EPSON
EXCEED YOUR VISION

# Guida per amministratore

NPD5668-00 IT

# Sommario

## Copyright

## Marchi

## Informazioni su questo manuale

Contrassegni e simboli. . . . . 6
Descrizioni utilizzate nel manuale. . . . . 6
Riferimenti per i sistemi operativi. . . . . 6

## Introduzione

Componenti del manuale. . . . . 8
Definizioni dei termini utilizzati in questa Guida. . . . 8

## Preparazione

Flusso delle impostazioni e della gestione dello scanner. . . . . 10
Esempio di ambiente di rete. . . . . 11
Introduzione di un esempio di impostazione di connessione dello scanner. . . . . 11
Preparazione della connessione a una rete. . . . . 12
Raccolta di informazioni sull'impostazione di connessione. . . . . 12
Specifiche dello scanner. . . . . 13
Utilizzo del numero di porta. . . . . 13
Tipo di assegnazione dell'indirizzo IP. . . . . 13
Server DNS e Server proxy. . . . . 13
Metodo di impostazione della connessione di rete. . . . . 13

## Connessione

Connessione alla rete. . . . . 15
Connessione alla rete dal Pannello di controllo. . 15
Connessione alla rete tramite il programma di installazione. . . . . 19

## Impostazioni delle funzioni

Software per la configurazione. . . . . 22
Web Config (pagina web per il dispositivo). . . . . 22
Utilizzo delle funzioni di scansione. . . . . 24
Scansione da computer. . . . . 24
Scansione tramite il pannello di controllo. . . . . 26
Configurazione delle impostazioni di sistema. . . . . 28
Configurazione delle impostazioni di sistema dal pannello di controllo. . . . . 28
Configurazione delle impostazioni di sistema tramite Web Config. . . . . 30

## Impostazioni di sicurezza di base

Introduzione delle funzioni di sicurezza di base. . . . 32
Configurazione della password di amministratore. . 33
Configurazione della password di amministratore dal pannello di controllo. . . . . 33
Configurazione della password di amministratore tramite Web Config. . . . . 33
Voci da bloccare con la password di amministratore. . . . . 34
Controllo dei protocolli. . . . . 35
Protocolli che si possono abilitare o disabilitare. . 36
Voci di impostazione del protocollo. . . . . 37

## Impostazioni di funzionamento e gestione

Conferma delle informazioni relative a un dispositivo. . . . . 40
Gestione dei dispositivi (Epson Device Admin). . . . 40
Ricezione di notifiche email al verificarsi di eventi. . 41
Notifiche e-mail. . . . . 41
Configurazione delle notifiche e-mail. . . . . 41
Configurazione di un server di posta. . . . . 42
Verifica della connessione al server di posta. . . . 44
Aggiornamento del firmware. . . . . 46
Aggiornamento del firmware tramite Web Config. . . . . 46
Aggiornamento del firmware tramite Epson Firmware Updater. . . . . 46
Backup delle impostazioni. . . . . 47
Esportazione delle impostazioni. . . . . 47
Importazione delle impostazioni. . . . . 47

## Risoluzione dei problemi

Suggerimenti per la risoluzione dei problemi. . . . . 49
Controllo del registro del server e del dispositivo di rete. . . . . 49
Inizializzazione delle impostazioni di rete. . . . . 49
Ripristino delle impostazioni di rete dal pannello di controllo. . . . . 49

**Sommario**

Verifica della comunicazione tra dispositivi e computer. . . . . .49
Verifica della connessione tramite un comando Ping — Windows. . . . . .49
Verifica della connessione tramite un comando Ping — Mac OS. . . . . .51
Problemi con il software di rete. . . . . .52
Impossibile accedere a Web Config. . . . . 52
Il nome di modello e/o l'indirizzo IP non vengono visualizzati in EpsonNet Config. . . . . .53

## *Appendice*

Introduzione del software di rete. . . . . .55
Epson Device Admin. . . . . 55
EpsonNet Config. . . . . 55
EpsonNet SetupManager. . . . . 56
Assegnazione di un indirizzo IP tramite EpsonNet Config. . . . . 56
Assegnazione dell'indirizzo IP tramite le impostazioni batch. . . . . .56
Assegnazione di un indirizzo IP a ciascun dispositivo. . . . . .59
Utilizzo della porta per lo scanner. . . . . .60

## *Impostazioni di sicurezza avanzate per Enterprise*

Impostazioni di sicurezza e prevenzione del pericolo. . . . . .62
Impostazioni delle funzioni di sicurezza. . . . . 63
Comunicazione SSL/TLS con lo scanner. . . . . 63
Informazioni sulla certificazione digitale. . . . . .63
Ottenimento e importazione di un certificato firmato CA. . . . . 64
Eliminazione di un certificato firmato CA. . . . . .67
Aggiornamento di un certificato auto-firmato. . . 68
Configurazione di Certificato CA. . . . . 69
Comunicazione crittografata tramite IPsec/IP Filtering. . . . . 71
Informazioni su IPsec/Filtro IP. . . . . .71
Configurazione di Criteri predefiniti. . . . . .72
Configurazione di Criteri gruppo. . . . . 75
Esempi di configurazione di IPsec/Filtro IP. . . . . 81
Configurazione di un certificato per IPsec/ Filtro IP. . . . . .82
Uso del protocollo SNMPv3. . . . . 83
Informazioni su SNMPv3. . . . . .83
Configurazione SNMPv3. . . . . 83
Connessione dello scanner a una rete IEEE802.1X. . 85
Configurazione di una rete IEEE802.1X. . . . . 85
Configurazione di un certificato per IEEE802.1X. . . . . .86
Risoluzione dei problemi per la sicurezza avanzata. .87
Ripristino delle impostazioni di sicurezza. . . . . 87
Problemi utilizzando le funzioni di sicurezza di rete. . . . . 88
Problema con l'uso di un certificato digitale. . . . .90

# Copyright

# Marchi

- ❏ EPSON® è un marchio registrato mentre EPSON EXCEED YOUR VISION o EXCEED YOUR VISION sono marchi di Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Avviso generale: gli altri nomi di prodotto qui riportati sono utilizzati solo a scopo identificativo e possono essere marchi dei rispettivi proprietari. Epson non rivendica alcun diritto su tali marchi.

# Informazioni su questo manuale

## Contrassegni e simboli

***Attenzione:***
*Istruzioni da seguire attentamente per evitare lesioni personali.*

***Importante:***
*Istruzioni da osservare per evitare danni alle apparecchiature.*

***Nota:***
*Istruzioni contenenti suggerimenti utili e limitazioni sull'uso dello scanner.*

### Informazioni correlate

➡ Facendo clic su questa icona, si passa alle informazioni correlate.

## Descrizioni utilizzate nel manuale

❏ Le schermate del driver dello scanner e di Epson Scan 2 (driver dello scanner) incluse nel presente manuale provengono da sistemi Windows 10 o OS X El Capitan. Il contenuto visualizzato nelle schermate varia a seconda del modello in uso e del contesto.

❏ Le illustrazioni usate nel presente manuale sono solo esempi. È possibile che non corrispondano esattamente al modello in uso, tuttavia il funzionamento è identico.

❏ Alcune voci di menu nella schermata del display LCD variano a seconda del modello in uso e delle impostazioni configurate.

## Riferimenti per i sistemi operativi

### Windows

In questo manuale, termini quali “Windows 10”, “Windows 8.1”, “Windows 8”, “Windows 7”, “Windows Vista”, “Windows XP”, Windows Server 2016, “Windows Server 2012 R2”, “Windows Server 2012”, “Windows Server 2008 R2”, “Windows Server 2008”, “Windows Server 2003 R2” e “Windows Server 2003” fanno riferimento ai seguenti sistemi operativi. Inoltre, il termine “Windows” viene utilizzato per tutte le versioni del sistema operativo.

❏ Sistema operativo Microsoft® Windows® 10

❏ Sistema operativo Microsoft® Windows® 8.1

❏ Sistema operativo Microsoft® Windows® 8

❏ Sistema operativo Microsoft® Windows® 7

❏ Sistema operativo Microsoft® Windows Vista®

- ❏ Sistema operativo Microsoft® Windows® XP
- ❏ Sistema operativo Microsoft® Windows® XP Professional x64 Edition
- ❏ Sistema operativo Microsoft® Windows Server® 2016
- ❏ Sistema operativo Microsoft® Windows Server® 2012 R2
- ❏ Sistema operativo Microsoft® Windows Server® 2012
- ❏ Sistema operativo Microsoft® Windows Server® 2008 R2
- ❏ Sistema operativo Microsoft® Windows Server® 2008
- ❏ Sistema operativo Microsoft® Windows Server® 2003 R2
- ❏ Sistema operativo Microsoft® Windows Server® 2003

### Mac OS

In questo manuale, il termine "Mac OS" viene utilizzato per fare riferimento a macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x e Mac OS X v10.6.8.

# Introduzione

## Componenti del manuale

Questo manuale è rivolto all'amministratore del dispositivo che ha il compito di collegare la stampante o lo scanner alla rete e contiene informazioni su come effettuare le impostazioni di utilizzo delle funzioni.

Per informazioni sull'utilizzo della funzione, consultare la *Guida utente*.

### Preparazione

Spiega i compiti dell'amministratore, come impostare i dispositivi e il software di gestione.

### Connessione

Spiega come collegare un dispositivo alla rete o alla linea telefonica. Inoltre, contiene informazioni sull'ambiente di rete, come l'utilizzo di una porta per il dispositivo, e sui server DNS e proxy.

### Impostazioni delle funzioni

Spiega le impostazioni per ciascuna funzione del dispositivo.

### Impostazioni di sicurezza di base

Spiega le impostazioni per ogni funzione, come la stampa, la scansione e l'invio di fax.

### Impostazioni di funzionamento e gestione

Spiega le operazioni relative al primo utilizzo dei dispositivi, quali la verifica delle informazioni e la manutenzione.

### Risoluzione dei problemi

Spiega l'inizializzazione delle impostazioni e la risoluzione dei problemi della rete.

### Impostazioni di sicurezza avanzate per Enterprise

Spiega il metodo di impostazione per il miglioramento della sicurezza del dispositivo, come l'utilizzo di un certificato CA, la comunicazione SSL/TLS e IPsec/IP Filtering.

A seconda del modello, alcune delle funzioni contenute in questo capitolo non sono supportate.

## Definizioni dei termini utilizzati in questa Guida

Nella presente guida vengono utilizzati i seguenti termini.

### Amministratore

Persona incaricata di installare e configurare il dispositivo o la rete in un ufficio o un'organizzazione. Per le organizzazioni di piccole dimensioni, questa persona può essere responsabile dell'amministrazione del dispositivo e della rete. Per le organizzazioni di grandi dimensioni, gli amministratori hanno autorità sulla rete o sui dispositivi sull'unità di gruppo di un dipartimento o una divisione, mentre gli amministratori di rete sono responsabili delle impostazioni di comunicazione al di fuori dell'organizzazione, come Internet.

### Amministratore di rete

Persona incaricata di controllare la comunicazione di rete. È la persona che ha configurato il router, il server proxy, il server DNS e il server di posta elettronica per controllare la comunicazione attraverso Internet o la rete.

### Utente

Persona che utilizza dispositivi quali stampanti o scanner.

### Web Config (pagina web del dispositivo)

Server web integrato nel dispositivo. È denominato Web Config. Qui è possibile verificare e modificare lo stato del dispositivo tramite il browser.

### Strumento

Termine generico che indica il software di configurazione o gestione di un dispositivo, come per esempio Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, ecc.

### Scansione Push

Termine generico che indica la scansione dal pannello di controllo del dispositivo.

### ASCII (American Standard Code for Information Interchange)

Uno dei codici di carattere standard. Vengono definiti 128 caratteri, tra cui lettere dell'alfabeto (a–z, A–Z), numeri arabi (0–9), simboli, caratteri di spazio e caratteri di controllo. Quando in questa guida viene fatto riferimento ad "ASCII", si indica 0x20–0x7E (numero esadecimale) elencato di seguito e non si includono i caratteri di controllo.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SP* | ! | " | # | $ | % | & | ' | ( | ) | * | + | , | - | . | / |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = | > | ? |
| @ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| P | Q | R | S | T | U | V | W | X | Y | Z | [ | \ | ] | ^ | _ |
| ` | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| p | q | r | s | t | u | v | w | x | y | z | { | \| | } | ~ | |

* Carattere di spazio.

### Unicode (UTF-8)

Un codice standard internazionale, che copre le principali lingue mondiali. Quando in questa guida viene fatto riferimento a "UTF-8", si indica la codifica caratteri in formato UTF-8.

# Preparazione

Questo capitolo spiega il ruolo dell'amministratore e la fase di preparazione prima di effettuare le impostazioni.

## Flusso delle impostazioni e della gestione dello scanner

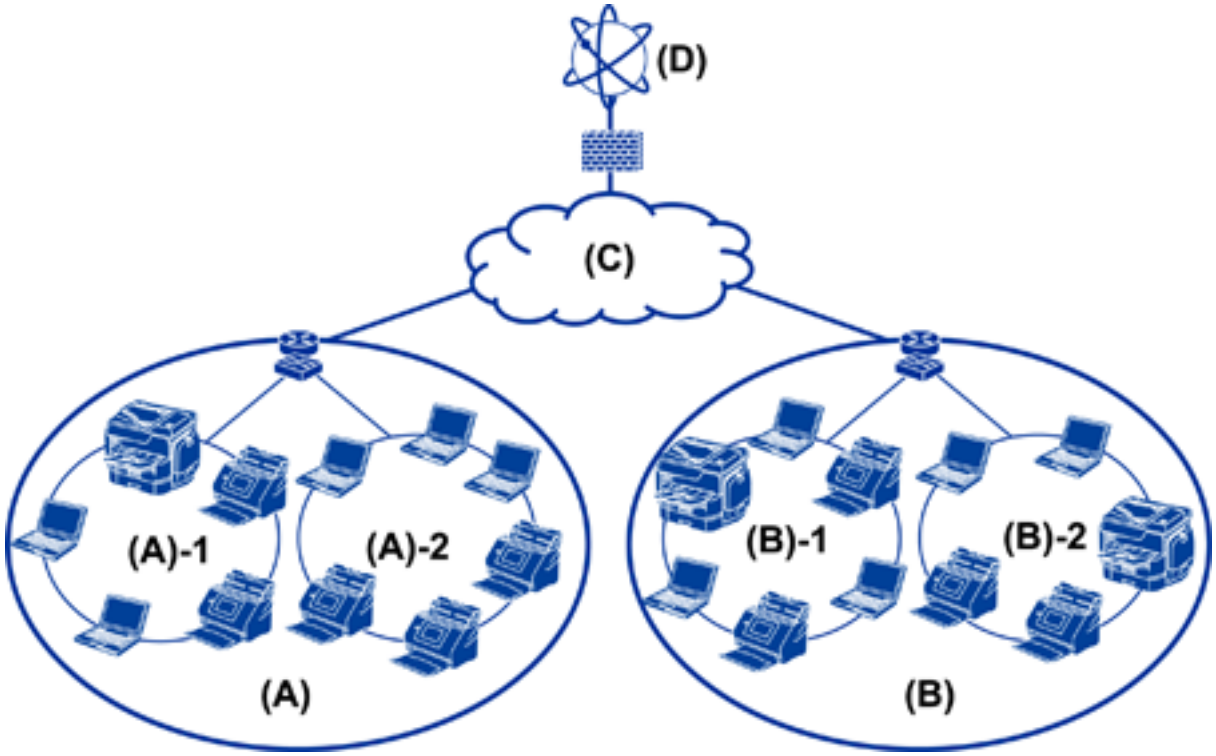
L'amministratore effettua le impostazioni della connessione di rete, la configurazione iniziale e la manutenzione dello scanner in modo da renderli disponibili agli utenti.

1. Preparazione
   - ❏ Raccolta delle informazioni relative alle impostazioni di connessione
   - ❏ Scelta del metodo di connessione
2. Connessione
   - ❏ Connessione alla rete dal pannello di controllo dello scanner
3. Impostazione delle funzioni
   - ❏ Impostazioni del driver dello scanner
   - ❏ Altre impostazioni avanzate
4. Impostazioni di sicurezza
   - ❏ Impostazioni di amministrazione
   - ❏ SSL/TLS
   - ❏ Controllo dei protocolli
   - ❏ Impostazioni di sicurezza avanzate (opzionali)
5. Funzionamento e gestione
   - ❏ Controllo dello stato del dispositivo
   - ❏ Emergenza di gestione degli eventi
   - ❏ Backup delle impostazioni del dispositivo

### Informazioni correlate

➡ “Preparazione” a pagina 10
➡ “Connessione” a pagina 15
➡ “Impostazioni delle funzioni” a pagina 22
➡ “Impostazioni di sicurezza di base” a pagina 32
➡ “Impostazioni di funzionamento e gestione” a pagina 40

# Esempio di ambiente di rete




(A): Ufficio 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Ufficio 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

## Introduzione di un esempio di impostazione di connessione dello scanner

Esistono principalmente due tipi di connessione a seconda della modalità di utilizzo dello scanner. Entrambe consentono di collegare lo scanner alla rete con il computer mediante l'hub.

❏ Connessione server/client (scanner con server Windows, gestione dei lavori)

❏ Connessione peer to peer (connessione diretta mediante computer client)

### Informazioni correlate

➡ “Connessione server/client” a pagina 12

➡ “Connessione peer to peer” a pagina 12

## Connessione server/client

Centralizzare la gestione dello scanner e dei lavori installando Document Capture Pro Server sul server. È adatta soprattutto a un lavoro che utilizza più scanner per effettuare la scansione di un grande numero di documenti in un determinato formato.

### Informazioni correlate

➡ "Definizioni dei termini utilizzati in questa Guida" a pagina 8

## Connessione peer to peer

Utilizzare uno scanner singolo con un relativo driver come Epson Scan 2 installato sul computer client. Installando Document Capture Pro (Document Capture) sul computer client è possibile gestire i lavori sui singoli computer client dello scanner.

### Informazioni correlate

➡ "Definizioni dei termini utilizzati in questa Guida" a pagina 8

# Preparazione della connessione a una rete

## Raccolta di informazioni sull'impostazione di connessione

Per la connessione di rete è necessario disporre di un indirizzo IP, un indirizzo gateway, ecc. Controllare in anticipo quanto segue.

| Divisioni | Elementi | Nota |
|---|---|---|
| Metodo di connessione del dispositivo | ❏ Ethernet | Utilizzare un cavo STP (Shielded Twisted Pair, Schermato a coppie intrecciate) di categoria 5e o superiore per la connessione Ethernet. |
| Informazioni sulla connessione LAN | ❏ Indirizzo IP<br>❏ Maschera di sottorete<br>❏ Gateway predefinito | Se si imposta automaticamente l'indirizzo IP utilizzando la funzione DHCP del router, non è necessario. |
| Informazioni sul server DNS | ❏ Indirizzo IP per DNS primario<br>❏ Indirizzo IP per DNS secondario | Se si utilizza un indirizzo IP statico, come l'indirizzo IP, configurare il server DNS.<br>Configurare quando effettuare l'assegnazione automatica tramite la funzione DHCP e quando il server DNS non può essere assegnato automaticamente. |
| Informazioni sul server proxy | ❏ Nome del server proxy<br>❏ Numero di porta | Configurare se si utilizza un server proxy per la connessione a Internet e se si utilizza il servizio Epson Connect o la funzione di aggiornamento automatico del firmware. |

# Specifiche dello scanner

La specifica che lo scanner supporta la modalità standard o di connessione, vedere la *Guida utente*.

# Utilizzo del numero di porta

Consultare l'"Appendice" per il numero di porta utilizzato dallo scanner.

### Informazioni correlate

➡ "Utilizzo della porta per lo scanner" a pagina 60

# Tipo di assegnazione dell'indirizzo IP

Ci sono due tipi di assegnazione di un indirizzo IP allo scanner.

### Indirizzo IP statico:

Assegnare l'indirizzo IP univoco predeterminato allo scanner.

L'indirizzo IP non viene modificato nemmeno quando si spegne lo scanner o il router, in modo che sia possibile gestire il dispositivo tramite l'indirizzo IP.

Questo tipo è adatto a una rete in cui vengono gestiti molti scanner, come un grande ufficio o una scuola.

### Assegnazione automatica tramite la funzione DHCP:

L'indirizzo IP corretto viene assegnato automaticamente quando la comunicazione tra lo scanner e il router che supporta la funzione DHCP avviene correttamente.

Se è scomodo modificare l'indirizzo IP per un dispositivo particolare, prenotare l'indirizzo IP in anticipo e poi assegnarlo.

# Server DNS e Server proxy

Se si utilizza un servizio di connessione a Internet, configurare il server DNS. In caso di mancata configurazione, è necessario specificare l'indirizzo IP per l'accesso poiché la risoluzione dei nomi potrebbe essere errata.

Il server proxy è posizionato in corrispondenza del gateway tra la rete e Internet e comunica con il computer, lo scanner e Internet (server opposto) per conto di ciascuno di essi. Il server opposto comunica solo con il server proxy. Pertanto, le informazioni sullo scanner quali l'indirizzo IP e il numero di porta sono illeggibili e ciò dovrebbe comportare una maggiore sicurezza.

È possibile vietare l'accesso a un URL specifico utilizzando la funzione di filtraggio, poiché il server proxy è in grado di controllare il contenuto della comunicazione.

# Metodo di impostazione della connessione di rete

Procedere come segue per effettuare le impostazioni di connessione per l'indirizzo IP dello scanner, la maschera di sottorete e il gateway predefinito.

### Dal pannello di controllo:

Configurare le impostazioni dal pannello di controllo dello scanner per ciascuno scanner. Connettersi alla rete una volta configurate le impostazioni di connessione dello scanner.

### Tramite il programma di installazione:

Se si utilizza il programma di installazione, la rete dello scanner e il computer client vengono impostati automaticamente. L'impostazione è disponibile seguendo le istruzioni del programma di installazione, anche se non si dispone di una conoscenza approfondita della rete.

### Tramite uno strumento:

Utilizzare uno strumento dal computer dell'amministratore. È possibile rilevare uno scanner e impostarlo, oppure creare un file SYLK per applicare le impostazioni batch agli scanner. È possibile impostare una serie di scanner, a condizione che siano connessi fisicamente tramite il cavo Ethernet. Pertanto, questa operazione è consigliata se si può costruire una rete Ethernet per l'impostazione.

### Informazioni correlate

➡ “Connessione alla rete dal Pannello di controllo” a pagina 15

➡ “Connessione alla rete tramite il programma di installazione” a pagina 19

➡ “Assegnazione di un indirizzo IP tramite EpsonNet Config” a pagina 56

# Connessione

Questo capitolo illustra l'ambiente o la procedura necessari per collegare lo scanner alla rete.

# Connessione alla rete

## Connessione alla rete dal Pannello di controllo

Collegare lo scanner alla rete tramite il pannello di controllo dello scanner.

Per ulteriori dettagli relativi al pannello di controllo dello scanner, consultare la *Guida utente*.

### Assegnazione dell'indirizzo IP

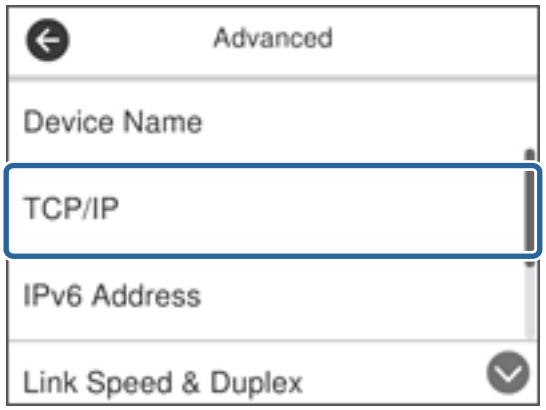
Impostare le voci di base come Indirizzo IP, Subnet Mask e Gateway predefinito.

1. Accendere lo scanner.
2. Scorrere la schermata verso sinistra sul pannello di controllo dello scanner, quindi toccare **Impostazioni**.

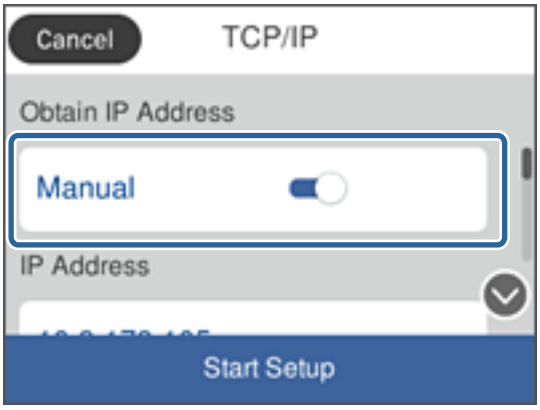

3. Toccare **Impostazioni di rete** > **Modifica impostazioni**.

   Se la voce non appare, scorrere la schermata verso l'alto per visualizzarla.

4. Toccare **TCP/IP**.

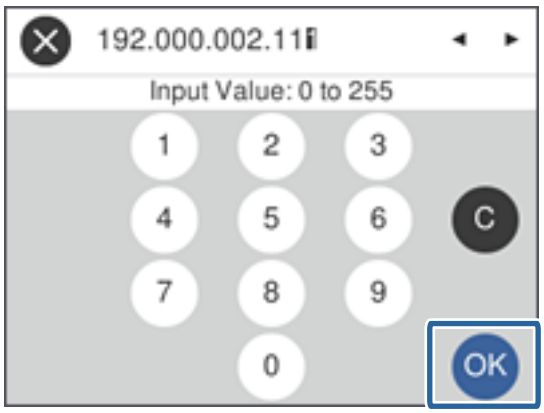



5. Selezionare **Manuale** per **Ottieni indirizzo IP**.




***Nota:***
*Quando si imposta l'indirizzo IP automaticamente tramite la funzione DHCP del router, selezionare* ***Automatico****. In tal caso, vengono impostati automaticamente anche* ***Indirizzo IP****,* ***Subnet Mask*** *e* ***Gateway predefinito*** *nei passaggi da 6 a 7, quindi andare al passaggio 8.*

6. Fare clic sul campo **Indirizzo IP**, immettere l'indirizzo IP tramite la tastiera visualizzata sullo schermo, quindi toccare **OK**.




Confermare il valore visualizzato sulla schermata precedente.

7. Impostare i valori per **Subnet Mask** e **Gateway predefinito**.

   Confermare il valore visualizzato sulla schermata precedente.

   ***Nota:***
   *Se la combinazione di Indirizzo IP, Subnet Mask e Gateway predefinito non è corretta, **Avvia configuraz.** è inattivo e non può effettuare le impostazioni. Verificare che non vi sia alcun errore nella voce inserita.*

8. Fare clic sul campo **DNS principale** per il **Server DNS**, immettere l'indirizzo IP per il server DNS primario tramite la tastiera visualizzata sullo schermo, quindi toccare **OK**.

   Confermare il valore visualizzato sulla schermata precedente.

   ***Nota:***
   *Quando si seleziona **Automatico** per le impostazioni di assegnazione dell'indirizzo IP, è possibile selezionare le impostazioni del server DNS da **Manuale** o **Automatico**. Se non è possibile ottenere automaticamente l'indirizzo del server DNS, selezionare **Manuale** e inserire l'indirizzo del server DNS. Quindi, inserire direttamente l'indirizzo del server DNS secondario. Se si seleziona **Automatico**, andare al passaggio 10.*

9. Fare clic sul campo **DNS secondario**, immettere l'indirizzo IP per il server DNS secondario tramite la tastiera visualizzata sullo schermo, quindi toccare **OK**.

