EPSON
EXCEED YOUR VISION

Ghidul administratorului

NPD5668-00 RO

Cuprins

Cuprins

Anexă

Setări de securitate avansate la nivel de întreprindere

Drept de proprietate intelectuală

Mărci înregistrate

- ❏ EPSON® este o marcă comercială înregistrată, iar EPSON EXCEED YOUR VISION sau EXCEED YOUR VISION este o marcă comercială a Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Notă generală: În publicația de față sunt utilizate alte nume de produse doar în scopuri de identificare și acestea pot fi mărci comerciale ale proprietarilor respectivi. Epson își declină orice drepturi asupra acestor mărci.

Despre acest manual

Indicatoare şi simboluri

> ⚠ ***Atenție:***
> *Instrucțiuni care trebuie urmate cu strictețe pentru a evita leziunile corporale.*

> ***Important:***
> *Instrucțiuni care trebuie respectate pentru a evita deteriorarea echipamentelor dumneavoastră.*

Notă:
Instrucțiuni care conțin indicații utile și restricții cu privire la operarea scanerului.

Informații conexe

➡ Făcând clic pe această pictogramă, aveți acces la informațiile conexe.

Figurile utilizate în acest manual

❏ Capturile de ecran cu driver-ul scannerului şi Epson Scan 2 (driver-ul scanerului) sunt efectuate în Windows 10 sau OS X El Capitan. Conținutul afișat pe ecran diferă în funcție de model și situație.

❏ Ilustrațiile utilizate în acest manual sunt doar exemple. Cu toate că în funcție de model pot exista mici diferențe, modul de funcționare este același.

❏ Unele elemente din meniul afișat pe ecranul LCD diferă în funcție de model şi de setările definite.

Referințe la sisteme de operare

Windows

În acest manual, termeni precum „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Vista”, „Windows XP”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012”, „Windows Server 2008 R2”, „Windows Server 2008”, „Windows Server 2003 R2”, şi „Windows Server 2003” se referă la următoarele sisteme de operare. În plus, termenul „Windows” este utilizat cu referire la toate versiunile.

❏ Sistem de operare Microsoft® Windows® 10

❏ Sistem de operare Microsoft® Windows® 8.1

❏ Sistem de operare Microsoft® Windows® 8

❏ Sistem de operare Microsoft® Windows® 7

❏ Sistem de operare Microsoft® Windows Vista®

❏ Sistem de operare Microsoft® Windows® XP

❏ Sistem de operare Microsoft® Windows® XP Professional x64 Edition

- ❏ Sistem de operare Microsoft® Windows Server® 2016
- ❏ Sistem de operare Microsoft® Windows Server® 2012 R2
- ❏ Sistem de operare Microsoft® Windows Server® 2012
- ❏ Sistem de operare Microsoft® Windows Server® 2008 R2
- ❏ Sistem de operare Microsoft® Windows Server® 2008
- ❏ Sistem de operare Microsoft® Windows Server® 2003 R2
- ❏ Sistem de operare Microsoft® Windows Server® 2003

Mac OS

În acest manual, „Mac OS" este utilizat pentru a se referi la macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x șiMac OS X v10.6.8.

Introducere

Componentă manual

Acest manual este destinat administratorului de dispozitiv responsabil de conectarea imprimantei sau scannerului la rețea și conține informații privind efectuarea setărilor pentru a utiliza funcțiile.

Consultați *Ghidul utilizatorului* pentru informații privind utilizarea funcțiilor.

Pregătirea

Explică sarcinile administratorului, modul de setare a dispozitivelor și software-ul pentru gestionare.

Conectarea

Explică modul de conectare a unui dispozitiv la rețea sau linia telefonică. Explică, de asemenea, mediul de rețea, precum utilizarea unui port pentru dispozitiv și informațiile privind DNS și serverul proxy.

Setări funcționale

Explică setările pentru fiecare funcție a dispozitivului.

Setări de securitate de bază

Explică setările pentru fiecare funcție, cum ar fi tipărirea, scanarea și faxul.

Setări de operare și gestionare

Explică operațiunile după începerea utilizării dispozitivelor, cum ar fi verificarea informațiilor și întreținerea.

Rezolvarea problemelor

Explică inițializarea setărilor și rezolvarea problemelor de rețea.

Setări de securitate avansate la nivel de întreprindere

Explică metoda de setare pentru a îmbunătăți securitatea dispozitivului, cum ar fi utilizarea Certificatului CA, a comunicării SSL/TLS și a filtrării IPsec/IP.

În funcție de model, unele funcții din acest capitol nu sunt acceptate.

Definiții ale termenilor utilizați în acest ghid

Următorii termeni sunt utilizați în acest ghid.

Administrator

Persoana responsabilă de instalarea și configurarea dispozitivului sau rețelei în cadrul unui birou sau organizații. Pentru organizații mici, această persoană poate fi responsabilă atât de administrarea dispozitivului, cât și de administrarea rețelei. Pentru organizații mari, administratorii au autoritate asupra rețelei sau dispozitivelor din cadrul grupului unui departament sau divizii, iar administratorii de rețea sunt responsabili de setările de comunicare cu exteriorul organizației, precum conexiunea Internet.

Introducere

Administratorul rețelei

Persoana responsabilă de controlarea comunicării prin rețea. Persoana care configurează routerul, serverul proxy, serverul DNS; i severul de e-mail pentru a controla comunicarea prin Internet sau prin rețea.

Utilizator

Persoana care utilizează dispozitive precum imprimanta sau scanerele.

Web Config (pagina web a dispozitivului)

Serverul web care este integrat în dispozitiv. Acesta este denumit Web Config. Puteți verifica și modifica starea dispozitivului utilizând browser-ul.

Instrument

Un termen generic pentru software-ul de configurare sau gestionare dispozitiv, cum ar fi Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, etc.

Scanare tip push

Un termen generic pentru scanarea de la panoul de control al dispozitivului.

ASCII (American Standard Code for Information Interchange — Cod standard american pentru schimb de informații)

Unul dintre codurile de caractere standard. Sunt definite 128 de caractere, inclusiv caractere precum cele din alfabet (a – z, A – Z), numere arabe (0 – 9), simboluri, spații goale și caractere de control. Când „ASCII” este descris în acest dispozitiv, indică 0x20 – 0x7E (număr hex) listate mai jos și nu implică niciun caracter de control.

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

* Caracter spațiu.

Unicode (UTF-8)

Un cod standard internațional, acoperind majoritatea limbilor globale. Când „UTF-8” este descris în acest ghid, sunt indicate caractere de codare în format UTF-8.

Pregătirea

Acest capitol explică rolul administratorului și pregătirea înainte de efectuarea setărilor.

Fluxul de setări scaner și gestionarea

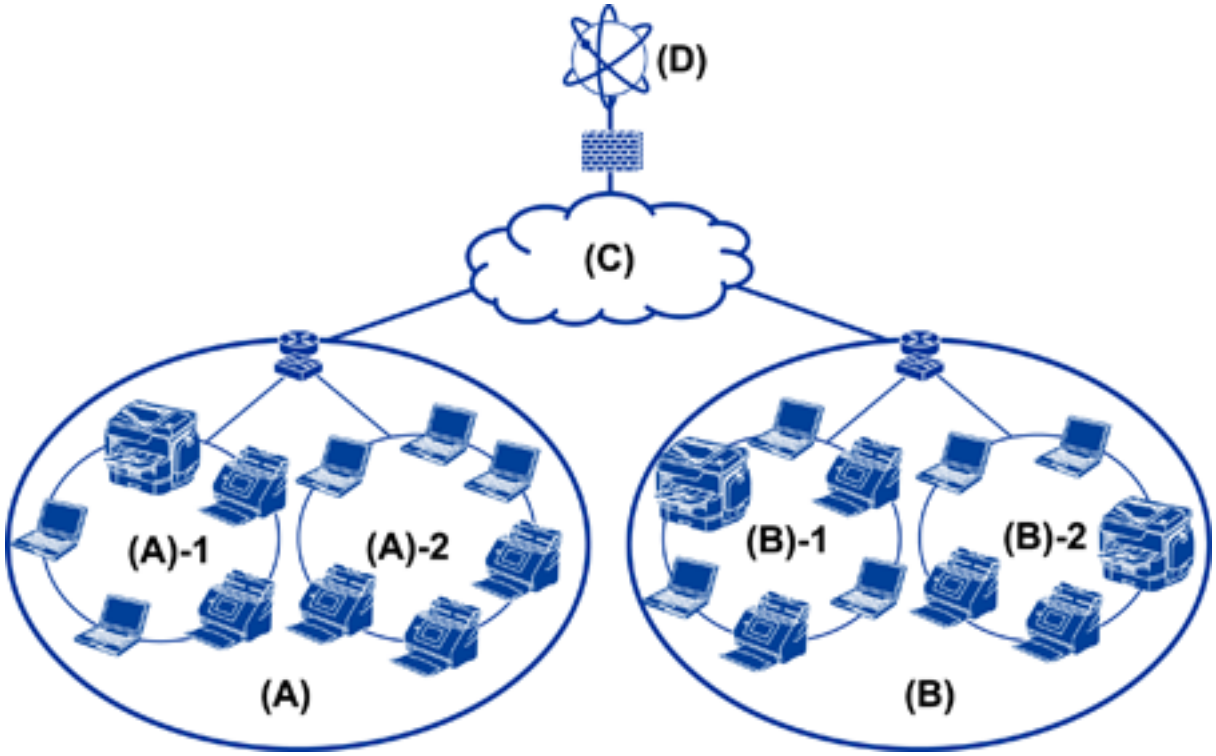
Administratorul efectuează setările de conectare la rețea, configurarea inițială și întreținerea pentru scaner astfel încât acestea să fie disponibile pentru utilizatori.

1. Pregătirea
   - ❏ Colectarea informațiilor de setare conexiune
   - ❏ Decizie privind metoda de conectare
2. Conectarea
   - ❏ Conexiune la rețea de la panoul de control al scanerului
3. Setarea funcțiilor
   - ❏ Setările driverului scanerului
   - ❏ Alte setări avansate
4. Setări de securitate
   - ❏ Setări de administrator
   - ❏ SSL/TLS
   - ❏ Control protocol
   - ❏ Setări de securitate avansate (opțiune)
5. Operare și gestionarea
   - ❏ Verificarea stării dispozitivului
   - ❏ Gestionarea în caz de urgență
   - ❏ Copierea de rezervă a setărilor dispozitivului

Informații conexe

➡ „Pregătirea” la pagina 10
➡ „Conectarea” la pagina 15
➡ „Setări funcționale” la pagina 22
➡ „Setări de securitate de bază” la pagina 32
➡ „Setări de operare și gestionare” la pagina 40

Exemplu de mediu de rețea



(A): Birou 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Birou 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Prezentarea exemplului de setare conexiune scaner

Există, în principal, două tipuri de conexiune, în funcție de modul de utilizare a scanerului. Ambele conectează scanerul la rețeaua computerului prin hub.

❏ Conexiune server/client (scanner utilizând server Windows, gestionare sarcini)

❏ Conexiune peer to peer (conexiune directă prin computer client)

Informații conexe

➡ „Conexiune server/client” la pagina 12

➡ „Conexiune Peer to Peer” la pagina 12

Conexiune server/client

Centralizați managementul scanerului și operațiunilor cu Document Capture Pro Server instalat pe server. Este ideal pentru lucrări care utilizează scanere multiple pentru a scana un număr mare de documente cu un anumit format.

Informații conexe

➡ „Definiții ale termenilor utilizați în acest ghid” la pagina 8

Conexiune Peer to Peer

Utilizați un scaner individual cu un driver de scaner, cum ar fi Epson Scan 2 instalat pe computerul client. Instalarea Document Capture Pro (Document Capture) pe computerul client vă permite să executați operațiuni pe computerele client individuale ale scanerului.

Informații conexe

➡ „Definiții ale termenilor utilizați în acest ghid” la pagina 8

Pregătirea conexiunii la o rețea

Colectarea informațiilor privind setarea conexiunii

Trebuie să aveți o adresă IP, adresă de gateway etc. pentru conexiune la rețea. Verificați următoarele în avans.

Divizii	Elemente	Notă
Metodă de conectare dispozitiv	❏ Ethernet	Utilizați un cablu de categoria 5e sau STP (Shielded Twisted Pair — Pereche torsadată ecranată) pentru conexiunea Ethernet.
Informații conexiune LAN	❏ Adresă IP ❏ Mască subrețea ❏ Gateway implicit	Dacă ați setat automat adresa IP utilizând funcția DHCP a routerului, aceasta nu este necesară.
Informații server DNS	❏ Adresa IP pentru DNS primar ❏ Adresa IP pentru DNS secundar	Dacă utilizați o adresă IP statică pentru adresa IP, configurați serverul DNS. Configurați când se va efectua automat alocarea utilizând funcția DHCP și când serverul DNS nu poate fi alocat automat.
Informații server proxy	❏ Nume server proxy ❏ Număr port	Configurați când se utilizează un server proxy pentru conexiunea la Internet și când se utilizează serviciul Epson Connect sau funcția de actualizare automată a firmware-ului.

Specificațiile scanerului

Pentru specificații privind scanerul în mod standard sau mod de conectare, consultați *Ghidul utilizatorului*.

Utilizare număr port

Consultați „Anexa” pentru a vedea ce număr de port utilizează scanerul.

Informații conexe

➡ „Utilizarea portului pentru scaner” la pagina 60

Tipul de atribuire al adresei IP

Există două tipuri de atribuire a unei adrese IP către scanner.

Adresă IP statică:

Atribuirea adresei IP unice predeterminate către scanner.

Adresa IP nu se schimbă nici atunci când scanerul sau routerul sunt închise, așa că puteți administra dispozitivul cu ajutorul adresei IP.

Acest tip este adecvat pentru o rețea care administrează multe scanere, de exemplu un birou sau o școală de dimensiuni mari.

Alocarea automată a funcției DHCP:

Adresa IP corectă este alocată în mod automat atunci când se realizează comunicația între scanner și routerul care este compatibil cu funcția DHCP.

În cazul în care nu este convenabil să modificați adresa IP pentru un anumit dispozitiv, salvați adresa IP în prealabil și apoi alocați-o.

Server DNS și server proxy

Dacă utilizați un serviciu de conexiune la Internet, configurați serverul DNS. Dacă nu îl configurați, trebuie să specificați o adresă IP pentru accesare, deoarece denumirea nu va fi stabilită.

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

Puteți interzice accesul la un anumit URL utilizând funcția de filtrare, deoarece serverul proxy este capabil să verifice conținutul comunicării.

Metodă pentru setarea conexiunii la rețea

Pentru setările de conexiune pentru adresa IP a scanerului, masca de subrețea și gateway-ul implicit, se procedează după cum urmează.

Folosind panoul de control:

Configurați setările utilizând panoul de control al scanerului pentru fiecare scaner. Conectați la rețea după configurarea setărilor de conexiune ale scanerului.

Folosind aplicația de instalare:

Dacă este utilizată aplicația de instalare, rețeaua scanerului și computerul client sunt setate automat. Setarea este disponibilă urmând instrucțiunile aplicației de instalare, chiar dacă nu aveți cunoștințe profunde privind rețeaua.

Utilizând un instrument:

Utilizați un instrument de la computerul administratorului. Puteți descoperi un scaner și apoi seta scanerul, sau puteți crea un fișier SYLK, pentru a efectua setările în lot la scanere. Puteți seta mai multe scanere, dar acestea trebuie conectate fizic prin cablu Ethernet înainte de setare. Prin urmare, acest lucru este recomandat în cazul în care puteți configura o rețea Ethernet pentru setare.

Informații conexe

➡ „Conectarea la rețea de la panoul de control” la pagina 15

➡ „Conectarea la rețea folosind aplicația de instalare” la pagina 19

➡ „Alocarea unei adrese IP utilizând EpsonNet Config” la pagina 56

Conectarea

Acest capitol explică mediul sau procedura de conectare a scanerului la rețea.

Conectarea la rețea

Conectarea la rețea de la panoul de control

Conectați scanerul la rețea folosind panoul de control al scanerului.

Pentru panoul de control al scanerului, consultați *Ghidul utilizatorului* pentru mai multe detalii.

Alocarea adresei IP

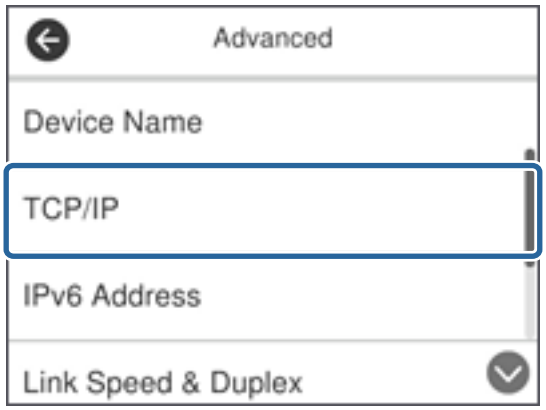
Configurați elementele de bază, precum Adresă IP, Mască subrețea și Gateway implicit.

1. Conectați scanerul la sursa de alimentare electrică.
2. Glisați pe ecran spre stânga pe panoul de control al scanerului, apoi atingeți **Setări**.

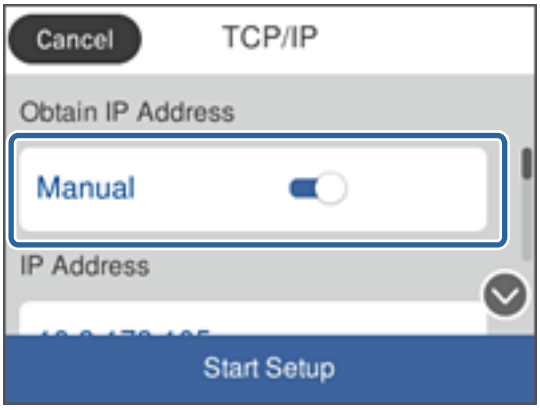
3. Atingeți **Setări rețea** > **Modificați setările**.

   Dacă elementul nu este afișat, glisați pe ecran în sus pentru a-l afișa.

4. Atingeți **TCP/IP**.

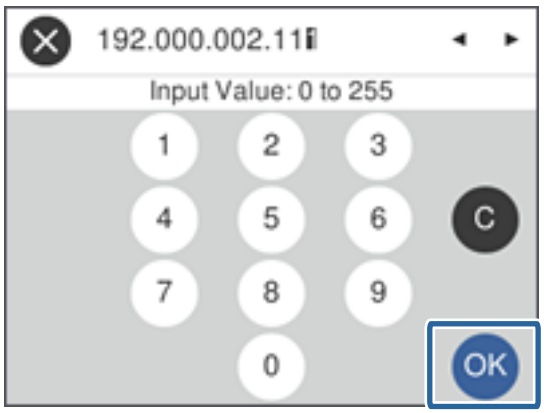


5. Selectați **Manual** pentru **Obținere parolă IP**.



Notă:
Când setați adresa IP automat utilizând funcția DHCP a routerului, selectați ***Automat****. În acel caz,* ***Adresă IP****,* ***Mască subrețea****, și* ***Gateway implicit*** *din pașii 6 – 7 sunt, de asemenea, setate automat, deci mergeți la pasul 8.*

6. Atingeți câmpul **Adresă IP**, introduceți adresa IP utilizând tastatura afișată pe ecran și apoi atingeți **OK**.



Confirmați valoarea reflectată pe ecranul anterior.

7. Configurați **Mască subrețea** și **Gateway implicit**.

Confirmați valoarea reflectată pe ecranul anterior.

Notă:
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.*

8. Atingeți câmpul **DNS principal** pentru **Server DNS**, introduceți adresa IP pentru serverul DNS primar utilizând tastatura afișată pe ecran și apoi atingeți **OK**.

   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 10.*

9. Atingeți câmpul **DNS secundar**, introduceți adresa IP pentru serverul DNS secundar utilizând tastatura afișată pe ecran și apoi atingeți **OK**.

   Confirmați valoarea reflectată pe ecranul anterior.

10. Atingeți **Pornire configurare**.

11. Atingeți **Închidere** pe ecranul de confirmare.

    Ecranul se va închide automat, după o anumită perioadă de timp, dacă nu atingeți **Închidere**.

Conectarea la Ethernet

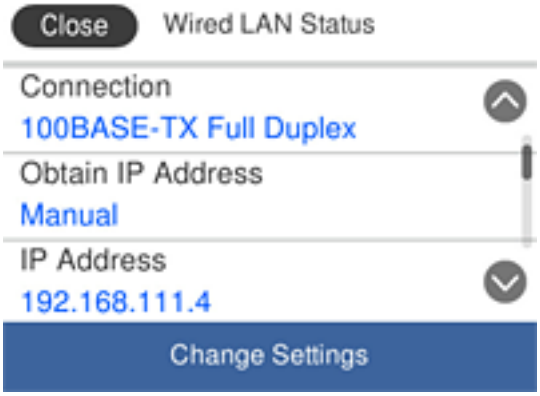
Conectați scanerul la rețea, utilizând un cablu Ethernet și verificați conexiunea.

1. Conectați scanerul și hubul (switch L2) prin cablu Ethernet.

   Pictograma de pe ecranul principal se modifică la  .

2. Atingeți  pe ecranul de pornire.

3. Glisați pe ecran în sus și apoi asigurați-vă că starea conexiunii și adresa IP sunt corecte.



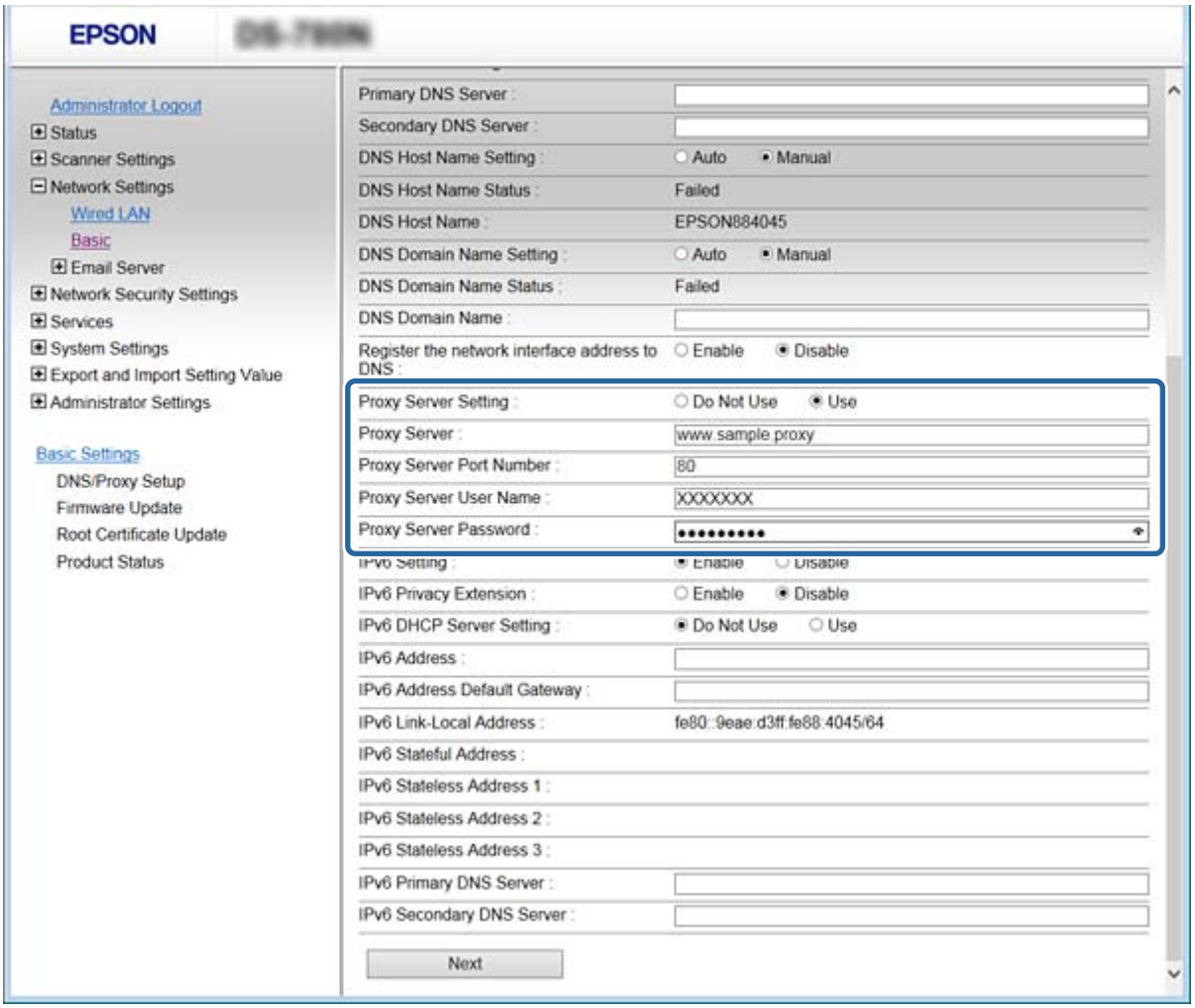
Setarea serverului proxy

Serverul proxy nu poate fi setat pe panou. Configurați utilizând Web Config.

