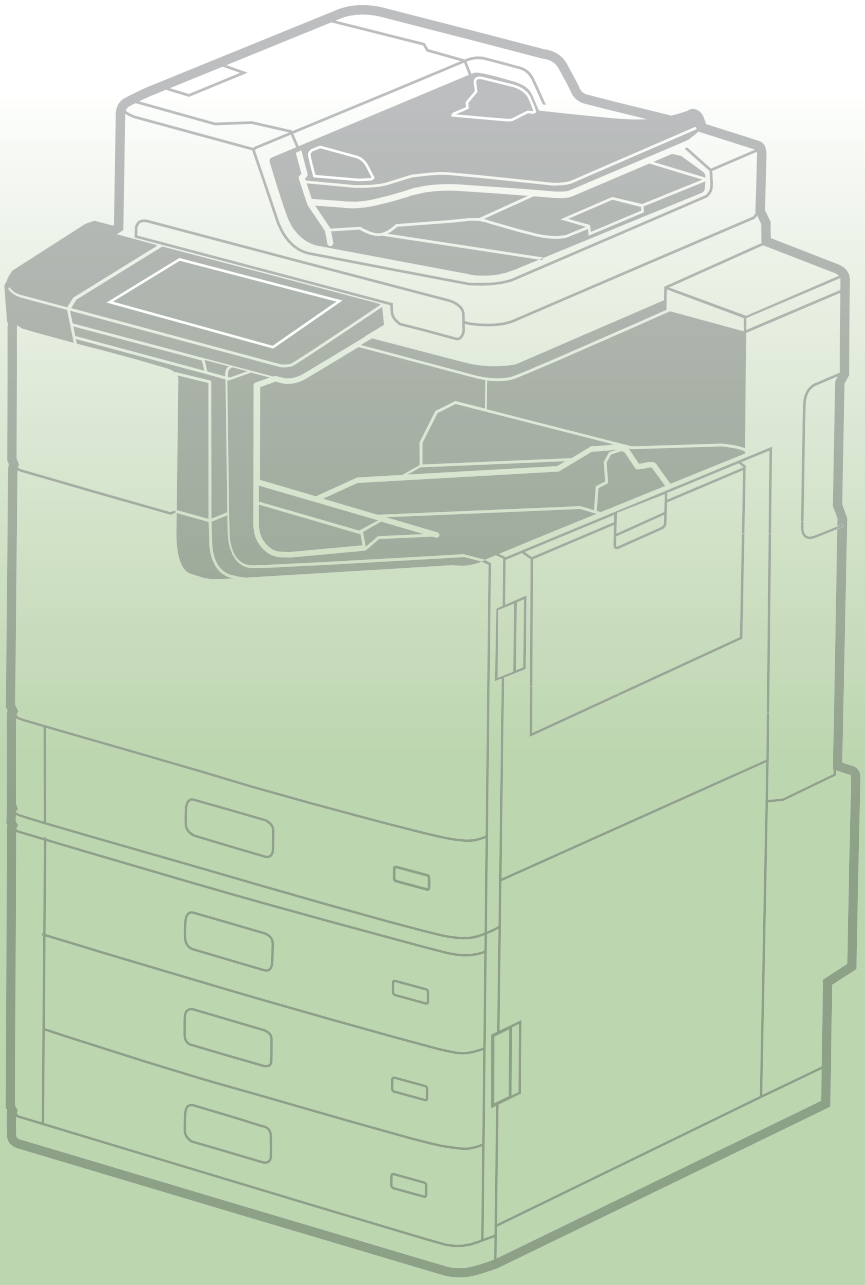
EPSON

Manuale sulla sicurezza



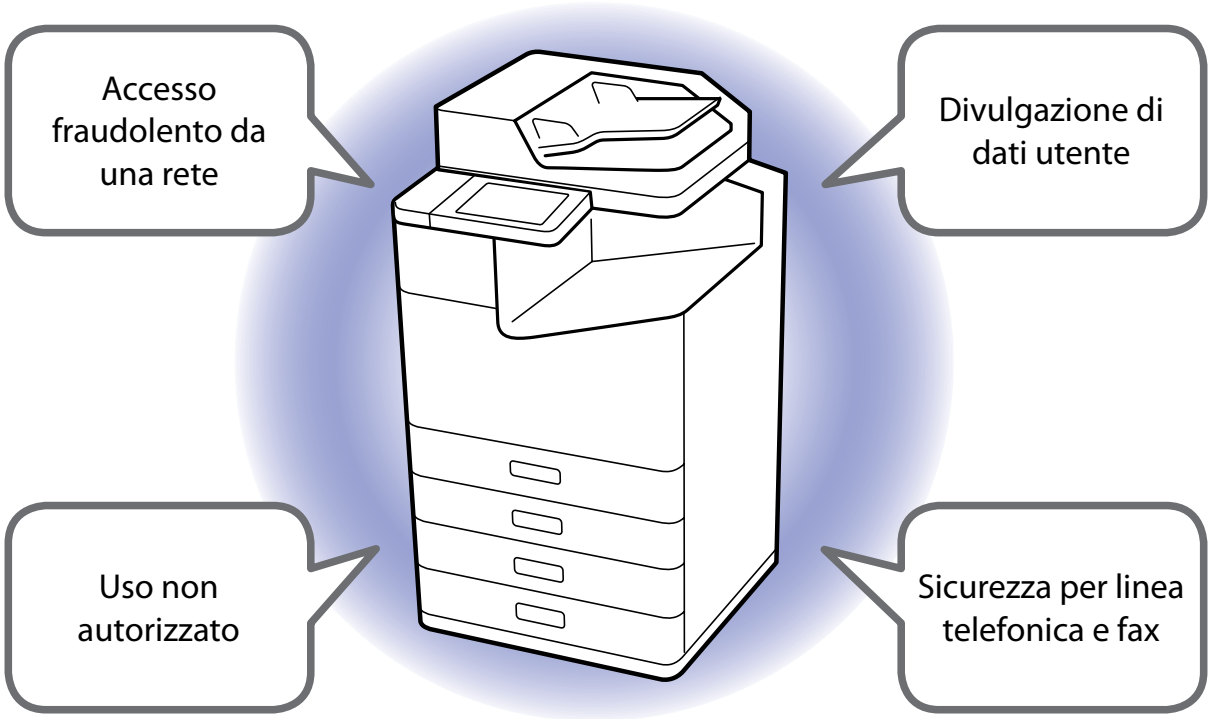
Sommario

1. Introduzione

Epson ha potenziato le funzioni compatibili con la rete dei suoi prodotti per una maggiore comodità di utilizzo.

Nel frattempo, la sofisticazione e la complessità sempre maggiori degli attacchi informatici da parte di terzi malintenzionati hanno aumentato le minacce ai dispositivi connessi alla rete, sollevando preoccupazioni sulle misure di sicurezza.

Poiché i prodotti Epson sono dotati di numerose funzioni, è necessario tenere conto della sicurezza, in particolare quando sono connessi alla rete, come nel caso di computer e server.



Il presente manuale descrive l'approccio di Epson alla sicurezza, contiene una serie di consigli per clienti e illustra all'utente le funzioni di sicurezza disponibili per l'uso.

Le icone accanto a ogni funzione nel testo hanno i seguenti significati.

: le funzioni di sicurezza con questo simbolo sono le impostazioni di base che devono essere eseguite dall'amministratore.

: le funzioni di sicurezza con questo simbolo possono essere configurate solo dall'amministratore e sono disponibili agli utenti nell'ambiente di sicurezza configurato.

: le funzioni di sicurezza con questo simbolo possono essere impostate e utilizzate da amministratori e utenti.

: altre funzioni di sicurezza. Applicabile alle funzioni di sicurezza integrate nei prodotti come da specifiche.

Consultare il manuale del prodotto in uso per le istruzioni di configurazione delle funzioni di sicurezza.

Si noti che le funzioni di sicurezza e la conformità agli standard di sicurezza indicate nel presente manuale variano a seconda del prodotto utilizzato. Alcuni prodotti potrebbero non disporre di queste funzioni o non essere conformi a questi standard di sicurezza. Consultare pertanto l'elenco delle funzioni nel manuale sulla sicurezza fornito separatamente per la compatibilità di ogni prodotto.

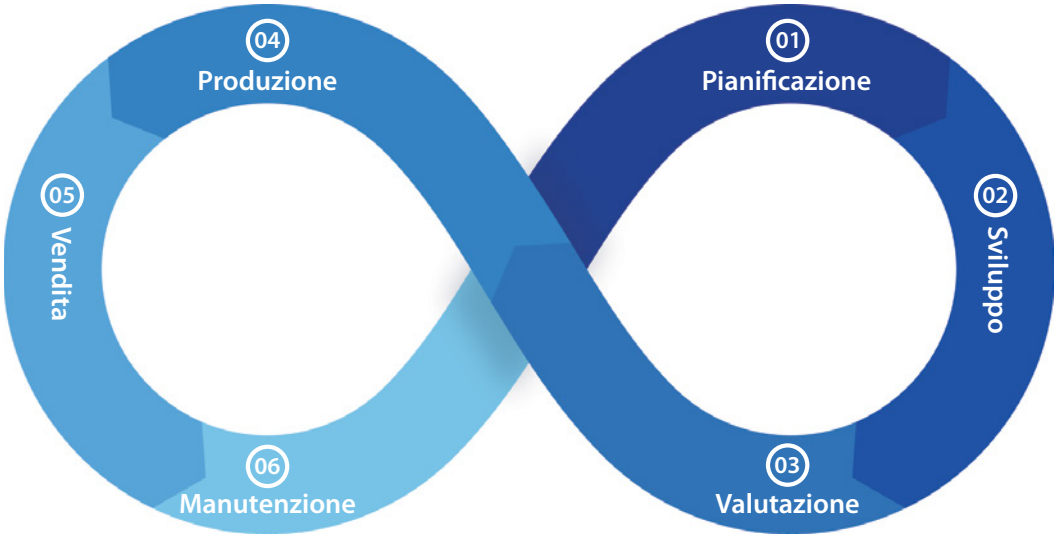
2. Criteri di base sulla sicurezza di EPSON

Epson adotta il seguente approccio in materia di sicurezza per garantire ai clienti la sicurezza e la facilità d'uso dei propri prodotti.

2-1. Criteri di base

Epson considera la sicurezza una caratteristica fondamentale della qualità del prodotto.

Garantiamo la sicurezza (endpoint) dei prodotti lungo l'intero ciclo di vita, dalla pianificazione allo sviluppo, la valutazione, la produzione, la vendita e la manutenzione, per garantire che i clienti possano utilizzare i nostri prodotti in condizioni di maggiore sicurezza, esaminando attentamente i diversi ambienti di utilizzo per ogni genere di prodotto.



