EPSON

DS-900WN DS-800WN

Ghidul administratorului

NPD7398-00 RO

Drept de proprietate intelectuală

Mărci înregistrate

- ❏ Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome, Chromebook and Android are trademarks of Google LLC.
- ❏ Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ Notificare generală: toate celelalte mărci comerciale sunt proprietatea deținătorilor respectivi și sunt utilizate doar în scopuri de identificare.

Cuprins

Setări de securitate avansate

Utilizarea caracteristicii Epson Open Platform

Montarea unui dispozitiv de autentificare

Întreținere

Introducere

Conținutul acestui document

Acest document oferă următoarele informații pentru administratorii scanerelor.

❏ Setări de rețea

❏ Pregătirea funcției de scanare

❏ Activați și gestionați setările de securitate

❏ Efectuați întreținerea zilnică

Pentru metodele standard de utilizare a scanerului, consultați *Ghidul utilizatorului*.

Utilizarea acestui ghid

Marcaje şi simboluri

> ⚠ ***Atenție:***
> *Instrucțiuni care trebuie respectate cu atenție, pentru evitarea vătămărilor corporale.*

> ***Important:***
> *Instrucțiuni care trebuie respectate pentru evitarea deteriorării echipamentului.*

Notă:
Furnizează informații complementare şi de referință.

Informații conexe

➡ Asigură legătura cu secțiunile aferente.

Descrieri utilizate în acest manual

❏ Capturile de ecran pentru aplicații sunt din Windows 10 sau din macOS High Sierra. Conținutul afișat pe ecran diferă în funcție de model şi de situație.

❏ Ilustrațiile utilizate în acest manual sunt numai pentru referință. Chiar dacă pot fi uşor diferite față de produsul real, metodele de operare sunt identice.

Referințe sisteme de operare

Windows

În acest manual, termeni precum „Windows 11”, „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Server 2022”, „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012”, „Windows Server 2008 R2” şi „Windows Server 2008” se referă la următoarele sisteme de operare. În plus, termenul „Windows” este utilizat cu referire la toate versiunile.

- ❏ Sistem de operare Microsoft® Windows® 11
- ❏ Sistem de operare Microsoft® Windows® 10
- ❏ Sistem de operare Microsoft® Windows® 8.1
- ❏ Sistem de operare Microsoft® Windows® 8
- ❏ Sistem de operare Microsoft® Windows® 7
- ❏ Sistem de operare Microsoft® Windows Server® 2022
- ❏ Sistem de operare Microsoft® Windows Server® 2019
- ❏ Sistem de operare Microsoft® Windows Server® 2016
- ❏ Sistem de operare Microsoft® Windows Server® 2012 R2
- ❏ Sistem de operare Microsoft® Windows Server® 2012
- ❏ Sistem de operare Microsoft® Windows Server® 2008 R2
- ❏ Sistem de operare Microsoft® Windows Server® 2008

Mac OS

În acest manual, termenul „Mac OS” este utilizat cu referire la Mac OS X 10.9 sau o versiune ulterioară, precum și la macOS 11 sau o versiune ulterioară.

Note despre parola de administrator

Note despre parola de administrator

Acest dispozitiv vă permite să setați o parolă de administrator pentru a împiedica utilizatori terți neautorizați să acceseze sau să modifice setările dispozitivului sau setările de rețea stocate în dispozitiv atunci când acesta este conectat la o rețea.

Dacă setați o parolă de administrator, trebuie să introduceți parola atunci când modificați setările în software-ul de configurare, cum ar fi Web Config.

Parola inițială de administrator este setată pe scaner, dar o puteți schimba la orice altă parolă.

Parola inițială de administrator

Parola inițială de administrator variază în funcție de eticheta atașată pe produs. Dacă există o etichetă „PASSWORD" atașată pe spate, introduceți numărul din 8 cifre afișat pe etichetă. Dacă nu este atașată nicio etichetă „PASSWORD", introduceți numărul de serie pe eticheta atașată pe spatele produsului pentru parola inițială de administrator.

Vă recomandăm să schimbați parola inițială de administrator de la setarea implicită.

Notă:
Niciun nume de utilizator nu este setat ca implicit.

Operațiuni care necesită parola de administrator

Dacă vi se solicită să introduceți parola de administrator în timpul următoarelor operațiuni, introduceți parola de administrator setată pe produs.

- ❏ Când vă conectați la setările avansate pentru Web Config
- ❏ Când operați un meniu pe panoul de comandă care a fost blocat de administrator
- ❏ Când modificați setările dispozitivului în aplicație
- ❏ Când actualizați firmware-ul dispozitivului
- ❏ Când schimbați sau resetați parola de administrator

Schimbarea parolei de administrator

Puteți modifica din panoul de comandă al produsului sau din Web Config.

La schimbarea parolei, noua parolă trebuie să aibă între 8 și 20 de caractere și să conțină doar caractere și simboluri alfanumerice de un singur octet.

Resetarea parolei de administrator

Puteți reseta parola de administrator la setarea inițială de la panoul de comandă al produsului sau din Web Config.

Dacă ați uitat parola și nu o puteți reseta la setările implicite, produsul trebuie reparat. Contactați distribuitorul local.

Setări necesare pentru scopul dumneavoastră

Setări necesare pentru scopul dumneavoastră

Consultați următoarele pentru a efectua setările necesare în funcție de scopul dumneavoastră.

Conectarea scanerului la rețea

Scop	Setări necesare
Doresc să conectez scanerul la rețea.	Configurați scanerul pentru scanarea în rețea. „Conectarea scanerului la rețea" la pagina 16
Doresc să conectez scanerul la un computer nou.	Efectuați setările de rețea pentru scanerul dumneavoastră pe noul computer. „Adăugarea sau ștergerea computerului sau a dispozitivelor" la pagina 22

Setări pentru scanare

Scop	Setări necesare
Doresc să trimit imagini scanate prin e-mail. (Scanare către e-mail)	1. Configurați serverul de e-mail pe care doriți să îl corelați. „Înregistrarea unui server de e-mail" la pagina 45 2. Înregistrați adresa de e-mail a destinatarului în **Persoane de contact** (opțional). Înregistrând adresa de e-mail nu trebuie să o introduceți de fiecare dată când doriți să trimiteți ceva, puteți doar să o selectați din Contacte. „Disponibilitatea contactelor" la pagina 54
Doresc să salvez imaginile scanate într-un folder din rețea. (Scanare către folder din rețea/FTP)	1. Creați un folder în rețeaua unde doriți să salvați imaginile. „Crearea unui folder de rețea" la pagina 48 2. Înregistrați calea către folder în **Persoane de contact** (opțional). Înregistrând calea de folder nu trebuie să o introduceți de fiecare dată când doriți să trimiteți ceva, puteți doar să o selectați din Contacte. „Disponibilitatea contactelor" la pagina 54
Doresc să salvez imaginile scanate într-un serviciu cloud. (Scanare către cloud)	Instalați Epson Connect. Consultați site-ul web al portalului Epson Connect pentru detalii privind configurarea. La configurare, aveți nevoie de un cont de utilizator pentru serviciul de stocare online la care doriți să vă conectați. https://www.epsonconnect.com/ http://www.epsonconnect.eu (doar Europa)

Personalizarea afișajului panoului de comandă

Scop	Setări necesare
Doresc să schimb elementele afișate pe panoul de comandă al scanerului.	Setați **Presetări** sau **Editare ecran principal**. Puteți înregistra setările preferate de scanare pe panoul de comandă și puteți edita elementele afișate. „Personalizarea afișajului panoului de comandă" la pagina 67

Setarea funcțiilor de securitate de bază

Scop	Setări necesare
Doresc să împiedic pe oricine altcineva decât administratorul să modifice setările scanerului.	Setați o parolă de administrator pentru scaner. „Setări administrative" la pagina 75
Doresc să dezactivez utilizarea scanerelor cu conexiuni USB.	Dezactivați interfața externă. „Dezactivarea Interfeței externe" la pagina 83

Setarea funcțiilor avansate de securitate

Scop	Setări necesare
Doresc să controlez ce protocoale să folosesc.	Activați sau dezactivați protocoalele. „Controlarea utilizând protocoale" la pagina 90
Doresc să criptez calea de comunicare.	1. Configurați certificatul dumneavoastră digital. „Utilizarea unui certificat digital" la pagina 93 2. Configurați comunicarea SSL/TLS. „Comunicare SSL/TLS cu scanerul" la pagina 98
Doresc să folosesc comunicarea criptată (IPsec). Doresc să pot folosi software-ul doar de pe un anumit computer (filtrare IP).	Configurați politici pentru filtrarea traficului. „Comunicare criptată utilizând filtrarea IPsec/IP" la pagina 99
Doresc să folosesc un scaner într-o rețea IEEE802.1X.	Configurați IEEE802.1X pentru scaner. „Conectarea scanerului la o rețea IEEE802.1X" la pagina 111

Sincronizarea scanerului cu un sistem de autentificare

Obțineți o cheie de produs de la site-ul web dedicat și activați Epson Open Platform pe scanerul dumneavoastră.

„Utilizarea caracteristicii Epson Open Platform" la pagina 119

Utilizarea unei opțiuni de autentificare (Epson Print Admin/Epson Print Admin Serverless)

Aveți nevoie de o cheie de licență pentru a utiliza opțiunea.

Contactați distribuitorul dumneavoastră pentru mai multe informații.

Notă:
Nu puteți utiliza Epson Print Admin Serverless când sistemul este sincronizat cu Epson Open Platform.

Setări de rețea

Conectarea scanerului la rețea

Această secțiune explică procedura de conectare a scanerului la rețea utilizând panoul de comandă al scanerului.

Notă:
Dacă scanerul și computerul sunt în același segment, vă puteți conecta și folosind programul de instalare.

Pentru a porni programul de instalare, accesați următorul site web, apoi introduceți numele produsului. Mergeți la ***Configurarea*** *și apoi începeți configurarea.*

https://epson.sn

Puteți vizualiza instrucțiunile de operare în Manuale video pe web. Accesați următorul URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

Înainte de stabilirea conexiunii la rețea

Înainte de a vă conecta la rețea, verificați în prealabil metoda de conectare și informațiile de setare a conexiunii.

Colectarea informațiilor privind setarea conexiunii

Pregătiți informațiile de setare necesare pentru conectare. Verificați următoarele informații în avans.

Divizii	Elemente	Notă
Metodă de conectare dispozitiv	❏ Ethernet ❏ Wi-Fi	Stabiliți modul de conectare a scanerului la rețea. Pentru LAN cablat, se conectează la switch-ul LAN. Pentru Wi-Fi, se conectează la rețeaua (SSID) punctului de acces.
Informații conexiune LAN	❏ Adresă IP ❏ Mască subrețea ❏ Gateway implicit	Stabiliți adresa IP care se va atribui scanerului. Când atribuiți adresa IP în mod static, toate valorile sunt obligatorii. Când atribuiți adresa IP în mod dinamic, utilizând funcția DHCP, aceste informații nu sunt obligatorii, deoarece sunt setate automat.
Informații conexiune Wi-Fi	❏ SSID ❏ Parolă	Acestea sunt SSID (numele rețelei) și parola punctului de acces la care se conectează scanerul. Dacă a fost setată filtrarea adresei MAC, înregistrați adresa MAC a scanerului înainte de a înregistra scanerul. Consultați următoarele pentru standardele acceptate. „Specificații de rețea” la pagina 29
Informații server DNS	❏ Adresa IP pentru DNS primar ❏ Adresa IP pentru DNS secundar	Acestea sunt necesare la specificarea serverelor DNS. Adresa DNS secundară este setată atunci când sistemul are o configurație redundantă și există un server DNS secundar. Dacă faceți parte dintr-o organizație de mici dimensiuni și nu setați serverul DNS, setați adresa IP a routerului.

Divizii	Elemente	Notă
Informații server proxy	❏ Nume server proxy	Setați această opțiune atunci când mediul de rețea utilizează serverul proxy pentru a accesa internetul din intranet, iar dumneavoastră utilizați funcția pentru accesul direct al scanerului la internet. Pentru următoarele funcții, scanerul se conectează direct la internet. ❏ Epson Connect Services ❏ Servicii cloud ale altor companii ❏ Actualizări firmware ❏ Trimiterea imaginilor scanate la SharePoint(WebDAV)
Informații privind numărul portului	❏ Număr de port de deblocat	Verificați numărul portului utilizat de scaner și de computer și eliberați portul blocat de un firewall, dacă este necesar. Consultați următoarele pentru numărul de port utilizat de scaner. „Utilizarea portului pentru scaner” la pagina 32

Atribuirea adresei IP

Acestea sunt următoarele tipuri de atribuire de adresă IP.

Adresă IP statică:

Atribuiți adresa IP predeterminată la scaner (gazdă) manual.

Informațiile pentru conectare la rețea (mască de subrețea, gateway implicit, server DNS etc.) trebuie setate manual.

Adresa IP nu se modifică nici atunci când dispozitivul este oprit, deci acest lucru este util atunci când doriți să gestionați dispozitive cu un mediu unde nu puteți modifica adresa IP sau doriți să gestionați dispozitivele utilizând adresa IP. Recomandăm setări pentru scaner, server etc. pe care le accesează numeroase computere. De asemenea, când utilizați funcții de securitate precum IPsec/IP Filtering, atribuiți o adresă IP fixă, astfel încât adresa IP să nu se modifice.

Atribuire automată prin utilizarea funcției DHCP (adresă IP dinamică):

Atribuiți automat adresa IP scanerului (gazdei) prin utilizarea funcției DHCP a serverului sau a routerului DHCP.

Informațiile pentru conectarea la rețea (mască de subrețea, gateway implicit, server DNS etc.) sunt setate automat, pentru a putea conecta cu ușurință dispozitivul la rețea.

Dacă dispozitivul sau routerul este oprit sau în funcție de setările serverului DHCP, este posibil ca adresa IP să se modifice la reconectare.

Se recomandă gestionarea dispozitivelor cu altă adresă IP și comunicarea cu protocoale care pot respecta adresa IP.

Notă:
Când utilizați funcția de rezervare adresă IP a DHCP, puteți atribui aceeași adresă IP dispozitivelor în orice moment.

Server DNS și server proxy

Serverul DNS are un nume de gazdă, un nume de domeniu al adresei de e-mail etc. în asociere cu informațiile privind adresa IP.

Comunicațiile sunt imposibile în cazul în care cealaltă parte este descrisă prin nume de gazdă, nume de domeniu etc. când computerul sau scanerul efectuează comunicația IP.

Interoghează serverul DNS pentru informațiile respective și obține adresa IP a celeilalte părți. Acest proces se numește rezoluție de nume.

În consecință, dispozitive precum computerele și scanerele pot comunica prin intermediul adresei IP.

Rezoluția de nume este necesară pentru ca scanerul să comunice utilizând funcția de e-mail sau funcția de conectare la internet.

Când utilizați aceste funcții, efectuați setările serverului DNS.

Când atribuiți adresa IP a scanerului utilizând funcția DHCP a serverului sau routerului DHCP, acesta este setat automat.

Serverul proxy este plasat la gateway-ul dintre rețea și internet și efectuează comunicarea cu computerul, scanerul și internetul (server opus) din partea fiecăruia dintre acestea. Serverul opus comunică doar cu serverul proxy. Prin urmare, informațiile despre scaner, cum ar fi adresa IP și numărul de port nu pot fi citite și este de așteptat o securitate sporită.

Când vă conectați la internet prin intermediul unui server proxy, configurați serverul proxy pe scaner.

Conectarea la rețea de la panoul de comandă

Conectați scanerul la rețea folosind panoul de comandă al scanerului.

Alocarea adresei IP

Configurați elementele de bază, precum Adresă gazdă, Mască subrețea, Gateway implicit.

Această secțiune explică procedura de configurare a unei adrese IP statice.

1. Porniți scanerul.
2. Selectați **Setări** pe ecranul principal de pe panoul de comandă al scanerului.
3. Selectați **Setări rețea** > **Complex** > **TCP/IP**.
4. Selectați **Manual** pentru **Obținere parolă IP**.

   Când setați adresa IP automat utilizând funcția DHCP a routerului, selectați **Automat**. În acel caz, **Adresă IP**, **Mască subrețea** și **Gateway implicit** din pașii 5 – 6 sunt, de asemenea, setate automat, deci mergeți la pasul 7.
5. Introduceți adresa IP.

   Focalizarea este mutată pe segmentul următor sau pe segmentul anterior, separate prin virgulă, dacă selectați ◀ și ▶.

   Confirmați valoarea reflectată pe ecranul anterior.
6. Configurați **Mască subrețea** și **Gateway implicit**.

   Confirmați valoarea reflectată pe ecranul anterior.

> ***Important:***
>
> *În cazul în care combinația dintre Adresă IP, Mască subrețea și Gateway implicit este incorectă,* ***Pornire configurare*** *este inactiv și nu puteți continua cu setările. Confirmați faptul că nu există nicio eroare în intrări.*

7. Introduceți adresa IP pentru serverul DNS primar.

   Confirmați valoarea reflectată pe ecranul anterior.

   Notă:
   *Când selectați **Automat** pentru setările de alocare adresă IP, puteți selecta setările de server DNS din **Manual** sau **Automat**. Dacă nu puteți obține automat adresa de server DNS, selectați **Manual** și introduceți adresa de server DNS. Apoi, introduceți direct adresa de server DNS secundar. Dacă selectați **Automat**, mergeți la pasul 9.*

8. Introduceți adresa IP pentru serverul DNS secundar.

   Confirmați valoarea reflectată pe ecranul anterior.

9. Atingeți **Pornire configurare**.

Setarea serverului proxy

Configurați serverul proxy dacă ambele aspecte sunt adevărate.

❏ Serverul proxy este conceput pentru conexiunea la Internet.

❏ Când utilizați o funcție prin care scanerul se conectează direct la internet, precum serviciul Epson Connect sau serviciile cloud ale unei alte companii.

1. Selectați **Setări** de pe ecranul principal.

   La efectuarea setărilor după setarea adresei IP, este afișat ecranul **Complex**. Treceți la pasul 3.

2. Selectați **Setări rețea** > **Complex**.

3. Selectați **Server proxy**.

4. Selectați **Se utiliz.** pentru **Setări server proxy**.

5. Introduceți adresa serverului proxy în formatul IPv4 sau FQDN.

   Confirmați valoarea reflectată pe ecranul anterior.

6. Introduceți numărul de port pentru serverul proxy.

   Confirmați valoarea reflectată pe ecranul anterior.

7. Atingeți **Pornire configurare**.

Conectarea la Ethernet

Conectați scanerul la rețea, utilizând un cablu LAN și apoi verificați conexiunea.

1. Conectați scanerul și hubul (switch LAN) prin folosirea unui cablu LAN.

2. Selectați  de pe ecranul principal.

3. Selectați **Ruter**.

4. Asigurați-vă că setările Conexiune și Adresă IP sunt corecte.

5. Atingeți **Închidere**.

Conectarea la LAN wireless (Wi-Fi)

Puteți conecta scanerul la rețeaua LAN wireless (Wi-Fi) în mai multe moduri. Alegeți metoda de conexiune care corespunde mediului și condițiilor de utilizare.

În cazul în care cunoașteți informațiile legate de routerul wireless, precum SSID și parola, puteți efectua setările manual.

Dacă routerul wireless acceptă WPS, puteți efectua setările folosind configurarea prin apăsarea unui buton.

După conectarea scanerului la rețea, conectați-vă la scaner de la dispozitivul pe care doriți să îl utilizați (computer, dispozitiv inteligent, tabletă etc.)

Notă privind utilizarea unei conexiuni Wi-Fi 5 GHz

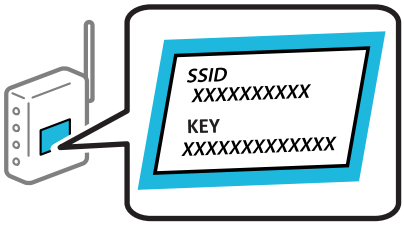
Acest scaner folosește în mod normal W52 (36ch) ca un canal atunci când se conectează la Wi-Fi Direct (Simple AP). Deoarece canalul pentru conexiunea LAN fără fir (Wi-Fi) este selectat automat, canalul utilizat poate diferi atunci când este utilizat în același timp cu o conexiune Wi-Fi Direct. În cazul în care canalele sunt diferite, comunicarea datelor cu scanerul poate fi lentă. Dacă nu interferează cu utilizarea, conectați-vă la SSID în banda de 2,4 GHz. În banda de frecvență de 2,4 GHz, canalele utilizate se vor potrivi.

Când setați rețeaua LAN fără fir la 5 GHz, vă recomandăm să dezactivați Wi-Fi Direct.

Efectuarea setărilor Wi-Fi prin introducerea unui SSID și a parolei

Puteți configura o rețea Wi-Fi prin introducerea informațiilor necesare pentru conectarea la un router wireless de la panoul de comandă al scanerului. Pentru a configura folosind această metodă, aveți nevoie de SSID-ul și parola pentru un router wireless.

Notă:
Dacă utilizați un router wireless cu setările implicite, SSID-ul și parola se află pe etichetă. Dacă nu cunoașteți SSID-ul și parola, contactați persoana care a configurat routerul wireless sau consultați documentația furnizată routerul wireless.



1. Apăsați  pe ecranul principal.
2. Selectați **Ruter**.
3. Atingeți **Start configurare**.

   În cazul în care conexiunea la rețea este deja configurată, sunt afișate detaliile conexiunii. Atingeți **Schimbați la conexiunea Wi-Fi.** sau **Modificați setările** pentru a modifica setările.
4. Selectați **Expert configurare Wi-Fi**.

5. Urmați instrucțiunile afișate pe ecran pentru a selecta SSID-ul, introduceți parola pentru router-ul wireless și începeți configurarea.

   Dacă doriți să verificați starea conexiunii la rețea a scanerului după finalizarea configurării, consultați linkul de informații de mai jos pentru detalii relevante.

   Notă:
   - ❏ *Dacă nu cunoașteți SSID-ul, verificați dacă acesta este scris pe eticheta routerului wireless. Dacă utilizați routerul wireless cu setările sale implicite, utilizați SSID-ul scris pe etichetă. Dacă nu puteți găsi informațiile, consultați documentația furnizată cu routerul wireless.*
   - ❏ *Parola este sensibilă la litere mari și mici.*
   - ❏ *Dacă nu cunoașteți parola, verificați dacă informația este scrisă pe eticheta routerului wireless. Pe etichetă, parola poate fi trecută ca „Network Key”, „Wireless Password”, etc. Dacă utilizați routerul wireless cu setările sale implicite, utilizați parola scrisă pe etichetă.*
   - ❏ *Dacă nu puteți vedea SSID la care doriți să vă conectați, utilizați software sau o aplicație pentru a configura Wi-Fi de la computerul sau dispozitivul dumneavoastră inteligent, cum ar fi smartphone sau tabletă. Pentru mai multe informații, introduceți „https://epson.sn” în browserul dumneavoastră pentru a accesa site-ul web, introduceți numele produsului dumneavoastră și mergeți la* ***Configurarea****.*

Informații conexe

➡ „Verificarea stării conexiunii la rețea” la pagina 28

Efectuarea setărilor Wi-Fi prin Push Button Setup (WPS)

Puteți configura automat o rețea Wi-Fi prin apăsarea unui buton pe routerul wireless. Dacă sunt îndeplinite următoarele condiții, puteți configura prin utilizarea acestei metode.

❏ Routerul wireless este compatibil cu WPS (Wi-Fi Protected Setup).

❏ Conexiunea Wi-Fi curentă a fost stabilită prin apăsarea unui buton pe routerul wireless.

Notă:
Dacă nu puteți găsi butonul sau efectuați configurarea utilizând software-ul, consultați documentația furnizată cu routerul wireless.

1. Apăsați  pe ecranul principal.
2. Selectați **Ruter**.
3. Atingeți **Start configurare**.

   În cazul în care conexiunea la rețea este deja configurată, sunt afișate detaliile conexiunii. Atingeți **Schimbați la conexiunea Wi-Fi.** sau **Modificați setările** pentru a modifica setările.
4. Selectați **Configurare cu buton fizic (WPS)**.
5. Urmați instrucțiunile de pe ecran.

   Dacă doriți să verificați starea conexiunii la rețea a scanerului după finalizarea configurării, consultați linkul de informații de mai jos pentru detalii relevante.

   Notă:
   În caz de întrerupere a conexiunii, reporniți routerul wireless, apropiați-l de scaner și încercați din nou.

Informații conexe

➡ „Verificarea stării conexiunii la rețea” la pagina 28

Efectuarea setărilor prin PIN Code Setup (WPS)

Vă puteți conecta automat la un router wireless prin utilizarea unui cod PIN. Puteți utiliza această metodă pentru a configura dacă un router wireless este capabil de WPS (Wi-Fi Protected Setup). Utilizați un computer pentru a introduce un cod PIN în routerul wireless.

1. Apăsați  pe ecranul principal.
2. Selectați **Ruter**.
3. Atingeți **Start configurare**.

   În cazul în care conexiunea la rețea este deja configurată, sunt afișate detaliile conexiunii. Atingeți **Schimbați la conexiunea Wi-Fi.** sau **Modificați setările** pentru a modifica setările.
4. Selectați **Altele** > **Config cod PIN (WPS)**
5. Urmați instrucțiunile de pe ecran.

   Dacă doriți să verificați starea conexiunii la rețea a scanerului după finalizarea configurării, consultați linkul de informații de mai jos pentru detalii relevante.

   Notă:
   Consultați documentația furnizată cu routerul wireless pentru detalii privind introducerea unui cod PIN.

Informații conexe

➡ „Verificarea stării conexiunii la rețea” la pagina 28

Adăugarea sau ștergerea computerului sau a dispozitivelor

Conectarea la un scaner care a fost conectat la rețea

Când scanerul a fost deja conectat la rețea, puteți conecta un computer sau un dispozitiv inteligent la scaner prin rețea.

Utilizarea unui scaner de rețea de la un al doilea computer

Recomandăm utilizarea programului de instalare pentru conectarea scanerului la un computer.

Pentru a porni programul de instalare, accesați următorul site web, apoi introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.

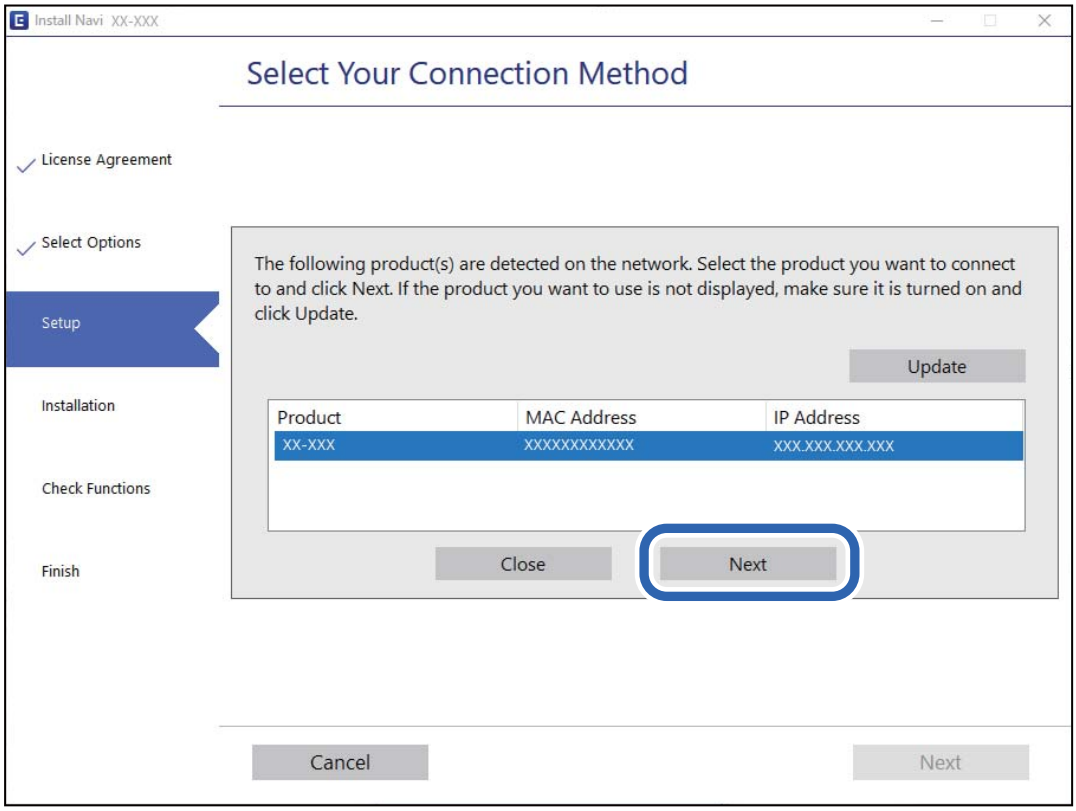
https://epson.sn

Puteți vizualiza instrucțiunile de operare în Manuale video pe web. Accesați următorul URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

Selectarea scanerului

Urmați instrucțiunile de pe ecran până la afișarea ecranului următor, selectați numele scanerului la care doriți să vă conectați, apoi faceți clic pe **Înainte**.



Urmați instrucțiunile de pe ecran.

Utilizarea unui scaner de rețea de la un dispozitiv inteligent

Puteți conecta un dispozitiv inteligent la scaner folosind una dintre următoarele metode.

Conectarea printr-un router wireless

Conectați dispozitivul inteligent la aceeași rețea Wi-Fi (SSID) ca scanerul.

Pentru detalii suplimentare, consultați următoarele informații.

„Efectuarea setărilor de conectare la un dispozitiv inteligent” la pagina 27

Conectarea prin Wi-Fi Direct

Conectați dispozitivul inteligent direct la scaner, fără un router wireless.

Pentru detalii suplimentare, consultați următoarele informații.

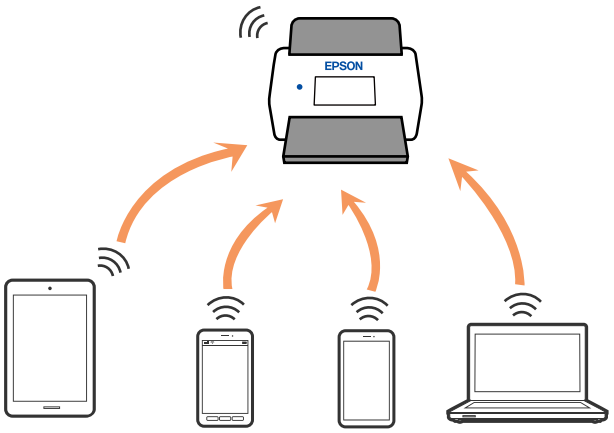
„Conectarea directă a unui dispozitiv inteligent la scaner (Wi-Fi Direct)” la pagina 24

Conectarea directă a unui dispozitiv inteligent la scaner (Wi-Fi Direct)

Wi-Fi Direct (Simple AP) permite conectarea unui dispozitiv inteligent direct la scaner fără un router wireless și scanarea de la dispozitivul inteligent.

Despre Wi-Fi Direct

Utilizați această metodă de conectare dacă nu folosiți o rețea Wi-Fi acasă sau la birou sau dacă doriți să conectați scanerul și computerul sau dispozitivul inteligent în mod direct. În acest mod, scanerul acționează ca router wireless și puteți conecta dispozitivele la scaner, fără a fi necesară utilizarea unui router wireless standard. Cu toate acestea, dispozitivele conectate direct la scaner nu pot comunica între ele prin intermediul scanerului.



Scanerul poate fi conectat utilizând simultan o conexiune Wi-Fi sau Ethernet, și Wi-Fi Direct (Simple AP). Totuși, dacă inițiați o conexiune de rețea în modul Wi-Fi Direct (Simple AP) când scanerul este conectat prin Wi-Fi, conexiunea Wi-Fi este deconectată temporar.

Conectarea la un dispozitiv inteligent utilizând Wi-Fi Direct

Această metodă permite conectarea scanerului direct la dispozitivele inteligente, fără un router wireless.

1. Selectați  de pe ecranul principal.
2. Selectați **Wi-Fi Direct**.
3. Selectați **Start configurare**.
4. Porniți Epson Smart Panel pe dispozitivul inteligent.
5. Urmați instrucțiunile din Epson Smart Panel pentru conectarea la scaner.

   Când dispozitivul inteligent este conectat la scaner, treceți la pasul următor.
6. Pe panoul de comandă al scanerului, selectați **Finalizat**.

Deconectarea conexiunii Wi-Fi Direct (Simple AP)

Există două metode disponibile pentru a dezactiva o conexiune Wi-Fi Direct (Simple AP); puteți dezactiva toate conexiunile utilizând panoul de comandă al scanerului sau puteți dezactiva fiecare conexiune de la computer sau dispozitivul inteligent.

Când doriți să dezactivați toate conexiunile, selectați  > **Wi-Fi Direct** > **Start configurare** > **Schimbare** > **Dezactivare Wi-Fi Direct**.

Important:

Când conexiunea Wi-Fi Direct (Simple AP) este dezactivată, toate computerele și dispozitivele inteligente conectate la scaner în conexiunea Wi-Fi Direct (Simple AP) sunt deconectate.

Notă:

Dacă doriți să deconectați un anumit dispozitiv, deconectați-vă de la dispozitiv, nu de la scaner. Utilizați una dintre următoarele metode pentru a deconecta conexiunea Wi-Fi Direct (Simple AP) de la dispozitiv.

