

# Ghidul utilizatorului de rețea



# Cuprins

<b>1</b>	<b>Introducere</b>	<b>1</b>
	Caracteristicile rețelei .....	1
	Alte caracteristici .....	2
<b>2</b>	<b>Modificarea setărilor de rețea</b>	<b>3</b>
	Modificarea setărilor de rețea ale aparatului.....	3
	Utilizarea panoului de control al aparatului (ADS-2800W/ADS-3600W) .....	3
	Verificarea stării rețelei (ADS-2800W/ADS-3600W).....	3
	Utilizarea BRAdmin Light (Windows®) .....	3
	Alte programe utilitare de administrare.....	6
	Administrare bazată pe web .....	6
	BRAdmin Professional 3 (Windows®) .....	6
<b>3</b>	<b>Configurarea aparatului pentru utilizarea într-o rețea wireless (ADS-2800W/ADS-3600W)</b>	<b>8</b>
	Prezentare generală .....	8
	Confirmarea mediului de rețea .....	9
	Conectat la un calculator printr-un punct de acces/router WLAN din rețea (Mod Infrastructură).....	9
	Conectat la un calculator cu posibilitate de conectare wireless, fără punct de acces/router WLAN în rețea (Mod Ad-hoc) .....	10
	Configurare .....	11
	Când SSID nu transmite.....	11
	Utilizarea WPS (Wi-Fi Protected Setup™) .....	18
	Utilizarea metodei PIN a Wi-Fi Protected Setup™ (WPS) .....	19
	Configurarea în modul Ad-hoc.....	22
	Utilizarea unui identificator SSID configurat .....	22
	Configurarea aparatului pentru o rețea wireless utilizând expertul de configurare din panoul de control al aparatului .....	29
	Utilizarea Wi-Fi Direct® .....	31
	Scanarea de pe dispozitivul mobil utilizând Wi-Fi Direct® .....	31
	Configurarea rețelei Wi-Fi Direct® .....	32
	Prezentare generală a configurării rețelei Wi-Fi Direct® .....	32
	Configurarea rețelei Wi-Fi Direct® utilizând metoda printr-o singură apăsare .....	33
	Configurarea rețelei Wi-Fi Direct® utilizând metoda printr-o singură apăsare a Wi-Fi Protected Setup™ (WPS) .....	34
	Configurarea rețelei Wi-Fi Direct® utilizând metoda PIN.....	34
	Configurarea rețelei Wi-Fi Direct® utilizând metoda PIN a Wi-Fi Protected Setup™ (WPS) .....	35
	Configurarea manuală a rețelei Wi-Fi Direct® .....	37
<b>4</b>	<b>Administrare bazată pe web</b>	<b>38</b>
	Prezentare generală .....	38
	Configurarea setărilor aparatului .....	39
	Configurarea unei parole de conectare .....	40

Utilizarea autentificării prin LDAP .....	41
Introducere în Autentificarea prin LDAP .....	41
Configurarea Autentificării prin LDAP utilizând Administrarea bazată pe web .....	41
Conectare pentru modificarea setărilor aparatului, utilizând panoul de control al aparatului .....	42
Restricționarea utilizatorilor .....	43
Configurarea autentificării Active Directory prin LDAP (ADS-2800W/ADS-3600W).....	43
Utilizarea LDAP (ADS-2800W/ADS-3600W).....	44
Modificarea configurării LDAP .....	44
Modificarea configurării LDAP cu ajutorul panoului de control al aparatului (ADS-2800W/ADS-3600W) .....	45
Sincronizarea cu serverul SNTTP.....	47
Modificarea configurării funcției Scanare către FTP .....	49
Modificarea configurării funcției Scanare către SFTP.....	50
Modificarea configurării funcției Scanare către rețea (Windows®).....	52
Modificarea configurării funcției Scanare către SharePoint (Windows®) .....	54
Configurarea setărilor avansate TCP/IP .....	56
Import/export agendă de adrese (ADS-2800W/ADS-3600W) .....	58
Importarea agendei de adrese .....	58
Exportarea agendei de adrese .....	58

## **5 Scanare către un server de e-mail (ADS-2800W/ADS-3600W) 59**

Prezentare generală .....	59
Restricții de dimensiune la utilizarea Scanării către un server de e-mail .....	59
Configurarea setărilor de Scanare către un server de e-mail .....	60
Înainte de a scana către un server de e-mail .....	60
Scanarea către un server de e-mail .....	61
Funcții suplimentare de scanare către server de e-mail .....	62
E-mail verificare transmitere (TX).....	62

## **6 Caracteristici de securitate 63**

Prezentare generală .....	63
Trimiterea securizată a unui e-mail (ADS-2800W/ADS-3600W) .....	64
Configurarea cu ajutorul administrării bazate pe web .....	64
Trimiterea unui e-mail folosind autentificarea utilizatorului .....	64
Trimiterea securizată a unui e-mail folosind SSL/TLS.....	65
Setări de securitate pentru SFTP .....	66
Crearea unei Asocieri de chei client.....	66
Exportarea unei Asocieri de chei client .....	67
Importarea unei Chei publice a serverului .....	68
Gestionare certificate multiple .....	69
Importarea unui certificat CA .....	69
Administrarea în siguranță a aparatului de rețea, utilizând IPsec.....	71
Introducere în IPsec .....	71
Configurarea IPsec utilizând administrarea bazată pe web .....	72
Configurarea unui Șablon de adresă IPsec utilizând administrarea bazată pe web .....	73
Configurarea unui șablon IPsec utilizând administrarea bazată pe web .....	74
Setările IKEv1 pentru un șablon IPsec .....	75
Setările IKEv2 pentru un șablon IPsec .....	77
Setările manuale pentru un șablon IPsec.....	80

Restricționarea funcțiilor de scanare de la dispozitive externe .....	83
Restricționarea funcțiilor de scanare de la dispozitive externe utilizând setările unui browser web .....	83
Blocarea securizată a funcțiilor 3.0 (ADS-2800W/ADS-3600W) .....	84
Înainte de a începe să utilizați Blocarea securizată a funcțiilor 3.0 .....	84
Pornirea/oprirea Blocarea securizată a funcțiilor .....	85
Configurarea Blocarea securizată a funcțiilor 3.0 utilizând administrarea bazată pe web .....	85
Actualizare firmware .....	86
<b>7 Depanarea</b> .....	<b>87</b>
Prezentare generală .....	87
Identificarea problemei .....	87
<b>8 Setări suplimentare de rețea (Windows®)</b> .....	<b>97</b>
Tipuri de setări .....	97
Instalarea driverelor utilizate pentru scanarea via Servicii web (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows® 10) .....	97
Instalarea scanării în rețea pentru modul Infrastructură în cazul în care utilizați funcția Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10) .....	99
<b>A Anexă</b> .....	<b>100</b>
Protocoale și funcții de securitate compatibile .....	100
Tabel funcții administrare bazată pe web .....	101
<b>B Index</b> .....	<b>114</b>

## Caracteristicile rețelei

Aparatul Brother poate fi partajat într-o rețea Ethernet wireless, IEEE 802.11b/g/n, utilizând serverul intern de scanare al rețelei. Serverul de scanare acceptă diverse funcții și metode de conectare, în funcție de sistemul de operare și de configurația rețelei. În tabelul următor sunt prezentate caracteristicile de rețea și conexiunile suportate de fiecare sistem de operare:

Sisteme de operare	Windows® XP 32 biți (SP3) Windows Vista® Windows® 7 Windows® 8 Windows® 8.1 Windows® 10 Windows Server® 2003 R2 32 biți (SP2) Windows Server® 2008 Windows Server® 2008 R2 Windows Server® 2012 Windows Server® 2012 R2 OS al serverului suportă doar scanarea	OS X v10.8.5, 10.9.x, 10.10.x, 10.11.x
<b>Scanare</b> Consultați <i>Manualul de utilizare</i> .	✓	✓
<b>BRAdmin Light</b> <sup>1</sup> Consultați <i>Utilizarea BRAdmin Light (Windows®)</i> la pagina 3.	✓	
<b>BRAdmin Professional 3</b> <sup>2</sup> Consultați <i>BRAdmin Professional 3 (Windows®)</i> la pagina 6.	✓	
<b>Management bazat pe web (browser web)</b> Consultați <i>Administrare bazată pe web</i> la pagina 38.	✓	✓
<b>Configurarea de la distanță</b> Consultați <i>Manualul de utilizare</i> .	✓	✓
<b>Status Monitor</b> Consultați <i>Manualul de utilizare</i> .	✓	
<b>Vertical Pairing (Asociere verticală)</b> Consultați <i>Instalarea scanării în rețea pentru modul Infrastructură în cazul în care utilizați funcția Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)</i> la pagina 99.	✓	

<sup>1</sup> BRAdmin Light este disponibil pentru descărcare la adresa web: [support.brother.com](http://support.brother.com)

<sup>2</sup> BRAdmin Professional 3 este disponibil pentru descărcare la adresa web: [support.brother.com](http://support.brother.com)

## Alte caracteristici

---

### LDAP (ADS-2800W/ADS-3600W)

Protocolul LDAP permite căutarea de pe calculator a unor informații precum adresele de e-mail. Dacă utilizați funcția Scanare către un server de e-mail, puteți utiliza căutarea LDAP pentru a găsi adresele de e-mail. (Consultați *Modificarea configurării LDAP cu ajutorul panoului de control al aparatului (ADS-2800W/ADS-3600W)* la pagina 45.)

### Scanare către un server de e-mail (ADS-2800W/ADS-3600W)

Funcția Scanare către un server de e-mail permite trimiterea documentelor scanate folosind internetul. (Consultați *Scanare către un server de e-mail (ADS-2800W/ADS-3600W)* la pagina 59.)

Înainte de a utiliza această funcție, trebuie să configurați setările necesare ale aparatului folosind panoul de control al aparatului, BRAdmin Professional 3 sau administrarea bazată pe web.

### Securitate

Aparatul dumneavoastră Brother folosește unele dintre cele mai recente protocoale disponibile de securitate și de criptare a rețelelor. (Consultați *Caracteristici de securitate* la pagina 63.)

### Wi-Fi Direct® (ADS-2800W/ADS-3600W)

Wi-Fi Direct® este una dintre metodele de configurare wireless dezvoltate de Wi-Fi Alliance®. Acest tip de conexiune este un tip standard Wi-Fi, care permite dispozitivelor să se inter-conecteze fără un punct de acces wireless, utilizând o metodă securizată. (Consultați *Utilizarea Wi-Fi Direct®* la pagina 31.)

## Modificarea setărilor de rețea ale aparatului

Setările de rețea ale aparatului pot fi modificate utilizând panoul de control, BRAdmin Light, administrarea bazată pe web sau BRAdmin Professional 3.


### Utilizarea panoului de control al aparatului (ADS-2800W/ADS-3600W)

---

Puteți configura aparatul pentru o rețea utilizând meniul Rețea din panoul de control.

### Verificarea stării rețelei (ADS-2800W/ADS-3600W)

---

- 1 Pe ecranul LCD al aparatului, apăsați .
- 2 Apăsați Rețea.
- 3 Apăsați Conexiune LAN.
- 4 Apăsați Stare conex. cablu.
- 5 Apăsați Status.

### Utilizarea BRAdmin Light (Windows®)

---

Utilitarul BRAdmin Light este conceput pentru configurarea inițială a dispozitivelor Brother conectate la rețea. Acesta poate, de asemenea, căuta produsele Brother într-un mediu TCP/IP, poate vizualiza starea și configura setările de bază ale rețelei, cum ar fi adresa IP.



#### Instalarea BRAdmin Light

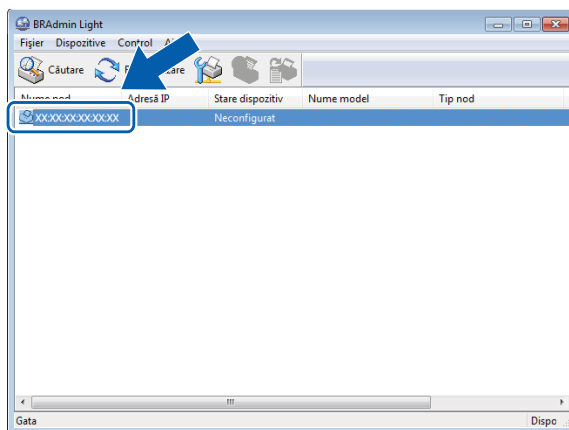
- 1 Asigurați-vă că aparatul este PORNIT.
- 2 Porniți computerul. Închideți eventualele aplicații deschise.
- 3 Introduceți discul DVD-ROM cu programul de instalare în unitatea DVD-ROM.
- 4 Faceți dublu clic pe **(Unitate DVD):\Instrumente\BRAdminLight\xxx\disc1\setup.exe**.

## Configurarea adresei IP, a măștii de subrețea și a gateway-ului utilizând BRAdmin Light

### NOTĂ

- Accesați pagina **Descărcări** pentru modelul dvs., din Brother Solutions Center la adresa [support.brother.com](http://support.brother.com) pentru a descărca cea mai recentă versiune a BRAdmin Light al Brother.
- Dacă aveți nevoie de un sistem de gestionare mai avansat al aparatului, utilizați cea mai recentă versiune a BRAdmin Professional 3. Accesați pagina **Descărcări** pentru modelul dvs., din Brother Solutions Center la adresa [support.brother.com](http://support.brother.com) pentru a descărca BRAdmin Professional 3. Acest utilitar este disponibil numai pentru utilizatorii Windows®.
- Dacă folosiți o funcție firewall a unei aplicații anti-spyware sau antivirus, dezactivați temporar aplicația. După ce ați verificat că puteți scana, reactivați aplicația.
- Nume nod: numele nodului este afișat în fereastra BRAdmin Light curentă. Numele implicit de nod al serverului de scanare „BRWxxxxxxxxxxx” pentru rețeaua wireless (unde „xxxxxxxxxxx” este adresa MAC/Ethernet a aparatului).
- În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apăsați pe **OK**.

- 1 Lansați BRAdmin Light.
  - Windows® XP, Windows Vista® și Windows® 7  
Faceți clic pe  (**Start**) > **Toate programele** > **Brother** > **BRAdmin Light** > **BRAdmin Light**.
  - Windows® 8, Windows® 8.1 și Windows® 10  
Faceți clic pe  (**BRAdmin Light**) din tava de sarcini.
- 2 BRAdmin Light caută automat dispozitivele noi.
- 3 Faceți dublu clic pe aparatul Brother.





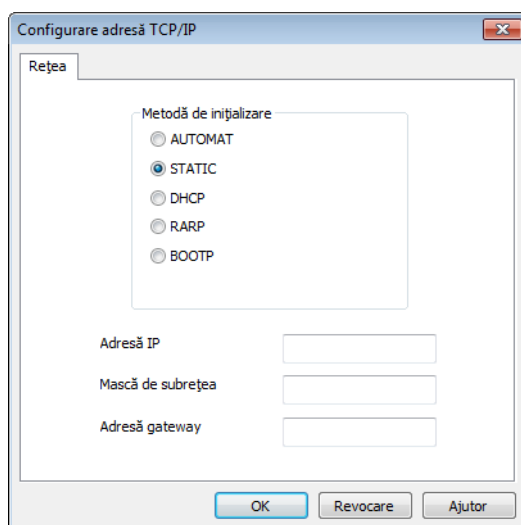
## NOTĂ

- Dacă serverul de scanare este setat pentru a folosi setările din fabricație (și nu utilizați un server DHCP/BOOTP/RARP), dispozitivul va fi afișat ca **Neconfigurat** în fereastra utilitarului BRAdmin Light.
- Puteți afișa adresa MAC (adresa Ethernet) și numele de nod ale aparatului dvs. folosind ecranul LCD al aparatului (ADS-2800W/ADS-3600W).

Pentru a găsi adresa MAC, apăsați  > Rețea > WLAN > Adresă MAC.

Pentru a găsi numele nodului, apăsați  > Rețea > WLAN > TCP/IP > Nume Nod.

- 4 Selectați **STATIC** din lista **Metodă de inițializare**. Introduceți **Adresă IP**, **Mască de subrețea** și **Adresă gateway** (dacă este necesar) pentru aparat.



- 5 Faceți clic pe **OK**.
- 6 Aparatul Brother apare în lista de dispozitive. Dacă acest lucru nu se întâmplă, verificați adresa IP la pasul 4.

## Alte programe utilitare de administrare

### Administrare bazată pe web

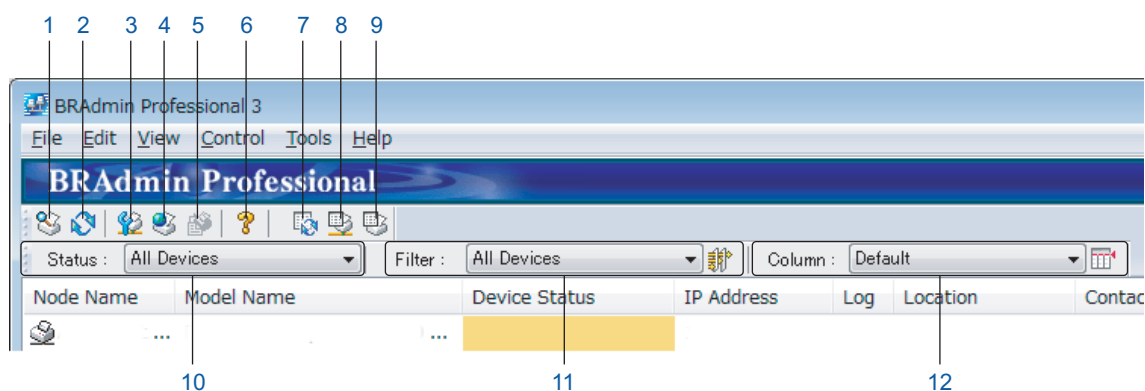
Puteți utiliza un browser web pentru a modifica setările serverului de scanare folosind HTTP (Protocol de transfer hipertext) sau HTTPS (Protocol de transfer hipertext prin protocol de codificare). (Consultați *Configurarea setărilor aparatului* la pagina 39.)

### BRAdmin Professional 3 (Windows®)

BRAdmin Professional 3 este un utilitar pentru administrarea avansată a dispozitivelor Brother conectate în rețea. Acest utilitar poate căuta produse Brother în rețea și le poate afișa într-o fereastră ușor de citit, în stil Explorer. Pictogramele își schimbă culoarea pentru a afișa starea fiecărui dispozitiv. Puteți configura setările rețelei și ale dispozitivului și puteți actualiza firmware-ul dispozitivului de la un computer Windows® din rețeaua dvs. De asemenea, BRAdmin Professional 3 poate înregistra într-un jurnal activitatea dispozitivelor Brother din rețea și poate exporta datele din jurnal în format HTML, CSV, TXT sau SQL.

#### NOTĂ

- Utilizați cea mai recentă versiune a utilitarului BRAdmin Professional 3. Accesați pagina **Descărcări** pentru modelul dvs., din Brother Solutions Center la adresa [support.brother.com](http://support.brother.com) pentru a descărca BRAdmin Professional 3 al Brother. Acest utilitar este disponibil numai pentru utilizatorii Windows®.
- Dacă folosiți o funcție firewall a unei aplicații anti-spyware sau antivirus, dezactivați temporar aplicația. După ce ați verificat că puteți scana, reactivați aplicația.
- Nume nod: Numele nodului pentru fiecare dispozitiv Brother din rețea apare în BRAdmin Professional 3. Numele implicit al nodului este „BRWxxxxxxxxxxx” pentru o rețea wireless (unde „xxxxxxxxxxx” este adresa MAC/Ethernet a aparatului).



#### 1 Căutare în rețea

Caută dispozitivele în rețeaua dvs.

În mod implicit, BRAdmin Professional este configurat pentru a vizualiza toate dispozitivele de rețea compatibile, din rețeaua dvs. locală, care au fost configurate cu o adresă IP valabilă.

#### 2 Obținerea stării dispozitivelor (TOATE)

Reîmprospătează starea dispozitivelor cu care comunică BRAdmin Professional.

### 3 Configurarea dispozitivelor neconfigurate

Dacă dispozitivul dvs. Brother conectat la rețea nu are o adresă IP valabilă, BRAdmin Professional vă permite să setați adresa IP a dispozitivului, masca de subrețea, adresa gateway și metoda boot.

### 4 Pagina de pornire a dispozitivului (Administrare bazată pe web)

Se conectează la serverul web încorporat în aparat (aveți în vedere că nu toate dispozitivele au un server web încorporat).

### 5 Trimitere fișier

Trimite un fișier la un dispozitiv.

### 6 Subiecte ajutor

Prezintă Fișierul ajutor pentru BRAdmin Professional 3.

### 7 Reîmprospătare jurnal

Reîmprospătează istoricul jurnalului.

### 8 Vizualizarea jurnalului dispozitivelor de rețea

Prezintă informațiile din jurnal referitoare la toate dispozitivele rețelei.

### 9 Vizualizarea jurnalului dispozitivelor locale


Prezintă informațiile din jurnal referitoare la toate dispozitivele care sunt conectate la computerele client, înregistrate în Setările jurnalului dispozitivelor locale.

### 10 Status (Stare)

Selectați o stare din lista derulantă.

### 11 Filter (Filtru)

Selectați un filtru din lista derulantă.

Pentru a selecta un filtru din lista derulantă, trebuie să adăugați meniuri, făcând clic pe  în prealabil.

### 12 Column (Coloana)

Opțiunea Setări coloană vă permite să selectați coloanele care se vor afișa pe ecranul principal de vizualizare al BRAdmin Professional.

## NOTĂ

---

Pentru mai multe informații despre BRAdmin Professional 3, faceți clic pe  .

---

# Configurarea aparatului pentru utilizarea într-o rețea wireless (ADS-2800W/ADS-3600W)

## Prezentare generală

Pentru conectarea aparatului la rețeaua wireless, vă recomandăm să parcurgeți una dintre metodele de configurare descrise în secțiunea *Ghid de instalare și configurare rapidă*. Accesați pagina modelului dvs., de pe Brother Solutions Center la adresa [solutions.brother.com/manuals](http://solutions.brother.com/manuals) pentru a descărca *Ghidul de instalare și configurare rapidă*.

Pentru mai multe informații referitoare la metodele și setările suplimentare de configurare wireless, citiți acest capitol. Pentru informații referitoare la setările TCP/IP, consultați *Modificarea setărilor de rețea ale aparatului* la pagina 3.

### NOTĂ

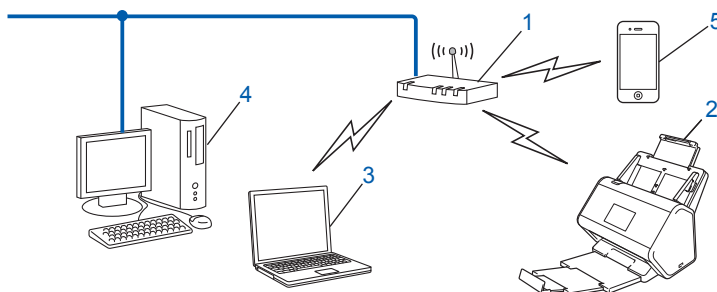
- Pentru a obține rezultate optime la scanarea documentelor zilnice, așezați aparatul Brother cât mai aproape de punctul de acces/routerul WLAN, cu obstacole minime. Obiectele de mari dimensiuni și pereții dintre cele două dispozitive, precum și interferența cu alte dispozitive electronice pot afecta viteza de transfer a datelor din documentele dumneavoastră.

Din cauza acestor factori, conectarea printr-o rețea wireless ar putea să nu fie cea mai bună metodă de conectare pentru toate tipurile de documente și aplicații. Dacă scanați fișiere mari, cum ar fi documentele cu mai multe pagini care conțin atât text, cât și imagini mari, vă recomandăm să utilizați un cablu USB pentru o viteză mai mare de transfer.

- Înainte de a configura setările wireless, trebuie să cunoașteți numele rețelei (SSID) și cheia de rețea.

## Confirmarea mediului de rețea

### Conectat la un calculator printr-un punct de acces/router WLAN din rețea (Mod Infrastructură)



#### 1 Punct de acces/router WLAN <sup>1</sup>

<sup>1</sup> În cazul în care calculatorul dvs. acceptă Intel® My WiFi Technology (MWT), puteți folosi computerul ca punct de acces compatibil cu Wi-Fi Protected Setup™ (WPS).

#### 2 Aparat conectat la rețeaua wireless (aparatură dumneavoastră)

#### 3 Computer cu posibilități de conectare wireless conectat la punctul de acces/routerul WLAN

#### 4 Calculator cablat (fără posibilități de conectare wireless), conectat la punctul de acces/routerul WLAN printr-un cablu de rețea


#### 5 Dispozitiv mobil conectat la punctul de acces/routerul WLAN

### Metodă de configurare

Următoarele sunt metode de configurare a aparatului dvs. Brother într-un mediu de rețea wireless. Alegeți metoda preferată pentru mediul dvs.:

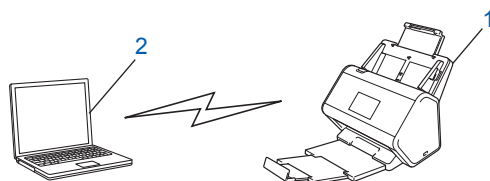
- Configurare wireless, temporar (recomandată). Consultați *Ghidul de instalare și configurare rapidă*.
- Configurare wireless printr-o singură apăsare utilizând WPS (Wi-Fi Protected Setup™). Consultați pagina 18.
- Configurare wireless prin metoda PIN utilizând WPS. Consultați pagina 19.
- Configurarea unei rețele wireless utilizând Setup Wizard (Expertul de configurare). Consultați pagina 29.

### Verificarea stării rețelei WLAN (ADS-2800W/ADS-3600W)

- 1 Pe ecranul LCD al aparatului, apăsați .
- 2 Apăsați Rețea.
- 3 Apăsați WLAN.
- 4 Apăsați ▲ sau ▼, apoi apăsați Status WLAN.
- 5 Apăsați Status.

## Conectat la un calculator cu posibilitate de conectare wireless, fără punct de acces/router WLAN în rețea (Mod Ad-hoc)

Acest tip de rețea nu are un punct central de acces/router WLAN. Fiecare client wireless comunică direct cu celălalt. Dacă face parte din această rețea, aparatul Brother wireless (aparatul dumneavoastră) va primi toate activitățile de scanare direct de la computerul care trimite datele de scanare.



**1 Aparat conectat la rețeaua wireless (aparatul dumneavoastră)**

**2 Computer cu posibilitate de conectare wireless**

Nu garantăm conexiunea la rețeaua wireless în modul Ad-hoc. Pentru a configura aparatul în modul Ad-hoc, consultați *Configurarea în modul Ad-hoc* la pagina 22.

# Configurare

## Când SSID nu transmite

- 1 Înainte de a configura aparatul, vă recomandăm să vă notați setările rețelei wireless. Veți avea nevoie de aceste informații pentru a începe configurarea.  
Verificați și notați setările curente ale rețelei wireless.

3

Numele rețelei (SSID)

Mod de comunicație	Metodă de autentificare	Mod de criptare	Cheie de rețea
Infrastructură	Sistem deschis	NIMIC	—
		WEP	
	Cheie partajată	WEP	
	WPA/WPA2-PSK	AES	
		TKIP <sup>1</sup>	

<sup>1</sup> TKIP este acceptat doar pentru WPA-PSK.

### De exemplu:

Numele rețelei (SSID)
HELLO

Mod de comunicație	Metodă de autentificare	Mod de criptare	Cheie de rețea
Infrastructură	WPA2-PSK	AES	12345678

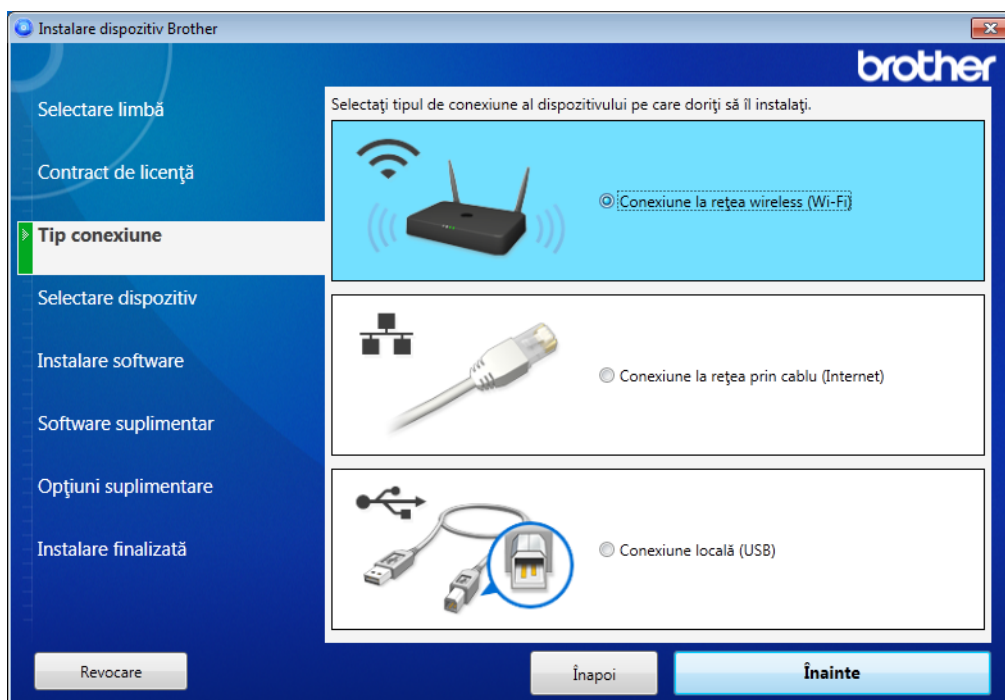
## NOTĂ

Dacă routerul dumneavoastră utilizează criptarea WEP, introduceți cheia utilizată ca prima cheie WEP. Aparatul Brother suportă numai utilizarea primei chei WEP.

