EPSON
EXCEED YOUR VISION

Vodič za administratore

NPD5668-00 SR

Sadržaj

Dodatak

Napredne bezbednosne postavke za Enterprise

Autorska prava

Zaštitni znakovi

- ❏ EPSON® predstavlja registrovani žig, a EPSON EXCEED YOUR VISION ili EXCEED YOUR VISION žig korporacije Seiko Epson.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Opšta napomena: ostali nazivi proizvoda upotrebljeni su u ovom dokumentu isključivo u identifikacione svrhe i možda predstavljaju zaštitne znakove svojih vlasnika. Epson se odriče svih prava na te žigove.

O ovom priručniku

Oznake i simboli

> ⚠ ***Oprez:***
> *Uputstva koja se moraju poštovati da bi se izbegle telesne povrede.*

> ***Važno:***
> *Uputstva koja se moraju poštovati da bi se izbeglo oštećenje opreme.*

Napomena:
Uputstva koja sadrže korisne savete i ograničenja koja se odnose na rad skenera.

Povezane informacije

➡ Klikom na ovu ikonu bićete prebačeni na povezane informacije.

Opisi korišćeni u ovom priručniku

❏ Snimci ekrana sa upravljačkim programom za skener i Epson Scan 2 (upravljački program za skener) su ekrani iz operativnih sistema Windows 10 ili OS X El Capitan. Sadržaj prikazan na ekranu varira u zavisnosti od modela i situacije.

❏ Ilustracije korišćene u ovom priručniku predstavljaju samo primere. Iako može postojati mala razlika u zavisnosti od modela, način rada je isti.

❏ Neke od stavki menija na LCD ekranu variraju u zavisnosti od modela i podešavanja.

Reference koje se odnose na operativne sisteme

Windows

Termini u ovom priručniku poput „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Vista“, „Windows XP“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“, „Windows Server 2008 R2“, „Windows Server 2008“, „Windows Server 2003 R2“ i „Windows Server 2003“ odnose se na operativne sisteme navedene u nastavku. Pored toga, termin „Windows“ odnosi se na sve verzije.

❏ Operativni sistem Microsoft® Windows® 10

❏ Operativni sistem Microsoft® Windows® 8.1

❏ Operativni sistem Microsoft® Windows® 8

❏ Operativni sistem Microsoft® Windows® 7

❏ Operativni sistem Microsoft® Windows Vista®

❏ Operativni sistem Microsoft® Windows® XP

- ❏ Operativni sistem Microsoft® Windows® XP Professional x64 Edition
- ❏ Operativni sistem Microsoft® Windows Server® 2016
- ❏ Operativni sistem Microsoft® Windows Server® 2012 R2
- ❏ Operativni sistem Microsoft® Windows Server® 2012
- ❏ Operativni sistem Microsoft® Windows Server® 2008 R2
- ❏ Operativni sistem Microsoft® Windows Server® 2008
- ❏ Operativni sistem Microsoft® Windows Server® 2003 R2
- ❏ Operativni sistem Microsoft® Windows Server® 2003

Mac OS

U ovom priručniku „Mac OS“ se koristi za upućivanje na macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x, i Mac OS X v10.6.8.

Uvod

Komponente priručnika

Ovaj priručnik je namenjen administratoru uređaja koji je zadužen za priključivanje štampača ili skenera na mrežu, a sadrži i informacije o tome kako podesiti funkcije za korišćenje.

Informacije o korišćenju funkcija potražite u *Korisnički vodič*.

Priprema

Objašnjava zadatke administratora, kako podesiti uređaje, kao i softver za upravljanje njima.

Priključivanje

Objašnjava kako priključiti uređaj na mrežu ili telefonsku liniju. Takođe objašnjava i mrežno okruženje, kao što je korišćenje ulaza za uređaj, informacije o DNS i ovlašćenom serveru.

Podešavanje funkcija

Objašnjava podešavanja za svaku funkciju uređaja.

Osnovne bezbednosne postavke

Objašnjava podešavanja za svaku funkciju, poput štampanja, skeniranja i slanja/primanja faksa.

Podešavanja u vezi s radom i upravljanjem

Objašnjava radnje koje se vrše kad uređaj počne da se koristi, poput provere informacija i održavanja.

Otklanjanje problema

Objašnjava započinjanje podešavanja i rešavanje problema s mrežom.

Napredne bezbednosne postavke za Enterprise

Objašnjava način podešavanja kojim se povećava bezbednost uređaja, poput korišćenja CA sertifikata, SSL/TLS komunikacije i IPsec/IP filtriranja.

U zavisnosti od modela, neke funkcije u ovom poglavlju nisu podržane.

Definicije i termini koji se koriste u ovom priručniku

U ovom priručniku se koriste sledeći termini.