① Pianificazione
Nella fase di pianificazione del prodotto monitoriamo costantemente le più recenti tendenze in ambito di sicurezza e le potenziali vulnerabilità. Inoltre ascoltiamo le richieste dei nostri clienti, identificando e analizzando i requisiti di sicurezza. In questo modo eliminiamo i potenziali problemi dei nostri prodotti prima del concretizzarsi di qualsiasi rischio.

② Sviluppo
Utilizzando le nostre piattaforme originali comuni e le nostre tecnologie messe a punto durante lo sviluppo di un'ampia gamma di prodotti, dalle stampanti da ufficio/domestiche alle stampanti commerciali/industriali per piccoli e grandi formati, ci impegniamo a migliorare la protezione contro i rischi per la sicurezza.

③ Valutazione
Oltre a realizzare test interni approfonditi, coinvolgiamo anche organizzazioni di terze parti per una valutazione oggettiva della sicurezza. Grazie al nostro rigoroso sistema di verifica della sicurezza, effettuiamo la valutazione a vari livelli per garantire un'elevata sicurezza dei prodotti.

④ Produzione
Per assicurare la massima qualità dei processi di produzione, abbiamo implementato un accurato sistema di gestione delle risorse informative che prevede l'installazione di un software presso i nostri stabilimenti finalizzato a garantire la funzionalità dei prodotti.

⑤ Vendita
Ci impegniamo a supportare i nostri clienti proponendo e implementando soluzioni volte a minimizzare i rischi per la sicurezza a seconda dell'ambiente di utilizzo e delle condizioni operative. Inoltre ci assicuriamo di risolvere rapidamente eventuali vulnerabilità che potrebbero emergere dopo l'installazione dei nostri prodotti.
Quando i prodotti devono essere sostituiti e smaltiti, ci assicuriamo di ripristinare i dispositivi alle impostazioni di fabbrica per evitare fughe di informazioni riservate.

⑥ Manutenzione
Siamo in grado di gestire rapidamente i problemi e le preoccupazioni legati alla sicurezza segnalati dai clienti che acquistano i nostri prodotti.

2-2. Fornire informazioni

Forniamo informazioni ai nostri clienti e li informiamo attivamente in materia di sicurezza.

2-3. Supporto nella risposta alle vulnerabilità

Dedichiamo un'attenzione costante alle vulnerabilità.

- Verifichiamo le vulnerabilità utilizzando gli strumenti standard del settore e ci impegniamo a fornire prodotti privi di vulnerabilità.
- Monitoriamo regolarmente le informazioni sulle vulnerabilità del software open source utilizzato nel firmware dei nostri prodotti.
- Analizziamo prontamente le nuove vulnerabilità rilevate e forniamo informazioni e contromisure.

2-4. Conformità a codici e standard

Ci impegniamo a rispettare e ottenere gli standard di sicurezza.

3. Procedura da seguire per l'installazione del prodotto

Per garantire una sicurezza ottimale, leggere quanto segue durante l'installazione e configurare le impostazioni necessarie in base al proprio ambiente di utilizzo.

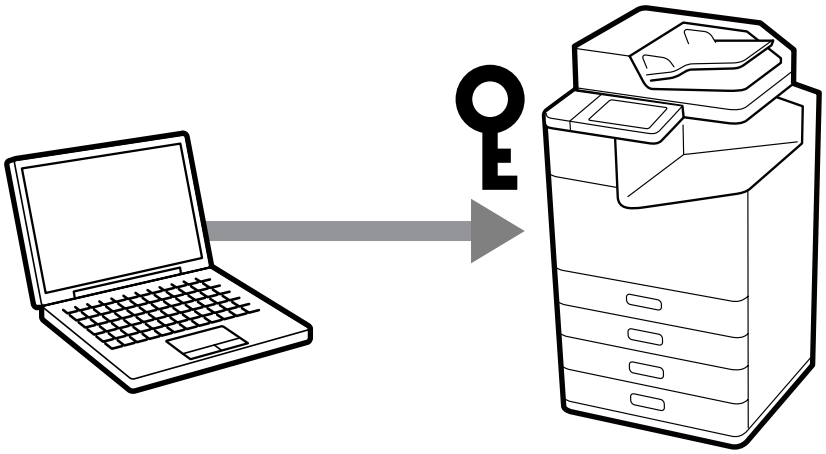
3-1. Password amministratore

Si raccomanda fortemente di impostare una password amministratore durante l'installazione di ciascun prodotto.

Se non viene impostata una password amministratore o il prodotto viene lasciato con le impostazioni predefinite di fabbrica, le impostazioni generali e di rete memorizzate nel prodotto possono essere accessibili o modificate illegalmente. Esiste anche il rischio di non proteggere adeguatamente le informazioni personali e riservate, come rubriche, ID e password.

La password amministratore deve essere una stringa di caratteri complessa e difficile da indovinare da parte di altri utenti. Deve essere composta da almeno 8 caratteri e contenere non solo lettere, ma anche simboli e numeri. È possibile impostare la password amministratore direttamente nelle impostazioni del pannello di controllo del prodotto o tramite la rete.

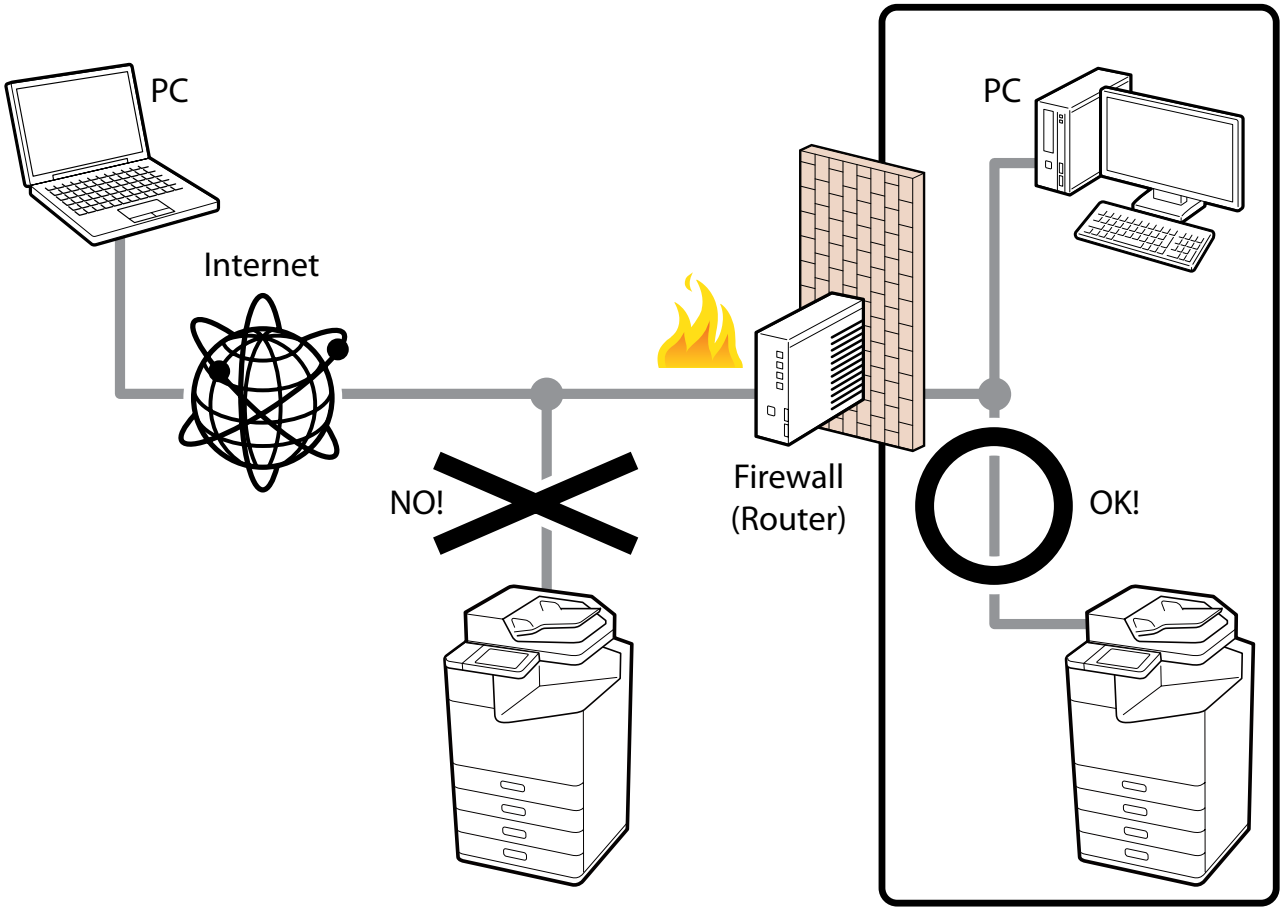
Pertanto alcuni prodotti sono dotati di password individuali predefinite per garantire una maggiore sicurezza.



3-2. Connessione a Internet

Installare i prodotti su una rete protetta da firewall senza collegarli direttamente a Internet. Si raccomanda di impostare e utilizzare un indirizzo IP privato quando si effettua questa operazione.

Anche quando si utilizza il prodotto in un ambiente IPv6, assicurarsi di limitare l'accesso al prodotto utilizzando un firewall o altri mezzi per impedire l'accesso diretto al prodotto da Internet.



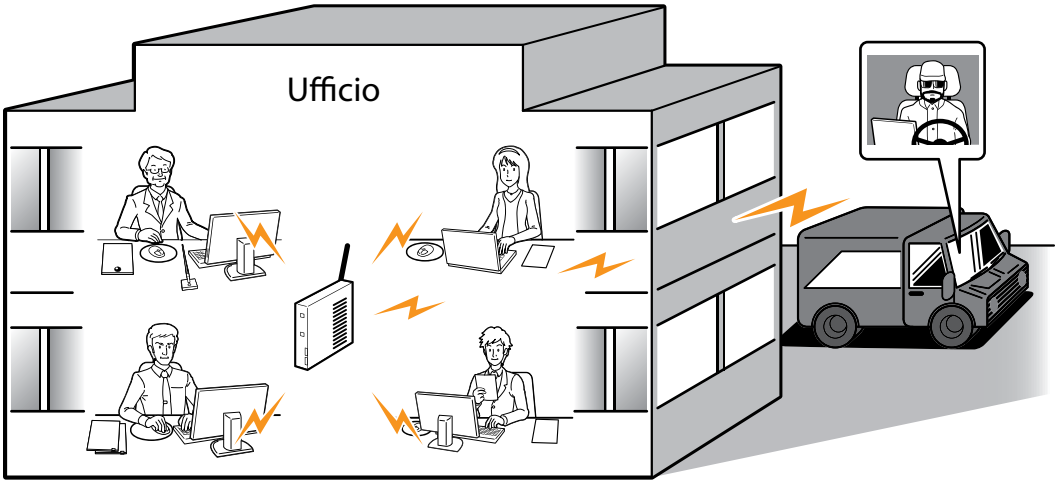
Per le funzioni di rete dei prodotti e per la stampa sono incluse interfacce di gestione, come ad esempio una schermata di gestione web. Sebbene Epson svolga test di vulnerabilità e si impegni a fornire prodotti privi di vulnerabilità, la connessione diretta a Internet comporta rischi imprevisti per la sicurezza, come operazioni non autorizzate e fughe di informazioni, per la rete del cliente e per i dispositivi connessi alla rete.