   Confermare il valore visualizzato sulla schermata precedente.

10. Toccare **Avvia configuraz.**.

11. Toccare **Chiudi** sulla schermata di conferma.

    Se non si tocca **Chiudi**, la schermata si chiude automaticamente dopo un determinato periodo di tempo.

## Connessione a Ethernet

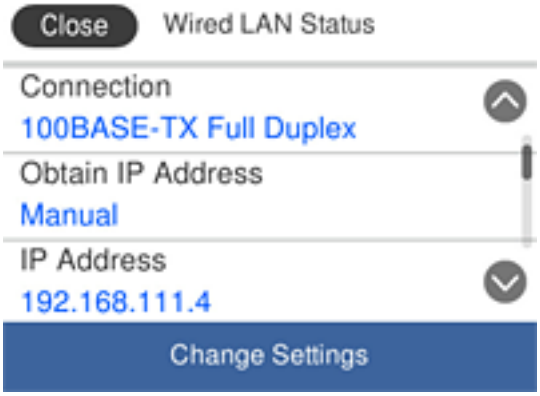
Collegare lo scanner alla rete utilizzando il cavo Ethernet e verificare la connessione.

1. Collegare lo scanner e l'hub (interruttore L2) tramite un cavo Ethernet.

   L'icona nella schermata iniziale diventa  .

2. Toccare  nella schermata iniziale.

3. Scorrere la schermata verso l'alto, quindi accertarsi che lo stato della connessione e l'indirizzo IP siano corretti.



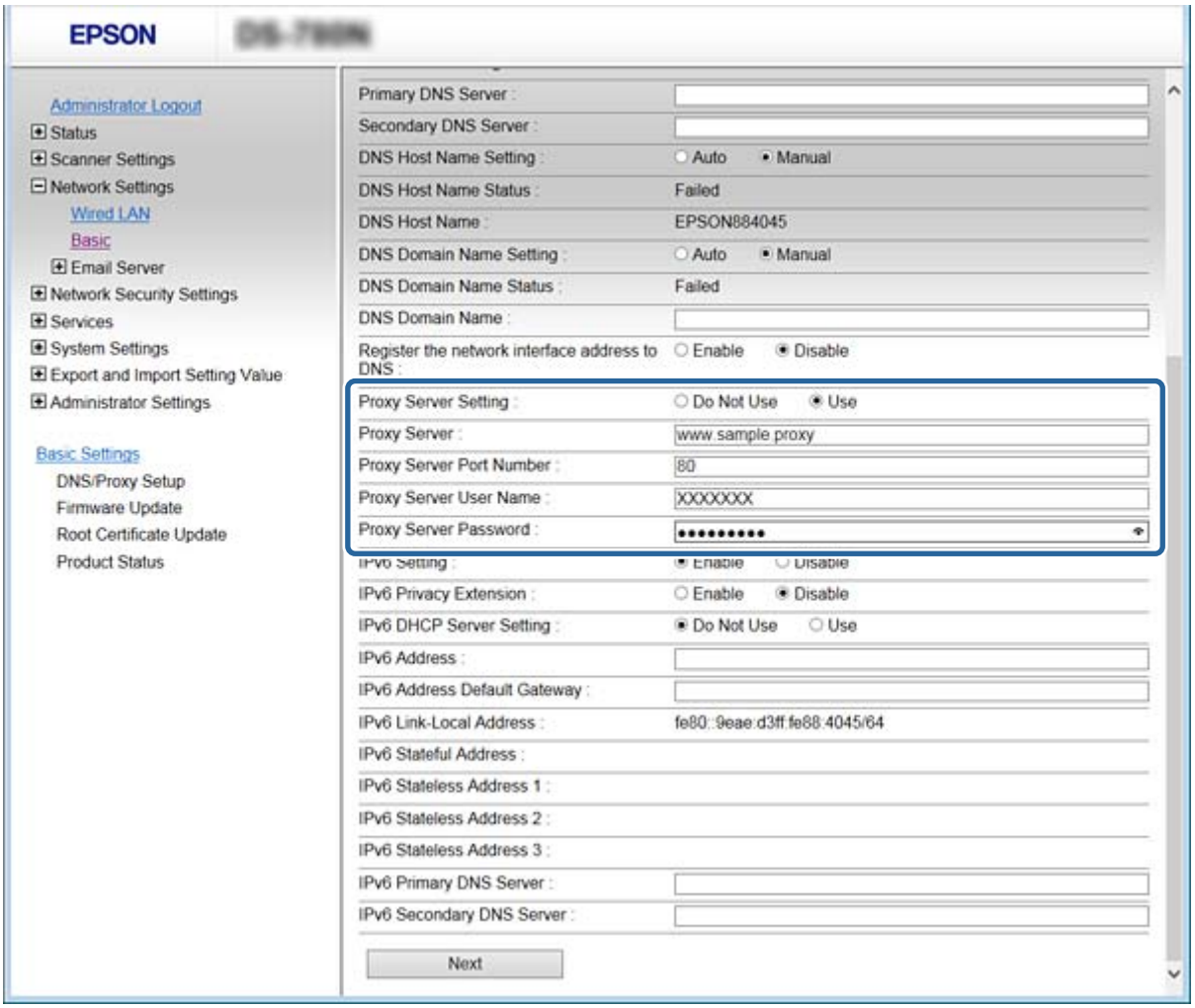

## Configurazione del server proxy

Il server proxy non può essere configurato sul pannello. Configurare tramite Web Config.

1. Accedere a Web Config e selezionare **Impostazioni di rete** > **Di base**.
2. Selezionare **Usa** in **Impostazione server proxy**.
3. Specificare il server proxy utilizzando un indirizzo IPv4 o in formato FQDN in **Server Proxy**, quindi inserire il numero di porta in **Numero porta server Proxy**.

   Per i server proxy che richiedono l'autenticazione, inserire il nome utente e la password per l'autenticazione al server Proxy.

4. Fare clic sul pulsante **Avanti**.




5. Confermare le impostazioni, quindi fare clic su **Impostazioni**.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Connessione alla rete tramite il programma di installazione

Si consiglia di utilizzare il programma di installazione per collegare lo scanner al computer. Per avviare il programma di installazione, seguire uno dei metodi indicati.

❏ Impostazione dal sito web

Accedere al seguente sito web, quindi immettere il nome del prodotto. Andare su **Impostazione**, quindi avviare la procedura di impostazione.

http://epson.sn

❏ Impostazione tramite il disco del software (solo per i modelli dotati di un disco software e per gli utenti in possesso di computer con unità di lettura disco.)

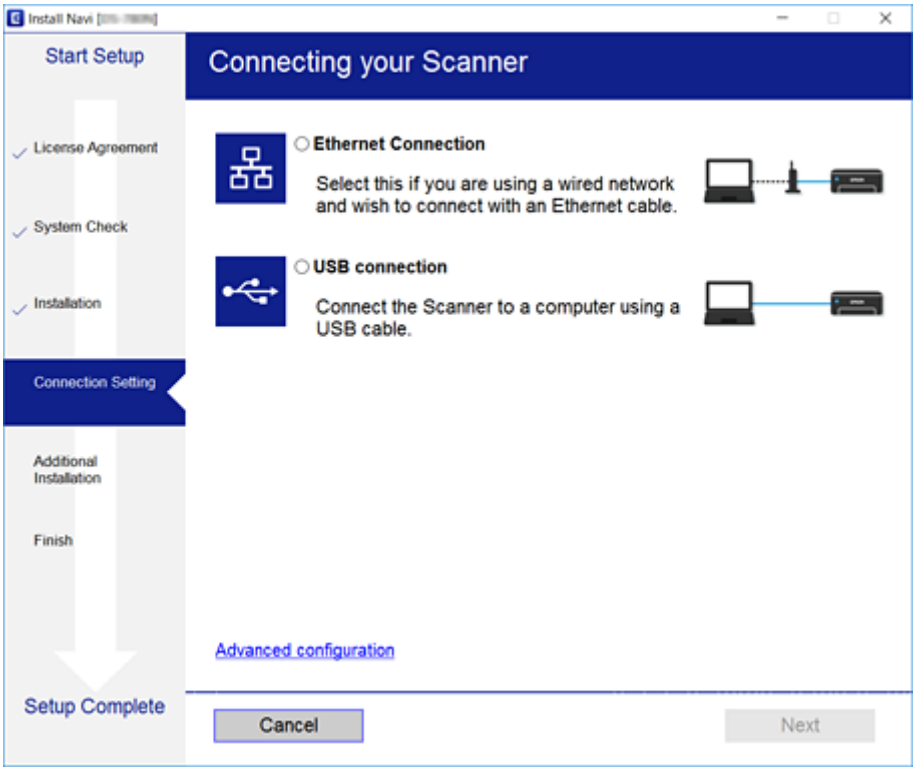
Inserire nel computer il disco del software e seguire le istruzioni visualizzate sullo schermo.

## Selezione dei metodi di connessione

Seguire le istruzioni visualizzate sullo schermo fino a quando viene visualizzata la schermata successiva, quindi selezionare il metodo di connessione dello scanner al computer.

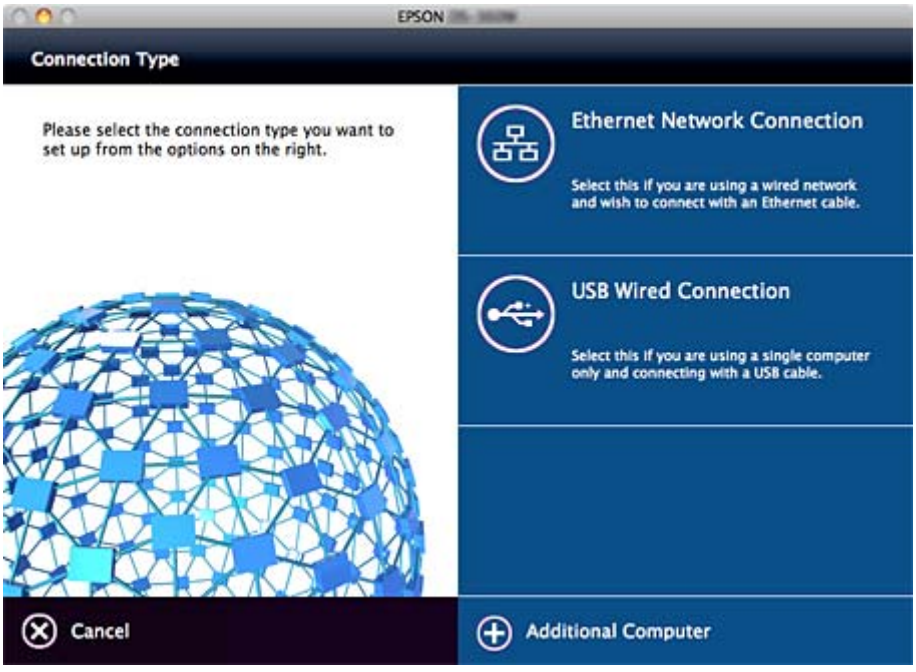
❏ Windows

Selezionare il tipo di connessione, quindi fare clic su **Avanti**.




❏ Mac OS

Selezionare il tipo di connessione.



**Connessione**

Seguire le istruzioni visualizzate sullo schermo. Il software viene installato.

# Impostazioni delle funzioni

In questo capitolo sono illustrate le prime impostazioni da effettuare per poter utilizzare il dispositivo in tutte le sue funzioni.

# Software per la configurazione

In questa sezione, viene illustrata la procedura per effettuare le impostazioni dal computer dell'amministratore tramite Web Config.

## Web Config (pagina web per il dispositivo)

### Informazioni su Web Config

Web Config è un'applicazione basata su browser per la configurazione delle impostazioni dello scanner.

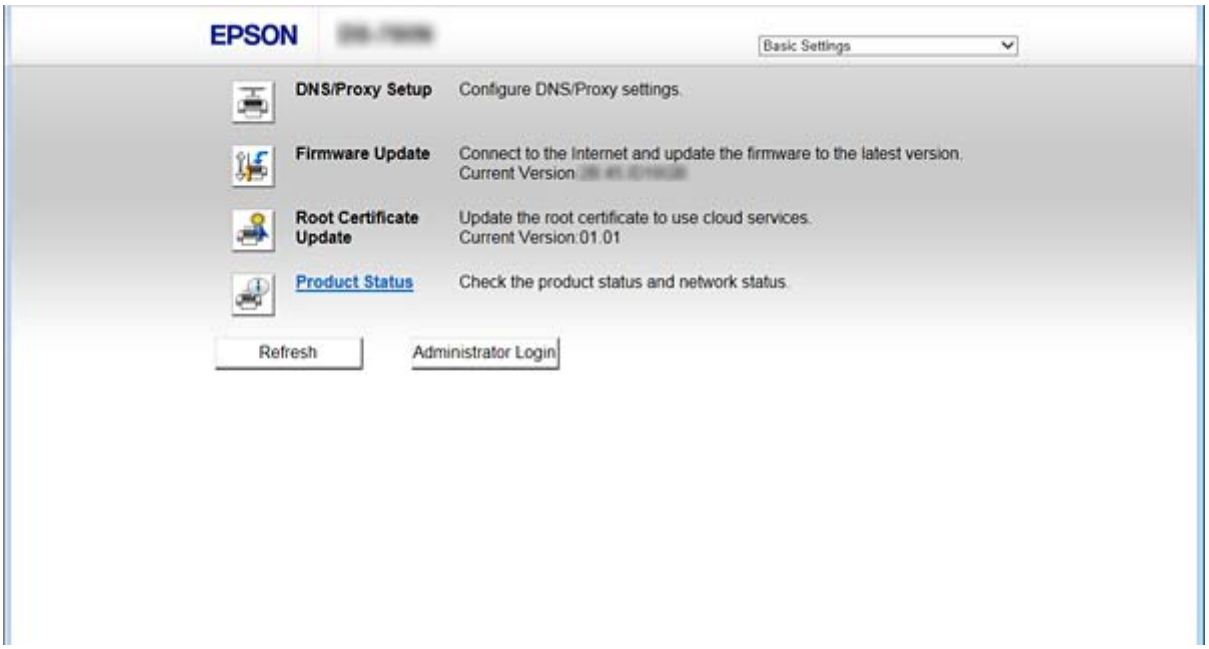
Per accedere alla pagina di Web Config, è necessario innanzitutto assegnare un indirizzo IP allo scanner.

***Nota:***
*È possibile bloccare le impostazioni configurando la password di amministratore per lo scanner.*

Esistono due pagine di impostazione, come mostrato di seguito.

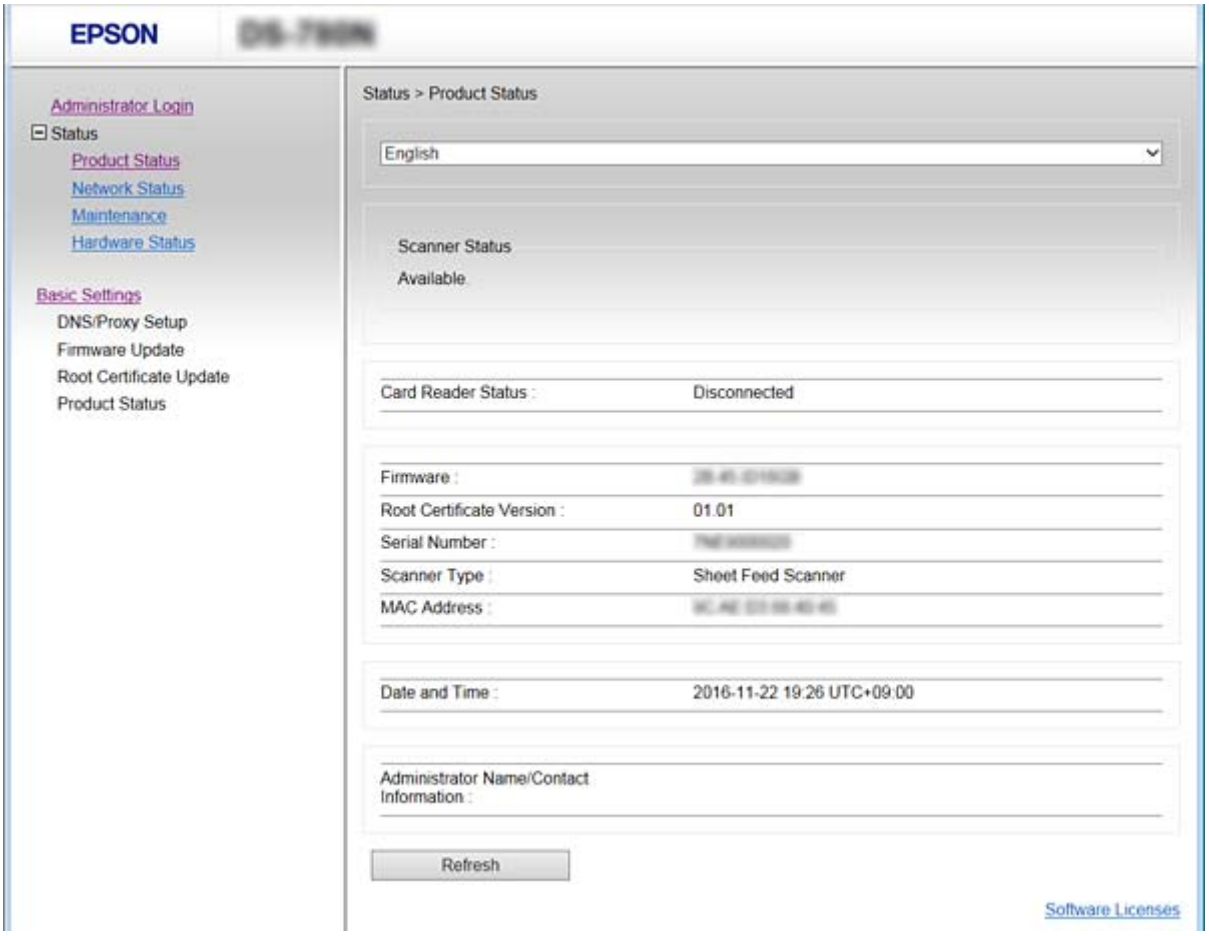
❏ **Impostazioni di base**

È possibile configurare le impostazioni di base per lo scanner.



❏ **Impostazioni avanzate**

È possibile configurare le impostazioni avanzate per lo scanner. Questa pagina è principalmente rivolta agli amministratori.




## Accesso a Web Config

Immettere l'indirizzo IP dello scanner in un browser web. JavaScript deve essere abilitato. Quando si accede a Web Config tramite HTTPS, nel browser verrà visualizzato un messaggio di avviso poiché viene utilizzato un certificato auto-firmato, memorizzato nello scanner.

❏ Accesso tramite HTTPS

IPv4: https://<indirizzo IP scanner> (senza < >)

IPv6: https://[indirizzo IP scanner]/ (con [ ])

❏ Accesso tramite HTTP

IPv4: http://<indirizzo IP scanner> (senza < >)

IPv6: http://[indirizzo IP scanner]/ (con [ ])

***Nota:***

❏ *Esempi*

*IPv4:*

*https://192.0.2.111/*

*http://192.0.2.111/*

*IPv6:*

*https://[2001:db8::1000:1]/*

*http://[2001:db8::1000:1]/*

❏ *Se il nome dello scanner è registrato con il server DNS, è possibile utilizzare il nome dello scanner al posto dell'indirizzo IP dello scanner.*

### Informazioni correlate

➡ "Comunicazione SSL/TLS con lo scanner" a pagina 63

➡ "Informazioni sulla certificazione digitale" a pagina 63

# Utilizzo delle funzioni di scansione

In base alla modalità di utilizzo dello scanner, installare il seguente software e utilizzarlo per effettuare le impostazioni.

❏ **Scansione da computer**

❏ Verificare la validità del servizio di scansione di rete con Web Config (valido con le impostazioni di fabbrica).

❏ Installare Epson Scan 2 sul computer e impostare l'indirizzo IP

❏ Quando si esegue la scansione mediante lavori, installare Document Capture Pro (Document Capture) e configurare le impostazioni del lavoro.

❏ **Scansione dal pannello operativo**

❏ Se si utilizza Document Capture Pro o Document Capture Pro Server:

Installare l'impostazione DHCP di Document Capture Pro o Document Capture Pro Server (modalità server, modalità client).

❏ Se si utilizza il protocollo WSD:

Verificare la validità di WSD in Web Config o sul pannello operativo (valido con le impostazioni di fabbrica)

Impostazioni aggiuntive del dispositivo (computer Windows).

## Scansione da computer

Installare il software e verificare che il servizio di scansione di rete sia abilitato per eseguire la scansione tramite una rete dal computer.

### Informazioni correlate

➡ "Software da installare" a pagina 25

➡ "Abilitare la scansione di rete" a pagina 25

## Software da installare

❏ Epson Scan 2

Questo è un driver dello scanner. Se si utilizza il dispositivo da un computer, installare il driver su ciascun computer client. Se è installato Document Capture Pro/Document Capture, è possibile eseguire le operazioni assegnate ai tasti del dispositivo.

Con EpsonNet SetupManager è possibile anche suddividere i driver della stampante in pacchetti.

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

Installare sul computer client. È possibile selezionare ed eseguire i lavori registrati su un computer su cui è installato Document Capture Pro/Document Capture sulla rete dal computer e dal pannello operativo dello scanner.

Inoltre, è possibile eseguire la scansione dal computer tramite la rete. Per eseguire la scansione è necessario Epson Scan 2.

### Informazioni correlate

➡ "EpsonNet SetupManager" a pagina 56

## Impostare l'indirizzo IP dello scanner su Epson Scan 2

Specificare l'indirizzo IP dello scanner per consentirne l'utilizzo sulla rete.

1. Avviare l'**Epson Scan 2 Utility** da **Start** > **Tutti i programmi** > **EPSON** > **Epson Scan 2**.

   Se è già registrato un altro scanner, andare al passaggio 2.

   Se non è registrato, andare al passaggio 4.

2. Fare clic su ▼ in **Scanner**.

3. Fare clic su **Settaggi**.

4. Fare clic su **Abilita modifica**, quindi su **Aggiungi**.

5. Selezionare il nome del modello dello scanner da **Modello**.

6. Selezionare l'indirizzo IP dello scanner da utilizzare da **Indirizzo** in **Ricerca rete**.

   Fare clic su  , quindi su  per aggiornare l'elenco. Se non si trova l'indirizzo IP dello scanner, selezionare **Inserire l'indirizzo** e inserire l'indirizzo IP.

7. Fare clic su **Aggiungi**.

8. Fare clic su **OK**.

## Abilitare la scansione di rete

È possibile impostare il servizio di scansione di rete quando si esegue la scansione da un computer client sulla rete. È attivata l'impostazione predefinita.

1. Accedere a Web Config e selezionare **Servizi** > **Scansione di rete**.

2. Assicurarsi che sia selezionato **Attiva scansione** di **EPSON Scan**.

   Se è selezionato, questa operazione è completata. Chiudere Web Config.

   Se è deselezionato, selezionarlo e andare al passaggio successivo.

3. Fare clic su **Avanti**.

4. Fare clic su **OK**.

   Viene effettuato il nuovo collegamento alla rete, quindi le impostazioni vengono abilitate.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Scansione tramite il pannello di controllo

Le funzioni di scansione su cartella e a indirizzo e-mail tramite il pannello di controllo dello scanner e il trasferimento dei risultati della scansione a e-mail, cartelle, ecc. vengono effettuate eseguendo un lavoro dal computer.

Per la trasmissione dei risultati della scansione, impostare il lavoro con Document Capture Pro Server o Document Capture Pro.

Per maggiori dettagli sulle impostazioni e la configurazione del lavoro, consultare la documentazione o la guida relative a Document Capture Pro Server o Document Capture Pro.

### Informazioni correlate

➡ "Impostazioni di Document Capture Pro Server/Document Capture Pro" a pagina 26

➡ "Configurazione di server e cartelle" a pagina 27

## Software da installare sul computer

❏ **Document Capture Pro Server**

Questa è la versione server di Document Capture Pro. Installarla su un server Windows. Il server può gestire centralmente più dispositivi e lavori. I lavori possono essere eseguiti in simultanea da più scanner.

Utilizzando la versione certificata di Document Capture Pro Server, è possibile gestire i lavori e la cronologia di scansione relativi a utenti e gruppi.

Per ulteriori dettagli su Document Capture Pro Server, contattare il centro Epson locale.

❏ **Document Capture Pro (Windows)/Document Capture (Mac OS)**

È possibile selezionare ed eseguire i lavori registrati sul computer dal pannello di controllo, come quando si esegue una scansione da un computer. Non è possibile eseguire i lavori registrati su un computer simultaneamente da più scanner.

## Impostazioni di Document Capture Pro Server/Document Capture Pro

Effettuare le impostazioni per utilizzare la funzione di scansione dal pannello operativo dello scanner.

1. Accedere a Web Config e selezionare **Servizi** > **Document Capture Pro**.

2. Selezionare **Modo operaz.**.

   ❏ Modalità server:

   Selezionare questa opzione quando si utilizza Document Capture Pro Server o Document Capture Pro solo per i lavori che sono stati impostati per un computer specifico.

   ❏ Modalità client:

   Impostare questa opzione quando si seleziona l'impostazione del lavoro di Document Capture Pro (Document Capture) installato su ciascun computer client nella rete senza specificare il computer.

3. Impostare le seguenti opzioni in base alla modalità selezionata.

   ❏ Modalità server:

   In **Indirizzo server**, specificare il server sul quale è installato Document Capture Pro Server. Può contenere tra 2 e 252 caratteri in formato IPv4, IPv6, nome host o FQDN. Nel formato FQDN è possibile utilizzare lettere, numeri, alfabeti e trattini (eccetto separatori e a inizio riga) US-ASCII.

   ❏ Modalità client:

   Specificare **Impostazioni gruppo** per utilizzare un gruppo di scanner specificato in Document Capture Pro (Document Capture).

4. Fare clic su **Impostazioni**.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Configurazione di server e cartelle

Document Capture Pro e Document Capture Pro Server salvano i dati acquisiti sul server o computer client una volta e utilizzano la funzione di trasferimento per eseguire le funzioni di scansione su cartella o scansione a indirizzo e-mail.

È necessario disporre delle autorità e informazioni da trasferire dal computer su cui è installato Document Capture Pro o Document Capture Pro Server al computer o servizio cloud.

Preparare le informazioni sulla funzione da utilizzare, facendo riferimento a quanto segue.

È possibile effettuare le impostazioni di queste funzioni utilizzando Document Capture Pro o Document Capture Pro Server. Per maggiori dettagli sulle impostazioni, consultare la documentazione o la guida relative a Document Capture Pro Server o Document Capture Pro.

| Nome | Impostazioni | Requisito |
|---|---|---|
| Scansione su cartella di rete (SMB) | Creazione e configurazione della condivisione della cartella di salvataggio | Account utente amministrativo per il computer che crea le cartelle di salvataggio. |
| | Destinazione per la scansione su cartella di rete (SMB) | Nome utente e password per accedere al computer che dispone della cartella di salvataggio, e privilegio di aggiornare la cartella di salvataggio. |
| Scansione su cartella di rete (FTP) | Configurazione dell'accesso al server FTP | Informazioni di accesso al server FTP e privilegio di aggiornare la cartella di salvataggio. |

| Nome | Impostazioni | Requisito |
|---|---|---|
| Scansione a e-mail | Configurazione del server e-mail | Informazioni di configurazione del server e-mail |
| Scansione a Document Capture Pro (se si utilizza Document Capture Pro Server) | Configurazione per l'accesso ai servizi cloud | Ambiente con accesso a Internet<br>Registrazione dell'account per i servizi cloud |

### Utilizzo della scansione WSD (solo Windows)

Se sul computer è installato Windows Vista o versioni successive, è possibile utilizzare la scansione WSD.

