

DS-790WN

Guida per amministratore

Impostazioni consigliate per soddisfare il vostro scopo

Impostazioni di Rete

Impostazioni richieste per la scansione

Impostazioni di sicurezza di base

Impostazioni di sicurezza avanzate

Impostazioni di autenticazione

Copyright

Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero, trasmessa in qualsiasi forma e con qualsiasi mezzo, elettronico, meccanico, di fotocopiatura, registrazione o altro, senza il previo consenso scritto di Seiko Epson Corporation. Nessuna responsabilità viene assunta in relazione all'uso delle informazioni in essa contenute. Né ci si assume alcuna responsabilità per eventuali danni derivanti dall'uso delle informazioni qui contenute. Le informazioni qui contenute sono state progettate solo per l'uso con questo prodotto Epson. Epson non è responsabile per l'utilizzo di queste informazioni con altri prodotti.

Né Seiko Epson Corporation né le sue affiliate sono responsabili verso l'acquirente di questo prodotto o verso terzi per danni, perdite, costi o spese sostenute dall'acquirente o da terzi a seguito di incidente, cattivo uso o abuso di questo prodotto oppure modifiche non autorizzate, riparazioni o alterazioni questo prodotto, oooore (esclusi gli Stati Uniti) la mancata stretta osservanza delle istruzioni operative e di manutenzione di Seiko Epson Corporation.

Seiko Epson Corporation e le sue affiliate non sono responsabili per eventuali danni o problemi derivanti dall'uso di opzioni o materiali di consumo diversi da quelli designati come prodotti originali Epson oppure prodotti approvati Epson da Seiko Epson Corporation.

Seiko Epson Corporation non potrà essere ritenuta responsabile per eventuali danni derivanti da interferenze elettromagnetiche che avvengono per l'uso di cavi di interfaccia diversi da quelli designati come prodotti approvati Epson da Seiko Epson Corporation.

© 2021 Seiko Epson Corporation

Il contenuto di questo manuale e le specifiche di questo prodotto sono soggette a modifiche senza preavviso.

Marchi

- ❑ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION e i rispettivi loghi sono marchi registrati o marchi di Seiko Epson.
- ❑ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❑ Chrome is a trademark of Google LLC.
- ❑ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❑ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❑ FeliCa e PaSoRi sono marchi registrati di Sony Corporation.
- ❑ MIFARE è un marchio registrato di NXP Semiconductor Corporation.
- ❑ Avviso generale: altri nomi di prodotti qui usati sono solo a scopo identificativo e possono essere marchi dei rispettivi proprietari. Epson non rivendica alcun diritto su tali marchi.

Sommario

Copyright

Marchi

Introduzione

Contenuto di questo documento.	8
Uso di questa guida.	8
Marchi e simboli.	8
Descrizioni utilizzate in questo manuale.	8
Riferimenti del sistema operativo.	9

Impostazioni consigliate per soddisfare il vostro scopo

Impostazioni consigliate per soddisfare il vostro scopo.	11
--	----

Impostazioni di Rete

Collegare lo scanner alla rete.	14
Prima di effettuare la connessione di rete.	14
Connessione alla rete dal Pannello di controllo.	16
Aggiunta o sostituzione del computer o di dispositivi.	20
Connessione a uno scanner che è stato collegato alla rete.	20
Collegare un dispositivo smart e lo scanner direttamente (Wi-Fi Direct).	22
Reimpostare il collegamento di rete.	24
Verifica dello stato della connessione di rete.	26
Verifica dello stato del collegamento di rete dal pannello di controllo.	27
Specifiche di rete.	28
Specifiche Wi-Fi.	28
Specifiche Ethernet.	29
Funzioni di rete e IPv4/IPv6.	30
Protocollo di sicurezza.	30
Utilizzo della porta per lo scanner.	30
Soluzione dei problemi.	32
Non è possibile collegarsi a una rete.	32

Software per la configurazione dello scanner

Web Config.	36
Esecuzione di Web Config su un browser web.	36

Esecuzione di Web Config in sistemi Windows.	36
Epson Device Admin.	37
Modello di configurazione.	37

Impostazioni richieste per la scansione

Configurazione di un server di posta.	42
Voci di impostazione del server di posta.	42
Verifica della connessione al server di posta.	43
Impostazione di una cartella di rete condivisa.	45
Creazione della cartella condivisa.	45
Rendere disponibili i contatti.	61
Comparazione della configurazione dei contatti.	62
Registrazione di una destinazione sui Contatti con Web Config.	62
Registrazione di destinazioni come gruppo usando Web Config.	64
Backup e importazione di contatti.	65
Esportazione e registrazione di massa dei contatti utilizzando lo strumento.	66
Cooperazione tra il server LDAP e gli utenti.	68
Utilizzo di Document Capture Pro Server.	71
Impostazione della modalità server.	71
Configurazione di AirPrint.	72
Problemi durante la preparazione della scansione in rete.	72
Suggerimenti per risolvere i problemi.	72
Impossibile accedere a Web Config.	72

Personalizzazione del display del pannello di controllo

Registrazione di Preimpostaz..	76
Opzioni del menu Preimpostaz..	77
Modifica della schermata iniziale del pannello di controllo.	78
Modifica del Disposizione della schermata iniziale.	79
Aggiungi icona.	79
Rimuovi icona.	80
Sposta icona.	81

Impostazioni di sicurezza di base

Introduzione delle funzioni di sicurezza del prodotto.	84
--	----

Impostazioni di amministrazione.	84
Configurazione della password di amministratore.	84
Utilizzo di Impostazione blocco per il pannello di controllo.	86
Effettuare l'accesso come amministratore dal pannello di controllo.	89
Disattivazione dell'interfaccia esterna.	90
Monitoraggio di uno scanner remoto.	91
Verifica delle informazioni per uno scanner remoto.	91
Ricezione di notifiche email al verificarsi di eventi.	91
Soluzione dei problemi.	92
Password di amministratore dimenticata.	92

Impostazioni di sicurezza avanzate

Impostazioni di sicurezza e prevenzione del pericolo.	94
Impostazioni delle funzioni di sicurezza.	95
Controllo tramite protocolli.	95
Controllo dei protocolli.	95
Protocolli che si possono abilitare o disabilitare.	95
Voci di impostazione del protocollo.	96
Uso di un certificato digitale.	98
Informazioni sulla certificazione digitale.	98
Configurazione di un Certificato firma CA.	99
Aggiornamento di un certificato auto-firmato.	102
Configurazione di un Certificato CA.	103
Comunicazione SSL/TLS con lo scanner.	103
Configurazione delle impostazioni SSL/TLS di base.	104
Configurazione di un certificato server per lo scanner.	104
Comunicazione crittografata tramite IPsec/IP Filtering.	105
Informazioni su IPsec/Filtro IP.	105
Configurazione dei criteri predefiniti.	105
Configurazione dei criteri di gruppo.	109
Esempi di configurazione di IPsec/Filtro IP.	115
Configurazione del certificato per IPsec/IP Filtering.	116
Connessione dello scanner a una rete IEEE802.1X	116
Configurazione di una rete IEEE 802.1X.	116
Configurazione di un certificato per IEEE 802.1X.	118
Risoluzione dei problemi per la sicurezza avanzata	118
Ripristino delle impostazioni di sicurezza.	118

Problemi utilizzando le funzioni di sicurezza di rete.	119
Problema con l'uso di un certificato digitale.	121

Impostazioni di autenticazione

Informazioni su Impostazioni di autenticazione.	126
Funzioni disponibili per Impostazioni di autenticazione.	126
Informazioni su Metodo autenticazione.	127
Software per la configurazione.	129
Aggiornare il firmware dello scanner.	129
Collegamento e configurazione di un dispositivo di autenticazione.	129
Elenco dei lettori di schede supportati.	129
Collegamento del dispositivo di autenticazione.	132
Impostazioni del dispositivo di autenticazione.	133
Registrazioni e impostazioni.	134
Installazione.	134
Abilitare l'autenticazione.	135
Impostazioni di autenticazione.	135
Registrare le Imp. utente.	137
Sincronizzazione con il Server LDAP.	143
Configurare il server e-mail.	147
Configurazione di Scan su La mia cart..	148
Personalizza funzioni One-touch.	150
Rapporti della Cronologia processi con Epson Device Admin.	150
Voci che possono essere incluse nel rapporto.	151
Effettuare l'accesso come amministratore dal pannello di controllo.	151
Disabilitazione di Impostazioni di autenticazione.	151
Eliminare le informazioni delle Impostazioni di autenticazione (Ripristina impostaz. predef.).	152
Soluzione dei problemi.	152
Impossibile leggere la scheda di autenticazione.	152

Manutenzione

Pulizia esterna dello scanner.	154
Pulizia interna dello scanner.	154
Sostituire il kit manutenzione rulli.	159
Codici kit montaggio rulli.	164
Azzerare il numero di scansioni.	164
Risparmio energetico.	164
Trasporto dello scanner.	165
Backup delle impostazioni.	166
Esportazione delle impostazioni.	166
Importazione delle impostazioni.	167

Ripristina impostaz. predef.	167
Aggiornamento Applicazioni e Firmware.	168
Aggiornamento del firmware dello scanner tramite il pannello di controllo.	168
Aggiornamento del firmware tramite Web Config.	169
Aggiornamento del firmware senza connettersi a Internet.	169



Introduzione

Contenuto di questo documento.	8
Uso di questa guida.	8

Contenuto di questo documento

Questo documento fornisce le seguenti informazioni agli amministratori dello scanner.

- Impostazioni di rete
- Preparazione della funzione di scansione
- Abilitare e gestire le impostazioni di sicurezza
- Abilitare e gestire le Impostazioni di autenticazione
- Effettuare giornalmente la manutenzione

Per i metodi standard di utilizzo dello scanner, consultare la *Guida utente*.

Nota:

Questo documento descrive le Impostazioni di autenticazione, che consentono di effettuare l'autenticazione in autonomia senza dover utilizzare un apposito server. In aggiunta alle Impostazioni di autenticazione descritte in questo manuale, è anche possibile creare un sistema di autenticazione utilizzando un server di autenticazione. Per creare un sistema, utilizzare Document Capture Pro Server Authentication Edition (il nome abbreviato è Document Capture Pro Server AE).

Per ulteriori informazioni, contattare la sede Epson locale.

Uso di questa guida

Marchi e simboli



Attenzione:

Istruzioni che devono essere seguite attentamente per evitare danni personali.



Importante:

Istruzioni che devono essere seguite per evitare danni alle apparecchiature.

Nota:

Fornisce informazioni complementari e di riferimento.

Informazioni correlate

➔ Collegamenti alle relative sezioni.

Descrizioni utilizzate in questo manuale

- Le schermate delle applicazioni si riferiscono a Windows 10 o macOS High Sierra. Il contenuto visualizzato nelle schermate varia a seconda del modello in uso e del contesto di utilizzo.
- Le illustrazioni usate in questo manuale sono di semplice riferimento. Sebbene possano differire leggermente dal prodotto effettivo, i metodi di esecuzione sono identici.

Riferimenti del sistema operativo

Windows

In questo manuale, termini quali “Windows 10”, “Windows 8.1”, “Windows 8”, “Windows 7”, “Windows Server 2019”, “Windows Server 2016”, “Windows Server 2012 R2”, “Windows Server 2012” e “Windows Server 2008 R2” fanno riferimento ai seguenti sistemi operativi. Inoltre, “Windows” fa riferimento a tutte le versioni e “Windows Server” fa riferimento a “Windows Server 2019”, “Windows Server 2016”, “Windows Server 2012 R2”, “Windows Server 2012” e “Windows Server 2008 R2”.

- 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 Server® 2019
- 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

Mac OS

In questo manuale, “Mac OS” è usato per riferirsi a macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan e OS X Yosemite.

Impostazioni consigliate per soddisfare il vostro scopo

Impostazioni consigliate per soddisfare il vostro scopo. 11

Impostazioni consigliate per soddisfare il vostro scopo

Vedere quanto segue per configurare le impostazioni necessarie per il proprio scopo.

Collegare lo scanner alla rete

Scopo	Impostazioni richieste
Desidero collegare lo scanner alla rete.	Configurare lo scanner per la scansione di rete. "Collegare lo scanner alla rete" a pagina 14
Desidero collegare lo scanner a un nuovo computer.	Configurare le impostazioni di rete per lo scanner sul nuovo computer. "Aggiunta o sostituzione del computer o di dispositivi" a pagina 20

Impostazioni per la scansione

Scopo	Impostazioni richieste
Desidero inviare le immagini acquisite tramite e-mail. (Scansione su e-mail)	1. Configurare il server e-mail che si desidera utilizzare. "Configurazione di un server di posta" a pagina 42 2. Registrare l'indirizzo e-mail del destinatario in Contatti (opzionale). Se si registra l'indirizzo e-mail non è necessario immetterlo manualmente per ogni invio; è sufficiente selezionarlo dai Contatti. "Rendere disponibili i contatti" a pagina 61
Desidero salvare le immagini acquisite in una cartella in rete. (Scansione su cartella rete/FTP)	1. Creare una cartella in rete per il salvataggio delle immagini. "Impostazione di una cartella di rete condivisa" a pagina 45 2. Registrare il percorso della cartella in Contatti (opzionale). Se si registra il percorso della cartella non è necessario immetterlo manualmente per ogni invio; è sufficiente selezionarlo dai Contatti. "Rendere disponibili i contatti" a pagina 61
Desidero salvare le immagini acquisite in un servizio cloud. (Scansione su Cloud)	Configurare Epson Connect. Per ulteriori informazioni sulla configurazione, consultare il sito web del portale Epson Connect. Per la configurazione è necessario un account utente per il servizio di archiviazione online che si desidera utilizzare. https://www.epsonconnect.com/ http://www.epsonconnect.eu (solo Europa)

Personalizzazione del display del pannello di controllo

Scopo	Impostazioni richieste
Desidero cambiare le icone visualizzate sul pannello di controllo dello scanner.	Impostare Preimpostaz. o Modifica schermata principale . È possibile registrare le impostazioni di scansione preferite nel pannello di controllo e modificare gli elementi visualizzati. "Personalizzazione del display del pannello di controllo" a pagina 75

Impostazione delle funzioni di sicurezza di base

Scopo	Impostazioni richieste
Desidero impedire a persone diverse dall'amministratore di modificare le impostazioni dello scanner.	Impostare una password di amministratore per lo scanner. "Impostazioni di amministrazione" a pagina 84
Desidero disabilitare l'uso degli scanner con connessioni USB.	Disattivare l'interfaccia esterna. "Disattivazione dell'interfaccia esterna" a pagina 90

Impostazione delle funzioni di sicurezza avanzate

Scopo	Impostazioni richieste
Desidero controllare quali protocolli utilizzare.	Abilitare o disabilitare i protocolli. "Controllo tramite protocolli" a pagina 95
Desidero crittografare il percorso di comunicazione.	1. Configurare il proprio certificato digitale. "Uso di un certificato digitale" a pagina 98 2. Configurare la comunicazione SSL/TLS. "Comunicazione SSL/TLS con lo scanner" a pagina 103
Desidero utilizzare la comunicazione crittografata (IPsec). Desidero utilizzare il software solo da un computer specifico (filtro IP).	Configurare i criteri per il filtraggio del traffico. "Comunicazione crittografata tramite IPsec/IP Filtering" a pagina 105
Desidero utilizzare uno scanner in una rete IEEE802.1X.	Impostare IEEE802.1X per lo scanner. "Connessione dello scanner a una rete IEEE802.1X" a pagina 116

Impostazione delle funzioni di autenticazione dello scanner

Scopo	Impostazioni richieste
Desidero abilitare Impostazioni di autenticazione.	Vedere quanto segue per maggiori informazioni su Impostazioni di autenticazione e Metodo autenticazione. "Informazioni su Impostazioni di autenticazione" a pagina 126 "Informazioni su Metodo autenticazione" a pagina 127

Utilizzare un sistema di autenticazione del server

Con Document Capture Pro Server Authentication Edition (abbreviato in Document Capture Pro Server AE), è possibile creare un sistema di autenticazione che utilizza un server per l'autenticazione.

Per ulteriori informazioni, contattare la sede Epson locale.

Impostazioni di Rete

Collegare lo scanner alla rete.	14
Aggiunta o sostituzione del computer o di dispositivi.	20
Verifica dello stato della connessione di rete.	26
Specifiche di rete.	28
Soluzione dei problemi.	32

Collegare lo scanner alla rete

Questa sezione descrive la procedura di connessione dello scanner alla rete utilizzando il pannello di controllo dello scanner.

Nota:

Se lo scanner e il computer si trovano nello stesso segmento, è possibile effettuare la connessione anche utilizzando il programma di installazione.

Impostazione dal sito web

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

<http://epson.sn>

Configurazione tramite il disco del software (solo per i modelli dotati di un disco software e per gli utenti che utilizzano un computer Windows con unità di lettura disco)

Inserire nel computer il disco del software e seguire le istruzioni a video.

Prima di effettuare la connessione di rete

Per connettersi alla rete, controllare in precedenza il metodo di connessione e impostare le informazioni relative alla connessione.

Raccolta di informazioni sull'impostazione di connessione

Preparare le informazioni di impostazione necessarie per la connessione. Controllare in anticipo quanto segue.

Divisioni	Elementi	Nota
Metodo di connessione del dispositivo	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Decidere come collegare lo scanner alla rete. Per LAN cablata, si connette allo switch LAN. Per Wi-Fi, si connette alla rete (SSID) del punto di accesso.
Informazioni sulla connessione LAN	<input type="checkbox"/> Indirizzo IP <input type="checkbox"/> Maschera di sottorete <input type="checkbox"/> Gateway predefinito	Decidere l'indirizzo IP da assegnare allo scanner. Quando si assegna un indirizzo IP statico, tutti i valori sono necessari. Quando si assegna un indirizzo IP dinamico tramite la funzione DHCP, queste informazioni non sono necessarie perché vengono impostate automaticamente.
Informazioni sulla connessione Wi-Fi	<input type="checkbox"/> SSID <input type="checkbox"/> Password	Si tratta dell'SSID (nome della rete) e della password del punto di accesso al quale lo scanner si connette. Se è stato impostato il filtraggio dell'indirizzo MAC, registrare in precedenza l'indirizzo MAC dello scanner, per poter registrare lo scanner. Per gli standard supportati, vedere quanto segue. "Specifiche di rete" a pagina 28

Divisioni	Elementi	Nota
Informazioni sul server DNS	<input type="checkbox"/> Indirizzo IP per DNS primario <input type="checkbox"/> Indirizzo IP per DNS secondario	Sono necessari quando si specificano i server DNS. Il DNS secondario viene impostato quando il sistema ha una configurazione ridondante ed esiste un server DNS secondario. Se si è in una piccola organizzazione e non si dispone di un server DNS, impostare l'indirizzo IP del router.
Informazioni sul server proxy	<input type="checkbox"/> Nome del server proxy	Impostarlo quando l'ambiente di rete utilizza il server proxy per accedere a Internet da intranet e si utilizza la funzione secondo cui lo scanner accede direttamente a Internet. Per le seguenti funzioni, lo scanner si collega direttamente a Internet. <ul style="list-style-type: none"> <input type="checkbox"/> Servizi Epson Connect <input type="checkbox"/> Servizi cloud di altre aziende <input type="checkbox"/> Aggiornamento del firmware <input type="checkbox"/> Invio di immagini scansionate a SharePoint (WebDAV)
Informazioni numero di porta	<input type="checkbox"/> Numero di porta da sbloccare	Verificare il numero di porta utilizzato dallo scanner e dal computer, quindi sbloccare la porta bloccata da un firewall, se necessario. Per il numero di porta utilizzato da questo scanner, vedere quanto segue. "Utilizzo della porta per lo scanner" a pagina 30

Assegnazione dell'indirizzo IP

Esistono i seguenti tipi di assegnazione di indirizzi IP.

Indirizzo IP statico:

Assegnare manualmente l'indirizzo IP predeterminato allo scanner (host).

Le informazioni per connettersi alla rete (maschera di sottorete, gateway predefinito, server DNS e così via) devono essere impostate manualmente.

L'indirizzo IP non cambia anche quando il dispositivo è disattivato, quindi è utile quando si desidera gestire i dispositivi con un ambiente in cui non è possibile modificare l'indirizzo IP o si desidera gestire i dispositivi utilizzando l'indirizzo IP. Si consiglia di impostarlo per lo scanner, il server, ecc., cui accedono molti computer. Inoltre, quando si utilizzano funzionalità di sicurezza come il filtro IPsec/IP, assegnare un indirizzo IP fisso in modo che l'indirizzo IP non cambi.

Assegnazione automatica tramite funzione DHCP (indirizzo IP dinamico):

Assegnare automaticamente l'indirizzo IP allo scanner (host) utilizzando la funzione DHCP del server DHCP o del router.

Le informazioni per connettersi alla rete (maschera di sottorete, gateway predefinito, server DNS e così via) vengono impostate automaticamente, in modo da poter connettere facilmente il dispositivo alla rete.

Se il dispositivo o il router sono spenti o in base alle impostazioni del server DHCP, l'indirizzo IP potrebbe cambiare quando ci si riconnette.

Si consiglia di gestire i dispositivi con modi diversi dall'indirizzo IP e di comunicare con i protocolli che possono seguire l'indirizzo IP.

Nota:

Quando si utilizza la funzione di riserva dell'indirizzo IP del DHCP, è possibile assegnare in qualsiasi momento lo stesso indirizzo IP ai dispositivi.

Server DNS e Server proxy

Il server DNS dispone di un nome host, nome di dominio dell'indirizzo e-mail, ecc., associato alle informazioni sull'indirizzo IP.

La comunicazione è impossibile se l'altra parte è descritta da nome host, nome di dominio, ecc. quando il computer o lo scanner eseguono la comunicazione IP.

Richiede queste informazioni al server DNS e ottiene l'indirizzo IP dell'altra parte. Questo processo è chiamato risoluzione del nome.

Pertanto, i dispositivi come computer e scanner possono comunicare utilizzando l'indirizzo IP.

La risoluzione dei nomi è necessaria per la comunicazione dello scanner utilizzando la funzione di posta elettronica o la funzione di connessione a Internet.

Quando si utilizzano tali funzioni, eseguire le impostazioni del server DNS.

Quando si assegna l'indirizzo IP dello scanner utilizzando la funzione DHCP del server DHCP o del router, tali impostazioni vengono configurate automaticamente.

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.

Quando ci si connette a Internet tramite un server proxy, configurare il server proxy sullo scanner.

Connessione alla rete dal Pannello di controllo

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

Assegnazione dell'indirizzo IP

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

Questa sezione spiega la procedura per impostare un indirizzo IP statico.

1. Accendere lo scanner.
2. Selezionare **Impostazioni** nella schermata iniziale del pannello di controllo dello scanner.
3. Selezionare **Impostazioni di rete > Avanzate > TCP/IP**.
4. Selezionare **Manuale** per **Otteni indirizzo IP**.

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 5 a 6, quindi andare al passaggio 7.

5. Immettere l'indirizzo IP.

Il focus si sposta sul segmento successivo o su quello precedente separato da un punto se si seleziona ◀ e ▶.

Confermare il valore visualizzato sulla schermata precedente.

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

Confermare il valore visualizzato sulla schermata precedente.



Importante:

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.

7. Immettere l'indirizzo IP per il server DNS primario.

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 9.

8. Immettere l'indirizzo IP per il server DNS secondario.

Confermare il valore visualizzato sulla schermata precedente.

9. Toccare **Avvia configuraz.**

Configurazione del server proxy

Impostare il server proxy se entrambe le seguenti condizioni sono vere.

- Il server proxy è stato creato per la connessione a Internet.
- Quando si utilizza una funzione in cui uno scanner si collega direttamente a Internet, quale il servizio Epson Connect o servizi cloud di altre aziende.

1. Selezionare **Impostazioni** nella schermata iniziale.

Se si effettuano le impostazioni dopo aver configurato l'indirizzo IP, viene visualizzata la schermata **Avanzate**. Andare al passaggio 3.

2. Scegliere **Impostazioni di rete > Avanzate**.

3. Selezionare **Server Proxy**.

4. Selezionare **Usa** per **Impostazioni server Proxy**.

5. Immettere l'indirizzo per il server proxy in formato IPv4 o FQDN.

Confermare il valore visualizzato sulla schermata precedente.

6. Immettere il numero di porta per il server proxy.

Confermare il valore visualizzato sulla schermata precedente.

7. Toccare **Avvia configuraz..**

Connessione a Ethernet

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

1. Collegare lo scanner e l'hub (interruttore LAN) tramite un cavo LAN.
2. Selezionare  nella schermata iniziale.
3. Selezionare **Router**.
4. Assicurarsi che le impostazioni di Connessione e Indirizzo IP siano corrette.
5. Toccare **Chiudi**.

Connessione alla LAN wireless (Wi-Fi)

È possibile collegare lo scanner alla rete wireless LAN (Wi-Fi) in diversi modi. Scegliere il metodo di connessione che corrisponde all'ambiente e alle condizioni in uso.

Se si conoscono le informazioni relative al router wireless, per esempio SSID e password, è possibile configurare le impostazioni manualmente.

Se il router wireless supporta WPS, è possibile effettuare le impostazioni tramite pulsante push.

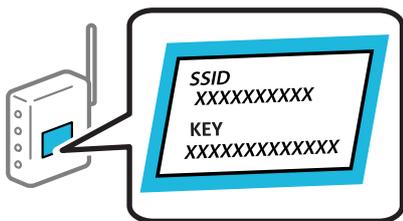
Dopo aver collegato lo scanner alla rete, connettersi allo scanner dal dispositivo che si desidera utilizzare (computer, dispositivo smart, tablet, e così via.)

Eeguire le impostazioni Wi-Fi inserendo il SSID e la password

È possibile impostare una rete Wi-Fi inserendo le informazioni necessarie per connettersi a un router wireless dal pannello di controllo dello scanner. Per eseguire l'impostazione usando questo metodo, occorrono l'SSID e la password per il router wireless.

Nota:

Se si utilizza un router wireless con le relative impostazioni predefinite, l'SSID e la password sono presenti sull'etichetta. Se non si individuano l'SSID e la password, contattare il responsabile dell'impostazione del router wireless oppure consultare la relativa documentazione.



1. Toccare  nella schermata iniziale.
2. Selezionare **Router**.

3. Toccare **Avvia configurazione**.

Se la connessione di rete è già impostata, vengono visualizzati i dettagli sulla connessione. Toccare **Modifica a connessione Wi-Fi**, o **Modifica impostazioni** per modificare le impostazioni.

4. Selezionare **Procedura guidata configurazione Wi-Fi**.

5. Seguire le istruzioni visualizzate sullo schermo per selezionare l'SSID, immettere la password per il router wireless e avviare l'installazione.

Se si desidera verificare lo stato della connessione di rete dello scanner al termine dell'installazione, consultare il seguente collegamento alle informazioni correlate per ulteriori dettagli.

Nota:

Se non si conosce l'SSID, controllare se si trova sull'etichetta del router wireless. Se si utilizzano le impostazioni predefinite del router wireless, utilizzare l'SSID presente sull'etichetta. Se non si trova alcuna informazione, consultare la documentazione fornita con il router wireless.

La password distingue tra maiuscole e minuscole.

Se non si conosce la password, controllare se tale informazione si trova sull'etichetta del router wireless. Sull'etichetta, la password potrebbe essere definita come "Network Key", "Wireless Password" e così via. Se si utilizzano le impostazioni predefinite del router wireless, utilizzare la password presente sull'etichetta.

Informazioni correlate

➔ ["Verifica dello stato della connessione di rete"](#) a pagina 26

Effettuare impostazioni Wi-Fi mediante pressione di un tasto (WPS)

È possibile impostare automaticamente una rete Wi-Fi premendo un pulsante sul router wireless. Se sono soddisfatte le seguenti condizioni, è possibile eseguire l'impostazione utilizzando questo metodo.

Il router wireless è compatibile con WPS (Wi-Fi Protected Setup).

La connessione Wi-Fi corrente è stata stabilita premendo un pulsante sul router wireless.

Nota:

Se non si riesce a individuare il pulsante o se si sta effettuando l'impostazione tramite il software, consultare la documentazione fornita con il router wireless.

1. Toccare  nella schermata iniziale.

2. Selezionare **Router**.

3. Toccare **Avvia configurazione**.

Se la connessione di rete è già impostata, vengono visualizzati i dettagli sulla connessione. Toccare **Modifica a connessione Wi-Fi**, o **Modifica impostazioni** per modificare le impostazioni.

4. Selezionare **Configurazione tasto (WPS)**.

5. Seguire le istruzioni visualizzate sullo schermo.

Se si desidera verificare lo stato della connessione di rete dello scanner al termine dell'installazione, consultare il seguente collegamento alle informazioni correlate per ulteriori dettagli.

Nota:

Se non è possibile stabilire una connessione, riavviare il router wireless, avvicinarlo allo scanner e riprovare.

Informazioni correlate

➔ [“Verifica dello stato della connessione di rete” a pagina 26](#)

Eeguire le impostazioni Wi-Fi mediante l'impostazione di un codice PIN (WPS)

È possibile connettersi automaticamente a un router wireless tramite un codice PIN. È possibile utilizzare questo metodo di impostazione se un router wireless è dotato della funzionalità WPS (Wi-Fi Protected Setup). Utilizzare un computer per immettere un codice PIN nel router wireless.

1. Toccare  nella schermata iniziale.

2. Selezionare **Router**.

3. Toccare **Avvia configurazione**.

Se la connessione di rete è già impostata, vengono visualizzati i dettagli sulla connessione. Toccare **Modifica a connessione Wi-Fi** o **Modifica impostazioni** per modificare le impostazioni.

4. Selezionare **Altri > Configurazione PIN (WPS)**

5. Seguire le istruzioni visualizzate sullo schermo.

Se si desidera verificare lo stato della connessione di rete dello scanner al termine dell'installazione, consultare il seguente collegamento alle informazioni correlate per ulteriori dettagli.

Nota:

Per ulteriori informazioni sull'immissione di un codice PIN, vedere la documentazione fornita con il router wireless in uso.

Informazioni correlate

➔ [“Verifica dello stato della connessione di rete” a pagina 26](#)

Aggiunta o sostituzione del computer o di dispositivi

Connessione a uno scanner che è stato collegato alla rete

Quando lo scanner è già stato collegato alla rete, è possibile collegare un computer o dispositivo smart allo scanner tramite la rete.

Uso dello scanner di rete da un secondo computer

Si consiglia di utilizzare il programma di installazione per collegare lo scanner al computer. È possibile eseguire il programma di installazione utilizzando uno dei seguenti metodi.

Impostazione dal sito web

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

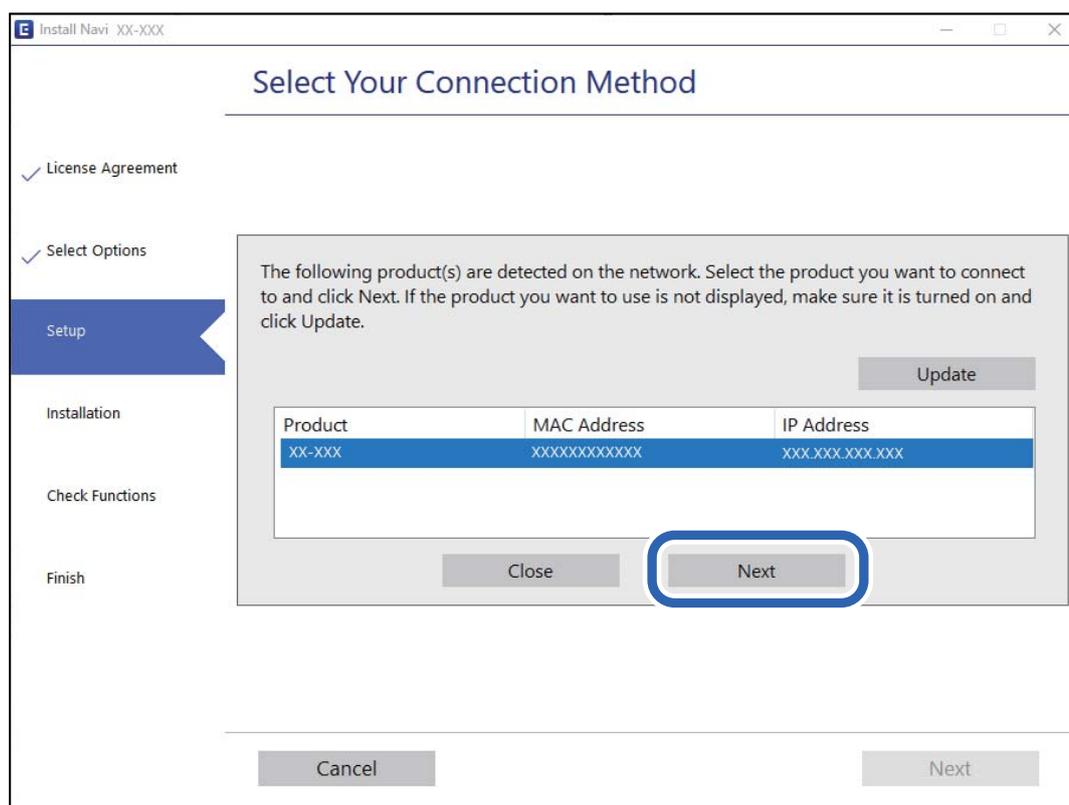
<http://epson.sn>

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

Inserire nel computer il disco del software e seguire le istruzioni a video.

Selezione dello scanner

Seguire le istruzioni a video finché non compare la seguente schermata, selezionare il nome dello scanner a cui connettersi e fare clic su **Avanti**.



Seguire le istruzioni visualizzate sullo schermo.

Uso dello scanner di rete da un dispositivo smart

È possibile connettere un dispositivo smart allo scanner tramite uno dei seguenti metodi.

Connessione di un router wireless

Connettere il dispositivo smart alla stessa rete Wi-Fi (SSID) dello scanner.

Fare riferimento a quanto segue per altre informazioni.

[“Configurazione di impostazioni per la connessione a dispositivi smart” a pagina 25](#)

Connessione tramite Wi-Fi Direct

Connettere il dispositivo smart direttamente allo scanner senza router wireless.

Fare riferimento a quanto segue per altre informazioni.

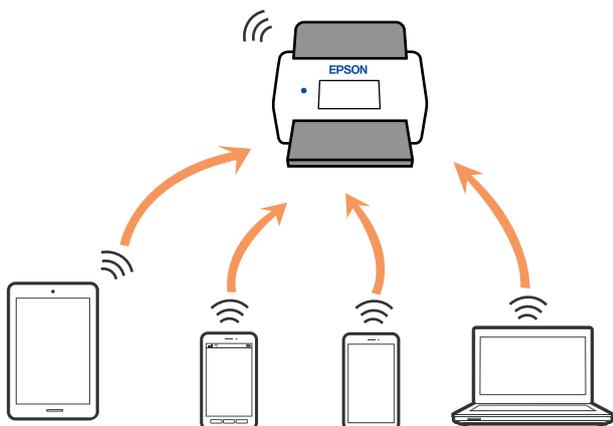
“Collegare un dispositivo smart e lo scanner direttamente (Wi-Fi Direct)” a pagina 22

Collegare un dispositivo smart e lo scanner direttamente (Wi-Fi Direct)

Wi-Fi Direct (AP semplice) consente di connettere un dispositivo smart direttamente allo scanner e senza un router wireless ed eseguire la scansione dal dispositivo smart.

Informazioni su Wi-Fi Direct

Utilizzare questo tipo di connessione quando non si utilizza la connessione Wi-Fi a casa o in ufficio, o quando si desidera collegare direttamente lo scanner, il computer e il dispositivo smart. In questo modo, lo scanner funziona come router wireless ed è possibile collegare i dispositivi allo scanner senza dover utilizzare un router wireless standard. Tuttavia, i dispositivi connessi direttamente allo scanner non possono comunicare tra loro attraverso lo scanner.



Lo scanner può essere collegato simultaneamente tramite connessione Wi-Fi o Ethernet e Wi-Fi Direct (AP semplice). Tuttavia, se si avvia una connessione di rete in Wi-Fi Direct (AP semplice) quando lo scanner è collegato tramite Wi-Fi, il Wi-Fi è temporaneamente scollegato.

Connessione a un dispositivo smart tramite Wi-Fi Direct

Questo metodo consente di collegare lo scanner direttamente ai dispositivi smart senza un router wireless.

1. Selezionare  nella schermata iniziale.
2. Selezionare **Wi-Fi Direct**.
3. Selezionare **Avvia configurazione**.

4. Avviare Epson Smart Panel sul dispositivo smart in uso.
5. Seguire le istruzioni visualizzate in Epson Smart Panel per collegare lo scanner.
Quando il dispositivo smart è collegato allo scanner, andare al passaggio successivo.
6. Nel pannello di controllo dello scanner, selezionare **Completo**.

Disconnessione Wi-Fi Direct (AP semplice)

Esistono due metodi disponibili per disabilitare una connessione Wi-Fi Direct (AP semplice); è possibile disabilitare tutte le connessioni utilizzando il pannello di controllo dello scanner o disabilitare ciascuna connessione dal computer o dal dispositivo smart.

Se si desidera disabilitare tutte le connessioni, selezionare   > **Wi-Fi Direct** > **Avvia configurazione** > **Modifica** > **Disabilita Wi-Fi Direct**.

Importante:

Quando la connessione Wi-Fi Direct (AP semplice) è disattivata, tutti i computer e i dispositivi smart connessi allo scanner con la connessione Wi-Fi Direct (AP semplice) sono disconnessi.

Nota:

Se si desidera disconnettere un dispositivo specifico, effettuare la disconnessione dal dispositivo invece che dallo scanner. Utilizzare uno dei seguenti metodi per disconnettere la connessione Wi-Fi Direct (AP semplice) dal dispositivo.

- Disconnettere la connessione Wi-Fi al nome di rete dello scanner (SSID).
- Connettere a un altro nome di rete (SSID).

Modifica delle impostazioni Wi-Fi Direct (AP semplice) quali l'SSID

Quando è abilitata la connessione Wi-Fi Direct (AP semplice), è possibile modificare le impostazioni da

  > **Wi-Fi Direct** > **Avvia configurazione** > **Modifica**, e successivamente vengono visualizzate le seguenti voci di menu.

Cambia nome rete

Modificare il nome della rete (SSID) Wi-Fi Direct (AP semplice) utilizzato per collegarsi allo scanner nel proprio nome casuale. È possibile impostare il nome della rete (SSID) usando i caratteri ASCII visualizzati nella tastiera software sul pannello di controllo. È possibile inserire fino a 22 caratteri.

Quando si cambia il nome della rete (SSID), tutti i dispositivi collegati vengono disconnessi. Utilizzare il nuovo nome della rete (SSID) se si desidera ricollegare il dispositivo.

Modifica password

Cambiare la password per Wi-Fi Direct (AP semplice) per collegarsi allo scanner al proprio valore arbitrario. È possibile impostare la password usando i caratteri ASCII visualizzati sulla tastiera software sul pannello di controllo. È possibile inserire da 8 a 22 caratteri.

Quando si modifica la password, tutti i dispositivi collegati vengono disconnessi. Utilizzare la nuova password se si desidera ricollegare il dispositivo.

Cambia gamma di frequenza

Modificare l'intervallo di frequenza di Wi-Fi Direct utilizzato per collegarsi allo scanner. È possibile selezionare 2,4 GHz o 5 GHz.

Quando si modifica l'intervallo di frequenza, tutti i dispositivi collegati vengono disconnessi. Ricollegare il dispositivo.