- ❏ *Deconectați conexiunea Wi-Fi de la rețeaua imprimantei (SSID).*
- ❏ *Conectați la o rețea cu alt nume (SSID).*

Modificarea setărilor Wi-Fi Direct (Simple AP) precum SSID

Când conexiunea Wi-Fi Direct (Simple AP) este activată, puteți modifica setările din  > **Wi-Fi Direct** > **Start configurare** > **Schimbare**, apoi sunt afișate următoarele elemente de meniu.

Schimbare nume rețea

Schimbați denumirea rețelei (SSID) Wi-Fi Direct (Simple AP) utilizată pentru conectarea la scaner cu o denumire arbitrară. Puteți seta denumirea rețelei (SSID) în caractere ASCII afișate pe tastatura virtuală a panoului de comandă. Puteți introduce până la 22 de caractere.

Când schimbați denumirea rețelei (SSID), toate dispozitivele conectate sunt deconectate. Folosiți noua denumire de rețea (SSID) dacă doriți să reconectați dispozitivul.

Modificare parolă

Modificați parola pentru Wi-Fi Direct (Simple AP) pentru conectarea scanerului la valoarea arbitrară. Puteți defini parola în caractere ASCII afișate pe tastatura software de pe panoul de comandă. Puteți introduce între 8 și 22 de caractere.

Când schimbați parola, toate dispozitivele conectate sunt deconectate. Utilizați noua parolă dacă doriți să reconectați dispozitivul.

Schimbare bandă de frecvență

Schimbați domeniul de frecvență al Wi-Fi Direct utilizat pentru conectarea la scaner. Puteți selecta 2,4 GHz sau 5 GHz.

Când schimbați domeniului de frecvență, toate dispozitivele conectate sunt deconectate. Reconectați dispozitivul.

Rețineți că nu puteți reconecta de la dispozitivele care nu sunt compatibile cu domeniul de frecvență de 5 GHz atunci când schimbați la 5 GHz.

În funcție de regiune, este posibil ca această setare să nu fie afișată.

Dezactivare Wi-Fi Direct

Dezactivați setările Wi-Fi Direct (Simple AP) ale scanerului. La dezactivarea acestora, toate dispozitivele conectate la scaner prin conexiunea Wi-Fi Direct (Simple AP) sunt deconectate.

Restaurare setări implicite

Restabiliți toate setările Wi-Fi Direct (Simple AP) la valorile lor implicite.

Informațiile de conectare Wi-Fi Direct (Simple AP) ale dispozitivului inteligent salvată pe scaner sunt șterse.

Notă:
*De asemenea, puteți defini următoarele setări din fila **Rețea** > **Wi-Fi Direct** din Web Config.*

- ❏ *Activarea sau dezactivarea Wi-Fi Direct (Simple AP)*
- ❏ *Schimbarea denumirii rețelei (SSID)*
- ❏ *Modificarea parolei*
- ❏ *Schimbarea domeniului de frecvență*
  În funcție de regiune, este posibil ca această setare să nu fie afișată.
- ❏ *Restabilirea setărilor Wi-Fi Direct (Simple AP)*

Restabilirea conexiunii la rețea

Această secțiune explică modul de setare a conexiunii de rețea și de schimbare a metodei de conexiune atunci când schimbați routerul wireless sau computerul.

Când schimbați routerul wireless

Când schimbați routerul wireless, efectuați setările pentru conexiunea dintre computer sau dispozitivul inteligent la scaner.

Trebuie să efectuați aceste setări dacă modificați furnizorul de servicii internet sau faceți alte modificări.

Efectuarea setărilor de conectare la computer

Recomandăm utilizarea programului de instalare pentru conectarea scanerului la un computer.

Pentru a porni programul de instalare, accesați următorul site web, apoi introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.

https://epson.sn

Puteți vizualiza instrucțiunile de operare în Manuale video pe web. Accesați următorul URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

Selectarea unei metode de conectare

Urmați instrucțiunile de pe ecran. Pe ecranul **Selectați opțiunea de instalare**, selectați **Configurați din nou conexiunea pentru Imprimantă (în cazul folosirii unui nou router de rețea, în cazul schimbării conexiunii de la USB la rețea etc.)**, apoi selectați **Înainte**.

Pentru finalizarea configurării, urmați instrucțiunile de pe ecran.

Dacă nu vă puteți conecta, consultați următoarele pentru a încerca să rezolvați problema.

„Nu se poate realiza conexiunea la rețea” la pagina 33

Efectuarea setărilor de conectare la un dispozitiv inteligent

Puteți utiliza scanerul de la un dispozitiv inteligent atunci când conectați scanerul la aceeași rețea Wi-Fi (SSID) ca dispozitiv inteligent. Pentru a utiliza scanerul de la un dispozitiv inteligent, accesați următorul site web și apoi introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.

https://epson.sn

Accesați site-ul web de pe dispozitivul inteligent pe care doriți să-l conectați la scaner.

Când schimbați computerul

Când schimbați computerul, efectuați setările de conexiune dintre computer și scaner.

Efectuarea setărilor de conectare la computer

Recomandăm utilizarea programului de instalare pentru conectarea scanerului la un computer.

Pentru a porni programul de instalare, accesați următorul site web, apoi introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.

https://epson.sn

Puteți vizualiza instrucțiunile de operare în Manuale video pe web. Accesați următorul URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

Urmați instrucțiunile de pe ecran.

Schimbarea metodei de conectare la computer

Această secțiune explică modul de schimbare a metodei de conectare atunci când computerul și scanerul sunt conectate.

Modificarea conexiunii de rețea de la Ethernet la Wi-Fi

Schimbați conexiunea Ethernet cu conexiunea Wi-Fi din panoul de comandă al scanerului. Metoda de schimbare a conexiunii este practic aceeași ca setările de conexiune Wi-Fi.

Informații conexe

➡ „Conectarea la LAN wireless (Wi-Fi)” la pagina 20

Modificarea conexiunii de rețea de la Wi-Fi la Ethernet

Urmați pașii de mai jos pentru a trece de la conexiunea Wi-Fi la conexiunea Ethernet.

1. Selectați **Setări** de pe ecranul principal.
2. Selectați **Setări rețea** > **Configurare LAN prin fir**.
3. Urmați instrucțiunile de pe ecran.

Trecerea de la USB la conexiune de rețea

Utilizați programul de instalare și reconfigurați cu o altă metodă de conectare.

Accesați următorul site web și introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.

https://epson.sn

Selectarea opțiunii de modificare a metodelor de conectare

Urmați instrucțiunile din fiecare fereastră. Pe ecranul **Selectați opțiunea de instalare**, selectați **Configurați din nou conexiunea pentru Imprimantă (în cazul folosirii unui nou router de rețea, în cazul schimbării conexiunii de la USB la rețea etc.)**, apoi selectați **Înainte**.

Selectați conexiunea de rețea pe care doriți să o utilizați, **Conectare prin rețeaua wireless (Wi-Fi)** sau **Conectare prin LAN cu fir (Ethernet)**, apoi faceți clic pe **Înainte**.

Pentru finalizarea configurării, urmați instrucțiunile de pe ecran.

Verificarea stării conexiunii la rețea

Puteți verifica starea conexiunii la rețea în următorul mod.

Verificarea stării conexiunii la rețea din Panoul de comandă

Puteți verifica starea conexiunii la rețea folosind pictograma de rețea sau informațiile de rețea de pe panoul de comandă al scanerului.

Verificarea stării conexiunii la rețea folosind pictograma de rețea

Puteți verifica starea conexiunii la rețea și intensitatea undei radio utilizând pictograma de rețea de pe ecranul principal al scanerului.

	Afișează starea de conexiune a rețelei. Selectați pictograma pentru a verifica și modifica setările curente. Aceasta este o comandă rapidă pentru meniul următor. **Setări** > **Setări rețea** > **Configurare Wi-Fi**	
		Scanerul nu este conectat la o rețea fără fir (Wi-Fi).
		Scanerul caută SSID, adresă de IP nesetată, sau are o problemă cu o rețea fără fir (Wi-Fi).
		Scanerul este conectat la o rețea fără fir (Wi-Fi). Numărul de bare indică puterea semnalului conexiunii. Cu cât sunt afișate mai multe bare, cu atât mai puternică este conexiunea.
		Scanerul nu este conectat la o rețea fără fir (Wi-Fi) în modul Wi-Fi Direct (Simple AP).
		Scanerul este conectat la o rețea fără fir (Wi-Fi) în modul Wi-Fi Direct (Simple AP).
		Scanerul nu este conectat la o rețea prin fir (Ethernet) sau nu este setat.
		Scanerul este conectat la o rețea cu fir (Ethernet).

Afișarea informațiilor de rețea detaliate pe panoul de comandă

Când scanerul este conectat la rețea, puteți vizualiza și alte informații privind rețeaua selectând meniurile de rețea pe care doriți să le consultați.

1. Selectați **Setări** de pe ecranul principal.
2. Selectați **Setări rețea** > **Stare rețea**.
3. Pentru a verifica informațiile, selectați meniurile pe care doriți să le verificați.
   - ❏ Stare rețea cu fir LAN/Wi-Fi

     Afișează informațiile despre rețea (nume dispozitiv, conexiune, intensitate semnal și altele) pentru conexiuni Ethernet sau Wi-Fi.
   - ❏ Stare Wi-Fi Direct

     Afișează dacă Wi-Fi Direct este activat sau dezactivat, precum și SSID, parola și altele, pentru conexiuni Wi-Fi Direct.
   - ❏ Stare server e-mail

     Afișează informații despre rețea pentru serverul de e-mail.

Specificații de rețea

Specificații Wi-Fi

Consultați următorul tabel pentru specificațiile Wi-Fi.

Țări sau regiuni cu excepția celor listate mai jos	**Tabel A**
Irlanda, Regatul Unit, Austria, Germania, Liechtenstein, Elveția, Franța, Belgia, Luxemburg, Țările de Jos, Italia, Portugalia, Spania, Danemarca, Finlanda, Norvegia, Suedia, Islanda, Croația, Cipru, Grecia, Macedonia de Nord, Serbia, Slovenia, Malta, Bosnia și Herțegovina, Kosovo, Muntenegru, Albania, Bulgaria, Republica Cehă, Estonia, Ungaria, Letonia, Lituania, Polonia, România, Slovacia, Israel, Australia, Noua Zeelandă, Taiwan	**Tabel B**
Turcia	DS-900WN: Numere de serie care încep cu XDA8: **tabel A** Numere de serie care încep cu XDA7: **tabel B**
	DS-800WN: Numere de serie care încep cu XDA2: **Tabel A** Numere de serie care încep cu XD9Z: **Tabel B**

Tabel A

Standarde	IEEE 802.11b/g/n*1
Gamă de frecvențe	2400–2483,5 MHz
Putere maximă de radiofrecvență transmisă	20 dBm (EIRP)
Canale	1/2/3/4/5/6/7/8/9/10/11/12/13
Moduri de conexiune	Infrastructură, Wi-Fi Direct (Simple AP)*2*3
Protocoale de securitate*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Disponibil doar pentru HT20.

*2 Nu este acceptat pentru IEEE 802.11b.

*3 Infrastructura și modurile Wi-Fi Direct sau o conexiune Ethernet pot fi folosite simultan.

*4 Wi-Fi Direct este compatibil numai cu WPA2-PSK (AES).

*5 Compatibilitate cu standardele WPA2, acceptă WPA/WPA2 Personal.

Tabel B

Standarde	IEEE 802.11a/b/g/n*1/ac
Intervale de frecvență	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz

Canale	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)
Moduri de conexiune	Infrastructură, Wi-Fi Direct (Simple AP) *4, *5		
Protocoale de securitate*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Disponibil doar pentru HT20.

*2 Indisponibil în Taiwan.

*3 Disponibilitatea acestor canale și utilizarea produsului în mediul exterior prin intermediul acestor canale variază în funcție de locație. Pentru informații suplimentare, consultați http://support.epson.net/wifi5ghz/

*4 Nu este acceptat pentru IEEE 802.11b.

*5 Infrastructura și modurile Wi-Fi Direct sau o conexiune Ethernet pot fi folosite simultan.

*6 Wi-Fi Direct este compatibil numai cu WPA2-PSK (AES).

*7 Compatibilitate cu standardele WPA2, acceptă WPA/WPA2 Personal.

Specificații Ethernet

Standarde	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energy Efficient Ethernet)*2
Mod Comunicație	Auto, Full-duplex 10Mbps, Semi-duplex 10Mbps, Full-duplex 100Mbps, Semi-duplex 100Mbps
Conector	RJ-45

*1 Utilizați un cablu STP 5e sau superior (abreviere de la Shielded twisted pair — bifilar torsadat ecranat) pentru a preveni riscul de interferențe radio.

*2 Dispozitivul conectat trebuie să respecte standardele IEEE802.3az.

Funcții de rețea și suport IPv4/IPv6

Caracteristici	Acceptat
Epson Scan 2	IPv4, IPv6

Caracteristici	Acceptat
Document Capture Pro/Document Capture	IPv4

Protocol de securitate

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

* Trebuie să utilizați un dispozitiv de conectare compatibil cu IEEE802.1X.

Utilizarea portului pentru scaner

Scanerul utilizează portul următor. Aceste porturi trebuie să primească permisiunea de a deveni disponibile de la administratorul rețelei, după cum este cazul.

Când expeditorul (clientul) este scanerul

Utilizare	Destinație (Server)	Protocol	Număr Port
Expedierea de fișiere (Când se folosește scanarea într-un folder de rețea de la scaner)	Server FTP/FTPS	FTP/FTPS (TCP)	20
			21
	Server de fișier	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	Server WebDAV	Protocol HTTP (TCP)	80
		Protocol HTTPS (TCP)	443
Expedierea de e-mailuri (Când se folosește scanarea la e-mail de la scaner)	Server SMTP	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
Conexiune POP before SMTP (Când funcția de scanare la e-mail este utilizată de la scaner)	Server POP	POP3 (TCP)	110

Utilizare	Destinație (Server)	Protocol	Număr Port
Când se folosește Epson Connect	Server Epson Connect	HTTPS	443
		XMPP	5222
Colectarea informațiilor privind utilizatorii (Folosiți contactele de la scaner)	Server LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Autentificarea utilizatorului la colectarea informațiilor de utilizator (La folosirea contactelor de la scaner) Autentificarea utilizatorului când se folosește scanarea într-un folder de rețea (SMB) de la scaner	Server KDC	Kerberos	88
WSD de control	Computer client	WSD (TCP)	5357
Căutați computerul la scanarea push dintr-o aplicație	Computer client	Descoperire Scanare Push în rețea	2968

Când expeditorul (clientul) este computerul client

Utilizare	Destinație (Server)	Protocol	Număr Port
Descoperiți scanerul dintr-o aplicație precum EpsonNet Config și driver de scaner.	Scaner	ENPC (UDP)	3289
Colectați și configurați informațiile MIB dintr-o aplicație precum EpsonNet Config și driver de scaner.	Scaner	SNMP (UDP)	161
Căutare scaner WSD	Scaner	WS-Discovery (UDP)	3702
Redirecționarea datelor de scanare dintr-o aplicație	Scaner	Scanare în rețea (TCP)	1865
Colectarea informațiilor despre lucrare la scanarea push dintr-o aplicație	Scaner	Scanare Push în rețea	2968
Web Config	Scaner	HTTP (TCP)	80
		HTTPS (TCP)	443

Rezolvarea problemelor

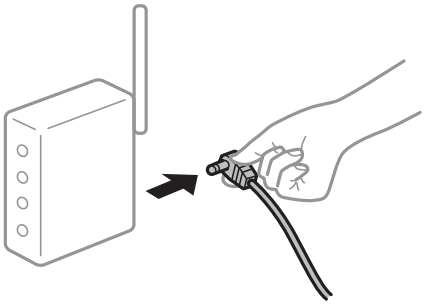
Nu se poate realiza conexiunea la rețea

Această problemă ar putea avea una dintre următoarele cauze.

Ceva este în neregulă cu dispozitivele de rețea pentru conexiunea Wi-Fi.

Soluții

Opriți dispozitivele pe care doriți să le conectați la rețea. Așteptați circa 10 secunde, apoi porniți dispozitivele în următoarea ordine: routerul wireless, computerul sau dispozitivul inteligent și scannerul. Reduceți distanța dintre scaner, computer sau dispozitivul inteligent față de routerul wireless pentru a facilita comunicațiile prin undă radio, apoi încercați să realizați din nou setările de rețea.



Dispozitivele nu pot primi semnale de la routerul wireless pentru că sunt prea departe unul de celălalt.

Soluții

După ce mutați computerul sau dispozitivul inteligent și scanerul mai aproape de routerul wireless, opriți și reporniți routerul wireless.

Atunci când schimbați routerul wireless, setările nu se potrivesc cu noul router.

Soluții

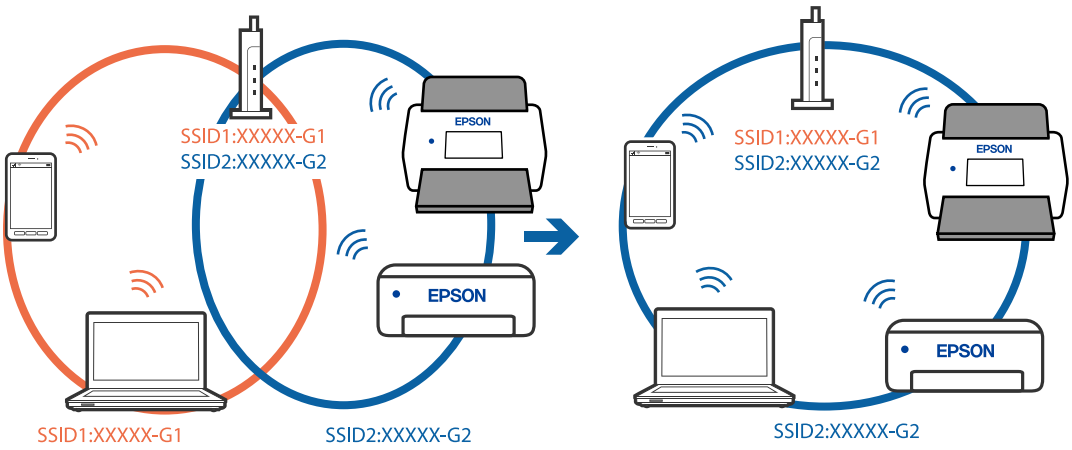
Efectuați din nou setările de conexiune pentru a se potrivi cu noul router wireless.

SSID-urile conectate de la computer sau de la dispozitivul inteligent și computer sunt diferite.

Soluții

Atunci când folosiți mai multe routere wireless în același timp sau când routerul wireless are mai multe SSID-uri, iar dispozitivele sunt conectate la SSID-uri diferite, nu puteți realiza conexiunea la routerul wireless.

Conectați computerul sau dispozitivul inteligent la același SSID ca scanerul.



Este disponibil un separator de confidențialitate pe routerul wireless.

Soluții

Majoritatea routerelor wireless au o funcție de separare de confidențialitate care blochează comunicația între dispozitivele conectate. Dacă nu puteți efectua comunicarea între scaner și computer sau dispozitivul inteligent, chiar dacă acestea sunt conectate la aceeași rețea, dezactivați separatorul de confidențialitate de la routerul wireless. Consultați manualul furnizat cu routerul wireless pentru detalii.

Adresa IP nu este atribuită corespunzător.

Soluții

Dacă adresa IP atribuită scanerului este 169.254.XXX.XXX, iar masca de subrețea este 255.255.0.0, este posibil ca adresa IP să nu fie atribuită corespunzător.

Selectați **Setări** > **Setări rețea** > **Complex** > **Configurare TCP/IP** pe panoul de comandă al scanerului și verificați adresa IP și masca de subrețea atribuite scanerului.

Reporniți routerul wireless sau resetați setările de rețea ale scanerului.

Există o problemă cu setările de rețea pe computer.

Soluții

Încercați să accesați orice site web de la computer, pentru a vă asigura că setările de rețea ale computerului sunt corecte. Dacă nu puteți accesa niciun site web, există o problemă cu computerul.

Verificați conexiunea computerului la rețea. Consultați documentația furnizată cu computerul pentru detalii.

Scanerul a fost conectat la Ethernet utilizând dispozitive care acceptă IEEE 802.3az (Ethernet eficient energetic).

Soluții

Când conectați scanerul prin Ethernet utilizând dispozitive care acceptă IEEE 802.3az (Ethernet eficient energetic), pot apărea următoarele probleme în funcție de hub-ul sau routerul utilizat.

- ❏ Conexiunea devine instabilă, scanerul se conectează și se deconectează în mod repetat.
- ❏ Conexiunea la scaner este imposibilă.
- ❏ Viteza de comunicație se reduce.

Urmați pașii de mai jos pentru a dezactiva IEEE 802.3az pentru scaner și apoi efectuați conexiunea.

1. Deconectați cablul Ethernet conectat la computer și la scaner.
2. Dacă IEEE 802.3az pentru computer este activat, dezactivați-l.

   Consultați documentația aferentă computerului pentru detalii.
3. Conectați computerul și scanerul în mod direct, utilizând un cablu Ethernet.
4. La scaner, verificați setările de rețea.

   Selectați **Setări** > **Setări rețea** > **Stare rețea** > **Stare rețea cu fir LAN/Wi-Fi**.
5. Verificați adresa IP a scanerului.

6. Pe computer, accesați Web Config.

   Lansați un browser web, apoi introduceți adresa IP a scanerului.

   „Cum să rulați Web Config într-un browser web” la pagina 38

7. Selectați fila **Rețea** > **LAN cu fir**.
8. Selectați **Dezactivat** pentru **IEEE 802.3az**.
9. Executați clic pe **Înainte**.
10. Executați clic pe **OK**.
11. Deconectați cablul Ethernet conectat la computer și la scaner.
12. Dacă ați dezactivat IEEE 802.3az pentru computer la pasul 2, activați-l.
13. Conectați cablurile Ethernet pe care le-ați deconectat în pasul 1 la computer și scaner.

Dacă problema reapare, este posibil să fie cauzată de alte dispozitive decât scanerul.

Scanerul este oprit.

Soluții

Asigurați-vă că scanerul este pornit.

De asemenea, așteptați până când indicatorul luminos de stare nu mai clipește, indicând că scanerul este pregătit să scaneze.

Software pentru configurarea scanerului

Aplicație pentru configurarea operațiilor scanerului (Web Config)

Web Config este o aplicație care rulează în browsere web, de exemplu în Microsoft Edge și Safari, pe un computer sau pe un dispozitiv inteligent. Puteți confirma starea scanerului sau puteți modifica serviciul de rețea și setările scanerului. Pentru a utiliza aplicația Web Config, conectați scanerul și computerul sau dispozitivul în aceeași rețea.

Sunt acceptate următoarele browsere. Utilizați cea mai recentă versiune.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

Notă:
Este posibil să vi se solicite să introduceți parola de administrator în timp ce utilizați acest dispozitiv. Consultați următoarele pentru detalii despre parola de administrator.

„Note despre parola de administrator" la pagina 11

Informații conexe

➡ „Imposibilitate de accesare Web Config" la pagina 65

Cum să rulați Web Config într-un browser web

Scanerul vine cu un software încorporat numit Web Config (o pagină web în care puteți efectua setări). Pentru a accesa Web Config, trebuie doar să introduceți adresa IP a unui scaner conectat la rețea în browserul dumneavoastră.

1. Verificați adresa IP a scanerului.

   Selectați **Setări** > **Setări rețea** > **Stare rețea** pe panoul de comandă al scanerului. Apoi selectați metoda de conexiune activă (**Stare rețea cu fir LAN/Wi-Fi** sau **Stare Wi-Fi Direct**) pentru a confirma adresa IP a scanerului.

   Exemplu de adresă IP: 192.168.100.201

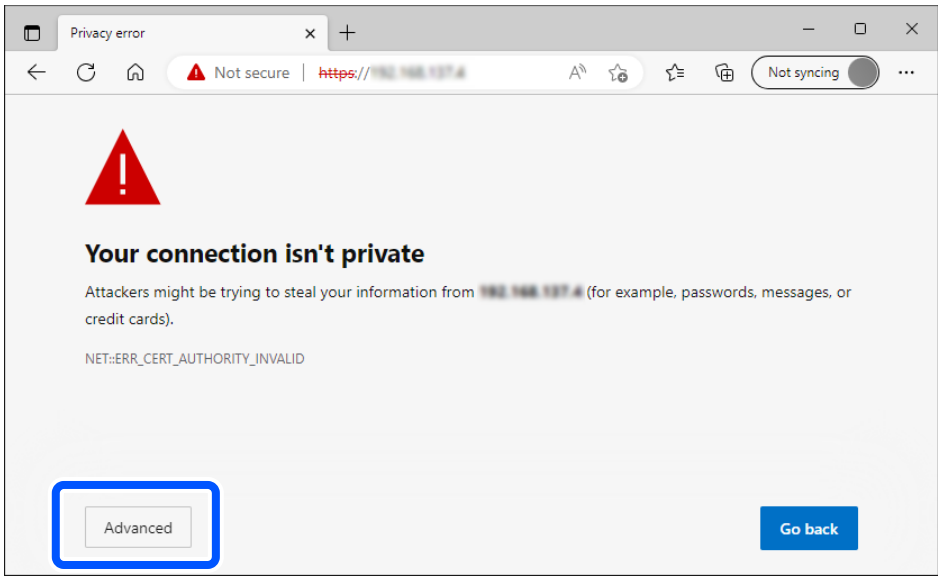
2. Lansați un browser de la un computer sau un dispozitiv inteligent, apoi introduceți adresa IP a scanerului în bara de adresă.

   Format: http://adresă IP scaner/

   Exemplu: http://192.168.100.201/

   Dacă în browser este afișat un ecran de avertizare, puteți ignora avertismentul și puteți afișa pagina web (Web Config). Întrucât scanerul folosește un certificat auto-semnat atunci când accesează HTTPS, atunci când porniți Web Config se afișează o avertizare în browser; acest lucru nu indică o problemă și poate fi ignorat. În funcție de browser, poate fi necesar să faceți clic pe **Setări avansate** pentru a vizualiza pagina web.

Exemplu: pentru Microsoft Edge



Notă:

❏ *Dacă nu este afișat un ecran de avertizare, treceți la pasul următor.*

❏ *Pentru adrese IPv6, utilizați următorul format.*

Format: http://[scanner's IP address]/

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

3. Pentru a modifica setările scanerului, trebuie să vă conectați ca administrator Web Config.

Faceți clic pe **autentificare** în partea din dreapta sus a ecranului. Introduceți **Nume utilizator** și **Parolă actuală**, apoi faceți clic pe **OK**.

În cele ce urmează, sunt furnizate valorile inițiale pentru informațiile de administrator Web Config.

·Nume utilizator: niciunul (gol)

·Parola: depinde de eticheta atașată pe produs.

Dacă există o etichetă „PASSWORD" atașată pe spate, introduceți numărul din 8 cifre afișat pe etichetă. Dacă nu este atașată nicio etichetă „PASSWORD", introduceți numărul de serie pe eticheta atașată pe spatele produsului pentru parola inițială de administrator.

Notă:

❏ *Dacă **deconectare** se afișează în partea din dreaptă sus a ecranului, înseamnă că sunteți deja conectat/ă ca administrator.*

❏ *Veți fi deconectat/ă automat după aproximativ 20 de minute de inactivitate.*

Epson Device Admin

Epson Device Admin este o aplicație multifuncțională care vă permite să gestionați dispozitivele dintr-o rețea.

Puteți utiliza șabloane de configurare pentru a aplica setări unificate la mai multe scanere dintr-o rețea, făcând-o adecvată pentru instalarea și gestionarea mai multor scanere.

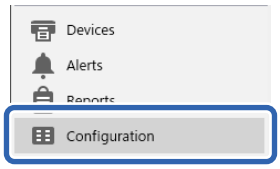
Puteți descărca Epson Device Admin de pe site-ul web de asistență Epson. Pentru detalii despre utilizarea acestei aplicații, consultați documentația sau ajutorul pentru Epson Device Admin.

Șablon de configurare

Crearea șablonului de configurare

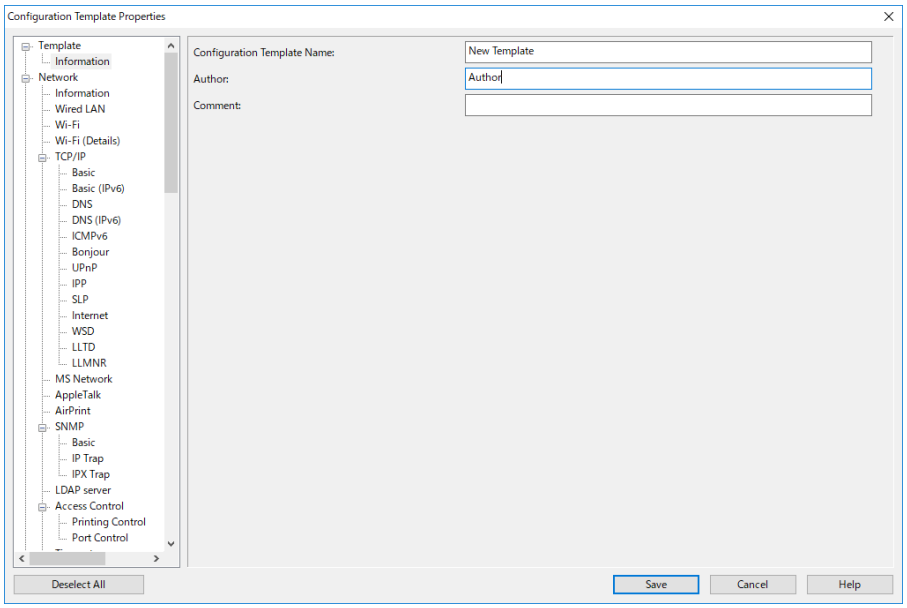
Creați un șablon de configurare de la zero.

1. Porniți Epson Device Admin.
2. Selectați **Configuration** în meniul de sarcini de pe bara laterală.



3. Selectați **New** în meniul panglică.

4. Definiți fiecare element.



Element	Explicație
Configuration Template Name	Numele șablonului de configurare. Introduceți maximum 1024 de caractere în Unicode (UTF-8).
Author	Informații privind creatorul șablonului. Introduceți maximum 1024 de caractere în Unicode (UTF-8).

Element	Explicație
Comment	Introduceți informații arbitrare. Introduceți maximum 1024 de caractere în Unicode (UTF-8).

5. Selectați elementele pe care doriți să le definiți în stânga.

   Notă:
   Faceți clic pe elementele de meniu din stânga pentru a comuta la fiecare ecran. Valoarea setată este menținută în cazul în care comutați ecranul, dar nu și dacă anulați ecranul. După ce ați finalizat toate setările, faceți clic pe ***Save****.*

Aplicarea șablonului de configurare

Aplicați scanerului șablonul de configurare salvat. Elementele selectate din șablon sunt imprimate. Dacă scanerul țintă nu dispune de o funcție adecvată, aceasta nu este aplicată.

Notă:
Când parola de administrator este setată pe scaner, configurați parola în prealabil.

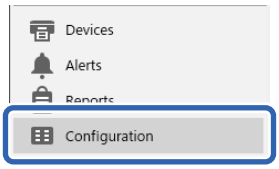
1. În meniul panglică al ecranului Listă dispozitive, selectați ***Options*** *>* ***Password manager****.*

2. Selectați ***Enable automatic password management****, apoi faceți clic pe* ***Password manager****.*

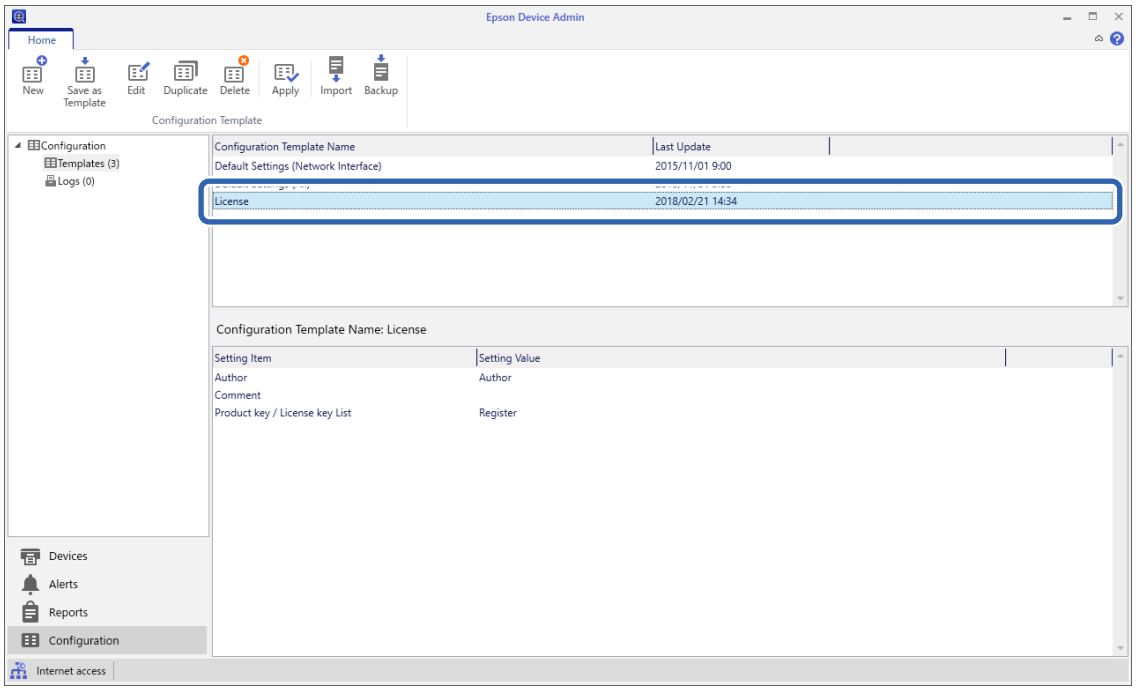
3. Selectați scanerul adecvat și apoi faceți clic pe ***Edit****.*

4. Setați parola, apoi faceți clic pe ***OK****.*

1. Selectați **Configuration** în meniul de sarcini de pe bara laterală.



2. Selectați șablonul de configurare pe care doriți să îl aplicați din **Configuration Template Name**.



3. Faceți clic pe **Apply** în meniul panglică.

   Este afișat ecranul pentru selectarea dispozitivului.