Se è possibile utilizzare il protocollo WSD, sul pannello di controllo dello scanner appare il menu **Computer (WSD)**.

1. Accedere a Web Config e selezionare **Servizi** > **Protocollo**.
2. Verificare che **Abilita WSD** sia selezionato in **Impostazioni WSD**.

   Se è selezionato, l'operazione è stata completata ed è possibile chiudere Web Config.

   Se non è selezionato, selezionarlo e andare al passaggio successivo.
3. Fare clic sul pulsante **Avanti**.
4. Confermare le impostazioni, quindi fare clic su **Impostazioni**.

# Configurazione delle impostazioni di sistema

## Configurazione delle impostazioni di sistema dal pannello di controllo

### Impostazione della luminosità dello schermo

Impostare la luminosità dello schermo LCD.

1. Toccare **Impostazioni** nella schermata iniziale.
2. Toccare **Impostazioni comuni** > **Luminosità LCD**.
3. Toccare  o  per regolare la luminosità.

   È possibile selezionare un'opzione di regolazione da 1 a 9.
4. Toccare **OK**.

## Configurazione del suono

Impostare il suono operativo del pannello e il segnale acustico di errore.

1. Toccare **Impostazioni** nella schermata iniziale.
2. Toccare **Impostazioni comuni** > **Suono**.
3. Impostare le seguenti voci come necessario.
   - ❏ Suono operativo
     Impostare il volume del suono del pannello operativo.
   - ❏ Segnale acustico di errore
     Impostare il volume del segnale acustico di errore.
4. Toccare **OK**.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Rilevamento della doppia alimentazione di originali

Determinare la funzione per rilevare la doppia alimentazione del documento da acquisire e interrompere la scansione quando si verifica questo problema.

Per eseguire la scansione di originali che si ritiene possano causare una doppia alimentazione, per esempio buste o carta con adesivi, impostarli su Off.

***Nota:***
*È possibile impostare questa opzione anche da Web Config o Epson Scan 2.*

1. Toccare **Impostazioni** nella schermata iniziale.
2. Toccare **Impostazioni di scansione esterne** > **Rilevam. doppia alim. a ultrasuoni**.
3. Toccare **Rilevam. doppia alim. a ultrasuoni** per attivarla o disattivarla.
4. Toccare **Chiudi**.

## Configurazione della modalità a bassa velocità

Configurare la scansione a bassa velocità per evitare inceppamenti carta durante la scansione di documenti sottili, per esempio una ricevuta.

1. Toccare **Impostazioni** nella schermata iniziale.
2. Toccare **Impostazioni di scansione esterne** > **Lento**.
3. Toccare **Lento** per attivarla o disattivarla.
4. Toccare **Chiudi**.

# Configurazione delle impostazioni di sistema tramite Web Config

## Impostazioni di risparmio energetico durante l'inattività

Effettuare le impostazioni di risparmio energetico per il periodo di inattività dello scanner. Impostare il periodo di tempo a seconda dell'ambiente di utilizzo.

***Nota:***
*È possibile effettuare le impostazioni di risparmio energetico anche nel pannello di controllo dello scanner.*

1. Accedere a Web Config e selezionare **Imp. di sistema** > **Risparmio energetico**.
2. Inserire l'orario del **Timer sospensione** per il passaggio alla modalità risparmio energetico in caso di inattività.

   È possibile impostare fino a 240 minuti a intervalli di un minuto.
3. Selezionare il tempo di spegnimento del **Timer spegnimento**.
4. Fare clic su **OK**.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Configurazione del pannello di controllo

Configurazione del pannello di controllo dello scanner. È possibile effettuare le seguenti impostazioni.

1. Accedere a Web Config e selezionare **Imp. di sistema** > **Pannello di controllo**.
2. Selezionare le seguenti voci, se necessario.
   - ❏ Lingua

     Selezionare la lingua visualizzata sul pannello di controllo.
   - ❏ Blocco pannello

     Se si seleziona **ATTIVA**, è necessaria la password di amministratore quando si esegue un'operazione che richiede l'autorizzazione dell'amministratore. Se la password di amministratore non è impostata, il blocco del pannello è disabilitato.
   - ❏ Timeout operazione

     Se si seleziona **ATTIVA**, quando si effettua l'accesso come amministratore, si viene disconnessi automaticamente e riportati alla schermata iniziale in caso di inattività per un certo periodo di tempo.

     È possibile impostare tra 10 secondi e 240 minuti a intervalli di un secondo.
3. Fare clic su **OK**.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Impostazione della restrizione per l'interfaccia esterna

È possibile limitare la connessione USB dal computer. Configurarla in modo da limitare la scansione in modalità diverse dalla connessione alla rete.

1. Accedere a Web Config e selezionare **Imp. di sistema** > **Interfaccia esterna**.
2. Selezionare **Abilita** o **Disabilita**.

   Per applicare la limitazione, selezionare **Disabilita**.
3. Toccare **OK**.

## Sincronizzazione di data e ora con il Time server

Se si utilizza un certificato CA, è possibile evitare problemi relativi all'orario.

1. Accedere a Web Config e selezionare **Imp. di sistema** > **Data e ora** > **Server di riferimento ora**.
2. Selezionare **Usa** per **Usa server di riferimento ora**.
3. Inserire l'indirizzo del time server come **Indirizzo server di riferimento ora**.

   È possibile utilizzare il formato IPv4, IPv6 o FQDN. Inserire fino a 252 caratteri. Se non viene specificato, lasciare il campo vuoto.
4. Immettere **Intervallo di aggiornamento (min)**.

   È possibile impostare fino a 10.800 minuti a intervalli di un minuto.
5. Fare clic su **OK**.

   ***Nota:***
   *È possibile verificare lo stato della connessione con il time server su* ***Stato server di riferimento ora****.*

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

# Impostazioni di sicurezza di base

In questo capitolo vengono illustrate le impostazioni di sicurezza di base che non richiedono un ambiente speciale.

## Introduzione delle funzioni di sicurezza di base

Verranno qui introdotte le funzioni di sicurezza di base dei dispositivi Epson.

| Nome della funzione | Tipo di funzione | Cosa impostare | Cosa evitare |
|---|---|---|---|
| Configurazione della password di amministratore | Bloccare le impostazioni di sistema, come quelle relative alla connessione di rete e USB, in modo che solo l'amministratore sia in grado di modificarle. | Un amministratore imposta una password per il dispositivo.<br>È possibile effettuare la configurazione o l'aggiornamento da qualsiasi posizione tramite Web Config, il pannello di controllo, Epson Device Admin e EpsonNet Config. | Impedire la lettura e la modifica illegali delle informazioni memorizzate sul dispositivo, come ID, password, impostazioni di rete e contatti. Inoltre, ridurre la varietà di rischi per la sicurezza, tra cui la fuga di informazioni, per l'ambiente di rete o nel rispetto delle politiche di sicurezza. |
| Comunicazioni SSL/TLS | Quando si accede a un server Epson su Internet da un dispositivo, come una comunicazione con un computer tramite un browser o un aggiornamento firmware, i contenuti della comunicazione vengono crittografati mediante la comunicazione SSL/TLS. | Ottenere un certificato firmato CA e importarlo nello scanner. | La rimozione di un'identificazione del dispositivo mediante il certificato firmato CA impedisce il furto d'identità e l'accesso non autorizzato. Inoltre, i contenuti della comunicazione SSL/TLS sono protetti impedendo la fuga di contenuti per i dati di stampa e le informazioni di configurazione. |
| Controllo protocolli | Controlla i protocolli utilizzati per la comunicazione tra dispositivi e computer e attiva/disattiva le funzioni. | Si tratta di un protocollo o servizio applicato alle funzioni consentite o vietate separatamente. | Ciò riduce i rischi per la sicurezza che possono verificarsi a causa di un utilizzo non intenzionale impedendo agli utenti di utilizzare funzioni non necessarie. |

### Informazioni correlate

➡ “Informazioni su Web Config” a pagina 22
➡ “EpsonNet Config” a pagina 55
➡ “Epson Device Admin” a pagina 55
➡ “Configurazione della password di amministratore” a pagina 33
➡ “Controllo dei protocolli” a pagina 35

# Configurazione della password di amministratore

Quando si imposta la password di amministratore, gli utenti diversi dagli amministratori non saranno in grado di modificare le impostazioni di amministrazione del sistema. È possibile impostare e modificare la password di amministratore utilizzando Web Config, il pannello di controllo dello scanner o il software (Epson Device Admin o EpsonNet Config). Quando si utilizza il software, consultare la documentazione relativa a ciascun software.

### Informazioni correlate

➡ "Configurazione della password di amministratore dal pannello di controllo" a pagina 33
➡ "Configurazione della password di amministratore tramite Web Config" a pagina 33
➡ "EpsonNet Config" a pagina 55
➡ "Epson Device Admin" a pagina 55

## Configurazione della password di amministratore dal pannello di controllo

È possibile configurare la password di amministratore dal pannello di controllo dello scanner.

1. Toccare **Impostazioni** nella schermata iniziale.
2. Toccare **Amministrazione sistema** > **Impostazioni amministratore**.

   Se la voce non appare, scorrere la schermata verso l'alto per visualizzarla.
3. Toccare **Password amministratore** > **Registra**.
4. Immettere la nuova password, quindi toccare **OK**.
5. Immettere nuovamente la password, quindi toccare **OK**.
6. Toccare **OK** sulla schermata di conferma.

   Viene visualizzata la schermata delle impostazioni di amministrazione.
7. Toccare **Impostazione blocco**, quindi toccare **OK** nella schermata di conferma.

   Impostazione blocco è impostata su **Attiv** e verrà richiesta la password di amministratore quando si utilizza la voce di menu bloccata.

***Nota:***

❏ *Impostando **Impostazioni** > **Impostazioni comuni** > **Timeout operazione** su **Attiv**, lo scanner effettuerà la disconnessione dopo un periodo di inattività sul pannello di controllo.*

❏ *È possibile modificare o eliminare la password di amministratore selezionando **Modifica** o **Ripristina** sulla schermata **Password amministratore** e inserendo la password di amministratore.*

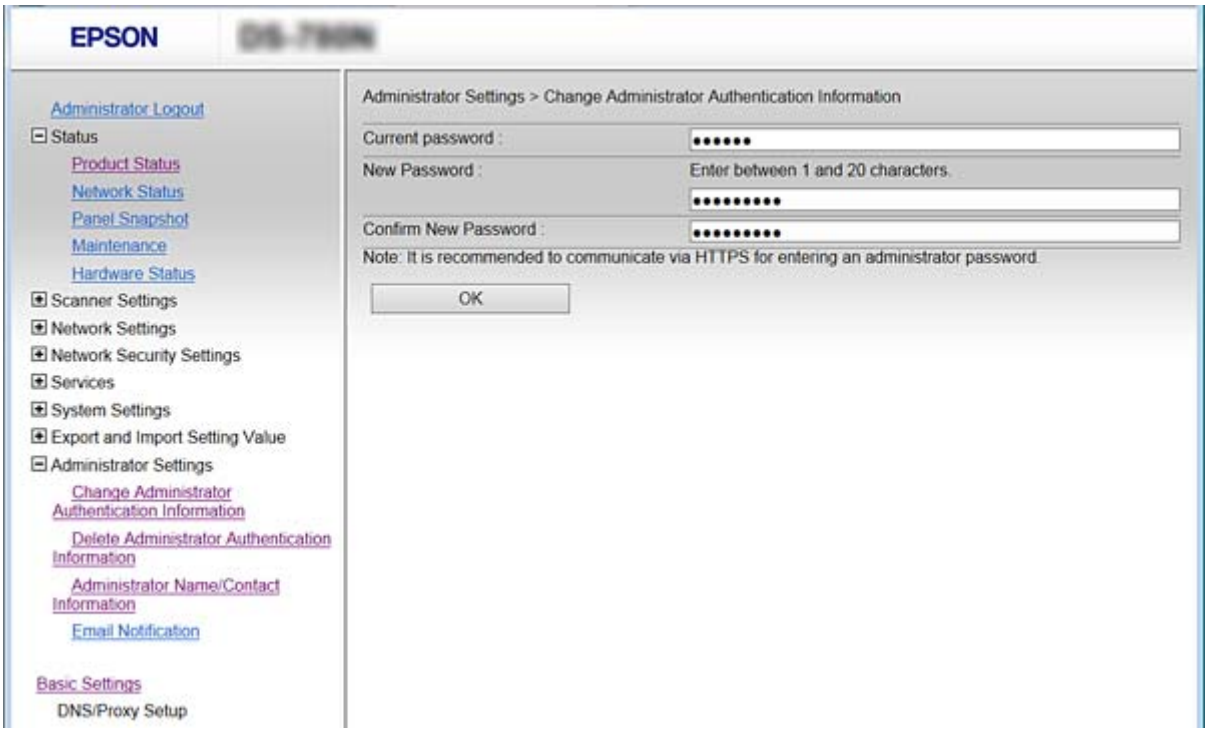
## Configurazione della password di amministratore tramite Web Config

È possibile impostare la password di amministratore utilizzando Web Config.

1. Accedere a Web Config e selezionare **Imp. amministratore** > **Modifica informazioni autenticazione amministratore**.

2. Immettere una password in **Nuova password** e **Conferma nuova password**. Inserire il nome utente, se necessario.

   Se si desidera cambiare la password, inserire una password corrente.




3. Selezionare **OK**.

   ***Nota:***

   ❏ *Per impostare o modificare le voci di menu bloccate, fare clic su* ***Login amministratore****, quindi inserire la password di amministratore.*

   ❏ *Per eliminare la password di amministrazione, fare clic su* ***Imp. amministratore*** *>* ***Elimina informazioni autenticazione amministratore****, quindi inserire la password di amministratore.*

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

# Voci da bloccare con la password di amministratore

Gli amministratori dispongono di privilegi di impostazione e modifica di tutte le funzioni dei dispositivi.

Inoltre, se si imposta la password di amministratore sul dispositivo, è possibile bloccarlo per impedire all'utente di modificare le voci relative alla gestione del dispositivo.

Un amministratore può controllare le seguenti voci.

**Impostazioni di sicurezza di base**

| Voce | Descrizione |
|---|---|
| Impostazione scanner | Configurazione del rilevamento della doppia alimentazione e della modalità a bassa velocità. |
| Impostazioni connessione Ethernet | Modificare il nome dei dispositivi e l'indirizzo IP, la configurazione del server DNS o del server proxy e le impostazioni relative alle connessioni di rete. |
| Impostazione servizi dell'utente | Configurazione per il controllo dei protocolli di comunicazione, della scansione in rete e dei servizi Document Capture Pro. |
| Impostazione server e-mail | Configurazione di un server di posta elettronica in comunicazione diretta con i dispositivi. |
| Impostazione di sicurezza | Impostazioni per la sicurezza della rete, come la comunicazione SSL/TLS, IPsec/IP filtering e IEEE802.1X. |
| Aggiornamento del certificato radice | Aggiornamento dei certificati radice richiesti per l'autenticazione a Document Capture Pro Server e l'aggiornamento del firmware da Web Config. |
| Aggiornamento del firmware | Controllare e aggiornare il firmware dei dispositivi. |
| Impostazione ora e timer | Tempo di passaggio alla modalità di riposo, spegnimento automatico, data/ora, timer di inattività, altre impostazioni relative a un timer. |
| Ripristino delle impostazioni predefinite | Configurazione del ripristino dello scanner alle impostazioni di fabbrica. |
| Impostazione di amministrazione | Impostazione del blocco o della password di amministratore. |
| Impostazione dispositivo certificato | Impostazione dell'ID del dispositivo di autenticazione. Impostazione dell'utilizzo dello scanner su un sistema di autenticazione che supporta i dispositivi di autenticazione. |

# Controllo dei protocolli

È possibile eseguire una scansione utilizzando vari percorsi e protocolli. Inoltre, è possibile utilizzare la scansione in rete da un numero non specificato di computer di rete. Per esempio, è consentita la scansione utilizzando solo percorsi e protocolli specifici. È possibile ridurre i rischi indesiderati in termini di protezione limitando la scansione da determinati percorsi o controllando le funzioni disponibili.

Configurare le impostazioni di protocollo.

1. Accedere a Web Config e selezionare **Servizi** > **Protocollo**.
2. Configurare ciascuna voce.
3. Fare clic su **Avanti**.
4. Fare clic su **OK**.

   Le impostazioni vengono applicate allo scanner.

### Informazioni correlate

➡ “Accesso a Web Config” a pagina 23

➡ “Protocolli che si possono abilitare o disabilitare” a pagina 36

➡ “Voci di impostazione del protocollo” a pagina 37

# Protocolli che si possono abilitare o disabilitare

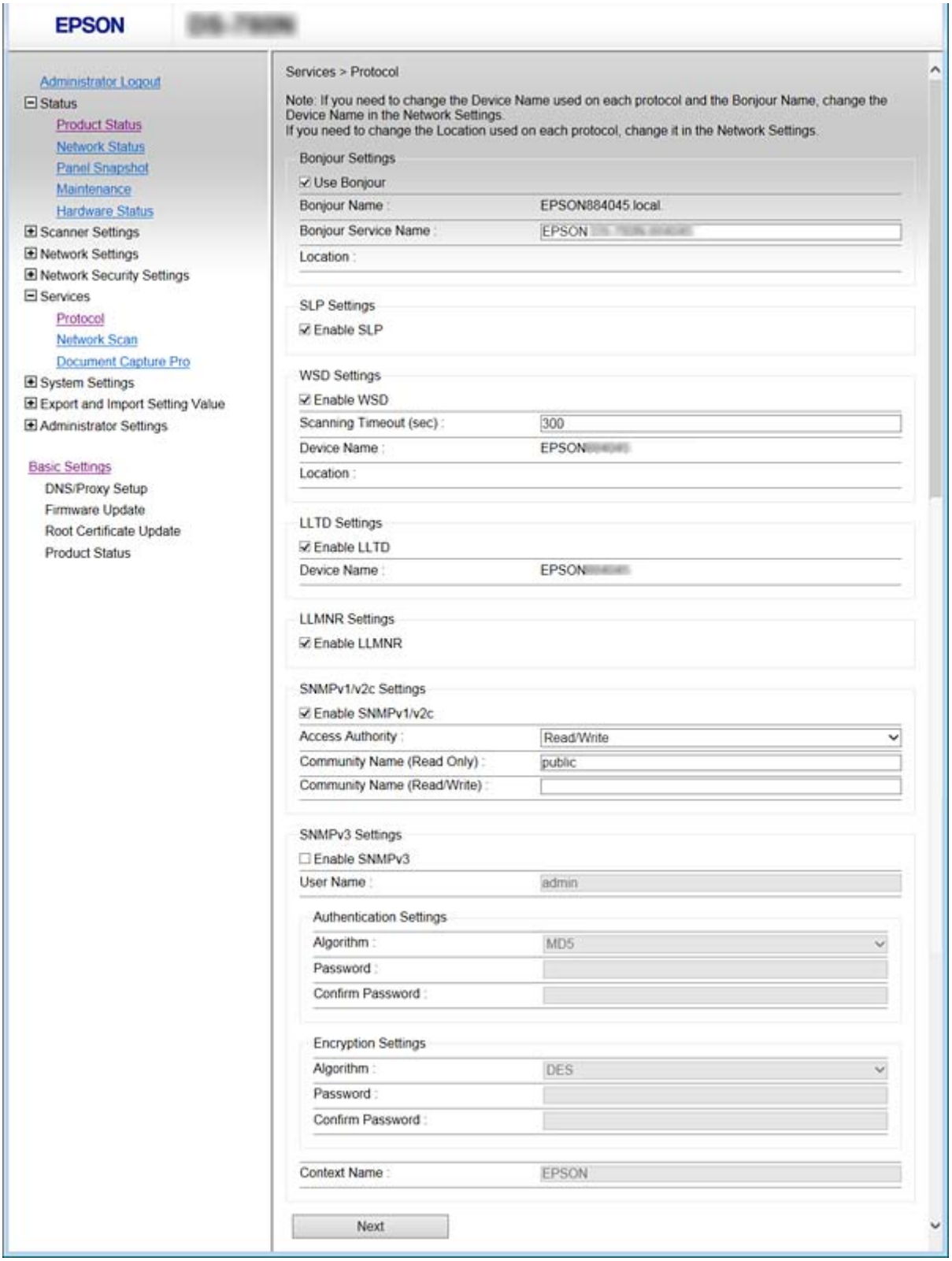
| Protocollo | Descrizione |
|---|---|
| Imp. Bonjour | È possibile specificare l'utilizzo di Bonjour. Bonjour viene utilizzato per la ricerca di dispositivi, per la scansione e così via. |
| Imp. SLP | È possibile abilitare o disabilitare la funzione SLP. SLP viene utilizzata per Epson Scan 2 e la ricerca in rete in EpsonNet Config. |
| Impostazioni WSD | È possibile abilitare o disabilitare la funzione WSD. Quando viene abilitato, è possibile aggiungere dispositivi WSD oppure eseguire la scansione dalla porta WSD. |
| Imp. LLTD | È possibile abilitare o disabilitare la funzione LLTD. Quando viene abilitato, viene visualizzato nella mappa di rete Windows. |
| Imp. LLMNR | È possibile abilitare o disabilitare la funzione LLMNR. Quando viene abilitato, è possibile utilizzare la risoluzione dei nomi senza NetBIOS anche se non è possibile utilizzare DNS. |
| Impostazioni SNMPv1/v2c | È possibile specificare se abilitare o meno SNMPv1/v2c. Viene utilizzato per la configurazione di dispositivi, il monitoraggio e così via. |
| Impostazioni SNMPv3 | È possibile specificare se abilitare o meno SNMPv3. Viene utilizzato per la configurazione di dispositivi crittografati, il monitoraggio ecc. |

### Informazioni correlate

➡ “Controllo dei protocolli” a pagina 35

➡ “Voci di impostazione del protocollo” a pagina 37

# Voci di impostazione del protocollo




| Elementi | Valore di impostazione e descrizione |
|---|---|
| Imp. Bonjour | |

## Impostazioni di sicurezza di base

| Elementi | Valore di impostazione e descrizione |
|---|---|
| Usa Bonjour | Selezionare per cercare o utilizzare dispositivi tramite Bonjour. |
| Nome Bonjour | Visualizza il nome Bonjour. |
| Nome servizio Bonjour | È possibile visualizzare e impostare il nome del servizio Bonjour. |
| Posizione | Visualizza il nome della posizione di Bonjour. |
| Imp. SLP | |
| Abilita SLP | Selezionare per abilitare la funzione SLP. Viene utilizzato per il rilevamento della rete in Epson Scan 2 e EpsonNet Config. |
| Impostazioni WSD | |
| Abilita WSD | Selezionare per consentire l'aggiunta di dispositivi tramite WSD, nonché la stampa e la scansione dalla porta WSD. |
| Timeout di scansione (sec) | Immettere il valore di timeout della comunicazione per la scansione WSD tra 3 e 3.600 secondi. |
| Nome dispositivo | Visualizza il nome del dispositivo WSD. |
| Posizione | Visualizza il nome della posizione di WSD. |
| Imp. LLTD | |
| Abilita LLTD | Selezionare per abilitare LLTD. Lo scanner viene visualizzato nella mappa di rete Windows. |
| Nome dispositivo | Visualizza il nome del dispositivo LLTD. |
| Imp. LLMNR | |
| Abilita LLMNR | Selezionare per abilitare LLMNR. È possibile utilizzare la risoluzione dei nomi senza NetBIOS anche se non è possibile utilizzare DNS. |
| Impostazioni SNMPv1/v2c | |
| Abilita SNMPv1/v2c | Selezionare per abilitare SNMPv1/v2c. Vengono visualizzati solo gli scanner che supportano SNMPv3. |
| Permesso di accesso | Impostare l'autorità di accesso quando si abilita SNMPv1/v2c. Selezionare **Sola lettura** o **Lettura/Scrittura**. |
| Nome community (sola lettura) | Immettere da 0 a 32 caratteri ASCII (0x20–0x7E). |
| Nome community (lettura/scrittura) | Immettere da 0 a 32 caratteri ASCII (0x20–0x7E). |
| Impostazioni SNMPv3 | |
| Abilita SNMPv3 | SNMPv3 è abilitata quando la casella è selezionata. |
| Nome utente | Immettere tra 1 e 32 caratteri utilizzando caratteri a singolo byte. |
| Impostazioni di autenticazione | |

**Impostazioni di sicurezza di base**

| Elementi | Valore di impostazione e descrizione |
|---|---|
| Algoritmo | Selezionare un algoritmo per un'autenticazione per SNMPv3. |
| Password | Inserire la password per un'autenticazione per SNMPv3.<br>Immettere tra 8 e 32 caratteri in ASCII (0x20–0x7E). Se non viene specificato, lasciare il campo vuoto. |
| Conferma password | Immettere la password configurata per conferma. |
| Impostazioni di crittografia | |
| Algoritmo | Selezionare un algoritmo per una crittografia per SNMPv3. |
| Password | Inserire la password per una crittografia per SNMPv3.<br>Immettere tra 8 e 32 caratteri in ASCII (0x20–0x7E). Se non viene specificato, lasciare il campo vuoto. |
| Conferma password | Immettere la password configurata per conferma. |
| Nome contesto | Inserire fino a 32 caratteri in Unicode (UTF-8). Se non viene specificato, lasciare il campo vuoto. Il numero di caratteri che è possibile inserire varia a seconda della lingua. |

### Informazioni correlate

➡ “Controllo dei protocolli” a pagina 35
➡ “Protocolli che si possono abilitare o disabilitare” a pagina 36

# Impostazioni di funzionamento e gestione

Questo capitolo spiega le voci relative alle operazioni quotidiane e alla gestione del dispositivo.

## Conferma delle informazioni relative a un dispositivo

È possibile verificare le seguenti informazioni relative al dispositivo in uso da **Stato** tramite Web Config.

❏ Stato del prodotto

Verificare la lingua, lo stato, il numero di prodotto, l'indirizzo MAC, ecc.

❏ Stato rete

Verificare le informazioni relative allo stato della connessione di rete, l'indirizzo IP, il server DNS, ecc.

❏ Miniatura pannello

Visualizzare un'istantanea dell'immagine sullo schermo che appare sul pannello di controllo del dispositivo.

❏ Manutenzione

Verificare la data di inizio, le informazioni sulla scansione, ecc.

❏ Stato hardware

Verificare lo stato dello scanner.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Gestione dei dispositivi (Epson Device Admin)

È possibile gestire e utilizzare vari dispositivi tramite Epson Device Admin. Epson Device Admin consente di gestire i dispositivi che si trovano su una rete diversa. Di seguito vengono delineate le principali funzioni di gestione.

Per ulteriori informazioni sulle funzioni e l'utilizzo del software, consultare la documentazione o la guida di Epson Device Admin.

❏ Rilevamento di dispositivi

È possibile rilevare i dispositivi sulla rete e registrarli in un elenco. Se i dispositivi Epson come stampanti e scanner sono collegati allo stesso segmento di rete del computer dell'amministratore, è possibile trovarli anche se non è stato assegnato loro un indirizzo IP.

È inoltre possibile rilevare i dispositivi collegati ai computer della rete tramite cavi USB. È necessario installare Epson Device USB Agent sul computer.