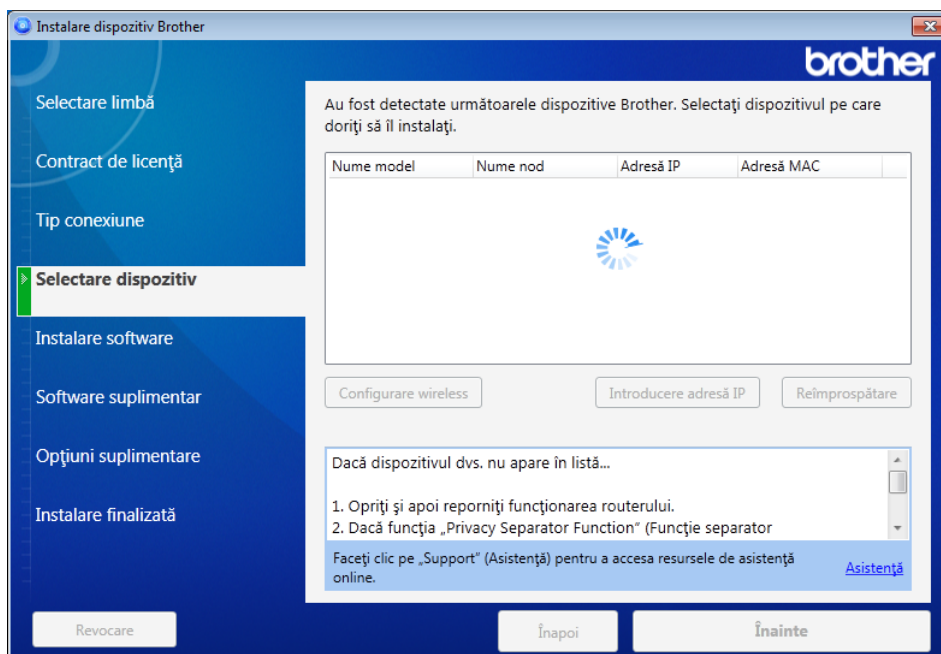
2 Procedați conform uneia dintre metodele de mai jos:

■ Windows®

- a Introduceți DVD-ROM-ul furnizat în unitatea DVD-ROM.
- b Selectați **Conexiune la rețea wireless (Wi-Fi)**, apoi faceți clic pe **Înainte**.



c Faceți clic pe **Configurare wireless**.





■ Macintosh

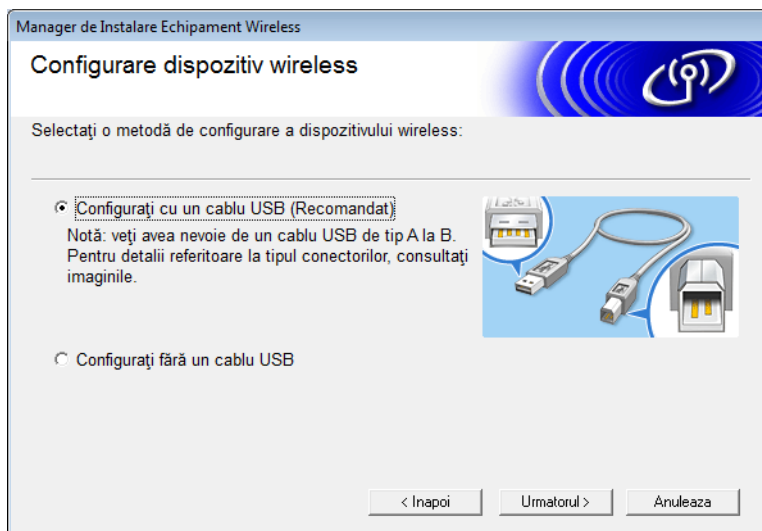
- a Descărcați pachetul complet de drivere și software de la Brother Solutions Center ([support.brother.com](http://support.brother.com)).
- b Faceți dublu clic pe pictograma **BROTHER** de pe desktop.
- c Faceți dublu clic pe **Utilities** (Utilitare).



- d Faceți dublu clic pe **Wireless Device Setup Wizard** (Expert configurare dispozitiv wireless).

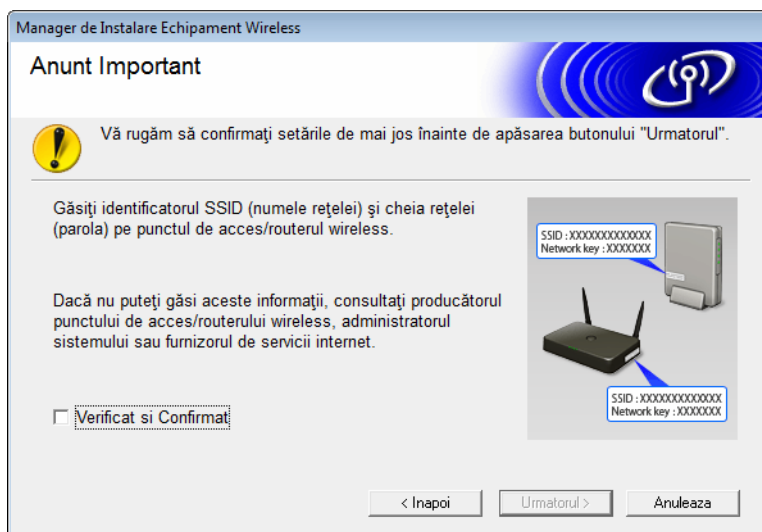


- 3 Selectați **Configurați cu un cablu USB (Recomandat)**, apoi faceți clic pe **Urmatorul**.  
Vă recomandăm să utilizați temporar un cablu USB.



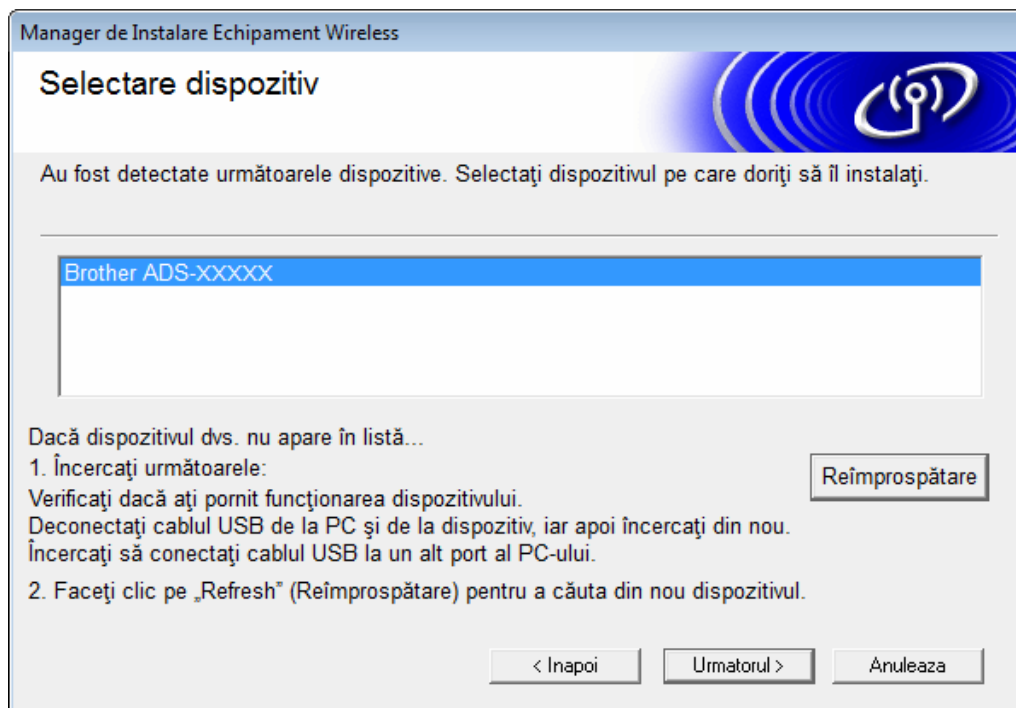
## NOTĂ

Dacă apare acest ecran, citiți **Anunt Important**. Confirmați SSID și cheia de rețea, selectați caseta **Verificat si Confirmat**, apoi faceți clic pe **Urmatorul**.



- 4 Conectați temporar cablul USB direct la calculator și la aparat.  
Dacă apare ecranul de confirmare, faceți clic pe **Urmatorul**.

- 5 Faceți clic pe **Urmatorul** (doar Windows®).

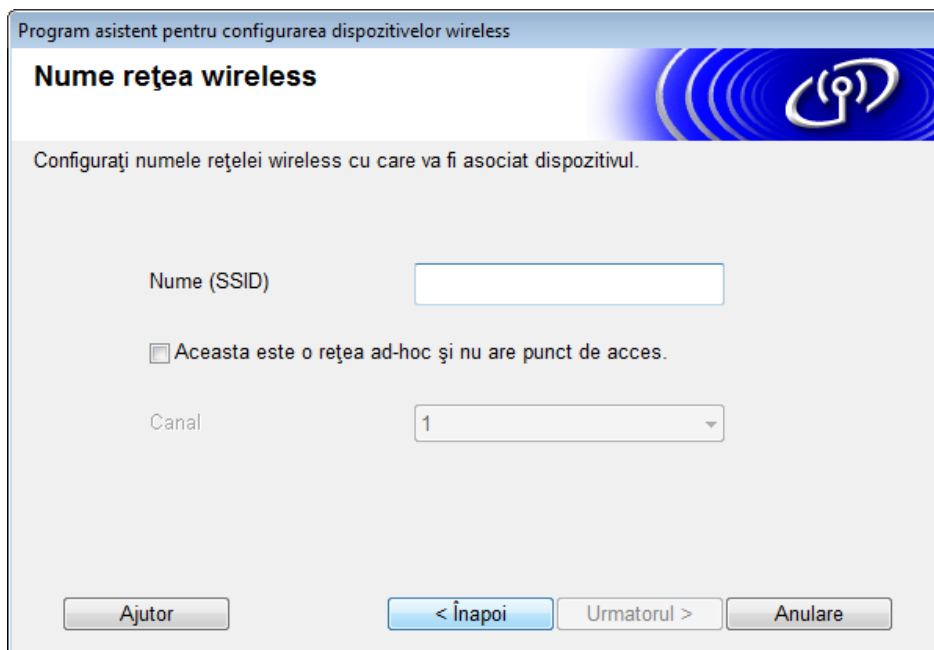


- 6 Procedați conform uneia dintre metodele de mai jos:

- Selectați SSID-ul dorit și faceți clic pe **Urmatorul**. Configurați apoi **Cheie rețea** și navigați la 10.
- Dacă SSID-ul pe care doriți să-l utilizați nu transmite, faceți clic pe **Avansat** și navigați la 7.



- 7 Introduceți un SSID nou în câmpul **Nume (SSID)** și faceți clic pe **Urmatorul**.



Program asistent pentru configurarea dispozitivelor wireless

### Nume rețea wireless

Configurați numele rețelei wireless cu care va fi asociat dispozitivul.

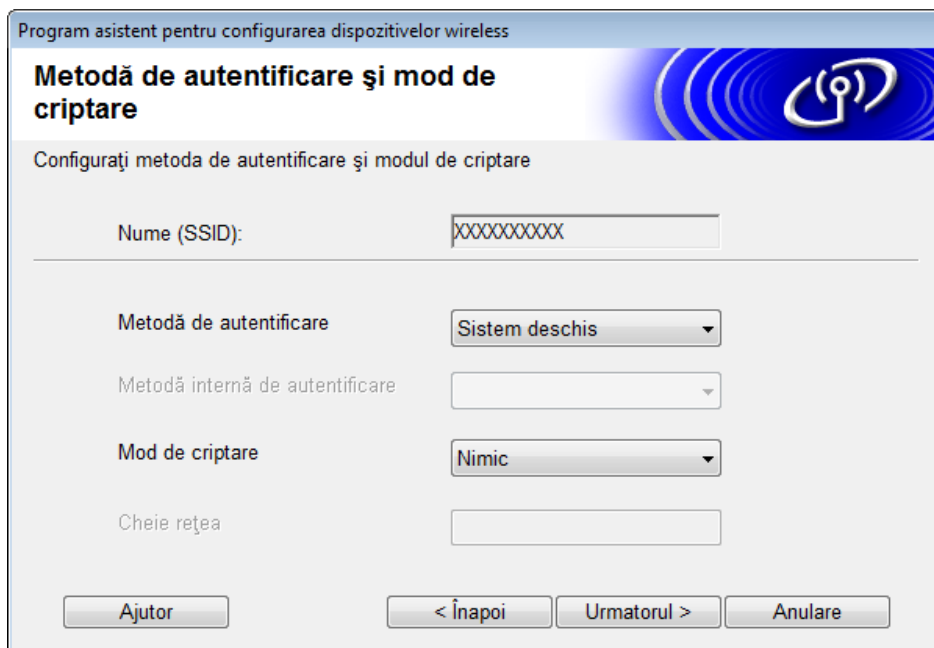
Nume (SSID)

Aceasta este o rețea ad-hoc și nu are punct de acces.

Canal

Ajutor < Înapoi Urmatorul > Anulare

- 8 Selectați **Metodă de autentificare** și **Mod de criptare** din listele derulante, introduceți o cheie de rețea în câmpul **Cheie rețea**, apoi faceți clic pe **Urmatorul** și mergeți la 10.



Program asistent pentru configurarea dispozitivelor wireless

### Metodă de autentificare și mod de criptare

Configurați metoda de autentificare și modul de criptare

Nume (SSID):

Metodă de autentificare

Metodă internă de autentificare

Mod de criptare

Cheie rețea

Ajutor < Înapoi Urmatorul > Anulare

- 9 Introduceți o nouă cheie de rețea în câmpul **Cheie rețea**, apoi faceți clic pe **Urmatorul**.

Program asistent pentru configurarea dispozitivelor wireless

### Configurarea cheii de rețea

Vă rugăm să introduceți cheia de securitate de rețea pe care ați verificat-o anterior.

Unde este cheia mea de rețea?

Cheie rețea

Tipul de autentificare și de criptare al rețelei fără fir va fi detectat automat. Trebuie numai să introduceți cheia rețelei.

Ajutor < Înapoi Urmatorul > Anulare

- 10 Faceți clic pe **Urmatorul**. Aparatul recepționează setările. (Ecranul următor poate fi diferit, în funcție de setările dvs.)

Program asistent pentru configurarea dispozitivelor wireless

### Confirmare setări rețea wireless

Faceți clic pe butonul „Urmatorul” pentru a trimite următoarele setări către dispozitiv

Adresă IP	Automat	Schimbare adresă IP
Mod de comunicare	Infrastructură	
Nume (SSID)	XXXXXXXXXX	
Metodă de autentificare	Sistem deschis	
Mod de criptare	Nimic	

Ajutor < Înapoi Urmatorul > Anulare

## NOTĂ


NU deconectați cablul USB până când instrucțiunile pas cu pas nu confirmă faptul că este finalizată configurarea și că puteți scoate cablul în siguranță.

- 11 Deconectați cablul USB dintre computer și aparat.
- 12 Faceți clic pe **Terminare**.

## Utilizarea WPS (Wi-Fi Protected Setup™)

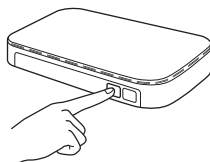
- 1 Confirmați existența simbolului WPS în punctul de acces/routerul wireless, așa cum se indică mai jos.




- 2 Așezați aparatul Brother în aria de acoperire a punctului de acces/routerului. Aria de acoperire poate diferi în funcție de mediul dvs. Consultați instrucțiunile furnizate odată cu punctul de acces/routerul wireless.
- 3 Pe ecranul LCD al aparatului, apăsați  > Rețea > WLAN > WPS.  
Când apare **Activare WLAN?**, apăsați **Da** pentru a accepta.

### NOTĂ

- Dacă nu porniți WPS de pe ecranul LCD al aparatului imediat după apăsarea butonului WPS de pe punctul de acces/routerul wireless, conexiunea poate eșua.
  - Dacă punctul de acces/routerul wireless acceptă WPS și doriți să configurați aparatul cu ajutorul metodei PIN (număr personal de identificare), consultați *Utilizarea metodei PIN a Wi-Fi Protected Setup™ (WPS)* la pagina 19.
- 4 Când ecranul LCD vă solicită să porniți WPS, apăsați butonul WPS de pe punctul de acces/routerul wireless (pentru mai multe informații, consultați instrucțiunile furnizate odată cu routerul/punctul de acces wireless).



Apăsați **OK** de pe ecranul LCD al aparatului Brother.

- 5 Aparatul dvs. detectează automat modul (WPS) utilizat de punctul de acces/routerul wireless și încearcă să se conecteze la rețeaua dvs. wireless.
- 6 Dacă dispozitivul wireless se conectează cu succes, ecranul LCD afișează mesajul **Conectat** până când apăsați **OK**.  
Configurarea wireless este acum finalizată. Indicatorul Wi-Fi  de pe panoul de control se aprinde, indicând că interfața de rețea a aparatului este setată pe WLAN.

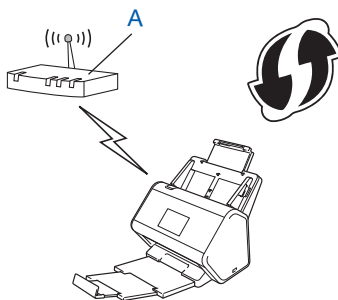
## Utilizarea metodei PIN a Wi-Fi Protected Setup™ (WPS)

Dacă punctul de acces/routerul WLAN acceptă WPS (Metoda PIN), configurați aparatul utilizând instrucțiunile.

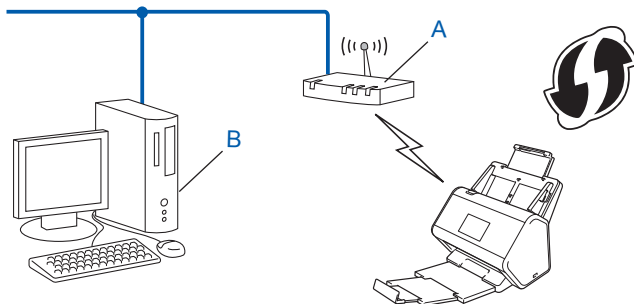
### NOTĂ

Metoda PIN (Personal Identification Number - număr personal de identificare) este una dintre metodele de conectare dezvoltate de Wi-Fi Alliance®. Prin introducerea unui cod PIN creat de către un *Aparat înregistrat* (aparatul dumneavoastră) la *Registrator* (un dispozitiv care administrează rețeaua LAN wireless), puteți configura setările rețelei WLAN și setările de securitate. Consultați *Manualul de utilizare* al punctului de acces/routerului WLAN pentru instrucțiuni referitoare la accesarea modului WPS.

- Conectarea în cazul în care punctul de acces/routerul WLAN (A) funcționează ca Registrator <sup>1</sup>.



- Conectarea în cazul în care un alt dispozitiv (B), cum ar fi un calculator, este utilizat ca Registrator <sup>1</sup>.




<sup>1</sup> Registratorul este în mod normal punctul de acces/routerul WLAN.

### NOTĂ

Punctele de acces sau routerele care acceptă WPS afișează simbolul:



- 1 Pe ecranul LCD al aparatului, apăsați .
- 2 Apăsați **Rețea**.
- 3 Apăsați **WLAN**.
- 4 Apăsați **▲** sau **▼** pentru a afișa **WPS** cu cod PIN.  
Apăsați **WPS** cu cod PIN.
- 5 Când se afișează **Activare WLAN?**, apăsați **Da** pentru a accepta.  
Va fi lansat expertul de configurare a dispozitivelor wireless.  
Pentru anulare, apăsați **Nu**.
- 6 Ecranul LCD afișează un cod PIN format din opt cifre și aparatul începe căutarea unui punct de acces.
- 7 Pe bara de adrese a browser-ului, introduceți adresa IP a punctului de acces (Registrator <sup>1</sup>).
- <sup>1</sup> Registratorul este în mod normal punctul de acces/routerul WLAN.
- 8 Accesați pagina de configurare WPS, introduceți în Registrator codul PIN afișat pe ecranul LCD, la pasul 6 și respectați instrucțiunile pas cu pas.

## NOTĂ

- Pagina de configurare diferă în funcție de marca punctului de acces/routerului utilizat. Consultați manualul de instrucțiuni al punctului de acces/routerului.
- Pentru a utiliza ca registrator un computer pe care este instalat Windows Vista<sup>®</sup>, Windows<sup>®</sup> 7, Windows<sup>®</sup> 8, Windows<sup>®</sup> 8.1 sau Windows<sup>®</sup> 10, acesta trebuie înregistrat în prealabil în rețeaua dvs. Consultați manualul de instrucțiuni al punctului de acces/routerului dvs. WLAN.
- Dacă utilizați Windows<sup>®</sup> 7, Windows<sup>®</sup> 8, Windows<sup>®</sup> 8.1 sau Windows<sup>®</sup> 10 ca registrator, puteți instala driverul scannerului după configurarea wireless, respectând instrucțiunile pas cu pas. Dacă doriți să instalați întregul pachet de drivere și software, pentru instalare urmați pașii din *Ghidul de instalare și configurare rapidă*.


### Windows Vista<sup>®</sup>/Windows<sup>®</sup> 7/Windows<sup>®</sup> 8/Windows<sup>®</sup> 8.1/Windows<sup>®</sup> 10

Dacă utilizați computerul ca și registrator, urmați pașii de mai jos:

#### a Windows Vista<sup>®</sup>

Faceți clic pe  (**Start**) > **Rețea** > **Adăugare dispozitiv fără fir**.


Windows<sup>®</sup> 7

Faceți clic pe  (**Start**) > **Dispozitive și imprimante** > **Adăugare dispozitiv**.

Windows<sup>®</sup> 8 și Windows<sup>®</sup> 8.1

Deplasați mouse-ul în colțul din dreapta jos al spațiului de lucru. Când apare bara de meniu, faceți clic pe **Setări** > **Panou de control** > **Dispozitive și imprimante** > **Adăugare dispozitiv**.

Windows<sup>®</sup> 10

Faceți clic pe  (**Start**) > **Setări** > **Dispozitive** > **Dispozitive conectate** > **Adăugare dispozitiv**.

#### b Selectați aparatul și faceți clic pe **Următorul**.

#### c Introduceți codul PIN afișat pe LCD, la pasul 6, apoi faceți clic pe **Următorul**.



**d** Selectați rețeaua la care doriți să vă conectați și apoi faceți clic pe **Următorul**.



**e** Faceți clic pe **Închidere**.

- 9** Dacă dispozitivul wireless se conectează cu succes, ecranul LCD afișează *Conectat*. În cazul în care conectarea a eșuat, pe ecranul LCD va fi afișat un cod de eroare. Notați-vă codul de eroare, consultați *Coduri de eroare LAN wireless (ADS-2800W/ADS-3600W)* la pagina 89 și corectați eroarea.

**OK!** **Windows®**

Ați finalizat configurarea rețelei wireless. Dacă doriți să continuați instalarea driverelor și a programelor software necesare pentru funcționarea dispozitivului dvs., introduceți DVD-ROM-ul în unitatea DVD.

## NOTĂ

Dacă ecranul Brother nu apare automat, faceți clic pe  (**Start**) > **Computer (Computerul meu)**. (Pentru Windows® 8, Windows® 8.1, Windows® 10: faceți clic pe pictograma  (**Explorator**) din bara de activități și apoi mergeți la **Acest computer/Acest PC**.) Faceți dublu clic pe pictograma DVD, apoi dublu clic pe **start.exe**.

## Macintosh

Ați finalizat configurarea rețelei wireless. Dacă doriți să continuați instalarea driverelor și a programelor software necesare pentru funcționarea dispozitivului dvs., selectați **Start Here OSX** din meniul driverului.

## Configurarea în modul Ad-hoc

### Utilizarea unui identificator SSID configurat

Dacă încercați să asociați aparatul cu un computer aflat deja în modul Ad-hoc, având identificatorul SSID configurat, urmați pașii de mai jos:

- 1 Înainte de a configura aparatul, vă recomandăm să vă notați setările rețelei wireless. Veți avea nevoie de aceste informații pentru a începe configurarea.  
Verificați și înregistrați setările curente ale rețelei wireless a computerului la care vă conectați.

### NOTĂ

Setările rețelei wireless a computerului la care vă conectați trebuie să fie definite pentru modul Ad-hoc cu un identificator SSID deja configurat. Pentru instrucțiuni despre configurarea computerului în modul Ad-hoc, consultați informațiile primite împreună cu computerul sau contactați administratorul de rețea.

Numele rețelei (SSID)

Mod de comunicație	Mod de criptare	Cheie de rețea
Ad-hoc	NIMIC	—
	WEP	

#### De exemplu:

Numele rețelei (SSID)
HELLO

Mod de comunicație	Mod de criptare	Cheie de rețea
Ad-hoc	WEP	12345

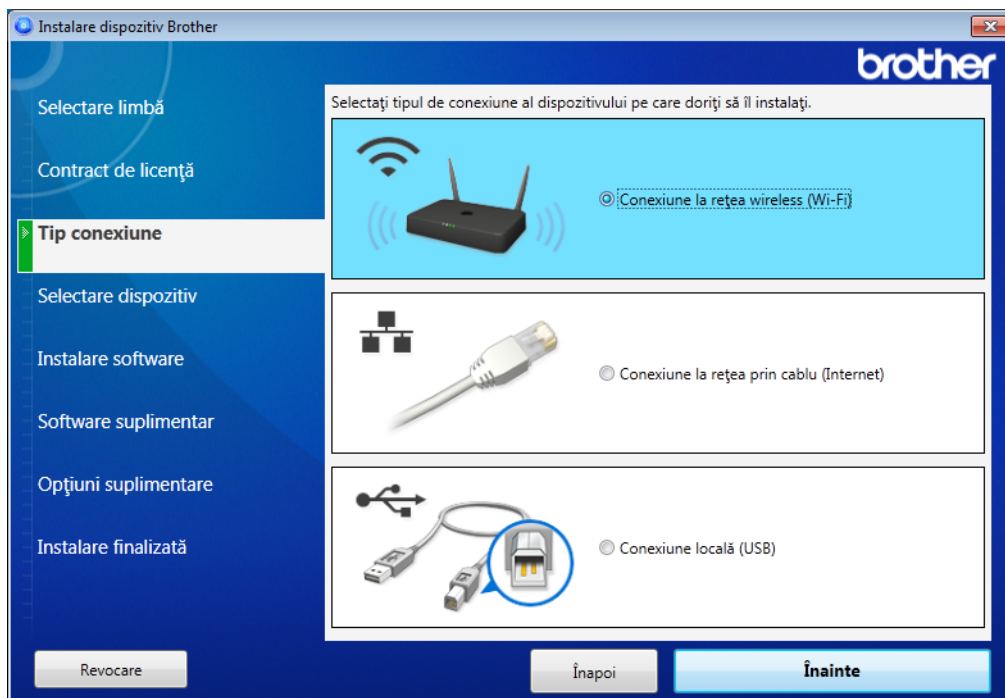
### NOTĂ

Aparatul Brother suportă numai utilizarea primei chei WEP.

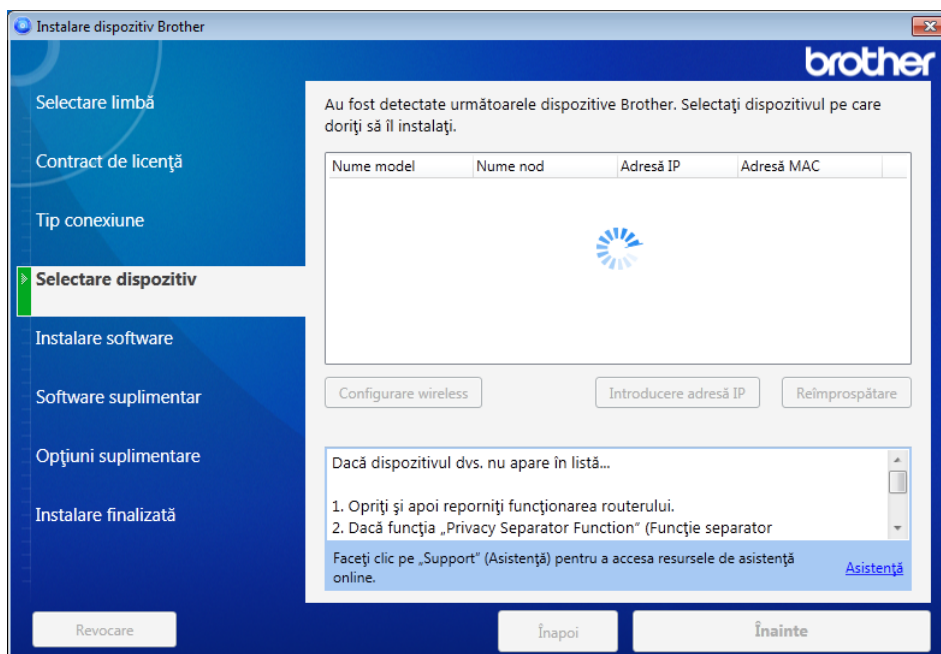
2 Procedați conform uneia dintre metodele de mai jos:

■ Windows®

- a Introduceți DVD-ROM-ul furnizat în unitatea DVD-ROM.
- b Selectați **Conexiune la rețea wireless (Wi-Fi)**, apoi faceți clic pe **Înainte**.



c Faceți clic pe **Configurare wireless**.