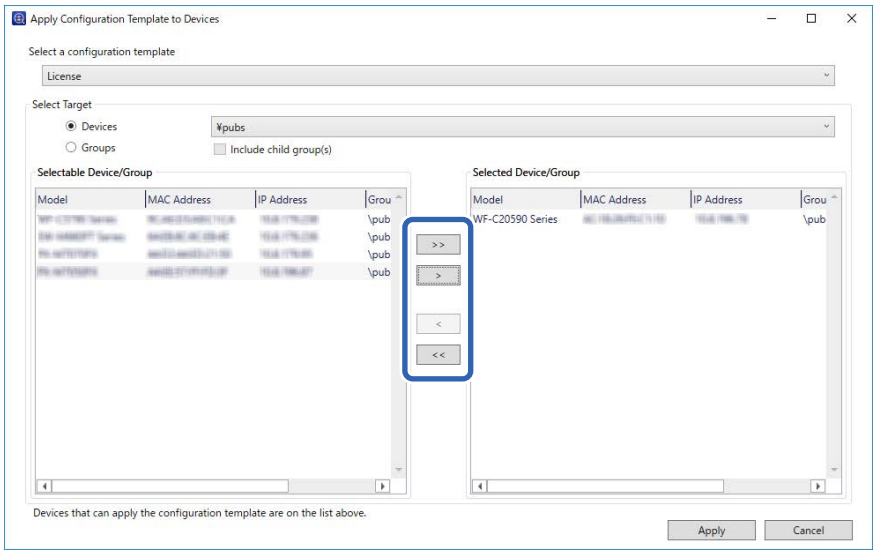
4. Selectați șablonul de configurare pe care doriți să îl aplicați.

   Notă:

   ❏ *Când selectați **Devices** și grupurile care conțin dispozitivele din meniul derulant, este afișat fiecare dispozitiv.*

   ❏ *Grupurile sunt afișate atunci când selectați **Groups**. Selectați **Include child group(s)** pentru a selecta automat grupurile copil din cadrul grupului selectat.*

5. Mutați scanerul sau grupurile cărora doriți să le aplicați șablonul la **Selected Device/Group**.



6. Executați clic pe **Apply**.

   Se afișează un ecran de confirmare pentru șablonul de configurare care urmează a fi aplicat.

7. Faceți clic pe **OK** pentru a aplica șablonul de configurare.

8. Când este afișat un mesaj care vă informează că procedura este completă, faceți clic pe **OK**.

9. Faceți clic pe **Details** și verificați informațiile.

   Afișarea simbolului la elementele aplicate indică efectuarea cu succes a aplicării.

10. Executați clic pe **Close**.

Setări necesare pentru scanare

Înregistrarea unui server de e-mail

Verificați următoarele înainte de a configura serverul de e-mail.

❏ Scanerul este conectat la rețea

❏ Informații de configurare pentru serverul de e-mail

Când utilizați un server de e-mail bazat pe Internet, verificați informațiile despre setări de la furnizor sau site-ul web.

Modul de înregistrare

Accesați Web Config, selectați fila **Rețea** > **Server e-mail** > **De bază**.

„Cum să rulați Web Config într-un browser web” la pagina 38

De asemenea, puteți efectua setări pe panoul de comandă al scanerului. Selectați **Setări** > **Setări rețea** > **Complex** > **Server e-mail** > **Setări server**.

Elemente de setare a serverului de e-mail

Element	Setări și explicație	
Metodă de autentificare	Indicați metoda de autentificare pentru ca scanerul să acceseze serverul de e-mail.	
	Oprit	Autentificarea este dezactivată la comunicarea cu un server de mail.
	ATENT. SMTP	Serverul de e-mail trebuie să accepte autentificarea SMTP.
	POP înainte de SMTP	Când selectați acest element, setați serverul POP3.
Cont autentificare	Dacă selectați **ATENT. SMTP** sau **POP înainte de SMTP** ca **Metodă de autentificare**, introduceți numele contului autentificat. Introduceți între 0 și 255 de caractere în ASCII (0x20–0x7E).	
Parolă autentificare	Dacă selectați **ATENT. SMTP** sau **POP înainte de SMTP** ca **Metodă de autentificare**, introduceți parola autentificată. Introduceți între 0 și 20 de caractere în ASCII (0x20–0x7E).	
Adresă e-mail expeditor	Setați adresa de e-mail care va fi folosită pentru a trimite e-mailuri de la scaner. Deși puteți utiliza o adresă de e-mail existentă, vă recomandăm să achiziționați și să configurați o adresă de e-mail dedicată, astfel încât să poată fi distinsă de e-mailurile trimise de la scaner. Introduceți între 0 și 255 de caractere în ASCII (0x20–0x7E), exceptând : ( ) < > [ ] ; ¥. Punctul „.” nu poate fi primul caracter.	
Adresă server SMTP	Introduceți între 0 și 255 de caractere folosind A–Z a–z 0–9 . -. Puteți folosi formatul IPv4 sau FQDN.	
Număr port server SMTP	Introduceți un număr între 1 și 65535.	
Conexiune securizată	Specificați metoda de conectare securizată pentru serverul de e-mail.	
	Fără	Dacă selectați **POP înainte de SMTP** în **Metodă de autentificare**, metoda de conectare va fi setată la **Fără**.
	SSL/TLS	Aceasta este disponibilă atunci când **Metodă de autentificare** este setată la **Oprit** sau la **ATENT. SMTP**.
	STARTTLS	Aceasta este disponibilă atunci când **Metodă de autentificare** este setată la **Oprit** sau la **ATENT. SMTP**.

Element	Setări și explicație
Validare certificat (doar Web Config)	Certificatul este validat atunci când este activată această funcție. Vă recomandăm să setați această opțiune la **Activare** când **Conexiune securizată** este setată la altceva decât **Fără**.
Adresă server POP3	Dacă selectați **POP înainte de SMTP** ca **Metodă de autentificare**, introduceți adresa serverului POP3. Puteți introduce între 0 și 255 de caractere folosind A–Z a–z 0–9 . Puteți folosi formatul IPv4 sau FQDN.
Număr port server POP3	Setați atunci când selectați **POP înainte de SMTP** în **Metodă de autentificare**. Introduceți un număr între 1 și 65535.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Verificarea conexiunii unui server de e-mail

1. Selectați meniul testului de conexiune.
   - ❏ **La configurarea din Web Config:**
     Selectați fila **Rețea** > **Server e-mail** > **Test conexiune** > **Start**.
   - ❏ **Când setați de la panoul de comandă:**
     Selectați **Setări** > **Setări rețea** >**Complex** > **Server e-mail** > **Verificare conexiune**.

   Va fi inițiată testarea conexiunii la serverul de e-mail.
2. Verificați rezultatele testului.
   - ❏ Testul are succes atunci când mesajul **Testarea conexiunii a reușit.** este afisat.
   - ❏ Dacă este afișată o eroare, urmați instrucțiunile din mesaj pentru a șterge eroarea.
     „Referințe privind testul conexiunii serverului de e-mail” la pagina 46

Referințe privind testul conexiunii serverului de e-mail

Mesaj	Cauză
Eroare de comunicare cu serverul SMTP. Verificați următoarele. - Setări rețea	Acest mesaj apare atunci când ❏ Scanerul nu este conectat la o rețea ❏ Serverul SMTP este nefuncțional ❏ Conexiunea de rețea s-a întrerupt în timpul comunicațiilor ❏ S-au primit date incomplete
Eroare de comunicare cu serverul POP3. Verificați următoarele. - Setări rețea	Acest mesaj apare atunci când ❏ Scanerul nu este conectat la o rețea ❏ Serverul POP3 este nefuncțional ❏ Conexiunea de rețea s-a întrerupt în timpul comunicațiilor ❏ S-au primit date incomplete

Mesaj	Cauză
A survenit o eroare în timpul conectării la serverul SMTP. Verificați următoarele. - Adresă server SMTP - Server DNS	Acest mesaj apare atunci când ❏ Conectarea la un server DNS nu a reușit ❏ Rezoluția de nume pentru un server SMTP nu a reușit
A survenit o eroare în timpul conectării la serverul POP3. Verificați următoarele. - Adresă server POP3 - Server DNS	Acest mesaj apare atunci când ❏ Conectarea la un server DNS nu a reușit ❏ Rezolvarea numelui pentru un server POP3 nu a reușit
Eroare de autentificare la serverul SMTP. Verificați următoarele. - Metodă de autentificare - Cont de autentificare - Parolă autentificare	Acest mesaj apare când autentificarea la serverul SMTP nu a reușit.
Eroare de autentificare la serverul POP3. Verificați următoarele. - Metodă de autentificare - Cont de autentificare - Parolă autentificare	Acest mesaj apare când autentificarea la serverul POP3 nu a reușit.
Metodă de comunicare neacceptată. Verificați următoarele. - Adresă server SMTP - Număr port server SMTP	Acest mesaj apare atunci când se încearcă efectuarea comunicării cu protocoale neacceptate.
Conectarea la serverul SMTP a eşuat. Modificaţi parametrul Conexiune securizată la Fără.	Acest mesaj apare atunci când are loc o nepotrivire SMTP între un server şi un client sau atunci când serverul nu acceptă conexiunile SMTP securizate (conexiunile SSL).
Conectarea la serverul SMTP a eşuat. Modificaţi parametrul Conexiune securizată la SSL/TLS.	Acest mesaj apare atunci când apare o neconcordanţă SMTP între un server şi un client sau atunci când serverul solicită să utilizeze o conexiune SSL/TLS pentru o conexiune securizată SMTP.
Conectarea la serverul SMTP a eşuat. Modificaţi parametrul Conexiune securizată la STARTTLS.	Acest mesaj apare atunci când apare o neconcordanţă SMTP între un server şi un client sau atunci când serverul solicită să utilizeze o conexiune STARTTLS pentru o conexiune securizată SMTP.
Conexiunea nu este de încredere. Verificați următoarele. - Data şi ora	Acest mesaj apare atunci când setarea de dată şi oră a scanerului este incorectă sau atunci când certificatul a expirat.
Conexiunea nu este de încredere. Verificați următoarele. - Certificat CA	Acest mesaj apare atunci când scanerul nu are un certificat rădăcină corespunzător serverului sau când un Certificat CA nu a fost importat.
Conexiunea nu este securizată.	Acest mesaj apare atunci când certificatul obținut este deteriorat.
Autentificarea serverului SMTP a eşuat. Modificaţi metoda de autentificare la SMTP-AUTH.	Acest mesaj apare atunci când apare o neconcordanță între server și client privind metoda de autentificare. Serverul acceptă ATENT. SMTP.
Autentificarea serverului SMTP a eşuat. Modificaţi metoda de autentificare la POP înainte de SMTP.	Acest mesaj apare atunci când apare o neconcordanță între server și client privind metoda de autentificare. Serverul nu acceptă ATENT. SMTP.
Adresa de e-mail a expeditorului este incorectă. Înlocuiți-o cu adresa de e-mail a serviciului dvs. de e-mail.	Acest mesaj apare atunci când adresa de e-mail specificată a expeditorului este eronată.
Nu se poate accesa produsul până la finalizarea procesării.	Acest mesaj apare atunci când scanerul este ocupat.

Crearea unui folder de rețea

Creați un folder de rețea pe computer. Computerul trebuie să fie conectat la aceeași rețea ca scanerul.

Metoda de setare a folderului de rețea variază în funcție de mediu. Acesta este un exemplu de creare a unui folder de rețea pe un computer desktop în următorul mediu.

❏ Sistem de operare: Windows 10

❏ Locație pentru crearea folderului partajat: Desktop

❏ Cale folder: C:\Users\xxxx\Desktop\scan_folder (creați un folder de rețea numit „scan_folder” pe desktop)

1. Conectați-vă la computerul pe care doriți să creați folderul de rețea cu un cont de utilizator care are autoritate de administrator.

   Notă:
   Dacă nu știți ce cont de utilizator are autoritate de administrator, consultați administratorul computerului.

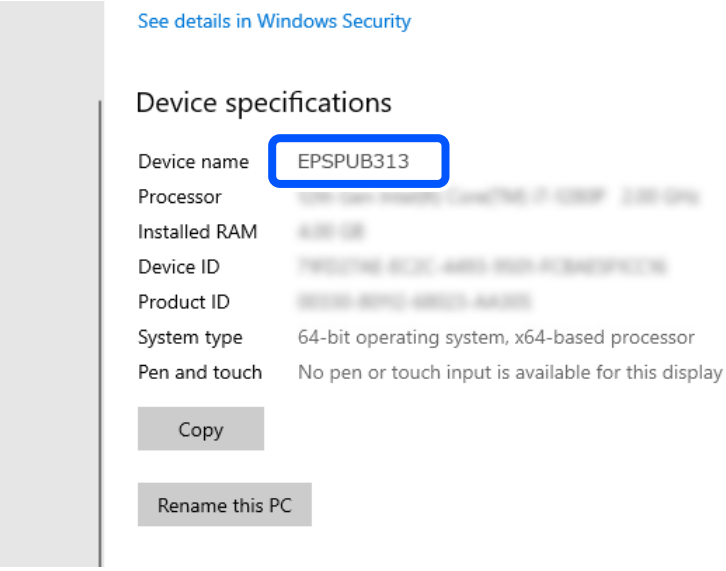
2. Asigurați-vă că numele dispozitivului (numele computerului) nu conține caractere pe doi octeți. Faceți clic pe butonul Start Windows, apoi selectați **Setări** > **Sistem** > **Despre**.

   Notă:
   Dacă există caractere pe doi octeți în numele dispozitivului, salvarea fișierului poate eșua.

3. Verificați dacă șirul afișat în **Specificații dispozitiv** > **Nume dispozitiv** nu conține caractere pe doi octeți.

   Nu ar trebui să existe probleme dacă numele dispozitivului conține doar caractere de un singur octet. Închideți ecranul.

   Exemplu: EPSPUB313



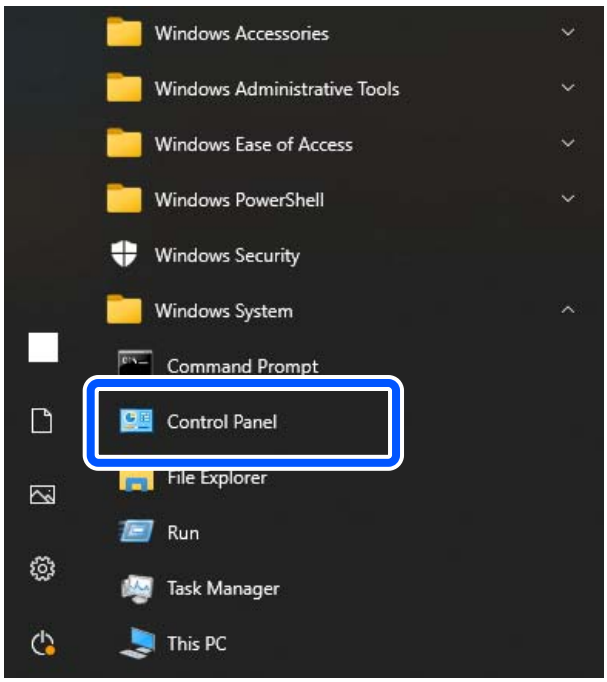
Important:

Dacă numele dispozitivului conține caractere pe doi octeți, utilizați un computer care nu utilizează caractere pe doi octeți sau redenumiți dispozitivul.

Dacă trebuie să schimbați numele dispozitivului, asigurați-vă că vă consultați în prealabil cu administratorul computerului, deoarece acest lucru poate afecta gestionarea computerului și accesul la resurse.

Apoi, verificați setările computerului.

4. Faceți clic pe butonul Windows Start și selectați **Sistem Windows** > **Panou de control**.



5. În Panoul de control, faceți clic pe **Rețea și Internet** > **Rețea și centru de partajare** > **Modificare setări avansate de partajare**.

   Se afișează profilul de rețea.

6. Asigurați-vă că ați selectat **Activare partajare fișiere și imprimantă** sub **Partajare fișiere și imprimantă** pentru profilul de rețea (profilul curent).

   Dacă este deja selectată, faceți clic pe **Anulare** și închideți fereastra.

   Când modificați setările, faceți clic pe **Salvare modificări** și închideți fereastra.

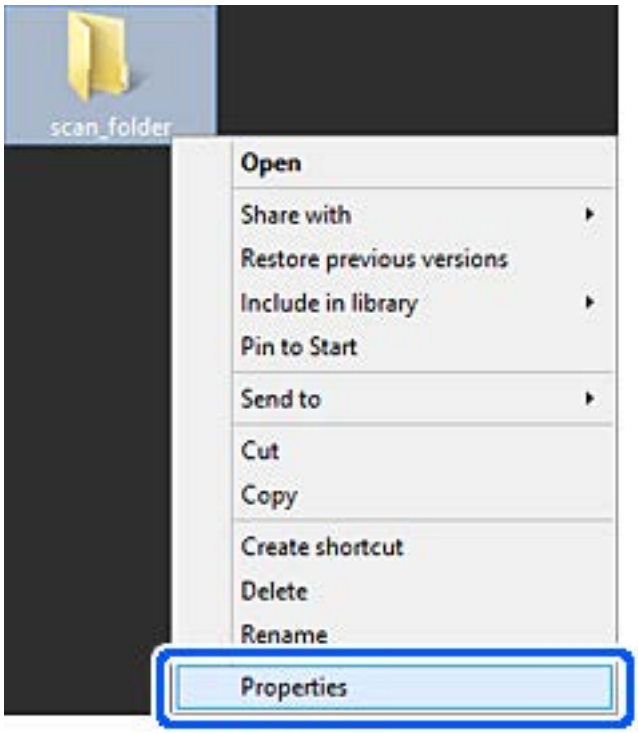
   Apoi, creați un folder de rețea.

7. Creați și denumiți un folder pe desktop.

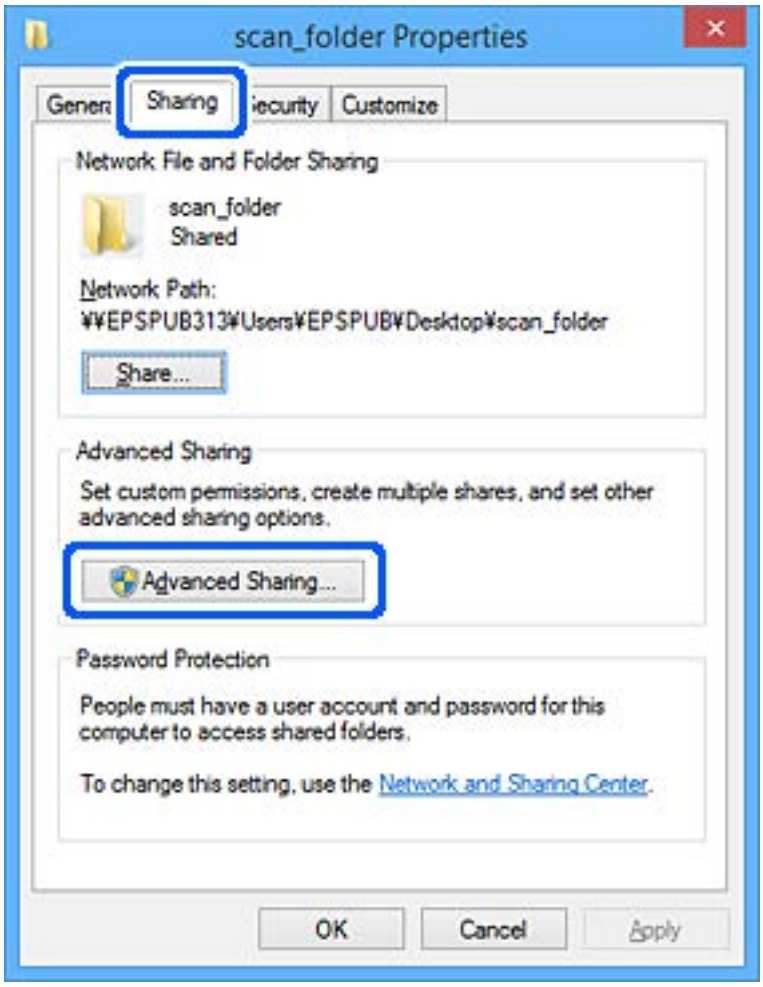
   Pentru numele folderului, introduceți între 1 și 12 caractere alfanumerice. Dacă numele depășește 12 caractere, este posibil să nu puteți accesa folderul în funcție de mediul dumneavoastră.

   Exemplu: scan_folder

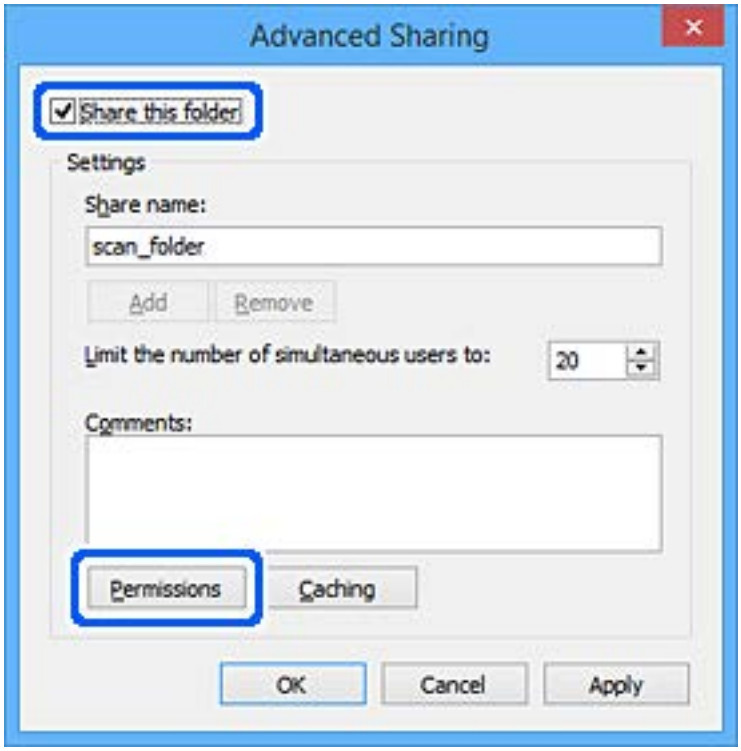
8. Faceți clic dreapta pe folder și selectați **Proprietăți**.



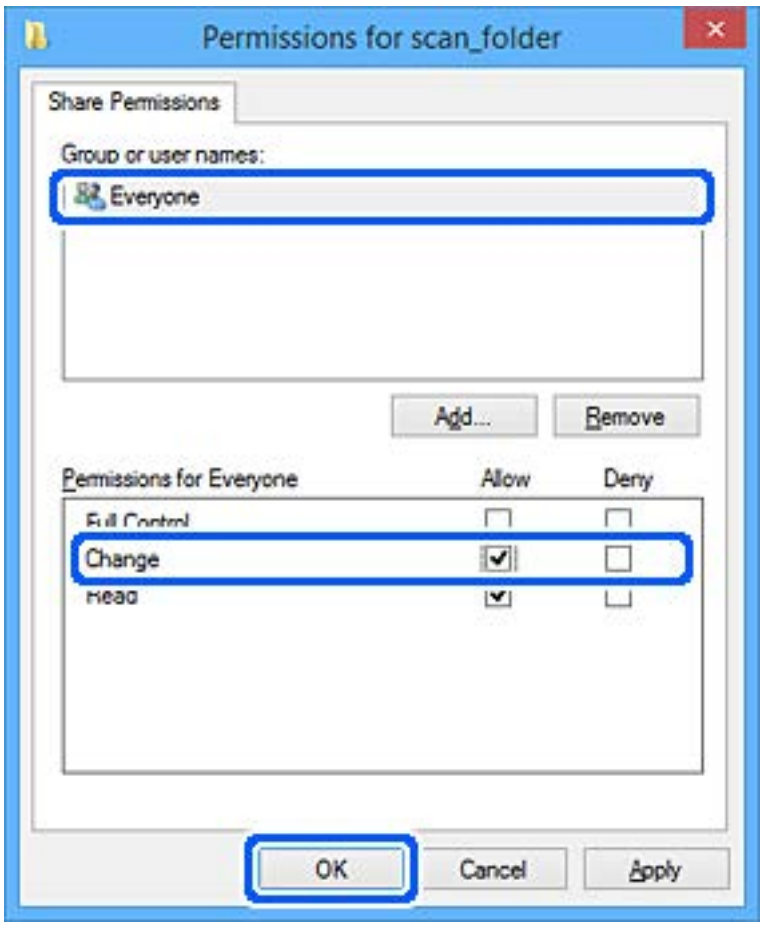
9. Faceți clic pe **Partajare complexă** în fila **Partajare**.



10. Selectați **Partajați acest folder**, apoi faceți clic pe **Permisiuni**.



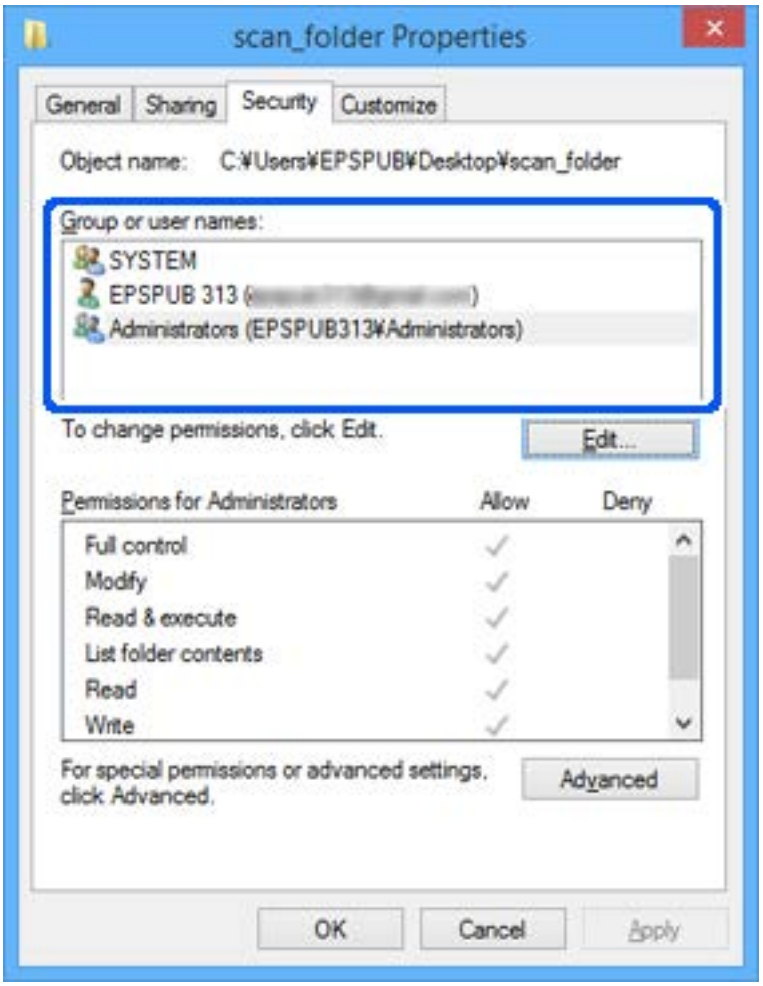
11. Selectați **Toți** din **Nume de grup sau de utilizator**, selectați **Se permite** din **Modificare** și faceți clic pe **OK**.



12. Faceți clic pe **OK** pentru a închide ecranul și a reveni la fereastra Proprietăți.

    Notă:
    Puteți verifica ce grupuri sau utilizatori au acces la folderul de rețea în fila ***Securitate*** *>* ***Nume de grup sau de utilizator****.*

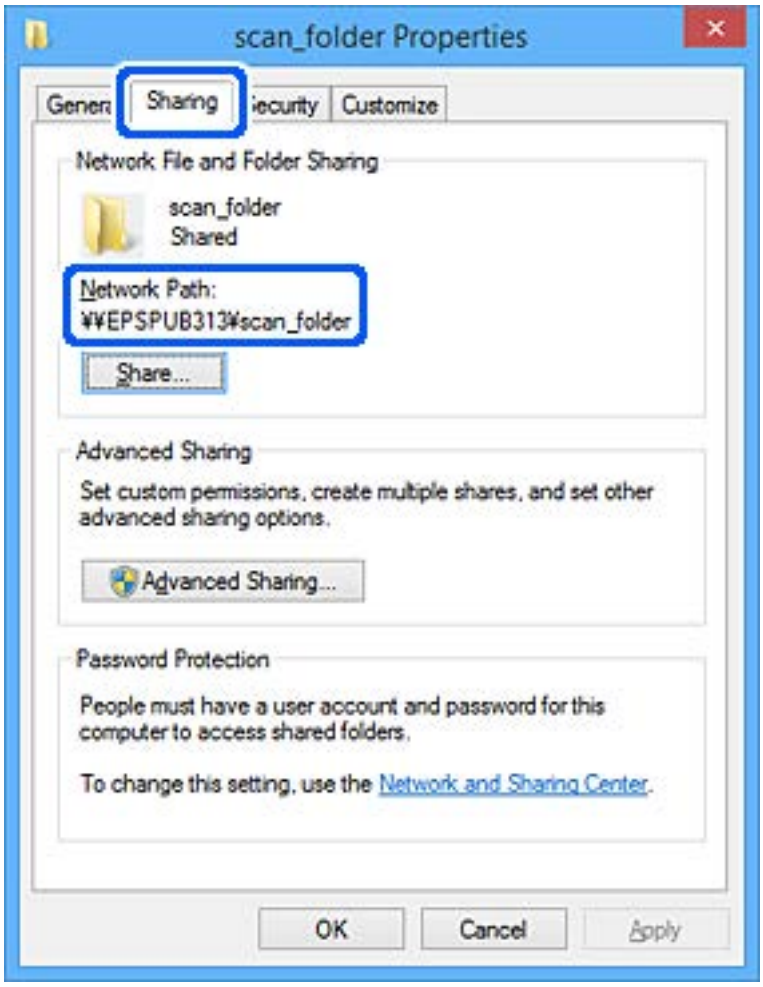
    Exemplu: Când utilizatorul conectat la computer, precum și Administratorii, pot accesa folderul de rețea



13. Selectați fila **Partajare**.

    Este afișată calea de rețea pentru folderul de rețea. Acesta este folosit când vă înregistrați la contactele dvs. pentru scaner. Vă rugăm să o notați.

Exemplu: \\EPSPUB313\scan_folder



14. Faceți clic pe **Închidere** sau pe **OK** pentru a închide fereastra.

Acest lucru finalizează crearea unui folder de rețea.

Disponibilitatea contactelor

Înregistrarea destinațiilor în lista de contacte a scanerului permite introducerea cu ușurință a destinației la scanare.

Puteți înregistra următoarele tipuri de destinații în lista de contacte. Puteți înregistra până la 300 de intrări în total.

Notă:
De asemenea, puteți utiliza serverul LDAP (căutare LDAP) pentru a introduce destinația.

E-mail	Destinație pentru e-mail. Trebuie să configurați setările serverului de e-mail în prealabil.
Folder de rețea	Destinație pentru date de scanare. Este necesar să pregătiți folderul de rețea în prealabil.

Informații conexe

➡ „Cooperarea între serverul LDAP și utilizatori” la pagina 61

Comparare configurare contacte

Există trei instrumente pentru configurarea contactelor scanerului: Web Config, Epson Device Admin și panoul de comandă al scanerului. Diferențele dintre aceste trei instrumente sunt enumerate în tabelul de mai jos.

Caracteristici	Web Config*	Epson Device Admin	Panoul de comandă al scanerului
Înregistrarea unei destinații	✓	✓	✓
Editarea unei destinații	✓	✓	✓
Adăugarea unui grup	✓	✓	✓
Editarea unui grup	✓	✓	✓
Ștergerea unei destinații sau a unor grupuri	✓	✓	✓
Ștergerea tuturor destinațiilor	✓	✓	–
Importul unui fișier	✓	✓	–
Exportarea într-un fișier	✓	✓	–

* Conectați-vă ca administrator pentru a efectua setări.

Înregistrarea unei destinații în Contacte utilizând Web Config

Notă:
Puteți înregistra, de asemenea, contactele la panoul de comandă al scanerului.

1. Accesați Web Config și selectați fila **Scanare** > **Persoane de contact**.
2. Selectați numărul pe care doriți să-l înregistrați, apoi faceți clic pe **Editare**.
3. Introduceți **Nume** și **Termen index**.
4. Selectați tipul de destinație ca opțiune **Tip**.

