

DS-790WN

Ghidul administratorului

**Setări necesare pentru scopul
dumneavoastră**

Setări de rețea

Setări necesare pentru scanare

Setări de securitate de bază

Setări de securitate avansate

Setări de autentificare

Drept de proprietate intelectuală

Nicio parte a acestei publicații nu poate fi reprodusă, stocată pe un sistem de preluare sau transmisă în orice formă sau prin orice mijloc electronic, mecanic, prin fotocopiare, înregistrare sau în alt mod, fără permisiunea scrisă prealabilă a Seiko Epson Corporation. Nu se presupune nicio responsabilitate în ceea ce privește brevetele relativ la utilizarea informațiilor incluse în prezentul manual. De asemenea, nu se presupune nicio responsabilitate pentru daune rezultând din utilizarea informațiilor incluse în prezentul manual. Informațiile incluse în prezentul manual sunt destinate a fi utilizate numai cu acest produs Epson. Epson nu este responsabilă de utilizarea acestor informații prin aplicarea la alte produse.

Nici Seiko Epson Corporation și nici filialele sale nu vor fi responsabile față de persoana care a achiziționat acest produs sau față de terți pentru daune, pierderi, costuri sau cheltuieli suportate de achizitor sau de terți ca rezultat al unui accident, utilizări eronate sau abuzive a acestui produs sau a unor modificări sau reparații neautorizate ale acestui produs sau (exclusiv teritoriul S.U.A.) nerespectarea strictă a instrucțiunilor de operare și de întreținere ale Seiko Epson Corporation.

Seiko Epson Corporation și filialele sale nu vor fi responsabile pentru nicio daună sau problemă apărută ca urmare a utilizării opțiunilor sau a altor produse consumabile altele decât cele desemnate de către Seiko Epson Corporation ca fiind produse originale Epson sau produse aprobate Epson.

Seiko Epson Corporation nu va fi responsabilă pentru nicio daună rezultată ca urmare a interferențelor electromagnetice care survine în urma utilizării oricărui cabluri de interfață altele decât cele desemnate ca produse aprobate Epson de către Seiko Epson Corporation.

© 2021 Seiko Epson Corporation

Conținutul acestui manual și specificațiile acestui produs se pot modifica fără notificare prealabilă.

Mărci înregistrate

- ❑ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION și logo-urile acestora sunt mărci înregistrate sau mărci comerciale ale Seiko Epson.
- ❑ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❑ Chrome is a trademark of Google LLC.
- ❑ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❑ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❑ FeliCa și PaSoRi sunt mărci comerciale înregistrate ale Sony Corporation.
- ❑ MIFARE este o marcă înregistrată a NXP Semiconductor Corporation.
- ❑ Notificare generală: celelalte nume de produse utilizate aici au doar scop de identificare și pot fi mărci comerciale ale deținătorilor lor. Epson își declină orice drepturi asupra acestor mărci.

Cuprins

Drept de proprietate intelectuală

Mărci înregistrate

Introducere

Conținutul acestui document.	8
Utilizarea acestui ghid.	8
Marcaje și simboluri.	8
Descrieri utilizate în acest manual.	8
Referințe privind sistemul de operare.	9

Setări necesare pentru scopul dumneavoastră

Setări necesare pentru scopul dumneavoastră.	11
--	----

Setări de rețea

Conectarea scannerului la rețea.	14
Înainte de stabilirea conexiunii la rețea.	14
Conectarea la rețea de la panoul de comandă.	16
Adăugarea sau ștergerea computerului sau a dispozitivelor.	20
Conectarea la un scanner care a fost conectat la rețea.	20
Conectarea directă a unui dispozitiv inteligent la scanner (Wi-Fi Direct).	22
Restabilirea conexiunii la rețea.	24
Verificarea stării conexiunii la rețea.	26
Verificarea stării conexiunii la rețea din Panoul de comandă.	26
Specificații de rețea.	28
Specificații Wi-Fi.	28
Specificații Ethernet.	29
Funcții de rețea și IPv4/IPv6.	29
Protocol de securitate.	30
Utilizarea portului pentru scanner.	30
Rezolvarea problemelor.	31
Nu se poate realiza conexiunea la rețea.	31

Software pentru configurarea scannerului

Web Config.	36
Executarea utilitarului Web Config într-un browser web.	36

Executarea utilitarului Web Config în Windows.	36
Epson Device Admin.	37
Șablon de configurare.	37

Setări necesare pentru scanare

Configurarea unui server de e-mail.	42
Elemente de setare server de e-mail.	42
Verificarea unei conexiuni de server de e-mail.	43
Configurarea unui folder partajat în rețea.	45
Crearea folderului partajat.	45
Disponibilitatea contactelor.	63
Comparare configurare contacte.	64
Înregistrarea unei destinații în Contacte utilizând Web Config.	64
Înregistrarea destinațiilor ca grup folosind Web Config.	66
Copierea de rezervă și importul contactelor.	67
Exportul și înregistrarea în masă a contactelor cu ajutorul unui instrument.	68
Cooperarea între serverul LDAP și utilizatori.	70
Utilizare Document Capture Pro Server.	73
Setarea modului server.	73
Configurarea AirPrint.	74
Probleme la pregătirea scanării în rețea.	74
Sugestii pentru remedierea problemelor.	74
Imposibilitate de accesare Web Config.	74

Personalizarea afișajului panoului de comandă

Înregistrarea Presetări.	78
Opțiunile de meniu din Presetări.	79
Editarea ecranului principal al panoului de comandă.	80
Modificarea parametrului Aspect al ecranului principal.	80
Adăugare pictogramă.	81
Ștergere pictogramă.	82
Mutare pictogramă.	83

Setări de securitate de bază

Introducerea caracteristicilor de securitate ale produsului.	86
Setări administrative.	86
Configurarea parolei de administrator.	86

Utilizarea Setare blocare pentru panoul de comandă.	88
Conectarea ca administrator din Panoul de comandă.	92
Dezactivarea Interfeței externe.	92
Monitorizarea unui scanner la distanță.	93
Verificarea informațiilor pentru un scanner la distanță.	93
Recepționarea notificărilor prin e-mail la apariția de evenimente.	93
Rezolvarea problemelor.	95
Parolă de administrator uitată.	95

Setări de securitate avansate

Setări de securitate și de prevenire a pericolelor.	97
Setări pentru funcția de securitate.	98
Controlarea utilizând protocoale.	98
Protocoale de control.	98
Protocoale pe care le puteți activa sau dezactiva.	98
Elemente de setare a protocoalelor.	99
Utilizarea unui certificat digital.	101
Despre certificarea digitală.	101
Configurarea unui Certificat semnat de CA.	101
Actualizarea unui certificat autosemnat.	105
Configurarea unui Certificat CA.	105
Comunicare SSL/TLS cu scannerul.	106
Configurarea setărilor de bază SSL/TLS.	106
Configurarea unui certificat de server pentru scanner.	107
Comunicare criptată utilizând filtrarea IPsec/IP.	108
Despre IPsec/IP Filtering.	108
Configurarea politicii implicite.	108
Configurarea politicii de grup.	111
Exemple de configurare IPsec/IP Filtering.	117
Configurarea unui certificat pentru filtrarea IPsec/IP.	118
Conectarea scannerului la o rețea IEEE802.1X.	119
Configurarea unei rețele IEEE 802.1X.	119
Configurarea unui certificat pentru IEEE 802.1X.	120
Rezolvarea problemelor pentru securitate avansată.	120
Restabilirea funcțiilor de securitate.	120
Probleme privind utilizarea caracteristicilor de securitate a rețelei.	121
Probleme privind utilizarea unui certificat digital.	123

Setări de autentificare

Despre Setări de autentificare.	128
Funcții disponibile pentru Setări de autentificare.	128
Despre Metodă de autentificare.	129
Software pentru configurare.	131
Actualizarea firmware-ului scannerului.	131
Conectarea și configurarea unui dispozitiv de autentificare.	131
Listă de compatibilitate cititoare de carduri.	131
Conectarea dispozitivului de autentificare.	134
Setările dispozitivului de autentificare.	135
Informații de înregistrare și setare.	136
Configurarea.	136
Activare autentificare.	137
Setări de autentificare.	137
Înregistrarea Setări utilizator.	139
Sincronizarea cu Server LDAP.	145
Setarea serverului de e-mail.	149
Setarea Scanare în fold. meu.	150
Personalizați funcțiile accesibile printr-o singură atingere.	152
Rapoarte Job History utilizând Epson Device Admin.	152
Elemente care pot fi incluse în raport.	152
Conectarea ca administrator din Panoul de comandă.	152
Dezactivarea Setări de autentificare.	153
Ștergerea informațiilor Setări de autentificare (Restaurare setări implicite).	153
Rezolvarea problemelor.	154
Nu se poate citi cardul de autentificare.	154

Întreținere

Curățarea exteriorului scannerului.	156
Curățarea în interiorul scannerului.	156
Înlocuirea kitului de ansamblu rolă.	161
Coduri ale kiturilor de ansamblu rolă.	166
Resetarea numărului de scanări.	166
Economisirea energiei.	166
Transportarea scannerului.	167
Copierea de rezervă a setărilor.	168
Exportarea setărilor.	168
Importați setările.	169
Restaurare setări implicite.	169
Actualizarea aplicațiilor și a firmware-ului.	170

Actualizarea firmware-ului scannerului utilizând panoul de comandă.	170
Actualizare firmware folosind Web Config.	171
Actualizarea firmware-ului fără conectarea la Internet.	171

Introducere

Conținutul acestui document.	8
Utilizarea acestui ghid.	8

Conținutul acestui document

Acest document oferă următoarele informații pentru administratorii scanerelor.

- Setări de rețea
- Pregătirea funcției de scanare
- Activați și gestionați setările de securitate
- Activați și gestionați Setări de autentificare
- Efectuați întreținerea zilnică

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

Notă:

Acest document explică Setări de autentificare care oferă autentificare autonomă fără a fi nevoie să utilizați un server de autentificare. Pe lângă Setări de autentificare introduse în acest manual, puteți configura și un sistem de autentificare folosind un server de autentificare. Pentru a construi un sistem, utilizați Document Capture Pro Server Authentication Edition (denumirea prescurtată este Document Capture Pro Server AE).

Pentru mai multe informații, contactați biroul local Epson.

Utilizarea acestui ghid

Marcaje și simboluri



Atenție:

Instrucțiuni care trebuie respectate cu atenție, pentru evitarea vătămarilor corporale.



Important:

Instrucțiuni care trebuie respectate pentru evitarea deteriorării echipamentului.

Notă:

Furnizează informații complementare și 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 și de situație.
- Ilustrațiile utilizate în acest manual sunt numai pentru referință. Chiar dacă pot fi ușor diferite față de produsul real, metodele de operare sunt identice.

Referințe privind sistemul de operare

Windows

În acest manual, termeni precum „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012” și „Windows Server 2008 R2” se referă la următoarele sisteme de operare. De asemenea, „Windows” se utilizează pentru a desemna toate versiunile și „Windows Server” se utilizează pentru a desemna „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012” și „Windows Server 2008 R2”.

- Sistemul de operare Microsoft® Windows® 10
- Sistemul de operare Microsoft® Windows® 8.1
- Sistemul de operare Microsoft® Windows® 8
- Sistemul de operare Microsoft® Windows® 7
- Sistemul de operare Microsoft® Windows Server® 2019
- Sistemul de operare Microsoft® Windows Server® 2016
- Sistemul de operare Microsoft® Windows Server® 2012 R2
- Sistemul de operare Microsoft® Windows Server® 2012
- Sistemul de operare Microsoft® Windows Server® 2008 R2

Mac OS

În acest manual, termenul „Mac OS” se utilizează pentru a face referire la macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan și OS X Yosemite.

Setări necesare pentru scopul dumneavoastră

Setări necesare pentru scopul dumneavoastră.	11
--	----

Setări necesare pentru scopul dumneavoastră

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

Conectarea scannerului la rețea

Scop	Setări obligatorii
Doresc să conectez scannerul la rețea.	Configurați scannerul pentru scanarea în rețea. „Conectarea scannerului la rețea” la pagina 14
Doresc să conectez scannerul la un computer nou.	Efectuați setările de rețea pentru scannerul dumneavoastră pe noul computer. „Adăugarea sau ștergerea computerului sau a dispozitivelor” la pagina 20

Setări pentru scanare

Scop	Setări obligatorii
Doresc să trimit imagini scanate prin e-mail. (Scanare către e-mail)	1. Configurați serverul de e-mail pe care doriți să îl corelați. „Configurarea unui server de e-mail” la pagina 42 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 63
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. „Configurarea unui folder partajat în rețea” la pagina 45 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 63
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 obligatorii
Doresc să schimb elementele afișate pe panoul de comandă al scannerului.	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 77

Setarea funcțiilor de securitate de bază

Scop	Setări obligatorii
Doresc să împiedic pe oricine altcineva decât administratorul să modifice setările scannerului.	Setați o parolă de administrator pentru scanner. „Setări administrative” la pagina 86
Doresc să dezactivez utilizarea scannerelor cu conexiuni USB.	Dezactivați interfața externă. „Dezactivarea Interfeței externe” la pagina 92

Setarea funcțiilor avansate de securitate

Scop	Setări obligatorii
Doresc să controlez ce protocoale să folosesc.	Activați sau dezactivați protocoalele. „Controlarea utilizând protocoale” la pagina 98
Doresc să cripez calea de comunicare.	1. Configurați certificatul digital. „Utilizarea unui certificat digital” la pagina 101 2. Configurați comunicarea SSL/TLS. „Comunicare SSL/TLS cu scannerul” la pagina 106
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 108
Doresc să folosesc un scanner într-o rețea IEEE802.1X.	Configurați IEEE802.1X pentru scanner. „Conectarea scannerului la o rețea IEEE802.1X” la pagina 119

Setarea funcțiilor pentru autentificare de către scanner

Scop	Setări obligatorii
Doresc să activez Setări de autentificare.	Consultați următoarele pentru mai multe informații despre Setări de autentificare și Metodă de autentificare disponibile. „Despre Setări de autentificare” la pagina 128 „Despre Metodă de autentificare” la pagina 129

Utilizarea sistemului de autentificare al unui server

Cu Document Capture Pro Server Authentication Edition (abreviat Document Capture Pro Server AE), puteți implementa un sistem de autentificare care utilizează un server pentru autentificare.

Pentru mai multe informații, contactați biroul local Epson.

Setări de rețea

Conectarea scannerului la rețea.	14
Adăugarea sau ștergerea computerului sau a dispozitivelor.	20
Verificarea stării conexiunii la rețea.	26
Specificații de rețea.	28
Rezolvarea problemelor.	31

Conectarea scannerului la rețea

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

Notă:

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

Configurarea de pe website

Accesați următorul site web și introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.
<http://epson.sn>

Configurarea utilizând discul cu software (numai pentru modelele prevăzute cu un disc cu software și utilizatorii cu computere Windows cu unități de disc).

Introduceți discul cu software în computer și urmați instrucțiunile de pe ecran.

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	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Stabiliți modul de conectare a scannerului 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	<input type="checkbox"/> Adresă IP <input type="checkbox"/> Mască subrețea <input type="checkbox"/> Gateway implicit	Stabiliți adresa IP care se va atribui scannerului. 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	<input type="checkbox"/> SSID <input type="checkbox"/> Parolă	Acestea sunt SSID (numele rețelei) și parola punctului de acces la care se conectează scannerul. Dacă a fost setată filtrarea adresei MAC, înregistrați adresa MAC a scannerului înainte de a înregistra scannerul. Consultați următoarele pentru standardele acceptate. „Specificații de rețea” la pagina 28
Informații server DNS	<input type="checkbox"/> Adresa IP pentru DNS primar <input type="checkbox"/> 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	<input type="checkbox"/> Nume server proxy	<p>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 scannerului la internet.</p> <p>Pentru următoarele funcții, scannerul se conectează direct la internet.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Epson Connect Services <input type="checkbox"/> Servicii cloud ale altor companii <input type="checkbox"/> Actualizări firmware <input type="checkbox"/> Trimiterea imaginilor scanate la SharePoint(WebDAV)
Informații privind numărul portului	<input type="checkbox"/> Număr de port de deblocat	<p>Verificați numărul portului utilizat de scanner și de computer și eliberați portul blocat de un firewall, dacă este necesar.</p> <p>Consultați următoarele pentru numărul de port utilizat de scanner.</p> <p>„Utilizarea portului pentru scanner” la pagina 30</p>

Atribuirea adresei IP

Acestea sunt următoarele tipuri de atribuire de adresă IP.

Adresă IP statică:

Atribuiți adresa IP predeterminată la scanner (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 scanner, 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 scannerului (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 scannerul 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 scannerul 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 scannerului 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, scannerul și internetul (server opus) din partea fiecăruia dintre acestea. Serverul opus comunică doar cu serverul proxy. Prin urmare, informațiile despre scanner, 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 scanner.

Conectarea la rețea de la panoul de comandă

Conectați scannerul la rețea folosind panoul de comandă al scannerului.

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 scannerul.
2. Selectați **Setări** pe ecranul principal de pe panoul de comandă al scannerului.
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 scannerul 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 scannerul la rețea, utilizând un cablu LAN și apoi verificați conexiunea.

1. Conectați scannerul 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 scannerul 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.

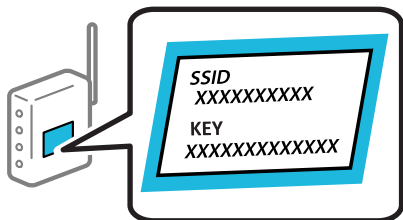
După conectarea scannerului la rețea, conectați-vă la scanner de la dispozitivul pe care doriți să îl utilizați (computer, dispozitiv inteligent, tabletă etc.)

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 scannerului. 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 scannerului 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.

Informații conexe

➔ „Verificarea stării conexiunii la rețea” la pagina 26

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 scannerului 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 scanner și încercați din nou.

Informații conexe

➔ „Verificarea stării conexiunii la rețea” la pagina 26

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. Apăsăți  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 scannerului 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 26

Adăugarea sau ștergerea computerului sau a dispozitivelor

Conectarea la un scanner care a fost conectat la rețea

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

Utilizarea unui scanner de rețea de la un al doilea computer

Recomandăm utilizarea programului de instalare pentru conectarea scannerului la un computer. Puteți rula programul de instalare utilizând una dintre următoarele metode.

Configurarea de pe website

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

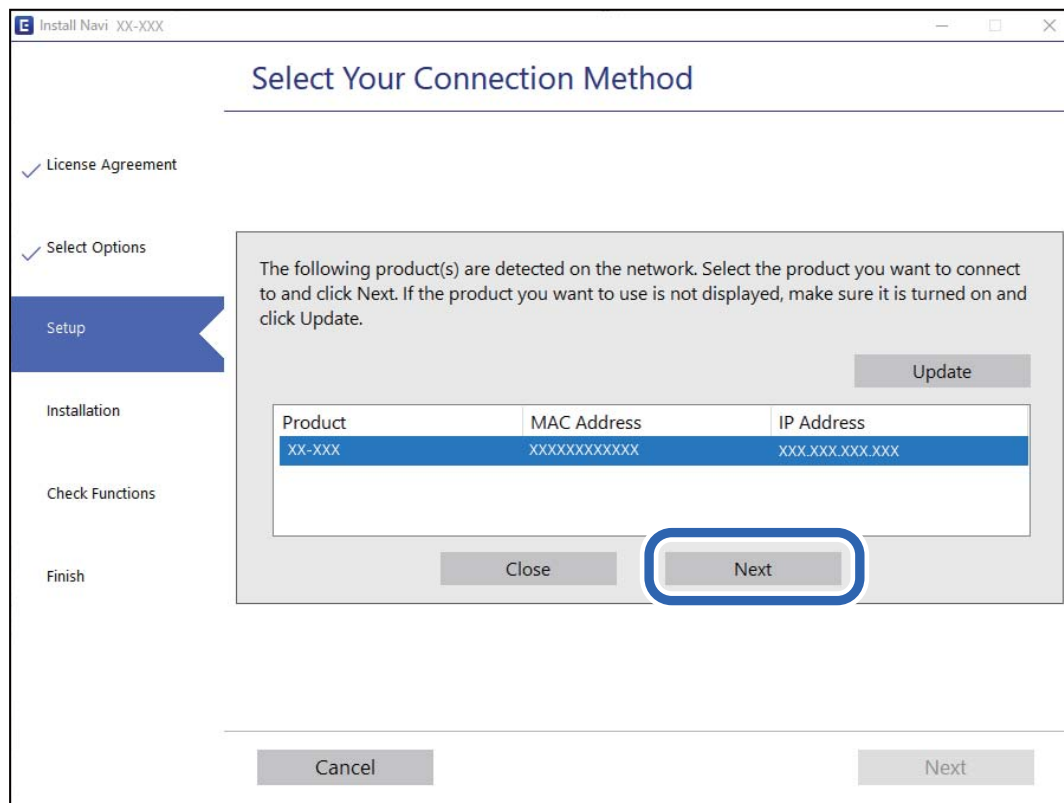
<http://epson.sn>

Configurarea utilizând discul cu software (numai pentru modelele prevăzute cu un disc cu software și utilizatorii cu computere Windows cu unități de disc).

Introduceți discul cu software în computer și urmați instrucțiunile de pe ecran.

Selectarea scannerului

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



Urmați instrucțiunile de pe ecran.

Utilizarea unui scanner de rețea de la un dispozitiv inteligent

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

Conectarea printr-un router wireless

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

Pentru detalii suplimentare, consultați următoarele informații.

[„Efectuarea setărilor de conectare la un dispozitiv inteligent” la pagina 25](#)

Conectarea prin Wi-Fi Direct

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

Pentru detalii suplimentare, consultați următoarele informații.

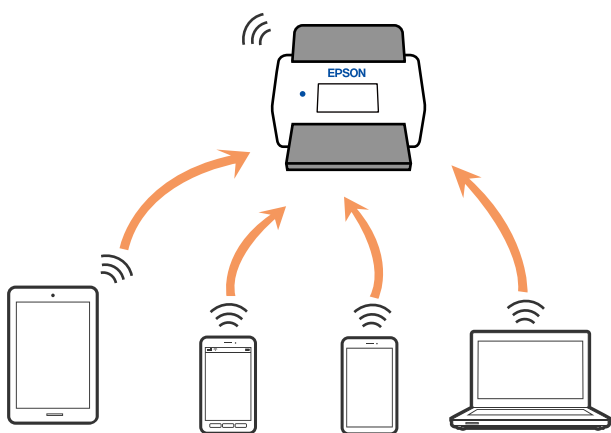
[„Conectarea directă a unui dispozitiv inteligent la scanner \(Wi-Fi Direct\)” la pagina 22](#)

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

Wi-Fi Direct (Simple AP) permite conectarea unui dispozitiv inteligent direct la scanner 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 scannerul și computerul sau dispozitivul inteligent în mod direct. În acest mod, scannerul acționează ca router wireless și puteți conecta dispozitivele la scanner, fără a fi necesară utilizarea unui router wireless standard. Cu toate acestea, dispozitivele conectate direct la scanner nu pot comunica între ele prin intermediul scannerului.



Scannerul 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 scannerul este conectat prin Wi-Fi, conexiunea Wi-Fi este deconectată temporar.

Conectarea la un dispozitiv inteligent utilizând Wi-Fi Direct

Această metodă permite conectarea scannerului 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. Urmăriți instrucțiunile din Epson Smart Panel pentru conectarea la scanner.
Când dispozitivul inteligent este conectat la scanner, treceți la pasul următor.
6. Pe panoul de comandă al scannerului, 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 scannerului 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 scanner 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 scanner. 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 scanner 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 scannerului 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 scanner. 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 scannerului. La dezactivarea acestora, toate dispozitivele conectate la scanner 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 scanner 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 scanner.

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 scannerului la un computer. Puteți rula programul de instalare utilizând una dintre următoarele metode.

- Configurarea de pe website
Accesați următorul site web și introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.
<http://epson.sn>
- Configurarea utilizând discul cu software (numai pentru modelele prevăzute cu un disc cu software și utilizatorii cu computere Windows cu unități de disc).
Introduceți discul cu software în computer și urmați instrucțiunile de pe ecran.

Selectarea metodelor de conectare

Urmați instrucțiunile de pe ecran. Pe ecranul **Selectați operațiunea**, 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 31

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 pe un dispozitiv inteligent, accesați următorul site web și apoi introduceți numele produsului. Mergeți la **Configurarea** și apoi începeți configurarea.

<http://epson.sn>

Accesați site-ul 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. Puteți rula programul de instalare utilizând următoarea metodă.

- Configurarea de pe website

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

<http://epson.sn>

- Configurarea utilizând discul cu software (numai pentru modelele prevăzute cu un disc cu software și utilizatorii cu computere Windows cu unități de disc).

Introduceți discul cu software în computer și urmați instrucțiunile de pe ecran.

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 18

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.

- Configurarea de pe website

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

<http://epson.sn>

- Configurarea utilizând discul cu software (numai pentru modelele prevăzute cu un disc cu software și utilizatorii cu computere Windows cu unități de disc).

Introduceți discul cu software în computer și urmați instrucțiunile de pe ecran.

Selectarea opțiunii de modificare a metodelor de conectare

Urmați instrucțiunile de pe ecran. Pe ecranul **Selectați operațiunea**, 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 scannerului.

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 scannerului.



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

Afișarea informațiilor de rețea detaliate pe panoul de comandă

Când scannerul 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
Australia Noua Zeelandă Taiwan Coreea de Sud	Tabel B

Tabel A

Standarde	IEEE 802.11b/g/n ^{*1}
Gamă de frecvențe	2,4 GHz
Putere maximă de radiofrecvență transmisă	2400 – 2483,5 MHz: 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 acceptă doar 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 IPv4/IPv6

Funcții	Acceptat
Epson Scan 2	IPv4, IPv6

Funcții	Acceptat
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

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 scanner

Scannerul 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 scannerul

Utilizare	Destinație (Server)	Protocol	Număr Port	
Expedierea de fișiere (Când se folosește scanarea într-un folder de rețea de la scanner)	Server FTP/FTPS	FTP/FTPS (TCP)	20	
			21	
	Server de fișier	SMB (TCP)	445	
			NetBIOS (UDP)	137
				138
	Server WebDAV	NetBIOS (TCP)	139	
Protocol HTTP (TCP)			80	
		Protocol HTTPS (TCP)	443	
Expedierea de e-mailuri (Când se folosește scanarea la e-mail de la scanner)	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 scanner)	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 scanner)	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 scanner) Autentificarea utilizatorului când se folosește scanarea într-un folder de rețea (SMB) de la scanner	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 scannerul dintr-o aplicație precum EpsonNet Config și driver de scanner.	Scanner	ENPC (UDP)	3289
Colectați și configurați informațiile MIB dintr-o aplicație precum EpsonNet Config și driver de scanner.	Scanner	SNMP (UDP)	161
Căutare scanner WSD	Scanner	WS-Discovery (UDP)	3702
Redirecționarea datelor de scanare dintr-o aplicație	Scanner	Scanare în rețea (TCP)	1865
Colectarea informațiilor despre lucrare la scanarea push dintr-o aplicație	Scanner	Scanare Push în rețea	2968
Web Config	Scanner	HTTP (TCP)	80
		HTTPS (TCP)	443

Rezolvarea problemelor

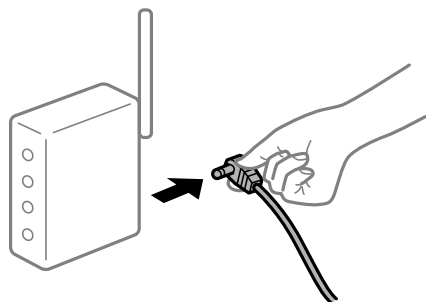
Nu se poate realiza conexiunea la rețea

Această problemă ar putea avea una dintre următoarele cauze.

