsiasi    |

| Nome del servizio | Protocollo | Porta locale | Porta remota |
|-------------------|------------|--------------|--------------|
| Kerberos (TCP)    | TCP        | Qualsiasi    | 88           |
| Kerberos (UDP)    | UDP        | Qualsiasi    | 88           |

<sup>1</sup> Per utilizzare l'autenticazione Kerberos, è necessario attivare le impostazioni DNS appropriate.

## Tipo/Codice

Quando si seleziona **ICMP** in **Protocollo**, sono supportati i tipi e i codici elencati di seguito.

| IPv4 |   |                              |
|------|---|------------------------------|
| Tipo |   | Codici supportati            |
| 0    | Echo Reply                              | 0                            |
| 3    | Destination Unreachable                 | 0,1,2,3,4,5,6,7,8,9,10,11,12 |
| 4    | Richiesta di rallentamento dell'origine | 0                            |
| 5    | Redirect                                | 0,1,2,3                      |
| 8    | Echo Request                            | 0                            |
| 9    | Router Advertisement                    | 0                            |
| 10   | Router Solicitations                    | 0                            |

Codice IPv4

0,1,2,3,4,5,6,7,8,9,10,11,12

| IPv6 |                         |                   |
|------|-------------------------|-------------------|
| Tipo |                         | Codici supportati |
| 1    | Destination Unreachable | 0,1,2,3,4         |
| 3    | Time Exceeded           | 0,1               |
| 4    | Parameter Problem       | 0,1,2             |
| 128  | Echo Request            | 0                 |
| 129  | Echo Reply              | 0                 |
| 133  | Router Solicitation     | 0                 |
| 134  | Router Advertisement    | 0                 |
| 135  | Neighbor Solicitation   | 0                 |
| 136  | Neighbor Advertisement  | 0                 |
| 137  | Redirect                | 0                 |

Codice IPv6

0,1,2,3,4



**brother**<sup>®</sup>

**Visitate il sito Brother sul World Wide Web  
<http://www.brother.com/>**



[www.brotherearth.com](http://www.brotherearth.com)