1. Accesați Web Config și selectați **Network Settings** > **Basic**.
2. Selectați **Use** în **Proxy Server Setting**.
3. Specificați serverul proxy în adresa IPv4 sau formatul FQDN în **Server proxy** și apoi introduceți numărul de port în **Proxy Server Port Number**.

   Pentru servere proxy care necesită autentificare, introduceți numele de utilizator și parola pentru autentificarea la serverul proxy.

4. Executați clic pe butonul **Next**.



5. Confirmați setările și apoi executați clic pe **Setări**.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Conectarea la rețea folosind aplicația de instalare

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

❏ Configurarea de pe site-ul web

Accesați următorul site web și apoi 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 prevăzute cu unități de disc)

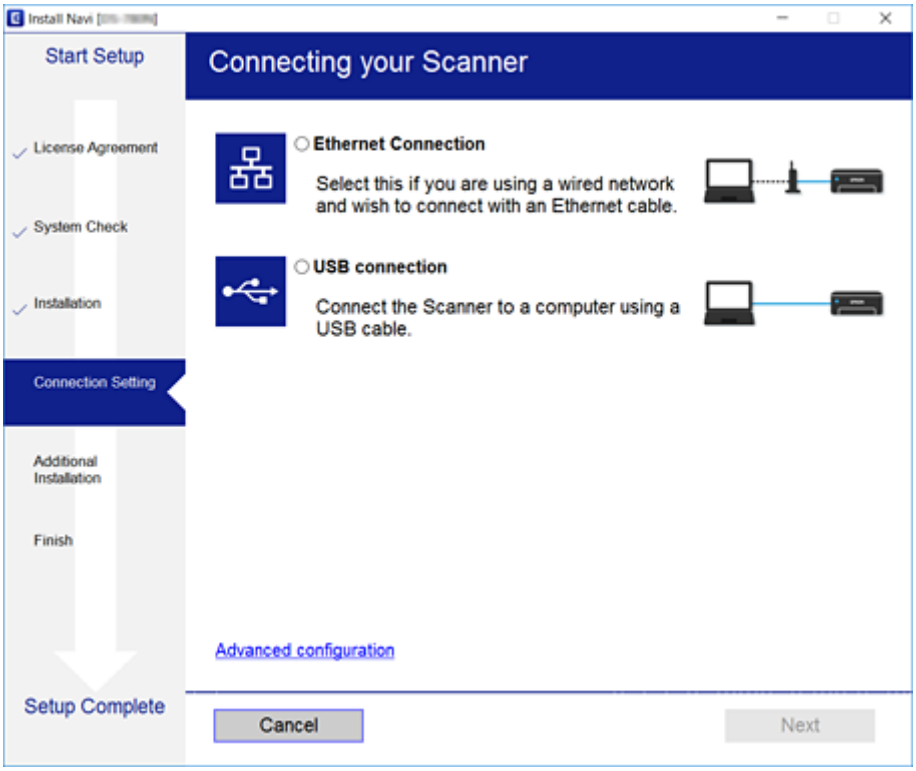
Introduceți discul cu software în computer și urmați instrucțiunile de pe ecran.

Selectarea metodelor de conectare

Urmați instrucțiunile de pe ecran până la afișarea ecranului următor, apoi selectați metoda de conectare a scanerului la computer.

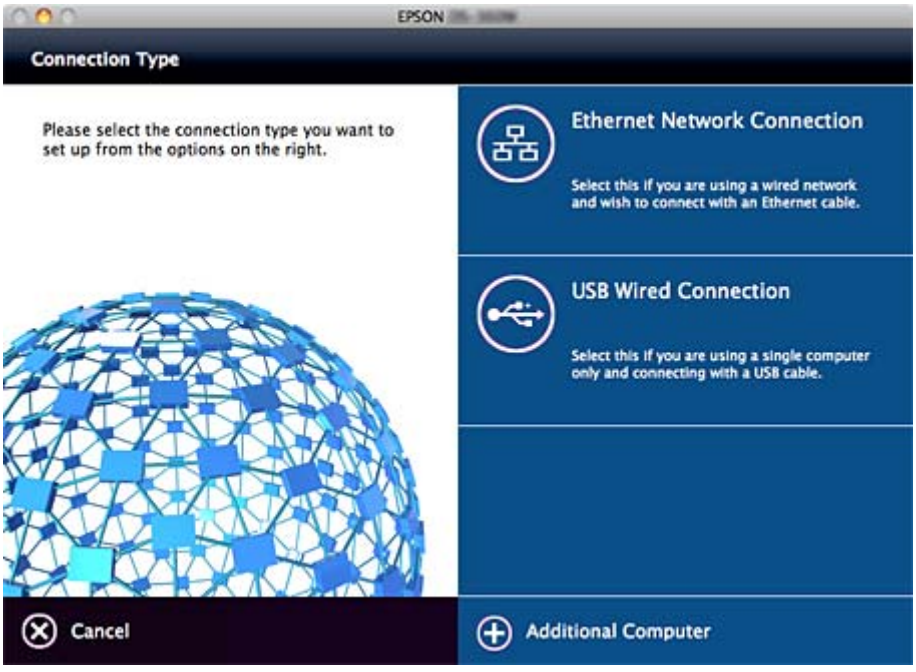
❏ Windows

Selectați tipul de conexiune și faceți clic pe **Înainte**.



❏ Mac OS

Selectați tipul de conexiune.



Conectarea

Urmați instrucțiunile afișate pe ecran. Software-ul necesar este instalat.

Setări funcționale

Acest capitol explică primele setări care trebuie efectuate pentru a utiliza fiecare funcție a acestui dispozitiv.

Software pentru setare

În această expunere, este explicată procedura pentru efectuarea setărilor de la computerul administratorului folosind Web Config.

Web Config (pagină web pentru dispozitive)

Despre Web Config

Web Config este o aplicație bazată pe browser pentru configurarea setărilor scanerului.

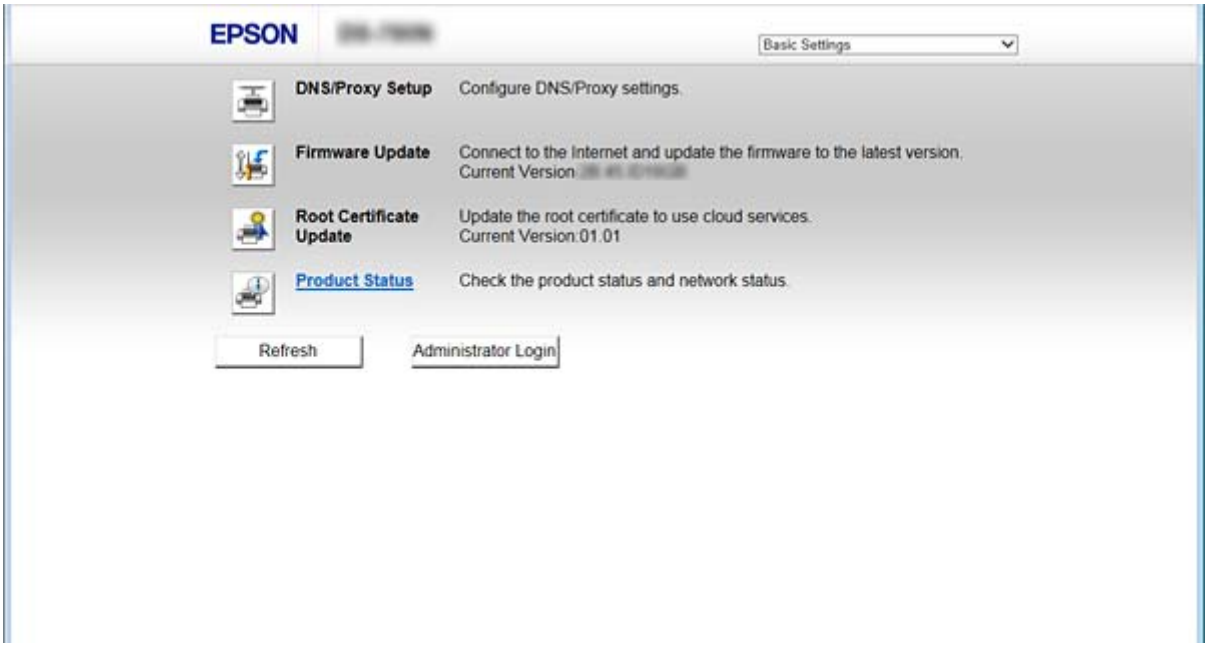
Pentru a accesa Web Config, trebuie să primiți mai întâi o adresă IP pentru scaner.

Notă:
Puteți bloca setările prin configurarea parolei de administrator pentru scaner.

Regăsiți mai jos două pagini de setări.

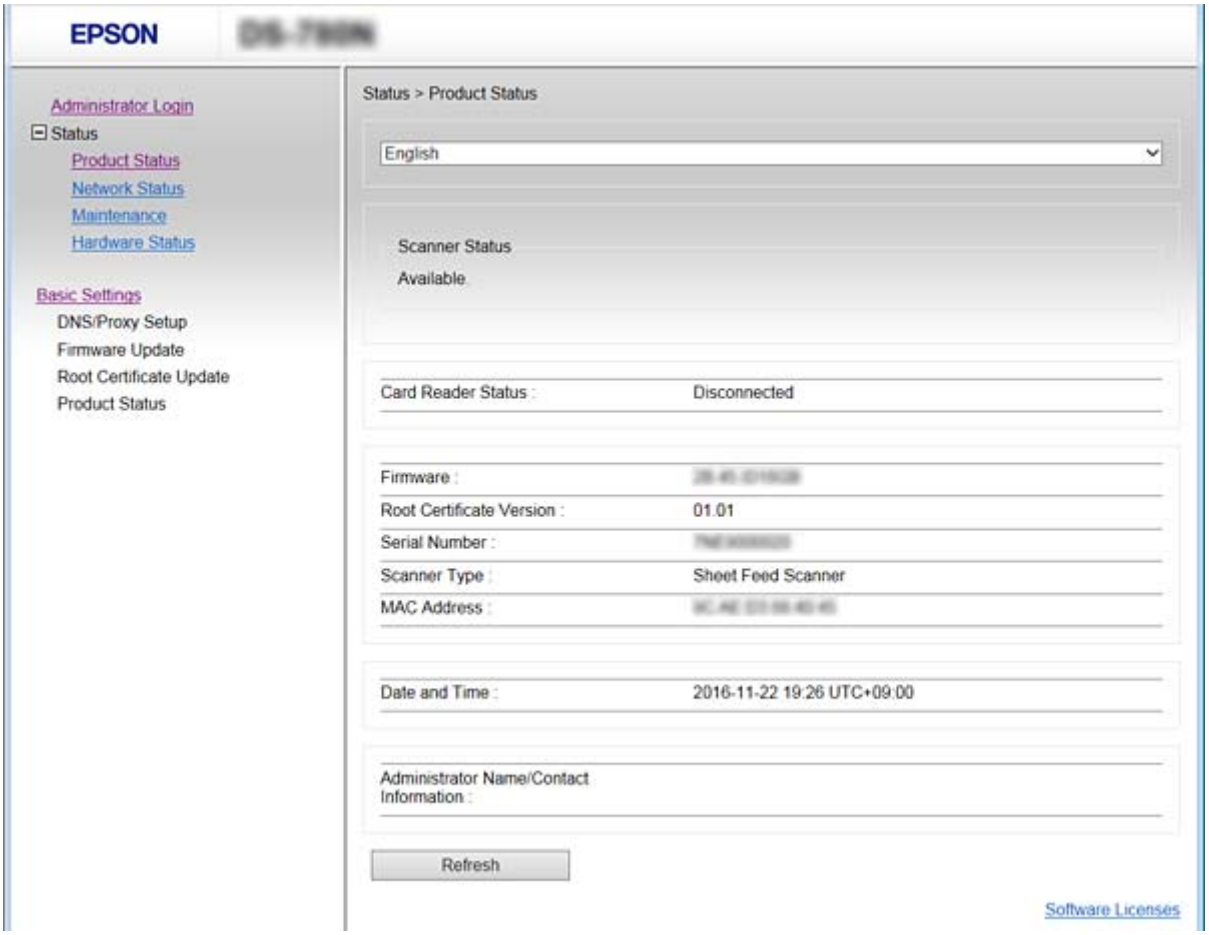
❏ **Basic Settings**

Puteți configura setările de bază pentru scaner.



❏ **Advanced Settings**

Puteți configura setările avansate pentru scaner. Această pagină se adresează în special unui administrator.



Accesarea Web Config

Introduceți adresa IP a scanerului într-un browser web. JavaScript trebuie să fie activat. La accesarea Web Config prin HTTPS, va apărea un mesaj de avertisment în browser, deoarece este utilizat un certificat auto-semnat stocat în scaner.

❏ Accesare via HTTPS

IPv4: https://<adresă IP scaner> (fără a include < >)

IPv6: https://[adresă IP scaner]/ (păstrați [ ])

❏ Accesare via HTTP

IPv4: http://<adresă IP scaner> (fără a include < >)

IPv6: http://[adresă IP scaner]/ (păstrați [ ])

Notă:

❏ *Exemple*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Dacă denumirea scanerului este înregistrată în serverul DNS, puteți folosi denumirea scanerului în locul adresei IP a imprimantei.*

Informații conexe

➡ „Comunicare SSL/TLS cu scanerul” la pagina 63

➡ „Despre certificarea digitală” la pagina 63

Utilizarea funcțiilor de scanare

În funcție de modul în care veți utiliza scanerul, instalați următorul software și efectuați setările pentru utilizarea acestuia.

❏ **Scanare de la computer**

❏ Confirmați validitatea serviciului de scanare în rețea cu Web Config (valabil la livrarea din fabrică).

❏ Instalați Epson Scan 2 pecomputer și setați adresa IP

❏ La scanarea utilizând operațiuni, instalați Document Capture Pro (Document Capture) și efectuați setările pentru operațiuni.

❏ **Scanare de la panoul de contorl**

❏ La utilizarea Document Capture Pro sau Document Capture Pro Server:

Instalați Document Capture Pro sau Document Capture Pro Server

Setare DCP (mod server, mod client).

❏ La utilizarea protocolului WSD:

Confirmați validitatea WSD pe Web Config sau panoul de operare (valabil la livrarea din fabrică)

Setări suplimentare ale dispozitivului (computer cu Windows).

Scanarea de la un computer

Instalați software-ul și activați serviciul de scanare în rețea pentru a scana prin rețea de la un computer.

Informații conexe

➡ „Software-ul care trebuie instalat” la pagina 25

➡ „Activarea scanării în rețea” la pagina 25

Software-ul care trebuie instalat

❏ Epson Scan 2

Acesta este un driver de scaner. În cazul în care utilizați dispozitivul de la un computer, instalați driverul pe computerul fiecărui client. Dacă Document Capture Pro/Document Capture este instalat, puteți efectua operațiile alocate butoanelor dispozitivului.

Cu EpsonNet SetupManager, driverele imprimantei pot fi distribuite și împreună în pachete.

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

Instalați pe computerul client. Puteți accesa și executa operațiuni înregistrate pe un computer cu Document Capture Pro/Document Capture instalat în rețea de la computer și panoul de operare al scanerului.

De asemenea, puteți scana de la computer prin rețea. Pentru scanare este necesar Epson Scan 2.

Informații conexe

➡ „EpsonNet SetupManager” la pagina 56

Setați adresa IP a scanerului la Epson Scan 2

Specificați adresa IP a scanerului astfel încât scanerul să poată fi utilizat în rețea.

1. Porniți **Epson Scan 2 Utility** din **Start** > **Toate programele** > **EPSON** > **Epson Scan 2**.

   Dacă este înregistrat deja un alt scaner, mergeți la pasul 2.

   Dacă nu este înregistrat, mergeți la pasul 4.

2. Executați clic pe ▼ din **Scaner**.

3. Faceți clic pe **Setări**.

4. Executați clic pe **Activare editare** și apoi pe **Adăugare**.

5. Selectați modelul scanerului din **Model**.

6. Selectați adresa IP a scanerului de utilizat din **Adresă** în **Căutare rețea**.

   Executați clic pe  și clic pe  pentru a actualiza lista. Dacă nu puteți găsi adresa IP a scanerului, selectați **Introduceți adresa** și introduceți adresa IP.

7. Faceți clic pe **Adăugare**.

8. Faceți clic pe **OK**.

Activarea scanării în rețea

Puteți seta serviciul de scanare în rețea atunci când scanați de la un computer client prin rețea. Setarea implicită este activată.

1. Accesați Web Config și selectați **Services** > **Network Scan**.

2. Asigurați-vă că ați selectat **Enable scanning** of **EPSON Scan**.

   Dacă este selectat, această sarcină este finalizată. Închideți Web Config.

   Dacă este debifat, selectați-l și mergeți la următorul pas.

3. Faceți clic pe **Next**.

4. Faceți clic pe **OK**.

   Rețeaua este reconectată și apoi setările sunt activate.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Scanarea utilizând panoul de control

Funcția de scanare în folder și funcția de scanare în mail utilizând panoul de control al scanerului, precum și transferul rezultatelor scanării la mail, în foldere etc. sunt efectuate prin executarea unei operațiuni de la computer.

La transferarea rezultatelor scanării, configurați operațiunea cu Document Capture Pro Server sau Document Capture Pro.

Pentru detalii privind setările și configurarea operațiunii, consultați documentați sau ajutorul pentru Document Capture Pro Server sau Document Capture Pro.

Informații conexe

➡ „Setări Document Capture Pro Server/Document Capture Pro” la pagina 26

➡ „Setarea serverelor și folderelor” la pagina 27

Software care trebuie instalat pe computer

❏ **Document Capture Pro Server**

Aceasta este versiunea de server a Document Capture Pro. Instalați-l pe un server Windows. Mai multe dispozitive și operațiuni pot fi gestionate central de server. Operațiunile pot fi executate simultan de la scanere multiple.

Prin utilizarea versiunii certificate a Document Capture Pro Server, puteți gestiona operațiuni și istoricul de scanare corelat cu utilizat și grupuri.

Pentru detalii privind Document Capture Pro Server, contactați biroul local Epson.

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

La fel ca în cazul scanării de la un computer, puteți accesa operațiuni înregistrate pe computer de la panoul de control și le puteți executa. Nu este posibilă executarea operațiunilor de computer de la mai multe scanere.

Setări Document Capture Pro Server/Document Capture Pro

Efectuați setările pentru utilizarea funcției de scanare de la panoul de operare al scanerului.

1. Accesați Web Config și selectați **Services** > **Document Capture Pro**.

2. Selectați **Mod funcționare**.

   ❏ Server Mode:

   Selectați atunci când utilizați Document Capture Pro Server sau când utilizați Document Capture Pro doar pentru operațiuni care au fost setate pentru un anumit computer.

   ❏ Client Mode:

   Setați atunci când selectați setarea de operațiune a Document Capture Pro (Document Capture) instalat pe fiecare compter client din rețea, fără specificarea computerului.

3. Setați următoarele în funcție de modul selectat.

   ❏ Server Mode:

   În **Server Address**, specificați serverul pe careDocument Capture Pro Server este instalat. Acesta poate abea între 2 și 252 de caractere în format IPv4, IPv6, nume gazdă, FQDN. În formatul FQDN, se pot utiliza litere US-ASCII, numere, alfabeturi și cratime (nu însă la începutul și sfârșitul cuvintelor).

   ❏ Client Mode:

   Specificați **Group Settings** pentru a utiliza un grup de scanere specificat din Document Capture Pro (Document Capture).

4. Faceți clic pe **Setări**.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Setarea serverelor și folderelor

Document Capture Pro și Document Capture Pro Server salvează datele scanate pe server sau computerul client și utilizează funcția de transfer pentru a executa funcția de scanare în folder și funcția de scanare la mail.

Aveți nevoie de autorizare și informații pentru a transfera de la computerul pe care ați instalat Document Capture Pro, Document Capture Pro Server la un alt computer sau serviciul cloud.

Pregătiți informațiile privind funcția pe care o veți utiliza, consultând următoarele.

Puteți efectua setări pentru aceste funcții utilizând Document Capture Pro sau Document Capture Pro Server. Pentru detalii privind setările, consultați documentația sau ajutorul pentru Document Capture Pro Server sau Document Capture Pro.

Nume	Setări	Cerință
Scanare în folderul de rețea (SMB)	Crearea și configurarea partajării folderului de salvare	Contul utilizatorului administrativ al computerului care creează foldere de salvare.
	Destinația pentru scanare în folderul de rețea (SMB)	Numele de utilizator și parola pentru conectarea pe un computer care are folderul de salvare și privilegiul de a actualiza folderul de salvare.
Scanare în folderul de rețea (FTP)	Setare pentru jurnalul de server FTP pornită	Informațiile de conectare pentru serverul FTP și privilegiul de a actualiza folderul de salvare.
Scanare în e-mail	Setare pentru serverul e-mailului	Informații privind setarea serverului e-mailului

Nume	Setări	Cerință
Scanare către Document Capture Pro (în timpul utilizării Document Capture Pro Server)	Configurare pentru înregistrare în servicii cloud	Mediu de conectare la internet Înregistrare cont pentru servicii cloud

Utilziați scanarea WSD (doar Windows)

În cazul în care computerul utilizează Windows Vista sau o versiune mai nouă, puteți utilza scanarea WSD.

Când poate fi utilizat protocolul WSD, meniul **Computer (WSD)** va fi afișat pe panoul de control al scanerului.

1. Accesați Web Config și selectați **Services** > **Protocol**.
2. Confirmați faptul că **Enable WSD** este bifată în **WSD Settings**.
   Dacă aceasta este bifată, sarcina este finalizată și puteți închide Web Config.
   Dacă nu este bifată, bifați-o și treceți la pasul următor.
3. Executați clic pe butonul **Next**.
4. Confirmați setările și apoi executați clic pe **Setări**.

Efectuarea setărilor de sistem

Efectuarea setărilor de sistem pe panoul de control

Setați luminozitatea ecranului

Setați luminozitatea ecranului LCD.