Administrator

Osoba zadužena za instaliranje i podešavanje uređaja ili mreže u kancelariji ili organizaciji. U malim organizacijama, ova osoba može biti zadužena za upravljanje i uređajem i mrežom. U velikim organizacijama administratori rukovode mrežom ili uređajima u grupnoj jedinici nekog odeljenja ili sektora, a administratori mreže su zaduženi za komunikacione postavke za vezu s okruženjem izvan organizacije, poput interneta.

Mrežni administrator

Osoba zadužena za kontrolisanje komunikacije na mreži. Osoba koja je postavila mrežnu skretnicu, ovlašćeni server, DNS server i server za e-poštu kako bi kontrolisala komunikaciju putem interneta ili mreže.

Korisnik

Osoba koja koristi uređaje kao što su štampači ili skeneri.

Web Config (veb-sajt štampača)

Veb-server koji je ugrađen u uređaj. Zove se Web Config. Na njemu pomoću pregledača možete proveriti i izmeniti status uređaja.

Alatka

Opšti termin za softver koji se koristi za podešavanje ili upravljanje uređajem, poput Epson Device Admin, EpsonNet Config, EpsonNet SetupManager itd.

Skeniranje s uređaja

Opšti termin za skeniranje s kontrolne table uređaja.

ASCII (Američki standardni kod za razmenu podataka, eng. American Standard Code for Information Interchange)

Jedan od standardnih znakovnih kodova. Definisano je 128 znakova, uključujući znakove kao što su slova (a–z, A–Z), arapski brojevi (0–9), simboli, prazna mesta i kontrolni znakovi. Kada se u ovom priručniku koristi termin „ASCII“, on označava 0x20–0x7E (heksadecimalni broj) naveden ispod i ne obuhvata kontrolne znakove.

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

* Znak razmaka.

Unicode (UTF-8)

Međunarodni standardni kod koji obuhvata velike svetske jezike. Kada se u ovom priručniku koristi termin „UTF-8“, on označava znakove u formatu UTF-8.

Priprema

U ovom poglavlju objašnjene su uloga administratora i pripreme koje treba izvršiti pre podešavanja.

Tok postavki skenera i upravljanja njime

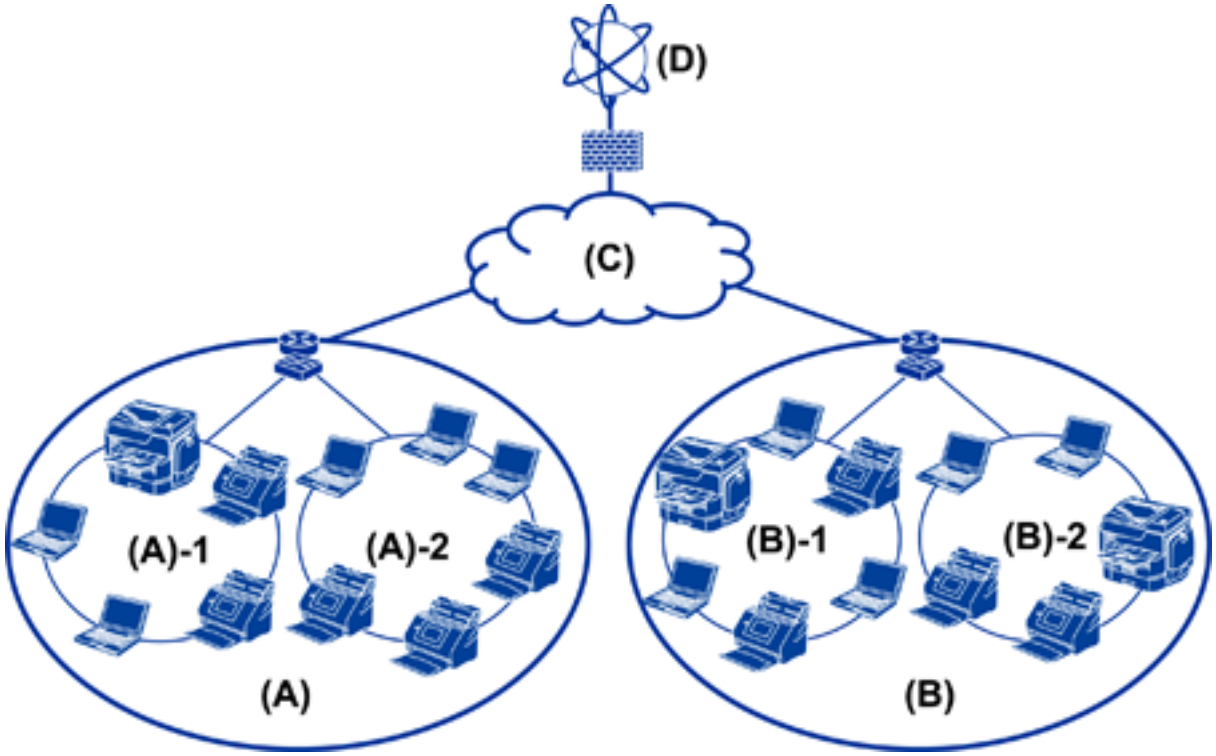
Administrator vrši podešavanje mrežne veze za skener, pravi početne postavke i vrši njihovo održavanje kako bi uređaji bili dostupni korisnicima.