❏ Impostazione dei dispositivi

È possibile eseguire un template contenente le voci di impostazione, come l'interfaccia di rete e l'origine carta, e applicarlo ad altri dispositivi come impostazioni condivise. Quando è connesso alla rete, è possibile assegnare un indirizzo IP su un dispositivo a cui non è stato assegnato un indirizzo IP.

❏ Controllo dei dispositivi

È possibile acquisire regolarmente lo stato e le informazioni dettagliate sui dispositivi collegati alla rete. È inoltre possibile monitorare i dispositivi collegati ai computer sulla rete tramite cavi USB e i dispositivi da altre aziende che sono stati registrati sull'elenco dei dispositivi. Per monitorare i dispositivi collegati tramite cavi USB, è necessario installare Epson Device USB Agent.

❏ Gestione di avvisi

È possibile monitorare gli avvisi relativi allo stato dei dispositivi e dei materiali di consumo. Il sistema invia automaticamente e-mail di notifica all'amministratore in base alle condizioni impostate.

❏ Gestione di report

È possibile creare report periodici man mano che il sistema accumula dati sull'utilizzo dei dispositivi e dei materiali di consumo. È quindi possibile salvare i report creati e inviarli via e-mail.

**Informazioni correlate**

➡ "Epson Device Admin" a pagina 55

# Ricezione di notifiche email al verificarsi di eventi

## Notifiche e-mail

È possibile utilizzare questa funzione per ricevere avvisi via e-mail quando si verifica un evento. È possibile registrare fino a 5 indirizzi e-mail e scegliere per quali eventi si desidera ricevere le notifiche.

Per utilizzare questa funzione è necessario configurare il server di posta.

**Informazioni correlate**

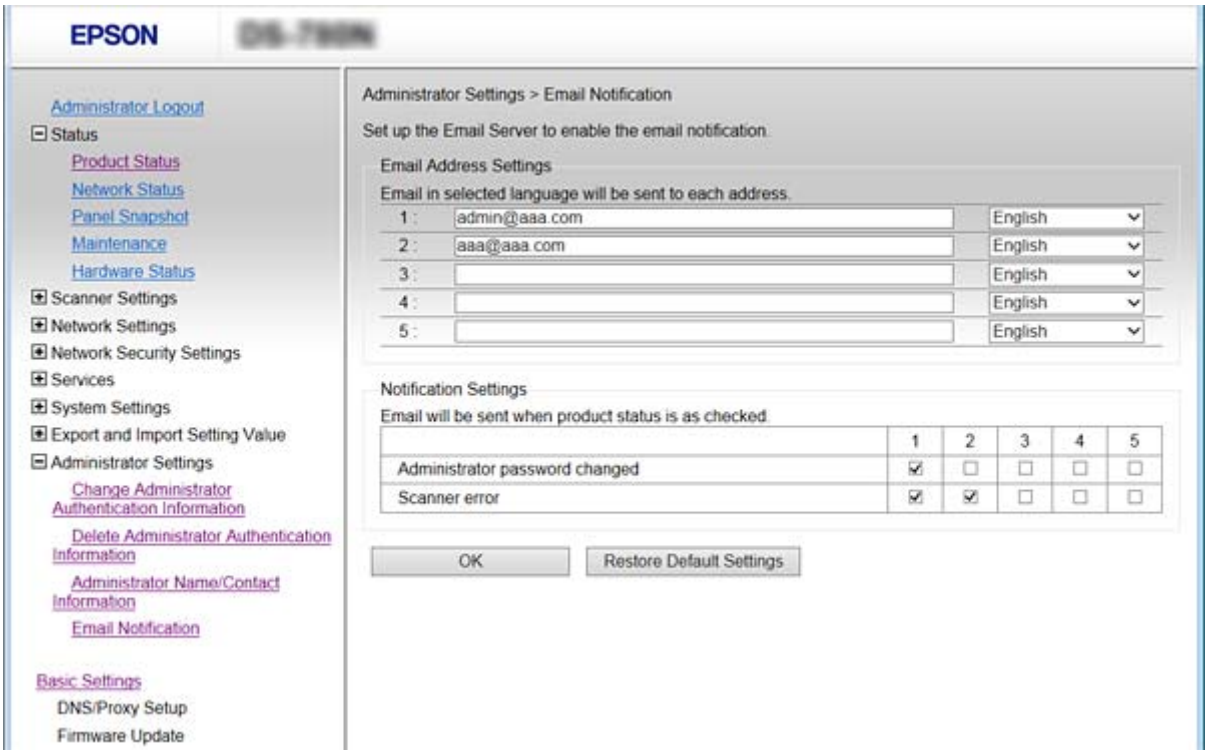
➡ "Configurazione di un server di posta" a pagina 42

## Configurazione delle notifiche e-mail

Per utilizzare la funzione, occorre configurare un server e-mail.

1. Accedere a Web Config e selezionare **Imp. amministratore** > **Notifica tramite e-mail**.
2. Inserire un indirizzo email al quale si desidera ricevere le notifiche.
3. Selezionare la lingua per le notifiche e-mail.

4. Selezionare le caselle per le notifiche che si desidera ricevere.




5. Fare clic su **OK**.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23
➡ "Configurazione di un server di posta" a pagina 42

## Configurazione di un server di posta

Verificare i punti seguenti prima di configurare.

❏ Lo scanner è connesso a una rete.

❏ Informazioni sul server e-mail del computer.

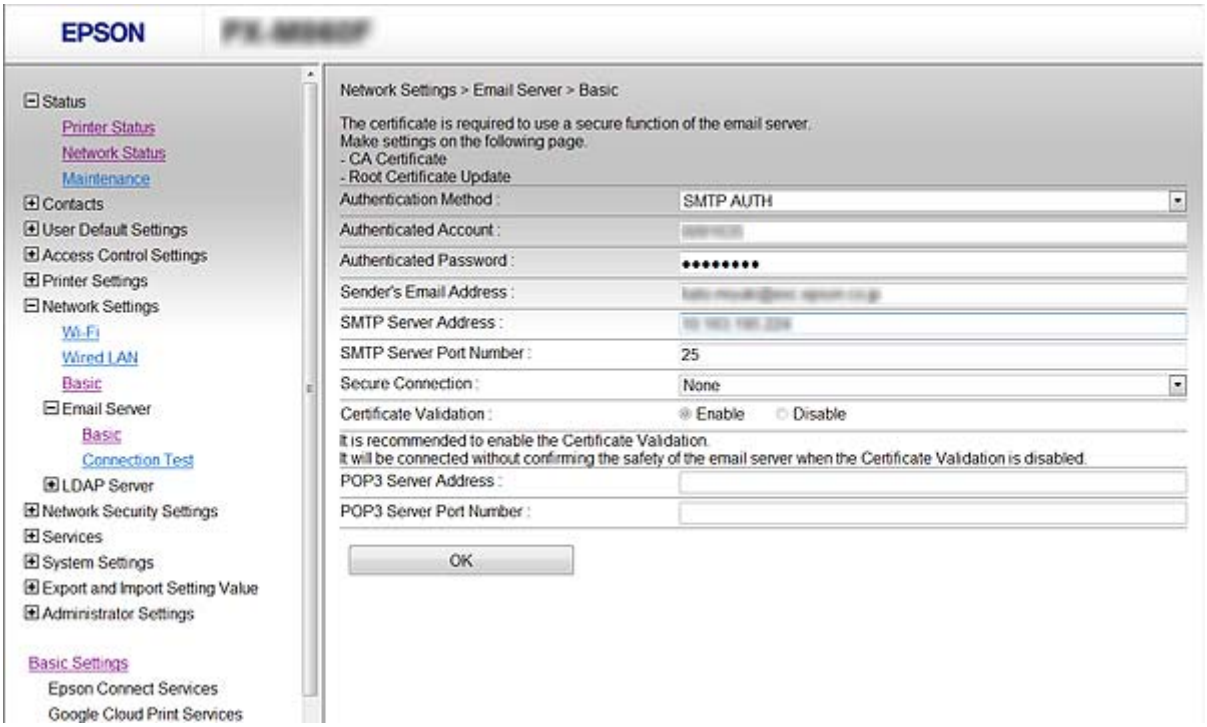
1. Accedere a Web Config e selezionare **Impostazioni di rete** > **Server e-mail** > **Di base**.
2. Immettere un valore per ciascuna voce.
3. Selezionare **OK**.

   Vengono visualizzate le impostazioni selezionate.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23
➡ "Voci di impostazione del server di posta" a pagina 43

# Voci di impostazione del server di posta




| Voci | Impostazioni e descrizione | |
|---|---|---|
| Metodo autenticazione | Specificare il metodo di autenticazione per l'accesso dello scanner al server di posta. | |
| | Disattiva | L'autenticazione viene disabilitata quando si comunica con un server di posta. |
| | AUT. SMTP | È necessario che un server di posta supporti l'autenticazione SMTP. |
| | POP prima di SMTP | Quando si seleziona questo metodo, configurare il server POP3. |
| Account autenticato | Se si seleziona **AUT. SMTP** o **POP prima di SMTP** come **Metodo autenticazione**, immettere il nome dell'account autenticato tra 0 e 255 caratteri in ASCII (0x20–0x7E). | |
| Password autenticata | Se si seleziona **AUT. SMTP** o **POP prima di SMTP** come **Metodo autenticazione**, immettere la password autenticata tra 0 e 20 caratteri utilizzando A–Z a–z 0–9! # $ % & ' * + - . / = ? ^ _ { \| } ~ @. | |
| Indirizzo e-mail mittente | Immettere l'indirizzo email del mittente. Immettere da 0 a 255 caratteri in ASCII (0x20–0x7E) ad eccezione di : ( ) < > [ ] ; ¥. Il primo carattere non può essere un punto "". | |
| Indirizzo server SMTP | Immettere tra 0 e 255 caratteri utilizzando A–Z a–z 0–9 . - . È possibile utilizzare il formato IPv4 o FQDN. | |
| Numero porta server SMTP | Immettere un numero tra 1 e 65535. | |

| Voci | Impostazioni e descrizione | |
|---|---|---|
| Connessione protetta | Specificare il metodo di connessione protetta per il server e-mail. | |
| | Nessuno | Se si seleziona **POP prima di SMTP** in **Metodo autenticazione**, il metodo di connessione viene impostato su **Nessuno**. |
| | SSL/TLS | Ciò è disponibile quando **Metodo autenticazione** viene impostato su **Disattiva** o **AUT. SMTP**. |
| | STARTTLS | Ciò è disponibile quando **Metodo autenticazione** viene impostato su **Disattiva** o **AUT. SMTP**. |
| Convalida certificato | Il certificato viene abilitato quando questa opzione viene abilitata. Si consiglia di impostare su **Abilita**. | |
| Indirizzo server POP3 | Se si seleziona **POP prima di SMTP** come **Metodo autenticazione**, immettere l'indirizzo del server POP3 da 0 e 255 caratteri utilizzando A–Z a–z 0–9 . - . È possibile utilizzare il formato IPv4 o FQDN. | |
| Numero porta server POP3 | Se si seleziona **POP prima di SMTP** come **Metodo autenticazione** immettere un numero compreso tra 1 e 65535. | |

### Informazioni correlate

➡ “Configurazione di un server di posta” a pagina 42

## Verifica della connessione al server di posta

1. Accedere a Web Config e selezionare **Impostazioni di rete** > **Server e-mail** > **Test di conn.**.
2. Selezionare **Avvia**.

   Viene avviato il test di connessione sul server e-mail. Dopo il test, viene visualizzato il rapporto di verifica.

### Informazioni correlate

➡ “Accesso a Web Config” a pagina 23
➡ “Riferimenti per test di connessione al server di posta” a pagina 44

## Riferimenti per test di connessione al server di posta

| Messaggi | Descrizione |
|---|---|
| Test di connessione riuscito. | Questo messaggio appare quando la connessione con il server è riuscita. |
| Errore di comunicazione server SMTP. Controllare quanto segue. - Impostazioni di rete | Questo messaggio appare quando<br>❏ Lo scanner non è connesso a una rete<br>❏ Il server SMTP è inattivo<br>❏ La connessione di rete viene disconnessa durante la comunicazione<br>❏ Si ricevono dati incompleti |

**Impostazioni di funzionamento e gestione**

| Messaggi | Descrizione |
|---|---|
| Errore di comunicazione server POP3. Controllare quanto segue. - Impostazioni di rete | Questo messaggio appare quando<br>❏ Lo scanner non è connesso a una rete<br>❏ Il server POP3 è inattivo<br>❏ La connessione di rete viene disconnessa durante la comunicazione<br>❏ Si ricevono dati incompleti |
| Errore durante la conness. al server SMTP. Controllare quanto segue. - Indirizzo server SMTP - Server DNS | Questo messaggio appare quando<br>❏ Connessione ad un server DNS non riuscita<br>❏ Risoluzione dei nomi di un server SMTP non riuscita |
| Errore durante la conness. al server POP3. Controllare quanto segue. - Indirizzo server POP3 - Server DNS | Questo messaggio appare quando<br>❏ Connessione ad un server DNS non riuscita<br>❏ Risoluzione dei nomi di un server POP3 non riuscita |
| Errore di autenticazione server SMTP. Controllare quanto segue. - Metodo autenticazione - Account autenticato - Password autenticata | Questo messaggio appare in caso di mancata autenticazione del server SMTP. |
| Errore di autenticazione server POP3. Controllare quanto segue. - Metodo autenticazione - Account autenticato - Password autenticata | Questo messaggio appare in caso di mancata autenticazione del server POP3. |
| Metodo di comunicazione non supportato. Controllare quanto segue. - Indirizzo server SMTP - Numero porta server SMTP | Questo messaggio appare quando si cerca di comunicare con protocolli non supportati. |
| Connessione al server SMTP non riuscita. Cambiare Connessione protetta in Nessuno. | Questo messaggio appare in caso di mancata corrispondenza SMTP tra server e client o quando il server non supporta una connessione protetta SMTP (connessione SSL). |
| Connessione al server SMTP non riuscita. Cambiare Connessione protetta in SSL/TLS. | Questo messaggio appare in caso di mancata corrispondenza SMTP tra server e client o quando il server richiede l'utilizzo di una connessione SSL/TLS per una connessione protetta SMTP. |
| Connessione al server SMTP non riuscita. Cambiare Connessione protetta in STARTTLS. | Questo messaggio appare in caso di mancata corrispondenza SMTP tra server e client o quando il server richiede l'utilizzo di una connessione STARTTLS per una connessione protetta SMTP. |
| Connessione non affidabile. Controllare quanto segue. - Data e ora | Questo messaggio appare quando l'impostazione di data e ora dello scanner non è corretta o il certificato è scaduto. |
| Connessione non affidabile. Controllare quanto segue. - Certificato CA | Questo messaggio appare quando lo scanner non dispone di un certificato root corrispondente al server o un Certificato CA non è stato importato. |
| Connessione non affidabile. | Questo messaggio appare quando il certificato ottenuto è danneggiato. |
| Autenticazione server SMTP non riuscita. Cambiare Metodo autenticazione in AUT. SMTP. | Questo messaggio appare in caso di mancata corrispondenza del metodo di autenticazione tra server e client. Il server supporta AUT. SMTP. |
| Autenticazione server SMTP non riuscita. Cambiare Metodo autenticazione in POP prima di SMTP. | Questo messaggio appare in caso di mancata corrispondenza del metodo di autenticazione tra server e client. Il server non supporta AUT. SMTP. |

| Messaggi | Descrizione |
|---|---|
| Indirizzo e-mail mittente non corretto. Passare all'indirizzo e-mail per il servizio e-mail in uso. | Questo messaggio appare quando l'indirizzo e-mail specificato del mittente è errato. |
| Impossibile accedere al prodotto fino al termine dell'elaborazione. | Questo messaggio appare quando lo scanner è occupato. |

### Informazioni correlate

➡ "Verifica della connessione al server di posta" a pagina 44

# Aggiornamento del firmware

## Aggiornamento del firmware tramite Web Config

Aggiorna il firmware utilizzando Web Config. Il dispositivo deve essere collegato a Internet.

1. Accedere a Web Config e selezionare **Impostazioni di base** > **Aggiornamento firmware**.
2. Fare clic su **Avvia**.

   La conferma del firmware si avvia e, se esiste il firmware aggiornato, vengono visualizzate le informazioni a esso relative.
3. Fare clic su **Avvia** e seguire le istruzioni visualizzate sullo schermo.

***Nota:***
*È possibile aggiornare il firmware anche tramite Epson Device Admin. È possibile verificare visivamente le informazioni sul firmware sulla lista dei dispositivi. Ciò è utile quando si desidera aggiornare il firmware di più dispositivi. Per ulteriori informazioni, consultare la guida o l'aiuto di Epson Device Admin.*

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23
➡ "Epson Device Admin" a pagina 55

## Aggiornamento del firmware tramite Epson Firmware Updater

È possibile scaricare il firmware del dispositivo sul computer dal sito web Epson, quindi collegare il dispositivo e il computer tramite un cavo USB per aggiornare il firmware. Se non è possibile aggiornare in rete, provare il seguente metodo.

1. Accedere al sito web Epson e scaricare il firmware.
2. Collegare il computer che contiene il firmware scaricato sul dispositivo tramite un cavo USB.
3. Fare doppio clic sul file .exe scaricato.

   Epson Firmware Updater viene avviato.

4. Seguire le istruzioni visualizzate sullo schermo.

# Backup delle impostazioni

Esportando le voci di impostazione su Web Config, è possibile copiarle agli altri scanner.

## Esportazione delle impostazioni

Esportare ogni impostazione dello scanner.

1. Accedere a Web Config, quindi selezionare **Esporta e imposta valore di impostazione** > **Esporta**.
2. Selezionare le impostazioni che si desidera esportare.

   Selezionare le impostazioni che si desidera esportare. Se si seleziona la categoria principale, vengono selezionate anche le sottocategorie. Tuttavia, non è possibile selezionare le sottocategorie che causano errori di duplicazione all'interno della stessa rete (ad esempio indirizzi IP e così via).
3. Immettere una password di crittografia del file esportato.

   Per importare il file, è necessaria la password. Lasciare vuoto se non si desidera crittografare il file.
4. Fare clic su **Esporta**.

> ***Importante:***
>
> *Per esportare le impostazioni di rete dello scanner, ad esempio nome dello scanner e indirizzo IP, selezionare **Abilitare per selezionare le singole impostazioni del dispositivo** e selezionare altre voci. Utilizzare solo i valori selezionati per lo scanner sostitutivo.*

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Importazione delle impostazioni

Importare il file Web Config esportato sullo scanner.

> ***Importante:***
>
> *Quando si importano valori che includono informazioni individuali, ad esempio nome dello scanner o indirizzo IP, assicurarsi che sulla stessa rete non sia presente lo stesso indirizzo. In caso di sovrapposizione dell'indirizzo IP, lo scanner non applica il valore.*

1. Accedere a Web Config, quindi selezionare **Esporta e imposta valore di impostazione** > **Importa**.
2. Selezionare il file esportato, quindi immettere la password crittografata.
3. Fare clic su **Avanti**.
4. Selezionare le impostazioni che si desidera installare, quindi fare clic su **Avanti**.

5. Fare clic su **OK**.

Le impostazioni vengono applicate allo scanner.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

# Risoluzione dei problemi

## Suggerimenti per la risoluzione dei problemi

È possibile reperire ulteriori informazioni nel seguente manuale.

❏ Guida utente

Fornisce istruzioni sull'uso dello scanner, sulla manutenzione e sulla risoluzione dei problemi.

## Controllo del registro del server e del dispositivo di rete

In caso di problemi con la connessione di rete, è possibile identificarne la causa consultando il registro del server di posta, del server LDAP, ecc., verificando lo stato mediante il registro di rete dei registri delle apparecchiature di sistema e i comandi, come i router.

## Inizializzazione delle impostazioni di rete

### Ripristino delle impostazioni di rete dal pannello di controllo

È possibile ripristinare tutte le impostazioni di rete ai valori originali.

1. Toccare **Impostazioni** nella schermata iniziale.
2. Toccare **Amministrazione sistema** > **Ripristina impostaz. predef.** > **Impostazioni di rete**.
3. Controllare il messaggio, quindi selezionare **Sì**.
4. Quando viene visualizzato un messaggio di completamento, toccare **Chiudi**.

   Se non si tocca **Chiudi**, la schermata si chiude automaticamente dopo un determinato periodo di tempo.

## Verifica della comunicazione tra dispositivi e computer

### Verifica della connessione tramite un comando Ping — Windows

È possibile usare un comando Ping per accertarsi che il computer sia connesso allo scanner. Seguire i passaggi riportati di seguito per verificare la connessione con un comando Ping.

**Risoluzione dei problemi**

1. Controllare l'indirizzo IP dello scanner per la connessione che si desidera verificare.

   È possibile effettuare questo controllo dalla schermata Epson Scan 2.

2. Visualizzare la schermata del prompt dei comandi del computer.

   ❏ Windows 10

   Fare clic con il pulsante destro del mouse sul pulsante di start oppure premerlo e tenerlo premuto, quindi selezionare **Prompt dei comandi**.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Visualizzare la schermata dell'applicazione e quindi selezionare **Prompt dei comandi**.

   ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 o precedente

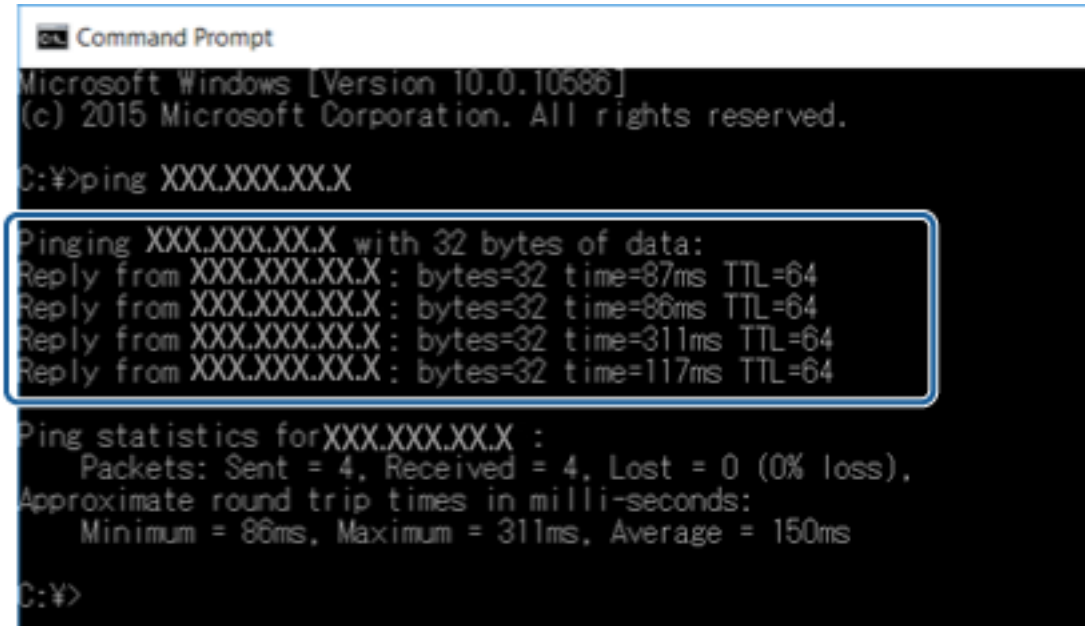
   Fare clic sul pulsante start, scegliere **Tutti i programmi** o **Programmi** > **Accessori** > **Prompt dei comandi**.

3. Digitare “ping xxx.xxx.xxx.xxx”, quindi premere il tasto Enter.

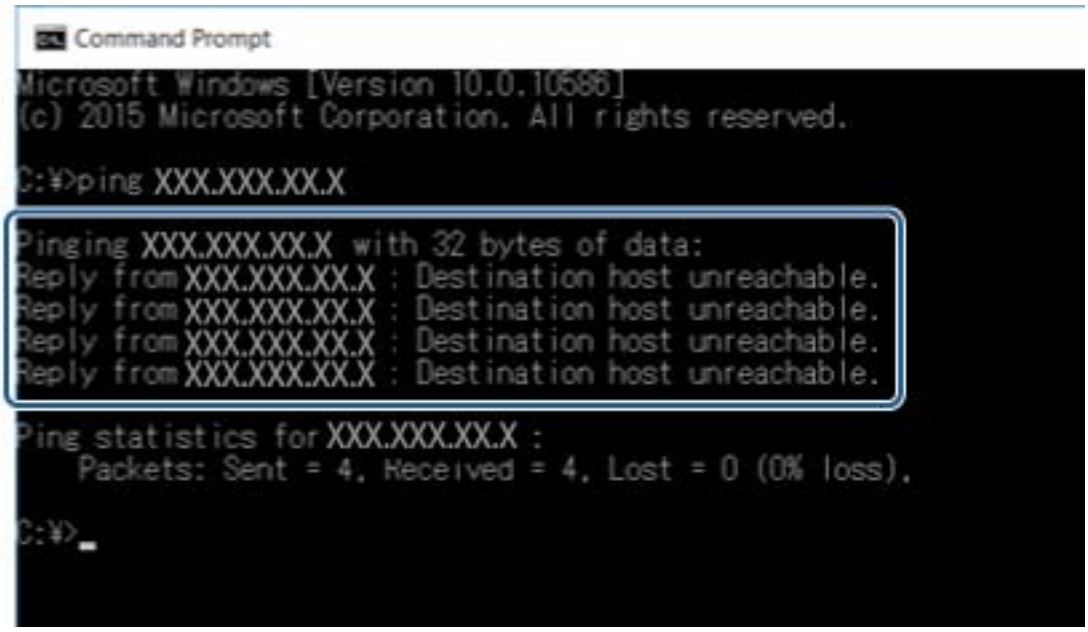
   Immettere l'indirizzo IP dello scanner per xxx.xxx.xxx.xxx.

4. Verificare lo stato della comunicazione.

   Se lo scanner e il computer stanno comunicando, viene visualizzato il seguente messaggio.



Se lo scanner e il computer non stanno comunicando, viene visualizzato il seguente messaggio.




## Verifica della connessione tramite un comando Ping — Mac OS

È possibile usare un comando Ping per accertarsi che il computer sia connesso allo scanner. Seguire i passaggi riportati di seguito per verificare la connessione con un comando Ping.

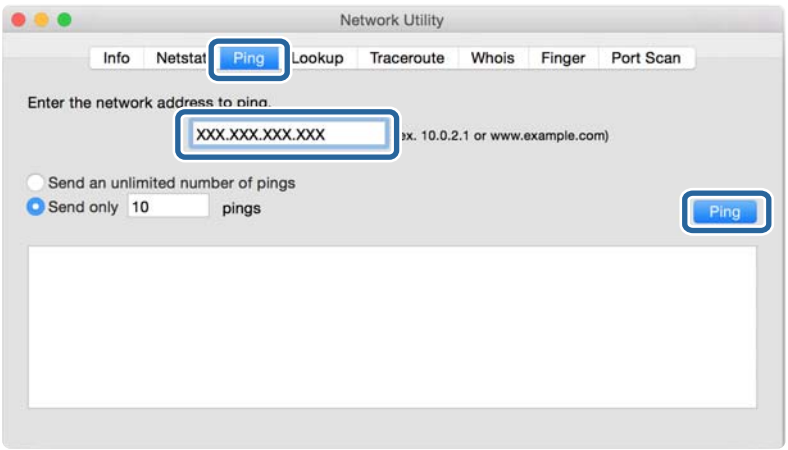
1. Controllare l'indirizzo IP dello scanner per la connessione che si desidera verificare.

   È possibile effettuare questo controllo dalla schermata Epson Scan 2.