   Notă:
   *Nu puteți modifica opțiunea **Tip** după finalizarea înregistrării. Dacă doriți să modificați tipul, ștergeți destinația și apoi înregistrați-vă din nou.*
5. Introduceți o valoare pentru fiecare element, apoi faceți clic pe **Aplicare**.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Setarea elementelor destinației

Elemente	Setări și explicație
Setări comune	
Nume	Introduceți un nume afișat în contacte cu 30 de caractere sau mai puține în format Unicode (UTF-16). Dacă nu specificați acest element, lăsați-l necompletat.
Termen index	Introduceți un nume folosind 30 de caractere sau mai puține în Unicode (UTF-16) pentru a căuta în contactele de pe panoul de comandă al scanerului. Dacă nu specificați acest element, lăsați-l necompletat.
Tip	Selectați tipul de adresă pe care doriți să o înregistrați.
Atribuire la Utilizare frecventă	Selectați setarea adresei înregistrate ca adresă utilizată frecvent. Când setați ca adresă frecvent utilizată, aceasta este afișată în ecranul superior al caracteristicii de scanare și puteți specifica destinația fără a afișa contactele.
E-mail	
Adresă de e-mail	Introduceți între 1 și 255 de caractere folosind A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Folder rețea (SMB)	
Salvare în	\\„Cale folder” Introduceți o locație unde este localizat folderul țintă, alcătuită din 1 și 253 de caractere în format Unicode (UTF-16), omițând „\\”. Introduceți calea de rețea afișată pe ecranul de proprietăți al folderului. Consultați următoarele pentru detalii despre setarea căii de rețea. „Crearea unui folder de rețea” la pagina 48
Nume utilizator	Introduceți un nume de utilizator pentru accesarea folderului din rețea cu 30 de caractere sau mai puține în format Unicode (UTF-16). Totuși, evitați să folosiți caractere de control (de la 0x00 la 0x1f, 0x7F).
Parolă	Introduceți o parolă pentru accesarea unui folder de rețea, folosind între 0 și 20 de caractere în format Unicode (UTF-16). Totuși, evitați să folosiți caractere de control (de la 0x00 la 0x1f, 0x7F).
FTP	
Conexiune securizată	Selectați FTP sau FTPS în funcție de protocolul de transfer fișiere acceptat de serverul FTP. Selectați **FTPS** pentru a permite scanerului să comunice cu măsuri de securitate.
Salvare în	Introduceți numele serverului între 1 și 253 de caractere în format Unicode (UTF-16), omițând „ftp://” sau „ftps://”.
Nume utilizator	Introduceți un nume de utilizator pentru accesarea serverului FTP, din 30 de caractere sau mai puțin, în format Unicode (UTF-16). Totuși, evitați să folosiți caractere de control (de la 0x00 la 0x1f, 0x7F). Dacă serverul permite conexiunile anonime, introduceți un nume de utilizator precum Anonymous sau FTP. Dacă nu specificați acest element, lăsați-l necompletat.
Parolă	Introduceți o parolă pentru accesarea serverului FTP. Parola trebuie să includă între 0 și 20 de caractere în format Unicode (UTF-16). Totuși, evitați să folosiți caractere de control (de la 0x00 la 0x1f, 0x7F). Dacă nu specificați acest element, lăsați-l necompletat.

Elemente	Setări și explicație
Mod conectare	Selectați modul de conexiune din meniu. Dacă un firewall este setat între scaner și serverul FTP, selectați **Mod pasiv**.
Număr port	Introduceți numărul de port de server FTP între 1 și 65535.
Validare certificat	Certificatul serverului FTP este validat când acest element este activat. Aceasta este disponibilă atunci când **FTPS** este selectat pentru **Conexiune securizată**. Pentru a configura, trebuie să importați Certificat CA la scaner.
SharePoint(WebDAV)*	
Conexiune securizată	Selectați HTTP sau HTTPS în funcție de protocolul de transfer de fișiere acceptat de server. Selectați **HTTPS** pentru a permite scanerului să comunice cu măsuri de securitate.
Salvare în	Introduceți numele serverului folosind între 1 și 253 de caractere în format Unicode (UTF -16), omițând „http://" sau „https://".
Nume utilizator	Introduceți un nume de utilizator pentru accesarea serverului, din 30 de caractere sau mai puțin, în format Unicode (UTF-16). Totuși, evitați să folosiți caractere de control (de la 0x00 la 0x1f, 0x7F). Dacă nu specificați acest element, lăsați-l necompletat.
Parolă	Introduceți o parolă pentru accesarea serverului folosind între 0 și 20 de caractere în format Unicode (UTF-16). Totuși, evitați să folosiți caractere de control (de la 0x00 la 0x1f, 0x7F). Dacă nu specificați acest element, lăsați-l necompletat.
Validare certificat	Certificatul serverului este validat când acest element este activat. Aceasta este disponibilă atunci când **HTTPS** este selectat pentru **Conexiune securizată**. Pentru a configura, trebuie să importați Certificat CA la scaner.
Server proxy	Selectați dacă veți utiliza sau nu un server proxy.

* SharePoint Online nu este acceptat atunci când scanați în folderul de rețea de la panoul de comandă al scanerului.

Dacă doriți să salvați imaginea scanată în SharePoint Online, utilizați Document Capture Pro după instalarea SharePoint Online Connector. Consultați manualul Document Capture Pro pentru detalii.

https://support.epson.net/dcp/

Înregistrarea destinațiilor ca grup folosind Web Config

Dacă tipul de destinație este setat la **E-mail**, puteți înregistra destinațiile ca grup.

1. Accesați Web Config și selectați fila **Scanare** > **Persoane de contact**.
2. Selectați numărul pe care doriți să-l înregistrați, apoi faceți clic pe **Editare**.
3. Selectați un grup din **Tip**.
4. Faceți clic pe **Selectare** pentru **Contact(e) pt Grup**.
   Sunt afișate destinațiile disponibile.
5. Selectați destinația pe care doriți să o înregistrați în grup și apoi faceți clic pe **Selectare**.

6. Introduceți un **Nume** şi **Termen index**.
7. Selectați dacă atribuiți sau nu grupul înregistrat la grupul frecvent utilizat.

   Notă:
   Destinațiile pot fi înregistrate pe mai multe grupuri.
8. Faceți clic pe **Aplicare**.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Copierea de rezervă şi importul contactelor

Utilizând Web Config sau alte instrumente, puteți efectua copierea de rezervă şi importul contactelor.

Pentru Web Config, puteți efectua copierea de rezervă a contactelor prin exportarea setărilor de scaner care includ contacte. Fişierul exportat nu poate fi editat, deoarece este exportat ca fişier binar.

Când importați setările scanerului la scaner, contactele sunt suprascrise.

Pentru Epson Device Admin, numai contactele pot fi exportate din ecranul de proprietăți al dispozitivului. De asemenea, dacă nu exportați elementele de securitate, puteți edita contactele exportate şi le puteți importa, deoarece acestea pot fi salvate ca fişier SYLK sau CSV.

Importarea contactelor cu Web Config

Dacă aveți un scaner care vă permite să realizați o copie de rezervă a contactelor şi este compatibil cu acest scaner, puteți înregistra cu uşurință contactele prin importarea fişierului de rezervă.

Notă:
Pentru instrucțiuni privind modul de realizare a copiilor de rezervă pentru contactele scanerului, consultați manualul furnizat cu scanerul.

Urmați paşii de mai jos pentru a importa contactele în acest scaner.

1. Accesați Web Config, selectați fila **Gestionare dispozitiv** > **Valoare de setare export şi import** > **Import**.
2. Selectați fişierul de rezervă pe care l-ați creat în **Fişier**, introduceți parola şi faceți clic pe **Înainte**.
3. Selectați caseta de validare **Persoane de contact** şi apoi faceți clic pe **Înainte**.

Copierea de rezervă a listei de contacte utilizând Web Config

Există riscul de a pierde datele de contact în cazul defectării scanerului. Vă recomandăm să realizați copii de siguranță ale datelor după fiecare actualizare a acestora. Epson nu îşi asumă responsabilitatea pentru pierderea datelor, pentru copierea de rezervă sau recuperarea datelor şi/sau a setărilor, nici chiar în perioada de garanție.

Folosind Web Config, puteți realiza o copie de rezervă a datelor despre contacte memorate în scaner şi puteți salva aceste date în computer.

1. Accesați Web Config şi apoi selectați fila **Gestionare dispozitiv** > **Valoare de setare export şi import** > **Export**.

2. Selectați caseta de validare **Persoane de contact** din categoria **Scanare**.
3. Introduceți o parolă pentru a cripta fișierul exportat.

   Aveți nevoie de parolă pentru a importa fișierul. Lăsați acest câmp necompletat dacă nu doriți să criptați fișierul.
4. Faceți clic pe **Export**.

Exportul şi înregistrarea în masă a contactelor cu ajutorul unui instrument

Dacă utilizați Epson Device Admin, puteți realiza o copie de rezervă a contactelor şi edita fișierele exportate, apoi le puteți înregistra pe toate odată.

Opțiunea este utilă dacă doriți să copiați de rezervă numai contactele sau când înlocuiți scanerul şi doriți să transferați contactele de la produsul vechi la cel nou.

Exportul contactelor

Salvați informațiile contactelor în fişier.

Puteți edita fișierele salvate în format SYLK sau format csv utilizând o aplicație de tip foaie de calcul tabelar sau un editor de texte. Le puteți înregistra pe toate simultan după ştergerea sau adăugarea informațiilor.

Informații care includ elemente de securitate, precum parola şi informațiile personale, pot fi salvate în format binar cu o parolă. Nu puteți edita fișierul. Acesta poate fi utilizat ca fişier copie de rezervă pentru informații, inclusiv elementele de securitate.

1. Porniți Epson Device Admin.
2. Selectați **Devices** în meniul de sarcini de pe bara laterală.
3. Selectați dispozitivul pe care doriți să îl configurați, din lista de dispozitive.
4. Faceți clic pe **Device Configuration** din fila **Home** de pe meniul panglică.

   Atunci când a fost setată parola administratorului, introduceți parola şi faceți clic pe **OK**.
5. Faceți clic pe **Common** > **Contacts**.
6. Selectați formatul de export din **Export** > **Export items**.
   - ❏ All Items

     Exportați fişierul binar criptat. Selectați când doriți să includeți elemente de securitate precum parola şi informațiile personale. Nu puteți edita fișierul. Dacă îl selectați, trebuie să setați parola. Faceți clic pe **Configuration** şi setați o parolă ASCII între 8 şi 63 de caractere lungime. Această parolă este necesară la importul fişierului binar.
   - ❏ Items except Security Information

     Exportați fişierele în format SYLK sau csv. Selectați atunci când doriți să editați informațiile fişierului exportat.
7. Faceți clic pe **Export**.

8. Specificați locația de salvare a fișierului, selectați tipul de fișier și faceți clic pe **Save**.

   Se afișează mesajul de finalizare.

9. Faceți clic pe **OK**.

   Verificați dacă fișierul este salvat în locația specificată.

Importul contactelor

Importați informațiile contactelor din fișier.

Puteți importa fișiere salvate în format SYLK sau în format csv, respectiv fișierul binar copiat de rezervă care include elementele de securitate.

1. Porniți Epson Device Admin.
2. Selectați **Devices** în meniul de sarcini de pe bara laterală.
3. Selectați dispozitivul pe care doriți să îl configurați, din lista de dispozitive.
4. Faceți clic pe **Device Configuration** din fila **Home** de pe meniul panglică.

   Atunci când a fost setată parola administratorului, introduceți parola și faceți clic pe **OK**.
5. Faceți clic pe **Common** > **Contacts**.
6. Faceți clic pe **Browse** la **Import**.
7. Selectați fișierul pe care doriți să îl importați și faceți clic pe **Open**.

   Când selectați fișierul binar, în **Password** introduceți parola setată la exportul fișierului.
8. Faceți clic pe **Import**.

   Se afișează ecranul de confirmare.
9. Faceți clic pe **OK**.

   Se afișează rezultatul validării.

   ❏ Edit the information read

   Faceți clic când doriți să editați informațiile individual.

   ❏ Read more file

   Faceți clic când doriți să importați mai multe fișiere.
10. Faceți clic pe **Import**, apoi pe **OK** în ecranul de finalizare a importului.

    Reveniți la ecranul de proprietăți al dispozitivului.
11. Faceți clic pe **Transmit**.
12. Faceți clic pe **OK** în mesajul de confirmare.

    Setările sunt trimise la scaner.
13. În ecranul de finalizare a trimiterii, faceți clic pe **OK**.

    Informațiile scanerului sunt actualizate.

Deschideți contactele din Web Config sau de la panoul de comandă al scanerului și verificați dacă este actualizat contactul.

Cooperarea între serverul LDAP și utilizatori

Când cooperați cu serverul LDAP, puteți utiliza informațiile de adresă înregistrate la serverul LDAP ca destinație a unui e-mail.

Configurarea serverului LDAP

Pentru a utiliza informațiile serverului LDAP, înregistrați-l la scaner.

1. Accesați Web Config și selectați fila **Rețea** > **Server LDAP** > **De bază**.
2. Introduceți o valoare pentru fiecare element.
3. Selectați **OK**.

   Sunt afișate setările pe care le-ați selectat.

Elemente de setare server LDAP

Elemente	Setări și explicație
Utilizare server LDAP	Selectați **Utilizare** sau **A nu se folosi**.
Adresă server LDAP	Introduceți adresa serverului LDAP. Introduceți între 1 și 255 de caractere în format IPv4, IPv6 sau FQDN. Pentru formatul FQDN, puteți folosi caractere alfanumerice în ASCII (0x20 – 0x7E) și „-”, exceptând începutul și sfârșitul adresei.
Număr port server LDAP	Introduceți numărul de port de server LDAP între 1 și 65535.
Conexiune securizată	Specificați metoda de autentificare atunci când scanerul accesează serverul LDAP.
Validare certificat	Când aceasta este activată, certificatul serverului LDAP este validat. Recomandăm setarea acestei funcții la **Activare**. Pentru a configura, **Certificat CA** trebuie importat la scaner.
Expirare căutare (sec.)	Setați intervalul de timp de căutare înainte de apariția expirării între 5 și 300.
Metodă de autentificare	Selectați una dintre metode. Dacă selectați **Autentificare Kerberos**, selectați **Setări Kerberos** pentru a face setări pentru Kerberos. Pentru a efectua Autentificare Kerberos, următorul mediu este obligatoriu. ❏ Scanerul și serverul DNS pot comunica. ❏ Ora scanerului, a serverului KDC și a serverului necesar pentru autentificare (server LDAP, server SMTP, server de fișiere) sunt sincronizate. ❏ Când serverului de serviciu i se atribuie o adresă IP, numele FQDN al serverului de serviciu este înregistrat în zona de căutare inversă a serverului DNS.
Domeniu Kerberos de utilizat	Dacă selectați **Autentificare Kerberos** pentru **Metodă de autentificare**, selectați domeniul Kerberos pe care doriți să îl utilizați.

Elemente	Setări și explicație
DN administrator / Nume utilizator	Introduceți, în Unicode (UTF-8), numele de utilizator pentru serverul LDAP, cu 128 de caractere sau mai puțin. Nu puteți utiliza caractere de control, precum 0x00 – 0x1F și 0x7F. Această setare nu este utilizată când opțiunea **Autentificare anonimă** este selectată ca **Metodă de autentificare**. Dacă nu specificați acest element, lăsați-l necompletat.
Parolă	Introduceți, în Unicode (UTF-8), parola pentru serverul LDAP, cu 128 de caractere sau mai puțin. Nu puteți utiliza caractere de control, precum 0x00 – 0x1F și 0X7F. Această setare nu este utilizată când opțiunea **Autentificare anonimă** este selectată ca **Metodă de autentificare**. Dacă nu specificați acest element, lăsați-l necompletat.

Setări Kerberos

Dacă selectați **Autentificare Kerberos** pentru **Metodă de autentificare** a **Server LDAP** > **De bază**, efectuați următoarele setări Kerberos din fila **Rețea** > **Setări Kerberos**. Puteți înregistra până la 10 setări pentru parametrii Kerberos.

Elemente	Setări și explicație
Domeniu	Introduceți domeniul autentificării Kerberos, cu 255 de caractere sau mai puține în sistem ASCII (0x20 – 0x7E). Dacă nu înregistrați acest element, lăsați-l necompletat.
Adresă KDC	Introduceți adresa serverului de autentificare Kerberos. Introduceți maximum 255 de caractere în format IPv4, IPv6 sau FQDN. Dacă nu înregistrați acest element, lăsați-l necompletat.
Număr port (Kerberos)	Introduceți numărul portului serverului Kerberos, între 1 și 65535.

Configurarea setărilor de căutare server LDAP

La definirea setărilor de căutare, puteți utiliza adresa de e-mail înregistrată la serverul LDAP.

1. Accesați Web Config și selectați fila **Rețea** > **Server LDAP** > **Setări căutare**.
2. Introduceți o valoare pentru fiecare element.
3. Faceți clic pe **OK** pentru a afișa rezultatul setării.

   Sunt afișate setările pe care le-ați selectat.

Elemente de setare căutare server LDAP

Elemente	Setări și explicație
Bază de căutare (Nume distinct)	Dacă doriți să căutați un domeniu arbitrar, indicați numele domeniului serverului LDAP. Introduceți între 0 și 128 de caractere în Unicode (UTF-8). Dacă nu căutați un atribut arbitrar, lăsați acest câmp necompletat. Exemplu pentru directorul serverului local: dc=server,dc=local

Elemente	Setări și explicație
Număr de intrări la căutare	Specificați numărul de intrări de căutare între 5 și 500. Numărul specificat de intrări de căutare este salvat și afișat temporar. Chiar dacă numărul de intrări depășește valoarea specificată și apare un mesaj de eroare, căutarea poate fi efectuată.
Atribut nume de utilizator	Specificați numele de atribut care se va afișa la căutarea numelor de utilizator. Introduceți între 1 și 255 de caractere în Unicode (UTF-8). Primul caracter trebuie să fie a – z sau A – Z. Exemplu: cn, uid
Atribut de afișare nume de utilizator	Specificați numele de atribut care se va afișa ca nume de utilizator. Introduceți între 0 și 255 de caractere în Unicode (UTF-8). Primul caracter trebuie să fie a – z sau A – Z. Exemplu: cn, sn
Atribut adresă de e-mail	Specificați numele de atribut care se va afișa la căutarea adreselor de e-mail. Introduceți o combinație cuprinsă între 1 și 255 de caractere, folosind A – Z, a – z, 0 – 9 și -. Primul caracter trebuie să fie a – z sau A – Z. Exemplu: mail
Atribut arbitrar 1 - Atribut arbitrar 4	Puteți specifica și alte atribute arbitrare de căutat. Introduceți între 0 și 255 de caractere în Unicode (UTF-8). Primul caracter ar trebui să fie a – z sau A – Z. Dacă nu doriți să căutați atribute arbitrare, lăsați acest câmp necompletat. Exemplu: o, ou

Verificarea conexiunii serverului LDAP

Efectuați testul de conexiune la serverul LDAP utilizând setul de parametri de la **Server LDAP** > **Setări căutare**.

1. Accesați Web Config și selectați fila **Rețea** > **Server LDAP** > **Test conexiune**.
2. Selectați **Start**.

   Testul de conexiune începe. După test, se afișează raportul de verificare.

Referințe privind testul conexiunii serverului LDAP

Mesaje	Explicație
Testarea conexiunii a reușit.	Acest mesaj apare când conexiunea cu serverul a reușit.
Testarea conexiunii a eșuat. Verificați setările.	Acest mesaj apare din următoarele motive: ❏ Adresa serverului LDAP este incorectă sau numărul de port este incorect. ❏ Un interval de timp a expirat. ❏ Opțiunea **A nu se folosi** este selectată ca **Utilizare server LDAP**. ❏ Dacă **Autentificare Kerberos** este selectată ca **Metodă de autentificare**, setări precum **Domeniu**, **Adresă KDC** și **Număr port (Kerberos)** sunt incorecte.

Mesaje	Explicație
Testarea conexiunii a eşuat. Verificați data şi ora pe produsul dvs. sau pe server.	Acest mesaj apare când conexiunea eşuează deoarece setările de oră pentru scaner şi pentru serverul LDAP nu corespund.
Autentificarea a eşuat. Verificați setările.	Acest mesaj apare din următoarele motive: ❏ **Nume utilizator** şi/sau **Parolă** sunt incorecte. ❏ Dacă **Autentificare Kerberos** este selectat ca **Metodă de autentificare**, este posibil ca data/ora să nu fie configurate.
Nu se poate accesa produsul până la finalizarea procesării.	Acest mesaj apare atunci când scanerul este ocupat.

Configurarea caracteristicii AirPrint

Accesați Web Config, selectați fila **Rețea**, apoi selectați **Configurare AirPrint**.

Elemente	Explicație
Nume serviciu Bonjour	Introduceți un nume de serviciu Bonjour, folosind text ASCII (0x20–0x7E) şi până la 41 de caractere.
Locație Bonjour	Introduceți o descriere a locației scanerului, folosind text Unicode (UTF-8) şi până la 127 de octeți.
Wide-Area Bonjour	Setați dacă se foloseşte sau nu Wide-Area Bonjour. Dacă se utilizează, scanerul trebuie să fie înregistrat pe serverul DNS pentru a căuta scanerul în segment.
Activare AirPrint	Permite Bonjour şi AirPrint (serviciu de scanare). Acest buton este disponibil numai când AirPrint este dezactivat. ***Notă:*** *Dacă AirPrint este dezactivat, scanarea Mopria de pe Chromebook, Windows şi aplicația Mopria Scan sunt, de asemenea, dezactivate.*

Probleme la pregătirea scanării în rețea

Sugestii pentru remedierea problemelor

❏ Verificarea mesajului de eroare

Dacă apar probleme, verificați mai întâi dacă există mesaje pe panoul de comandă al scanerului sau pe ecranul driverului. Dacă mesajul e-mail de notificare este setat la apariția evenimentelor, puteți afla imediat care este situația.

❏ Verificarea stării comunicațiilor

Verificați starea comunicării computerului server sau a computerului client utilizând comenzi precum ping şi ipconfig.

❏ Test de conexiune

Pentru verificarea conexiunii dintre scaner şi serverul de e-mail, efectuaţi testul de conexiune de la scaner. De asemenea, verificaţi conexiunea de la computerul client la server, pentru a stabili starea comunicaţiilor.

❏ Iniţializarea setărilor

Dacă setările şi starea comunicaţiei nu prezintă probleme, problemele pot fi remediate prin dezactivarea sau iniţializarea setărilor de reţea ale scanerului, urmate de reconfigurare.

Imposibilitate de accesare Web Config

Adresa IP nu este alocată scanerului.

Soluţii

O adresă IP validă nu poate fi alocată scanerului. Configuraţi adresa IP folosind panoul de comandă al scanerului. Puteţi confirma informaţiile privind setarea actuală din panoul de comandă al scanerului.

Browser-ul web nu acceptă nivelul de criptare pentru SSL/TLS.

Soluţii

SSL/TLS are Forţă criptare. Puteţi deschide Web Config utilizând un browser web care acceptă criptări în masă, în modul indicat mai jos. Verificaţi dacă utilizaţi un browser web acceptat.

❏ 80 bit: AES256/AES128/3DES

❏ 112 bit: AES256/AES128/3DES

❏ 128 bit: AES256/AES128

❏ 192 bit: AES256

❏ 256 bit: AES256

Certificat semnat de CA este expirat.

Soluţii

Dacă există o problemă cu data de expirare a certificatului, mesajul „Certificatul a expirat” este afişat la conectarea la Web Config cu comunicare SSL/TLS (https). Dacă mesajul apare înainte de data de expirare a acestuia, asiguraţi-vă că data scanerului este configurată corect.

Numele comun al certificatului şi al scanerului nu concordă.

Soluţii

Dacă numele comun al certificatului şi al scanerului nu concordă, se afişează mesajul „Numele certificatului de securitate nu se potriveşte···” la accesarea Web Config utilizând comunicaţia SSL/TLS (https). Aceasta se întâmplă deoarece următoarele adrese IP nu corespund.

❏ Adresa IP a scanerului adăugată la numele comun pentru crearea unui Certificat auto-semnat sau CSR

❏ Adresa IP introdusă în browserul web când se rulează Web Config

Pentru Certificat auto-semnat, actualizaţi certificatul.

Pentru Certificat semnat de CA, obţineţi din nou certificatul pentru scaner.

Setarea adresei locale pentru server proxy nu este setată pe browser-ul web.

Soluții

Când scanerul este setat să utilizeze un server proxy, configurați browser-ul web să nu se conecteze la adresa locală prin intermediul serverului proxy.

❏ Windows:

Selectați **Panou de control** > **Rețea și Internet** > **Opțiuni Internet** > **Conexiuni** > **Setări LAN** > **Server proxy**, iar apoi configurați pentru a nu folosi serverul proxy pentru LAN (adresele locale).

❏ Mac OS:

Selectați **Preferințe sistem** (sau **Setări sistem**) > **Rețea** > **Avansat** > **Proxy-uri**, iar apoi înregistrați adresa locală pentru **Se omit setările proxy pentru aceste gazde și domenii**.

Exemplu:

192.168.1.*: Adresă locală 192.168.1.XXX, mască subrețea 255.255.255.0

192.168.*.*: Adresă locală 192.168.XXX.XXX, mască subrețea 255.255.0.0

DHCP este dezactivat în setările computerului.

Soluții

Dacă DHCP pentru obținerea unei adrese IP este automat dezactivat pe computer, nu puteți accesa Web Config. Activați DHCP.

Exemplu pentru Windows 10:

Deschideți Panoul de control și apoi faceți clic pe **Rețea și Internet** > **Rețea și centru de partajare** > **Modificare setări adaptor**. Deschideți ecranul Proprietăți al conexiunii pe care o utilizați, apoi deschideți ecranul de proprietăți pentru **Protocol Internet Versiunea 4 (TCP/IPv4)** sau **Protocol Internet Versiunea 6 (TCP/IPv6)**. Verificați dacă **Obtain an IP address automatically (Obținere adresă IP în mod automat)** este selectat pe ecranul afișat.

Personalizarea afișajului panoului de comandă

Înregistrarea Presetări

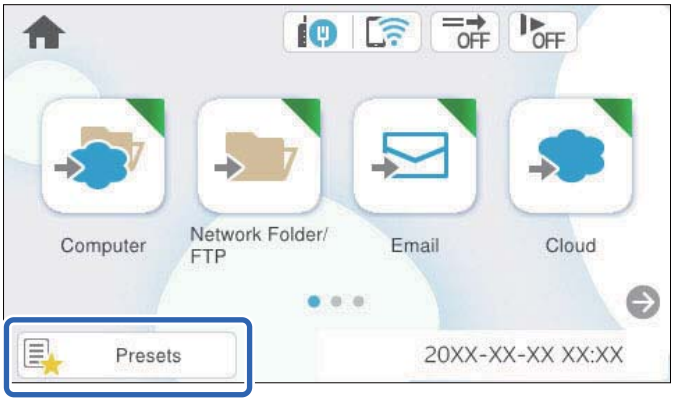
Puteți înregistra setările de scanare frecvent utilizate ca **Presetări**. Puteți înregistra până la 48 de presetări.

Notă:

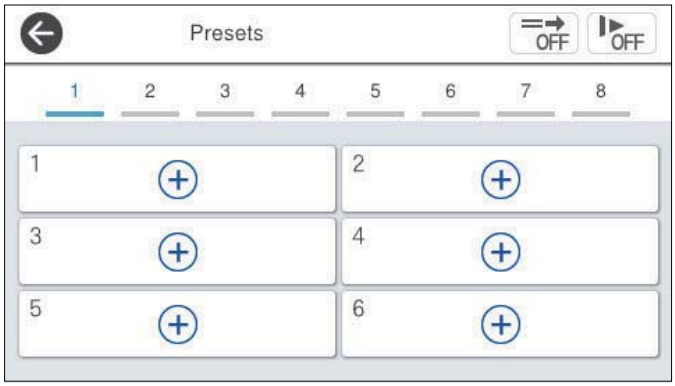
- *Puteți înregistra setările curente selectând ★ pe ecranul de începere a scanării.*
- *Puteți înregistra **Presetări** și în Web Config.*

  *Selectați fila **Scanare** > **Presetări**.*
- *Dacă selectați **Scanare către computer** la înregistrare, puteți înregistra lucrarea creată în Document Capture Pro ca **Presetări**. Aceasta este disponibilă doar pentru computerele conectate printr-o rețea. Înregistrați lucrarea în Document Capture Pro în avans.*
- *Dacă funcția de autentificare este activată, doar administratorul poate înregistra **Presetări**.*

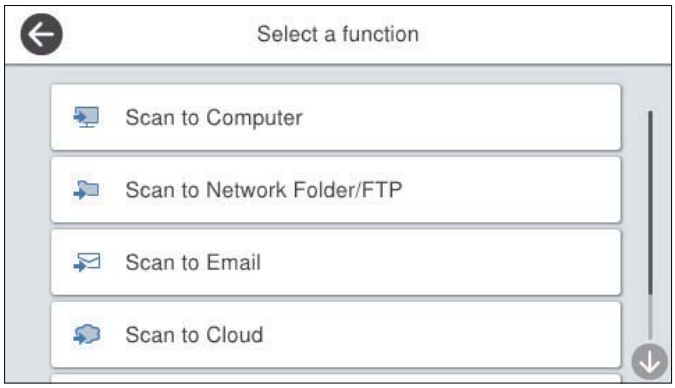
1. Selectați **Presetări** pe ecranul principal de pe panoul de comandă al scanerului.



2. Selectați ⊕.



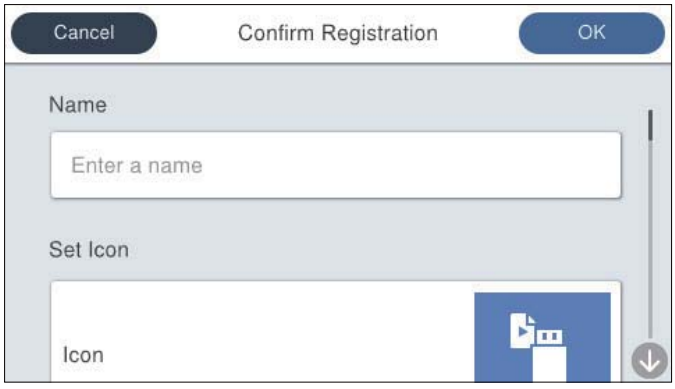
3. Selectați meniul pe care doriți să îl utilizați pentru a înregistra o presetare.



4. Setați fiecare element și selectați ☆+.

Notă:
*Când selectați **Scanare către computer**, selectați computerul pe care este instalat Document Capture Pro, apoi selectați o lucrare înregistrată. Aceasta este disponibilă doar pentru computerele conectate printr-o rețea.*

5. Efectuați setările presetării.
   - ❏ **Nume**: setați numele.
   - ❏ **Setați pictograma**: Setați imaginea și culoarea pictogramei pe care doriți să o afișați.
   - ❏ **Setări trimitere rapidă**: începe scanarea imediat, fără confirmare, când presetarea este selectată.
   - ❏ **Conținut**: verificați setările de scanare.



6. Selectați **OK**.

Opțiunile de meniu din Presetări

Puteți modifica setările unei presetări selectând › în fiecare presetare.

Modificare nume:

Modifică numele presetării.

Modificați pictograma:

Modifică imaginea pictogramei și culoarea presetării.

Setări trimitere rapidă:

Începe scanarea imediat, fără confirmare, când presetarea este selectată.

Modificare poziție:

Modifică ordinea de afișare a presetărilor.

Ștergere:

Șterge presetarea.

Adăugați sau eliminați pictograma pe pagina de pornire:

Adaugă sau șterge pictograma de presetare din ecranul principal.

Confirmare detalii:

Vizualizați setările unei presetări. Puteți încărca presetarea selectând **Ut. această setare**.

Editarea ecranului principal al panoului de comandă

Puteți particulariza ecranul principal selectând **Setări** > **Editare ecran principal** pe panoul de comandă al scanerului.

- Aspect: modifică metoda de afișare a pictogramelor de meniu.
  „Modificarea parametrului Aspect al ecranului principal” la pagina 70
- Adăugare pictogramă: adaugă pictograme la setările **Presetări** pe care le-ați stabilit sau restabilește pictogramele șterse de pe ecran.
  „Adăugare pictogramă” la pagina 71
- Ștergere pictogramă: elimină pictogramele de pe ecranul principal.
  „Ștergere pictogramă” la pagina 72
- Mutare pictogramă: modifică ordinea de afișare a pictogramelor.
  „Mutare pictogramă” la pagina 73
- Restaur. afișare pictograme implicite: restabilește setările implicite de afișare pentru ecranul principal.