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

Soluții

Opriti 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 scanner, 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 scannerul mai aproape de routerul wireless, opriti și reporniți routerul wireless.

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

Soluții

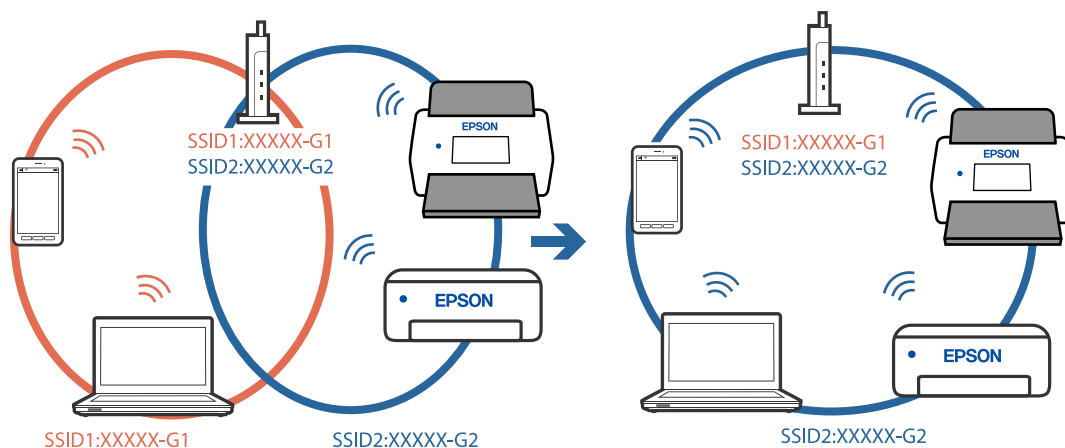
Efectuați din nou setările de conexiune pentru a se potrivi cu noul router wireless.

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 scannerul.



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 scanner 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 scannerului 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 scannerului și verificați adresa IP și masca de subrețea atribuite scannerului.

Reporniți routerul wireless sau resetați setările de rețea ale scannerului.

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.

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

Soluții

Când conectați scannerul 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, scannerul se conectează și se deconectează în mod repetat.
- Conexiunea la scanner este imposibilă.
- Viteza de comunicație se reduce.

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

1. Deconectați cablul Ethernet conectat la computer și la scanner.
2. Dacă IEEE 802.3az pentru computer este activat, dezactivați-l.
Consultați documentația aferentă computerului pentru detalii.
3. Conectați computerul și scannerul în mod direct, utilizând un cablu Ethernet.
4. La scanner, verificați setările de rețea.
Selectați **Setări > Setări rețea > Stare rețea > Stare rețea cu fir LAN/Wi-Fi**.
5. Verificați adresa IP a scannerului.

6. Pe computer, accesați Web Config.
Lansați un browser web, apoi introduceți adresa IP a scannerului.
[„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)
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 scanner.
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 scanner.
Dacă problema reapare, este posibil să fie cauzată de alte dispozitive decât scannerul.

■ **Scannerul este oprit.**

Soluții

Asigurați-vă că scannerul este pornit.

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

Software pentru configurarea scannerului

Web Config.	36
Epson Device Admin.	37

Web Config

Web Config este o aplicație care rulează într-un browser web, de exemplu în Internet Explorer și Safari pe un computer. Puteți confirma starea scannerului sau puteți modifica serviciul de rețea și setările scannerului. Deoarece scanerile sunt accesate și operate direct din rețea, acest lucru este adecvat pentru configurarea pe rând a scannerelor. Pentru a utiliza Web Config, conectați computerul la aceeași rețea ca și scannerul.

Sunt acceptate următoarele browsere.

Microsoft Edge, Windows Internet Explorer 8 sau superior, Firefox*, Chrome*, Safari*

* Utilizați cea mai recentă versiune.

Executarea utilitarului Web Config într-un browser web

1. Verificați adresa IP a scannerului.

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

2. Lansați un browser web de la un computer sau un dispozitiv inteligent, apoi introduceți adresa IP a scannerului.

Format:

IPv4: http://adresa IP a scannerului/

IPv6: http://[adresa IP a scannerului]/

Exemple:

IPv4: http://192.168.100.201/

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

Notă:

Întrucât scannerul 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.

3. Conectați-vă ca administrator pentru a modifica setările scannerului.

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

Notă:

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

· Nume utilizator: niciunul (gol)

· Parolă: numărul de serie al scannerului

Pentru a găsi numărul de serie, verificați eticheta atașată în partea din spate a scannerului.

Dacă **Deconectarea administratorului** este afișat în partea din dreapta-sus a ecranului, v-ați conectat deja ca administrator.

Executarea utilitarului Web Config în Windows

Atunci când conectați un computer la scanner prin utilizarea WSD, urmați pașii de mai jos pentru a executa utilitarul Web Config.

1. Deschideți lista de scanere din computer.

Windows 10

Faceți clic pe butonul Start, apoi selectați **Sistem Windows > Panou de control > Vizualizare dispozitive și imprimante în Hardware și sunet**.

Windows 8.1/Windows 8

Selectați **Desktop > Setări > Panou de control > Vizualizare dispozitive și imprimante din Hardware și sunete** (sau **Hardware**).

Windows 7

Faceți clic pe butonul Start și selectați **Panou de control > Vizualizare dispozitive și imprimante din Hardware și sunete**.

2. Faceți clic dreapta pe scanner și selectați **Proprietăți**.

3. Selectați fila **Serviciu web** și faceți clic pe adresa URL.

Întrucât scannerul 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.

Notă:

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

· Nume utilizator: niciunul (gol)

· Parolă: numărul de serie al scannerului

Pentru a găsi numărul de serie, verificați eticheta atașată în partea din spate a scannerului.

Dacă **Deconectarea administratorului** este afișat în partea din dreapta-sus a ecranului, v-ați conectat deja ca administrator.

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.

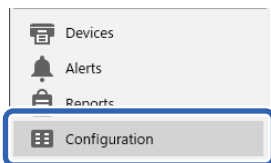
Șablon de configurare

Crearea șablonului de configurare

Creați un șablon de configurare de la zero.

1. Porniți Epson Device Admin.

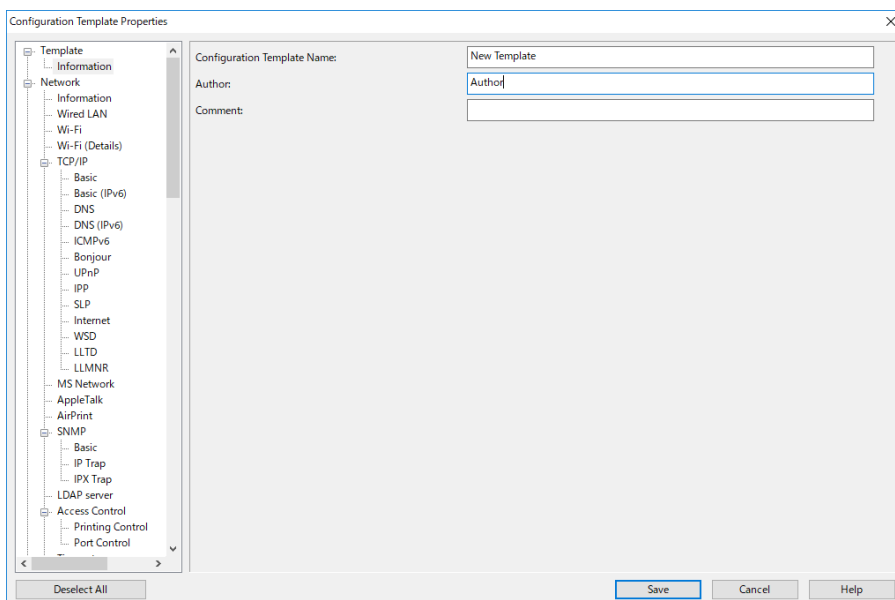
2. Selectați **Configuration** în meniul de sarcini de pe bara laterală.



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).
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

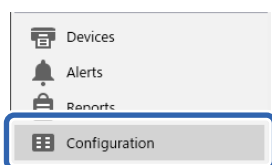
Aplicați scannerului șablonul de configurare salvat. Elementele selectate din șablon sunt imprimate. Dacă scannerul țintă nu dispune de o funcție adecvată, aceasta nu este aplicată.

Notă:

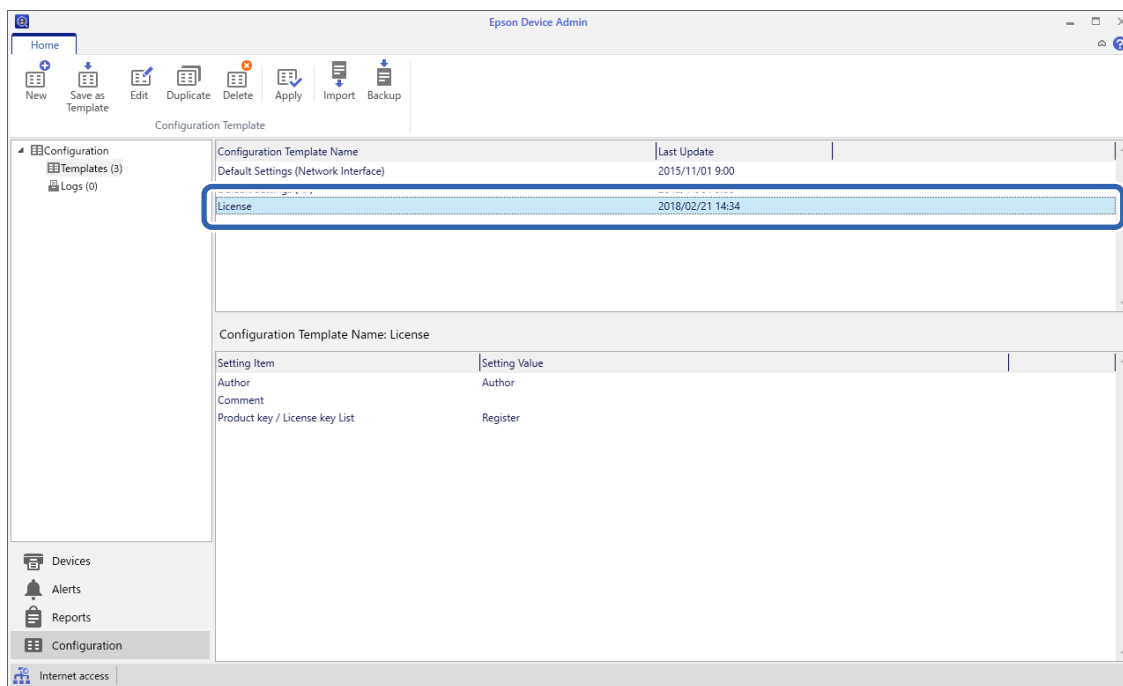
Când parola de administrator este setată pe scanner, configurați parola în prealabil.

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 scannerul adecvat și apoi faceți clic pe **Edit**.
4. Setati 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.

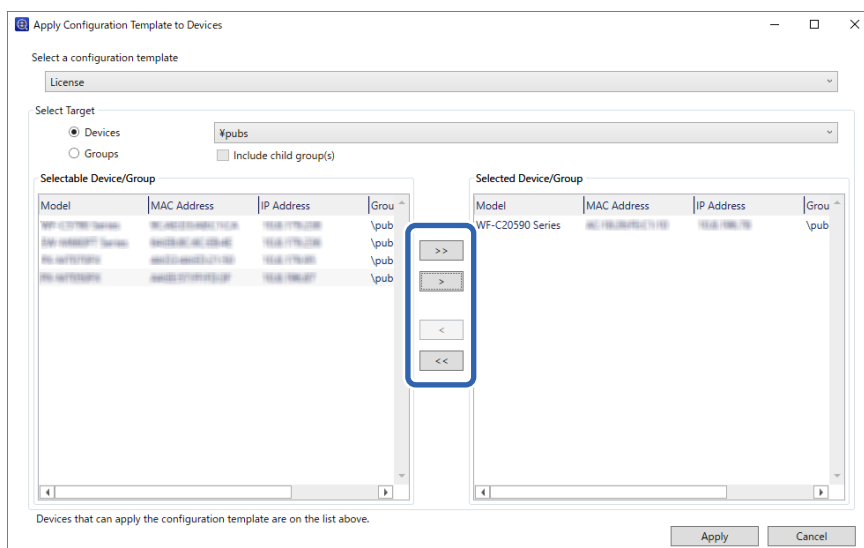


4. Selectați șablonul de configurare pe care doriți să îl aplicați.

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 scannerul 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

Configurarea unui server de e-mail.	42
Configurarea unui folder partajat în rețea.	45
Disponibilitatea contactelor.	63
Utilizare Document Capture Pro Server.	73
Configurarea AirPrint.	74
Probleme la pregătirea scanării în rețea.	74

Configurarea unui server de e-mail

Setați serverul de e-mail din Web Config.

Când scannerul poate trimite mesajul de e-mail prin configurarea serverului de e-mail, sunt posibile următoarele situații.

- Transferă rezultatele scanării prin e-mail
- Primește notificarea prin e-mail de la scanner

Înainte de configurare, verificați aspectele de mai jos.

- Scannerul este conectat la rețeaua care poate accesa serverul de e-mail.
- Informațiile de configurare pentru e-mail ale computerului care utilizează același server de e-mail ca scannerul.

Notă:

- Când utilizați serverul de e-mail pe internet, confirmați informațiile de configurare de la furnizor sau de pe site-ul web.
- Puteți seta, de asemenea, serverul de e-mail de la panoul de comandă. Accesați conform procedurii de mai jos.

Setări > Setări rețea > Complex > Server e-mail > Setări server

1. Accesați Web Config și selectați fila **Rețea > Server e-mail > De bază**.
2. Introduceți o valoare pentru fiecare element.
3. Selectați **OK**.
Sunt afișate setările pe care le-ați selectat.

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

Elemente de setare server de e-mail

Elemente	Setări și explicație	
Metodă de autentificare	Indicați metoda de autentificare pentru ca scannerul să acceseze serverul de e-mail.	
	Oprit	Autentificarea este dezactivată la comunicarea cu un server de mail.
	ATENT. SMTP	Este necesar ca un server de mail să accepte autentificarea SMTP.
	POP înainte de SMTP	Configurați serverul POP3 când selectați această metodă.
Cont autentificare	Dacă selectați ATENT. SMTP sau POP înainte de SMTP drept Metodă de autentificare , introduceți numele contului autentificat folosind între 0 și 255 de caractere în format ASCII (0x20 – 0x7E).	
Parolă autentificare	Dacă selectați ATENT. SMTP sau POP înainte de SMTP drept Metodă de autentificare , introduceți parola autentificată, folosind între 0 și 20 de caractere, în format ASCII (0x20 – 0x7E).	

Elemente	Setări și explicație	
Adresă e-mail expeditor	Introduceți adresa de e-mail a expeditorului. 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 .
Validare certificat	Certificatul este validat atunci când este activată această funcție. Recomandăm setarea acestei funcții la Activare .	
Adresă server POP3	Dacă selectați POP înainte de SMTP ca Metodă de autentificare , introduceți adresa de server POP3 între 0 și 255 caractere folosind A – Z a – z 0 – 9 . - . Puteți folosi formatul IPv4 sau FQDN.	
Număr port server POP3	Dacă selectați POP înainte de SMTP ca Metodă de autentificare , introduceți un număr între 1 și 65535.	

Verificarea unei conexiuni de server de e-mail

Puteți testa conexiunea cu serverul de e-mail prin efectuarea verificării conexiunii.

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

Va fi inițiată testarea conexiunii la serverul de e-mail. După test, se afișează raportul de verificare.

Notă:

Aveți posibilitatea de a efectua verificarea conexiunii la serverul de e-mail de la panoul de comandă. Accesați conform procedurii de mai jos.

Setări > Setări rețea > Complex > Server e-mail > Verificare conexiune

Referințe privind testul conexiunii serverului de e-mail

Mesaje	Cauză
Testarea conexiunii a reușit.	Acest mesaj apare când conexiunea cu serverul a reușit.

Mesaje	Cauză
Eroare de comunicare cu serverul SMTP. Verificați următoarele. - Setări rețea	Acest mesaj apare atunci când <ul style="list-style-type: none"> <input type="checkbox"/> Scannerul nu este conectat la o rețea <input type="checkbox"/> Serverul SMTP este nefuncțional <input type="checkbox"/> Conexiunea de rețea s-a întrerupt în timpul comunicațiilor <input type="checkbox"/> S-au primit date incomplete
Eroare de comunicare cu serverul POP3. Verificați următoarele. - Setări rețea	Acest mesaj apare atunci când <ul style="list-style-type: none"> <input type="checkbox"/> Scannerul nu este conectat la o rețea <input type="checkbox"/> Serverul POP3 este nefuncțional <input type="checkbox"/> Conexiunea de rețea s-a întrerupt în timpul comunicațiilor <input type="checkbox"/> S-au primit date incomplete
A survenit o eroare în timpul conectării la serverul SMTP. Verificați următoarele. - Adresă server SMTP - Server DNS	Acest mesaj apare atunci când <ul style="list-style-type: none"> <input type="checkbox"/> Conectarea la un server DNS nu a reușit <input type="checkbox"/> 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 <ul style="list-style-type: none"> <input type="checkbox"/> Conectarea la un server DNS nu a reușit <input type="checkbox"/> 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 eșuat. Modificați parametrul Conexiune securizată la Fără.	Acest mesaj apare atunci când apare o neconcordanță SMTP între un server și un client sau atunci când serverul nu acceptă conexiunea securizată SMTP (conexiune SSL).
Conectarea la serverul SMTP a eșuat. Modificați parametrul Conexiune securizată la SSL/TLS.	Acest mesaj apare atunci când apare o neconcordanță SMTP între un server și un client sau atunci când serverul solicită să utilizeze o conexiune SSL/TLS pentru o conexiune securizată SMTP.
Conectarea la serverul SMTP a eșuat. Modificați parametrul Conexiune securizată la STARTTLS.	Acest mesaj apare atunci când apare o neconcordanță SMTP între un server și 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 și ora	Acest mesaj apare atunci când setarea de dată și oră a scannerului este incorectă sau atunci când certificatul a expirat.
Conexiunea nu este de încredere. Verificați următoarele. - Certificat CA	Acest mesaj apare atunci când scannerul 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.

Mesaje	Cauză
Autentificarea serverului SMTP a eșuat. Modificați 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 eșuat. Modificați 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 scannerul este ocupat.

Configurarea unui folder partajat în rețea

Configurați un folder partajat de rețea pentru salvarea imaginii scanate.

La salvarea unui fișier în folder, scannerul este conectat cu numele de utilizator al computerului pe care a fost creat folderul.

Crearea folderului partajat

Informații conexe

- ➔ „Înainte de crearea folderului partajat” la pagina 45
- ➔ „Verificarea profilului de rețea” la pagina 46
- ➔ „Locația de creare a folderului partajat și un exemplu de securitate” la pagina 46
- ➔ „Adăugarea unui grup sau utilizator care permite accesul” la pagina 59

Înainte de crearea folderului partajat

Înainte de crearea folderului partajat, verificați următoarele.

- Scannerul este conectat la rețeaua unde poate accesa computerul pe care se va crea folderul partajat.
- Numele computerului unde va fi creat folderul partajat nu conține un caracter cu mai mulți octeți.



Important:


Când un caracter cu mai mulți octeți este inclus în numele computerului, este posibil ca salvarea fișierului în folderul partajat să nu reușească.

În acest caz, comutați la un computer al cărui nume nu include caracterul cu mai mulți octeți sau modificați numele computerului.

Când modificați numele computerului, confirmați cu administratorul în prealabil, deoarece aceasta poate modifica unele setări, precum gestionarea computerului, accesul la resurse etc.

Verificarea profilului de rețea

La computerul unde se va crea folderul partajat, verificați dacă partajarea folderelor este disponibilă.

1. Conectați-vă la computerul unde contul de utilizator cu autoritate de administrator va crea folderul partajat.
2. Selectați **Panou de control > Rețea și Internet > Centru rețea și partajare**.
3. Faceți clic pe **Setări de partajare avansate**, apoi faceți clic pe  pentru profilul cu **(profil curent)** în profilurile de rețea afișate.
4. Verificați dacă opțiunea **Activare partajare fișiere și imprimante** este selectată în **Partajare fișiere și imprimante**.
Dacă este deja selectată, faceți clic pe **Anulare** și închideți fereastra.
Când modificați setările, faceți clic pe **Salvare modificări** și închideți fereastra.

Locația de creare a folderului partajat și un exemplu de securitate

În funcție de locația unde este creat folderul partajat, securitatea și facilitățile variază.

Pentru operarea folderului partajat de la scanere sau alte computere, sunt necesare următoarele permisiuni de citire și modificare pentru folder.

Fila **Partajare > Partajare avansată > Permișiuni**

Controlează permisiunea de acces din rețea a folderului partajat.

Permișiunea de acces din fila **Securitate**

Controlează permisiunea de acces din rețea și de acces local a folderului partajat.

Când setați **Toți** la folderul partajat creat pe desktop, ca exemplu de creare a unui folder partajat, se va permite accesul tuturor utilizatorilor care pot accesa computerul.

Cu toate acestea, utilizatorul care nu deține autoritate nu le poate accesa, deoarece desktopul (folderul) se află sub controlul folderului de utilizator, iar setările de securitate ale folderului se utilizează de utilizator sunt transmise acestuia. Utilizatorul cărui i se permite accesul în fila **Securitate** (utilizator conectat și administrator, în acest caz) poate opera folderul.

Consultați mai jos modalitatea de creare a locației adecvate.

Acest exemplu este valabil pentru crearea folderului „scan_folder”.

Informații conexe

- ➔ [„Exemplu de configurare pentru servere de fișiere” la pagina 46](#)
- ➔ [„Exemplu de configurare pentru un computer personal” la pagina 53](#)

Exemplu de configurare pentru servere de fișiere

Această explicație este un exemplu de creare a folderului partajat în folderul rădăcină al computerului partajat, precum serverul de fișiere, în condițiile următoare.

Utilizatorii cu drept de control al accesului, cum ar fi persoanele care dispun de același domeniu al unui computer pentru a crea un folder partajat, pot accesa respectivul folder partajat.

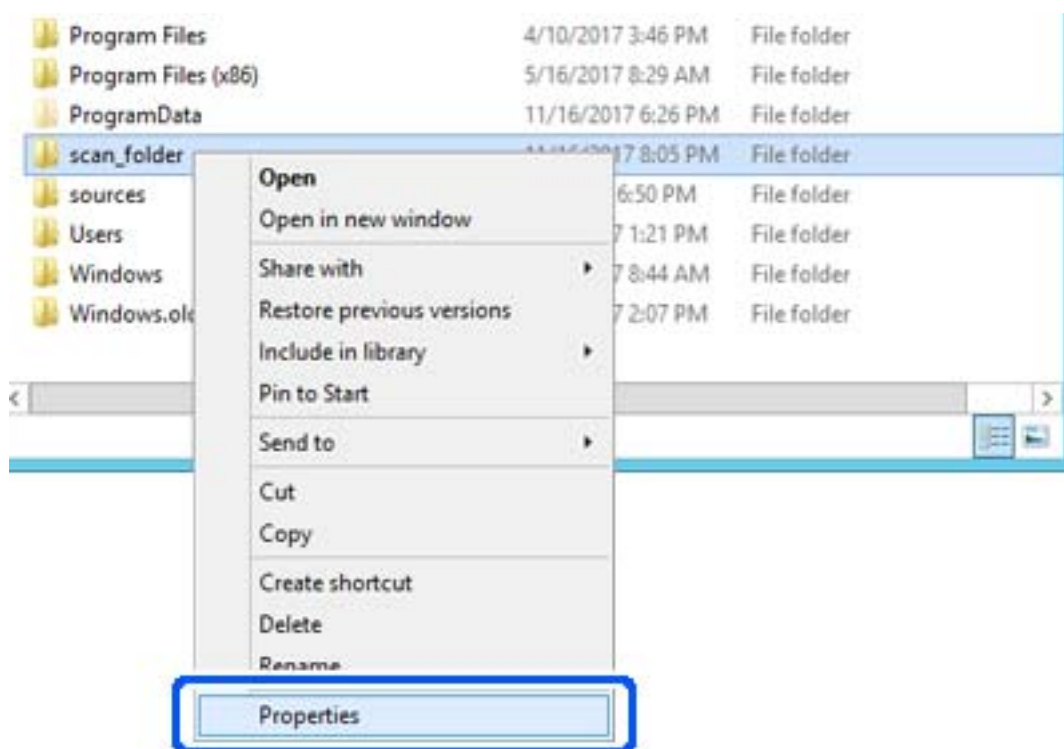
Setați această configurație atunci când permiteți oricărui utilizator să citească și să scrie în folderul partajat de pe computer, precum serverul de fișiere și computerul partajat.

- Locație pentru crearea folderului partajat: Folderul rădăcină al unității
- Cale folder: C:\scan_folder
- Permisii de acces prin intermediul rețelei (Partajare permisiuni): Toți
- Permisii de acces la sistemul de fișiere (Securitate): Utilizatori autentificați

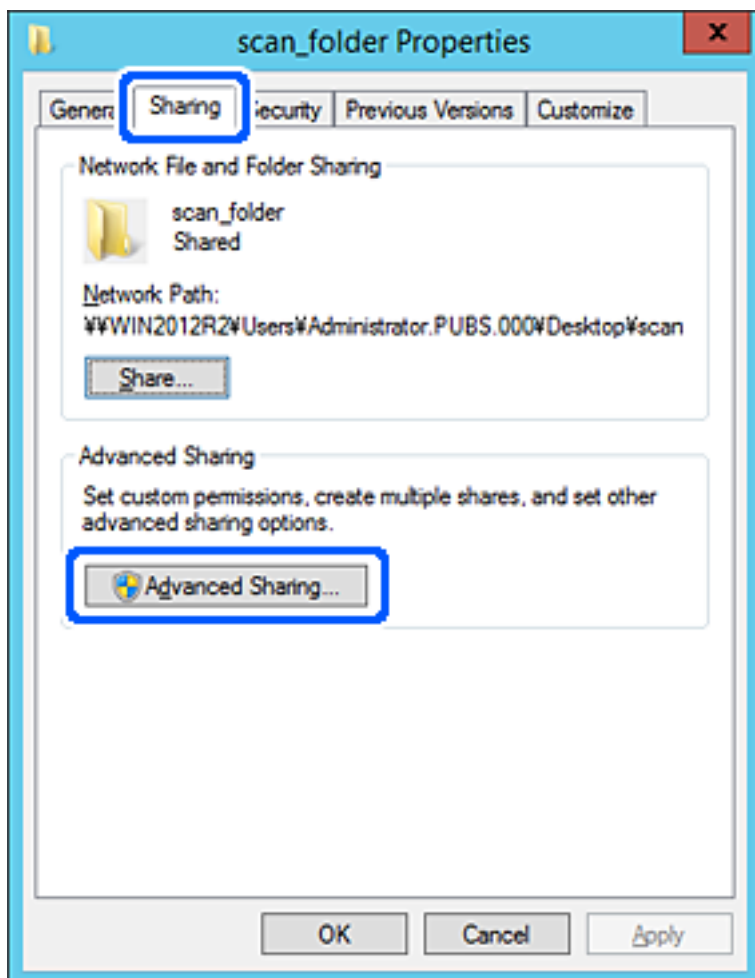
1. Conectați-vă la computerul unde contul de utilizator cu autoritate de administrator va crea folderul partajat.
2. Porniți Explorer.
3. Creați folderul în rădăcina unității și denumiți-l „scan_folder”.

Pentru numele folderului, introduceți între 1 și 12 caractere alfanumerice. Dacă se depășește limita de caractere a numelui folderului, este posibil să nu îl puteți accesa normal, în funcție de diferențele dintre medii.