Tenere presente che non è possibile connettersi nuovamente utilizzando dispositivi che non supportano l'intervallo di frequenza da 5 GHz quando si passa a 5 GHz.

L'impostazione potrebbe non essere visualizzata in alcune regioni.

Disabilita Wi-Fi Direct

Disattivare le impostazioni Wi-Fi Direct (AP semplice) dello scanner. Quando le si disabilita, tutti i dispositivi collegati allo scanner in connessione Wi-Fi Direct (AP semplice) sono disconnessi.

Ripristina impostaz. predef.

Ripristinare tutte le impostazioni predefinite di Wi-Fi Direct (AP semplice).

Le informazioni sulla connessione Wi-Fi Direct (AP semplice) del dispositivo smart salvate sullo scanner vengono eliminate.

Nota:

*È inoltre possibile impostare la scheda **Rete** > **Wi-Fi Direct** su Web Config per le seguenti impostazioni.*

- Abilitazione o disabilitazione di Wi-Fi Direct (AP semplice)*
- Modifica del nome della rete (SSID)*
- Modifica della password*
- Modifica dell'intervallo di frequenza*
L'impostazione potrebbe non essere visualizzata in alcune regioni.
- Ripristino delle impostazioni di Wi-Fi Direct (AP semplice)*

Reimpostare il collegamento di rete

Questa sezione spiega come creare le impostazioni del collegamento di rete e modificare il metodo di connessione quando viene sostituito il router wireless o il computer.

Quando si sostituisce il router wireless

Quando si sostituisce il router wireless, configurare le impostazioni per il collegamento tra il computer o il dispositivo smart e lo scanner.

È necessario regolare queste impostazioni se cambia il fornitore del servizio internet, ecc.

Creazione di impostazioni per la connessione al computer

Si consiglia di utilizzare il programma di installazione per collegare lo scanner al computer. È possibile eseguire il programma di installazione utilizzando uno dei seguenti metodi.

Impostazione dal sito web

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

<http://epson.sn>

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

Inserire nel computer il disco del software e seguire le istruzioni a video.

Selezionare i metodi di connessione

Seguire le istruzioni visualizzate sullo schermo. Nella schermata **Seleziona l'operazione**, selezionare **Reimposta configurazione di Stampante (per un nuovo router di rete o il passaggio da USB a rete, ecc.)**, quindi fare clic su **Avanti**.

Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.

Se non è possibile eseguire la connessione, vedere quanto segue per cercare di risolvere il problema.

[“Non è possibile collegarsi a una rete” a pagina 32](#)

Configurazione di impostazioni per la connessione a dispositivi smart

È possibile utilizzare lo scanner da un dispositivo smart quando si collega lo scanner alla stessa rete Wi-Fi (SSID) del dispositivo smart. Per utilizzare lo scanner da un dispositivo smart, accedere al seguente sito web, quindi immettere il nome del prodotto. Andare su **Impostazione**, quindi avviare la procedura di impostazione.

<http://epson.sn>

Accedere al sito web dal dispositivo smart che si desidera collegare allo scanner.

Quando si sostituisce il computer

Quando si sostituisce il computer, configurare le impostazioni di collegamento tra il computer e lo scanner.

Creazione di impostazioni per la connessione al computer

Si consiglia di utilizzare il programma di installazione per collegare lo scanner al computer. È possibile eseguire il programma di installazione utilizzando il seguente metodo.

Impostazione dal sito web

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

<http://epson.sn>

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

Inserire nel computer il disco del software e seguire le istruzioni a video.

Seguire le istruzioni visualizzate sullo schermo.

Modifica del metodo di connessione sul computer

Questa sezione illustra come modificare il metodo di connessione quando il computer e lo scanner sono collegati.

Modifica della connessione di rete da Ethernet a Wi-Fi

Passare dalla connessione Ethernet alla connessione Wi-Fi dal pannello di controllo dello scanner. La modifica del metodo di connessione è sostanzialmente equivalente alle impostazioni di connessione Wi-Fi.

Informazioni correlate

➔ [“Connessione alla LAN wireless \(Wi-Fi\)” a pagina 18](#)

Modifica della connessione di rete da Wi-Fi a Ethernet

Seguire i passaggi riportati sotto per la modifica dalla connessione Wi-Fi alla connessione Ethernet.

1. Selezionare **Impostazioni** nella schermata iniziale.
2. Selezionare **Impostazioni di rete > Configurazione LAN cablata**.
3. Seguire le istruzioni visualizzate sullo schermo.

Modifica da USB a connessione di rete

Procedere come segue per utilizzare il programma di installazione ed eseguire nuovamente la configurazione con un metodo di connessione diverso.

Impostazione dal sito web

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

<http://epson.sn>

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

Inserire nel computer il disco del software e seguire le istruzioni a video.

Selezionare modifica metodi di collegamento

Seguire le istruzioni visualizzate sullo schermo. Nella schermata **Seleziona l'operazione**, selezionare **Reimposta configurazione di Stampante (per un nuovo router di rete o il passaggio da USB a rete, ecc.)**, quindi fare clic su **Avanti**.

Selezionare la connessione di rete che si desidera utilizzare, **Connetti tramite rete wireless (Wi-Fi)** o **Connetti tramite LAN cablata (Ethernet)**, quindi fare clic su **Avanti**.

Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.

Verifica dello stato della connessione di rete

È possibile controllare lo stato della connessione di rete nel modo seguente.

Verifica dello stato del collegamento di rete dal pannello di controllo

È possibile verificare lo stato di collegamento della rete tramite l'icona di rete nel pannello di controllo dello scanner.

Controllare lo stato di collegamento della rete usando l'icona rete

È possibile verificare lo stato di connessione e la potenza delle onde radio tramite l'icona di rete nella schermata iniziale dello scanner.



	<p>Visualizza lo stato della connessione di rete.</p> <p>Selezionare l'icona per verificare e modificare le impostazioni correnti. Di seguito è illustrata la scorciatoia per il seguente menu.</p> <p>Impostazioni > Impostazioni di rete > Configurazione Wi-Fi</p>
	<p>Lo scanner non è connesso a una rete wireless (Wi-Fi).</p>
	<p>Lo scanner sta cercando l'SSID, ha disattivato l'impostazione dell'indirizzo IP oppure ha un problema con una rete wireless (Wi-Fi).</p>
	<p>Lo scanner è connesso a una rete wireless (Wi-Fi).</p> <p>Il numero di barrette indica la potenza di segnale della connessione. Maggiore è il numero di barrette visualizzate, maggiore è la potenza del segnale.</p>
	<p>Lo scanner non è collegato a una rete wireless (Wi-Fi) in modalità Wi-Fi Direct (AP semplice).</p>
	<p>Lo scanner è collegato a una rete wireless (Wi-Fi) in modalità Wi-Fi Direct (AP semplice).</p>
	<p>Lo scanner non è collegato a una rete cablata (Ethernet) oppure l'impostazione è stata disattivata.</p>
	<p>Lo scanner è collegato a una rete cablata (Ethernet).</p>

Visualizzazione delle informazioni dettagliate sulla rete dal pannello di controllo

Quando lo scanner è connesso alla rete, è possibile visualizzare anche altre informazioni relative alla rete selezionando il menu della rete da verificare.

1. Selezionare **Impostazioni** nella schermata iniziale.

2. Scegliere **Impostazioni di rete > Stato rete**.
3. Per controllare altre informazioni, selezionare i menu da controllare.
 - Stato LAN cablata/Wi-Fi
Consente di visualizzare le informazioni di rete (nome del dispositivo, connessione, potenza del segnale e altro ancora) per connessioni Ethernet o Wi-Fi.
 - Stato di Wi-Fi Direct
Visualizza se la funzione Wi-Fi Direct è attivata o disattivata, e l'SSID, la password e altro ancora per le connessioni Wi-Fi Direct.
 - Stato server e-mail
Consente di visualizzare le informazioni di rete per il server di posta.

Specifiche di rete

Specifiche Wi-Fi

Consultare la tabella seguente per le specifiche Wi-Fi.

Paesi o regioni diversi da quanto elencato di seguito	Tabella A
Australia Nuova Zelanda Taiwan Corea del sud	Tabella B

Tabella A

Standard	IEEE 802.11b/g/n ^{*1}
Gamma di frequenza	2,4 GHz
Potenza massima radiofrequenza trasmessa	2.400–2.483,5 MHz: 20 dBm (EIRP)
Canali	1/2/3/4/5/6/7/8/9/10/11/12/13
Modalità di connessione	Infrastruttura, Wi-Fi Direct (AP semplice) ^{*2*3}
Protocolli di sicurezza ^{*4}	WEP (64/128bit), WPA2-PSK (AES) ^{*5} , WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Disponibile solo per HT20.

*2 Non supportato per IEEE 802.11b.

*3 È possibile utilizzare contemporaneamente le modalità Infrastruttura e Wi-Fi Direct o una connessione Ethernet.

*4 Wi-Fi Direct supporta solo WPA2-PSK (AES).

*5 Conforme agli standard WPA2 con supporto per WPA/WPA2 Personal.

Tabella B

Standard	IEEE 802.11a/b/g/n ^{*1} /ac		
Intervalli di frequenza	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Canali	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 ^{*2} /13 ^{*2}
		5 GHz ^{*3}	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 ^{*2} /13 ^{*2}
		5 GHz ^{*3}	W52 (36/40/44/48) W58 (149/153/157/161/165)
Modalità di connessione	Infrastruttura, Wi-Fi Direct (AP semplice) ^{*4, *5}		
Protocolli di sicurezza ^{*6}	WEP (64/128bit), WPA2-PSK (AES) ^{*7} , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Disponibile solo per HT20.

*2 Non disponibile a Taiwan.

*3 La disponibilità di questi canali e la possibilità di utilizzo del prodotto all'esterno variano a seconda dell'area geografica. Per ulteriori informazioni, vedere <http://support.epson.net/wifi5ghz/>

*4 Non supportato per IEEE 802.11b.

*5 È possibile utilizzare contemporaneamente le modalità Infrastruttura e Wi-Fi Direct o una connessione Ethernet.

*6 Wi-Fi Direct supporta solo WPA2-PSK (AES).

*7 Conforme agli standard WPA2 con supporto per WPA/WPA2 Personal.

Specifiche Ethernet

Standard	IEEE802.3i (10BASE-T) ^{*1} IEEE802.3u (100BASE-TX) ^{*1} IEEE802.3ab (1000BASE-T) ^{*1} IEEE802.3az (Ethernet a efficienza energetica) ^{*2}
Modalità di comunicazione	Auto, Full duplex 10 Mbps, Half duplex 10 Mbps, Full duplex 100 Mbps, Half duplex 100 Mbps
Connettore	RJ-45

*1 Usare un cavo STP (doppino intrecciato schermato) di categoria 5e o superiore per evitare rischi di interferenza radio.

*2 Il dispositivo collegato deve essere conforme alle norme IEEE802.3az.

Funzioni di rete e IPv4/IPv6

Funzioni	Supportate
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

Protocollo di sicurezza

IEEE802.1X*	
Filtraggio IPsec/IP	
SSL/TLS	HTTPS Server/Client
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* È necessario utilizzare un dispositivo di connessione conforme alla IEEE802.1X.

Utilizzo della porta per lo scanner

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

Quando il mittente (client) è lo scanner

Usa	Destinazione (Server)	Protocollo	Numero di porta	
Invio di file (quando si utilizza la funzione di scansione a una cartella di rete dallo scanner)	Server FTP/FTPS	FTP/FTPS (TCP)	20	
			21	
	File server	SMB (TCP)	445	
			NetBIOS (UDP)	137
				138
	Server WebDAV	Protocollo HTTP (TCP)	80	
Protocollo HTTPS(TCP)			443	
Invio di e-mail (quando si utilizza la funzione di scansione a un indirizzo e-mail dallo scanner)	Server SMTP	SMTP (TCP)	25	
		SMTP SSL/TLS (TCP)	465	
		SMTP STARTTLS (TCP)	587	

Usa	Destinazione (Server)	Protocollo	Numero di porta
POP prima di connessione SMTP (quando si utilizza la funzione di scansione a un indirizzo e-mail dallo scanner)	Server POP	POP3 (TCP)	110
Quando si utilizza Epson Connect	Server Epson Connect	HTTPS	443
		XMPP	5222
Raccolta di informazioni sull'utente (utilizzare i contatti dello scanner)	Server LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Autenticazione utente per la raccolta di informazioni sull'utente (quando si utilizzano i contatti dello scanner) Autenticazione utente quando si utilizza la scansione su cartella di rete (SMB) dallo scanner	Server KDC	Kerberos	88
Controllo WSD	Computer client	WSD (TCP)	5357
Ricerca del computer quando viene eseguita la scansione push da un'applicazione	Computer client	Rilevamento scansione Push di rete	2968

Quando il mittente (client) è il computer client

Usa	Destinazione (Server)	Protocollo	Numero di porta
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 un'applicazione	Scanner	Scansione di rete (TCP)	1865
Raccolta di informazioni sul lavoro quando viene eseguita la scansione push da un'applicazione	Scanner	Scansione Push di rete	2968
Web Config	Scanner	HTTP (TCP)	80
		HTTPS (TCP)	443

Soluzione dei problemi

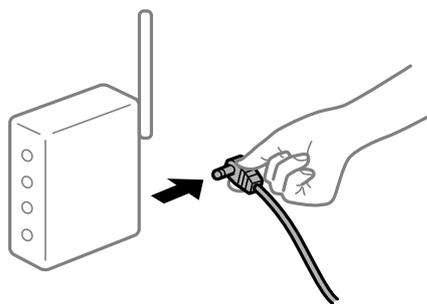
Non è possibile collegarsi a una rete

Potrebbe essersi verificato uno dei seguenti problemi.

■ Si è verificato un problema con i dispositivi di rete per il collegamento Wi-Fi.

Soluzioni

Spegnere i dispositivi che si vogliono collegare alla rete. Attendere circa 10 secondi, quindi accendere i dispositivi nel seguente ordine: router wireless, computer o dispositivo smart e scanner. Avvicinare lo scanner e il computer o dispositivo smart al router wireless per facilitare la comunicazione delle onde radio, quindi provare a effettuare nuovamente le impostazioni di rete.



■ I dispositivi non possono ricevere segnali dal router wireless poiché sono troppo lontani.

Soluzioni

Dopo aver avvicinato il computer o il dispositivo smart e lo scanner al router wireless, spegnere il router wireless, quindi accenderlo nuovamente.

■ Quando si sostituisce il router wireless, le impostazioni non corrispondono a quelle del nuovo router.

Soluzioni

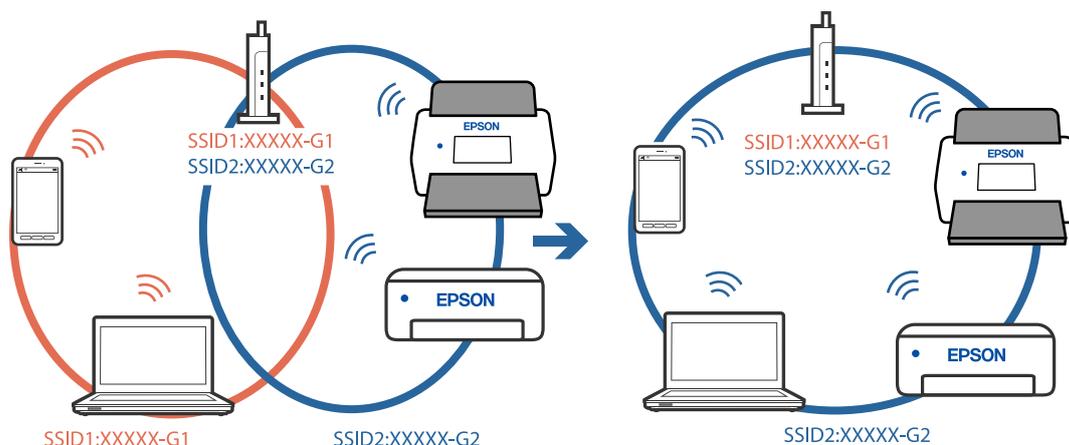
Creare nuovamente le impostazioni di collegamento in modo che corrispondano al nuovo router wireless.

■ Gli SSID connessi dal computer o da dispositivi smart e computer sono diversi.

Soluzioni

Quando si utilizzano router wireless multipli contemporaneamente o il router wireless ha SSID multipli e i dispositivi sono connessi a SSID diversi, la connessione al router wireless non è possibile.

Connettere il computer o lo smart device allo stesso SSID dello scanner.



È disponibile un separatore di riservatezza sul router wireless.

Soluzioni

Molti router wireless hanno una funzione di separatore di riservatezza, che blocca la comunicazione tra dispositivi collegati. Se la comunicazione tra lo scanner e il computer o il dispositivo smart non è possibile anche se sono collegati alla stessa rete, disabilitare il separatore di riservatezza sul router wireless. Per ulteriori dettagli, consultare il manuale fornito in dotazione con il router wireless.

L'indirizzo IP non è stato assegnato correttamente.

Soluzioni

Se l'indirizzo IP assegnato allo scanner è 169.254.XXX.XXX e la maschera di sottorete è 255.255.0.0, l'indirizzo IP potrebbe non essere stato assegnato correttamente.

Selezionare **Impostazioni > Impostazioni di rete > Avanzate > Impostazioni TCP/IP** dal pannello di controllo dello scanner, quindi verificare l'indirizzo IP e la maschera di sottorete assegnata allo scanner.

Riavviare il router wireless o ripristinare le impostazioni di rete dello scanner.

C'è un problema con le impostazioni di rete sul computer.

Soluzioni

Provare ad accedere a qualsiasi sito web dal computer per assicurarsi che le relative impostazioni di rete siano corrette. Se non è possibile accedere a qualsiasi sito web, il problema è a livello di computer.

Verificare la connessione di rete del computer. Per i dettagli, vedere la documentazione fornita con il computer.

Lo scanner è collegato tramite Ethernet utilizzando dispositivi che supportano IEEE 802.3az (Energy Efficient Ethernet).

Soluzioni

Quando si connette lo scanner tramite Ethernet utilizzando dispositivi che supportano IEEE 802.3az (Energy Efficient Ethernet), possono verificarsi i seguenti problemi a seconda dell'hub o del router in uso.

- La connessione diventa instabile, lo scanner si connette e disconnette ripetutamente.
- Non è possibile connettersi allo scanner.
- La velocità di comunicazione si rallenta.

Attenersi alla seguente procedura per disabilitare IEEE 802.3az per lo scanner, quindi connettersi.

1. Rimuovere il cavo Ethernet collegato al computer e allo scanner.
2. Quando è abilitato IEEE 802.3az per il computer, disabilitarlo.
Per i dettagli, vedere la documentazione fornita con il computer.
3. Collegare direttamente il computer allo scanner mediante un cavo Ethernet.
4. Sullo scanner, verificare le impostazioni di rete.
Selezionare **Impostazioni > Impostazioni di rete > Stato rete > Stato LAN cablata/Wi-Fi**.
5. Verificare l'indirizzo IP dello scanner.
6. Sul computer, accedere a Web Config.
Avviare un browser web e immettere l'indirizzo IP dello scanner.
[“Esecuzione di Web Config su un browser web” a pagina 36](#)
7. Selezionare la scheda **Rete > LAN cablata**.
8. Selezionare **DISATTIVA** per **IEEE 802.3az**.
9. Fare clic su **Avanti**.
10. Fare clic su **OK**.
11. Rimuovere il cavo Ethernet collegato al computer e allo scanner.
12. Se si è disabilitato IEEE 802.3az per il computer nel passaggio 2, abilitarlo.
13. Collegare i cavi Ethernet rimossi nel passaggio 1 al computer e allo scanner.
Se il problema persiste, è possibile che il problema sia causato da dispositivi diversi dallo scanner.

■ Lo scanner è spento.

Soluzioni

Assicurarsi che lo scanner sia acceso.

Inoltre, attendere che la spia di stato smetta di lampeggiare, indicando che lo scanner è pronto per eseguire la scansione.

Software per la configurazione dello scanner

Web Config.	36
Epson Device Admin.	37

Web Config

Web Config è un'applicazione eseguibile da un browser web, come Internet Explorer e Safari, su un computer. È possibile verificare lo stato dello scanner e modificare le impostazioni dello scanner e del servizio di rete. Poiché gli scanner sono accessibili e gestiti direttamente dalla rete, è adatta a configurare uno scanner per volta. Per utilizzare Web Config, collegare il computer alla stessa rete dello scanner.

Sono supportati i browser seguenti.

Microsoft Edge, Windows Internet Explorer 8 o versioni successive, Firefox*, Chrome*, Safari*

* Utilizzare la versione più recente.

Esecuzione di Web Config su un browser web

1. Verificare l'indirizzo IP dello scanner.

Selezionare **Impostazioni** > **Impostazioni di rete** > **Stato rete** sul pannello di controllo dello scanner. Successivamente, selezionare lo stato del metodo di connessione attivo (**Stato LAN cablata/Wi-Fi** o **Stato di Wi-Fi Direct**) per verificare l'indirizzo IP dello scanner.

2. Lanciare un browser web da un computer o dispositivo smart, quindi inserire l'indirizzo IP dello scanner.

Formato:

IPv4: http://indirizzo IP dello scanner/

IPv6: http://[indirizzo IP dello scanner]/

Esempi:

IPv4: http://192.168.100.201/

IPv6: http://[2001:db8::1000:1]/

Nota:

Poiché lo scanner utilizza un certificato autofirmato quando si accede a HTTPS, viene visualizzato un avviso sul browser quando si avvia Web Config; tuttavia ciò non indica un problema e può essere ignorato.

3. Accedere come amministratore per modificare le impostazioni dello scanner.

Fare clic su **Login amministratore** in alto a destra dello schermo. Inserire **Nome utente** e **Password corrente**, quindi fare clic su **OK**.

Nota:

- Di seguito sono forniti i valori iniziali per le informazioni amministratore di Web Config.

·Nome utente: nessuno (vuoto)

·Password: numero di serie dello scanner

Per trovare il numero di serie, verificare l'etichetta sul retro dello scanner.

- Se viene visualizzato **Logout amministratore** nella parte superiore destra dello schermo, è già stato effettuato l'accesso come amministratore.

Esecuzione di Web Config in sistemi Windows

Quando si collega un computer allo scanner tramite WSD, procedere come segue per eseguire Web Config.

1. Aprire l'elenco degli scanner sul computer.
 - Windows 10
Fare clic sul pulsante Start, quindi selezionare **Sistema Windows > Pannello di controllo > Visualizza dispositivi e stampanti in Hardware e suoni**.
 - Windows 8.1/Windows 8
Selezionare **Desktop > Impostazioni > Pannello di controllo > Visualizza dispositivi e stampanti in Hardware e suoni** (o in **Hardware**).
 - Windows 7
Fare clic sul pulsante Start e selezionare **Pannello di controllo > Visualizza dispositivi e stampanti in Hardware e suoni**.
2. Fare clic con il pulsante destro del mouse sullo scanner in uso e scegliere **Proprietà**.
3. Selezionare la scheda **Servizio Web** e fare clic sull'URL visualizzato.

Poiché lo scanner utilizza un certificato autofirmato quando si accede a HTTPS, viene visualizzato un avviso sul browser quando si avvia Web Config; tuttavia ciò non indica un problema e può essere ignorato.

Nota:

 - Di seguito sono forniti i valori iniziali per le informazioni amministratore di Web Config.*
 - Nome utente: nessuno (vuoto)*
 - Password: numero di serie dello scanner*
 - Per trovare il numero di serie, verificare l'etichetta sul retro dello scanner.*
 - Se viene visualizzato **Logout amministratore** nella parte superiore destra dello schermo, è già stato effettuato l'accesso come amministratore.*

Epson Device Admin

Epson Device Admin è un'applicazione multifunzione per la gestione dei dispositivi collegati su una rete.

È possibile utilizzare i modelli di configurazione per applicare le stesse impostazioni a più scanner su una rete, rendendoli adatti per l'installazione e la gestione di più scanner.

È possibile scaricare Epson Device Admin dal sito web del supporto Epson. Per i dettagli su come utilizzare l'applicazione, consultare la documentazione o la guida di Epson Device Admin.

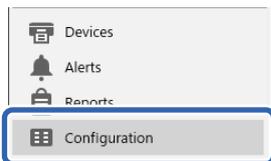
Modello di configurazione

Creazione del modello di configurazione

Creare un nuovo modello di configurazione.

1. Avviare Epson Device Admin.

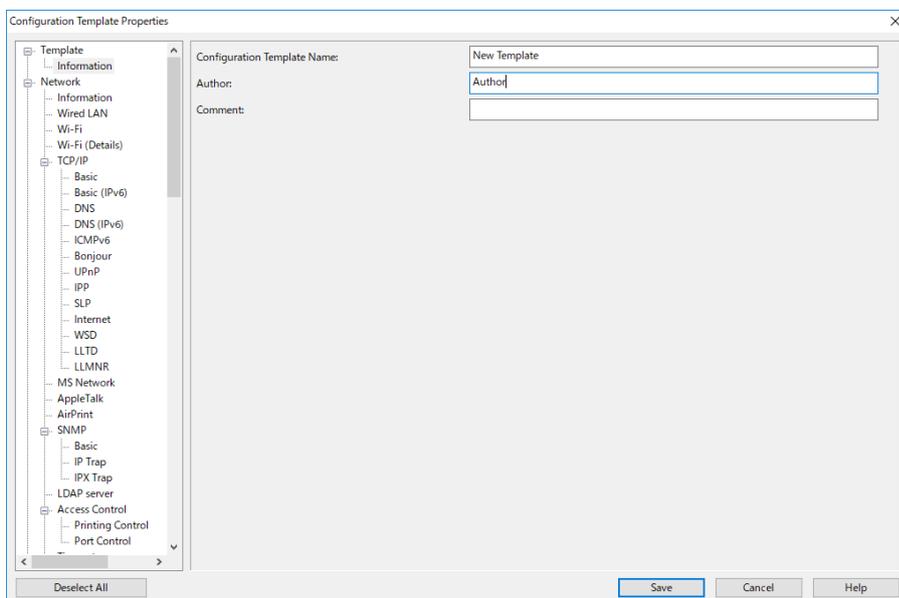
2. Selezionare **Configurazione** sul menu delle attività della barra laterale.



3. Selezionare **Nuovo** sul menu barra multifunzione.



4. Impostare ogni voce.



Voce	Descrizione
Nome modello di configurazione	Nome del modello di configurazione. Immettere fino a 1024 caratteri in Unicode (UTF-8).
Autore	Informazioni sul creatore del modello. Immettere fino a 1024 caratteri in Unicode (UTF-8).
Commento	Immettere informazioni a piacere. Immettere fino a 1024 caratteri in Unicode (UTF-8).

5. Selezionare le voci che si desidera impostare sulla sinistra.

Nota:

Fare clic sulle voci di menu a sinistra per passare a ciascuna schermata. Il valore impostato viene mantenuto se si cambia schermata, ma non se si annulla la schermata. Una volta terminata l'effettuazione delle impostazioni, toccare **Salva**.

Applicazione del modello di configurazione

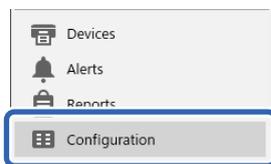
Applicare il modello di configurazione salvato allo scanner. Gli elementi selezionati sul modello sono applicati. Se lo scanner di destinazione non dispone della funzione appropriata, il modello non viene applicato.

Nota:

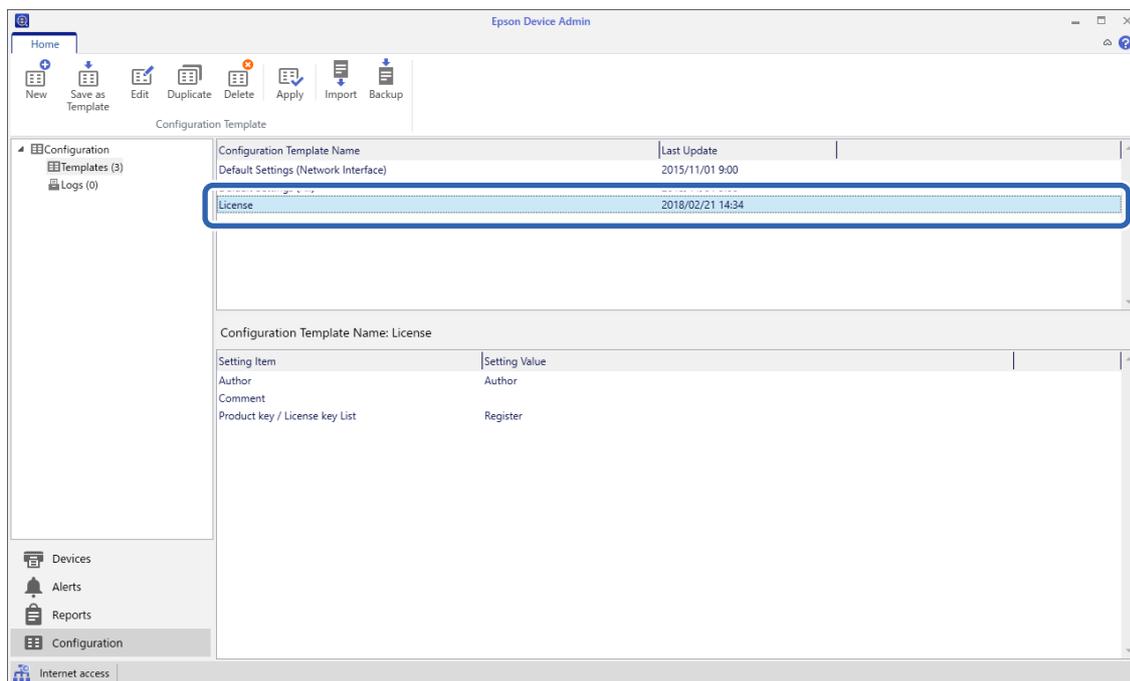
Se sullo scanner è impostata la password di amministratore, configurare la password in anticipo.

1. Nel menu a tendina della schermata Elenco dispositivi, selezionare **Opzioni > Gestione password**.
2. Selezionare **Abilita gestione password automatica**, quindi fare clic su **Gestione password**.
3. Selezionare lo scanner appropriato, quindi fare clic su **Modifica**.
4. Impostare la password e fare clic su **OK**.

1. Selezionare **Configurazione** sul menu delle attività della barra laterale.



2. Selezionare il modello di configurazione da applicare da **Nome modello di configurazione**.



3. Fare clic su **Applica** sul menu barra multifunzione.
Viene visualizzata la schermata di selezione della periferica.

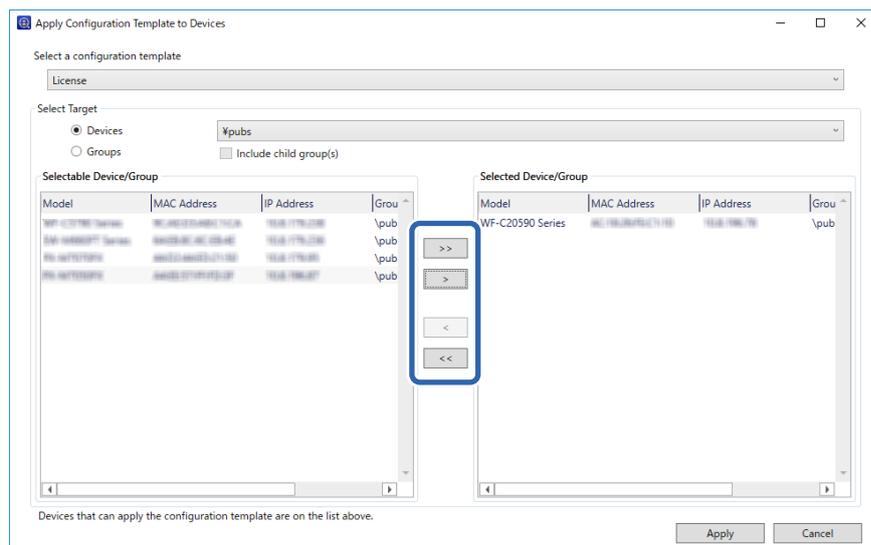


4. Selezionare il modello di configurazione da applicare.

Nota:

- Quando si seleziona **Stampante** e i gruppi contenenti le periferiche dal menu a discesa, viene visualizzata ogni periferica.
- Selezionando **Gruppi** vengono visualizzati i gruppi. Selezionare **Includi gruppi secondari** per selezionare automaticamente i gruppi secondari all'interno del gruppo selezionato.

5. Spostare lo scanner o i gruppi cui si desidera applicare il modello in **Dispositivo/Gruppo selezionato**.



6. Fare clic su **Applica**.
Viene visualizzata una schermata di conferma per il modello di configurazione da applicare.
7. Fare clic su **OK** per applicare il modello di configurazione.
8. Quando viene visualizzato un messaggio che indica che la procedura è stata completata, fare clic su **OK**.
9. Fare clic su **Dettagli** e controllare le informazioni.
Quando viene visualizzato sugli elementi applicati, l'applicazione è stata completata correttamente.
10. Fare clic su **Chiudi**.

Impostazioni richieste per la scansione

Configurazione di un server di posta.	42
Impostazione di una cartella di rete condivisa.	45
Rendere disponibili i contatti.	61
Utilizzo di Document Capture Pro Server.	71
Configurazione di AirPrint.	72
Problemi durante la preparazione della scansione in rete.	72

Configurazione di un server di posta

Impostare il server di posta elettronica da Web Config.

Quando lo scanner può inviare delle e-mail impostando il server di posta elettronica, sono possibili le seguenti operazioni.

- Trasferimento dei risultati della scansione tramite e-mail
- Ricezione della notifica via e-mail dallo scanner

Verificare quando segue prima di effettuare le impostazioni.

- Lo scanner è connesso alla rete che può accedere al server di posta.
- Informazioni di impostazione della posta elettronica del computer che utilizza lo stesso server di posta dello scanner.

Nota:

- Quando si utilizza il server di posta su Internet, verificare le informazioni di impostazione fornite dal provider o dal sito web.
- È possibile configurare il server di posta anche dal pannello di controllo. Accesso come descritto di seguito.

Impostazioni > Impostazioni di rete > Avanzate > Server e-mail > Impostazioni server

1. Accedere a Web Config e selezionare la scheda **Rete > Server e-mail > Di base**.
2. Inserire un valore per ciascuna voce.
3. Selezionare **OK**.
Vengono visualizzate le impostazioni selezionate.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Voci di impostazione del server di posta

Elementi	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 in ASCII (0x20–0x7E).	

Elementi	Impostazioni e descrizione	
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.	
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.	

Verifica della connessione al server di posta

È possibile controllare la connessione al server di posta eseguendo il controllo di connessione.

1. Accedere a Web Config e selezionare la scheda **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 report di controllo.

Nota:

È possibile verificare la connessione al server di posta anche dal pannello di controllo. Accesso come descritto di seguito.

Impostazioni > Impostazioni di rete > Avanzate > Server e-mail > Controllo connessione

Riferimenti per test di connessione al server di posta

Messaggi	Causa
Test di connessione riuscito.	Questo messaggio appare quando la connessione con il server avviene correttamente.

Messaggi	Causa
<p>Errore di comunicazione server SMTP. Controllare quanto segue. - Impostazioni di rete</p>	<p>Questo messaggio appare quando</p> <ul style="list-style-type: none"> <input type="checkbox"/> Lo scanner non è connesso a una rete <input type="checkbox"/> Il server SMTP è inattivo <input type="checkbox"/> La connessione di rete viene disattivata durante la comunicazione <input type="checkbox"/> Sono stati ricevuti dati incompleti
<p>Errore di comunicazione server POP3. Controllare quanto segue. - Impostazioni di rete</p>	<p>Questo messaggio appare quando</p> <ul style="list-style-type: none"> <input type="checkbox"/> Lo scanner non è connesso a una rete <input type="checkbox"/> Il server POP3 è inattivo <input type="checkbox"/> La connessione di rete viene disattivata durante la comunicazione <input type="checkbox"/> Sono stati ricevuti dati incompleti
<p>Errore durante la conness. al server SMTP. Controllare quanto segue. - Indirizzo server SMTP - Server DNS</p>	<p>Questo messaggio appare quando</p> <ul style="list-style-type: none"> <input type="checkbox"/> La connessione a un server DNS non è riuscita <input type="checkbox"/> La risoluzione del nome per un server SMTP non è riuscita
<p>Errore durante la conness. al server POP3. Controllare quanto segue. - Indirizzo server POP3 - Server DNS</p>	<p>Questo messaggio appare quando</p> <ul style="list-style-type: none"> <input type="checkbox"/> La connessione a un server DNS non è riuscita <input type="checkbox"/> Risoluzione dei nomi per un server POP3 non riuscita
<p>Errore di autenticazione server SMTP. Controllare quanto segue. - Metodo autenticazione - Account autenticato - Password autenticata</p>	<p>Questo messaggio appare quando si verifica un errore nel server di autenticazione SMTP.</p>
<p>Errore di autenticazione server POP3. Controllare quanto segue. - Metodo autenticazione - Account autenticato - Password autenticata</p>	<p>Questo messaggio appare quando si verifica un errore nel server di autenticazione POP3.</p>
<p>Metodo di comunicazione non supportato. Controllare quanto segue. - Indirizzo server SMTP - Numero porta server SMTP</p>	<p>Questo messaggio appare quando si cerca di comunicare con protocolli non supportati.</p>
<p>Connessione al server SMTP non riuscita. Cambiare Connessione protetta in Nessuno.</p>	<p>Questo messaggio appare quando si verifica una mancata corrispondenza SMTP tra un server e un client, o quando il server non supporta la connessione protetta SMTP (connessione SSL).</p>
<p>Connessione al server SMTP non riuscita. Cambiare Connessione protetta in SSL/TLS.</p>	<p>Questo messaggio appare in caso di mancata corrispondenza SMTP tra un server e un client, o quando il server richiede di utilizzare una connessione SSL/TLS per una connessione protetta SMTP.</p>
<p>Connessione al server SMTP non riuscita. Cambiare Connessione protetta in STARTTLS.</p>	<p>Questo messaggio viene visualizzato in caso di mancata corrispondenza di SMTP tra un server e un client o quando il server richiede di utilizzare una connessione STARTTLS per una connessione protetta SMTP.</p>
<p>Connessione non affidabile. Controllare quanto segue. - Data e ora</p>	<p>Questo messaggio appare quando le impostazioni di data e ora dello scanner non sono corrette o il certificato è scaduto.</p>
<p>Connessione non affidabile. Controllare quanto segue. - Certificato CA</p>	<p>Questo messaggio appare quando lo scanner non dispone di un certificato radice corrispondente al server, o non è stato importato un Certificato CA.</p>
<p>Connessione non affidabile.</p>	<p>Questo messaggio appare quando il certificato ottenuto è danneggiato.</p>

Messaggi	Causa
Autenticazione server SMTP non riuscita. Cambiare Metodo autenticazione in AUT. SMTP.	Questo messaggio appare in caso di mancata corrispondenza del metodo di autenticazione tra un server e un 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 un server e un client. Il server non supporta AUT. SMTP.
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 del mittente specificato non è corretto.
Impossibile accedere al prodotto fino al termine dell'elaborazione.	Questo messaggio appare quando lo scanner è occupato.

Impostazione di una cartella di rete condivisa

Impostare una cartella di rete per salvare un'immagine acquisita.

Quando si salva un file nella cartella, lo scanner accede come utente del computer su cui è stata creata la cartella.