1. Atingeți **Setări** pe ecranul de pornire.
2. Atingeți **Setări comune** > **Luminozitate LCD**.
3. Atingeți  sau  pentru a regla luminozitatea.
   Puteți regla de la 1 la 9.
4. Atingeți **OK**.

Setarea sunetului

Setați sunetul de operare de la panou și sunetele de eroare.

1. Atingeți **Setări** pe ecranul de pornire.
2. Atingeți **Setări comune** > **Sunet**.

3. Configurați următoarele elemente după cum este necesar.
   - ❏ Sunet operațional
     Setați volumul sunetului operațional de la panoul de operare.
   - ❏ Sunet de eroare
     Setați volumul sunetului de eroare.
4. Atingeți **OK**.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Detectarea alimentării duble a documentului original

Determinați funcția de detectare a alimentării duble a documentului de scanat și opriți scanarea atunci când au loc alimentări multiple.

Pentru a scana originale care considerați că vor face obiectul unor alimentări multiple, cum ar fi plicuri sau hârtie cu autocolant, setați funcția la Off (Dezactivare).

Notă:
Se poate seta și din Web Config sau Epson Scan 2.

1. Atingeți **Setări** pe ecranul de pornire.
2. Atingeți **Setări scanare externe** > **Det. ultrason. alim. dublă**.
3. Atingeți **Det. ultrason. alim. dublă** pentru a activa sau dezactiva.
4. Atingeți **Închidere**.

Setați modul de viteză redusă

Setați pentru a scana la viteză redusă astfel încât să evitați blocajele de hârtie în timpul scanării unor documente subțiri, cum ar fi șiraifuri.

1. Atingeți **Setări** pe ecranul de pornire.
2. Atingeți **Setări scanare externe** > **Lent**.
3. Atingeți **Lent** pentru a activa sau dezactiva.
4. Atingeți **Închidere**.

Efectuarea setărilor de sistem utilizând Web Config

Setări de economisire a energiei în timpul perioadei de inactivitate

Efectuați setările de economisire a energiei pentru perioada de inactivitate a scanerului. Setați timpul în funcție de mediul de utilizare.

Notă:
Aveți posibilitatea de a efectua setările de economisire a energiei pe panoul de control al scanerului.

1. Accesați Web Config și selectați **System Settings** > **Power Saving**.
2. Introduceți timpul pentru **Sleep Timer** pentru comutare la modul de economisire energie în perioada de inactivitate.

   Puteți seta până la 240 de minute în trepte de un minut.
3. Selectați timpul de oprire pentru **Power Off Timer**.
4. Faceți clic pe **OK**.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Setarea panoului de control

Configurarea pentru panoul de control al scanerului. Pentru efectuarea configurării, puteți proceda în modul următor.

1. Accesați Web Config și selectați **System Settings** > **Control Panel**.
2. Configurați următoarele elemente după cum este necesar.
   - ❏ Language

     Selectați limba afișată de la panoul de control.
   - ❏ Panel Lock

     În cazul în care selectați **ON**, este necesară parola de administrator atunci când efectuați operațiuni pentru care este necesar să dispuneți de autoritatea administratorului. În cazul în care parola administratorului nu este setată, blocarea panoului este dezactivată.
   - ❏ Operation Timeout

     În cazul în care selectați **ON**, atunci când vă conectați în calitate de administrator, sunteți deconectat în mod automat și direcționat către ecranul inițial dacă nu există nicio activitate pentru o anumită perioadă de timp.

     Puteți seta între 10 secunde și 240 de minute la indicatorul secundelor.
3. Faceți clic pe **OK**.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Setarea restricției pentru interfața externă

Puteți restricționa conexiunea USB de la computer. Setați pentru a limita alte scanări decât cele prin rețea.

1. Accesați Web Config și selectați **System Settings** > **External Interface**.
2. Selectați **Enable** sau **Disable**.

   Pentru a restricționa, selectați **Disable**.
3. Atingeți **OK**.

Sincronizarea datei și orei cu serverul de timp

Dacă folosiți un certificat CA, puteți preveni problemele referitoare la timpul.

1. Accesați Web Config și selectați **System Settings** > **Date and Time** > **Time Server**.
2. Selectați **Use** pentru **Use Time Server**.
3. Introduceți adresa serverului de timp **Time Server Address**.

   Puteți folosi formatul IPv4, IPv6 sau FQDN. Introduceți 252 caractere sau mai puțin. Dacă nu specificați acest lucru, lăsați spațiul gol.
4. Introduceți **Update Interval (min)**.

   Puteți seta până la 10,800 de minute la indicatorul minutelor.
5. Faceți clic pe **OK**.

   Notă:
   *Puteți confirma starea conexiunii cu serverul de timp la **Time Server Status**.*

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Setări de securitate de bază

Acest capitol explică setările de securitate de bază care nu necesită un mediu special.

Prezentarea funcțiilor de securitate de bază

Vă prezentăm funcțiile de securitate de bază ale dispozitivelor Epson.

Denumire funcție	Tip funcție	Ce trebuie setat	Ce trebuie prevenit
Configurare pentru parola de administrator	Blocați setările de sistem, precum setările de conexiune la rețea și USB, astfel încât acestea să poată fi modificate doar de către administrator.	Administratorul setează o parolă pentru dispozitiv. Configurarea sau actualizarea sunt disponibile oriunde din Web Config, panoul de control, Epson Device Admin și EpsonNet Config.	Previne citirea ilegală și modificarea informațiilor stocate pe dispozitiv, cum ar fi ID-ul, parola, setările de rețea și contactele. Reduce, de asemenea, o gamă largă de riscuri de securitate, cum ar fi scurgerea de informații pentru mediul de rețea sau privind politica de securitate.
Comunicări SSL/TLS	La accesarea unui server Epson pe Internet de la un dispozitiv, cum ar fi comunicarea cu un computer prin intermediul unui browser sau actualizări software, conținutul comunicării este criptat de comunicarea SSL/TLS.	Obțineți un certificat semnat CA și apoi importați-l la scaner.	Identificarea dispozitivului prin certificare semnată CA previne arogarea unor identități false și accesul neautorizat. În plus, conținutul comunicării SSL/TLS este protejat și se previn scurgerile de conținut privind datele de tipărire și informațiile de configurare.
Protocoale de control	Protocoale de control utilizate pentru comunicare între dispozitive și comptuere și activare/dezactivare funcții.	Un protocol sau serviciu care este aplicat funcțiilor permise sau interzise separat.	Reducerea riscurilor de securitate care pot apărea prin utilizarea neintenționată, împiedicând utilizatorii să folosească funcțiile inutile.

Informații conexe

➡ „Despre Web Config” la pagina 22
➡ „EpsonNet Config” la pagina 55
➡ „Epson Device Admin” la pagina 55
➡ „Configurarea parolei de administrator” la pagina 32
➡ „Protocoale de control” la pagina 35

Configurarea parolei de administrator

Când setați parola de administrator, utilizatorii care nu sunt administratori nu vor putea modifica setările pentru administrarea sistemului. Puteți seta și modifica parola de administrator folosind Web Config, panoul de control al

scanerului sau software-ul (Epson Device Admin sau EpsonNet Config). Când utilizați software-ul, consultați documentația pentru fiecare software.

Informații conexe

➡ „Configurarea parolei de administrator de la panoul de control” la pagina 33
➡ „Configurarea parolei de administrator utilizând Web Config” la pagina 33
➡ „EpsonNet Config” la pagina 55
➡ „Epson Device Admin” la pagina 55

Configurarea parolei de administrator de la panoul de control

Puteți seta parola de administrator de la panoul de control al scanerului.

1. Atingeți **Setări** pe ecranul de pornire.
2. Atingeți **Administrare sistem** > **Setări administrator**.

   Dacă elementul nu este afișat, glisați pe ecran în sus pentru a-l afișa.
3. Atingeți **Parolă administrator** > **Înregistrare**.
4. Introduceți noua parolă și atingeți **OK**.
5. Introduceți parola din nou și apoi atingeți **OK**.
6. Atingeți **OK** pe ecranul de confirmare.

   Este afișat ecranul cu setările de administrator.
7. Atingeți **Setare blocare** și apoi atingeți **OK** pe ecranul de confirmare.

   Setare blocare este setată la **Act.**, iar parola de administrator va fi necesară atunci când operați un element de meniu blocat.

Notă:

❏ *Dacă setați **Setări** > **Setări comune** > **Operația a expirat** la **Act.**, scanerul vă va deconecta după o perioadă de inactivitate pe panoul de control.*

❏ *Puteți modifica sau șterge parola de administrator atunci când selectați **Schimbare** sau **Resetare** pe ecranul **Parolă administrator** și introduceți parola de administrator.*

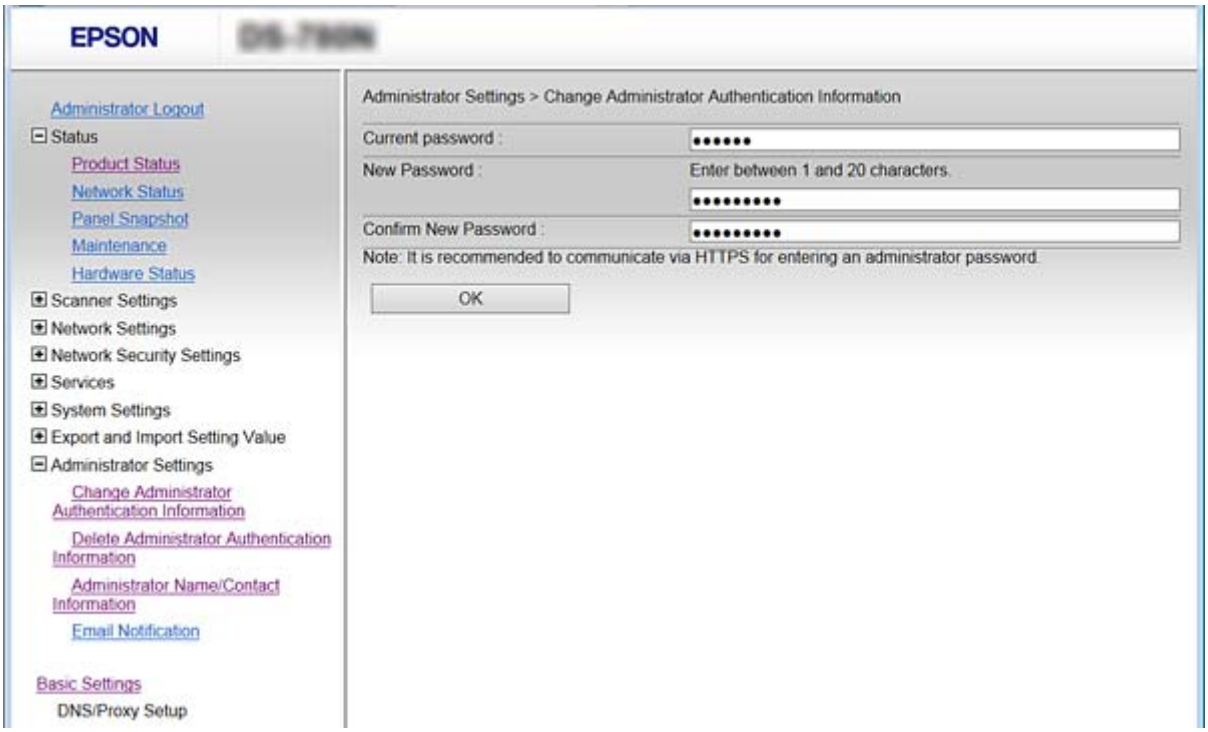
Configurarea parolei de administrator utilizând Web Config

Puteți seta parola de administrator folosind Web Config.

1. Accesați Web Config și selectați **Administrator Settings** > **Change Administrator Authentication Information**.

2. Introduceți o parolă pentru **New Password** și **Confirm New Password**. Introduceți numele de utilizator, dacă este necesar.

   Dacă doriți să schimbați parola cu una nouă, introduceți parola curentă.



3. Selectați **OK**.

   Notă:

   ❏ *Pentru a seta sau modifica elementele de meniu blocate, executați clic pe **Administrator Login** și apoi introduceți parola de administrator.*

   ❏ *Pentru a șterge parola de administrator, executați clic pe **Administrator Settings** > **Delete Administrator Authentication Information** și apoi introduceți parola de administrator.*

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Elemente care vor fi blocate prin parola de administrator

Administratorii au privilegii de setare și modificare pentru toate funcțiile dispozitivelor.

De asemenea, dacă setați parola de administrator pe dispozitiv, o puteți bloca astfel încât să nu poată fi modificate elemente privind gestionarea dispozitivului.

Următoarele sunt elementele pe care administratorul le poate controla.

Element	Descriere
Setare scaner	Setarea detectării alimentării duble și a modului de viteză redusă.

Setări de securitate de bază

Element	Descriere
Setări de conexiune Ethernet	Modificare nume dispozitive și adresă IP, configurare server DNS sau server proxy și modificări ale setărilor legate de conexiuni în rețea.
Setare servicii utilizator	Configurare pentru controlarea protocoalelor de comunicare, scanare în rețea și servicii Document Capture Pro.
Setare server de e-mail	Configurarea unui server de e-mail cu care dispozitivele comunică direct.
Setări de securitate	Setări pentru securitatea rețelei, cum ar fi comunicarea SSL/TLS, filtrarea IPsec/IP și IEEE802.1X.
Actualizare certificat rădăcină	Actualizare a certificatelor rădăcină necesare pentru autentificare Document Capture Pro Server și actualizare firmware din Web Config.
Actualizare firmware	Verificarea si actualizarea firmware-ului dispozitivelor.
Timp, setare temporizator	Timp tranziție la starea de repaus, oprire automată, dată/oră, temporizator stare de nefuncționare, alte setări privind temporizatorul.
Restabilire la setări implicite	Setări pentru scaner care vor fi resetate la setările din fabrică.
Setări de administrator	Setarea funcției de blocare sau a parolei de administrator.
Setare dispozitiv certificat	Setare ID dispozitiv de autentificare. Setați la utilizarea scanerului pe un sistem de autentificare ce acceptă dispozitive de autentificare.

Protocoale de control

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. De exemplu, este permisă scanarea utilizând doar căile și protocoalele specificate. Puteți reduce riscurile de securitate cauzate de accesul neautorizat prin restricționarea scanării de la anumite căi specifice sau prin controlarea funcțiilor disponibile.

Configurați setările protocoalelor.

1. Accesați Web Config și selectați **Services** > **Protocol**.
2. Configurați fiecare articol.
3. Faceți clic pe **Next**.
4. Faceți clic pe **OK**.

   Setările vor fi aplicate la nivelul scanerului.

Informații conexe

➡ „Accesarea Web Config” la pagina 23
➡ „Protocoale pe care le puteți activa sau dezactiva” la pagina 36
➡ „Elemente de setare a protocoalelor” la pagina 37

Protocoale pe care le puteți activa sau dezactiva

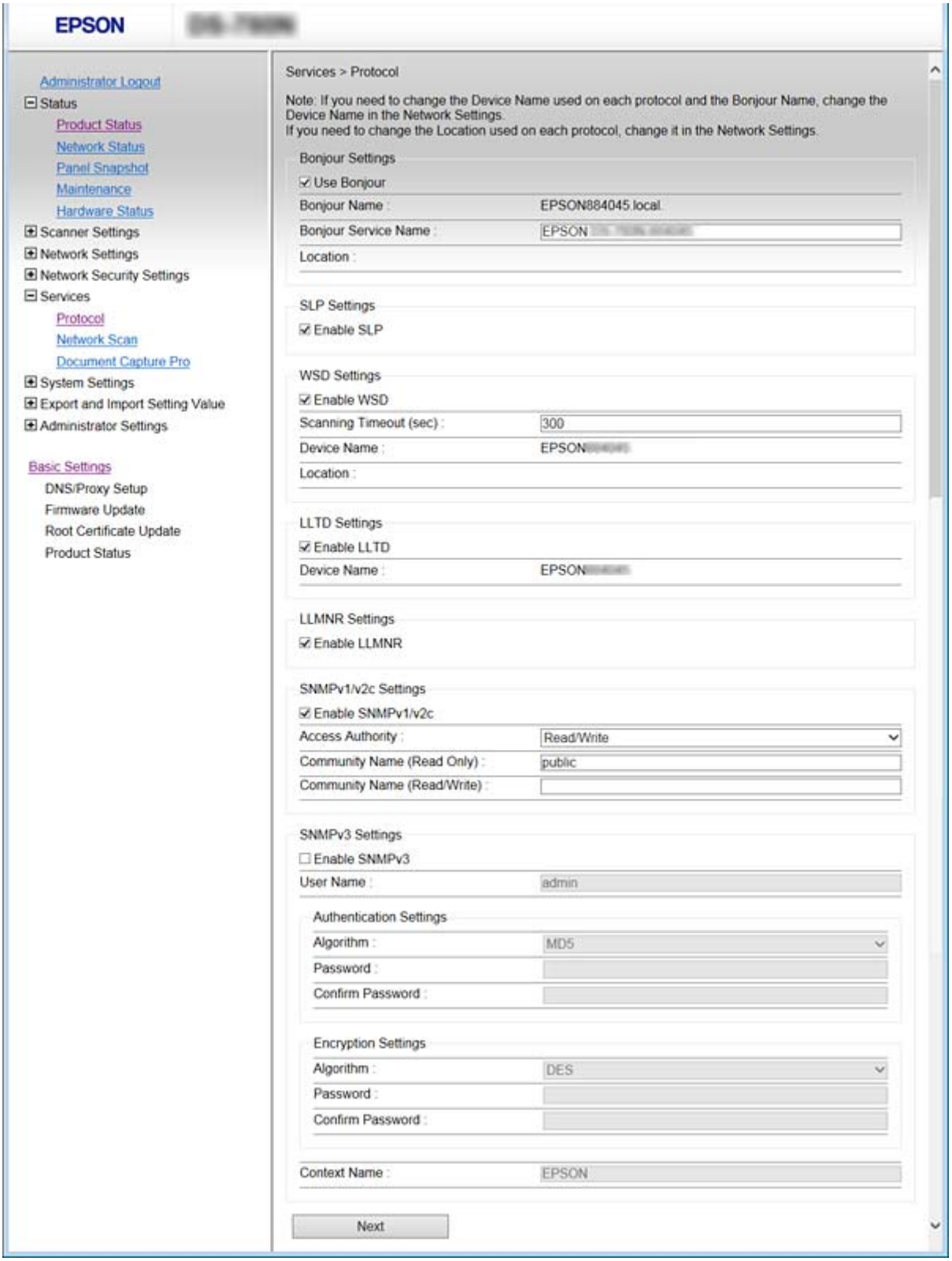
Protocol	Descriere
Bonjour Settings	Puteți să specificați dacă doriți să utilizați serviciul Bonjour. Bonjour este utilizat pentru căutarea dispozitivelor, scanare şi multe altele.
SLP Settings	Puteți activa sau dezactiva funcția SLP. Funcția SLP este utilizată pentru Epson Scan 2 și pentru căutarea în rețea prin intermediul EpsonNet Config.
WSD Settings	Puteți activa sau dezactiva funcția WSD. Când această funcție este activată, puteți să adăugați dispozitive WSD sau să scanați folosind portul WSD.
LLTD Settings	Puteți activa sau dezactiva funcția LLTD. Când această funcție este activată, este afișată în harta de rețea a sistemului Windows.
LLMNR Settings	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.
SNMPv1/v2c Settings	Puteți să specificați dacă doriți sau nu să activați caracteristica SNMPv1/v2c. Aceasta este utilizată pentru configurarea dispozitivelor, monitorizare etc.
SNMPv3 Settings	Puteți să specificați dacă doriți sau nu să activați caracteristica SNMPv3. Aceasta este utilizată pentru configurarea dispozitivelor criptate, monitorizare etc.

Informații conexe

➡ „Protocoale de control” la pagina 35

➡ „Elemente de setare a protocoalelor” la pagina 37

Elemente de setare a protocoalelor



Elemente	Valoare setată și descriere
Bonjour Settings	

Setări de securitate de bază

Elemente	Valoare setată și descriere
Use Bonjour	Selectați această opțiune pentru a căuta sau utiliza dispozitive folosind serviciul Bonjour.
Bonjour Name	Afișează numele Bonjour.
Bonjour Service Name	Puteți afișa și seta numele serviciului Bonjour.
Location	Afișează numele locației Bonjour.
SLP Settings	
Enable SLP	Selectați această opțiune pentru a activa funcția SLP. Se utilizează pentru descoperirea în rețea în Epson Scan 2 și Epson Net Config.
WSD Settings	
Enable WSD	Selectați această opțiune pentru a permite adăugarea dispozitivelor utilizând WSD, precum și imprimarea și scanarea de la portul WSD.
Scanning Timeout (sec)	Introduceți valoarea de expirare a comunicațiilor pentru scanarea WSD, între 3 și 3.600 de secunde.
Device Name	Afișează numele dispozitivului WSD.
Location	Afișează numele locației WSD.
LLTD Settings	
Enable LLTD	Selectați această opțiune pentru a activa LLTD. Scanerul este afișată în harta de rețea a sistemului Windows.
Device Name	Afișează numele dispozitivului LLTD.
LLMNR Settings	
Enable LLMNR	Selectați această opțiune pentru a activa LLMNR. Puteți utiliza rezoluții de nume fără NetBIOS, chiar dacă nu puteți utiliza serviciul DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Selectați această opțiune pentru a activa SNMPv1/v2c. Vor fi afișate numai scanerele care acceptă SNMPv3.
Access Authority	Setați autoritatea de acces atunci când este activată funcția SNMPv1/v2c. Selectați **Read Only** sau **Read/Write**.
Community Name (Read Only)	Introduceți între 0 și 32 de caractere ASCII (între 0x20 și 0x7E).
Community Name (Read/Write)	Introduceți între 0 și 32 de caractere ASCII (între 0x20 și 0x7E).
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 este activat atunci când caseta este bifată.
User Name	Introduceți între 1 și 32 de caractere folosind caractere a câte un octet.

Setări de securitate de bază

Elemente	Valoare setată și descriere
Authentication Settings	
Algorithm	Selectați un algoritm de autentificare pentru SNMPv3.
Password	Introduceți o parolă de autentificare pentru SNMPv3. Introduceți între 8 și 32 de caractere în ASCII (0x20 – 0x7E). Dacă nu specificați acest lucru, lăsați spațiul gol.
Confirm Password	Pentru confirmare, introduceți parola configurată.
Encryption Settings	
Algorithm	Selectați un algoritm de criptare pentru SNMPv3.
Password	Introduceți o parolă de criptare pentru SNMPv3. Introduceți între 8 și 32 de caractere în ASCII (0x20 – 0x7E). Dacă nu specificați acest lucru, lăsați spațiul gol.
Confirm Password	Pentru confirmare, introduceți parola configurată.
Context Name	Introduceți cel mult 32 de caractere în Unicode (UTF-8). Dacă nu specificați acest lucru, lăsați spațiul gol. Numărul de caractere care pot fi introduse variază în funcție de limbă.

Informații conexe

➡ „Protocoale de control” la pagina 35

➡ „Protocoale pe care le puteți activa sau dezactiva” la pagina 36

Setări de operare și gestionare

Acest capitol explică elementele legate de funcțiile zilnice și gestionarea dispozitivului.

Confirmarea informațiilor despre un dispozitiv

Puteți verifica următoarele informații privind dispozitivul de operare din **Status** utilizând Web Config.

❏ Product Status

Verificați limba, starea, numărul de produs, adresa MAC etc.

❏ Network Status

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

❏ Panel Snapshot

Afișați o captură de ecran care este afișată pe panoul de control al dispozitivului.

❏ Maintenance

Verificați data de începere, informațiile privind scanarea, etc.