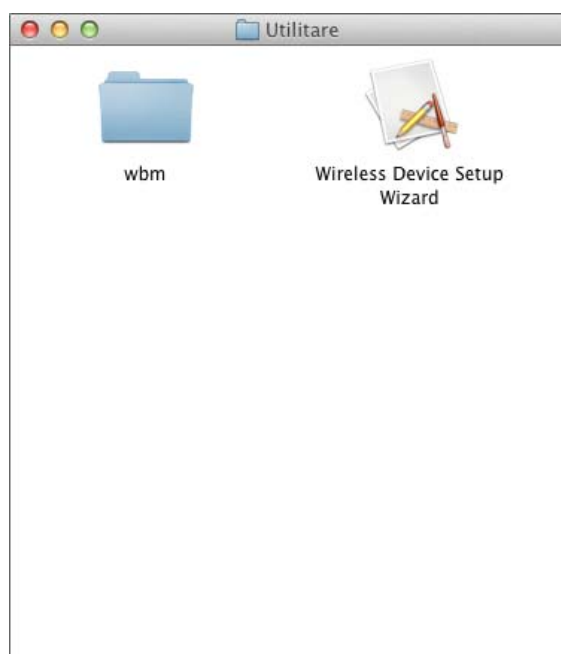


■ Macintosh

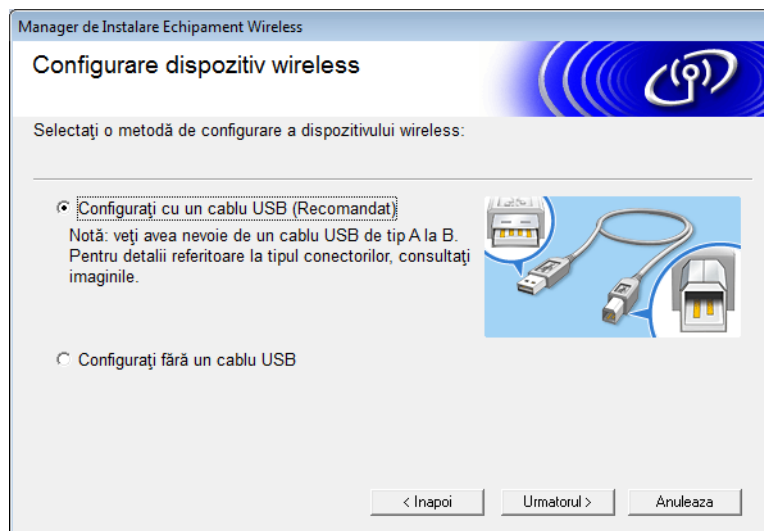
- a Descărcați pachetul complet de drivere și software de la Brother Solutions Center ([support.brother.com](http://support.brother.com)).
- b Faceți dublu clic pe pictograma **BROTHER** de pe desktop.
- c Faceți dublu clic pe **Utilities** (Utilitare).



- d Faceți dublu clic pe **Wireless Device Setup Wizard** (Expert configurare dispozitiv wireless).



- 3 Selectați **Configurați cu un cablu USB (Recomandat)**, apoi faceți clic pe **Urmatorul**.  
Vă recomandăm să utilizați temporar un cablu USB.



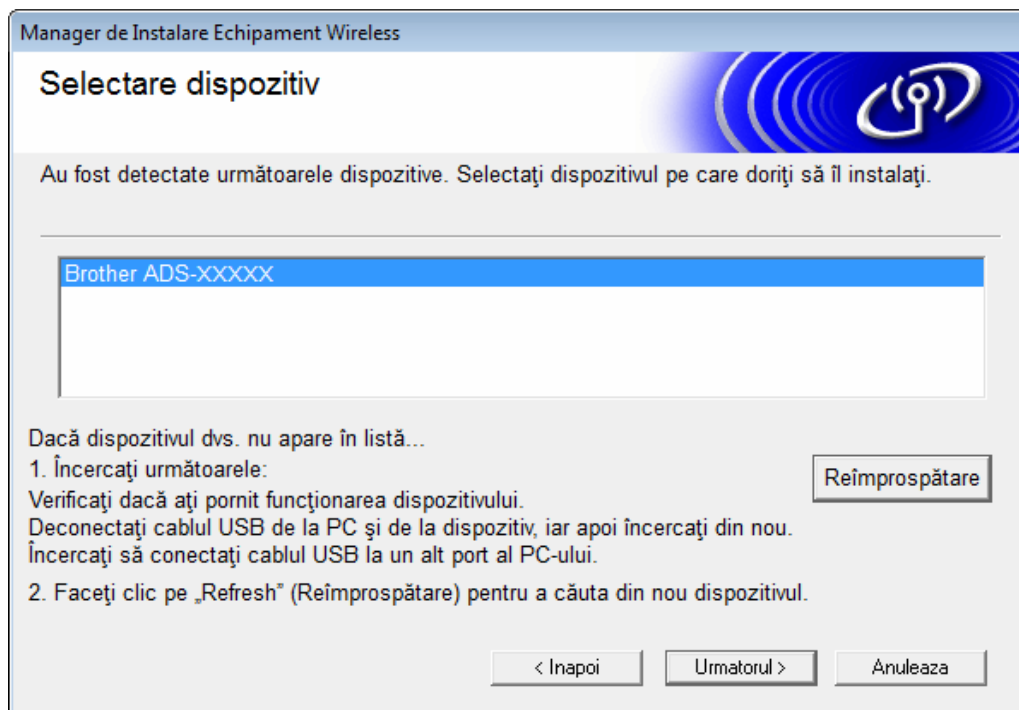
## NOTĂ

Dacă apare acest ecran, citiți **Anunt Important**. Confirmați SSID și cheia de rețea, selectați caseta **Verificat si Confirmat**, apoi faceți clic pe **Urmatorul**.



- 4 Conectați temporar cablul USB direct la calculator și la aparat.  
Dacă apare ecranul de confirmare, faceți clic pe **Urmatorul**.

- 5 Faceți clic pe **Urmatorul** (doar Windows®).




- 6 Faceți clic pe **Avansat**.



## NOTĂ

Dacă lista este goală, confirmați că punctul de acces este alimentat și transmite identificatorul SSID, iar apoi verificați dacă aparatul și computerul se află în aria de acoperire pentru comunicare wireless. Faceți clic pe **Reactualizare**.

- 7 Bifați căsuța **Aceasta este o rețea ad-hoc și nu are punct de acces.**, apoi faceți clic pe **Urmatorul**.



Program asistent pentru configurarea dispozitivelor wireless

### Nume rețea wireless

Configurați numele rețelei wireless cu care va fi asociat dispozitivul.

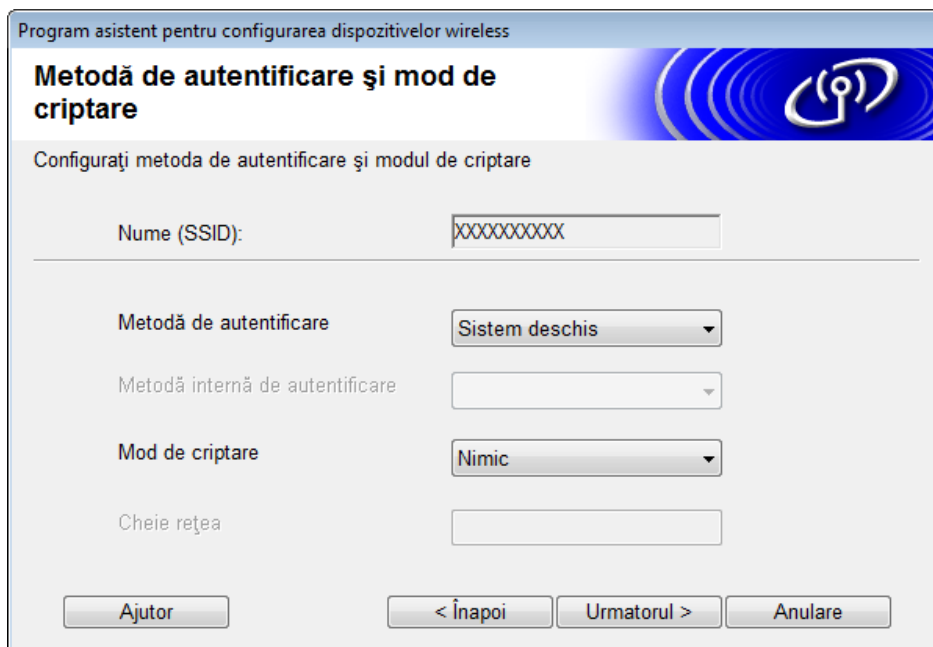
Nume (SSID)

Aceasta este o rețea ad-hoc și nu are punct de acces.

Canal

Ajutor < Înapoi Urmatorul > Anulare

- 8 Selectați **Metodă de autentificare** și **Mod de criptare** din listele derulante, introduceți o cheie de rețea în câmpul **Cheie rețea**, apoi faceți clic pe **Urmatorul**.



Program asistent pentru configurarea dispozitivelor wireless

### Metodă de autentificare și mod de criptare

Configurați metoda de autentificare și modul de criptare

Nume (SSID):

Metodă de autentificare

Metodă internă de autentificare

Mod de criptare

Cheie rețea

Ajutor < Înapoi Urmatorul > Anulare

- 9 Faceți clic pe **Urmatorul**. Aparatul recepționează setările. (În exemplul următor, modul de criptare este WEP.)



Program asistent pentru configurarea dispozitivelor wireless

### Confirmare setări rețea wireless

Faceți clic pe butonul „Urmatorul” pentru a trimite următoarele setări către dispozitiv

Adresă IP	Automat	<input type="button" value="Schimbare adresă IP"/>
Mod de comunicare	Infrastructură	
Nume (SSID)	XXXXXXXXXX	
Metodă de autentificare	Cheie partajată	
Mod de criptare	WEP	

- 10 Deconectați cablul USB dintre computer și aparat.
- 11 Faceți clic pe **Terminare**.



## Configurarea aparatului pentru o rețea wireless utilizând expertul de configurare din panoul de control al aparatului

Înainte de a configura aparatul, vă recomandăm să vă notați setările rețelei wireless. Veți avea nevoie de aceste informații pentru a începe configurarea.

- 1 Verificați și notați setările actuale ale rețelei wireless a calculatorului la care vă conectați.

Numele rețelei (SSID)

Cheie de rețea

De exemplu:

Numele rețelei (SSID)
HELLO

Cheie de rețea
12345

### NOTĂ

- Punctul dvs. de acces/routerul poate accepta utilizarea mai multor chei WEP; totuși, aparatul Brother acceptă doar utilizarea primei chei WEP.
- Dacă aveți nevoie de asistență în timpul configurării și doriți să contactați Centrul de asistență clienți Brother, asigurați-vă că sunt pregătite SSID (Numele rețelei) și Cheia de rețea. Noi nu vă putem ajuta să găsiți aceste informații.
- Trebuie să cunoașteți aceste informații (SSID și Cheia de rețea) pentru a continua configurarea wireless.

#### Cum pot găsi aceste informații?

- a Consultați documentația furnizată și punctul de acces/routerul wireless.
- b SSID inițial poate fi numele producătorului sau numele modelului.
- c Dacă nu cunoașteți informațiile de securitate, vă rugăm să întrebați producătorul router-ului, administratorul de sistem sau furnizorul de Internet.

- 2 Pe ecranul LCD al aparatului dvs. Brother, apăsați  > Rețea > WLAN > Expert setare.

- 3 Aparatul caută rețeaua, apoi afișează o listă de SSID disponibile. Când este afișată o listă de SSID, apăsați ▲ sau ▼ pentru a afișa SSID la care doriți să vă conectați, apoi apăsați SSID.

- 4 Apăsați OK.

**5** Procedați conform uneia dintre metodele de mai jos:

- Dacă utilizați o metodă de autentificare și criptare care solicită o Cheie de rețea, introduceți Cheia de rețea pe care ați scris-o la primul pas.  
După ce introduceți toate caracterele, apăsați OK, apoi apăsați Da pentru a aplica setările.
- Dacă metoda de autentificare este Sistem deschis, iar modul dvs. de criptare este Niciunul, treceți la pasul următor.
- Dacă punctul de acces/routerul WLAN acceptă WPS, se afișează Punctul de acces / ruterul selectat suportă WPS. Utilizați WPS? Pentru a vă conecta aparatul utilizând modul wireless automat, apăsați Da. (Dacă ați selectat Nu (Manual), introduceți Cheia de rețea pe care ați scris-o la primul pas.) Când se afișează Porniți WPS la punctul de acces / ruterul fără fir, apoi apăsați pe [Următorul]. apăsați butonul WPS din punctul de acces/routerul WLAN, apoi apăsați Următorul.

**6** Aparatul încearcă să se conecteze la dispozitivul wireless selectat.

Dacă dispozitivul wireless se conectează cu succes, ecranul LCD al aparatului afișează Conectat.

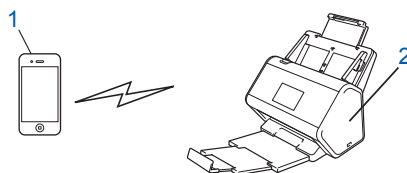
Ați finalizat configurarea rețelei wireless. Pentru instalarea driverelor și software-ului necesar pentru utilizarea aparatului, introduceți DVD-ROM de instalare în unitatea calculatorului sau vizitați pagina **Descărcări** a modelului dvs., din Brother Solutions Center la [support.brother.com](http://support.brother.com)

## Utilizarea Wi-Fi Direct®

- Scanarea de pe dispozitivul mobil utilizând Wi-Fi Direct®
- Configurarea rețelei Wi-Fi Direct®
- Configurarea setărilor rețelei Wi-Fi Direct® de pe panoul de control al aparatului

### Scanarea de pe dispozitivul mobil utilizând Wi-Fi Direct®

Wi-Fi Direct® este una dintre metodele de configurare wireless dezvoltate de Wi-Fi Alliance®. Vă permite configurarea unei rețele wireless securizate între aparatul Brother și un dispozitiv mobil, precum dispozitivul Android™, dispozitivul Windows® Phone, iPhone, iPod touch sau iPad, fără a utiliza un punct de acces. Wi-Fi Direct® acceptă configurarea rețelei wireless utilizând metoda printr-o singură apăsare sau metoda PIN a Wi-Fi Protected Setup™ (WPS). Puteți configura, de asemenea, o rețea wireless, prin setarea manuală a unui SSID și a parolei. Caracteristica Wi-Fi Direct® a aparatului Brother acceptă securitate WPA2™ cu criptare AES.



#### 1 Dispozitiv mobil

#### 2 Aparatul dvs. Brother

### NOTĂ

- Deși aparatul Brother poate fi utilizat atât într-o rețea prin cablu, cât și într-o rețea wireless, poate fi folosită o singură metodă de conectare într-un anumit moment. Cu toate acestea, puteți utiliza în același timp o conexiune la rețeaua wireless și o conexiune Wi-Fi Direct®, sau o conexiune la rețeaua cablată și o conexiune Wi-Fi Direct®.
- Dispozitivul care acceptă Wi-Fi Direct® poate deveni Group Owner (G/O) (Proprietar grup). Când configurați o rețea Wi-Fi Direct® G/O servește ca punct de acces.
- Modul Ad-hoc și Wi-Fi Direct® nu pot fi utilizate în același timp. Dezactivați o funcție pentru a o activa pe cealaltă. Pentru utilizarea Wi-Fi Direct® în timp ce utilizați modul Ad-hoc, setați I/F de rețea la „LAN prin cablu” sau dezactivați modul Ad-hoc și conectați aparatul Brother la punctul de acces.

## Configurarea rețelei Wi-Fi Direct®

Configurați setările rețelei Wi-Fi Direct® de pe panoul de control al aparatului.

### ■ Prezentare generală a configurării rețelei Wi-Fi Direct®

Instrucțiunile următoare oferă cinci metode de configurare a aparatului Brother într-un mediu de rețea wireless. Alegeți metoda preferată pentru mediul dvs.

- Configurați rețeaua Wi-Fi Direct® utilizând metoda printr-o singură apăsare
- Configurați rețeaua Wi-Fi Direct® utilizând metoda printr-o singură apăsare a Wi-Fi Protected Setup™ (WPS)
- Configurați rețeaua Wi-Fi Direct® utilizând metoda PIN
- Configurați rețeaua Wi-Fi Direct® utilizând metoda PIN a Wi-Fi Protected Setup™ (WPS)
- Configurați rețeaua Wi-Fi Direct® manual

## Prezentare generală a configurării rețelei Wi-Fi Direct®

Instrucțiunile următoare oferă cinci metode de configurare a aparatului Brother într-un mediu de rețea wireless. Alegeți metoda preferată pentru mediul dvs.

Verificați configurarea dispozitivului mobil.

### 1 Dispozitivul dvs. mobil acceptă Wi-Fi Direct®?

Opțiune	Descriere
Da	Mergeți la pasul 2.
Nu	Mergeți la pasul 3.

### 2 Dispozitivul dvs. mobil acceptă metoda printr-o singură apăsare pentru Wi-Fi Direct®?

Opțiune	Descriere
Da	Consultați <i>Configurarea rețelei Wi-Fi Direct® utilizând metoda printr-o singură apăsare</i> la pagina 33.
Nu	Consultați <i>Configurarea rețelei Wi-Fi Direct® utilizând metoda PIN</i> la pagina 34.

### 3 Dispozitivul dvs. mobil acceptă Wi-Fi Protected Setup™ (WPS)?

Opțiune	Descriere
Da	Mergeți la pasul 4.
Nu	Consultați <i>Configurarea manuală a rețelei Wi-Fi Direct®</i> la pagina 37.

**4** Dispozitivul dvs. mobil acceptă metoda printr-o singură apăsare pentru Wi-Fi Protected Setup™ (WPS)?

Opțiune	Descriere
Da	Consultați <i>Configurarea rețelei Wi-Fi Direct® utilizând metoda printr-o singură apăsare a Wi-Fi Protected Setup™ (WPS)</i> la pagina 34.
Nu	Consultați <i>Configurarea rețelei Wi-Fi Direct® utilizând metoda PIN a Wi-Fi Protected Setup™ (WPS)</i> la pagina 35.



Pentru utilizarea funcționalității Brother iPrint&Scan într-o rețea Wi-Fi Direct® configurată cu ajutorul metodei printr-o singură apăsare sau prin configurarea metodei PIN, dispozitivul utilizat pentru configurarea Wi-Fi Direct® trebuie să ruleze în Android™ 4.0 sau versiuni mai noi.

## Configurarea rețelei Wi-Fi Direct® utilizând metoda printr-o singură apăsare

Dacă dispozitivul dvs. mobil acceptă Wi-Fi Direct®, urmați acești pași pentru configurarea unei rețele Wi-Fi Direct®.

### NOTĂ

Când aparatul primește solicitarea Wi-Fi Direct® de la dispozitivul mobil, apare mesajul *A fost primită o cerere pentru o conexiune Wi-Fi Direct*. Pentru conectare, apăsați pe [OK]. pe ecranul LCD. Apăsați OK pentru conectare.



- 1 Apăsați  > Rețea > Wi-Fi Direct > Buton comandă.
- 2 Activați Wi-Fi Direct® pe dispozitivul mobil (consultați manualul de utilizare al dispozitivului mobil pentru instrucțiuni) când apare *Activați Wi-Fi Direct* pe un alt dispozitiv. Apoi apăsați pe [OK] . pe ecranul LCD al aparatului. Apăsați OK de pe aparat, pentru a începe configurarea rețelei Wi-Fi Direct®. Pentru anulare, apăsați .
- 3 Procedați conform uneia dintre metodele de mai jos:
  - Dacă aparatul Brother este Group Owner (G/O) (Proprietar grup), conectați dispozitivul mobil direct la aparat.
  - Dacă aparatul Brother nu este (G/O), afișează denumirile dispozitivelor care vă permit să configurați o rețea Wi-Fi Direct®. Selectați dispozitivul mobil la care doriți să vă conectați și apăsați pe OK. Căutați din nou dispozitivele disponibile, apăsând *Rescanare*.
- 4 Dacă dispozitivul mobil se conectează cu succes, ecranul LCD al aparatului afișează *Conectat*. Acum ați finalizat configurarea rețelei Wi-Fi Direct®.

## Configurarea rețelei Wi-Fi Direct<sup>®</sup> utilizând metoda printr-o singură apăsare a Wi-Fi Protected Setup<sup>™</sup> (WPS)

Dacă dispozitivul dvs. mobil acceptă WPS (PBC: Push Button Configuration - Configurare prin apăsarea unui buton), urmați acești pași pentru configurarea unei rețele Wi-Fi Direct<sup>®</sup>.

### NOTĂ

Când aparatul primește solicitarea Wi-Fi Direct<sup>®</sup> de la dispozitivul mobil, apare mesajul A fost primită o cerere pentru o conexiune Wi-Fi Direct. Pentru conectare, apăsați pe [OK]. pe ecranul LCD. Apăsați OK pentru conectare.



- 1 Apăsați  > Rețea > Wi-Fi Direct > Deținător grup.
- 2 Apăsați Pornit.
- 3 Rulați în sus sau în jos ori apăsați ▲ sau ▼ pentru a selecta opțiunea Buton comandă. Apăsați Buton comandă.
- 4 Când apare Wi-Fi Direct activat?, apăsați Pornit pentru a accepta. Pentru anulare, apăsați Oprit.
- 5 Activați metoda de configurare printr-o singură apăsare WPS a dispozitivului mobil (consultați manualul de utilizare al dispozitivului mobil pentru instrucțiuni), când apare Activați Wi-Fi Direct pe un alt dispozitiv. Apoi apăsați pe [OK]. pe ecranul LCD al aparatului. Apăsați OK de pe ecranul LCD al aparatului Brother.  
Acest lucru va porni configurarea Wi-Fi Direct<sup>®</sup>. Pentru anulare, apăsați .
- 6 Dacă dispozitivul mobil se conectează cu succes, ecranul LCD al aparatului afișează Conectat. Ați finalizat configurarea rețelei Wi-Fi Direct<sup>®</sup>.


## Configurarea rețelei Wi-Fi Direct<sup>®</sup> utilizând metoda PIN

Dacă dispozitivul dvs. mobil acceptă metoda PIN a Wi-Fi Direct<sup>®</sup>, urmați acești pași pentru configurarea unei rețele Wi-Fi Direct<sup>®</sup>:

### NOTĂ

Când aparatul primește solicitarea Wi-Fi Direct<sup>®</sup> de la dispozitivul mobil, apare mesajul A fost primită o cerere pentru o conexiune Wi-Fi Direct. Pentru conectare, apăsați pe [OK]. pe ecranul LCD. Apăsați OK pentru conectare.

- 1 Apăsați  > Rețea > Wi-Fi Direct > Cod PIN.
- 2 Când apare Wi-Fi Direct activat?, apăsați Pornit pentru a accepta. Pentru anulare, apăsați Oprit.
- 3 Activați Wi-Fi Direct<sup>®</sup> pe dispozitivul mobil (consultați manualul de utilizare al dispozitivului mobil pentru instrucțiuni) când apare Activați Wi-Fi Direct pe un alt dispozitiv. Apoi apăsați pe [OK]. pe ecranul LCD al aparatului. Apăsați OK de pe aparat, pentru a începe configurarea rețelei Wi-Fi Direct<sup>®</sup>. Pentru anulare, apăsați .



- 4 Procedați conform uneia dintre metodele de mai jos:
- Dacă aparatul dvs. Brother este Group Owner (G/O) (Proprietar grup), așteaptă o solicitare de conectare de la dispozitivul mobil. Când apare **Cod PIN**, introduceți PIN-ul afișat pe dispozitivul mobil în aparat. Apăsați **OK** pentru a finaliza configurarea.  
Dacă este afișat PIN-ul pe aparatul Brother, introduceți PIN-ul în dispozitivul mobil.
  - Dacă aparatul Brother nu este G/O, afișează denumirile dispozitivelor care vă permit să configurați o rețea Wi-Fi Direct®. Selectați dispozitivul mobil la care doriți să vă conectați și apăsați pe **OK**.  
Căutați din nou dispozitivele disponibile, apăsând **Rescanare**.
- 5 Procedați conform uneia dintre metodele de mai jos:
- Apăsați **Afișare cod PIN** pentru a afișa PIN-ul pe aparat și introduceți PIN-ul în dispozitivul mobil. Treceți la pasul următor.
  - Apăsați **Introducere cod PIN** pentru a introduce în aparat un PIN afișat de dispozitivul mobil, apoi apăsați **OK**. Treceți la pasul următor.
- Dacă dispozitivul mobil nu afișează un PIN, apăsați  pe aparatul Brother.
- Întoarceți-vă la primul pas și încercați din nou.
- 6 Dacă dispozitivul mobil se conectează cu succes, ecranul LCD al aparatului afișează **Conectat**. Ați finalizat configurarea rețelei Wi-Fi Direct®.

## Configurarea rețelei Wi-Fi Direct® utilizând metoda PIN a Wi-Fi Protected Setup™ (WPS)

Dacă dispozitivul dvs. mobil acceptă metoda PIN a Wi-Fi Protected Setup™ (WPS), urmați acești pași pentru configurarea unei rețele Wi-Fi Direct®.

### NOTĂ

Când aparatul primește solicitarea Wi-Fi Direct® de la dispozitivul mobil, apare mesajul **A fost primită o cerere pentru o conexiune Wi-Fi Direct**. Pentru conectare, apăsați pe **[OK]** pe ecranul LCD. Apăsați **OK** pentru conectare.

- 1 Apăsați  > **Rețea** > **Wi-Fi Direct** > **Deținător grup**.
- 2 Apăsați **Pornit**.
- 3 Rulați în sus sau în jos ori apăsați **▲** sau **▼** pentru a selecta opțiunea **Cod PIN**. Apăsați **Cod PIN**.
- 4 Când apare **Wi-Fi Direct activat?**, apăsați **Pornit** pentru a accepta. Pentru anulare, apăsați **Oprit**.
- 5 Când apare **Activați Wi-Fi Direct** pe un alt dispozitiv. Apoi apăsați pe **[OK]**, activați metoda de configurare WPS PIN a dispozitivului mobil (consultați manualul de utilizare al dispozitivului mobil pentru instrucțiuni), apoi apăsați **OK** pe aparatul Brother. Începe configurarea rețelei Wi-Fi Direct®. Pentru anulare, apăsați .

- 6 Aparatul așteaptă o solicitare de conectare de la dispozitivul mobil. Când apare Cod PIN, introduceți PIN-ul afișat pe dispozitivul mobil în aparat. Apăsați OK.
- 7 Dacă dispozitivul mobil se conectează cu succes, ecranul LCD al aparatului afișează Conectat. Acum ați finalizat configurarea rețelei Wi-Fi Direct®.




## Configurarea manuală a rețelei Wi-Fi Direct®

Dacă dispozitivul dvs. mobil nu acceptă Wi-Fi Direct® sau WPS, trebuie să configurați manual o rețea Wi-Fi Direct®.

### NOTĂ

Când aparatul primește solicitarea Wi-Fi Direct® de la dispozitivul mobil, apare mesajul A fost primită o cerere pentru o conexiune Wi-Fi Direct. Pentru conectare, apăsați pe [OK]. pe ecranul LCD. Apăsați OK pentru conectare.

- 1 Apăsați  > Rețea > Wi-Fi Direct > Manual.
- 2 Când apare Wi-Fi Direct activat?, apăsați Pornit pentru a accepta. Pentru anulare, apăsați Oprit.
- 3 Aparatul afișează numele SSID și parola timp de două minute. Accesați ecranul cu setările rețelei wireless al dispozitivului mobil și introduceți numele SSID și parola.
- 4 Dacă dispozitivul mobil se conectează cu succes, ecranul LCD al aparatului afișează Conectat. Ați finalizat configurarea rețelei Wi-Fi Direct®.

## Prezentare generală

Puteți utiliza un browser web standard pentru a gestiona aparatul de la un computer din rețeaua dumneavoastră, folosind protocolul HTTP (Protocol de transfer hipertext) sau HTTPS (Protocol de transfer hipertext prin protocol de codificare).

- Obțineți informații referitoare la stare, întreținere și despre versiunea de software pentru aparatul Brother și pentru serverul de scanare.
- Modificați detaliile referitoare la configurarea rețelei și aparatului (consultați *Configurarea setărilor aparatului* la pagina 39).
- Configurați setările pentru a restricționa accesul neautorizat al altor persoane.
  - Consultați *Configurarea unei parole de conectare* la pagina 40.
  - Consultați *Configurarea autentificării Active Directory prin LDAP (ADS-2800W/ADS-3600W)* la pagina 43.
- Configurați/modificați setările de rețea.
  - Consultați *Modificarea configurării funcției Scanare către FTP* la pagina 49.
  - Consultați *Modificarea configurării funcției Scanare către SFTP* la pagina 50.
  - Consultați *Modificarea configurării funcției Scanare către rețea (Windows®)* la pagina 52.
  - Consultați *Sincronizarea cu serverul Sntp* la pagina 47.
  - Consultați *Utilizarea LDAP (ADS-2800W/ADS-3600W)* la pagina 44.
  - Consultați *Configurarea setărilor avansate TCP/IP* la pagina 56.
- Import/export agendă. (Consultați *Import/export agendă de adrese (ADS-2800W/ADS-3600W)* la pagina 58.)

### NOTĂ

Vă recomandăm să folosiți Microsoft® Internet Explorer® 8.0/10.0/11.0 pentru Windows® și Safari 8.0 pentru Macintosh. Asigurați-vă că browserul web are activat atât Javascript, cât și cookie-urile. Dacă utilizați un browser web diferit, asigurați-vă că este compatibil cu HTTP 1.0 și HTTP 1.1.


Trebuie să utilizați protocolul TCP/IP din rețeaua dvs. și să aveți o adresă IP valabilă, înregistrată pe serverul de scanare și în calculatorul dvs.

## Configurarea setărilor aparatului

- 1 Lansați Administrarea bazată pe web.
  - a Porniți browserul web.
  - b Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: `http://192.168.1.2`.