2. Eseguire Network Utility.

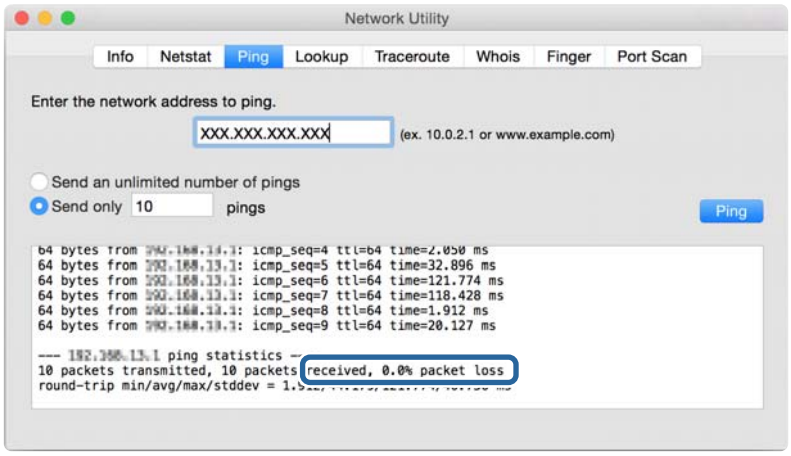
   Digitare “Network Utility” in **Spotlight**.

3. Fare clic sulla scheda **Ping**, inserire l'indirizzo IP controllato al passaggio 1 e quindi fare clic su **Ping**.

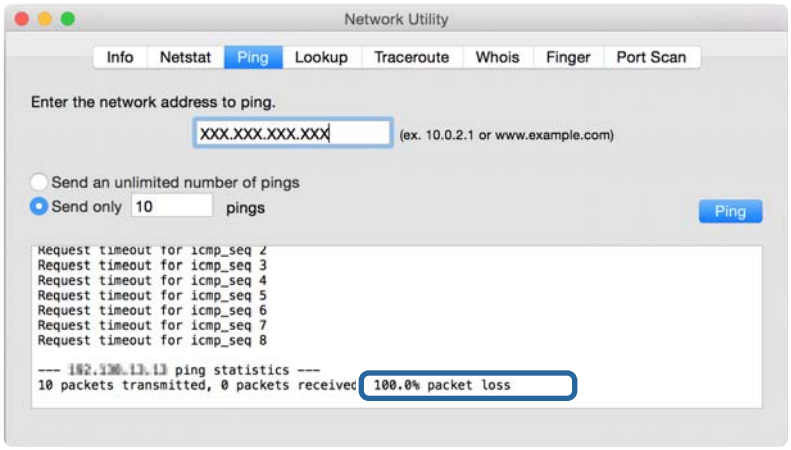


4. Verificare lo stato della comunicazione.

   Se lo scanner e il computer stanno comunicando, viene visualizzato il seguente messaggio.




   Se lo scanner e il computer non stanno comunicando, viene visualizzato il seguente messaggio.




# Problemi con il software di rete

## Impossibile accedere a Web Config

### L'indirizzo IP dello scanner è stato configurato correttamente?

Configurare l'indirizzo IP utilizzando Epson Device Admin o EpsonNet Config.

### Il tuo browser supporta le crittografie di massa per la Livello di crittografia per SSL/TLS?

Le crittografie di massa per la Livello di crittografia per SSL/TLS sono come indicato di seguito. È possibile accedere a Web Config solo in un browser che supporta le seguenti crittografie di massa. Verificare il supporto di crittografia del browser in uso.

- ❏ 80bit: AES256/AES128/3DES
- ❏ 112bit: AES256/AES128/3DES
- ❏ 128bit: AES256/AES128

❏ 192bit: AES256

❏ 256bit: AES256

### Il messaggio “Scaduto” appare quando si accede a Web Config utilizzando la comunicazione SSL (https).

Se il certificato è scaduto, ottenere di nuovo il certificato. Se il messaggio appare prima della data di scadenza, assicurarsi che la data dello scanner sia configurata correttamente.

### Il messaggio “Il nome del certificato di sicurezza non corrisponde…” appare quando si accede a Web Config utilizzando la comunicazione SSL (https).

L'indirizzo IP dello scanner immesso per **Nome comune** per la creazione di un certificato auto-firmato o di una richiesta CSR non corrisponde all'indirizzo immesso nel browser. Ottenere e importare nuovamente un certificato o cambiare il nome dello scanner.

### L'accesso allo scanner avviene tramite un server proxy.

Se si sta utilizzando un server proxy con lo scanner, occorre configurare le impostazioni proxy del browser in uso.

❏ Windows:

Selezionare **Pannello di controllo** > **Rete e Internet** > **Opzioni Internet** > **Connessioni** > **Impostazioni LAN** > **Server proxy**, quindi configurare l'opzione di non utilizzare il server proxy per gli indirizzi locali.

❏ Mac OS:

Selezionare **Preferenze di Sistema** > **Network** > **Avanzate** > **Proxy**, quindi registrare l'indirizzo locale per **Ignora le impostazioni proxy per i seguenti host e domini**.

Esempio:

192.168.1.*: Indirizzo locale 192.168.1.XXX, maschera sottorete 255.255.255.0

192.168.*.*: Indirizzo locale 192.168.XXX.XXX, maschera sottorete 255.255.0.0

### Informazioni correlate

➡ “Accesso a Web Config” a pagina 23

➡ “Assegnazione dell'indirizzo IP” a pagina 15

➡ “Assegnazione di un indirizzo IP tramite EpsonNet Config” a pagina 56

## Il nome di modello e/o l'indirizzo IP non vengono visualizzati in EpsonNet Config

### È stato selezionato Blocca, Annulla, o Arresta quando appare una schermata di protezione di Windows o una schermata di firewall?

Se si seleziona **Blocca**, **Annulla** o **Arresta**, l'indirizzo IP e il nome di modello non appariranno in EpsonNet Config o in EpsonNet Setup.

Per correggere tale problema, registrare EpsonNet Config come eccezione in Windows firewall e nel software di protezione di terzi. Se si sta utilizzando un antivirus o un programma di protezione, chiuderlo e riprovare a utilizzare EpsonNet Config.

### L'impostazione dell'errore di scadenza comunicazione è troppo breve?

Eseguire EpsonNet Config e selezionare **Tools** > **Options** > **Timeout**, quindi aumentare il periodo di tempo per l'impostazione di **Communication Error**. Tenere presente che tale impostazione può rallentare l'esecuzione di EpsonNet Config.

### Informazioni correlate

➡ "Esecuzione di EpsonNet Config — Windows" a pagina 56

➡ "Esecuzione di EpsonNet Config — Mac OS" a pagina 56

# Appendice

## Introduzione del software di rete

Di seguito verrà descritto il software che configura e gestisce i dispositivi.

### Epson Device Admin

Epson Device Admin è un'applicazione che vi consente di installare dei dispositivi in rete e successivamente di configurarli e gestirli. È possibile acquisire informazioni dettagliate sui dispositivi, come lo stato e materiali di consumo, inviare notifiche di avviso e creare report sull'utilizzo dei dispositivi. È inoltre possibile eseguire un template contenente le voci delle impostazioni e applicarlo ad altri dispositivi come impostazioni condivise. È possibile scaricare Epson Device Admin dal sito Web del supporto Epson. Per ulteriori informazioni, vedere la documentazione o la guida di Epson Device Admin.

#### Esecuzione di Epson Device Admin (solo per Windows)

Selezionare **Tutti i programmi** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

***Nota:***
*Se appare l'avviso del firewall, consentire l'accesso per Epson Device Admin.*

### EpsonNet Config

EpsonNet Config consente all'amministratore di configurare le impostazioni di rete dello scanner, quali l'assegnazione di un indirizzo IP e la modifica della modalità di connessione. La funzione di impostazione batch è supportata in Windows. Per ulteriori informazioni, vedere la documentazione o la guida di EpsonNet Config.

### Esecuzione di EpsonNet Config — Windows

Selezionare **Tutti i programmi** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

***Nota:***
*Se appare l'avviso del firewall, consentire l'accesso per EpsonNet Config.*

### Esecuzione di EpsonNet Config — Mac OS

Selezionare **Vai** > **Applicazioni** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

## EpsonNet SetupManager

EpsonNet SetupManager è un software per la creazione di un pacchetto per una semplice installazione dello scanner, come l'installazione e la configurazione del driver dello scanner e l'installazione di Document Capture Pro. Questo software consente all'amministratore di creare dei pacchetti specifici di software e di distribuirli tra i vari gruppi.

Per ulteriori informazioni, visitare il sito web locale Epson.

# Assegnazione di un indirizzo IP tramite EpsonNet Config

È possibile assegnare un indirizzo IP allo scanner mediante EpsonNet Config. EpsonNet Config consente di assegnare un indirizzo IP a uno scanner al quale non ne è stato assegnato uno dopo aver effettuato la connessione tramite un cavo Ethernet.

## Assegnazione dell'indirizzo IP tramite le impostazioni batch

### Creazione del file per le impostazioni batch

Utilizzando l'indirizzo MAC e il nome del modello come chiavi, è possibile creare un nuovo file SYLK per impostare l'indirizzo IP.

1. Aprire un foglio di calcolo (come Microsoft Excel) o un editor di testo.

2. Inserire “Info_MACAddress”, “Info_ModelName” e “TCPIP_IPAddress” nella prima riga come nomi delle voci di impostazione.

   Inserire le voci di impostazione per le seguenti stringhe di testo. Per distinguere tra maiuscole/minuscole e caratteri a doppio byte/a singolo byte, se un solo carattere è diverso la voce non sarà riconosciuta.

   Immettere il nome della voce di impostazione come descritto di seguito; in alternativa, EpsonNet Config non è in grado di riconoscere le voci di impostazione.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|
| | | |
| | | |

3. Inserire l'indirizzo MAC, il nome del modello e l'indirizzo IP per ogni interfaccia di rete.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|
| 0000XXXX0001 | ALC-XXXXX | 192.168.100.102 |
| 0000XXXX0002 | ALC-XXXXX | 192.168.100.103 |
| 0000XXXX0003 | ALC-XXXXX | 192.168.100.104 |

4. Inserire un nome e salvare come file SYLK (*.slk).

## Configurazione delle impostazioni batch mediante il file di configurazione

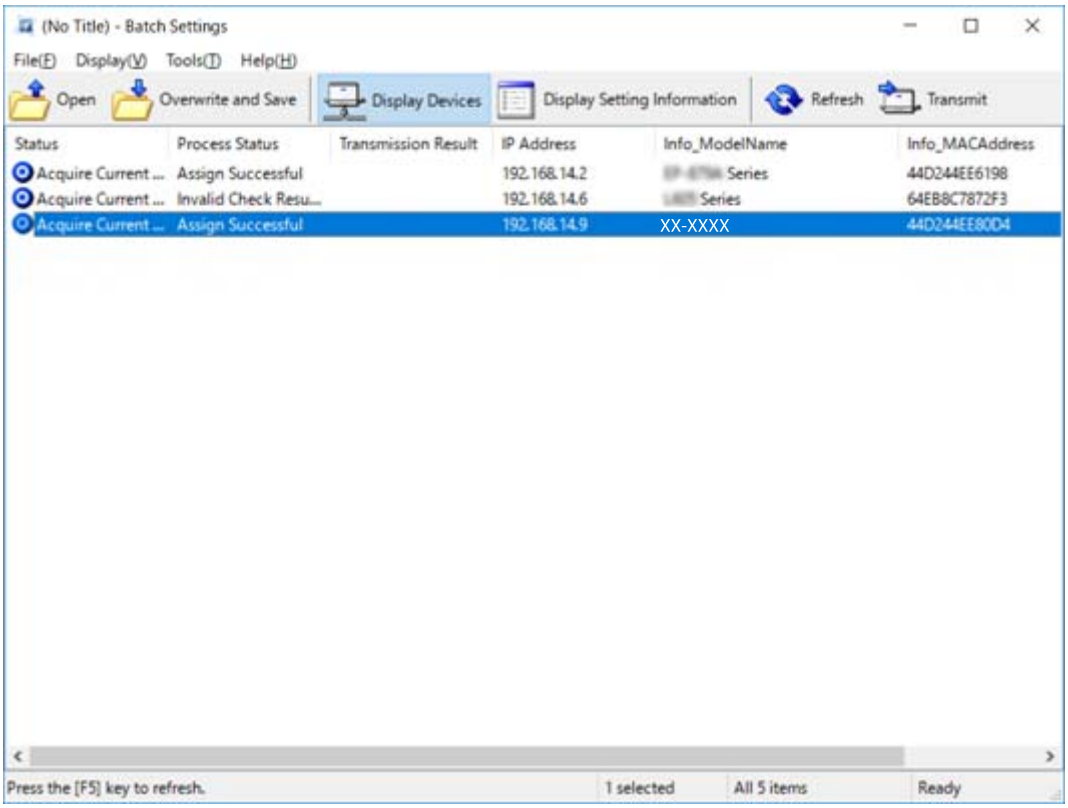
Assegnare contemporaneamente gli indirizzi IP nel file di configurazione (file SYLK). È necessario creare il file di configurazione prima di effettuare l'assegnazione.

1. Collegare tutti i dispositivi alla rete utilizzando cavi Ethernet.
2. Accendere lo scanner.
3. Avviare EpsonNet Config.

   Viene visualizzato un elenco degli scanner sulla rete. La visualizzazione degli scanner potrebbe richiedere del tempo.
4. Fare clic su **Tools** > **Batch Settings**.
5. Fare clic su **Open**.
6. Nella schermata di selezione del file, selezionare il file SYLK (*.slk) contenente le impostazioni, quindi fare clic su **Open**.

7. Selezionare i dispositivi per i quali si desidera eseguire le impostazioni batch impostando la colonna di **Status** su **Unassigned** e lo **Process Status** su **Assign Successful**.

   Quando si effettuano selezioni multiple, premere Ctrl o Shift e fare clic o trascinare con il mouse.




8. Fare clic su **Transmit**.

9. Quando viene visualizzata la schermata per l'immissione della password, inserire la password e fare clic su **OK**.

   Trasmettere le impostazioni.

   ***Nota:***
   *Le informazioni vengono trasmesse all'interfaccia di rete fino al completamento della barra di avanzamento. Non spegnere il dispositivo o l'adattatore wireless e non inviare tutti i dati al dispositivo.*

10. Nella schermata **Transmitting Settings**, fare clic su **OK**.

11. Controllare lo stato del dispositivo impostato.

    Per i dispositivi che visualizzano  o  , verificare il contenuto del file di impostazioni o assicurarsi che il dispositivo sia stato riavviato correttamente.

| Icona | Status | Process Status | Descrizione |
|---|---|---|---|
|  | Setup Complete | Setup Successful | Impostazione completata correttamente. |
|  | Setup Complete | Rebooting | Quando le informazioni sono state trasmesse, è necessario riavviare tutti i dispositivi per applicare le impostazioni. Viene eseguito un controllo per determinare se il dispositivo può essere collegato dopo il riavvio. |
|  | Setup Complete | Reboot Failed | Impossibile confermare il dispositivo dopo la trasmissione delle impostazioni. Verificare che il dispositivo sia acceso o che sia stato riavviato correttamente. |
|  | Setup Complete | Searching | Ricerca del dispositivo indicato nel file delle impostazioni.* |
|  | Setup Complete | Search Failed | Impossibile controllare i dispositivi che sono già stati impostati. Verificare che il dispositivo sia acceso o che sia stato riavviato correttamente.* |

    * Solo quando vengono visualizzate le informazioni di configurazione.

**Informazioni correlate**

➡ "Esecuzione di EpsonNet Config — Windows" a pagina 56

➡ "Esecuzione di EpsonNet Config — Mac OS" a pagina 56

# Assegnazione di un indirizzo IP a ciascun dispositivo

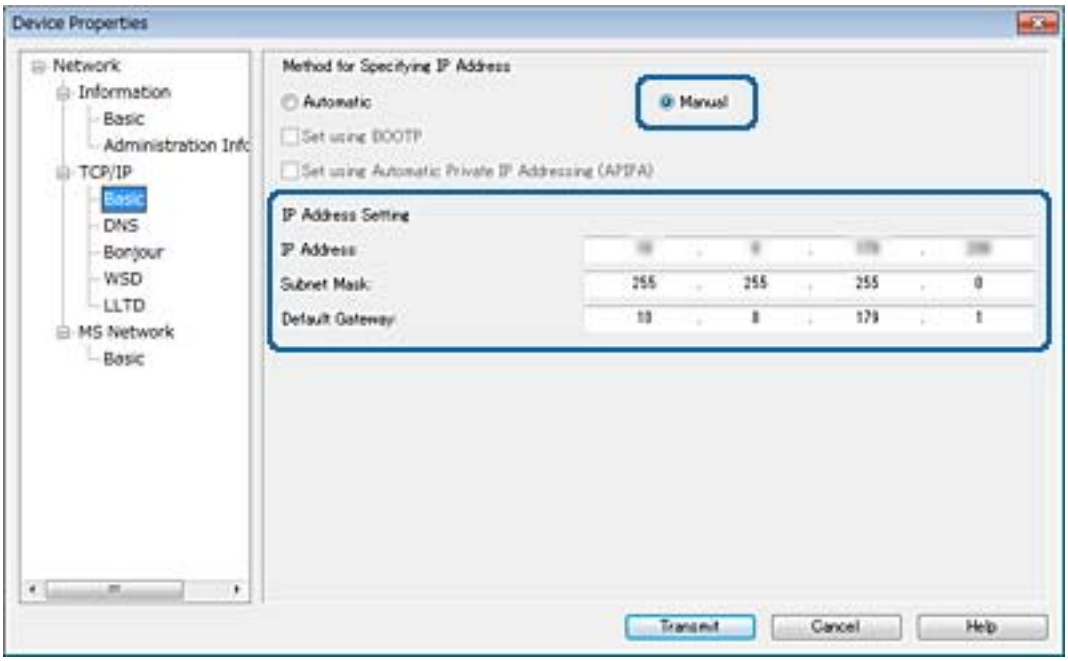
Assegnare un indirizzo IP allo scanner mediante EpsonNet Config.

1. Accendere lo scanner.
2. Collegare lo scanner alla rete utilizzando un cavo Ethernet.
3. Avviare EpsonNet Config.

   Viene visualizzato un elenco degli scanner sulla rete. La visualizzazione degli scanner potrebbe richiedere del tempo.
4. Fare doppio clic sullo scanner da assegnare.

   ***Nota:***
   *Se sono collegati più scanner dello stesso modello, è possibile identificare lo scanner tramite l'indirizzo MAC.*
5. Selezionare **Network** > **TCP/IP** > **Basic**.

6. Inserire gli indirizzi per **IP Address**, **Subnet Mask** e **Default Gateway**.




***Nota:***
*Inserire un indirizzo statico quando si collega lo scanner a una rete sicura.*

7. Fare clic su **Transmit**.

   Viene visualizzata la schermata che conferma la trasmissione delle informazioni.

8. Fare clic su **OK**.

   Viene visualizzata la schermata di completamento della trasmissione.

   ***Nota:***
   *Le informazioni vengono trasmesse al dispositivo, quindi appare il messaggio "Configurazione completata con successo". Non spegnere il dispositivo e non inviare dati al servizio.*

9. Fare clic su **OK**.

### Informazioni correlate

➡ "Esecuzione di EpsonNet Config — Windows" a pagina 56
➡ "Esecuzione di EpsonNet Config — Mac OS" a pagina 56

# Utilizzo della porta per lo scanner

Lo scanner utilizza la seguente porta. Se necessario, l'amministratore di rete dovrebbe rendere disponibili queste porte.

## Appendice

| Mittente (Client) | Usa | Destinazione (Server) | Protocollo | Numero di porta |
|---|---|---|---|---|
| Scanner | Invio e-mail (notifica e-mail) | Server SMTP | SMTP (TCP) | 25 |
| | | | SMTP SSL/TLS (TCP) | 465 |
| | | | SMTP STARTTLS (TCP) | 587 |
| | POP prima della connessione SMTP (notifica e-mail) | Server POP | POP3 (TCP) | 110 |
| | Controllo WSD | Computer client | WSD (TCP) | 5357 |
| | Ricercare il computer quando viene eseguita la funzione Push Scan da Document Capture Pro | Computer client | Rilevamento scansione Push di rete | 2968 |
| | Raccolta di informazioni sul lavoro quando viene eseguita la funzione Push Scan da Document Capture Pro | Computer client | Scansione Push di rete | 2968 |
| Computer client | Rilevare lo scanner da un'applicazione come EpsonNet Config e dal driver dello scanner. | Scanner | ENPC (UDP) | 3289 |
| | Raccogliere e configurare le informazioni MIB da un'applicazione come EpsonNet Config e dal driver dello scanner. | Scanner | SNMP (UDP) | 161 |
| | Ricerca di uno scanner WSD | Scanner | WS-Discovery (UDP) | 3702 |
| | Inoltro dei dati di scansione da Document Capture Pro | Scanner | Scansione di rete (TCP) | 1865 |

# Impostazioni di sicurezza avanzate per Enterprise

In questo capitolo verranno illustrate le funzioni di sicurezza avanzate.

## Impostazioni di sicurezza e prevenzione del pericolo

Quando un dispositivo è collegato a una rete, è possibile accedervi da una postazione remota. Inoltre, molte persone possono condividere il dispositivo, un'opzione utile per migliorare l'efficienza operativa e la convenienza. Tuttavia, i rischi quali l'accesso e l'uso illegale e la manomissione sono aumentati. Se si utilizza il dispositivo in un ambiente con accesso a Internet, i rischi sono ancora maggiori.

Per evitare questo rischio, i dispositivi Epson dispongono di una varietà di tecnologie di sicurezza.

Impostare il dispositivo come necessario in base alle condizioni ambientali che sono state create con le informazioni relative all'ambiente del cliente.

| Nome | Tipo di funzione | Cosa impostare | Cosa evitare |
|---|---|---|---|
| Comunicazione SSL/TLS | Il percorso di comunicazione di un computer e di un dispositivo vengono crittografati mediante la comunicazione SSL/TLS. Il contenuto della comunicazione tramite un browser è protetto. | Impostare un certificato CA per il server, un certificato firmato da una CA (Certificate Authority) per il dispositivo. | Impedire la fuga di informazioni sulle impostazioni e dei contenuti dei dati trasferiti dal computer allo scanner. È inoltre possibile proteggere l'accesso al server Epson su Internet dal dispositivo tramite un aggiornamento del firmware, per esempio. |
| IPsec/IP filtering | È possibile impostare questa opzione per consentire l'eliminazione dei dati che provengono da un determinato client o di un tipo particolare. Poiché IPsec protegge i dati per unità di pacchetti IP (crittografia e autenticazione), è possibile comunicare in modo sicuro protocolli di scansione non protetti. | Stabilire un criterio di base e individuale per impostare il client o il tipo di dati che possono accedere al dispositivo. | Proteggere l'accesso non autorizzato, la manomissione e l'intercettazione dei dati di comunicazione al dispositivo. |
| SNMPv3 | Sono state aggiunte caratteristiche quali il monitoraggio dei dispositivi collegati sulla rete, l'integrità dei dati per il controllo del protocollo SNMP, la crittografia, l'autenticazione degli utenti, ecc. | Attivare SNMPv3, quindi impostare il metodo di autenticazione e crittografia. | Garantire la modifica delle impostazioni attraverso la rete e la riservatezza nel monitoraggio dello stato. |

| Nome | Tipo di funzione | Cosa impostare | Cosa evitare |
|---|---|---|---|
| IEEE802.1X | Consente la connessione solo a un utente che è autenticato a Ethernet. Consente solo a un utente autorizzato di utilizzare il dispositivo. | Impostazione di autenticazione al server RADIUS (server di autenticazione). | Proteggere l'accesso e l'utilizzo non autorizzato del dispositivo. |
| Lettura della scheda ID | È possibile utilizzare il dispositivo avvicinando una scheda ID al dispositivo autenticato collegato. È possibile limitare l'acquisizione dei log per ciascun utente e dispositivo e limitare l'uso dei dispositivi e delle funzioni disponibili di ogni utente e gruppo. | Collegare un dispositivo di autenticazione al dispositivo, quindi impostare le informazioni di un utente nel sistema di autenticazione. | Impedire l'utilizzo non autorizzato del dispositivo e truffe in rete. |

**Informazioni correlate**

➡ “Comunicazione SSL/TLS con lo scanner” a pagina 63
➡ “Comunicazione crittografata tramite IPsec/IP Filtering” a pagina 71
➡ “Uso del protocollo SNMPv3” a pagina 83
➡ “Connessione dello scanner a una rete IEEE802.1X” a pagina 85

## Impostazioni delle funzioni di sicurezza

Se si imposta IPsec/IP filtering o IEEE802.1X, si consiglia di accedere a Web Config utilizzando l'SSL o il TLS per comunicare le informazioni relative alle impostazioni al fine di ridurre i rischi per la sicurezza, come la manomissione o l'intercettazione.

# Comunicazione SSL/TLS con lo scanner

Quando si imposta il certificato del server tramite la comunicazione SSL/TLS (Secure Sockets Layer/Transport Layer Security) con lo scanner, è possibile crittografare il percorso di comunicazione tra computer. Effettuare questa operazione se si desidera impedire l'accesso remoto e non autorizzato.

## Informazioni sulla certificazione digitale

❏ Certificato firmato CA

Un certificato firmato da un ente di certificazione CA (Certificate Authority) deve essere ottenuto da un apposito ente. È possibile garantire delle comunicazioni sicure utilizzando un certificato firmato CA. È possibile utilizzare un certificato firmato CA per ciascuna funzione di sicurezza.

❏ Certificato CA

Un certificato CA indica che una terza parte ha verificato l'identità di un server. Risulta essere un componente chiave per un tipo di comunicazione Web sicuro. Occorre ottenere un certificato CA per l'autenticazione server da un ente CA emittente.

❏ Certificato auto-firmato

Il certificato auto-firmato è un certificato emesso e firmato dallo scanner stesso. Tale certificato non è affidabile e non consente di evitare le truffe. Se si utilizza questo certificato per una comunicazione SSL/TLS, un avviso di sicurezza potrebbe venire visualizzato sul browser. È possibile utilizzare questo certificato solo per la comunicazione SSL/TLS.

### Informazioni correlate

➡ "Ottenimento e importazione di un certificato firmato CA" a pagina 64

➡ "Eliminazione di un certificato firmato CA" a pagina 67

➡ "Aggiornamento di un certificato auto-firmato" a pagina 68

# Ottenimento e importazione di un certificato firmato CA

## Ottenimento di un certificato firmato CA

Per ottenere un certificato firmato CA, creare una richiesta CSR (Certificate Signing Request) e inviarla all'ente di certificazione. È possibile creare una richiesta CSR tramite la pagina Web Config e un computer.

Effettuare i passaggi che seguono per creare una richiesta CSR e ottenere un certificato firmato CA utilizzando Web Config. Quando si crea una richiesta CSR tramite Web Config, il certificato sarà in formato PEM/DER.

1. Accedere a Web Config, quindi selezionare **Imp. di protezione rete**. Quindi, selezionare **SSL/TLS** > **Certificato** o **IPsec/Filtro IP** > **Certificato client** o **IEEE802.1X** > **Certificato client**.

2. Fare clic su **Genera** in **CSR**.

   Viene aperta una pagina per la creazione della richiesta CSR.