❏ Hardware Status

Verificați starea scanerului.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Gestionarea dispozitivelor (Epson Device Admin)

Puteți gestiona și opera mai multe dispozitive utilizând Epson Device Admin. Epson Device Admin vă permite să gestionați dispozitive localizate într-o rețea diferită. Următoarele prezintă funcțiile de gestionare principale.

Pentur mai multe informații privind funcțiile și utilizarea software-ului, consultați documentația sau ajutorul Epson Device Admin.

❏ Descoperirea dispozitivelor

Puteți descoperi dispozitivele din rețea, și apoi le puteți înregistra într-o listă. Dacă dispozitive Epson, cum ar fi imprimante și scanere, sunt conectate la același segment de rețea cu computerul administratorului, le puteți găsi chiar și în cazul în care acestora nu le-a fost alocată o adresă IP.

Puteți descoperi, de asemenea, dispozitivele conectate la computerele din rețea prin cabluri USB. Trebuie să instalați Epson Device USB Agent pe computer.

❏ Setarea dispozitivelor

Puteți realiza un șablon conținând elementele de setare, precum interfața de rețea și sursa de hârtie, și îl puteți aplica altor dispozitive sub formă de setări partajate. Atunci când este conectat la rețea, aveți posibilitatea să alocați o adresă de IP unui dispozitiv căruia nu i-a fost atribuită o adresă IP.

❏ Monitorizarea dispozitivelor

Puteți obține în mod regulat informații detaliate despre dispozitivele din rețea. De asemenea, puteți monitoriza dispozitivele conectate la computerele din rețea prin cabluri USB și dispozitive de la alte companii care au fost înregistrate în lista de dispozitive. Pentru a monitoriza dispozitivele conectate prin cabluri USB, trebuie să instalați Epson Device USB Agent.

❏ Gestionarea alertelor

Puteți monitoriza alerte cu privire la starea dispozitivelor si consumabilelor. Sistemul trimite automat e-mailuri de notificare administratorului, bazat pe condițiile setate.

❏ Gestionarea rapoartelor

Aveți posibilitatea să creați rapoarte regulate, deoarece sistemul acumulează date privind utilizarea dispozitivului și consumabilelor. Apoi puteți salva aceste rapoarte create și le puteți trimite prin e-mail.

Informații conexe

➡ „Epson Device Admin” la pagina 55

Recepționarea notificărilor prin e-mail la apariția de evenimente

Despre notificările prin e-mail

Puteți utiliza această funcție pentru a primi alerte prin e-mail atunci când apar evenimente. Puteți înregistra până la 5 adrese de e-mail și puteți alege evenimentele pentru care doriți să primiți notificări.

Serverul de e-mail trebuie configurat pentru a utiliza această funcție.

Informații conexe

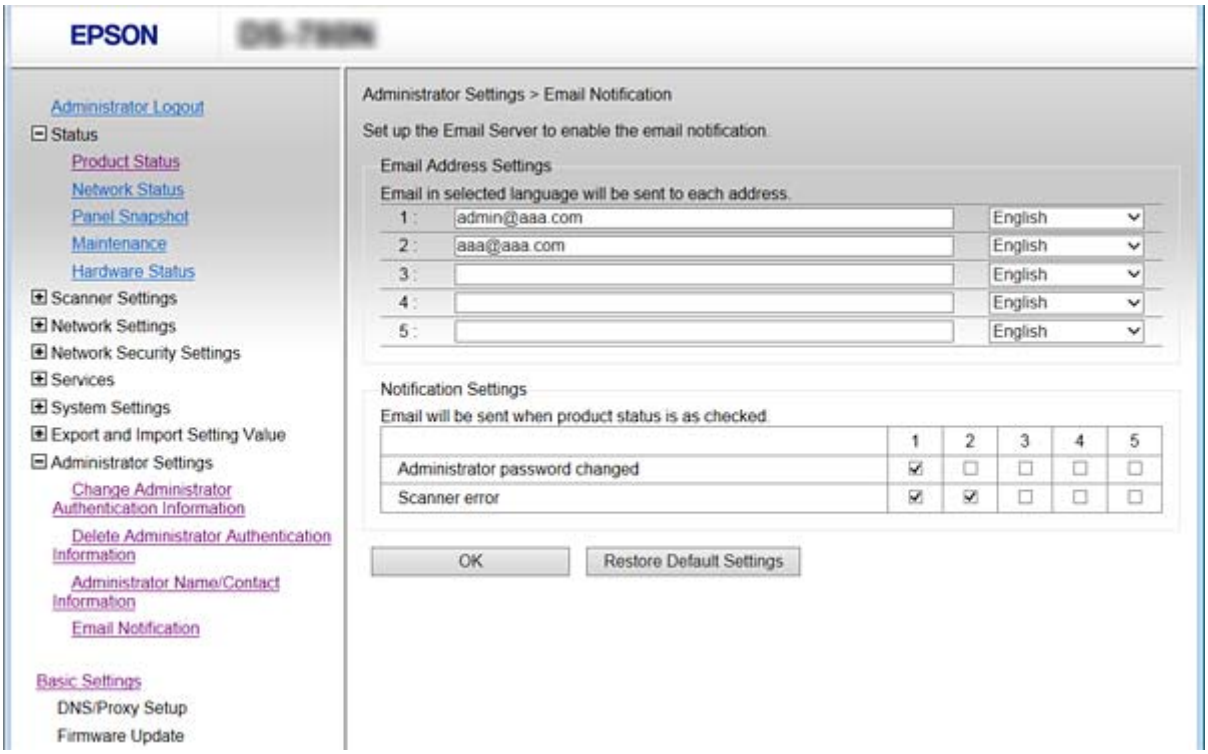
➡ „Configurarea unui server de e-mail” la pagina 42

Configurarea notificării prin e-mail

Pentru a utiliza această funcție, trebuie să configurați un server de e-mail.

1. Accesați Web Config și selectați **Administrator Settings** > **Email Notification**.
2. Introduceți adresa de e-mail la care doriți să primiți notificările.
3. Selectați limba pentru notificările prin e-mail.

4. Bifați casetele pentru notificările pe care doriți să le primiți.



5. Faceți clic pe **OK**.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

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

Configurarea unui server de e-mail

Verificați următoarele aspecte înainte de a realiza configurarea.

❏ Scanerul este conectat la rețea.

❏ Informațiile serverului de e-mail al computerului.

1. Accesați Web Config și selectați **Network Settings** > **Email Server** > **Basic**.

2. Introduceți o valoare pentru fiecare element.

3. Selectați **OK**.

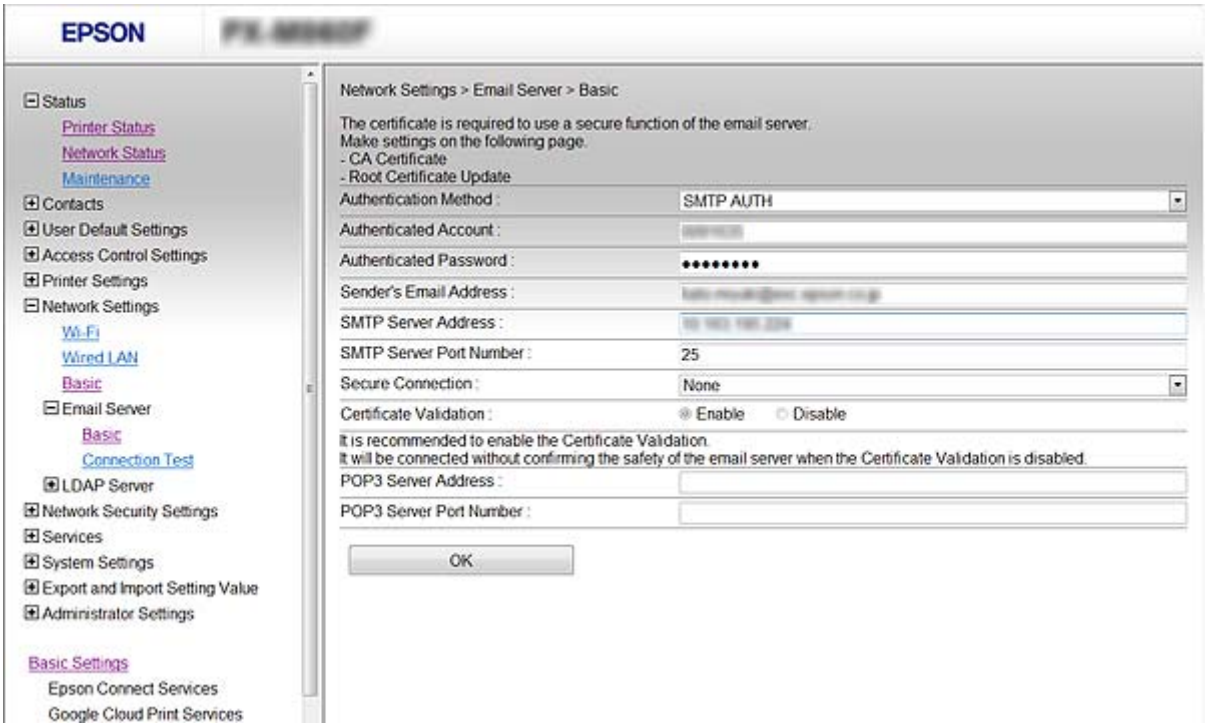
   Setările pe care le-ați selectat sunt afișate.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Elemente de setare server de e-mail” la pagina 43

Elemente de setare server de e-mail



Elemente	Setări și explicații	
Authentication Method	Indicați metoda de autentificare pentru ca scanerul să acceseze serverul de e-mail.	
	Off	Autentificarea este dezactivată la comunicarea cu un server de mail.
	SMTP AUTH	Este necesar ca un server de mail să accepte autentificarea SMTP.
	POP before SMTP	Configurați serverul POP3 când selectați această metodă.
Authenticated Account	Dacă selectați **SMTP AUTH** sau **POP before SMTP** drept **Authentication Method**, introduceți numele contului autentificat folosind între 0 şi 255 de caractere în format ASCII (0x20–0x7E).	
Authenticated Password	Dacă selectați **SMTP AUTH** sau **POP before SMTP** drept **Authentication Method**, introduceți parola de autentificare între 0 şi 20 de caractere folosind A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Introduceți adresa de e-mail a expeditorului. Introduceți între 0 şi 255 de caractere în ASCII (0x20–0x7E), exceptând : ( ) < > [ ] ; ¥. Punctul „.” nu poate fi primul caracter.	
SMTP Server Address	Introduceți între 0 şi 255 de caractere folosind A–Z a–z 0–9. - . Puteți folosi formatul IPv4 sau FQDN.	
SMTP Server Port Number	Introduceți un număr între 1 şi 65535.	

Elemente	Setări și explicații	
Secure Connection	Specificați metoda de conectare securizată pentru serverul de e-mail.	
	None	Dacă selectați **POP before SMTP** în **Authentication Method**, metoda de conectare va fi setată la **None**.
	SSL/TLS	Aceasta este disponibilă atunci când **Authentication Method** este setată la **Off** sau la **SMTP AUTH**.
	STARTTLS	Aceasta este disponibilă atunci când **Authentication Method** este setată la **Off** sau la **SMTP AUTH**.
Certificate Validation	Certificatul este validat atunci când este activată această funcție. Recomandăm setarea acestei funcții la **Enable**.	
POP3 Server Address	Dacă selectați **POP before SMTP** ca **Authentication Method**, introduceți adresa de server POP3 între 0 și 255 caractere folosind A–Z a–z 0–9 . - . Puteți folosi formatul IPv4 sau FQDN.	
POP3 Server Port Number	Dacă selectați **POP before SMTP** ca **Authentication Method**, introduceți un număr între 1 și 65535.	

Informații conexe

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

Verificarea unei conexiuni de server de e-mail

1. Accesați Web Config și selectați **Network Settings** > **Email Server** > **Connection Test**.
2. Selectați **Start**.

   Va fi inițiată testarea conexiunii la serverul de e-mail. După derularea testului, este afișat raportul de verificare.

Informații conexe

➡ „Accesarea Web Config” la pagina 23
➡ „Referințe privind testul conexiunii serverului de e-mail” la pagina 44

Referințe privind testul conexiunii serverului de e-mail

Mesaje	Explicație
Connection test was successful.	Acest mesaj apare când conexiunea la server a reușit.
SMTP server communication error. Check the following. - Network Settings	Acest mesaj apare atunci când ❏ Scanerul nu este conectat la nicio rețea ❏ Serverul SMTP este nefuncțional ❏ Conexiunea la rețea este întreruptă în timpul comunicațiilor ❏ S-au primit date incomplete

Mesaje	Explicație
POP3 server communication error. Check the following. - Network Settings	Acest mesaj apare atunci când ❏ Scanerul nu este conectat la nicio rețea ❏ Serverul POP3 este nefuncțional ❏ Conexiunea la rețea este întreruptă în timpul comunicațiilor ❏ S-au primit date incomplete
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Acest mesaj apare atunci când ❏ Conectarea la un server DNS a eşuat ❏ Rezoluția numelui pentru un server SMTP a eşuat
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Acest mesaj apare atunci când ❏ Conectarea la un server DNS a eşuat ❏ Rezoluția numelui pentru un server POP3 a eşuat
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Acest mesaj apare atunci când autentificarea la serverul SMTP eşuează.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Acest mesaj apare atunci când autentificarea la serverul POP3 eşuează.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Acest mesaj apare atunci când încercați să comunicați folosind protocoale neacceptate.
Connection to SMTP server failed. Change Secure Connection to None.	Acest mesaj apare atunci când are loc o nepotrivire SMTP între un server şi un client sau atunci când serverul nu acceptă conexiunile SMTP securizate (conexiunile SSL).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Acest mesaj apare atunci când are loc o nepotrivire SMTP între un server şi un client sau atunci când serverul solicită utilizarea unei conexiuni SSL/TLS în vederea obținerii unei conexiuni SMTP securizate.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Acest mesaj apare atunci când are loc o nepotrivire SMTP între un server şi un client sau atunci când serverul solicită utilizarea unei conexiuni STARTTLS în vederea obținerii unei conexiuni SMTP securizate.
The connection is untrusted. Check the following. - Date and Time	Acest mesaj apare atunci când setările referitoare la data şi ora scanerului sunt incorecte sau când certificatul a expirat.
The connection is untrusted. Check the following. - CA Certificate	Acest mesaj apare atunci când scanerul nu are un certificat rădăcină care să corespundă serverului sau atunci când nu a fost importat niciun CA Certificate.
The connection is not secured.	Acest mesaj apare atunci când certificatul obținut este deteriorat.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Acest mesaj apare atunci când are loc o nepotrivire în ceea ce priveşte metoda de autentificare între un server şi un client. Serverul acceptă SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Acest mesaj apare atunci când are loc o nepotrivire în ceea ce priveşte metoda de autentificare între un server şi un client. Serverul nu acceptă SMTP AUTH.

Mesaje	Explicație
Sender's Email Address is incorrect. Change to the email address for your email service.	Acest mesaj apare atunci când adresa de e-mail specificată pentru expeditor este incorectă.
Cannot access the product until processing is complete.	Acest mesaj apare când scanerul este ocupat.

Informații conexe

➡ „Verificarea unei conexiuni de server de e-mail” la pagina 44

Actualizare firmware

Actualizare firmware folosind Web Config

Actualizează firmware folosind Web Config. Dispozitivul trebuie să fie conectat la internet.

1. Accesați Web Config și selectați **Basic Settings** > **Firmware Update**.
2. Faceți clic pe **Start**.

   Începe confirmarea firmware-ului, iar informațiile privind firmware-ul sunt afișate, în cazul în care există firmware-ul actualizat.
3. Faceți clic pe **Start** și urmăriți instrucțiunile afișate pe ecran.

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

➡ „Accesarea Web Config” la pagina 23
➡ „Epson Device Admin” la pagina 55

Actualizare firmware folosind Epson Firmware Updater

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.

1. Accesați site-ul web Epson și descărcați firmware-ul.
2. Conectați calculatorul care conține firmware-ul descărcat la dispozitiv prin intermediul cablului USB.
3. Faceți dublu clic pe fișierul .exe descărcat.

   Aplicația Epson Firmware Updater pornește.

4. Urmați instrucțiunile afișate pe ecran.

Copierea de rezervă a setărilor

Prin exportul elementelor de setare în Web Config, puteți copia elementele la alte scanere.

Exportarea setărilor

Exportați fiecare setare a scanerului.

1. Accesați Web Config și apoi selectați **Export and Import Setting Value** > **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.

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

> ***Important:***
> *Dacă doriți să exportați setările de rețea ale scanerului, cum ar fi numele scanerului și adresa IP, selectați* ***Enable to select the individual settings of device*** *și selectați mai multe articole. Utilizați numai valorile selectate pentru scanerul de înlocuire.*

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Importarea setărilor

Importați fișierul Web Config exportat în scaner.

> ***Important:***
> *Atunci când importați valori care includ informații individuale, cum ar fi numele sau adresa IP a scanerului, asigurați-vă că aceeași adresă IP nu mai există în cadrul rețelei. Dacă adresa IP există deja, scanerul nu va reflecta valoarea.*

1. Accesați Web Config și apoi selectați **Export and Import Setting Value** > **Import**.
2. Selectați fișierul exportat și apoi introduceți parola de criptare.
3. Faceți clic pe **Next**.

4. Selectați setările pe care doriți să le importați și apoi executați clic pe **Next**.
5. Faceți clic pe **OK**.

Setările vor fi aplicate la nivelul scanerului.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Soluționarea problemelor

Sugestii pentru soluționarea problemelor

Puteți găsi mai multe informații în următoarele manuale.

❏ Ghidul utilizatorului

Furnizează instrucțiuni despre utilizarea, întreținerea și rezolvarea problemelor scanerului.

Verificarea jurnalului pentru server și dispozitivul de rețea

În cazul problemelor cu conexiunea de rețea, puteți efectua identificarea cauzei confirmând jurnalul serverului de mail, a serverului LDAP, etc., verificând starea utilizând jurnalul de rețea din jurnalele și comenzile echipamentelor de sistem, precum routere.

Inițializarea setărilor de rețea

Restabilirea setărilor de rețea de la panoul de control

Puteți restabili toate setările rețelei la setările implicite.

1. Atingeți **Setări** pe ecranul de pornire.
2. Atingeți **Administrare sistem** > **Restaurare setări implicite** > **Setări rețea**.
3. Verificați mesajul și apoi atingeți **Da**.
4. Când este afișat un mesaj de finalizare, atingeți **Închidere**.

   Ecranul se va închide automat, după o anumită perioadă de timp, dacă nu atingeți **Închidere**.

Verificarea comunicării între dispozitive și computere

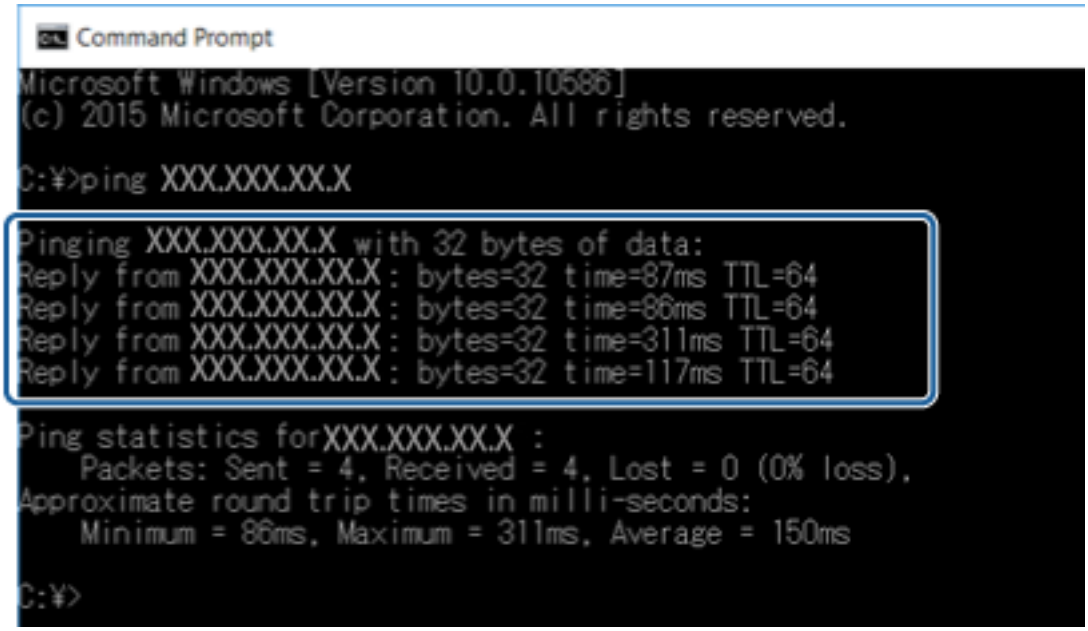
Verificarea conexiunii utilizând o comandă Ping — Windows

Puteți utiliza o comandă Ping pentru a vă asigura că computerul este conectat la scaner. Urmați pașii de mai jos pentru a verifica conexiunea utilizând o comandă Ping.

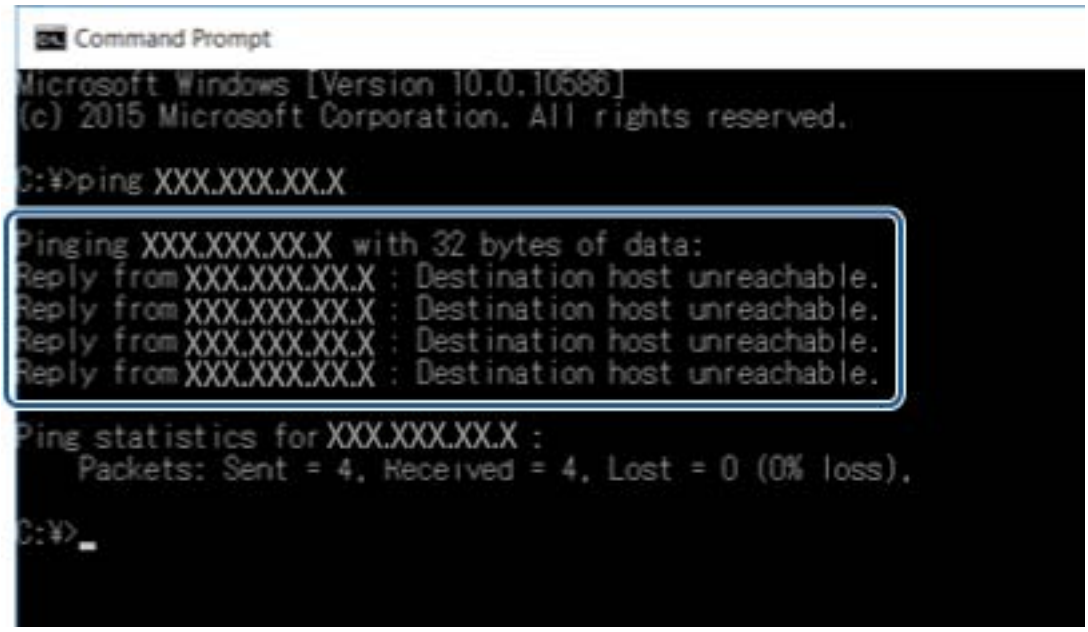
1. Verificați adresa IP a scanerului pentru conexiunea pe care doriți să o verificați.

   Puteți verifica aceasta utilizând Epson Scan 2.