### NOTĂ

- Dacă utilizați un Sistem nume domeniu (DNS) sau activați o denumire NetBIOS, puteți introduce în locul adresei IP un alt nume, de exemplu „ScannerPartajat”.
  - De exemplu:  
`http://ScannerPartajat/`
- De asemenea, dacă activați o denumire NetBIOS, puteți utiliza numele nodului.
  - De exemplu:  
`http://brwxxxxxxxxxxxxx/`
- Puteți găsi denumirea NetBIOS în panoul de control al aparatului, la `Nume Nod`.
- Pentru a utiliza protocolul HTTPS sigur pentru configurarea setărilor cu ajutorul administrării bazate pe web, trebuie să configurați un certificat CA înainte de a lansa Administrarea bazată pe web. Consultați *Gestionare certificate multiple* la pagina 69.

- 2 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit-o, și apoi faceți clic pe .
- 3 Puteți configura acum setările aparatului.

### NOTĂ

Dacă ați modificat setările protocolului, reporniți aparatul Brother după ce faceți clic pe **Submit** (Trimitere) pentru a activa configurarea.

## Configurarea unei parole de conectare

Vă recomandăm setarea unei parole de conectare pentru a preveni accesul neautorizat la Administrarea bazată pe web.

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).
- 2 Când apare ecranul Administrare bazată pe web, faceți clic pe fila **Administrator**, apoi faceți clic pe **Login Password** (Parolă de conectare) din bara de navigare situată în partea stângă.
- 3 Introduceți parola dorită (până la 32 de caractere).
- 4 Reintroduceți parola în câmpul **Confirm New Password** (Confirmare parolă nouă).
- 5 Faceți clic pe **Submit** (Trimitere).  
Următoarea dată când accesați administrarea bazată pe web, introduceți parola în caseta **Login** (Conectare) și apoi faceți clic pe ➡.  
După ce ați terminați, deconectați-vă, făcând clic pe ➡.

### NOTĂ

De asemenea, puteți configura o parolă de conectare făcând clic pe **Please configure the password** (Configurați parola) din Administrare bazată pe web.

# Utilizarea autentificării prin LDAP

## Introducere în Autentificarea prin LDAP

Autentificarea prin LDAP restricționează utilizarea aparatului Brother. Dacă Autentificarea prin LDAP este activată, panoul de control al aparatului se va bloca. Nu puteți modifica setările aparatului până când nu introduceți un ID și o parolă de utilizator.

- Puteți obține adresa de e-mail în funcție de ID-ul utilizatorului, de la serverul LDAP, atunci când trimiteți datele scanate la un server de e-mail.  
Pentru a utiliza această caracteristică, selectați opțiunea **Get Mail Address** (Obținerea adresei de e-mail). Adresa dvs. de e-mail va fi setată ca expeditor atunci când aparatul va transmite datele scanate către un server de e-mail, sau ca destinatar, dacă doriți să trimiteți datele scanate către adresa dvs. de e-mail.

Puteți modifica setările de autentificare prin LDAP utilizând Administrarea bazată pe web sau BRAdmin Professional 3 (Windows®).

## Configurarea Autentificării prin LDAP utilizând Administrarea bazată pe web

- 1 Porniți browserul web.
- 2 Tastați „http://adresa IP a aparatului” pe bara de adrese a browser-ului dvs. (unde „http://adresa IP a aparatului” este adresa IP a aparatului).  
De exemplu:  
http://192.168.1.2
- 3 Faceți clic pe fila **Administrator**.
- 4 Faceți clic pe meniul **User Restriction Function** (Funcție de restricționare utilizatori) din bara de navigare din stânga.
- 5 Selectați **LDAP Authentication** (Autentificare prin LDAP).
- 6 Faceți clic pe **Submit** (Trimitere).
- 7 Selectați **LDAP Authentication** (Autentificare prin LDAP) din bara de navigare din stânga.

## 8 Configurați setările următoare:

Opțiune	Descriere
<b>Remember User ID</b> (Memorare ID utilizator)	Selecționați această opțiune pentru a salva ID-ul utilizatorului.
<b>LDAP Server Address</b> (Adresă server LDAP)	Introduceți adresa IP sau numele serverului (spre exemplu: ad.exemplu.com) din serverul LDAP.
<b>Get Mail Address</b> (Obținere adresă de e-mail)	Selecționați această opțiune pentru a obține adresa de e-mail pentru aparatul dvs., din serverul LDAP.
<b>LDAP Server Port</b> (Port server LDAP)	Introduceți numărul portului serverului LDAP.
<b>LDAP Search Root</b> (Rădăcină căutare LDAP)	Introduceți rădăcina de căutare LDAP.
<b>Attribute of Name (Search Key)</b> (Atribut nume (Cheie de căutare))	Introduceți atributul pe care doriți să-l utilizați drept cheie de căutare.

## 9 Faceți clic pe **Submit** (Trimitere).

## Conectare pentru modificarea setărilor aparatului, utilizând panoul de control al aparatului

### NOTĂ

Dacă Autentificarea prin LDAP este activată, panoul de control al aparatului se va bloca până când introduceți ID-ul și parola dvs. de utilizator în panoul de control al aparatului.

- 1 Pe panoul de control al aparatului, utilizați ecranul tactil pentru a introduce ID-ul de utilizator și parola.
- 2 Apăsăți OK.
- 3 Dacă autentificarea este reușită, panoul de control al aparatului se va debloca.

## Restricționarea utilizatorilor

### Configurarea autentificării Active Directory prin LDAP (ADS-2800W/ADS-3600W)

Autentificarea Active Directory restricționează utilizarea aparatului Brother. Dacă Autentificarea Active Directory este activată, panoul de control al aparatului va fi blocat. Pentru a utiliza funcțiile de scanare, introduceți un ID de utilizator, numele domeniului și parola.

#### NOTĂ

- Autentificarea Active Directory acceptă autentificarea Kerberos.
- Trebuie să configurați mai întâi protocolul simplu (SNTP) (Server de timp în rețea).

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).
- 2 Faceți clic pe fila **Administrator**.
- 3 Faceți clic pe meniul **User Restriction Function** (Funcție de restricționare utilizatori) din bara de navigare din stânga.
- 4 Selectați **Active Directory Authentication** (Autentificare Active Directory).
- 5 Faceți clic pe **Submit** (Trimitere).
- 6 Selectați **Active Directory Authentication** (Autentificare Active Directory) din bara de navigare din stânga.
- 7 Configurați setările următoare:
  - **Remember User ID** (Memorare ID utilizator)  
Selectați această opțiune pentru a salva ID-ul utilizatorului.
  - **Active Directory Server Address** (Adresă server Active Directory)  
Introduceți adresa IP sau numele serverului (de exemplu: „ad.exemplu.com”) al serverului directorului activ.
  - **Active Directory Domain Name** (Nume domeniu Active Directory)  
Introduceți Numele domeniului Active Directory.
  - **Protocol & Authentication Method** (Protocol și metodă de autentificare)  
Selectați protocolul și metoda de autentificare.
  - **Get Mail Address** (Obținere adresă de e-mail)  
Selectați această opțiune pentru a obține adresa de e-mail pentru aparatul dvs., din serverul LDAP (disponibil doar pentru metoda de autentificare **LDAP + kerberos**).
  - **Get User’s Home Directory** (Obținere director de pornire al utilizatorului)  
Selectați această opțiune pentru a obține directorul de pornire și setați-l ca Scanare în destinația rețelei.
  - **LDAP Server Port** (Port server LDAP)  
Introduceți numărul portului serverului LDAP (disponibil doar pentru metoda de autentificare **LDAP + kerberos**).

- **LDAP Search Root** (Rădăcină căutare LDAP)

Introduceți rădăcina de căutare LDAP (doar pentru metoda de autentificare **LDAP + kerberos**).

- **Fetch DNS** (Obținere DNS)

Urmați instrucțiunile pas cu pas.

- **SNTP**

Consultați pagina 47 pentru mai multe informații despre protocolul SNTP.

8 Faceți clic pe **Submit** (Trimitere).

## Deblocare aparat atunci când Autentificarea Active Directory este activată

1 Pe ecranul LCD al aparatului, utilizați ecranul tactil pentru a vă introduce ID utilizator și Parola.

2 Apăsați OK.

3 După ce sunt datele vă sunt autentificate, panoul de control se deblochează, permițându-vă să utilizați funcțiile de scanare.

## NOTĂ

Nu puteți modifica nicio setare dacă este activată **Active Directory Authentication** (Autentificare Active Directory).

## Utilizarea LDAP (ADS-2800W/ADS-3600W)

Protocolul LDAP vă permite să căutați adrese de e-mail de pe server utilizând funcția de Scanare către server de e-mail.

## Modificarea configurării LDAP

1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul 1 de la pagina 39).

2 Faceți clic pe **Network** (Rețea) de pe pagina web a aparatului.

3 Faceți clic pe **Protocol** (Protocol) din bara de navigare din stânga.

4 Selectați caseta de verificare **LDAP** și apoi faceți clic pe **Submit** (Trimitere).

5 Reporniți aparatul Brother pentru a activa configurarea.

6 În calculatorul dvs., din fila **Address Book** (Agendă de adrese), selectați **LDAP** din bara de navigare din stânga.

7 Configurați setările LDAP următoare:

- **LDAP Server Address** (Adresă server LDAP)

- **Port** (Numărul portului implicit este 389.)

- **Search Root** (Rădăcină căutare)

- **Authentication** (Autentificare)



- **Username** (Nume utilizator)  
Disponibilitatea acestei selecții depinde de metoda de autentificare utilizată.
- **Password** (Parolă)  
Disponibilitatea acestei selecții depinde de metoda de autentificare utilizată.
- **Kerberos Server Address** (Adresă server Kerberos)  
Disponibilitatea acestei selecții depinde de metoda de autentificare utilizată.
- **SNTP**
- **Timeout for LDAP** (Expirare timp pentru LDAP)
- **Attribute of Name (Search Key)** (Atribut nume (Cheie de căutare))
- **Attribute of Email** (Atribut e-mail)


8 Când ați terminat, faceți clic pe **Submit** (Trimiteți). Asigurați-vă că **Status** (Stare) este setată pe **OK** la pagina Rezultat test.

## NOTĂ

- Protocolul LDAP nu este compatibil cu următoarele limbi: chineză simplificată, chineză tradițională și coreeană.
- Dacă serverul LDAP acceptă autentificarea Kerberos, vă recomandăm să selectați Kerberos pentru setarea **Authentication** (Autentificare). Aceasta asigură o autentificare sigură între serverul LDAP și aparat. Trebuie să configurați protocolul SNTP (server de timp în rețea) sau trebuie să configurați corect data, ora și fusul orar în panoul de control al aparatului pentru autentificarea Kerberos. (Pentru informații privind setările SNTP, consultați *Sincronizarea cu serverul SNTP* la pagina 47.)


## Modificarea configurării LDAP cu ajutorul panoului de control al aparatului (ADS-2800W/ADS-3600W)

După ce configurați setările LDAP, utilizați funcția de căutare LDAP a aparatului pentru a găsi adresele de e-mail.

- 1 Încărcați documentul pe care doriți să-l scanați și trimiteți-l prin e-mail la aparatul dvs.
- 2 Pe ecranul LCD al aparatului, apăsați la `serv.de email`.
- 3 Apăsați `Agendă`.
- 4 Apăsați  pentru căutare.
- 5 Introduceți primele caracterele folosite pentru căutare utilizând butoanele de pe ecranul LCD.

## NOTĂ

- Puteți introduce până la 15 caractere.
- Pentru mai multe informații despre metoda de introducere a textului, consultați *Introducerea textului (ADS-2800W/ADS-3600W)* din *manualul de utilizare*.

- 6 Apăsați OK.  
Rezultatele căutării LDAP apar pe ecranul LCD cu  înaintea rezultatelor din agenda locală de adrese. Dacă nu există o corespondență între server și agenda locală de adrese, pe ecranul LCD se afișează Nu au fost găsite rezultate.
- 7 Apăsați ▲ sau ▼ pentru a derula până când găsiți numele dorit, apoi apăsați pe numele respectiv.
- 8 Dacă rezultatul include mai mult decât o adresă de e-mail, apăsați pe adresa de e-mail dorită.
- 9 Apăsați Aplicare.
- 10 Apăsați OK.

---

### NOTĂ


Apăsați Opțiuni pentru a regla setările de scanare înainte de a scana documentul.

---

- 11 Apăsați Pornire.

---

### NOTĂ

- Funcția LDAP a acestui aparat suportă LDAPv3.
  - Pentru informații suplimentare faceți clic pe  din partea dreaptă a ecranului de setări LDAP.
-

## Sincronizarea cu serverul SNTP

Simple Network Time Protocol (SNTP) este utilizat pentru sincronizarea orei utilizate de aparat pentru autentificare cu serverul de timp SNTP (aceasta nu este ora afișată pe ecranul LCD al aparatului). Puteți sincroniza regulat ora aparatului cu ora UTC (Coordinated Universal Time - Ora universală coordonată) furnizată de serverul de timp SNTP.

### NOTĂ

- Această funcție nu este disponibilă în unele țări.
- Cu excepția setării Date&Time (Data&Ora), opțiunea SNTP va funcționa fără modificarea setărilor inițiale.

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).
- 2 Când apare ecranul Administrare bazată pe web, faceți clic pe **Network** (Rețea), apoi pe meniul **Protocol** din bara de navigare din stânga.
- 3 Selectați caseta de verificare **SNTP**.
- 4 Faceți clic pe **Advanced Setting** (Setări avansate).
  - **Status** (Stare)  
Afișează dacă setările serverului SNTP sunt activate sau dezactivate.
  - **Synchronization Status** (Stare sincronizare)  
Confirmați cea mai recentă stare a sincronizării.
  - **SNTP Server Method** (Metodă server SNTP)  
Selectați **AUTO** sau **STATIC**.
    - **AUTO**  
Dacă aveți un server DHCP în rețea, serverul SNTP obține automat adresa de la acel server.
    - **STATIC**  
Introduceți adresa pe care doriți să o utilizați.
  - **Primary SNTP Server Address** (Adresă server SNTP primar), **Secondary SNTP Server Address** (Adresă server SNTP secundar)  
Introduceți adresa serverului (până la 64 de caractere).  
Adresa serverului SNTP secundar este utilizată ca adresă de rezervă pentru adresa serverului SNTP primar. Dacă serverul primar este indisponibil, aparatul va contacta serverul SNTP secundar.
  - **Primary SNTP Server Port** (Port server SNTP primar), **Secondary SNTP Server Port** (Port server SNTP secundar)  
Introduceți numărul portului (între 1 și 65535).  
Portul serverului SNTP secundar este utilizat ca port de rezervă pentru portul serverului SNTP primar. Dacă portul primar este indisponibil, aparatul va contacta portul SNTP secundar.

### ■ Synchronization Interval (Interval sincronizare)

Introduceți numărul de ore dintre încercările de sincronizare ale serverului (între 1 și 168 ore).

## NOTĂ

- Trebuie să configurați **Date&Time** (Data & Ora) pentru a sincroniza ora utilizată de aparat cu serverul de timp SNTP. Faceți clic pe **Date&Time**, (Data & Ora), apoi configurați **Date&Time** (Data & Ora) pe ecranul **General** (Generalități).

**Date&Time**

Date: 01 / 01 / 2015

Clock Type:  12h Clock  24h Clock

Time: 01 : 26 PM

Time Zone: UTC+09:00

Auto Daylight:  Off  On

Synchronize with SNTP server

To synchronize the "Date&Time" with your SNTP server you must configure the SNTP server settings.

[SNTP](#)

Cancel Submit

- Selectați caseta de verificare **Synchronize with SNTP server** (Sincronizare cu serverul SNTP). Verificați dacă setările pentru fusul orar sunt corecte și selectați diferența de timp dintre locația dvs. și UTC din lista derulantă **Time Zone** (Fus orar). De exemplu, fusul orar pentru coasta de est în SUA și Canada este UTC-5, pentru Marea Britanie este UTC, iar pentru Europa Centrală este UTC+1.

- 5 Faceți clic pe **Submit** (Trimitere).

## Modificarea configurării funcției Scanare către FTP

Scanarea către FTP permite scanarea unui document direct pe un server FTP din rețeaua locală sau din Internet. Pentru mai multe informații despre Scanarea către FTP, consultați *Scanarea documentelor către un server FTP* din *manualul de utilizare*.

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).
- 2 Când apare ecranul Administrare bazată pe web, faceți clic în fila **Scan** (Scanare), apoi faceți clic pe **Scan to FTP/SFTP/Network/SharePoint** (Scanare către FTP/SFTP/Rețea/SharePoint) din bara de navigare din stânga.
- 3 Bifați căsuța de selectare **FTP** în numerele de profil (de la 1 la 25).
- 4 Faceți clic pe **Submit** (Trimitere).
- 5 Faceți clic pe **Scan to FTP/SFTP/Network/SharePoint Profile** (Scanare către FTP/SFTP/Rețea/Profil SharePoint) din bara de navigare din stânga.
- 6 Faceți clic pe **FTP** din dreptul Nr. de profil pe care l-ați selectat în pasul ❸. Puteți configura următoarele setări pentru Scanare către FTP:
  - **Profile Name** (Nume profil) (până la 15 caractere)
  - **Host Address** (Adresă gazdă)
  - **Username** (Nume utilizator)
  - **Password** (Parolă)
  - **Store Directory** (Director stocare)
  - **File Name** (Nume fișier)
  - **Quality** (Calitate)
  - **Auto Color detect adjust** (Reglaj automat detecție culoare)
  - **File Type** (Tip fișier)
  - **Password for Secure PDF** (Parolă pentru PDF securizat) (ADS-2400N / ADS-3000N)
  - **Document Size** (Mărime document)
  - **Margin Settings** (Setări margini)
  - **File Size** (Mărime fișier)
  - **Auto Deskew** (Autocorectare înclinare)
  - **Skip Blank Page** (Omitere pagini albe)
  - **Skip blank page sensitivity** (Omitere sensibilitate pagini albe)
  - **2-sided Scan** (Scanare față-verso)
  - **Brightness** (Luminozitate)
  - **Contrast** (Contrast)
  - **Continuous Scan** (Scanare continuă) (ADS-2800W / ADS-3600W)
  - **Passive Mode** (Mod pasiv)
  - **Port Number** (Număr port)

Setați **Passive Mode** (Mod pasiv) pe **Off** (Oprit) sau **On** (Pornit) în funcție de configurarea serverului FTP și configurarea firewall a rețelei. Implicit, această setare este **On** (Pornit). De asemenea, puteți modifica numele portului utilizat pentru a accesa serverul FTP. Valoarea implicită pentru această setare este port 21. În majoritatea cazurilor, aceste două setări pot rămâne la valoarea implicită.
- 7 Faceți clic pe **Submit** (Trimitere).

## Modificarea configurării funcției Scanare către SFTP

Scanarea către SFTP permite scanarea unui document direct pe un server SFTP din rețeaua locală sau din Internet. Pentru mai multe informații despre Scanarea către SFTP, consultați *Scanarea documentelor către un server SFTP* din manualul de utilizare.

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul 1 de la pagina 39).
- 2 Când apare ecranul Administrare bazată pe web, faceți clic în fila **Scan** (Scanare), apoi faceți clic pe **Scan to FTP/SFTP/Network/SharePoint** (Scanare către FTP/SFTP/Rețea/SharePoint) din bara de navigare din stânga.
- 3 Alegeți căsuța de selectare **SFTP** în numerele de profil (de la 1 la 25).
- 4 Faceți clic pe **Submit** (Trimitere).
- 5 Faceți clic pe **Scan to FTP/SFTP/Network/SharePoint Profile** (Scanare către FTP/SFTP/Rețea/Profil SharePoint) din bara de navigare din stânga.
- 6 Faceți clic pe **SFTP** din dreptul Nr. de profil pe care l-ați selectat în pasul 3. Puteți configura următoarele setări pentru Scanare către SFTP:
  - **Profile Name** (Nume profil) (până la 15 caractere)
  - **Host Address** (Adresă gazdă)
  - **Username** (Nume utilizator)
  - **Auth. Method** (Metodă de autentificare)
  - **Password** (Parolă)
  - **Client Key Pair** (Asociere chei client)
  - **Server Public Key** (Cheia publică a serverului)
  - **Store Directory** (Director stocare)
  - **File Name** (Nume fișier)
  - **Quality** (Calitate)
  - **Auto Color detect adjust** (Reglaj automat detecție culoare)
  - **File Type** (Tip fișier)
  - **Password for Secure PDF** (Parolă pentru PDF securizat) (ADS-2400N / ADS-3000N)
  - **Document Size** (Mărime document)
  - **Margin Settings** (Setări margini)
  - **File Size** (Mărime fișier)
  - **Auto Deskew** (Autocorectare înclinare)
  - **Skip Blank Page** (Omitere pagini albe)
  - **Skip blank page sensitivity** (Omitere sensibilitate pagini albe)
  - **2-sided Scan** (Scanare față-verso)
  - **Brightness** (Luminozitate)

- **Contrast** (Contrast)
- **Continuous Scan** (Scanare continuă) (ADS-2800W / ADS-3600W)
- **Port Number** (Număr port)

Puteți modifica numărul portului utilizat pentru accesarea serverului SFTP.

Valoarea implicită pentru această setare este port 21. În majoritatea cazurilor, această setare poate rămâne la valoarea implicită.

- 7 Faceți clic pe **Submit** (Trimitere).

## Modificarea configurării funcției Scanare către rețea (Windows®)

Funcția Scanare către rețea permite scanarea documentelor direct într-un director partajat aflat în rețeaua locală sau de pe internet. Pentru mai multe informații despre Scanarea către rețea, consultați *Scanarea documentelor într-un director/locație de rețea partajată (Windows®)* din manualul de utilizare.

### NOTĂ

Funcția Scanare către rețea acceptă autentificarea NTLMv2.

Trebuie să configurați protocolul SNTP (server de timp în rețea) sau trebuie să configurați corect data, ora și fusul orar în panoul de control al aparatului pentru autentificare. (Pentru informații privind setările SNTP, consultați *Sincronizarea cu serverul SNTP* la pagina 47. Pentru informații privind configurarea datei, orei și fusului orar, consultați *manualul de utilizare*.)

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul 1 de la pagina 39).
- 2 Când apare ecranul Administrare bazată pe web, faceți clic în fila **Scan** (Scanare), apoi faceți clic pe **Scan to FTP/SFTP/Network/SharePoint** (Scanare către FTP/SFTP/Rețea/SharePoint) din bara de navigare din stânga.
- 3 Alegeți căsuța de selectare **Network** (Rețea) în numerele de profil (de la 1 la 25).
- 4 Faceți clic pe **Submit** (Trimitere).
- 5 Faceți clic pe **Scan to FTP/SFTP/Network/SharePoint Profile** (Scanare către FTP/SFTP/Rețea/Profil SharePoint) din bara de navigare din stânga.
- 6 Faceți clic pe **Network** (Rețea) din dreptul Nr. de profil pe care l-ați selectat în pasul 3. Puteți configura următoarele setări pentru Scanare către rețea:
  - **Profile Name** (Nume profil) (până la 15 caractere)
  - **Network Folder Path** (Cale folder rețea)
  - **File Name** (Nume fișier)
  - **Quality** (Calitate)
  - **Auto Color detect adjust** (Reglaj automat detecție culoare)
  - **File Type** (Tip fișier)
  - **Password for Secure PDF** (Parolă pentru PDF securizat) (ADS-2400N / ADS-3000N)
  - **Document Size** (Mărime document)
  - **Margin Settings** (Setări margini)
  - **File Size** (Mărime fișier)
  - **Auto Deskew** (Autocorectare înclinare)
  - **Skip Blank Page** (Omitere pagini albe)
  - **Skip blank page sensitivity** (Omitere sensibilitate pagini albe)
  - **2-sided Scan** (Scanare față-verso)



- **Brightness** (Luminozitate)
- **Contrast** (Contrast)
- **Continuous Scan** (Scanare continuă) (ADS-2800W / ADS-3600W)
- **Use PIN for Authentication** (Utilizare PIN pentru autentificare)
- **PIN Code** (Cod PIN)
- **Auth. Method** (Metodă de autentificare)
- **Username** (Nume utilizator)
- **Password** (Parolă)
- **Date&Time** (Data și ora)

7 Faceți clic pe **Submit** (Trimitere).

## Modificarea configurării funcției Scanare către SharePoint (Windows®)

### SharePoint

Scanați documentele direct către un server SharePoint când trebuie să partajați documentul scanat. Pentru confort sporit, configurați profile diferite, pentru a salva destinațiile dvs. preferate de Scanare către SharePoint. Pentru mai multe informații despre Scanarea către SharePoint, consultați *Scanarea documentelor către SharePoint* din *manualul de utilizare*.

### NOTĂ

Funcția Scanare către SharePoint acceptă autentificarea NTLMv2.

Trebuie să configurați protocolul SNTP (server de timp în rețea) sau trebuie să configurați corect data, ora și fusul orar în panoul de control al aparatului pentru autentificare. (Pentru informații privind setările SNTP, consultați *Sincronizarea cu serverul SNTP* la pagina 47. Pentru informații privind configurarea datei, orei și fusului orar, consultați *manualul de utilizare*.)

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul 1 de la pagina 39).
- 2 Când apare ecranul Administrare bazată pe web, faceți clic în fila **Scan** (Scanare), apoi faceți clic pe **Scan to FTP/SFTP/Network/SharePoint** (Scanare către FTP/SFTP/Rețea/SharePoint) din bara de navigare din stânga.
- 3 Alegeți căsuța de selectare **SharePoint** în numerele de profil (de la 1 la 25).
- 4 Faceți clic pe **Submit** (Trimitere).
- 5 Faceți clic pe **Scan to FTP/SFTP/Network/SharePoint Profile** (Scanare către FTP/SFTP/Rețea/Profil SharePoint) din bara de navigare din stânga.
- 6 Faceți clic pe **SharePoint** din dreptul Nr. de profil pe care l-ați selectat în pasul 3. Puteți configura următoarele setări pentru Scanare către SharePoint:
  - **Profile Name** (Nume profil) (până la 15 caractere)
  - **SharePoint Site Address** (Adresa locației SharePoint)
  - **SSL/TLS**

### NOTĂ

**SSL/TLS** apare doar când selectați **HTTPS** din **SharePoint Site Address** (Adresa locației SharePoint).

- **File Name** (Nume fișier)
- **Quality** (Calitate)
- **Auto Color detect adjust** (Reglaj automat detecție culoare)
- **File Type** (Tip fișier)
- **Password for Secure PDF** (Parolă pentru PDF securizat) (ADS-2400N / ADS-3000N)
- **Document Size** (Mărime document)

- **Margin Settings** (Setări margini)
- **File Size** (Mărime fișier)
- **Auto Deskew** (Autocorectare înclinare)
- **Skip Blank Page** (Omitere pagini albe)
- **Skip blank page sensitivity** (Omitere sensibilitate pagini albe)
- **2-sided Scan** (Scanare față-verso)
- **Brightness** (Luminozitate)
- **Contrast** (Contrast)
- **Continuous Scan** (Scanare continuă) (ADS-2800W / ADS-3600W)
- **Use PIN for Authentication** (Utilizare PIN pentru autentificare)
- **PIN Code** (Cod PIN)
- **Auth. Method** (Metodă de autentificare)
- **Username** (Nume utilizator)
- **Password** (Parolă)
- **Date&Time** (Data și ora)

7 Faceți clic pe **Submit** (Trimitere).

## Configurarea setărilor avansate TCP/IP

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul 1 de la pagina 39).
- 2 Faceți clic pe fila **Network** (Rețea), apoi selectați tipul de conexiune (**Wired** (Prin cablu) sau **Wireless** (Wireless)).
- 3 Selectați **TCP/IP** din meniul de navigare din stânga.
- 4 Faceți clic pe **Advanced Setting** (Setări avansate). Configurați setările următoare: (exemplul de mai jos utilizează **TCP/IP Advanced Settings (Wired)** (Setări avansate TCP/IP) (prin cablu)).

**TCP/IP Advanced Settings (Wired)**

Boot Tries: 3

RARP Boot Settings:  No Subnet Mask,  No Gateway

TCP Timeout: 5 minute(s)

DNS Server Method: AUTO

Primary DNS Server IP Address: 0.0.0.0

Secondary DNS Server IP Address: 0.0.0.0

Gateway Timeout: 21 second(s)

Cancel Submit

- **Boot Tries** (Încercări de boot)  
Introduceți numărul de încercări de pornire utilizând metoda Boot (Pornire) (între 0 și 32767).
- **RARP Boot Settings** (Setări de boot RARP)  
Selectați **No Subnet Mask** (Fără mască de subrețea) sau **No Gateway** (Fără gateway).
  - **No Subnet Mask** (Fără mască de subrețea)  
Mască de subrețea nu este modificată automat.
  - **No Gateway** (Fără Gateway)  
Adresa gateway-ului nu este modificată automat.
- **TCP Timeout** (Expirare timp TCP)  
Introduceți numărul de minute până la expirarea timpului TCP (între 0 și 32767).
- **DNS Server Method** (Metodă server DNS)  
Selectați **AUTO** sau **STATIC**.

- **Primary DNS Server IP Address** (Adresă IP server DNS primar), **Secondary DNS Server IP Address** (Adresă IP server DNS secundar)

Introduceți adresa IP a serverului.

Adresa IP a serverului DNS secundar este utilizată ca adresă de rezervă pentru adresa IP a serverului DNS primar.

Dacă serverul DNS primar este indisponibil, aparatul va contacta serverul DNS secundar.

- **Gateway Timeout** (Expirare timp gateway)

Introduceți numărul de secunde înainte ca routerul să dea eroarea de timp expirat (între 1 și 32767).

- 5 Faceți clic pe **Submit** (Trimitere).