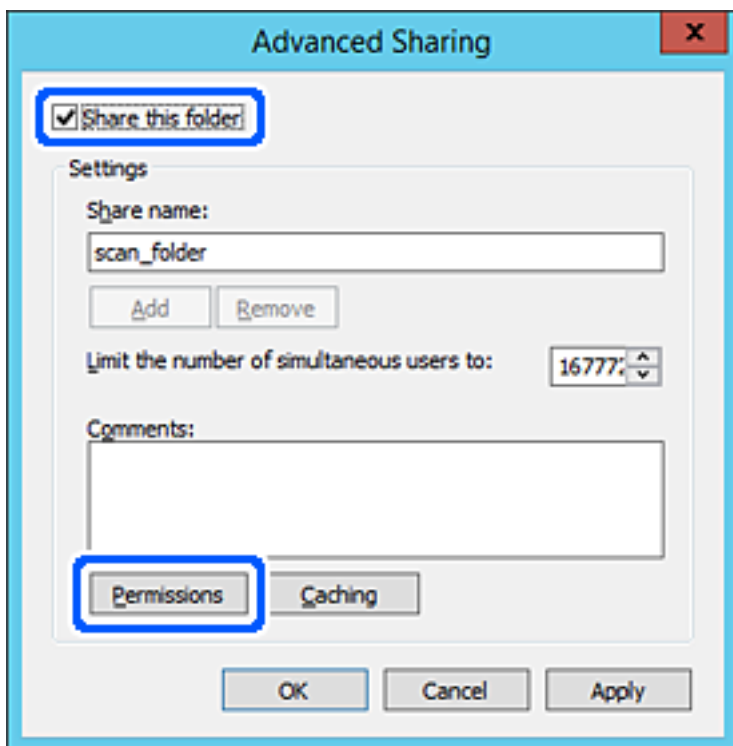
4. Faceți clic dreapta pe folder și selectați **Proprietăți**.



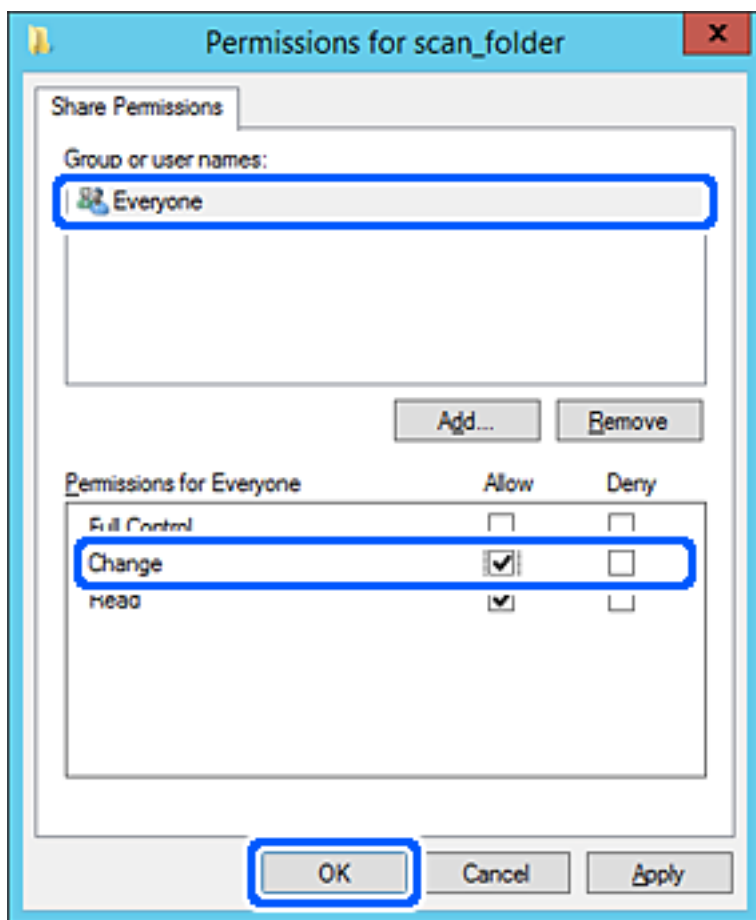
5. Faceți clic pe **Partajare complexă** în fila **Partajare**.



6. Selectați **Partajați acest folder**, apoi faceți clic pe **Permișiuni**.

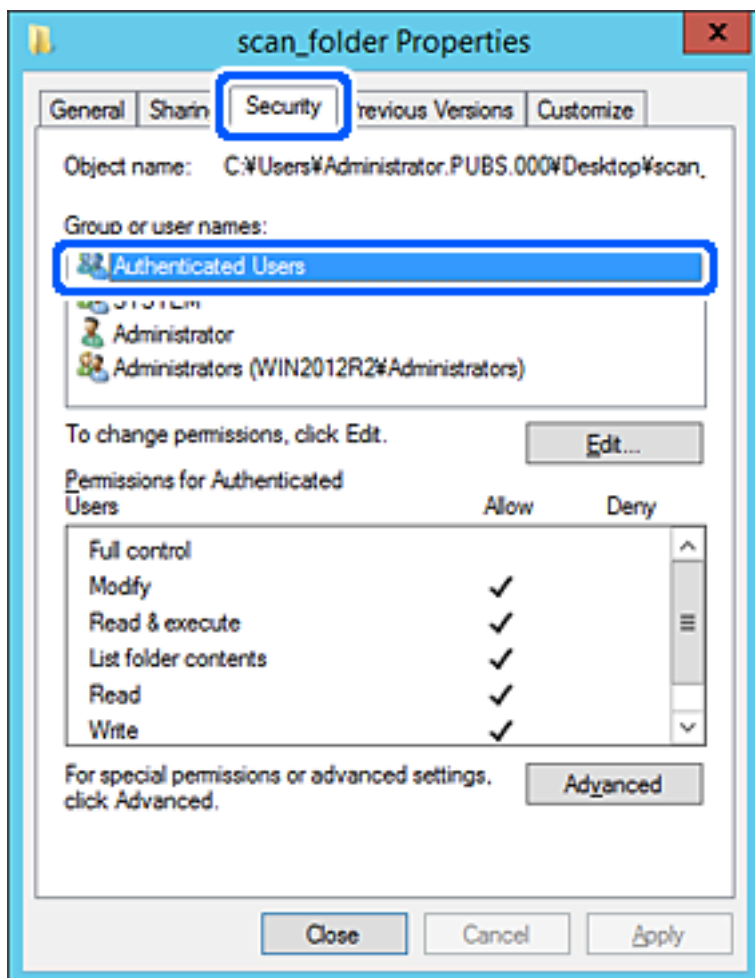


7. Selectați grupul **Toți** din **Nume de grup sau de utilizator**, selectați **Se permite** la **Modificare** și faceți clic pe **OK**.



8. Faceți clic pe **OK**.

9. Selectați fila **Securitate**, apoi selectați **Utilizatori autentificați** din **Nume grup sau utilizator**.

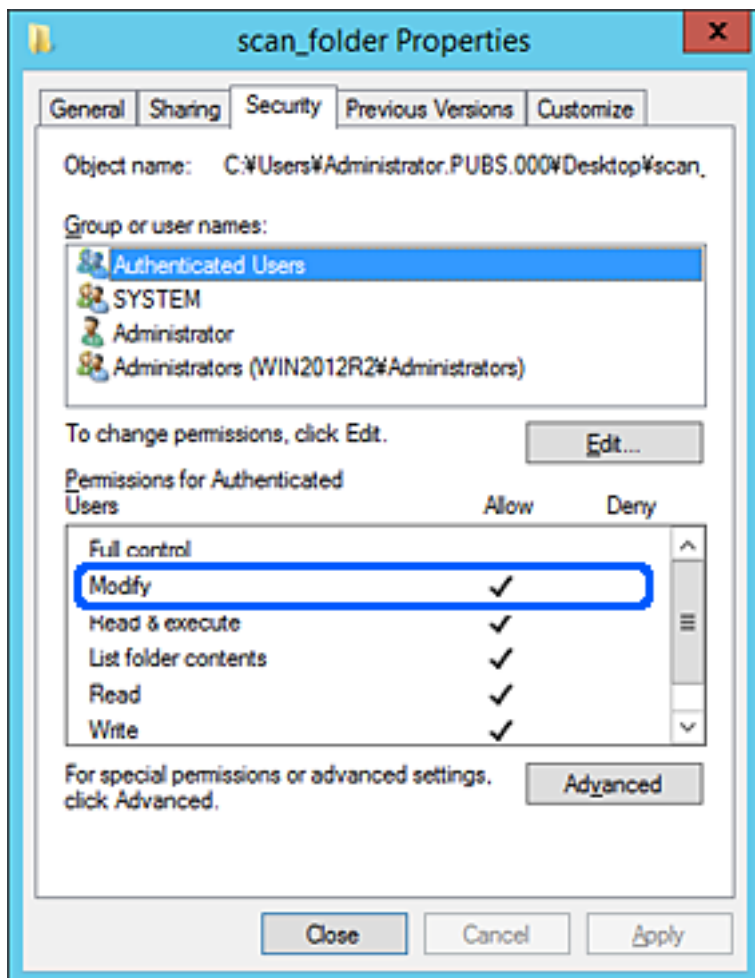


„Utilizatori autentificați” este grupul special care îi include pe toți utilizatorii care se pot conecta la domeniu sau la computer. Acest grup este afișat numai atunci când folderul este creat imediat sub folderul rădăcină.

Dacă nu este afișat, îl puteți adăuga făcând clic pe **Editare**. Pentru mai multe detalii, consultați Informații conexe.

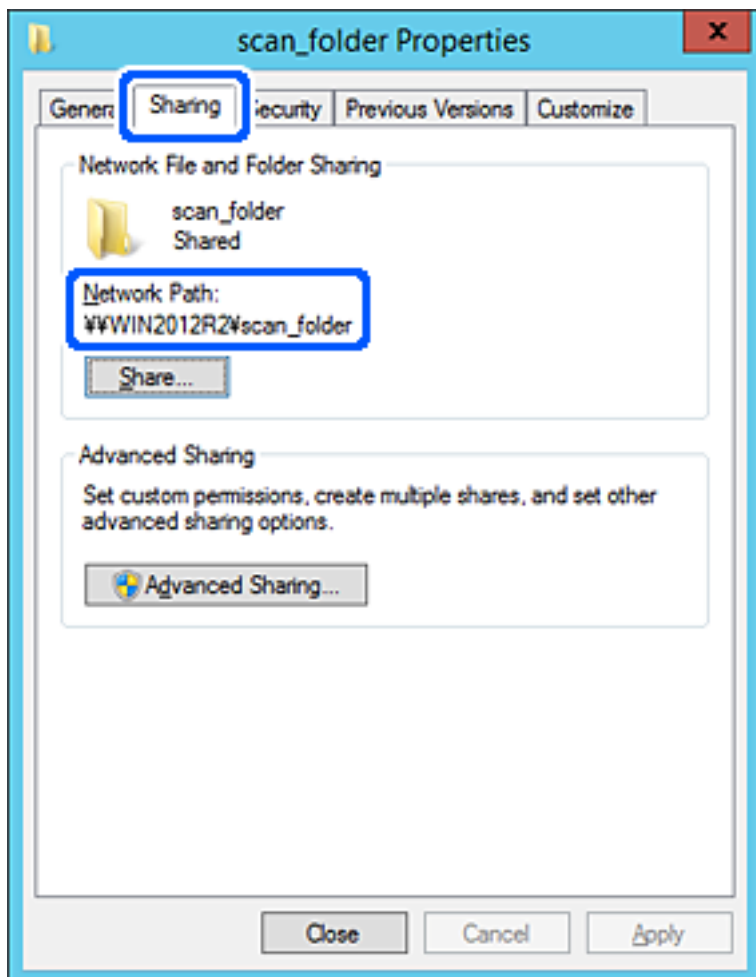
10. Verificați dacă opțiunea **Se permite** pentru **Modificare** este selectată în **Permisuni pentru utilizatori autentificați**.

Dacă nu este selectată, selectați **Utilizatori autentificați**, faceți clic pe **Editare**, selectați **Se permite** pentru **Modificare** în **Permisuni pentru utilizatori autentificați**, apoi faceți clic pe **OK**.



11. Selectați fila **Partajare**.

Este afișată calea de rețea a folderului partajat. Aceasta este utilizată la înregistrarea în contactele scannerului. Vă rugăm să o notați.



12. Faceți clic pe **OK** sau pe **Închidere** pentru a închide ecranul.

Verificați dacă fișierul permite scrierea sau citirea în folderul partajat de la computerele din același domeniu.

Informații conexe

- ➔ „Adăugarea unui grup sau utilizator care permite accesul” la pagina 59
- ➔ „Înregistrarea unei destinații în Contacte utilizând Web Config” la pagina 64

Exemplu de configurare pentru un computer personal

Această explicație este un exemplu de creare a folderului partajat pe desktopul utilizatorului care se conectează curent la computer.

Utilizatorul care se conectează la computer și care deține autoritate de administrator poate accesa folderul desktop și folderul document care se află sub folderul Utilizator.

Setați această configurație atunci când NU doriți să permiteți unui alt utilizator să citească și să scrie în folderul partajat de la un computer personal.

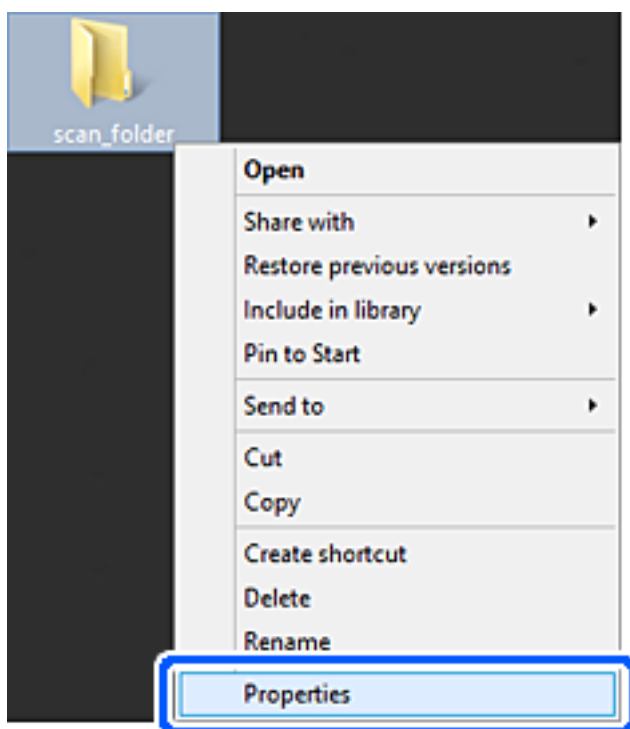
- Locație pentru crearea folderului partajat: Desktop

- Cale folder: C:\Users\xxxx\Desktop\scan_folder
- Permisuni de acces prin intermediul rețelei (Partajare permisiuni): Toți
- Permisuni de acces la sistemul de fișiere (Securitate): Nu adăugați sau adăugați nume de utilizator/grup pentru a permite accesul

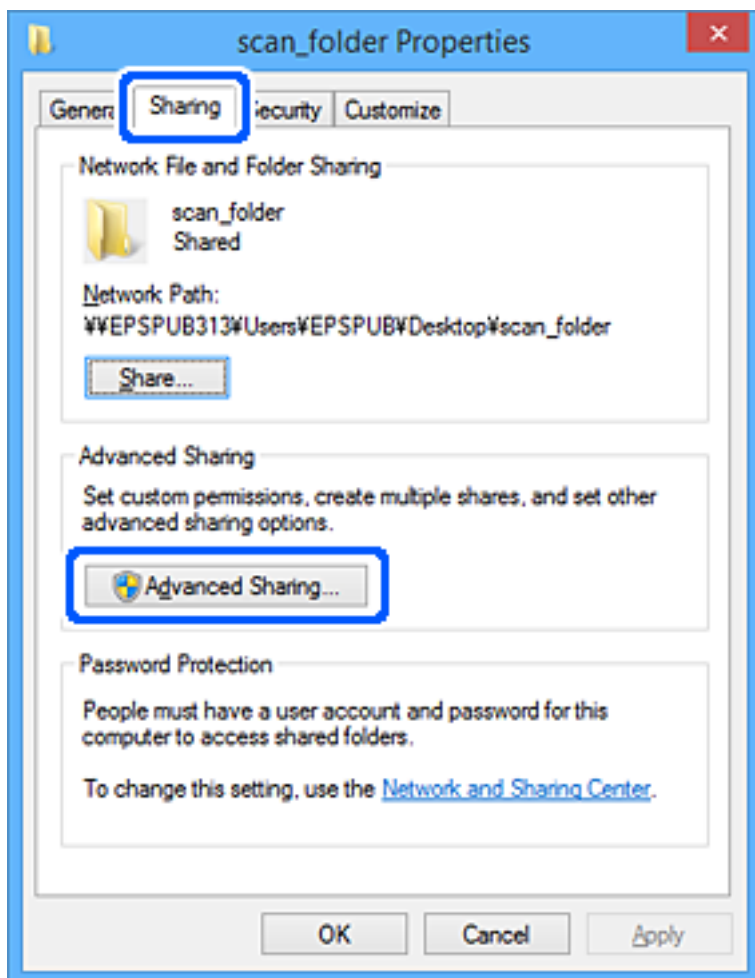
1. Conectați-vă la computerul unde contul de utilizator cu autoritate de administrator va crea folderul partajat.
2. Porniți Explorer.
3. Creați folderul pe desktop și denumiți-l „scan_folder”.

Pentru numele folderului, introduceți între 1 și 12 caractere alfanumerice. Dacă se depășește limita de caractere a numelui folderului, este posibil să nu îl puteți accesa normal, în funcție de diferențele dintre medii.

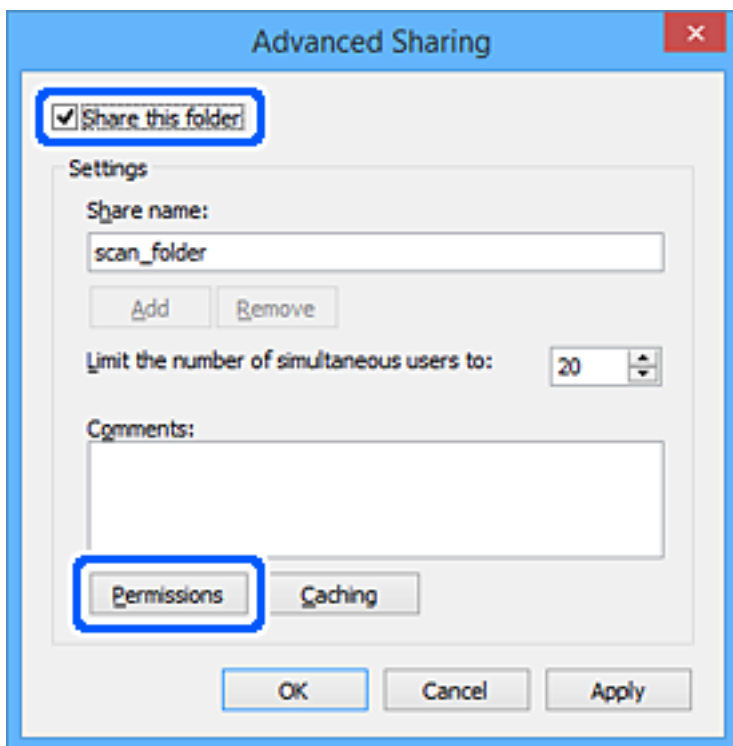
4. Faceți clic dreapta pe folder și selectați **Proprietăți**.



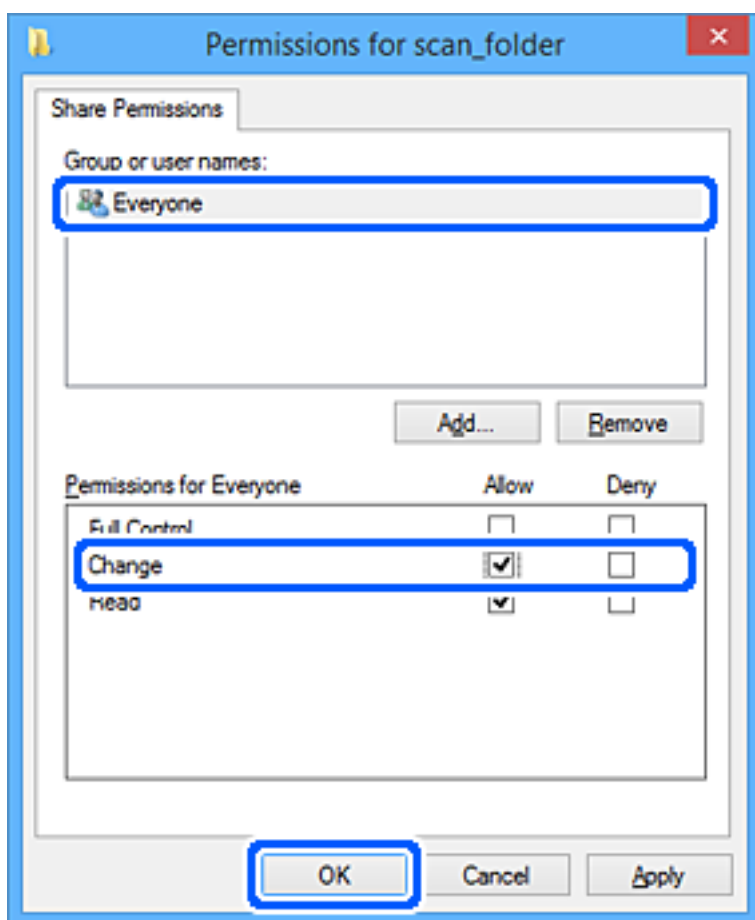
5. Faceți clic pe **Partajare complexă** în fila **Partajare**.



6. Selectați **Partajați acest folder**, apoi faceți clic pe **Permișiuni**.

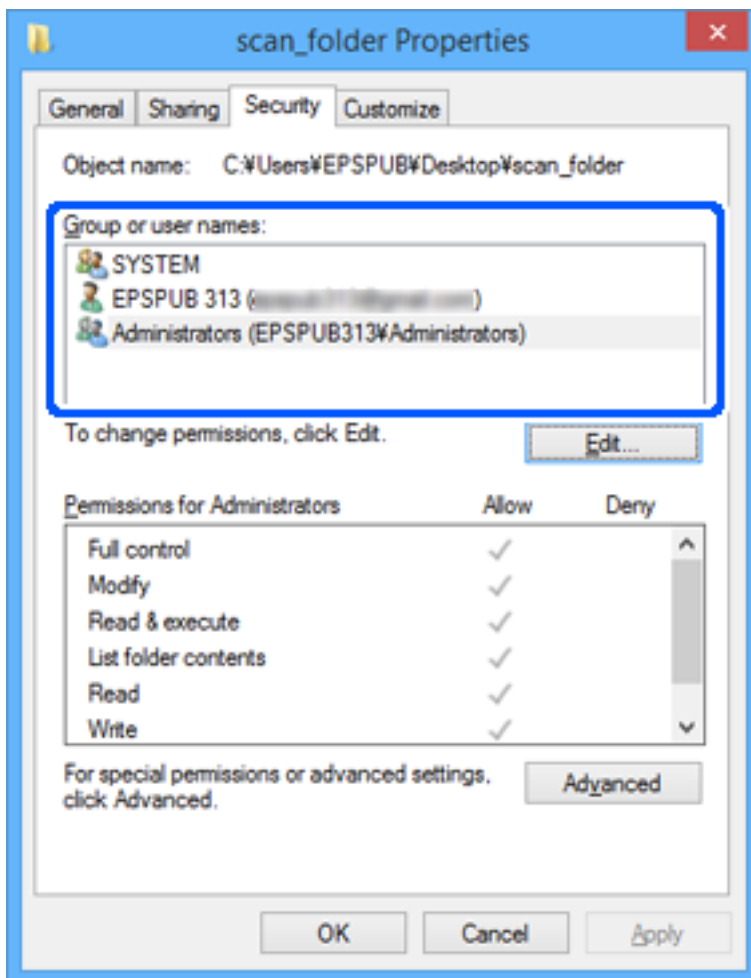


7. Selectați grupul **Toți** din **Nume de grup sau de utilizator**, selectați **Se permite** la **Modificare** și faceți clic pe **OK**.



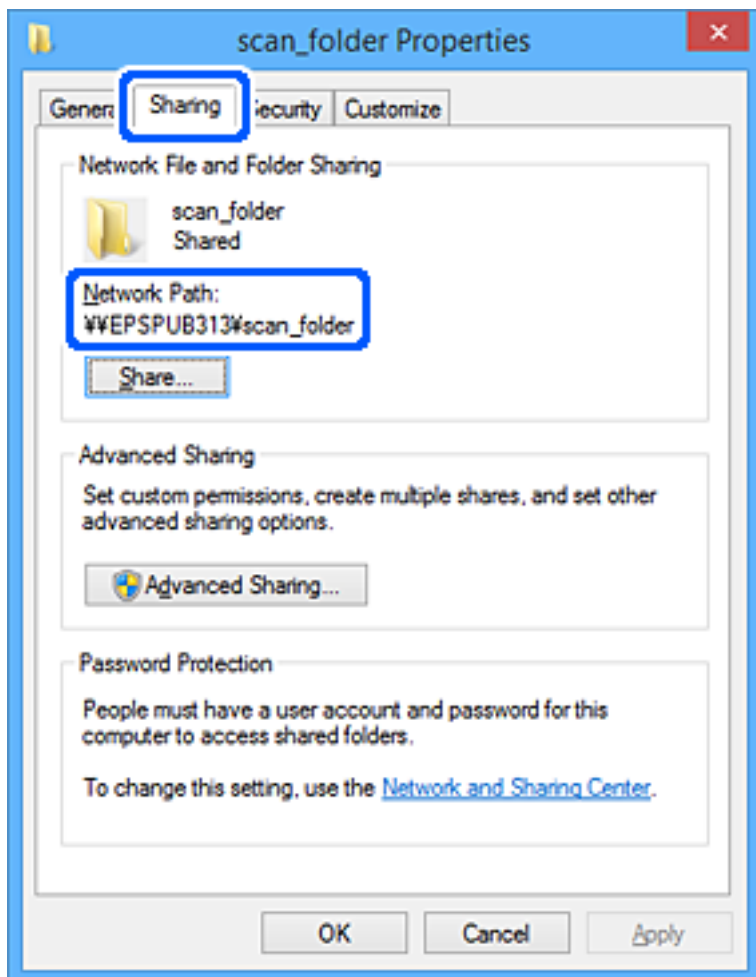
8. Faceți clic pe **OK**.
9. Selectați fila **Securitate**.
10. Bifați grupul sau utilizatorul din **Nume de grup sau de utilizator**.
Grupul sau utilizatorul afișat aici poate accesa folderul partajat.
În acest caz, utilizatorul care se conectează la acest computer și administratorul pot accesa folderul partajat.

Adăugați permisiunea de acces, dacă este necesar. O puteți adăuga făcând clic pe **Editare**. Pentru mai multe detalii, consultați Informații conexe.



11. Selectați fila **Partajare**.

Este afișată calea de rețea a folderului partajat. Aceasta este utilizată la înregistrarea în contactele scannerului. Vă rugăm să o notați.



12. Faceți clic pe **OK** sau pe **Închidere** pentru a închide ecranul.

Verificați dacă fișierul permite scrierea sau citirea în folderul partajat de la computerele utilizatorilor sau ale grupurilor cu permisiune de acces.