2. Afișați ecranul de linie de comandă al computerului.
   - ❏ Windows 10
     Faceți clic dreapta pe butonul Start sau apăsați-l și mențineți-l, apoi selectați **Linie de comandă**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Afișați ecranul de aplicație și apoi selectați **Linie de comandă**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 sau o versiune anterioară
     Faceți clic pe butonul Start, selectați **Toate programele** sau **Programe** > **Accesorii** > **Linie de comandă**.
3. Introduceți „ping xxx.xxx.xxx.xxx” și apoi apăsați tasta Enter.
   Introduceți adresa IP a scanerului pentru xxx.xxx.xxx.xxx.
4. Verificați starea comunicației.
   Dacă scanerul și computerul comunică, este afișat următorul mesaj.



Dacă scanerul şi computerul nu comunică, este afişat următorul mesaj.



Verificarea conexiunii utilizând o comandă ping — Mac OS

Puteți utiliza o comandă Ping pentru a vă asigura că computerul este conectat la scaner. Urmați pașii de mai jos pentru a verifica conexiunea utilizând o comandă Ping.

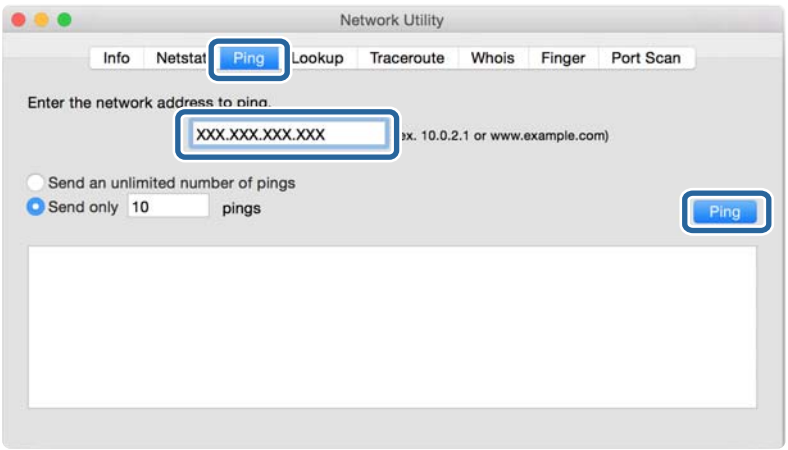
1. Verificați adresa IP a scanerului pentru conexiunea pe care doriți să o verificați.

   Puteți verifica aceasta utilizând Epson Scan 2.

2. Executați Utilitar de rețea.

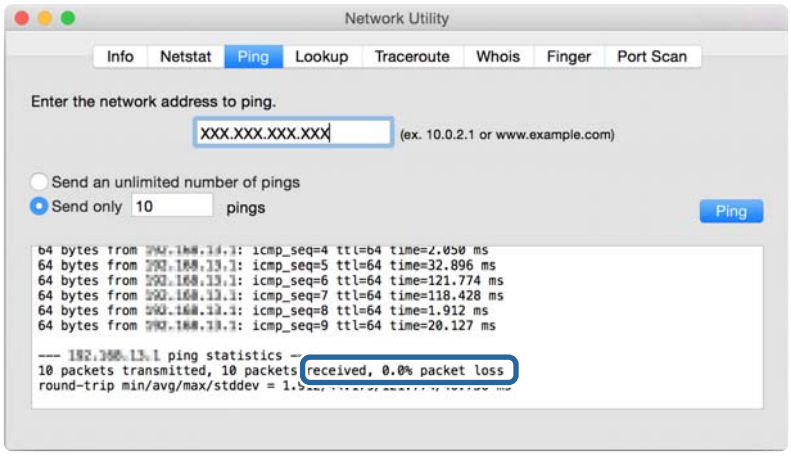
   Enter „Utilitar de rețea” în **Spotlight**.

3. Executați clic pe fila **Ping**, introduceți adresa de IP verificată în pasul 1 și apoi executați clic pe **Ping**.

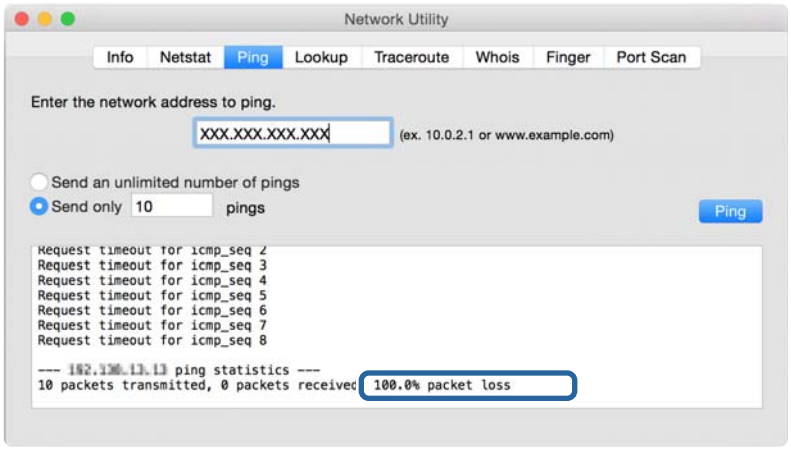


4. Verificați starea comunicării.

   Dacă scanerul şi computerul comunică, este afişat următorul mesaj.



   Dacă scanerul şi computerul nu comunică, este afişat următorul mesaj.



Probleme privind utilizarea software-ului de rețea

Nu se poate accesa Web Config

Adresa IP a scanerului este configurată în mod corespunzător?

Configurați adresa IP folosind Epson Device Admin sau EpsonNet Config.

Browser-ul dumneavoastră acceptă criptări în serie pentru Encryption Strength pentru SSL/TLS?

Criptările în serie pentru Encryption Strength pentru SSL/TLS sunt următoarele. Web Config poate fi accesat doar într-un browser care acceptă următoarele criptări în serie. Verificați compatibilitatea de criptare a browser-ului dumneavoastră.

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

❏ 192bit: AES256

❏ 256bit: AES256

Mesajul „Neactualizat” apare când accesați Web Config folosind comunicarea SSL (https).

Dacă certificatul nu este actualizat, obțineți din nou certificatul. Dacă mesajul apare înainte de data de expirare a acestuia, asigurați-vă că data scanerului este configurată corect.

Mesajul „Denumirea certificatului de securitate nu se potrivește…” apare când accesați Web Config folosind comunicarea SSL (https).

Adresa IP a scanerului introdusă pentru **Common Name** în vederea creării unui certificat autosemnat sau a unei CSR nu se potrivește cu adresa introdusă în browser. Obțineți și importați din nou un certificat sau schimbați denumirea scanerului.

Scanerul este accesat via un server proxy.

Dacă folosiți un server proxy cu scanerul dumneavoastră, trebuie să configurați setările proxy ale browser-ului dumneavoastră.

❏ 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 adresele locale.

❏ Mac OS:

Selectați **Preferințe sistem** > **Rețea** > **Avansat** > **Proxy-uri**, iar apoi înregistrați adresa locală pentru **Ocolește configurările 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

Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Alocarea adresei IP” la pagina 15

➡ „Alocarea unei adrese IP utilizând EpsonNet Config” la pagina 56

Denumirea de model şi/sau adresa IP nu sunt afişate pe EpsonNet Config

Ați selectat Blocare, Anulare sau Închidere când s-a afişat un ecran de securitate Windows sau un ecran de paravan de protecție?

Dacă selectați **Blocare**, **Anulare** sau **Închidere**, adresa IP sau denumirea modelului nu vor fi afişate pe EpsonNet Config sau EpsonNet Setup.

Pentru a corecta acest lucru, înregistrați EpsonNet Config ca excepție folosind paravanul de protecție Windows și software comercial de securitate. Dacă folosiți un program antivirus sau de securitate, închideți acest program și apoi încercați să folosiți EpsonNet Config.

Setarea de eroare de expirare a comunicației are o durată prea scurtă?

Executați EpsonNet Config și selectați **Tools** > **Options** > **Timeout**, iar apoi măriți durata de timp pentru setarea **Communication Error**. Dacă nu procedați în acest mod, EpsonNet Config poate funcționa mult mai greu.

Informații conexe

➡ „Executarea EpsonNet Config — Windows” la pagina 56

➡ „Executarea EpsonNet Config — Mac OS” la pagina 56

Anexă

Prezentarea software-ului de rețea

În cele ce urmează, este descris software-ul de configurare și gestionare a dispozitivelor.

Epson Device Admin

Epson Device Admin este o aplicație care vă permite să instalați dispozitive în rețea, iar apoi să configurați și să gestionați dispozitivele respective. Puteți achiziționa informații detaliate despre dispozitive, precum starea și consumabilele, puteți trimite notificări de alerte și crea rapoarte privind utilizarea dispozitivului. Puteți realiza, de asemenea, un șablon conținând elementele de setare și îl puteți aplica altor dispozitive sub formă de setări partajate. Puteți descărca Epson Device Admin de pe website-ul de Epson asistență. Pentru informații suplimentare, a se vedea documentația sau solicitați ajutorul Epson Device Admin.

Executarea Epson Device Admin (doar Windows)

Selectați **Toate programele** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Notă:
Dacă apare o alertă de firewall, permiteți accesul pentru Epson Device Admin.

EpsonNet Config

EpsonNet Config permite administratorului să configureze setările de rețea ale scanerului, precum alocarea unei adrese de IP și modificarea modului de conexiune. Caracteristica de setare în serie este acceptată pe Windows. Pentru informații suplimentare, a se vedea documentația sau solicitați ajutorul EpsonNet Config.

Executarea EpsonNet Config — Windows

Selectați **Toate programele** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Notă:
Dacă apare o alertă de firewall, permiteți accesul pentru EpsonNet Config.

Executarea EpsonNet Config — Mac OS

Selectați **Start** > **Aplicații** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager este un software pentru crearea unui pachet pentru o instalare simplă de scaner, precum instalarea driverului de scanaer, instalarea Document Capture Pro. Acest software permite administratorului să creeze pachete de software unice și să le distribuie grupurilor.

Pentru mai multe informații, vizitați website-ul regional Epson.

Alocarea unei adrese IP utilizând EpsonNet Config

Puteți aloca o adresă IP la scaner utilizând EpsonNet Config. EpsonNet Config vă permite să atribuiți o adresă IP la un scaner căruia nu i-a fost alocată una după conectarea utilizând un cablu Ethernet.

Alocarea adresei IP utilizând setările în lot

Crearea unui fișier pentru setările în lot

Utilizând adresa MAC și denumirea modelului pe post de chei, puteți crea un fișier SYLK pentru a seta adresa IP.

1. Deschideți o aplicație de foaie de calcul (cum ar fi Microsoft Excel) sau un editor text.
2. Introduceți „Info_MACAddress”, „Info_ModelName” și „TCPIP_IPAddress” pe primul rând, ca denumiri ale elementelor de setare.

   Introduceți elementele de setare pentru următoarele șiruri de text. Pentru a face distincție între majuscule/minuscule și caractere dublu-octet/octet, dacă numai un caracter este diferit, elementul nu va fi recunoscut.

   Introduceți denumirea elementului de setare conform descrierii de mai jos; în caz contrar EpsonNet Config nu poate recunoaște elementele de setare.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Introduceți adresa MAC, denumirea modelului și adresa IP pentru fiecare interfață de rețea.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Introduceți un nume și salvați ca fișier SYLK (*.slk).

Efectuarea setărilor în lot utilizând fișierul de configurare

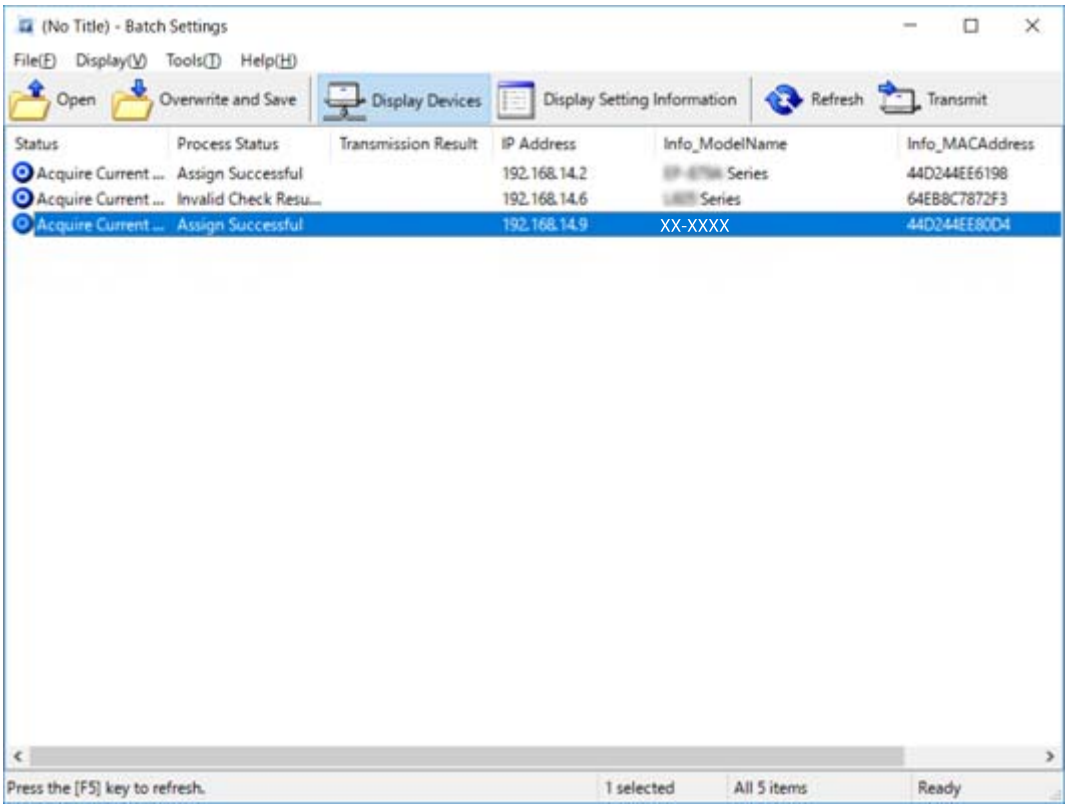
Alocați adresele IP în fișierul de configurare (fișier SYLK), pe rând. Trebuie să creați fișierul de configurare înaintea alocării.

1. Conectați toate dispozitivele la rețea folosind cabluri Ethernet.
2. Conectați scanerul la sursa de alimentare electrică.
3. Deschideți EpsonNet Config.

   Este afișată o listă a scanerelor din rețea. Poate fi necesar un interval de timp înainte de a fi afișate.
4. Executați clic pe **Tools** > **Batch Settings**.
5. Faceți clic pe **Open**.
6. Pe ecranul de selectare fișier, selectați fișierul SYLK (*.slk) conținând setările și apoi executați clic pe **Open**.

7. Selectați dispozitivele pentru care doriți să efectuați setările în lot cu coloana **Status** setată la **Unassigned** și **Process Status** setată la **Assign Successful**.

   Când efectuați setări multiple, apăsați Ctrl sau Shift și executați clic sau glisați cu mouse-ul.



8. Faceți clic pe **Transmit**.

9. Când este afișat ecranul de introducere a parolei, introduceți parola și executați clic pe **OK**.

   Transmiteți setările.

   Notă:
   Informațiile sunt transmise prin interfața de rețea până când bara de progres este finalizată. Nu opriți dispozitivul sau adaptorul wireless și nu trimiteți date la dispozitiv.

10. Pe ecranul **Transmitting Settings**, executați clic pe **OK**.

11. Verificați starea dispozitivului setat.

    Pentru dispozitive care indică  sau  , verificați conținutul fișierului cu setări sau dacă dispozitivul a repornit normal.

Pictogramă	Status	Process Status	Explicație
	Setup Complete	Setup Successful	Configurarea s-a finalizat normal.
	Setup Complete	Rebooting	După ce informațiile au fost transmise, fiecare dispozitiv trebuie repornit pentru a activa setările. Este efectuată o verificare pentru a determina dacă dispozitivul poate fi sau nu conectat după repornire.
	Setup Complete	Reboot Failed	Nu se poate confirma dispozitivul după transmiterea setărilor. Verificați dacă dispozitivul a pornit sau dacă a repornit normal.
	Setup Complete	Searching	Căutare pentru dispozitivul indicat în fișierul de setări.*
	Setup Complete	Search Failed	Nu se pot verifica dispozitivele care au fost deja configurate. Verificați dacă dispozitivul a pornit sau dacă a repornit normal.*

    * Doar când sunt afișate informațiile de setare.

Informații conexe

➡ „Executarea EpsonNet Config — Windows” la pagina 56
➡ „Executarea EpsonNet Config — Mac OS” la pagina 56

Alocarea unei adrese IP fiecărui dispozitiv

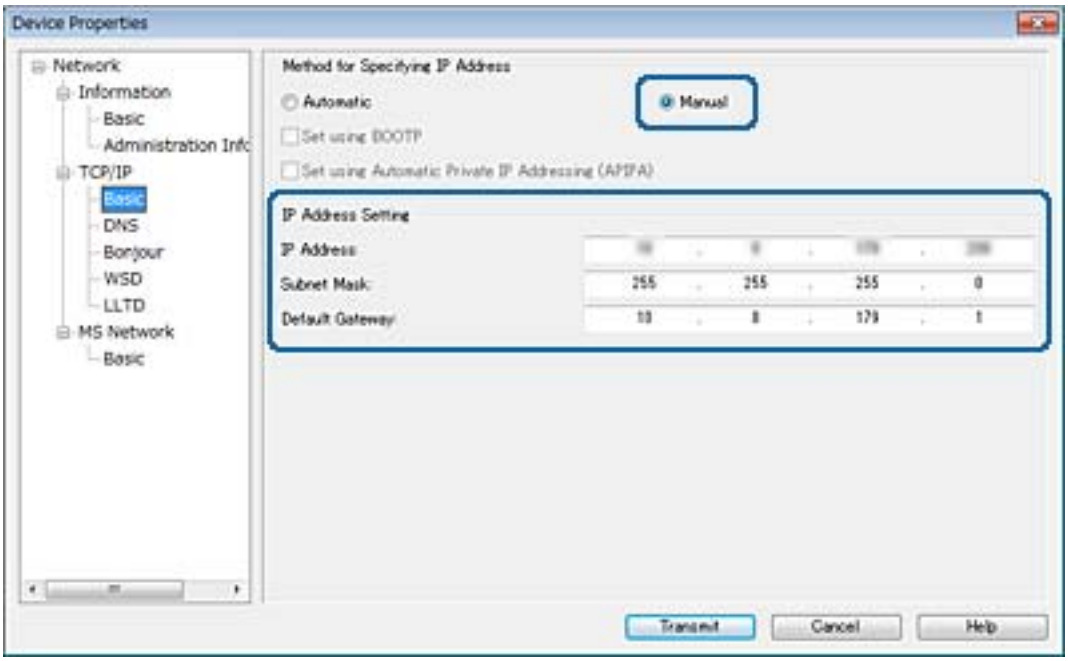
Alocați o adresă IP scanerului utilizând EpsonNet Config.

1. Conectați scanerul la sursa de alimentare electrică.
2. Conectați scanerul la rețea folosind un cablu Ethernet.
3. Deschideți EpsonNet Config.

   Este afișată o listă a scanerelor din rețea. Poate fi necesar un interval de timp înainte de a fi afișate.
4. Faceți dublu clic pe scanerul la care doriți alocarea.

   Notă:
   Dacă ați conectat mai multe scanere de același model, puteți identifica scanerul utilizând adresa MAC.
5. Selectați **Network** > **TCP/IP** > **Basic**.

6. Introduceți adresele pentru **IP Address**, **Subnet Mask**, și **Default Gateway**.



Notă:
Introduceți o adresă statică atunci când conectați scanerul la o rețea securizată.

7. Faceți clic pe **Transmit**.

   Se afișează ecranul care confirmă transmiterea informațiilor.

8. Faceți clic pe **OK**.

   Este afișat ecranul pentru finalizarea transmisiei.

   Notă:
   Informațiile sunt transmise dispozitivului, iar apoi este afișat mesajul „Configurare finalizată cu succes”. Nu opriți dispozitivul și nu trimiteți date la serviciu.

9. Faceți clic pe **OK**.

Informații conexe

➡ „Executarea EpsonNet Config — Windows” la pagina 56
➡ „Executarea EpsonNet Config — Mac OS” la pagina 56

Utilizarea portului pentru scaner

Scanerul utilizează portul următor. Aceste porturi trebuie puse la dispoziție de administratorul rețelei, dacă este necesar.

Anexă

Expeditor (client)	Utilizați	Detinație (server)	Protocol	Număr port
Scaner	Expediere e-mail (notificare e-mail)	Server SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP înainte de conexiune SMTP (notificare e-mail)	Server POP	POP3 (TCP)	110
	WSD de control	Computer client	WSD (TCP)	5357
	Căutați computerul atunci când este executată scanarea din Document Capture Pro	Computer client	Descoperire scanare prin comunicare în rețea	2968
	Colectarea informațiilor despre lucrare în timpul unei scanări push din Document Capture Pro	Computer client	Scanare push în rețea	2968
Computer client	Descoperiți scanerul dintr-o aplicație precum EpsonNet Config și driver de scaner.	Scaner	ENPC (UDP)	3289
	Colectați și configurați informațiile MIB dintr-o aplicație precum EpsonNet Config și driver de scaner.	Scaner	SNMP (UDP)	161
	Căutare scaner WSD	Scaner	WS-Discovery (UDP)	3702
	Redirecționarea datelor de scanare de la Document Capture Pro	Scaner	Scanare în rețea (TCP)	1865

Setări de securitate avansate la nivel de întreprindere

În acest capitol, vom descrie funcțiile de securitate avansate.

Setări de securitate și de prevenire a pericolelor

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

Pentru a evita astfel de riscuri, dispozitivele Epson dispun de o varietate de tehnologii de securitate.

Setați dispozitivul în modul necesar în funcție de condițiile de mediu, care au fost integrate cu informațiile de mediu ale clientului.

Nume	Tip funcție	Ce trebuie setat	Ce trebuie prevenit
Comunicare SSL/TLS	Calea de comunicare dintre un computer și un dispozitiv este criptată utilizând comunicarea SSL/TLS. Conținutul comunicării printr-un browser este protejat.	Setați un certificat CA pentru server, acesta fiind un certificat semnat de către o CA (Autoritate de certificare) pentru dispozitiv.	Preveniți scurgerea de informații privind setările și conținutul datelor transferate la scaner de la calculator. Accesul la serverul Epson pe Internet de la dispozitiv poate fi, de asemenea, protejat folosind o actualizare de firmware etc.
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 prin unitatea de pachete IP (criptare si autentificare), puteți comunica în condiții de siguranță un protocol de scanare nesecurizat.	Creați o politică de bază și o politică individuală pentru a seta clientul sau tipul de date care pot accesa dispozitivul.	Protejați împotriva accesului neautorizat, manipulării frauduloase a datelor și interceptării datelor de comunicare de la dispozitiv.
SNMPv3	Sunt adăugate funcții, cum ar fi monitorizarea dispozitivelor conectate în rețea, integritatea datelor la protocolul SNMP de control, criptarea, autentificarea etc.	Permiteți SNMPv3, apoi setați metoda de autentificare și criptare.	Asigurați setări de modificare prin intermediul rețelei, confidențialitate în stare de monitorizare.
IEEE802.1X	Permite conectarea doar a unui utilizator care este autentificat prin Ethernet. Permite utilizarea dispozitivului doar de către un utilizator autentificat.	Setare de autentificare la server RADIUS (server de autentificare).	Protejați împotriva accesării și utilizării neautorizate a dispozitivului.