## Import/export agendă de adrese (ADS-2800W/ADS-3600W)

### Importarea agendei de adrese

---

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).
- 2 Faceți clic pe fila **Address Book** (Agendă de adrese).
- 3 Selectați **Import** din meniul de navigare din stânga.
- 4 Introduceți **“Address Book” data file** (Fișierul de date „Agendă de adrese”) sau **“Group” data file** (Fișierul de date „Grup”).
- 5 Faceți clic pe **Submit** (Trimitere).

### Exportarea agendei de adrese

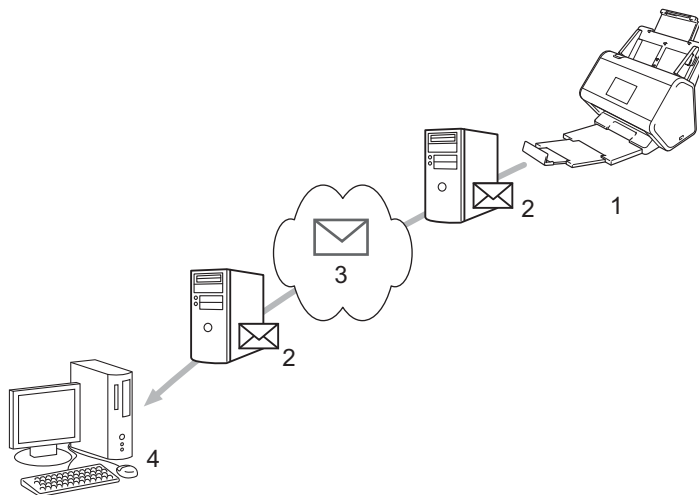
---

- 1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).
- 2 Faceți clic pe fila **Address Book** (Agendă de adrese).
- 3 Selectați **Export** din meniul de navigare din stânga.
- 4 Faceți clic pe butonul **Export to file** (Export către fișier).

## Scanare către un server de e-mail (ADS-2800W/ADS-3600W)

### Prezentare generală

Funcția Scanare către un server de e-mail vă permite să trimiteți documente prin e-mail, ca atașamente.



- 1 Expeditor
- 2 Server de e-mail
- 3 Internet
- 4 Destinatar

### Restricții de dimensiune la utilizarea Scanării către un server de e-mail

Dacă datele de imagine ale unui document sunt prea mari, transmiterea poate să eșueze.

## Configurarea setărilor de Scanare către un server de e-mail

Înainte de a utiliza funcția Scanare către server de e-mail, trebuie să configurați aparatul Brother pentru a comunica cu rețeaua și serverul de e-mail. Puteți configura aceste elemente utilizând Administrarea bazată pe web, Configurarea de la distanță sau BRAdmin Professional 3. Trebuie să vă asigurați că următoarele elemente sunt configurate pe aparat:

- Adresă IP (Dacă utilizați deja aparatul în rețea, adresa IP a aparatului a fost configurată corect.)
- Adresă de e-mail
- Adresa serverului/portul SMTP/Metoda de autentificare/Metoda de criptare/Verificarea certificatului serverului
- Numele și parola contului SMTP-AUTH

Dacă nu cunoașteți aceste elemente, contactați administratorul de rețea.

### NOTĂ

Deși trebuie să configurați o adresă de e-mail pe aparatul dvs., acesta nu are o funcție de primire a mesajelor de e-mail. De aceea, dacă destinatarul răspunde la un e-mail trimis de pe aparatul dvs., aparatul nu îl poate recepționa.

## Înainte de a scana către un server de e-mail

Este posibil să trebuiască să configurați elementele următoare (utilizând Administrarea bazată pe web sau Configurarea la distanță):

- Subiect Exped
- Limita Dimens
- Notificare (pentru mai multe informații, consultați *E-mail verificare transmitere (TX)* la pagina 62)



## Scanarea către un server de e-mail

---

- 1 Încărcați documentul.
- 2 Derulați la stânga sau la dreapta ori apăsați ◀ sau ▶ pentru a afișa la serv.de email.
- 3 Selectați adresa de e-mail pe care doriți s-o utilizați și apoi apăsați OK.
- 4 Apăsați Pornire.

Pentru informații suplimentare cu privire la setările pentru e-mail, consultați *Trimiterea documentelor scanate direct la o adresă de e-mail (ADS-2800W/ADS-3600W)* din manualul de utilizare.

După scanarea documentului, acesta va fi transmis automat către adresa de e-mail specificată prin serverul SMTP.

După ce transmiterea s-a încheiat, ecranul LCD al aparatului afișează ecranul de pornire.

### NOTĂ

---

Unele servere de e-mail nu permit trimiterea documentelor de mari dimensiuni prin e-mail (adesea, administratorul de sistem stabilește o limită maximă pentru dimensiunea mesajelor de e-mail). Cu funcția Scanare către un server de e-mail activată, aparatul va afișa *Memorie plină* atunci când încercați să trimiteți documente prin e-mail care depășesc 1 MB ca dimensiune, iar documentul nu va fi trimis. Divizați documentul în mai multe documente mai mici care vor fi acceptate de către serverul de e-mail.

---

## Funcții suplimentare de scanare către server de e-mail


### E-mail verificare transmitere (TX)

---

Utilizați funcția E-mail verificare TX pentru a solicita o notificare din partea computerului de destinație că e-mail-ul dvs. a fost recepționat și procesat.

#### Configurarea mesajelor TX

Utilizați panoul de control al aparatului pentru a activa funcția de verificare. Dacă `Setez Mail TX` este Pornit, e-mailul conține un câmp suplimentar care este populat automat cu data și ora sosirii e-mailului.

- 1 Pe ecranul LCD al aparatului, apăsați .
- 2 Apăsați `Rețea`.
- 3 Apăsați `E-mail`.
- 4 Apăsați `Setez Mail TX`.
- 5 Apăsați `Notificare`.
- 6 Apăsați `Pornit (sau Oprit)`.

#### NOTĂ

---

- Notificare privind starea mesajului (MDN)  
Acest câmp solicită starea mesajului de e-mail după trimiterea prin sistemul de transport SMTP (Simple Mail Transfer Protocol - Protocol simplu de transfer al corespondenței). După ce destinatarul a recepționat mesajul, aceste date sunt folosite în momentul în care aparatul sau utilizatorul citește e-mail-ul primit. De exemplu, dacă mesajul este deschis și citit, destinatarul va trimite o notificare către aparatul sau utilizatorul inițial. Destinatarul trebuie să activeze câmpul MDN pentru a putea trimite un raport de notificare; în caz contrar solicitarea va fi ignorată.
  - Acest aparat Brother nu poate primi mesaje de e-mail. Pentru a utiliza funcția de verificare TX, trebuie să redirecționați notificarea de retur către o adresă de e-mail diferită. Configurați adresa de e-mail cu ajutorul ecranului LCD al aparatului. Apăsați `Rețea > E-mail > Adresa Mail`, apoi introduceți adresa de e-mail la care doriți să primiți notificarea.
-

## Prezentare generală

Aparatul dumneavoastră Brother folosește unele dintre cele mai recente protocoale disponibile de securitate și de criptare a rețelelor. Aceste caracteristici de rețea pot fi integrate în planul dumneavoastră global de securizare a rețelei pentru a contribui la protejarea datelor și la prevenirea accesului neautorizat la aparat.

Puteți configura următoarele caracteristici de securitate:

- Trimiterea securizată a unui e-mail (consultați *Trimiterea securizată a unui e-mail (ADS-2800W/ADS-3600W)* la pagina 64)
- Gestionarea mai multor certificate (consultați *Gestionare certificate multiple* la pagina 69)
- Crearea unei Asocieri de chei ale clientului (consultați *Crearea unei Asocieri de chei client* la pagina 66)
- Exportarea unei Asocieri de chei ale clientului (consultați *Exportarea unei Asocieri de chei client* la pagina 67)
- Importarea unei Chei publice a serverului (consultați *Importarea unei Chei publice a serverului* la pagina 68)
- Administrarea în siguranță a aparatului de rețea, utilizând IPsec (consultați *Administrarea în siguranță a aparatului de rețea, utilizând IPsec* la pagina 71)
- Restricționarea funcției de scanare de la dispozitive externe (consultați *Restricționarea funcțiilor de scanare de la dispozitive externe* la pagina 83)
- Blocarea securizată a funcțiilor 3.0 (consultați *Blocarea securizată a funcțiilor 3.0 (ADS-2800W/ADS-3600W)* la pagina 84)


### NOTĂ

Recomandăm dezactivarea protocoalelor FTP și TFTP. Accesarea aparatului folosind aceste protocoale nu este sigură. Totuși, dacă dezactivați FTP, funcția Scanare către FTP va fi dezactivată. (Pentru mai multe informații despre configurarea setărilor protocolului, consultați *Configurarea setărilor aparatului* la pagina 39.)

## Trimiterea securizată a unui e-mail (ADS-2800W/ADS-3600W)

### Configurarea cu ajutorul administrării bazate pe web

Configurați trimiterea securizată de e-mailuri cu autentificarea utilizatorului sau trimiterea și primirea de e-mailuri folosind SSL/TLS.

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: http://192.168.1.2.
- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi faceți clic pe .
- 4 Faceți clic pe **Network** (Rețea).
- 5 Faceți clic pe **Protocol**.
- 6 Faceți clic pe **Advanced Setting** (Setări avansate) din **SMTP** și asigurați-vă că starea **SMTP** este **Enabled** (Activat).
- 7 Configurați setările **SMTP** din această pagină.

### NOTĂ

- Puteți confirma faptul că setările pentru e-mail sunt corecte prin trimiterea unui e-mail de test după ce configurarea este finalizată.
  - Dacă nu cunoașteți setările serverului SMTP, contactați administratorul de sistem sau furnizorul de servicii de internet (ISP) pentru mai multe informații.
- 8 Când ați terminat, faceți clic pe **Submit** (Trimite). Apare caseta de dialog **Test Send E-mail Configuration** (Configurare e-mail trimitere de probă).
  - 9 Urmați instrucțiunile pas cu pas pentru a efectua testul folosind setările curente.

### Trimiterea unui e-mail folosind autentificarea utilizatorului

Acest aparat prioritizează metodele SMTP-AUTH pentru trimiterea mesajelor de e-mail printr-un server de e-mail care necesită autentificarea utilizatorului. Această metodă împiedică orice utilizatori neautorizați să acceseze serverul de e-mail. Puteți utiliza administrarea bazată pe web sau BRAdmin Professional 3 pentru a configura aceste setări. Puteți utiliza metoda SMTP-AUTH pentru notificare e-mail, rapoarte e-mail și Scanare către server de e-mail.

#### Setări client de e-mail

- Trebuie să potriviți setările metodei de autentificare SMTP cu metoda utilizată de către aplicația de e-mail.
- Contactați administratorul de rețea sau furnizorul de servicii de internet (ISP) cu privire la configurarea clientului de e-mail.
- Trebuie să bifați caseta **SMTP-AUTH** din **Server Authentication Method** (Metodă de autentificare server) pentru a activa autentificarea serverului SMTP.

## Setări SMTP

- Puteți schimba numărul portului SMTP utilizând administrarea bazată pe web. Acest lucru este util dacă furnizorul de servicii internet (ISP) implementează serviciul „Outbound Port 25 Blocking (OP25B)” (Blocarea portului 25 de ieșire).
- Înlocuind numărul portului SMTP cu un anumit număr, folosit de furnizorul de servicii internet (ISP) pentru serverul SMTP (de exemplu portul 587), puteți trimite un e-mail prin serverul SMTP.

## Trimiterea securizată a unui e-mail folosind SSL/TLS

Acest aparat acceptă SSL/TLS pentru trimiterea unui mesaj de e-mail folosind un server de e-mail care necesită comunicație SSL/TLS securizată. Pentru a trimite mesaje de e-mail prin intermediul unui server de e-mail care utilizează comunicarea SSL/TLS, trebuie să configurați corect SSL/TLS.

### Verificarea certificatului serverului

- Dacă ați selectat **SSL** sau **TLS** pentru SSL/TLS, caseta **Verify Server Certificate** (Verificare certificat server) va fi bifată automat pentru a verifica certificatul serverului.
  - Certificatul serverului este verificat în timpul încercării de conectare la server în timpul trimiterii e-mailului.
  - Dacă nu trebuie să verificați certificatul serverului, debifați caseta **Verify Server Certificate** (Verificare certificat server).

### Număr port

- Dacă ați selectat **SSL** sau **TLS**, valoarea selectată pentru **Port** va fi modificată în funcție de protocol. Pentru a modifica manual numărul portului, selectați **SSL/TLS** și apoi introduceți numărul portului.
- Trebuie să configurați metoda de comunicare SMTP în funcție de serverul de e-mail. Pentru detalii despre setările serverului de e-mail, contactați administratorul de rețea sau furnizorul de servicii internet (ISP).  
În majoritatea cazurilor, serviciile securizate de poștă electronică web necesită următoarele setări:

## SMTP

**Port:** 587

**Server Authentication Method** (Metodă de autentificare server): SMTP-AUTH

**SSL/TLS:** TLS

## Setări de securitate pentru SFTP

Puteți configura setările cheii de securitate pentru conexiunea SFTP.

### Crearea unei Asocieri de chei client

---

Asocierea de chei client este creată pentru stabilirea unei conexiuni SFTP.

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: `http://192.168.1.2`.

### NOTĂ

---

- Dacă utilizați un Sistem nume domeniu (DNS) sau activați o denumire NetBIOS, puteți introduce în locul adresei IP un alt nume, de exemplu „ScannerPartajat”.

- De exemplu:

`http://ScannerPartajat/`


De asemenea, dacă activați o denumire NetBIOS, puteți utiliza numele nodului.

- De exemplu:

`http://brnxxxxxxxxxxxxx/`

Denumirea NetBIOS poate fi vizualizată în Raportul de configurare a rețelei.

---

- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi apăsați .
- 4 Faceți clic pe fila **Network** (Rețea).
- 5 Faceți clic pe fila **Security** (Securitate).
- 6 Faceți clic pe **Client Key Pair** (Asociere chei client) din bara de navigare din stânga.
- 7 Faceți clic pe **Create New Client Key Pair** (Creare Asociere chei client nouă).
- 8 În câmpul **Client Key Pair Name** (Denumire asociere chei client), introduceți denumirea dorită (până la 20 de caractere).
- 9 Faceți clic pe lista derulantă **Public Key Algorithm** (Algoritmul cheii publice) și apoi selectați algoritmul dorit.
- 10 Faceți clic pe **Submit** (Trimitere).  
Asocierea de chei client este creată și salvată în memoria aparatului dvs. Denumirea asocierii de chei client și algoritmul cheii publice apar în **Client Key Pair List** (Listă asociere chei client).

## Exportarea unei Asocieri de chei client

---

Asocierea de chei client este utilizată pentru stabilirea unei conexiuni SFTP, când este selectată cheia publică drept protocol de autentificare.

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: `http://192.168.1.2`.

### NOTĂ

---

- Dacă utilizați un Sistem nume domeniu (DNS) sau activați o denumire NetBIOS, puteți introduce în locul adresei IP un alt nume, de exemplu „ScannerPartajat”.

- De exemplu:

`http://ScannerPartajat/`


De asemenea, dacă activați o denumire NetBIOS, puteți utiliza numele nodului.

- De exemplu:

`http://brnxxxxxxxxxxxxx/`

Denumirea NetBIOS poate fi vizualizată în Raportul de configurare a rețelei.

---

- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi apăsați .
- 4 Faceți clic pe fila **Network** (Rețea).
- 5 Faceți clic pe fila **Security** (Securitate).
- 6 Faceți clic pe **Client Key Pair** (Asociere chei client) din bara de navigare din stânga.
- 7 Faceți clic pe **Export Public Key** (Exportare cheie publică) prezentată în **Client Key Pair List** (Listă asociere chei client).
- 8 Faceți clic pe **Submit** (Trimitere).
- 9 Specificați locația în care doriți să salvați fișierul.

Asocierea de chei client este exportată în calculatorul dvs.

## Importarea unei Chei publice a serverului

---

Cheia publică a serverului este utilizată pentru stabilirea unei conexiuni SFTP, când se folosește scanarea către SFTP.

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: `http://192.168.1.2`.

### NOTĂ

---

- Dacă utilizați un Sistem nume domeniu (DNS) sau activați o denumire NetBIOS, puteți introduce în locul adresei IP un alt nume, de exemplu „ScannerPartajat”.

- De exemplu:

`http://ScannerPartajat/`


De asemenea, dacă activați o denumire NetBIOS, puteți utiliza numele nodului.

- De exemplu:

`http://brnxxxxxxxxxxxxx/`

Denumirea NetBIOS poate fi vizualizată în Raportul de configurare a rețelei.

---

- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi apăsați .
- 4 Faceți clic pe fila **Network** (Rețea).
- 5 Faceți clic pe fila **Security** (Securitate).
- 6 Faceți clic pe **Server Public Key** (Cheie publică server) din bara de navigare din stânga.
- 7 Faceți clic pe **Import Public Key** (Importare cheie publică) prezentată în **Server Public Key List** (Listă chei publice server).
- 8 Specificați fișierul pe care doriți să îl importați.
- 9 Faceți clic pe **Submit** (Trimitere).

Cheia publică a serverului este importată în aparatul dvs.



## Gestionare certificate multiple

Funcția de gestionare a mai multor certificate vă permite să utilizați administrarea bazată pe web pentru a gestiona fiecare certificat instalat pe aparat. În administrarea bazată pe web, navigați la ecranul **CA Certificate** (Certificat CA) pentru a vizualiza conținutul certificatelor, a șterge sau a exporta certificatele.

Puteți memora până la trei certificate CA pentru a utiliza SSL.

Vă recomandăm să memorați cu un certificat mai puțin decât numărul permis, rezervând astfel un loc liber în cazul expirării unui certificat. Când un certificat expiră, importați un certificat nou în locul liber și apoi ștergeți certificatul expirat. Astfel vă asigurați că evitați problemele de configurare.

### NOTĂ

Când utilizați comunicarea SSL pentru SMTP, nu trebuie să selectați un certificat. Certificatul necesar este selectat automat.

## Importarea unui certificat CA

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: `http://192.168.1.2`.

### NOTĂ

- Dacă utilizați un Sistem nume domeniu (DNS) sau activați o denumire NetBIOS, puteți introduce în locul adresei IP un alt nume, de exemplu „ScannerPartajat”.

- De exemplu:


`http://ScannerPartajat/`

De asemenea, dacă activați o denumire NetBIOS, puteți utiliza numele nodului.

- De exemplu:

`http://brwxxxxxxxxxxxxx/`

Puteți găsi denumirea NetBIOS în panoul de control al aparatului, la `Nume Nod`.

- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi faceți clic pe .
- 4 Faceți clic pe fila **Network** (Rețea) și apoi faceți clic pe **Security** (Securitate).
- 5 Faceți clic pe **CA Certificate** (Certificat CA).
- 6 Faceți clic pe **Import CA Certificate** (Importare certificat CA) și selectați certificatul.
- 7 Faceți clic pe **Submit** (Trimitere).

## Exportarea unui certificat CA

---

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: `http://192.168.1.2`.

### NOTĂ

---

- Dacă utilizați un Sistem nume domeniu (DNS) sau activați o denumire NetBIOS, puteți introduce în locul adresei IP un alt nume, de exemplu „ScannerPartajat”.

- De exemplu:

`http://ScannerPartajat/`


De asemenea, dacă activați o denumire NetBIOS, puteți utiliza numele nodului.

- De exemplu:

`http://brwxxxxxxxxxxxxx/`

Puteți găsi denumirea NetBIOS în panoul de control al aparatului, la `Nume Nod`.

---

- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi faceți clic pe .
- 4 Faceți clic pe fila **Network** (Rețea) și apoi faceți clic pe **Security** (Securitate).
- 5 Faceți clic pe **CA Certificate** (Certificat CA).
- 6 Selectați certificatul pe care doriți să îl exportați și faceți clic pe **Export**.
- 7 Faceți clic pe **Submit** (Trimitere).

## Administrarea în siguranță a aparatului de rețea, utilizând IPsec

### ■ Introducere în IPsec

IPsec (Securitate protocol internet) este un protocol de securitate care utilizează o funcție opțională a Protocolului Internet, pentru prevenirea manipulării datelor și asigurarea confidențialității datelor transmise ca pachete IP. IPsec criptează datele transmise în rețea. Deoarece datele sunt criptate la nivel de rețea, aplicațiile care folosesc un protocol de nivel mai înalt utilizează IPsec chiar dacă utilizatorul nu este înștiințat despre utilizarea sa.

### ■ Configurarea IPsec utilizând administrarea bazată pe web

Condițiile de conectare IPsec constau în două tipuri de **Template** (șabloane): **Address** (Adresă) și **IPsec**. Puteți seta până la 10 condiții de conectare.

### ■ Configurarea unui Șablon de adresă IPsec utilizând administrarea bazată pe web

### ■ Configurarea unui șablon IPsec utilizând administrarea bazată pe web

6

## Introducere în IPsec

---

IPsec acceptă următoarele funcții:

### ■ Transmisii IPsec

Conform condițiilor de configurare IPsec, computerul conectat la rețea transmite date și primește date de la dispozitivul specificat, utilizând IPsec. După ce dispozitivele încep să comunice utilizând IPsec, cheile se schimbă utilizând mai întâi Internet Key Exchange (Schimb chei Internet) (IKE), apoi datele criptate sunt transmise cu ajutorul cheilor.

În plus, IPsec are două moduri de operare: modul Transport și modul Tunel. Modul Transport este utilizat în principiu pentru comunicarea realizată între dispozitive, iar modul Tunel este utilizat în medii precum Rețele virtuale private (VPN).

## NOTĂ

---

Pentru transmisii IPsec sunt necesare următoarele condiții:

- Un calculator care poate comunica utilizând IPsec este conectat la rețea.
- Aparatul Brother este configurat pentru comunicarea IPsec.
- Calculatorul conectat la aparatul Brother este configurat pentru conexiuni IPsec.

### ■ Setări IPsec

Setările necesare pentru efectuarea conexiunilor cu ajutorul IPsec. Aceste setări pot fi configurate utilizând administrarea bazată pe web.

## NOTĂ


---

Pentru configurarea setărilor IPsec, trebuie să utilizați browserul din calculatorul conectat la rețea.


---

## Configurarea IPsec utilizând administrarea bazată pe web

Condițiile de conectare IPsec constau în două tipuri de **Template** (șabloane): **Address** (Adresă) și **IPsec**. Puteți seta până la 10 condiții de conectare.

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: http://192.168.1.2.
- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi faceți clic pe .
- 4 Faceți clic pe fila **Network** (Rețea).
- 5 Faceți clic pe fila **Security** (Securitate).
- 6 Faceți clic pe meniul **IPsec** din bara de navigare din stânga.
- 7 În câmpul **Status** (Stare), activați sau dezactivați IPsec.
- 8 Selectați **Negotiation Mode** (Mod negociere) pentru IKE Faza 1.  
IKE este un protocol utilizat pentru schimbarea cheilor de criptare, în scopul efectuării comunicării criptate cu ajutorul IPsec.  
În modul **Main** (Principal), viteza de procesare este mică, dar nivelul de securitate este mare. În modul **Aggressive** (Agresiv), viteza de procesare este mai mare decât în modul **Main** (Principal), dar nivelul de securitate este mai mic.
- 9 În câmpul **All Non-IPsec Traffic** (Tot traficul non-IPsec), selectați acțiunea pe care urmează să o întreprindeți pentru pachetele non-IPsec.  
Când utilizați servicii web, trebuie să selectați **Allow** (Permitere) pentru **All Non-IPsec Traffic** (Tot traficul non-IPsec). Dacă ați selectat **Drop** (Eliminare), serviciile web nu pot fi utilizate.
- 10 În câmpul **Broadcast/Multicast Bypass** (Bypass transmisie/transmisie multipunct), selectați **Enabled** (Activat) sau **Disabled** (Dezactivat).
- 11 În câmpul **Protocol Bypass** (Bypass protocol), selectați caseta de verificare pentru opțiune/opțiunile dorite.
- 12 În tabelul **Rules** (Reguli), selectați caseta de verificare **Enabled** (Activat) pentru a activa șablonul.  
Dacă selectați mai multe casete de verificare, cele cu numere mai mici au prioritate dacă setările pentru casetele de verificare selectate sunt în conflict.
- 13 Faceți clic pe lista derulantă corespunzătoare, pentru a selecta **Address Template** (Șablon de adresă) utilizat pentru condițiile de conectare IPsec.  
Pentru a adăuga un **Address Template** (șablon de adresă), faceți clic pe **Add Template** (Adăugare șablon).
- 14 Faceți clic pe lista derulantă corespunzătoare, pentru a selecta **IPsec Template** (Șablon IPsec) utilizat pentru condițiile de conectare IPsec.  
Pentru a adăuga un **IPsec Template** (Șablon IPsec), faceți clic pe **Add Template** (Adăugare șablon).
- 15 Faceți clic pe **Submit** (Trimitere).  
Dacă trebuie repornit calculatorul pentru a înregistra noile setări, este afișat ecranul de confirmare a repornirii. Dacă există un element liber în șablonul pe care l-ați activat în tabelul **Rules** (Reguli), apare un mesaj de eroare.  
Confirmați alegerile și trimiteți din nou.

## Configurarea unui Șablon de adresă IPsec utilizând administrarea bazată pe web

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: http://192.168.1.2.
- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi faceți clic pe .
- 4 Faceți clic pe fila **Network** (Rețea).
- 5 Faceți clic pe fila **Security** (Securitate).
- 6 Faceți clic pe meniul **IPsec Address Template** (Șablon de adresă IPsec) din bara de navigare din stânga. Apare lista șabloanelor, afișând 10 șabloane de adrese. Faceți clic pe butonul **Delete** (Ștergere) pentru a șterge un **Address Template** (Șablon de adresă). Când un **Address Template** (Șablon de adresă) este în uz, nu poate fi șters.
- 7 Faceți clic pe **Address Template** (Șablon de adresă), pe care doriți să-l creați. Apare **IPsec Address Template** (Șablon de adresă IPsec).
- 8 În câmpul **Template Name** (Nume șablon), introduceți un nume pentru șablon (până la 16 caractere).
- 9 Selectați o opțiune **Local IP Address** (Adresă locală IP) pentru specificarea condițiilor de afișare a adresei IP pentru expeditor:
  - **IP Address** (Adresa IP)
 

Specificați adresa IP. Selectați **ALL IPv4 Address** (Adresa ALL IPv4), **ALL IPv6 Address** (Adresa ALL IPv6), **All Link Local IPv6** (IPv6 pentru orice legătură), sau **Custom** (Personalizat) din lista derulantă.

Dacă ați selectat **Custom** (Personalizat) din lista derulantă, introduceți adresa IP specificată (IPv4 sau IPv6) în caseta de text.
  - **IP Address Range** (Interval de adrese IP)
 

Introduceți adresele IP de început și de sfârșit, pentru intervalul de adrese IP din casetele de text. Dacă adresele IP de început și de sfârșit nu sunt standardizate conform formatului IPv4 sau IPv6, sau adresa IP de sfârșit este mai scurtă decât adresa de început, va apărea o eroare.
  - **IP Address / Prefix** (Adresă IP/Prefix)
 

Specificați adresa IP utilizând sistemul de notare CIDR.

De exemplu: 192.168.1.1/24

Deoarece prefixul este specificat sub forma unei măști de subrețea de 24-bit (255.255.255.0) pentru 192.168.1.1, adresele 192.168.1.xxx sunt valide.
- 10 Selectați o opțiune **Remote IP Address** (Adresă IP la distanță) pentru specificarea condițiilor de afișare a adresei IP pentru destinatar:
  - **Any** (Oricare)
 

Activează toate adresele IP.

■ **IP Address** (Adresa IP)

Vă permite să introduceți adresa IP specificată (IPv4 sau IPv6) în caseta de text.

■ **IP Address Range** (Interval de adrese IP)

Vă permite să introduceți adresele IP de început și de sfârșit, pentru intervalul de adrese IP. Dacă adresele IP de început și de sfârșit nu sunt standardizate conform IPv4 sau IPv6, sau adresa IP de sfârșit este mai scurtă decât adresa de început, va apărea o eroare.

■ **IP Address / Prefix** (Adresă IP/Prefix)

Specificați adresa IP utilizând sistemul de notare CIDR.

De exemplu: 192.168.1.1/24


Deoarece prefixul este specificat sub forma unei măști de subrețea de 24-bit (255.255.255.0) pentru 192.168.1.1, adresele 192.168.1.xxx sunt valide.

11 Faceți clic pe **Submit** (Trimitere).

## NOTĂ

Când modificați setările pentru șablonul în uz, ecranul IPsec din administrarea bazată pe web se închide și se redeschide.

## Configurarea unui șablon IPsec utilizând administrarea bazată pe web

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: http://192.168.1.2.
- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi faceți clic pe .
- 4 Faceți clic pe fila **Network** (Rețea).
- 5 Faceți clic pe fila **Security** (Securitate).
- 6 Faceți clic pe meniul **IPsec Template** (Șablon IPsec) din bara de navigare din stânga. Apare lista șabloanelor, afișând 10 șabloane IPsec. Faceți clic pe butonul **Delete** (Ștergere) pentru a șterge un **IPsec Template** (Șablon IPsec). Când un **IPsec Template** (Șablon IPsec) este în uz, nu poate fi șters.
- 7 Faceți clic pe **IPsec Template** (Șablon IPsec), pe care doriți să-l creați. Apare ecranul **IPsec Template** (Șablon IPsec). Câmpurile de configurare diferă în funcție de opțiunile selectate pentru **Use Prefixed Template** (Utilizare șablon cu prefix) și **Internet Key Exchange (IKE)** (Schimb chei Internet).
- 8 În câmpul **Template Name** (Nume șablon), introduceți un nume pentru șablon (până la 16 caractere).
- 9 Selectați opțiunile **Internet Key Exchange (IKE)** (Schimb chei Internet).
- 10 Faceți clic pe **Submit** (Trimitere).