Creazione della cartella condivisa

Informazioni correlate

- ➔ [“Prima di creare la cartella condivisa” a pagina 45](#)
- ➔ [“Verifica del profilo di rete” a pagina 46](#)
- ➔ [“Posizione in cui creare la cartella condivisa e esempio di sicurezza” a pagina 46](#)
- ➔ [“Aggiunta di un gruppo o di un utente cui consentire l'accesso” a pagina 57](#)

Prima di creare la cartella condivisa

Prima di creare la cartella condivisa, verificare quanto segue.

- Lo scanner è connesso alla rete in cui può accedere al computer in cui verrà creata la cartella condivisa.
- Nessun carattere multi-byte è presente nel nome del computer in cui verrà creata la cartella condivisa.

Importante:

Quando un carattere multi-byte è presente nel nome del computer, il salvataggio del file nella cartella condivisa potrebbe non riuscire.

In tal caso, passare a un computer che non comprenda un carattere multi-byte nel nome o modificare il nome del computer.

Quando si modifica il nome del computer, assicurarsi di confermare in precedenza tutto ciò con l'amministratore, poiché questo fatto potrebbe interessare alcune impostazioni, ad esempio la gestione del computer, l'accesso alle risorse, ecc.

Verifica del profilo di rete

Sul computer in cui verrà creata la cartella condivisa, controllare se è disponibile la condivisione di cartelle.

1. Accedere al computer in cui la cartella condivisa verrà creata dall'account utente con autorità di amministratore.
2. Selezionare **Pannello di Controllo > Rete e Internet > Centro connessioni di rete e condivisione**.
3. Fare clic su **Modifica impostazioni di condivisione avanzate**, quindi fare clic su  per il profilo con **(profilo corrente)** nei profili di rete visualizzati.
4. Controllare se **Attiva condivisione file e stampanti** è selezionata in **Condivisione file e stampanti**.
Se è già selezionata, fare clic su **Annulla** e chiudere la finestra.
Quando si modificano le impostazioni, fare clic su **Salva modifiche** e chiudere la finestra.

Posizione in cui creare la cartella condivisa e esempio di sicurezza

A seconda della posizione in cui viene creata la cartella condivisa, la sicurezza e la comodità variano.

Per utilizzare la cartella condivisa dagli scanner o da altri computer, sono necessarie le seguenti autorizzazioni di lettura e modifica per la cartella.

Scheda **Condivisione** > poi **Condivisione avanzata** > **Autorizzazioni**

Controlla il permesso di accesso della rete alla cartella condivisa.

Autorizzazione di accesso della scheda **Sicurezza**

Controlla il permesso di accesso della rete e l'accesso locale alla cartella condivisa.

Quando si imposta **Tutti** per la cartella condivisa creata sul desktop, come esempio di creazione di una cartella condivisa, sarà consentito l'accesso a tutti gli utenti che possono accedere al computer.

Tuttavia, l'utente che non dispone di autorità non può accedere perché il desktop (cartella) è sotto il controllo della cartella utente, quindi al desktop vengono assegnate le impostazioni di sicurezza della cartella utente. L'utente cui è consentito l'accesso nella scheda **Sicurezza** (utente connesso e amministratore in questo caso) può utilizzare la cartella.

Vedere di seguito per la creazione della posizione corretta.

Questo esempio vale per quando si crea la cartella "scan_folder".

Informazioni correlate

➔ [“Esempio di configurazione per un i file server” a pagina 46](#)

➔ [“Esempio di configurazione per un personal computer” a pagina 52](#)

Esempio di configurazione per un i file server

La presente spiegazione fornisce un esempio per la creazione di una cartella condivisa sulla radice dell'unità del computer condiviso, quale il file server nell'esempio seguente.

Gli utenti con accesso controllabile, quali coloro che hanno lo stesso dominio del computer su cui creare una cartella condivisa, possono accedere alla cartella condivisa.

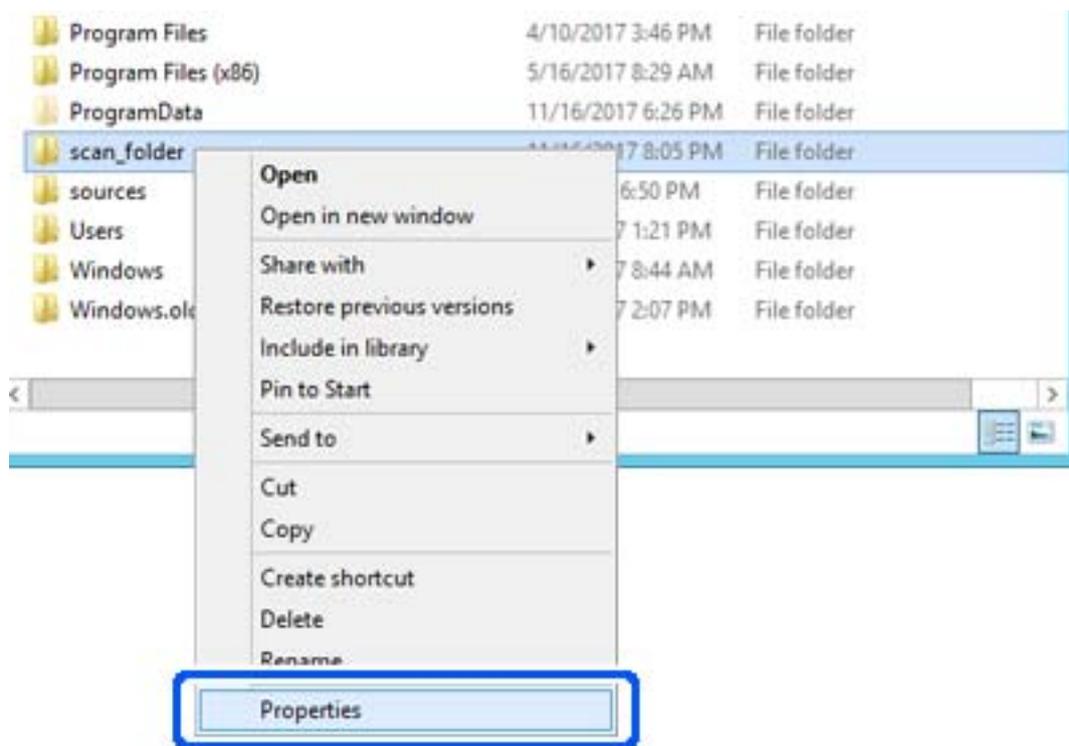
Impostare questa configurazione quando si consente a qualsiasi utente di leggere e scrivere nella cartella condivisa del computer, ad esempio il file server e il computer condiviso.

- Luogo per la creazione della cartella condivisa: radice dell'unità
- Percorso cartella: C:\scan_folder
- Autorizzazione di accesso tramite rete (Permessi di condivisione): tutti
- Autorizzazione di accesso al file system (Sicurezza): utenti autenticati

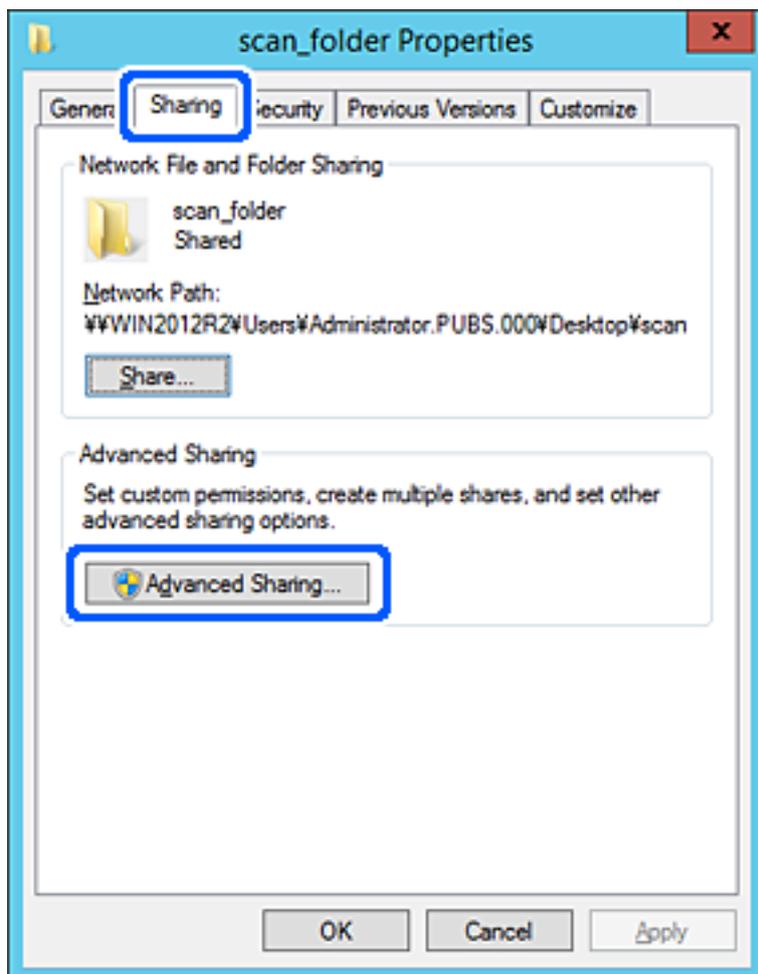
1. Accedere al computer in cui la cartella condivisa verrà creata dall'account utente con autorità di amministratore.
2. Avviare Esplora risorse.
3. Creare la cartella sulla radice dell'unità, quindi denominarla "scan_folder".

Per il nome della cartella, immettere tra 1 e 12 caratteri alfanumerici. Se si supera il limite dei caratteri per il nome della cartella, potrebbe non essere possibile accedervi normalmente a seconda dell'ambiente.

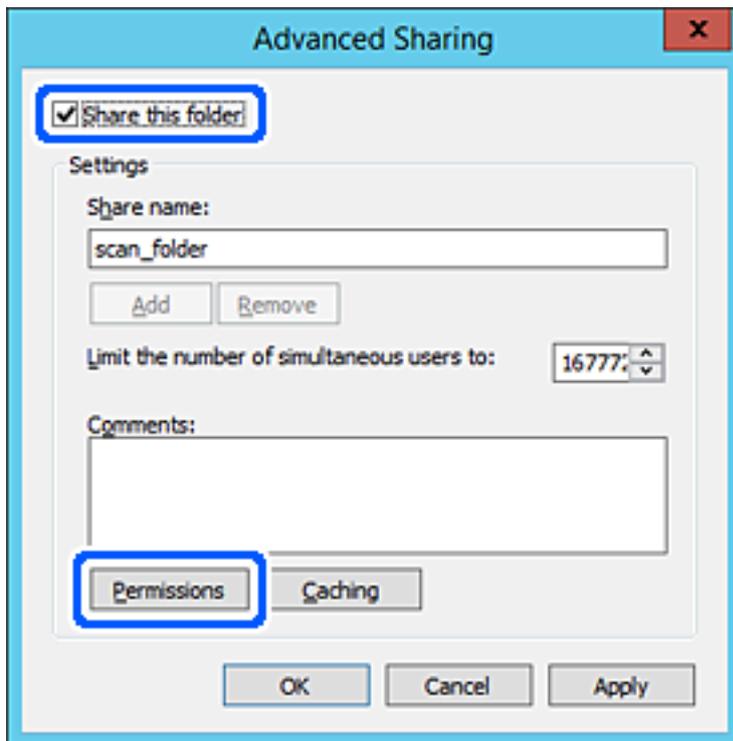
4. Fare clic con il pulsante destro del mouse sulla cartella, quindi selezionare **Proprietà**.



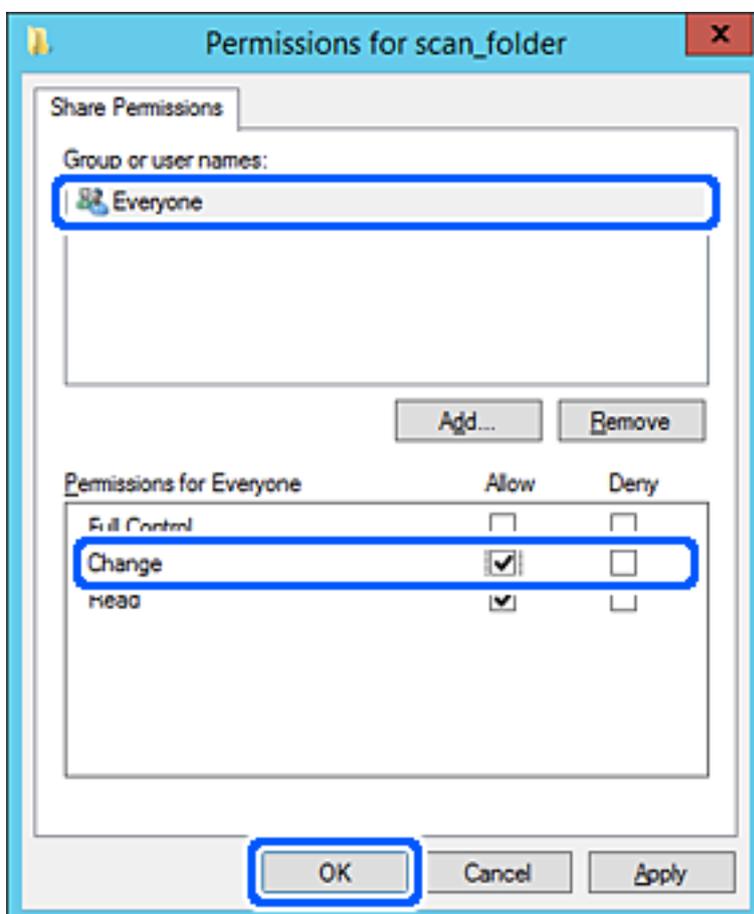
5. Fare clic su **Condivisione avanzata** nella scheda **Condivisione**.



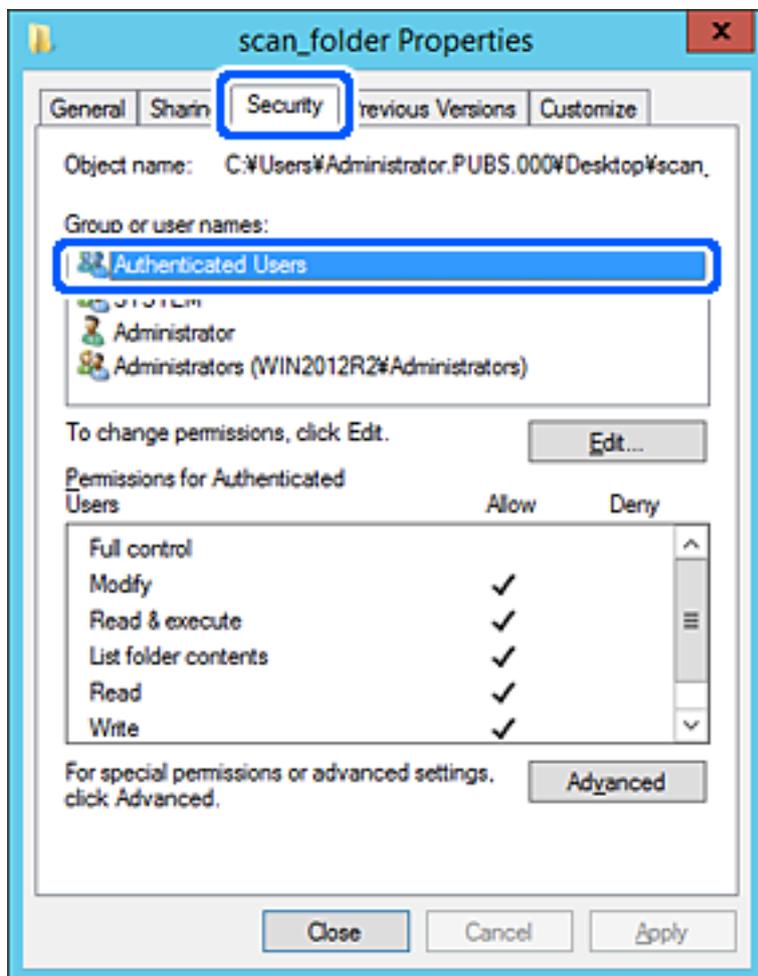
6. Selezionare **Condividi questa cartella** e fare clic su **Autorizzazioni**.



7. Selezionare il gruppo **Tutti** in **Utenti e gruppi**, selezionare **Consenti** in **Modifica** e fare clic su **OK**.



8. Fare clic su **OK**.
9. Selezionare la scheda **Sicurezza**, poi selezionare **Utenti autenticati** in **Utenti e gruppi**.

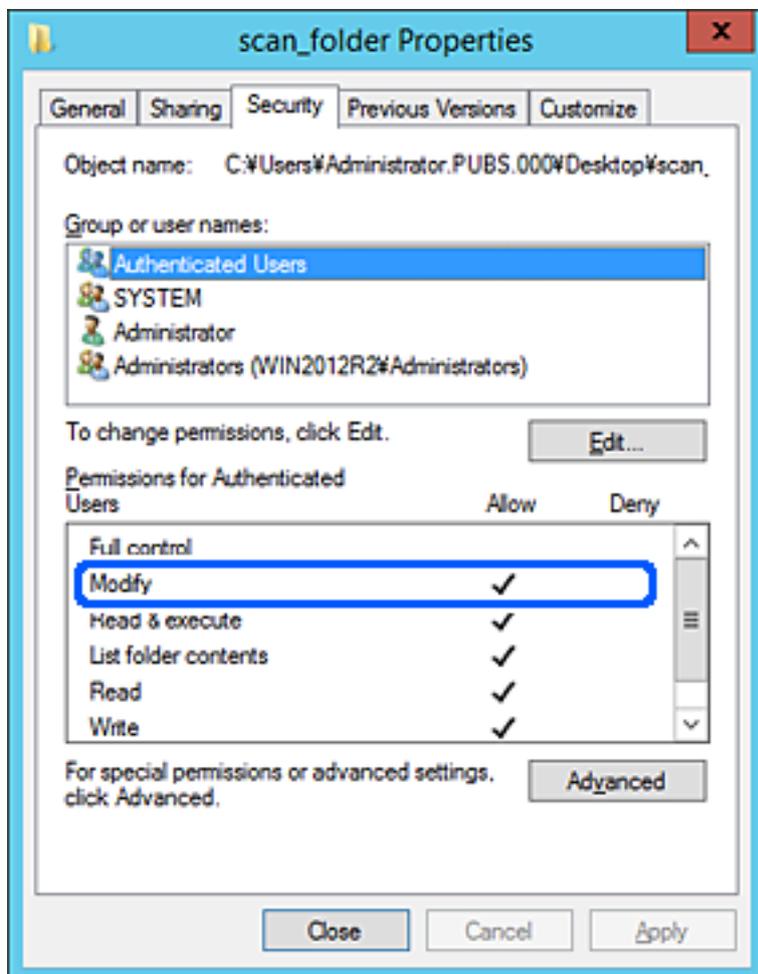


"Utenti autenticati" è il gruppo speciale che comprende tutti gli utenti che possono accedere al dominio o al computer. Il gruppo viene visualizzato solo se la cartella viene creata appena sotto la cartella principale.

Se non appare, è possibile aggiungerle facendo clic su **Modifica**. Per ulteriori informazioni, vedere Informazioni correlate.

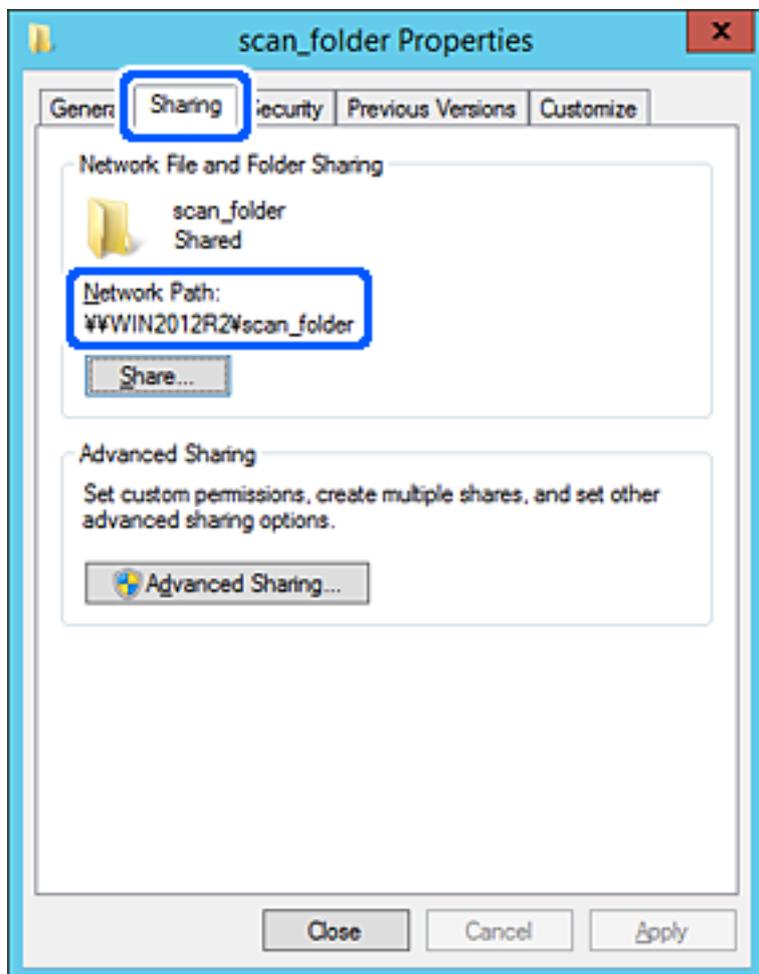
10. Verificare che **Consenti in Modifica** sia selezionato sotto **Autorizzazioni per utenti autenticati**.

Se non è selezionato, selezionare **Utenti autenticati**, fare clic su **Modifica**, selezionare **Consenti in Modifica** sotto **Autorizzazioni per utenti autenticati**, quindi fare clic su **OK**.



11. Selezionare la scheda **Condivisione**.

Il percorso di rete della cartella condivisa viene visualizzato. Esso viene utilizzato quando ci si registra ai contatti dello scanner. È consigliabile prenderne nota.



12. Fare clic su **OK** o **Chiudi** per chiudere la schermata.

Controllare se il file può essere scritto o letto sulla cartella condivisa dai computer dello stesso dominio.

Informazioni correlate

- ➔ [“Aggiunta di un gruppo o di un utente cui consentire l'accesso” a pagina 57](#)
- ➔ [“Registrazione di una destinazione sui Contatti con Web Config” a pagina 62](#)

Esempio di configurazione per un personal computer

Questa spiegazione è un esempio per la creazione della cartella condivisa sul desktop dell'utente che ha attualmente accesso al computer.

L'utente che accede al computer e che dispone di autorità amministrativa può accedere alla cartella desktop e alla cartella dei documenti che si trovano nella cartella Utente.

Impostare questa configurazione quando NON si desidera autorizzare la lettura e la scrittura da parte di un altro utente alla cartella condivisa su un personal computer.

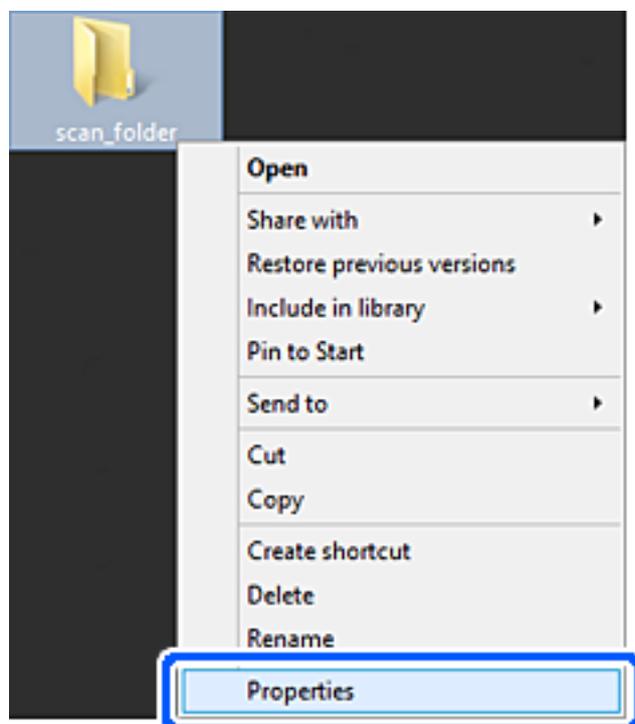
- Luogo per la creazione della cartella condivisa: Desktop

- Percorso cartella: C:\Users\xxxx\Desktop\scan_folder
- Autorizzazione di accesso tramite rete (Permessi di condivisione): tutti
- Autorizzazione di accesso al file system (Sicurezza): togliere o aggiungere nomi utente/gruppo cui consentire l'accesso

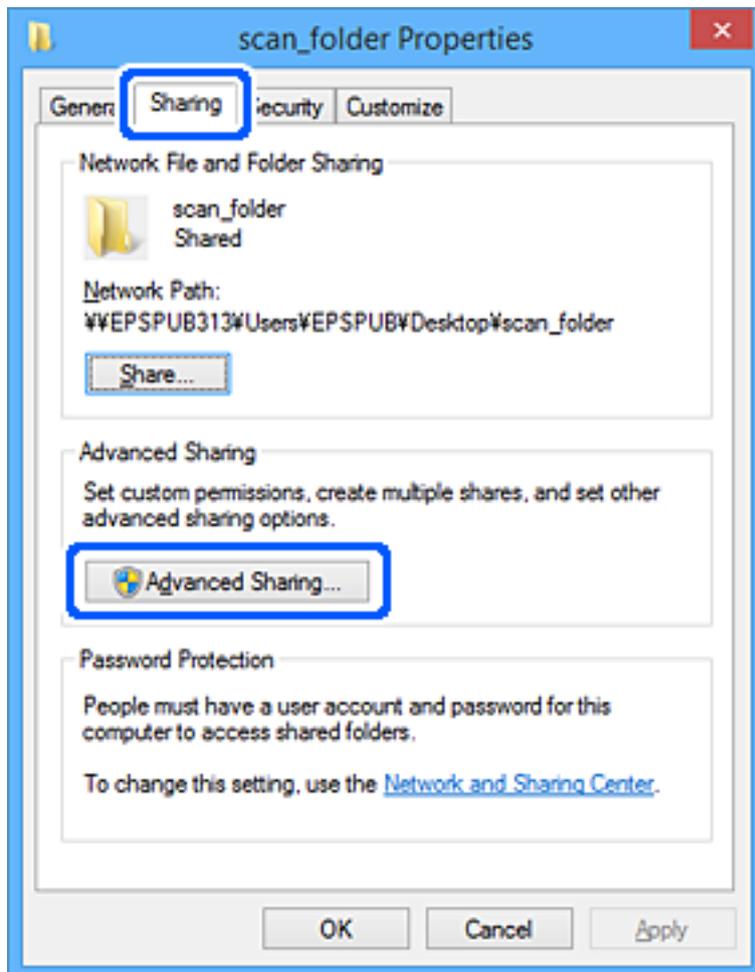
1. Accedere al computer in cui la cartella condivisa verrà creata dall'account utente con autorità di amministratore.
2. Avviare Esplora risorse.
3. Creare la cartella sul desktop quindi denominarla "scan_folder".

Per il nome della cartella, immettere tra 1 e 12 caratteri alfanumerici. Se si supera il limite dei caratteri per il nome della cartella, potrebbe non essere possibile accedervi normalmente a seconda dell'ambiente.

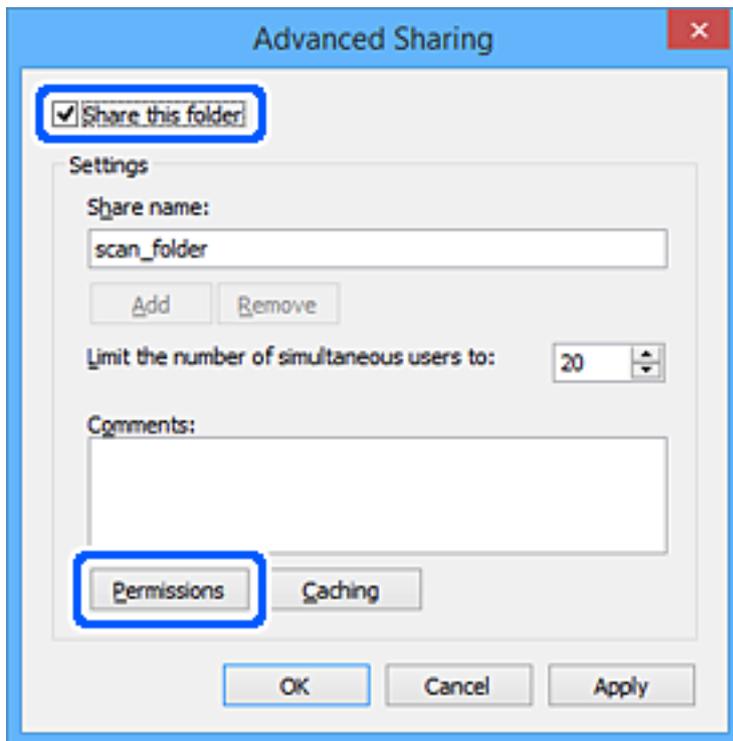
4. Fare clic con il pulsante destro del mouse sulla cartella, quindi selezionare **Proprietà**.



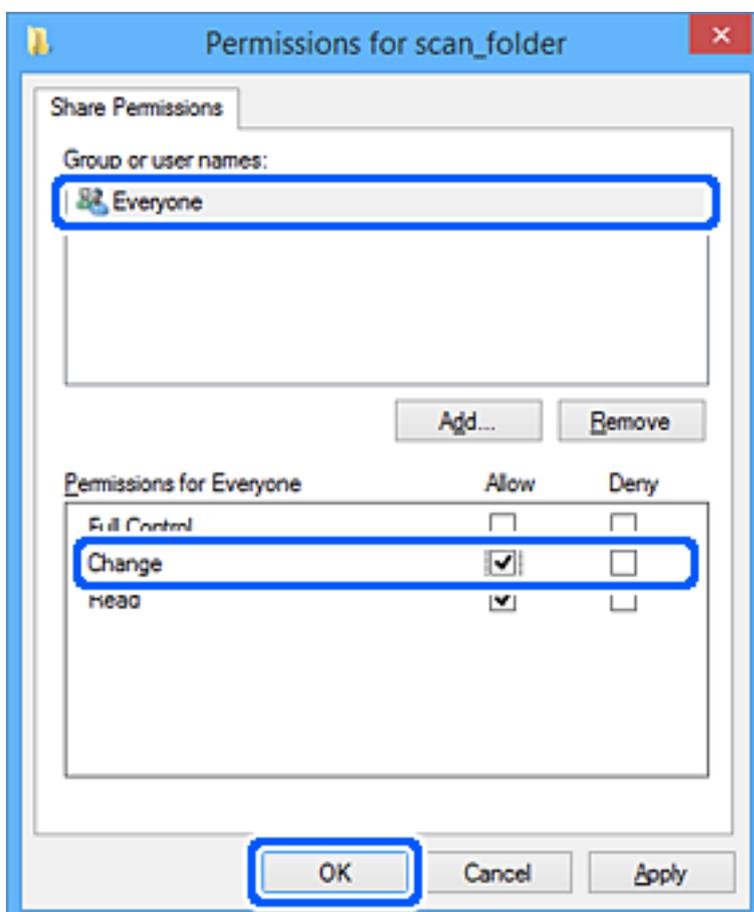
5. Fare clic su **Condivisione avanzata** nella scheda **Condivisione**.



6. Selezionare **Condividi questa cartella** e fare clic su **Autorizzazioni**.



7. Selezionare il gruppo **Tutti** in **Utenti e gruppi**, selezionare **Consenti** in **Modifica** e fare clic su **OK**.

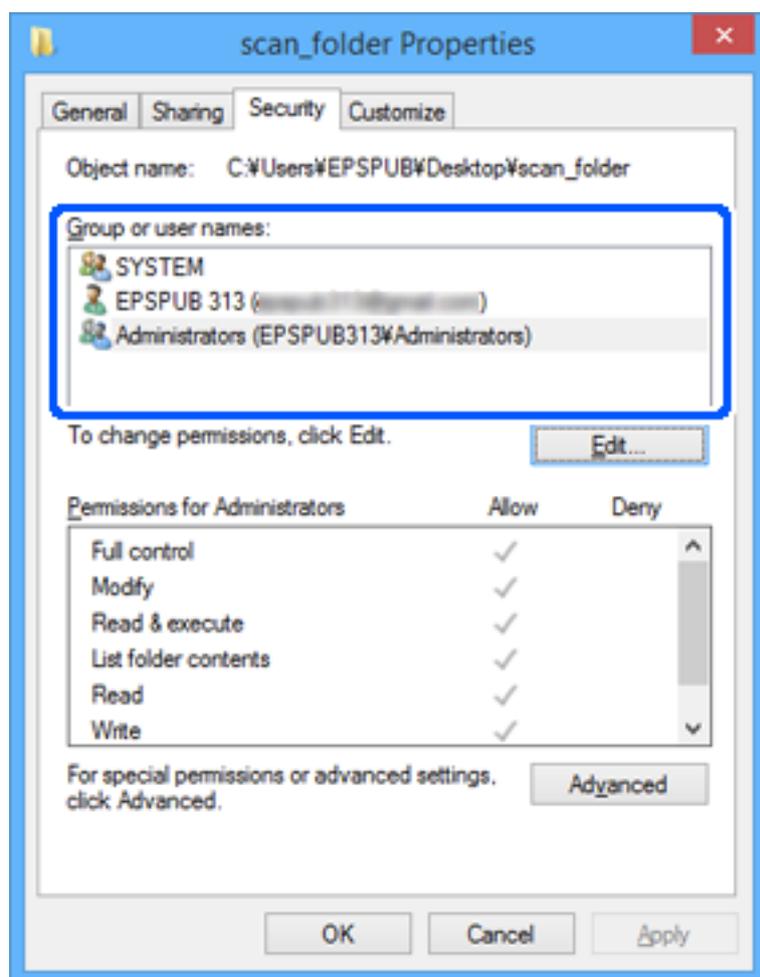


8. Fare clic su **OK**.
9. Selezionare la scheda **Sicurezza**.
10. Selezionare il gruppo o l'utente in **Utenti e gruppi**.

Il gruppo o l'utente visualizzato qui può accedere alla cartella condivisa.

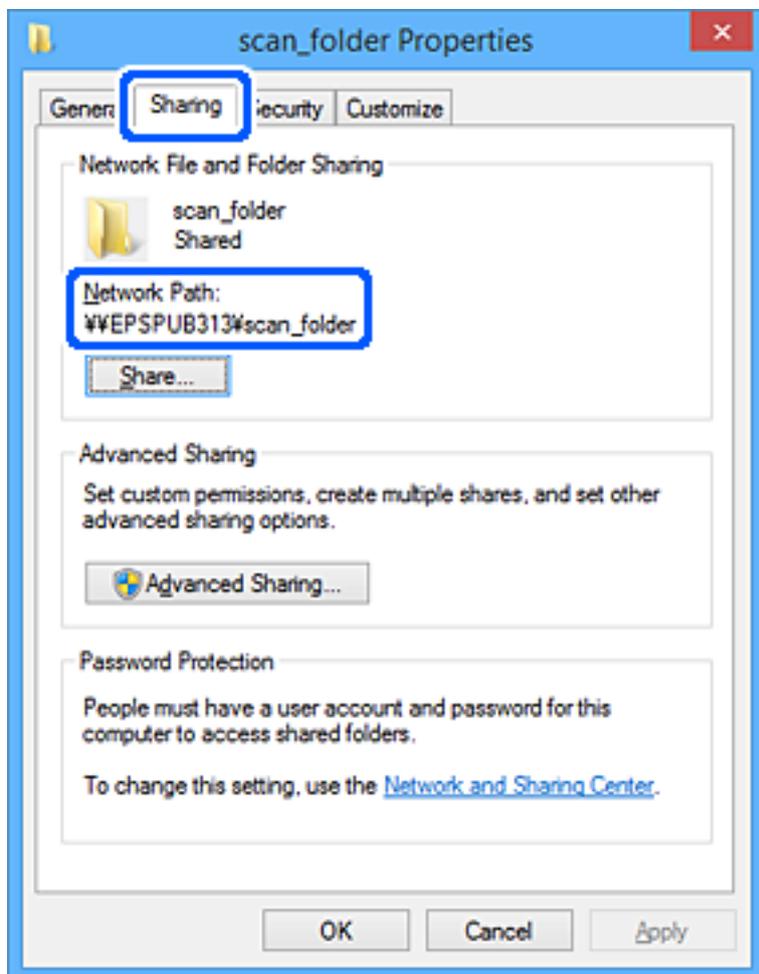
In questo caso, l'utente che accede a questo computer e l'amministratore possono accedere alla cartella condivisa.

Se necessario, aggiungere altre autorizzazioni di accesso. È possibile aggiungerle facendo clic su **Modifica**. Per ulteriori informazioni, vedere Informazioni correlate.



11. Selezionare la scheda **Condivisione**.

Il percorso di rete della cartella condivisa viene visualizzato. Esso viene utilizzato quando ci si registra ai contatti dello scanner. È consigliabile prenderne nota.



12. Fare clic su **OK** o **Chiudi** per chiudere la schermata.

Controllare se il file può essere scritto o letto sulla cartella condivisa dai computer degli utenti o dei gruppi con l'autorizzazione di accesso.

Informazioni correlate

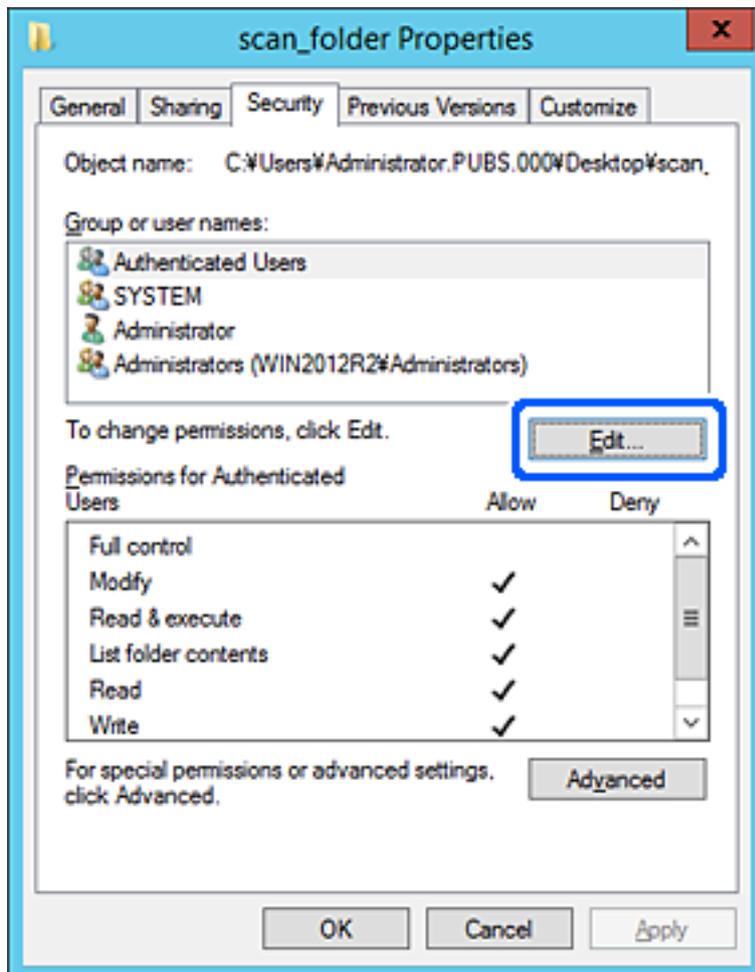
- ➔ “Aggiunta di un gruppo o di un utente cui consentire l'accesso” a pagina 57
- ➔ “Registrazione di una destinazione sui Contatti con Web Config” a pagina 62

Aggiunta di un gruppo o di un utente cui consentire l'accesso

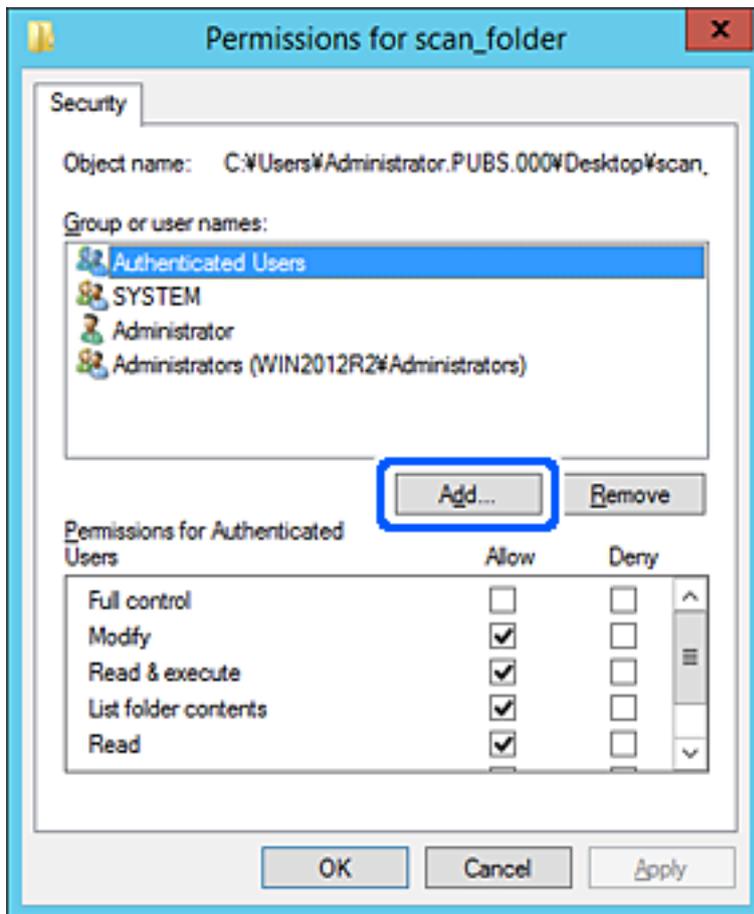
È possibile aggiungere un gruppo o un utente cui consentire l'accesso.