Nume	Tip funcție	Ce trebuie setat	Ce trebuie prevenit
Citiți cartela de identificare	Puteți utiliza dispozitivul cu ajutorul unei cartele de identificare la dispozitivul autentificat conectat. Puteți limita obținerea jurnalelor pentru fiecare utilizator și dispozitiv și limita utilizarea dispozitivelor disponibile și funcțiile disponibile pentru fiecare utilizator și grup.	Conectați un dispozitiv de autentificare la dispozitiv și apoi setați informațiile despre utilizator în sistemul de autentificare.	Preveniți utilizarea neautorizată și falsificarea datelor dispozitivului.

Informații conexe

➡ „Comunicare SSL/TLS cu scanerul” la pagina 63
➡ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 71
➡ „Utilizarea protocolului SNMPv3” la pagina 82
➡ „Conectarea scanerului la o rețea IEEE802.1X” la pagina 84

Setări ale funcției de securitate

Când setați filtrarea IPsec/IP sau IEEE802.1X, se recomandă să accesați Web Config utilizând SSL/TLS pentru a comunica informațiile de setări pentru a reduce riscurile de securitate, precum manipularea frauduloasă sau interceptarea.

Comunicare SSL/TLS cu scanerul

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

Despre certificarea digitală

❏ Certificat semnat de o CA

Un certificat semnat de o CA (autoritate de certificare) trebuie obținut de la o autoritate de certificare. Puteți asigura comunicări securizate folosind un certificat CA-semnat. Puteți folosi un certificat CA-semnat pentru fiecare caracteristică de securitate.

❏ Certificat CA

Un certificat CA arată că o terță parte a verificat identitatea unui server. Acesta este o componentă cheie pentru asigurarea unui site securizat. Trebuie să obțineți un certificat CA pentru autentificarea serverului de la o CA care emite acest certificat.

❏ Certificat autosemnat

Certificatul autosemnat este un certificat pe care scanerul îl emite și îl semnează singur. Acest certificat nu prezintă siguranță și nu poate împiedica falsificarea adresei. Dacă folosiți acest certificat pentru un certificat SSL/TLS, o alertă de securitate poate fi afișată în browser. Puteți folosi acest certificat numai pentru o comunicare SSL/TLS.

Informații conexe

➡ „Obținerea și importul unui certificat CA-semnat” la pagina 64
➡ „Ștergerea unui certificat CA-semnat” la pagina 67
➡ „Actualizarea unui certificat autosemnat” la pagina 68

Obținerea și importul unui certificat CA-semnat

Obținerea unui certificat CA-semnat

Pentru obținerea unui certificat CA-semnat, creați 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 **Network Security Settings**. Apoi, selectați **SSL/TLS** > **Certificate** sau **IPsec/IP Filtering** > **Client Certificate** sau **IEEE802.1X** > **Client Certificate**.

2. Faceți clic pe **Generate** 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 **Network Security Settings**. Apoi, selectați **SSL/TLS** > **Certificate** sau **IPsec/IP Filtering** > **Client Certificate** sau **IEEE802.1X** > **Client Certificate**.

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 mai generați niciodată un element CSR. Dacă faceți acest lucru, nu veți mai putea importa un CA-signed Certificate emis.*

7. Trimiteți elementul CSR unei autorități de certificare și obțineți un CA-signed Certificate.

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

8. Salvați CA-signed Certificate emis pe un computer conectat la scaner.

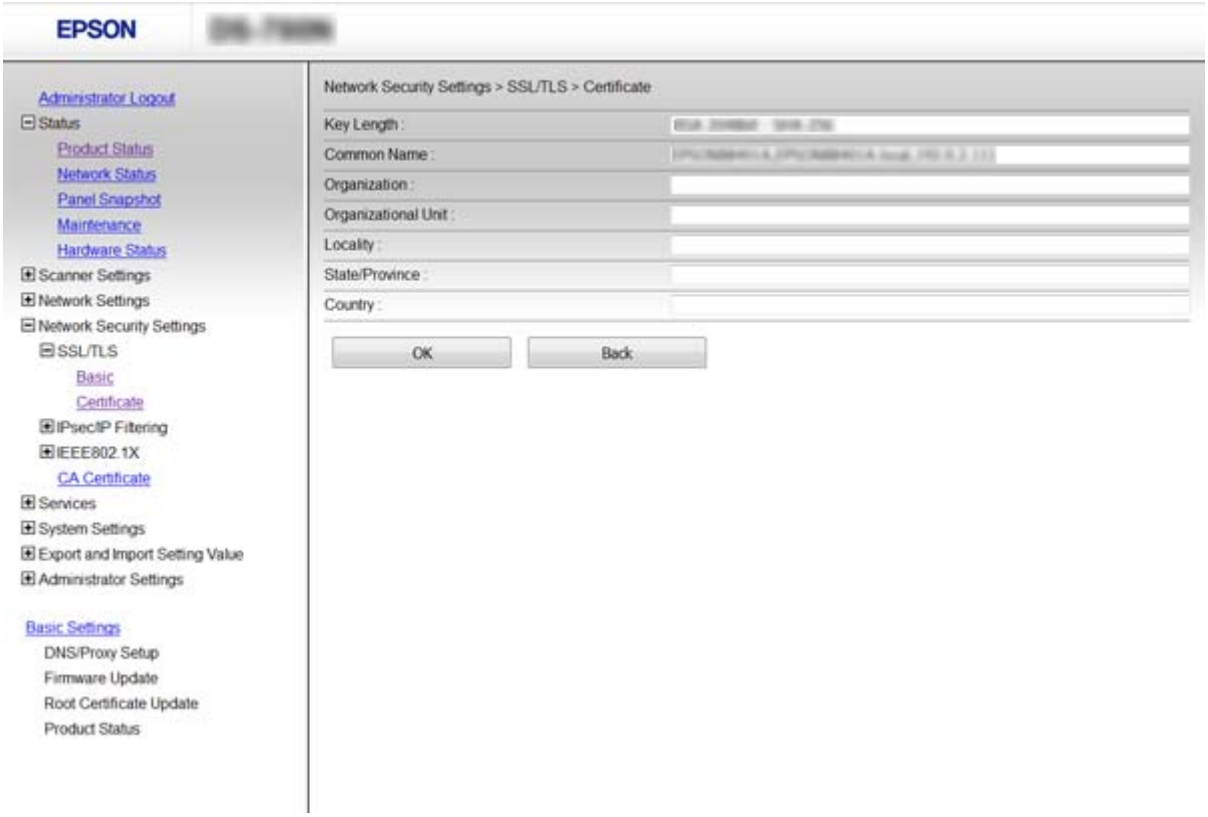
   Obținerea unui CA-signed Certificate este finalizată când salvați un certificat la o destinație.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Elemente setare CSR” la pagina 65
➡ „Import al unui certificat CA-semnat” la pagina 66

Elemente setare CSR



Elemente	Setări și explicații
Key Length	Selectați o lungime de cheie pentru o CSR.
Common Name	Puteți introduce între 1 și 128 de caractere. Dacă aceasta este o adresă IP, aceasta trebuie să fie o adresă IP statică. Exemplu: URL pentru accesarea Web Config: https://10.152.12.225 Nume obișnuit: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Puteți introduce între 0 și 64 caractere în ASCII (0x20 – 0x7E). Puteți separa numele distinctive cu virgule.
Country	Introduceți un cod de țară, având un număr de două cifre indicat de ISO-3166.

Informații conexe

➡ „Obținerea unui certificat CA-semnat” la pagina 64

Import al unui certificat CA-semnat

Important:

❏ *Asigurați-vă că data și ora scanerului sunt setate corect.*

❏ *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 **Network Security Settings**. Apoi, selectați **SSL/TLS** > **Certificate** sau **IPsec/IP Filtering** > **Client Certificate** sau **IEEE802.1X** > **Client Certificate**.

2. Faceți clic pe **Import**.

   O pagină de import certificat este deschisă.

3. Introduceți o valoare pentru fiecare element.

   În funcție de locul unde creați o CSR și un format de fișier al unui certificat, 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

   ❏ **Private Key**: Nu configurați pentru că scanerul conține o cheie privată.

   ❏ **Password**: Nu configurați.

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

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

   ❏ **Private Key**: Trebuie să setați.

   ❏ **Password**: Nu configurați.

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

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

   ❏ **Private Key**: Nu configurați.

   ❏ **Password**: Opțional

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

4. Faceți clic pe **OK**.

   Un mesaj de finalizare este afișat.

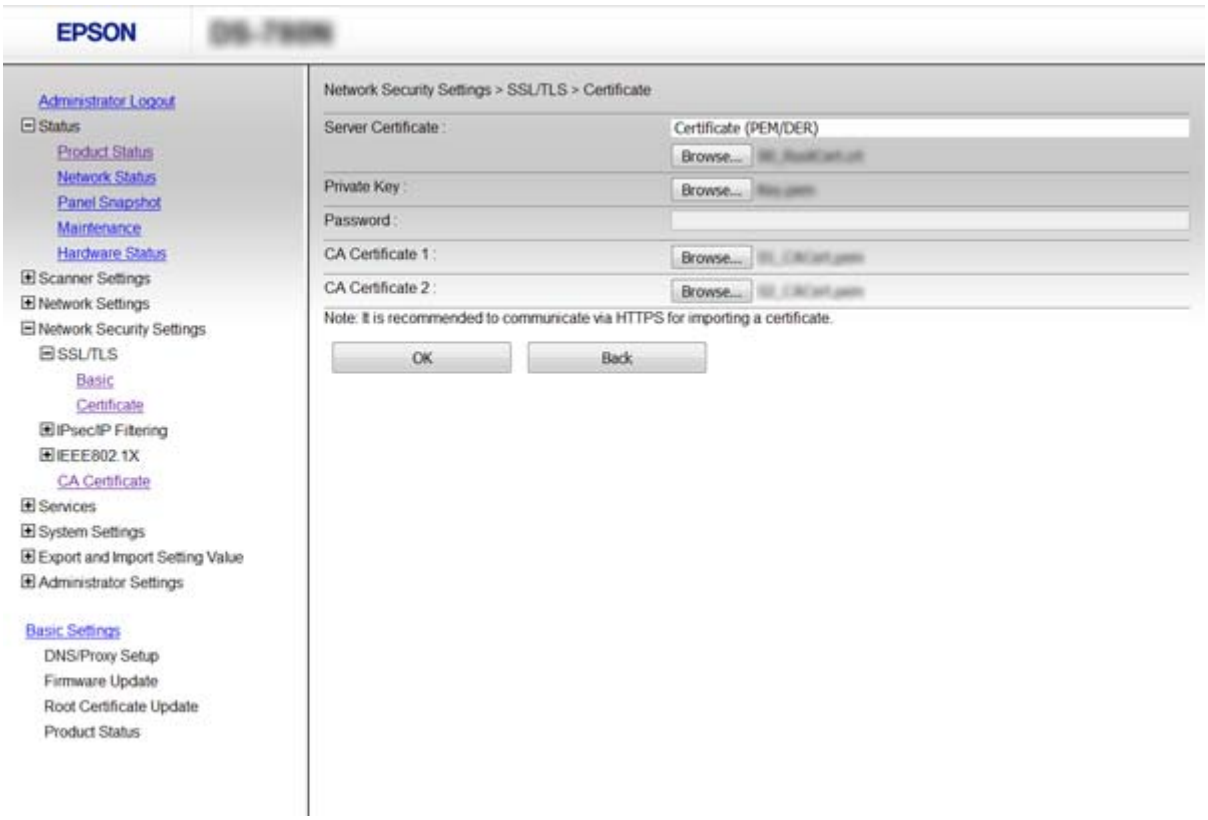
Notă:
*Faceți clic pe **Confirm** pentru a verifica informația de certificare.*

Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Certificat CA-semnat Import elemente de setare” la pagina 67

Certificat CA-semnat Import elemente de setare



Elemente	Setări și explicații
Server Certificate sau Client Certificate	Selectați formatul unui certificat.
Private Key	Dacă obțineți un certificat în format PEM/DER folosind o CSR creată de pe un computer, indicați un fișier de cheie privată care corespunde certificatului.
Password	Introduceți o parolă pentru a cripta o cheie privată.
CA Certificate 1	Dacă formatul certificatului dumneavoastră este **Certificate (PEM/DER)**, importați un certificat al unei autorități de certificare care emite un certificat de server. Indicați un fișier dacă aveți nevoie.
CA Certificate 2	Dacă formatul certificatului dumneavoastră este **Certificate (PEM/DER)**, importați un certificat al unei autorități de certificare care emite **CA Certificate 1**. Indicați un fișier dacă aveți nevoie.

Informații conexe

➡ „Import al unui certificat CA-semnat” la pagina 66

Ştergerea unui certificat CA-semnat

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

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

1. Accesați Web Config și apoi selectați **Network Security Settings**. Apoi, selectați **SSL/TLS** > **Certificate** sau **IPsec/IP Filtering** > **Client Certificate** sau **IEEE802.1X** > **Client Certificate**.
2. Faceți clic pe **Delete**.
3. În mesajul care apare, confirmați faptul că doriți să ștergeți certificatul.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Actualizarea unui certificat autosemnat

Dacă scanerul este compatibil cu caracteristica de server HTTPS, puteți actualiza un certificat autosemnat. Când accesați Web Config folosind un certificat autosemnat, apare un mesaj de avertizare.

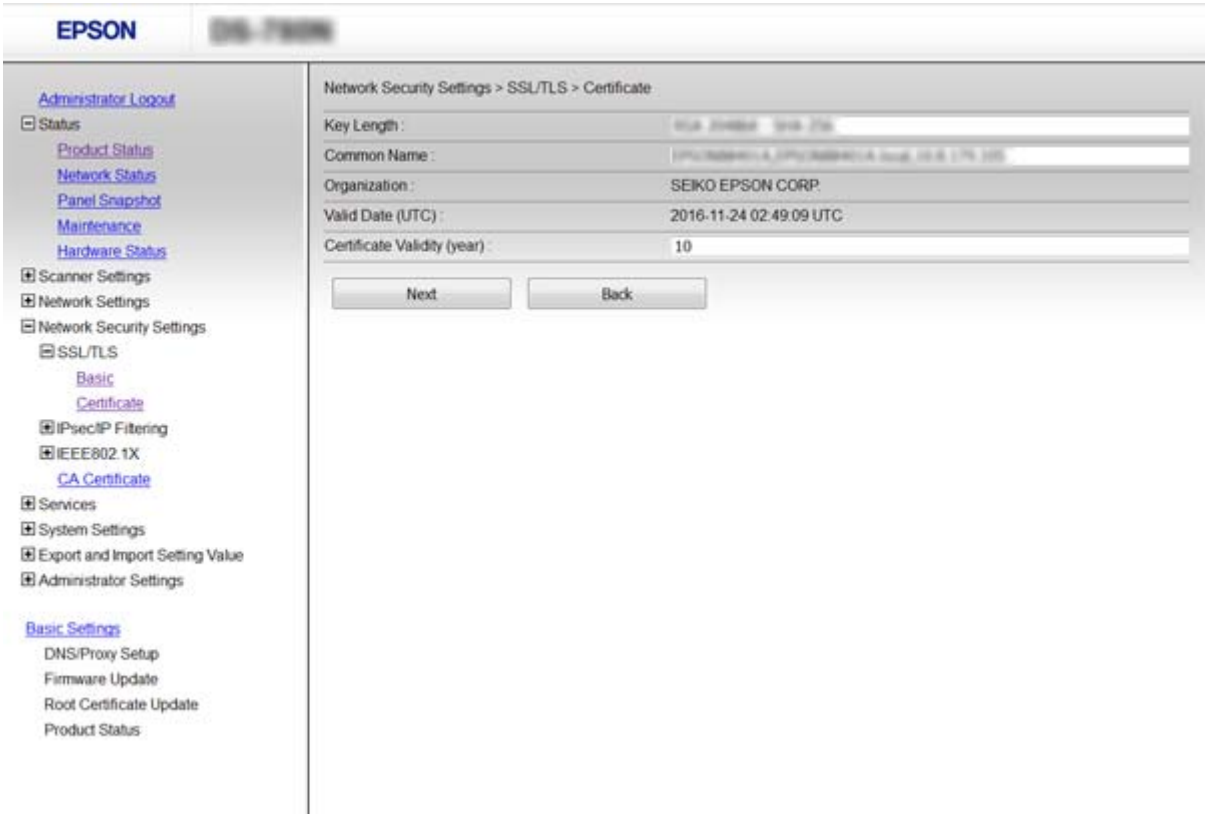
Folosiți temporar un certificat autosemnat până ce obțineți și importați un certificat CA-semnat.

1. Accesați Web Config și selectați **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Faceți clic pe **Update**.
3. Introduceți **Common Name**.

   Introduceți o adresă IP sau un identificator, precum denumirea FQDN, pentru scaner. Puteți introduce între 1 și 128 de caractere.

   Notă:
   Puteți separa numele distinctive (CN) cu virgule.

4. Indicați o perioadă de valabilitate pentru certificat.



5. Faceți clic pe **Next**.

   Un mesaj de confirmare este afișat.

6. Faceți clic pe **OK**.

   Scanerul este actualizat.

Notă:
*Faceți clic pe **Confirm** pentru a verifica informația de certificare.*

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Configurați CA Certificate

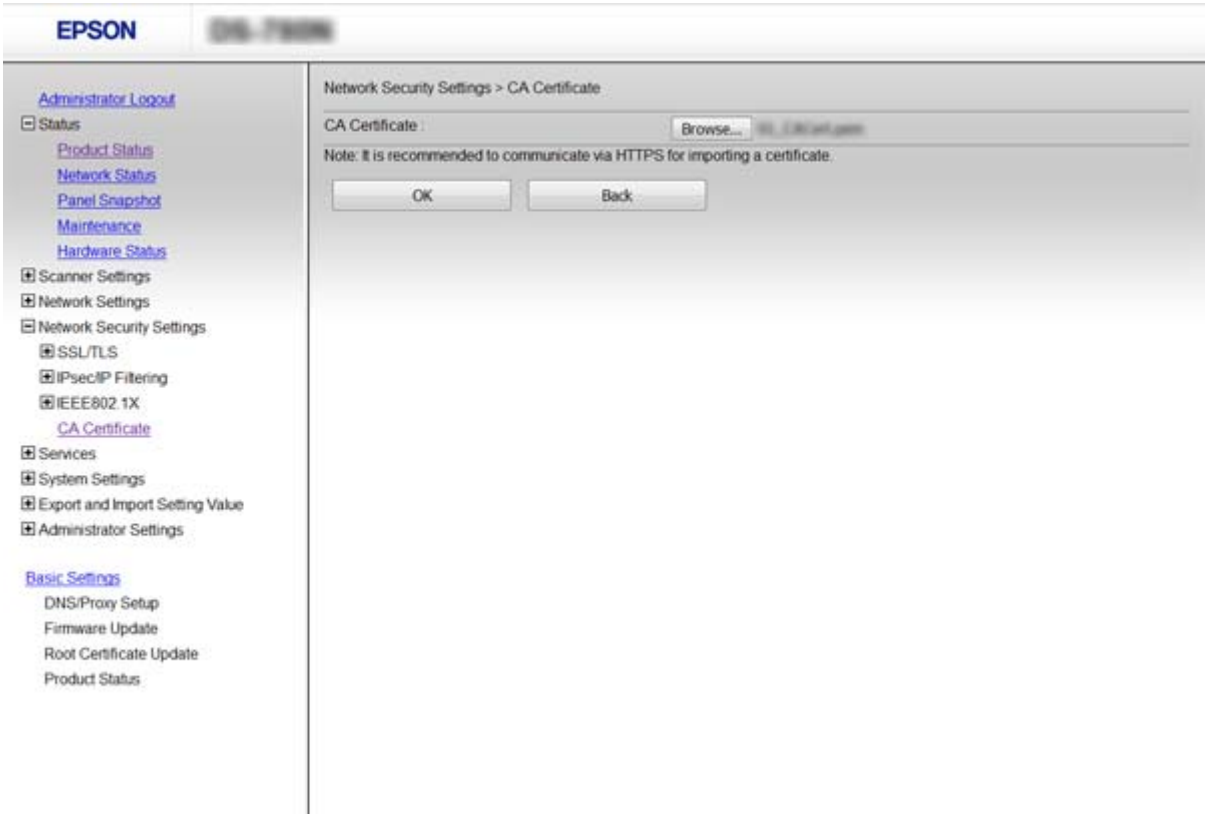
Puteți să importați, afișați și ștergeți un CA Certificate.

Importarea unui CA Certificate

1. Accesați Web Config și apoi selectați **Network Security Settings** > **CA Certificate**.

2. Faceți clic pe **Import**.

3. Specificați CA Certificate pe care doriți să-l importați.



4. Faceți clic pe **OK**.

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

Informații conexe

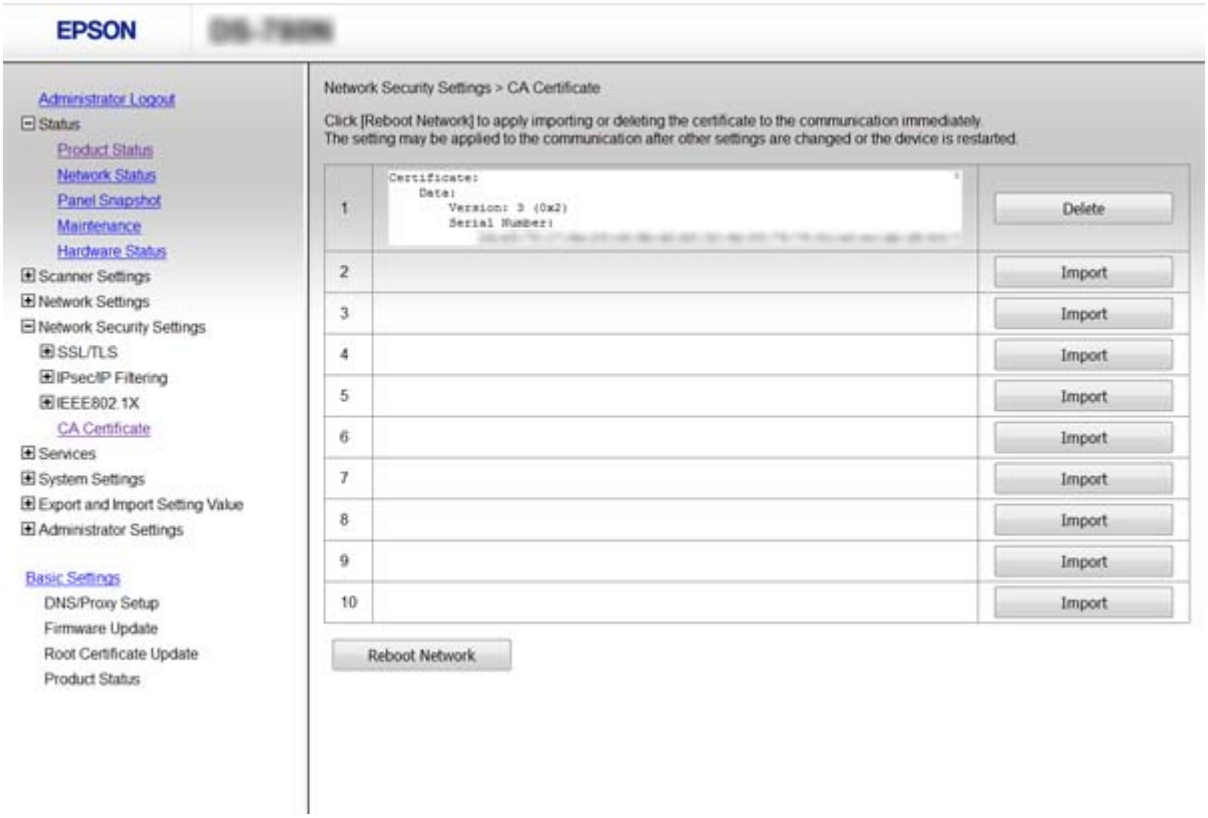
➡ „Accesarea Web Config” la pagina 23

Ştergerea unui CA Certificate

Puteți să ștergeți CA Certificate pe care l-ați importat.