3-3. Rete LAN wireless

Quando si utilizza una rete LAN wireless, impostare la sicurezza della rete LAN wireless in modo appropriato.

Il vantaggio di una rete LAN wireless è che consente di connettere liberamente il prodotto tramite una rete per comunicare con i terminali di computer e smartphone quando ci si trova nell'area di copertura di un segnale. Tuttavia, se la sicurezza non è impostata correttamente, si potrebbero verificare problemi come i seguenti, causati da terze parti malintenzionate.

- Le informazioni personali, come i propri dati di stampa, di scansione, l'ID e la password, potrebbero essere visti da terzi (intercettati).
- Il contenuto delle comunicazioni potrebbe essere riscritto in modo fraudolento (falsificato).
- L'identità di determinate persone o dispositivi può essere rubata e utilizzata per le comunicazioni (furto d'identità).



Consultare il manuale del prodotto per informazioni dettagliate sull'impostazione di una rete LAN wireless.

3-4. Disabilitazione di funzioni e protocolli inutilizzati

Disattivare le funzioni e i protocolli inutilizzati.

I protocolli e le funzioni possono essere abilitati o disabilitati singolarmente, evitando rischi per la sicurezza in caso di utilizzo involontario.

3-5. Aggiornamento al firmware e al software più recente

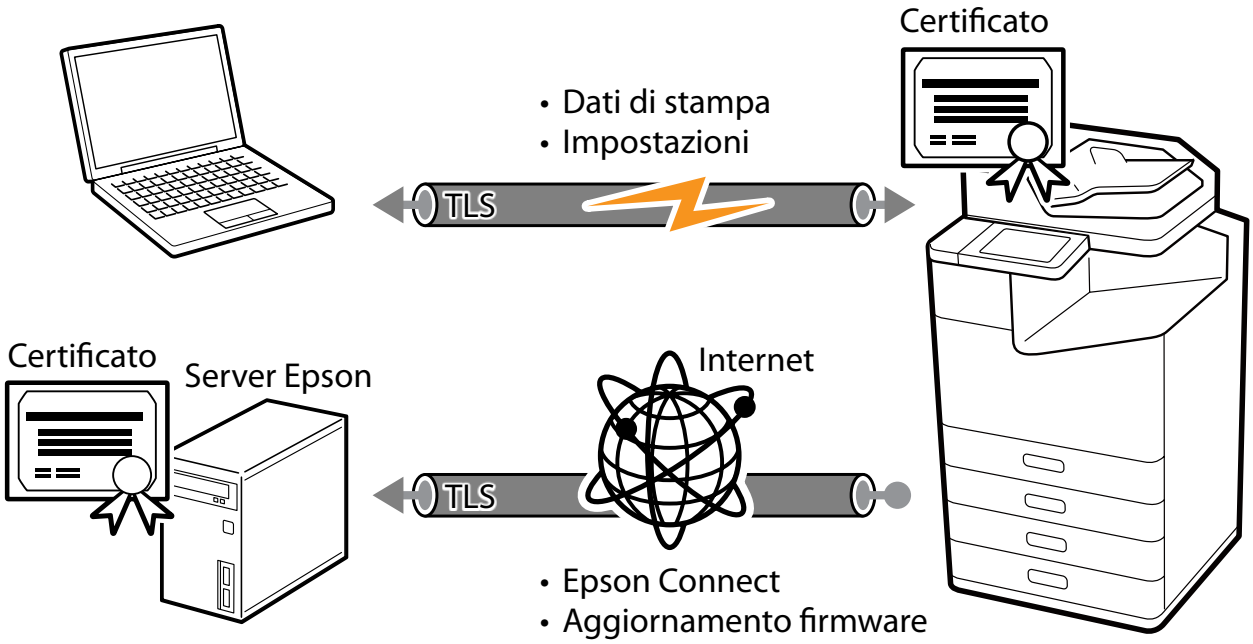
Se necessario, forniamo il firmware e il software più recenti. Per utilizzare il prodotto, assicurarsi di effettuare l'aggiornamento al firmware più recente.

Il firmware e il software più recenti non includono solo funzionalità aggiuntive, ma anche correzioni di difetti e vulnerabilità. Per ulteriori informazioni sul firmware o sul software, consultare la cronologia delle modifiche apportate al firmware o al software.

4. Sicurezza rete

4-1. Comunicazione TLS

Poiché le trasmissioni sono protette da TLS, è possibile impedire la divulgazione di informazioni sulle impostazioni e del contenuto dei dati di stampa utilizzando il protocollo IPPS per la stampa e configurando il prodotto tramite il proprio browser. È inoltre possibile impedire l'invio di informazioni a dispositivi non autorizzati utilizzando la funzione di convalida del server, importando il certificato firma CA e lavorando con l'infrastruttura a chiave pubblica aziendale (PKI). È possibile configurare il livello di crittografia per utilizzare un algoritmo di crittografia molto più sicuro. Si è inoltre protetti da TLS quando si accede al server Epson su Internet tramite il prodotto per Epson Connect e aggiornamenti firmware.



È possibile selezionare la versione e il livello di crittografia del TLS da utilizzare.

Le versioni e i livelli di crittografia TLS supportati sono i seguenti.

Versione TLS

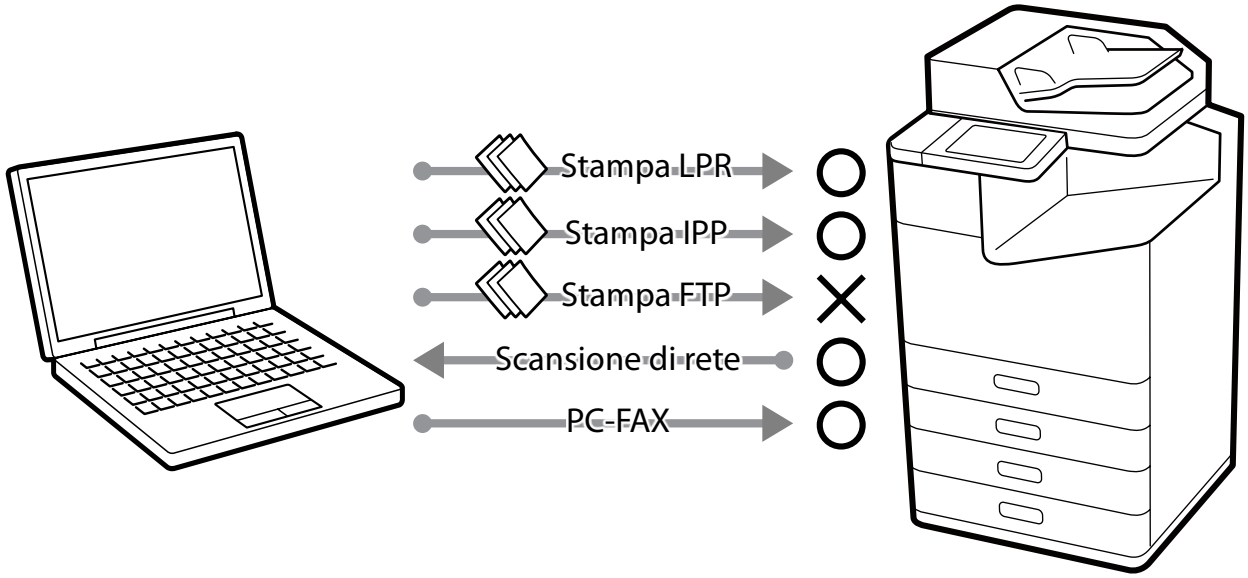
- TLS1.1
- TLS1.2
- TLS1.3

Livello di crittografia

- 80 bit
- 112 bit
- 128 bit
- 192 bit
- 256 bit

4-2. Controllo delle autorizzazioni e delle esclusioni dei protocolli

Il prodotto comunica tramite vari protocolli durante la stampa, la scansione e l'invio di un PC-FAX. È possibile prevenire i rischi di sicurezza derivanti dall'uso non intenzionale impostando autorizzazioni e divieti specifici per ciascun protocollo.



Vedere l'appendice per informazioni sui rischi per la sicurezza quando i protocolli e le funzioni sono abilitati e sulle limitazioni quando sono disabilitati.

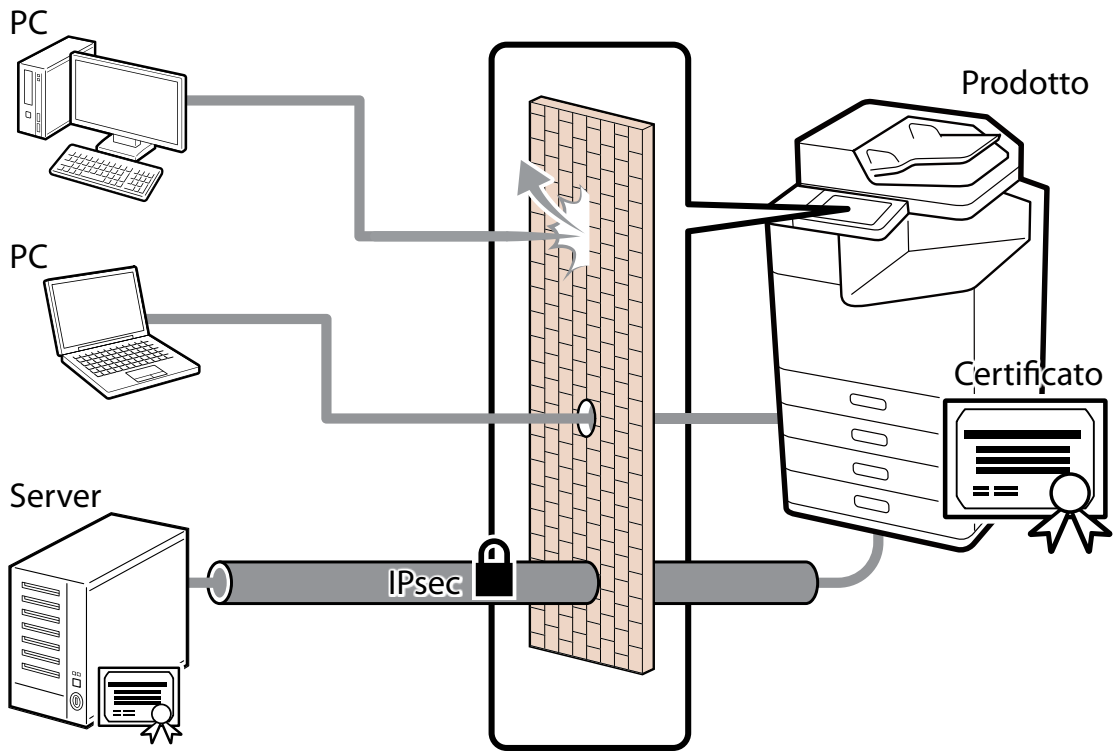
I protocolli e le funzioni che possono essere abilitati o disabilitati sono i seguenti.