1. Fare clic con il pulsante destro del mouse sulla cartella e selezionare **Proprietà**.
2. Selezionare la scheda **Sicurezza**.

3. Fare clic su **Modifica**.



4. Fare clic su **Aggiungi** sotto **Utenti e gruppi**.



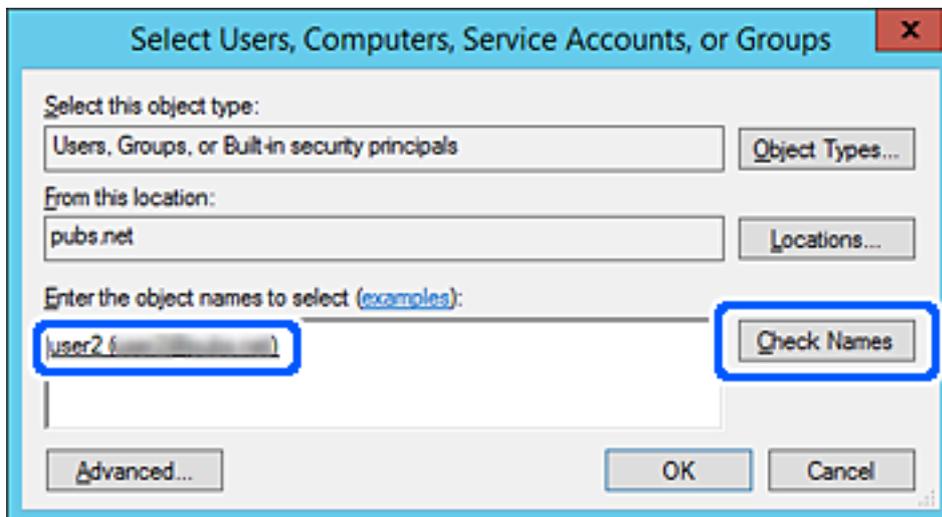
5. Immettere il nome del gruppo o dell'utente cui si desidera consentire l'accesso, quindi fare clic su **Controlla nomi**.

Viene aggiunta una sottolineatura al nome.

Nota:

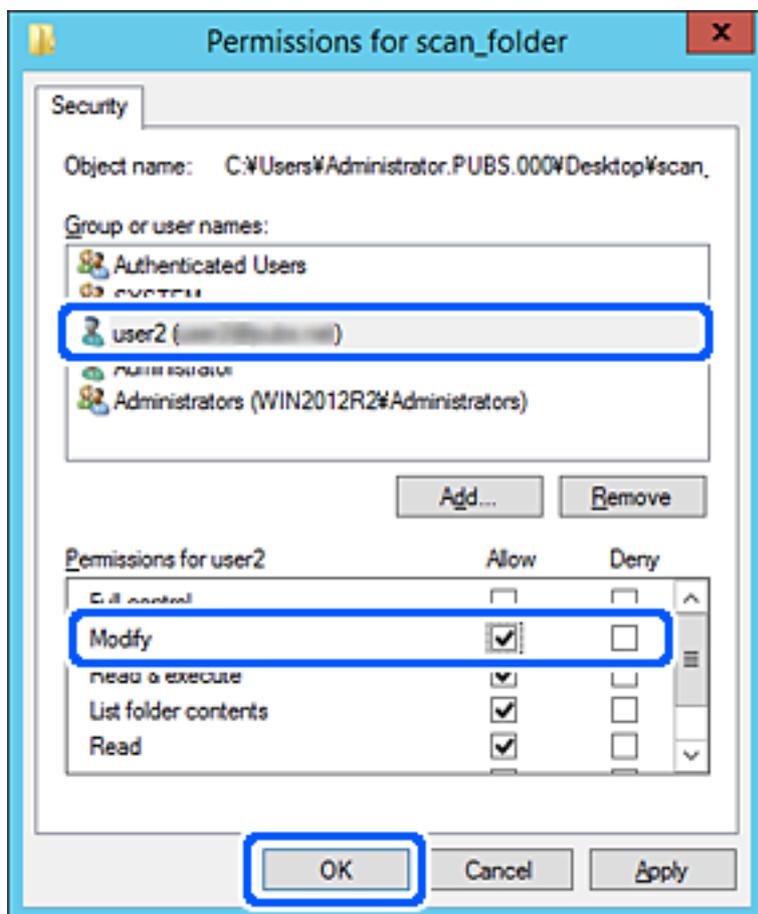
Se non si conosce il nome completo del gruppo o dell'utente, immettere parte del nome e quindi fare clic su **Controlla nomi**. Vengono elencati i nomi dei gruppo o degli utenti che corrispondono a una parte del nome, quindi è possibile selezionare il nome completo dall'elenco.

Se un solo nome corrisponde, il nome completo con sottolineatura viene visualizzato in **Immettere il nome dell'oggetto da selezionare**.



6. Fare clic su OK.

7. Nella scheda Autorizzazioni, selezionare il nome utente inserito in **Utenti e gruppi**, selezionare il permesso di accesso in **Modifica**, quindi fare clic su **OK**.



8. Fare clic su **OK** o **Chiudi** per chiudere la schermata.

Controllare se il file può essere scritto o letto sulla cartella condivisa dai computer degli utenti o dei gruppi con l'autorizzazione di accesso.

Rendere disponibili i contatti

La registrazione delle destinazioni nell'elenco dei contatti dello scanner consente di inserire facilmente la destinazione durante la scansione.

È possibile registrare i seguenti tipi di destinazioni nell'elenco dei contatti. È possibile salvare fino a 300 voci in totale.

Nota:

È inoltre possibile utilizzare il server LDAP (ricerca LDAP) per inserire la destinazione.

E-mail	Destinazione per la posta elettronica. Occorre configurare in anticipo le impostazioni del server di posta.
Cartella di rete	Destinazione per i dati di scansione. È necessario configurare la cartella di rete in anticipo.

Informazioni correlate

➔ [“Cooperazione tra il server LDAP e gli utenti” a pagina 68](#)

Comparazione della configurazione dei contatti

Esistono tre strumenti per la configurazione dei contatti dello scanner: Web Config, Epson Device Admin e il pannello di controllo dello scanner. Le differenze tra i tre strumenti sono elencate nella tabella che segue.

Funzioni	Web Config*	Epson Device Admin	Pannello di controllo dello scanner
Registrazione di una destinazione	✓	✓	✓
Modifica di una destinazione	✓	✓	✓
Aggiunta di un gruppo	✓	✓	✓
Modifica di un gruppo	✓	✓	✓
Eliminazione di destinazione o gruppi	✓	✓	✓
Eliminazione di tutte le destinazioni	✓	✓	-
Importazione di un file	✓	✓	-
Esportazione di un file	✓	✓	-

* Accedere come amministratore per configurare le impostazioni.

Registrazione di una destinazione sui Contatti con Web Config

Nota:

È possibile registrare i contatti anche nel pannello di controllo dello scanner.

1. Accedere a Web Config e selezionare la scheda **Scansione > Contatti**.
2. Selezionare il numero che si desidera registrare e fare clic su **Modifica**.
3. Immettere **Nome** e **Parola indice**.
4. Selezionare il tipo di destinazione come opzione di **Tipo**.

Nota:

Una volta completata la registrazione, non è possibile modificare l'opzione **Tipo**. Se si desidera modificare il tipo, eliminare la destinazione e registrarla nuovamente.

5. Immettere un valore per ciascuna voce, quindi fare clic su **Applica**.

Informazioni correlate

➔ “Esecuzione di Web Config su un browser web” a pagina 36

Voci di impostazione della destinazione

Elementi	Impostazioni e descrizione
Impostazioni comuni	
Nome	Immettere un nome visualizzato nei contatti utilizzando un massimo di 30 caratteri in Unicode (UTF-8). Se non si specifica questa voce, lasciare il campo vuoto.
Parola indice	Immettere un nome utilizzando un massimo di 30 caratteri in Unicode (UTF-8) per cercare tra i contatti sul pannello di controllo dello scanner. Se non si specifica questa voce, lasciare il campo vuoto.
Tipo	Selezionare il tipo di indirizzo che si desidera registrare.
Assegna ad uso frequente	Scegliere di impostare l'indirizzo registrato come indirizzo utilizzato di frequente. L'opzione di uso frequente di un indirizzo viene visualizzata nella schermata superiore della scansione ed è possibile specificare la destinazione senza visualizzare i contatti.
E-mail	
Indirizzo e-mail	Immettere tra 1 e 255 caratteri utilizzando A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Rete cartella (SMB)	
Salva con nome	\\“Percorso cartella” Immettere il percorso della cartella di destinazione utilizzando tra 1 e 253 caratteri in Unicode (UTF-8), omettendo “\\”. Immettere il percorso di rete visualizzato nella schermata delle proprietà della cartella. Vedere quanto segue per maggiori informazioni sull'impostazione del percorso di rete. “Esempio di configurazione per un personal computer” a pagina 52
Nome utente	Immettere un nome utente per accedere a una cartella di rete utilizzando un massimo di 30 caratteri in Unicode (UTF-8). Tuttavia, evitare di utilizzare caratteri di controllo (0x00-0x1F, 0x7F).
Password	Immettere una password per accedere a una cartella di rete utilizzando un massimo di 20 caratteri in Unicode (UTF-8). Tuttavia, evitare di utilizzare caratteri di controllo (0x00-0x1F, 0x7F).
FTP	
Connessione protetta	Selezionare FTP o FTPS a seconda del protocollo di trasferimento file che il server FTP supporta. Selezionare FTPS per consentire allo scanner di comunicare con misure di sicurezza.
Salva con nome	Immettere il nome del server utilizzando tra 1 e 253 caratteri in ASCII (0x20-0x7E), omettendo “ftp://” o “ftps://”.

Elementi	Impostazioni e descrizione
Nome utente	Immettere un nome utente per accedere a un server FTP utilizzando un massimo di 30 caratteri in Unicode (UTF-8). Tuttavia, evitare di utilizzare caratteri di controllo (0x00–0x1F, 0x7F). Se il server consente le connessioni anonime, immettere un nome utente come "Anonimo" e l'FTP. Se non si specifica questa voce, lasciare il campo vuoto.
Password	Immettere una password per accedere a un server FTP utilizzando un massimo di 20 caratteri in Unicode (UTF-8). Tuttavia, evitare di utilizzare caratteri di controllo (0x00–0x1F, 0x7F). Se non si specifica questa voce, lasciare il campo vuoto.
Modalità connessione	Selezionare il metodo di connessione dal menu. Se è stato impostato un firewall tra lo scanner e il server FTP, selezionare Modalità passiva .
Numero porta	Immettere un numero di porta del server FTP tra 1 e 65535.
Convalida certificato	Il certificato del server FTP viene validato quando questa opzione è abilitata. Questa funzione è disponibile quando è selezionato FTPS come Connessione protetta . Per impostare, è necessario importare il Certificato CA sullo scanner.
SharePoint(WebDAV)	
Connessione protetta	Selezionare HTTP o HTTPS a seconda del protocollo di trasferimento file supportato dal server. Selezionare HTTPS per consentire allo scanner di comunicare con misure di sicurezza.
Salva con nome	Immettere il nome del server utilizzando tra 1 e 253 caratteri in ASCII (0x20–0x7E), omettendo "http://" o "https://".
Nome utente	Immettere un nome utente per accedere a un server con un massimo di 30 caratteri in Unicode (UTF-8). Tuttavia, evitare di utilizzare caratteri di controllo (0x00–0x1F, 0x7F). Se non si specifica questa voce, lasciare il campo vuoto.
Password	Immettere una password per accedere a un server con un massimo di 20 caratteri in Unicode (UTF-8). Tuttavia, evitare di utilizzare caratteri di controllo (0x00–0x1F, 0x7F). Se non si specifica questa voce, lasciare il campo vuoto.
Convalida certificato	Il certificato del server viene validato quando questa opzione è abilitata. Questa funzione è disponibile quando è selezionato HTTPS come Connessione protetta . Per impostare, è necessario importare il Certificato CA sullo scanner.
Server proxy	Selezionare se utilizzare o meno un server proxy.

Registrazione di destinazioni come gruppo usando Web Config

Se il tipo di destinazione è impostato su **E-mail**, è possibile registrare le destinazioni come un gruppo.

1. Accedere a Web Config e selezionare la scheda **Scansione > Contatti**.
2. Selezionare il numero che si desidera registrare e fare clic su **Modifica**.
3. Selezionare un gruppo da **Tipo**.
4. Fare clic su **Seleziona per Contatti per Gruppo**.
Vengono visualizzate le destinazioni disponibili.

5. Selezionare la destinazione che si desidera registrare nel gruppo, quindi fare clic su **Seleziona**.
6. Immettere **Nome** e **Parola indice**.
7. Scegliere se identificare il gruppo registrato come gruppo utilizzato di frequente.

Nota:

Le destinazioni possono essere registrate su più gruppi.

8. Fare clic su **Applica**.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Backup e importazione di contatti

Utilizzando Web Config o altri strumenti, è possibile eseguire il backup e l'importazione di contatti.

Per Web Config, è possibile eseguire il backup dei contatti esportando le impostazioni dello scanner che contengono i contatti. Il file esportato non può essere modificato perché viene esportato come file binario.

Quando si importano le impostazioni dello scanner sullo scanner, i contatti vengono sovrascritti.

Per Epson Device Admin, i contatti possono essere esportati solo dalla schermata di proprietà del dispositivo. Inoltre, se non si esportano gli elementi correlati alla sicurezza, è possibile modificare i contatti esportati e importarli poiché tale file può essere salvato come file SYLK o CSV.

Importazione di contatti tramite Web Config

Se si dispone di uno scanner che consente di eseguire il backup dei contatti ed è compatibile con questo scanner, è possibile registrare facilmente i contatti importando il file di backup.

Nota:

Per istruzioni su come eseguire il backup dei contatti dello scanner, vedere il manuale fornito con lo scanner.

Per importare i contatti in questo scanner, procedere come segue.

1. Accedere a Web Config, selezionare la scheda **Gestione dispositivo** > **Esporta e imposta valore di impostazione** > **Importa**.
2. Selezionare il file di backup creato in **File**, inserire la password, quindi fare clic **Avanti**.
3. Selezionare la scheda **Contatti** e fare clic su **Avanti**.

Backup dei contatti tramite Web Config

I dati relativi ai contatti potrebbero andare persi in caso di malfunzionamento dello scanner. Si consiglia pertanto di eseguire un backup quando i dati vengono aggiornati. Anche durante il periodo di garanzia, Epson non può essere ritenuta responsabile della perdita di dati e non è tenuta a eseguire il backup o il recupero di dati e/o impostazioni.

Tramite Web Config, è inoltre possibile effettuare il backup dei dati memorizzati nello scanner sul computer.

1. Accedere a Web Config e selezionare la scheda **Gestione dispositivo** > **Esporta e imposta valore di impostazione** > **Esporta**.
2. Selezionare la casella di controllo **Contatti** nella categoria **Scansione**.
3. Inserire una password per crittografare il file esportato.
È necessaria la password per importare il file. Lasciare il campo vuoto se non si desidera crittografare il file.
4. Fare clic su **Esporta**.

Esportazione e registrazione di massa dei contatti utilizzando lo strumento

Se si usa Epson Device Admin, è possibile eseguire il backup solo dei contatti e modificare i file esportati, quindi registrarli tutti in una volta.

Questa funzione è utile se si desidera eseguire il backup solo dei contatti o quando si sostituisce lo scanner e si desidera trasferire i contatti da quella vecchia a quella nuova.

Esportazione di contatti

Salvare le informazioni dei contatti in un file.

È possibile modificare i file salvati in formato SYLK o in formato csv utilizzando un'applicazione per foglio di calcolo o un editor di testo. È possibile registrarli tutti in una volta dopo aver eliminato o aggiunto qualche informazione.

Le informazioni che includono elementi di sicurezza quali password e informazioni personali possono essere salvate in formato binario con una password. Non è possibile modificare il file. Esso può essere utilizzato come file di backup delle informazioni, comprese le voci di sicurezza.

1. Avviare Epson Device Admin.
2. Selezionare **Stampante** sul menu delle attività della barra laterale.
3. Selezionare dall'elenco il dispositivo che si desidera configurare.
4. Fare clic su **Configurazione periferica** nella scheda **Principale** sul menu a nastro.
Una volta impostata la password dell'amministratore, inserire la password e fare clic su **OK**.
5. Fare clic su **Comune** > **Contatti**.
6. Selezionare il formato di esportazione da **Esporta** > **Esporta elementi**.
 - Tutti gli elementi
Esportare il file binario crittografato. Selezionare se si desidera includere le voci di sicurezza quali password e informazioni personali. Non è possibile modificare il file. Se si seleziona quanto sopra, è necessario impostare una password. Fare clic su **Configurazione** e impostare una password tra 8 e 63 caratteri in ASCII. Tale password sarà necessaria quando si importerà il file binario.

Elementi tranne informazioni di protezione

Esportare i file in formato SYLK o csv. Selezionare se si desidera modificare le informazioni del file esportato.

7. Fare clic su **Esporta**.
8. Specificare il luogo in cui salvare il file, selezionare il tipo di file quindi fare clic su **Salva**.
Viene visualizzato il messaggio di completamento.
9. Fare clic su **OK**.
Controllare che il file sia salvato nel luogo specificato.

Importazione di contatti

Importare le informazioni dei contatti da un file.

È possibile importare i file salvati in formato SYLK o in formato csv, oppure il file binario di backup che include gli elementi di sicurezza.

1. Avviare Epson Device Admin.
2. Selezionare **Stampante** sul menu delle attività della barra laterale.
3. Selezionare dall'elenco il dispositivo che si desidera configurare.
4. Fare clic su **Configurazione periferica** nella scheda **Principale** sul menu a nastro.
Una volta impostata la password dell'amministratore, inserire la password e fare clic su **OK**.
5. Fare clic su **Comune** > **Contatti**.
6. Fare clic su **Sfoggia** in **Importa**.
7. Selezionare il file che si desidera importare, quindi fare clic su **Apri**.
Quando si seleziona il file binario, in **Password** immettere la password impostata all'esportazione del file.
8. Fare clic su **Importa**.
Viene visualizzata la schermata di conferma.
9. Fare clic su **OK**.
Viene visualizzato il risultato di validazione.
 - Modifica le informazioni caricate
Fare clic se si desidera modificare le informazioni singolarmente.
 - Carica più file
Fare clic se si desidera importare più file.

10. Fare clic su **Importa**, quindi fare clic su **OK** sulla schermata di completamento dell'importazione.
Ritornare alla schermata delle proprietà del dispositivo.
11. Fare clic su **Trasmetti**.
12. Fare clic su **OK** sul messaggio di conferma.
Le impostazioni vengono inviate allo scanner.
13. Nella schermata di completamento dell'invio, fare clic su **OK**.
Le informazioni dello scanner vengono aggiornate.
Aprire i contatti da Web Config o dal pannello di controllo dello scanner e verificare siano aggiornati.

Cooperazione tra il server LDAP e gli utenti

Quando si coopera con il server LDAP, è possibile utilizzare le informazioni di indirizzo registrate nel server LDAP come destinazione di una e-mail.

Configurazione del server LDAP

Per utilizzare le informazioni sul server LDAP, registrarlo sullo scanner.

1. Accedere a Web Config e selezionare la scheda **Rete > Server LDAP > Di base**.
2. Inserire un valore per ciascuna voce.
3. Selezionare **OK**.
Vengono visualizzate le impostazioni selezionate.

Voci di impostazione del server LDAP

Elementi	Impostazioni e descrizione
Usa server LDAP	Selezionare Usa o Non utilizzare .
Indirizzo server LDAP	Immettere l'indirizzo del server LDAP. Immettere tra 1 e 255 caratteri in formato IPv4, IPv6 o FQDN. Per il formato FQDN, è possibile utilizzare caratteri alfanumerici in ASCII (0x20-0x7E) e "-"; tranne per l'inizio e la fine dell'indirizzo.
Numero porta server LDAP	Immettere un numero di porta del server LDAP tra 1 e 65535.
Connessione protetta	Specificare il metodo di autenticazione per l'accesso dello scanner al server LDAP.
Convalida certificato	Quando questa voce è abilitata, il certificato del server LDAP viene convalidato. Si consiglia di impostare su Abilita . Per effettuare la configurazione, il Certificato CA deve essere importato sullo scanner.
Timeout di ricerca (sec)	Impostare la lunghezza del tempo di ricerca prima della scadenza tra 5 e 300.

Elementi	Impostazioni e descrizione
Metodo autenticazione	<p>Selezionare uno dei metodi.</p> <p>Se si sceglie Autenticazione Kerberos, selezionare Impostazioni Kerberos per effettuare le impostazioni per Kerberos.</p> <p>Per eseguire Autenticazione Kerberos, è necessario il seguente ambiente.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Lo scanner e il server DNS possono comunicare. <input type="checkbox"/> L'ora dello scanner e quelle del server KDC e del server richiesto per l'autenticazione (server LDAP, server SMTP, file server) vengono sincronizzate. <input type="checkbox"/> Quando il server di servizio viene assegnato come indirizzo IP, l'FQDN del server di servizio viene registrato nella zona di ricerca inversa del server DNS.
Ambiente Kerberos da utilizzare	Se si sceglie Autenticazione Kerberos come Metodo autenticazione , selezionare il dominio Kerberos che si desidera utilizzare.
DN amministratore / Nome utente	Immettere il nome utente del server LDAP con un massimo di 128 caratteri in Unicode (UTF-8). Non è consentito utilizzare i caratteri di controllo, per esempio 0x00–0x1F e 0x7F. Questa impostazione non viene utilizzata quando è selezionato Autenticazione anonima come Metodo autenticazione . Se non si specifica questa voce, lasciare il campo vuoto.
Password	Immettere la password del server di autenticazione LDAP con un massimo di 128 caratteri in Unicode (UTF-8). Non è consentito utilizzare i caratteri di controllo, per esempio 0x00–0x1F e 0x7F. Questa impostazione non viene utilizzata quando è selezionato Autenticazione anonima come Metodo autenticazione . Se non si specifica questa voce, lasciare il campo vuoto.

Impostazioni Kerberos

Selezionando **Autenticazione Kerberos** come **Metodo autenticazione** del **Server LDAP** > **Di base**, effettuare le seguenti impostazioni Kerberos dalla scheda **Rete** > **Impostazioni Kerberos**. È possibile registrare fino a 10 impostazioni Kerberos.

Elementi	Impostazioni e descrizione
Ambiente (dominio)	Immettere il dominio di autenticazione Kerberos con un massimo di 255 caratteri in ASCII (0x20–0x7E). Se non si registra questa voce, lasciare il campo vuoto.
Indirizzo KDC	Immettere l'indirizzo del server di autenticazione Kerberos. Inserire un massimo di 255 caratteri in formato IPv4, IPv6 o FQDN. Se non si registra questa voce, lasciare il campo vuoto.
Numero porta (Kerberos)	Immettere un numero di porta del server Kerberos tra 1 e 65535.

Configurazione delle impostazioni di ricerca del server LDAP

Quando si definiscono le impostazioni di ricerca, è possibile utilizzare l'indirizzo e-mail registrato nel server LDAP.

1. Accedere a Web Config e selezionare la scheda **Rete** > **Server LDAP** > **Imp. di ricerca**.
2. Inserire un valore per ciascuna voce.

- Fare clic su **OK** per visualizzare il risultato dell'impostazione.

Vengono visualizzate le impostazioni selezionate.

Voci delle impostazioni di ricerca del server LDAP

Elementi	Impostazioni e descrizione
Base ricerca (nome distinto)	Se si desidera ricercare un dominio arbitrario, specificare il nome del dominio del server LDAP. Immettere tra 0 e 128 caratteri in Unicode (UTF-8). Se non si effettua la ricerca con un attributo specifico, lasciare il campo vuoto. Esempio di directory del server locale: dc=server,dc=locale
Numero di voci di ricerca	Specificare il numero di voci di ricerca tra 5 e 500. Il numero specificato di voci di ricerca viene salvato e visualizzato temporaneamente. Anche se il numero di voci di ricerca è superiore a quello specificato e appare un messaggio di errore, è possibile completare la ricerca.
Attributo nome utente	Specificare il nome di attributo da visualizzare quando si ricercano i nomi utente. Immettere tra 1 e 255 caratteri in Unicode (UTF-8). Il primo carattere dovrebbe essere a-z o A-Z. Esempio: cn, uid
Attributo visualizzazione nome utente	Specificare il nome di attributo da visualizzare come nome utente. Immettere tra 0 e 255 caratteri in Unicode (UTF-8). Il primo carattere dovrebbe essere a-z o A-Z. Esempio: cn, sn
Attributo indirizzo e-mail	Specificare il nome di attributo da visualizzare quando si ricercano i gli indirizzi e-mail. Immettere una combinazione tra 1 e 255 caratteri utilizzando A-Z, a-z, 0-9 e -. Il primo carattere dovrebbe essere a-z o A-Z. Esempio: e-mail
Attributo arbitrario 1 - Attributo arbitrario 4	È possibile specificare altri attributi arbitrari per la ricerca. Immettere tra 0 e 255 caratteri in Unicode (UTF-8). Il primo carattere deve essere a-z o A-Z. Se non si desidera effettuare la ricerca per attributi specifici, lasciare vuoto. Esempio: o, ou

Verifica della connessione al server LDAP

Esegui il test di connessione al server LDAP utilizzando il parametro impostato in **Server LDAP > Imp. di ricerca**.

- Accedere a Web Config e selezionare la scheda **Rete > Server LDAP > Test di conn.**

- Selezionare **Avvia**.

Il test di connessione viene avviato. Dopo il test, viene visualizzato il report di controllo.

Riferimenti per il test di connessione al server LDAP

Messaggi	Descrizione
Test di connessione riuscito.	Questo messaggio appare quando la connessione con il server avviene correttamente.

Messaggi	Descrizione
Test di conn. non riuscito. Controllare le imp.	Questo messaggio appare per le seguenti ragioni: <ul style="list-style-type: none"> <input type="checkbox"/> L'indirizzo o il numero di porta del server LDAP non è corretto. <input type="checkbox"/> Si è verificata una scadenza. <input type="checkbox"/> Non utilizzare è selezionato come Usa server LDAP. <input type="checkbox"/> Se Autenticazione Kerberos è selezionata come Metodo autenticazione, le impostazioni come Ambiente (dominio), Indirizzo KDC e Numero porta (Kerberos) sono errate.
Test di conn. non riuscito. Verificare la Data e ora sul prodotto o sul server.	Questo messaggio compare quando non è possibile stabilire una connessione a causa della mancata corrispondenza tra le impostazioni di orario dello scanner e del server LDAP.
Autenticazione non riuscita. Controllare le imp.	Questo messaggio appare per le seguenti ragioni: <ul style="list-style-type: none"> <input type="checkbox"/> Nome utente e/o Password sono errati. <input type="checkbox"/> Se Autenticazione Kerberos è selezionata come Metodo autenticazione, la data e l'ora potrebbero non essere configurate.
Impossibile accedere al prodotto fino al termine dell'elaborazione.	Questo messaggio appare quando lo scanner è occupato.

Utilizzo di Document Capture Pro Server

Con Document Capture Pro Server è possibile gestire il metodo di ordinamento, il formato di salvataggio e la destinazione di inoltro di un risultato di scansione eseguito dal pannello di controllo dello scanner. È possibile richiedere ed eseguire un lavoro precedentemente registrato sul server dal pannello di controllo dello scanner.

Installarlo sul computer server.

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

Impostazione della modalità server

Per usare Document Capture Pro Server, effettuare le seguenti impostazioni.

1. Accedere a Web Config e selezionare la scheda **Scansione > Document Capture Pro**.
2. Selezionare **Modalità server** per **Modalità**.
3. Inserire l'indirizzo del server su cui è installato Document Capture Pro Server come **Indirizzo server**.
Immettere tra 2 e 255 caratteri in formato IPv4, IPv6, nome host o FQDN. Per il formato FQDN, è possibile utilizzare caratteri alfanumerici in ASCII (0x20–0x7E) e "-", tranne per l'inizio e la fine dell'indirizzo.
4. Fare clic su **OK**.
Viene effettuato il nuovo collegamento alla rete, quindi le impostazioni vengono abilitate.

Configurazione di AirPrint

Accedere a Web Config, selezionare la scheda **Rete**, quindi selezionare **Configurazione di AirPrint**.

Elementi	Descrizione
Nome servizio Bonjour	Immettere un nome di servizio Bonjour utilizzando testo ASCII (0x20–0x7E) e fino a 41 caratteri.
Ubicazione Bonjour	Immettere una descrizione della posizione dello scanner utilizzando testo Unicode (UTF-8) e fino a 127 byte.
Wide-Area Bonjour	Impostare se utilizzare o meno Wide-Area Bonjour. In caso di utilizzo, lo scanner deve essere registrato sul server DNS per essere in grado di cercare lo scanner sul segmento.
Abilita AirPrint	Bonjour e AirPrint (servizio di scansione) vengono abilitati.

Problemi durante la preparazione della scansione in rete

Suggerimenti per risolvere i problemi

Verifica del messaggio di errore

Quando si verifica un problema, verificare innanzitutto se ci sono messaggi sul pannello di controllo o nella schermata del driver dello scanner. Se si è impostata la notifica per e-mail quando si verificano gli eventi, è possibile apprendere tempestivamente lo stato.

Verifica dello stato della comunicazione

Controllare lo stato di comunicazione del computer server o del computer client utilizzando il comando ping e ipconfig.

Test di connessione

Per verificare la connessione tra lo scanner e il server e-mail, utilizzare il test di connessione dello scanner. Inoltre, controllare la connessione dal computer client al server per verificare lo stato della comunicazione.

Inizializzazione delle impostazioni

Se le impostazioni e lo stato della comunicazione non mostrano alcun problema, i problemi possono essere risolti disattivando o inizializzando le impostazioni di rete dello scanner e impostandole di nuovo.

Impossibile accedere a Web Config

■ L'indirizzo IP non è assegnato allo scanner.

Soluzioni

Nessun indirizzo IP valido è assegnato allo scanner. Configurare l'indirizzo IP utilizzando il pannello di controllo dello scanner. È possibile verificare le informazioni di impostazione dal pannello di controllo dello scanner.

■ Il browser web non supporta il livello di crittografia per SSL/TLS.

Soluzioni

SSL/TLS è dotato di Livello di crittografia. È possibile aprire Web Config utilizzando un browser web che supporta crittografie di massa come indicato di seguito. Verificare che il browser in uso sia supportato.

- 80 bit: AES256/AES128/3DES
- 112 bit: AES256/AES128/3DES
- 128 bit: AES256/AES128
- 192 bit: AES256
- 256 bit: AES256

■ Il Certificato firma CA è scaduto.

Soluzioni

Se esiste un problema con la data di scadenza del certificato, quando ci si connette a Web Config con comunicazione SSL/TLS (https), viene visualizzato "Il certificato è scaduto". Se il messaggio appare prima della data di scadenza, assicurarsi che la data dello scanner sia configurata correttamente.

■ Il nome comune del certificato e dello scanner non corrispondono.

Soluzioni

Se il nome comune del certificato e dello scanner non corrispondono, viene visualizzato il messaggio "Il nome del certificato di sicurezza non corrisponde" quando si accede a Web Config utilizzando la comunicazione SSL/TLS (https). Ciò accade perché i seguenti indirizzi IP non corrispondono.

- L'indirizzo IP dello scanner inserito nel nome comune per la creazione di un Certificato firma personale o CSR
- L'indirizzo IP immesso nel browser web durante l'esecuzione di Web Config

Per Certificato firma personale, aggiornare il certificato.

Per il Certificato firma CA, procurarsi nuovamente il certificato per lo scanner.

■ L'impostazione del server proxy dell'indirizzo locale non è impostata sul browser web.

Soluzioni

Quando lo scanner è impostato per utilizzare un server proxy, configurare il browser web affinché non si connetta all'indirizzo locale tramite il server proxy.

- 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 LAN (indirizzi locali).

- Mac OS:

Selezionare **Preferenze di Sistema > Network > Avanzate > Proxy**, quindi salvare 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

■ DHCP è disabilitato nelle impostazioni del computer.

Soluzioni

Se il DHCP per l'ottenimento automatico di un indirizzo IP è disabilitato sul computer, non è possibile accedere a Web Config. Abilitare DHCP.

Esempio per Windows 10:

aprire il pannello di controllo e fare clic su **Rete e Internet** > **Centro connessioni di rete e condivisione** > **Modifica impostazioni scheda**. Aprire la schermata delle proprietà della connessione in uso e aprire la schermata delle proprietà di **Protocollo Internet versione 4 (TCP/IPv4)** o **Protocollo Internet versione 6 (TCP/IPv6)**. Verificare che **Ottieni automaticamente un indirizzo IP** sia selezionato nella schermata visualizzata.

Personalizzazione del display del pannello di controllo

Registrazione di Preimpostaz. 76

Modifica della schermata iniziale del pannello di controllo. 78

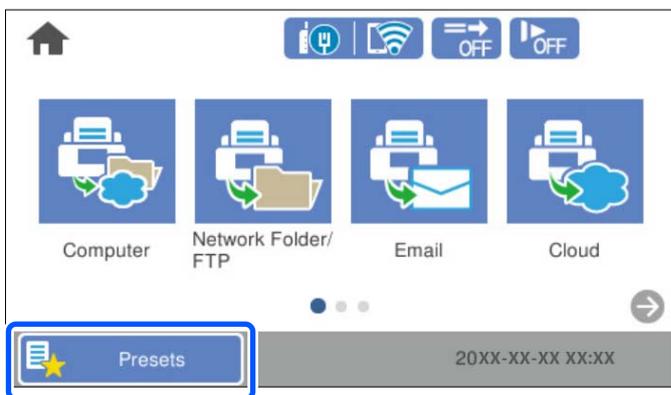
Registrazione di Preimpostaz.

È possibile registrare le impostazioni di scansione utilizzate di frequente come **Preimpostaz.** È possibile registrare fino a 48 predefiniti.

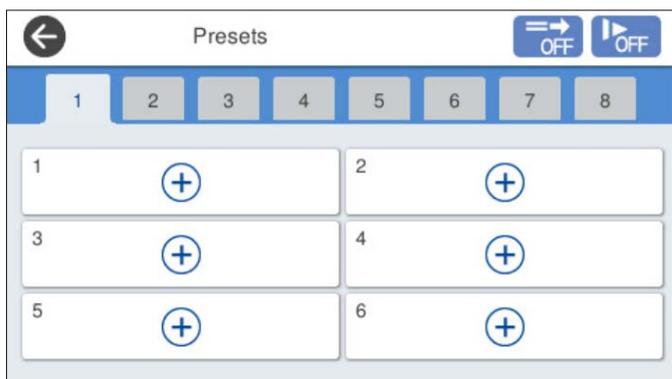
Nota:

- ❑ È possibile registrare le impostazioni correnti selezionando  nella schermata di avvio della scansione.
- ❑ È anche possibile registrare i **Preimpost.** in Web Config.
Selezionare la scheda **Scansione > Preimpost.**
- ❑ Se si seleziona **Scansione su computer** durante la registrazione, è possibile registrare il lavoro creato in Document Capture Pro come **Preimpost.** Questa funzione è disponibile solo per i computer connessi a una rete. Registrare il lavoro in Document Capture Pro in anticipo.
- ❑ Se la funzione di autenticazione è abilitata, solo l'amministratore può registrare i **Preimpost.**

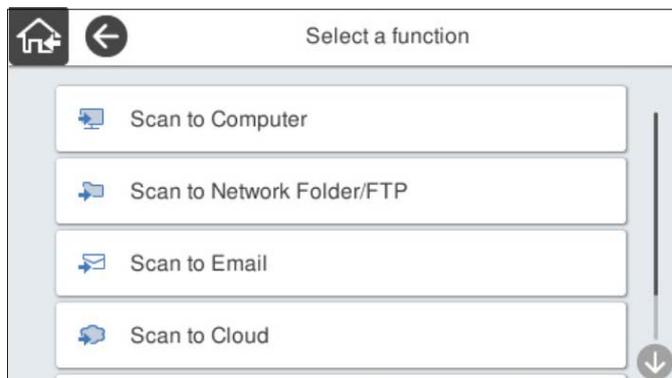
1. Selezionare **Preimpostaz.** nella schermata iniziale del pannello di controllo dello scanner.



2. Selezionare .



3. Selezionare il menu che si desidera utilizzare per registrare un predefinito.



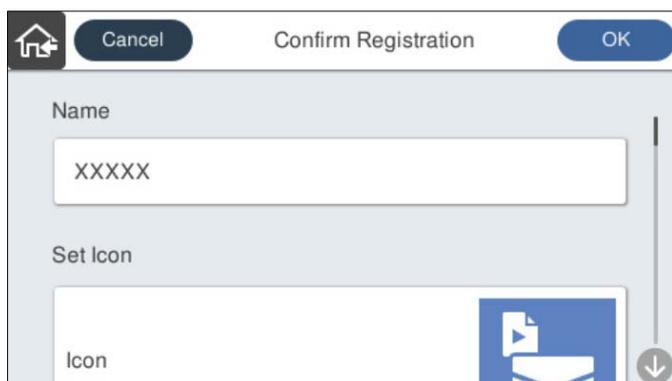
4. Impostare ciascuna voce, quindi selezionare .