Modificarea parametrului Aspect al ecranului principal

1. Selectați **Setări** > **Editare ecran principal** > **Aspect** pe panoul de comandă al scanerului.

2. Selectați **Linie** sau **Matrice**.

   Linie:

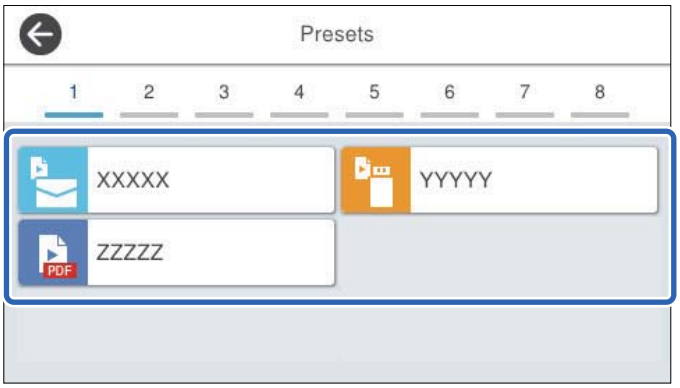
   Matrice:

3. Selectați pentru a reveni și a consulta ecranul principal.

Adăugare pictogramă

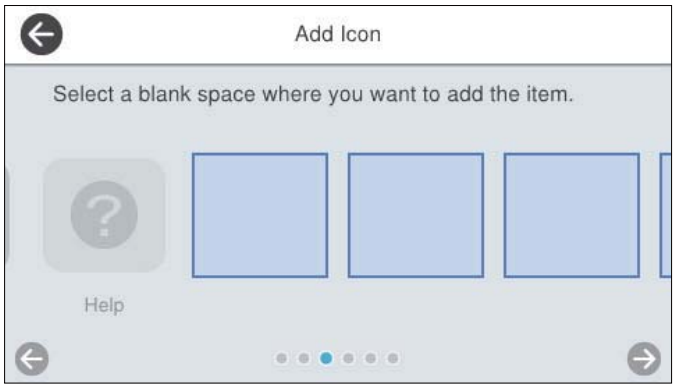
1. Selectați **Setări** > **Editare ecran principal** > **Adăugare pictogramă** pe panoul de comandă al scanerului.
2. Selectați **Funcție** sau **Presetări**.
   - ❏ Funcție: afișează funcțiile implicite indicate pe ecranul principal.
   - ❏ Presetări: afișează presetările înregistrate.

3. Selectați elementul pe care doriți să-l adăugați la ecranul principal.



4. Selectați spațiul liber unde doriți să adăugați elementul.

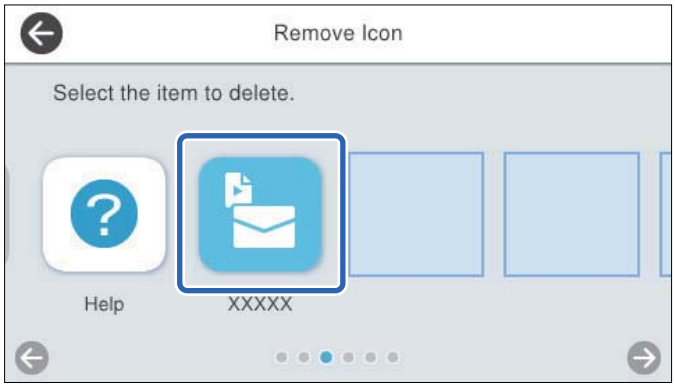
   Dacă doriți să adăugați mai multe pictograme, repetați pașii 3 și 4.



5. Selectați pentru a reveni și a consulta ecranul principal.

Ştergere pictogramă

1. Selectați **Setări** > **Editare ecran principal** > **Ştergere pictogramă** pe panoul de comandă al scanerului.
2. Selectați pictograma pe care doriți să o eliminați.



3. Selectați **Da** pentru a finaliza.

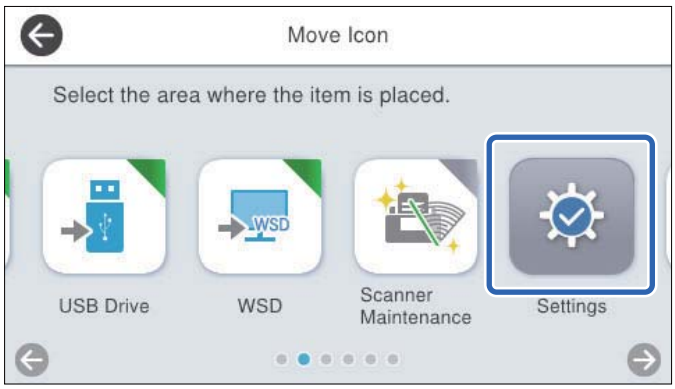
   Dacă doriți să eliminați mai multe pictograme, repetați procedurile 2 și 3.

4. Selectați pentru a reveni și a consulta ecranul principal.

Mutare pictogramă

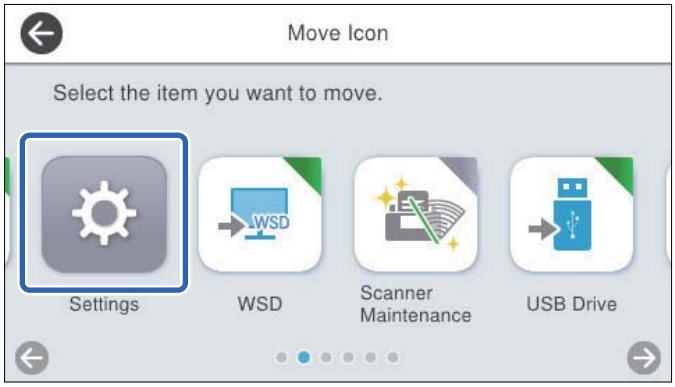
1. Selectați **Setări** > **Editare ecran principal** > **Mutare pictogramă** pe panoul de comandă al scanerului.

2. Selectați pictograma pe care doriți să o mutați.



3. Selectați cadrul destinație.

   Dacă în cadrul destinație se găsește deja o altă pictogramă, pictogramele sunt înlocuite.



4. Selectați pentru a reveni și a consulta ecranul principal.

Setări de securitate de bază

Introducerea funcțiilor de securitate ale produsului

Această secțiune prezintă funcția de securitate a dispozitivelor Epson.

Numele funcției	Tipul funcției	Ce se setează	Ce se previne
Configurarea parolei de administrator	Blochează setările sistemului, cum ar fi configurarea conexiunii pentru rețea sau USB.	Un administrator setează o parolă pentru dispozitiv. Puteți seta sau modifica parola atât de la Web Config, cât și de la panoul de comandă al scanerului.	Previne citirea și modificarea ilegală a informațiilor stocate pe dispozitiv, cum ar fi ID-ul, parola, setările de rețea etc. De asemenea, reduceți o gamă largă de riscuri de securitate, precum scurgerea de informații pentru mediul de rețea sau politica de securitate.
Setări control acces	Dacă vă conectați la dispozitiv cu un cont de utilizator înregistrat în prealabil, puteți utiliza dispozitivul.	Înregistrați orice cont de utilizator. Puteți înregistra până la 10 conturi de utilizator.	Restricționarea utilizatorilor împiedică utilizarea neautorizată a dispozitivului.
Configurarea pentru interfață externă	Controlează interfața care se conectează la dispozitiv.	Activează sau dezactivează conexiunea USB la computer.	Conexiune USB a computerului: previne utilizarea neautorizată a dispozitivului prin interzicerea scanării fără transfer prin rețea.

Informații conexe

➡ „Configurarea parolei de administrator” la pagina 75
➡ „Dezactivarea Interfeței externe” la pagina 83

Setări administrative

Configurarea parolei de administrator

Când setați parola de administrator, puteți împiedica utilizatorii să modifice setările de management de sistem. Valorile implicite sunt setate în momentul achiziției. Schimbați-le după cum este necesar.

Notă:
În cele ce urmează, sunt furnizate valorile implicite pentru informațiile de administrator.

❏ *Nume utilizator (utilizat doar pentru Web Config): niciunul (gol)*

❏ *Parola: Depinde de eticheta atașată pe produs.*

Dacă există o etichetă „PASSWORD” atașată pe spate, introduceți numărul din 8 cifre afișat pe etichetă. Dacă nu este atașată nicio etichetă „PASSWORD”, introduceți numărul de serie pe eticheta atașată pe spatele produsului pentru parola inițială de administrator.

Puteți modifica parola de administrator prin Web Config, panoul de comandă al scanerului sau Epson Device Admin. La utilizarea Epson Device Admin, consultați ghidul Epson Device Admin sau indicațiile de ajutor.

Schimbarea parolei de administrator utilizând Web Config

Schimbați parola administratorului în Web Config.

1. Accesați Web Config și selectați fila **Securitate produs** > **Modificare Parolă administrator**.
2. Introduceți informațiile necesare în **Parolă actuală**, **Nume utilizator**, **Parolă nouă** și **Confirmați parola nouă**.

   Noua parolă trebuie să aibă între 8 și 20 de caractere și să conțină doar caractere și simboluri alfanumerice cu un singur octet.

   Notă:
   În cele ce urmează, sunt furnizate valorile implicite pentru informațiile de administrator.

   ❏ *Nume utilizator: niciunul (gol)*

   ❏ *Parola: Depinde de eticheta atașată pe produs.*

   Dacă există o etichetă „PASSWORD” atașată pe spate, introduceți numărul din 8 cifre afișat pe etichetă. Dacă nu este atașată nicio etichetă „PASSWORD”, introduceți numărul de serie pe eticheta atașată pe spatele produsului pentru parola inițială de administrator.

   > ***Important:***
   > *Asigurați-vă că rețineți parola de administrator pe care ați setat-o. Dacă vă uitați parola, nu o veți putea reseta și va trebui să solicitați ajutor personalului de service.*

3. Selectați **OK**.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Modificarea parolei de administrator de la panoul de comandă al scanerului

Puteți schimba parola de administrator de la panoul de comandă al scanerului.

1. Selectați **Setări** pe panoul de comandă al scanerului.
2. Selectați **Administrare sistem** > **Setări administrator**.
3. Selectați **Parolă administrator** > **Schimbare**.
4. Introduceți parola curentă.

   Notă:
   Parola inițială de administrator (implicită) din momentul achiziției variază în funcție de eticheta atașată pe produs. Dacă există o etichetă „PASSWORD” atașată pe spate, introduceți numărul din 8 cifre afișat pe etichetă. Dacă nu este atașată nicio etichetă „PASSWORD”, introduceți numărul de serie pe eticheta atașată pe spatele produsului pentru parola inițială de administrator.

5. Introduceți noua parolă.

   Noua parolă trebuie să aibă între 8 și 20 de caractere și să conțină doar caractere și simboluri alfanumerice cu un singur octet.

> ***Important:***
>
> *Asigurați-vă că rețineți parola de administrator pe care ați setat-o. Dacă vă uitați parola, nu o veți putea reseta și va trebui să solicitați ajutor personalului de service.*

6. Introduceți noua parolă din nou pentru confirmare.

Un mesaj de finalizare este afișat.

Utilizarea Setare blocare pentru panoul de comandă

Puteți utiliza Setare blocare pentru a bloca panoul de comandă astfel încât să împiedicați utilizatorii să modifice elemente legate de setările sistemului.

Setarea Setare blocare de la panoul de comandă

1. Dacă doriți să anulați **Setare blocare** odată ce a fost activată, atingeți în colțul din dreapta sus al ecranului de pornire pentru a vă conecta ca administrator.

   nu se afișează când **Setare blocare** este dezactivată. Dacă doriți să activați această setare, treceți la pasul următor.

2. Selectați **Setări**.
3. Selectați **Administrare sistem** > **Setări administrator**.
4. Selectați **Act.** sau **Dez.** ca **Setare blocare**.

Setarea Setare blocare din Web Config

1. Selectați fila **Gestionare dispozitiv** > **Panou de control**.
2. Selectați **Activat** sau **Dezactivat** pentru **Blocare panou**.
3. Executați clic pe **OK**.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Elemente Setare blocare pe meniul Setări

Aceasta este o listă de elemente care sunt blocate în meniul **Setări** de pe panoul de comandă prin Setare blocare.

✓: se va bloca.

- : nu se va bloca.

Meniul Setări		**Setare blocare**
Setări de bază		-
	Luminozitate LCD	-
	Sunete	-
	Temporiz. oprire	✓
	Temporizator oprire	✓
	Pornire directă	✓
	Setări dată/oră	✓
	Limbă/Language	✓/-*
	Tastatură (În funcție de regiunea în care vă aflați, este posibil ca această funcție să nu fie disponibilă.)	-
	Operațiunea a expirat	✓
	Conexiune PC prin USB	✓
Setări scaner		-
	Lent	-
	Temporizare oprire alimentare dublă	✓
	Funcția DFDS	-
	Protecție hârtie	✓
	Detectare murdărie geam	✓
	Det. ultrason. alim. dublă	✓
	Expirare timp mod alimentare automată	✓
	Confirmare destinatar	✓
Editare ecran principal		✓
	Aspect	✓
	Adăugare pictogramă	✓
	Ştergere pictogramă	✓
	Mutare pictogramă	✓
	Restaur. afişare pictograme implicite	✓
Setări utilizator		✓

Meniul Setări		**Setare blocare**
	Folder de rețea/FTP	✓
	E-mail	✓
	Cloud	✓
	Unitate USB	✓
Setări rețea		✓
	Configurare Wi-Fi	✓
	Configurare LAN prin fir	✓
	Stare rețea	✓
	Complex	✓
Setări serviciu web		✓
	Servicii Epson Connect	✓
Document Capture Pro		-
	Modificați setările	✓
Administrator Contacte		-
	Înregistrare/Ştergere	✓/-*
	Frecvent	-
	Vizualizare opțiuni	-
	Opțiuni de căutare	-
Administrare sistem		✓
	Administrator Contacte	✓
	Setări administrator	✓
	Restricții	✓
	Control acces	✓
	Criptare cu parolă	✓
	Cercetare clienți	✓
	Setări WSD	✓
	Restaurare setări implicite	✓
	Actualizare firmware	✓
Informații dispozitiv		-

Meniul Setări			**Setare blocare**
	Număr de serie		-
	Versiune curentă		-
	Număr total scanări		-
	Număr scanări 1 fețe		-
	Număr scanări 2 fețe		-
	Număr scanări foaie suport		-
	Număr de scanări după înlocuirea rolei		-
	Număr de scanări după Curățare obișnuită		-
	Stare dispozitiv de autentificare		-
	Informații Epson Open Platform		-
	Menu (Resetați numărul de scanări)		✓
Întreținere scaner			-
	Curățare role		-
	Înlocuire rolă de întreținere		-
		Resetați numărul de scanări	✓
		Cum se înlocuieşte	-
	Curățare obișnuită		-
		Resetați numărul de scanări	✓
		Curățarea	-
	Curățare Geam		-
Setarea alertei de înlocuire a roților			✓
	Setare alertă contor		✓
Setări alerte curățare periodică			✓
	Setare alerte avertizare		✓
	Setare alertă contor		✓

* Puteți seta dacă să permiteți sau nu modificări în **Administrare sistem** > **Restricții**.

Conectarea ca administrator din Panoul de comandă

Când **Setare blocare** este activat, puteți utiliza oricare dintre următoarele metode pentru a vă conecta de la panoul de comandă al scanerului.

1. Atingeți  în partea dreaptă sus a ecranului.

2. Când este afișat ecranul **Selectare utilizator**, selectați **Administrator**.
3. Introduceți parola pentru conectare.

   Este afișat un mesaj de conectare completă, apoi este afișat ecranul principal pe panoul de comandă.

Pentru a vă deconecta, atingeți  în partea din dreapta sus a ecranului sau apăsați butonul .

Restricționarea funcțiilor disponibile (Control acces)

Puteți restricționa utilizatorii prin înregistrarea conturilor de utilizatori la nivelul scanerului.

Când Control acces este activat, utilizatorul poate utiliza funcții de scanare prin introducerea parolei în panoul de comandă al scanerului și prin conectare. Nu puteți scana dacă nu vă conectați.

Puteți scana de la un computer înregistrându-vă Nume utilizator și Parolă în driverul scanerului (Epson Scan 2). Consultați secțiunea de asistență Epson Scan 2 sau *Ghidul utilizatorului* al produsului pentru mai multe detalii privind efectuarea setărilor.

Crearea contului de utilizator

Puteți crea un cont Control acces.

1. Accesați Web Config și apoi selectați fila **Securitate produs** > **Setări control acces** > **Setări utilizator**.
2. Faceți clic pe **Adăugare** pentru numărul pe care doriți să-l înregistrați.

   > ***Important:***
   >
   > *Când utilizați un scaner cu un sistem de autentificare de la Epson sau de la altă companie, înregistrați Nume utilizator în Setări control acces în sloturile numerotate de la 2 la 10.*
   >
   > *Software-ul de aplicație, cum ar fi sistemul de autentificare, utilizează slotul numărul 1, astfel încât numele de utilizator nu este afișat pe panoul de comandă al scanerului.*

3. Setați fiecare element.

   ❏ Nume utilizator:

   Introduceți numele afișat în lista de nume de utilizator cu o lungime cuprinsă între 1 și 14 caractere, folosind caractere alfanumerice.

   ❏ Parolă:

   Introduceți o parolă cu până la 20 de caractere în ASCII (0x20–0x7E). Când inițializați parola, lăsați-o necompletată.

   ❏ Bifați caseta de validare pentru a activa sau dezactiva fiecare funcție.

   Selectați **Scanare** dacă doriți să permiteți funcțiile de scanare.

4. Faceți clic pe **Aplicare**.

Editarea contului de utilizator

Puteți edita contul înregistrat Control acces.

1. Accesați Web Config și apoi selectați fila **Securitate produs** > **Setări control acces** > **Setări utilizator**.
2. Faceți clic pe **Editare** pentru numărul pe care doriți să-l editați.
3. Modificați fiecare element.
4. Faceți clic pe **Aplicare**.

Ștergerea contului de utilizator

Puteți șterge contul înregistrat Control acces.

1. Accesați Web Config și apoi selectați fila **Securitate produs** > **Setări control acces** > **Setări utilizator**.
2. Faceți clic pe **Editare** pentru numărul pe care doriți să-l ștergeți.
3. Faceți clic pe **Ștergere**.

> ***Important:***
> *Când faceți clic pe **Ștergere**, contul de utilizator va fi șters fără un mesaj de confirmare. Aveți grijă când ștergeți contul.*

Activarea Control acces

Atunci când activați Control acces, doar utilizatorul înregistrat va putea să utilizeze imprimata.

Notă:
Când Setări control acces este activat, trebuie să notificați utilizatorul cu privire la informațiile contului său.

1. Accesați Web Config și apoi selectați fila **Securitate produs** > **Setări control acces** > **De bază**.
2. Selectați **Activează controlul accesului**.

   Dacă activați Setări control acces și scanați de la un computer care nu are informații de autentificare, selectați **Permiteți imprimarea și scanarea fără informații de autentificare de pe un computer**.
3. Faceți clic pe **OK**.

Conectarea pe un scaner pe care este activat Control acces

Când **Control acces** este activat, puteți utiliza oricare dintre următoarele metode pentru a vă conecta de la panoul de comandă al scanerului.

1. Atingeți în partea dreaptă sus a ecranului.
2. Când este afișat ecranul **Selectare utilizator**, selectați utilizatorul.
3. Introduceți parola pentru conectare.

   Este afișat un mesaj de conectare completă, apoi este afișat ecranul principal pe panoul de comandă.

Pentru a vă deconecta, atingeți  în partea din dreapta sus a ecranului sau apăsați butonul .

Dezactivarea Interfeței externe

Puteți dezactiva interfața folosită pentru a conecta dispozitivul la scaner. Realizați setările de restricție pentru a restricționa scanarea prin alte mijloace decât prin rețea.

Notă:
Aveți posibilitatea de a efectua setările de restricționare și pe panoul de comandă al scanerului.

Conexiune PC prin USB: ***Setări*** *>* ***Setări de bază*** *>* ***Conexiune PC prin USB***

1. Accesați Web Config și selectați fila **Securitate produs** > **Interfață externă**.
2. Selectați **Dezactivare** pentru funcțiile pe care doriți să le setați.

   Selectați **Activare** când doriți să anulați controlul.

   Conexiune PC prin USB

   Puteți restricționa utilizarea conexiunii USB de la computer. Dacă doriți să o restricționați, selectați **Dezactivare**.
3. Faceți clic pe **OK**.
4. Verificați pentru a vă asigura că portul dezactivat nu poate fi folosit.

   Conexiune PC prin USB

   Dacă driverul a fost instalat pe computer

   Conectați scanerul la computer cu ajutorul unui cablu USB, apoi confirmați că scanerul nu scanează.

   Dacă driverul nu a fost instalat pe computer

   Windows:

   Deschideți managerul de dispozitive și mențineți-l deschis, conectați scanerul la computer utilizând un cablu USB și apoi confirmați faptul că afișajul managerului de dispozitive nu se modifică.

   Mac OS:

   Conectați scanerul la computer cu ajutorul unui cablu USB, apoi confirmați că scanerul nu poate fi adăugat din **Imprimante și scanere**.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Activarea verificării programului la pornire

Dacă activați funcția de verificare a programului, scanerul efectuează verificarea la pornire pentru a identifica dacă terțe părți neautorizate au manipulat în vreun mod programul. Dacă sunt detectate probleme, scanerul nu pornește.

Notă:
Activarea acestei funcții crește timpul de pornire al scanerului.

1. Accesați Web Config, apoi selectați fila **Securitate produs** > **Verificare program la pornire**.

   Notă:
   De asemenea, puteți efectua setări pe panoul de comandă al scanerului.

   Setări > ***Administrare sistem*** > ***Verificare program la pornire***

2. Selectați **Activat** pentru a activa **Verificare program la pornire**.

3. Faceți clic pe **OK**.

Dezactivarea scanării în rețea de la computer

Puteți efectua următoarele setări în Web Config pentru a dezactiva scanarea în rețea folosind Epson Scan 2 de la computer.

1. Accesați Web Config, apoi selectați fila **Scanare** > **Scanare rețea**.

2. În **Epson Scan 2**, debifați caseta de selectare **Activare scanare**.

3. Executați clic pe **Înainte**.

   Se afișează ecranul de confirmare a setării.

4. Executați clic pe **OK**.

Activarea sau dezactivarea scanării WSD

Notă:
De asemenea, puteți efectua setări pe panoul de comandă al scanerului. Selectați ***Setări*** *>****Administrare sistem*** *>* ***Setări WSD****.*

Puteți activa sau dezactiva scanarea WSD.

Dacă nu doriți ca scanerul să fie configurat de către computerul dumneavoastră ca dispozitiv de scanare WSD, dezactivați setările WSD.

1. Accesați Web Config, apoi selectați fila **Securitate rețea** > **Protocol**.

2. În **Setări WSD**, modificați starea casetei de validare **Activare WSD**.

3. Faceți clic pe **Înainte**.

   Se afișează ecranul de confirmare a setării.

4. Faceți clic pe **OK**.

Notă:
În cazul în care computerul dumneavoastră configurează în continuare scanerul ca un dispozitiv de scanare WSD, selectați fila ***Scanare*** *>* ***Scanare rețea*** *și apoi debifați caseta de validare* ***Activare scanare*** *în* ***AirPrint****.*

Dacă AirPrint este dezactivat, scanarea Mopria de pe Chromebook, Windows și aplicația Mopria Scan sunt, de asemenea, dezactivate.

Monitorizarea unui scaner la distanță

Verificarea informațiilor pentru un scaner la distanță

Puteți verifica următoarele informații ale scanerului funcțional de la **Stare** folosind Web Config.

❏ Stare produs

Verificați starea, serviciul cloud, numărul de produs, adresa MAC etc.

❏ Stare rețea

Verificați informațiile privind starea conexiunii la rețea, adresa IP, serverul DNS etc.

❏ Stare utilizare

Verificați scanările din prima zi, numărul de scanări etc.

❏ Stare echipament hardware

Verificați starea fiecărei funcții a scanerului.

❏ Instantaneu panou

Afișează o captură a ecranului afișat pe panoul de comandă al scanerului.

Recepționarea notificărilor prin e-mail la apariția de evenimente

Despre notificările prin e-mail

Aceasta este funcția de notificare care, la apariția unor evenimente precum oprirea scanării sau erori la scaner, trimite un mesaj e-mail la adresa specificată.

Puteți înregistra până la cinci destinații și defini setările de notificare pentru fiecare destinație.

Pentru a utiliza această funcție, trebuie să configurați serverul de e-mail înainte de a defini notificările.

Informații conexe

➡ „Înregistrarea unui server de e-mail” la pagina 45

Configurarea notificării prin e-mail

Configurați notificarea prin e-mail utilizând Web Config.

1. Accesați Web Config și selectați fila **Gestionare dispozitiv** > **Înștiințare prin e-mail**.
2. Configurați subiectul notificărilor prin e-mail.

   Selectați conținutul afișat în subiect din două meniuri derulante.

   ❏ Conținutul selectat este afișat lângă **Subiect**.

   ❏ Nu se poate seta același conținut în partea stângă și în partea dreaptă.

   ❏ Când numărul de caractere din **Locație** depășește 32 de octeți, caracterele care depășesc 32 de octeți sunt omise.

3. Introduceți adresa de e-mail pentru trimiterea mesajului de notificare.

   Utilizați A – Z a – z 0 – 9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @ și introduceți între 1 și 255 de caractere.

4. Selectați limba pentru notificările prin e-mail.

5. Selectați caseta de validare pentru evenimentul pentru care doriți să primiți notificare.

   Numărul de **Setări de înștiințare** este corelat cu numărul de destinație al **Setări pentru adresa de e-mail**.

   Exemplu:

   Dacă doriți să trimiteți o notificare la adresa de e-mail setată pentru numărul 1 din **Setări pentru adresa de e-mail** când parola administratorului s-a modificat, selectați caseta de validare pentru coloana **1** din linia **Parametrul Parolă administrator a fost modificat**.

6. Faceți clic pe **OK**.

   Confirmați trimiterea unei notificări prin e-mail în urma apariției unui eveniment.

   Exemplu: parola administratorului s-a schimbat.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Elemente pentru notificarea prin e-mail

Elemente	Setări și explicație
Parametrul Parolă administrator a fost modificat	Notă atunci când parola de administrator este schimbată.
Eroare la scaner	Notă atunci când apare o eroare a scanerului.
Eroare Wi-Fi	Notificare când s-a produs o eroare la interfața LAN wireless.

Utilizarea Web Config pentru a controla sursa de alimentare a scanerului

În cazul în care computerul dumneavoastră este la distanță față de scaner, puteți utiliza în continuare Web Config pentru a opri sau reporni scanerul.

1. Accesați Web Config, apoi selectați fila **Gestionare dispozitiv** > **Pornire**.

2. Selectați **Oprire alimentare** sau **Repornire**.

3. Faceți clic pe **Executare**.

Restabilirea setărilor implicite

Puteți selecta setările de rețea sau alte setări stocate în scaner și puteți restabili aceste setări la valorile implicite.

1. Accesați Web Config, apoi selectați fila **Gestionare dispozitiv** > **Restaurare setări implicite**.

   Notă:
   De asemenea, puteți efectua setări pe panoul de comandă al scanerului.

   Setări > ***Administrare sistem*** > ***Restaurare setări implicite***

2. Selectați elementele pe care doriți să le restabiliți.

3. Faceți clic pe **Executare**.

   În final, urmați instrucțiunile afișate pe ecran.

Informații Epson Remote Services

Epson Remote Services este un serviciu care colectează periodic informații despre scaner prin Internet. Acest lucru poate fi utilizat pentru a preconiza momentul în care consumabilele și piesele de schimb trebuie să fie înlocuite sau completate și pentru a rezolva rapid eventualele erori sau probleme.

Contactați distribuitorul dumneavoastră pentru mai multe informații despre Epson Remote Services.

Rezolvarea problemelor

Parolă de administrator uitată

Aveți nevoie de asistență din partea personalului de service. Contactați distribuitorul dumneavoastră local.

Notă:
În cele ce urmează, sunt furnizate valorile inițiale pentru administratorul Web Config.

- *Nume utilizator: niciunul (gol)*
- *Parola: Depinde de eticheta atașată pe produs.*

  Dacă există o etichetă „PASSWORD" atașată pe spate, introduceți numărul din 8 cifre afișat pe etichetă.

  Dacă nu este atașată nicio etichetă „PASSWORD", introduceți numărul de serie pe eticheta atașată pe spatele produsului pentru parola inițială de administrator.

Dacă restabiliți parola de administrator, aceasta este resetată la valoarea inițială din momentul achiziției.

Setări de securitate avansate

Setări de securitate și de prevenire a pericolelor

Atunci când un scaner este conectat la o rețea, îl puteți accesa dintr-o locație aflată la distanță. În plus, mai multe persoane pot partaja scanerul, ceea ce este util pentru îmbunătățirea eficienței operaționale și a comodității. Cu toate acestea, riscurile, cum ar fi accesul ilegal, folosirea ilegală și manipularea frauduloasă a datelor sunt crescute. Dacă folosiți scanerul într-un mediu unde puteți accesa internetul, riscurile sunt chiar mai mari.

Pentru scanerele fără protecție la accesul din exterior, va fi posibilă citirea jurnalelor cu lucrările de tipărire, stocate în imprimantă, de pe internet.

Pentru a evita acest risc, scanerele Epson dispun de o varietate de tehnologii de securitate.

Setați scanerul așa cum este necesar, în funcție de condițiile de mediu integrate cu informațiile de mediu ale clientului.

Nume	Tipul caracteristicii	Ce să setați	Ce să preveniți
Controlul protocolului	Controlează protocoalele și serviciile care vor fi utilizate pentru comunicația între scanere și computere și activează și dezactivează funcții.	Un protocol sau serviciu aplicat funcțiilor permise sau interzise separat.	Reducerea riscurilor de securitate care pot apărea prin utilizarea neintenționată, împiedicând utilizatorii să folosească funcțiile inutile.
Comunicații SSL/TLS	Conținutul comunicației este criptat în cazul comunicațiilor SSL/TLS la accesarea serverului Epson pe internet de pe scaner, cum ar fi comunicația cu computerul prin intermediul browserului web, utilizarea Epson Connect și actualizarea firmware-ului.	Obțineți un certificat semnat CA și importați-l la scaner.	Identificarea scanerului prin certificare semnată CA previne asumarea de identități false și accesul neautorizat. În plus, conținutul comunicației SSL/TLS este protejat și se previn scurgerile de conținut privind datele de tipărire și informațiile de configurare.
Filtrare IPsec/IP	Puteți seta pentru a permite întreruperea transferului de date de la un anumit client sau un anumit tip. Deoarece IPsec protejează datele pe unități de pachete IP (criptare și autentificare), puteți comunica în condiții de siguranță cu un protocol nesecurizat.	Creați o politică de bază și o politică individuală pentru a seta clientul sau tipul de date care pot accesa scanerul.	Protejați împotriva accesului neautorizat, a manipulării frauduloase a datelor și a interceptării datelor de comunicații la scaner.
IEEE 802.1X	Permite doar utilizatorilor autentificați să se conecteze la rețea. Permite utilizarea scanerului doar de către un utilizator autentificat.	Setare de autentificare la serverul RADIUS (server de autentificare).	Protejați împotriva accesării și utilizării neautorizate a scanerului.

Informații conexe

- „Controlarea utilizând protocoale” la pagina 90
- „Comunicare SSL/TLS cu scanerul” la pagina 98
- „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 99
- „Conectarea scanerului la o rețea IEEE802.1X” la pagina 111

Setări pentru funcția de securitate

La setarea filtrării IPsec/IP sau IEEE 802.1X, se recomandă accesarea Web Config utilizând SSL/TLS pentru a comunica informațiile privind setările, pentru a reduce riscurile de securitate precum modificarea sau interceptarea.

Asigurați-vă că parola de administrator este configurată înaintea setării pentru filtrarea IPsec/IP sau IEEE 802.1X.

Controlarea utilizând protocoale

Puteți scana folosind o varietate de modalități și protocoale. De asemenea, puteți utiliza scanarea în rețea de la un număr nespecificat de computere din rețea.

Puteți reduce riscurile de securitate cauzate de accesul neautorizat prin restricționarea scanării de la anumite căi sau prin controlarea funcțiilor disponibile.

Protocoale de control

Configurați setările protocoalelor acceptate de scaner.

1. Accesați Web Config și selectați fila **Securitate rețea** tab > **Protocol**.
2. Configurați fiecare articol.
3. Faceți clic pe **Înainte**.
4. Faceți clic pe **OK**.

   Setările vor fi aplicate la nivelul scanerului.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Protocoale pe care le puteți activa sau dezactiva

Protocol	Descriere
Setări Bonjour	Puteți să specificați dacă doriți să utilizați serviciul Bonjour. Bonjour este utilizat pentru căutarea dispozitivelor, scanare şi multe altele.
Setări SLP	Puteți activa sau dezactiva funcția SLP. Funcția SLP este utilizată pentru scanarea push și pentru căutarea în rețea prin intermediul EpsonNet Config.
Setări WSD	Puteți activa sau dezactiva funcția WSD. Când această funcție este activată, puteți să adăugați dispozitive WSD şi să scanați de la portul WSD.
Setări LLTD	Puteți activa sau dezactiva funcția LLTD. Când această funcție este activată, este afișată în harta de rețea a sistemului Windows.
Setări LLMNR	Puteți activa sau dezactiva funcția LLMNR. Când această funcție este activată, puteți utiliza rezoluții de nume fără NetBIOS, chiar dacă nu puteți utiliza serviciul DNS.

Protocol	Descriere
Setări SNMPv1/v2c	Puteți să specificați dacă doriți sau nu să activați caracteristica SNMPv1/v2c. Aceasta este utilizată pentru configurarea dispozitivelor, monitorizare etc.
Setări SNMPv3	Puteți să specificați dacă doriți sau nu să activați caracteristica SNMPv3. Aceasta este utilizată pentru configurarea dispozitivelor criptate, monitorizare etc.

Elemente de setare a protocoalelor

Setări Bonjour

Elemente	Valoare de setare și descriere
Utilizare Bonjour	Selectați această opțiune pentru a căuta sau utiliza dispozitive folosind serviciul Bonjour.
Nume Bonjour	Afișează numele Bonjour.
Nume serviciu Bonjour	Afișează numele serviciului Bonjour.
Locație	Afișează numele locației Bonjour.
Wide-Area Bonjour	Setați dacă se va utiliza Wide-Area Bonjour.