- Bonjour
- SLP
- WSD
- LLTD
- LLMNR
- LPR
- RAW (Porta 9100/Porta personalizzata)
- IPP/IPPS
- FTP
- SNMP
- SSL/TLS
- Condivisione di rete Microsoft
- Scansione di rete (EPSON Scan)
- PC-FAX

4-3. IPsec/Filtro IP

È possibile filtrare gli indirizzi IP, i tipi di servizi, i numeri di porta per la ricezione e la trasmissione, ecc. utilizzando la funzione IPsec/Filtro IP. A seconda della combinazione di questi filtri, è possibile impostare se accettare o bloccare i dati da un determinato client e se accettare o bloccare tipi di dati specifici. Analogamente, è possibile comunicare con una maggiore sicurezza combinando le protezioni utilizzando IPsec.

I protocolli di stampa e di scansione poco sicuri diventano a loro volta oggetti protetti in quanto la protezione all'interno di unità di pacchetti IP (crittografia e autenticazione) è inclusa tra le funzioni di protezione di IPsec. Nel metodo di autenticazione tramite IPsec sono supportate le chiavi precondivise e i certificati.



Gli algoritmi e i metodi di scambio chiave supportati sono i seguenti:

Metodo di scambio chiave

- IKEv1
- IKEv2

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/AH

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

I criteri di base interessano tutti gli utenti che accedono al prodotto. Impostare criteri individuali per controllare l'accesso in base alle proprie esigenze specifiche.

4-4. Autenticazione IEEE 802.1X

IEEE 802.1X è uno standard per controllare l'accesso a ciascuna porta del dispositivo di rete. Le reti IEEE 802.1X sono compilate da server RADIUS (server di autenticazione) e hub di commutazione con una funzione di autenticazione.

I prodotti Epson sono conformi allo standard IEEE 802.1X e possono essere connessi a un ambiente di rete che contiene informazioni riservate.

Sono supportati i seguenti metodi di autenticazione e algoritmi di crittografia:

Metodo autenticazione

- EAP-TLS
- PEAP-TLS
- PEAP/MSCHAPv2
- EAP-TTLS

Algoritmo di crittografia

- AES128
- AES256
- 3DES
- RC4

4-5. SNMP

SNMP è un protocollo per il monitoraggio dello stato e la modifica delle impostazioni dei dispositivi e degli strumenti di gestione supportati.

SNMPv1 e SNMPv2c non supportano la crittografia delle comunicazioni e devono essere utilizzati all'interno di una rete protetta da un firewall o simile. Inoltre, per utilizzare le comunicazioni SNMP, modificare il nome della comunità predefinito.

SNMPv3 può essere utilizzato per autenticare e crittografare le comunicazioni SNMP (pacchetti) per monitorare lo stato e configurare le modifiche con strumenti di gestione dei dispositivi compatibili. In questo modo è possibile garantire la riservatezza durante la modifica delle impostazioni o il monitoraggio dello stato in rete.

SNMPv3 supporta i seguenti algoritmi di autenticazione e crittografia.

Algoritmi di autenticazione SNMPv3

- MD5
- SHA-1

Algoritmi di crittografia SNMPv3

- DES
- AES128

4-6. SMB

SMB è un protocollo per la condivisione di file in rete.

SMB1.0 e SMB2.0 non supportano la crittografia delle comunicazioni e devono essere utilizzati all'interno di una rete protetta da un firewall o simile.

SMB3.0 può essere utilizzato per autenticare e crittografare le comunicazioni SMB (pacchetti) con dispositivi compatibili. Ciò garantisce la riservatezza della condivisione dei file in rete.

4-7. WPA3

Il prodotto supporta WPA3, la più recente tecnologia di autenticazione e crittografia per il Wi-Fi (LAN wireless). WPA3 fornisce una protezione più robusta ed efficace per salvaguardare i propri dati sulla rete wireless.

4-8. Separazione tra le interfacce

Il prodotto include un'interfaccia USB, un'interfaccia LAN cablata standard, un'interfaccia LAN cablata aggiuntiva, un'interfaccia LAN wireless e un'interfaccia fax. Ogni interfaccia è indipendente, limitando l'accesso solo ai protocolli che possono essere gestiti da quell'interfaccia, e non fornisce alcuna funzionalità di trasferimento o instradamento diretto. Per fare un esempio specifico, l'accesso da una linea telefonica pubblica (linea fax) è limitato all'elaborazione secondo le procedure di comunicazione fax. Qualsiasi deviazione da tale procedura comporta un errore di disconnessione della comunicazione, pertanto non vi è alcun rischio di accesso non autorizzato. Inoltre viene verificata la correttezza dei dati fax ricevuti come dati immagine prima di essere importati. Non vi è alcun rischio che venga impiantato malware dannoso tramite la funzione di trasferimento attraverso il prodotto, che potrebbe causare la contaminazione da virus o l'accesso non autorizzato. Solo gli utenti autorizzati possono eseguire la funzione di trasferimento. Ad esempio, l'intrusione nella rete da una linea telefonica pubblica attraverso il prodotto, l'accesso a una LAN cablata da una LAN wireless o l'accesso non autorizzato tramite Internet al prodotto connesso a un computer tramite USB.

5. Protezione del prodotto

5-1. Blocco della connessione USB da computer

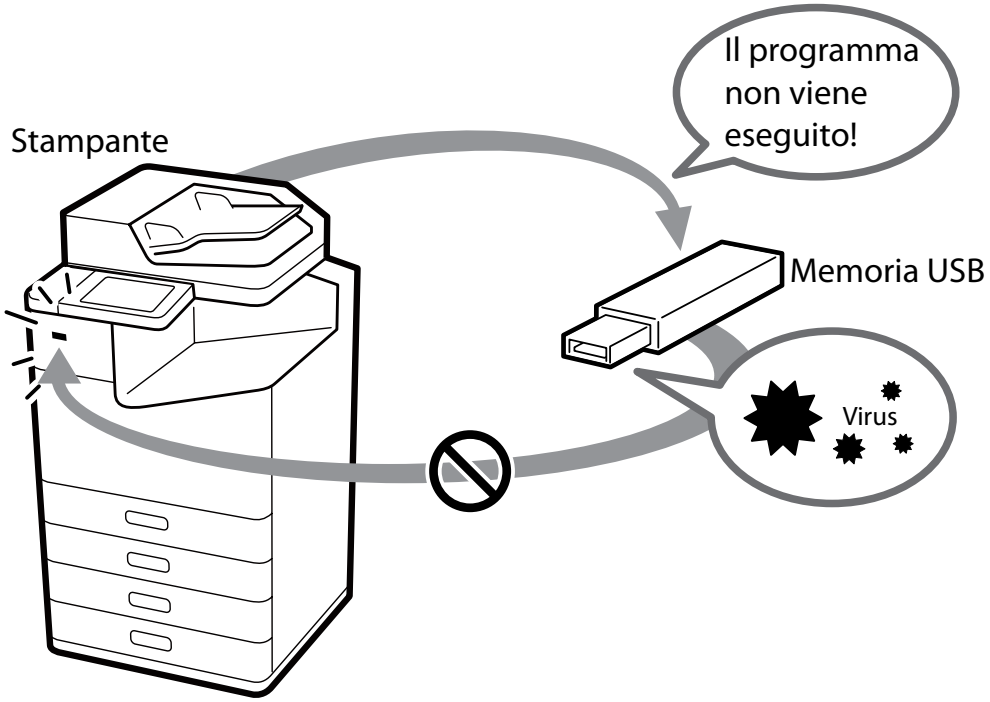
È possibile disattivare l'accesso al prodotto tramite connessione USB da un computer. Impostare questa opzione per proibire la stampa o la scansione tramite connessione diretta a un computer mediante cavo USB.

5-2. Disattivazione dell'interfaccia esterna

È possibile disattivare le schede di memoria e le interfacce di memoria USB. In questo modo è possibile impedire la duplicazione illegale dei dati attraverso la scansione non autorizzata di documenti riservati presenti in ufficio.

5-3. Gestione di virus introdotti tramite memorie USB

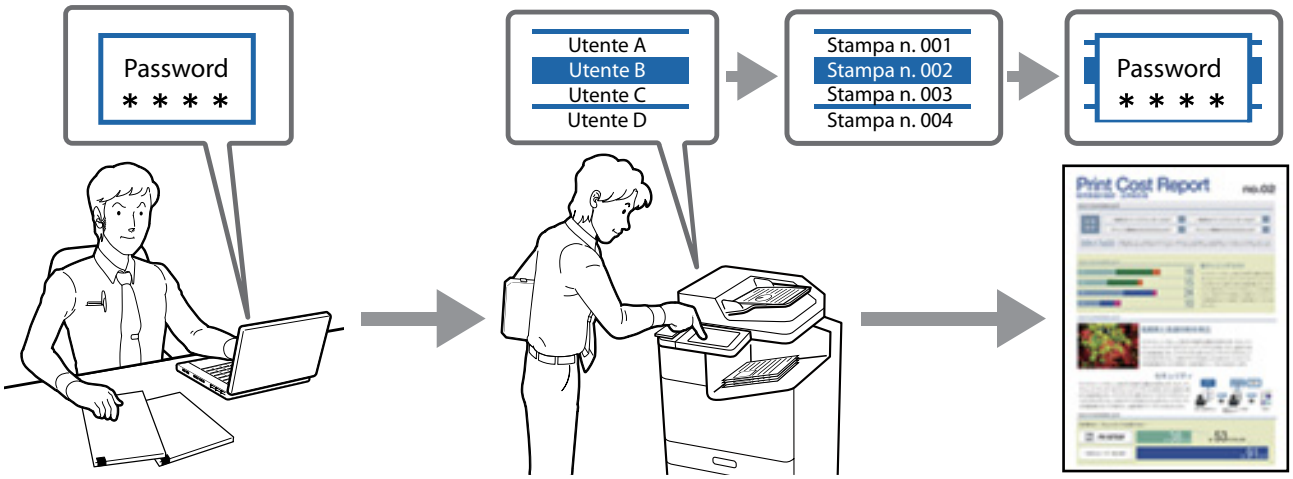
Poiché nei prodotti Epson non esistono funzioni eseguibili su memorie USB, non c'è alcun pericolo che il prodotto venga infettato da virus tramite questo tipo di memorie.