Informații conexe

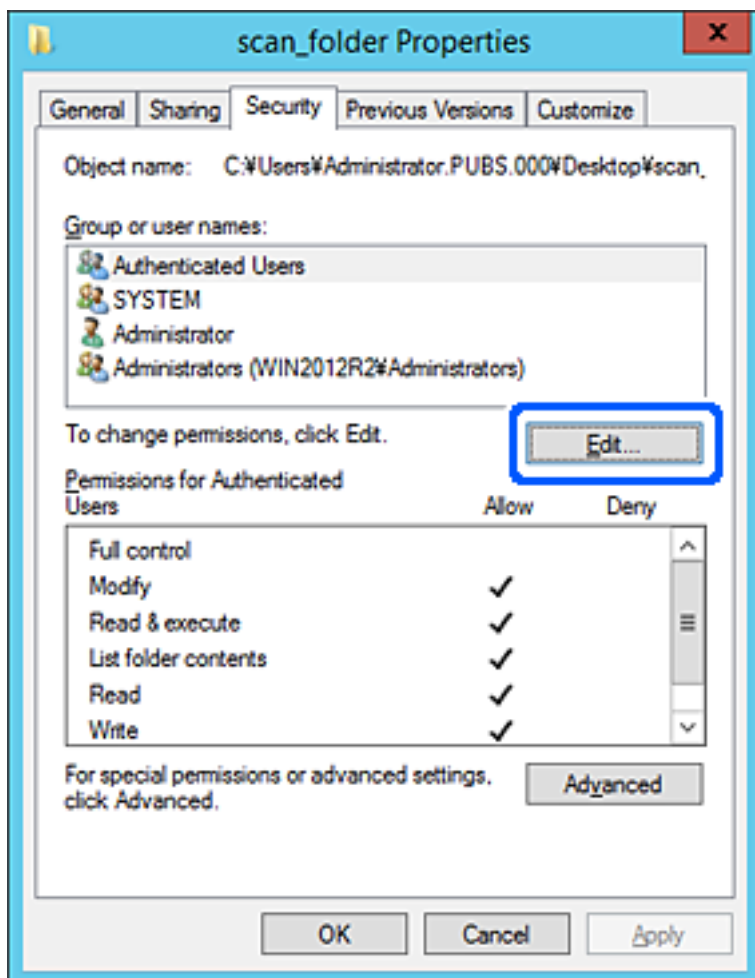
- ➔ „Adăugarea unui grup sau utilizator care permite accesul” la pagina 59
- ➔ „Înregistrarea unei destinații în Contacte utilizând Web Config” la pagina 64

Adăugarea unui grup sau utilizator care permite accesul

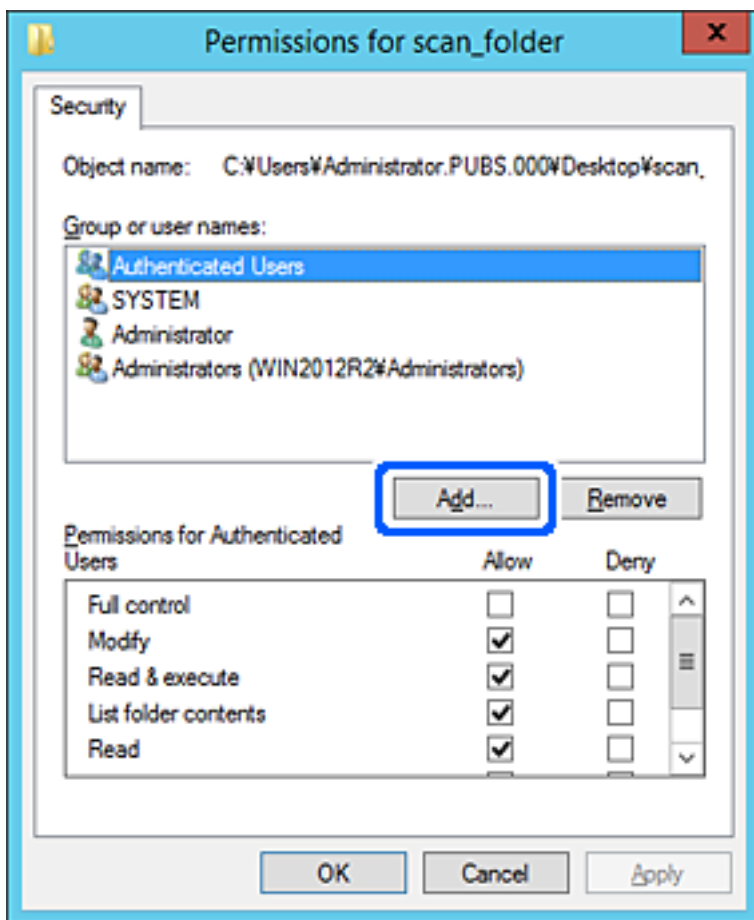
Puteți adăuga grupul sau utilizatorul care permite accesul.

1. Faceți clic dreapta pe folder și selectați **Proprietăți**.
2. Selectați fila **Securitate**.

3. Faceți clic pe **Editare**.



4. Faceți clic pe **Adăugare** sub **Nume utilizator sau grup**.



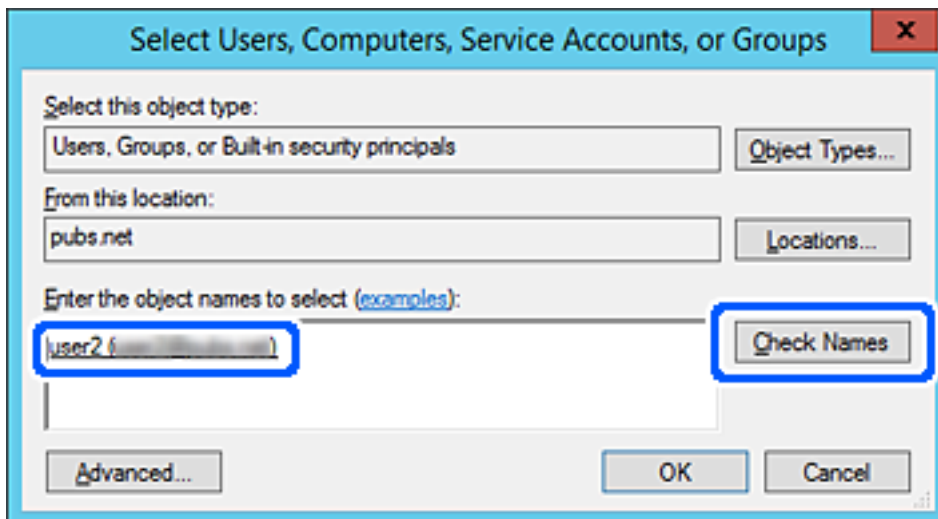
5. Introduceți numele de grup sau de utilizator căruia doriți să îi permiteți accesul, apoi faceți clic pe **Verificare nume**.

La nume este adăugată o linie de subliniere.

Notă:

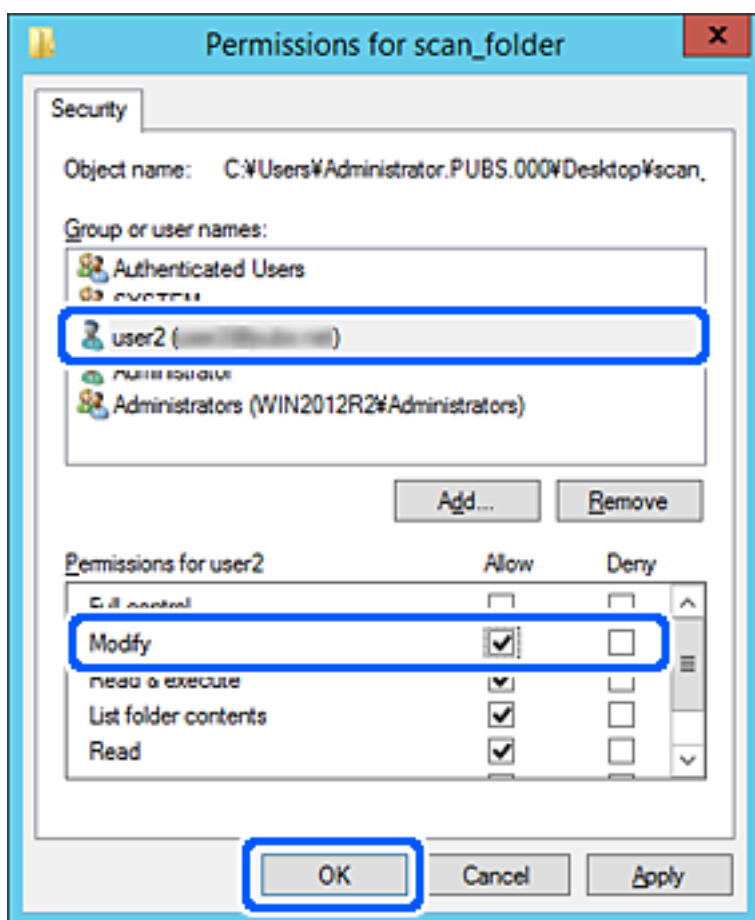
Dacă nu cunoașteți numele complet al grupului sau al utilizatorului, introduceți o parte a numelui, apoi faceți clic pe **Verificare nume**. Sunt enumerate numele de grupuri sau de utilizatori care corespund unei părți a numelui, iar apoi puteți selecta numele complet din listă.

Dacă se potrivește un singur nume, numele complet cu linia de subliniere este afișat în **Introducere nume obiect de selectat**.



6. Executați clic pe **OK**.

- În ecranul Permisuni, selectați numele de utilizator introdus în **Nume utilizator sau grup**, selectați permisiunea de acces la **Modificare** și faceți clic pe **OK**.



- Faceți clic pe **OK** sau pe **Închidere** pentru a închide ecranul.

Verificați dacă fișierul permite scrierea sau citirea în folderul partajat de la computerele utilizatorilor sau ale grupurilor cu permisiune de acces.

Disponibilitatea contactelor

Înregistrarea destinațiilor în lista de contacte a scannerului 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 70

Comparare configurare contacte

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

Caracteristici	Web Config*	Epson Device Admin	Panoul de comandă al scannerului
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 scannerului.

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

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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-8). Dacă nu specificați acest element, lăsați-l necompletat.
Termen index	Introduceți un nume folosind 30 de caractere sau mai puține în Unicode (UTF-8) pentru a căuta în contactele de pe panoul de comandă al scannerului. 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-8), omițând „\”. Introduceți calea de rețea afișată pe ecranul de proprietăți al folderului. Consultați următoarele pentru detalii despre setarea căii de rețea. „Exemplu de configurare pentru un computer personal” la pagina 53
Nume utilizator	Introduceți un nume de utilizator pentru accesarea folderului din rețea cu 30 de caractere sau mai puține în format Unicode (UTF-8). Cu toate acestea, evitați să folosiți caractere de control (de la 0x00 la 0x1F, 0x7F).
Parolă	Introduceți o parolă pentru accesarea folderului din rețea cu 20 de caractere sau mai puțin în format Unicode (UTF-8). Cu toate acestea, 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 scannerului să comunice cu măsuri de securitate.
Salvare în	Introduceți numele serverului între 1 și 253 de caractere în ASCII (0x20 – 0x7E), 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-8). Cu toate acestea, 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, din 20 de caractere sau mai puțin, în format Unicode (UTF-8). Cu toate acestea, 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 scanner 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 scanner.
SharePoint(WebDAV)	
Conexiune securizată	Selectați HTTP sau HTTPS în funcție de protocolul de transfer de fișiere acceptat de server. Selectați HTTPS pentru a permite scannerului să comunice cu măsuri de securitate.
Salvare în	Introduceți numele serverului, între 1 și 253 de caractere ASCII (0x20 – 0x7E), 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-8). Cu toate acestea, 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, din 20 de caractere sau mai puțin, în format Unicode (UTF-8). Cu toate acestea, 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 scanner.
Server proxy	Selectați dacă veți utiliza sau nu un server proxy.

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** și **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

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

Copierea de rezervă și importul contactelor

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

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

Când importați setările scannerului la scanner, 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 și le puteți importa, deoarece acestea pot fi salvate ca fișier SYLK sau CSV.

Importarea contactelor cu Web Config

Dacă aveți un scanner care vă permite să realizați o copie de rezervă a contactelor și este compatibil cu acest scanner, puteți înregistra cu ușurință contactele prin importarea fișierului de rezervă.

Notă:

Pentru instrucțiuni privind modul de realizare a copiilor de rezervă pentru contactele scannerului, consultați manualul furnizat cu scannerul.

Urmați pașii de mai jos pentru a importa contactele în acest scanner.

1. Accesați Web Config, selectați fila **Gestionare dispozitiv > Valoare de setare export și import > Import**.
2. Selectați fișierul de rezervă pe care l-ați creat în **Fișier**, introduceți parola și faceți clic pe **Înainte**.
3. Selectați caseta de validare **Persoane de contact** și 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 scannerului. Vă recomandăm să realizați copii de siguranță ale datelor după fiecare actualizare a acestora. Epson nu își asumă responsabilitatea pentru pierderea datelor, pentru copierea de rezervă sau recuperarea datelor și/sau a setărilor, nici chiar în perioada de garanție.

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

1. Accesați Web Config și apoi selectați fila **Gestionare dispozitiv > Valoare de setare export și 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 și înregistrarea în masă a contactelor cu ajutorul unui instrument

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

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

Exportul contactelor

Salvați informațiile contactelor în fișier.

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 ștergerea sau adăugarea informațiilor.

Informații care includ elemente de securitate, precum parola și informațiile personale, pot fi salvate în format binar cu o parolă. Nu puteți edita fișierul. Acesta poate fi utilizat ca fișier 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 și faceți clic pe **OK**.
5. Faceți clic pe **Common > Contacts**.
6. Selectați formatul de export din **Export > Export items**.
 - All Items
Exportați fișierul binar criptat. Selectați când doriți să includeți elemente de securitate precum parola și informațiile personale. Nu puteți edita fișierul. Dacă îl selectați, trebuie să setați parola. Faceți clic pe **Configuration** și setați o parolă ASCII între 8 și 63 de caractere lungime. Această parolă este necesară la importul fișierului binar.
 - Items except Security Information
Exportați fișierele în format SYLK sau csv. Selectați atunci când doriți să editați informațiile fișierului 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 scanner.
13. În ecranul de finalizare a trimiterii, faceți clic pe **OK**.
Informațiile scannerului sunt actualizate.
Deschideți contactele din Web Config sau de la panoul de comandă al scannerului 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 scanner.

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 scannerul 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 scanner.
Expirare căutare (sec.)	Setați intervalul de timp de căutare înainte de apariția expirării între 5 și 300.

Elemente	Setări și explicație
Metodă de autentificare	<p>Selecționați una dintre metode.</p> <p>Dacă selecționați Autentificare Kerberos, selecționați Setări Kerberos pentru a face setări pentru Kerberos.</p> <p>Pentru a efectua Autentificare Kerberos, următorul mediu este obligatoriu.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Scanerul și serverul DNS pot comunica. <input type="checkbox"/> Ora scanerului, a serverului KDC și a serverului necesar pentru autentificare (server LDAP, server SMTP, server de fișiere) sunt sincronizate. <input type="checkbox"/> 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 selecționați Autentificare Kerberos pentru Metodă de autentificare , selecționați domeniul Kerberos pe care doriți să îl utilizați.
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 selecționați **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 selecționați fila **Rețea > Server LDAP > Setări căutare**.
2. Introduceți o valoare pentru fiecare element.

- 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
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**.

- Accesați Web Config și selectați fila **Rețea > Server LDAP > Test conexiune**.

- 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.

Mesaje	Explicație
Testarea conexiunii a eșuat. Verificați setările.	Acest mesaj apare din următoarele motive: <ul style="list-style-type: none"> <input type="checkbox"/> Adresa serverului LDAP este incorectă sau numărul de port este incorect. <input type="checkbox"/> Un interval de timp a expirat. <input type="checkbox"/> Opțiunea A nu se folosi este selectată ca Utilizare server LDAP. <input type="checkbox"/> Dacă Autentificare Kerberos este selectată ca Metodă de autentificare, setări precum Domeniu, Adresă KDC și Număr port (Kerberos) sunt incorecte.
Testarea conexiunii a eșuat. Verificați data și ora pe produsul dvs. sau pe server.	Acest mesaj apare când conexiunea eșuează deoarece setările de oră pentru scaner și pentru serverul LDAP nu corespund.
Autentificarea a eșuat. Verificați setările.	Acest mesaj apare din următoarele motive: <ul style="list-style-type: none"> <input type="checkbox"/> Nume utilizator și/sau Parolă sunt incorecte. <input type="checkbox"/> 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 scenerul este ocupat.

Utilizare Document Capture Pro Server

Utilizând Document Capture Pro Server, puteți gestiona metoda de sortare, formatul de salvare și destinația de redirecționare a unui rezultat de scanare executat de la panoul de control al scannerului. Puteți accesa și executa o operațiune înregistrată anterior pe server, de la panoul de control al scannerului.

Instalați-o pe computerul server.

Pentru mai multe informații despre Document Capture Pro Server, contactați biroul Epson local.

Setarea modului server

Pentru utilizarea Document Capture Pro Server, efectuați configurarea în modul următor.

1. Accesați Web Config și selectați fila **Scanare > Document Capture Pro**.
2. Selectați **Mod server** pentru **Mod**.
3. Introduceți adresa serverului cu Document Capture Pro Server instalat pe el pentru **Adresă server**.
Introduceți între 2 și 255 de caractere în format IPv4, IPv6, numele gazdei sau FQDN. Pentru formatul FQDN, puteți folosi caractere alfanumerice în ASCII (0x20 – 0x7E) și „-”, exceptând începutul și sfârșitul adresei.
4. Faceți clic pe **OK**.
Rețeaua este reconectată și apoi setările sunt activate.

Configurarea 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) și până la 41 de caractere.
Locație Bonjour	Introduceți o descriere a locației scannerului, folosind text Unicode (UTF-8) și până la 127 de octeți.
Wide-Area Bonjour	Stabiliți dacă se utilizează sau nu Wide-Area Bonjour. Dacă se utilizează, scannerul trebuie să fie înregistrat pe serverul DNS pentru a căuta scannerul în segment.
Activare AirPrint	Bonjour și AirPrint (serviciu de scanare) sunt activate.

Probleme la pregătirea scanării în rețea

Sugestii pentru remediarea problemelor

Verificarea mesajului de eroare

Dacă apar probleme, verificați mai întâi dacă există mesaje pe panoul de comandă al scannerului 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 și ipconfig.

Test de conexiune

Pentru verificarea conexiunii dintre scanner și serverul de e-mail, efectuați testul de conexiune de la scanner. De asemenea, verificați conexiunea de la computerul client la server, pentru a stabili starea comunicațiilor.

Inițializarea setărilor

Dacă setările și starea comunicației nu prezintă probleme, problemele pot fi remediate prin dezactivarea sau inițializarea setărilor de rețea ale scannerului, urmate de reconfigurare.

Imposibilitate de accesare Web Config

Adresa IP nu este alocată scannerului.

Soluții

O adresă IP validă nu poate fi alocată scannerului. Configurați adresa IP folosind panoul de comandă al scannerului. Puteți confirma informațiile privind setarea actuală din panoul de comandă al scannerului.

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

Soluții

SSL/TLS are o forță de criptare. Puteți deschide Web Config utilizând un browser web care acceptă criptări în masă, în modul indicat mai jos. Verificați dacă utilizați 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.

Soluții

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

Numele comun al certificatului și al scannerului nu concordă.

Soluții

Dacă numele comun al certificatului și al scannerului nu concordă, se afișează mesajul „Numele certificatului de securitate nu se potrivește...” la accesarea Web Config utilizând comunicația SSL/TLS (https). Aceasta se întâmplă deoarece următoarele adrese IP nu corespund.

- Adresa IP a scannerului 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, actualizați certificatul.

Pentru Certificat semnat de CA, obțineți din nou certificatul pentru scanner.

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

Soluții

Când scannerul 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 > 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

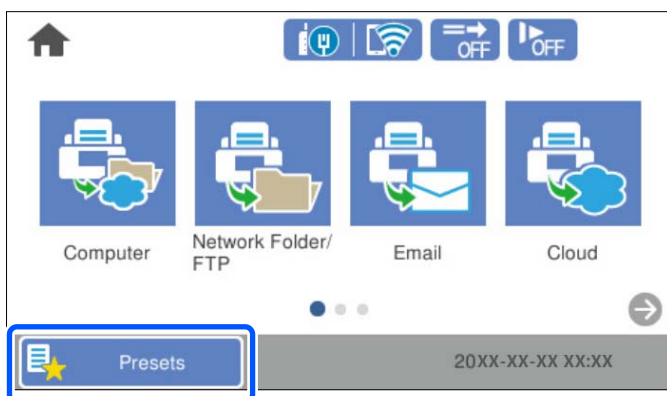
Înregistrarea Presetări.	78
Editarea ecranului principal al panoului de comandă.	80

Înregistrarea Presetări

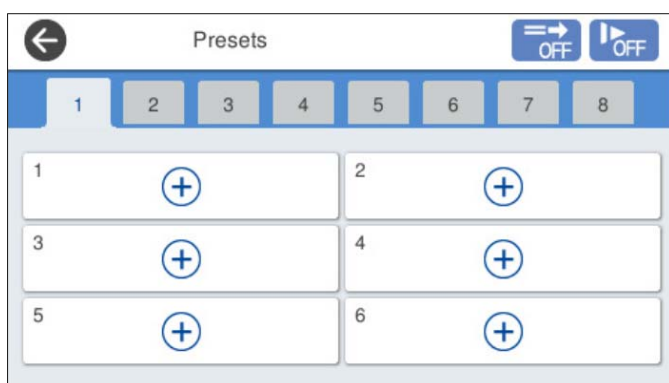
Puteți înregistra setările de scanare frecvent utilizate ca **Presetări**. Puteți înregistra până la 48 de presetări.

Notă:

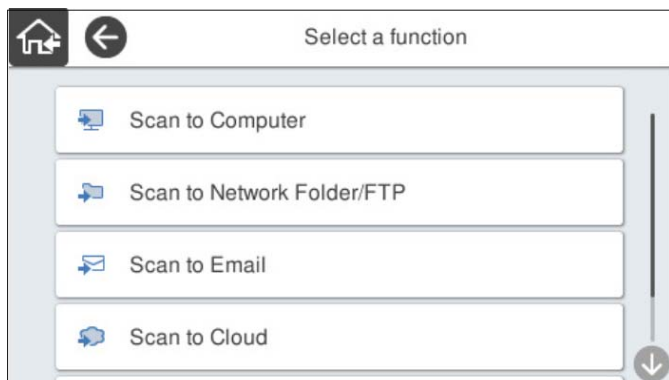
- Puteți înregistra setările curente selectând  pe ecranul de începere a scanării.
 - Puteți înregistra **Presetări** și în Web Config.
 Selectați fila **Scanare** > **Presetări**.
 - Dacă selectați **Scanare către computer** la înregistrare, puteți înregistra lucrarea creată în Document Capture Pro 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 scannerului.



2. Selectați .



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



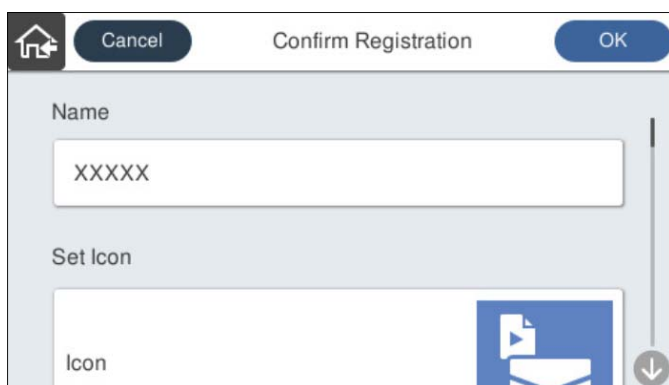
4. Setați fiecare element și selectați .

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.
Când utilizați Document Capture Pro Server, chiar dacă setați software-ul pentru a confirma conținutul unei lucrări înainte de scanare, **Setări trimitere rapidă** a presetării scannerului are prioritate față de software.
- 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 scannerului.

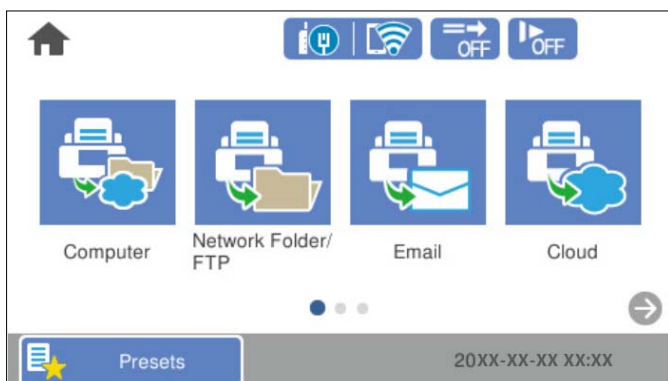
- Aspect: modifică metoda de afișare a pictogramelor de meniu.
[„Modificarea parametrului Aspect al ecranului principal” la pagina 80](#)
- Adăugare pictogramă: adaugă pictograme la setările **Presetări** pe care le-ați stabilit sau restabilește pictogramele șterse de pe ecran.
[„Adăugare pictogramă” la pagina 81](#)
- Ștergere pictogramă: elimină pictogramele de pe ecranul principal.
[„Ștergere pictogramă” la pagina 82](#)
- Mutare pictogramă: modifică ordinea de afișare a pictogramelor.
[„Mutare pictogramă” la pagina 83](#)
- Restaur. afișare pictograme implicite: restabilește setările implicite de afișare pentru ecranul principal.
- Tapet: schimbați culoarea de fundal a ecranului principal.

Modificarea parametrului Aspect al ecranului principal

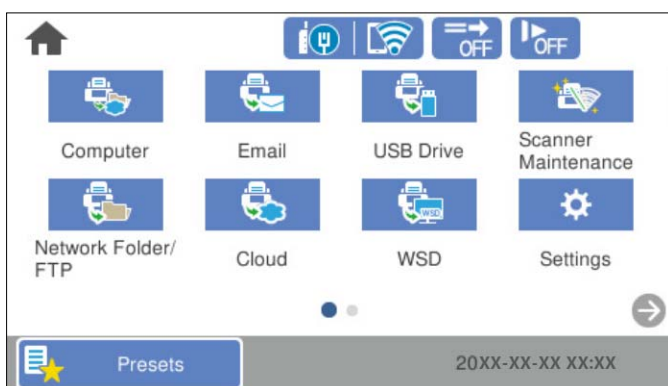
1. Selectați **Setări > Editare ecran principal > Aspect** pe panoul de comandă al scannerului.


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

Linie:



Matrice:

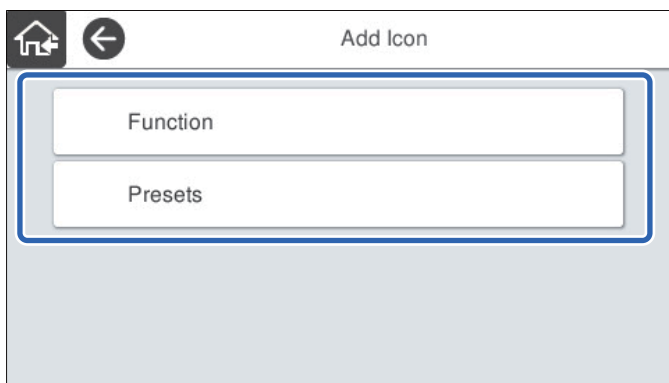


3. Selectați  pentru a reveni și a consulta ecranul principal.

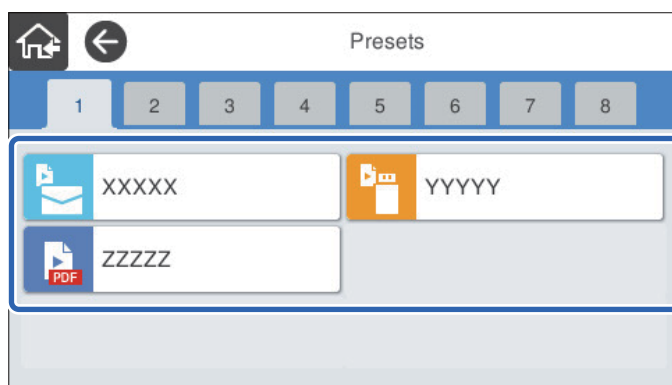
Adăugare pictogramă

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

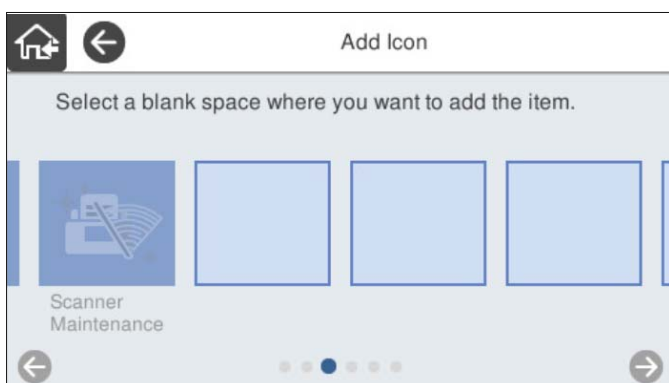
- ❑ Presetări: afișează presetările înregistrate.