Nota:

Quando si seleziona **Scansione su computer**, selezionare il computer su cui è installato Document Capture Pro, quindi selezionare un lavoro registrato. Questa funzione è disponibile solo per i computer connessi a una rete.

5. Configurare le impostazioni predefinite.

- Nome:** impostare il nome.
- Imposta Icona:** impostare l'immagine e il colore dell'icona da visualizzare.
- Impostazione Invio rapido:** consente di avviare immediatamente la scansione senza chiedere conferma quando si seleziona il predefinito.
Quando si utilizza Document Capture Pro Server, anche se si imposta il software affinché richieda di verificare i contenuti di un lavoro prima della scansione, **Impostazione Invio rapido** nei predefiniti dello scanner ha la priorità rispetto al software.
- Contenuti:** verificare le impostazioni di scansione.



6. Selezionare OK.

Opzioni del menu Preimpostaz.

È possibile modificare le impostazioni di un predefinito selezionando  in ogni predefinito.

Modifica nome:

consente di modificare il nome del predefinito.

Modifica Icona:

consente di modificare l'immagine dell'icona e il colore del predefinito.

Impostazione Invio rapido:

consente di avviare immediatamente la scansione senza chiedere conferma quando si seleziona il predefinito.

Modifica posizione:

consente di modificare l'ordine di visualizzazione dei predefiniti.

Elimina:

elimina il predefinito.

Aggiungi o rimuovi Icona su Home:

consente di aggiungere o eliminare l'icona del predefinito dalla schermata iniziale.

Conferma Dettagli:

visualizza le impostazioni di un predefinito. È possibile caricare il predefinito selezionando **Usa questa impostazione**.

Modifica della schermata iniziale del pannello di controllo

È possibile personalizzare la schermata iniziale selezionando **Impostazioni > Modifica schermata principale** sul pannello di controllo dello scanner.

- Disposizione:** consente di modificare il metodo di visualizzazione delle icone del menu.
“[Modifica del Disposizione della schermata iniziale](#)” a pagina 79
- Aggiungi icona:** consente di aggiungere icone alle impostazioni dei **Preimpostaz.** effettuate o di ripristinare le icone rimosse dalla schermata.
“[Aggiungi icona](#)” a pagina 79
- Rimuovi icona:** rimuove le icone dalla schermata iniziale.
“[Rimuovi icona](#)” a pagina 80
- Sposta icona:** consente di modificare l'ordine di visualizzazione delle icone.
“[Sposta icona](#)” a pagina 81
- Ripristina visualiz. icona predefinita:** ripristina le impostazioni di visualizzazione predefinite per la schermata iniziale.
- Sfondo:** consente di modificare il colore di sfondo della schermata iniziale.

Modifica del Disposizione della schermata iniziale

1. Selezionare **Impostazioni > Modifica schermata principale > Disposizione** sul pannello di controllo dello scanner.
2. Selezionare **Linea** o **Matrice**.

Linea:



Matrice:

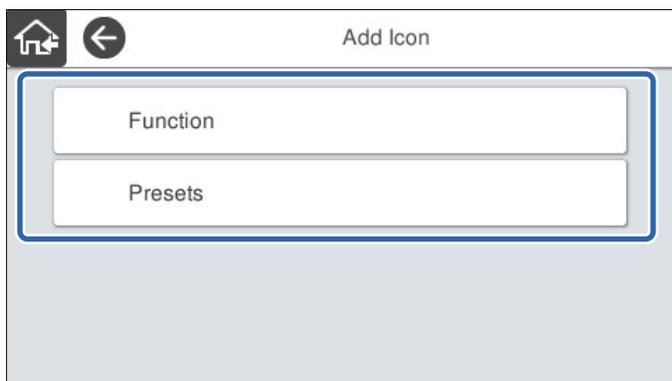


3. Selezionare  per tornare alla schermata iniziale e verificare le voci.

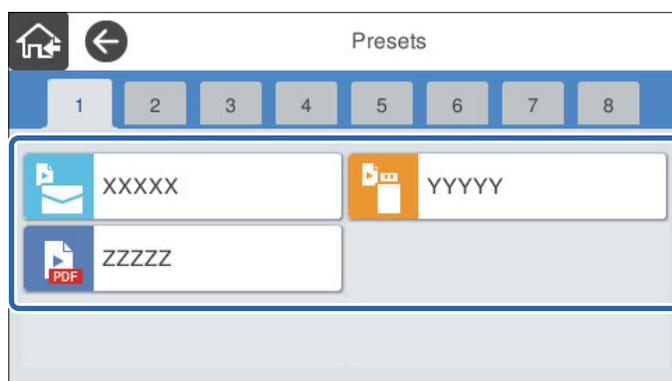
Aggiungi icona

1. Selezionare **Impostazioni > Modifica schermata principale > Aggiungi icona** sul pannello di controllo dello scanner.
2. Selezionare **Funzione** o **Preimpostaz..**
 - Funzione:** visualizza le funzioni predefinite visualizzate nella schermata iniziale.

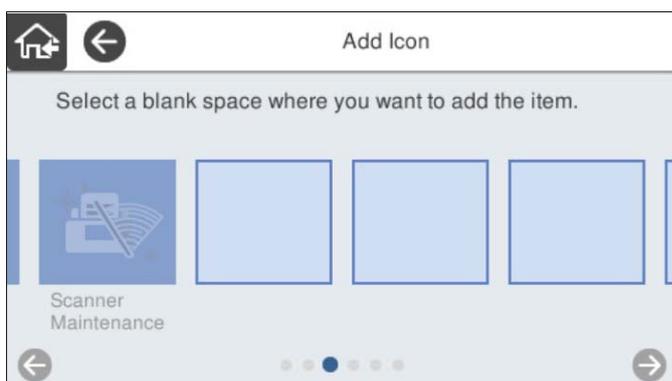
- ❑ Preimpostaz.: visualizza i predefiniti registrati.



3. Selezionare la voce che si desidera aggiungere alla schermata iniziale.



4. Selezionare lo spazio vuoto dove aggiungere la voce.
Se si desidera aggiungere più icone, ripetere i passaggi da 3 a 4.

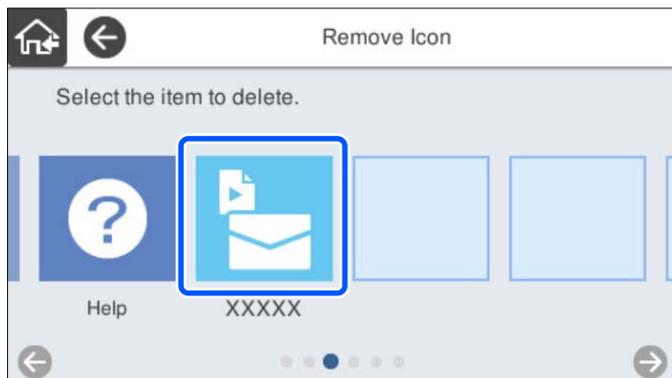


5. Selezionare  per tornare alla schermata iniziale e verificare le voci.

Rimuovi icona

1. Selezionare **Impostazioni** > **Modifica schermata principale** > **Rimuovi icona** sul pannello di controllo dello scanner.

2. Selezionare l'icona da rimuovere.

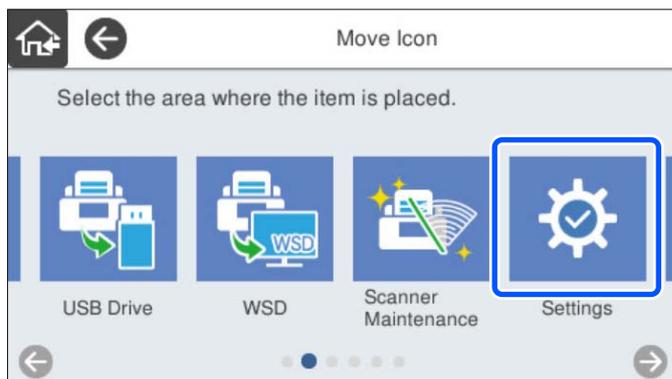


3. Selezionare **Sì** per finire.
Se si desidera rimuovere più icone, ripetere i passaggi da 2 a 3.

4. Selezionare  per tornare alla schermata iniziale e verificare le voci.

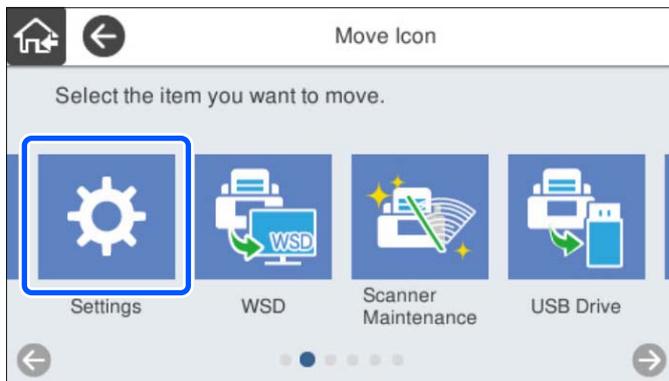
Sposta icona

1. Selezionare **Impostazioni** > **Modifica schermata principale** > **Sposta icona** sul pannello di controllo dello scanner.
2. Selezionare l'icona che si desidera spostare.



3. Selezionare il riquadro di destinazione.

Se nel riquadro di destinazione è già stata impostata un'altra icona, questa verrà sostituita.



4. Selezionare  per tornare alla schermata iniziale e verificare le voci.

Impostazioni di sicurezza di base

Introduzione delle funzioni di sicurezza del prodotto.	84
Impostazioni di amministrazione.	84
Disattivazione dell'interfaccia esterna.	90
Monitoraggio di uno scanner remoto.	91
Soluzione dei problemi.	92

Introduzione delle funzioni di sicurezza del prodotto

Questa sezione illustra le funzioni di sicurezza dei dispositivi Epson.

Nome della funzione	Tipo di funzione	Cosa impostare	Cosa evitare
Configurazione della password di amministratore	Blocca le impostazioni di sistema, tra cui la configurazione della connessione di rete o USB.	Un amministratore imposta una password per il dispositivo. È possibile impostare o modificare sia da Web Config che dal pannello di controllo dello scanner.	Impedire la lettura e la modifica illegali delle informazioni memorizzate sul dispositivo, come ID, password, impostazioni di rete e così via. 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.
Configurazione per interfaccia esterna	Controlla l'interfaccia che si collega al dispositivo.	Attivare o disattivare la connessione USB con il computer.	Connessione USB del computer: impedisce l'utilizzo non autorizzato del dispositivo vietando di effettuare la scansione senza un collegamento alla rete.

Informazioni correlate

- ➔ [“Configurazione della password di amministratore” a pagina 84](#)
- ➔ [“Disattivazione dell'interfaccia esterna” a pagina 90](#)

Impostazioni di amministrazione

Configurazione della password di amministratore

Impostando la password dell'amministratore, è possibile impedire agli utenti di modificare le impostazioni di gestione del sistema. I valori predefiniti vengono impostati al momento dell'acquisto. Modificarli come desiderato.

Nota:

Di seguito sono elencati i valori predefiniti per le informazioni amministratore.

- Nome utente (utilizzato solo per Web Config): nessuno (vuoto)
- Password: numero di serie dello scanner

Per trovare il numero di serie, verificare l'etichetta sul retro dello scanner.

È possibile modificare la password di amministratore utilizzando Web Config, il pannello di controllo dello scanner o Epson Device Admin. Quando si utilizza Epson Device Admin, consultare la guida o l'aiuto di Epson Device Admin.

Modifica della password di amministratore tramite Web Config

Modificare la password di amministratore in Web Config.

1. Accedere a Web Config e selezionare la scheda **Sicurezza prodotto** > **Cambia password amministratore**.
2. Inserire le informazioni necessarie in **Password corrente**, **Nome utente**, **Nuova password** e **Conferma nuova password**.

Inserire almeno un carattere per la nuova password.

Nota:

Di seguito sono elencati i valori predefiniti per le informazioni amministratore.

- Nome utente: nessuno (vuoto)*
- Password: numero di serie dello scanner*

Per trovare il numero di serie, verificare l'etichetta sul retro dello scanner.



Importante:

Assicurarsi di ricordare la password dell'amministratore impostata. Se si dimentica la password, non sarà possibile reimpostarla e sarà necessario richiedere assistenza al personale addetto.

3. Selezionare **OK**.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web”](#) a pagina 36

Modifica della password di amministratore dal pannello di controllo

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

1. Selezionare **Impostazioni** sul pannello di controllo dello scanner.
2. Selezionare **Amministrazione sistema** > **Impostazioni amministratore**.
3. Selezionare **Password amministratore** > **Modifica**.

4. Immettere la password corrente.

Nota:

La password di amministratore impostata al momento dell'acquisto (valore predefinito) è il numero di serie dello scanner.

Per trovare il numero di serie, verificare l'etichetta sul retro dello scanner.

5. Immettere la nuova password.

Inserire almeno un carattere.



Importante:

Assicurarsi di ricordare la password dell'amministratore impostata. Se si dimentica la password, non sarà possibile reimpostarla e sarà necessario richiedere assistenza al personale addetto.

6. Immettere nuovamente la nuova password per confermare.

Viene visualizzato un messaggio di completamento.

Utilizzo di Impostazione blocco per il pannello di controllo

È possibile utilizzare Impostazione blocco per bloccare il pannello di controllo e impedire agli utenti di modificare le voci relative alle impostazioni di sistema.

Nota:

Se si abilita Impostazioni di autenticazione sullo scanner, Impostazione blocco è abilitato anche per il pannello di controllo. Il pannello di controllo non può essere sbloccato quando Impostazioni di autenticazione è abilitato.

Anche se si disabilita Impostazioni di autenticazione, Impostazione blocco rimane abilitato. Per disabilitarlo è possibile configurare le impostazioni dal pannello di controllo o da Web Config.

Impostare Impostazione blocco dal pannello di controllo

1. Per disabilitare **Impostazione blocco** una volta abilitata, toccare  nell'angolo in alto a destra della schermata Home per accedere come amministratore.



non viene visualizzato quando **Impostazione blocco** è disabilitato. Se si desidera abilitare questa impostazione, passare alla fase successiva.

2. Selezionare **Impostazioni**.
3. Selezionare **Amministrazione sistema > Impostazioni amministratore**.
4. Selezionare **Attiva** o **Dis.** come **Impostazione blocco**.

Impostare Impostazione blocco da Web Config

1. Selezionare la scheda **Gestione dispositivo > Pannello di controllo**.
2. Selezionare **ATTIVA** o **DISATTIVA** per **Blocco pannello**.
3. Fare clic su **OK**.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Voci relative a Impostazione blocco nel menu Impostazioni

Questo è un elenco delle voci che vengono bloccate nel menu **Impostazioni** del pannello di controllo con Impostazione blocco.

✓: da bloccare.

- : da non bloccare.

Menu Impostazioni		Impostazione blocco
Impostazioni base		-
	Luminosità LCD	-
	Suoni	-
	Timer sospens.	✓
	Timer spegnimento	✓
	Impostazioni data/ora	✓
	Lingua/Language	✓/-*
	Tastiera (Questa funzione potrebbe non essere disponibile in alcune aree geografiche)	-
	Time out operazione	✓
	Connessione PC tramite USB	✓
	Alimentazione diretta	✓
Impost. scansione		-
	Lento	-
	Tempo di arresto doppia aliment.	✓
	Funzione DFDS	-
	Protezione carta	✓
	Rilevamento sporcizia del vetro	✓
	Rilevam. doppia alim. a ultrasuoni	✓
	Timeout Modo Alimentazione automatica	✓
	Conferma destinatario	✓
Modifica schermata principale		✓
	Disposizione	✓
	Aggiungi icona	✓
	Rimuovi icona	✓
	Sposta icona	✓
	Ripristina visualiz. icona predefinita	✓
	Sfondo	✓
Impostazioni utente		✓

Menu Impostazioni		Impostazione blocco
	Cartella rete/FTP	✓
	E-mail	✓
	Cloud	✓
	Unità USB	✓
Impostazioni di rete		✓
	Configurazione Wi-Fi	✓
	Configurazione LAN cablata	✓
	Stato rete	✓
	Avanzate	✓
Impostazioni servizio web		✓
	Servizi Epson Connect	✓
Document Capture Pro		-
	Modifica impostazioni	✓
Gestione Contatti		-
	Registra/Elimina	✓/-*
	Frequente	-
	Visualizza opzioni	-
	Ricerca opzioni	-
Amministrazione sistema		✓
	Gestione Contatti	✓
	Impostazioni amministratore	✓
	Limiti	✓
	Crittografia password	✓
	Ricerca clienti	✓
	Impostazioni WSD	✓
	Ripristina impostaz. predef.	✓
	Aggiornamento firmware	✓
Informazioni dispositivo		-

Menu Impostazioni		Impostazione blocco
	Numero seriale	-
	Versione corrente	-
	Numero totale di scansioni	-
	Numero di scansioni su fronte	-
	Num. scansioni fronte-retro	-
	N. di scansioni del Foglio supporto	-
	Numero di scansioni dopo sostituzione rulli	-
	Numero di scansioni dopo pulizia regolare	-
	Ripristinare il numero di scansioni	✓
Manutenzione scanner		-
	Pulizia del rullo	-
	Sostituzione rulli	-
	Ripristinare il numero di scansioni	✓
	Come sostituire	-
	Pulizia regolare	-
	Ripristinare il numero di scansioni	✓
	Come pulire	-
	Pulizia del vetro	-
Impostazione dell'avviso sostituzione rullo		✓
	Conta impost. Allarme	✓
Impostazioni avviso pulizia regolare		✓
	Impostazione di avvertenza	✓
	Conta impost. Allarme	✓

* È possibile specificare se consentire o meno modifiche in **Amministrazione sistema > Limiti**.

Effettuare l'accesso come amministratore dal pannello di controllo

È possibile utilizzare uno dei seguenti metodi per accedere come amministratore dal pannello di controllo dello scanner.

1. Toccare  in alto a destra dello schermo.
 - Quando Impostazioni di autenticazione è abilitato, l'icona viene visualizzata sulla schermata **Benvenuto** (la schermata di standby dell'autenticazione).

Quando Impostazioni di autenticazione è disabilitato, l'icona è visualizzata nella schermata Home.

2. Toccare **Sì** quando compare la schermata di conferma.

3. Immettere la password di amministratore.

Viene visualizzato un messaggio di accesso completato, quindi sul pannello di controllo compare la schermata iniziale.

Per uscire, toccare  in alto a destra della schermata Home.

Disattivazione dell'interfaccia esterna

È possibile disattivare l'interfaccia utilizzata per collegare il dispositivo allo scanner. Effettuare le impostazioni di restrizione per limitare la scansione in modalità diverse dalla connessione alla rete.

Nota:

È possibile effettuare le impostazioni di restrizione anche nel pannello di controllo dello scanner.

Connessione PC tramite USB: **Impostazioni > Impostazioni base > Connessione PC tramite USB**

1. Accedere a Web Config e selezionare la scheda **Sicurezza prodotto > Interfaccia esterna**.

2. Selezionare **Disabilita** sulle funzioni che si desidera impostare.

Selezionare **Abilita** se si desidera annullare il controllo.

Connessione PC tramite USB

È possibile limitare l'utilizzo della connessione USB dal computer. Se si desidera applicare una limitazione, selezionare **Disabilita**.

3. Fare clic su **OK**.

4. Verificare che la porta disabilitata non possa essere utilizzata.

Connessione PC tramite USB

Se il driver è stato installato sul computer

Collegare lo scanner al computer mediante un cavo USB e verificare che lo scanner non esegua scansioni.

Se il driver non è stato installato sul computer

Windows:

Aprire Gestione dispositivi e tenerlo aperto, collegare lo scanner al computer utilizzando un cavo USB, quindi verificare che i contenuti visualizzati da Gestione dispositivi rimangano invariati.

Mac OS:

Collegare lo scanner al computer mediante un cavo USB e verificare che non è possibile aggiungere lo scanner da **Stampanti e scanner**.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Monitoraggio di uno scanner remoto

Verifica delle informazioni per uno scanner remoto

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

- Stato del prodotto
Verificare lo stato, il servizio cloud, 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.
- Stato di utilizzo
Verificare il primo giorno di scansione, il conteggio delle scansioni, ecc.
- Stato hardware
Verificare lo stato di ciascuna funzione dello scanner.
- Miniatura pannello
Visualizza un'istantanea della schermata visualizzata sul pannello di controllo dello scanner.

Ricezione di notifiche email al verificarsi di eventi

Notifiche e-mail

Questa è la funzione di notifica che, quando si verificano eventi come l'arresto della scansione e un errore dello scanner, invia un'e-mail all'indirizzo specificato.

È possibile registrare fino a cinque destinazioni e impostare le impostazioni di notifica per ciascuna destinazione.

Per utilizzare questa funzione, è necessario impostare il server di posta prima di impostare le notifiche.

Informazioni correlate

➔ [“Configurazione di un server di posta” a pagina 42](#)

Configurazione delle notifiche e-mail

Configurare le notifiche e-mail utilizzando Web Config.

1. Accedere a Web Config e selezionare la scheda **Gestione dispositivo > Notifica tramite e-mail**.
2. Impostare l'oggetto delle notifiche e-mail.
Selezionare il contenuto che sarà visualizzato sull'oggetto dai due menu a discesa.
 - Il contenuto selezionato viene visualizzato accanto a **Oggetto**.
 - Lo stesso contenuto non può essere impostato sia a sinistra che a destra.
 - Quando il numero di caratteri in **Posizione** supera i 32 byte, i caratteri superiori a 32 byte vengono omessi.

3. Inserire l'indirizzo e-mail cui inviare l'e-mail di notifica.

Usare A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @ e inserire da 1 a 255 caratteri.

4. Selezionare la lingua per le notifiche e-mail.

5. Seleziona la casella di controllo dell'evento per il quale si desidera ricevere una notifica.

Il numero di **Impostazioni di notifica** è collegato al numero di destinazione di **Impostazioni indirizzo e-mail**.

Esempio:

Se si desidera inviare una notifica all'indirizzo e-mail impostato per il numero 1 in **Impostazioni indirizzo e-mail** quando si modifica la password di amministratore, selezionare la casella di controllo per la colonna 1 nella riga **Password amministratore modificata**.

6. Fare clic su **OK**.

Verificare che la notifica via e-mail venga inviata, causando un evento.

Esempio: la password di amministratore è stata modificata.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Elementi per la notifica e-mail

Elementi	Impostazioni e descrizione
Password amministratore modificata	Notifica quando la password dell'amministratore è stata modificata.
Errore scanner	Notifica quando si verifica un errore dello scanner.
Interruzione del Wi-Fi	Notifica quando si verifica un errore dell'interfaccia LAN wireless.

Soluzione dei problemi

Password di amministratore dimenticata

Hai bisogno di aiuto da parte del personale dell'assistenza. Contattare il rivenditore locale.

Nota:

Di seguito sono forniti i valori iniziali per l'amministratore di Web Config.

- Nome utente: nessuno (vuoto)
- Password: numero di serie dello scanner

Per trovare il numero di serie, verificare l'etichetta sul retro dello scanner. Se si ripristinano le impostazioni predefinite per la password amministratore, questa viene riportata ai valori iniziali.

Impostazioni di sicurezza avanzate

Impostazioni di sicurezza e prevenzione del pericolo.	94
Controllo tramite protocolli.	95
Uso di un certificato digitale.	98
Comunicazione SSL/TLS con lo scanner.	103
Comunicazione crittografata tramite IPsec/IP Filtering.	105
Connessione dello scanner a una rete IEEE802.1X.	116
Risoluzione dei problemi per la sicurezza avanzata.	118

Impostazioni di sicurezza e prevenzione del pericolo

Quando uno scanner è collegato a una rete, è possibile accedervi da una postazione remota. Inoltre, molti utenti possono condividere lo scanner, 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 lo scanner in un ambiente con accesso a Internet, i rischi sono ancora maggiori.

Per gli scanner che non dispongono di una protezione di accesso dall'esterno, sarà possibile leggere i contatti memorizzati nello scanner da Internet.

Per evitare questo rischio, gli scanner Epson dispongono di una varietà di tecnologie di sicurezza.

Impostare lo scanner 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
Controllo protocolli	Controlla i protocolli e servizi utilizzati per la comunicazione tra scanner e computer, attiva e 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.
Comunicazioni SSL/TLS	Il contenuto della comunicazione è crittografato mediante comunicazioni SSL/TLS quando si accede al server Epson su Internet dallo scanner, per esempio se si comunica con il computer tramite browser web utilizzando Epson Connect e si aggiorna il firmware.	Ottenere un certificato firmato CA e importarlo nello scanner.	La rimozione di un'identificazione dello scanner 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 scansione e le informazioni di configurazione.
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 non protetti.	Stabilire un criterio di base e individuale per impostare il client o il tipo di dati che possono accedere allo scanner.	Proteggere l'accesso non autorizzato, la manomissione e l'intercettazione dei dati di comunicazione allo scanner.
IEEE 802.1X	Consente solo agli utenti autenticati di connettersi alla rete. Consente solo a un utente autorizzato di utilizzare lo scanner.	Impostazione di autenticazione al server RADIUS (server di autenticazione).	Proteggere l'accesso e l'utilizzo non autorizzato dello scanner.

Informazioni correlate

- ➔ [“Controllo tramite protocolli” a pagina 95](#)
- ➔ [“Comunicazione SSL/TLS con lo scanner” a pagina 103](#)

- ➔ [“Comunicazione crittografata tramite IPsec/IP Filtering”](#) a pagina 105
- ➔ [“Connessione dello scanner a una rete IEEE802.1X”](#) a pagina 116

Impostazioni delle funzioni di sicurezza

Se si imposta Filtro IPsec/IP o IEEE 802.1X, 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.

Assicurarsi di configurare la password dell'amministratore prima di impostare il filtro IPsec/IP o IEEE 802.1X.

Controllo tramite 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.

È possibile ridurre i rischi indesiderati in termini di protezione limitando la scansione da determinati percorsi o controllando le funzioni disponibili.

Controllo dei protocolli

Configurare le impostazioni del protocollo supportate dallo scanner.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete** tab > **Protocollo**.
2. Configurare ciascuna voce.
3. Fare clic su **Avanti**.
4. Fare clic su **OK**.

Le impostazioni vengono applicate allo scanner.

Informazioni correlate

- ➔ [“Esecuzione di Web Config su un browser web”](#) a pagina 36

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 utilizzato per la funzione Push Scan e la ricerca in rete di EpsonNet Config.
Impostazioni WSD	È possibile abilitare o disabilitare la funzione WSD. Quando è abilitata, è possibile aggiungere dispositivi WSD ed eseguire scansioni dalla porta WSD.

Protocollo	Descrizione
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.

Voci di impostazione del protocollo

Imp. Bonjour

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	Visualizza il nome del servizio Bonjour.
Posizione	Visualizza il nome della posizione di Bonjour.
Wide-Area Bonjour	Impostare se usare Wide-Area Bonjour.

Imp. SLP

Elementi	Valore di impostazione e descrizione
Abilita SLP	Selezionare per abilitare la funzione SLP. Viene utilizzato ad esempio per la ricerca in rete in EpsonNet Config.

Impostazioni WSD

Elementi	Valore di impostazione e descrizione
Abilita WSD	Selezionare per consentire l'aggiunta di dispositivi tramite WSD, nonché 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

Elementi	Valore di impostazione e descrizione
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

Elementi	Valore di impostazione e descrizione
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

Elementi	Valore di impostazione e descrizione
Abilita SNMPv1/v2c	Selezionare per abilitare SNMPv1/v2c.
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

Elementi	Valore di impostazione e descrizione
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	
Algoritmo	Selezionare un algoritmo per un'autenticazione per SNMPv3.
Password	Inserire la password per un'autenticazione per SNMPv3. Immettere tra 8 e 32 caratteri in ASCII (0x20–0x7E). Se non si specifica questa voce, 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. Immettere tra 8 e 32 caratteri in ASCII (0x20–0x7E). Se non si specifica questa voce, lasciare il campo vuoto.
Conferma password	Immettere la password configurata per conferma.

Elementi	Valore di impostazione e descrizione
Nome contesto	Inserire fino a 32 caratteri in Unicode (UTF-8). Se non si specifica questa voce, lasciare il campo vuoto. Il numero di caratteri che è possibile inserire varia a seconda della lingua.

Uso di un certificato digitale

Informazioni sulla certificazione digitale

Certificato firma CA

Si tratta di un certificato firmato dalla CA (Certificate Authority, ente di certificazione). È possibile ottenerlo facendone richiesta all'ente di certificazione. Esso certifica l'esistenza dello scanner e viene utilizzato per comunicazioni SSL/TLS allo scopo di garantire la sicurezza della comunicazione dei dati.

Quando viene utilizzato per la comunicazione SSL/TLS, viene considerato come un certificato del server.

Quando è impostato sulla comunicazione IPsec/IP Filtering o IEEE 802.1x, viene utilizzato come certificato del client.

Certificato CA

Si tratta di un certificato concatenato con il Certificato firma CA, chiamato anche Certificato CA intermedio. Viene utilizzato dal browser web per convalidare il percorso del certificato dello scanner quando accede al server dell'altra parte o a Web Config.

Per il Certificato CA, impostare quando convalidare il percorso del certificato del server in accesso dallo scanner. Per lo scanner, impostare per certificare il percorso del Certificato firma CA per la connessione SSL/TLS.

È possibile ottenere il Certificato CA dello scanner dall'ente di certificazione che rilascia il Certificato CA.

È inoltre possibile ottenere il Certificato CA usato per convalidare il server dell'altra parte dall'ente di certificazione che ha emesso il Certificato firma CA dell'altro server.

Certificato firma personale

Si tratta di un certificato che lo scanner firma ed emette da sola. Viene chiamato anche certificato radice. Dal momento che l'emittente certifica se stesso, non è affidabile e non riesce a prevenire il furto d'identità.

Usarlo quando si effettuano le impostazioni di sicurezza e si esegue una comunicazione SSL/TLS semplice, senza il Certificato firma CA.

Se si utilizza questo certificato per una comunicazione SSL/TLS, sul browser potrebbe essere visualizzato un avviso di sicurezza, dal momento che il certificato non è registrato sul browser. È possibile utilizzare il Certificato firma personale solo per la comunicazione SSL/TLS.

Informazioni correlate

- ➔ [“Configurazione di un Certificato firma CA” a pagina 99](#)
- ➔ [“Aggiornamento di un certificato auto-firmato” a pagina 102](#)
- ➔ [“Configurazione di un Certificato CA” a pagina 103](#)

Configurazione di un Certificato firma 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 e selezionare la scheda **Sicurezza rete**. Quindi, selezionare **SSL/TLS > Certificato o IPsec/Filtro IP > Certificato client o IEEE802.1X > Certificato client**.

Qualunque cosa si scelga, è possibile ottenere lo stesso certificato e utilizzarlo in comune.

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

Viene aperta una pagina per la creazione della richiesta CSR.

3. Inserire 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 la scheda **Sicurezza 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

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

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. È possibile inserire da 1 a 5 indirizzi IPv4, indirizzi IPv6, nomi host e FQDN separandoli con virgole. Il primo elemento viene memorizzato nel nome comune e gli altri elementi vengono memorizzati nel campo alias dell'oggetto del certificato. Esempio: Indirizzo IP dello scanner: 192.0.2.123, nome dello scanner: EPSONA1B2C3 Nome comune: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
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.
Indirizzo e-mail mittente	È possibile inserire l'indirizzo e-mail del mittente per l'impostazione del server di posta. Inserire lo stesso indirizzo e-mail di Indirizzo e-mail mittente per la scheda Rete > Server e-mail > Di base .

Importazione di un certificato firmato CA

Importare nello scanner il Certificato firma CA ottenuto.



Importante:

- Assicurarsi che la data e l'ora dello scanner siano impostate correttamente. Il certificato potrebbe non essere valido.
- 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 e selezionare la scheda **Sicurezza 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. Inserire un valore per ciascuna voce. Impostare **Certificato CA 1** e **Certificato CA 2** quando si verifica il percorso del certificato nel browser web che accede allo scanner.

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

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Voci di impostazione per l'importazione del certificato firmato CA

Elementi	Impostazioni e descrizione
Certificato server o Certificato client	Selezionare un formato di certificato. Per la connessione SSL/TLS, viene visualizzato il file Certificato server. Per IPsec/IP Filtering o IEEE 802.1X, viene visualizzato il file Certificato client.
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	Se il formato di file è Certificato con chiave privata (PKCS#12) , immettere la password per la crittografia della chiave privata impostata al momento del rilascio del certificato.
Certificato CA 1	Se il formato del certificato è Certificato (PEM/DER) , importare un certificato di un ente di certificazione che emette un Certificato firma CA da usare come 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.

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 la scheda **Sicurezza 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

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Aggiornamento di un certificato auto-firmato

Dal momento che il Certificato firma personale viene rilasciato dallo scanner, è possibile aggiornarlo quando è scaduto o quando il contenuto descritto cambia.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete** tab > **SSL/TLS > Certificato**.
2. Fare clic su **Aggiorna**.
3. Immettere **Nome comune**.

È possibile inserire fino a 5 indirizzi IPv4, indirizzi IPv6, nomi host e FQDN composti da 1 a 128 caratteri, separandoli con virgole. Il primo parametro viene memorizzato nel nome comune e gli altri vengono memorizzati nel campo alias dell'oggetto del certificato.

Esempio:

Indirizzo IP dello scanner: 192.0.2.123, Nome scanner: EPSONA1B2C3

Nome comune: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Specificare un periodo di validità per il certificato.
5. Fare clic su **Avanti**.
6. Fare clic su **OK**.

Viene visualizzato un messaggio di conferma.

Lo scanner viene aggiornato.

Nota:

È possibile controllare le informazioni del certificato da **Sicurezza rete** scheda > **SSL/TLS > Certificato > Certificato firma personale** e clicca **Conferma**.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Configurazione di un Certificato CA

Quando si imposta il Certificato CA, è possibile convalidare il percorso del certificato CA del server cui lo scanner accede. Ciò può prevenire il furto d'identità.

È possibile ottenere il Certificato CA dall'ente di certificazione che rilascia il Certificato firma CA.

Importazione di un Certificato CA

Importare nello scanner il Certificato CA.

1. Accedere a Web Config e selezionare la scheda **Sicurezza 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

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Eliminazione di un Certificato CA

È possibile eliminare il Certificato CA importato.

1. Accedere a Web Config quindi selezionare la scheda **Sicurezza 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.
4. Fare clic su **Riavvia rete** quindi verificare che il certificato CA eliminato non sia elencato nella schermata aggiornata.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

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.

Configurazione delle impostazioni SSL/TLS di base

Se lo scanner supporta la funzionalità del server HTTPS, è possibile utilizzare la comunicazione SSL/TLS per codificare le comunicazioni. È possibile configurare e gestire lo scanner utilizzando Web Config garantendo comunque la sicurezza.

Configurare il livello di crittografia e la funzione di ridirezione.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete > SSL/TLS > Di base**.
2. Selezionare un valore per ciascuna voce.
 - Livello di crittografia
Selezionare il livello di crittografia.
 - Reindirizza HTTP su HTTPS
Reindirizzare su HTTPS quando si accede a HTTP.
3. Fare clic su **Avanti**.
Viene visualizzato un messaggio di conferma.
4. Fare clic su **OK**.
Lo scanner viene aggiornato.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Configurazione di un certificato server per lo scanner

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete > SSL/TLS > Certificato**.
2. Specificare un certificato da utilizzare in **Certificato server**.
 - Certificato firma personale
Un certificato auto-firmato è stato generato dallo scanner. Se non si ottiene un certificato firmato CA, selezionare questa opzione.
 - Certificato firma CA
Se si ottiene e si importa preventivamente un certificato firmato CA, è possibile specificare questa opzione.
3. Fare clic su **Avanti**.
Viene visualizzato un messaggio di conferma.
4. Fare clic su **OK**.
Lo scanner viene aggiornato.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

➔ [“Configurazione di un Certificato firma CA” a pagina 99](#)

➔ [“Configurazione di un Certificato CA” a pagina 103](#)

Comunicazione crittografata tramite IPsec/IP Filtering

Informazioni su IPsec/Filtro IP

È possibile filtrare il traffico in base agli indirizzi IP, servizi e porta usando la funzione IPsec/IP Filtering. 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.

Nota:

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

Configurazione dei criteri predefiniti

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.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete > IPsec/Filtro IP > Di base**.
2. Inserire 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

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Voci di impostazione di Criteri predefiniti

Criteri predefiniti

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

Controllo accesso

Configurare un metodo di controllo per il traffico dei pacchetti IP.

Elementi	Impostazioni e descrizione
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 **Versione IKE**. 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.

Elementi	Impostazioni e descrizione
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.

Elementi	Impostazioni e descrizione	
Locale	Metodo autenticazione	Per selezionare Certificato , occorre ottenere e importare preventivamente un certificato firmato CA.
	Tipo ID	Se si seleziona Chiave precondivisa come Metodo autenticazione , selezionare il tipo di ID per lo scanner.
	ID	Inserire l'ID dello scanner che corrisponde al tipo di ID. Non è possibile utilizzare "@", "#" e "=" come primo carattere. Nome distintivo: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=". Indirizzo IP: immettere il formato IPv4 o IPv6. FQDN: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, a–z, 0–9, "-" e il punto (.). Indirizzo e-mail: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@". ID chiave: immettere da 1 a 255 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.

Elementi		Impostazioni e descrizione
Remoto	Metodo autenticazione	Per selezionare Certificato , occorre ottenere e importare preventivamente un certificato firmato CA.
	Tipo ID	Se si seleziona Chiave precondivisa come Metodo autenticazione , selezionare il tipo di ID per il dispositivo da autenticare.
	ID	Inserire l'ID dello scanner che corrisponde al tipo di ID. Non è possibile utilizzare "@", "#" e "=" come primo carattere. Nome distintivo: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=". Indirizzo IP: immettere il formato IPv4 o IPv6. FQDN: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, a–z, 0–9, "-" e il punto (.). Indirizzo e-mail: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@". ID chiave: immettere da 1 a 255 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.

Elementi	Impostazioni e descrizione
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.

Elementi	Impostazioni e descrizione
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

Si consiglia di selezionare **Qualsiasi** per tutte le impostazioni, oppure di selezionare una voce diversa da **Qualsiasi** per ciascuna impostazione. Se si seleziona **Qualsiasi** per alcune impostazioni e si seleziona una voce diversa da **Qualsiasi** per altre impostazioni, il dispositivo potrebbe non essere in grado di comunicare in base all'altro dispositivo che si desidera autenticare.

Elementi		Impostazioni e descrizione
IKE	Crittografia	Selezionare l'algoritmo di crittografia per IKE. 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. Le voci variano a seconda della versione di IKE.
ESP	Crittografia	Selezionare l'algoritmo di crittografia per ESP. Questa funzione è disponibile quando è selezionato ESP come Protocollo sicurezza .
	Autenticazione	Selezionare l'algoritmo di autenticazione per ESP. Questa funzione è disponibile quando è selezionato ESP come Protocollo sicurezza .
AH	Autenticazione	Selezionare l'algoritmo di crittografia per AH. Questa funzione è disponibile quando è selezionato AH come Protocollo sicurezza .

Configurazione dei 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.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete > IPsec/Filtro IP > Di base**.
2. Fare clic su una scheda numerata che si desidera configurare.
3. Inserire 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.

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.

Elementi	Impostazioni e descrizione
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**.

Nota:

Se un indirizzo IPv6 viene assegnato automaticamente, la connessione potrebbe risultare non disponibile. Configurare un indirizzo IPv6 statico.

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.