3. Immettere un valore per ciascuna voce.

   ***Nota:***
   *La lunghezza della chiave e le abbreviazioni disponibili variano a seconda dell'ente di certificazione. Creare una richiesta in base alle regole di ciascun ente di certificazione.*

4. Fare clic su **OK**.

   Viene visualizzato un messaggio di completamento.

5. Selezionare **Imp. di protezione rete**. Quindi, selezionare **SSL/TLS** > **Certificato** o **IPsec/Filtro IP** > **Certificato client** o **IEEE802.1X** > **Certificato client**.

6. Fare clic su uno dei pulsanti di scaricamento di **CSR** in base a un formato specificato da ciascun ente di certificazione per lo scaricamento di una richiesta CSR su un computer.

   ***Importante:***
   *Non generare di nuovo un CSR. In caso contrario, potrebbe non risultare possibile importare un Certificato firma CA emesso.*

7. Inviare la richiesta CSR a un ente di certificazione e ottenere un Certificato firma CA.

   Seguire le regole di ciascun ente di certificazione sul metodo e la forma dell'invio.

8. Salvare il Certificato firma CA emesso su un computer connesso allo scanner.

   L'ottenimento di un Certificato firma CA risulta completato quando si salva il certificato su una destinazione.

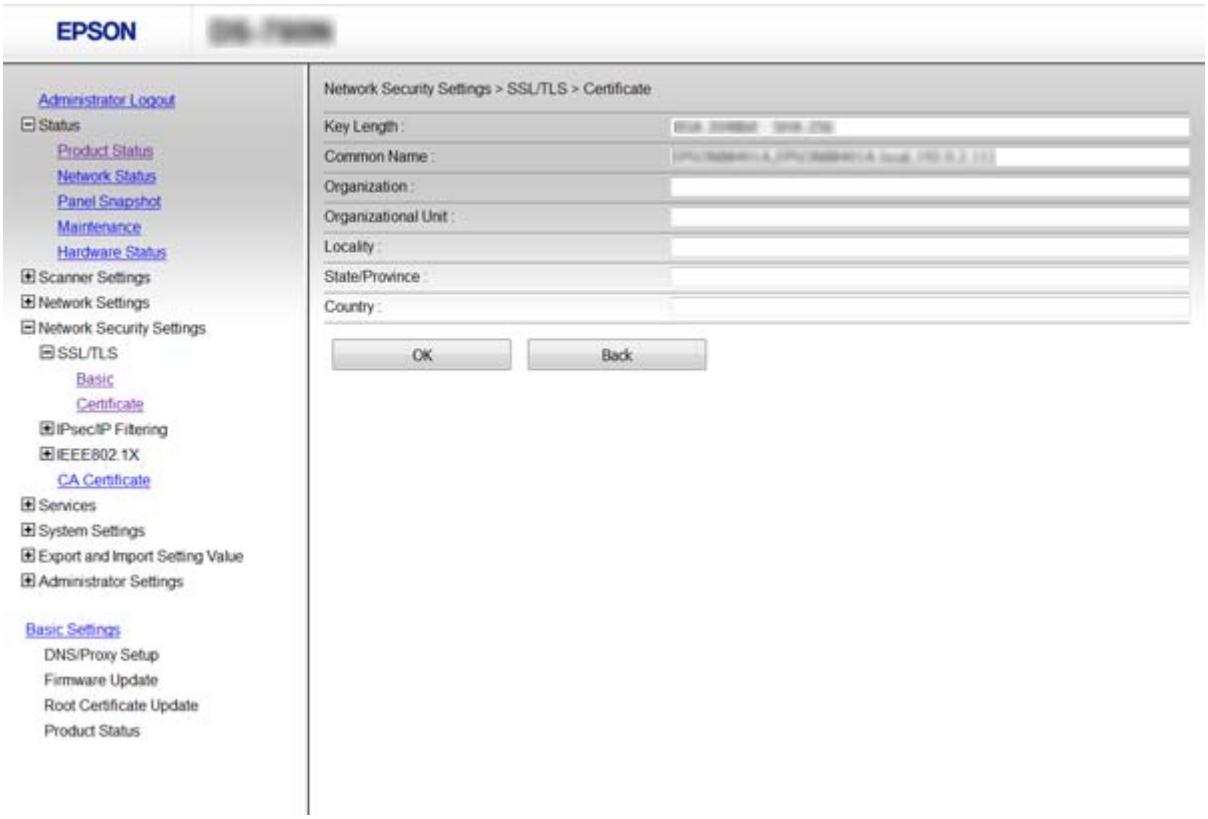
### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

➡ "Voci di impostazione CSR" a pagina 65

➡ "Importazione di un certificato firmato CA" a pagina 66

## *Voci di impostazione CSR*




| Elementi | Impostazioni e descrizione |
|---|---|
| Lunghezza chiave | Selezionare una lunghezza di chiave per una richiesta CSR. |
| Nome comune | È possibile inserire da 1 a 128 caratteri. Se si tratta di un indirizzo IP, l'indirizzo deve essere di tipo statico.<br>Esempio:<br>URL per l'accesso a Web Config: https://10.152.12.225<br>Nome comune: 10.152.12.225 |
| Organizzazione/ Unità organizzativa/ Località/ Stato/Provincia | È possibile immettere tra 0 e 64 caratteri in ASCII (0x20–0x7E). È possibile separare i nomi distinti tramite virgole. |
| Paese | Immettere un codice paese in numero a due cifre specificato da ISO-3166. |

### Informazioni correlate

➡ "Ottenimento di un certificato firmato CA" a pagina 64

## Importazione di un certificato firmato CA

***Importante:***

❏ *Assicurarsi che la data e l'ora dello scanner siano impostate correttamente.*

❏ *Se si ottiene un certificato tramite una richiesta CSR creata da Web Config, è possibile importare un certificato una volta.*

1. Accedere a Web Config, quindi selezionare **Imp. di protezione rete**. Quindi, selezionare **SSL/TLS** > **Certificato** o **IPsec/Filtro IP** > **Certificato client** o **IEEE802.1X** > **Certificato client**.

2. Fare clic su **Importa**.

   Viene aperta una pagina per l'importazione del certificato.

3. Immettere un valore per ciascuna voce.

   A seconda dell'ente presso il quale si richiede un CSR e del formato file del certificato, le impostazioni richieste possono variare. Immettere i valori per le voci richieste in base a quanto segue.

   ❏ Certificato in formato PEM/DER ottenuto tramite Web Config

      ❏ **Chiave privata**: Non configurare in quanto lo scanner contiene una chiave privata.

      ❏ **Password**: Non configurare.

      ❏ **Certificato CA 1**/**Certificato CA 2**: Opzionale

   ❏ Certificato in formato PEM/DER ottenuto tramite un computer

      ❏ **Chiave privata**: Impostazione necessaria.

      ❏ **Password**: Non configurare.

      ❏ **Certificato CA 1**/**Certificato CA 2**: Opzionale

   ❏ Certificato in formato PKCS#12 ottenuto tramite un computer

      ❏ **Chiave privata**: Non configurare.

      ❏ **Password**: Opzionale

      ❏ **Certificato CA 1**/**Certificato CA 2**: Non configurare.

4. Fare clic su **OK**.

   Viene visualizzato un messaggio di completamento.

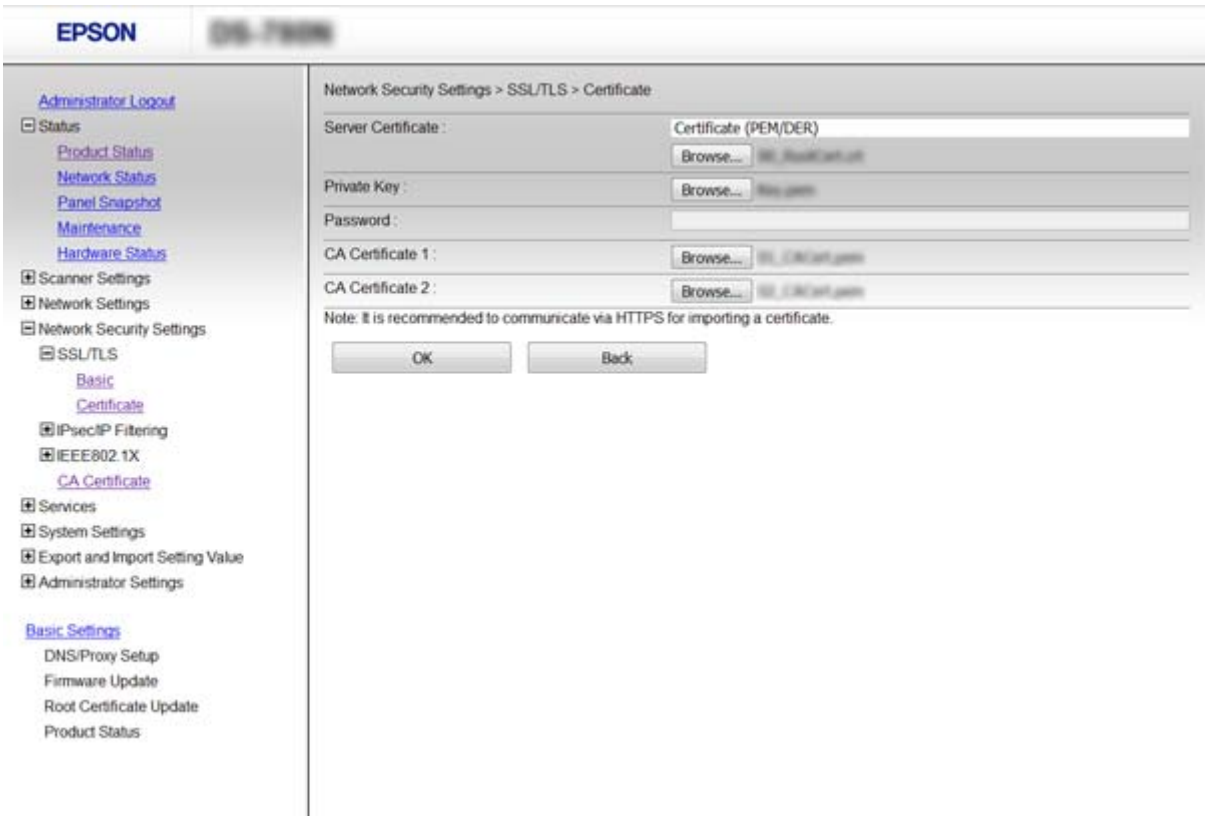
***Nota:***
*Fare clic su* ***Conferma*** *per verificare le informazioni del certificato.*

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

➡ "Voci di impostazione per l'importazione del certificato firmato CA" a pagina 67

### *Voci di impostazione per l'importazione del certificato firmato CA*




| Voci | Impostazioni e descrizione |
|---|---|
| Certificato server o Certificato client | Selezionare un formato di certificato. |
| Chiave privata | Se si ottiene un certificato di formato PEM/DER tramite una richiesta CSR da un computer, specificare un file di chiave privata che corrisponda al certificato. |
| Password | Immettere una password per crittografare la chiave privata. |
| Certificato CA 1 | Se il formato del certificato è **Certificato (PEM/DER)**, importare un certificato di un ente di certificazione che emette un certificato server. Specificare un file, se necessario. |
| Certificato CA 2 | Se il formato del certificato è **Certificato (PEM/DER)**, importare un certificato di un ente di certificazione che emette un certificato **Certificato CA 1**. Specificare un file, se necessario. |

#### Informazioni correlate

➡ "Importazione di un certificato firmato CA" a pagina 66

## Eliminazione di un certificato firmato CA

È possibile eliminare un certificato importato quando il certificato scade o quando una connessione crittografata non è più necessaria.

> ***Importante:***
> *Se si ottiene un certificato tramite una richiesta CSR creata da Web Config, non è possibile importare di nuovo un certificato eliminato. In tal caso, creare una richiesta CSR e ottenere di nuovo un certificato.*

1. Accedere a Web Config, quindi selezionare **Imp. di protezione rete**. Quindi, selezionare **SSL/TLS** > **Certificato** o **IPsec/Filtro IP** > **Certificato client** o **IEEE802.1X** > **Certificato client**.
2. Fare clic su **Elimina**.
3. Confermare l'eliminazione del certificato nel messaggio visualizzato.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Aggiornamento di un certificato auto-firmato

Se lo scanner supporta la funzione di server HTTPS, è possibile aggiornare un certificato auto-firmato. Quando si accede a Web Config utilizzando un certificato auto-firmato, appare un messaggio di avvertenza.

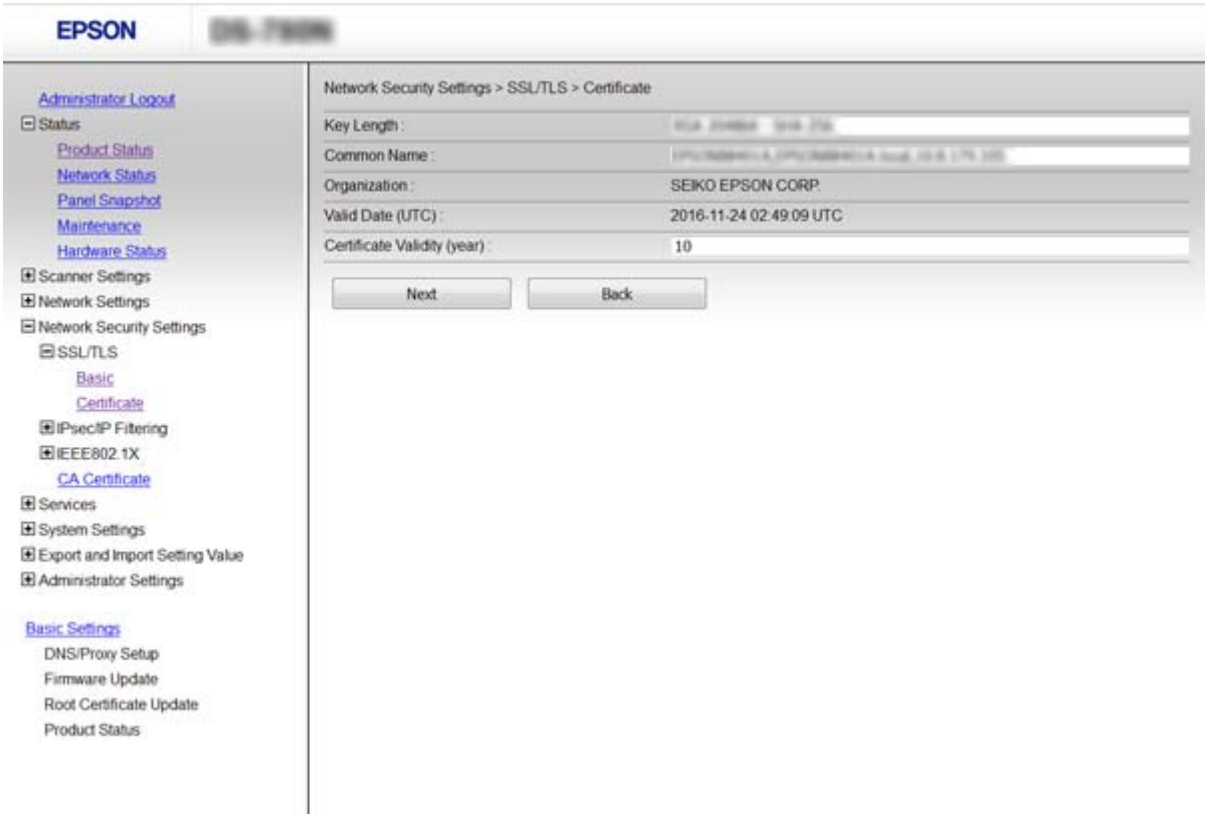
Utilizzare un certificato auto-firmato temporaneamente mentre si attende di ottenere e importare un certificato firmato CA.

1. Accedere a Web Config e selezionare **Imp. di protezione rete** > **SSL/TLS** > **Certificato**.
2. Fare clic su **Aggiorna**.
3. Immettere **Nome comune**.

   Immettere un indirizzo IP o un identificatore quale un nome FQDN per lo scanner. È possibile inserire da 1 a 128 caratteri.

   ***Nota:***
   *È possibile separare i nomi distinti (CN) tramite virgole.*

4. Specificare un periodo di validità per il certificato.




5. Fare clic su **Avanti**.

   Viene visualizzato un messaggio di conferma.

6. Fare clic su **OK**.

   Lo scanner viene aggiornato.

***Nota:***
*Fare clic su **Conferma** per verificare le informazioni del certificato.*

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

# Configurazione di Certificato CA

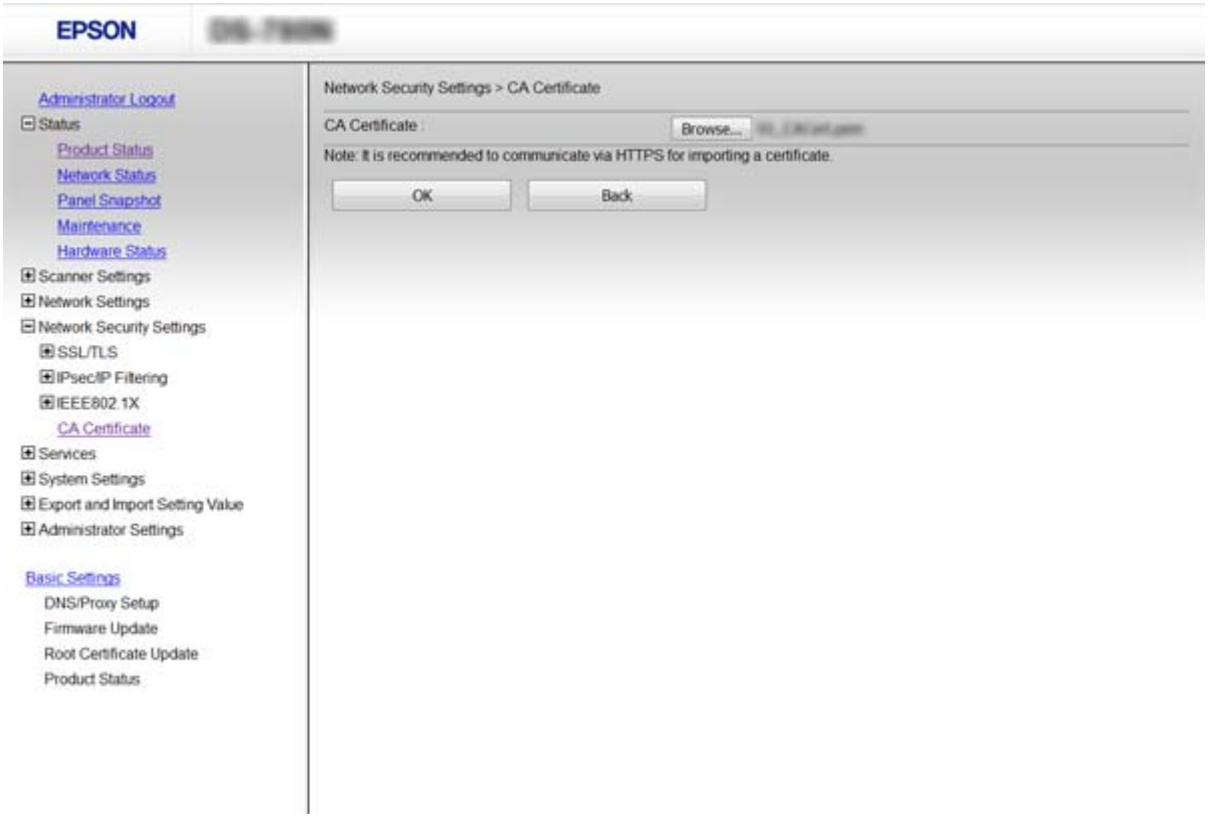
È possibile importare, visualizzare ed eliminare un Certificato CA.

## Importazione di un Certificato CA

1. Accedere a Web Config, quindi selezionare **Imp. di protezione rete** > **Certificato CA**.

2. Fare clic su **Importa**.

3. Specificare il Certificato CA che si desidera importare.




4. Fare clic su **OK**.

Al termine dell'importazione, si torna alla schermata **Certificato CA** e viene visualizzato il Certificato CA importato.

### Informazioni correlate

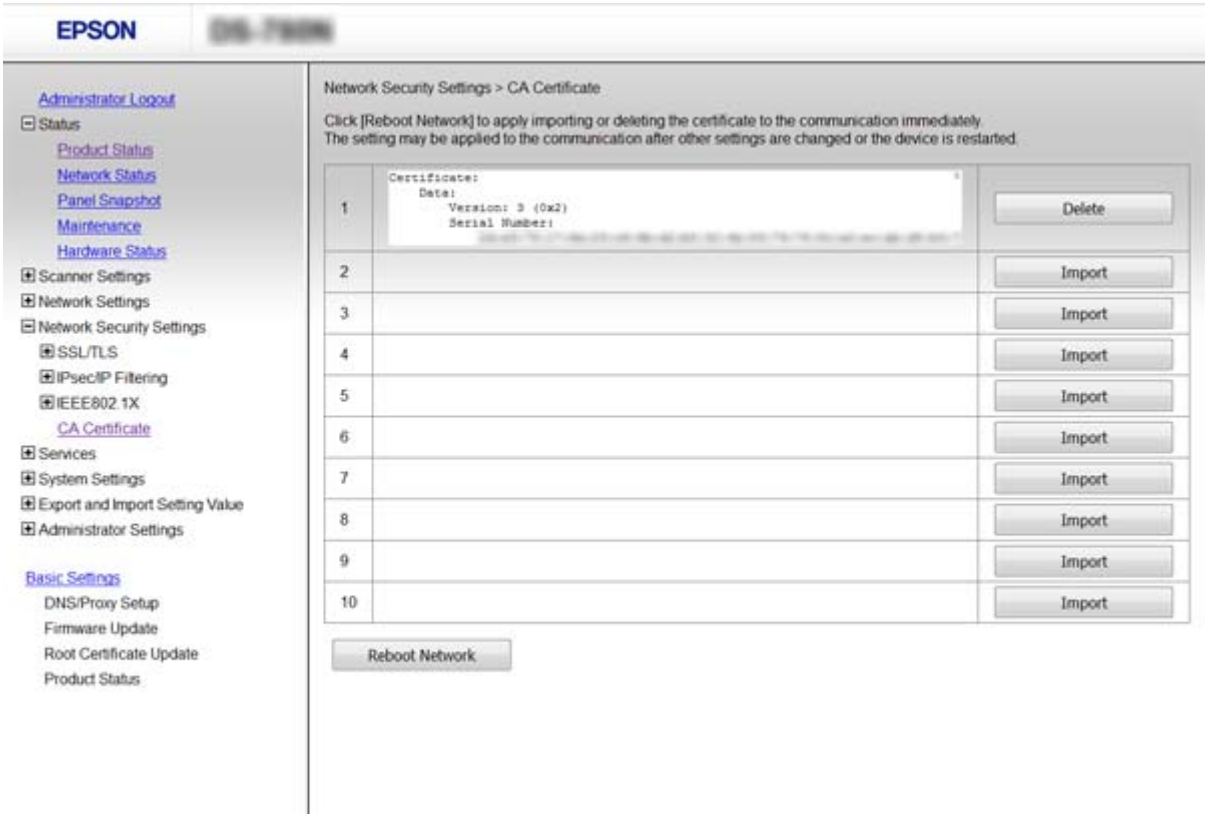
➡ "Accesso a Web Config" a pagina 23

## Eliminazione di un Certificato CA

È possibile eliminare il Certificato CA importato.

1. Accedere a Web Config, quindi selezionare **Imp. di protezione rete** > **Certificato CA**.

2. Fare clic su **Elimina** accanto al Certificato CA che si desidera eliminare.




3. Confermare l'eliminazione del certificato nel messaggio visualizzato.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

# Comunicazione crittografata tramite IPsec/IP Filtering

## Informazioni su IPsec/Filtro IP

Se lo scanner supporta IPsec/IP Filtering, è possibile filtrare il traffico in base agli indirizzi IP, ai servizi e alla porta. Tramite le combinazioni del filtro, è possibile configurare lo scanner per accettare o bloccare i client e i dati specificati. Inoltre, è possibile migliorare il livello di sicurezza utilizzando il filtro IPsec.

Per filtrare il traffico, configurare i criteri predefiniti. I criteri predefiniti vengono applicati a ogni utente o gruppo che si connette allo scanner. Per un controllo maggiormente dettagliato su utenti o gruppi di utenti, configurare i criteri di gruppo. I criteri di gruppo sono costituiti da una o più regole da applicare a utenti o gruppi di utenti. Lo scanner controlla i pacchetti IP che corrispondono ai criteri configurati. I pacchetti IP vengono autenticati dapprima in base ai criteri di gruppo, da 1 a 10, quindi in base ai criteri predefiniti.

***Nota:***
*I computer che eseguono Windows Vista o versioni più recenti, oppure Windows Server 2008 o versioni più recenti, supportano IPsec.*

# Configurazione di Criteri predefiniti

1. Accedere a Web Config e selezionare **Imp. di protezione rete** > **IPsec/Filtro IP** > **Di base**.
2. Immettere un valore per ciascuna voce.
3. Fare clic su **Avanti**.

   Viene visualizzato un messaggio di conferma.
4. Fare clic su **OK**.

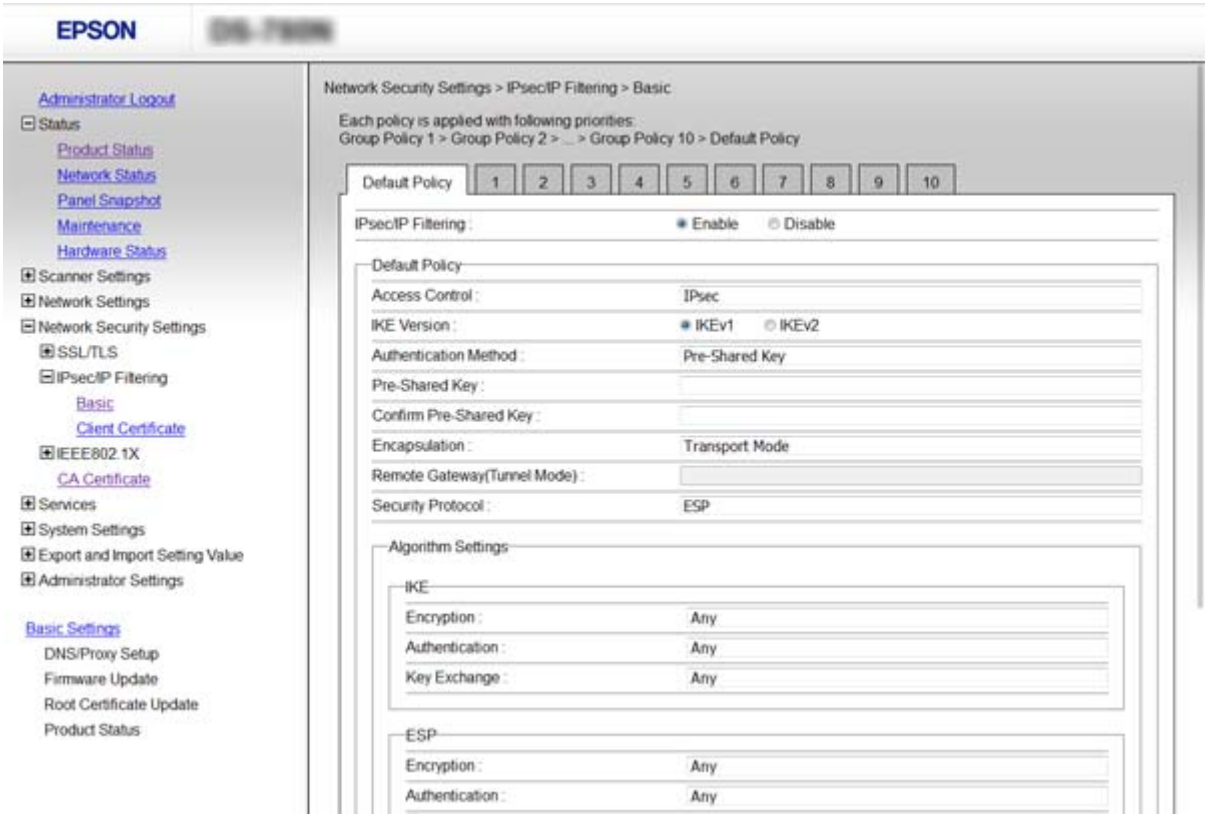
   Lo scanner viene aggiornato.