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.

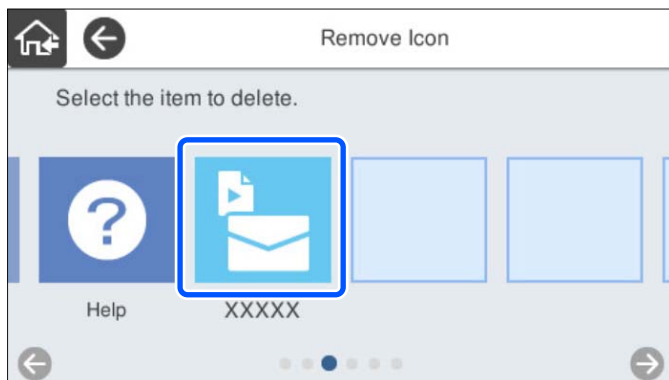



5. Selectați  pentru a reveni și a consulta ecranul principal.

Ștergere pictogramă

1. Selectați **Setări** > **Editare ecran principal** > **Ștergere pictogramă** pe panoul de comandă al scannerului.

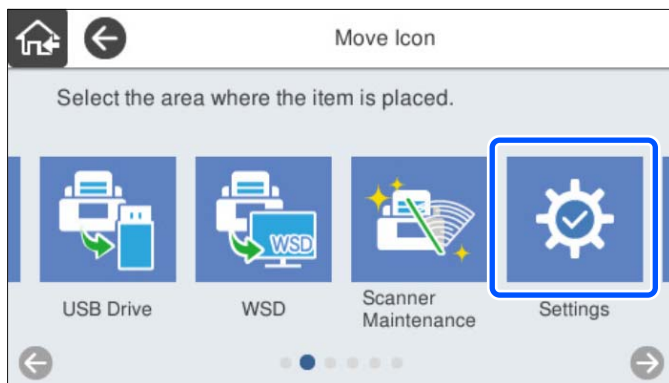
2. Selectați pictograma pe care doriți să o eliminați.



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.

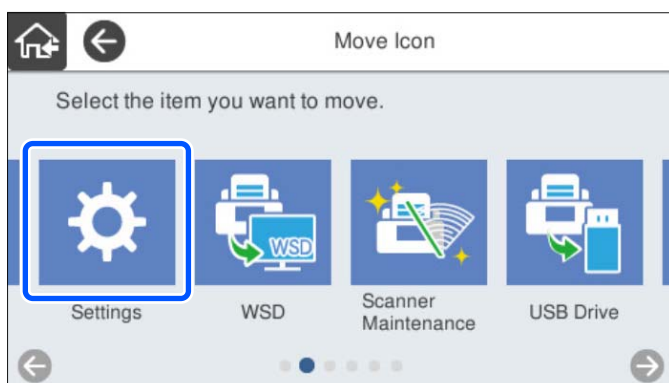
Mutare pictogramă


1. Selectați **Setări** > **Editare ecran principal** > **Mutare pictogramă** pe panoul de comandă al scannerului.
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 caracteristicilor de securitate ale produsului.	86
Setări administrative.	86
Dezactivarea Interfeței externe.	92
Monitorizarea unui scaner la distanță.	93
Rezolvarea problemelor.	95

Introducerea caracteristicilor de securitate ale produsului

Această secțiune introduce funcția de securitate a dispozitivelor Epson.

Denumirea caracteristicii	Tipul caracteristicii	Ce să setați	Ce să preveniți
Configurare pentru parola 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 scannerului.	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.
Configurație pentru interfața 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 86
- ➔ „Dezactivarea Interfeței externe” la pagina 92

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)
- Parolă: numărul de serie al scannerului

Pentru a găsi numărul de serie, verificați eticheta atașată în partea din spate a scannerului.

Puteți modifica parola de administrator prin Web Config, panoul de comandă al scannerului 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**.

Introduceți cel puțin un caracter pentru noua parolă.

Notă:

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

Nume utilizator: niciunul (gol)

Parolă: numărul de serie al scannerului

Pentru a găsi numărul de serie, verificați eticheta atașată în partea din spate a scannerului.



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

➔ [„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)

Modificarea parolei de administrator de la panoul de comandă

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

1. Selectați **Setări** pe panoul de comandă al scannerului.
2. Selectați **Administrare sistem > Setări administrator**.
3. Selectați **Parolă administrator > Schimbare**.

4. Introduceți parola curentă.

Notă:

Setarea în momentul achiziției (valoarea implicită) pentru parola de administrator este numărul de serie al scannerului.

Pentru a găsi numărul de serie, verificați eticheta atașată în partea din spate a scannerului.

5. Introduceți noua parolă.
Introduceți cel puțin un caracter.

 **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.

Notă:

Dacă activați Setări de autentificare pe scanner, Setare blocare este activată și pentru panoul de comandă. Panoul de comandă nu poate fi deblocat atunci când Setări de autentificare sunt activate.

Chiar dacă dezactivați Setări de autentificare, Setare blocare rămâne activată. Dacă doriți să o dezactivați, puteți face setări din panoul de comandă sau din Web Config.

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

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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	✓
	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	✓
	Pornire directă	✓
Setări scanner		-
	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		✓

Meniul Setări		Setare blocare
	Aspect	✓
	Adăugare pictogramă	✓
	Ștergere pictogramă	✓
	Mutare pictogramă	✓
	Restaur. afișare pictograme implicite	✓
	Tapet	✓
Setări utilizator		✓
	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/Ștergere	✓/!*
	Frecvent	-
	Vizualizare opțiuni	-
	Opțiuni de căutare	-
Administrare sistem		✓


Meniul Setări		Setare blocare
	Administrator Contacte	✓
	Setări administrator	✓
	Restricții	✓
	Criptare cu parolă	✓
	Cercetare clienți	✓
	Setări WSD	✓
	Restaurare setări implicite	✓
	Actualizare firmware	✓
Informații dispozitiv		-
	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	-
	Resetați numărul de scanări	✓
Întreținere scanner		-
	Curățare role	-
	Înlocuire rolă de întreținere	-
	Resetați numărul de scanări	✓
	Cum se înlocuiește	-
	Curățare obișnuită	-
	Resetați numărul de scanări	✓
	Curățarea	-
	Curățare Geam	-
Setarea alertei de înlocuire a roților		✓
	Setare alertă contor	✓
Setări alerte curățare periodică		✓


Meniul Setări		Setare blocare
	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

Puteți utiliza oricare dintre următoarele metode pentru a vă conecta ca administrator de la panoul de comandă al scannerului.

1. Atingeți  în partea dreaptă sus a ecranului.
 - Când se activează Setări de autentificare, pictograma este afișată pe ecranul **Bun venit** (ecranul de așteptare a autentificării).
 - Când se dezactivează Setări de autentificare, pictograma este afișată pe ecranul principal.
2. Atingeți **Da** când este afișat ecranul de confirmare.
3. Introduceți parola administratorului.
Este afișat un mesaj de conectare completă, apoi este afișat ecranul principal pe panoul de comandă.

Pentru a vă deconecta, atingeți  în partea dreaptă sus a ecranului principal.

Dezactivarea Interfeței externe

Puteți dezactiva interfața folosită pentru a conecta dispozitivul la scanner. 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 scannerului.

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

Dacă driverul nu a fost instalat pe computer

Windows:

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

Mac OS:

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

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

Monitorizarea unui scanner la distanță

Verificarea informațiilor pentru un scanner la distanță

Puteți verifica următoarele informații ale scannerului 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 scannerului.

Instantaneu panou

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

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 scanner, 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

➔ „Configurarea unui server de e-mail” la pagina 42

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

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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 scanner	Notă atunci când apare o eroare a scannerului.
Eroare Wi-Fi	Notificare când s-a produs o eroare la interfața LAN wireless.

Rezolvarea problemelor

Parolă de administrator uitată

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

Notă:

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

- Nume utilizator: niciunul (gol)*
- Parolă: numărul de serie al scannerului*

Pentru a găsi numărul de serie, verificați eticheta atașată în partea din spate a scannerului. Dacă restaurați setările implicite pentru parola de administrator, aceasta va fi resetată la valorile inițiale.

Setări de securitate avansate

Setări de securitate și de prevenire a pericolelor.	97
Controlarea utilizând protocoale.	98
Utilizarea unui certificat digital.	101
Comunicare SSL/TLS cu scannerul.	106
Comunicare criptată utilizând filtrarea IPsec/IP.	108
Conectarea scannerului la o rețea IEEE802.1X.	119
Rezolvarea problemelor pentru securitate avansată.	120

Setări de securitate și de prevenire a pericolelor

Atunci când un scanner este conectat la o rețea, îl puteți accesa dintr-o locație aflată la distanță. În plus, mai multe persoane pot partaja scannerul, 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 scannerul într-un mediu unde puteți accesa internetul, riscurile sunt chiar mai mari.

Pentru scanerile 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, scanerile Epson dispun de o varietate de tehnologii de securitate.

Setați scannerul 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 scanner, 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 scanner.	Identificarea scannerului 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 scannerul.	Protejați împotriva accesului neautorizat, a manipulării frauduloase a datelor și a interceptării datelor de comunicații la scanner.
IEEE 802.1X	Permite doar utilizatorilor autentificați să se conecteze la rețea. Permite utilizarea scannerului doar de către un utilizator autentificat.	Setare de autentificare la serverul RADIUS (server de autentificare).	Protejați împotriva accesării și utilizării neautorizate a scannerului.

Informații conexe

- ➔ „Controlarea utilizând protocoale” la pagina 98
- ➔ „Comunicare SSL/TLS cu scannerul” la pagina 106
- ➔ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 108
- ➔ „Conectarea scannerului la o rețea IEEE802.1X” la pagina 119

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 scanner.

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 scannerului.

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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 și 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 și 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. Scannerul 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/Sciere .
Nume comunitate (Numai citire)	Introduceți între 0 și 32 de caractere ASCII (între 0x20 și 0x7E).
Nume comunitate (Citire/Sciere)	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 scannerului 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 scannerului la accesarea serverului celeilalte părți sau a Web Config.

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

Puteți obține certificatul CA al scannerului 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 scannerul 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 101](#)

➔ [„Actualizarea unui certificat autosemnat” la pagina 105](#)

➔ [„Configurarea unui Certificat CA” la pagina 105](#)

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 scanner.

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

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

Elemente setare CSR

Elemente	Setări și explicație
Lungime cheie	Selectați o lungime de cheie pentru o CSR.

Elemente	Setări și explicație
Nume comun	<p>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.</p> <p>Primul element este stocat în numele comun, iar celelalte elemente sunt stocate în câmpul alias al subiectului certificatului.</p> <p>Exemplu:</p> <p>Adresa IP a scannerului: 192.0.2.123, Nume scanner: EPSONA1B2C3</p> <p>Nume comun: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123</p>
Organizație/ Unitate organizatorică/ Localitate/ Stat/Provincie	Puteți introduce între 0 și 64 de caractere în ASCII (0x20 – 0x7E). Puteți separa numele distincte cu virgulă.
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 scanner.



Important:

- Asigurați-vă că data și ora scannerului 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. Setări **Certificat CA 1** și **Certificat CA 2** când verificați calea certificatului în browser-ul web care accesează scannerul.

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 scannerul 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

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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.

Ștergerea 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 **Ștergere**.

3. În mesajul care apare, confirmați faptul că doriți să ștergeți certificatul.

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

Actualizarea unui certificat autosemnat

Deoarece Certificat auto-semnat este emis de către scanner, 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 scannerului: 192.0.2.123, Nume scanner: 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**.

Scannerul 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

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

Configurarea unui Certificat CA

La setarea Certificat CA, puteți valida calea către certificatul CA al serverului pe care îl accesează scannerul. 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 scanner.

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

➔ [„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)

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

➔ [„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)

Comunicare SSL/TLS cu scannerul

Atunci când certificatul de server este stabilit cu ajutorul comunicării SSL/TLS (Standard de securitate în informații/Protocol pentru securitatea transferurilor) cu scannerul, 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 scannerul acceptă funcția de server HTTPS, puteți utiliza o comunicare de tip SSL/TLS pentru criptarea comunicațiilor. Puteți configura și gestiona scannerul utilizând Web Config, asigurând în același timp securitatea acestuia.

Configurați puterea de criptare și funcția de redirectionare.

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**.
Scannerul este actualizat.

Informații conexe

➔ [„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)

Configurarea unui certificat de server pentru scanner

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 scanner. 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**.
Scannerul este actualizat.

Informații conexe

- ➔ [„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)
- ➔ [„Configurarea unui Certificat semnat de CA” la pagina 101](#)
- ➔ [„Configurarea unui Certificat CA” la pagina 105](#)

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 scannerul 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 scanner. 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**.
Scannerul este actualizat.

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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 scannerul.

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 scanner.
	ID	Introduceți ID-ul scannerului 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 scannerului 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 scannerul numai pe același LAN, selectați această opțiune. Pachetele IP de strat 4 sau ulterior sunt criptate.
Mod tunel	Dacă folosiți scannerul 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. Scannerul 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**.
Scannerul 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 scannerul.

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 scanner.
	ID	Introduceți ID-ul scannerului 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 scannerului 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 scannerul numai pe același LAN, selectați această opțiune. Pachetele IP de strat 4 sau ulterior sunt criptate.
Mod tunel	Dacă folosiți scannerul 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 .

Combinatie 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

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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 scanner din aplicații precum Epson Device Admin și un driver de scanner
SNMP	UDP	161	Orice port	Achiziția și configurarea MIB din aplicații precum Epson Device Admin și driverul de scanner 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 scanner

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 și a setărilor scannerului

Acest exemplu permite comunicări ale datelor de scanare și configurației scannerului 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: Permite 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 scannerul.

Politică implicită:

- IPsec/IP Filtering: Activare
- Control acces: Refuzare acces

Politică grup:

- Se activează această Politică grup: Bifați caseta.
- Control acces: Permite acces
- Adresă la distanță (Gazdă): Adresă IP a unui client al administratorului

Notă:

Indiferent de configurarea politicii, clientul va putea accesa și configura scannerul.

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

- ➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36
- ➔ „Configurarea unui Certificat semnat de CA” la pagina 101
- ➔ „Configurarea unui Certificat CA” la pagina 105

Conectarea scannerului la o rețea IEEE802.1X

Configurarea unei rețele IEEE 802.1X

Când setați IEEE 802.1X la scanner, 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 scannerul 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**.
 Scannerul este actualizat.

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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 rețelei curente.	
Tip EAP	Selectați o opțiune pentru o metodă de autentificare între scanner și un server RADIUS. EAP-TLS PEAP-TLS PEAP/MSCHAPv2 EAP-TTLS	Trebuie să obțineți și să importați un certificat CA-semnat (certificat semnat de o autoritate de certificare). Trebuie să configurați parola.
	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).

Elemente	Setări și explicație	
Parolă	Configurați o parolă pentru a autentifica scannerul. 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.	
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	Puteți configura validarea certificatelor indiferent de metoda de autentificare. Importați certificatul în 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

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

➔ [„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)

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

Utilizarea 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

- ➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36
- ➔ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 108

Comunicare imposibilă cu Comunicare IPsec

Specificați algoritmul incompatibil cu scannerul sau cu computerul.

Scannerul 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 108

Înterupere bruscă a comunicării

Adresa IP a scannerului 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 scannerului.

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 (scanner)**) a scannerului 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 scannerului.

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 scannerului nu va fi găsită.

Folosiți o adresă IP statică.

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

➔ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 108

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 scannerului. Conectați scannerul și computerul și refaceți setarea privind filtrarea IPsec/IP.

Informații conexe

➔ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 108

Imposibil de accesat scannerul după configurarea IEEE 802.1X

Setările IEEE 802.1X sunt incorecte.

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

Conectați scannerul și un computer, apoi configurați din nou IEEE 802.1X.

Informații conexe

➔ „Configurarea unei rețele IEEE 802.1X” la pagina 119

Probleme privind utilizarea unui certificat digital

Nu se poate importa un Certificat semnat de CA

Certificat semnat de CA și 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 scanner după trimiterea CSR către o autoritate de certificare?
Obțineți din nou certificatul CA-semnat cu CSR.

Certificat semnat de CA depășește 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 103

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 105

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 și 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 101](#)

Apare o avertizare privind un certificat digital

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

Mesaje	Cauză/Cum să procedați
Fișier nevalid.	<p>Cauză:</p> <p>Se pare că nu importați un fișier de certificat în format X509.</p> <p>Cum să procedați:</p> <p>Asigurați-vă că selectați certificatul corect trimis de o autoritate de certificare de încredere.</p>
	<p>Cauză:</p> <p>Dimensiunea fișierului pe care l-ați importat este prea mare. Dimensiunea maximă permisă pentru fișier este de 5 KB.</p> <p>Cum să procedați:</p> <p>Dacă selectați fișierul corect, certificatul ar putea fi deteriorat sau falsificat.</p>
	<p>Cauză:</p> <p>Lanțul inclus în certificat este invalid.</p> <p>Cum să procedați:</p> <p>Pentru mai multe informații privind certificatul, consultați site-ul autorității de certificare.</p>
Nu se pot utiliza Certificate de server care includ mai mult de trei certificate CA.	<p>Cauză:</p> <p>Fișierul certificatului în format PKCS#12 include mai mult de 3 certificate CA.</p> <p>Cum să procedați:</p> <p>Importați fiecare certificat transformat din format PKCS#12 în format PEM sau importați fișierul certificatului în format PKCS#12 care include maximum 2 certificate CA.</p>
Certificatul a expirat. Verificați dacă certificatul este valid sau verificați data și ora de pe produs.	<p>Cauză:</p> <p>Certificatul nu este actualizat.</p> <p>Cum să procedați:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Dacă certificatul nu este actualizat, obțineți și importați noul certificat. <input type="checkbox"/> Dacă certificatul este actualizat, asigurați-vă că data și ora scannerului sunt setate corect.
Cheia privată este obligatorie.	<p>Cauză:</p> <p>Nicio cheie privată nu se potrivește cu certificatul.</p> <p>Cum să procedați:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Dacă certificatul este în format PEM/DER și este obținut de la o CSR folosind un computer, indicați fișierul pentru cheia privată. <input type="checkbox"/> Dacă certificatul este în format PKCS#12 și este obținut de la o CSR folosind un computer, creați un fișier care include cheia privată.
	<p>Cauză:</p> <p>Ați importat din nou certificatul PEM/DER obținut de la o CSR folosind Web Config.</p> <p>Cum să procedați:</p> <p>Dacă certificatul este în format PEM/DER și este obținut de la o CSR folosind Web Config, îl puteți importa o singură dată.</p>

Mesaje	Cauză/Cum să procedați
Configurare eșuată.	Cauză: Configurarea nu poate fi finalizată pentru că comunicarea între scanner și computer a eșuat sau fișierul nu poate fi citit din cauza unor erori. Cum să procedați: După ce verificați fișierul și comunicația indicate, importați din nou fișierul.

Informații conexe

➔ [„Despre certificarea digitală” la pagina 101](#)

Ștergerea din greșeală a unui certificat CA-semnat

Nu există fișier de rezervă pentru certificatul semnat CA.

Dacă aveți fișierul 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 șters. Creați o CSR și obțineți un certificat nou.

Informații conexe

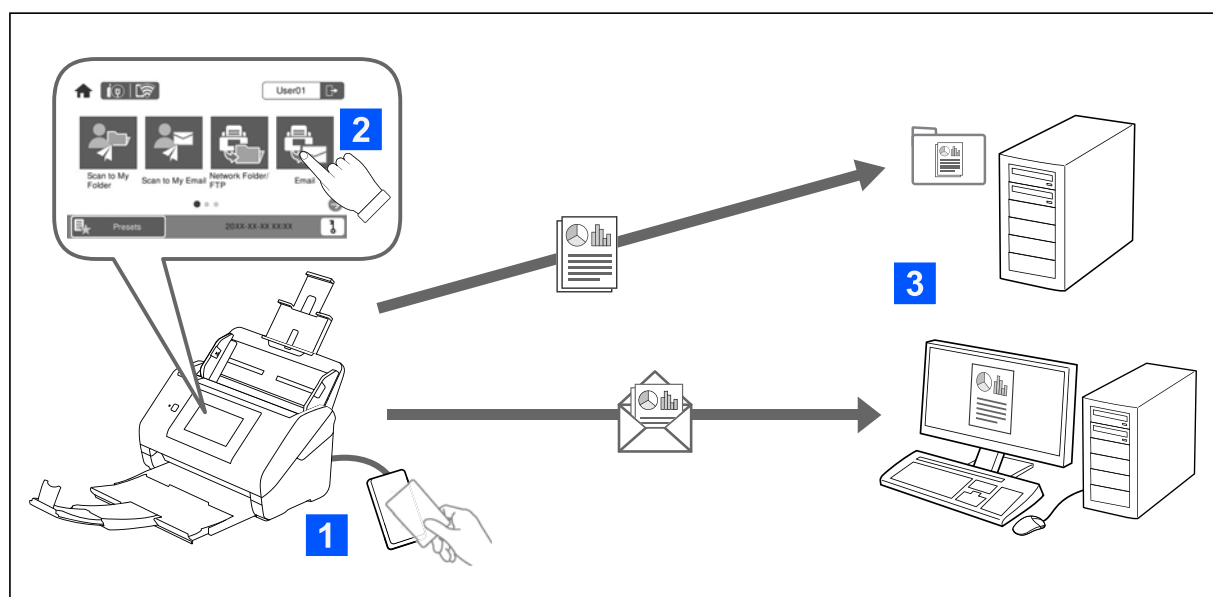
➔ [„Import al unui certificat CA-semnat” la pagina 103](#)

➔ [„Ștergerea unui certificat CA-semnat” la pagina 104](#)

Setări de autentificare

Despre Setări de autentificare.	128
Despre Metodă de autentificare.	129
Software pentru configurare.	131
Actualizarea firmware-ului scannerului.	131
Conectarea și configurarea unui dispozitiv de autentificare.	131
Informații de înregistrare și setare.	136
Rapoarte Job History utilizând Epson Device Admin.	152
Conectarea ca administrator din Panoul de comandă.	152
Dezactivarea Setări de autentificare.	153
Ștergerea informațiilor Setări de autentificare (Restaurare setări implicite).	153
Rezolvarea problemelor.	154

Despre Setări de autentificare



Când se activează Setări de autentificare, este necesară autentificarea utilizatorului pentru a începe scanarea. Puteți seta metodele de scanare care pot fi utilizate de fiecare utilizator și puteți preveni operațiunile accidentale.

Puteți specifica adresa de e-mail a utilizatorului autentificat ca destinație de scanare (Sc. în ct. meu e-mail) sau să salvați datele fiecărui utilizator într-un folder personal (Scanare în fold. meu). De asemenea, puteți specifica alte metode de scanare.

Notă:

- Nu puteți scana de la un computer sau un dispozitiv inteligent când Setări de autentificare sunt activate.
- Pe lângă Setări de autentificare introduse în acest manual, puteți configura și un sistem de autentificare folosind un server de autentificare. Pentru a construi un sistem, utilizați Document Capture Pro Server Authentication Edition (denumirea prescurtată este Document Capture Pro Server AE). Pentru mai multe informații, contactați biroul local Epson.

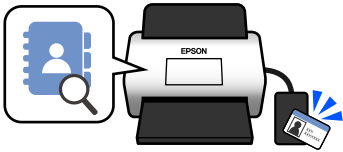
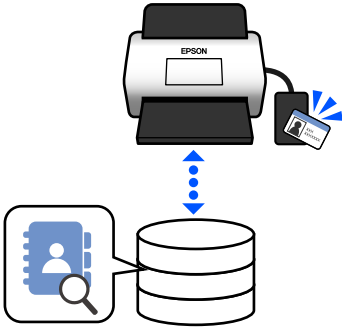
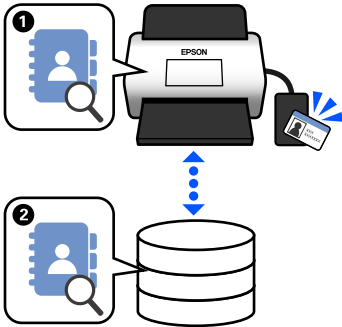
Funcții disponibile pentru Setări de autentificare

Funcție de scanare pe panoul de control	Setări de autentificare	
	Când este activată	Când este dezactivată
Scanare în fold. meu Salvează imaginile în folderul atribuit utilizatorului autentificat.	✓	-
Scanare în ct. meu e-mail Salvează imaginile în adresa de e-mail a utilizatorului autentificat.	✓	-
Scanare în folder rețea/FTP Salvează imaginile într-un folder din rețea.	✓	✓

Funcție de scanare pe panoul de control	Setări de autentificare	
	Când este activată	Când este dezactivată
<p>Scanare către computer</p> <p>Salvează imaginile pe un computer conectat folosind lucrări create în Document Capture Pro (Windows)/Document Capture (Mac OS).</p> <p>* Când Setări de autentificare este activat, puteți utiliza doar lucrările înregistrate în Presetări.</p>	✓*	✓
<p>Scanare către e-mail</p> <p>Trimite imagini la adresa de e-mail pe care ați setat-o.</p>	✓	✓
<p>Scanare în Cloud</p> <p>Trimite imagini către serviciul cloud pe care l-ați setat.</p>	✓	✓
<p>Scanare în unitate USB</p> <p>Salvează imaginile pe o unitate USB conectată la scanner. Aceasta este disponibilă doar atunci când nu este conectat niciun dispozitiv de autentificare la scanner.</p>	✓	✓
<p>Scanare către WSD</p> <p>Salvează imaginile pe un computer conectat utilizând funcția WSD.</p>	-	✓
<p>Presetări</p> <p>Puteți înregistra până la 48 de funcții de scanare presetate.</p> <p>Puteți alocă până la cinci Presetări utilizatorilor înregistrați în Bază de date locală. Presetări alocate sunt disponibile doar pentru acel utilizator. Presetări care nu au fost alocate niciunui utilizator pot fi folosite de toți utilizatorii.</p>	✓	✓

Despre Metodă de autentificare

Acest scanner poate furniza autentificare folosind următoarele metode fără a fi nevoie să implementați un server de autentificare.