Nota:

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.

Protocollo trasporto

Se si seleziona **Numero porta** per **Metodo di scelta porta**, occorre configurare un modo di incapsulazione.

Elementi	Impostazioni e descrizione
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.

Esempio: 20,80,119,5220

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.

Esempio: 25,80,143,5220

Se non viene immesso un numero di porta, vengono controllate tutte le porte.

Versione IKE

Selezionare **IKEv1** o **IKEv2** per **Versione IKE**. 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.

Elementi	Impostazioni e descrizione
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.

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	Se si seleziona Chiave precondivisa come Metodo autenticazione , selezionare il tipo di ID per lo scanner.
	ID	Inserire l'ID dello scanner che corrisponde al tipo di ID. Non è possibile utilizzare "@", "#" e "=" come primo carattere. Nome distintivo: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=". Indirizzo IP: immettere il formato IPv4 o IPv6. FQDN: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, a–z, 0–9, "-" e il punto (.). Indirizzo e-mail: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@". ID chiave: immettere da 1 a 255 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	Se si seleziona Chiave precondivisa come Metodo autenticazione , selezionare il tipo di ID per il dispositivo da autenticare.
	ID	Inserire l'ID dello scanner che corrisponde al tipo di ID. Non è possibile utilizzare "@", "#" e "=" come primo carattere. Nome distintivo: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "=". Indirizzo IP: immettere il formato IPv4 o IPv6. FQDN: immettere una combinazione tra 1 e 255 caratteri utilizzando A–Z, a–z, 0–9, "-" e il punto (.). Indirizzo e-mail: immettere da 1 a 255 caratteri ASCII (0x20–0x7E) a 1 byte. È necessario includere "@". ID chiave: immettere da 1 a 255 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.

Elementi	Impostazioni e descrizione
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.

Elementi	Impostazioni e descrizione
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

Si consiglia di selezionare **Qualsiasi** per tutte le impostazioni, oppure di selezionare una voce diversa da **Qualsiasi** per ciascuna impostazione. Se si seleziona **Qualsiasi** per alcune impostazioni e si seleziona una voce diversa da **Qualsiasi** per altre impostazioni, il dispositivo potrebbe non essere in grado di comunicare in base all'altro dispositivo che si desidera autenticare.

Elementi		Impostazioni e descrizione
IKE	Crittografia	Selezionare l'algoritmo di crittografia per IKE. 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. Le voci variano a seconda della versione di IKE.
ESP	Crittografia	Selezionare l'algoritmo di crittografia per ESP. Questa funzione è disponibile quando è selezionato ESP come Protocollo sicurezza .
	Autenticazione	Selezionare l'algoritmo di autenticazione per ESP. Questa funzione è disponibile quando è selezionato ESP come Protocollo sicurezza .
AH	Autenticazione	Selezionare l'algoritmo di crittografia per AH. Questa funzione è disponibile quando è selezionato AH come Protocollo sicurezza .

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.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

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 Epson Device Admin e di un driver dello scanner
SNMP	UDP	161	Qualsiasi porta	Acquisizione e configurazione di MIB da applicazioni quali Epson Device Admin e il driver dello scanner Epson
WSD	TCP	Qualsiasi porta	5357	Controllo WSD
WS-Discovery	UDP	3702	Qualsiasi porta	Ricerca di scanner WSD
Network Scan	TCP	1865	Qualsiasi porta	Inoltro dei dati di scansione da Document Capture Pro
Network Push Scan	TCP	Qualsiasi porta	2968	Acquisizione di informazioni sui lavori per la funzione Push Scan da Document Capture Pro
Network Push Scan Discovery	UDP	2968	Qualsiasi porta	Ricerca di un computer dallo scanner

Nome del servizio	Tipo protocollo	Numero porta locale	Numero porta remota	Funzioni controllate
Dati FTP (Remoto)	TCP	Qualsiasi porta	20	Client FTP (inoltrato dati di scansione) Tuttavia, ciò può controllare solo un server FTP che utilizza un numero di porta remota 20.
Controllo FTP (Remoto)	TCP	Qualsiasi porta	21	Client FTP (controllo dei dati di scansione inoltrati)
CIFS (Remoto)	TCP	Qualsiasi porta	445	Client CIFS (inoltrato di dati di scansione a una cartella)
NetBIOS Name Service (Remoto)	UDP	Qualsiasi porta	137	Client CIFS (inoltrato di dati di scansione a una cartella)
NetBIOS Datagram Service (Remoto)	UDP	Qualsiasi porta	138	
NetBIOS Session Service (Remoto)	TCP	Qualsiasi porta	139	
HTTP (Locale)	TCP	80	Qualsiasi porta	Server HTTP(S) (inoltrato dati di Web Config e WSD)
HTTPS (Locale)	TCP	443	Qualsiasi porta	
HTTP (Remoto)	TCP	Qualsiasi porta	80	Client HTTP(S) (aggiornamento del firmware e del certificato radice)
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.

Ricezione di dati di scansione e impostazioni dello scanner

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, HTTP (Locale), HTTPS (Locale) e Network Scan.

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 del certificato per IPsec/IP Filtering

Configurare il certificato client per IPsec/IP Filtering. Quando lo si imposta, è possibile utilizzare il certificato come metodo di autenticazione per IPsec/IP Filtering. Per configurare l'ente di certificazione, andare su **Certificato CA**.

1. Accedere a Web Config e selezionare la scheda **Sicurezza 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, è possibile copiarlo e utilizzarlo in IPsec/IP Filtering. Per copiarlo, selezionare il certificato da **Copia da**, quindi fare clic su **Copia**.

Informazioni correlate

- ➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)
- ➔ [“Configurazione di un Certificato firma CA” a pagina 99](#)
- ➔ [“Configurazione di un Certificato CA” a pagina 103](#)

Connessione dello scanner a una rete IEEE802.1X

Configurazione di una rete IEEE 802.1X

Quando si imposta IEEE 802.1X allo scanner, è possibile utilizzarlo sulla rete collegata a un server RADIUS, a uno switch LAN con funzione di autenticazione o a un punto di accesso.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete** > **IEEE802.1X** > **Di base**.

2. Inserire un valore per ciascuna voce.

Se si desidera utilizzare lo scanner su una rete Wi-Fi, fare clic su **Configurazione connessione wireless** e selezionare o immettere un SSID.

Nota:

È possibile condividere le impostazioni tra Ethernet e Wi-Fi.

3. Fare clic su **Avanti**.

Viene visualizzato un messaggio di conferma.

4. Fare clic su **OK**.

Lo scanner viene aggiornato.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Voci di impostazione di rete IEEE 802.1X

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).	
IEEE802.1X (Wi-Fi)	Viene visualizzato lo stato della connessione di IEEE802.1X (Wi-Fi).	
Metodo di connessione	Viene visualizzato il metodo di connessione di una rete corrente.	
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.
EAP-TTLS		
ID utente	Configurare un ID da utilizzare per l'autenticazione di un server RADIUS. Immettere da 1 a 128 caratteri ASCII (0x20–0x7E) a 1 byte.	
Password	Configurare una password per autenticare lo scanner. 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. Immettere da 0 a 128 caratteri ASCII (0x20–0x7E) a 1 byte.	

Elementi	Impostazioni e descrizione	
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 come Tipo EAP , è possibile configurare un nome anonimo al posto di un ID utente per la fase 1 di un'autenticazione PEAP. Immettere da 0 a 128 caratteri ASCII (0x20–0x7E) a 1 byte.	
Livello di crittografia	È possibile selezionare una delle seguenti opzioni.	
	Alto	AES256/3DES
	Medio	AES256/3DES/AES128/RC4

Configurazione di un certificato per IEEE 802.1X

Configurare il certificato client per IEEE802.1X. Quando lo si imposta, è possibile utilizzare **EAP-TLS** e **PEAP-TLS** come metodo di autenticazione di IEEE 802.1X. Per configurare il certificato dell'ente di certificazione, andare su **Certificato CA**.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete > IEEE802.1X > Certificato client**.
2. Immettere un certificato in **Certificato client**.

Se si è già importato un certificato pubblicato da un ente di certificazione, è possibile copiarlo e utilizzarlo in IEEE802.1X. Per copiarlo, selezionare il certificato da **Copia da**, quindi fare clic su **Copia**.

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Risoluzione dei problemi per la sicurezza avanzata

Ripristino delle impostazioni di sicurezza

Se si stabilisce un ambiente dalla sicurezza elevata come IPsec/IP Filtering, 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 utilizzando Web Config

È possibile disabilitare IPsec/Filtro IP utilizzando Web Config.

1. Accedere a Web Config e selezionare la scheda **Sicurezza rete > IPsec/Filtro IP > Di base**.
2. Disattivare la **IPsec/Filtro IP**.

Problemi utilizzando le funzioni di sicurezza di rete

Chiave pre-condivisa dimenticata

Ri-configurare una chiave pre-condivisa.

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

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

Informazioni correlate

- ➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)
- ➔ [“Comunicazione crittografata tramite IPsec/IP Filtering” a pagina 105](#)

Impossibile utilizzare la comunicazione IPsec

Specificare l’algoritmo che lo scanner o il computer non supporta.

Lo scanner supporta i seguenti algoritmi. Verificare le impostazioni del computer.

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	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
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 105](#)

Impossibile comunicare istantaneamente

L'indirizzo IP dello scanner è stato modificato o non può essere utilizzato.

Quando l'indirizzo IP registrato all'indirizzo locale su Criteri gruppo è stato modificato o non può essere utilizzato, non è possibile eseguire la comunicazione IPsec. 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 (scheda **Sicurezza 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 stato modificato o non può essere utilizzato.

Quando l'indirizzo IP registrato all'indirizzo remoto su Criteri gruppo è stato modificato o non può essere utilizzato, non è possibile eseguire la comunicazione IPsec.

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 (scheda **Sicurezza rete** > **IPsec/Filtro IP** > **Di base** > **Criteri gruppo** > **Indirizzo remoto(Host)**) potrebbe non essere trovato.

Utilizzare un indirizzo IP statico.

Informazioni correlate

- ➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)
- ➔ [“Comunicazione crittografata tramite IPsec/IP Filtering” a pagina 105](#)

Impossibile connettersi dopo la configurazione di IPsec/IP Filtering

Le impostazioni di IPsec/IP Filtering non sono corrette.

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 105](#)

Impossibile accedere allo scanner dopo la configurazione di IEEE 802.1X

Le impostazioni di IEEE 802.1X non sono corrette.

Disabilitare IEEE 802.1X e il modo Wi-Fi dal pannello di controllo dello scanner. Collegare lo scanner e un computer, quindi configurare nuovamente IEEE 802.1X.

Collegare lo scanner e un computer, quindi configurare nuovamente IEEE 802.1X.

Informazioni correlate

- ➔ [“Configurazione di una rete IEEE 802.1X” a pagina 116](#)

Problema con l'uso di un certificato digitale

Impossibile importare un Certificato firma CA

Il Certificato firma CA e le informazioni sulla CSR non corrispondono.

Se il Certificato firma 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 firma CA ha dimensioni maggiori di 5 KB.

Non è possibile importare un Certificato firma CA superiore a 5 KB.

La password per l'importazione del certificato non è corretta.

Immettere la password corretta. Se la password è stata dimenticata, non è possibile importare il certificato. Ottenere di nuovo un Certificato firma CA.

Informazioni correlate

➔ [“Importazione di un certificato firmato CA” a pagina 100](#)

Impossibile aggiornare un certificato auto-firmato

Il Nome comune non è stato immesso.

Il **Nome comune** deve venire immesso.

Sono stati inseriti dei caratteri non supportati per Nome comune.

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

Nel nome comune è stato incluso uno spazio o una virgola.

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 102](#)

Impossibile creare una richiesta CSR

Il Nome comune non è stato immesso.

Il Nome comune deve venire immesso.

Sono stati inseriti dei caratteri non supportati per Nome comune, Organizzazione, Unità organizzativa, Località e Stato/Provincia.

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

È stato incluso uno spazio o una virgola 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 99](#)

Visualizzazione di avvertenza relativa a un certificato digitale

Messaggi	Causa/Operazione da eseguire
Inserire un certificato server.	<p>Causa: Non è stato selezionato un file da importare.</p> <p>Operazione da eseguire: Selezionare un file e fare clic su Importa.</p>
Certificato CA 1 non inserito.	<p>Causa: Il certificato CA 1 non viene immesso e risulta immesso solo il certificato CA 2.</p> <p>Operazione da eseguire: Importare innanzitutto il certificato CA 1.</p>
Il valore seguente non è valido.	<p>Causa: Caratteri non supportati sono presenti nel percorso del file e/o nella password.</p> <p>Operazione da eseguire: Assicurarsi che nelle voci siano immessi i caratteri corretti.</p>
Data e ora non valide.	<p>Causa: La data e l'ora dello scanner non sono state impostate.</p> <p>Operazione da eseguire: Impostare la data e l'ora utilizzando Web Config o EpsonNet Config.</p>
Password non valida.	<p>Causa: La password impostata per il certificato CA e la password immessa non corrispondono.</p> <p>Operazione da eseguire: Immettere la password corretta.</p>

Messaggi	Causa/Operazione da eseguire
File non valido.	<p>Causa:</p> <p>Si sta importando un file di certificato in formato X509.</p> <p>Operazione da eseguire:</p> <p>Assicurarsi di selezionare il certificato corretto inviato da un ente di certificazione fidato.</p>
	<p>Causa:</p> <p>Il file importato è di dimensioni eccessive. Le dimensioni massime del file sono di 5 KB.</p> <p>Operazione da eseguire:</p> <p>Se è stato selezionato il file corretto, il certificato potrebbe essere danneggiato o manipolato.</p>
	<p>Causa:</p> <p>La catena contenuta nel certificato non è valida.</p> <p>Operazione da eseguire:</p> <p>Per ulteriori informazioni sul certificato, vedere il sito Web dell'ente di certificazione.</p>
Impossibile usare i certificati server che includono oltre 3 certificati CA.	<p>Causa:</p> <p>Il file di certificato in formato PKCS#12 contiene più di 3 certificati CA.</p> <p>Operazione da eseguire:</p> <p>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.</p>
Il certificato è scaduto. Verificare se il certificato è valido o controllare data e ora sul prodotto.	<p>Causa:</p> <p>Il certificato è scaduto.</p> <p>Operazione da eseguire:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Se il certificato è scaduto, ottenere e importare un nuovo certificato. <input type="checkbox"/> Se il certificato non è scaduto, assicurarsi che la data e l'ora dello scanner siano impostate correttamente.
Chiave privata obbligatoria.	<p>Causa:</p> <p>Non risulta abbinata una chiave privata al certificato.</p> <p>Operazione da eseguire:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Se il certificato è in formato PEM/DER e viene ottenuto da una richiesta CSR tramite computer, specificare il file della chiave privata. <input type="checkbox"/> 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.
	<p>Causa:</p> <p>Il certificato PEM/DER ottenuto da una richiesta CSR è stato reimportato tramite Web Config.</p> <p>Operazione da eseguire:</p> <p>Se il certificato è in formato PEM/DER e viene ottenuto da una richiesta CSR tramite Web Config, è possibile importarlo una sola volta.</p>

Messaggi	Causa/Operazione da eseguire
Configurazione non riuscita.	Causa: 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. Operazione da eseguire: Dopo aver verificato il file specificato e la comunicazione, importare di nuovo il file.

Informazioni correlate

➔ [“Informazioni sulla certificazione digitale” a pagina 98](#)

Eliminazione erronea di un certificato firmato CA

Non esiste alcun file di backup per il certificato firmato CA.

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

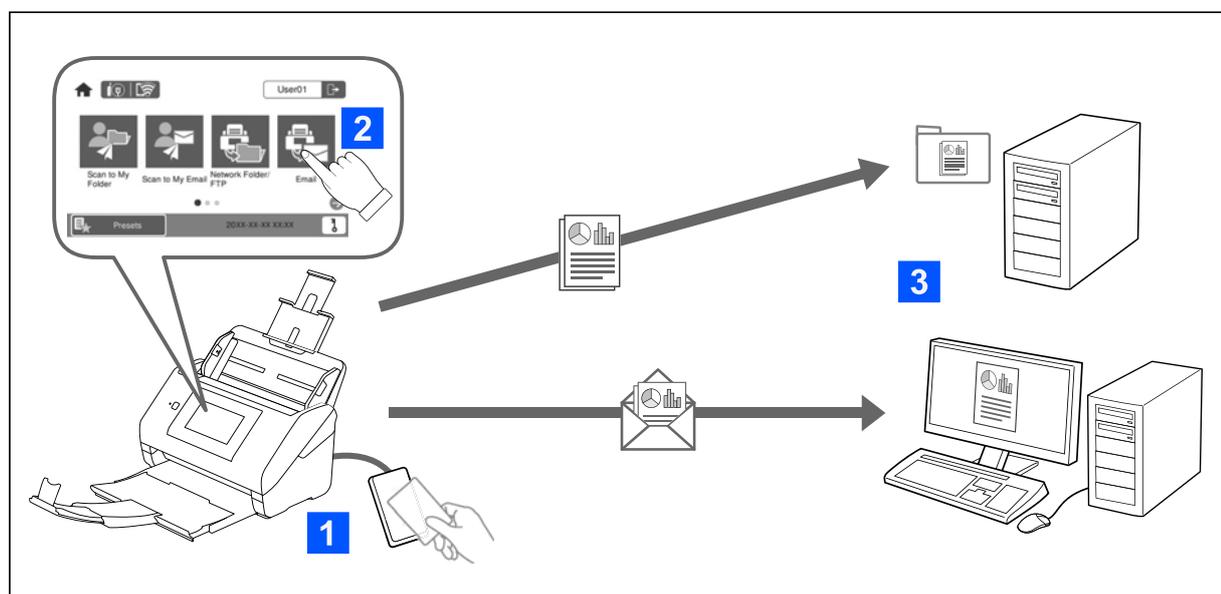
➔ [“Importazione di un certificato firmato CA” a pagina 100](#)

➔ [“Eliminazione di un certificato firmato CA” a pagina 101](#)

Impostazioni di autenticazione

Informazioni su Impostazioni di autenticazione.	126
Informazioni su Metodo autenticazione.	127
Software per la configurazione.	129
Aggiornare il firmware dello scanner.	129
Collegamento e configurazione di un dispositivo di autenticazione.	129
Registrazioni e impostazioni.	134
Rapporti della Cronologia processi con Epson Device Admin.	150
Effettuare l'accesso come amministratore dal pannello di controllo.	151
Disabilitazione di Impostazioni di autenticazione.	151
Eliminare le informazioni delle Impostazioni di autenticazione (Ripristina impostaz. predef.).	152
Soluzione dei problemi.	152

Informazioni su Impostazioni di autenticazione



Quando Impostazioni di autenticazione è abilitato, è necessaria l'autenticazione dell'utente per avviare la scansione. È possibile impostare i metodi di scansione utilizzabili da ciascun utente in modo da prevenire operazioni accidentali.

È possibile specificare come destinazione di scansione l'indirizzo e-mail dell'utente autenticato (Scan su La mia e-mail), o salvare i dati di ogni utente in una cartella personale (Scan su La mia cart.). È inoltre possibile specificare altri metodi di scansione.

Nota:

- ❑ Non è possibile eseguire la scansione da computer o dispositivo smart quando Impostazioni di autenticazione è abilitato.
- ❑ In aggiunta alle Impostazioni di autenticazione descritte in questo manuale, è anche possibile creare un sistema di autenticazione utilizzando un server di autenticazione. Per creare un sistema, utilizzare Document Capture Pro Server Authentication Edition (il nome abbreviato è Document Capture Pro Server AE). Per ulteriori informazioni, contattare la sede Epson locale.

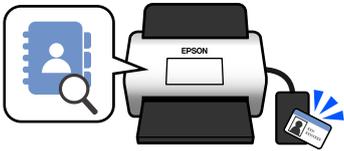
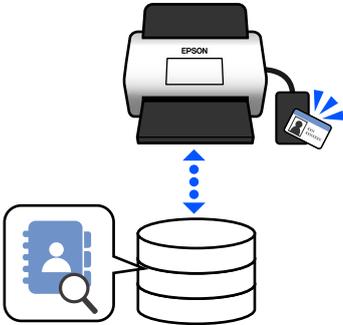
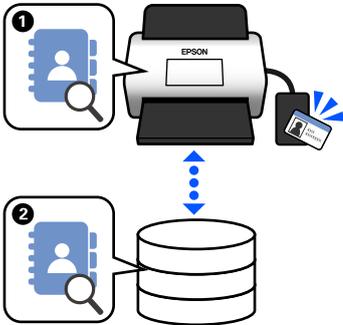
Funzioni disponibili per Impostazioni di autenticazione

Funzione di scansione del pannello di controllo	Impostazioni di autenticazione	
	Abilitato	Disabilitato
Scan su La mia cart. Salva le immagini nella cartella assegnata all'utente autenticato.	✓	-
Scan su La mia e-mail Invia le immagini all'indirizzo e-mail dell'utente autenticato.	✓	-
Scans. su cartella rete/FTP Salva le immagini in una cartella sulla rete.	✓	✓

Funzione di scansione del pannello di controllo	Impostazioni di autenticazione	
	Abilitato	Disabilitato
<p>Scansione su computer</p> <p>Salva le immagini su un computer collegato utilizzando i lavori creati in Document Capture Pro (Windows)/Document Capture (Mac OS).</p> <p>* Quando Impostazioni di autenticazione è abilitato, è possibile utilizzare solo i lavori registrati in Preimpostaz..</p>	✓*	✓
<p>Scansione su e-mail</p> <p>Invia le immagini all'indirizzo e-mail impostato.</p>	✓	✓
<p>Scansione su Cloud</p> <p>Invia le immagini al servizio cloud impostato.</p>	✓	✓
<p>Scan su unità USB.</p> <p>Salva le immagini su una chiavetta USB collegata allo scanner. Questa funzione è disponibile solo quando allo scanner non sono collegati dispositivi di autenticazione.</p>	✓	✓
<p>Esegui scansione su WSD</p> <p>Salva le immagini su un computer collegato utilizzando la funzione WSD.</p>	-	✓
<p>Preimpostaz.</p> <p>È possibile registrare fino a 48 funzioni di scansione predefinite.</p> <p>È possibile assegnare fino a cinque Preimpostaz. agli utenti registrati nel DB locale. I Preimpostaz. assegnati sono disponibili solo per quell'utente. I Preimpostaz. che non sono stati assegnati a un utente specifico possono essere utilizzati da tutti gli utenti.</p>	✓	✓

Informazioni su Metodo autenticazione

Questo scanner può eseguire la funzione di autenticazione utilizzando i seguenti metodi senza dover creare un server di autenticazione.

	DB locale	LDAP	DB locale e LDAP
Posizione delle informazioni utente	<p>Memoria dello scanner</p> <p>Questo metodo di autenticazione verifica le informazioni utente registrate nello scanner e le confronta con l'utente che sta utilizzando la funzione di scansione.</p>	<p>Server LDAP*</p> <p>Questo metodo di autenticazione verifica le informazioni utente del server LDAP sincronizzato con la stampante. Poiché è possibile memorizzare temporaneamente nello scanner come cache fino a 300 voci di informazioni utente dal server LDAP, è possibile eseguire l'autenticazione utilizzando la cache se il server LDAP non funziona.</p> <p>* Server che fornisce un servizio di directory in grado di comunicare con LDAP.</p>	<p>Memoria dello scanner e server LDAP</p> <p>Verificare prima le informazioni utente registrate nello scanner (1) e, in caso di mancata corrispondenza, confrontare le informazioni utente con quelle memorizzate sul server LDAP (2).</p>
			
Numero di utenti registrati	50 (memoria dello scanner)	Illimitata (server LDAP)	50 (memoria dello scanner) Illimitata (server LDAP)
Cache di memoria dello scanner	-	300	Massimo 300 (50 degli slot della cache sono condivisi con Imp. utente in DB locale)
Metodi di accesso	<p>È possibile utilizzare uno qualsiasi dei seguenti metodi.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Mostrare una scheda di autenticazione o immettere ID utente e Password <input type="checkbox"/> Mostrare una carta di autenticazione o immettere un Numero di identità <input type="checkbox"/> Immettere ID utente e Password <input type="checkbox"/> Immettere un ID utente <input type="checkbox"/> Immettere un Numero di identità 		
Limiti della funzione "Scansione a"	Impostare singolarmente per ciascun utente	Stesse impostazioni per tutti gli utenti LDAP	Utenti DB locale: impostare singolarmente Utenti LDAP: stesse impostazioni per tutti gli utenti
Assegnare i Preimpost az. agli utenti	Fino a 5 per utente	- (Non possono essere impostati singolarmente)	Utenti DB locale: fino a 5 per utente Utenti LDAP: -

Software per la configurazione

Configurare utilizzando Web Config o Epson Device Admin.

- Quando si usa Web Config è possibile configurare lo scanner solo tramite un browser web.

[“Web Config” a pagina 36](#)

- Quando si usa Epson Device Admin è possibile configurare più scanner contemporaneamente utilizzando un modello di configurazione.

[“Epson Device Admin” a pagina 37](#)

Aggiornare il firmware dello scanner

Prima di abilitare Impostazioni di autenticazione, aggiornare il firmware dello scanner alla versione più recente. Connettere innanzitutto lo scanner a Internet.



Importante:

Mentre è in corso l'aggiornamento, non spegnere né il computer, né lo scanner.

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Gestione dispositivo** > **Aggiornamento firmware** e seguire le istruzioni a schermo per aggiornare il firmware.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Principale** > **Firmware** > **Aggiorna** nella schermata dell'elenco dei dispositivi, quindi seguire le istruzioni a schermo per aggiornare il firmware.

Nota:

L'aggiornamento non è necessario se è già installato il firmware più recente.

Collegamento e configurazione di un dispositivo di autenticazione

Se si desidera collegare e utilizzare un dispositivo di autenticazione come un lettore di schede IC, è necessario prima configurare il dispositivo. Ciò non è necessario se non si utilizza un dispositivo di autenticazione.

Informazioni correlate

➔ [“Collegamento del dispositivo di autenticazione” a pagina 132](#)

➔ [“Impostazioni del dispositivo di autenticazione” a pagina 133](#)

Elenco dei lettori di schede supportati

Questo elenco non garantisce il funzionamento dei lettori di schede presenti nell'elenco.

Si: supportato (le informazioni di identificazione sono leggibili utilizzando le impostazioni standard del lettore di schede.)

No: non compatibile

Prodotto-re	Modello	Numero di modello	Scheda di autenticazione							Modo
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultra-light	Standard	Lite/Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Si	Si*1	Si*1	Si*1	No	No	No	Tastiera
RF IDEAS	pcProx	RDR-7081BKU	Si*1	No	Si	Si	No	No	No	Tastiera
RF IDEAS	pcProx	RDR-7581AKU	Si	No	Si*1	Si*1	No	No	No	Tastiera
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	No	No	Si	Si	No	No	No	Tastiera
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Si	No	Si	Si	Si	Si	Si	Tastiera
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Si	Si	Si	Si	Si	Si	Si	Tastiera
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Si	Si	Si	Si	Si	Si	Si	Tastiera
ELATEC	TWN4 Slim	T4QC-FC3B7	Si	Si	Si	Si	Si	Si	Si	Tastiera
HID Global	OMNI-KEY 5427	OMNI-KEY5427CK OMNI-KEY5427CK gen2	Si	Si	Si	Si	Si	No	Si	Tastiera*1

Prodotto- re	Mo- dello	Nu- mero di mo- dello	Scheda di autenticazione							IEC/ ISO14 443 (Ty- peB) Com- plian- ce	Modo
			HID Global	DMZ	MIFARE		FeliCa™				
			iClass	EM40 02	Clas- sic	Ultra- light	Stan- dard	Lite/ Lite-S			
ACS	ACR122 U	ACR122 U	No	No	Si*2	Si*2	Si	No	Si*2	PC/SC	
ACS	ACR125 2	ACR125 2	No	No	Si*2	Si*2	Si	Si	Si*2	PC/SC	
Sony	PaSoRi	RC- S330/S	No	No	Si*2	Si*2	Si*2	Si*2	Si*2	PaSoRi	
Sony	PaSoRi	RC- S380/P RC- S380/S	No	No	Si*2	Si*2	Si*2	Si*2	Si*2	PaSoRi	
DMZ	Leitor RFID Univer- sal	DMZ00 8	Si	Si	Si	Si	Si	Si	Si	Tastiera	
DMZ	Leitor RFID Mul- ti-125	DMZ08 7	No	Si	No	No	No	No	No	Tastiera	
DMZ	Leitor RFID Mifare	DMZ08 8	No	No	Si	Si	No	No	No	Tastiera	
DMZ	Biome- tric & RFID Reader	DMZ07 3	No	Si	No	No	No	No	No	Tastiera	
inepro	SCR708	SCR708	Si*1	Si*1	Si*1	Si*1	Si*1	Si*1	Si*1	Tastiera	
Y Soft	YU0308 8 001	MU038 8	Si	Si	Si	Si	Si	Si	Si	Tastiera	
Carta- dis	TCM3 Carta- dis MiFare Card Reader	ZTCM3- MIFARE	No	No	Si	Si	No	No	Si	Tastiera	
MICI Net- work Co., Ltd.	EM & Mifare Card Reader	mCR-6 00	No	No	Si	Si	No	No	Si	Tastiera	

Prodotto-	Modello	Numero di modello	Scheda di autenticazione							Modo
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultra-light	Standard	Lite/Lite-S		
NT-wa-re	MiCard Multi-Tech4-PI	T4DT-FB4WU F-PI	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Tastiera
NT-wa-re	MiCard Plus-2-V2	RDR-80 081AG U-NT2-20	Sì*1	Sì*1	Sì*1	Sì*1	No	No	No	Tastiera
NT-wa-re	MiCard V3 Multi	MiCard V3 Multi	Sì	Sì	Sì	Sì	Sì	Sì	No	Tastiera

- *1 È necessario modificare le impostazioni del lettore di schede tramite il software proprietario fornito dal produttore del lettore.
- *2 Se è necessario utilizzare dati in un'area specifica della scheda diversi dall'ID standard della scheda, come un ID di autenticazione, configurando le impostazioni del prodotto, contattare il proprio partner o rappresentante locale Epson per ulteriori informazioni sulle modalità di configurazione del prodotto.

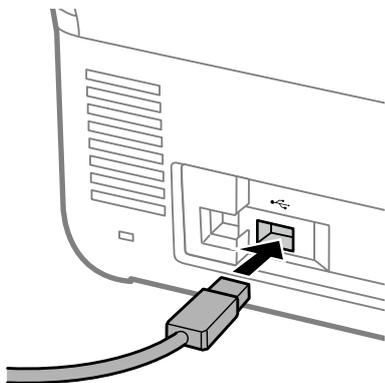
Collegamento del dispositivo di autenticazione



Importante:

Quando si collega il dispositivo di autenticazione a più scanner, utilizzare un prodotto con lo stesso numero di modello.

Collegare il cavo USB del lettore di schede alla porta USB dell'interfaccia esterna sullo scanner.



Controllo operativo per il dispositivo di autenticazione

È possibile verificare lo stato della connessione e il riconoscimento della scheda di autenticazione del dispositivo di autenticazione nel pannello di controllo dello scanner.

Selezionando **Impostazioni > Informazioni dispositivo > Stato dispositivo di autenticazione**, vengono visualizzate le informazioni.

Impostazioni del dispositivo di autenticazione

Impostare il formato di lettura per le informazioni di autenticazione ricevute da una scheda di autenticazione.

È possibile impostare il seguente metodo di lettura per il dispositivo di autenticazione.

- Leggere un'area specifica della scheda di autenticazione, ad esempio il numero di dipendente o l'identificativo personale.
- Utilizzare le informazioni della scheda di autenticazione tranne l'UID (informazioni della scheda di autenticazione quali il numero di serie.)

È possibile utilizzare uno strumento per generare i parametri operativi. Rivolgersi al rivenditore per ulteriori dettagli.

Nota:

Utilizzo di schede di autenticazione di diversi produttori:

Quando si utilizzano le informazioni sulla scheda UID (informazioni di identificazione della scheda come il numero di serie), è possibile utilizzare una varietà di tipi di schede di autenticazione. Non possono essere mischiate quando si utilizzano altre informazioni sulla scheda.

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Gestione dispositivo > Lettore di schede**.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Impostazioni amministratore > Impostazioni autenticaz. > Lettore di schede** dal modello di configurazione.

Voce	Descrizione
Vendor ID	Impostare l'ID del fornitore del dispositivo di autenticazione che limita l'utilizzo da 0000 a FFFF utilizzando 4 caratteri alfanumerici. Se non si desidera un limite, immettere 0000.
Product ID	Impostare l'ID prodotto del dispositivo di autenticazione che limita l'utilizzo da 0000 a FFFF utilizzando 4 caratteri alfanumerici. Se non si desidera un limite, immettere 0000.
Parametro operativo	Impostare il parametro di funzionamento del dispositivo di autenticazione tra 0 e 8192 caratteri. Sono disponibili A-Z, a-z, 0-9, +, /, =, spazio e avanzamento riga.
Lettore di schede	Selezionare il formato di conversione per il dispositivo di autenticazione. È possibile verificare i dettagli relativi al formato. Si veda il link fornito nella descrizione dell'articolo.
Formato di salvataggio ID scheda di autenticazione	Selezionare il formato di conversione per le informazioni di autenticazione di un documento di identità. È possibile verificare i dettagli relativi al formato. Si veda il link fornito nella descrizione dell'articolo.
Imposta intervallo ID scheda	Abilitare la specifica della posizione di lettura.

Voce	Descrizione
Posizione di inizio testo	Specificare la posizione di partenza del testo per la lettura delle informazioni di identificazione. È possibile specificare tra 1 e 4096.
Numero di caratteri	Specificare il numero di caratteri da leggere dalla posizione di partenza delle informazioni di identificazione. È possibile specificare tra 1 e 4096.

Registrazioni e impostazioni

Installazione

Configurare le impostazioni necessarie a seconda del Metodo autenticazione e del metodo di scansione utilizzati.

 **Importante:**

Prima di iniziare la configurazione, verificare che l'impostazione dell'ora dello scanner sia corretta.

Se l'impostazione dell'ora non è corretta, viene visualizzato il messaggio di errore "La licenza è scaduta", che potrebbe causare la mancata installazione dello scanner. Inoltre, per utilizzare una funzione di sicurezza come la comunicazione SSL/ TLS o IPsec, è necessario che sia impostata l'ora corretta. È possibile impostare l'ora come segue.

Web Config: scheda **Gestione dispositivo** > **Data e ora** > **Data e ora**.

Pannello di controllo dello scanner: **Impostazioni** > **Impostazioni base** > **Impostazioni data/ora**.

Impostazioni	DB locale	LDAP	DB locale e LDAP
Abilitare l'autenticazione È necessario abilitare l'autenticazione prima di configurarne le impostazioni. "Abilitare l'autenticazione" a pagina 135	✓	✓	✓
Impostazioni di autenticazione Impostare il Metodo autenticazione e come autenticare l'utente. "Impostazioni di autenticazione" a pagina 135	✓	✓	✓
Registrazione le Imp. utente Registrare le impostazioni per ciascun utente. È anche possibile registrare gli utenti in gruppo utilizzando un file CSV. "Registrazione le Imp. utente" a pagina 137	✓	–	✓
Sincronizzazione con il Server LDAP Configurare le impostazioni di sincronizzazione del server LDAP. "Sincronizzazione con il Server LDAP" a pagina 143	–	✓	✓

Impostazioni	DB locale	LDAP	DB locale e LDAP
<p>Impostazione del Server e-mail</p> <p>Configurare le impostazioni del server e-mail. Impostare questa opzione quando si utilizzano funzioni che richiedono impostazioni del server e-mail quali Scan su La mia e-mail.</p> <p>"Configurare il server e-mail" a pagina 147</p>	✓	✓	✓
<p>Configurazione di Scan su La mia cart.</p> <p>Impostare le cartelle di destinazione. Impostare questa opzione quando si utilizza la funzione Scan su La mia cart..</p> <p>"Configurazione di Scan su La mia cart." a pagina 148</p>	✓	✓	✓
<p>Personalizza funzioni One-touch</p> <p>Impostare questa opzione quando si modificano le voci visualizzate sul pannello di controllo dello scanner. È possibile visualizzare sul pannello di controllo solo le icone desiderate o modificare l'ordine delle icone.</p> <p>"Personalizza funzioni One-touch" a pagina 150</p>	✓	✓	✓

Abilitare l'autenticazione

È necessario abilitare l'autenticazione prima di configurarne le impostazioni.

Quando si esegue la configurazione da Web Config:

Selezionare **Attivo (dispositivo/Server LDAP)** dalla scheda **Sicurezza prodotto > Di base > Autenticazione**.

Quando si esegue la configurazione da Epson Device Admin:

Nel modello di configurazione, selezionare **Attivo (dispositivo/Server LDAP)** in **Impostazioni amministratore > Impostazioni autenticaz. > Generali > Autenticazione**.

Nota:

Se si abilita Impostazioni di autenticazione sullo scanner, Impostazione blocco è abilitato anche per il pannello di controllo. Il pannello di controllo non può essere sbloccato quando Impostazioni di autenticazione è abilitato.

Anche se si disabilita Impostazioni di autenticazione, Impostazione blocco rimane abilitato. Per disabilitarlo è possibile configurare le impostazioni dal pannello di controllo o da Web Config.

Informazioni correlate

- ➔ ["Impostare Impostazione blocco dal pannello di controllo" a pagina 86](#)
- ➔ ["Impostare Impostazione blocco da Web Config" a pagina 86](#)

Impostazioni di autenticazione

Impostare il Metodo autenticazione e come autenticare l'utente.

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Sicurezza prodotto > Impostazioni di autenticazione**.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Impostazioni amministratore** > **Impostazioni autenticaz.** > **Impostazioni di autenticazione** dal modello di configurazione.

Voce	Descrizione
Metodo autenticazione	<p>Selezionare il Metodo autenticazione.</p> <ul style="list-style-type: none"> <input type="checkbox"/> DB locale Eeguire l'autenticazione utilizzando le Imp. utente registrate nello scanner. È necessario registrare l'utente nello scanner. <input type="checkbox"/> LDAP Eeguire l'autenticazione utilizzando le informazioni utente del server LDAP sincronizzato con lo scanner. Occorre configurare in anticipo le impostazioni del server LDAP. <input type="checkbox"/> DB locale e LDAP Eeguire l'autenticazione utilizzando le informazioni utente registrate nello scanner o nel server LDAP sincronizzato con lo scanner. È necessario registrare le informazioni utente nello scanner e configurare il server LDAP.
Come autenticare l'utente	<p>Selezionare come autenticare un utente.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Scheda o ID utente e password Utilizzare una scheda di autenticazione per autenticare gli utenti. È inoltre possibile utilizzare un ID utente e una password per l'autenticazione. <input type="checkbox"/> ID utente e password Utilizzare un ID utente e una password per autenticare gli utenti. Non è consentito utilizzare una scheda di autenticazione per eseguire l'autenticazione quando si seleziona questa funzione. <input type="checkbox"/> ID utente Utilizzare solo un ID utente per autenticare gli utenti. Non è necessario impostare una password. <input type="checkbox"/> Scheda o Numero di identità Utilizzare una scheda di autenticazione per autenticare gli utenti. È inoltre possibile usare un Numero di identità. <input type="checkbox"/> Numero di identità Utilizzare solo un numero di ID per autenticare gli utenti.
Consenti all'utente di registrare schede di autenticazione	<p>Abilitarlo per consentire agli utenti di registrare la scheda di autenticazione sul sistema.</p> <p>Se si seleziona LDAP per Metodo autenticazione, non è consentito impostare questa opzione.</p> <p>Per ulteriori informazioni su come gli utenti possono registrare le proprie schede di autenticazione, consultare "Registrazione di una scheda di autenticazione" nella <i>Guida utente</i>.</p>
Cifre minime di Numero di identità	<p>Selezionare il numero minimo di cifre per il numero ID.</p>
Memorizzazione nella cache per utenti autenticati LDAP	<p>Quando si utilizza l'autenticazione da server LDAP, è possibile impostare se utilizzare o meno la memorizzazione nella cache per le informazioni utente.</p>
Usa le informazioni utente nell'autenticazione SMTP	<p>Quando si utilizzano un ID utente e una password per l'autenticazione, è possibile impostare se utilizzare o meno le informazioni utente per l'autenticazione SMTP. Il sistema utilizza l'ultimo ID utente e l'ultima password registrati.</p>
Restrizioni per gli utenti autenticati LDAP	<p>Se viene utilizzato LDAP, è possibile impostare le funzioni disponibili all'utente.</p>

Registrare le Imp. utente

Registrare le Imp. utente utilizzate per l'autenticazione utente. È possibile registrarle con uno dei seguenti metodi.