6. Sicurezza di stampa/scansione

6-1. Processi riservati

È possibile garantire la privacy/riservatezza dei documenti e impedire a persone non autorizzate di vedere stampe lasciate incustodite nel dispositivo inviando i propri documenti come "Processo riservato".



Inserire una password per stampare.

Selezionare un lavoro di stampa sul prodotto e inserire la password.

Stampa completata.

6-2. Dicitura di protezione da copia

È possibile proteggere l'originalità di un documento con la stampa di filigrana di protezione da copia che crea una dicitura in filigrana trasparente sull'originale. La filigrana trasparente diventerà visibile quando l'originale viene utilizzato per effettuare copie.

Risultati copia: testo ritagliato

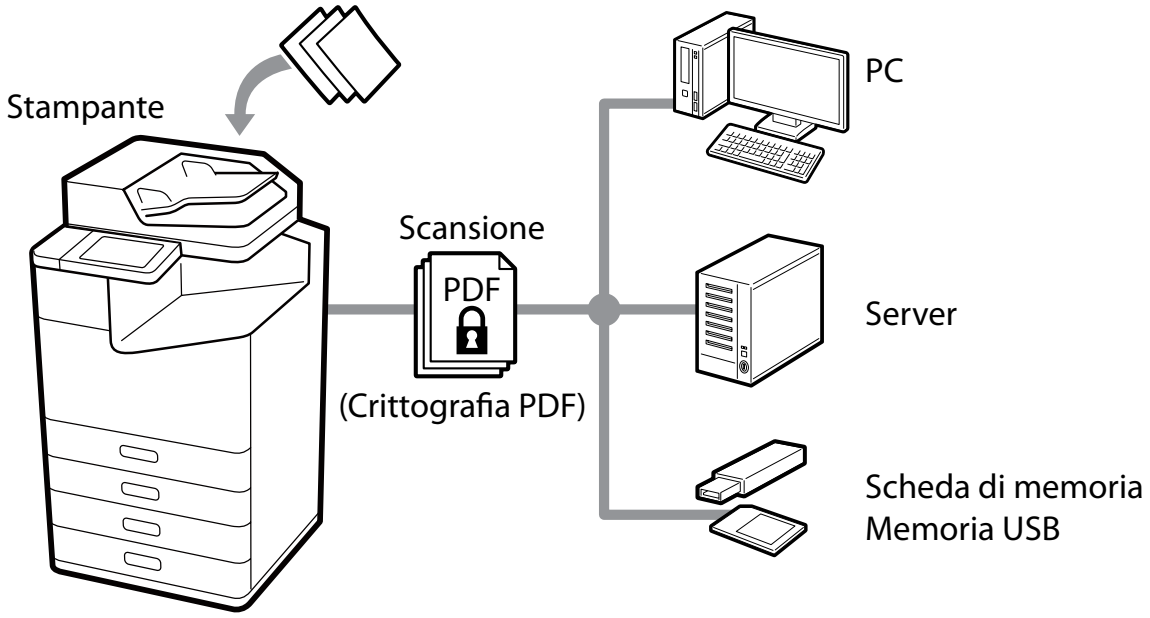
Risultati copia: goffratura

6-3. Filigrana

Le filigrane quali le diciture riservato e importante (in formato testo o BMP) possono essere sovrimpresse sui documenti. In aggiunta è possibile selezionare un "nome utente" o un "nome computer". Ricordando al destinatario di maneggiare con cura i documenti è possibile scoraggiarne l'uso non autorizzato.

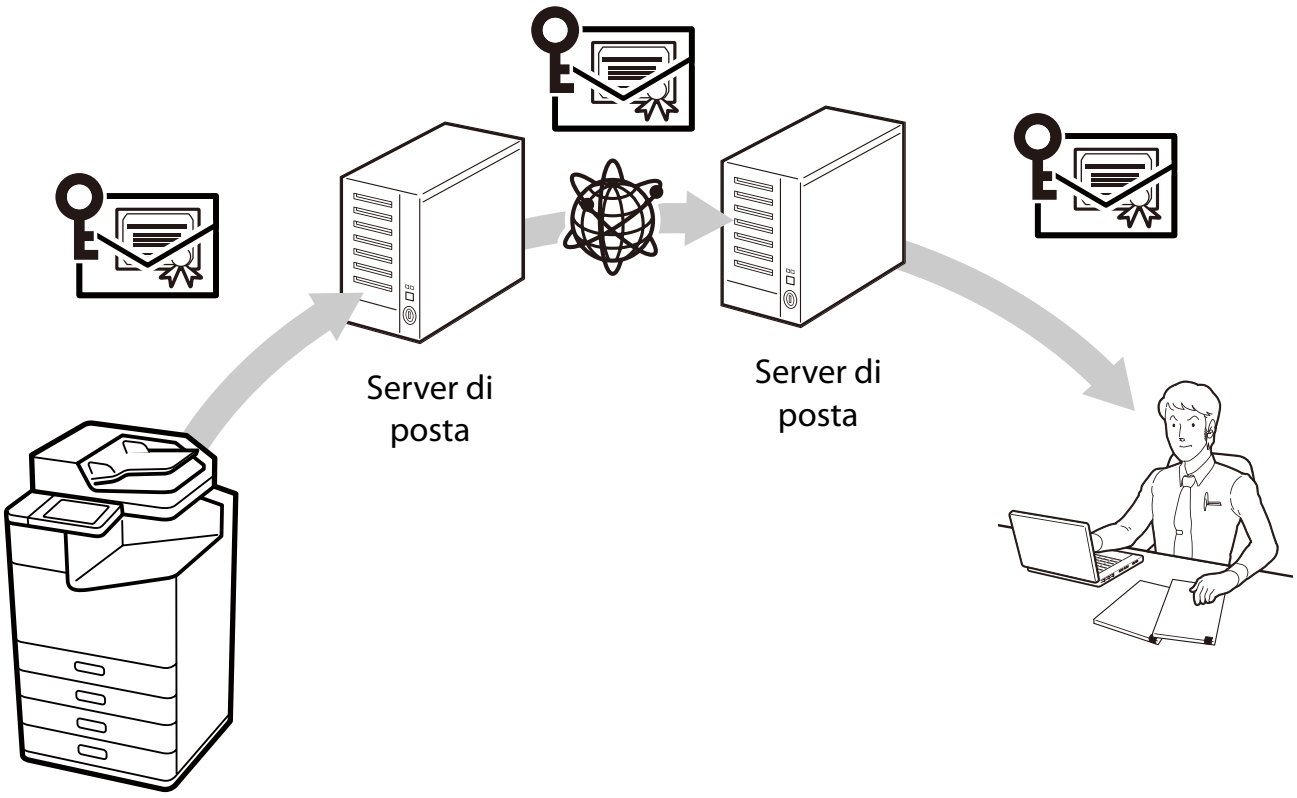
6-4. Crittografia PDF

È possibile convertire tramite scansione un documento in un file PDF protetto da password. In questo modo si impedisce a terze parti di visualizzare i documenti senza autorizzazione.



6-5. S/MIME

L'utilizzo di S/MIME consente all'utente di aggiungere una firma digitale e/o di crittografare una e-mail per Scansione su e-mail e Da fax a e-mail. Anche quando una e-mail passa attraverso vari server e-mail, è possibile proteggerla dalla falsificazione, intercettazione o manomissione. S/MIME salvaguarderà l'autenticità e l'integrità del messaggio proteggendo nel contempo la sicurezza dei dati e garantendone il non ripudio.



Gli algoritmi supportati sono i seguenti.

Algoritmo di crittografia

- AES-128
- AES-192
- AES-256
- 3DES

Algoritmo hash per la firma digitale

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

6-6. Restrizioni di dominio

Applicando regole restrittive ai nomi dominio degli indirizzi e-mail, è possibile ridurre il rischio di trasmissioni erronee e fughe di informazioni per le funzioni Scansione su e-mail e inoltro di fax.

6-7. Supporto per password di autenticazione lunghe

Oggi si raccomanda di impostare password lunghe per aumentarne la sicurezza.
È possibile impostare un massimo di 70 caratteri come password di autorizzazione utilizzata per Scansione su cartella rete/FTP, Scansione su e-mail e Notifica tramite e-mail.
È possibile impostare un criterio password per le password più lunghe impostate per i file server e i server di posta.

6-8. Restrizioni all'accesso ai file da PDL

Disabilitando l'accesso ai file da PDL (linguaggio di descrizione pagina), è possibile prevenire il rischio di fughe di informazioni causate da dati di stampa dannosi che rubano i file all'interno della stampante. Anche se i dati di stampa dannosi vengono trasmessi, il prodotto può essere utilizzato in sicurezza senza che i file vengano letti.

6-9. Stampa sicura

Se si desidera proteggere la sicurezza dei percorsi di trasmissione per la stampa, è possibile utilizzare un IPPS crittografato mediante TLS.

7. Sicurezza fax

7-1. Limitazioni teleselezione

Se si desidera inserire un numero di fax direttamente utilizzando il tastierino numerico, è possibile fare in modo che l'invio del fax avvenga solo quando si inserisce la destinazione per due volte correttamente. Tra le impostazioni è inoltre possibile vietare l'inserimento di un numero di telefono direttamente utilizzando il tastierino numerico e fare in modo che i fax vengano inviati solo tramite composizione rapida e solo a indirizzi registrati nella propria rubrica indirizzi. In questo modo si riduce il rischio di fughe di informazioni derivanti da trasmissioni errate causate da errori nell'inserimento dei numeri di telefono.

7-2. Conferma elenco indirizzi

È possibile confermare gli indirizzi selezionati prima dell'invio di un fax. In questo modo si riduce il rischio di divulgazione di informazioni derivanti da trasmissioni errate causate da errori nell'inserimento di un indirizzo.

7-3. Rilevamento del segnale di linea

È possibile impedire trasmissioni errate inviando i fax dopo la conferma del rilevamento di un segnale di linea.

Il rilevamento del segnale di linea potrebbe non essere disponibile in alcuni paesi e in alcune regioni.

7-4. Misure contro i fax abbandonati

È possibile impostare "Stampa fax dopo la visualizzazione" per salvare un fax ricevuto nella posta in arrivo (ricezione in memoria) e stamparlo dopo averlo confermato sul pannello di controllo. In questo modo si impedisce la divulgazione di informazioni e la perdita di materiale stampato dei fax ricevuti causate da fax lasciati incustoditi.