	Bază de date locală	LDAP	Bază de date locală și LDAP
Locația informațiilor or utilizatorul ui	<p>Memorie scanner</p> <p>Această metodă de autentificare verifică informațiile de utilizator înregistrate pe scanner și le compară cu utilizatorul care utilizează funcția de scanare.</p>	<p>Server LDAP*</p> <p>Această metodă de autentificare verifică informațiile utilizatorului serverului LDAP sincronizat cu scannerul. Deoarece până la 300 de elemente de informații despre utilizator de pe serverul LDAP pot fi stocate temporar în scanner în memoria cache, autentificarea poate fi efectuată folosind memoria cache dacă serverul LDAP se defectează.</p> <p>* Un server care oferă un serviciu de director care poate comunica cu LDAP.</p>	<p>Memoria scannerului și serverul LDAP</p> <p>Verificați mai întâi informațiile despre utilizator înregistrate în scanner (1), iar dacă nu există potriviri, verificați informațiile despre utilizator prin raportare la serverul LDAP (2).</p>
			
Număr de utilizatori înregistrați	50 (memorie scanner)	Nelimitat (server LDAP)	50 (memorie scanner) Nelimitat (server LDAP)
Memorie cache scanner	-	300	Max 300 (50 de sloturi de memorie cache sunt partajate cu Setări utilizator în Bază de date locală)
Metode de conectare	<p>Puteți utiliza oricare dintre următoarele metode.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Apropiati un card de autentificare sau introduceți un ID utilizator și o Parolă <input type="checkbox"/> Apropiati un card de autentificare sau introduceți un Număr de identificare <input type="checkbox"/> Introduceți un ID utilizator și o Parolă <input type="checkbox"/> Introduceți un ID utilizator <input type="checkbox"/> Introduceți o Număr de identificare 		
Limitele funcției „Scanare la”	Setați individual pentru fiecare utilizator	Aceleași setări pentru toți utilizatorii LDAP	Utilizatori Bază de date locală: setați individual Utilizatori LDAP: aceleași setări pentru toți utilizatorii
Alocarea Presetări utilizatorilor or	Până la 5 per utilizator	- (Nu se poate seta individual)	Utilizatori Bază de date locală: până la 5 per utilizator Utilizatori LDAP: -

Software pentru configurare

Configurați utilizând Web Config sau Epson Device Admin.

- Când utilizați Web Config, puteți configura scannerul doar prin utilizarea unui browser web.
[„Web Config” la pagina 36](#)
- Când utilizați Epson Device Admin, puteți configura mai multe scanere simultan folosind un șablon de configurare.
[„Epson Device Admin” la pagina 37](#)

Actualizarea firmware-ului scannerului

Înainte de a activa Setări de autentificare, actualizați firmware-ul scannerului la cea mai recentă versiune. Conectați scannerul la Internet, în prealabil.



Important:

Nu opriți computerul sau scannerul în timpul actualizării.

La configurarea din Web Config:

Selectați fila **Gestionare dispozitiv** > **Actualizare firmware** și urmați instrucțiunile de pe ecran pentru a actualiza firmware-ul.

La configurarea din Epson Device Admin:

Select **Home** > **Firmware** > **Update** listei de dispozitive, apoi urmați instrucțiunile de pe ecran pentru a actualiza firmware-ul.

Notă:

Dacă cel mai recent firmware este deja instalat, nu este necesar să efectuați actualizarea.

Conectarea și configurarea unui dispozitiv de autentificare

Dacă doriți să vă conectați și să utilizați un dispozitiv de autentificare, cum ar fi un cititor de carduri IC, mai întâi trebuie să configurați dispozitivul. Acest lucru nu este necesar dacă nu utilizați un dispozitiv de autentificare.

Informații conexe

- ➔ [„Conectarea dispozitivului de autentificare” la pagina 134](#)
- ➔ [„Setările dispozitivului de autentificare” la pagina 135](#)

Listă de compatibilitate cititoare de carduri

Această listă nu garantează operațiuni pentru cititoarele de carduri din listă.

Da: acceptat (Informațiile de identificare pot fi citite cu setările standard ale cititorului de carduri.)

Nu: nu este compatibil

Pro-ducător	Model	Număr model	Card de autentificare							IEC/ISO14443 (TypeB) Compliance	Mod
			HID Global	DMZ	MIFARE		FeliCa™				
			iClass	EM4002	Clas-sic	Ultra-light	Stan-dard	Lite/Lite-S			
RF IDEAS	pcProx Plus	RDR-80081AKU	Da	Da*1	Da*1	Da*1	Nu	Nu	Nu	Tastatură	
RF IDEAS	pcProx	RDR-7081BKU	Da*1	Nu	Da	Da	Nu	Nu	Nu	Tastatură	
RF IDEAS	pcProx	RDR-7581AKU	Da	Nu	Da*1	Da*1	Nu	Nu	Nu	Tastatură	
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Nu	Nu	Da	Da	Nu	Nu	Nu	Tastatură	
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Da	Nu	Da	Da	Da	Da	Da	Tastatură	
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Da	Da	Da	Da	Da	Da	Da	Tastatură	
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Da	Da	Da	Da	Da	Da	Da	Tastatură	
ELATEC	TWN4 Slim	T4QC-FC3B7	Da	Da	Da	Da	Da	Da	Da	Tastatură	
HID Global	OMNI-KEY 5427	OMNI-KEY5427CK OMNI-KEY5427CK gen2	Da	Da	Da	Da	Da	Nu	Da	Tastatură*1	
ACS	ACR122U	ACR122U	Nu	Nu	Da*2	Da*2	Da	Nu	Da*2	PC/SC	

Pro-ducător	Model	Număr model	Card de autentificare							IEC/ISO14443 (TypeB) Compliance	Mod
			HID Global	DMZ	MIFARE		FeliCa™				
			iClass	EM4002	Clasic	Ultra-light	Standard	Lite/Lite-S			
ACS	ACR1252	ACR1252	Nu	Nu	Da*2	Da*2	Da	Da	Da*2	PC/SC	
Sony	PaSoRi	RC-S330/S	Nu	Nu	Da*2	Da*2	Da*2	Da*2	Da*2	PaSoRi	
Sony	PaSoRi	RC-S380/P RC-S380/S	Nu	Nu	Da*2	Da*2	Da*2	Da*2	Da*2	PaSoRi	
DMZ	Leitor RFID Universal	DMZ008	Da	Da	Da	Da	Da	Da	Da	Tastatură	
DMZ	Leitor RFID Multi-125	DMZ087	Nu	Da	Nu	Nu	Nu	Nu	Nu	Tastatură	
DMZ	Leitor RFID Mifare	DMZ088	Nu	Nu	Da	Da	Nu	Nu	Nu	Tastatură	
DMZ	Biometric & RFID Reader	DMZ073	Nu	Da	Nu	Nu	Nu	Nu	Nu	Tastatură	
inepro	SCR708	SCR708	Da*1	Da*1	Da*1	Da*1	Da*1	Da*1	Da*1	Tastatură	
Y Soft	YU03088001	MU0388	Da	Da	Da	Da	Da	Da	Da	Tastatură	
Cardadis	TCM3 Cardadis MiFare Card Reader	ZTCM3-MIFARE	Nu	Nu	Da	Da	Nu	Nu	Da	Tastatură	
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Nu	Nu	Da	Da	Nu	Nu	Da	Tastatură	

Pro-ducător	Model	Număr model	Card de autentificare							Mod
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Clas-sic	Ultra-light	Stan-dard	Lite/Lite-S		
NT-wa-re	MiCard Multi-Tech4-PI	T4DT-FB4WU F-PI	Da	Da	Da	Da	Da	Da	Da	Tasta-tură
NT-wa-re	MiCard Plus-2-V2	RDR-80 081AG U-NT2-20	Da*1	Da*1	Da*1	Da*1	Nu	Nu	Nu	Tasta-tură
NT-wa-re	MiCard V3 Mul-ti	MiCard V3 Mul-ti	Da	Da	Da	Da	Da	Da	Nu	Tasta-tură

*1 Trebuie să modificați setările cititorului de carduri utilizând software-ul proprietar furnizat de producătorul cititorului de carduri.

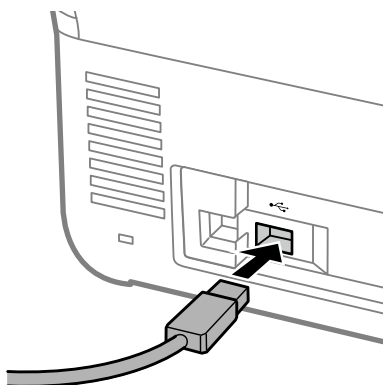
*2 Dacă trebuie să utilizați date dintr-o anumită zonă a cardului, altele decât ID-ul standard al cardului ca ID de autentificare prin configurarea setărilor produsului, vă rugăm să contactați partenerul dumneavoastră Epson sau reprezentantul local pentru mai multe informații despre o modalitate de a configura produsul.

Conectarea dispozitivului 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 scanner.



Verificarea funcționării dispozitivului de autentificare

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

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

Setările dispozitivului de autentificare

Selectați formatul de citire pentru informațiile de autentificare preluate de la un card de autentificare.

Puteți seta următoarea metodă de citire pentru dispozitivul de autentificare.

- Citirea unei anumite porțiuni a unui card de autentificare, precum un număr de angajat sau un ID personal.
- Utilizați informațiile de pe cardul de autentificare, cu excepția UID (informații de pe cardul de autentificare, precum numărul de serie).

Puteți utiliza un instrument pentru a genera parametrii operaționali. Solicitați detalii de la distribuitor.

Notă:

Utilizarea cardurilor de autentificare furnizate de alți producători:

Dacă utilizați informațiile de card UID (informațiile cardului de identificare, cum ar fi numărul de serie), puteți folosi o combinație de tipuri diferite de carduri de autentificare. Acest lucru nu este posibil dacă utilizați alte informații ale cardului.

La configurarea din Web Config:

Selectați fila **Gestionare dispozitiv > Cititor de carduri**.

La configurarea din Epson Device Admin:

Selectați **Administrator Settings > Authentication Settings > Card Reader** din șablonul de configurare.

Element	Explicație
Vendor ID	Setați ID-ul de producător al dispozitivului de autentificare care limitează utilizarea de la 0000 la FFFF, utilizând 4 caractere alfanumerice. Dacă nu doriți să aplicați o limitare, setați la 0000.
Product ID	Setați ID-ul de produs al dispozitivului de autentificare care limitează utilizarea de la 0000 la FFFF, utilizând 4 caractere alfanumerice. Dacă nu doriți să aplicați o limitare, setați la 0000.
Parametru de operare	Setați parametrul operațional al dispozitivului de autentificare între 0 și 8 192 de caractere. Sunt disponibile caracterele A-Z, a-z, 0-9, +, /, =, spațiu și salt la linie nouă.
Cititor de carduri	Selectați formatul de conversie pentru dispozitivul de autentificare. Puteți verifica detaliile formatului. Consultați linkul furnizat în descrierea articolului.
Format salvare ID carte de autentificare	Selectați formatul de conversie pentru informațiile de autentificare ale unui card de indentificare. Puteți verifica detaliile formatului. Consultați linkul furnizat în descrierea articolului.
Setare interval ID card	Permiteți specificarea poziției de citire.
Poziție început text	Specificați poziția de început a textului pentru citirea informațiilor de identificare. Puteți specifica o valoare între 1 și 4096.
Număr de caractere	Specificați numărul de caractere care trebuie citite din poziția de început a informațiilor de identificare. Puteți specifica o valoare între 1 și 4096.

Informații de înregistrare și setare

Configurarea

Efectuați setările necesare în funcție de Metodă de autentificare și metoda de scanare pe care o utilizați.



Important:

Înainte de a începe configurarea, verificați dacă setarea orei pentru scanner este corectă.

Dacă setarea orei este incorectă, se afișează mesajul de eroare „Licența a expirat”, ceea ce poate duce la imposibilitatea de a configura scannerul. De asemenea, pentru a utiliza o funcție de securitate precum comunicația SSL/TLS sau IPsec, este necesară setarea orei corecte. Pentru a seta ora, procedați după cum urmează.

Fila Web Config: **Gestionare dispozitiv** > **Data și ora** > **Data și ora**.

Panoul de comandă al scannerului: **Setări** > **Setări de bază** > **Setări dată/oră**.

Setări	Bază de date locală	LDAP	Bază de date locală și LDAP
Activare autentificare Trebuie să activați autentificarea înainte de a efectua setările de autentificare. „Activare autentificare” la pagina 137	✓	✓	✓
Setări de autentificare Setarea Metodă de autentificare și a modului de autentificare a utilizatorului. „Setări de autentificare” la pagina 137	✓	✓	✓
Înregistrarea Setări utilizator Înregistrați setările pentru fiecare utilizator. Puteți înregistra, de asemenea, utilizatorii în masă utilizând un fișier CSV. „Înregistrarea Setări utilizator” la pagina 139	✓	–	✓
Sincronizarea cu Server LDAP Efectuați setările de sincronizare a serverului LDAP. „Sincronizarea cu Server LDAP” la pagina 145	–	✓	✓
Setarea Server e-mail Efectuați setările serverului de e-mail. Setări acest lucru atunci când utilizați funcții care necesită setări ale serverului de e-mail, cum ar fi Sc. în ct. meu e-mail. „Setarea serverului de e-mail” la pagina 149	✓	✓	✓
Setarea Scanare în fold. meu Setări folderele de destinație. Setări aceasta atunci când utilizați funcția Scanare în fold. meu. „Setarea Scanare în fold. meu” la pagina 150	✓	✓	✓

Setări	Bază de date locală	LDAP	Bază de date locală și LDAP
<p>Personalizați funcțiile accesibile printr-o singură atingere</p> <p>Setați acest lucru când schimbați elementele afișate pe panoul de comandă al scannerului. Puteți afișa doar pictogramele de care aveți nevoie pe panoul de comandă sau puteți modifica ordinea pictogramelor.</p> <p>„Personalizați funcțiile accesibile printr-o singură atingere” la pagina 152</p>	✓	✓	✓

Activare autentificare

Trebuie să activați autentificarea înainte de a efectua setările de autentificare.

La configurarea din Web Config:

Selectați **Activare (Dispozitiv/Server LDAP)** din fila **Securitate produs > De bază > Autentificare**.

La configurarea din Epson Device Admin:

Pe șablonul de configurare, selectați **Activare (Dispozitiv/Server LDAP)** din **Administrator Settings > Authentication Settings > Basic > Authentication**.

Notă:

Dacă activați Setări de autentificare pe scanner, Setare blocare este activată și pentru panoul de comandă. Panoul de comandă nu poate fi deblocat atunci când Setări de autentificare sunt activate.

Chiar dacă dezactivați Setări de autentificare, Setare blocare rămâne activată. Dacă doriți să o dezactivați, puteți face setări din panoul de comandă sau din Web Config.

Informații conexe

- ➔ [„Setarea Setare blocare de la panoul de comandă” la pagina 88](#)
- ➔ [„Setarea Setare blocare din Web Config” la pagina 88](#)

Setări de autentificare

Setarea Metodă de autentificare și a modului de autentificare a utilizatorului.

La configurarea din Web Config:

Selectați fila **Securitate produs > Setări de autentificare**.

La configurarea din Epson Device Admin:

Selectați **Administrator Settings > Authentication Settings > Authentication Settings** din șablonul de configurare.

Element	Explicație
Metodă de autentificare	<p>Selectați Metodă de autentificare.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Bază de date locală Autentificare utilizând Setări utilizator înregistrate pe scanner. Este necesară înregistrarea utilizatorului pe scanner. <input type="checkbox"/> LDAP Autentificare utilizând informațiile de utilizator ale serverului LDAP sincronizat scannerul. Trebuie să configurați setările serverului LDAP în prealabil. <input type="checkbox"/> Bază de date locală și LDAP Autentificare utilizând informațiile de utilizator înregistrate la scanner sau ale serverului LDAP sincronizat cu imprimanta. Trebuie să înregistrați utilizatorul pe scanner și să configurați serverul LDAP.
Cum se autentifică utilizatorul	<p>Selectați modul de autentificare a utilizatorului.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Carte sau ID utilizator și parolă Utilizați un card de autentificare pentru autentificarea utilizatorilor. De asemenea, pentru autentificare puteți utiliza un ID de utilizator și o parolă. <input type="checkbox"/> ID utilizator și parolă Utilizați un ID de utilizator și o parolă pentru autentificarea utilizatorilor. Nu puteți utiliza un card de autentificare pentru a vă autentifica atunci când selectați această funcție. <input type="checkbox"/> ID utilizator Utilizați numai un ID de utilizator pentru a autentifica utilizatorii. Nu trebuie să setați o parolă. <input type="checkbox"/> Carte sau număr de identificare Utilizați un card de autentificare pentru autentificarea utilizatorilor. De asemenea, puteți utiliza un Număr de identificare. <input type="checkbox"/> Număr de identificare Utilizați numai un număr ID pentru autentificarea utilizatorilor.
Se permite utilizatorilor să înregistreze carduri de autentificare	<p>Activați opțiunea dacă permiteți utilizatorilor să înregistreze cardul de autentificare în sistem.</p> <p>Dacă selectați LDAP pentru Metodă de autentificare, nu puteți seta această opțiune.</p> <p>Pentru mai multe informații despre modul în care utilizatorii își pot înregistra cardurile de autentificare, consultați „Înregistrarea unui card de autentificare” din <i>Ghidul utilizatorului</i>.</p>
Numărul minim de cifre pentru numărul de identificare	<p>Selectați numărul minim de cifre pentru numărul ID.</p>
Memorare în cache pentru utilizatorii autentificați LDAP	<p>Atunci când utilizați autentificarea la un server LDAP, puteți seta dacă se utilizează sau nu memorarea în cache pentru informațiile utilizatorului.</p>
Folosiți informațiile utilizatorului din autentificarea SMTP	<p>Atunci când se utilizează un ID de utilizator și o parolă pentru autentificare, puteți seta dacă se utilizează sau nu informațiile utilizatorului pentru autentificarea SMTP. Sistemul utilizează ultimul ID de utilizator și ultima parolă conectate.</p>
Restricții pentru utilizatori autentificați LDAP	<p>Dacă utilizați LDAP, puteți seta funcțiile care sunt disponibile utilizatorului.</p>

Înregistrarea Setări utilizator

Înregistrați Setări utilizator utilizate pentru autentificarea utilizatorului. Puteți înregistra folosind oricare dintre următoarele metode.

- Înregistrarea Setări utilizator una câte una (Web Config)
- Înregistrarea Setări utilizator multiple ca lot utilizând un fișier CSV (Web Config)
- Înregistrarea User Settings pe mai multe scanere ca lot utilizând un șablon de configurare (Epson Device Admin)

Informații conexe

- ➔ „Înregistrarea Setări utilizator individual (Web Config)” la pagina 139
- ➔ „Înregistrarea unor multiple Setări utilizator utilizând un fișier CSV (Web Config)” la pagina 140
- ➔ „Înregistrarea User Settings pe scanere multiple ca lot (Epson Device Admin)” la pagina 143

Înregistrarea Setări utilizator individual (Web Config)

Accesați Web Config și selectați fila **Securitate produs > Setări utilizator > Adăugare**, apoi accesați Setări utilizator.

Element	Explicație
ID utilizator	Introduceți ID-ul utilizatorului pe care doriți să îl utilizați pentru autentificare într-un interval de la 1 la 83 de octeți, care poate fi exprimat în Unicode (UTF-8). Întrucât caseta ID utilizator nu este sensibilă la litere mari și mici, vă puteți autentifica folosind litere mari sau mici.
Afișare nume utilizator	Introduceți numele de utilizator afișat pe panoul de comandă al scannerului, utilizând maximum 32 de caractere exprimate în Unicode (UTF-16). Puteți lăsa necompletat acest câmp.
Parolă	Introduceți parola care se va utiliza pentru autentificare, în limita a 32 de caractere ASCII. Parola depinde de tipul caracterelor. Lăsați acest câmp necompletat dacă selectați ID utilizator pentru Cum se autentifică utilizatorul .
ID carte de autentificare	Introduceți ID-ul cardului de autentificare, în limita a 116 de caractere ASCII. Puteți lăsa necompletat acest câmp. Când permiteți opțiunea Se permite utilizatorilor să înregistreze carduri de autentificare pentru Setări de autentificare , este reflectat rezultatul înregistrat de utilizatori.
Număr de identificare	Acest element este afișat când Carte sau număr de identificare sau Număr de identificare este selectat în Setări de autentificare > Cum se autentifică utilizatorul . Introduceți un număr care se situează undeva între numărul setat în Setări de autentificare > Numărul minim de cifre pentru numărul de identificare și are până la 8 cifre.

Element	Explicație
Generare automată	Acest element este afișat când Carte sau număr de identificare sau Număr de identificare este selectat în Setări de autentificare > Cum se autentifică utilizatorul . Faceți clic pentru a genera automat un număr de identificare cu același număr de cifre pe care l-ați selectat în Numărul minim de cifre pentru numărul de identificare .
Departament	Introduceți numele departamentului și alte date care identifică utilizatorul într-un interval de 40 de caractere care pot fi exprimate în Unicode (UTF-16). Puteți lăsa necompletat acest câmp.
Adresă de e-mail	Introduceți adresa de e-mail a utilizatorului în maximum 200 de caractere în ASCII. Aceasta este utilizată ca destinație pentru funcția Sc. în ct. meu e-mail . Puteți lăsa necompletat acest câmp.
Scanare în fold. meu	Setați destinațiile de salvare individual când selectați Individual în Scanare în fold. meu > Tip setare . Consultați secțiunea următoare pentru mai multe informații despre elementele de setare. „Setarea Scanare în fold. meu” la pagina 150
Restricții	Puteți restricționa funcțiile pentru fiecare utilizator. Selectați funcția a cărei utilizare o permiteți.
Presetări	Puteți configura până la cinci presetări care sunt disponibile doar pentru utilizatorul selectat din Presetări înregistrate pe scanner. <input type="checkbox"/> Presetări care nu au fost alocate unui utilizator pot fi folosite de alt utilizator. Presetări care nu au fost alocate niciunui utilizator pot fi folosite de toți utilizatorii. <input type="checkbox"/> Dacă un utilizator are disponibil doar o singură Presetări, aceasta se încarcă automat după autentificare. Dacă sunt disponibile mai multe Presetări, după autentificare este afișată o listă Presetări. <input type="checkbox"/> Nu puteți crea sau afișa Presetări care utilizează funcții care au fost restricționate în Restricții .

Înregistrarea unor multiple Setări utilizator utilizând un fișier CSV (Web Config)

Introduceți setările pentru fiecare utilizator într-un fișier CSV și înregistrați-le ca lot.

Crearea unui fișier CSV

Creați un fișier CSV pentru a importa Setări utilizator.

Notă:

Dacă înregistrați una sau mai multe setări Setări utilizator în avans și apoi exportați un fișier configurat (fișier CSV), puteți utiliza setarea înregistrată ca referință pentru introducerea elementelor de setare.

1. Accesați Web Config și selectați fila **Securitate produs > Setări utilizator**.
2. Executați clic pe **Export**.

3. Selectați formatul de fișier pentru **Format fișier**.

Pentru selectare, consultați informațiile de mai jos.

Element	Explicație
CSV UTF-16 (delimitare prin tabulator)	<p>Selectați opțiunea când editați fișierul utilizând Microsoft Excel.</p> <p>Fiecare parametru este delimitat de „[]” (paranteze drepte). Introduceți parametrii între „[]”.</p> <p>Când actualizați fișierul, se recomandă suprascrierea acestuia. Dacă salvați fișierul pentru prima dată, selectați Unicode text (*.txt) ca format al fișierului.</p>
CSV UTF-8 (delimitare prin virgulă)	<p>Selectați opțiunea când editați fișierul utilizând un editor de texte sau o macrocomandă, fără Microsoft Excel.</p>
CSV UTF-8 (delimitare prin punct și virgulă)	

4. Executați clic pe **Export**.

5. Editați și salvați acest fișier CSV într-o aplicație de calcul tabelar precum Microsoft Excel sau într-un editor de texte.



Important:

La editarea fișierului, nu modificați informațiile de codificare și din antet.

Elemente de setare a fișierului CSV

Element	Setări și explicație
UserID	Introduceți ID-ul utilizatorului pentru a utiliza autentificarea între 1 și 83 de octeți în Unicode.
UserName	Introduceți numele de utilizator afișat pe panoul de comandă al imprimantei, utilizând maximum 32 de caractere în Unicode. Puteți lăsa necompletat acest câmp.
Password	<p>Introduceți parola care se va utiliza pentru autentificare, în limita a 32 de caractere ASCII. Când importați, aceasta este setată ca parolă în loc de EncPassword.</p> <p>Lăsați acest câmp necompletat dacă selectați ID utilizator pentru Cum se autentifică utilizatorul.</p> <p>Când exportați, acest câmp este întotdeauna necompletat.</p>
AuthenticationCardID	<p>Definiți rezultatul citirii cardului de autentificare. Când permiteți opțiunea Se permite utilizatorilor să înregistreze carduri de autentificare în Setări de autentificare, este reflectat rezultatul înregistrat de utilizatori.</p> <p>Introduceți maximum 116 caractere ASCII. Puteți lăsa necompletat acest câmp.</p>

Element	Setări și explicație
IDNumber	<p>Acest element este afișat când Carte sau număr de identificare sau Număr de identificare este selectat în Setări de autentificare > Cum se autentifică utilizatorul.</p> <p>Introduceți un număr care se situează undeva între numărul setat în Setări de autentificare > Numărul minim de cifre pentru numărul de identificare și are până la 8 cifre.</p> <p>Un număr ID nu poate fi duplicat. În cazul în care este duplicat, veți fi informat cu privire la eroare la importul fișierului. Dacă este necompletat, acestuia i se alocă automat un număr.</p>
Department	<p>Introduceți numele departamentului în mod arbitrar, pentru a diferenția utilizatorii.</p> <p>Introduceți maximum 40 de caractere în Unicode. Puteți lăsa necompletat acest câmp.</p>
MailAddress	<p>Definiți adresa de e-mail pentru utilizatori. Aceasta este utilizată ca destinație pentru funcția Sc. în ct. meu e-mail.</p> <p>Puteți folosi A-Z, a-z, 0-9, !#%&'*+-. /=?^_{}~@. Introduceți 200 caractere sau mai puțin. Nu puteți utiliza „,” (virgulă) pentru primul caracter. Puteți lăsa necompletat acest câmp.</p>
FolderProtocol	<p>Setarea tipului de funcție Scanare în fold. meu.</p> <p>Folder în rețea/FTP (SMB): 0, FTP: 1</p>
FolderPath	<p>Configurați destinația de salvare pentru funcția Scanare în fold. meu.</p>
FolderUserName	<p>Configurați numele de utilizator pentru funcția Scanare în fold. meu.</p>
FolderPassword	<p>Configurați o parolă de autentificare a folderului de destinație pentru funcția Scanare în fold. meu, fără a depăși 32 de caractere ASCII.</p> <p>Când importați, aceasta este setată ca parolă în loc de EncPassword. Când exportați, acest câmp este întotdeauna necompletat.</p>
FtpPassive	<p>Configurați modul de conectare pentru serverul FTP dacă FTP este selectat drept Tip pentru funcția Scanare în fold. meu.</p> <p>Mod activ: 0, Mod pasiv: 1</p>
FtpPort	<p>Configurați numărul portului pentru expedierea datelor scanate către serverul FTP între 0 și 65535 dacă FTP este selectat ca Tip pentru funcția Scanare în fold. meu.</p>
ScanToMemory	<p>Setați restricțiile pentru Scanare în unitate USB.</p> <p>Nu este permis: 0, Permis: 1</p>
ScanToMail	<p>Setați restricțiile pentru Scanare către e-mail.</p> <p>Puteți seta Scanare în ct. meu e-mail doar când s-a activat Scanare către e-mail.</p> <p>Nu este permis: 0, Permis: 1</p>
ScanToFolder	<p>Setați restricțiile pentru Scanare către folder din rețea/FTP.</p> <p>Puteți seta Scanare în fold. meu doar când s-a activat Scanare către folder din rețea/FTP.</p> <p>Nu este permis: 0, Permis: 1</p>
ScanToCloud	<p>Setați restricțiile pentru Scanare către cloud.</p> <p>Nu este permis: 0, Permis: 1</p>

Element	Setări și explicație
ScanToComputer	Setați restricțiile pentru Scanare către computer. Nu este permis: 0, Permis: 1
PresetIndex	Setați Presetări dorite pentru asocierea cu utilizatorul. Puteți configura până la cinci numere de înregistrare Presetări separate prin virgulă.
EncPassword	Când exportați setări de utilizator, parametrul setat pentru Password este criptat, apoi valoarea este codificată cu algoritmul BASE64 și redată la ieșire. La importul cu noua parolă pentru Password , această valoare este ignorată. În cazul în care câmpul Password este necompletat, se utilizează această valoare și parola rămâne în starea anterioară exportului.
EncFolderPassword	Când exportați, parametrul setat pentru FolderPassword este criptat, iar apoi valoarea este codificată de BASE64 și transmisă. La importul cu noua parolă pentru FolderPassword , această valoare este ignorată. În cazul în care câmpul FolderPassword este necompletat, se utilizează această valoare și parola rămâne în starea anterioară exportului.