- Registrare le Imp. utente una per volta (Web Config)
- Registrare più Imp. utente in batch utilizzando un file CSV (Web Config)
- Registrare le Impostazioni utente su più scanner in batch utilizzando il modello di configurazione (Epson Device Admin)

Informazioni correlate

- ➔ [“Registrare le Imp. utente singolarmente \(Web Config\)” a pagina 137](#)
- ➔ [“RegISTRAZIONE di più Imp. utente utilizzando un file CSV \(Web Config\)” a pagina 138](#)
- ➔ [“RegISTRAZIONE di Impostazioni utente su più scanner in batch \(Epson Device Admin\)” a pagina 141](#)

Registrare le Imp. utente singolarmente (Web Config)

Accedere a Web Config e selezionare la scheda **Sicurezza prodotto > Imp. utente > Aggiungi**, quindi immettere le Imp. utente.

Voce	Descrizione
ID utente	Immettere l'ID utente che si desidera utilizzare per l'autenticazione utilizzando tra 1 e 83 byte esprimibili in Unicode (UTF-8). Poiché l'ID utente non distingue tra caratteri maiuscoli e minuscoli, è possibile accedere utilizzando lettere maiuscole o minuscole.
Visualizzazione nome utente	Immettere il nome utente visualizzato nel pannello di controllo dello scanner utilizzando un massimo di 32 caratteri esprimibili in Unicode (UTF-16). È possibile lasciare questo campo vuoto.
Password	Immettere la password che si desidera utilizzare per l'autenticazione utilizzando un massimo di 32 caratteri ASCII. La password distingue maiuscole e minuscole. Lasciare questo campo vuoto se si seleziona ID utente per Come autenticare l'utente .
ID scheda di autenticazione	Immettere l'ID della scheda di autenticazione utilizzando un massimo di 116 caratteri ASCII. È possibile lasciare questo campo vuoto. Quando si seleziona Consenti all'utente di registrare schede di autenticazione per Impostazioni di autenticazione , viene applicato il risultato registrato dagli utenti.
Numero di identità	Questa voce viene visualizzata quando si seleziona Scheda o Numero di identità o Numero di identità in Impostazioni di autenticazione > Come autenticare l'utente . Inserire un numero che rientri nel numero impostato in Impostazioni di autenticazione > Cifre minime di Numero di identità e abbia un massimo di 8 cifre.
Genera automaticamente	Questa voce viene visualizzata quando si seleziona Scheda o Numero di identità o Numero di identità in Impostazioni di autenticazione > Come autenticare l'utente . Fare clic per generare automaticamente un numero ID con lo stesso numero di cifre selezionate in Cifre minime di Numero di identità .

Voce	Descrizione
Reparto	Immettere il nome del dipartimento e altri dati che identifichino l'utente utilizzando un massimo di 40 caratteri esprimibili in Unicode (UTF-16). È possibile lasciare questo campo vuoto.
Indirizzo e-mail	Immettere l'indirizzo e-mail dell'utente utilizzando un massimo di 200 caratteri in ASCII. Viene utilizzato come destinazione per Scan su La mia e-mail . È possibile lasciare questo campo vuoto.
Scan su La mia cart.	Impostare le destinazioni di salvataggio singolarmente quando si seleziona Individuale in Scan su La mia cart. > Tipo impostazioni . Per maggiori informazioni su ogni voce di impostazione, vedere di seguito. "Configurazione di Scan su La mia cart." a pagina 148
Limiti	È possibile limitare le funzioni per ogni utente. Selezionare la funzione di cui si consente l'utilizzo.
Preimpost.	È possibile impostare fino a cinque predefiniti disponibili solo per l'utente selezionato dai Preimpost. registrati nello scanner. <input type="checkbox"/> I Preimpost. assegnati a un utente possono essere utilizzati esclusivamente da tale utente. I Preimpost. che non sono stati assegnati a un utente specifico possono essere utilizzati da tutti gli utenti. <input type="checkbox"/> Se un utente ha una sola serie di Preimpost., verrà caricata automaticamente dopo l'autenticazione. Se sono disponibili più Preimpost., sarà visualizzato un elenco di Preimpost. dopo l'autenticazione. <input type="checkbox"/> Non è possibile creare o visualizzare Preimpost. che utilizzano funzioni limitate in Limiti .

Registrazione di più Imp. utente utilizzando un file CSV (Web Config)

Inserire le impostazioni per ogni utente in un file CSV e registrarle in batch.

Creazione di un file CSV

Creare un file CSV per importare le Imp. utente.

Nota:

Se si registra una o più serie di Imp. utente in anticipo e successivamente si esporta un file formattato (file CSV), è possibile utilizzare l'impostazione registrata come riferimento per l'inserimento delle voci di impostazione.

1. Accedere a Web Config e selezionare la scheda **Sicurezza prodotto** > **Imp. utente**.
2. Fare clic su **Esporta**.
3. Selezionare un formato file per **Formato file**.
Selezionarlo facendo riferimento a quanto segue.

Voce	Descrizione
CSV UTF-16 (con valori delimitati da tabulazioni)	Selezionare quando si modifica il file tramite Microsoft Excel. Ogni parametro è racchiuso tra “[]” (parentesi). Immettere i parametri fra “[]”. Quando si aggiorna il file, si consiglia di sovrascriverlo. Se si salva nuovamente il file, selezionare testo Unicode (*.txt) per il formato del file.
CSV UTF-8 (con valori delimitati da virgole)	Selezionare quando si modifica il file tramite editor di testo o macro senza Microsoft Excel.
CSV UTF-8 (con valori delimitati da punto e virgola)	

- Fare clic su **Esporta**.
- Modificare e salvare il file CSV in un foglio di calcolo come Microsoft Excel o un editor di testo.



Importante:

Quando si modifica il file, non modificare le informazioni di codifica e di intestazione.

Voci di impostazione del file CSV

Voce	Impostazioni e descrizione
UserID	Immettere l’ID utente per l’autenticazione utilizzando tra 1 e 83 byte in Unicode.
UserName	Immettere il nome utente visualizzato sul pannello di controllo dello scanner utilizzando un massimo di 32 caratteri in Unicode. È possibile lasciare questo campo vuoto.
Password	Immettere la password per l’autenticazione utilizzando un massimo di 32 caratteri ASCII. Durante l’importazione viene utilizzata come password al posto di EncPassword . Lasciare questo campo vuoto se si seleziona ID utente per Come autenticare l’utente . Durante l’esportazione, è sempre vuoto.
AuthenticationCardID	Impostare il risultato della lettura della scheda di autenticazione. Quando si seleziona Consenti all’utente di registrare schede di autenticazione in Impostazioni di autenticazione , viene applicato il risultato registrato dagli utenti. Immettere un massimo di 116 caratteri ASCII. È possibile lasciare questo campo vuoto.
IDNumber	Questa voce viene visualizzata quando si seleziona Scheda o Numero di identità o Numero di identità in Impostazioni di autenticazione > Come autenticare l’utente . Inserire un numero che rientri nel numero impostato in Impostazioni di autenticazione > Cifre minime di Numero di identità e abbia un massimo di 8 cifre. Un numero di ID non può essere duplicato. Se è duplicato, si verrà avvisati dell’errore durante l’importazione del file. Se lasciato vuoto, viene automaticamente assegnato un numero.

Voce	Impostazioni e descrizione
Department	Immettere il nome del reparto in modo arbitrario per distinguere gli utenti. Immettere un massimo di 40 caratteri in Unicode. È possibile lasciare questo campo vuoto.
MailAddress	Impostare l'indirizzo e-mail per gli utenti. Viene utilizzato come destinazione per Scan su La mia e-mail . È possibile utilizzare A-Z, a-z, 0-9, !#'%&*+-. /=?^_{}~@. Inserirne fino a 200 caratteri. Non è consentito utilizzare "," (virgola) come primo carattere. È possibile lasciare questo campo vuoto.
FolderProtocol	Impostare il tipo della funzione Scan su La mia cart.. Cartella di rete/FTP (SMB): 0, FTP: 1
FolderPath	Impostare la destinazione di salvataggio per la funzione Scan su La mia cart..
FolderUserName	Impostare il nome utente per la funzione Scan su La mia cart..
FolderPassword	Impostare una password per autenticare la cartella di destinazione per la funzione Scan su La mia cart. in 32 caratteri ASCII. Durante l'importazione viene utilizzata come password al posto di EncPassword . Durante l'esportazione, è sempre vuoto.
FtpPassive	Impostare la modalità di connessione per il server FTP quando si seleziona FTP come Tipo per la funzione Scan su La mia cart.. Modalità attiva: 0, Modalità passiva: 1
FtpPort	Impostare il numero di porta per inviare dati di scansione al server FTP da 0 a 65535 quando si seleziona FTP come Tipo per la funzione Scan su La mia cart..
ScanToMemory	Impostare le restrizioni per Scan su unità USB.. Non consentito: 0, consentito: 1
ScanToMail	Impostare le restrizioni per Scansione su e-mail. È possibile impostare Scan su La mia e-mail solo quando Scansione su e-mail è abilitato. Non consentito: 0, consentito: 1
ScanToFolder	Impostare le restrizioni per Scansione su cartella rete/FTP. È possibile impostare Scan su La mia cart. solo quando Scansione su cartella rete/FTP è abilitato. Non consentito: 0, consentito: 1
ScanToCloud	Impostare le restrizioni per Scansione su Cloud. Non consentito: 0, consentito: 1
ScanToComputer	Impostare le restrizioni per Scansione su computer. Non consentito: 0, consentito: 1
PresetIndex	Impostare i Preimpost. da associare all'utente. È possibile impostare fino a cinque numeri di registrazione di Preimpost. separati da virgole.

Voce	Impostazioni e descrizione
EncPassword	<p>Quando si esportano le impostazioni utente, il parametro impostato per Password è crittografato, quindi il valore viene codificato da BASE64 ed emesso.</p> <p>Quando si importa con la nuova password per Password, questo valore è ignorato.</p> <p>Se Password è vuoto, viene utilizzato questo valore e la password rimane com'era prima dell'esportazione.</p>
EncFolderPassword	<p>Durante l'esportazione il parametro impostato per FolderPassword è crittografato, quindi il valore viene codificato da BASE64 ed emesso.</p> <p>Quando si importa con la nuova password per FolderPassword, questo valore è ignorato.</p> <p>Se FolderPassword è vuoto, viene utilizzato questo valore e la password rimane com'era prima dell'esportazione.</p>

Importare un file CSV

1. Accedere a Web Config e selezionare la scheda **Sicurezza prodotto** > **Imp. utente**.
2. Fare clic su **Importa**.
3. Selezionare il file che si desidera importare.
4. Fare clic su **Importa**.
5. Dopo aver controllato le informazioni visualizzate, fare clic su **OK**.

Registrazione di Impostazioni utente su più scanner in batch (Epson Device Admin)

È possibile registrare le Impostazioni utente utilizzate in DB locale in batch mediante un server LDAP o un file CSV/ENE.

Nota:

*Un file ENE è un file binario fornito da Epson che crittografa e salva le informazioni relative ai **Contatti**, come informazioni personali, e le Imp. utente. Può essere esportato da Epson Device Admin ed è possibile impostare una password. È utile quando si desiderano importare le Imp. utente da un file di backup.*

Importazione da file CSV/ENE

1. Selezionare **Impostazioni amministratore** > **Impostazioni autenticaz.** > **Impostazioni utente** dal modello di configurazione.
2. Fare clic su **Importa**.
3. Selezionare **File CSV o ENE da Importa sorgente**.
4. Fare clic su **Sfoggia**.
Viene visualizzata la schermata di selezione del file.

5. Selezionare il file che si desidera importare per aprirlo.
6. Selezionare un metodo di importazione.
 - Sovrascrivi e aggiungi: sovrascrive se esiste lo stesso ID utente; aggiunge un nuovo ID se non esiste.
 - Sostituisci tutto: sostituisce tutto con le impostazioni utente che si desidera importare.
7. Fare clic su **Importa**.

Viene visualizzata la schermata di conferma delle impostazioni.
8. Fare clic su **OK**.

Viene visualizzato il risultato di validazione.

Nota:

 - Se il numero di impostazioni utente importate supera il numero massimo, un messaggio richiederà di eliminare alcune impostazioni utente. Eliminare eventuali impostazioni utente in eccesso prima dell'importazione.
 - Selezionare le impostazioni utente che si desidera eliminare prima dell'importazione, quindi fare clic su **Elimina**.
9. Fare clic su **Importa**.

Le impostazioni utente vengono importate nel modello di configurazione.

Importazione dal server LDAP

1. Selezionare **Impostazioni amministratore > Impostazioni autenticaz. > Impostazioni utente** dal modello di configurazione.
2. Fare clic su **Importa**.
3. Selezionare **LDAP** da **Importa sorgente**.
4. Fare clic su **Impostazioni**.

Vengono visualizzate le impostazioni del **Server LDAP**.

Nota:

Questa impostazione del server LDAP ha lo scopo di importare le impostazioni utente dal server LDAP. Le impostazioni utente importate (copiate) vengono utilizzate per l'autenticazione degli utenti utilizzando direttamente lo scanner.

*Se invece si seleziona **LDAP** o **DB e LDAP locale** come metodo di autenticazione, gli utenti vengono autenticati comunicando con il server LDAP.*
5. Impostare ciascuna voce.

Quando si importano le impostazioni utente da un server LDAP, è possibile configurare le seguenti impostazioni oltre alle impostazioni LDAP.

Per ulteriori voci, vedere le Informazioni correlate.

Voce		Descrizione
Impostazioni server LDAP	Tipo server LDAP	Consente di selezionare il tipo di server LDAP.

Voce		Descrizione	
Impostazioni di ricerca	Filtro di ricerca	È possibile impostare il testo utilizzato per il filtro di ricerca LDAP. Selezionare Personal. per modificare il testo di ricerca.	
	Opzioni	Tipo	È possibile impostare il tipo di destinazione di salvataggio per Esegui scansione nella mia cartella.
		Modo connessione	Quando Tipo è impostato su FTP , è possibile impostare la modalità di connessione FTP.
		Numero porta	Quando Tipo è impostato su FTP , è possibile impostare il numero di porta che si desidera utilizzare.

6. Effettuare il test di connessione secondo necessità facendo clic su **Test connessione**.
Consente di acquisire e visualizzare 10 impostazioni utente dal server LDAP.
7. Fare clic su **OK**.
8. Selezionare un metodo di importazione.
 - Sovrascrivi e aggiungi: sovrascrive se esiste lo stesso ID utente; aggiunge un nuovo ID se non esiste.
 - Sostituisci tutto: sostituisce tutto con le impostazioni utente che si desidera importare.
9. Fare clic su **Importa**.
Viene visualizzata la schermata di conferma delle impostazioni.
10. Fare clic su **OK**.
Viene visualizzato il risultato di validazione.
11. Fare clic su **Importa**.
Le impostazioni utente vengono importate nel modello di configurazione.

Informazioni correlate

- ➔ [“Configurazione di un server LDAP” a pagina 144](#)
- ➔ [“Configurazione delle impostazioni di ricerca del server LDAP” a pagina 145](#)

Sincronizzazione con il Server LDAP

Configurare le impostazioni del Server LDAP per lo scanner.

Configurare le impostazioni sia per il server primario che per il server secondario in base alle esigenze.

Nota:

*Le impostazioni del Server LDAP sono condivise con **Contatti**.*

Servizi disponibili

Sono supportati i seguenti servizi di directory.

Nome del servizio	Versione
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Configurazione di un server LDAP

Per utilizzare un server LDAP è necessario innanzitutto configurarlo.

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Rete > Server LDAP > Di base (Server primario)** o **Di base (Server secondario)**.

Se si seleziona **Autenticazione Kerberos** come **Metodo autenticazione**, selezionare **Rete > Impostazioni Kerberos** per configurare le impostazioni per Kerberos.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Rete > Server LDAP > Impostazioni server (Server principale)** o **Impostazioni server (Server secondario)** dal modello di configurazione.

Se si seleziona **Autenticazione Kerberos** come **Metodo autenticazione**, selezionare **Rete — Protezione > Impostazioni Kerberos** per configurare le impostazioni per Kerberos.

Voce	Impostazioni e descrizione
Usa server LDAP	Selezionare Usa o Non utilizzare .
Indirizzo server LDAP	Immettere l'indirizzo del server LDAP. Immettere tra 1 e 255 caratteri in formato IPv4, IPv6 o FQDN. Per il formato FQDN è possibile utilizzare caratteri alfanumerici in ASCII (0x20–0x7E) e trattini, tranne per l'inizio e la fine dell'indirizzo.
Numero porta server LDAP (Numero porta)	Immettere un numero di porta del server LDAP tra 1 e 65535.
Connessione protetta	Specificare il metodo di autenticazione per l'accesso dello scanner al server LDAP.
Convalida certificato	Il certificato del server LDAP viene validato quando questa opzione è abilitata. Sugeriamo di impostarlo su Abilita . Per effettuare la configurazione, il Certificato CA deve essere importato sullo scanner.
Timeout di ricerca (sec)	Impostare il lasso di tempo di ricerca prima della scadenza tra 5 e 300 secondi.
Metodo autenticazione	Selezionare il metodo di autenticazione. Se si seleziona Autenticazione Kerberos , configurare in anticipo le impostazioni per Kerberos. Per eseguire Autenticazione Kerberos, è necessario il seguente ambiente. <input type="checkbox"/> Lo scanner e il server DNS possono comunicare. <input type="checkbox"/> L'ora dello scanner e quelle del server KDC e del server richiesto per l'autenticazione (server LDAP, server SMTP, file server) vengono sincronizzate. <input type="checkbox"/> Quando il server di servizio viene assegnato come indirizzo IP, l'FQDN per il server di servizio viene registrato nella zona di ricerca inversa del server DNS.
Ambiente Kerberos da utilizzare	Se si sceglie Autenticazione Kerberos come Metodo autenticazione , selezionare il dominio Kerberos che si desidera utilizzare.

Voce	Impostazioni e descrizione
DN amministratore / Nome utente	Immettere il nome utente del server LDAP con un massimo di 128 caratteri in Unicode (UTF-8). Non è possibile utilizzare caratteri di controllo, per esempio 0x00–0x1F e 0x7F. Questa impostazione non viene utilizzata quando è selezionato Autenticazione anonima come Metodo autenticazione . Se non si desidera specificare questa voce, lasciare il campo vuoto.
Password	Immettere la password del server di autenticazione LDAP con un massimo di 128 caratteri in Unicode (UTF-8). Non è possibile utilizzare caratteri di controllo, per esempio 0x00–0x1F e 0x7F. Questa impostazione non viene utilizzata quando è selezionato Autenticazione anonima come Metodo autenticazione . Se non si desidera specificare questa voce, lasciare il campo vuoto.

Impostazioni Kerberos

Se è stato selezionato **Autenticazione Kerberos** in **Metodo autenticazione**, è necessario configurare le impostazioni Kerberos. È possibile registrare fino a 10 impostazioni Kerberos.

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Rete** > **Impostazioni Kerberos**.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Rete** > **Protezione** > **Impostazioni Kerberos** dal modello di configurazione.

Voce	Impostazioni e descrizione
Ambiente (dominio)	Immettere il dominio di autenticazione Kerberos con un massimo di 255 caratteri in ASCII (0x20–0x7E). Se non si desidera registrare questa voce, lasciare il campo vuoto.
Indirizzo KDC	Immettere l'indirizzo del server di autenticazione Kerberos. Inserire un massimo di 255 caratteri in formato IPv4, IPv6 o FQDN. Se non si desidera registrare questa voce, lasciare il campo vuoto.
Numero porta (Kerberos)	Immettere un numero di porta del server Kerberos tra 1 e 65535.

Configurazione delle impostazioni di ricerca del server LDAP

Consente di impostare gli attributi di ricerca per le impostazioni utente.

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Rete** > **Server LDAP** > **Impostazioni di ricerca (autenticazione)**.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Impostazioni amministratore** > **Impostazioni autenticaz.** > **Server LDAP** > **Impostazioni di ricerca (Autenticazione)** dal modello di configurazione.

Voce	Impostazioni e descrizione
Base ricerca (nome distinto)	Specificare la posizione di partenza quando si effettua la ricerca delle informazioni utente dal server LDAP. Immettere tra 0 e 128 caratteri in Unicode (UTF-8). Se non si effettua la ricerca con un attributo specifico, lasciare il campo vuoto. Esempio di directory del server locale: dc=server,dc=locale

Voce	Impostazioni e descrizione
Attributo ID utente	Specificare il nome di attributo da visualizzare quando si ricerca per numero di ID. Immettere tra 1 e 255 caratteri in ASCII. Il primo carattere dovrebbe essere a-z o A-Z. Esempio: cn, uid
Attributo visualizzazione nome utente	Specificare il nome di attributo da visualizzare come nome utente. Immettere tra 0 e 255 caratteri in ASCII. Il primo carattere dovrebbe essere a-z o A-Z. È possibile lasciarlo vuoto. Esempio: cn, name
Attributo ID scheda di autenticazione	Specificare il nome di attributo da visualizzare come ID scheda di autenticazione. Immettere tra 0 e 255 caratteri in ASCII. Il primo carattere dovrebbe essere a-z o A-Z. È possibile lasciarlo vuoto. Esempio: cn, sn
Attributo numero ID	Specificare il nome di attributo da visualizzare quando si ricerca per numero di ID. Immettere tra 1 e 255 caratteri in ASCII. Il primo carattere dovrebbe essere a-z o A-Z. Esempio: cn, id
Attributo reparto	Specificare il nome di attributo da visualizzare come nome reparto. Immettere tra 0 e 255 caratteri in ASCII. Il primo carattere dovrebbe essere a-z o A-Z. È possibile lasciarlo vuoto. Esempio: ou, ou-cl
Attributo indirizzo e-mail	Specificare il nome di attributo da visualizzare quando si ricercano i gli indirizzi e-mail. Immettere tra 1 e 255 caratteri in ASCII. Il primo carattere dovrebbe essere a-z o A-Z. Esempio: mail
Salva in Attributo	Specificare il nome dell'attributo che fa riferimento alla destinazione per Eseguì scansione nella mia cartella. Immettere tra 0 e 255 caratteri in ASCII. Esempio: homeDirectory

Verifica della connessione al server LDAP

Esegui il test di connessione al server LDAP utilizzando il parametro impostato in **Server LDAP > Imp. di ricerca**.

1. Accedere a Web Config e selezionare la scheda **Rete > Server LDAP > Test di conn.**
2. Selezionare **Avvia**.

Il test di connessione viene avviato. Dopo il test, viene visualizzato il report di controllo.

Riferimenti per il test di connessione al server LDAP

Messaggi	Descrizione
Test di connessione riuscito.	Questo messaggio appare quando la connessione con il server avviene correttamente.

Messaggi	Descrizione
Test di conn. non riuscito. Controllare le imp.	Questo messaggio appare per le seguenti ragioni: <ul style="list-style-type: none"> <input type="checkbox"/> L'indirizzo o il numero di porta del server LDAP non è corretto. <input type="checkbox"/> Si è verificata una scadenza. <input type="checkbox"/> Non utilizzare è selezionato come Usa server LDAP. <input type="checkbox"/> Se Autenticazione Kerberos è selezionata come Metodo autenticazione, le impostazioni come Ambiente (dominio), Indirizzo KDC e Numero porta (Kerberos) sono errate.
Test di conn. non riuscito. Verificare la Data e ora sul prodotto o sul server.	Questo messaggio compare quando non è possibile stabilire una connessione a causa della mancata corrispondenza tra le impostazioni di orario dello scanner e del server LDAP.
Autenticazione non riuscita. Controllare le imp.	Questo messaggio appare per le seguenti ragioni: <ul style="list-style-type: none"> <input type="checkbox"/> Nome utente e/o Password sono errati. <input type="checkbox"/> Se Autenticazione Kerberos è selezionata come Metodo autenticazione, la data e l'ora potrebbero non essere configurate.
Impossibile accedere al prodotto fino al termine dell'elaborazione.	Questo messaggio appare quando lo scanner è occupato.

Configurare il server e-mail

Quando si utilizza **Scan su La mia e-mail**, impostare il server e-mail.

Nota:

*È possibile impostare **Scan su La mia e-mail** solo quando **Scansione su e-mail** è abilitato.*

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Rete > Server e-mail > Di base**.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Comune > Server email > Impostazioni server posta** dal modello di configurazione.

Voce	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	Il server e-mail deve supportare l'autenticazione SMTP.
	POP prima di SMTP	Se si seleziona questa voce, impostare un server POP3.
Account autenticato	Se si seleziona AUT. SMTP o POP prima di SMTP come Metodo autenticazione , inserire il nome dell'account autenticato. Immettere tra 0 e 255 caratteri in ASCII (0x20-0x7E).	
Password autenticata	Se si seleziona AUT. SMTP o POP prima di SMTP come Metodo autenticazione , inserire la password autenticata. Immettere tra 0 e 20 caratteri in ASCII (0x20-0x7E).	
Indirizzo e-mail mittente	Immettere l'indirizzo email del mittente. Immettere tra 0 e 255 caratteri in ASCII (0x20-0x7E) ad eccezione di : () < > [] ; ¥. Il primo carattere non può essere un punto "".	

Voce	Impostazioni e descrizione	
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.	
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	Quando questa opzione è abilitata, il certificato viene convalidato. Sugeriamo di impostarlo su Abilita .	
Indirizzo server POP3	Se si seleziona POP prima di SMTP come Metodo autenticazione , immettere l'indirizzo del server POP3. È possibile immettere tra 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 , specificare il numero di porta. Immettere un numero tra 1 e 65535.	

Configurazione di Scan su La mia cart.

Consente di salvare le immagini acquisite nella cartella assegnata a ciascun utente. È possibile impostare le voci seguenti come una cartella dedicata.

Nota:

È possibile impostare *Esegui scansione nella mia cartella* solo quando *Scansione su cartella rete/FTP* è abilitato.

Salva in impostazioni	Metodo autenticazione	Posizione dell'impostazione del percorso della cartella
Specificare una cartella di rete per le Impostazioni di autenticazione per creare automaticamente una cartella personale sotto la cartella specificata utilizzando il nome dell'ID utente.	<input type="checkbox"/> DB locale <input type="checkbox"/> LDAP <input type="checkbox"/> DB locale e LDAP	Scanner (impostazioni Scan su La mia cart.)
Assegnare diverse cartelle di rete singole a ciascun utente.	DB locale	Scanner (Imp. utente)
	LDAP	Attributi LDAP
	DB locale e LDAP	Scanner (Imp. utente) o attributi LDAP

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Sicurezza prodotto** > **Scansione su cartella rete/FTP**.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Impostazioni amministratore** > **Impostazioni autenticaz.** > **Scansione su cartella rete/FTP** > **Scan su La mia cart.** dal modello di configurazione.

Voce		Descrizione
Salva in Impostazione	Tipo impostazioni	<p><input type="checkbox"/> Condivise: Crea automaticamente una cartella denominata con l’ID utente sotto il percorso della cartella o l’URL specificato in Salva con nome e salva le immagini scansionate in questa cartella.</p> <p><input type="checkbox"/> Individuale: Impostare la destinazione di salvataggio per i risultati di scansione per ciascun utente. È possibile impostare gli utenti del DB locale nelle impostazioni utente. Gli utenti LDAP utilizzano la posizione di archiviazione acquisita dagli attributi di ricerca del server LDAP.</p>
	Tipo	<p>Selezionare il protocollo di trasmissione in base alla destinazione di uscita della scansione. Per una cartella di rete: Rete cartella (SMB) Per un server FTP: FTP</p>
	Salva con nome	<p>Specificare il percorso o l’URL del percorso di uscita. Immettere un massimo di 160 caratteri in Unicode (UTF-16).</p>
	Modalità connessione	<p>Impostare quando si seleziona FTP in Tipo. Selezionare una modalità di comunicazione sul server FTP.</p>
	Numero porta	<p>Impostare quando si seleziona FTP in Tipo. Immettere il numero di porta per l’invio dei dati acquisiti ad un server FTP compreso tra 0 e 65535.</p>
Impostazioni di autenticazione	Tipo impostazioni	<p>Impostare questa opzione quando si seleziona Individuale come Tipo impostazioni in Salva in Impostazione. Impostare “Nome utente” e “Password” per accedere alla cartella.</p> <p><input type="checkbox"/> Condivise: Utilizzare un Nome utente e una Password condivisi per tutti gli utenti.</p> <p><input type="checkbox"/> Individuale: Per gli utenti DB locale, impostare Nome utente e Password singolarmente in Impostazioni utente. Gli utenti LDAP non possono essere configurati singolarmente. Nome utente e Password impostati con questa voce vengono utilizzati come batch.</p>
	Nome utente	<p>Immettere il nome utente per accedere alla cartella di destinazione della scansione. Immettere un massimo di 30 caratteri in Unicode (UTF-16). Impostare quando si utilizza un server Condivise o LDAP.</p>
	Password	<p>Inserire la password corrispondente al Nome utente. Immettere un massimo di 20 caratteri in Unicode (UTF-16). Impostare quando si utilizza un server Condivise o LDAP.</p>

Proibire la modifica della destinazione per Scansione su cartella rete/FTP

Voce	Descrizione
Vieta l'immissione manuale della destinazione	Se abilitata, l'utente non può modificare la destinazione predefinita.

Personalizza funzioni One-touch

È possibile visualizzare solo le icone necessarie modificando il layout delle icone visualizzato nella schermata iniziale del pannello di controllo.

Quando si esegue la configurazione da Web Config:

Selezionare la scheda **Sicurezza prodotto** > **Personalizza funzioni One-touch**.

Quando si esegue la configurazione da Epson Device Admin:

Selezionare **Impostazioni amministratore** > **Impostazioni autenticaz.** > **Personalizza funzioni One-touch** dal modello di configurazione.

Nota:

Nei seguenti casi, le icone per le funzioni specificate non vengono visualizzate nella schermata principale.

- Quando si selezionano funzioni non consentite a causa di **Limiti**.*
- Quando l'indirizzo e-mail per un utente che ha effettuato l'accesso non è registrato. (Scan su La mia e-mail)*
- Quando la cartella di destinazione non è impostata. (Scan su La mia cart.)*

Voce	Descrizione
Funzioni massime per schermo	Selezionare il layout delle icone visualizzate sul pannello di controllo. L'immagine cambia in base al layout selezionato.
Schermo(i)	Selezionare il numero di pagine.
Numero	Selezionare le funzioni che si desidera visualizzare per ogni posizione numerata.

Rapporti della Cronologia processi con Epson Device Admin

È possibile creare un rapporto della Cronologia processi per ogni gruppo e utente utilizzando Epson Device Admin. È possibile salvare fino a 3000 istanze di cronologia di utilizzo nello scanner. È possibile creare il rapporto specificando un periodo o impostando una pianificazione periodica.

Per esportare la Cronologia processi in forma di rapporto, selezionare **Opzioni** > **Impostazioni Epson Print Admin Serverless/Autenticazione** > **Gestisci i dispositivi compatibili con Epson Print Admin Serverless/Autenticazione** dal menu della barra multifunzione nella schermata Elenco dispositivi.

Per ulteriori informazioni su come creare un rapporto utente, consultare la documentazione per Epson Device Admin.

Voci che possono essere incluse nel rapporto

È possibile esportare le seguenti voci nel rapporto utente.

Data/ID lavoro/Operazione/ID utente/Reparto/Risultato/Dettagli risultato/Scansione: Tipo di destinazione/
Scansione: Destinazione/Scansione: Formato carta/Scansione: Doppio lato/Scansione: Colore/Scansione: Pagine/
Stampante: Modello/Stampante: Indirizzo IP/Stampante: Numero di serie/Stampante: Reparto/Stampante:
Percorso/Stampante: Commento/Stampante: Nota

Effettuare l'accesso come amministratore dal pannello di controllo

È possibile utilizzare uno dei seguenti metodi per accedere come amministratore dal pannello di controllo dello scanner.

1. Toccare  in alto a destra dello schermo.
 - Quando Impostazioni di autenticazione è abilitato, l'icona viene visualizzata sulla schermata **Benvenuto** (la schermata di standby dell'autenticazione).
 - Quando Impostazioni di autenticazione è disabilitato, l'icona è visualizzata nella schermata Home.
2. Toccare **Sì** quando compare la schermata di conferma.
3. Immettere la password di amministratore.
Viene visualizzato un messaggio di accesso completato, quindi sul pannello di controllo compare la schermata iniziale.

Per uscire, toccare  in alto a destra della schermata Home.

Disabilitazione di Impostazioni di autenticazione

È possibile disabilitare Impostazioni di autenticazione utilizzando Web Config.

Nota:

Le Imp. utente registrate nello scanner verranno salvate anche se Impostazioni di autenticazione è disabilitato. È possibile rimuoverle ripristinando le impostazioni predefinite dello scanner.

1. Accedere a Web Config.
2. Selezionare la scheda **Sicurezza prodotto > Di base > Autenticazione**.
3. Selezionare **DISATTIVA**.
4. Fare clic su **Avanti**.
5. Fare clic su **OK**.

Nota:

Anche se si disabilita Impostazioni di autenticazione, Impostazione blocco rimane abilitato. Per disabilitarlo è possibile configurare le impostazioni dal pannello di controllo o da Web Config.

Informazioni correlate

- ➔ [“Impostare Impostazione blocco dal pannello di controllo” a pagina 86](#)
- ➔ [“Impostare Impostazione blocco da Web Config” a pagina 86](#)

Eliminare le informazioni delle Impostazioni di autenticazione (Ripristina impostaz. predef.)

Per eliminare tutte le informazioni relative a Impostazioni di autenticazione (Lettore di schede, Metodo autenticazione, Imp. utente e così via), ripristinare tutte le impostazioni dello scanner predefinite.

Selezionare **Impostazioni** > **Amministrazione sistema** > **Ripristina impostaz. predef.** > **Tutte le impostazioni** nel pannello di controllo.



Importante:

Verranno eliminati anche tutti i contatti e le altre impostazioni di rete. Le impostazioni eliminate non possono essere ripristinate.

Soluzione dei problemi

Impossibile leggere la scheda di autenticazione

Controllare quanto segue.

- Verificare se il dispositivo di autenticazione sia collegato correttamente allo scanner.
Collegare il dispositivo di autenticazione alla porta USB dell'interfaccia esterna sul retro dello scanner.
- Verificare che il dispositivo di autenticazione e la scheda di autenticazione siano supportati.

Manutenzione

Pulizia esterna dello scanner.	154
Pulizia interna dello scanner.	154
Sostituire il kit manutenzione rulli.	159
Azzerare il numero di scansioni.	164
Risparmio energetico.	164
Trasporto dello scanner.	165
Backup delle impostazioni.	166
Ripristina impostaz. predef..	167
Aggiornamento Applicazioni e Firmware.	168

Pulizia esterna dello scanner

Pulire eventuali macchie sulla struttura esterna con un panno asciutto o un panno inumidito con un detergente delicato e acqua.



Importante:

- Non usare mai alcool, solventi o liquidi corrosivi per pulire lo scanner. Si possono verificare deformazioni o scolorimento.
- Non lasciare che l'acqua penetri all'interno del prodotto. Ciò potrebbe causare un malfunzionamento.
- Non aprire mai l'involucro dello scanner.

1. Premere il pulsante  per spegnere lo scanner.
2. Scollegare l'adattatore CA dallo scanner.
3. Pulire l'involucro esterno con un panno imbevuto con detergente delicato ed acqua.

Nota:

Pulire il touchscreen con un panno morbido e asciutto.

Pulizia interna dello scanner

Dopo aver utilizzato lo scanner per un certo periodo di tempo, i residui di carta e la polvere sul rullo o sulla parte in vetro all'interno dello scanner potrebbero causare problemi di alimentazione della carta o di qualità dell'immagine acquisita. Pulire la parte interna dello scanner ogni 5,000 scansioni.

È possibile verificare l'ultimo numero di scansioni sul pannello di controllo o in Epson Scan 2 Utility.

Se una superficie è macchiata con un materiale difficile da rimuovere, utilizzare un kit di pulizia originale Epson per rimuovere le macchie. Utilizzare una piccola quantità di detergente su un panno da pulizia per rimuovere le macchie.

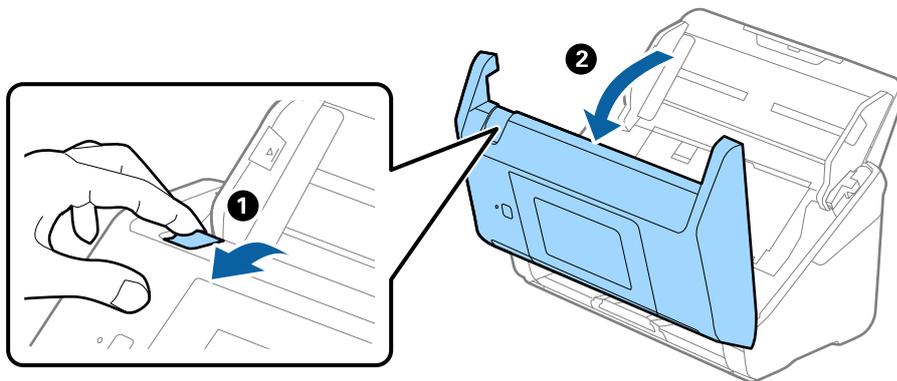


Importante:

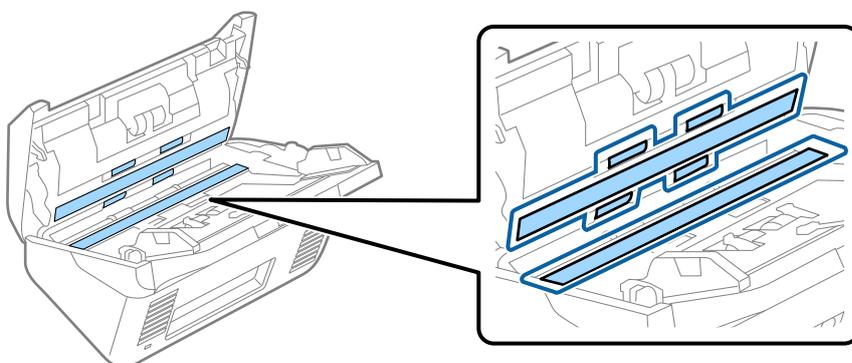
- Non usare mai alcool, solventi o liquidi corrosivi per pulire lo scanner. Si possono verificare deformazioni o scolorimento.
- Non spruzzare liquidi o lubrificanti sullo scanner. Danni all'apparecchiatura o ai circuiti potrebbero compromettere il funzionamento.
- Non aprire mai l'involucro dello scanner.