## Setările IKEv1 pentru un șablon IPsec

### Template Name (Nume șablon)

Introduceți un nume pentru șablon (până la 16 caractere).

### Use Prefixed Template (Utilizare șablon cu prefix)

Selecționați **Custom** (Personalizat), **IKEv1 High Security** (Securitate ridicată IKEv1), **IKEv1 Medium Security** (Securitate medie IKEv1), **IKEv2 High Security** (Securitate ridicată IKEv2) sau **IKEv2 Medium Security** (Securitate medie IKEv2). Elementele setării diferă în funcție de șablonul selectat.

### NOTĂ

Șablonul implicit poate fi diferit dacă ați selectat **Main** (Principal) sau **Aggressive** (Agresiv) pentru **Negotiation Mode** (Mod de negociere) de pe ecranul de configurare IPsec.

### Internet Key Exchange (IKE) (Schimb de chei Internet (IKE))

IKE este un protocol de comunicare utilizat pentru schimbarea cheilor de criptare, în scopul efectuării comunicării criptate cu ajutorul IPsec. Pentru a efectua comunicarea criptată doar de această dată, este stabilit algoritmul de criptare necesar pentru IPsec și sunt partajate cheile de criptare. Pentru IKE, cheile de criptare sunt schimbate utilizând metoda de schimbare chei Diffie-Hellman și este efectuată comunicarea criptată, limitată la IKE.

Dacă ați selectat **Custom** (Personalizat) în **Use Prefixed Template** (Utilizare șablon cu prefix), selecționați **IKEv1**, **IKEv2**, sau **Manual** (Manual). Dacă ați selectat o setare diferită de **Custom** (Personalizat), se vor afișa IKE, tipul de autentificare și securitatea capsulării selectate în **Use Prefixed Template** (Utilizare șablon cu prefix).

### Authentication Type (Tip de autentificare)

Configurați autentificarea și criptarea IKE.

#### ■ Diffie-Hellman Group (Grupul Diffie-Hellman)

Această metodă de schimbare a cheilor permite cheilor secrete să fie schimbate în siguranță pe o rețea neprotejată. Metoda de schimbare a cheilor Diffie-Hellman utilizează o problemă cu logaritmi discreți, și nu cheia secretă, pentru trimiterea și primirea informațiilor generate cu ajutorul unui număr oarecare și cheii secrete.

Selecționați **Group1** (Grup 1), **Group2** (Grup 2), **Group5** (Grup 5), sau **Group14** (Grup 14).

#### ■ Encryption (Criptare)

Selecționați **DES**, **3DES**, **AES-CBC 128**, sau **AES-CBC 256**.

#### ■ Hash

Selecționați **MD5**, **SHA1**, **SHA256**, **SHA384** sau **SHA512**.

#### ■ SA Lifetime (Durata de viață SA)

Specificați durata de viață SA a IKE.

Introduceți timpul (secunde) și numărul de kilobiți (KByte).

### Encapsulating Security (Securitate capsulare)

#### ■ Protocol

Selecționați **ESP**, **AH+ESP** sau **AH**.

## NOTĂ

- ESP este un protocol utilizat pentru efectuarea comunicării criptate cu ajutorul IPsec. ESP criptează sarcina (conținutul comunicat) și adaugă informații suplimentare. Pachetul IP constă în antet și sarcina criptată, care urmează după antet. Pe lângă datele criptate, pachetul IP conține și informații referitoare la metoda de criptare și cheia de criptare, datele de autentificare și altele.
- AH (Antetul de autentificare) face parte din protocolul IPsec, care autentifică expeditorul și împiedică manipularea datelor (asigură caracterul complet al datelor). În pachetul IP, datele sunt introduse imediat după antet. În plus, pachetele includ valorile hash, care sunt calculate utilizând o ecuație din conținutul comunicat, cheia secretă și așa mai departe, pentru a împiedica falsificarea expeditorului și manipularea datelor. Spre deosebire de ESP, conținutul comunicat nu este criptat, iar datele sunt trimise și primite ca text întreg.

### ■ Encryption (Criptare)

Selectați **DES**, **3DES**, **AES-CBC 128**, sau **AES-CBC 256**. Criptarea poate fi selectată doar atunci când este selectat **ESP** în **Protocol**.

### ■ Hash

Selectați **None** (Nimic), **MD5**, **SHA1**, **SHA256**, **SHA384**, sau **SHA512**.

**None** (Nimic) poate fi selectat doar atunci când este selectat **ESP** în **Protocol**.

Când este selectat **AH+ESP** în **Protocol** (Protocol), selectați fiecare protocol pentru **Hash(AH)** și **Hash(ESP)**.

### ■ SA Lifetime (Durata de viață SA)

Specificați durata de viață SA a IPsec.

Introduceți timpul (secunde) și numărul de kilobiți (KByte).

### ■ Encapsulation Mode (Mod de capsulare)

Selectați **Transport** (Transport) sau **Tunnel** (Tunel).

### ■ Remote Router IP-Address (Adresa IP a routerului la distanță)

Specificați adresa IP (IPv4 sau IPv6) a routerului la distanță. Introduceți aceste informații doar dacă este selectat modul **Tunnel** (Tunel).

## NOTĂ

SA (Security Association) (Asociere securitate) este o metodă de comunicare criptată, care utilizează IPsec sau IPv6 și face schimb de informații, precum metoda de criptare și cheia de criptare, pentru stabilirea unui canal securizat de comunicare înainte de a începe comunicarea. SA se poate referi și la un canal criptat de comunicare virtuală creat deja. SA utilizat pentru IPsec stabilește metoda de criptare, schimbă cheile și efectuează autentificarea reciprocă, în funcție de procedura standard IKE (Schimb chei Internet). În plus, SA este actualizat periodic.

### Perfect Forward Secrecy (PFS) (Confidențialitate perfectă în expedierea mesajelor)

PFS nu derivă chei din cheile precedente, care au fost utilizate pentru criptarea mesajelor. În plus, dacă o cheie utilizată pentru criptarea unui mesaj a fost derivată dintr-o cheie-părinte, acea cheie-părinte nu este utilizată pentru derivarea altor chei. Astfel, chiar dacă este compromisă o cheie, dauna se limitează doar la mesajele care au fost criptate utilizând acea cheie.

Selectați **Enabled** (Activat) sau **Disabled** (Dezactivat).



### Authentication Method (Metodă de autentificare)

Selectați metoda de autentificare. Selectați **Pre-Shared Key** (Cheie pre-partajată) sau **Certificates** (CertIFICATE).

#### Pre-Shared Key (Cheie pre-partajată)

Dacă se criptează comunicarea, cheia de criptare este schimbată și partajată înainte de a utiliza alt canal.

Dacă ați selectat **Pre-Shared Key** (Cheie pre-partajată) pentru **Authentication Method** (Metoda de autentificare), introduceți **Pre-Shared Key** (Cheie pre-partajată) (până la 32 caractere).

##### ■ Local ID Type/ID (Tip ID local/ID)

Selectați tipul ID al expeditorului, apoi introduceți ID-ul.

Pentru tip, selectați **IPv4 Address** (Adresa IPv4), **IPv6 Address** (Adresa IPv6), **FQDN**, **E-mail Address** (Adresa de e-mail) sau **Certificate** (Certificat). Dacă ați selectat **Certificate** (Certificat), introduceți numele obișnuit al certificatului în câmpul **ID**.

##### ■ Remote ID Type/ID (Tip ID la distanță/ID)

Selectați tipul ID al destinatarului, apoi introduceți ID-ul.

Pentru tip, selectați **IPv4 Address** (Adresa IPv4), **IPv6 Address** (Adresa IPv6), **FQDN**, **E-mail Address** (Adresa de e-mail) sau **Certificate** (Certificat). Dacă ați selectat **Certificate** (Certificat), introduceți numele obișnuit al certificatului în câmpul **ID**.

#### Certificate (Certificat)

Dacă ați selectat **Certificates** (CertIFICATE) pentru **Authentication Method** (Metoda de autentificare), selectați certificatul.

### NOTĂ

Puteți selecta doar certificatele care au fost create utilizând pagina **Certificate** (Certificat) de pe ecranul de configurare Securitate a administrării bazate pe web.

## Setările IKEv2 pentru un șablon IPsec

### Template Name (Nume șablon)

Introduceți un nume pentru șablon (până la 16 caractere).

### Use Prefixed Template (Utilizare șablon cu prefix)

Selectați **Custom** (Personalizat), **IKEv1 High Security** (Securitate ridicată IKEv1), **IKEv1 Medium Security** (Securitate medie IKEv1), **IKEv2 High Security** (Securitate ridicată IKEv2) sau **IKEv2 Medium Security** (Securitate medie IKEv2). Elementele setării diferă în funcție de șablonul selectat.

### NOTĂ

Șablonul implicit poate fi diferit dacă ați selectat **Main** (Principal) sau **Aggressive** (Agresiv) pentru **Negotiation Mode** (Mod de negociere) de pe ecranul de configurare **IPsec**.

## Internet Key Exchange (IKE) (Schimb de chei Internet (IKE))

IKE este un protocol de comunicare utilizat pentru schimbarea cheilor de criptare, în scopul efectuării comunicării criptate cu ajutorul IPsec. Pentru a efectua comunicarea criptată doar de această dată, este stabilit algoritmul de criptare necesar pentru IPsec și sunt partajate cheile de criptare. Pentru IKE, cheile de criptare sunt schimbate utilizând metoda de schimbare chei Diffie-Hellman și este efectuată comunicarea criptată, limitată la IKE.

Dacă ați selectat **Custom** (Personalizat) în **Use Prefixed Template** (Utilizare șablon cu prefix), selectați **IKEv1**, **IKEv2**, sau **Manual** (Manual).

Dacă ați selectat o setare diferită de **Custom** (Personalizat), se vor afișa IKE, tipul de autentificare și securitatea capsulării selectate în **Use Prefixed Template** (Utilizare șablon cu prefix).

### Authentication Type (Tip de autentificare)

Configurați autentificarea și criptarea IKE.

#### ■ Diffie-Hellman Group (Grupul Diffie-Hellman)

Această metodă de schimbare a cheilor permite cheilor secrete să fie schimbate în siguranță pe o rețea neprotejată. Metoda de schimbare a cheilor Diffie-Hellman utilizează o problemă cu logaritmi discreți, și nu cheia secretă, pentru trimiterea și primirea informațiilor generate cu ajutorul unui număr oarecare și cheii secrete.

Selectați **Group1** (Grup 1), **Group2** (Grup 2), **Group5** (Grup 5), sau **Group14** (Grup 14).

#### ■ Encryption (Criptare)

Selectați **DES**, **3DES**, **AES-CBC 128**, sau **AES-CBC 256**.

#### ■ Hash

Selectați **MD5**, **SHA1**, **SHA256**, **SHA384** sau **SHA512**.

#### ■ SA Lifetime (Durata de viață SA)

Specificați durata de viață SA a IKE.

Introduceți timpul (secunde) și numărul de kilobiți (KByte).

### Encapsulating Security (Securitate capsulare)

#### ■ Protocol

Selectați **ESP**.

## NOTĂ

ESP este un protocol utilizat pentru efectuarea comunicării criptate cu ajutorul IPsec. ESP criptează sarcina (conținutul comunicat) și adaugă informații suplimentare. Pachetul IP constă în antet și sarcina criptată, care urmează după antet. Pe lângă datele criptate, pachetul IP conține și informații referitoare la metoda de criptare și cheia de criptare, datele de autentificare și altele.

#### ■ Encryption (Criptare)

Selectați **DES**, **3DES**, **AES-CBC 128**, sau **AES-CBC 256**.

#### ■ Hash

Selectați **MD5**, **SHA1**, **SHA256**, **SHA384**, sau **SHA512**.

#### ■ SA Lifetime (Durata de viață SA)

Specificați durata de viață SA a IPsec.

Introduceți timpul (secunde) și numărul de kilobiți (KByte).

■ **Encapsulation Mode** (Mod de capsulare)

Selectați **Transport** (Transport) sau **Tunnel** (Tunel).

■ **Remote Router IP-Address** (Adresa IP a routerului la distanță)

Specificați adresa IP (IPv4 sau IPv6) a routerului la distanță. Introduceți aceste informații doar dacă este selectat modul **Tunnel** (Tunel).

## NOTĂ

SA (Security Association) (Asociere securitate) este o metodă de comunicare criptată, care utilizează IPsec sau IPv6 și face schimb de informații, precum metoda de criptare și cheia de criptare, pentru stabilirea unui canal securizat de comunicare înainte de a începe comunicarea. SA se poate referi și la un canal criptat de comunicare virtuală, care a fost creat. SA utilizat pentru IPsec stabilește metoda de criptare, schimbă cheile și efectuează autentificarea reciprocă, în funcție de procedura standard IKE (Schimb chei Internet). În plus, SA este actualizat periodic.

## Perfect Forward Secrecy (PFS) (Confidențialitate perfectă în expedierea mesajelor)

PFS nu derivă chei din cheile precedente, care au fost utilizate pentru criptarea mesajelor. În plus, dacă o cheie utilizată pentru criptarea unui mesaj a fost derivată dintr-o cheie-părinte, acea cheie-părinte nu este utilizată pentru derivarea altor chei. Astfel, chiar dacă este compromisă o cheie, dauna se limitează doar la mesajele care au fost criptate utilizând acea cheie.

Selectați **Enabled** (Activat) sau **Disabled** (Dezactivat).

## Authentication Method (Metodă de autentificare)

Selectați metoda de autentificare. Selectați **Pre-Shared Key** (Cheie pre-partajată), **Certificates** (Certificate), **EAP - MD5** sau **EAP - MS-CHAPv2**.

### Pre-Shared Key (Cheie pre-partajată)

Dacă se criptează comunicarea, cheia de criptare este schimbată și partajată înainte de a utiliza alt canal.

Dacă ați selectat **Pre-Shared Key** (Cheie pre-partajată) pentru **Authentication Method** (Metoda de autentificare), introduceți **Pre-Shared Key** (Cheie pre-partajată) (până la 32 caractere).

■ **Local ID Type/ID** (Tip ID local/ID)

Selectați tipul ID al expeditorului, apoi introduceți ID-ul.

Pentru tip, selectați **IPv4 Address** (Adresa IPv4), **IPv6 Address** (Adresa IPv6), **FQDN**, **E-mail Address** (Adresa de e-mail) sau **Certificate** (Certificat).

Dacă ați selectat **Certificate** (Certificat), introduceți numele obișnuit al certificatului în câmpul **ID**.

■ **Remote ID Type/ID** (Tip ID la distanță/ID)

Selectați tipul ID al destinatarului, apoi introduceți ID-ul.

Pentru tip, selectați **IPv4 Address** (Adresa IPv4), **IPv6 Address** (Adresa IPv6), **FQDN**, **E-mail Address** (Adresa de e-mail) sau **Certificate** (Certificat).

Dacă ați selectat **Certificate** (Certificat), introduceți numele obișnuit al certificatului în câmpul **ID**.

## Certificate (Certificat)

Dacă ați selectat **Certificates** (Certificate) pentru **Authentication Method** (Metoda de autentificare), selectați certificatul.

## NOTĂ

Puteți selecta doar certificatele care au fost create utilizând pagina **Certificate** (Certificat) de pe ecranul de configurare Securitate a administrării bazate pe web.

## EAP

EAP este un protocol de autentificare care este o extensie a PPP. Atunci când utilizați EAP cu IEEE 802.1x, se folosește o cheie diferită pentru autentificarea utilizatorului în timpul fiecărei sesiuni.

Următoarele setări sunt necesare doar când este selectat **EAP - MD5** sau **EAP - MS-CHAPv2** sau **Authentication Method** (Metoda de autentificare):

■ **Mode** (Mod)

Selectați **Server-Mode** (Mod server) sau **Client-Mode** (Mod client).

■ **Certificate** (Certificat)

Selectați certificatul.

■ **User Name** (Nume utilizator)

Introduceți un nume de utilizator (până la 32 caractere).

■ **Password** (Parolă)

Introduceți o parolă (până la 32 caractere). Parola trebuie introdusă de două ori pentru confirmare.

■ **Certificate** (Certificat)

Apăsați acest buton pentru a trece la ecranul de configurare **Certificate** (Certificat).

## Setările manuale pentru un șablon IPsec

### Template Name (Nume șablon)

Introduceți un nume pentru șablon (până la 16 caractere).

### Use Prefixed Template (Utilizare șablon cu prefix)

Selectați **Custom** (Personalizat), **IKEv1 High Security** (Securitate ridicată IKEv1), **IKEv1 Medium Security** (Securitate medie IKEv1), **IKEv2 High Security** (Securitate ridicată IKEv2) sau **IKEv2 Medium Security** (Securitate medie IKEv2). Setările diferă în funcție de șablonul selectat.

## NOTĂ

Șablonul implicit poate fi diferit dacă ați selectat **Main** (Principal) sau **Aggressive** (Agresiv) pentru **Negotiation Mode** (Mod de negociere) de pe ecranul de configurare **IPsec**.

### Internet Key Exchange (IKE) (Schimb de chei Internet (IKE))

IKE este un protocol de comunicare utilizat pentru schimbarea cheilor de criptare, în scopul efectuării comunicării criptate cu ajutorul IPsec. Pentru a efectua comunicarea criptată doar de această dată, este stabilit algoritmul de criptare necesar pentru IPsec și sunt partajate cheile de criptare. Pentru IKE, cheile de criptare sunt schimbate utilizând metoda de schimbare chei Diffie-Hellman și este efectuată comunicarea criptată, limitată la IKE.

Dacă ați selectat **Custom** (Personalizat) în **Use Prefixed Template** (Utilizare șablon cu prefix), selectați **IKEv1**, **IKEv2**, sau **Manual** (Manual).

Dacă ați selectat o setare diferită de **Custom** (Personalizat), se vor afișa IKE, tipul de autentificare și securitatea capsulării selectate în **Use Prefixed Template** (Utilizare șablon cu prefix).

### Authentication Key (Cheia de autentificare) (ESP, AH)

Specificați cheia utilizată pentru autentificare. Introduceți valorile **In/Out** (Intrare/ieșire).

Aceste setări sunt necesare când este selectat **Custom** (Personalizat) pentru **Use Prefixed Template** (Utilizare șablon cu prefix), **Manual** (Manual) este selectat pentru **IKE**, iar o setare diferită de **None** (Nimic) este selectată pentru **Hash** în secțiunea **Encapsulating Security** (Securitate capsulare).

## NOTĂ

Numărul de caractere pe care îl puteți seta poate fi diferit, în funcție de setarea selectată pentru **Hash** în secțiunea **Encapsulating Security** (Securitate capsulare).

Dacă lungimea cheii de autentificare specificate diferă de algoritmul hash selectat, va apărea o eroare.

- **MD5**: 128 biți (16 baiți)
- **SHA1**: 160 biți (20 baiți)
- **SHA256**: 256 biți (32 baiți)
- **SHA384**: 384 biți (48 baiți)
- **SHA512**: 512 biți (64 baiți)

Dacă specificați cheia în Cod ASCII, scrieți caracterele între ghilimele (").

### Code key (Cheie cod) (ESP)

Specificați cheia utilizată pentru criptare. Introduceți valorile **In/Out** (Intrare/ieșire).

Aceste setări sunt necesare când este selectat **Custom** (Personalizat) în **Use Prefixed Template** (Utilizare șablon cu prefix), **Manual** (Manual) este selectat în **IKE**, iar **ESP** este selectat în **Protocol** din **Encapsulating Security** (Securitate capsulare).

## NOTĂ

Numărul de caractere pe care îl puteți seta poate fi diferit, în funcție de setarea selectată pentru **Encryption** (Criptare) în secțiunea **Encapsulating Security** (Securitate capsulare).

Dacă lungimea cheii de cod specificate diferă de algoritmul de criptare selectat, va apărea o eroare.

- **DES**: 64 biți (8 baiți)
- **3DES**: 192 biți (24 baiți)
- **AES-CBC 128**: 128 biți (16 baiți)
- **AES-CBC 256**: 256 biți (32 baiți)

Dacă specificați cheia în Cod ASCII, scrieți caracterele între ghilimele (").

### SPI

Acești parametri sunt utilizați pentru identificarea informațiilor de securitate. În general, un dispozitiv gazdă conține Asocieri multiple de securitate (SA-uri) pentru o serie de tipuri de comunicare IPsec. Astfel, este necesară identificarea SA aplicabil atunci când se primește un pachet IPsec. Parametrul SPI, care identifică SA, este inclus în Antetul de autentificare (AH) și antetul Sarcinii de securitate capsulare (ESP).

Aceste setări sunt necesare când este selectat **Custom** (Personalizat) pentru **Use Prefixed Template** (Utilizare șablon cu prefix), iar **Manual** (Manual) este selectat pentru **IKE**.

Introduceți valorile **In/Out** (Intrare/ieșire) (3 – 10 caractere).

### Encapsulating Security (Securitate capsulare)

#### ■ Protocol

Selectați **ESP** sau **AH**.

## NOTĂ

- ESP este un protocol utilizat pentru efectuarea comunicării criptate cu ajutorul IPsec. ESP criptează sarcina (conținutul comunicat) și adaugă informații suplimentare. Pachetul IP constă în antet și sarcina criptată, care urmează după antet. Pe lângă datele criptate, pachetul IP conține și informații referitoare la metoda de criptare și cheia de criptare, datele de autentificare și altele.
- AH face parte din protocolul IPsec, care autentifică expeditorul și împiedică manipularea datelor (asigură caracterul complet al datelor). În pachetul IP, datele sunt introduse imediat după antet. În plus, pachetele includ valorile hash, care sunt calculate utilizând o ecuație din conținutul comunicat, cheia secretă și așa mai departe, pentru a împiedica falsificarea expeditorului și manipularea datelor. Spre deosebire de ESP, conținutul comunicat nu este criptat, iar datele sunt trimise și primite ca text întreg.

### ■ Encryption (Criptare)

Selectați **DES**, **3DES**, **AES-CBC 128**, sau **AES-CBC 256**. Criptarea poate fi selectată doar atunci când este selectat **ESP** în **Protocol**.

### ■ Hash

Selectați **None** (Nimic), **MD5**, **SHA1**, **SHA256**, **SHA384**, sau **SHA512**.

**None** (Nimic) poate fi selectat doar atunci când este selectat **ESP** în **Protocol**.

### ■ SA Lifetime (Durata de viață SA)

Specificați durata de viață SA a IKE.

Introduceți timpul (secunde) și numărul de kilobiți (KByte).

### ■ Encapsulation Mode (Mod de capsulare)

Selectați **Transport** (Transport) sau **Tunnel** (Tunel).

### ■ Remote Router IP-Address (Adresa IP a routerului la distanță)

Specificați adresa IP (IPv4 sau IPv6) a destinației conexiunii. Introduceți aceste informații doar dacă este selectat modul **Tunnel** (Tunel).

## NOTĂ

SA (Security Association) (Asociere securitate) este o metodă de comunicare criptată, care utilizează IPsec sau IPv6 și face schimb de informații, precum metoda de criptare și cheia de criptare, pentru stabilirea unui canal securizat de comunicare înainte de a începe comunicarea. SA se poate referi și la un canal criptat de comunicare virtuală, care a fost creat. SA utilizat pentru IPsec stabilește metoda de criptare, schimbă cheile și efectuează autentificarea reciprocă, în funcție de procedura standard IKE (Schimb chei Internet). În plus, SA este actualizat periodic.

### Submit (Trimitere)

Apăsați acest buton pentru înregistrarea setărilor.

## NOTĂ

Când modificați setările pentru șablonul în uz, ecranul IPsec din administrarea bazată pe web se închide și se redeschide.


## Restricționarea funcțiilor de scanare de la dispozitive externe

Această caracteristică vă permite să restricționați funcțiile de scanare de la dispozitive externe.

Când restricționați funcțiile de scanare de la dispozitive externe, pe dispozitiv apare un mesaj de eroare și utilizatorii nu pot utiliza acele funcții de scanare.

### Restricționarea funcțiilor de scanare de la dispozitive externe utilizând setările unui browser web

---

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: `http://192.168.1.2`.
- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi apăsați .
- 4 Faceți clic pe fila **Scan** (Scanare).
- 5 Faceți clic pe meniul **Scan from PC** (Scanare din calculator) din bara de navigare.
- 6 Selectați **Pull Scan** (Extragere scanare) pentru modul dezactivat.
- 7 Faceți clic pe **Submit** (Trimitere).

## Blocarea securizată a funcțiilor 3.0 (ADS-2800W/ADS-3600W)

Blocarea securizată a funcțiilor vă permite să restricționați accesul utilizatorilor la următoarele operațiuni ale aparatului:

- Scanare către PC
- Scanare către FTP/SFTP
- Scanare către rețea
- Scanare către USB
- Scanare către web
- Scanare către serverul de e-mail
- Scanare către SharePoint
- Scanare către WSS (Web Service Scan)
- Aplicații

De asemenea, blocarea securizată a funcțiilor previne schimbarea setărilor implicite ale aparatului de către utilizatori, limitând accesul la setările aparatului.

Înainte de utilizarea caracteristicilor de securitate, trebuie să introduceți mai întâi o parolă de administrator.

Administratorul poate configura restricții pentru utilizatori individuali, împreună cu parola utilizatorului.


Scrieți-vă cu atenție parola. Dacă o uitați, va trebui să resetați parola stocată în aparat. Pentru informații despre resetarea parolei, contactați Centrul de asistență clienți Brother.

### NOTĂ

- Blocarea securizată a funcțiilor poate fi setată utilizând Administrarea bazată pe web sau BRAdmin Professional 3 (doar Windows®).
- Doar administratorii pot seta limitări și efectua modificări pentru fiecare utilizator.
- (Pentru ADS-3600W)  
Utilizați autentificarea prin card pentru comutarea la un utilizator diferit și accesați funcțiile de scanare, precum Scanare către PC, Scanare către FTP sau Scanare către rețea.

### Înainte de a începe să utilizați Blocarea securizată a funcțiilor 3.0

Puteți configura setările Blocarea securizată a funcțiilor utilizând un browser web. Mai întâi, efectuați următoarele:

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: <http://192.168.1.2>.
- 3 Introduceți o parolă de administrator în caseta **Login** (Conectare). (Aceasta este o parolă pentru conectarea la pagina web a aparatului.) Faceți clic pe .



## Pornirea/oprirea Blocarea securizată a funcțiilor

---

- 1 Faceți clic pe **Administrator**.
- 2 Faceți clic pe **User Restriction Function** (Funcție de restricționare utilizatori).
- 3 Selectați **Secure Function Lock** (Blocarea securizată a funcțiilor) sau **Off** (Oprit).
- 4 Faceți clic pe **Submit** (Trimitere).

## Configurarea Blocarea securizată a funcțiilor 3.0 utilizând administrarea bazată pe web

---

Setați grupurile cu restricții și utilizatorii cu parolă și ID card (ID NFC)<sup>1</sup>. Puteți seta până la 100 de grupuri restricționate și 100 de utilizatori. Configurați aceste setări utilizând un browser web. Pentru configurarea paginii web, consultați *Înainte de a începe să utilizați Blocarea securizată a funcțiilor 3.0* la pagina 84 și urmați pașii de mai jos:

<sup>1</sup> Pentru ADS-3600W.

- 1 Faceți clic pe **Administrator**.
- 2 Faceți clic pe **User Restriction Function** (Funcție de restricționare utilizatori).
- 3 Selectați **Secure Function Lock** (Blocarea securizată a funcțiilor).
- 4 Faceți clic pe **Submit** (Trimitere).
- 5 Faceți clic pe **User List xx-xx** (Listă utilizatori xx-xx).
- 6 În câmpul **User List** (Listă utilizatori), introduceți numele utilizatorului, care trebuie să conțină până la 20 de caractere.
- 7 În caseta **PIN Number** (Număr PIN), introduceți o parolă formată din patru cifre.
- 8 (Pentru ADS-3600W)  
În caseta **Card ID** (ID card), introduceți numărul cardului (până la 16 caractere).<sup>1</sup>  
<sup>1</sup> Puteți utiliza numere de la 0 la 9 și litere de la A la F (nu sunt sensibile la litere mari sau mici).
- 9 Selectați **User List / Restricted Functions** (Listă utilizatori/Funcții restricționate) din lista derulantă, pentru fiecare utilizator.
- 10 Faceți clic pe **Submit** (Trimitere).

## Actualizare firmware


Puteți actualiza firmware-ul la cea mai recentă versiune vizitând site-ul Brother.

### NOTĂ

---

Dacă utilizați un server proxy pentru comunicarea pe internet, va trebui să introduceți detaliile în setările Proxy.

---

- 1 Porniți browserul web.
- 2 Pe bara de adrese a browser-ului dvs., introduceți adresa IP a aparatului. Spre exemplu: <http://192.168.1.2>.
- 3 În mod implicit, nu este necesară nicio parolă. Introduceți parola, în cazul în care ați definit o parolă, și apoi apăsați .
- 4 Faceți clic pe fila **Administrator**.
- 5 Faceți clic pe meniul **Firmware Update** (Actualizare firmware) din bara de navigare.
- 6 Faceți clic pe **Check for new firmware** (Căutare firmware nou).

## Prezentare generală

În acest capitol sunt prezentate soluții de rezolvare a problemelor tipice de rețea care apar la folosirea aparatului Brother.

Pentru a descărca alte manuale pentru aparatul dvs., accesați pagina modelului dvs., din Brother Solutions Center, la adresa [solutions.brother.com/manuals](http://solutions.brother.com/manuals)

## Identificarea problemei

Înainte de a citi acest capitol, asigurați-vă că sunt configurate următoarele elemente.

### Asigurați-vă că ați verificat următoarele:

Adaptorul de c.a. este conectat corect și aparatul Brother este pornit.
Punctul de acces, routerul sau hubul este pornit și butonul de conectare luminează intermitent.
Ambalajul de protecție a fost îndepărtat de pe aparat.
Capacul frontal, capacul padului de separare și capacul care protejează rolele de preluare a hârtiei sunt complet închise.