Setări SLP

Elemente	Valoare de setare și descriere
Activare SLP	Selectați această opțiune pentru a activa funcția SLP. Aceasta este utilizată precum căutarea în rețea în EpsonNet Config.

Setări WSD

Elemente	Valoare de setare și descriere
Activare WSD	Selectați această opțiune pentru a permite adăugarea dispozitivelor utilizând WSD și scanarea de la portul WSD.
Expirare scanare (sec.)	Introduceți valoarea de expirare a comunicațiilor pentru scanarea WSD, între 3 și 3.600 de secunde.
Nume dispozitiv	Afișează numele dispozitivului WSD.
Locație	Afișează numele locației WSD.

Setări LLTD

Elemente	Valoare de setare și descriere
Activare LLTD	Selectați această opțiune pentru a activa LLTD. Scanerul este afișată în harta de rețea a sistemului Windows.
Nume dispozitiv	Afișează numele dispozitivului LLTD.

Setări LLMNR

Elemente	Valoare de setare și descriere
Activare LLMNR	Selectați această opțiune pentru a activa LLMNR. Puteți utiliza rezoluții de nume fără NetBIOS, chiar dacă nu puteți utiliza serviciul DNS.

Setări SNMPv1/v2c

Elemente	Valoare de setare și descriere
Activare SNMPv1/v2c	Selectați această opțiune pentru a activa SNMPv1/v2c.
Autoritate de acces	Setați autoritatea de acces atunci când este activată funcția SNMPv1/v2c. Selectați **Doar citire** sau **Citire/Scriere**.
Nume comunitate (Numai citire)	Introduceți între 0 și 32 de caractere ASCII (între 0x20 și 0x7E).
Nume comunitate (Citire/Scriere)	Introduceți între 0 și 32 de caractere ASCII (între 0x20 și 0x7E).

Setări SNMPv3

Elemente		Valoare de setare și descriere
Activare SNMPv3		SNMPv3 este activat atunci când caseta este bifată.
Nume utilizator		Introduceți între 1 și 32 de caractere folosind caractere a câte 1 octet.
Setări de autentificare		
	Algoritm	Selectați un algoritm de autentificare pentru SNMPv3.
	Parolă	Introduceți o parolă de autentificare pentru SNMPv3. Introduceți între 8 și 32 de caractere în ASCII (0x20 – 0x7E). Dacă nu specificați acest element, lăsați-l necompletat.
	Confirmare parolă	Pentru confirmare, introduceți parola configurată.
Setări de criptare		
	Algoritm	Selectați un algoritm de criptare pentru SNMPv3.
	Parolă	Introduceți o parolă de criptare pentru SNMPv3. Introduceți între 8 și 32 de caractere în ASCII (0x20 – 0x7E). Dacă nu specificați acest element, lăsați-l necompletat.
	Confirmare parolă	Pentru confirmare, introduceți parola configurată.
Nume contextual		Introduceți cel mult 32 de caractere în Unicode (UTF-8). Dacă nu specificați acest element, lăsați-l necompletat. Numărul de caractere care pot fi introduse variază în funcție de limbă.

Utilizarea unui certificat digital

Despre certificarea digitală

❏ Certificat semnat de CA

Acesta este un certificat semnat de către CA (Autoritatea de certificare). Pentru a-l obține, trebuie să vă adresați autorității de certificare. Acest certificat atestă existența scanerului și faptul că aceasta este utilizată pentru comunicațiile SSL/TLS, pentru a asigura siguranța comunicației datelor.

Când este utilizat pentru comunicațiile SSL/TLS, se utilizează ca certificat de server.

Când este setat la IPsec/IP Filtering sau comunicații IEEE 802.1X, este utilizat ca certificat de client.

❏ Certificat CA

Acesta este un certificat corelat cu Certificat semnat de CA, denumit și certificat CA intermediar. Este utilizat de către browserul web pentru a valida calea certificatului scanerului la accesarea serverului celeilalte părți sau a Web Config.

Pentru certificatul CA, setați momentul validării căii certificatului serverului prin accesare de la scaner. Pentru scaner, setați certificarea căii Certificat semnat de CA pentru certificare SSL/TLS.

Puteți obține certificatul CA al scanerului de la autoritatea de certificare de la care a fost emis certificatul CA.

De asemenea, puteți obține certificatul CA utilizat pentru validarea serverului celeilalte părți de la autoritatea de certificare care a emis Certificat semnat de CA al celuilalt server.

❏ Certificat auto-semnat

Acesta este un certificat pe care scanerul îl semnează și și-l emite sie însuși. Se mai numește și certificat rădăcină. Deoarece emitentul se auto-certifică, nu prezintă încredere și nu poate preveni preluarea de identități.

Utilizați-l când efectuați setarea de securitate și la efectuarea de comunicații SSL/TLS simple fără Certificat semnat de CA.

Dacă folosiți acest certificat pentru o comunicație SSL/TLS, este posibil să se afișeze o alertă de securitate în browserul web, întrucât certificatul nu este înregistrat la un browser web. Puteți folosi Certificat auto-semnat numai pentru o comunicație SSL/TLS.

Informații conexe

➡ „Configurarea unui Certificat semnat de CA” la pagina 93

➡ „Actualizarea unui certificat autosemnat” la pagina 97

➡ „Configurarea unui Certificat CA” la pagina 97

Configurarea unui Certificat semnat de CA

Obținerea unui certificat CA-semnat

Pentru obținerea unui certificat CA-semnat, creați o CSR (Cerere de semnare certificat) și trimiteți această cerere spre autoritatea de certificare. Puteți crea o CSR folosind Web Config și un computer.

Urmați etapele pentru a crea o CSR și a obține un certificat CA-semnat folosind Web Config. Când creați o CSR folosind Web Config, certificatul este în formatul PEM/DER.

1. Accesați Web Config și apoi selectați fila **Securitate rețea**. Apoi, selectați **SSL/TLS** > **Certificat** sau **IPsec/IP Filtering** > **Certificat client** sau **IEEE802.1X** > **Certificat client**.

   Indiferent de opțiunea selectată, puteți obține același certificat și îl puteți utiliza în comun.

2. Faceți clic pe **Generare** a/al **CSR**.

   O pagină de creare CSR este deschisă.

3. Introduceți o valoare pentru fiecare element.

   Notă:
   Lungimea disponibilă pentru cheie și abrevierile variază în funcție de autoritatea de certificare. Creați o cerere în conformitate cu regulile fiecărei autorități de certificare.

4. Faceți clic pe **OK**.

   Un mesaj de finalizare este afișat.

5. Selectați fila **Securitate rețea**. Apoi, selectați **SSL/TLS** > **Certificat** sau **IPsec/IP Filtering** > **Certificat client** sau **IEEE802.1X** > **Certificat client**.

6. Faceți clic pe unul dintre butoanele de descărcare a **CSR** în conformitate cu formatul indicat de către fiecare autoritate de certificare pentru a descărca o CSR pe un computer.

   > ***Important:***
   > *Nu generați din nou o CSR. Dacă faceți acest lucru, nu veți putea importa un Certificat semnat de CA emis.*

7. Trimiteți CSR unei autorități de certificare și obțineți un Certificat semnat de CA.

   Urmați regulile fiecărei autorități de certificare cu privire la metoda și forma de trimitere.

8. Salvați Certificat semnat de CA emis pe un computer conectat la scaner.

   Obținerea unui Certificat semnat de CA este finalizată când salvați un certificat la o destinație.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Elemente setare CSR

Elemente	Setări și explicație
Lungime cheie	Selectați o lungime de cheie pentru o CSR.
Nume comun	Puteți introduce între 1 și 128 de caractere. Dacă aceasta este o adresă IP, aceasta trebuie să fie o adresă IP statică. Puteți introduce între 1 și 5 adrese IPv4, adrese IPv6, nume de gazdă, FQDN-uri, separate prin virgulă. Primul element este stocat în numele comun, iar celelalte elemente sunt stocate în câmpul alias al subiectului certificatului. Exemplu: Adresa IP a scanerului: 192.0.2.123, Nume scaner: EPSONA1B2C3 Nume comun: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

Elemente	Setări și explicație
Organizație/ Unitate organizatorică/ Localitate/ Stat/Provincie	Puteți introduce între 0 și 64 de caractere în ASCII (0x20 – 0x7E). Puteți separa numele distincte cu virgule.
Țară	Introduceți un cod de țară, având un număr de două cifre indicat de ISO-3166.
Adresă e-mail expeditor	Puteți introduce adresa de e-mail a expeditorului pentru setarea serverului de e-mail. Introduceți aceeași adresă de e-mail ca **Adresă e-mail expeditor** pentru fila **Rețea** > **Server e-mail** > **De bază**.

Import al unui certificat CA-semnat

Importați Certificat semnat de CA obținut la scaner.

Important:

❏ *Asigurați-vă că data și ora scanerului sunt setate corect. Certificatul poate fi nevalid.*

❏ *Dacă obțineți un certificat folosind o CSR creată din Web Config, puteți importa un certificat o singură dată.*

1. Accesați Web Config și apoi selectați fila **Securitate rețea**. Apoi, selectați **SSL/TLS** > **Certificat** sau **IPsec/IP Filtering** > **Certificat client** sau **IEEE802.1X** > **Certificat client**.

2. Faceți clic pe **Import**

   O pagină de import certificat este deschisă.

3. Introduceți o valoare pentru fiecare element. Setați **Certificat CA 1** și **Certificat CA 2** când verificați calea certificatului în browser-ul web care accesează scanerul.

   În funcție de locul unde creați o CSR și formatul de fișier al certificatului, setările necesare pot varia. Introduceți valorile pentru elementele necesare în conformitate cu cele indicate mai jos.

   ❏ Un certificat în format PEM/DER obținut de la Web Config

   ❏ **Cheie privată**: nu configurați, deoarece scanerul conține o cheie privată.

   ❏ **Parolă**: nu configurați.

   ❏ **Certificat CA 1**/**Certificat CA 2**: Opțional

   ❏ Un certificat în format PEM/DER obținut de la un computer

   ❏ **Cheie privată**: Trebuie să setați.

   ❏ **Parolă**: nu configurați.

   ❏ **Certificat CA 1**/**Certificat CA 2**: Opțional

   ❏ Un certificat în format PKCS#12 obținut de la un computer

   ❏ **Cheie privată**: nu configurați.

   ❏ **Parolă**: Opțional

   ❏ **Certificat CA 1**/**Certificat CA 2**: Nu configurați.

4. Faceți clic pe **OK**.

   Un mesaj de finalizare este afișat.

Notă:
*Faceți clic pe **Confirmare** pentru a verifica informația de certificat.*

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Elemente de setare pentru importarea certificatului CA semnat

Elemente	Setări și explicație
Certificat server sau Certificat client	Selectați un format de certificat. Pentru conexiunea SSL/TLS, este afișat Certificat server. Pentru filtrarea IPsec/IP sau IEEE 802.1X, este afișat Certificat client.
Cheie privată	Dacă obțineți un certificat în format PEM/DER prin utilizarea CSR creat de către un computer, specificați un fișier cheie privat corespunzător certificatului.
Parolă	Dacă formatul fișierului este **Certificat cu cheie privată (PKCS#12)** introduceți parola pentru criptarea cheii private care este setată la obținerea certificatului.
Certificat CA 1	Dacă formatul certificatului dumneavoastră este **Certificat (PEM/DER)**, importați un certificat al unei autorități de certificare care emite un Certificat semnat de CA utilizat ca certificat de server. Specificați un fișier dacă este nevoie.
Certificat CA 2	Dacă formatul certificatului dumneavoastră este **Certificat (PEM/DER)**, importați un certificat ale unei autorități de certificare care emite Certificat CA 1. Specificați un fișier dacă este nevoie.

Ştergerea unui certificat CA-semnat

Puteți șterge un certificat importat când certificatul a expirat sau când nu mai este necesară o conexiune criptată.

> ***Important:***
> *Dacă obțineți un certificat folosind o CSR creată din Web Config, nu mai puteți importa din nou un certificat șters.În acest caz, creați o CSR și obțineți din nou un certificat.*

1. Accesați Web Config și apoi selectați fila **Securitate rețea**.Apoi, selectați **SSL/TLS** > **Certificat** sau **IPsec/IP Filtering** > **Certificat client** sau **IEEE802.1X** > **Certificat client**.
2. Faceți clic pe **Ştergere**.
3. În mesajul care apare, confirmați faptul că doriți să ștergeți certificatul.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Actualizarea unui certificat autosemnat

Deoarece Certificat auto-semnat este emis de către scaner, îl puteți utiliza atunci când a expirat sau când este modificat conținutul descris.

1. Accesați Web Config și selectați fila **Securitate rețea** tab > **SSL/TLS** > **Certificat**.
2. Faceți clic pe **Actualizare**.
3. Introduceți **Nume comun**.

   Puteți introduce până la 5 adrese IPv4, adrese IPv6, nume de gazdă, FQDN-uri între 1 și 128 de caractere și separate prin virgulă. Primul parametru este stocat în numele comun, iar ceilalți sunt stocați în câmpul alias al subiectului certificatului.

   Exemplu:

   Adresa IP a scanerului: 192.0.2.123, Nume scaner: EPSONA1B2C3

   Nume obișnuit: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Indicați o perioadă de valabilitate pentru certificat.
5. Faceți clic pe **Înainte**.

   Un mesaj de confirmare este afișat.
6. Faceți clic pe **OK**.

   Scanerul este actualizat.

Notă:
*Puteți verifica informațiile de certificat din fila **Securitate rețea** > **SSL/TLS** > **Certificat** > **Certificat auto-semnat** și faceți clic pe **Confirmare**.*

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Configurarea unui Certificat CA

La setarea Certificat CA, puteți valida calea către certificatul CA al serverului pe care îl accesează scanerul. Aceasta poate preveni asumarea de false identități.

Puteți obține Certificat CA de la autoritatea de certificare de la care a fost emis Certificat semnat de CA.

Importarea unui Certificat CA

Importați Certificat CA la scaner.

1. Accesați Web Config, apoi selectați fila **Securitate rețea** > **Certificat CA**.
2. Faceți clic pe **Import**.
3. Specificați Certificat CA pe care doriți să-l importați.
4. Faceți clic pe **OK**.

După terminarea importului, veți reveni la ecranul **Certificat CA**, iar Certificat CA importat va fi afișat.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Ștergerea unui Certificat CA

Puteți șterge fișierul importat Certificat CA.

1. Accesați Web Config și apoi selectați fila **Securitate rețea** > **Certificat CA**.
2. Faceți clic pe **Ștergere** lângă fișierul Certificat CA pe care doriți să îl ștergeți.
3. Confirmați că doriți să ștergeți certificatul în mesajul afișat.
4. Faceți clic pe **Reinițializare rețea** și apoi asigurați-vă că certificatul CA șters nu este listat pe ecranul actualizat.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Comunicare SSL/TLS cu scanerul

Atunci când certificatul de server este stabilit cu ajutorul comunicării SSL/TLS (Standard de securitate în informații/Protocol pentru securitatea transferurilor) cu scanerul, puteți cripta calea de comunicare între computere. Faceți acest lucru dacă doriți să evitați accesul neautorizat de la distanță.

Configurarea setărilor de bază SSL/TLS

Dacă scanerul acceptă funcția de server HTTPS, puteți utiliza o comunicare de tip SSL/TLS pentru criptarea comunicațiilor. Puteți configura și gestiona scanerul utilizând Web Config, asigurând în același timp securitatea acestuia.

Configurați puterea de criptare și funcția de redirecționare.

1. Accesați Web Config și selectați fila **Securitate rețea** > **SSL/TLS** > **De bază**.
2. Selectați o valoare pentru fiecare element.
   - ❏ Forță criptare
     Selectați nivelul de putere de criptare.
   - ❏ Redirecționare HTTP către HTTPS
     Redirecționare către HTTPS atunci când este accesat HTTP.
3. Faceți clic pe **Înainte**.
   Este afișat un mesaj de confirmare.

4. Faceți clic pe **OK**.

   Scanerul este actualizat.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Configurarea unui certificat de server pentru scaner

1. Accesați Web Config și selectați fila **Securitate rețea** > **SSL/TLS** > **Certificat**.
2. Indicați un certificat pentru a fi folosit pe **Certificat server**.
   - ❏ Certificat auto-semnat

     Un certificat autosemnat a fost generat de scaner. Dacă nu obțineți un certificat semnat CA, selectați această opțiune.
   - ❏ Certificat semnat de CA

     Dacă obțineți și importați un certificat semnat CA în prealabil, puteți indica acest lucru.
3. Faceți clic pe **Înainte**.

   Un mesaj de confirmare este afișat.
4. Faceți clic pe **OK**.

   Scanerul este actualizat.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38
➡ „Configurarea unui Certificat semnat de CA” la pagina 93
➡ „Configurarea unui Certificat CA” la pagina 97

Comunicare criptată utilizând filtrarea IPsec/IP

Despre IPsec/IP Filtering

Puteți filtra traficul în funcție de adresele IP; de servicii și de port utilizând funcția IPsec/IP Filtering (IPsec/Filtrare IP). Prin combinarea filtrării, puteți configura scanerul să accepte sau să blocheze clienți indicați și date indicate. În plus, puteți îmbunătăți nivelul de securitate folosind un IPsec.

Notă:
Computerele care rulează Windows Vista sau o versiune mai nouă sau Windows Server 2008 sau mai nouă acceptă IPsec.

Configurarea politicii implicite

Pentru a filtra traficul, configurați politica implicită. Politica implicită se aplică fiecărui utilizator sau grup care se conectează la scaner. Pentru un control mai rafinat al utilizatorilor și al grupurilor de utilizatori, configurați politicile de grup.

1. Accesați Web Config și apoi selectați fila **Securitate rețea** > **IPsec/IP Filtering** > **De bază**.
2. Introduceți o valoare pentru fiecare element.
3. Faceți clic pe **Înainte**.

   Un mesaj de confirmare este afișat.
4. Faceți clic pe **OK**.

   Scanerul este actualizat.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Elemente de setare Politică implicită

Politică implicită

Elemente	Setări și explicație
IPsec/IP Filtering	Puteți activa sau dezactiva o funcție de filtrare IPsec/IP.

❏ **Control acces**

Configurați o metodă de control pentru traficul pachetelor IP.

Elemente	Setări și explicație
Permitere acces	Selectați această opțiune pentru a permite trecerea pachetelor IP configurate.
Refuzare acces	Selectați această opțiune pentru a împiedica pachetele IP configurate să treacă.
IPsec	Selectați această opțiune pentru a permite pachetelor IPsec configurate să treacă.

❏ **Versiune IKE**

Selectați **IKEv1** sau **IKEv2** pentru **Versiune IKE**. Selectați una dintre acestea, în funcție de dispozitivul la care este conectat scanerul.

❏ IKEv1

Următoarele elemente sunt afișate atunci când selectați **IKEv1** pentru **Versiune IKE**.

Elemente	Setări și explicație
Metodă de autentificare	Pentru a selecta **Certificat**, trebuie să obțineți și să importați un certificat semnat CA în prealabil.
Cheie pre-partajată	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
Confirmare Cheie pre-partajată	Pentru confirmare, introduceți cheia configurată.

❏ IKEv2

Următoarele elemente sunt afișate atunci când selectați **IKEv2** pentru **Versiune IKE**.

Elemente		Setări și explicație
Local	Metodă de autentificare	Pentru a selecta **Certificat**, trebuie să obțineți și să importați un certificat semnat CA în prealabil.
	Tip ID	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, selectați tipul ID-ului pentru scaner.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@", „#" și „=" pentru primul caracter. **Nume distinct**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=". **Adresă IP**: Introduceți formatul IPv4 sau IPv6. **FQDN**: introduceți o combinație cuprinsă între 1 și 255 de caractere folosind A – Z, a – z, 0 – 9, „-" și punct (.). **Adresă de e-mail**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@". **ID cheie**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E).
	Cheie pre-partajată	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirmare Cheie pre-partajată	Pentru confirmare, introduceți cheia configurată.

Elemente		Setări și explicație
La distanță	Metodă de autentificare	Pentru a selecta **Certificat**, trebuie să obțineți și să importați un certificat semnat CA în prealabil.
	Tip ID	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, selectați tipul de ID pentru dispozitivul pe care doriți să-l autentificați.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@", „#" și „=" pentru primul caracter. **Nume distinct**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=". **Adresă IP**: Introduceți formatul IPv4 sau IPv6. **FQDN**: introduceți o combinație cuprinsă între 1 și 255 de caractere folosind A – Z, a – z, 0 – 9, „-" și punct (.). **Adresă de e-mail**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@". **ID cheie**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E).
	Cheie pre-partajată	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirmare Cheie pre-partajată	Pentru confirmare, introduceți cheia configurată.

❏ Încapsulare

Dacă selectați **IPsec** pentru **Control acces**, trebuie să configurați un mod capsulare.

Elemente	Setări și explicație
Mod transport	Dacă utilizați scanerul numai pe același LAN, selectați această opțiune. Pachetele IP de strat 4 sau ulterior sunt criptate.
Mod tunel	Dacă folosiți scanerul într-o rețea cu conexiune la internet, precum IPsec-VPN, selectați această opțiune. Antetul și datele pachetelor IP sunt criptate. **Poartă gateway la distanță (Mod tunel)**: dacă selectați **Mod tunel** pentru **Încapsulare**, introduceți o adresă de gateway folosind între 1 și 39 de caractere.

❏ Protocol de securitate

Dacă selectați **IPsec** pentru **Control acces**, selectați o opțiune.

Elemente	Setări și explicație
ESP	Selectați această opțiune pentru a garanta integritatea unei autentificări și a datelor și pentru a cripta datele.
AH	Selectați această opțiune pentru a garanta integritatea unei autentificări și a datelor. Chiar dacă este interzisă criptarea datelor, puteți folosi IPsec.

❏ **Setări algoritm**

Se recomandă să selectați **Oricare** pentru toate setările sau să selectați un alt element decât **Oricare** pentru fiecare setare. Dacă selectați **Oricare** pentru unele setări și selectați un alt element decât **Oricare** pentru celelalte setări, este posibil ca dispozitivul să nu comunice, în funcție de celălalt dispozitiv pe care doriți să-l autentificați.

Elemente		Setări și explicație
IKE	Criptare	Selectați algoritmul de criptare pentru IKE. Elementele variază în funcție de versiunea IKE.
	Autentificare	Selectați algoritmul de autentificare pentru IKE.
	Schimb de chei	Selectați algoritmul de schimb cheie pentru IKE. Elementele variază în funcție de versiunea IKE.
ESP	Criptare	Selectați algoritmul de criptare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Protocol de securitate**.
	Autentificare	Selectați algoritmul de autentificare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Protocol de securitate**.
AH	Autentificare	Selectați algoritmul de criptare pentru AH. Aceasta este disponibilă atunci când **AH** este selectat pentru **Protocol de securitate**.

Configurarea politicii de grup

O politică de grup înseamnă una sau mai multe reguli aplicate unui utilizator sau grup de utilizatori. Scanerul controlează pachetele IP care corespund politicilor configurate. Pachetele IP sunt autentificate în ordinea unei politici de grup de 1 la 10, iar apoi în funcție de politica implicită.

1. Accesați Web Config și apoi selectați fila **Securitate rețea** > **IPsec/IP Filtering** > **De bază**.
2. Executați clic pe o filă numerotată pe care doriți să o configurați.
3. Introduceți o valoare pentru fiecare element.
4. Faceți clic pe **Înainte**.

   Un mesaj de confirmare este afișat.
5. Faceți clic pe **OK**.

   Scanerul este actualizat.

Elemente de setare Politică grup

Elemente	Setări și explicație
Se activează această Politică grup	Puteți activa sau dezactiva o politică de grup.

Control acces

Configurați o metodă de control pentru traficul pachetelor IP.

Elemente	Setări și explicație
Permitere acces	Selectați această opțiune pentru a permite trecerea pachetelor IP configurate.
Refuzare acces	Selectați această opțiune pentru a împiedica pachetele IP configurate să treacă.
IPsec	Selectați această opțiune pentru a permite pachetelor IPsec configurate să treacă.

Adresă locală (scaner)

Selectați o adresă IPv4 sau o adresă IPv6 care corespunde mediului dumneavoastră de rețea. Dacă o adresă IP este alocată automat, puteți selecta **Utilizare adresă IPv4 obținută automat**.

Notă:
Dacă o adresă IPv6 este alocată automat, conexiunea nu va fi disponibilă. Configurați o adresă IPv6 statică.

Adresă la distanță (Gazdă)

Introduceți o adresă IP a dispozitivului pentru a controla accesul. Adresa IP trebuie să aibă 43 de caractere sau mai puține. Dacă nu introduceți o adresă IP, toate adresele sunt controlate.

Notă:
Dacă o adresă IP este alocată automat (de exemplu, alocată de DHCP), s-ar putea ca conexiunea să nu fie disponibilă. Configurați o adresă IP statică.

Metodă de selectare port

Selectați o metodă pentru a specifica porturile.

❏ Nume serviciu

Dacă selectați **Nume serviciu** pentru **Metodă de selectare port**, selectați o opțiune.

❏ Protocol transport

Dacă selectați **Număr port** pentru **Metodă de selectare port**, trebuie să configurați un mod capsulare.

Elemente	Setări și explicație
Orice protocol	Selectați această opțiune pentru a controla toate tipurile de protocol.
TCP	Selectați această opțiune pentru a controla datele pentru difuzare unică.
UDP	Selectați această opțiune pentru a controla datele pentru transmitere și difuzare multiplă.
ICMPv4	Selectați această opțiune pentru a controla comanda ping.

❏ Port local

Dacă selectați **Număr port** pentru **Metodă de selectare port** și dacă selectați **TCP** sau **UDP** pentru **Protocol transport**, introduceți numerele de port pentru a controla pachetele recepționate, separându-le prin virgulă. Puteți introduce maximum 10 numere de port.

Exemplu: 20,80,119,5220

Dacă nu introduceți un număr de port, toate porturile sunt controlate.

❏ Port la distanță

Dacă selectați **Număr port** pentru **Metodă de selectare port** și dacă selectați **TCP** sau **UDP** pentru **Protocol transport**, introduceți numerele de port pentru a controla pachetele trimise, separându-le prin virgulă. Puteți introduce maximum 10 numere de port.

Exemplu: 25,80,143,5220

Dacă nu introduceți un număr de port, toate porturile sunt controlate.

Versiune IKE

Selectați **IKEv1** sau **IKEv2** pentru **Versiune IKE**. Selectați una dintre acestea, în funcție de dispozitivul la care este conectat scanerul.

❏ IKEv1

Următoarele elemente sunt afișate atunci când selectați **IKEv1** pentru **Versiune IKE**.

Elemente	Setări și explicație
Metodă de autentificare	Dacă selectați **IPsec** pentru **Control acces**, selectați o opțiune. Un certificat folosit este comun cu o politică implicită.
Cheie pre-partajată	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
Confirmare Cheie pre-partajată	Pentru confirmare, introduceți cheia configurată.

❏ IKEv2

Următoarele elemente sunt afișate atunci când selectați **IKEv2** pentru **Versiune IKE**.

Elemente		Setări și explicație
Local	Metodă de autentificare	Dacă selectați **IPsec** pentru **Control acces**, selectați o opțiune. Un certificat folosit este comun cu o politică implicită.
	Tip ID	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, selectați tipul ID-ului pentru scaner.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@", „#" și „=" pentru primul caracter. **Nume distinct**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=". **Adresă IP**: Introduceți formatul IPv4 sau IPv6. **FQDN**: introduceți o combinație cuprinsă între 1 și 255 de caractere folosind A – Z, a – z, 0 – 9, „-" și punct (.). **Adresă de e-mail**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@". **ID cheie**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E).
	Cheie pre-partajată	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirmare Cheie pre-partajată	Pentru confirmare, introduceți cheia configurată.
La distanță	Metodă de autentificare	Dacă selectați **IPsec** pentru **Control acces**, selectați o opțiune. Un certificat folosit este comun cu o politică implicită.
	Tip ID	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, selectați tipul de ID pentru dispozitivul pe care doriți să-l autentificați.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@", „#" și „=" pentru primul caracter. **Nume distinct**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=". **Adresă IP**: Introduceți formatul IPv4 sau IPv6. **FQDN**: introduceți o combinație cuprinsă între 1 și 255 de caractere folosind A – Z, a – z, 0 – 9, „-" și punct (.). **Adresă de e-mail**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@". **ID cheie**: Introduceți 1 – 255 caractere ASCII de 1 octet (0x20 – 0x7E).
	Cheie pre-partajată	Dacă selectați **Cheie pre-partajată** pentru **Metodă de autentificare**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirmare Cheie pre-partajată	Pentru confirmare, introduceți cheia configurată.

Încapsulare

Dacă selectați **IPsec** pentru **Control acces**, trebuie să configurați un mod capsulare.

Elemente	Setări și explicație
Mod transport	Dacă utilizați scanerul numai pe același LAN, selectați această opțiune. Pachetele IP de strat 4 sau ulterior sunt criptate.
Mod tunel	Dacă folosiți scanerul într-o rețea cu conexiune la internet, precum IPsec-VPN, selectați această opțiune. Antetul și datele pachetelor IP sunt criptate. **Poartă gateway la distanță (Mod tunel)**: dacă selectați **Mod tunel** pentru **Încapsulare**, introduceți o adresă de gateway folosind între 1 și 39 de caractere.

Protocol de securitate

Dacă selectați **IPsec** pentru **Control acces**, selectați o opțiune.

Elemente	Setări și explicație
ESP	Selectați această opțiune pentru a garanta integritatea unei autentificări și a datelor și pentru a cripta datele.
AH	Selectați această opțiune pentru a garanta integritatea unei autentificări și a datelor. Chiar dacă este interzisă criptarea datelor, puteți folosi IPsec.

Setări algoritm

Se recomandă să selectați **Oricare** pentru toate setările sau să selectați un alt element decât **Oricare** pentru fiecare setare. Dacă selectați **Oricare** pentru unele setări și selectați un alt element decât **Oricare** pentru celelalte setări, este posibil ca dispozitivul să nu comunice, în funcție de celălalt dispozitiv pe care doriți să-l autentificați.

Elemente		Setări și explicație
IKE	Criptare	Selectați algoritmul de criptare pentru IKE. Elementele variază în funcție de versiunea IKE.
	Autentificare	Selectați algoritmul de autentificare pentru IKE.
	Schimb de chei	Selectați algoritmul de schimb cheie pentru IKE. Elementele variază în funcție de versiunea IKE.
ESP	Criptare	Selectați algoritmul de criptare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Protocol de securitate**.
	Autentificare	Selectați algoritmul de autentificare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Protocol de securitate**.
AH	Autentificare	Selectați algoritmul de criptare pentru AH. Aceasta este disponibilă atunci când **AH** este selectat pentru **Protocol de securitate**.

Combinație dintre Adresă locală (scaner) și Adresă la distanță (Gazdă) pe Politică grup

		Setarea Adresă locală (scaner)		
		IPv4	IPv6*2	Orice adrese*3
Setarea Adresă la distanță (Gazdă)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Gol	✓	✓	✓

*1 Dacă **IPsec** este selectat pentru **Control acces**, nu puteți specifica o lungime de prefix.

*2 Dacă **IPsec** este selectat pentru **Control acces**, puteți selecta o adresă de legătură locală (fe80::), dar politica de grup va fi dezactivată.

*3 Cu excepția adreselor de legătură locală IPv6.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Referințe privind numele de serviciu în politica de grup

Notă:
Sunt afișate servicii indisponibile, care nu pot fi selectate.

Nume serviciu	Tip protocol	Număr port local	Număr port de la distanță	Funcții controlate
Oricare	–	–	–	Toate serviciile
ENPC	UDP	3289	Orice port	Căutarea unui scaner din aplicații precum Epson Device Admin și un driver de scaner
SNMP	UDP	161	Orice port	Achiziția și configurarea MIB din aplicații precum Epson Device Admin și driverul de scaner Epson
WSD	TCP	Orice port	5357	Controlarea WSD
WS-Discovery	UDP	3702	Orice port	Căutare scanere WSD
Network Scan	TCP	1865	Orice port	Redirecționarea datelor scanate de la Document Capture Pro
Network Push Scan	TCP	Orice port	2968	Achiziție a informațiilor despre lucrare în cazul unei scanări push din Document Capture Pro
Network Push Scan Discovery	UDP	2968	Orice port	Căutarea unui computer de la scaner

Nume serviciu	Tip protocol	Număr port local	Număr port de la distanță	Funcții controlate
Date FTP (La distanță)	TCP	Orice port	20	Client FTP (redirecționare date scanate) Totuși, acesta poate controla doar un server FTP care utilizează numărul de port la distanță 20.
Control FTP (La distanță)	TCP	Orice port	21	Client FTP (controlare pentru redirecționare date scanate)
CIFS (La distanță)	TCP	Orice port	445	Client CIFS (redirecționare date scanate către un folder)
NetBIOS Name Service (La distanță)	UDP	Orice port	137	Client CIFS (redirecționare date scanate către un folder)
NetBIOS Datagram Service (La distanță)	UDP	Orice port	138	
NetBIOS Session Service (La distanță)	TCP	Orice port	139	
HTTP (Local)	TCP	80	Orice port	Server HTTP(S) (redirecționarea datelor Web Config și WSD)
HTTPS (Local)	TCP	443	Orice port	
HTTP (La distanță)	TCP	Orice port	80	Client HTTP(S) (actualizarea firmware-ului și a certificatului rădăcină)
HTTPS (La distanță)	TCP	Orice port	443	

Exemple de configurare IPsec/IP Filtering

Primirea numai de pachete IPsec

Acest exemplu este numai pentru configurarea unei politici implicite.