1. Accesați Web Config şi apoi selectați **Network Security Settings** > **CA Certificate**.

2. Faceți clic pe **Delete** din dreptul CA Certificate pe care doriți să îl ștergeți.



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

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Comunicare criptată utilizând filtrarea IPsec/IP

Despre IPsec/IP Filtering

Dacă scanerul este compatibil cu IPsec/Filtrare IP, puteți filtra traficul în funcție de adresele IP, de servicii și de port. Prin combinarea filtrării, puteți configura scanerul să accepte sau să blocheze clienți indicați și date indicate. În plus, puteți îmbunătăți nivelul de securitate folosind un IPsec.

Pentru a filtra traficul, configurați politica implicită. Politica implicită se aplică fiecărui utilizator sau grup care se conectează la scaner. Pentru un control mai rafinat al utilizatorilor și al grupurilor de utilizatori, configurați politicile de grup. O politică de grup înseamnă una sau mai multe reguli aplicate unui utilizator sau grup de utilizatori. Scanerul controlează pachetele IP care corespund politicilor configurate. Pachetele IP sunt autentificate în ordinea unei politici de grup de 1 la 10, iar apoi în funcție de politica implicită.

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

Configurarea Default Policy

1. Accesați Web Config şi selectați **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Introduceți o valoare pentru fiecare element.
3. Faceți clic pe **Next**.

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

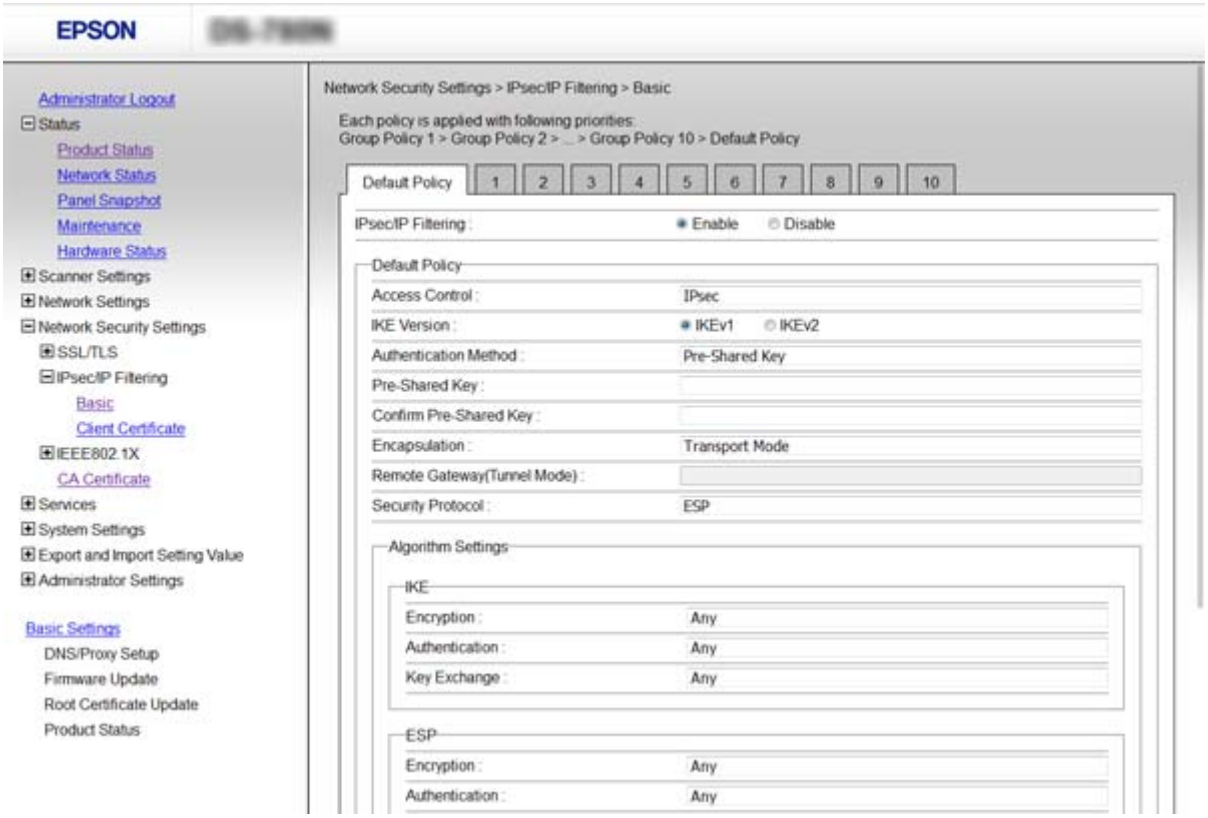
   Scanerul este actualizat.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Elemente de setare Default Policy” la pagina 72

Elemente de setare Default Policy



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

Setări de securitate avansate la nivel de întreprindere

Elemente	Setări și explicații	
Access Control	Configurați o metodă de control pentru traficul pachetelor IP.	
	Permit Access	Selectați această opțiune pentru a permite pachetelor IP configurate să treacă.
	Refuse Access	Selectați această opțiune pentru a împiedica pachetele IP configurate să treacă.
	IPsec	Selectați această opțiune pentru a permite pachetelor IPsec configurate să treacă.
IKE Version	Selectați IKEv1 sau IKEv2 pentru versiunea IKE. Selectați una dintre acestea, în funcție de dispozitivul la care este conectat scanerul.	
IKEv1	Următoarele elemente sunt afișate atunci când selectați **IKEv1** pentru **IKE Version**.	
	Authentication Method	Pentru a selecta **Certificate**, trebuie să obțineți și să importați un certificat CA-semnat în prealabil.
	Pre-Shared Key	Dacă selectați **Pre-Shared Key** pentru **Authentication Method**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirm Pre-Shared Key	Pentru confirmare, introduceți cheia configurată.
IKEv2	Următoarele elemente sunt afișate atunci când selectați **IKEv2** pentru **IKE Version**.	
Local	Authentication Method	Pentru a selecta **Certificate**, trebuie să obțineți și să importați un certificat CA-semnat în prealabil.
	ID Type	Selectați tipul de ID pentru scaner.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@”, „#” și „=” pentru primul caracter. **Distinguished Name**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=”. **IP Address**: 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 (.). **Email Address**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@”. **Key ID**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E).
	Pre-Shared Key	Dacă selectați **Pre-Shared Key** pentru **Authentication Method**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirm Pre-Shared Key	Pentru confirmare, introduceți cheia configurată.

Setări de securitate avansate la nivel de întreprindere

Elemente	Setări și explicații	
Remote	Authentication Method	Pentru a selecta **Certificate**, trebuie să obțineți și să importați un certificat CA-semnat în prealabil.
	ID Type	Selectați tipul de ID pentru dispozitivul pe care doriți să-l autentificați.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@", „#" și „=" pentru primul caracter. **Distinguished Name**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=". **IP Address**: 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 (.). **Email Address**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@". **Key ID**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E).
	Pre-Shared Key	Dacă selectați **Pre-Shared Key** pentru **Authentication Method**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirm Pre-Shared Key	Pentru confirmare, introduceți cheia configurată.
Encapsulation	Dacă selectați **IPsec** pentru **Access Control**, trebuie să configurați un mod capsulare.	
	Transport Mode	Dacă utilizați scanerul numai pe același LAN, selectați această opțiune. Pachetele IP de strat 4 sau ulterior sunt criptate.
	Tunnel Mode	Dacă folosiți scanerul într-o rețea cu conexiune la Internet, precum IPsec-VPN, selectați această opțiune. Antetul și datele pachetelor IP sunt criptate.
Remote Gateway(Tunnel Mode)	Dacă selectați **Tunnel Mode** pentru **Encapsulation**, introduceți o adresă de gateway folosind între 1 și 39 de caractere.	
Security Protocol	**IPsec** pentru **Access Control**, selectați o opțiune.	
	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 criptarea datelor este interzisă, puteți folosi IPsec.
Algorithm Settings		
IKE	Encryption	Selectați algoritmul de criptare pentru IKE. Elementele variază în funcție de versiunea IKE.
	Authentication	Selectați algoritmul de autentificare pentru IKE.
	Key Exchange	Selectați algoritmul de schimb cheie pentru IKE. Elementele variază în funcție de versiunea IKE.

Elemente	Setări și explicații	
ESP	Encryption	Selectați algoritmul de criptare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Security Protocol**.
	Authentication	Selectați algoritmul de autentificare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Security Protocol**.
AH	Authentication	Selectați algoritmul de criptare pentru AH. Aceasta este disponibilă atunci când **AH** este selectat pentru **Security Protocol**.

Informații conexe

➡ „Configurarea Default Policy” la pagina 72

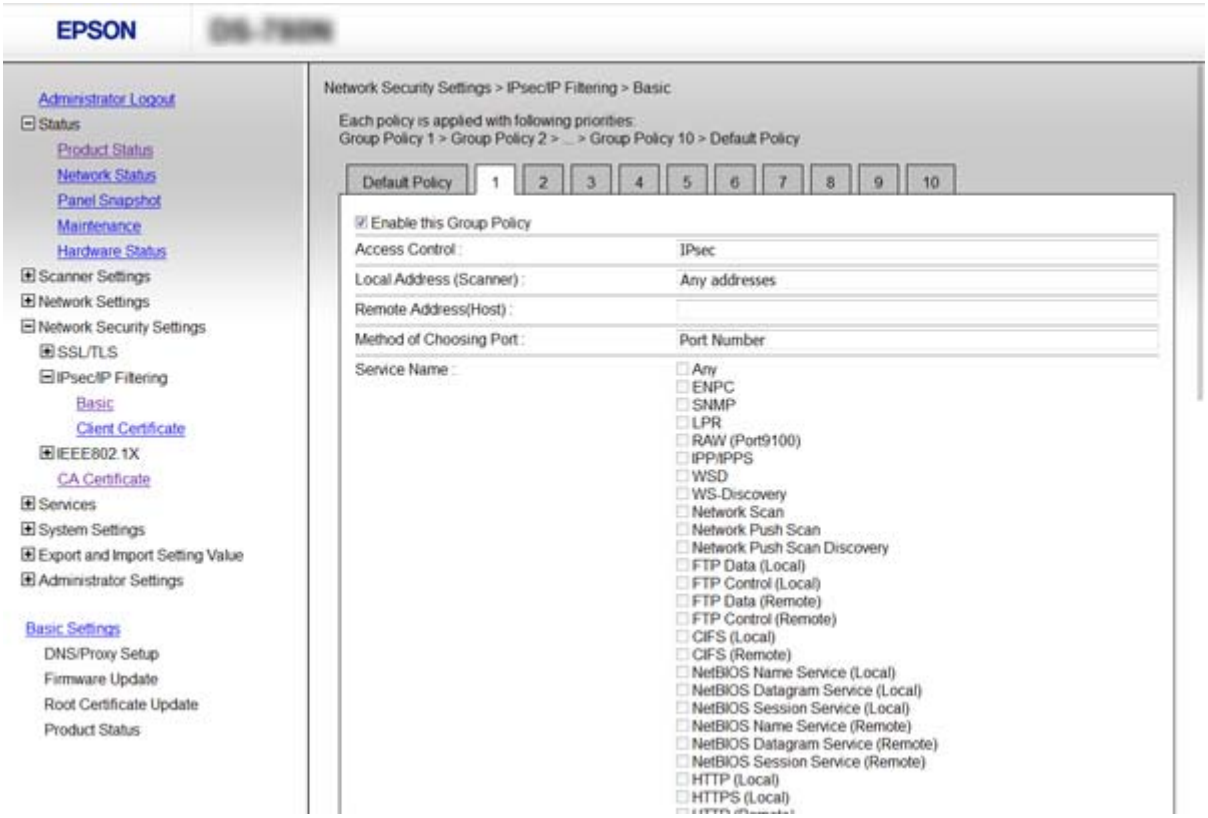
Configurarea Group Policy

1. Accesați Web Config și selectați **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Executați clic pe o filă numerotată pe care doriți să o configurați.
3. Introduceți o valoare pentru fiecare element.
4. Faceți clic pe **Next**.
   Un mesaj de confirmare este afișat.
5. Faceți clic pe **OK**.
   Scanerul este actualizat.

Informații conexe

➡ „Accesarea Web Config” la pagina 23
➡ „Elemente de setare Group Policy” la pagina 76

Elemente de setare Group Policy



Elemente	Setări și explicații	
Enable this Group Policy	Puteți activa sau dezactiva o politică de grup.	
Access Control	Configurați o metodă de control pentru traficul pachetelor IP.	
	Permit Access	Selectați această opțiune pentru a permite pachetelor IP configurate să treacă.
	Refuse Access	Selectați această opțiune pentru a împiedica pachetele IP configurate să treacă.
	IPsec	Selectați această opțiune pentru a permite pachetelor IPsec configurate să treacă.
Local Address (Scanner)	Selectați o adresă IPv4 sau o adresă IPv6 care corespunde mediului dumneavoastră de rețea. Dacă o adresă IP este alocată automat, puteți selecta **Use auto-obtained IPv4 address**.	
Remote Address(Host)	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.*	
Method of Choosing Port	Selectați o metodă pentru a specifica porturile.	
Service Name	Dacă selectați **Service Name** pentru **Method of Choosing Port**, selectați o opțiune.	

Setări de securitate avansate la nivel de întreprindere

Elemente	Setări și explicații	
Transport Protocol	Dacă selectați **Port Number** pentru **Method of Choosing Port**, trebuie să configurați un mod capsulare.	
	Any 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.
Local Port	Dacă selectați **Port Number** pentru **Method of Choosing Port** și dacă selectați **TCP** sau **UDP** pentru **Transport Protocol**, 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.	
Remote Port	Dacă selectați **Port Number** pentru **Method of Choosing Port** și dacă selectați **TCP** sau **UDP** pentru **Transport Protocol**, 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.	
IKE Version	Selectați IKEv1 sau IKEv2 pentru versiunea IKE. Selectați una dintre acestea, în funcție de dispozitivul la care este conectat scanerul.	
IKEv1	Următoarele elemente sunt afișate atunci când selectați **IKEv1** pentru **IKE Version**.	
	Authentication Method	Dacă selectați **IPsec** pentru **Access Control**, selectați o opțiune. Un certificat folosit este comun cu o politică implicită.
	Pre-Shared Key	Dacă selectați **Pre-Shared Key** pentru **Authentication Method**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirm Pre-Shared Key	Pentru confirmare, introduceți cheia configurată.
IKEv2	Următoarele elemente sunt afișate atunci când selectați **IKEv2** pentru **IKE Version**.	

Setări de securitate avansate la nivel de întreprindere

Elemente	Setări și explicații	
Local	Authentication Method	Dacă selectați **IPsec** pentru **Access Control**, selectați o opțiune. Un certificat folosit este comun cu o politică implicită.
	ID Type	Selectați tipul de ID pentru scaner.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@", „#" și „=" pentru primul caracter. **Distinguished Name**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=". **IP Address**: 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 (.). **Email Address**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@". **Key ID**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E).
	Pre-Shared Key	Dacă selectați **Pre-Shared Key** pentru **Authentication Method**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirm Pre-Shared Key	Pentru confirmare, introduceți cheia configurată.
Remote	Authentication Method	Dacă selectați **IPsec** pentru **Access Control**, selectați o opțiune. Un certificat folosit este comun cu o politică implicită.
	ID Type	Selectați tipul de ID pentru dispozitivul pe care doriți să-l autentificați.
	ID	Introduceți ID-ul scanerului care corespunde tipului de ID. Nu puteți utiliza „@", „#" și „=" pentru primul caracter. **Distinguished Name**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „=". **IP Address**: 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 (.). **Email Address**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E). Trebuie să includeți „@". **Key ID**: Introduceți 1 – 128 caractere ASCII de 1 octet (0x20 – 0x7E).
	Pre-Shared Key	Dacă selectați **Pre-Shared Key** pentru **Authentication Method**, introduceți o cheie pre-partajată folosind între 1 și 127 de caractere.
	Confirm Pre-Shared Key	Pentru confirmare, introduceți cheia configurată.

Setări de securitate avansate la nivel de întreprindere

Elemente	Setări și explicații	
Encapsulation	Dacă selectați **IPsec** pentru **Access Control**, trebuie să configurați un mod capsulare.	
	Transport Mode	Dacă utilizați scanerul numai pe același LAN, selectați această opțiune. Pachetele IP de strat 4 sau ulterior sunt criptate.
	Tunnel Mode	Dacă folosiți scanerul într-o rețea cu conexiune la Internet, precum IPsec-VPN, selectați această opțiune. Antetul și datele pachetelor IP sunt criptate.
Remote Gateway(Tunnel Mode)	Dacă selectați **Tunnel Mode** pentru **Encapsulation**, introduceți o adresă de gateway folosind între 1 și 39 de caractere.	
Security Protocol	Dacă selectați **IPsec** pentru **Access Control**, selectați o opțiune.	
	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 criptarea datelor este interzisă, puteți folosi IPsec.
Algorithm Settings		
IKE	Encryption	Selectați algoritmul de criptare pentru IKE. Elementele variază în funcție de versiunea IKE.
	Authentication	Selectați algoritmul de autentificare pentru IKE.
	Key Exchange	Selectați algoritmul de schimb cheie pentru IKE. Elementele variază în funcție de versiunea IKE.
ESP	Encryption	Selectați algoritmul de criptare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Security Protocol**.
	Authentication	Selectați algoritmul de autentificare pentru ESP. Aceasta este disponibilă atunci când **ESP** este selectat pentru **Security Protocol**.
AH	Authentication	Selectați algoritmul de autentificare pentru AH. Aceasta este disponibilă atunci când **AH** este selectat pentru **Security Protocol**.

Informații conexe

- „Configurarea Group Policy” la pagina 75
- „Combinație dintre Local Address (Scanner) și Remote Address(Host) pe Group Policy” la pagina 80
- „Referințe privind numele de serviciu în politica de grup” la pagina 80

Combinație dintre Local Address (Scanner) şi Remote Address(Host) pe Group Policy

		Setarea Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Setarea Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Gol	✓	✓	✓

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

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

*3 Cu excepția adreselor de legătură locală IPv6.

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
Any	–	–	–	Toate serviciile
ENPC	UDP	3289	Orice port	Căutarea unui scaner din aplicații precum EpsonNet Config și un driver de scaner
SNMP	UDP	161	Orice port	Obținerea și configurarea MIB din aplicații precum EpsonNet Config și driverul de scaner Epson
WSD	TCP	Orice port	5357	Controlarea WSD
WS-Discovery	UDP	3702	Orice port	Căutarea unui scaner din WSD
Network Scan	TCP	1865	Orice port	Redirecționarea datelor de scanare de la Document Capture Pro
Network Push Scan Discovery	UDP	2968	Orice port	Căutarea unui computer de la scaner
Network Push Scan	TCP	Orice port	2968	Achiziție a informațiilor despre lucrare în cazul unei scanări de la Document Capture Pro sau Document Capture
HTTP (Local)	TCP	80	Orice port	Server HTTP(S) (redirecționarea datelor Web Config și WSD)
HTTPS (Local)	TCP	443	Orice port	
HTTP (Remote)	TCP	Orice port	80	Client HTTP(S) (comunicare între actualizare firmware și actualizare certificat root)
HTTPS (Remote)	TCP	Orice port	443	

Exemple de configurare IPsec/IP Filtering

Primirea numai de pachete IPsec

Acest exemplu este numai pentru configurarea unei politici implicite.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: Introduceți maximum 127 de caractere.

Group Policy:

Nu configurați.

Acceptarea scanării utilizând Epson Scan 2 și setările scanerului

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

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Bifați caseta.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: Adresă IP a unui client

❏ **Method of Choosing Port**: **Service Name**

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

Acceptarea accesului numai de la o adresă IP specificată

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

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**:**Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Bifați caseta.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: Adresă IP a unui client al administratorului

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

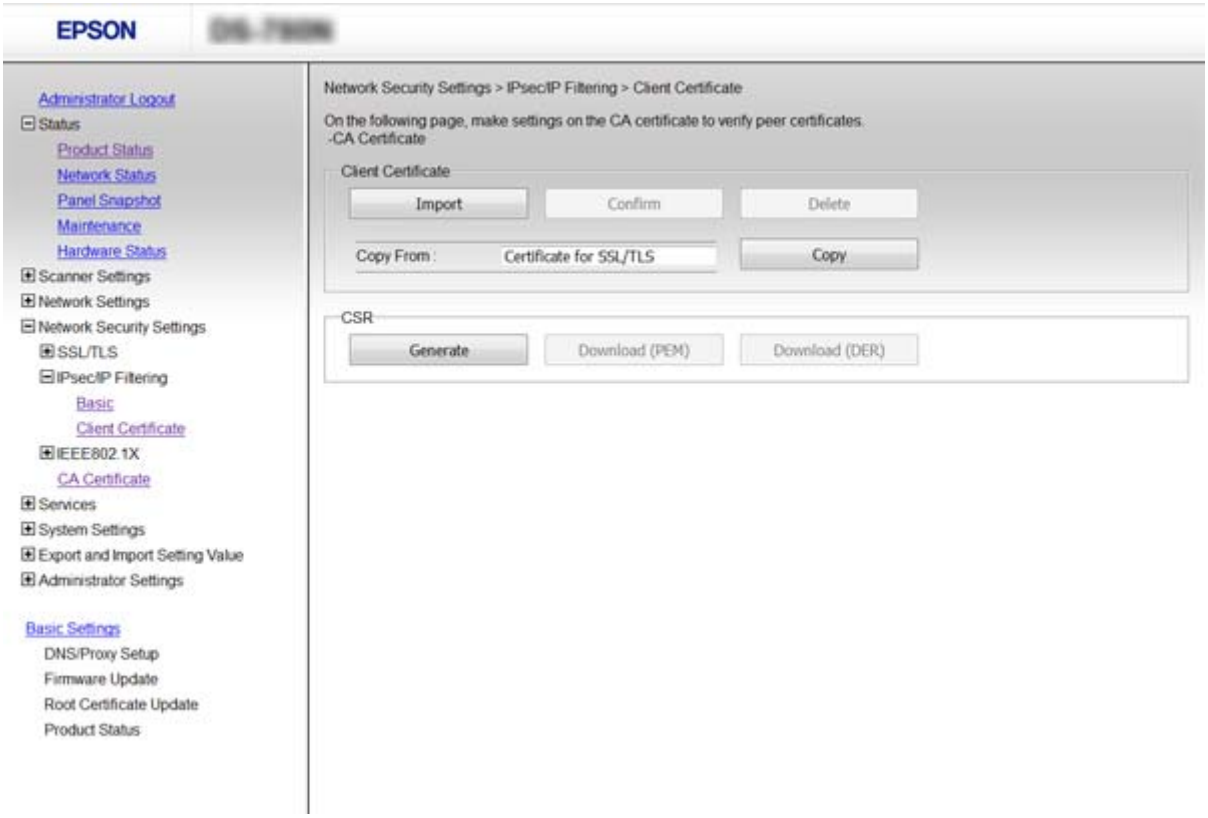
Configurarea certificatului pentru IPsec/IP Filtering

Configurarea certificatului clientului pentru filtrarea IPsec/IP. Dacă doriți să configurați autoritatea de certificare, mergeți la **CA Certificate**.

1. Accesați Web Config și selectați **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importați certificatul în **Client Certificate**.