Inoltre, è possibile impedire la stampa e l'eliminazione arbitrarie da parte di utenti non autorizzati impostando che venga richiesta una password per poter accedere alla posta in arrivo.

7-5. Rapporto conferma trasmissione

È possibile verificare che un fax sia stato effettivamente inviato all'indirizzo corretto stampando rapporti in cui sono riportati i dettagli sulla trasmissione, come il rapporto sulle informazioni di invio, il rapporto sulle informazioni di inoltro e il rapporto sulla gestione dell'invio.

7-6. Eliminazione dei dati di backup dei fax ricevuti

È possibile eliminare i dati di backup* dei fax ricevuti dal pannello di controllo. È inoltre possibile fare in modo che i dati di backup vengono eliminati automaticamente, impedendo nuove stampe non autorizzate dei dati dei fax ricevuti.

* I dati di backup dei fax ricevuti vengono salvati nel prodotto (impostazione predefinita) per consentire di stampare nuovamente i fax quando i risultati di stampa non sono chiari o vanno persi.

7-7. Limitazione dell'invio a più destinatari

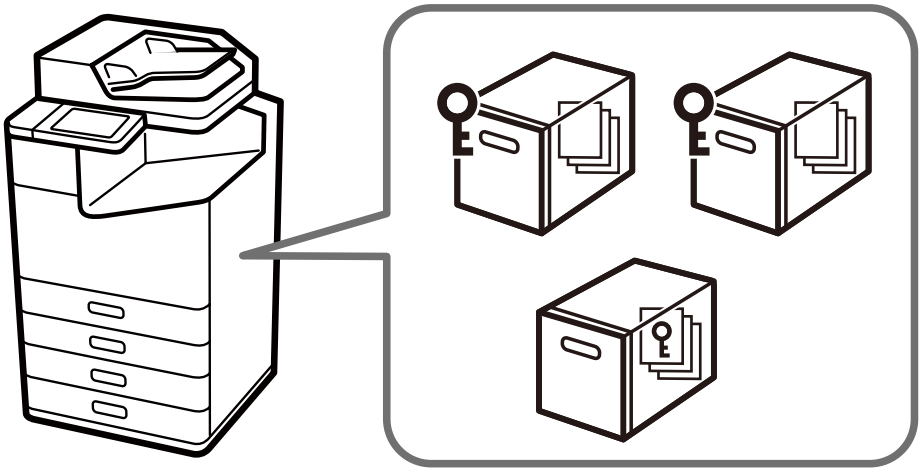
È possibile impostare il prodotto in modo che possa essere selezionato solo 1 destinatario.

Impedendo la selezione di più destinatari si riduce il rischio di inviare un fax a un destinatario indesiderato e di divulgare informazioni.

8. Protezione dei dati utente

8-1. Sicurezza dell'archiviazione

È possibile impostare password univoche per le cartelle condivise e i documenti sui modelli dotati di cartelle condivise. Queste password possono impedire le divulgazione e la perdita di informazioni e la manomissione non autorizzata. L'utilizzo dell'archiviazione può inoltre essere soggetto al controllo degli accessi. Se le cartelle condivise non vengono utilizzate, è inoltre possibile proibire l'uso della funzione cartella condivisa.



8-2. Protezione della rubrica indirizzi

È possibile prevenire la fuga e l'alterazione non autorizzata delle informazioni sulla rubrica indirizzi poiché per la modifica in batch delle rubriche indirizzi memorizzate nel prodotto è necessaria una password di amministratore (se è stata impostata una password di amministratore). Inoltre, poiché le rubriche indirizzi sono esportabili come file crittografato, è possibile impedire la divulgazione di informazioni personali, come i numeri di fax e gli indirizzi e-mail, durante la sostituzione o il backup del prodotto.

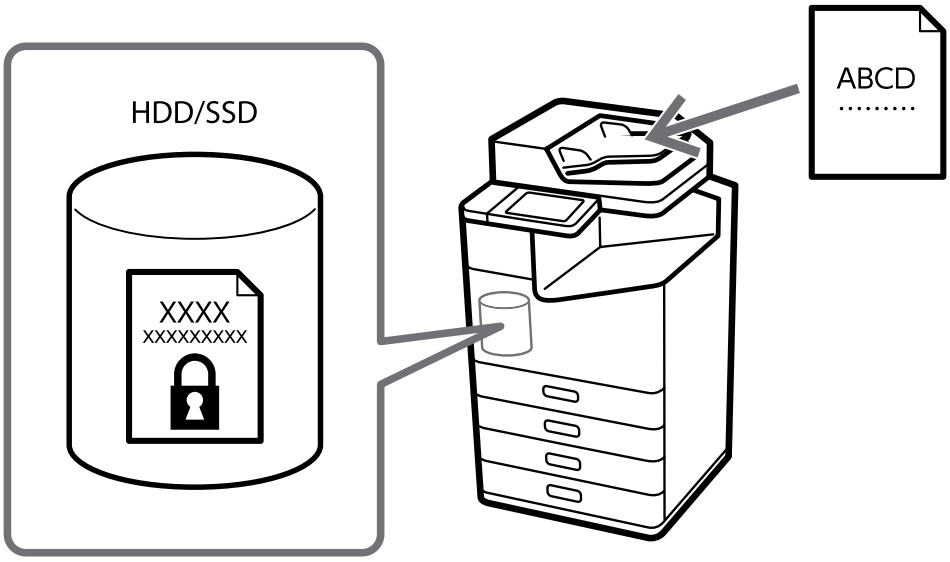
8-3. Gestione dei dati elaborati da un prodotto

I dati delle funzioni di stampa, di copia e di scansione vengono salvati temporaneamente in un prodotto, quindi vengono eliminati al completamento di un lavoro o quando il prodotto viene spento. I dati dei fax vengono eliminati al completamento dell'invio o della ricezione del fax. Tenere presente che, sebbene i fax ricevuti vengano salvati come dati e conservati dalla funzione di backup, è possibile modificare l'impostazione in modo che i dati vengano eliminati automaticamente (vedere 7-6).

8-4. Crittografia dei dati salvati su disco rigido/SSD

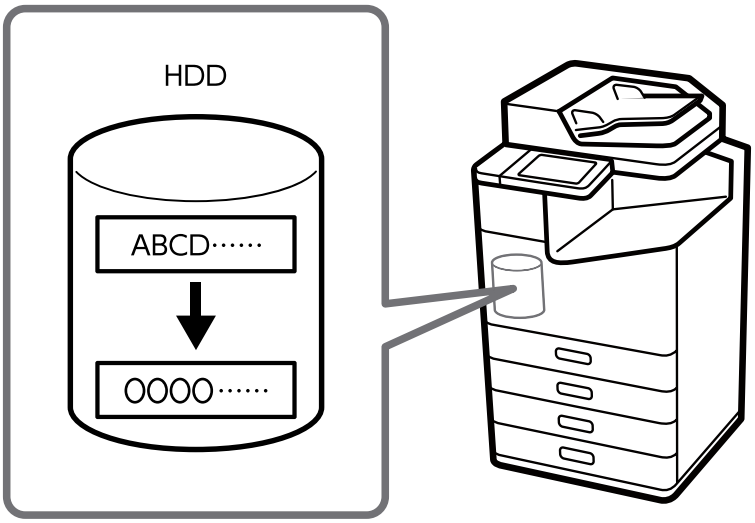
Proteggiamo sempre i dati dei clienti tramite crittografia quando vengono salvati dati su un disco rigido interno/SSD all'interno un prodotto. Nel caso improbabile di un attacco da parte di terzi malintenzionati, il contenuto dei dati memorizzati non sarà visibile. Il disco rigido/SSD è dotato di un'unità di auto-crittografia e i dati dei documenti vengono crittografati con AES-256.

La crittografia dei dati impedisce l'accesso non autorizzato o l'attacco dannoso ai dati personali se il disco rigido/SSD viene rubato.



8-5. Eliminazione sequenziale dei dati dei lavori

Quando questa funzione è abilitata, i dati dei lavori memorizzati temporaneamente sul disco rigido dell'unità vengono eliminati automaticamente dopo essere stati sovrascritti con una dicitura speciale. Ciò impedisce a terzi malintenzionati di recuperare dati dei lavori residui.



8-6. Crittografia password

È possibile crittografare le password memorizzate nel prodotto. Le informazioni crittografate sono le seguenti:

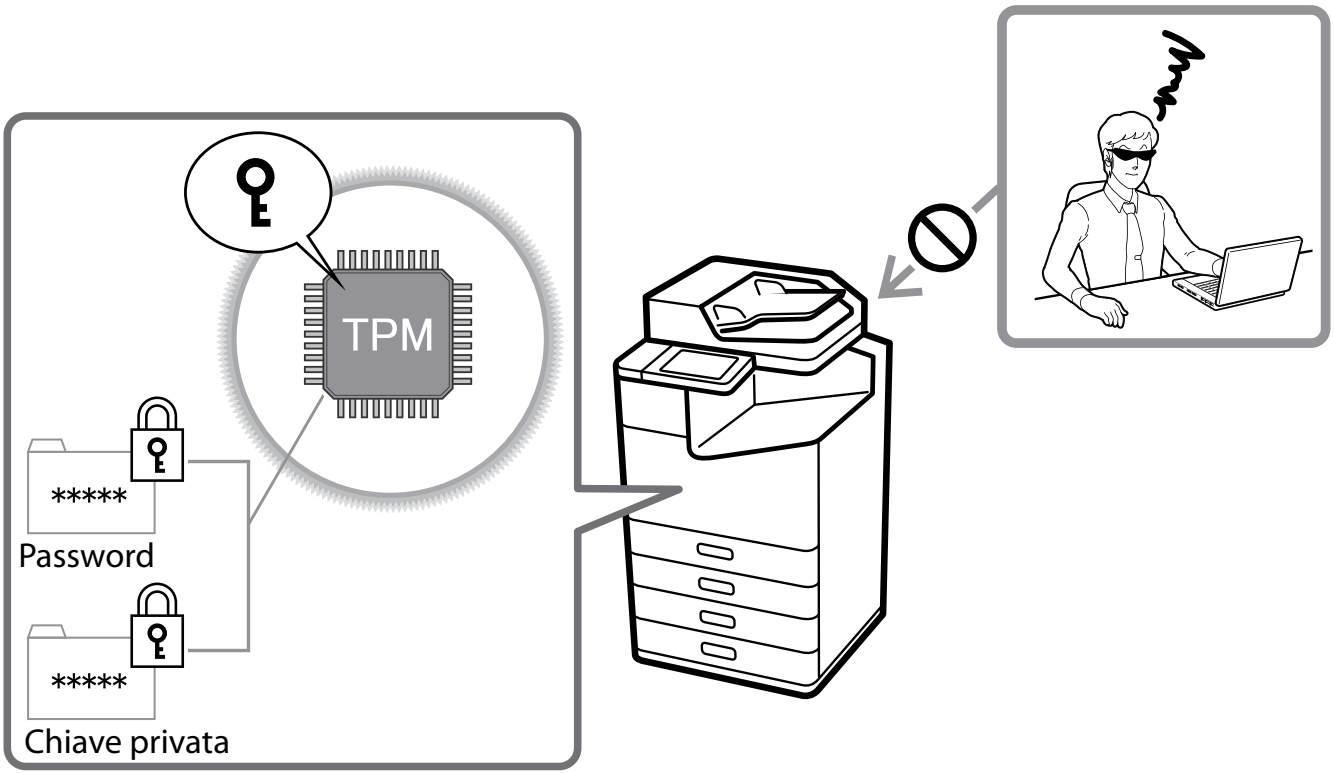
- Password amministratore.
- Password utente per il controllo degli accessi.
- Chiavi di autenticazione per dischi rigidi, chiavi private di certificati, ecc. Password per l'accesso a Scansione su cartella rete/FTP.