Politică implicită:

❏ **IPsec/IP Filtering**: **Activare**

❏ **Control acces**: **IPsec**

❏ **Metodă de autentificare**: **Cheie pre-partajată**

❏ **Cheie pre-partajată**: Introduceți maximum 127 de caractere.

Politică grup: nu configurați.

Recepționarea datelor de scanare şi a setărilor scanerului

Acest exemplu permite comunicări ale datelor de scanare și configurației scanerului de la servicii specificate.

Politică implicită:

❏ **IPsec/IP Filtering**: **Activare**

❏ **Control acces**: **Refuzare acces**

Politică grup:

❏ **Se activează această Politică grup**: Bifați caseta.

❏ **Control acces**: **Permitere acces**

❏ **Adresă la distanță (Gazdă)**: Adresă IP a unui client

❏ **Metodă de selectare port**: **Nume serviciu**

❏ **Nume serviciu**: Bifați caseta **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)** și **Network Scan**.

Acceptarea accesului numai de la o adresă IP specificată

În acest exemplu, o adresă IP specifică este autorizată să acceseze scanerul.

Politică implicită:

❏ **IPsec/IP Filtering**: **Activare**

❏ **Control acces**:**Refuzare acces**

Politică grup:

❏ **Se activează această Politică grup**: Bifați caseta.

❏ **Control acces**: **Permitere acces**

❏ **Adresă la distanță (Gazdă)**: Adresă IP a unui client al administratorului

Notă:
Indiferent de configurarea politicii, clientul va putea accesa și configura scanerul.

Configurarea unui certificat pentru filtrarea IPsec/IP

Configurați certificatul de client pentru filtrarea IPsec/IP. La setare, puteți utiliza certificatul ca metodă de autentificare pentru filtrare IPsec/IP. Dacă doriți să configurați autoritatea de certificare, accesați **Certificat CA**.

1. Accesați Web Config apoi selectați fila **Securitate rețea** > **IPsec/IP Filtering** > **Certificat client**.

2. Importați certificatul în **Certificat client**.

   Dacă ați importat deja un certificat publicat de o autoritate de certificare, puteți copia certificatul și îl puteți utiliza pentru filtrarea IPsec/IP. Pentru copiere, selectați certificatul din **Copiere de la** și apoi faceți clic pe **Copiere**.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

➡ „Configurarea unui Certificat semnat de CA” la pagina 93

➡ „Configurarea unui Certificat CA” la pagina 97

Conectarea scanerului la o rețea IEEE802.1X

Configurarea unei rețele IEEE 802.1X

Când setați IEEE 802.1X la scaner, îl puteți utiliza într-o rețea conectându-l la un server RADIUS, la un switch LAN cu funcție de autentificare sau la un punct de acces.

1. Accesați Web Config și apoi selectați fila **Securitate rețea** > **IEEE802.1X** > **De bază**.
2. Introduceți o valoare pentru fiecare element.

   Dacă doriți să utilizați scanerul într-o rețea Wi-Fi, faceți clic pe **Setare Wi-Fi** și selectați sau introduceți un SSID.

   Notă:
   Puteți partaja setările între Ethernet și Wi-Fi.
3. Faceți clic pe **Înainte**.

   Un mesaj de confirmare este afișat.
4. Faceți clic pe **OK**.

   Scanerul este actualizat.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Elemente de setare rețea IEEE 802.1X

Elemente	Setări și explicație	
IEEE802.1X (LAN cu fir)	Puteți activa sau dezactiva setările paginii (**IEEE802.1X** > **De bază**) pentru IEEE802.1X (LAN prin cablu).	
IEEE802.1X (Wi-Fi)	Este afișată starea IEEE802.1X (Wi-Fi) pentru conexiune.	
Metodă de conectare	Este afișată metoda de conectare a unei rețele curente.	
Tip EAP	Selectați o opțiune pentru o metodă de autentificare între scaner și un server RADIUS.	
	EAP-TLS	Trebuie să obțineți și să importați un certificat semnat CA.
	PEAP-TLS	
	PEAP/MSCHAPv2	Trebuie să configurați o parolă.
	EAP-TTLS	
ID utilizator	Configurați un ID pentru a-l utiliza pentru autentificarea unui server RADIUS. Introduceți între 1 și 128 de caractere ASCII de câte 1 octet (între 0x20 și 0x7E).	
Parolă	Configurați o parolă pentru a autentifica scanerul. Introduceți între 1 și 128 de caractere ASCII de câte 1 octet (între 0x20 și 0x7E). Dacă utilizați un server Windows drept server RADIUS, veți putea introduce până la 127 de caractere.	

Elemente	Setări și explicație	
Confirmare parolă	Pentru confirmare, introduceți parola configurată.	
ID server	Puteți configura un ID de server pentru a vă autentifica pe un server RADIUS specificat. Autentificatorul verifică dacă un ID de server este inclus în câmpul subject/subjectAltName al unui certificat de server care este trimis sau nu de pe un server RADIUS. Introduceți între 0 și 128 de caractere ASCII de câte 1 octet (între 0x20 și 0x7E).	
Validare certificat (LAN prin fir)	Dacă doriți să efectuați **Validare certificat** utilizând **IEEE802.1X (LAN cu fir)**, selectați **Activare**. Dacă selectați Enable (Activare), consultați informațiile aferente și importați **Certificat CA**. Rețineți faptul că Validare certificat este activat întotdeauna în IEEE802.1X (Wi-Fi). Asigurați-vă că importați Certificat CA.	
Nume anonim	Dacă selectați **PEAP-TLS** sau **PEAP/MSCHAPv2** pentru **Tip EAP**, puteți configura un nume anonim în locul unui ID de utilizator pentru etapa 1 a autentificării PEAP. Introduceți între 0 și 128 de caractere ASCII de câte 1 octet (între 0x20 și 0x7E).	
Forță criptare	Puteți selecta una dintre următoarele opțiuni.	
	Tare	AES256/3DES
	Mediu	AES256/3DES/AES128/RC4

Informații conexe

➡ „Configurarea unui Certificat CA” la pagina 97

Configurarea unui certificat pentru IEEE 802.1X

Configurarea unui certificat de client pentru IEEE802.1X. La setare, puteți utiliza **EAP-TLS** și **PEAP-TLS** ca metodă de autentificare pentru IEEE 802.1X. Dacă doriți să configurați certificatul oferit de autoritatea de certificare, accesați **Certificat CA**.

1. Accesați Web Config apoi selectați fila **Securitate rețea** > **IEEE802.1X** > **Certificat client**.
2. Introduceți un certificat în **Certificat client**.

   Dacă ați importat deja un certificat publicat de o autoritate de certificare, puteți copia certificatul și îl puteți utiliza în IEEE802.1X. Pentru copiere, selectați certificatul din **Copiere de la** și apoi faceți clic pe **Copiere**.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Rezolvarea problemelor pentru securitate avansată

Restabilirea funcțiilor de securitate

Când stabiliți un mediu extrem de securizat, precum filtrarea IPsec/IP sau este posibil să nu puteți efectua comunicația cu unele dispozitive din cauza setărilor incorecte sau problemelor cu dispozitivul sau serverul. În

acest caz, restabiliți setările de securitate pentru a efectua setările pentru dispozitiv din nou sau pentru a permite utilizarea temporară.

Dezactivarea funcției de securitate utilizând Web Config

Puteți dezactiva IPsec/IP Filtering folosind Web Config.

1. Accesați Web Config și selectați fila **Securitate rețea** > **IPsec/IP Filtering** > **De bază**.
2. Dezactivați **IPsec/IP Filtering**.

Probleme privind utilizarea caracteristicilor de securitate a rețelei

Uitarea unei chei pre-partajate

Reconfigurați o cheie prepartajată.

Pentru a schimba cheia, accesați Web Config și selectați fila **Securitate rețea** > **IPsec/IP Filtering** > **De bază** > **Politică implicită** sau **Politică grup**.

Când schimbați cheia pre-partajată, configurați cheia pre-partajată pentru computere.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38
➡ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 99

Comunicare imposibilă cu Comunicare IPsec

Specificați algoritmul incompatibil cu scanerul sau cu computerul.

Scanerul este compatibil cu următorii algoritmi. Verificați setările computerului.

Metode de securitate	Algoritmi
Algoritm de criptare IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Algoritm de autentificare IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritm de schimbare cheie 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*
Algoritm de criptare ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Algoritm de autentificare ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritm de autentificare AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* disponibil doar pentru IKEv2

Informații conexe

➡ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 99

Întrerupere bruscă a comunicării

Adresa IP a scanerului s-a modificat sau nu poate fi utilizată.

Când adresa IP înregistrată la adresa locală din Politică grup a fost modificată sau nu poate fi utilizată, nu se pot efectua comunicațiile IPsec. Dezactivați IPsec folosind panoul de comandă al scanerului.

Dacă DHCP nu mai este valid, ați efectuat repornirea sau adresa IPv6 nu mai este validă sau nu a fost obținută, adresa IP înregistrată pentru fila Web Config (**Securitate rețea** > **IPsec/IP Filtering** > **De bază** > **Politică grup** > **Adresă locală (scaner)**) a scanerului nu va fi găsită.

Folosiți o adresă IP statică.

Adresa IP a computerului s-a modificat sau nu poate fi utilizată.

Când adresa IP înregistrată la adresa la distanță din Politică grup a fost modificată sau nu poate fi utilizată, nu se pot efectua comunicațiile IPsec.

Dezactivați IPsec folosind panoul de comandă al scanerului.

Dacă DHCP nu mai este valid, ați efectuat repornirea sau adresa IPv6 nu mai este validă sau nu a fost obținută, adresa IP înregistrată pentru fila Web Config (**Securitate rețea** > **IPsec/IP Filtering** > **De bază** > **Politică grup** > **Adresă la distanță (Gazdă)**) a scanerului nu va fi găsită.

Folosiți o adresă IP statică.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

➡ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 99

Nu se poate realiza conectarea după configurarea filtrării IPsec/IP

Setările IPsec/IP Filtering sunt incorecte.

Dezactivați filtrarea IPsec/IP din panoul de control al scanerului. Conectați scanerul și computerul și refaceți setarea privind filtrarea IPsec/IP.

Informații conexe

➡ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 99

Imposibil de accesat dispozitivul după configurarea IEEE 802.1X

Setările IEEE 802.1X sunt incorecte.

Dezactivați IEEE 802.1X și Wi-Fi de la panoul de comandă al scanerului. Conectați scanerul și un computer, apoi configurați din nou IEEE 802.1X.

Informații conexe

➡ „Configurarea unei rețele IEEE 802.1X” la pagina 111

Probleme privind utilizarea unui certificat digital

Nu se poate importa un Certificat semnat de CA

Certificat semnat de CA şi informațiile din CSR nu corespund.

Dacă informațiile din Certificat semnat de CA și CSR nu corespund, CSR nu se poate importa. Verificați următoarele:

❏ Încercați să importați certificatul spre un dispozitiv care nu are aceleași informații?

Verificați informațiile CSR și apoi importați certificatul spre un dispozitiv care are aceleași informații.

❏ Ați suprascris CSR salvată în scaner după trimiterea CSR către o autoritate de certificare?

Obțineți din nou certificatul CA-semnat cu CSR.

Certificat semnat de CA depăşeşte 5 KB.

Nu puteți importa un Certificat semnat de CA care depășește 5 KB.

Parola pentru importul certificatului este incorectă.

Introduceți parola corectă. Dacă ați uitat parola, nu puteți importa certificatul. Obțineți din nou Certificat semnat de CA.

Informații conexe

➡ „Import al unui certificat CA-semnat” la pagina 95

Actualizare imposibilă a unui certificat autosemnat

Nume comun nu a fost introdus.

Nume comun trebuie introdus.

S-au introdus caractere neacceptate în Nume comun.

Introduceți între 1 și 128 de caractere în format IPv4, IPv6, denumire gazdă sau FQDN în ASCII (0x20–0x7E).

Numele comun include un spațiu sau o virgulă.

Dacă este inclusă o virgulă, **Nume comun** este divizat în acest punct. Dacă numai un spațiu este introdus înainte sau după o virgulă, survine o eroare.

Informații conexe

➡ „Actualizarea unui certificat autosemnat” la pagina 97

Nu poate fi creată o CSR

Nume comun nu a fost introdus.

Trebuie introdus **Nume comun**.

S-au introdus caractere neacceptate în Nume comun, Organizație, Unitate organizatorică, Localitate şi Stat/Provincie.

Introduceți caractere în format IPv4, IPv6, denumire gazdă sau FQDN în ASCII (0x20–0x7E).

Nume comun include un spațiu sau o virgulă.

Dacă este inclusă o virgulă, **Nume comun** este divizat în acest punct. Dacă numai un spațiu este introdus înainte sau după o virgulă, survine o eroare.

Informații conexe

➡ „Obținerea unui certificat CA-semnat” la pagina 93

Apare o avertizare privind un certificat digital

Mesaje	Cauză/Cum să procedați
Introduceți un Certificat de server.	**Cauză:** Nu ați selectat un fişier pentru a fi importat. **Cum să procedați:** Selectați un fişier şi faceți clic pe **Import**.
Certificatul CA 1 nu a fost introdus.	**Cauză:** Certificatul CA 1 nu este introdus şi este introdus numai certificatul CA 2. **Cum să procedați:** Importați mai întâi certificatul CA 1.
Valoare invalidă mai jos.	**Cauză:** Caractere incompatibile sunt incluse în calea fişierului şi/sau parolă. **Cum să procedați:** Asigurați-vă că respectivele caractere sunt introduse corect pentru element.
Data şi ora sunt nevalide.	**Cauză:** Data şi ora scanerului nu au fost setate. **Cum să procedați:** Setați data şi ora folosind Web Config sau EpsonNet Config.
Parolă nevalidă.	**Cauză:** Parola setată pentru certificatul CA şi parola introdusă nu corespund. **Cum să procedați:** Introduceți parola corectă.

Mesaje	Cauză/Cum să procedați
Fişier nevalid.	**Cauză:** Se pare că nu importați un fişier de certificat în format X509. **Cum să procedați:** Asigurați-vă că selectați certificatul corect trimis de o autoritate de certificare de încredere.
	Cauză: Dimensiunea fişierului pe care l-ați importat este prea mare. Dimensiunea maximă permisă pentru fişier este de 5 KB. **Cum să procedați:** Dacă selectați fişierul corect, certificatul ar putea fi deteriorat sau falsificat.
	Cauză: Lanțul inclus în certificat este invalid. **Cum să procedați:** Pentru mai multe informații privind certificatul, consultați site-ul autorității de certificare.
Nu se pot utiliza Certificate de server care includ mai mult de trei certificate CA.	**Cauză:** Fişierul certificatului în format PKCS#12 include mai mult de 3 certificate CA. **Cum să procedați:** Importați fiecare certificat transformat din format PKCS#12 în format PEM sau importați fişierul certificatului în format PKCS#12 care include maximum 2 certificate CA.
Certificatul a expirat. Verificați dacă certificatul este valid sau verificați data şi ora de pe produs.	**Cauză:** Certificatul nu este actualizat. **Cum să procedați:** ❏ Dacă certificatul nu este actualizat, obțineți şi importați noul certificat. ❏ Dacă certificatul este actualizat, asigurați-vă că data şi ora scanerului sunt setate corect.
Cheia privată este obligatorie.	**Cauză:** Nicio cheie privată nu se potrivește cu certificatul. **Cum să procedați:** ❏ Dacă certificatul este în format PEM/DER şi este obținut de la o CSR folosind un computer, indicați fişierul pentru cheia privată. ❏ Dacă certificatul este în format PKCS#12 şi este obținut de la o CSR folosind un computer, creați un fişier care include cheia privată.
	Cauză: Ați importat din nou certificatul PEM/DER obținut de la o CSR folosind Web Config. **Cum să procedați:** Dacă certificatul este în format PEM/DER şi este obținut de la o CSR folosind Web Config, îl puteți importa o singură dată.

Mesaje	Cauză/Cum să procedați
Configurare eşuată.	**Cauză:** Configurarea nu poate fi finalizată pentru că comunicarea între scaner şi computer a eşuat sau fişierul nu poate fi citit din cauza unor erori. **Cum să procedați:** După ce verificați fişierul şi comunicația indicate, importați din nou fişierul.

Informații conexe

➡ „Despre certificarea digitală” la pagina 93

Ştergerea din greşeală a unui certificat CA-semnat

Nu există fişier de rezervă pentru certificatul semnat CA.

Dacă aveți fişierul copie de rezervă, importați din nou certificatul.

Dacă obțineți un certificat folosind o CSR creată din Web Config, nu mai puteți importa din nou un certificat şters. Creați o CSR şi obțineți un certificat nou.

Informații conexe

➡ „Import al unui certificat CA-semnat” la pagina 95
➡ „Ştergerea unui certificat CA-semnat” la pagina 96

Utilizarea caracteristicii Epson Open Platform

Prezentare generală Epson Open Platform

Epson Open Platform este o platformă care vă permite să utilizați sisteme de autentificare cu acest scaner.

Se poate utiliza cu Epson Print Admin (Sistem de autentificare Epson) sau un sistem de autentificare terț. Puteți obține jurnale care conțin dispozitivul și utilizatorul, puteți configura dispozitivele pe care le pot utiliza utilizatorii și grupurile, seta limite pentru funcții și așa mai departe.

În cazul în care conectați un dispozitiv de autentificare, puteți efectua, de asemenea, autentificarea utilizatorului utilizând cardul ID.

Configurarea Epson Open Platform

Activați Epson Open Platform pentru a putea folosi dispozitivul din sistemul de autentificare.

1. Obțineți o cheie de produs de pe site-ul web dedicat.

   Consultați manualul Epson Open Platform pentru mai multe detalii precum modul de obținere al cheii de produs.

2. Accesați Web Config, apoi selectați fila **Epson Open Platform** > **Cheia produsului sau Cheie de licență**.

3. Verificați și configurați fiecare element.

   ❏ Număr de serie

   Va fi afișat numărul de serie al dispozitivului.

   ❏ Versiune Epson Open Platform

   Selectați versiunea de Epson Open Platform. Versiunea corespunzătoare variază în funcție de sistemul de autentificare.

   ❏ Cheia produsului sau Cheie de licență

   Introduceți cheia de produs pe care ați obținut-o.

4. Faceți clic pe **Înainte**.

   Se afișează ecranul de confirmare a setării.

5. Faceți clic pe **OK**.

   Setările sunt aplicate la nivelul scanerului.

   Notă:
   Nu puteți utiliza Epson Print Admin Serverless când sistemul este sincronizat cu Epson Open Platform.

Validarea Epson Open Platform

Puteți verifica valabilitatea Epson Open Platform utilizând oricare dintre următoarele metode.

❏ Web Config

O cheie de produs a fost introdusă în fila **Epson Open Platform** > **Cheia produsului sau Cheie de licență** > **Cheia produsului sau Cheie de licență**, iar fila **Epson Open Platform** > **Sistem de autentificare** este afișată în partea stângă a structurii arborescente de meniu.

❏ Panoul de comandă al scanerului

Verificați dacă este afișată cheia de produs în **Setări** > **Informații dispozitiv** > **Informații Epson Open Platform**.

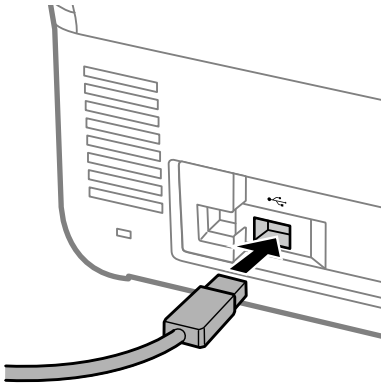
Montarea unui dispozitiv de autentificare

Conectarea dispozitivului de autentificare

Notă:
Un dispozitiv de autentificare este utilizat când se utilizează un sistem de autentificare.

> ***Important:***
> *Când conectați dispozitivul de autentificare la mai multe scanere, utilizați un produs cu același număr de model.*

Conectați cablul USB al cititorului de carduri la portul USB al interfeței externe de pe scaner.



Verificarea funcționării dispozitivului de autentificare

Puteți verifica starea conexiunii și recunoașterea cardului de autentificare pentru dispozitivul de autentificare din panoul de control al scanerului.

Informațiile sunt afișate dacă selectați **Setări** > **Informații dispozitiv** > **Stare dispozitiv de autentificare**.

Confirmarea recunoașterii cardului de autentificare

Puteți verifica dacă pot fi recunoscute cardurile de autentificare folosind Web Config.

1. Accesați Web Config, apoi selectați fila **Gestionare dispozitiv** > **Cititor de carduri**.
2. Țineți cardul de autentificare peste cititorul de carduri de autentificare.
3. Faceți clic pe **Verificare**.
   Se afișează rezultatul.

Soluționarea problemelor dispozitivului de autentificare

Nu se poate citi cardul de autentificare

Verificați următoarele aspecte.

❏ Verificați dacă dispozitivul de autentificare este conectat corect la scaner.
Conectați dispozitivul de autentificare la portul USB al interfeței externe de pe partea din spate a scanerului.

❏ Verificați dacă dispozitivul de autentificare și cardul de autentificare sunt certificate.
Contactați distribuitorul pentru informații privind dispozitivele și cardurile de autentificare acceptate.

Întreținere

Curățarea exteriorului scanerului

Ștergeți orice pete de pe carcasa exterioară cu o lavetă uscată sau cu o lavetă umezită cu detergent slab și apă.

Important:

- ❏ *Nu utilizați niciodată alcool, diluanți sau solvenți corozivi pentru a curăța scanerul. Se pot produce deformarea sau decolorarea.*
- ❏ *Nu permiteți pătrunderea apei în interiorul produsului. Aceasta poate cauza producerea unei defecțiuni.*
- ❏ *Nu deschideți niciodată carcasa scanerului.*

1. Apăsați butonul ⏻ pentru a opri scanerul.
2. Deconectați adaptorul de alimentare cu curent alternativ de la scaner.
3. Curățați carcasa exterioară cu o lavetă umezită cu detergent slab și apă.

   Notă:
   Ștergeți ecranul tactil utilizând o lavetă moale și uscată.

Curățarea în interiorul scanerului

După utilizarea pentru un timp a scanerului, praful de hârtie și din cameră depus pe rolă sau pe piesa de sticlă din interiorul scanerului poate crea probleme de alimentare a hârtiei sau probleme de calitate a imaginii scanate. Curățați interiorul scanerului la fiecare 5,000 de scanări.

Puteți verifica numărul cel mai recent de scanări pe panoul de comandă sau în Epson Scan 2 Utility.

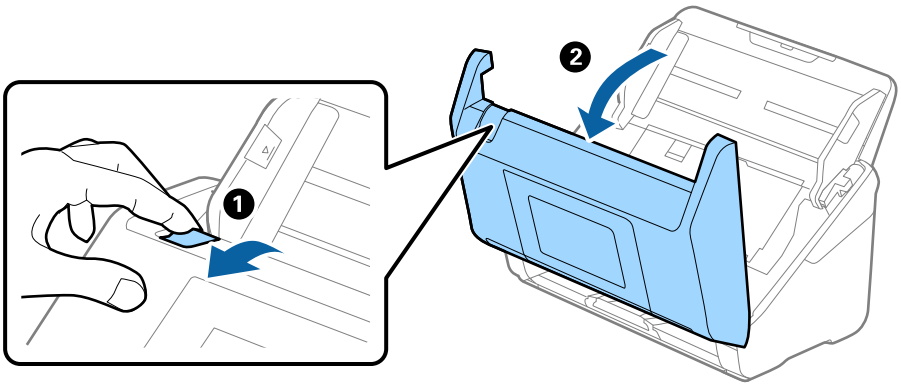
Dacă suprafața este pătată cu un material dificil de eliminat, utilizați un set de curățare Epson original pentru eliminarea petelor. Utilizați o cantitate redusă de soluție de curățare pe laveta de curățare pentru a elimina petele.

Important:

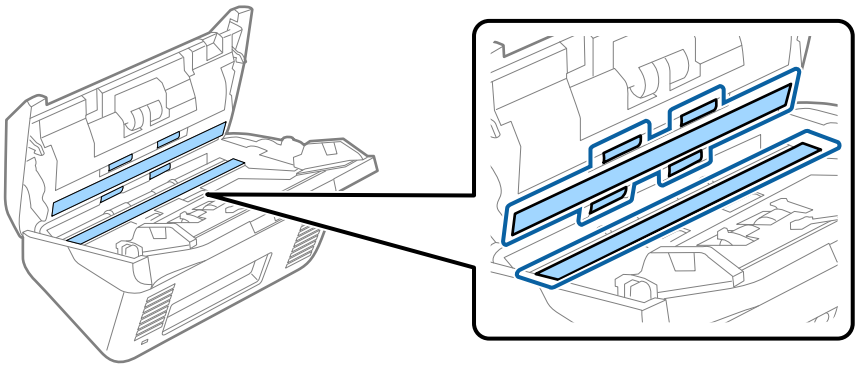
- ❏ *Nu utilizați niciodată alcool, diluanți sau solvenți corozivi pentru a curăța scanerul. Se pot produce deformarea sau decolorarea.*
- ❏ *Nu pulverizați niciodată lichid sau lubrifiant pe scaner. Deteriorarea echipamentului sau a circuitelor poate duce la operații anormale.*
- ❏ *Nu deschideți niciodată carcasa scanerului.*

1. Apăsați butonul ⏻ pentru a opri scanerul.
2. Deconectați adaptorul de rețea de la scaner.

3. Trageți maneta și deschideți capacul scanerului.



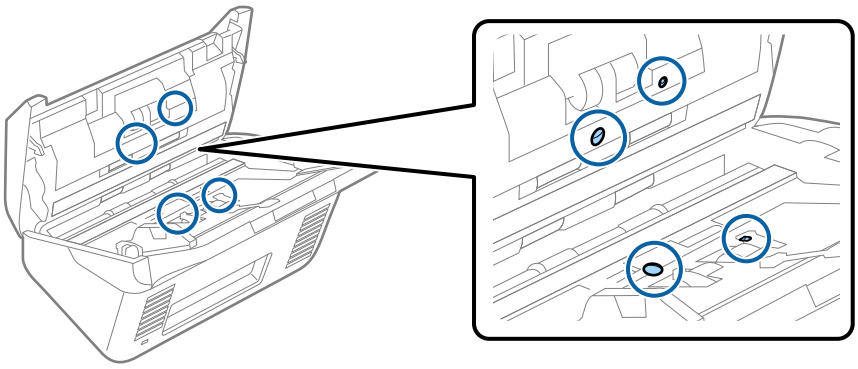
4. Ștergeți toate petele de pe rola de plastic (4 locații) și de pe suprafața de sticlă la baza părții interioare a capacului scanerului. Ștergeți cu o lavetă moale, fără scame, umezită cu o cantitate mică de agent de curățare dedicat sau apă.



Important:

- *Nu apăsați cu o forță prea mare pe suprafața de sticlă.*
- *Nu utilizați o perie sau o unealtă dură. Orice zgârieturi pe sticlă pot afecta calitatea scanării.*
- *Nu pulverizați soluții de curățare direct pe suprafața de sticlă.*

5. Ștergeți toate petele de pe senzori cu un tampon de bumbac.

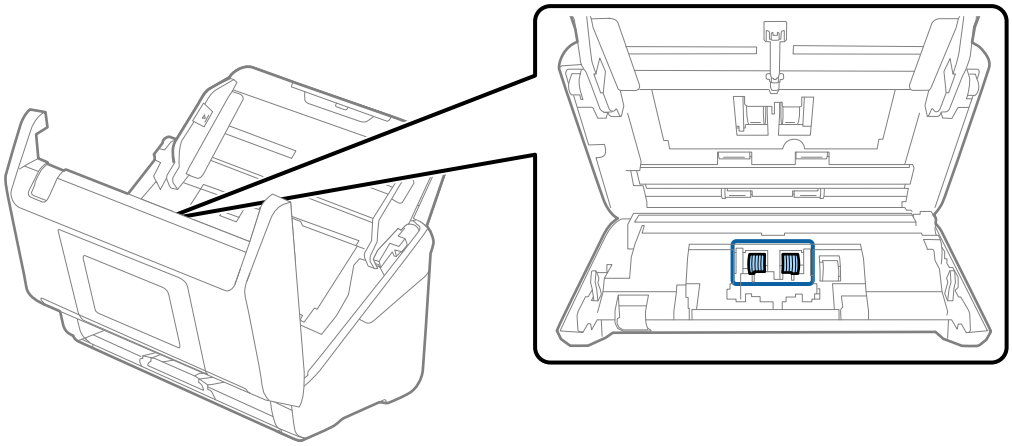


Important:

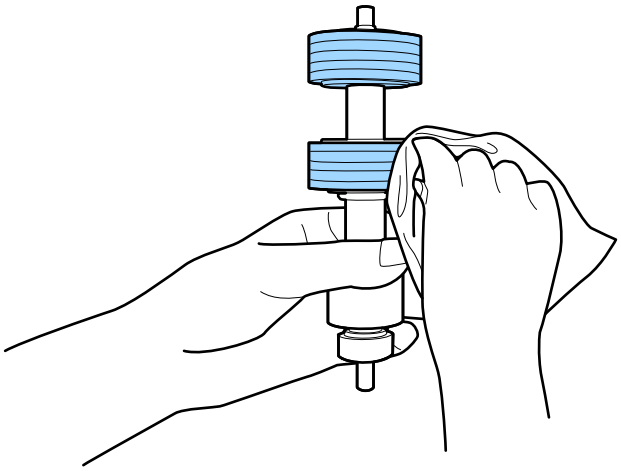
Nu utilizați lichide precum soluții de curățare pe tamponul de bumbac.

6. Deschideți capacul și scoateți rola de separare.

   Consultați „Înlocuirea kitului de ansamblu rolă” pentru mai multe detalii.



7. Ștergeți rola de separare. Ștergeți cu o lavetă moale, fără scame, umezită cu o cantitate mică de agent de curățare dedicat sau apă.

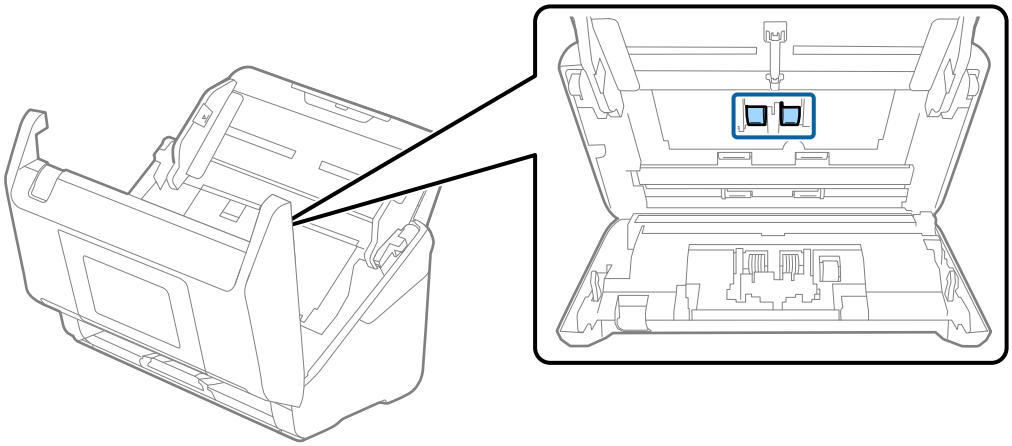


Important:

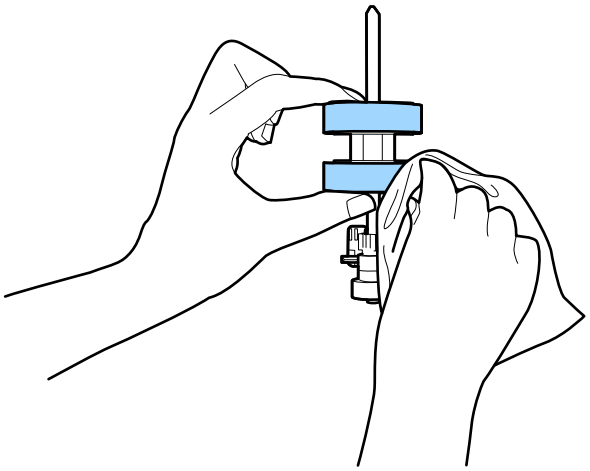
Utilizați numai un set de curățare Epson original sau o lavetă moale, umedă pentru curățarea rolei. Utilizarea unei lavete uscate poate deteriora suprafața rolei.

8. Deschideți capacul și scoateți rola de preluare.

   Consultați „Înlocuirea kitului de ansamblu rolă” pentru mai multe detalii.



9. Ștergeți rola de preluare. Ștergeți cu o lavetă moale, fără scame, umezită cu o cantitate mică de agent de curățare dedicat sau apă.