### Mergeți la pagină pentru soluție:

- *Nu pot finaliza configurarea rețelei wireless.* la pagina 88.
- *Coduri de eroare LAN wireless (ADS-2800W/ADS-3600W)* la pagina 89.
- *Aparatul Brother nu este găsit în rețea în timpul instalării dispozitivului Brother* la pagina 91.
- *Aparatul Brother nu poate scana în rețea. Aparatul Brother nu a fost găsit în rețea chiar dacă instalarea s-a finalizat cu succes.* la pagina 92.
- *Utilizez un program software de securitate.* la pagina 94.
- *Doresc să verific dacă dispozitivele de rețea funcționează corect.* la pagina 95.


## Nu pot finaliza configurarea rețelei wireless.

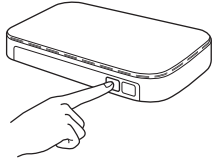
Problemă	Interfață	Soluție
Aparatul nu s-a conectat la rețea în timpul configurării wireless?	wireless	Oprii routerul wireless și apoi porniți-l din nou, după care încercați să configurați din nou setările wireless.
Setările de securitate (SSID/Cheie de rețea) sunt corecte?	wireless	Confirmați setările de securitate. <ul style="list-style-type: none"> <li>■ Numele producătorului sau numărul modelului punctului de acces/routerului WLAN poate fi utilizat ca setare de securitate implicită.</li> <li>■ Consultați instrucțiunile punctului de acces/routerului WLAN pentru informații despre găsirea setărilor de securitate.</li> <li>■ Întrebați producătorul punctului de acces/routerului WLAN, furnizorul de servicii internet (ISP) sau administratorul de rețea.</li> </ul>
Utilizați filtrarea adreselor MAC?	wireless	Confirmați că adresa MAC a aparatului Brother este acceptată de filtru. Puteți găsi adresa MAC utilizând panoul de control al aparatului Brother.
Punctul de acces/routerul WLAN este în modul invizibil (nu se difuzează identificatorul SSID)?	wireless	<ul style="list-style-type: none"> <li>■ Introduceți manual numele SSID corect.</li> <li>■ Verificați numele SSID sau Cheia de rețea în instrucțiunile punctului de acces/routerului WLAN și reconfigurați rețeaua wireless. (Pentru informații suplimentare, consultați <i>Când SSID nu transmite</i> la pagina 11.)</li> </ul>
Am verificat și încercat toate soluțiile de mai sus, însă tot nu pot să finalizez configurarea wireless. Mai pot face și altceva?	wireless	Utilizați Network Connection Repair Tool (Instrumentul de reparare a conexiunii de rețea). Consultați <i>Aparatul Brother nu poate scana în rețea. Aparatul Brother nu a fost găsit în rețea chiar dacă instalarea s-a finalizat cu succes.</i> la pagina 92.
Setările dvs. de securitate (SSID/parolă) nu sunt corecte.	Wi-Fi Direct®	Confirmați SSID și parola. După ce configurați manual rețeaua, SSID și parola se afișează pe ecranul aparatului Brother. Dacă dispozitivul dvs. mobil acceptă configurarea manuală, SSID și parola vor fi afișate pe ecranul dispozitivului mobil.
Utilizați Android™ 4.0.	Wi-Fi Direct®	Dacă dispozitivul mobil se deconectează (la aproximativ șase minute după ce utilizați Wi-Fi Direct®), încercați metoda printr-o singură apăsare, utilizând WPS (recomandat) și setați aparatul Brother în modul G/O.
Aparatul Brother este așezat prea departe de dispozitivul mobil.	Wi-Fi Direct®	Mutați aparatul Brother la o distanță de aproximativ 1 metru față de dispozitivul mobil atunci când configurați setările rețelei Wi-Fi Direct®.
Există unele obstacole (de exemplu, pereți sau mobilier) între aparat și dispozitivul mobil.	Wi-Fi Direct®	Deplasați aparatul Brother într-o zonă fără obstacole.
Există un computer fără fir, un dispozitiv care acceptă Bluetooth, un cuptor cu microunde sau un telefon digital fără fir în apropierea aparatului Brother sau a dispozitivului mobil.	Wi-Fi Direct®	Îndepărtați alte dispozitive de aparatul Brother sau dispozitivul mobil.

Problemă	Interfață	Soluție
Dacă ați verificat și ați încercat tot ceea ce este menționat mai sus, dar nu se poate finaliza totuși configurarea Wi-Fi Direct®, efectuați următoarele operațiuni:	Wi-Fi Direct®	<ul style="list-style-type: none"> <li>■ Opritiți aparatul Brother și reporniți-l. Apoi încercați să configurați din nou setările Wi-Fi Direct®.</li> <li>■ Dacă utilizați aparatul Brother drept client, confirmați numărul de dispozitive permise în rețeaua actuală Wi-Fi Direct®, apoi verificați câte dispozitive sunt conectate.</li> </ul>

### Coduri de eroare LAN wireless (ADS-2800W/ADS-3600W)

Dacă se afișează pe ecranul LCD un cod de eroare, localizați codul în tabel și utilizați soluția recomandată pentru remedierea erorii.

Cod eroare	Setări recomandate
TS-01	<p>Setarea wireless nu este activată.</p> <p>Porniți setarea wireless:</p> <ol style="list-style-type: none"> <li>1 Pe aparat, apăsați  &gt; Rețea &gt; WLAN &gt; Expert setare.</li> <li>2 Când este afișat Activare WLAN?, apăsați Da, pentru a porni expertul de configurare wireless.</li> </ol>
TS-02	<p>Punctul de acces/routerul wireless nu poate fi detectat.</p> <ol style="list-style-type: none"> <li>1 Verificați următoarele: <ul style="list-style-type: none"> <li>■ Asigurați-vă că punctul de acces/routerul wireless este pornit.</li> <li>■ Deplasați aparatul într-o zonă fără obstacole sau mai aproape de punctul de acces/routerul wireless.</li> <li>■ Amplasați temporar aparatul la o distanță de aproximativ 1 metru față de punctul de acces/router wireless, atunci când configurați setările wireless.</li> <li>■ Dacă punctul dvs. de acces/routerul wireless utilizează filtrarea adreselor MAC, confirmați faptul că adresa MAC a aparatului Brother este permisă în filtru.</li> </ul> </li> <li>2 Dacă ați introdus manual SSID și informațiile de securitate (SSID/metoda de autentificare/metoda de criptare/cheia de rețea), informațiile pot fi incorecte.</li> </ol> <p>Confirmați SSID și informațiile de securitate și reintroduceți informațiile corecte, după caz.</p> <p>Acest dispozitiv nu acceptă un SSID/ESSID de 5 GHz și trebuie să selectați un SSID/ESSID de 2,4 GHz. Asigurați-vă că punctul de acces/routerul este setat la modul mixt de 2,4 GHz sau 2,4 GHz/5 GHz.</p>
TS-03	<p>Setările introduse pentru rețeaua wireless și securitate pot fi incorecte.</p> <p>Confirmați setările rețelei wireless.</p> <p>Confirmați faptul că SSID/metoda de autentificare/metoda de criptare/ID utilizator/parola utilizator, introduse sau selectate, sunt corecte.</p>

Cod eroare	Setări recomandate												
<p>TS-04</p>	<p>Metodele de autentificare/criptare utilizate prin punctul de acces/routerul wireless selectat nu sunt acceptate de aparatul dvs.</p> <p>Pentru modul infrastructură, modificați metodele de autentificare și criptare ale punctului de acces/routerului wireless. Aparatul acceptă următoarele metode de autentificare:</p> <table border="1" data-bbox="444 453 1198 751"> <thead> <tr> <th data-bbox="444 453 821 495">Metodă de autentificare</th> <th data-bbox="821 453 1198 495">Metodă de criptare</th> </tr> </thead> <tbody> <tr> <td data-bbox="444 495 821 583" rowspan="2">WPA-Personal</td> <td data-bbox="821 495 1198 537">TKIP</td> </tr> <tr> <td data-bbox="821 537 1198 583">AES</td> </tr> <tr> <td data-bbox="444 583 821 625">WPA2-Personal</td> <td data-bbox="821 583 1198 625">AES</td> </tr> <tr> <td data-bbox="444 625 821 709" rowspan="2">Deschis</td> <td data-bbox="821 625 1198 667">WEP</td> </tr> <tr> <td data-bbox="821 667 1198 709">Nimic (fără criptare)</td> </tr> <tr> <td data-bbox="444 709 821 751">Cheie partajată</td> <td data-bbox="821 709 1198 751">WEP</td> </tr> </tbody> </table> <p>Dacă nu s-a soluționat problema dvs., SSID sau setările rețelei pe care le-ați introdus pot fi incorecte. Confirmați setările rețelei wireless.</p> <p>Pentru modul Ad-hoc, modificați metodele de autentificare și criptare ale computerului dvs. pentru setarea wireless. Aparatul acceptă doar metoda de autentificare Deschisă, cu criptare WEP opțională.</p>	Metodă de autentificare	Metodă de criptare	WPA-Personal	TKIP	AES	WPA2-Personal	AES	Deschis	WEP	Nimic (fără criptare)	Cheie partajată	WEP
Metodă de autentificare	Metodă de criptare												
WPA-Personal	TKIP												
	AES												
WPA2-Personal	AES												
Deschis	WEP												
	Nimic (fără criptare)												
Cheie partajată	WEP												
<p>TS-05</p>	<p>Informația privind securitatea (SSID/cheia rețelei) este incorectă.</p> <p>Confirmați SSID și informațiile de securitate (Cheie de rețea).</p> <p>Dacă routerul dumneavoastră utilizează criptarea WEP, introduceți cheia utilizată ca prima cheie WEP. Aparatul Brother suportă numai utilizarea primei chei WEP.</p>												
<p>TS-06</p>	<p>Informațiile de securitate wireless (metoda de autentificare/metoda de criptare/cheia de rețea) sunt incorecte.</p> <p>Confirmați informațiile de securitate wireless (metoda de autentificare/metoda de criptare/cheia de rețea) cu ajutorul tabelului care prezintă Metoda de autentificare la eroarea TS-04.</p> <p>Dacă routerul dumneavoastră utilizează criptarea WEP, introduceți cheia utilizată ca prima cheie WEP. Aparatul Brother suportă numai utilizarea primei chei WEP.</p>												
<p>TS-07</p>	<p>Aparatul nu poate detecta un punct de acces/router wireless care are WPS activat.</p> <p>Pentru configurarea setărilor wireless cu ajutorul WPS, trebuie să utilizați atât aparatul dvs., cât și punctul de acces/routerul wireless.</p> <p>Dacă nu știți cum să utilizați punctul de acces/routerul wireless cu ajutorul WPS, consultați documentația furnizată pentru punctul de acces/routerul wireless, întrebați producătorul punctului de acces/routerului wireless, sau întrebați administratorul rețelei dvs.</p> 												
<p>TS-08</p>	<p>Sunt detectate două sau mai multe puncte de acces wireless, care au WPS activat.</p> <p>Confirmați dacă numai un punct de acces/router wireless din această gamă are activă metoda WPS și încercați din nou.</p>												
<p>TS-20</p>	<p>Aparatul încearcă încă să se conecteze la rețeaua dvs. wireless. Vă rugăm să așteptați câteva minute și apoi să verificați starea WLAN.</p>												

**Aparatul Brother nu este găsit în rețea în timpul instalării dispozitivului Brother**




Întrebare	Interfață	Soluție
Computerul dvs. este conectat la rețea?	prin cablu/ wireless	Computerul trebuie să fie conectat la o rețea, de exemplu un mediu LAN sau servicii Internet. Pentru asistență, contactați administratorul de rețea.
Aparatul este conectat la rețea și are o adresă IP valabilă?	prin cablu/ wireless	(Rețea cablată) Verificați dacă <i>Status din Stare conex. cablu este XXXX-XX</i> activ. (Unde XXXX-XX este interfața dvs. selectată Ethernet.) Consultați <i>Verificarea stării rețelei (ADS-2800W/ADS-3600W)</i> la pagina 3. Dacă apare mesajul LCD <i>Inactiv sau Prin cablu - DEZACTIVAT</i> , întrebați administratorul rețelei dvs. dacă adresa dvs. IP este valabilă sau nu.  (Rețea wireless) Verificați dacă <i>Status din Status WLAN nu este Eșuare conectare</i> . Consultați <i>Verificarea stării rețelei WLAN (ADS-2800W/ADS-3600W)</i> la pagina 9. Dacă apare mesajul LCD <i>Eșuare conectare</i> , întrebați administratorul rețelei dvs. dacă adresa dvs. IP este valabilă sau nu.
Utilizați un program software de securitate?	prin cablu/ wireless	<ul style="list-style-type: none"> <li>■ În fereastra de dialog a programului de instalare, căutați din nou aparatul Brother.</li> <li>■ Permiteți accesul când mesajul de alertă al software-ului de securitate apare în timpul instalării dispozitivului Brother.</li> <li>■ Pentru informații suplimentare despre programul software de securitate, consultați <i>Utilizez un program software de securitate</i> la pagina 94.</li> </ul>
Utilizați un router Wi-Fi?	wireless	Separatorul de confidențialitate de pe routerul dvs. Wi-Fi poate fi activat. Dezactivați separatorul de confidențialitate.
Aparatul Brother se află prea departe de punctul de acces/routerul WLAN?	wireless	Amplasați aparatul Brother la o distanță de aproximativ 1 metru de punctul de acces/routerul WLAN atunci când configurați setările rețelei wireless.
Între aparat și punctul de acces/routerul WLAN există obstacole (pereți sau mobilier, de exemplu)?	wireless	Deplasați aparatul Brother într-o zonă fără obstacole sau mai aproape de punctul de acces/routerul WLAN.
În apropierea aparatului Brother sau a punctului de acces/routerului WLAN, există un computer fără fir, un dispozitiv Bluetooth, un cuptor cu microunde sau un telefon digital fără fir?	wireless	Îndepărtați toate aceste dispozitive de aparatul Brother sau de punctul de acces/routerul WLAN.

**Aparatul Brother nu poate scana în rețea.**

**Aparatul Brother nu a fost găsit în rețea chiar dacă instalarea s-a finalizat cu succes.**

Întrebare	Interfață	Soluție
Utilizați un program software de securitate?	prin cablu/wireless	Consultați <i>Utilizez un program software de securitate</i> . la pagina 94.
Aparatului dvs. Brother i se alocă o adresă IP disponibilă?	prin cablu/wireless	<ul style="list-style-type: none"> <li>■ Confirmați adresa IP și masca de subrețea Verificați dacă adresele IP și măștile de subrețea ale computerului și ale aparatului Brother sunt corecte și se află în aceeași rețea. Pentru informații suplimentare despre verificarea adresei IP și a măștii de subrețea, adresați-vă administratorului de rețea.</li> <li>■ (Windows®) Confirmați adresa IP și masca de subrețea folosind aplicația Network Connection Repair Tool (Instrumentul de refacere a conexiunii de rețea). Utilizați Instrumentul de reparare a conexiunii de rețea pentru a remedia setările rețelei aparatului Brother (va alocă adresa IP corectă și masca de subrețea). Pentru utilizarea Instrumentului de reparare a conexiunii de rețea, solicitați informațiile necesare administratorului rețelei și apoi urmați pașii de mai jos:</li> </ul> <p><b>NOTĂ</b></p> <ul style="list-style-type: none"> <li>• (Windows® XP) Trebuie să vă conectați cu drepturi de administrator.</li> <li>• Asigurați-vă că aparatul Brother este pornit și conectat la aceeași rețea ca și computerul dumneavoastră.</li> </ul>




Întrebare	Interfață	Soluție
Aparatului dvs. Brother i se alocă o adresă IP disponibilă? (continuare)	prin cablu/ wireless	<p>1 Introduceți DVD-ROM-ul furnizat în unitatea DVD-ROM. Dacă apare meniul principal al DVD-ROM, închideți-l.</p> <p>2 Deschideți directorul computerului pentru sistemul de operare:</p> <ul style="list-style-type: none"> <li>■ Windows® XP Faceți clic pe <b>Start &gt; Toate programele &gt; Accessorii &gt; Windows Explorer &gt; Computerul meu.</b></li> <li>■ Windows Vista®/Windows® 7 Faceți clic pe  (<b>Start</b>) &gt; <b>Computer.</b></li> <li>■ Windows® 8/Windows® 8.1 Faceți clic pe pictograma  (<b>Explorator</b>) din bara de activități și apoi mergeți la <b>Acest computer.</b></li> <li>■ Windows® 10 Faceți clic pe  pictograma (<b>Explorator</b>) din bara de activități și apoi mergeți la <b>Acest PC.</b></li> </ul> <p>3 Faceți dublu clic pe <b>Unitate DVD</b>, dublu clic pe <b>Instrumente</b>, dublu clic pe <b>NetTool</b> și apoi dublu clic pe <b>BrotherNetTool.exe</b> pentru a rula programul.</p> <p><b>NOTĂ</b></p> <p>Dacă apare ecranul <b>Control cont utilizator</b>: (Windows Vista®) Faceți clic pe <b>Continuare (Permite)</b>. (Windows® 7/Windows® 8/Windows® 8.1/Windows® 10) faceți clic pe <b>Da</b>.</p> <p>4 Urmați instrucțiunile de pe ecran.</p> <p>Dacă adresa IP și masca de subrețea nu au fost definite corect nici după ce ați utilizat Network Connection Repair Tool (Instrumentul de reparare a conexiunii de rețea), adresați-vă administratorului de rețea pentru a obține aceste informații.</p>
Conectați aparatul Brother la rețea utilizând funcționalitățile de conectare fără fir?	wireless	<ul style="list-style-type: none"> <li>■ Verificați <i>Status</i> din <i>Status WLAN</i>. Consultați <i>Verificarea stării rețelei WLAN (ADS-2800W/ADS-3600W)</i> la pagina 9. Dacă apare mesajul LCD <i>Eșuare conectare</i>, întrebați administratorul rețelei dvs. dacă adresa dvs. IP este valabilă sau nu.</li> <li>■ Consultați <i>Aparatul Brother nu este găsit în rețea în timpul instalării dispozitivului Brother</i> la pagina 91.</li> </ul>
Am verificat și încercat toate soluțiile de mai sus, dar aparatul Brother nu scanează. Mai pot face și altceva?	prin cablu/ wireless	Dezinstalați și reinstalați dispozitivul Brother.

**Utilizez un program software de securitate.**

Întrebare	Interfață	Soluție
<p>Ați selectat <b>Acceptare</b> în fereastra de dialog de alertă de securitate în timpul instalării dispozitivului Brother, în procesul de pornire a aplicațiilor sau în timpul utilizării funcțiilor de scanare?</p>	<p>prin cablu/wireless</p>	<p>Dacă nu ați selectat <b>Acceptare</b> în caseta de dialog cu mesajul de avertizare, este posibil ca funcția firewall a programului software de securitate să refuze accesul. Anumite programe software de securitate pot să blocheze accesul fără afișarea casetei de dialog care conține mesajul de avertizare. Pentru a permite accesul, consultați instrucțiunile privind software-ul de securitate sau contactați producătorul.</p>
<p>Doresc să știu ce număr de port trebuie definit în setările programului software de securitate.</p>	<p>prin cablu/wireless</p>	<p>Pentru caracteristicile de rețea Brother se utilizează următoarele numere de port:</p> <ul style="list-style-type: none"> <li>■ Scanare în rețea → Număr de port 54925/Protocol UDP</li> <li>■ Scanare în rețea, Configurare de la distanță <sup>1</sup> → Număr de port 161 și 137/Protocol UDP</li> <li>■ BRAdmin Light <sup>1</sup> → Număr de port 161/Protocol UDP</li> </ul> <p><sup>1</sup> Doar Windows®.</p> <p>Pentru informații privind deschiderea portului, consultați instrucțiunile software-ului de securitate sau contactați producătorul.</p>

**Doresc să verific dacă dispozitivele de rețea funcționează corect.**

Întrebare	Interfață	Soluție
Aparatul Brother și punctul de acces/routerul sau hubul de rețea sunt pornite?	prin cablu/wireless	Asigurați-vă că ați confirmat toate instrucțiunile din <i>Asigurați-vă că ați verificat următoarele</i> : la pagina 87.
Unde pot găsi setările de rețea ale aparatului Brother, cum ar fi adresa IP?	prin cablu/wireless	<ul style="list-style-type: none"> <li>■ Pentru administrarea bazată pe web</li> <li>1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).</li> <li>2 Când apare ecranul Administrare bazată pe web, faceți clic pe fila <b>Network</b> (Rețea), apoi faceți clic pe <b>Network Status</b> (Stare rețea) din bara de navigare din partea stângă.</li> <li>■ Pentru Panoul de control (ADS-2800W/ADS-3600W)</li> </ul> <p>Verificați setările din <i>Rețea de pe panoul de control al aparatului</i>.</p>
Cum pot verifica starea conexiunii aparatului Brother?	prin cablu/wireless	<ul style="list-style-type: none"> <li>■ Pentru administrarea bazată pe web</li> <li>1 Lansați administrarea bazată pe web și accesați aparatul Brother (consultați pasul ❶ de la pagina 39).</li> <li>2 Când apare ecranul Administrare bazată pe web, faceți clic pe fila <b>Network</b> (Rețea), apoi faceți clic pe <b>Network Status</b> (Stare rețea) din bara de navigare din partea stângă.</li> <li>■ Pentru Panoul de control (ADS-2800W/ADS-3600W)</li> </ul> <p>(Rețea cablată)          Verificați dacă <i>Status</i> din <i>Stare conex. cablu</i> este <i>XXXX-XX</i> activ (unde <i>XXXX-XX</i> este interfața dvs. selectată Ethernet).          Pentru a verifica starea rețelei: apăsați  &gt; <i>Rețea</i> &gt; <i>Conexiune LAN</i> &gt; <i>Stare conex. cablu</i> &gt; <i>Status</i>.          Dacă apare mesajul LCD <i>Inactiv sau Prin cablu - DEZACTIVAT</i>, întrebați administratorul rețelei dvs. dacă adresa dvs. IP este valabilă sau nu.</p> <p>(Rețea wireless)          Verificați dacă <i>Status</i> din <i>Status WLAN</i> nu este <i>Eșuare conectare</i>.          Consultați <i>Verificarea stării rețelei WLAN (ADS-2800W/ADS-3600W)</i> la pagina 9. Dacă apare mesajul LCD <i>Eșuare conectare</i>, întrebați administratorul rețelei dvs. dacă adresa dvs. IP este valabilă sau nu.</p>

Întrebare	Interfață	Soluție
Puteți „apela” (prin comandă ping) aparatul Brother de la computerul dumneavoastră?	prin cablu/ wireless	<p>Apelați (prin comandă ping) aparatul Brother de la computerul dvs. introducând adresa IP sau numele nodului în linia de comandă a Windows®:</p> <p>ping &lt;adresaip&gt; sau &lt;numenod&gt;.</p> <ul style="list-style-type: none"> <li>■ Realizat cu succes &gt; Aparatul Brother funcționează corespunzător și este conectat la aceeași rețea ca și computerul.</li> <li>■ Eșuat &gt; Aparatul Brother nu este conectat la aceeași rețea ca și computerul. (Windows®) Întrebați administratorul de rețea și utilizați instrumentul de reparare a conexiunii de rețea pentru a corecta automat adresa IP și masca de subrețea. Pentru mai multe informații despre Instrumentul de reparare a conexiunii de rețea, consultați secțiunea <i>Aparatul Brother are atribuită o adresă IP disponibilă?</i> din <i>Aparatul Brother nu poate scana în rețea. Aparatul Brother nu a fost găsit în rețea chiar dacă instalarea s-a finalizat cu succes.</i> la pagina 92.</li> </ul> <p>(Macintosh) Verificați dacă adresa IP și a măștii de subrețea sunt corecte. Consultați secțiunea <i>Confirmare adresă IP și mască de subrețea</i> din <i>Aparatul Brother nu poate scana în rețea. Aparatul Brother nu a fost găsit în rețea chiar dacă instalarea s-a finalizat cu succes.</i> la pagina 92.</p>
Aparatul Brother se conectează la rețeaua wireless?	wireless	<p>Verificați Status din Status WLAN. Consultați <i>Verificarea stării rețelei WLAN (ADS-2800W/ADS-3600W)</i> la pagina 9. Dacă apare mesajul LCD <i>Eșuare conectare</i>, întrebați administratorul rețelei dvs. dacă adresa dvs. IP este valabilă sau nu.</p>
Am verificat și încercat toate soluțiile de mai sus, însă tot am probleme. Mai pot face și altceva?	wireless	<p>Consultați instrucțiunile punctului de acces/routerului WLAN pentru a afla informații despre identificatorul SSID și Cheia de rețea și pentru a le defini corect. Pentru mai multe informații despre SSID și Cheia de rețea, consultați secțiunea <i>Setările de securitate (SSID/Cheie de rețea) sunt corecte?</i> din <i>Nu pot finaliza configurarea rețelei wireless.</i> la pagina 88.</p>

## Tipuri de setări

Sunt disponibile și următoarele caracteristici de rețea opționale:

- Servicii web pentru scanare (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1 și Windows® 10)
- Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1 și Windows® 10)

### NOTĂ




Verificați dacă aparatul și computerul gazdă utilizează aceeași subrețea sau dacă routerul este configurat corect astfel încât datele să fie transmise între cele două dispozitive.

## Instalarea driverelor utilizate pentru scanarea via Servicii web (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)

Caracteristica Servicii web vă permite să monitorizați aparatele din rețea, ceea ce simplifică procesul de instalare a driverelor. Driverelor utilizate pentru scanare folosind Servicii web pot fi instalate făcând clic dreapta pe pictograma scannerului de pe computer, iar portul Servicii web (port WSD) al computerului va fi creat automat. (Pentru informații suplimentare despre scanarea cu ajutorul Serviciilor web, consultați *Scanarea utilizând servicii web (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1 și Windows® 10)* din *Manualul de utilizare*.)

### NOTĂ

Înainte de a configura această setare, trebuie să vă configurați adresa IP a aparatului.

- 1 Deschideți setările de rețea pentru sistemul de operare:
  - Windows Vista®  
Faceți clic pe  (Start) > **Rețea**.
  - Windows® 7  
Faceți clic pe  (Start) > **Panou de control** > **Rețea și Internet** > **Vizualizare computere și dispozitive din rețea**.
  - Windows® 8/Windows® 8.1  
Deplasați mouse-ul în colțul din dreapta jos al spațiului de lucru. Când apare bara de meniu, faceți clic pe **Setări** > **Modificare setări pentru PC** > **Dispozitive** > **Adăugare dispozitiv**.
  - Windows® 10  
Faceți clic pe  (Start) > **Setări** > **Dispozitive** > **Imprimante și scanere**.
- 2 Va fi afișat numele folosit pentru Serviciile web de aparat, împreună cu pictograma scannerului.
  - Windows Vista®/Windows® 7/Windows® 8/Windows® 8.1  
Faceți clic dreapta pe aparatul pe care doriți să îl instalați.
  - Windows® 10  
Faceți clic pe aparatul pe care doriți să îl instalați.

## NOTĂ

---

Numele folosit de aparatul Brother pentru Servicii web este numele modelului dvs. și adresa MAC (adresa Ethernet) (de exemplu Brother ADS-XXXXX (numele modelului) [XXXXXXXXXXXXX] (adresa MAC/adresa Ethernet)).

---

- 3 Începeți instalarea aparatului:
  - Windows Vista®/Windows® 7  
Faceți clic pe **Instalare** în meniul derulant al aparatului.
  - Windows® 8/Windows® 8.1  
Selectați aparatul pe care doriți să îl instalați.
  - Windows® 10  
Faceți clic pe **Adăugare dispozitive**.



## Instalarea scanării în rețea pentru modul Infrastructură în cazul în care utilizați funcția Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)

Windows® Vertical Pairing este o tehnologie care permite aparatului wireless compatibil cu Vertical Pairing să se conecteze la rețeaua de infrastructură utilizând metoda PIN a WPS și caracteristica Servicii web. De asemenea, aceasta permite instalarea driverului scannerului din pictograma scannerului în ecranul **Adăugare dispozitiv**.

Dacă sunteți în modul Infrastructură, puteți conecta aparatul la rețeaua fără fir și apoi instalați driverul scannerului utilizând această caracteristică. Urmați pașii de mai jos:

### NOTĂ

- Dacă ați setat pentru caracteristica Servicii web a aparatului opțiunea Oprit, trebuie să selectați din nou opțiunea Pornit. Setarea implicită pentru Servicii web a aparatului Brother este Pornit. Puteți modifica setarea definită pentru Servicii web utilizând administrarea bazată pe web (browser web) sau BRAdmin Professional 3.
- Asigurați-vă că punctul de acces/routerul WLAN include sigla de compatibilitate Windows® 7, Windows® 8, Windows® 8.1 sau Windows® 10. Dacă nu sunteți sigur în privința siglei de compatibilitate, contactați producătorul routerului/punctului de acces.
- Asigurați-vă că sigla de compatibilitate Windows® 7, Windows® 8, Windows® 8.1 sau Windows® 10 este inclusă de computerul dvs. Dacă nu sunteți sigur în privința siglei de compatibilitate, contactați producătorul computerului.
- În cazul în care configurați rețeaua wireless utilizând o placă externă wireless NIC (Card de interfață de rețea), asigurați-vă că placa wireless NIC include sigla de compatibilitate Windows® 7, Windows® 8, Windows® 8.1 sau Windows® 10. Pentru informații suplimentare, contactați producătorul plăcii fără fir NIC.
- Pentru a utiliza ca registrator un computer pe care este instalat Windows® 7, Windows® 8, Windows® 8.1 sau Windows® 10, acesta trebuie înregistrat în prealabil în rețeaua dvs. Consultați instrucțiunile punctului de acces/routerului WLAN.