8-7. TPM

Nei modelli dotati di TPM (Trusted Platform Module), le chiavi di crittografia per il ripristino delle password crittografate e le informazioni sulle chiavi private sono memorizzate sul chip TPM. Il chip TPM non è accessibile dall'esterno della stampante, proteggendola da analisi non autorizzate a livello hardware.

I veri numeri casuali di TPM vengono usati per i numeri casuali utilizzati per le configurazioni tramite sessioni del browser (Web Config). I veri numeri casuali di TPM sono inoltre utilizzati per la generazione di chiavi di autenticazione per il disco rigido/SSD crittografato.

Questi modelli sono dotati di chip con specifiche TPM2.0.



8-8. Mirroring del disco rigido

Se si installa un'opzione aggiuntiva del disco rigido, anche in caso di malfunzionamento di un disco rigido è possibile continuare a svolgere tutte le funzioni con l'altro disco rigido senza perdere i dati memorizzati.

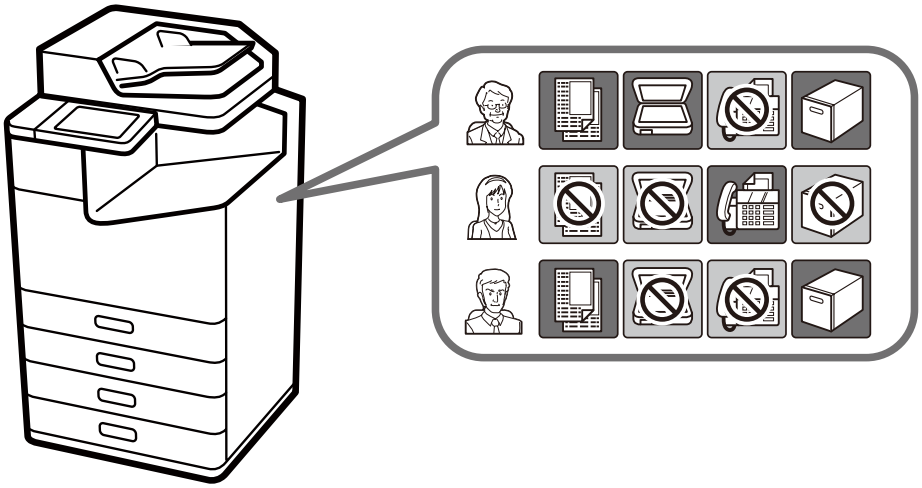
9. Limitazioni operative

9-1. Blocco pannello

Quando si utilizza il blocco pannello, è necessario inserire la password amministratore per avere accesso al pannello di controllo. Quando il pannello è protetto dalla password amministratore in uffici aperti, strutture pubbliche e luoghi simili, è possibile impedire la modifica delle impostazioni da parte degli utenti.

9-2. Controllo degli accessi

È possibile limitare l'uso delle funzioni di stampa, scansione, fax* e casella a singoli utenti per minimizzare i rischi per la sicurezza a seconda dei loro ruoli e delle loro mansioni lavorative. Inoltre, gli utenti vengono disconnessi automaticamente dopo essere stati inattivi nel pannello di controllo per un determinato periodo di tempo.



* È possibile limitare solo la trasmissione fax.

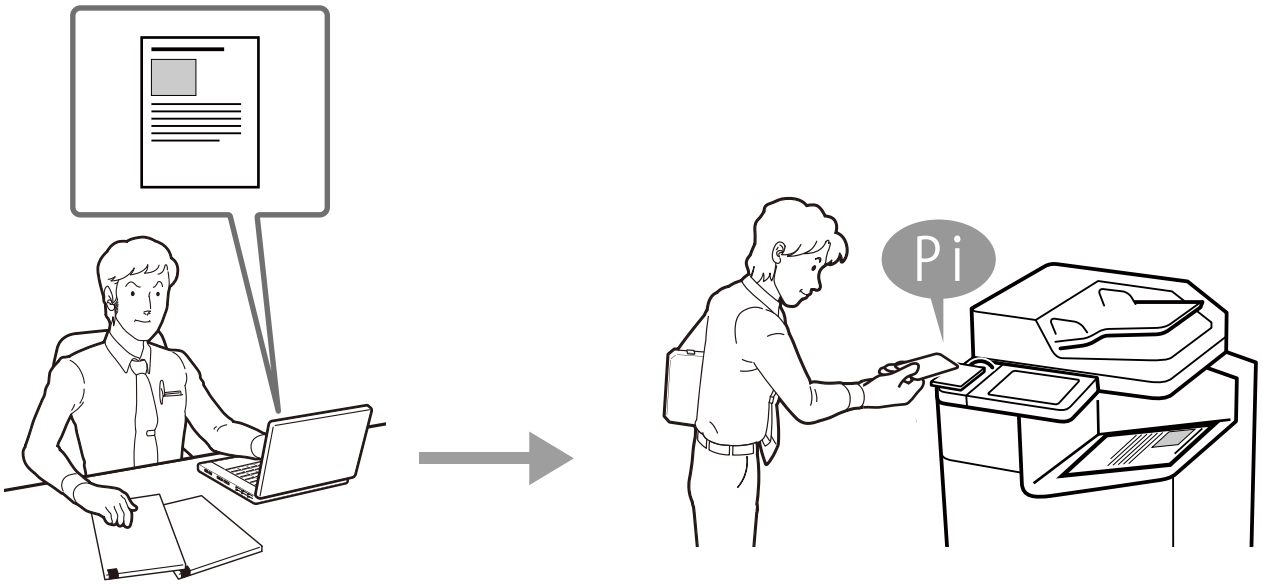
9-3. Stampa/scansione autenticata

Quando è installata la funzione opzionale Epson Print Admin o Epson Print Admin Serverless, è possibile utilizzare dispositivi di autenticazione, come l'autenticazione ID/password e i lettori di schede IC, per autenticare gli utenti che effettuano stampe o scansioni. Se gli utenti eseguono l'autenticazione e le operazioni davanti al prodotto, si evita la fuga di informazioni dai materiali stampati o dai documenti incustoditi che altri utenti potrebbero prendere per sbaglio.

Gli utenti collegati tramite LDAP e registrati sulla stampante possono utilizzare questo metodo di autenticazione.

Inoltre, con alcuni scanner indipendenti, è possibile autenticare la scansione tramite autenticazione ID/password o dispositivi di autenticazione, come i lettori di schede IC, utilizzando l'autenticazione dell'unità principale o Document Capture Pro Server Authentication Edition.

Gli utenti collegati tramite LDAP e registrati sulla stampante possono utilizzare questo metodo di autenticazione.



9-4. Criteri password

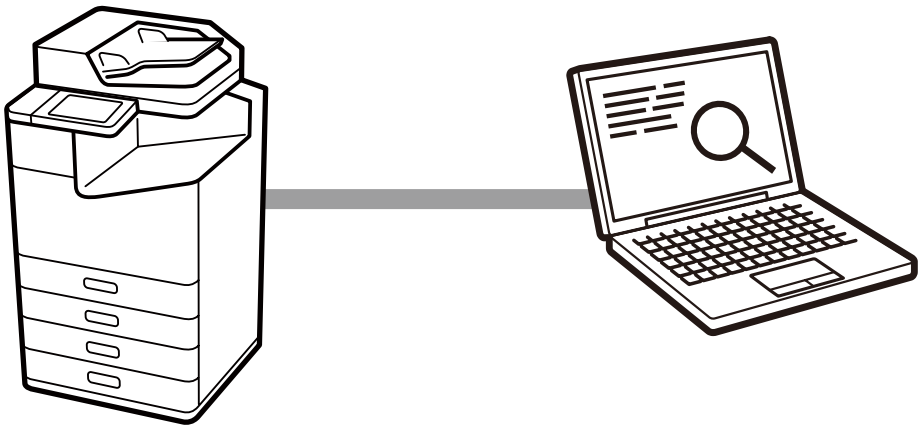
È possibile applicare criteri password per le password di amministratore, controllo degli accessi e fax. Una password forte che richieda diverse condizioni tra le seguenti può contribuire a impedire il cracking della password da parte di utenti malintenzionati.

- Numero minimo di caratteri per le password.
- Includere/non includere lettere maiuscole nelle password.
- Includere/non includere lettere minuscole nelle password.
- Includere/non includere numeri nelle password.
- Includere/non includere simboli nelle password.

9-5. Log di controllo

La funzione Log di controllo consente di registrare la cronologia di stampe, copie, scansioni, fax e modifiche alle impostazioni a scopo di verifica. Può aiutare a individuare in anticipo un eventuale uso improprio e a rintracciare i problemi di sicurezza se tale log viene verificato periodicamente.

Vengono conservati fino a 20.000 log di controllo (fino a 5.000 per alcuni modelli).



10. Sicurezza del prodotto

10-1. Aggiornamenti firmware automatici

Se gli aggiornamenti firmware automatici sono abilitati, è possibile aggiornare il firmware automaticamente a un orario specificato. Poiché gli aggiornamenti avvengono a un orario specificato, è possibile utilizzare sempre il firmware più aggiornato senza interrompere alcuna operazione.

10-2. Protezione dagli aggiornamenti firmware illegali

Durante gli aggiornamenti del firmware viene eseguita l'autenticazione con la password amministratore. Inoltre la comunicazione dati con il prodotto è protetta da HTTPS e la legittimità del firmware del prodotto viene verificata tramite firma prima della sovrascrittura del firmware. Ciò impedisce la modifica non autorizzata del firmware da parte di terzi malintenzionati.