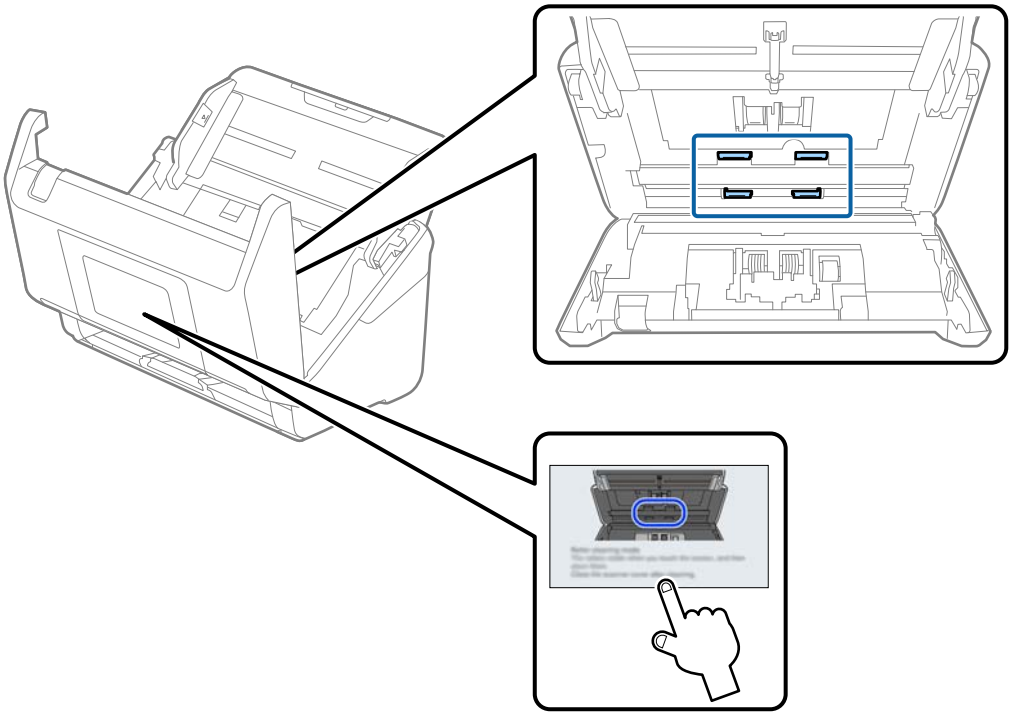


> ***Important:***
>
> *Utilizați numai un set de curățare Epson original sau o lavetă moale, umedă pentru curățarea rolei. Utilizarea unei lavete uscate poate deteriora suprafața rolei.*

10. Închideți capacul scanerului.
11. Conectați adaptorul de alimentare cu curent alternativ la priză și porniți scanerul.
12. Selectați **Întreținere scaner** din ecranul principal.
13. În ecranul **Întreținere scaner**, selectați **Curățare role**.
14. Trageți maneta pentru a deschide capacul scanerului.

    Scanerul intră în modul de curățare a rolei.

15. Rotiți lent rolele de la bază apăsând oriunde pe ecranul LCD. Ștergeți suprafața rolelor utilizând un set de curățare Epson original sau o lavetă moale, umezită cu apă. Repetați operația până când rolele sunt curate.



> ***Atenție:***
> *Aveți grijă să nu vă prindeți mâinile sau părul în mecanism la acționarea rolei. Aceasta poate provoca vătămări corporale.*

16. Închideți capacul scanerului.

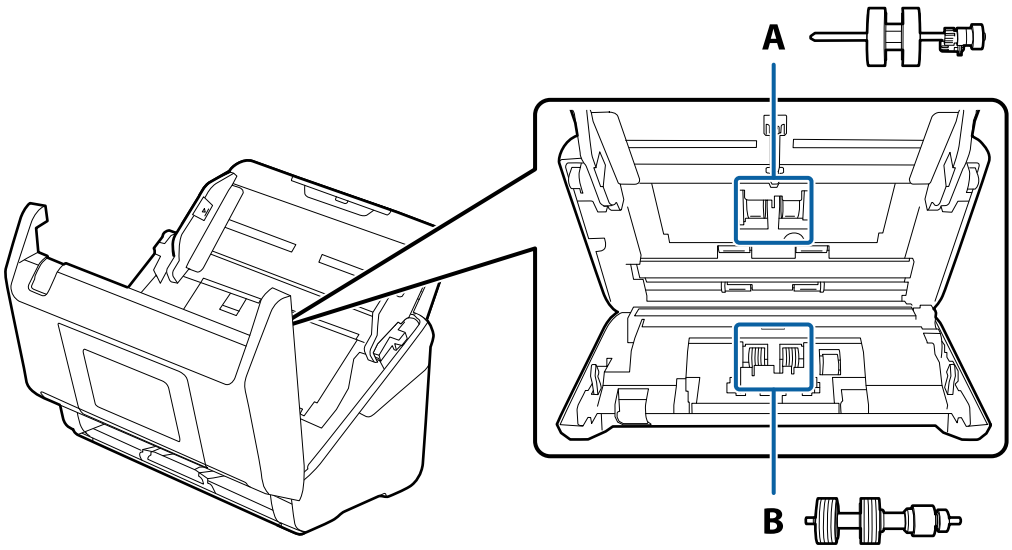
    Scanerul iese din modul de curățare a rolei.

Informații conexe

➡ „Înlocuirea kitului de ansamblu rolă” la pagina 131

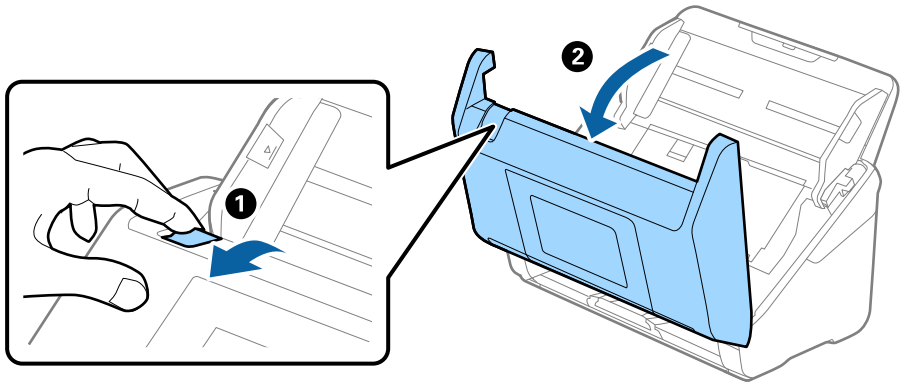
Înlocuirea kitului de ansamblu rolă

Kitul de ansamblu rolă (rola de preluare și rola de separare) trebuie înlocuit atunci când numărul de scanări depășește durata de viață a rolelor. Când pe panoul de comandă sau pe ecranul computerului dumneavoastră este afișat un mesaj de înlocuire, urmați pașii de mai jos pentru înlocuirea kitului.

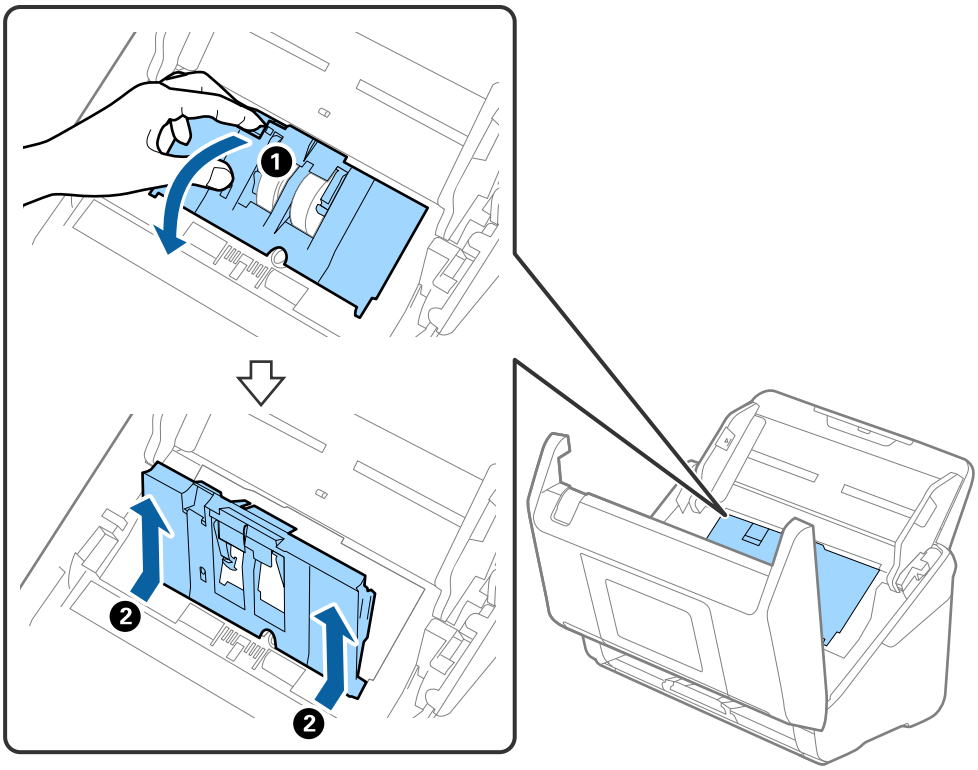


A: rolă de preluare, B: rolă de separare

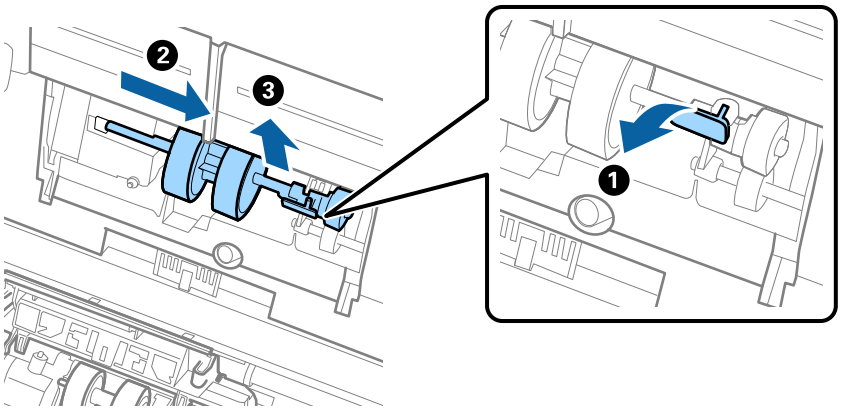
1. Apăsați butonul ⏻ pentru a opri scanerul.
2. Deconectați adaptorul de alimentare cu curent alternativ de la scaner.
3. Trageți maneta și deschideți capacul scanerului.



4. Deschideți capacul rolei de preluare, apoi glisați-o și îndepărtați-o.

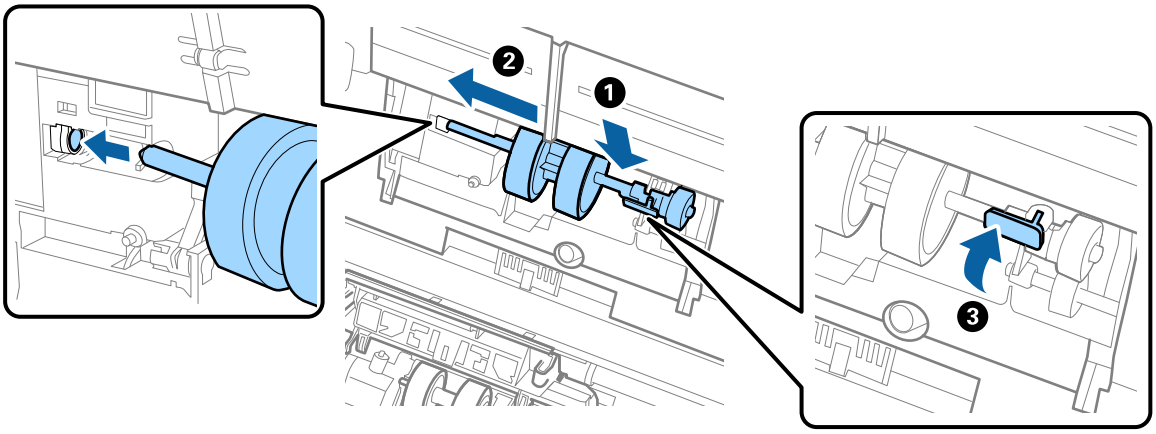


5. Trageți în jos sistemul de prindere al axei rolei, apoi glisați și îndepărtați rolele de preluare instalate.

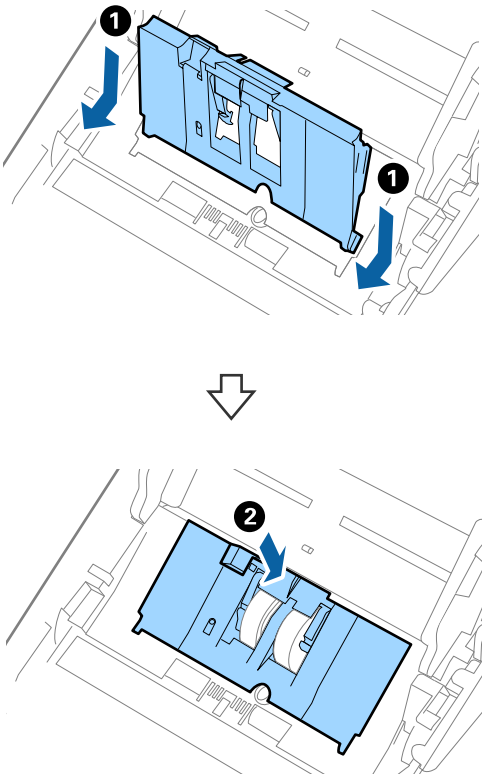


> ***Important:***
>
> *Nu trageți forțat rola de preluare. Aceasta poate deteriora partea interioară a scanerului.*

6. Menținând apăsat sistemul de prindere, glisați noua rolă de preluare înspre stânga și introduceți-o în orificiul din scaner. Apăsați pe sistemul de prindere pentru a-l fixa.

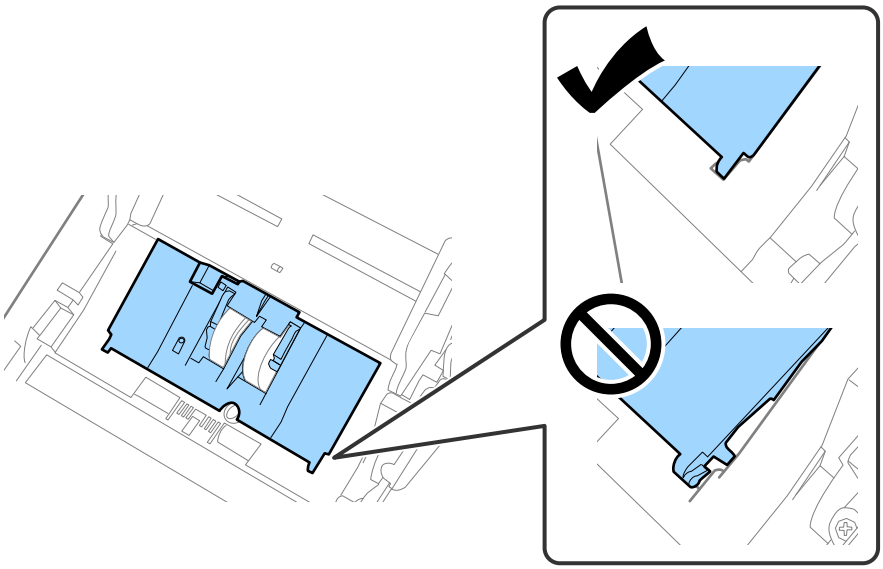


7. Introduceți marginea capacului rolei de preluare în canal și glisați-o. Închideți ferm capacul.

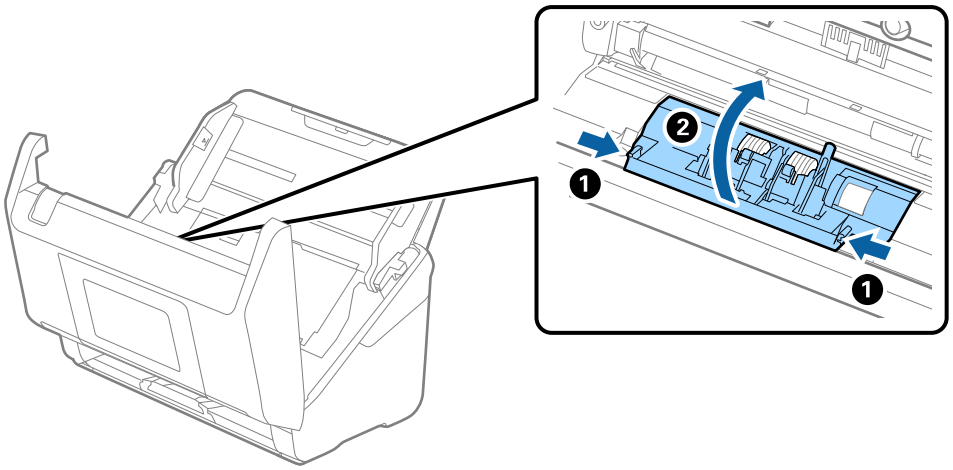


Important:

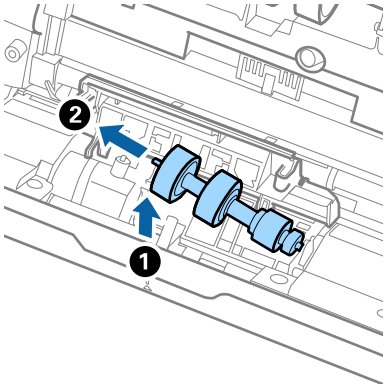
- ❏ *Asigurați-vă că este corect închis capacul rolei de preluare.*
- ❏ *În cazul în care capacul se închide cu dificultate, asigurați-vă că rolele de preluare sunt corect instalate.*
- ❏ *Nu instalați capacul în poziție ridicată.*



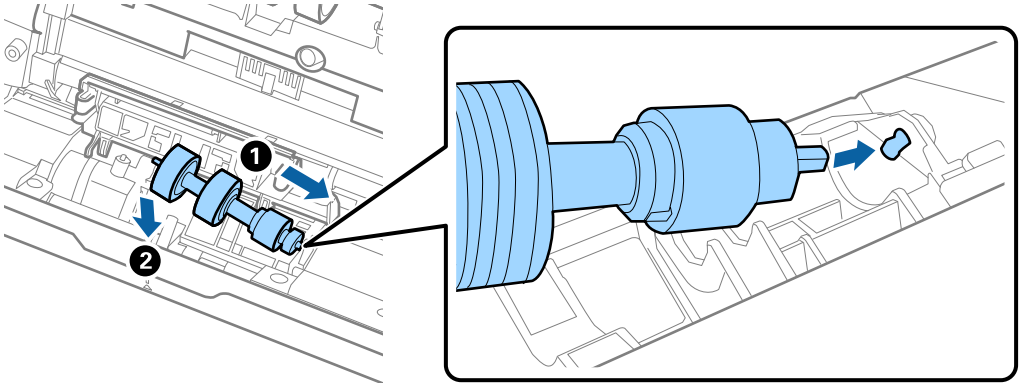
8. Apăsați pe cârligele de la ambele capete ale capacului rolei de separare pentru a deschide capacul.



9. Ridicați partea stângă a rolei de separare și apoi glisați și scoateți rolele de separare instalate.



10. Introduceți axa noii role de separare în orificiul din partea dreaptă și apoi coborâți rola.



11. Închideți capacul rolei de separare.

> ***Important:***
> *În cazul în care capacul este dificil de închis, asigurați-vă că rolele de separare sunt corect instalate.*

12. Închideți capacul scanerului.

13. Conectați adaptorul de alimentare cu curent alternativ și apoi porniți scanerul.

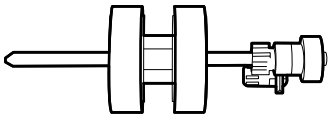
14. Resetați numărul de scanări de la panoul de comandă.

Notă:
Eliminați rola de preluare și rola de separare, respectând normele și regulamentele autorității locale. Nu le dezasamblați.

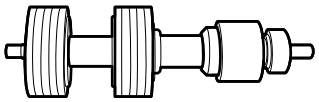
Coduri ale kiturilor de ansamblu rolă

Piesele de schimb (rola de preluare și rola de separare) trebuie înlocuite atunci când numărul de scanări depășește valoarea de service. Puteți verifica numărul cel mai recent de scanări pe panoul de comandă sau în Epson Scan 2 Utility.

A



B



A: rolă de preluare, B: rolă de separare

Nume piesă	Coduri	Ciclu de viață
Kit ansamblu rolă 2	B12B819711 B12B819721 (doar India)	200,000*

* Această valoare a fost obținută prin scanarea consecutivă utilizând hârtie originală de test Epson și reprezintă o valoare orientativă a ciclului de înlocuire. Ciclul de înlocuire poate varia în funcție de diferite tipuri de hârtie, precum hârtia care generează o cantitate mare de praf sau hârtie cu o suprafață dură, care poate reduce ciclul de viață.

Resetarea numărului de scanări după înlocuirea rolelor

Resetați numărul de scanări utilizând panoul de comandă sau Epson Scan 2 Utility după înlocuirea kitului de ansamblu role.

Această secțiune explică cum să resetați folosind panoul de comandă.

1. Atingeți **Întreținere scaner** pe ecranul principal.
2. Atingeți **Înlocuire rolă de întreținere**.
3. Atingeți **Resetați numărul de scanări**.
4. Selectați **Număr de scanări după înlocuirea rolei** și apoi atingeți **Da**.

Notă:
Pentru a reseta din Epson Scan 2 Utility, porniți Epson Scan 2 Utility, faceți clic pe fila ***Contor****, apoi faceți clic pe* ***Reinițializ.*** *în* ***Kit de recunoaştere si preluare corectă a colilor de hârtie****.*

Informații conexe

➡ „Înlocuirea kitului de ansamblu rolă” la pagina 131

Economisirea energiei

Puteți economisi energie utilizând modul Inactiv sau modul Deconectat automat atunci când scanerul nu execută nicio operație. Puteți stabili intervalul de timp după care scanerul intră în modul Inactiv și se deconectează automat de la sursa de alimentare electrică. Orice creștere va afecta eficiența energetică a produsului. Luați în considerare mediul înconjurător înainte de a efectua modificări.

1. Selectați **Setări** de pe ecranul principal.
2. Selectați **Setări de bază**.
3. Selectați **Temporiz. oprire** sau **Setări oprire**, apoi realizați setările.

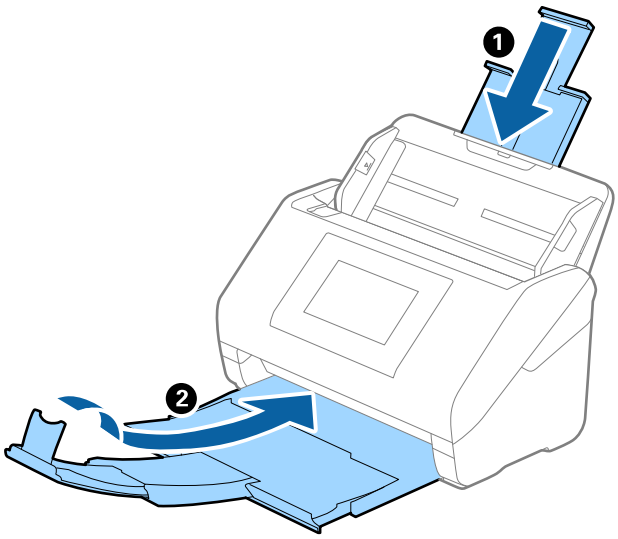
   Notă:
   Caracteristicile disponibile pot varia în funcție de locația de achiziție.

Transportarea scanerului

Când trebuie să transportați scanerul pentru a-l muta sau pentru reparații, urmați pașii de mai jos pentru a-l împacheta.

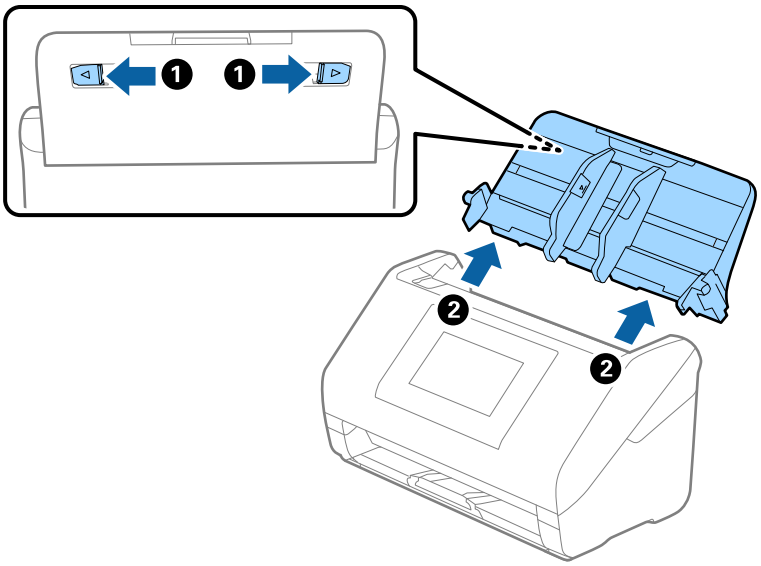
1. Apăsați butonul ⏻ pentru a opri scanerul.
2. Deconectați adaptorul de alimentare cu curent alternativ.
3. Scoateți cablurile și dispozitivele.

   Îndepărtați Paper Alignment Plate opțională sau furnizată dacă este atașată.
4. Închideți extensia tăvii de intrare și tava de ieșire.



Important:
Asigurați-vă că închideți tava de ieșire în siguranță; în caz contrar, se poate deteriora pe durata transportului.

5. Scoateți tava de intrare.



6. Atașați materialele de ambalare furnizate împreună cu scanerul, apoi împachetați din nou scanerul în ambalajul original sau într-un ambalaj rezistent.

Copierea de rezervă a setărilor

Puteți exporta în fișier valoarea setată, definită în Web Config. O puteți utiliza pentru copierea de rezervă a contactelor, a valorilor setate, înlocuirea scanerului etc.

Fișierul exportat nu poate fi editat, deoarece este exportat ca fișier binar.

Exportarea setărilor

Exportați setarea pentru scaner.

1. Accesați Web Config și apoi selectați fila **Gestionare dispozitiv** > **Valoare de setare export și import** > **Export**.

2. Selectați setările pe care doriți să le exportați.

   Selectați setările pe care doriți să le exportați. Dacă selectați categoria părinte, vor fi selectate și subcategoriile. Cu toate acestea, subcategoriile care cauzează erori prin duplicarea acestora în cadrul aceleiași rețele (cum ar fi adresele IP etc.) nu pot fi selectate.

3. Introduceți o parolă pentru a cripta fișierul exportat.

   Aveți nevoie de parolă pentru a importa fișierul. Lăsați acest câmp necompletat dacă nu doriți să criptați fișierul.

4. Faceți clic pe **Export**.

> ***Important:***
> *Dacă doriți să exportați setările de rețea ale scanerului, cum ar fi numele imprimantei și adresa IPv6, selectați **Activați pentru a selecta setările individuale ale dispozitivului** și selectați mai multe articole. Utilizați numai valorile selectate pentru scanerul de înlocuire.*

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Importați setările

Importați fișierul exportat Web Config la nivelul scanerului.

> ***Important:***
> *La importarea valorilor care includ informații individuale, precum numele scanerului sau adresa IP, asigurați-vă că nu este utilizată aceeași adresă IP de mai multe ori în cadrul aceleiași rețele.*

1. Accesați Web Config, și apoi selectați fila **Gestionare dispozitiv** > **Valoare de setare export și import** > **Import**.
2. Selectați fișierul exportat, apoi introduceți parola criptată.
3. Faceți clic pe **Înainte**.
4. Selectați setările pe care doriți să le importați și apoi faceți clic pe **Înainte**.
5. Faceți clic pe **OK**.

Setările sunt aplicate la nivelul scanerului.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Restaurare setări implicite

Pe panoul de comandă, selectați **Setări** > **Administrare sistem** > **Restaurare setări implicite**, apoi selectați elementele pe care doriți să le restabiliți la valorile implicite.

❏ Setări rețea: restabiliți setările de rețea la starea inițială.

❏ Toate exceptând Setări rețea: restabiliți alte setări la starea inițială, cu excepția setărilor de rețea.

❏ Toate setările: restabiliți toate setările la starea inițială de la momentul achiziției.

> ***Important:***
> *Dacă selectați și executați **Toate setările**, toate datele de setări înregistrate pe scaner, inclusiv contactele, vor fi șterse. Setările șterse nu pot fi restabilite.*

Notă:
De asemenea, puteți efectua setări pe Web Config.

*Fila **Gestionare dispozitiv** > **Restaurare setări implicite***

Actualizarea aplicațiilor și a firmware-ului

Puteți elimina anumite probleme și îmbunătăți sau adăuga funcționalități prin actualizarea aplicațiilor și a firmware-ului. Asigurați-vă că utilizați cea mai recentă versiune a aplicațiilor și a firmware-ului.

Important:

❏ *Nu opriți computerul sau scanerul în timpul actualizării.*

Notă:
*Când scanerul se poate conecta la internet, puteți actualiza firmware-ul din Web Config. Selectați fila **Gestionare dispozitiv** > **Actualizare firmware**, verificați mesajul afișat, apoi faceți clic pe **Start**.*

1. Asigurați-vă că scanerul și computerul sunt conectate și computerul este conectat la internet.

2. Porniți EPSON Software Updater și actualizați aplicațiile sau firmware-ul.

   Notă:
   Sistemele de operare Windows Server nu sunt acceptate.

   ❏ Windows 11

   Faceți clic pe butonul start și apoi selectați **Toate aplicațiile** > **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 10

   Faceți clic pe butonul de start, apoi selectați **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Introduceți numele aplicației în câmpul de căutare, apoi selectați pictograma afișată.

   ❏ Windows 7

   Faceți clic pe butonul de start și apoi selectați **Toate programele** sau **Programe** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Selectați **Finder** > **Accesare** > **Aplicații** > **Epson Software** > **EPSON Software Updater**.

Notă:
Dacă nu găsiți aplicația pe care doriți să o actualizați în lista de aplicații, nu o puteți actualiza utilizând EPSON Software Updater. Verificați cele mai recente versiuni ale aplicațiilor pe site-ul local Epson.

http://www.epson.com

Actualizarea firmware-ului scanerului utilizând panoul de comandă

Dacă scanerul poate fi conectată la Internet, puteți actualiza firmware-ul acesteia utilizând panoul de comandă. De asemenea, puteți configura scanerul să verifice cu regularitate actualizările firmware și să vă notifice dacă acestea există.

1. Selectați **Setări** de pe ecranul principal.
2. Selectați **Administrare sistem** > **Actualizare firmware** > **Actualizare**.

   Notă:
   *Selectați **Notificare** > **Act.** pentru a seta scanerul să verifice cu regularitate actualizările firmware disponibile.*
3. Consultați mesajul afișat pe ecran și începeți căutarea actualizărilor disponibile.
4. Dacă pe ecranul LCD este afișat un mesaj care vă informează că este disponibilă o actualizare firmware, urmați instrucțiunile de pe ecran pentru a începe actualizarea.

> ***Important:***
> - *Nu opriți și nu deconectați scanerul de la sursa de alimentare electrică înainte de finalizarea actualizării; în caz contrar, scanerul poate suferi o defecțiune.*
> - *Dacă actualizarea firmware nu este finalizată sau nu a reușit, scanerul nu pornește normal, iar la viitoarea pornire a scanerului se afișează mesajul „Recovery Mode” pe ecranul LCD. În această situație, trebuie să actualizați din nou programul firmware cu ajutorul unui computer. Conectați scanerul la computer cu ajutorul unui cablu USB. Când la imprimantă este afișat mesajul „Recovery Mode” pe scaner, actualizarea firmware prin intermediul unei conexiuni de rețea nu este posibilă. De la computer, accesați site-ul web Epson local și descărcați cea mai recentă versiune a firmware-ului scanerului. Pentru etapele următoare, consultați instrucțiunile de pe site-ul web.*

Actualizare firmware folosind Web Config

Când scanerul se poate conecta la internet, puteți actualiza firmware-ul din Web Config.

1. Accesați Web Config și selectați fila **Gestionare dispozitiv** > **Actualizare firmware**.
2. Faceți clic pe **Start** și apoi urmați instrucțiunile afișate pe ecran.

   Începe confirmarea firmware-ului, iar informațiile privind firmware-ul sunt afișate, în cazul în care există firmware-ul actualizat.

Notă:
Puteți actualiza firmware-ul și folosind Epson Device Admin. Puteți confirma vizual informațiile firmware pe lista cu dispozitive. Este util atunci când doriți să actualizați firmware-ul pentru mai multe dispozitive. Pentru mai multe detalii, consultați ghidul sau secțiunea de ajutor pentru Epson Device Admin.

Informații conexe

➡ „Cum să rulați Web Config într-un browser web” la pagina 38

Actualizarea firmware-ului fără conectarea la Internet

Puteți descărca firmware-ul pentru dispozitiv de pe site-ul web Epson de la computer, iar apoi puteți conecta dispozitivul și computerul cu ajutorul cablului USB pentru a actualiza firmware-ul. If you cannot update over the network, try this method.

Notă:
Înainte de a actualiza, asigurați-vă că driverul de scaner Epson Scan 2 este instalat pe computer. Dacă nu este instalată aplicația Epson Scan 2, instalați-o.

1. Consultați site-ul web Epson pentru cele mai recente versiuni de actualizare de firmware.

   http://www.epson.com

   ❏ Dacă există firmware pentru scanerul dvs., descărcați-l și treceți la pasul următor.

   ❏ Dacă nu există informații despre firmware pe site-ul web, înseamnă că utilizați deja cel mai recent firmware.

2. Conectați computerul care conține firmware-ul descărcat la scaner prin intermediul cablului USB.

3. Faceți dublu clic pe fișierul .exe descărcat.

   Aplicația Epson Firmware Updater pornește.

4. Urmați instrucțiunile de pe ecran.