- 1 Porniți aparatul.
- 2 Setați aparatul în mod WPS (consultați *Utilizarea metodei PIN a Wi-Fi Protected Setup™ (WPS)* la pagina 19).
- 3 Deschideți meniul „Adăugare dispozitiv” pentru sistemul de operare:
  - Windows® 7  
Faceți clic pe  (Start) > **Dispozitive și imprimante** > **Adăugare dispozitiv**.
  - Windows® 8/Windows® 8.1  
Deplasați mouse-ul în colțul din dreapta jos al spațiului de lucru. Când apare bara de meniu, faceți clic pe **Setări** > **Panou de control** > **Hardware și sunete** > **Dispozitive și imprimante** > **Adăugare dispozitiv**.
  - Windows® 10  
Faceți clic pe  (Start) > **Setări** > **Dispozitive** > **Imprimante și scanere** > **Adăugați o imprimantă sau un scanner**.
- 4 Selectați aparatul dvs. și introduceți codul PIN afișat de aparat.
- 5 Selectați rețeaua de infrastructură la care doriți să vă conectați și apoi faceți clic pe **Următorul**.
- 6 Când aparatul dvs. este afișat în caseta de dialog **Dispozitive și imprimante**, configurarea wireless și instalarea driverului scannerului sunt finalizate cu succes.


## Protocoale și funcții de securitate compatibile

<b>Interfață</b>	Ethernet	10BASE-T, 100BASE-TX
	Wireless (ADS-2800W/ ADS-3600W)	IEEE 802.11b/g/n (Mod infrastructură/Mod ad-hoc) IEEE 802.11g/n (Wi-Fi Direct®)
<b>Rețea (comun)</b>	Protocol (IPv4)	ARP, RARP, BOOTP, DHCP, APIPA (Auto IP), rezoluție denumire WINS/NetBIOS, rezolvitor DNS, mDNS, respondent LLMNR, Custom Raw Port/Port9100, Client SMTP, Client și Server FTP, Client LDAP (doar ADS-2800W/ADS-3600W), Client CIFS, Client WebDAV, SNMPv1/v2c/v3 (MD5/SHA1), server HTTP/HTTPS, client și server TFTP, ICMP, Servicii web (scanare), Client SNTP
	Protocol (IPv6)	NDP, RA, rezolvitor DNS, mDNS, respondent LLMNR, Custom Raw, Port/Port9100, Client SMTP, Client și Server FTP, Client LDAP, Client CIFS, Server TELNET, SNMPv1/v2c/v3, server HTTP/HTTPS, client și server TFTP, ICMPv6, Servicii web (scanare), Client SNTP, Client WebDav
<b>Rețea (securitate)</b>	Prin cablu	SMTP-AUTH, SSL/TLS (HTTPS, SMTP), SSH, SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos, IPsec
	Wireless (ADS-2800W/ ADS-3600W)	SMTP-AUTH, SSL/TLS (HTTPS, SMTP), SSH, SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos, Ipsec
<b>Email (Securitate)</b> (ADS-2800W/ ADS-3600W)	Prin cablu și wireless	SMTP-AUTH, SSL/TLS (SMTP)
<b>Rețea (Wireless)</b> (ADS-2800W/ ADS-3600W)	Certificare wireless	Licență de marcă de certificare Wi-Fi (WPA™/WPA2™ - Enterprise, Personal), Licență de marcă de identificator Wi-Fi Protected Setup™ (WPS), Wi-Fi CERTIFICAT Wi-Fi Direct®



## Tabel funcții administrare bazată pe web

### NOTĂ

Pentru informații suplimentare, faceți clic  în partea dreaptă a fiecărei pagini a interfeței de administrare bazată pe web.

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
General (Informații generale)	-	<b>Status</b> (Stare)	<b>Device Status / Automatic Refresh / Web Language / Device Location</b> (Stare dispozitiv/Reîmprospătare automată/Limbă web/Locație dispozitiv)	Afișare stare, contact și locație dispozitiv. Puteți schimba limba interfeței de administrare bazată pe web.
	-	<b>Auto Refresh Interval</b> (Interval de reîmprospătare automată)	<b>Refresh Interval</b> (Interval de reîmprospătare)	Configurare interval de reîmprospătare (între 15 secunde și 60 de minute).
	-	<b>Maintenance Information</b> (Informații privind întreținerea)	<b>Node Information / Remaining Life / Total Pages Scanned / Replace Count / Reset Count / Error Count / Error History (last 10 errors)</b> (Informații nod/Durată de viață/Număr total de pagini scanate/Înlocuire contor/Resetare contor/Contor erori/Istoric erori (ultimele 10 erori))	Se afișează informațiile despre întreținerea aparatului Brother, inclusiv cele despre model, consumabile, contor de pagini și erori. Faceți clic pe <b>Submit</b> (Trimitere) pentru a converti această pagină cu informații despre întreținere într-un fișier CSV.
	-	<b>Find Device</b> (Găsire dispozitiv)	<b>Node Name / Model Name / Device Status / IP Address</b> (Nume nod/ Nume model/Stare dispozitiv/ Adresă IP)	Afișați toate dispozitivele conectate la rețea.
	-	<b>Contact &amp; Location</b> (Contact și locație)	<b>Contact / Location</b> (Contact/Locație)	După ce configurați aici contactul și locația, acestea pot fi afișate în meniul <b>General</b> (Informații generale) > <b>Status</b> (Stare) > <b>Device Location</b> (Locație dispozitiv).
	-	<b>Sleep Time</b> (Timp de hibernare)	<b>Sleep Time</b> (Timp de hibernare)	Configurarea timpului de hibernare (până la 90 minute).
	-	<b>Auto Power Off</b> (Oprire automată)	<b>Auto Power Off</b> (Oprire automată)	
	-	<b>Volume</b> (Volum)	<b>Beep</b> (Sunet bip)	Configurați volumul sunetului ( <b>Off / Low / Medium / High</b> (Oprit / Mic / Mediu / Mare).

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
<b>General</b> (Informații generale) (continuare)	-	<b>Panel</b> (Panou) (ADS-2800W/ ADS-3600W)	<b>Backlight / Dim Timer</b> (Iluminare de fundal/Temporizator estompere)	
	-	<b>Scheduled Maintenance Alert</b> (Alertă întreținere programată)	<b>Scheduled Maintenance Alert</b> (Alertă întreținere programată)	
<b>Address book</b> (Agendă de adrese) (ADS-2800W/ ADS-3600W)	-	<b>Address</b> (Adresă)	<b>Address / E-mail Address / Name</b> (Adresă/Adresă de e-mail/Nume)	Înregistrați adresa de e-mail și numele (până la 300).
	-	<b>Setup Groups</b> (Grupuri de configurare)	<b>Group / Address / Name / Members</b> (Grup/Adresă/Nume/Membri)	Înregistrați grupul de contacte (până la 20). Selectați <b>Address#</b> (Adresă#) și faceți clic pe <b>Select</b> (Selectare) pentru a configura membrii grupului.
	-	<b>LDAP</b>	<b>LDAP Search / Quick Settings / Advanced Settings</b> (Căutare LDAP/Setări rapide/Setări avansate)	Configurați setările LDAP.
	-	<b>Import</b>	“ <b>Address Book</b> ” data file / “ <b>Group</b> ” data file (Fișierul de date „Agendă de adrese”/Fișierul de date „Grup”)	
	-	<b>Export</b>		
<b>E-mail</b> (ADS-2800W/ ADS-3600W)	-	<b>E-mail Send</b> (Trimitere e-mail)	<b>E-mail Subject / E-mail Message / Size Limit / Request Delivery Notification (Send) / SMTP</b> (Subiect e-mail/Mesaj e-mail/Dimensiune limită/Solicitare notificare de primire (Trimitere)/SMTP)	Configurați setările de trimitere a e-mailurilor, inclusiv subiect, mesaj, dimensiune limită a e-mailului sau notificarea primirii. Faceți clic pe <b>SMTP</b> pentru a accesa <b>Network</b> (Rețea) > <b>Network</b> (Rețea) > <b>Protocol</b> > <b>SMTP</b> > <b>Advanced Setting</b> (Setare avansată).
<b>Scan</b> (Scanare)	-	<b>Scan</b> (Scanare)	<b>Multifeed Detection / Scan offset correction / Front Page Offset X / Front Page Offset Y / Back Page Offset X / Back Page Offset Y / Display Scan Result</b> (Detectare alimentare multiplă/Corecție abatere scanare/Abatere prima pagină X/Abatere prima pagină Y/Abatere ultima pagină X/Abatere ultima pagină Y/Afișare rezultat scanare)	

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Scan (Scanare) (continuare)	-	<b>Scan Job e-mail report</b> (Raport e-mail proiect scanare) (ADS-2800W/ ADS-3600W)	<b>SMTP Server Address / Administrator Address / SMTP / Scan to E-mail Server / Scan to FTP / Scan to SFTP / Scan to Network / Scan to SharePoint</b> (Adresa serverului SMTP/Adresa administratorului/SMTP/Scanare către un server de e-mail/Scanare către FTP/Scanare către SFTP/ Scanare către rețea/Scanare către SharePoint)	
	-	<b>Scan File Name</b> (Nume fișier scanat)	<b>File Name Style / Add Date &amp; Time / Counter / Scan to USB 1-5 / Scan to E-mail Server 1-10 / Scan to FTP/SFTP 1-15 / Scan to Network/SharePoint 1-15</b> (Stil nume fișier/Adăugare Data & Ora/ Contorizare/Scanare către USB 1 – 5/ Scanare către un server de e-mail 1 – 10/Scanare către FTP/ SFTP 1 – 15/Scanare către rețea/ SharePoint 1 – 15)	
	-	<b>Scan to USB</b> (Scanare către USB)	<b>File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF</b> (ADS-2400N / ADS-3000N) / <b>Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan</b> (ADS-2800W / ADS-3600W) (Nume fișier/ Calitate/Reglaj automat detecție culoare/Tip fișier/Parolă pentru securitate PDF (ADS-2400N / ADS-3000N)/Dimensiune document/Setări margini/ Dimensiune fișier/ Autocorectare înclinare/Omitere pagini albe/Omitere sensibilitate pagini albe/Scanare față-verso/ Luminositate/Contrast/Scanare continuă (ADS-2800W / ADS-3600W))	Configurați setările Scanării către USB.

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
<b>Scan</b> (Scanare) (continuare)	-	<b>Scan to E-mail Server</b> (Scanare către un server de e-mail) (ADS-2800W/ ADS-3600W)	<b>File Name / Quality / Auto Color detect adjust / Color / Black and White/Gray / File Type / Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan</b> (ADS-2800W / ADS-3600W) / <b>Send to My E-mail</b> (Nume fișier/ Calitate/Reglaj detecție automată culoare/Culoare/Alb-negru/ Gri/ Tip fișier/Dimensiune document/ Setări margini/Dimensiune fișier/ Autocorectare înclinare/Omitere pagini albe/Omitere sensibilitate pagini albe/Scanare față-verso/ Luminozitate/Contrast/ Scanare continuă (ADS-2800W / ADS-3600W)/Trimitere pe e-mailul meu)	Configurați setările Scanării către server de e-mail.
	-	<b>Scan to PC</b> (Scanare către PC) (ADS-2400N/ ADS-3000N)	<b>Scan to</b> (Scanare către)	
	-	<b>Scan to FTP/SFTP/ Network/ SharePoint</b> (Scanare către FTP/SFTP/ Rețea/ SharePoint)	<b>Profile 1-25 / Send to My Folder</b> (ADS-2800W / ADS-3600W) (Profil 1 – 25/Trimitere în Directorul meu (ADS-2800W / ADS-3600W))	Configurați setările Scanării către FTP/SFTP/Rețea/ SharePoint.
	-	<b>Scan to FTP/SFTP/ Network/ SharePoint Profile</b> (Scanare către FTP/SFTP/ Rețea/Profil SharePoint)	<b>Profile 1-25</b> (Profil 1 – 25)	Configurați setările profilului.

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
<b>Scan</b> (Scanare) (continuare)	-	<b>Profile (FTP)</b> (Profil (FTP))	<b>Profile Name / Host Address / Username / Password / Store Directory / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF</b> (ADS-2400N / ADS-3000N) / <b>Document Size / Margin Settings / File Size / Auto Des skew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan</b> (ADS-2800W / ADS-3600W) / <b>Passive Mode / Port Number</b> (Nume profil/Adresă gazdă/ Nume de utilizator/Parolă/Director stocare/Nume fișier/Calitate/Reglaj automat detecție culoare/Tip fișier/ Parolă pentru securitate PDF (ADS-2400N / ADS-3000N)/ Dimensiune document/Setări margini/Dimensiune fișier/ Autocorectare înclinare/Omitere pagini albe/Omitere sensibilitate pagini albe/Scanare față-verso/ Luminozitate/Contrast/Scanare continuă (ADS-2800W / ADS-3600W)/Mod pasiv/ Număr port)	Configurați setările profilului. Pentru mai multe informații, consultați <i>Modificarea configurării funcției Scanare către FTP</i> la pagina 49.

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Scan (Scanare) (continuare)	-	Profile (SFTP) (Profil (SFTP))	<b>Profile Name / Host Address / Username / Auth. Method / Client Key Pair / Server Public Key / Store Directory / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF (ADS-2400N / ADS-3000N) / Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan (ADS-2800W / ADS-3600W) / Port Number</b> (Nume profil/Adresă gazdă/Nume de utilizator/Metodă de autentificare/Asociere chei client/Cheia publică a serverului/Director stocare/Nume fișier/Calitate/Reglaj automat detecție culoare/Tip fișier/Parolă pentru securitate PDF (ADS-2400N / ADS-3000N)/Dimensiune document/Setări margini/Dimensiune fișier/Autocorectareînclinare/Omitere pagini albe/Omitere sensibilitate pagini albe/Scanare față-verso/Luminozitate/Contrast/Scanare continuă (ADS-2800W / ADS-3600W)/Număr port)	Configurați setările profilului. Pentru mai multe informații, consultați <i>Modificarea configurării funcției Scanare către SFTP</i> la pagina 50

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Scan (Scanare) (continuare)	-	Profile Network (Profil Rețea)	<p><b>Profile Name / Network Folder Path / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF</b> (ADS-2400N / ADS-3000N) / <b>Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan</b> (ADS-2800W / ADS-3600W) / <b>Use PIN for Authentication / PIN Code / Auth. Method / Username / Password / Date&amp;Time</b> (Nume profil/Cale folder rețea/Nume fișier/Calitate/Reglaj automat detecție culoare/Tip fișier/ Parolă pentru securitate PDF (ADS-2400N / ADS-3000N)/ Dimensiune document/Setări margini/ Dimensiune fișier/ Autocorectare înclinare/Omitere pagini albe/Omitere sensibilitate pagini albe/ Scanare față-verso/Luminozitate/ Contrast/Scanare continuă (ADS-2800W/ADS-3600W) Utilizare PIN pentru autentificare/Cod PIN/ Metodă de autentificare/ Nume utilizator/Parolă/Data&amp;Ora)</p>	<p>Configurați setările profilului. Pentru mai multe informații, consultați <i>Modificarea configurării funcției Scanare către rețea (Windows®)</i> la pagina 52.</p>

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Scan (Scanare) (continuare)	-	<b>Profile (SharePoint)</b> (Profil (SharePoint))	<b>Profile Name / SharePoint Site Address / SSL/TLS / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF (ADS-2400N / ADS-3000N) / Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-Sided Scan / Brightness / Contrast / Continuous Scan (ADS-2800W / ADS-3600W) / Use PIN for Authentication / Pin Code / Auth. Method / Username / Password / Date&amp;Time</b> (Nume profil/ Adresă site SharePoint/SSL/TLS/ Nume fișier/Calitate/Reglaj automat detecție culoare/Tip fișier/ Parolă pentru securitate PDF (ADS-2400N/ADS-3000N)/ Dimensiune document/Setări margini/ Dimensiune fișier/ Autocorectare înclinare/Omitere pagini albe/Omitere sensibilitate pagini albe/Scanare față-verso/Luminozitate/ Contrast/Scanare continuă (ADS-2800W/ADS-3600W) Utilizare PIN pentru autentificare/Cod PIN/ Metodă de autentificare/Nume utilizator/Parolă/Data&Ora)	Configurați setările profilului. Pentru mai multe informații, consultați <i>Modificarea configurării funcției Scanare către SharePoint (Windows®)</i> la pagina 54.
	-	<b>Scan to Network Device</b> (Scanare către dispozitivul de rețea) (ADS-2400N/ ADS-3000N)	<b>Network Device1 / Type / Destination / Network Device2 / Type / Destination / Network Device3 / Type / Destination</b> (Dispozitiv de rețea1/Tip/Destinație/ Dispozitiv de rețea3/Tip/Destinație/ Dispozitiv de rețea3/Tip/Destinație)	
	-	<b>Scan from PC</b> (Scanare de la PC)	<b>Pull Scan</b> (Extragere scanare)	
<b>Administrator</b>	-	<b>Login Password</b> (Parolă de conectare)	<b>Password</b> (Parolă)	Configurați parola utilizată pentru conectarea la Administrarea bazată pe web. Puteți modifica doar setările din fila <b>General</b> (Informații generale) fără a vă conecta.



Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Administrator (continuare)	-	<b>User Restriction Function</b> (Funcția de restricționare utilizatori) (ADS-2800W/ ADS-3600W)		
	-	<b>Secure Function Lock</b> (Blocarea securizată a funcțiilor) (ADS-2800W/ ADS-3600W)	<b>Web / PC / Network / FTP/SFTP / E-mail Server / Share Point / WS Scan / USB</b> (Web/PC/Rețea/FTP/SFTP/Server e-mail/SharePoint/Scanare WS/USB)	<b>Secure Function Lock</b> (Blocarea securizată a funcțiilor) restricționează funcțiile de scanare și funcțiile de conectare web, pe baza permisiunilor de utilizator.  Pentru mai multe informații, consultați <i>Blocarea securizată a funcțiilor 3.0</i> (ADS-2800W/ADS-3600W) la pagina 84.
	-	<b>Active Directory Authentication</b> (Autentificare Active Directory) (ADS-2800W/ ADS-3600W)	<b>Remember User ID / Active Directory Server Address / Active Directory Domain Name / Get User's Home Directory / Protocol &amp; Authentication Method / Get Mail Address / LDAP Server Port / LDAP Search Root / SNTP</b> (Memorare ID utilizator/Adresă server Active Directory/Nume domeniu Active Directory/Obținere director de pornire al utilizatorului/Protocol și metodă de autentificare/Obținere adresă de e-mail/Port server LDAP/Rădăcină căutare LDAP/SNTP)	<b>Active Directory Authentication</b> (Autentificare Active Directory) restricționează utilizarea aparatului Brother.  Pentru mai multe informații, consultați <i>Configurarea autentificării Active Directory prin LDAP</i> (ADS-2800W/ADS-3600W) la pagina 43.
	-	<b>LDAP Authentication</b> (Autentificare prin LDAP) (ADS-2800W/ ADS-3600W)	<b>Remember User ID / LDAP Server Address / Get Mail Address / LDAP Server Port / LDAP Search Root / Attribute of Name (Serch Key) / SNTP</b> (Memorare ID utilizator/Adresă server LDAP/Obținere adresă de e-mail/Port server LDAP)/Rădăcină căutare LDAP/Atribut nume (cheie de căutare)/SNTP)	<b>LDAP Authentication</b> (Autentificare prin LDAP) restricționează utilizarea aparatului Brother.  Pentru mai multe informații, consultați <i>Modificarea configurării LDAP</i> la pagina 44.
	-	<b>Setting Lock</b> (Configurarea blocării) (ADS-2800W/ ADS-3600W)	<b>Setting Lock / Password</b> (Configurarea blocării/Parolă)	Configurați parola pentru a modifica setările aparatului cu ajutorul ecranului LCD al aparatului Brother.
	-	<b>Signed PDF</b> (PDF semnat)	<b>Select the Certificate / Certificate</b> (Selectare certificat/Certificat)	Configurați setările certificatului pentru PDF semnat.

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Administrator (continuare)	-	<b>Date &amp; Time</b> (Data & Ora)	<b>Date / Clock Type / Time / Time Zone / Auto Daylight / Synchronize with SNTP server / SNTP</b> (Data/Tip ceas/Ora/Fus orar/Oră de vară/Sincronizare cu serverul SNTP/SNTP)	
	-	<b>Reset Menu</b> (Meniul Resetare)	<b>Machine Reset / Network / Address Book / All Settings / Factory Reset</b> (Resetare aparat/Rețea/Agendă cu adrese/Toate setările/Resetare la setările din fabrică)	
	-	<b>Firmware Update</b> (Actualizare firmware)	<b>Model Name / Serial Number / Firmware Version / MAIN / Firmware Update / Proxy</b> (Nume model/Serie/Versiune Firmware/MAIN/Actualizare firmware/Proxy)	Consultați <i>Actualizare firmware</i> la pagina 86.
Network (Rețea)	Network (Rețea)	<b>Network Status</b> (Stare rețea)	<b>Wired / Wireless</b> (Prin cablu/Wireless)	Afișați starea rețelei.
		<b>Interface</b> (Interfață) (ADS-2800W/ ADS-3600W)	<b>Interface / Wi-Fi Direct</b> (Interfață/Wi-Fi Direct)	Modificați interfața.
		<b>Protocol</b> (Protocol)	<b>Web Based Management (Web Server) / Telnet / SNTP / Remote Setup / Raw Port / Web Services / Proxy / Network Scan / SMTP / FTP Server / FTP Client / SFTP / TFTP / WebDAV / CIFS / LDAP / mDNS / LLNMR / SNTP</b> (Administrare bazată pe web (server Web)/Telnet/SNTP/Configurare de la distanță/Raw Port/Servicii Web/Proxy/Scanare rețea/SMTP/Server FTP/Client FTP/SFTP/TFTP/ WebDAV/CIFS/LDAP/mDNS/LLNMR/SNTP)	Configurați setările pentru protocol ale aparatului Brother. Selectați caseta de dialog pentru fiecare protocol pe care doriți să îl utilizați.
		<b>Notification</b> (Notificare)	<b>SMTP Server Address / Device E-mail Address / SMTP / Administrator Address</b> (Adresă server SMTP/Adresă de e-mail dispozitiv/SMTP/Adresă administrator)	Configurați setările pentru notificările de erori.
		<b>E-mail Reports</b> (Rapoarte e-mail) (ADS-2800W / ADS-3600W)	<b>SMTP Server Address / E-mail Address / SMTP / Date&amp;Time / Administrator Address</b> (Adresă server SMTP/Adresă de e-mail/ SMTP/ Data&Ora/Adresă administrator)	

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Network (Rețea) (continuare)	Wired (Prin cablu)	<b>TCP/IP (Wired)</b> (TCP/IP (prin cablu))	<b>Ethernet 10/100/1000 BASE-T / IP Address / Subnet Mask / Gateway / Boot Method / Advanced Settings / Interface</b> (Ethernet 10/100/1000 BASE-T/Adresă IP/Mască subrețea/ Gateway/Metodă BOOT/Setări avansate/Interfață)	Configurați setările TCP/IP (prin cablu).
		<b>Node Name (Wired)</b> (Nume nod (prin cablu))	<b>Node Name</b> (Nume nod)	
		<b>NetBIOS</b> (Wired) (NetBIOS (prin cablu))	<b>NETBIOS/IP / Computer Name / WINS Server Method / Primary WINS Server IP Address / Secondary WINS Server IP Address</b> (ETBIOS/IP/Nume computer/Metodă server WINS/Adresă IP server WINS primar/Adresă IP server WINS secundar)	
		<b>IPv6 (Wired)</b> (IPv6 (prin cablu))	<b>IPv6 / Static IPv6 Address / Primary DNS Server IP Address / Secondary DNS Server IP Address / IPv6 Address List</b> (IPv6 / Adresă IPv6 Statistică / Adresă IP server DNS primar / Adresă IP server DNS secundar / Listă adresă IPv6)	
		<b>Ethernet</b>	<b>Ethernet Mode</b> (Mod Ethernet)	
		<b>Wired 802.1x Authentication</b> (Autentificare 802.1x prin cablu)	<b>Wired 802.1x status / Authentication Method / Inner Authentication Method / User ID / Password / Client Certificate / Server Certificate Verification / Server ID / Certificate</b> (Stare 802.1x prin cablu/Metodă de autentificare/ Metodă de autentificare internă/ ID utilizator/Parolă/Certificat client/ Verificare certificat server/ID server/ Certificat)	
	<b>Wireless</b> (ADS-2800W/ ADS-3600W)	<b>TCP/IP (Wireless)</b>	<b>IEEE 802.11b/g/n / IP Address / Subnet Mask / Gateway / Boot Method / Advanced Settings / Interface</b> (IEEE 802.11b/g/n/Adresă IP/Mască subrețea/Gateway/ Metodă BOOT/Setări avansate/ Interfață)	Configurați setările TCP/IP (Wireless).

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Network (Rețea) (continuare)	Wireless (ADS-2800W/ ADS-3600W) (continuare)	<b>Node Name (Wireless)</b> (Nume nod wireless))	<b>Node Name</b> (Nume nod)	
		<b>NetBIOS (Wireless)</b>	<b>NETBIOS/IP / Computer Name / WINS Server Method / Primary WINS Server IP Address / Secondary WINS Server IP Address</b> (ETBIOS/IP/Nume computer/Metodă server WINS/ Adresă IP server WINS primar/ Adresă IP server WINS secundar)	
		<b>IPv6 (Wireless)</b>	<b>IPv6 / Static IPv6 Address / Primary DNS Server IP Address / Secondary DNS Server IP Address / IPv6 Address List</b> (IPv6 / Adresă IPv6 Statistică / Adresă IP server DNS primar / Adresă IP server DNS secundar / Listă adresă IPv6)	
		<b>Wireless (Setup Wizard) (Wireless (Expert configurare))</b>		Faceți clic pe <b>Start Wizard</b> (Pornire expert) pentru a începe configurarea expertă a rețelei wireless.
		<b>Wireless (Personal)</b>	<b>Current Status / Communication Mode / Wireless Network Name (SSID) / Channel / Authentication Method / Encryption Mode / Network key</b> (Stare actuală/Mod de comunicare/Nume rețea wireless (SSID)/Canal/Metodă de autentificare/ Mod de criptare/Cheie rețea)	
		<b>Wireless (Enterprise)</b>	<b>Current Status / Communication Mode / Wireless Network Name (SSID) / Channel / Authentication Method / Inner Authentication Method / Encryption Mode / User ID / Password / Client Certificate / Server Certificate Verification / Server ID / Certificate</b> (Stare actuală/Mod de comunicare/ Nume rețea wireless (SSID)/Canal/ Metodă de autentificare/Metodă de autentificare internă/Mod de criptare/ ID utilizator/Parolă/Certificat client/ Verificare certificat server/ID Server/ Certificat)	

Categorie principală	Sub-categorie	Meniul funcții	Opțiuni funcții	Descriere/setări opționale
Network (Rețea) (continuare)	Security (Securitate)	<b>IPv4 Filter</b> (Filtru IPv4)	<b>Use IP Filtering Feature / Administrator IP Address / Access Setting</b> (Utilizare funcție de filtrare IP/Adresă IP administrator/ Setare acces)	Configurați setările de acces prin filtrarea adreselor IP.
		<b>Certificate</b> (Certificat)	<b>Certificate List / Create Self-Signed Certificate / Create CSR / Install Certificate / Import Certificate and Private Key</b> (Listă certificate/Creare certificat auto-semnat/Creare CSR/ Instalare certificat/Import certificat și Cheie publică)	Configurați setările certificatului.
		<b>CA Certificate</b> (Certificat CA)	<b>CA Certificate List / Import CA Certificate</b> (Listă certificate CA/Import certificat CA)	Configurați setările certificatului CA.
		<b>Client Key Pair</b> (Asociere chei client)	<b>Client Key Pair List / Create New Client Key Pair</b> (Listă asocieri chei client/Creare asociere chei client nouă)	Configurați setările pentru asocierea cheilor client.
		<b>Server Public Key</b> (Cheia publică a serverului)	<b>Server Public Key List / Import Server Public Key</b> (Listă chei publice server/Import cheie publică server)	Configurați setările pentru cheia publică a serverului.
		<b>IPsec</b>	<b>Status / Negotiation Mode / All Non-IPsec Traffic / Broadcast/Multicast Bypass / Protocol Bypass / Rules</b> (Stare/Mod negociere/Tot traficul non-IPsec/ Bypass transmisie/transmisie multipunct/Bypass protocol/Reguli)	Configurați setările IPsec.
		<b>IPsec Address Template</b> (Șablon adresă IPsec)	<b>Template List</b> (Listă șabloane)	
		<b>IPsec Template</b> (Șablon IPsec)	<b>Template List</b> (Listă șabloane)	

# B

## Index

### A

Administrare bazată pe web (browser web) ..... 6  
Adresă MAC ..... 4, 5, 6, 98

### B

BRAdmin Light ..... 1, 3  
BRAdmin Professional 3 ..... 1, 6

### C

Configurarea de la distanță ..... 1

### F

FTP ..... 49, 50

### H

HTTP ..... 38

### I

Instrument de reparare a conexiunii de rețea ..... 92

### L

LDAP ..... 44

### M

Management bazat pe web (browser web) ..... 1  
Metodă PIN ..... 19  
Mod Ad-hoc ..... 10, 22  
Mod Infrastructură ..... 9

### P

Protocoale și funcții de securitate compatibile ..... 100

### R

Rețea wireless ..... 8

### S

Servicii web ..... 97  
SMTP-AUTH ..... 64  
Status Monitor ..... 1

### V

Vertical Pairing ..... 1, 97

### Z

WPS (Wi-Fi Protected Setup™) ..... 19