10-3. Avvio sicuro

All'avvio, il sistema verifica la legittimità del firmware del prodotto tramite firma. Se rileva che il firmware è stato sovrascritto e si tratta di firmware non autorizzato, l'avvio viene interrotto e viene richiesto all'utente di aggiornare il firmware.

10-4. Rilevamento di infiltrazioni malware

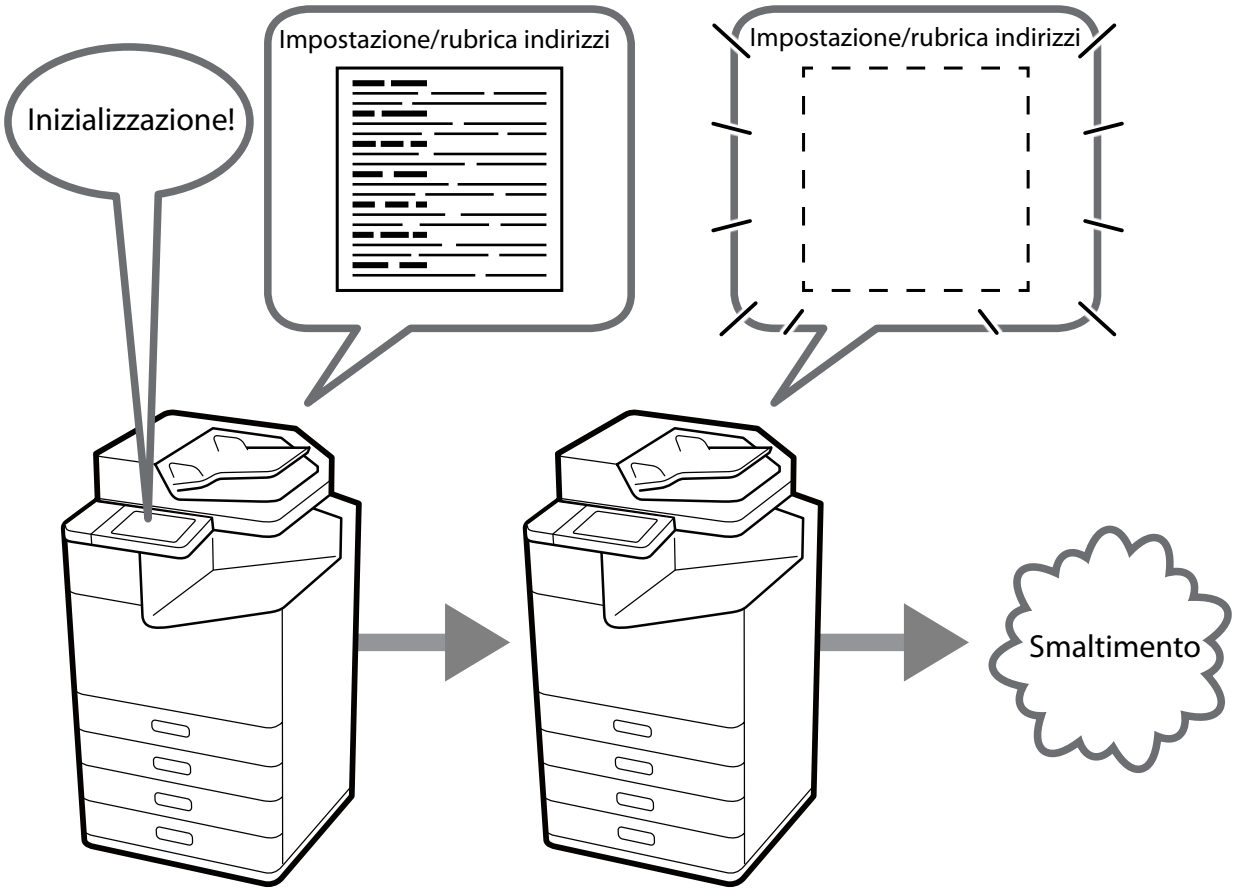
Quando il prodotto è in funzione, viene costantemente monitorata la possibile infiltrazione di malware nel firmware. Se viene rilevato un malware, il prodotto viene riavviato per eliminarlo.

11. Misure di sicurezza per lo smaltimento del prodotto

11-1. Ripristino delle impostazioni predefinite

Quando si trasferisce o si smaltisce un prodotto, è possibile riportare tutte le impostazioni (incluse quelle presenti sul disco rigido interno/SSD) ai valori di fabbrica (inizializzazione) per evitare la divulgazione di informazioni riservate.

Inoltre è possibile effettuare la cancellazione del disco rigido/SSD tramite "cancellazione mediante modifica della chiave di crittografia all'interno dell'unità di auto-crittografia (Alta velocità)" o "cancellazione mediante modifica della chiave di crittografia e sovrascrittura con una dicitura speciale (Sovrascrittura, Tripla sovrascrittura)".



12. Certificati e standard di sicurezza

12-1. ISO15408/IEEE 2600.2™

Questo prodotto ha ottenuto il certificato ISO/IEC 15408 in conformità allo standard IEEE Std. 2600.2™-2009[*1], uno standard internazionale per la sicurezza delle informazioni.

IEEE Std. 2600.2™

IEEE Std. 2600.2™ è uno standard internazionale che specifica i criteri per la sicurezza delle informazioni per le periferiche multifunzione. È possibile rafforzare globalmente la sicurezza delle periferiche multifunzione dotandole di funzionalità di sicurezza conformi allo standard, come l'identificazione e l'autenticazione utente, il controllo degli accessi, la sovrascrittura dei dati, la protezione di rete, la gestione della sicurezza, la funzionalità di autotest e i log di controllo.

ISO/IEC 15408

ISO/IEC 15408, chiamato anche Common Criteria (CC), è uno standard internazionale per la valutazione indipendente e oggettiva delle misure di sicurezza nei prodotti e nei sistemi informatici al fine di determinare se tali misure sono state progettate e implementate correttamente.

Ai fini della certificazione ISO/IEC 15408 vengono valutate versioni specifiche di firmware, manuali e altre componenti. La versione del firmware in un prodotto acquistato può essere diversa da quella certificata.

L'utilizzo di una versione certificata può comportare alcune limitazioni alle funzionalità del prodotto.

Il logo del certificato CCRA dimostra che il prodotto è stato valutato e certificato conformemente al Japan Information Technology Security Evaluation and Certification Scheme (JISEC[*2]).
Ciò non implica o garantisce che il prodotto sia completamente privo di vulnerabilità. Inoltre ciò non implica che il prodotto sia dotato di tutte le funzioni di sicurezza necessarie per qualsiasi ambiente operativo.

*1 Profilo di protezione approvato dal governo degli Stati Uniti — Profilo di protezione del governo degli Stati Uniti per i dispositivi di stampa su carta versione 1.0 (IEEE Std. 2600.2™-2009)

*2 JISEC (Japan Information Technology Security Evaluation and Certification Scheme)

Rischi per la sicurezza quando le funzioni di protocollo sono abilitate e limitazioni quando sono disabilitate

Funzioni di sicurezza/ protocollo	Rischi per la sicurezza quando sono abilitate	Limitazioni quando sono disabilitate
Bonjour	Le informazioni sui dispositivi in rete potrebbero essere lette da terzi.	Non sarà possibile effettuare ricerche tramite Bonjour dal computer.
SLP	Poiché il mittente non è autenticato, in caso di attacco spoofing può essere sfruttato per disabilitare il servizio.	Il computer non sarà in grado di utilizzare SLP per recuperare o ricercare informazioni sul dispositivo.
WSD	I dati stampati potrebbero essere letti da terzi poiché la comunicazione non è criptata.	Non sarà possibile stampare ed effettuare scansioni tramite WSD.
LLTD	Le informazioni sui dispositivi in rete potrebbero essere lette da terzi.	I dispositivi non saranno visualizzati in "Dispositivi e stampanti" in Windows.
LLMNR	Le informazioni sui dispositivi in rete potrebbero essere lette da terzi.	Non sarà possibile effettuare ricerche tramite LLMNR dal computer.
LPR	I dati stampati potrebbero essere letti da terzi poiché la comunicazione non è criptata.	Non sarà possibile stampare tramite LPR.
RAW (porta 9100/qualsiasi porta)	I dati stampati potrebbero essere letti da terzi poiché la comunicazione non è criptata.	Non sarà possibile stampare tramite la porta RAW.
IPP/IPPS	Per IPP, i dati di stampa potrebbero essere letti da terzi poiché la comunicazione non è criptata. Per IPPS non vi sono rischi di sicurezza.	Non sarà possibile stampare utilizzando IPP/IPPS, ad esempio da AirPrint o macOS.
FTP	I dati stampati potrebbero essere letti da terzi poiché la comunicazione non è criptata.	Non sarà possibile stampare o trasferire file tramite FTP.
SNMP	Per SNMPv1 e v2c, le informazioni sui dispositivi e i dati relativi alle impostazioni potrebbero essere letti da terzi poiché la comunicazione non è criptata. Per SNMPv3 non vi sono rischi di sicurezza.	Non è possibile utilizzare strumenti di gestione che utilizzano SNMP. Inoltre gli strumenti di gestione e le applicazioni fornite da Epson non saranno disponibili.

Funzioni di sicurezza/ protocollo	Rischi per la sicurezza quando sono abilitate	Limitazioni quando sono disabilitate
SSL/TLS	A seconda della versione TLS e della lunghezza della chiave impostata, la forza di crittografia potrebbe essere debole e il cifrario potrebbe essere decifrato.	La connessione tramite HTTPS da un browser non sarà possibile.
Condivisione di rete Microsoft	I dati scansionati e i dati condivisi su file potrebbero essere letti da terzi.	Il trasferimento di file e la condivisione di file in rete tramite SMB non saranno possibili.
Scansione rete (EPSON Scan)	I dati scansionati potrebbero essere letti da terzi poiché la comunicazione non è criptata.	La scansione tramite rete non sarà possibile.
PC-FAX	I dati fax in rete potrebbero essere letti da terzi poiché la comunicazione non è criptata.	La funzione PC-FAX non può essere utilizzata.

EPSON

Attenzione

- È vietata la riproduzione parziale o integrale del presente documento.
- I contenuti del presente documento sono soggetti a future modifiche senza preavviso.
- Il presente documento è a scopo esclusivamente informativo. Per maggiori dettagli sull'utilizzo, consultare il manuale relativo a ciascun prodotto.

Trademark

- Microsoft is trademark of the Microsoft group of companies.
- Wi-Fi is trademarks of Wi-Fi Alliance.
- Other product names are the trademarks or registered trademarks of their respective companies.

NPD6296-05 IT