### Informazioni correlate

➡ “Accesso a Web Config” a pagina 23

➡ “Voci di impostazione di Criteri predefiniti” a pagina 72

## Voci di impostazione di Criteri predefiniti




| Elementi | Impostazioni e descrizione |
|---|---|
| IPsec/Filtro IP | È possibile abilitare o disabilitare una funzione di IPsec/IP Filtering. |

## Impostazioni di sicurezza avanzate per Enterprise

| Elementi | Impostazioni e descrizione | |
|---|---|---|
| Controllo accesso | Configurare un metodo di controllo per il traffico dei pacchetti IP. | |
| | Consenti accesso | Selezionare questa opzione per consentire la ricezione dei pacchetti IP configurati. |
| | Rifiuta accesso | Selezionare questa opzione per respingere la ricezione dei pacchetti IP configurati. |
| | IPsec | Selezionare questa opzione per consentire la ricezione dei pacchetti IPsec. |
| Versione IKE | Selezionare IKEv1 o IKEv2 per la versione IKE.<br>Selezionare una delle voci a seconda del dispositivo collegato allo scanner. | |
| IKEv1 | Quando si seleziona **IKEv1** per la **Versione IKE** vengono visualizzati i seguenti elementi. | |
| | Metodo autenticazione | Per selezionare **Certificato**, occorre ottenere e importare preventivamente un certificato firmato CA. |
| | Chiave precondivisa | Se si seleziona **Chiave precondivisa** per **Metodo autenticazione**, immettere una chiave pre-condivisa contenente da 1 a 127 caratteri. |
| | Chiave precondivisa già condivisa | Immettere la chiave configurata per conferma. |
| IKEv2 | Quando si seleziona **IKEv2** per la **Versione IKE** vengono visualizzati i seguenti elementi. | |
| Locale | Metodo autenticazione | Per selezionare **Certificato**, occorre ottenere e importare preventivamente un certificato firmato CA. |
| | Tipo ID | Selezionare il tipo di ID per lo scanner. |
| | ID | Inserire l'ID dello scanner che corrisponde al tipo di ID.<br>Non è possibile utilizzare "@", "#" e "=" come primo carattere.<br>**Nome distintivo**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=".<br>**Indirizzo IP**: immettere il formato IPv4 o IPv6.<br>**FQDN**: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, 0–9, "-" e il punto (.).<br>**Indirizzo e-mail**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@".<br>**ID chiave**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. |
| | Chiave precondivisa | Se si seleziona **Chiave precondivisa** per **Metodo autenticazione**, immettere una chiave pre-condivisa contenente da 1 a 127 caratteri. |
| | Chiave precondivisa già condivisa | Immettere la chiave configurata per conferma. |

## Impostazioni di sicurezza avanzate per Enterprise

| Elementi | Impostazioni e descrizione | |
|---|---|---|
| Remoto | Metodo autenticazione | Per selezionare **Certificato**, occorre ottenere e importare preventivamente un certificato firmato CA. |
| | Tipo ID | Selezionare il tipo di ID per il dispositivo da autenticare. |
| | ID | Inserire l'ID dello scanner che corrisponde al tipo di ID.<br>Non è possibile utilizzare "@", "#" e "=" come primo carattere.<br>**Nome distintivo**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=".<br>**Indirizzo IP**: immettere il formato IPv4 o IPv6.<br>**FQDN**: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, 0–9, "-" e il punto (.).<br>**Indirizzo e-mail**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@".<br>**ID chiave**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. |
| | Chiave precondivisa | Se si seleziona **Chiave precondivisa** per **Metodo autenticazione**, immettere una chiave pre-condivisa contenente da 1 a 127 caratteri. |
| | Chiave precondivisa già condivisa | Immettere la chiave configurata per conferma. |
| Incapsulazione | Se si seleziona **IPsec** per **Controllo accesso**, occorre configurare un modo di incapsulazione. | |
| | Modo Trasporto | Se si utilizza lo scanner soltanto sulla stessa LAN, selezionare questa opzione. I pacchetti IP di livello 4 o successivo sono crittografati. |
| | Modo Tunnel | Se si utilizza lo scanner nella rete con accesso a Internet come IPsec-VPN, selezionare questa opzione. L'intestazione e i dati dei pacchetti IP sono crittografati. |
| Indirizzo gateway remoto | Se si seleziona **Modo Tunnel** per **Incapsulazione**, immettere un indirizzo gateway contenente da 1 a 39 caratteri. | |
| Protocollo sicurezza | **IPsec** per **Controllo accesso**, selezionare un'opzione. | |
| | ESP | Selezionare questa opzione per garantire l'integrità di un'autenticazione e dei dati e per crittografare i dati. |
| | AH | Selezionare questa opzione per garantire l'integrità di un'autenticazione e dei dati. Anche se la crittografia dei dati è proibita, è possibile utilizzare IPsec. |
| Impostazioni algoritmo | | |
| IKE | Crittografia | Selezionare l'algoritmo di crittografia per IKE.<br>Le voci variano a seconda della versione di IKE. |
| | Autenticazione | Selezionare l'algoritmo di autenticazione per IKE. |
| | Scambio chiave | Selezionare l'algoritmo di sostituzione chiave per IKE.<br>Le voci variano a seconda della versione di IKE. |

**Impostazioni di sicurezza avanzate per Enterprise**

| Elementi | Impostazioni e descrizione | |
|---|---|---|
| ESP | Crittografia | Selezionare l'algoritmo di crittografia per ESP.<br>Ciò è disponibile quando come **Protocollo sicurezza** è impostato **ESP**. |
| | Autenticazione | Selezionare l'algoritmo di autenticazione per ESP.<br>Ciò è disponibile quando come **Protocollo sicurezza** è impostato **ESP**. |
| AH | Autenticazione | Selezionare l'algoritmo di crittografia per AH.<br>Ciò è disponibile quando come **Protocollo sicurezza** è impostato **AH**. |

### Informazioni correlate

➡ "Configurazione di Criteri predefiniti" a pagina 72

## Configurazione di Criteri gruppo

1. Accedere a Web Config e selezionare **Imp. di protezione rete** > **IPsec/Filtro IP** > **Di base**.
2. Fare clic su una scheda numerata che si desidera configurare.
3. Immettere un valore per ciascuna voce.
4. Fare clic su **Avanti**.

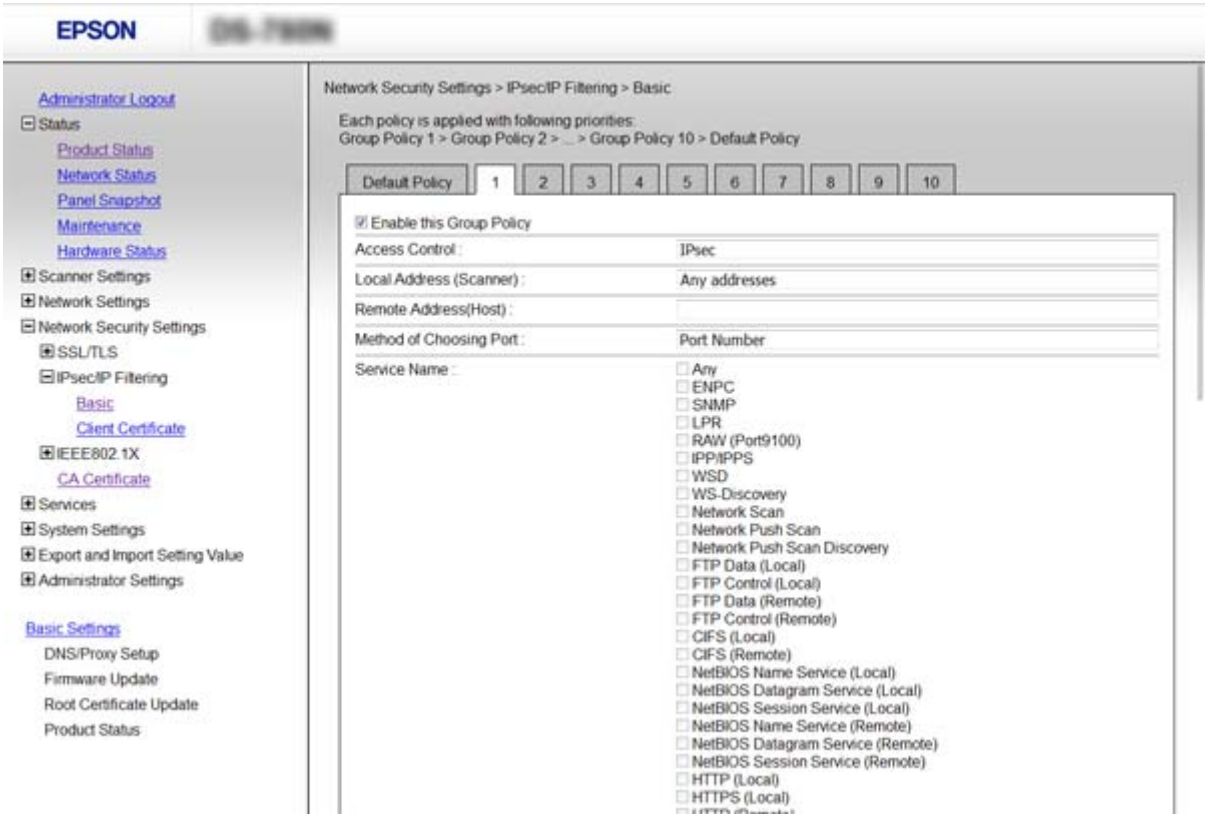
   Viene visualizzato un messaggio di conferma.
5. Fare clic su **OK**.

   Lo scanner viene aggiornato.

### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23
➡ "Voci di impostazione di Criteri gruppo" a pagina 76

## Voci di impostazione di Criteri gruppo




| Elementi | Impostazioni e descrizione | |
|---|---|---|
| Abilita criterio di gruppo | È possibile abilitare o disabilitare i criteri di gruppo. | |
| Controllo accesso | Configurare un metodo di controllo per il traffico dei pacchetti IP. | |
| | Consenti accesso | Selezionare questa opzione per consentire la ricezione dei pacchetti IP configurati. |
| | Rifiuta accesso | Selezionare questa opzione per respingere la ricezione dei pacchetti IP configurati. |
| | IPsec | Selezionare questa opzione per consentire la ricezione dei pacchetti IPsec. |
| Indirizzo locale (scanner) | Selezionare un indirizzo IPv4 o IPv6 che corrisponda al proprio ambiente di rete. Se un indirizzo IP viene assegnato automaticamente, è possibile selezionare **Usa indirizzo IPv4 ottenuto automaticamente**. | |
| Indirizzo remoto(Host) | Immettere l'indirizzo IP di un dispositivo per controllarne l'accesso. L'indirizzo IP deve contenere un massimo di 43 caratteri. Se non viene immesso un indirizzo IP, vengono controllati tutti gli indirizzi.<br>***Nota:***<br>*Se un indirizzo IP viene assegnato automaticamente (ad esempio, tramite DHCP), la connessione potrebbe risultare non disponibile. Configurare un indirizzo IP statico.* | |
| Metodo di scelta porta | Selezionare un metodo per specificare le porte. | |
| Nome servizio | Se si seleziona **Nome servizio** per **Metodo di scelta porta**, selezionare un'opzione. | |

## Impostazioni di sicurezza avanzate per Enterprise

| Elementi | Impostazioni e descrizione | |
|---|---|---|
| Protocollo trasporto | Se si seleziona **Numero porta** per **Metodo di scelta porta**, occorre configurare un modo di incapsulazione. | |
| | Qualsiasi protocollo | Selezionare questa opzione per controllare tutti i tipi di protocollo. |
| | TCP | Selezionare questa opzione per controllare i dati per unicast. |
| | UDP | Selezionare questa opzione per controllare i dati per broadcast e multicast. |
| | ICMPv4 | Selezionare questa opzione per controllare il comando ping. |
| Porta locale | Se si seleziona **Numero porta** per **Metodo di scelta porta** e se si seleziona **TCP** o **UDP** per **Protocollo trasporto**, inserire i numeri di porta per controllare la ricezione di pacchetti, separandoli con una virgola. È possibile immettere un massimo di 10 numeri di porta.<br>Esempio: 20,80,119,5220<br>Se non viene immesso un numero di porta, vengono controllate tutte le porte. | |
| Porta remota | Se si seleziona **Numero porta** per **Metodo di scelta porta** e se si seleziona **TCP** o **UDP** per **Protocollo trasporto**, inserire i numeri di porta per controllare l'invio di pacchetti, separandoli con una virgola. È possibile immettere un massimo di 10 numeri di porta.<br>Esempio: 25,80,143,5220<br>Se non viene immesso un numero di porta, vengono controllate tutte le porte. | |
| Versione IKE | Selezionare IKEv1 o IKEv2 per la versione IKE.<br>Selezionare una delle voci a seconda del dispositivo collegato allo scanner. | |
| IKEv1 | Quando si seleziona **IKEv1** per la **Versione IKE** vengono visualizzati i seguenti elementi. | |
| | Metodo autenticazione | Se si seleziona **IPsec** per **Controllo accesso**, selezionare un'opzione. Il certificato usato è comune con criteri predefiniti. |
| | Chiave precondivisa | Se si seleziona **Chiave precondivisa** per **Metodo autenticazione**, immettere una chiave pre-condivisa contenente da 1 a 127 caratteri. |
| | Chiave precondivisa già condivisa | Immettere la chiave configurata per conferma. |
| IKEv2 | Quando si seleziona **IKEv2** per la **Versione IKE** vengono visualizzati i seguenti elementi. | |

## Impostazioni di sicurezza avanzate per Enterprise

| Elementi | Impostazioni e descrizione | |
|---|---|---|
| Locale | Metodo autenticazione | Se si seleziona **IPsec** per **Controllo accesso**, selezionare un'opzione. Il certificato usato è comune con criteri predefiniti. |
| | Tipo ID | Selezionare il tipo di ID per lo scanner. |
| | ID | Inserire l'ID dello scanner che corrisponde al tipo di ID.<br>Non è possibile utilizzare "@", "#" e "=" come primo carattere.<br>**Nome distintivo**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=".<br>**Indirizzo IP**: immettere il formato IPv4 o IPv6.<br>**FQDN**: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, 0–9, "-" e il punto (.).<br>**Indirizzo e-mail**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@".<br>**ID chiave**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. |
| | Chiave precondivisa | Se si seleziona **Chiave precondivisa** per **Metodo autenticazione**, immettere una chiave pre-condivisa contenente da 1 a 127 caratteri. |
| | Chiave precondivisa già condivisa | Immettere la chiave configurata per conferma. |
| Remoto | Metodo autenticazione | Se si seleziona **IPsec** per **Controllo accesso**, selezionare un'opzione. Il certificato usato è comune con criteri predefiniti. |
| | Tipo ID | Selezionare il tipo di ID per il dispositivo da autenticare. |
| | ID | Inserire l'ID dello scanner che corrisponde al tipo di ID.<br>Non è possibile utilizzare "@", "#" e "=" come primo carattere.<br>**Nome distintivo**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=".<br>**Indirizzo IP**: immettere il formato IPv4 o IPv6.<br>**FQDN**: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, 0–9, "-" e il punto (.).<br>**Indirizzo e-mail**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@".<br>**ID chiave**: immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. |
| | Chiave precondivisa | Se si seleziona **Chiave precondivisa** per **Metodo autenticazione**, immettere una chiave pre-condivisa contenente da 1 a 127 caratteri. |
| | Chiave precondivisa già condivisa | Immettere la chiave configurata per conferma. |

## Impostazioni di sicurezza avanzate per Enterprise

| Elementi | Impostazioni e descrizione | |
|---|---|---|
| Incapsulazione | Se si seleziona **IPsec** per **Controllo accesso**, occorre configurare un modo di incapsulazione. | |
| | Modo Trasporto | Se si utilizza lo scanner soltanto sulla stessa LAN, selezionare questa opzione. I pacchetti IP di livello 4 o successivo sono crittografati. |
| | Modo Tunnel | Se si utilizza lo scanner nella rete con accesso a Internet come IPsec-VPN, selezionare questa opzione. L'intestazione e i dati dei pacchetti IP sono crittografati. |
| Indirizzo gateway remoto | Se si seleziona **Modo Tunnel** per **Incapsulazione**, immettere un indirizzo gateway contenente da 1 a 39 caratteri. | |
| Protocollo sicurezza | Se si seleziona **IPsec** per **Controllo accesso**, selezionare un'opzione. | |
| | ESP | Selezionare questa opzione per garantire l'integrità di un'autenticazione e dei dati e per crittografare i dati. |
| | AH | Selezionare questa opzione per garantire l'integrità di un'autenticazione e dei dati. Anche se la crittografia dei dati è proibita, è possibile utilizzare IPsec. |
| Impostazioni algoritmo | | |
| IKE | Crittografia | Selezionare l'algoritmo di crittografia per IKE.<br>Le voci variano a seconda della versione di IKE. |
| | Autenticazione | Selezionare l'algoritmo di autenticazione per IKE. |
| | Scambio chiave | Selezionare l'algoritmo di sostituzione chiave per IKE.<br>Le voci variano a seconda della versione di IKE. |
| ESP | Crittografia | Selezionare l'algoritmo di crittografia per ESP.<br>Ciò è disponibile quando come **Protocollo sicurezza** è impostato **ESP**. |
| | Autenticazione | Selezionare l'algoritmo di autenticazione per ESP.<br>Ciò è disponibile quando come **Protocollo sicurezza** è impostato **ESP**. |
| AH | Autenticazione | Selezionare l'algoritmo di autenticazione per AH.<br>Ciò è disponibile quando come **Protocollo sicurezza** è impostato **AH**. |

### Informazioni correlate


➡ “Configurazione di Criteri gruppo” a pagina 75

➡ “Combinazione di Indirizzo locale (scanner) e Indirizzo remoto(Host) su Criteri gruppo” a pagina 80

➡ “Riferimenti del nome del servizio per i criteri del gruppo” a pagina 80

## Combinazione di Indirizzo locale (scanner) e Indirizzo remoto(Host) su Criteri gruppo

| | | Impostazione di Indirizzo locale (scanner) | | |
|---|---|---|---|---|
| | | IPv4 | IPv6*2 | Ogni indirizzo*3 |
| **Impostazione di Indirizzo remoto(Host)** | IPv4*1 | ✓ | – | ✓ |
| | IPv6*1, *2 | – | ✓ | ✓ |
| | Vuoto | ✓ | ✓ | ✓ |

*1 Se **IPsec** è selezionato per **Controllo accesso**, non è possibile specificare una lunghezza del prefisso.

*2 Se **IPsec** è selezionato per **Controllo accesso**, è possibile selezionare un indirizzo locale di collegamento (fe80::) ma i criteri di gruppo saranno disattivati.

*3 Eccetto l'indirizzo locale di collegamento IPv6.

## Riferimenti del nome del servizio per i criteri del gruppo

***Nota:***
*I servizi non disponibili vengono visualizzati ma non possono essere selezionati.*

| Nome del servizio | Tipo protocollo | Numero porta locale | Numero porta remota | Funzioni controllate |
|---|---|---|---|---|
| Qualsiasi | – | – | – | Tutti i servizi |
| ENPC | UDP | 3289 | Qualsiasi porta | Ricerca di uno scanner da applicazioni quali EpsonNet Config e di un driver dello scanner |
| SNMP | UDP | 161 | Qualsiasi porta | Acquisizione e configurazione di MIB da applicazioni quali EpsonNet Config e il driver dello scanner Epson |
| WSD | TCP | Qualsiasi porta | 5357 | Controllo WSD |
| WS-Discovery | UDP | 3702 | Qualsiasi porta | Ricerca di uno scanner da WSD |
| Network Scan | TCP | 1865 | Qualsiasi porta | Inoltro dati di scansione da Document Capture Pro |
| Network Push Scan Discovery | UDP | 2968 | Qualsiasi porta | Ricerca di un computer dallo scanner. |
| Network Push Scan | TCP | Qualsiasi porta | 2968 | Acquisizione delle informazioni sui lavori per la funzione Push Scan da Document Capture Pro o Document Capture |
| HTTP (Locale) | TCP | 80 | Qualsiasi porta | Server HTTP(S) (inoltro dati di Web Config e WSD) |
| HTTPS (Locale) | TCP | 443 | Qualsiasi porta | |

| Nome del servizio | Tipo protocollo | Numero porta locale | Numero porta remota | Funzioni controllate |
|---|---|---|---|---|
| HTTP (Remoto) | TCP | Qualsiasi porta | 80 | Client HTTP(S) (comunicazione tra aggiornamento firmware e aggiornamento del certificato root) |
| HTTPS (Remoto) | TCP | Qualsiasi porta | 443 | |

# Esempi di configurazione di IPsec/Filtro IP

### Sola ricezione di pacchetti IPsec

Questo esempio è relativo alla sola configurazione di criteri predefiniti.

**Criteri predefiniti**:

❏ **IPsec/Filtro IP**: **Abilita**

❏ **Controllo accesso**: **IPsec**

❏ **Metodo autenticazione**: **Chiave precondivisa**

❏ **Chiave precondivisa**: Immettere fino a 127 caratteri.

**Criteri gruppo**:

Non configurare.

### Accettare una scansione utilizzando Epson Scan 2 e le impostazioni di scansione

Questo esempio consente le comunicazioni di dati di scansione e la configurazione dello scanner da servizi specificati.

**Criteri predefiniti**:

❏ **IPsec/Filtro IP**: **Abilita**

❏ **Controllo accesso**: **Rifiuta accesso**

**Criteri gruppo**:

❏ **Abilita criterio di gruppo**: Selezionare la casella.

❏ **Controllo accesso**: **Consenti accesso**

❏ **Indirizzo remoto(Host)**: Indirizzo IP di un client

❏ **Metodo di scelta porta**: **Nome servizio**

❏ **Nome servizio**: Selezionare la casella di **ENPC**, **SNMP**, **Network Scan**, **HTTP (Locale)** e **HTTPS (Locale)**.

### Ricezione di accesso solo da un indirizzo IP specificato

In questo esempio si consente l'accesso allo scanner a un indirizzo IP specificato.

**Criteri predefiniti**:

❏ **IPsec/Filtro IP**: **Abilita**

❏ **Controllo accesso**:**Rifiuta accesso**

**Criteri gruppo**:

❏ **Abilita criterio di gruppo**: Selezionare la casella.

❏ **Controllo accesso**: **Consenti accesso**

❏ **Indirizzo remoto(Host)**: Indirizzo IP di un client di amministratore

***Nota:***
*Indipendentemente dalla configurazione dei criteri, il client sarà in grado di accedere e configurare lo scanner.*

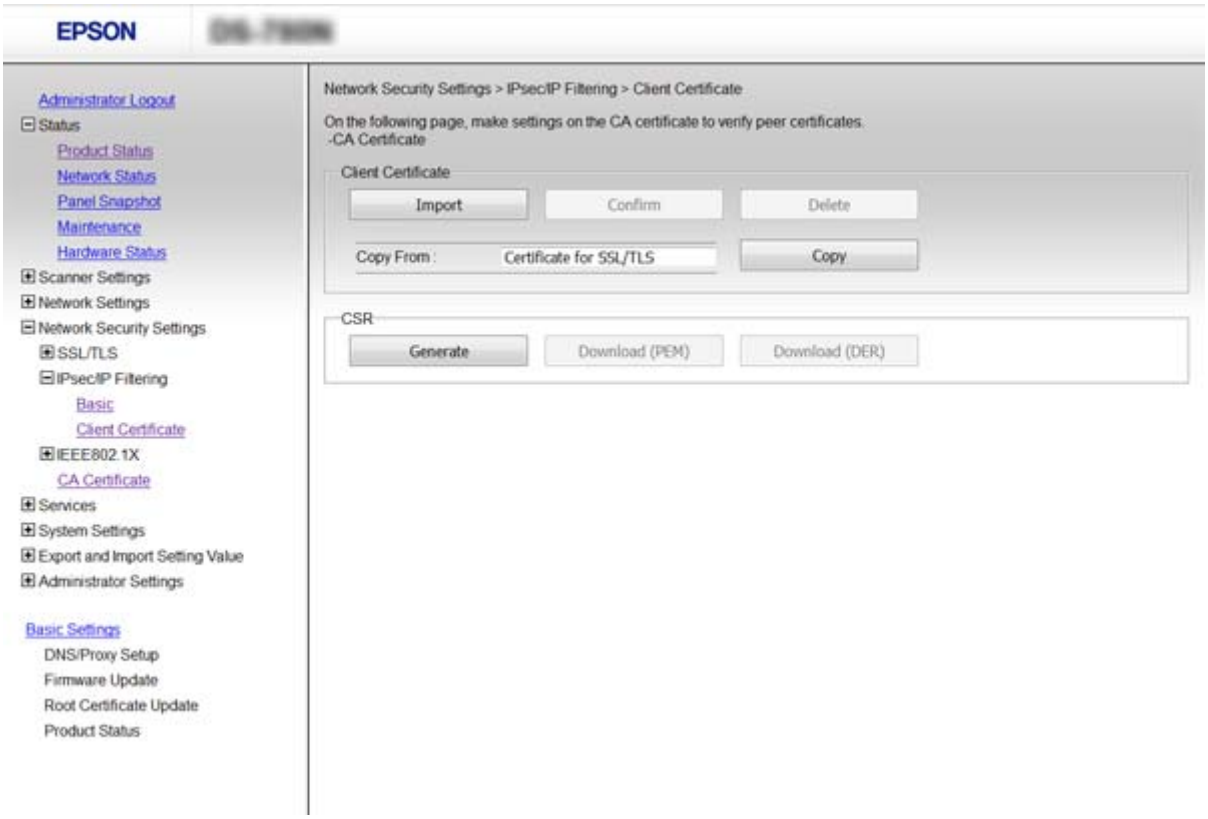
# Configurazione di un certificato per IPsec/Filtro IP

Configurare il certificato client per IPsec/IP Filtering. Per configurare l'ente di certificazione, andare su **Certificato CA**.

1. Accedere a Web Config e selezionare **Imp. di protezione rete** > **IPsec/Filtro IP** > **Certificato client**.

2. Importare il certificato in **Certificato client**.

   Se si è già importato un certificato pubblicato da un ente di certificazione in IEEE802.1X o SSL/TLS, è possibile copiare il certificato e utilizzarlo in IPsec/IP Filtering. Per copiare, selezionare il certificato da **Copia da**, quindi fare clic su **Copia**.




### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

➡ "Ottenimento e importazione di un certificato firmato CA" a pagina 64

# Uso del protocollo SNMPv3

## Informazioni su SNMPv3

SNMP è un protocollo che effettua operazioni di monitoraggio e controllo allo scopo di raccogliere informazioni sui dispositivi collegati alla rete. SNMPv3 è la versione di gestione delle funzioni di sicurezza, che è stata migliorata.