   Dacă ați importat deja un certificat publicat de către o autoritate de certificare în IEEE802.1X sau SSL/TLS, veți putea copia certificatul respectiv și îl veți putea utiliza pentru filtrarea IPsec/IP. Pentru copiere, selectați certificatul din **Copy From**, după care faceți clic pe **Copy**.



Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Obținerea și importul unui certificat CA-semnat” la pagina 64

Utilizarea protocolului SNMPv3

Despre SNMPv3

SNMP este un protocol care efectuează monitorizarea și controlează colectarea informațiilor privind dispozitivele conectate la rețea. SNMPv3 este o versiune îmbunătățită a funcției de securitate management.

La utilizarea SNMPv3, monitorizarea stării și modificările setărilor comunicării SNMP (pachet) pot fi autentificate și criptate pentru a proteja comunicarea SNMP (pachet) împotriva riscurilor din rețea, precum monitorizarea conversațiilor de către o terță parte, arogarea unor identități false și manipularea frauduloasă.

Configurarea SNMPv3

Dacă scanerul acceptă protocol SNMPv3, puteți monitoriza și controla accesele la scaner.

1. Accesați Web Config și selectați **Services** > **Protocol**.
2. Introduceți o valoare pentru fiecare element **SNMPv3 Settings**.
3. Faceți clic pe **Next**.

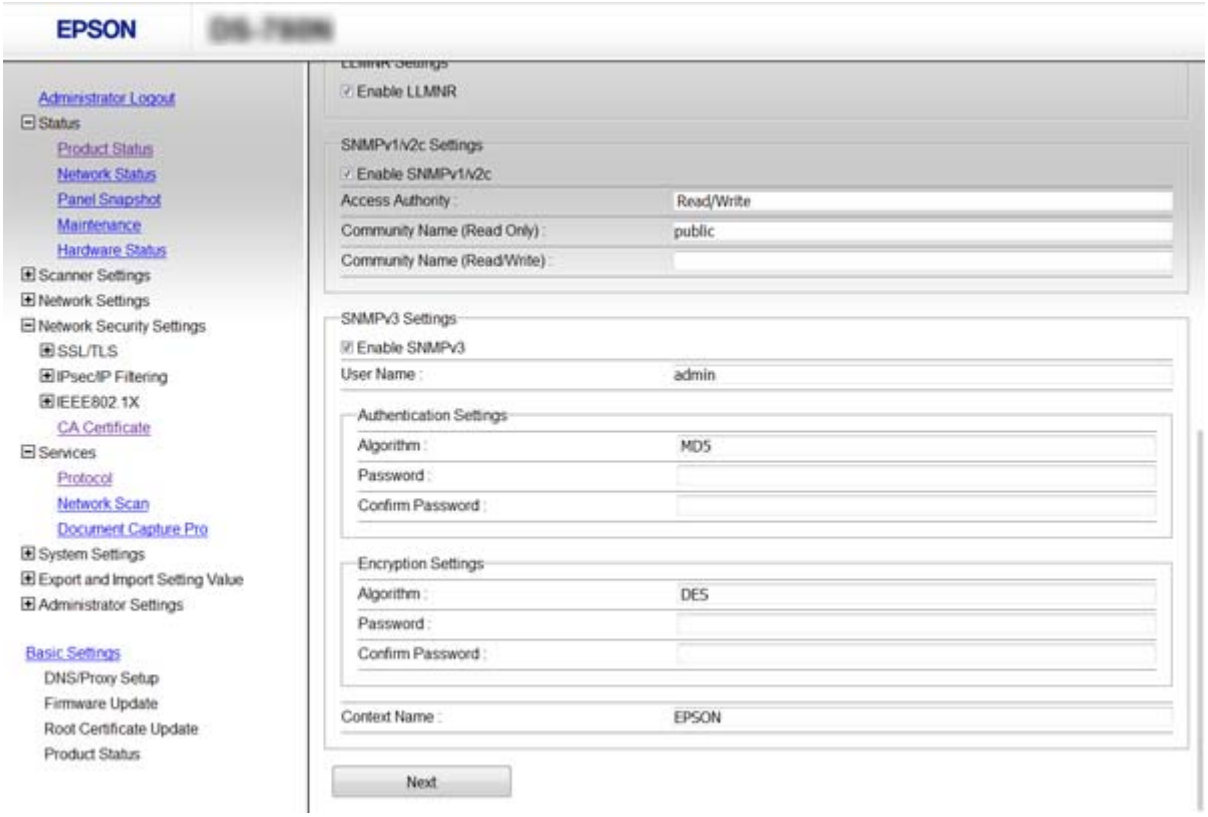
   Un mesaj de confirmare este afișat.
4. Faceți clic pe **OK**.

   Scanerul este actualizat.

Informații conexe

➡ „Accesarea Web Config” la pagina 23
➡ „Elemente de setare pentru SNMPv3” la pagina 83

Elemente de setare pentru SNMPv3



Elemente	Setări şi explicaţii
Enable SNMPv3	SNMPv3 este activat când caseta este bifată.
User Name	Introduceţi între 1 şi 32 de caractere, utilizând caractere de 1 octet.
Authentication Settings	
Algorithm	Selectaţi un algoritm pentru autentificare.
Password	Introduceţi între 8 şi 32 de caractere în ASCII (0x20-0x7E).
Confirm Password	Introduceţi parola configurată pentru confirmare.
Encryption Settings	
Algorithm	Selectaţi un algoritm pentru criptare.
Password	Introduceţi între 8 şi 32 de caractere în ASCII (0x20-0x7E).
Confirm Password	Introduceţi parola configurată pentru confirmare.
Context Name	Introduceţi între 1 şi 32 de caractere, utilizând caractere de 1 octet.

Informaţii conexe

➡ „Configurarea SNMPv3” la pagina 83

Conectarea scanerului la o reţea IEEE802.1X

Configurarea unei reţele IEEE802.1X

Dacă scanerul este compatibil cu IEEE802.1X, puteţi folosi scanerul pe o reţea cu autentificare care este conectată la un server RADIUS şi un distribuitor ca aplicaţie de autentificare.

1. Accesaţi Web Config şi selectaţi **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Introduceţi o valoare pentru fiecare element.
3. Faceţi clic pe **Next**.

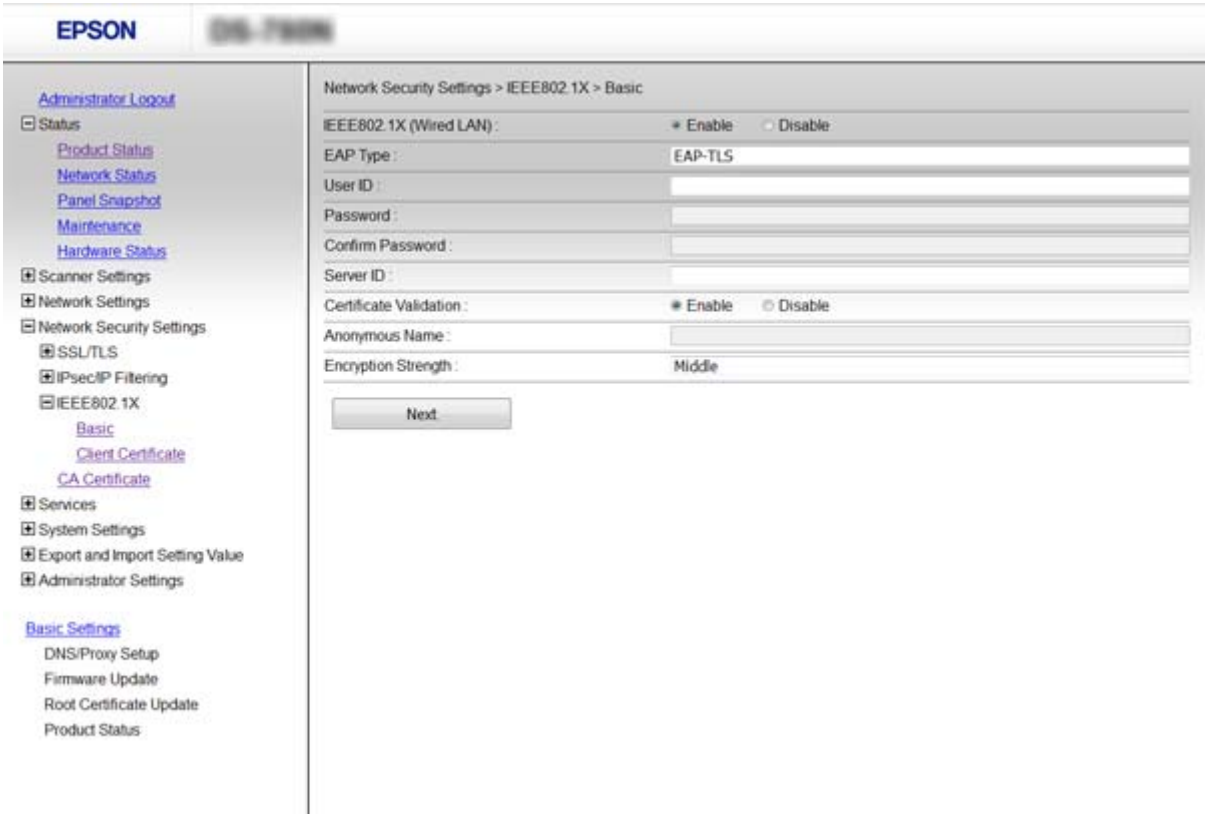
   Un mesaj de confirmare este afişat.
4. Faceţi clic pe **OK**.

   Scanerul este actualizat.

Informaţii conexe

➡ „Accesarea Web Config” la pagina 23
➡ „Elemente de setare reţea IEEE802.1X” la pagina 85
➡ „Imposibil de accesat imprimanta sau scanerul după configurarea IEEE802.1X” la pagina 89

Elemente de setare rețea IEEE802.1X



Elemente	Setări și explicații	
IEEE802.1X (Wired LAN)	Puteți activa sau dezactiva setările paginii (**IEEE802.1X** > **Basic**) pentru IEEE802.1X (LAN prin cablu).	
EAP Type	Selectați o opțiune pentru o metodă de autentificare între scaner și un server RADIUS.	
	EAP-TLS	Trebuie să obțineți și să importați un certificat CA-semnat (certificat semnat de o autoritate de certificare).
	PEAP-TLS	
	PEAP/MSCHAPv2	Trebuie să configurați parola.
User ID	Configurați un ID pentru a-l utiliza pentru autentificarea unui server RADIUS. Introduceți între 1 și 128 de caractere ASCII (între 0x20 și 0x7E) a câte un octet.	
Password	Configurați o parolă pentru a autentifica scanerul. Introduceți între 1 și 128 de caractere ASCII (între 0x20 și 0x7E) a câte un octet. Dacă utilizați un server Windows drept server RADIUS, veți putea introduce până la 127 de caractere.	
Confirm Password	Pentru confirmare, introduceți parola configurată.	
Server ID	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 (între 0x20 și 0x7E) a câte un octet.	
Certificate Validation	Puteți configura validarea certificatelor indiferent de metoda de autentificare. Importați certificatul în **CA Certificate**.	

Elemente	Setări și explicații	
Anonymous Name	Dacă selectați **PEAP-TLS** sau **PEAP/MSCHAPv2** pentru **Authentication Method**, 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 (între 0x20 și 0x7E) a câte un octet.	
Encryption Strength	Puteți selecta una dintre următoarele opțiuni.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Informații conexe

➡ „Configurarea unei rețele IEEE802.1X” la pagina 84

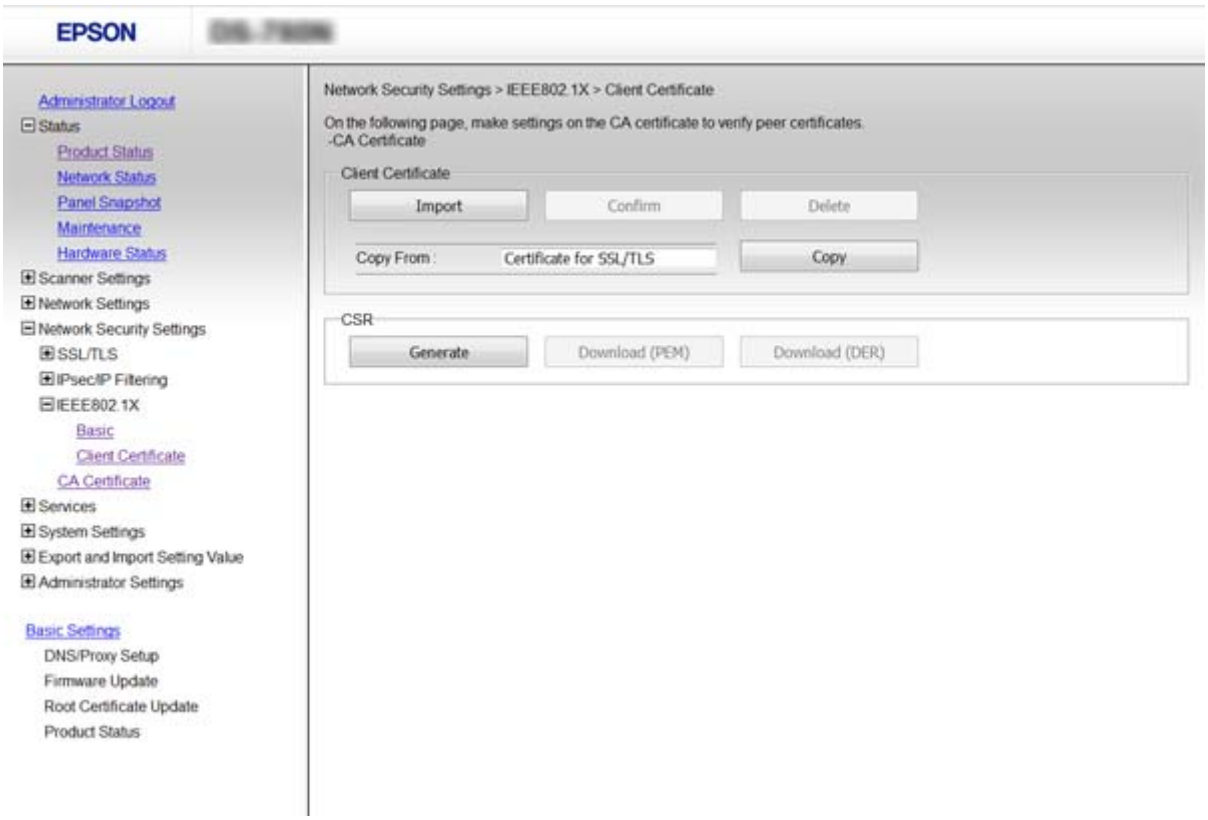
Configurarea certificatului pentru IEEE802.1X

Configurați certificatul clientului pentru IEEE802.1X. Dacă doriți să configurați certificatul autorității de certificare, mergeți la **CA Certificate**.

1. Accesați Web Config și selectați **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. Introduceți un certificat în **Client Certificate**.

   Veți putea copia certificatul, dacă acesta este publicat de către o autoritate de certificare. Pentru copiere, selectați certificatul din **Copy From**, după care faceți clic pe **Copy**.



Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Obținerea și importul unui certificat CA-semnat” la pagina 64

Rezolvarea problemelor pentru securitate avansată

Restabilirea funcțiilor de securitate

Când stabiliți un mediu extrem de securizat, precum filtrarea IPsec/IP sau IEEE802.1X, este posibil să nu puteți efectua comunicarea 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 panoul de control

Puteți dezactiva filtrarea IPsec/IP sau IEEE802.1X de la panoul de control al scanerului.

1. Atingeți **Setări** > **Setări rețea**.
2. Atingeți **Modificați setările**.
3. Atingeți elementele pe care doriți să le dezactivați.
   - ❏ **IPsec/IP Filtering**
   - ❏ **IEEE802.1X**
4. Când este afișat un mesaj de finalizare, atingeți **Continuare**.

Restabilirea funcției de securitate utilizând Web Config

Pentru IEEE802.1X, este posibil ca dispozitivele să nu fie recunoscute în rețea. În acest caz, dezactivați funcția de la panoul de control al scanerului.

Pentru Filtrare IPsec/IP Filtering, puteți dezactiva funcția dacă accesați dispozitivul de la computer.

Dezactivarea filtrării IPsec/IP utilizând Web Config

1. Accesați Web Config și selectați **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Selectați **Disable** pentru **IPsec/IP Filtering** în **Default Policy**.
3. Executați clic pe **Next** și apoi debifați **Enable this Group Policy** pentru toate politicile de grup.
4. Faceți clic pe **OK**.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Probleme privind utilizarea caracteristicilor de securitate a rețelei

Uitarea unei chei pre-partajate

Configurați din nou cheia folosind Web Config.

Pentru a schimba cheia, accesați Web Config și selectați **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** sau **Group Policy**.

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

Informații conexe

➡ „Accesarea Web Config” la pagina 23

Comunicare imposibilă cu Comunicare IPsec

Folosiți un algoritm incompatibil pentru setările computerului?

Scanerul este compatibil cu următorii algoritmi.

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	Grup DH 1, Grup DH 2, Grup DH 5, Grup DH 14, Grup DH 15, Grup DH 16, Grup DH 17, Grup DH 18, Grup DH 19, Grup DH 20, Grup DH 21, Grup DH 22, Grup DH 23, Grup DH 24, Grup DH 25, Grup DH 26, Grup DH 27*, Grup DH 28*, Grup DH 29*, Grup DH 30*
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 71

Întrerupere bruscă a comunicării

Adresa IP a scanerului este nevalidă sau a fost modificată?

Dezactivați IPsec folosind panoul de control al scanerului.

Dacă DHCP nu mai este valid, ați efectuat repornirea sau adresa IPv6 nu mai este validă sau nu a fost obținută, adresa IP înregistrată pentru Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) a scanerului nu va fi găsită.

Folosiți o adresă IP statică.

Adresa IP a computerului este invalidă sau a fost modificată?

Dezactivați IPsec folosind panoul de control al scanerului.

Dacă DHCP nu mai este valid, ați efectuat repornirea sau adresa IPv6 nu mai este validă sau nu a fost obținută, adresa IP înregistrată pentru Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) a scanerului nu va fi găsită.

Folosiți o adresă IP statică.

Informații conexe

➡ „Accesarea Web Config” la pagina 23

➡ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 71

Nu se poate realiza conectarea după configurarea filtrării IPsec/IP

Valoarea setată ar putea fi incorectă.

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

Informații conexe

➡ „Comunicare criptată utilizând filtrarea IPsec/IP” la pagina 71

Imposibil de accesat imprimanta sau scanerul după configurarea IEEE802.1X

Setările pot fi incorecte.

Dezactivați IEEE802.1X de la panoul de control al scanerului. Conectați scanerul și un computer și apoi configurați din nou IEEE802.1X.

Informații conexe

➡ „Configurarea unei rețele IEEE802.1X” la pagina 84

Probleme privind utilizarea unui certificat digital

Certificatul CA-semnat nu poate fi importat

Certificatul CA-semnat şi informațiile din CSR corespund?

Dacă informațiile certificatului CA-semnat și ale CSR nu corespund, CSR nu poate fi importată. Verificați următoarele:

❏ Încercați să importați certificatul spre un dispozitiv care nu are aceleași informații?
Verificați informațiile CSR şi apoi importați certificatul spre un dispozitiv care are aceleaşi informații.

❏ Ați suprascris CSR salvată în scaner după trimiterea CSR către o autoritate de certificare?
Obțineți din nou certificatul CA-semnat cu CSR.

Certificatul CA-semnat are peste 5 KB?

Nu puteți importa un certificat CA-semnat care depăşeşte 5 KB.

Parola pentru importul certificatului este corectă?

Dacă ați uitat parola, nu puteți importa certificatul.

Informații conexe

➡ „Import al unui certificat CA-semnat” la pagina 66

Actualizare imposibilă a unui certificat autosemnat

A fost introdus Common Name?

Common Name trebuie introdus.

În Common Name au fost introduse caractere incompatibile? De exemplu, japoneza este incompatibilă.

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

În Common Name este inclus(ă) un spațiu sau o virgulă?

Dacă este inclusă o virgulă, **Common Name** 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 68

Nu poate fi creată o CSR

A fost introdus Common Name?

Trebuie introdus **Common Name**.

S-au introdus caractere nepermise în Common Name, Organization, Organizational Unit, Locality, State/Province? De exemplu, japoneza este incompatibilă.

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

În Common Name este inclus(ă) un spațiu sau o virgulă?

Dacă este inclusă o virgulă, **Common Name** 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 64

Apare o avertizare privind un certificat digital

Mesaje	Cauză/Cum să procedați
Enter a Server Certificate.	**Cauză:** Nu ați selectat un fișier pentru a fi importat. **Cum să procedați:** Selectați un fișier și faceți clic pe **Import**.
CA Certificate 1 is not entered.	**Cauză:** Certificatul CA 1 nu este introdus și este introdus numai certificatul CA 2. **Cum să procedați:** Importați mai întâi certificatul CA 1.
Invalid value below.	**Cauză:** Caractere incompatibile sunt incluse în calea fișierului și/sau parolă. **Cum să procedați:** Asigurați-vă că respectivele caractere sunt introduse corect pentru element.
Invalid date and time.	**Cauză:** Data și ora scanerului nu au fost setate. **Cum să procedați:** Setați data și ora folosind Web Config sau EpsonNet Config.
Invalid password.	**Cauză:** Parola setată pentru certificatul CA și parola introdusă nu corespund. **Cum să procedați:** Introduceți parola corectă.

Setări de securitate avansate la nivel de întreprindere

Mesaje	Cauză/Cum să procedați
Invalid file.	**Cauză:** Se pare că nu importați un fișier de certificat în format X509. **Cum să procedați:** Asigurați-vă că selectați certificatul corect trimis de o autoritate de certificare de încredere.
	Cauză: Dimensiunea fișierului pe care l-ați importat este prea mare. Dimensiunea maximă permisă pentru fișier este de 5 KB. **Cum să procedați:** Dacă selectați fișierul corect, certificatul ar putea fi deteriorat sau falsificat.
	Cauză: Lanțul inclus în certificat este invalid. **Cum să procedați:** Pentru mai multe informații privind certificatul, consultați site-ul autorității de certificare.
Cannot use the Server Certificates that include more than three CA certificates.	**Cauză:** Fișierul certificatului în format PKCS#12 include mai mult de 3 certificate CA. **Cum să procedați:** Importați fiecare certificat transformat din format PKCS#12 în format PEM sau importați fișierul certificatului în format PKCS#12 care include maximum 2 certificate CA.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Cauză:** Certificatul nu este actualizat. **Cum să procedați:** ❏ Dacă certificatul nu este actualizat, obțineți și importați noul certificat. ❏ Dacă certificatul este actualizat, asigurați-vă că data și ora scanerului sunt setate corect.
Private key is required.	**Cauză:** Nicio cheie privată nu se potrivește cu certificatul. **Cum să procedați:** ❏ Dacă certificatul este în format PEM/DER și este obținut de la o CSR folosind un computer, indicați fișierul pentru cheia privată. ❏ Dacă certificatul este în format PKCS#12 și este obținut de la o CSR folosind un computer, creați un fișier care include cheia privată.
	Cauză: Ați importat din nou certificatul PEM/DER obținut de la o CSR folosind Web Config. **Cum să procedați:** Dacă certificatul este în format PEM/DER și este obținut de la o CSR folosind Web Config, îl puteți importa o singură dată.

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

Informații conexe

➡ „Despre certificarea digitală” la pagina 63

Ştergerea din greşeală a unui certificat CA-semnat

Există un fişier copie de rezervă pentru certificat?

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

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

Informații conexe

➡ „Ştergerea unui certificat CA-semnat” la pagina 67

➡ „Import al unui certificat CA-semnat” la pagina 66