Importul unui fișier CSV

1. Accesați Web Config și selectați fila **Securitate produs > Setări utilizator**.
2. Executați clic pe **Import**.
3. Selectați fișierul pe care doriți să îl importați.
4. Executați clic pe **Import**.
5. După verificarea informațiilor afișate, faceți clic pe **OK**.

Înregistrarea User Settings pe scanere multiple ca lot (Epson Device Admin)

Puteți înregistra User Settings utilizate în Bază de date locală ca lot utilizând un server LDAP sau un fișier CSV/ENE.

Notă:

*Un fișier ENE este un fișier binar furnizat de Epson care criptează și salvează informații pentru **Contacts**, cum ar fi informații personale și Setări utilizator. Poate fi exportat din Epson Device Admin și puteți seta o parolă. Este util atunci când doriți să importați Setări utilizator dintr-un fișier de copie de rezervă.*

Importul dintr-un fișier CSV/ENE

1. Selectați **Administrator Settings > Authentication Settings > User Settings** din șablonul de configurare.
2. Executați clic pe **Import**.
3. Selectați opțiunea **CSV or ENE File** din **Import Source**.

4. Executați clic pe **Browse**.
Este afișat ecranul pentru selectarea fișierului.
5. Selectați fișierul pe care doriți să îl importați pentru a-l deschide.
6. Selectați o metodă de import.
 - Overwrite and Add: suprascrie dacă există același ID de utilizator; adaugă un nou ID dacă nu există.
 - Replace All: înlocuiește totul cu setările utilizatorului pe care doriți să le importați.
7. Executați clic pe **Import**.
Se afișează ecranul de confirmare a setării.
8. Executați clic pe **OK**.
Se afișează rezultatul validării.

Notă:

 - Dacă numărul de setări de utilizator importate depășește numărul care poate fi importat, un mesaj vă va solicita să ștergeți unele setări de utilizator. Ștergeți orice setări ale utilizatorului în exces înainte de a importa.
 - Selectați setările utilizatorului pe care doriți să le ștergeți înainte de a le importa, apoi faceți clic pe **Delete**.
9. Executați clic pe **Import**.
Setările utilizatorului sunt importate în șablonul de configurare.

Importul de pe serverul LDAP

1. Selectați **Administrator Settings > Authentication Settings > User Settings** din șablonul de configurare.
2. Executați clic pe **Import**.
3. Selectați opțiunea **LDAP** din **Import Source**.
4. Executați clic pe **Settings**.

Setările **LDAP Server** sunt afișate.

Notă:

Această setare de server LDAP este pentru importarea setărilor utilizatorului de pe serverul LDAP. Setările utilizatorului importate (copiate) sunt folosite pentru a autentifica utilizatorii folosind chiar scannerul.

*Pe de altă parte, când selectați **LDAP** sau **Local DB and LDAP** ca metodă de autentificare, utilizatorii sunt autentificați prin comunicarea cu serverul LDAP.*

5. Setati fiecare element.

Când importați setările utilizatorului de pe un server LDAP, puteți configura și următoarele setări pe lângă setările LDAP.

Pentru alte elemente, consultați Informații conexe.

Element		Explicație
LDAP Server Settings	LDAP Server Type	Vă permite să selectați tipul de server LDAP.

Element		Explicație	
Search Settings	Search Filter	Puteți seta textul utilizat pentru filtrul de căutare LDAP. Selectați Custom pentru a edita textul de căutare.	
	Options	Type	Puteți seta tipul de destinație de salvare pentru Scan To My Folder .
		Connection Mode	Când Type este setat la FTP , puteți seta modul de conexiune FTP.
		Port Number	Când Type este setat la FTP , puteți seta numărul portului pe care doriți să-l utilizați.

6. Efectuați testul de conexiune după cum este necesar, făcând clic pe **Connection Test**.
Achiziționează și afișează 10 setări de utilizator de la serverul LDAP.
7. Executați clic pe **OK**.
8. Selectați o metodă de import.
 - Overwrite and Add: suprascrie dacă există același ID de utilizator; adaugă un nou ID dacă nu există.
 - Replace All: înlocuiește totul cu setările utilizatorului pe care doriți să le importați.
9. Executați clic pe **Import**.
Se afișează ecranul de confirmare a setării.
10. Executați clic pe **OK**.
Se afișează rezultatul validării.
11. Executați clic pe **Import**.
Setările utilizatorului sunt importate în șablonul de configurare.

Informații conexe

- ➔ [„Configurarea unui server LDAP” la pagina 146](#)
- ➔ [„Configurarea setărilor de căutare server LDAP” la pagina 147](#)

Sincronizarea cu Server LDAP

Efectuați setările Server LDAP pentru scanner.

Efectuați setări atât pentru serverul principal, cât și pentru serverul secundar, după cum este necesar.

Notă:

Setările *Server LDAP* sunt partajate cu *Persoane de contact*.

Servicii disponibile

Sunt acceptate următoarele servicii de director.

Nume serviciu	Versiune
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Configurarea unui server LDAP

Pentru a utiliza un server LDAP, mai întâi trebuie să configurați serverul LDAP.

La configurarea din Web Config:

Selectați fila **Rețea** > **Server LDAP** > **De bază (Server principal)** sau **De bază (Server secundar)**.

Dacă selectați **Autentificare Kerberos** ca **Metodă de autentificare**, selectați **Rețea** > **Setări Kerberos** pentru a face setări pentru Kerberos.

La configurarea din Epson Device Admin:

Selectați **Network** > **LDAP server** > **Server Settings (Primary Server)** sau **Server Settings (Secondary Server)** din șablonul de configurare.

Dacă selectați **Autentificare Kerberos** ca **Metodă de autentificare**, selectați **Network — Security** > **Setări Kerberos** pentru a face setări pentru Kerberos.

Element	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 utiliza caracterele alfanumerice din ASCII (0x20–0x7E) și „-”, cu excepția începutului și a sfârșitului adresei.
Număr port server LDAP (Port number)	Introduceți numărul de port de server LDAP între 1 și 65535.
Conexiune securizată	Indicați metoda de autentificare pentru ca scannerul să acceseze serverul LDAP.
Validare certificat	Certificatul serverului LDAP este autentificat când acest element este activat. Recomandăm setarea opțiunii la Activare . Pentru a configura, Certificat CA trebuie importat la scanner.
Expirare căutare (sec.)	Setați intervalul de timp de căutare înainte de apariția expirării între 5 și 300 de secunde.
Metodă de autentificare	Selectați metoda de autentificare. Dacă selectați Autentificare Kerberos , faceți setările pentru Kerberos în avans. Pentru a efectua Autentificare Kerberos, următorul mediu este obligatoriu. <input type="checkbox"/> Scannerul și serverul DNS pot comunica. <input type="checkbox"/> Ora scannerului, a serverului KDC și a serverului necesar pentru autentificare (server LDAP, server SMTP, server de fișiere) sunt sincronizate. <input type="checkbox"/> 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.

Element	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 doriți să 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 doriți să specificați acest element, lăsați-l necompletat.

Setări Kerberos

Dacă ați selectat **Autentificare Kerberos** ca **Metodă de autentificare**, trebuie să efectuați setări Kerberos. Puteți înregistra până la 10 setări Kerberos.

La configurarea din Web Config:

Selectați fila **Rețea** > **Setări Kerberos**.

La configurarea din Epson Device Admin:

Selectați **Network** > **Security** > **Setări Kerberos** din șablonul de configurare.

Element	Setări și explicație
Domeniu	Introduceți domeniul autentificării Kerberos, cu 255 de caractere sau mai puține în sistem ASCII (0x20–0x7E). Dacă nu doriți să 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 doriți să înregistrați acest element, lăsați-l necompletat.
Număr port (Kerberos)	Introduceți numărul portului serverului Kerberos, între 1 și 65535.

Configurarea setărilor de căutare server LDAP

Setează atributele de căutare pentru setările utilizatorului.

La configurarea din Web Config:

Selectați fila **Rețea** > **Server LDAP** > **Setări căutare (autentificare)**.

La configurarea din Epson Device Admin:

Selectați **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** din șablonul de configurare.

Element	Setări și explicație
Search Base (Distinguished Name)	Specificați poziția de început pentru căutarea informațiilor de utilizator pe serverul 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

Element	Setări și explicație
User ID Attribute	Specificați numele de atribut care se va afișa la căutarea numărului ID. Introduceți între 1 și 255 de caractere în ASCII. Primul caracter trebuie să fie a-z sau A-Z. Exemplu: cn, uid
User name Display Attribute	Specificați numele de atribut care se va afișa ca nume de utilizator. Introduceți între 0 și 255 de caractere în ASCII. Primul caracter trebuie să fie a-z sau A-Z. Puteți lăsa necompletat acest câmp. Exemplu: cn, name
Authentication Card ID Attribute	Specificați numele de atribut care se va afișa ca ID de card de autentificare. Introduceți între 0 și 255 de caractere în ASCII. Primul caracter trebuie să fie a-z sau A-Z. Puteți lăsa necompletat acest câmp. Exemplu: cn, sn
ID Number Attribute	Specificați numele de atribut care se va afișa la căutarea numărului ID. Introduceți între 1 și 255 de caractere în ASCII. Primul caracter trebuie să fie a-z sau A-Z. Exemplu: cn, id
Department Attribute	Specificați numele de atribut care se va afișa ca nume de departament. Introduceți între 0 și 255 de caractere în ASCII. Primul caracter trebuie să fie a-z sau A-Z. Puteți lăsa necompletat acest câmp. Exemplu: ou, ou-cl
Email Address Attribute	Specificați numele de atribut care se va afișa la căutarea adreselor de e-mail. Introduceți între 1 și 255 de caractere în ASCII. Primul caracter trebuie să fie a-z sau A-Z. Exemplu: mail
Save To Attribute	Specificați numele atributului care indică destinația pentru Scan To My Folder. Introduceți între 0 și 255 de caractere în ASCII. Exemplu: homeDirectory

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.

Mesaje	Explicație
Testarea conexiunii a eșuat. Verificați setările.	Acest mesaj apare din următoarele motive: <ul style="list-style-type: none"> <input type="checkbox"/> Adresa serverului LDAP este incorectă sau numărul de port este incorect. <input type="checkbox"/> Un interval de timp a expirat. <input type="checkbox"/> Opțiunea A nu se folosi este selectată ca Utilizare server LDAP. <input type="checkbox"/> Dacă Autentificare Kerberos este selectată ca Metodă de autentificare, setări precum Domeniu, Adresă KDC și Număr port (Kerberos) sunt incorecte.
Testarea conexiunii a eșuat. Verificați data și ora pe produsul dvs. sau pe server.	Acest mesaj apare când conexiunea eșuează deoarece setările de oră pentru scaner și pentru serverul LDAP nu corespund.
Autentificarea a eșuat. Verificați setările.	Acest mesaj apare din următoarele motive: <ul style="list-style-type: none"> <input type="checkbox"/> Nume utilizator și/sau Parolă sunt incorecte. <input type="checkbox"/> 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 scenerul este ocupat.

Setarea serverului de e-mail

Când utilizați **Sc. în ct. meu e-mail**, setați Server de e-mail.

Notă:

Puteți seta Sc. în ct. meu e-mail doar când s-a activat Scanare către e-mail.

La configurarea din Web Config:

Selectați fila **Rețea > Server e-mail > De bază**.

La configurarea din Epson Device Admin:

Selectați **Common > Email Server > Mail Server Settings** din șablonul de configurare.

Element	Setări și explicație	
Metodă de autentificare	Indicați metoda de autentificare pentru ca scenerul 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	Introduceți adresa de e-mail a expeditorului. Introduceți între 0 și 255 de caractere în ASCII (0x20–0x7E), exceptând : () < > [] ; ¥. Punctul „.” nu poate fi primul caracter.	

Element	Setări și explicație	
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 .
Validare certificat	Certificatul este autentificat atunci când este activată această funcție. Recomandăm setarea opțiunii la Activare .	
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	Dacă selectați POP înainte de SMTP ca Metodă de autentificare , specificați numărul portului. Introduceți un număr între 1 și 65535.	

Setarea Scanare în fold. meu

Salvează imaginile scanate în folderul atribuit fiecărui utilizator. Puteți seta următoarele ca un folder dedicat.

Notă:

Puteți seta Scan To My Folder doar când s-a activat Scanare către folder din rețea/FTP.

Setarea Salvare în	Metodă de autentificare	Locație de setare cale folder
Specificați un folder de rețea pentru toate Setări de autentificare pentru a crea automat un folder personal sub folderul specificat folosind numele ID-ului utilizatorului.	<input type="checkbox"/> Bază de date locală <input type="checkbox"/> LDAP <input type="checkbox"/> Bază de date locală și LDAP	Scanner (setare Scanare în fold. meu)
Alocați diferite foldere de rețea individual fiecărui utilizator.	Bază de date locală	Scanner (Setări utilizator)
	LDAP	Atribute LDAP
	Bază de date locală și LDAP	Scanner (Setări utilizator) sau atribute LDAP

La configurarea din Web Config:

Selectați fila **Securitate produs** > **Scanare către folder din rețea/FTP**.

La configurarea din Epson Device Admin:

Selectați **Administrator Settings** > **Authentication Settings** > **Scanare către folder din rețea/FTP** > **Scan to My Folder** din șablonul de configurare.

Element		Explicație
Setare salvare	Tip setare	<input type="checkbox"/> Partajat: Creează automat un folder denumit după ID-ul utilizatorului sub calea folderului sau URL-ul specificat în Salvare în și salvează imaginile scanate în acest folder. <input type="checkbox"/> Individual: Configurați destinația de salvare a rezultatelor de scanare pentru fiecare utilizator. Utilizatorii Bază de date locală pot fi configurați în setările utilizatorului. Utilizatorii LDAP folosesc locația de stocare achiziționată din atributele de căutare ale serverului LDAP.
	Tip	Selectați protocolul de transmisie în funcție de destinația de ieșire a scanării. Pentru un folder de rețea: Folder rețea (SMB) Pentru un server FTP: FTP
	Salvare în	Specificați calea sau URL-ul căii de ieșire. Introduceți maximum 160 de caractere în Unicode (UTF-16).
	Mod conectare	Setări atunci când selectați FTP în Tip . Selectați un mod de conexiune cu serverul FTP.
	Număr port	Setări atunci când selectați FTP în Tip . Introduceți numărul portului la care se vor trimite datele scanate la un server FTP, cuprins între 0 și 65535.
Setări de autentificare	Tip setare	Setări atunci când selectați Individual ca Tip setare în Setare salvare . Setări „Nume utilizator” și „Parolă” pentru a accesa folderul. <input type="checkbox"/> Partajat: Utilizați Nume utilizator și Parolă comune pentru toți utilizatorii. <input type="checkbox"/> Individual: Pentru utilizatorii Bază de date locală, setați Nume utilizator și Parolă individual în Setări utilizator . Utilizatorii LDAP nu pot fi configurați individual. Nume utilizator și Parolă setate de acest element sunt folosite ca lot.
	Nume utilizator	Introduceți numele de utilizator pentru a accesa folderul de destinație a datelor de scanare de ieșire. Introduceți maximum 30 de caractere în Unicode (UTF-16). Setări aceasta atunci când utilizați un server Partajat sau LDAP.
	Parolă	Introduceți parola corespunzătoare pentru Nume utilizator . Introduceți maximum 20 de caractere în Unicode (UTF-16). Setări aceasta atunci când utilizați un server Partajat sau LDAP.

Interzicerea schimbării destinației pentru Scanare către folder din rețea/FTP

Element	Explicație
Interziceți introducerea manuală a destinației	Când opțiunea este activată, utilizatorul nu poate modifica destinația implicită.

Personalizați funcțiile accesibile printr-o singură atingere

Puteți afișa doar pictogramele necesare prin editarea dispunerii pictogramelor afișate pe ecranul principal pentru panoul de control.

La configurarea din Web Config:

Selectați fila **Securitate produs** > **Personalizați funcțiile accesibile printr-o singură atingere**.

La configurarea din Epson Device Admin:

Selectați **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** din șablonul de configurare.

Notă:

În următoarele cazuri, pictogramele funcțiilor specificate nu sunt afișate pe ecranul principal.

- Atunci când selectați funcțiile care nu sunt permise din cauza **Restricții**.
- Atunci când nu este înregistrată adresa de e-mail pentru un utilizator conectat. (Sc. în ct. meu e-mail)
- Atunci când folderul de destinație nu este setat. (Scanare în fold. meu)

Element	Explicație
Funcții maxime per ecran	Selectați dispunerea pictogramelor afișate pe panoul de comandă. Imaginea se modifică în funcție de dispunerea selectată.
Ecran(e)	Selectați numărul de pagini.
Număr	Selectați funcțiile pe care doriți să le afișați pentru fiecare poziție numerotată.

Rapoarte Job History utilizând Epson Device Admin

Puteți crea un raport Job History pentru fiecare grup și fiecare utilizator, folosind Epson Device Admin. Puteți salva până la 3 000 de instanțe de istoric de utilizare în scanner. Puteți crea raportul specificând o perioadă sau definind un program regulat.

Pentru a genera Job History sub formă de raport, selectați **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** din meniul tip panglică din ecranul Listă dispozitive.

Pentru detalii despre cum să creați un raport de utilizator, consultați documentația pentru Epson Device Admin.


Elemente care pot fi incluse în raport


Puteți genera următoarele elemente în raportul utilizatorului.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Conectarea ca administrator din Panoul de comandă

Puteți utiliza oricare dintre următoarele metode pentru a vă conecta ca administrator de la panoul de comandă al scannerului.

1. Atingeți  în partea dreaptă sus a ecranului.
 - Când se activează Setări de autentificare, pictograma este afișată pe ecranul **Bun venit** (ecranul de așteptare a autentificării).
 - Când se dezactivează Setări de autentificare, pictograma este afișată pe ecranul principal.
2. Atingeți **Da** când este afișat ecranul de confirmare.
3. Introduceți parola administratorului.
Este afișat un mesaj de conectare completă, apoi este afișat ecranul principal pe panoul de comandă.

Pentru a vă deconecta, atingeți  în partea dreaptă sus a ecranului principal.

Dezactivarea Setări de autentificare

Puteți dezactiva Setări de autentificare folosind Web Config.

Notă:

Setări utilizator înregistrate la scanner vor fi salvate chiar dacă Setări de autentificare sunt dezactivate. Le puteți elimina restabilind scannerul la setările implicite.

1. Accesați Web Config.
2. Selectați fila **Securitate produs > De bază > Autentificare**.
3. Selectați **Dezactivat**.
4. Executați clic pe **Înainte**.
5. Executați clic pe **OK**.

Notă:

Chiar dacă dezactivați Setări de autentificare, Setare blocare rămâne activată. Dacă doriți să o dezactivați, puteți face setări din panoul de comandă sau din Web Config.

Informații conexe

- ➔ „Setarea Setare blocare de la panoul de comandă” la pagina 88
- ➔ „Setarea Setare blocare din Web Config” la pagina 88

Ștergerea informațiilor Setări de autentificare (Restaurare setări implicite)

Pentru a șterge toate informațiile despre Setări de autentificare (Cititor de carduri, Metodă de autentificare, Setări utilizator, și așa mai departe), restaurați toate setările scannerului la setările implicite din momentul achiziției.

Selectați **Setări > Administrare sistem > Restaurare setări implicite > Toate setările** pe panoul de comandă.



Important:

Toate contactele și alte setări de rețea vor fi, de asemenea, șterse. Setările șterse nu pot fi restabilite.

Rezolvarea problemelor

Nu se poate citi cardul de autentificare

Verificați următoarele aspecte.

- Verificați dacă dispozitivul de autentificare este conectat corect la scanner.
 - Conectați dispozitivul de autentificare la portul USB al interfeței externe de pe partea din spate a scannerului.
- Verificați dacă dispozitivul de autentificare și cardul de autentificare sunt acceptate.

Întreținere


Curățarea exteriorului scannerului.	156
Curățarea în interiorul scannerului.	156
Înlocuirea kitului de ansamblu rolă.	161
Resetarea numărului de scanări.	166
Economisirea energiei.	166
Transportarea scannerului.	167
Copierea de rezervă a setărilor.	168
Restaurare setări implicite.	169
Actualizarea aplicațiilor și a firmware-ului.	170

Curățarea exteriorului scannerului

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 scannerul. Se pot produce deformarea sau decolorarea.
- Nu permiteți pătrunderea apei în interiorul produsului. Aceasta poate cauza producerea unei defecțiuni.
- Nu deschideți niciodată carcasa scannerului.

1. Apăsați butonul  pentru a opri scannerul.
2. Deconectați adaptorul de alimentare cu curent alternativ de la scanner.
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 scannerului


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

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

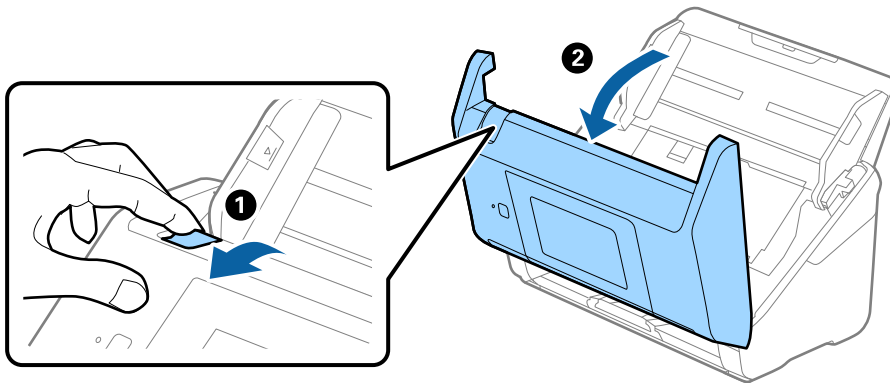
Dacă suprafața este pătată cu un material dificil de eliminat, utilizați un set de curățare Epson original pentru eliminarea petelor. Utilizați o cantitate redusă de soluție de curățare pe laveta de curățare pentru a elimina petele.

 **Important:**

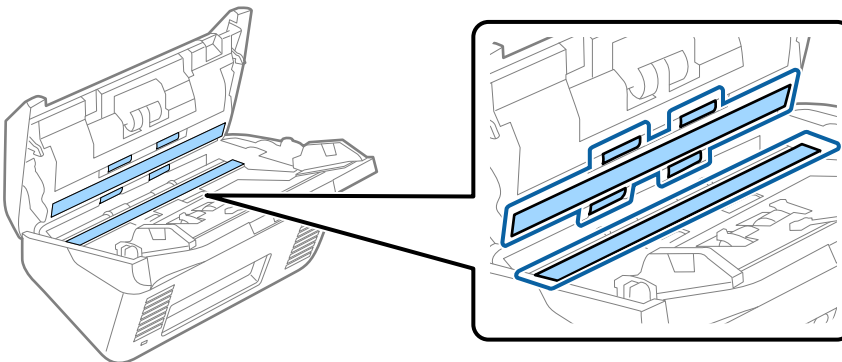
- Nu utilizați niciodată alcool, diluanți sau solvenți corozivi pentru a curăța scannerul. Se pot produce deformarea sau decolorarea.
- Nu pulverizați niciodată lichid sau lubrifianț pe scanner. Deteriorarea echipamentului sau a circuitelor poate duce la operații anormale.
- Nu deschideți niciodată carcasa scannerului.

1. Apăsați butonul  pentru a opri scannerul.
2. Deconectați adaptorul de alimentare cu curent alternativ de la scanner.

3. Trageți maneta și deschideți capacul scannerului.



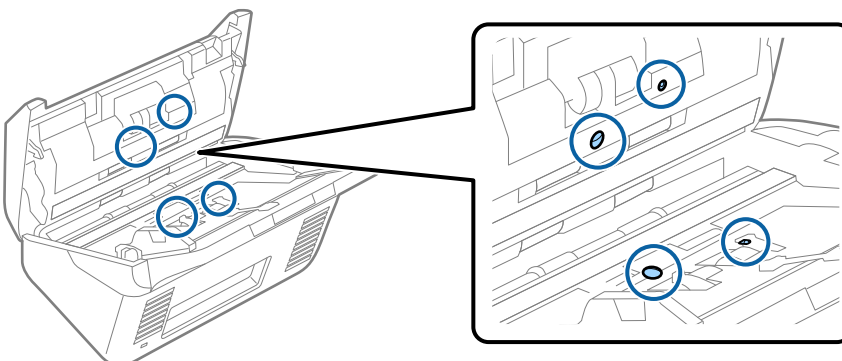
4. Ștergeți toate petele de pe rola de plastic și de pe suprafața de sticlă de la baza părții interioare a capacului scannerului, utilizând o lavetă moale sau un kit de curățare Epson original.



! Important:

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

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

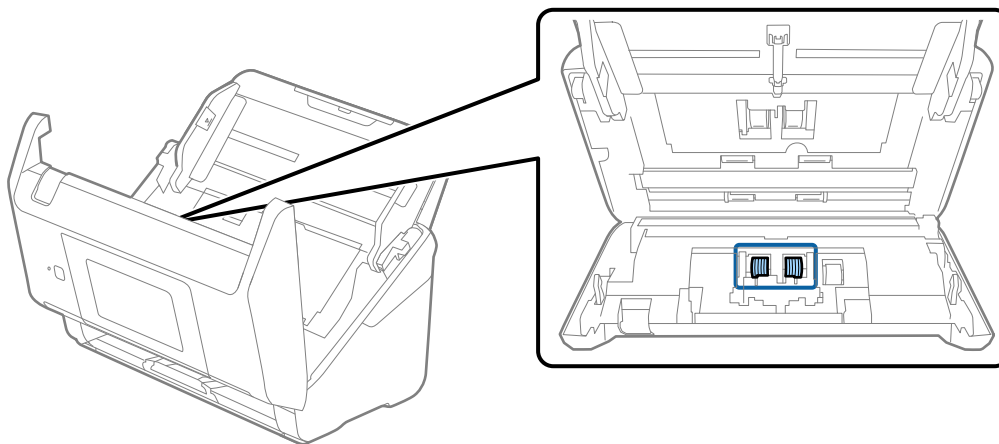


! *Important:*

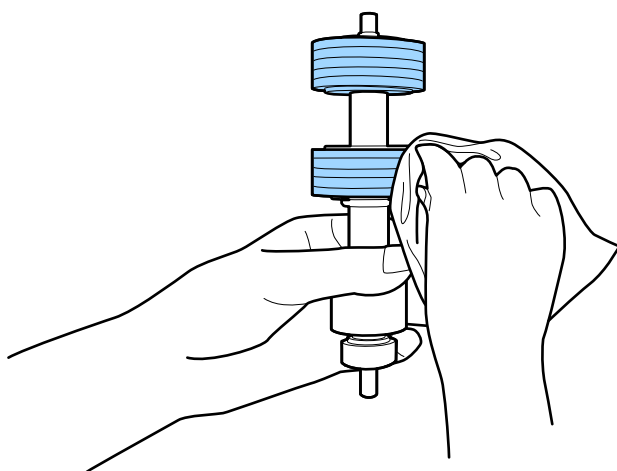
Nu utilizați lichide precum soluții de curățare pe tamponul de bumbac.