Quando si utilizza SNMPv3, è possibile autenticare e crittografare le modifiche alle impostazioni e il monitoraggio dello stato della comunicazione SNMP (pacchetto) in modo da proteggere la comunicazione SNMP (pacchetto) dai rischi connessi alla rete, come l'intercettazione, il furto d'identità e la manomissione.

## Configurazione SNMPv3

Se lo scanner supporta il protocollo SNMPv3, è possibile monitorare e controllare gli accessi allo scanner.

1. Accedere a Web Config e selezionare **Servizi** > **Protocollo**.
2. Immettere un valore per ciascuna voce delle **Impostazioni SNMPv3**.
3. Fare clic su **Avanti**.

   Viene visualizzato un messaggio di conferma.
4. Fare clic su **OK**.

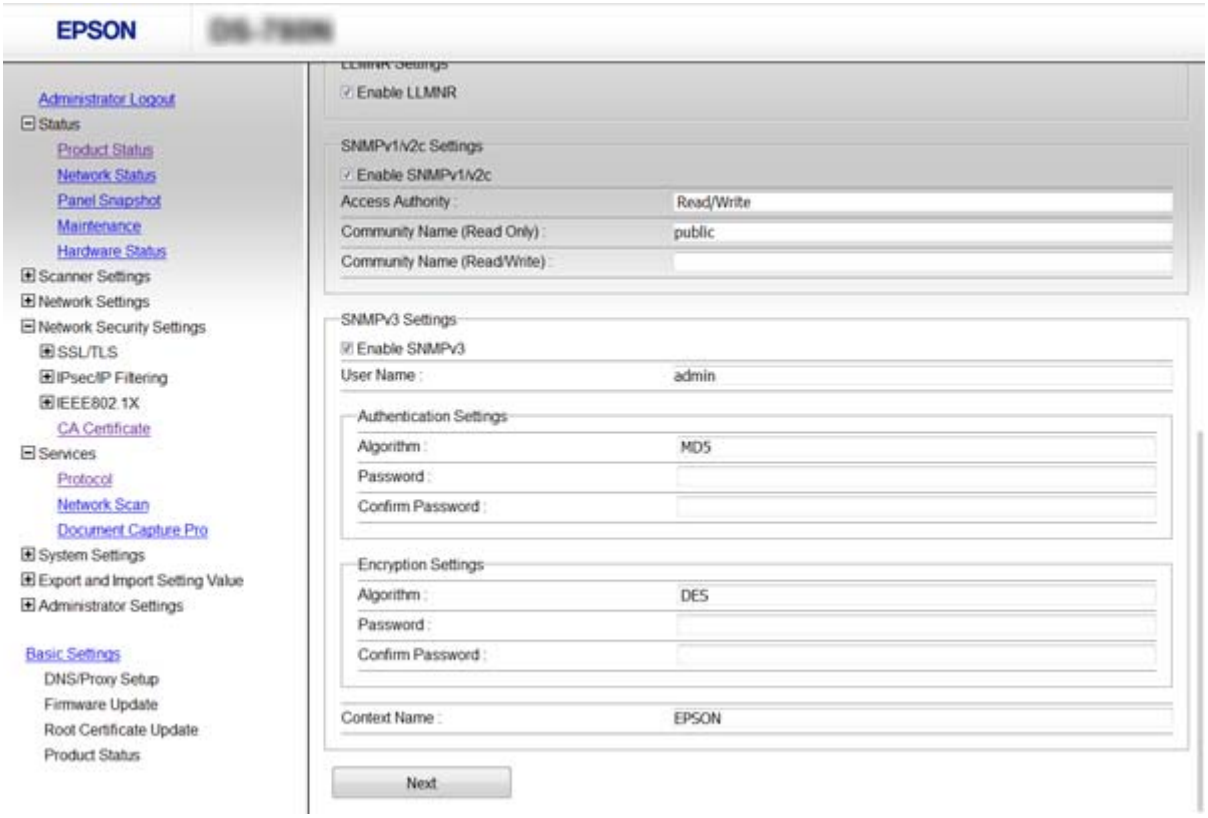
   Lo scanner viene aggiornato.

### Informazioni correlate

➡ “Accesso a Web Config” a pagina 23

➡ “Voci di impostazione SNMPv3” a pagina 84

# Voci di impostazione SNMPv3




| Voci | Impostazioni e descrizione |
|---|---|
| Abilita SNMPv3 | Il protocollo SNMPv3 risulta abilitato quando la relativa casella viene selezionata. |
| Nome utente | Immettere tra 1 e 32 caratteri a singolo byte. |
| Impostazioni di autenticazione | |
| Algoritmo | Selezionare un algoritmo di autenticazione. |
| Password | Immettere tra 8 e 32 caratteri in ASCII (0x20-0x7E). |
| Conferma password | Immettere la password configurata per conferma. |
| Impostazioni di crittografia | |
| Algoritmo | Selezionare un algoritmo di crittografia. |
| Password | Immettere tra 8 e 32 caratteri in ASCII (0x20-0x7E). |
| Conferma password | Immettere la password configurata per conferma. |
| Nome contesto | Immettere tra 1 e 32 caratteri a singolo byte. |

### Informazioni correlate

➡ “Configurazione SNMPv3” a pagina 83

# Connessione dello scanner a una rete IEEE802.1X

## Configurazione di una rete IEEE802.1X

Se lo scanner supporta IEEE802.1X, è possibile utilizzarlo su una rete con autenticazione connessa a un server RADIUS e con un hub come autenticatore.

1. Accedere a Web Config e selezionare **Imp. di protezione rete** > **IEEE802.1X** > **Di base**.
2. Immettere un valore per ciascuna voce.
3. Fare clic su **Avanti**.

   Viene visualizzato un messaggio di conferma.
4. Fare clic su **OK**.

   Lo scanner viene aggiornato.

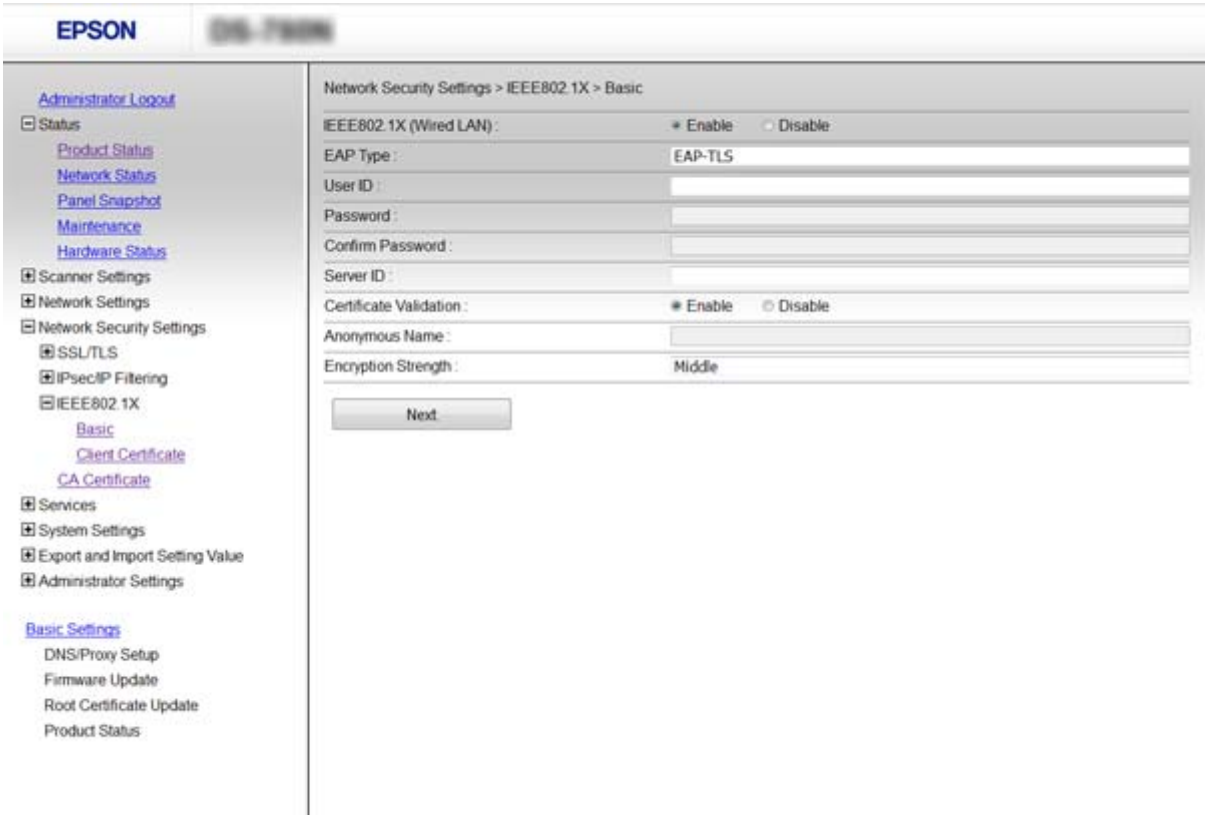
### Informazioni correlate

➡ “Accesso a Web Config” a pagina 23

➡ “Voci di impostazione di rete IEEE802.1X” a pagina 85

➡ “Impossibile accedere alla stampante o allo scanner dopo la configurazione di IEEE802.1X” a pagina 90

## Voci di impostazione di rete IEEE802.1X



**Impostazioni di sicurezza avanzate per Enterprise**

| Elementi | Impostazioni e descrizione | |
|---|---|---|
| IEEE802.1X (LAN cablata) | È possibile abilitare e disabilitare le impostazioni della pagina (**IEEE802.1X** > **Di base**) per IEEE802.1X (LAN cablata). | |
| Tipo EAP | Selezionare un'opzione per un metodo di autenticazione tra lo scanner e un server RADIUS. | |
| | EAP-TLS | Occorre ottenere e importare un certificato firmato CA. |
| | PEAP-TLS | |
| | PEAP/MSCHAPv2 | Occorre configurare una password. |
| ID utente | Configurare un ID da utilizzare per l'autenticazione di un server RADIUS.<br>Immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. | |
| Password | Configurare una password per autenticare lo scanner.<br>Immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte. Se si utilizza un server Windows come server RADIUS, è possibile immettere fino a 127 caratteri. | |
| Conferma password | Immettere la password configurata per conferma. | |
| ID server | È possibile configurare un ID server per effettuare l'autenticazione a un server RADIUS specificato. L'autenticatore verifica se un ID server è contenuto o meno nel campo subject/subjectAltName di un certificato server inviato da un server RADIUS.<br>Immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 0 byte. | |
| Convalida certificato | È possibile impostare la convalida certificato indipendentemente dal metodo di autenticazione. Importare il certificato in **Certificato CA**. | |
| Nome anonimo | Se si seleziona **PEAP-TLS** o **PEAP/MSCHAPv2** per **Metodo autenticazione**, è possibile configurare un nome anonimo al posto di un ID utente per la fase 1 di un'autenticazione PEAP.<br>Immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 0 byte. | |
| Livello di crittografia | È possibile selezionare una delle seguenti opzioni. | |
| | Alto | AES256/3DES |
| | Medio | AES256/3DES/AES128/RC4 |

**Informazioni correlate**

➡ "Configurazione di una rete IEEE802.1X" a pagina 85

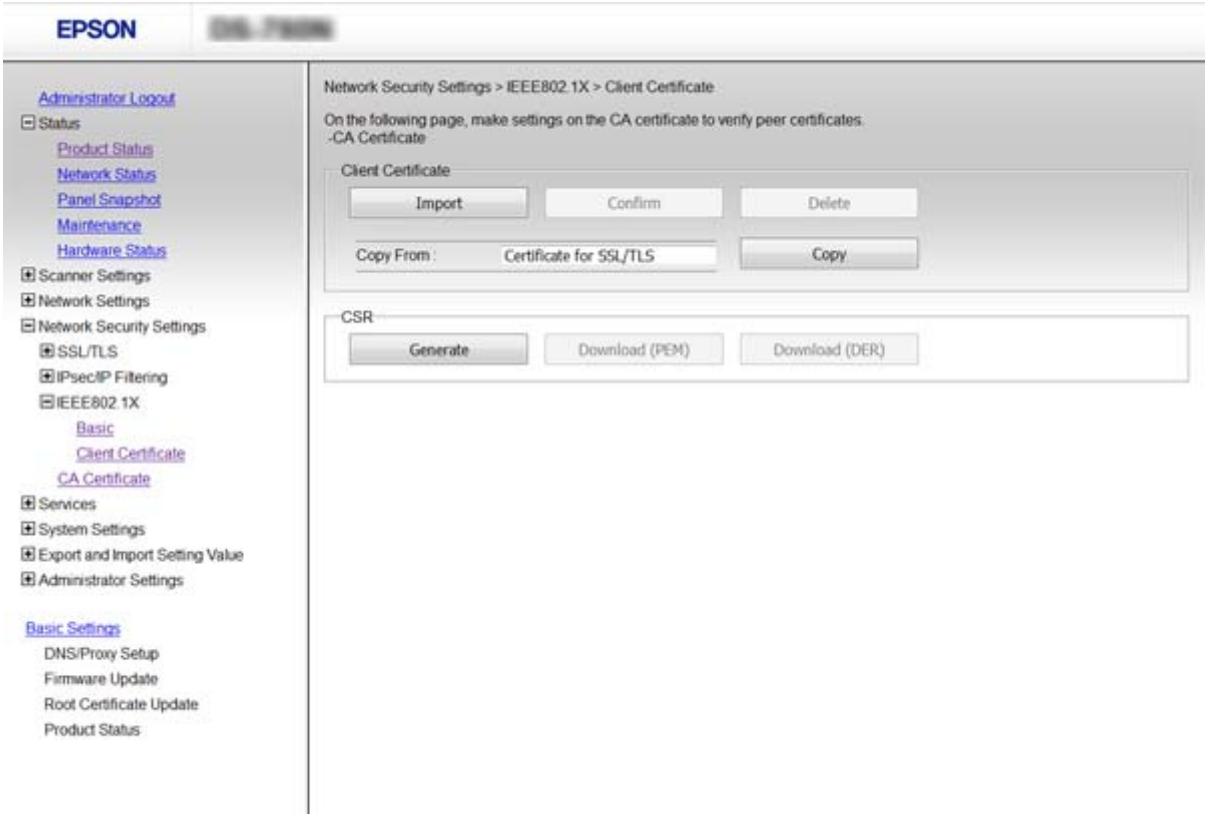
# Configurazione di un certificato per IEEE802.1X

Configurare il certificato client per IEEE802.1X. Per configurare il certificato dell'ente di certificazione, andare su **Certificato CA**.

1. Accedere a Web Config e selezionare **Imp. di protezione rete** > **IEEE802.1X** > **Certificato client**.

2. Immettere un certificato in **Certificato client**.

   È possibile copiare il certificato, se pubblicato da un ente di certificazione. Per copiare, selezionare il certificato da **Copia da**, quindi fare clic su **Copia**.




**Informazioni correlate**

➡ “Accesso a Web Config” a pagina 23

➡ “Ottenimento e importazione di un certificato firmato CA” a pagina 64

# Risoluzione dei problemi per la sicurezza avanzata

## Ripristino delle impostazioni di sicurezza

Se si stabilisce un ambiente dalla sicurezza elevata come IPsec/IP Filtering o IEEE802.1X, si potrebbe non essere in grado di comunicare con i dispositivi a causa di impostazioni errate o di problemi con il dispositivo o server. In questo caso, ripristinare le impostazioni di sicurezza al fine di effettuare nuovamente le impostazioni del dispositivo o consentirne un utilizzo temporaneo.

### Disattivazione della funzione di sicurezza dal pannello di controllo

È possibile disabilitare IPsec/IP Filtering o IEEE802.1X dal pannello di controllo dello scanner.

1. Toccare **Impostazioni** > **Impostazioni di rete**.

2. Toccare **Modifica impostazioni**.
3. Toccare le voci che si desidera disattivare.
   - ❏ **IPsec/Filtro IP**
   - ❏ **IEEE802.1X**
4. Quando viene visualizzato un messaggio di completamento, toccare **Proc.**.

## Ripristino della funzione di sicurezza tramite Web Config

Per IEEE802.1X, i dispositivi potrebbero non essere riconosciuti sulla rete. In tal caso, disabilitare la funzione dal pannello di controllo dello scanner.

Per IPsec/IP Filtering, è possibile disattivare la funzione se il dispositivo è accessibile dal computer.

### *Disattivazione di IPsec/IP Filtering tramiteWeb Config*

1. Accedere a Web Config e selezionare **Imp. di protezione rete** > **IPsec/Filtro IP** > **Di base**.
2. Selezionare **Disabilita** per **IPsec/Filtro IP** in **Criteri predefiniti**.
3. Fare clic su **Avanti**, quindi rimuovere **Abilita criterio di gruppo** per tutti i criteri di gruppo.
4. Fare clic su **OK**.

#### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

# Problemi utilizzando le funzioni di sicurezza di rete

## Chiave pre-condivisa dimenticata

#### Configurare nuovamente la chiave tramite Web Config.

Per modificare la chiave, accedere a Web Config e selezionare **Imp. di protezione rete** > **IPsec/Filtro IP** > **Di base** > **Criteri predefiniti** o **Criteri gruppo**.

Quando si modifica la chiave pre-condivisa, configurarla per i computer.

#### Informazioni correlate

➡ "Accesso a Web Config" a pagina 23

## Impossibile utilizzare la comunicazione IPsec

### Si sta utilizzando un algoritmo non supportato per le impostazioni del computer?

Lo scanner supporta i seguenti algoritmi.

| Metodo sicurezza | Algoritmi |
|---|---|
| Algoritmo di crittografia IKE | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES |
| Algoritmo di autenticazione IKE | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| Algoritmo di sostituzione chiave IKE | Gruppo DH 1, Gruppo DH 2, Gruppo DH 5, Gruppo DH 14, Gruppo DH 15, Gruppo DH 16, Gruppo DH 17, Gruppo DH 18, Gruppo DH 19, Gruppo DH 20, Gruppo DH 21, Gruppo DH 22, Gruppo DH 23, Gruppo DH 24, Gruppo DH 25, Gruppo DH 26, Gruppo DH 27*, Gruppo DH 28*, Gruppo DH 29*, Gruppo DH 30* |
| Algoritmo di crittografia ESP | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES |
| Algoritmo di autenticazione ESP | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| Algoritmo di autenticazione AH | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |

* disponibile solo per IKEv2

### Informazioni correlate

➡ “Comunicazione crittografata tramite IPsec/IP Filtering” a pagina 71

## Impossibile comunicare istantaneamente

### L'indirizzo IP dello scanner è errato o è stato modificato?

Disabilitare IPsec utilizzando il pannello di controllo dello scanner.

Se il server DHCP non è aggiornato, se è stato effettuato un riavvio o se l'indirizzo IPv6 è scaduto o non è stato ottenuto, l'indirizzo IP registrato per Web Config dello scanner (**Imp. di protezione rete** > **IPsec/Filtro IP** > **Di base** > **Criteri gruppo** > **Indirizzo locale (scanner)**) potrebbe non essere trovato.

Utilizzare un indirizzo IP statico.

### L'indirizzo IP del computer è errato o è stato modificato?

Disabilitare IPsec utilizzando il pannello di controllo dello scanner.

Se il server DHCP non è aggiornato, se è stato effettuato un riavvio o se l'indirizzo IPv6 è scaduto o non è stato ottenuto, l'indirizzo IP registrato per Web Config dello scanner (**Imp. di protezione rete** > **IPsec/Filtro IP** > **Di base** > **Criteri gruppo** > **Indirizzo remoto(Host)**) potrebbe non essere trovato.

Utilizzare un indirizzo IP statico.

### Informazioni correlate

➡ “Accesso a Web Config” a pagina 23

➡ “Comunicazione crittografata tramite IPsec/IP Filtering” a pagina 71

## Impossibile connettersi dopo la configurazione di IPsec/IP Filtering

### Il valore impostato potrebbe essere errato.

Disabilitare IPsec/IP Filtering dal pannello di controllo dello scanner. Collegare lo scanner al computer ed effettuare di nuovo le impostazioni IPsec/IP Filtering.

### Informazioni correlate

➡ "Comunicazione crittografata tramite IPsec/IP Filtering" a pagina 71

## Impossibile accedere alla stampante o allo scanner dopo la configurazione di IEEE802.1X

### Le impostazioni potrebbero essere errate.

Disabilitare IEEE802.1X dal pannello di controllo dello scanner. Collegare lo scanner e un computer, quindi configurare nuovamente IEEE802.1X.

### Informazioni correlate

➡ "Configurazione di una rete IEEE802.1X" a pagina 85

# Problema con l'uso di un certificato digitale

## Impossibile importare un certificato firmato CA

### Il certificato firmato CA e le informazioni della richiesta CSR corrispondono?

Se il certificato firmato CA e la richiesta CSR non presentano le stesse informazioni, la richiesta CSR non può essere importata. Verificare quanto segue:

❏ Si sta provando a importare il certificato su un dispositivo che non presenta le stesse informazioni?

Verificare le informazioni della richiesta CSR, quindi importare il certificato su un dispositivo che presenti le stesse informazioni.

❏ È stata sovrascritta la richiesta CSR salvata nello scanner dopo l'invio della richiesta CSR a un ente di certificazione?

Ottenere un nuovo certificato firmato CA con la richiesta CSR.

### Il certificato firmato CA è superiore a 5 KB?

Non è possibile importare un certificato firmato CA superiore a 5 KB.

### La password per l'importazione del certificato è corretta?

Se la password è stata dimenticata, non è possibile importare il certificato.

### Informazioni correlate

➡ "Importazione di un certificato firmato CA" a pagina 66

## Impossibile aggiornare un certificato auto-firmato

### Il Nome comune è stato immesso?

Il **Nome comune** deve venire immesso.

### Sono stati immessi caratteri non supportati in Nome comune? Ad esempio, i caratteri giapponesi non sono supportati.

Immettere tra 1 e 128 caratteri in formato IPv4, IPv6, nome host o FQDN in ASCII (0x20-0x7E).

### Sono stati inclusi una virgola o uno spazio in Nome comune?

Se è stata immessa una virgola, il **Nome comune** risulta diviso in tale punto. Se viene immesso solo uno spazio prima o dopo una virgola, si verificherà un errore.

### Informazioni correlate

➡ "Aggiornamento di un certificato auto-firmato" a pagina 68

## Impossibile creare una richiesta CSR

### Il Nome comune è stato immesso?

Il **Nome comune** deve venire immesso.

### Sono stati immessi caratteri non supportati in Nome comune, Organizzazione, Unità organizzativa, Località, Stato/Provincia? Ad esempio, i caratteri giapponesi non sono supportati.

Immettere caratteri in formato IPv4, IPv6, nome host o FQDN in ASCII (0x20-0x7E).

### Sono stati inclusi una virgola o uno spazio in Nome comune?

Se è stata immessa una virgola, il **Nome comune** risulta diviso in tale punto. Se viene immesso solo uno spazio prima o dopo una virgola, si verificherà un errore.

### Informazioni correlate

➡ "Ottenimento di un certificato firmato CA" a pagina 64

## Visualizzazione di avvertenza relativa a un certificato digitale

| Messaggi | Causa/Operazione da eseguire |
|---|---|
| Inserire un certificato server. | **Causa:**<br>Non è stato selezionato un file da importare.<br>**Operazione da eseguire:**<br>Selezionare un file e fare clic su **Importa**. |

## Impostazioni di sicurezza avanzate per Enterprise

| Messaggi | Causa/Operazione da eseguire |
|---|---|
| Certificato CA 1 non inserito. | **Causa:**<br>Il certificato CA 1 non viene immesso e risulta immesso solo il certificato CA 2.<br>**Operazione da eseguire:**<br>Importare innanzitutto il certificato CA 1. |
| Il valore seguente non è valido. | **Causa:**<br>Caratteri non supportati sono presenti nel percorso del file e/o nella password.<br>**Operazione da eseguire:**<br>Assicurarsi che nelle voci siano immessi i caratteri corretti. |
| Data e ora non valide. | **Causa:**<br>La data e l'ora dello scanner non sono state impostate.<br>**Operazione da eseguire:**<br>Impostare la data e l'ora utilizzando Web Config o EpsonNet Config. |
| Password non valida. | **Causa:**<br>La password impostata per il certificato CA e la password immessa non corrispondono.<br>**Operazione da eseguire:**<br>Immettere la password corretta. |
| File non valido. | **Causa:**<br>Si sta importando un file di certificato in formato X509.<br>**Operazione da eseguire:**<br>Assicurarsi di selezionare il certificato corretto inviato da un ente di certificazione fidato. |
| | **Causa:**<br>Il file importato è di dimensioni eccessive. Le dimensioni massime del file sono di 5 KB.<br>**Operazione da eseguire:**<br>Se è stato selezionato il file corretto, il certificato potrebbe essere danneggiato o manipolato. |
| | **Causa:**<br>La catena contenuta nel certificato non è valida.<br>**Operazione da eseguire:**<br>Per ulteriori informazioni sul certificato, vedere il sito Web dell'ente di certificazione. |
| Impossibile usare i certificati server che includono oltre 3 certificati CA. | **Causa:**<br>Il file di certificato in formato PKCS#12 contiene più di 3 certificati CA.<br>**Operazione da eseguire:**<br>Importare ciascun certificato durante la conversione dal formato PKCS#12 al formato PEM oppure importare un file di certificato in formato PKCS#12 che contenga massimo 2 certificati CA. |

| Messaggi | Causa/Operazione da eseguire |
|---|---|
| Il certificato è scaduto. Verificare se il certificato è valido o controllare data e ora sul prodotto. | **Causa:**<br>Il certificato è scaduto.<br>**Operazione da eseguire:**<br>❏ Se il certificato è scaduto, ottenere e importare un nuovo certificato.<br>❏ Se il certificato non è scaduto, assicurarsi che la data e l'ora dello scanner siano impostate correttamente. |
| Chiave privata obbligatoria. | **Causa:**<br>Non risulta abbinata una chiave privata al certificato.<br>**Operazione da eseguire:**<br>❏ Se il certificato è in formato PEM/DER e viene ottenuto da una richiesta CSR tramite computer, specificare il file della chiave privata.<br>❏ Se il certificato è in formato PKCS#12 e viene ottenuto da una richiesta CSR tramite computer, creare un file che contenga la chiave privata. |
| | **Causa:**<br>Il certificato PEM/DER ottenuto da una richiesta CSR è stato reimportato tramite Web Config.<br>**Operazione da eseguire:**<br>Se il certificato è in formato PEM/DER e viene ottenuto da una richiesta CSR tramite Web Config, è possibile importarlo una sola volta. |
| Configurazione non riuscita. | **Causa:**<br>Impossibile terminare la configurazione poiché la comunicazione tra lo scanner e il computer non è riuscita o il file non può essere letto a causa di alcuni errori.<br>**Operazione da eseguire:**<br>Dopo aver verificato il file specificato e la comunicazione, importare di nuovo il file. |

### Informazioni correlate

➡ “Informazioni sulla certificazione digitale” a pagina 63

## Eliminazione erronea di un certificato firmato CA

### Esiste un file di backup del certificato?

Se si dispone di un file di backup, importare di nuovo il certificato.

Se si ottiene un certificato tramite una richiesta CSR creata da Web Config, non è possibile importare di nuovo un certificato eliminato. Creare una richiesta CSR e ottenere un nuovo certificato.

### Informazioni correlate

➡ “Eliminazione di un certificato firmato CA” a pagina 67

➡ “Importazione di un certificato firmato CA” a pagina 66