1. Premere il pulsante  per spegnere lo scanner.
2. Scollegare l'adattatore CA dallo scanner.

3. Tirare la leva e aprire il coperchio dello scanner.



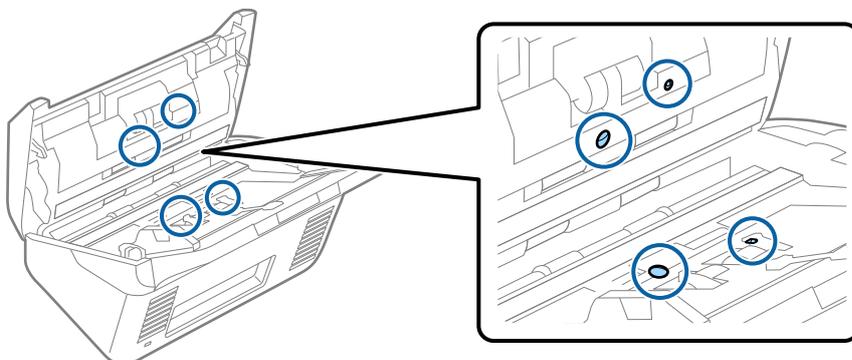
4. Pulire eventuali macchie sul rullo di plastica e sulla superficie di vetro nella parte interna del coperchio dello scanner con un panno morbido o usando il kit di pulizia Epson.



! Importante:

- Non mettere troppa forza sulla superficie del vetro.
- Non utilizzare spazzole o strumenti duri. Eventuali graffi sul vetro possono incidere sulla qualità della scansione.
- Non spruzzare detergente direttamente sulla superficie del piano di lettura.

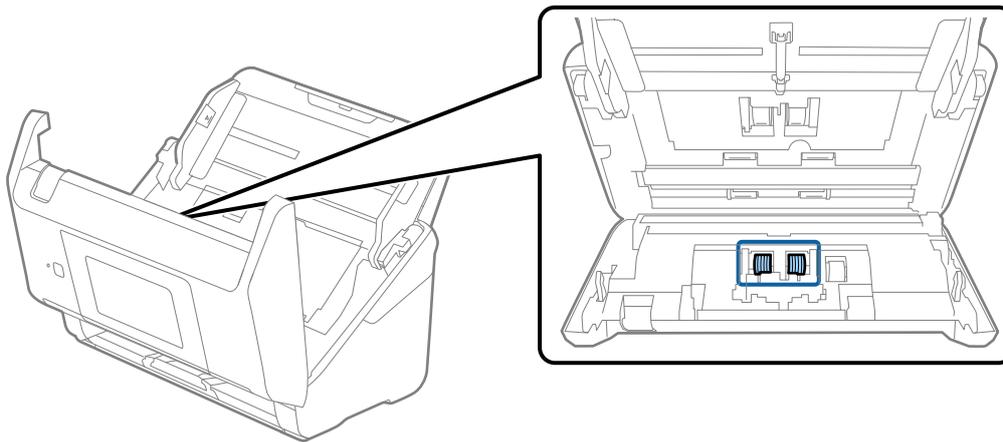
5. Pulire eventuali macchie sui sensori con un batuffolo di cotone.



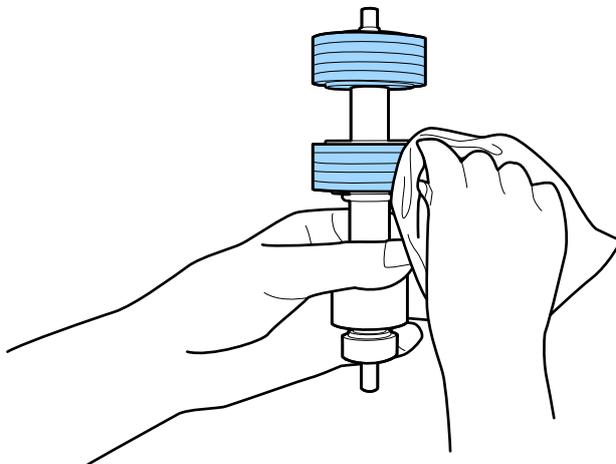
! Importante:

Non usare liquidi come detersivi sul batuffolo di cotone.

6. Aprire il coperchio, quindi rimuovere il rullo di separazione.
Vedere “Sostituzione del Kit di montaggio rullo” per ulteriori dettagli.



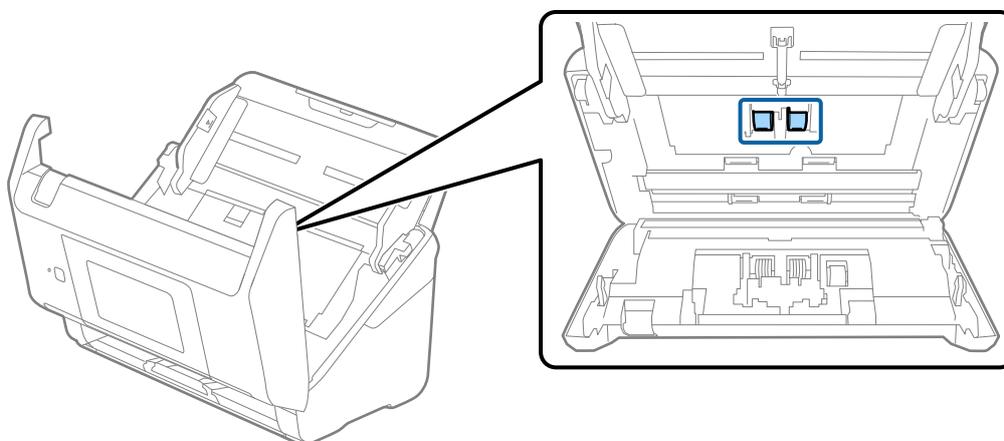
7. Eliminare la polvere o sporcizia sul rullo separatore con un kit di pulizia originale Epson o un panno morbido e umido.



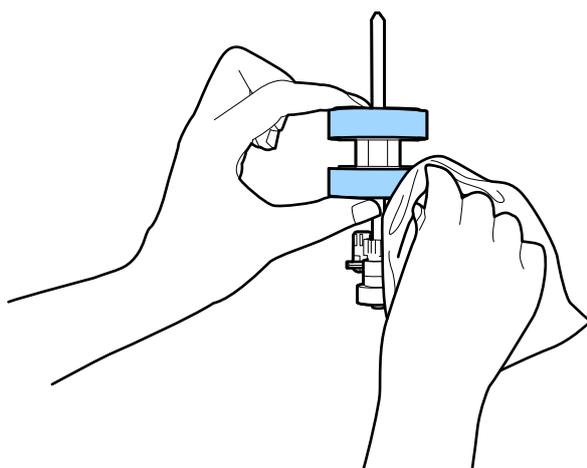
! Importante:

Usare solo un kit di pulizia originale Epson o un panno morbido e umido per pulire il rullo. L'uso di un panno asciutto può danneggiare la superficie del rullo.

8. Aprire il coperchio, quindi rimuovere il rullo di prelievo.
Vedere “Sostituzione del Kit di montaggio rullo” per ulteriori dettagli.



9. Eliminare la polvere o sporcizia sul rullo di prelievo con un kit di pulizia originale Epson o un panno morbido e umido.

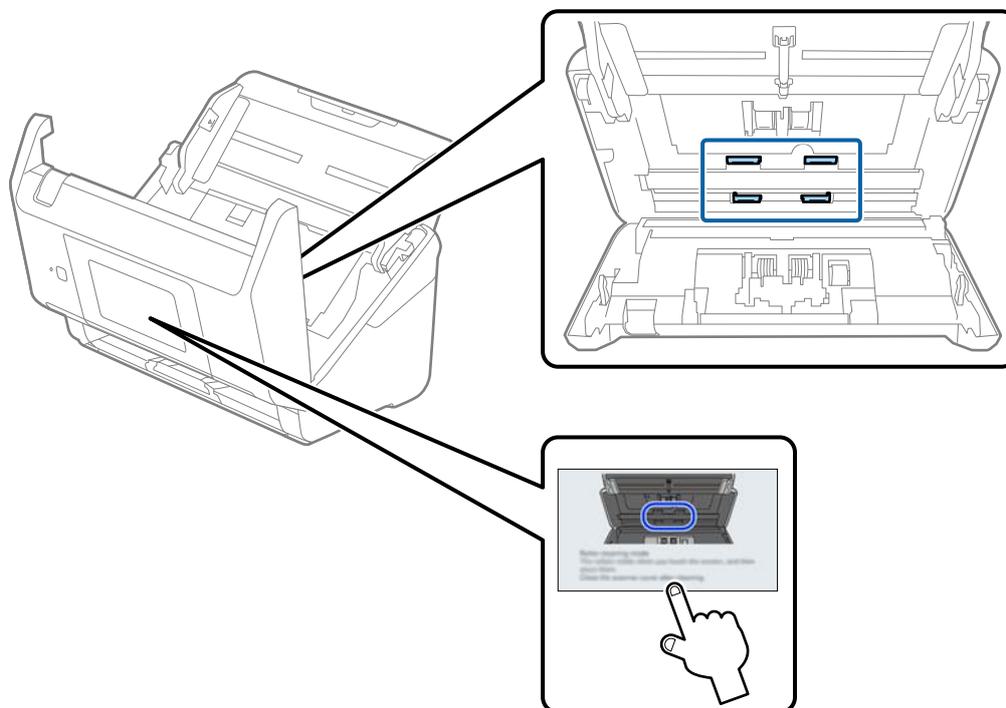


! Importante:

Usare solo un kit di pulizia originale Epson o un panno morbido e umido per pulire il rullo. L'uso di un panno asciutto può danneggiare la superficie del rullo.

10. Chiudere il coperchio dello scanner.
11. Inserire l'adattatore CA, quindi accendere lo scanner.
12. Selezionare **Manutenzione scanner** dalla schermata home.
13. Sulla schermata **Manutenzione scanner**, selezionare **Pulizia del rullo**.
14. Tirare la leva per aprire il coperchio dello scanner.
Lo scanner entra in modalità pulizia rullo.

15. Ruotare lentamente i rulli in basso, toccando un punto qualsiasi del display LCD. Pulire la superficie dei rulli con un kit di pulizia originale Epson o un panno morbido inumidito con acqua. Ripetere finché i rulli non siano puliti.



⚠ Attenzione:

Fare attenzione a non andare con le mani o i capelli nel meccanismo quando si opera sul rullo. Ciò potrebbe causare lesioni.

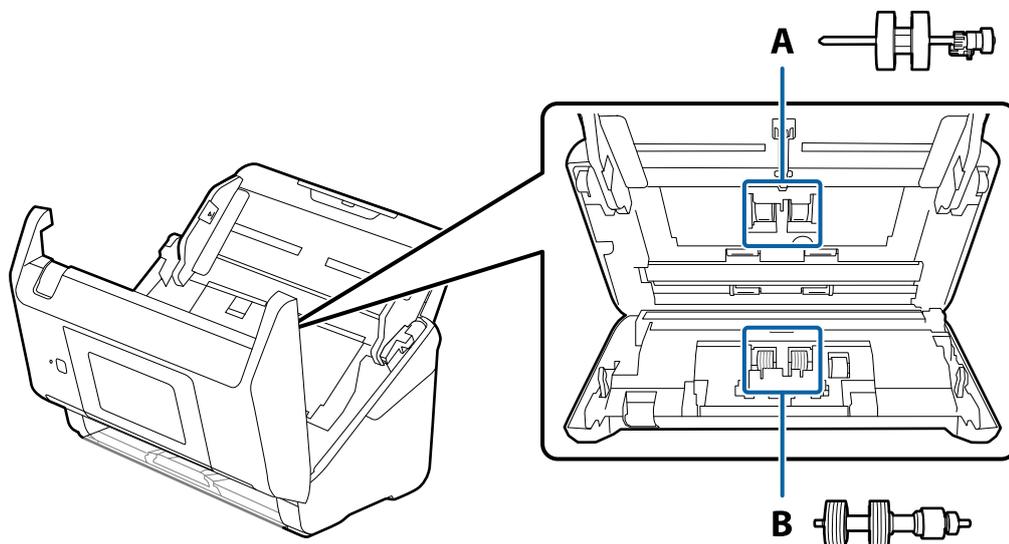
16. Chiudere il coperchio dello scanner.
Lo scanner esce dalla modalità pulizia rullo.

Informazioni correlate

➔ [“Sostituire il kit manutenzione rulli” a pagina 159](#)

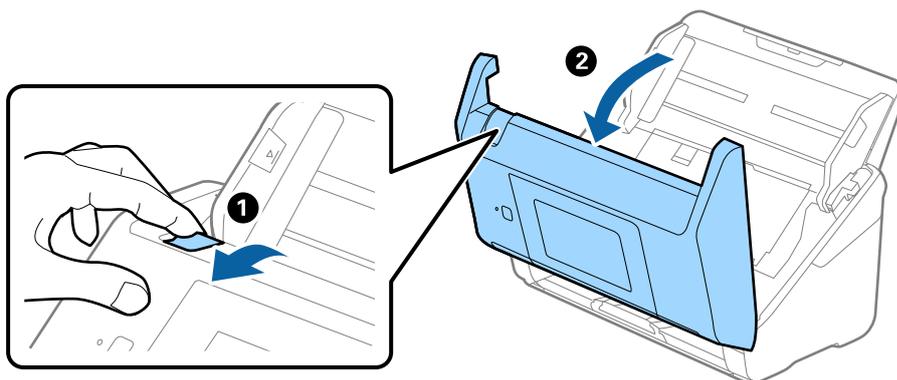
Sostituire il kit manutenzione rulli

Il kit di montaggio rulli (rullo raccogliitore e rullo di separazione) deve essere sostituito quando il numero di scansioni supera il ciclo di vita dei rulli. Quando sul pannello di controllo o sullo schermo del computer viene visualizzato un messaggio di sostituzione, attenersi alla seguente procedura per sostituirlo.

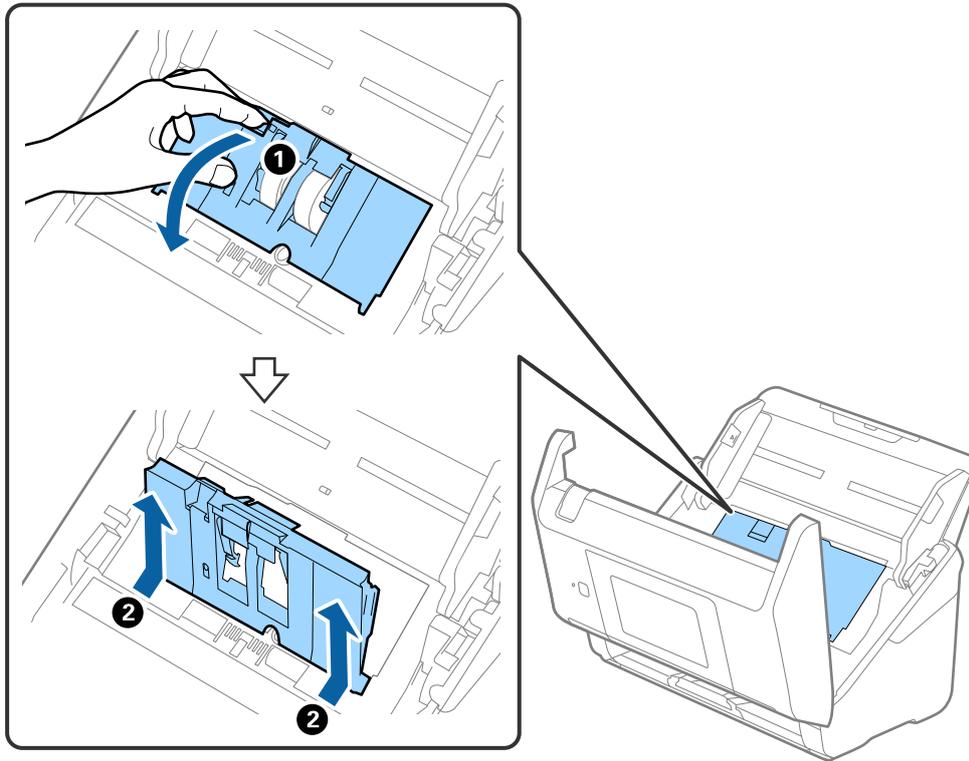


A: rullo raccogliitore, B: rullo di separazione

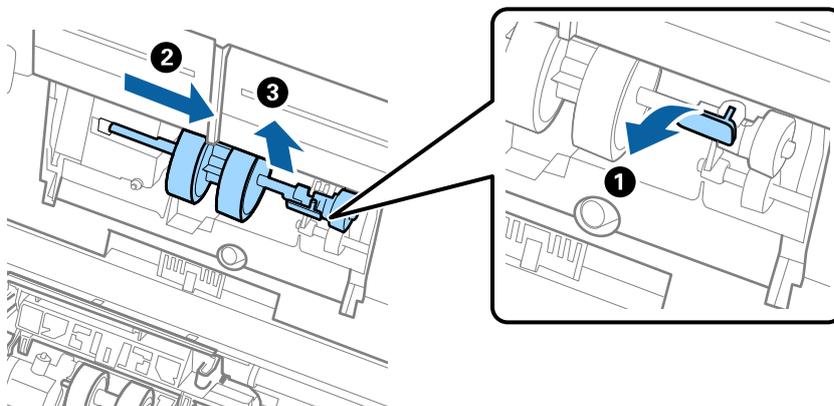
1. Premere il pulsante  per spegnere lo scanner.
2. Scollegare l'adattatore CA dallo scanner.
3. Tirare la leva e aprire il coperchio dello scanner.



4. Aprire il coperchio del rullo raccoglitore, quindi farlo scorrere e rimuoverlo.



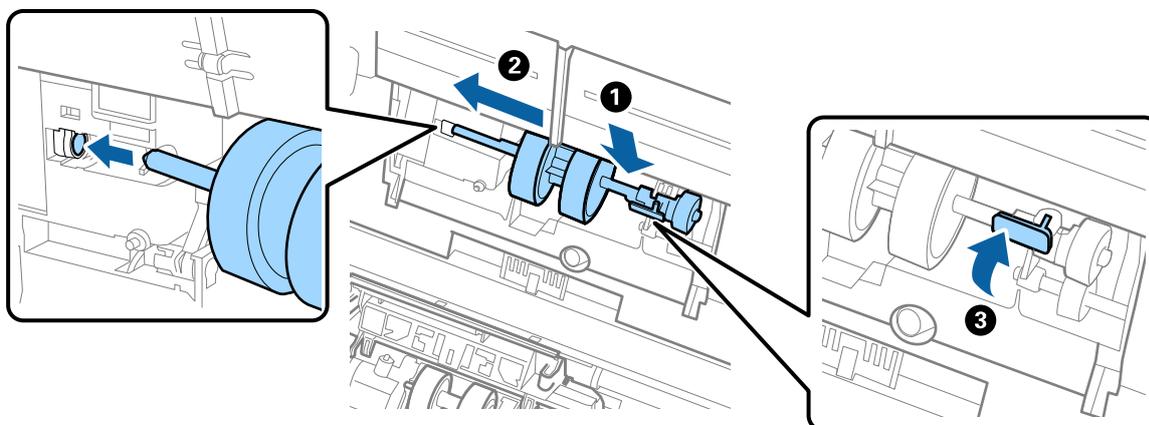
5. Abbassare il dispositivo dell'asse del rullo, e quindi far scorrere e rimuovere i rulli raccoglitori installati.



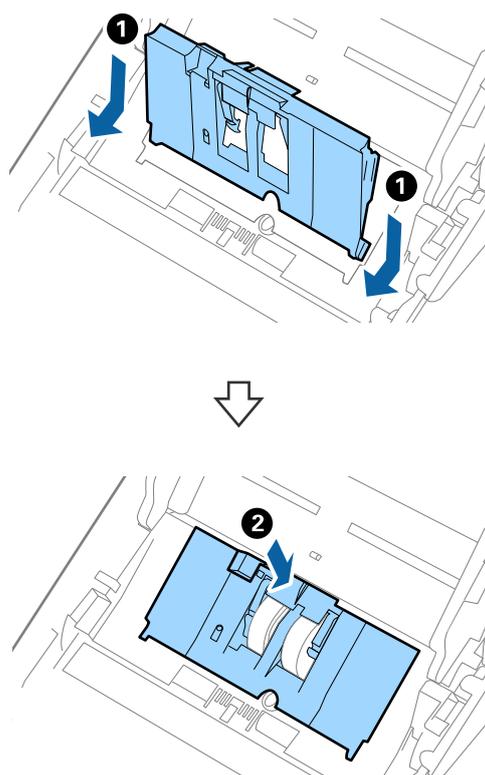
Importante:

Non estrarre il rullo raccoglitore con la forza. Questo potrebbe danneggiare l'interno dello scanner.

6. Tenendo premuto il dispositivo, far scorrere il nuovo rullo raccogliitore verso sinistra e inserirlo nella posizione corretta nello scanner. Premere il dispositivo per fissarlo.

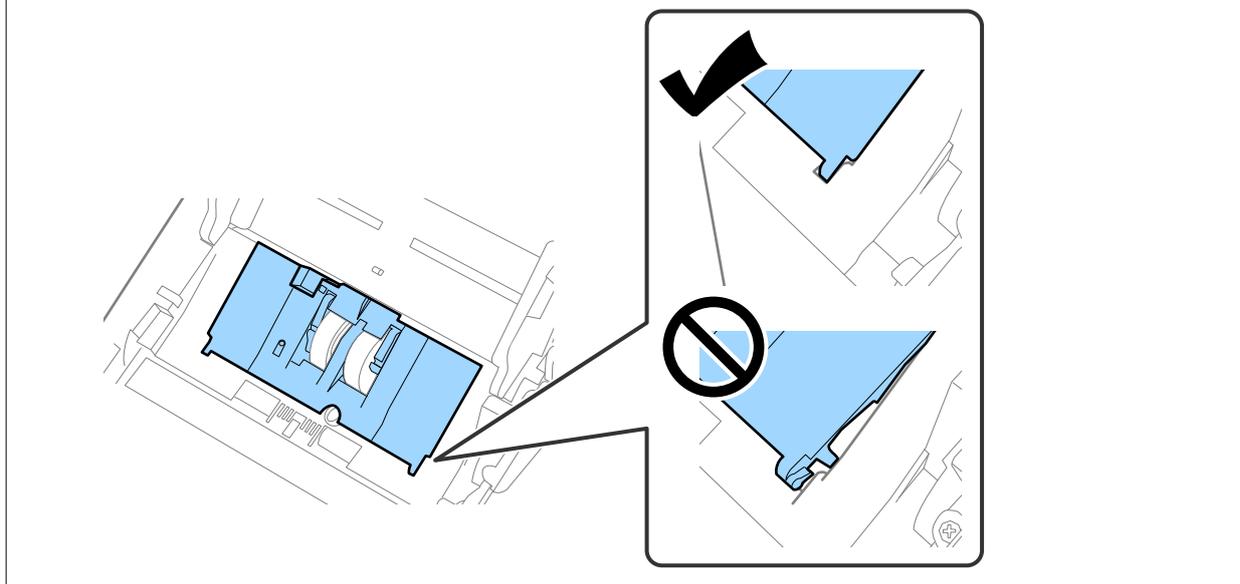


7. Mettere il bordo del coperchio del rullo raccogliitore nella scanalatura e farlo scorrere. Chiudere il coperchio saldamente.

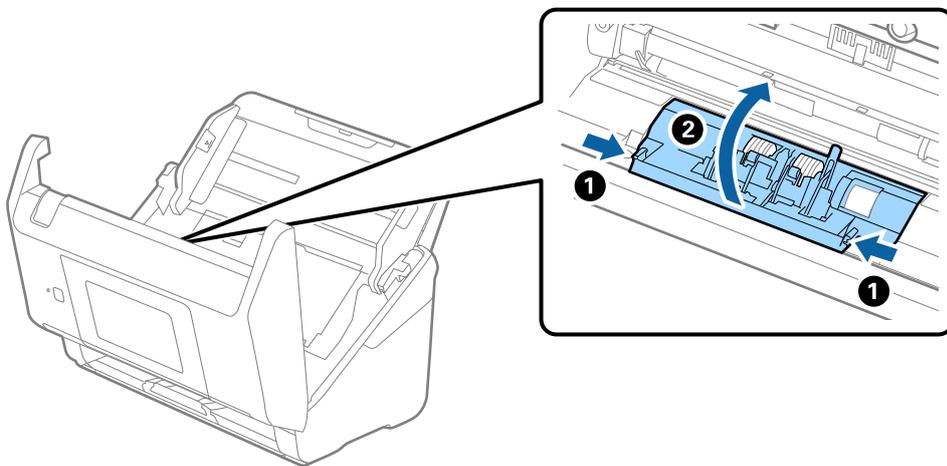


! *Importante:*

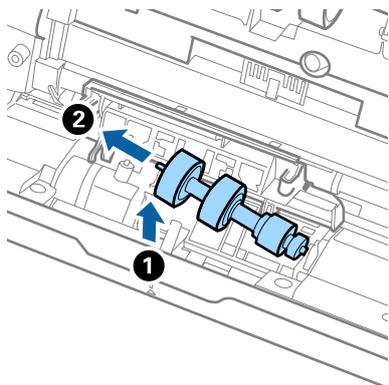
- ❑ Assicurarsi che il coperchio raccoglitore sia chiuso correttamente.
- ❑ Assicurarsi che il coperchio raccoglitore sia installato correttamente se il coperchio è difficile da chiudere.
- ❑ Non installare il coperchio mentre è sollevato.



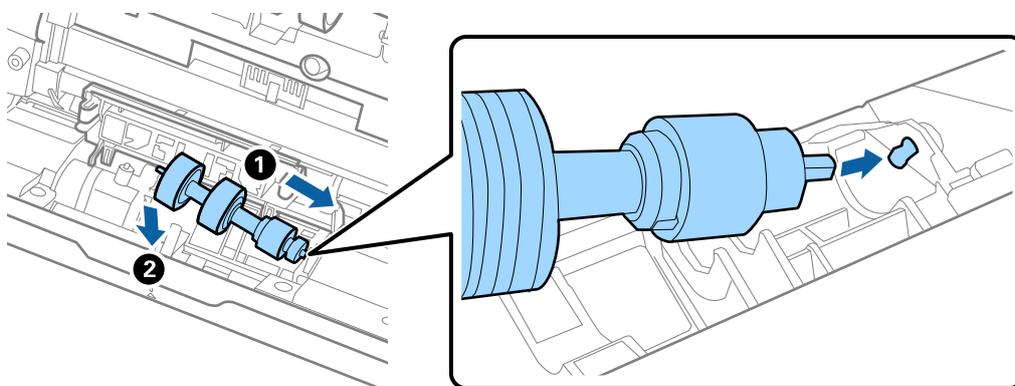
8. Premere i ganci su entrambe le estremità del coperchio del rullo di ritenzione per aprire il coperchio.



9. Sollevare il lato sinistro del rullo di ritenzione, e quindi far scorrere e rimuovere i rulli di ritenzione installati.



10. Inserire l'asse del nuovo rullo di ritenzione nella posizione corretta e quindi abbassare il rullo.



11. Chiudere il coperchio del rullo di ritenzione.



Importante:

Se il coperchio è difficile da chiudere, assicurarsi che i rulli di separazione siano installati correttamente.

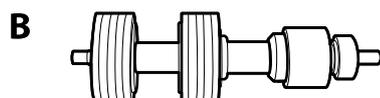
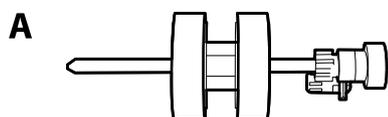
12. Chiudere il coperchio dello scanner.
13. Inserire l'adattatore CA, quindi accendere lo scanner.
14. Azzerare il numero di scansioni sul pannello di controllo.

Nota:

Smaltire il rullo di prelievo e il rullo di separazione secondo le regole e le normative dell'autorità locale. Non smontarli.

Codici kit montaggio rulli

Le parti (rullo di prelievo e rullo di separazione) devono essere sostituite quando il numero di scansioni supera il numero di servizio. È possibile verificare l'ultimo numero di scansioni sul pannello di controllo o in Epson Scan 2 Utility.



A: rullo di prelievo, B: rullo di separazione

Nome parte	Codici	Ciclo di vita
Kit montaggio rulli	B12B819671 B12B819681 (esclusivo per l'India)	200,000*

* Numero di scansioni consecutive utilizzando il test Epson su documenti originali, e rappresenta un riferimento per il ciclo di sostituzione. Il ciclo di sostituzione può variare a seconda dei vari tipi di carta usati, come la carta che genera molta polvere o la carta con una superficie ruvida che può ridurre il ciclo di vita.

Azzerare il numero di scansioni

Azzerare il numero di scansioni dopo aver sostituito il kit rulli.

1. Selezionare **Impostazioni > Informazioni dispositivo > Ripristinare il numero di scansioni > Numero di scansioni dopo sostituzione rulli** nella schermata iniziale.
2. Toccare **Sì**.

Informazioni correlate

➔ [“Sostituire il kit manutenzione rulli” a pagina 159](#)

Risparmio energetico

È possibile risparmiare energia utilizzando la modalità sleep o la modalità spegnimento automatico, quando non si eseguono operazioni dallo scanner. È possibile impostare il periodo di tempo prima che lo scanner entri in modalità sleep e si spenga automaticamente. Qualsiasi aumento influenzerà l'efficienza energetica del prodotto. Considerare l'impatto ambientale prima di apportare modifiche.

1. Selezionare **Impostazioni** nella schermata iniziale.

2. Selezionare **Impostazioni base**.
3. Selezionare **Imp. di spegn.**, quindi configurare le impostazioni desiderate.

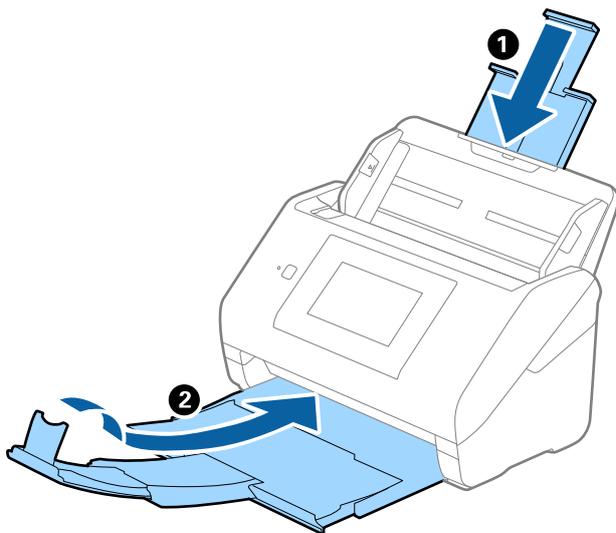
Nota:

Le funzionalità disponibili possono variare in base al luogo di acquisto.

Trasporto dello scanner

Quando è necessario trasportare lo scanner per spostamenti o per le riparazioni, seguire i passaggi che seguono per imballarlo.

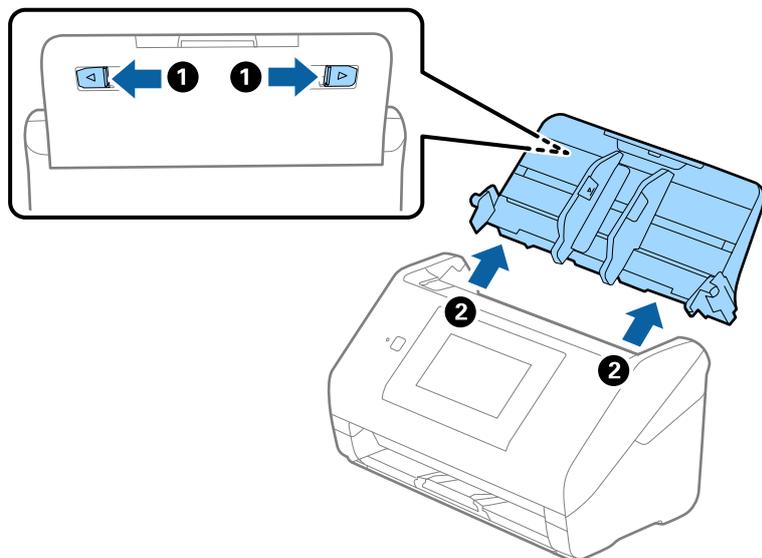
1. Premere il tasto  per spegnere lo scanner.
2. Scollegare l'adattatore CA.
3. Rimuovere i cavi e il dispositivo.
4. Chiudere la prolunga del vassoio di alimentazione e il vassoio di uscita.



Importante:

Assicurarsi di chiudere bene il vassoio di uscita altrimenti può essere danneggiato durante il trasporto.

5. Rimuovere il vassoio di alimentazione.



6. Montare i materiali di protezione forniti con lo scanner, quindi reimballare lo scanner nella confezione originale o in una scatola robusta.

Backup delle impostazioni

È possibile esportare su file il valore delle impostazioni presenti in Web Config. È possibile utilizzare tale file come backup dei contatti, dei valori di impostazione, per sostituire lo scanner, ecc.

Il file esportato non può essere modificato perché viene esportato come file binario.

Esportazione delle impostazioni

Esportare le impostazioni per lo scanner.

1. Accedere a Web Config, quindi selezionare la scheda **Gestione dispositivo > 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. Inserire una password per crittografare il file esportato.

È necessaria la password per importare il file. Lasciare il campo vuoto se non si desidera crittografare il file.

4. Fare clic su **Esporta**.



Importante:

*Per esportare le impostazioni di rete dello scanner, per esempio nome della stampante e indirizzo IPv6, selezionare **Abilitare per selezionare le singole impostazioni del dispositivo**, quindi selezionare le altre voci. Utilizzare solo i valori selezionati per lo scanner sostitutivo.*

Informazioni correlate

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

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.

1. Accedere a Web Config, quindi selezionare la scheda **Gestione dispositivo > Esporta e imposta valore di impostazione > Importa**.
2. Selezionare il file esportato, quindi inserire 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

➔ [“Esecuzione di Web Config su un browser web” a pagina 36](#)

Ripristina impostaz. predef.

Sul pannello di controllo, selezionare **Impostazioni > Amministrazione sistema > Ripristina impostaz. predef.**, quindi selezionare le voci che desidera ripristinare ai valori predefiniti.

- Impostazioni di rete: ripristina le impostazioni relative alla rete al loro stato iniziale.
- Tutto tranne Impostazioni di rete: ripristina le altre impostazioni al loro stato iniziale, tranne per le impostazioni relative alla rete.
- Tutte le impostazioni: ripristina tutte le impostazioni al loro stato iniziale al momento dell'acquisto.

 **Importante:**

Se si seleziona e si esegue **Tutte le impostazioni**, tutti i dati di impostazione registrati sullo scanner, compresi i contatti e le impostazioni di autenticazione utente, saranno eliminati. Le impostazioni eliminate non possono essere ripristinate.

Aggiornamento Applicazioni e Firmware

L'aggiornamento di applicazioni e firmware potrebbe consentire di risolvere alcuni problemi e aggiungere funzionalità o migliorare quelle esistenti. Verificare che sia in uso la versione più recente di applicazioni e firmware.

 **Importante:**

Mentre è in corso l'aggiornamento, non spegnere né il computer, né lo scanner.

Nota:

Quando lo scanner è collegabile a Internet, è possibile aggiornare il firmware da Web Config. Selezionare la scheda **Gestione dispositivo > Aggiornamento firmware**, verificare il messaggio visualizzato e fare clic su **Avvia**.

1. Assicurarsi che lo scanner e il computer siano collegati e che il computer sia connesso a Internet.
2. Avviare EPSON Software Updater e aggiornare le applicazioni o il firmware.

Nota:

I sistemi operativi Windows Server non sono supportati.

Windows 10

Fare clic sul pulsante Start e selezionare **Epson Software > EPSON Software Updater**.

Windows 8.1/Windows 8

Immettere il nome dell'applicazione nell'accesso alla ricerca, quindi selezionare l'icona visualizzata.

Windows 7

Fare clic sul pulsante Start e selezionare **Tutti i programmi o Programmi > Epson Software > EPSON Software Updater**.

Mac OS

Selezionare **Finder > Vai > Applicazioni > Epson Software > EPSON Software Updater**.

Nota:

Se l'applicazione che si desidera aggiornare non viene visualizzata nell'elenco, non è possibile aggiornarla mediante EPSON Software Updater. Verificare le versioni più recenti delle applicazioni sul sito web Epson locale.

<http://www.epson.com>

Aggiornamento del firmware dello scanner tramite il pannello di controllo

Se lo scanner è collegabile a Internet, è possibile aggiornare il firmware dello scanner utilizzando il pannello di controllo. È inoltre possibile impostare lo scanner affinché verifichi periodicamente eventuali aggiornamenti del firmware e informi l'utente della relativa disponibilità.

1. Selezionare **Impostazioni** nella schermata iniziale.
2. Selezionare **Amministrazione sistema > Aggiornamento firmware > Aggiorna**.
Nota:
*Selezionare **Notifica > Attiva** per impostare la verifica periodica di aggiornamenti del firmware disponibili nello scanner.*
3. Leggere il messaggio visualizzato a schermo e iniziare a cercare gli aggiornamenti disponibili.
4. Se sullo schermo LCD viene visualizzato un messaggio relativo alla disponibilità di un aggiornamento software, seguire le istruzioni sullo schermo per avviare l'aggiornamento.



Importante:

- Non spegnere o scollegare lo scanner dalla presa fino al completamento dell'aggiornamento; in caso contrario, lo scanner potrebbe essere soggetto a malfunzionamenti.
- Se l'aggiornamento del firmware non viene completato o non riesce, lo scanner non si avvia normalmente e sullo schermo LCD compare "Recovery Mode" alla successiva accensione dello scanner. In tal caso, occorre aggiornare nuovamente il firmware utilizzando un computer. Collegare lo scanner al computer mediante un cavo USB. Se "Recovery Mode" viene visualizzato sullo scanner, non è possibile aggiornare il firmware tramite una connessione di rete. Sul computer, accedere al sito web Epson locale e quindi scaricare il firmware dello scanner più recente. Vedere le istruzioni sul sito Web per i passaggi successivi.

Aggiornamento del firmware tramite Web Config

Quando lo scanner è collegabile a Internet, è possibile aggiornare il firmware da Web Config.

1. Accedere a Web Config e selezionare la scheda **Gestione dispositivo > Aggiornamento firmware**.
2. Fare click su **Avvia**, quindi seguire le istruzioni a video.

La conferma del firmware si avvia e, se esiste il firmware aggiornato, vengono visualizzate le informazioni a esso relative.

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

➔ ["Esecuzione di Web Config su un browser web" a pagina 36](#)

Aggiornamento del firmware senza connettersi a Internet

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.

Nota:

Prima dell'aggiornamento, assicurarsi che il driver dello scanner Epson Scan 2 sia installato sul computer. Se Epson Scan 2 non è installato, installarlo nuovamente.

1. Visitare il sito web di Epson per le versioni di aggiornamento del firmware più recenti.
<http://www.epson.com>
 - Se il firmware per lo scanner è presente, scaricarlo e andare al passaggio successivo.
 - Se sul sito web non sono presenti informazioni sul firmware, si sta già utilizzando il firmware più recente.
2. Collegare il computer contenente il firmware scaricato allo scanner tramite un cavo USB.
3. Fare doppio clic sul file .exe scaricato.
Epson Firmware Updater viene avviato.
4. Seguire le istruzioni visualizzate sullo schermo.