6. Deschideți capacul și scoateți rola de separare.

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



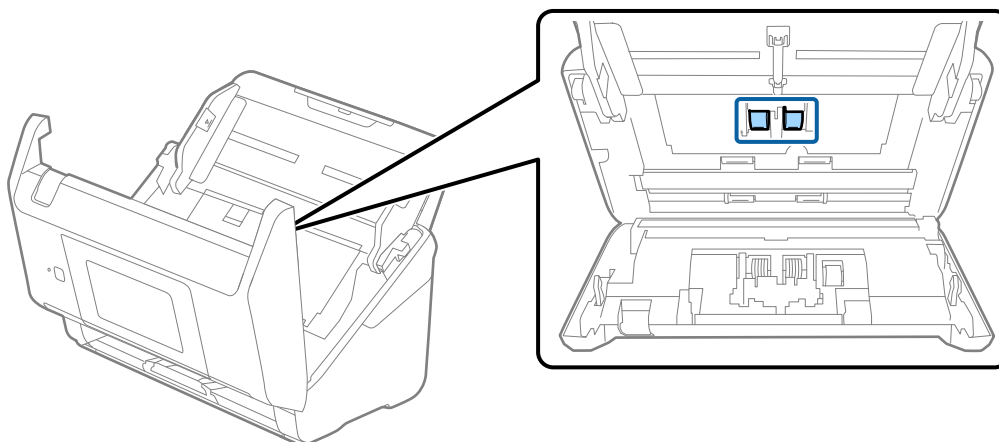
7. Ștergeți praful sau murdăria de pe rola de separare utilizând un set de curățare Epson original sau o lavetă moale, umedă.



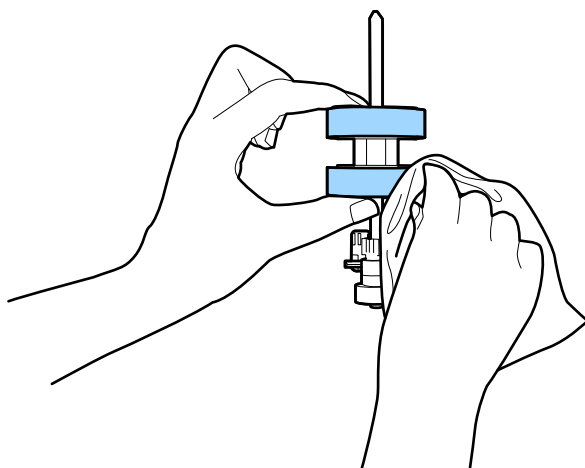
! *Important:*

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 praful sau murdăria de pe rola de preluare utilizând un set de curățare Epson original sau o lavetă moale, umedă.

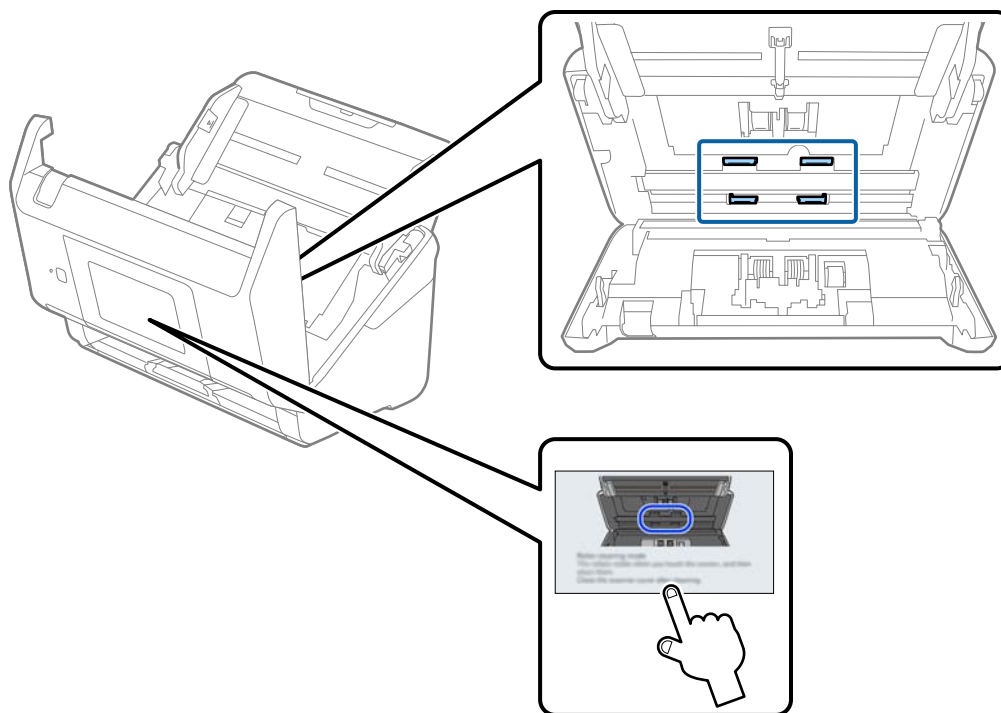


! Important:

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 scannerului.
11. Conectați adaptorul de alimentare cu curent alternativ și apoi porniți scannerul.
12. Selectați **Întreținere scanner** din ecranul principal.
13. În ecranul **Întreținere scanner**, selectați **Curățare role**.
14. Trageți maneta pentru a deschide capacul scannerului.
Scannerul 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.

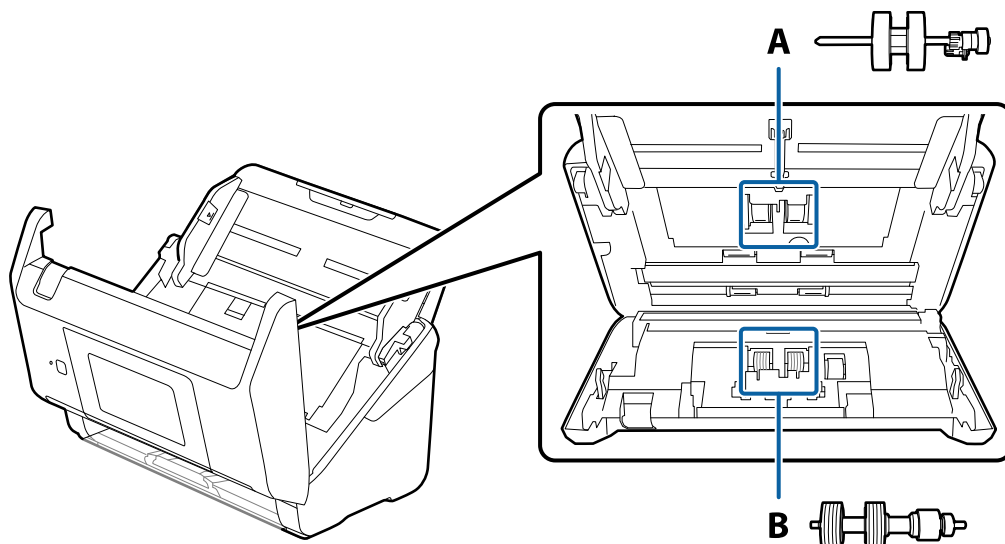
16. Închideți capacul scannerului.
Scannerul iese din modul de curățare a rolei.

Informații conexe


➔ „Înlocuirea kitului de ansamblu rolă” la pagina 161

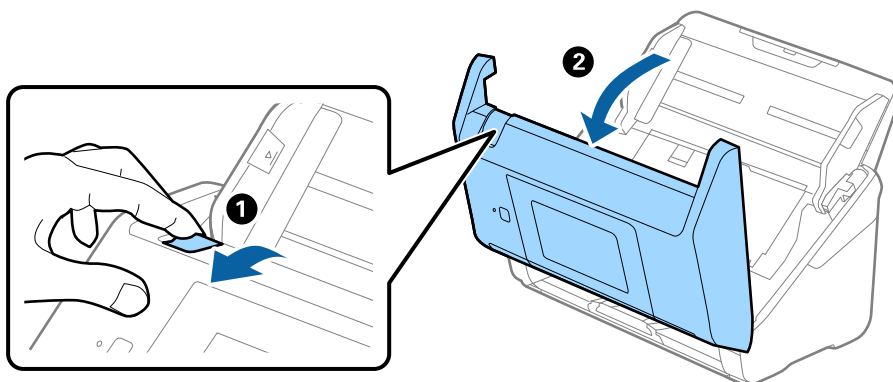
Înlocuirea kitului de ansamblu rolă

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

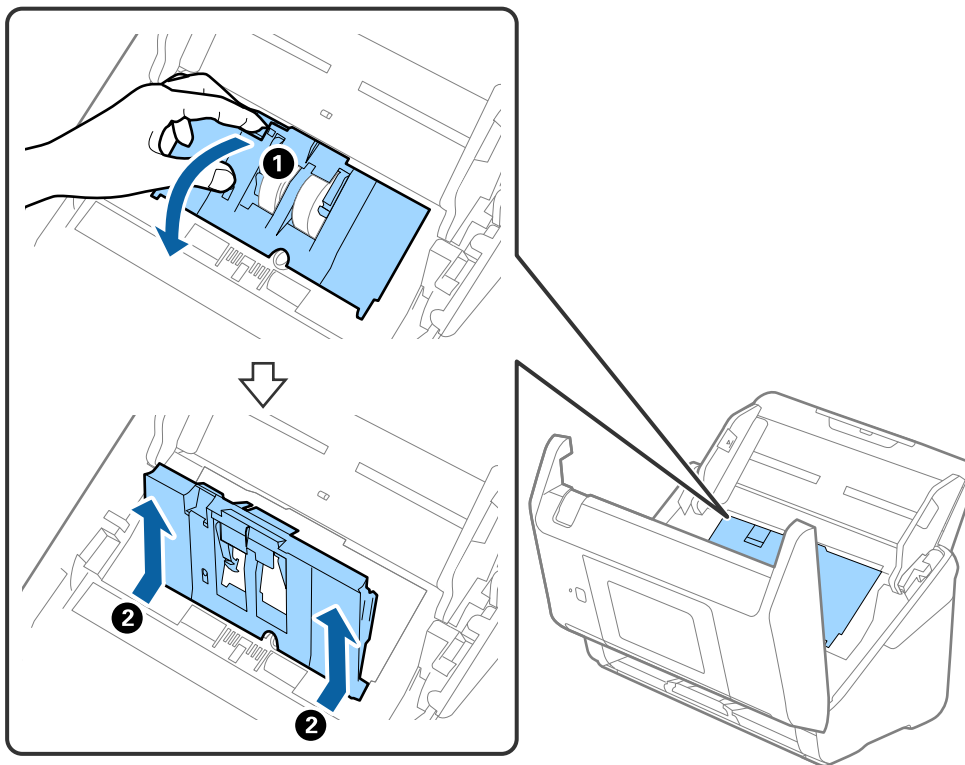


A: rolă de preluare, B: rolă de separare

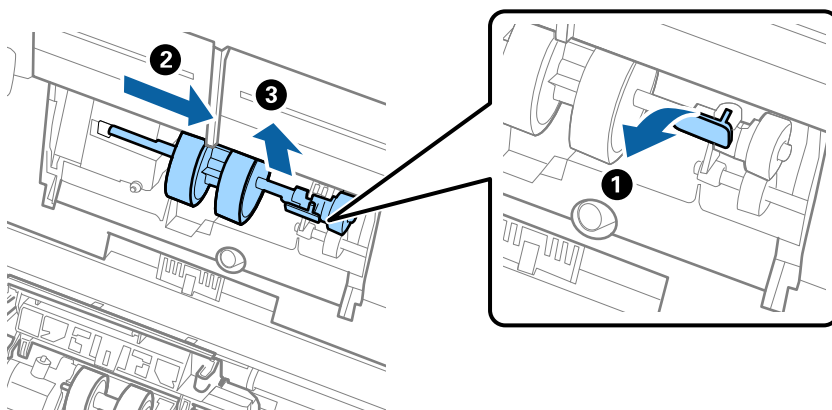
1. Apăsați butonul  pentru a opri scannerul.
2. Deconectați adaptorul de alimentare cu curent alternativ de la scanner.
3. Trageți maneta și deschideți capacul scannerului.



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



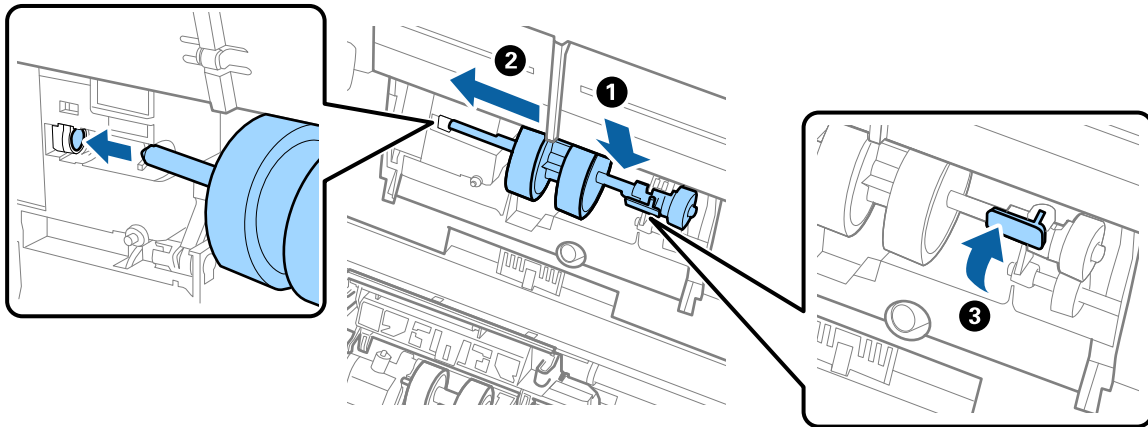
5. Trageți în jos sistemul de prindere al axei rolei, apoi glisați și îndepărtați rolele de preluare instalate.



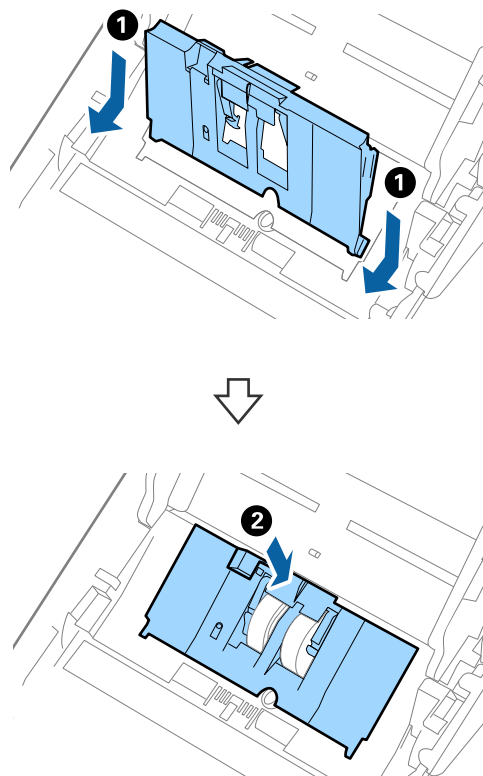
Important:

Nu trageți forțat rola de preluare. Aceasta poate deteriora partea interioară a scannerului.

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

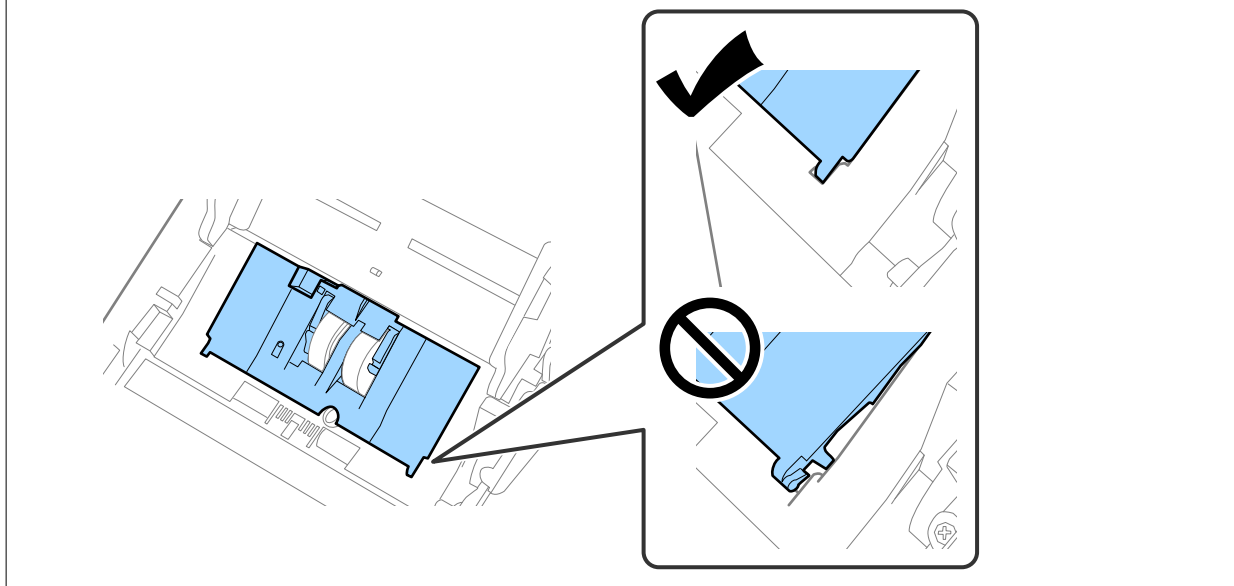


7. Introduceți marginea capacului rolei de preluare în canal și glisați-o. Închideți ferm capacul.

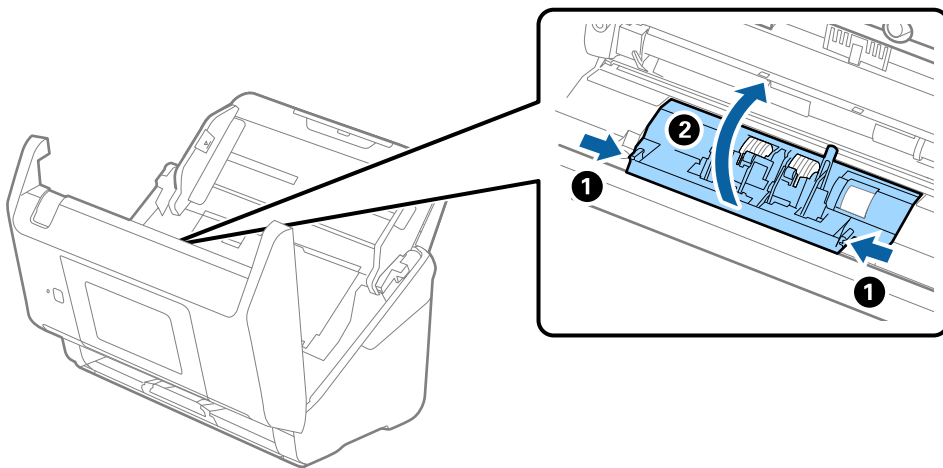


! *Important:*

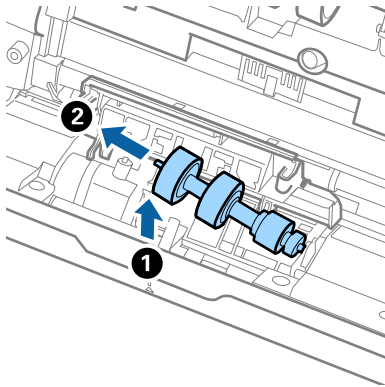
- ❑ Asigurați-vă că este corect închis capacul rolei de preluare.
- ❑ În cazul în care capacul se închide cu dificultate, asigurați-vă că rolele de preluare sunt corect instalate.
- ❑ Nu instalați capacul în poziție ridicată.



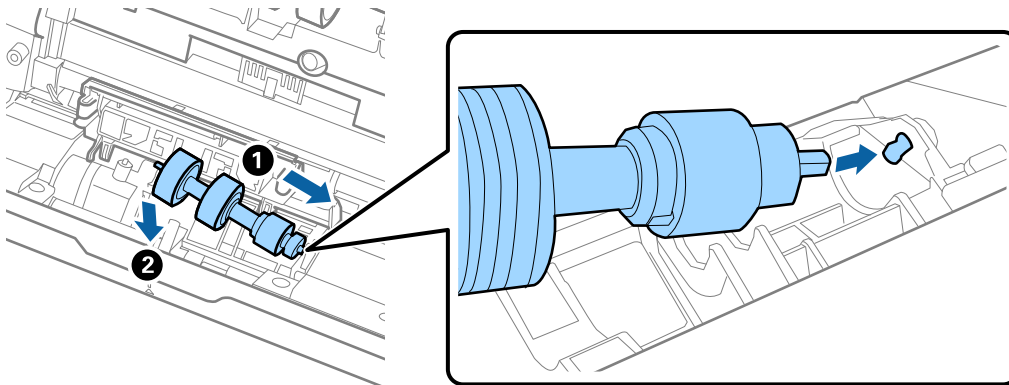
8. Apăsați pe cârligele de la ambele capete ale capacului rolei de separare pentru a deschide capacul.



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.

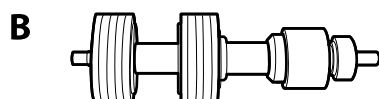
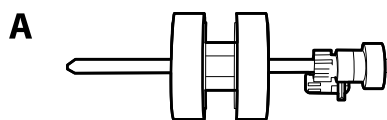
12. Închideți capacul scannerului.
13. Conectați adaptorul de alimentare cu curent alternativ și apoi porniți scannerul.
14. Resetați numărul de scanări de la panoul de comandă.

Notă:

Eliminați rola de preluare și rola de separare, respectând normele și regulamentele autorității locale. Nu le dezamblați.

Coduri ale kiturilor de ansamblu rolă

Piese 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: rolă de preluare, B: rolă de separare

Nume piesă	Coduri	Ciclu de viață
Kit ansamblu rolă	B12B819671 B12B819681 (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

Resetați numărul de scanări după înlocuirea setului de asamblare a rolor.

1. Selectați **Setări** > **Informații dispozitiv** > **Resetați numărul de scanări** > **Număr de scanări după înlocuirea rolei** din ecranul principal.
2. Atingeți **Da**.

Informații conexe

➔ „Înlocuirea kitului de ansamblu rolă” la pagina 161

Economisirea energiei

Puteți economisi energie utilizând modul Inactiv sau modul cu oprire automată atunci când scannerul nu execută nicio operație. Puteți stabili intervalul de timp după care scannerul intră în modul Inactiv și se oprește automat. Orice creștere va afecta eficiența energetică a produsului. Luați în considerare mediul înainte de a efectua orice modificări.

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


2. Selectați **Setări de bază**.
3. Selectați **Setări oprire**, apoi realizați setările.

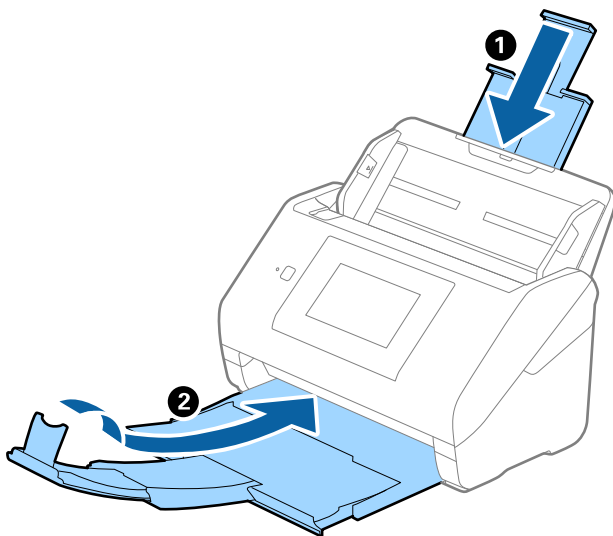
Notă:

Caracteristicile disponibile pot varia în funcție de locația de achiziție.

Transportarea scannerului

Când trebuie să transportați scannerul pentru a-l muta sau pentru reparații, urmați pașii de mai jos pentru a-l împacheta.

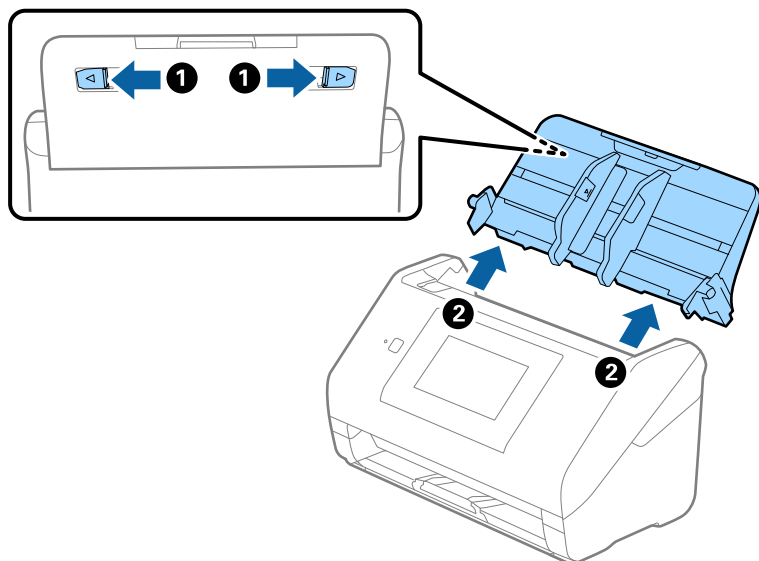
1. Apăsați pe butonul  pentru a opri scannerul.
2. Deconectați adaptorul de c.a.
3. Scoateți cablurile și dispozitivele.
4. Închideți extensia tăvii de intrare și tava de ieșire.



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 scannerul, apoi împachetați din nou scannerul 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 scannerului etc.

Fișierul exportat nu poate fi editat, deoarece este exportat ca fișier binar.

Exportarea setărilor

Exportați setarea pentru scanner.

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 scannerului, 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 scannerul de înlocuire.*

Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

Importați setările

Importați fișierul exportat Web Config la nivelul scannerului.



Important:

La importarea valorilor care includ informații individuale, precum numele scannerului 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 scannerului.


Informații conexe

➔ „Executarea utilitarului Web Config într-un browser web” la pagina 36

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 setare înregistrate pe scanner, inclusiv contactele și setările de autentificare ale utilizatorului, vor fi șterse. Setările șterse nu pot fi restabilite.

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 scannerul în timpul actualizării.

Notă:

Când scannerul 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 scannerul 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 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 scannerului utilizând panoul de comandă

Dacă scannerul poate fi conectată la Internet, puteți actualiza firmware-ul acestuia utilizând panoul de comandă. De asemenea, puteți configura scannerul 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

➔ [„Executarea utilitarului Web Config într-un browser web” la pagina 36](#)

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. Dacă nu puteți efectua actualizarea prin rețea, încercați această metodă.

Notă:

Înainte de a efectua actualizarea, asigurați-vă că driverul de scaner Epson Scan 2 este instalat pe computerul dumneavoastră. Dacă Epson Scan 2 nu este instalat, instalați-l din nou.

1. Verificați site-ul web Epson pentru cele mai recente lansări de actualizări pentru firmware.
<http://www.epson.com>
 - Dacă firmware-ul pentru scanerul dumneavoastră există, descărcați-l și treceți la pasul următor.
 - Dacă nu există nicio informație cu privire la firmware pe site-ul web, atunci utilizați deja cea mai recentă versiune.
2. Conectați la scaner computerul care conține firmware-ul descărcat prin intermediul cablului USB.
3. Faceți dublu clic pe fișierul .exe descărcat.
Aplicația Epson Firmware Updater pornește.
4. Urmați instrucțiunile de pe ecran.