1. Priprema
   - ❏ Prikupljanje informacija o podešavanju veze
   - ❏ Donošenje odluke o načinu povezivanja
2. Povezivanje
   - ❏ Povezivanje na mrežu preko kontrolne table skenera
3. Podešavanje funkcija
   - ❏ Podešavanja upravljačkog programa skenera
   - ❏ Ostala napredna podešavanja
4. Bezbednosna podešavanja
   - ❏ Podešavanja za administratore
   - ❏ SSL/TLS
   - ❏ Kontrola protokola
   - ❏ Napredna bezbednosne postavke (Opcija)
5. Rukovanje i upravljanje
   - ❏ Provera statusa uređaja
   - ❏ Rešavanje nastalih događaja
   - ❏ Pravljenje rezervne kopije podešavanja

Povezane informacije

➡ “Priprema” na strani 10
➡ “Priključivanje” na strani 15
➡ “Podešavanje funkcija” na strani 22
➡ “Osnovne bezbednosne postavke” na strani 32
➡ “Podešavanja u vezi s radom i upravljanjem” na strani 40

Primer mrežnog okruženja



(A): Kancelarija 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Kancelarija 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Primer predstavljanja postavki za povezivanje skenera

Uglavnom postoje dva tipa povezivanja zavisno od toga kako će se koristiti skener. Oba povezuju skener na mrežu pomoću računara preko čvorišta.

❏ Veza server/klijent (skener pomoću Windows servera, upravljanje zadacima)

❏ Veza lokalne mreže (direktna veze pomoću računara klijenta)

Povezane informacije

➡ “Veza server/klijent” na strani 12

➡ “Veza lokalne mreže” na strani 12

Veza server/klijent

Centralizujte upravljanje skenerom i zadacima pomoću Document Capture Pro Server instaliranog na server. Za zadatak koji koristi više skenera najprikladnije je da skenira veliki broj dokumenata u određenom formatu.

Povezane informacije

➡ "Definicije i termini koji se koriste u ovom priručniku" na strani 8

Veza lokalne mreže

Koristite pojedinačni skener sa upravljačkim programom skenera kao što je Epson Scan 2 instaliranim na računar klijent. Instaliranje Document Capture Pro (Document Capture) na računar klijent omogućava vam da pokrećete zadatke na pojedinačnim računarima klijentima skenera.

Povezane informacije

➡ "Definicije i termini koji se koriste u ovom priručniku" na strani 8

Priprema povezivanja na mrežu

Prikupljanje informacija o podešavanju veze

Potrebno je da imate IP adresu, adresu mrežnog prolaza itd. za mrežno povezivanje. Sledeće stavke proverite unapred.

Odeljak	Stavke	Napomena
Način povezivanja uređaja	❏ Ethernet veza	Za Ethernet vezu koristite STP kabl (kabl sa upredenim paricama) kategorije 5e ili više.
Informacije o LAN vezi	❏ IP adresa ❏ Maska podmreže ❏ Podrazumevani mrežni prolaz	Ako automatski podesite IP adresu pomoću DHCP funkcije skretnice, ovo nije potrebno.
Informacije o DNS serveru	❏ IP adresa za primarni DNS ❏ IP adresa za sekundarni DNS	Ako kao IP adresu koristite statičku IP adresu, konfigurišite DNS server. Izvršite konfiguraciju kada se vrši automatsko dodeljivanje pomoću DHCP funkcije i kada DNS server ne može biti dodeljen automatski.
Informacije o ovlašćenom serveru	❏ Naziv ovlašćenog servera ❏ Broj ulaza	Izvršite konfiguraciju prilikom korišćenja ovlašćenog servera za internet vezu i prilikom korišćenja servisa Epson Connect ili funkcije automatskog ažuriranja upravljačkog softvera.

Specifikacije skenera

Tehnički podatak da skener podržava standardni ili mrežni režim, pogledajte *Korisnički vodič*.

Korišćenje broja ulaza

Broj ulaza koji skener koristi potražite u „Dodatku“.

Povezane informacije

➡ “Korišćenje ulaza za skener” na strani 60

Vrste IP adresa za dodeljivanje

Postoje dve vrste adresa koje se mogu dodeliti skeneru.

Statička IP adresa:

Dodelite unapred određenu jedinstvenu IP adresu skeneru.

IP adresa se ne menja čak i kada se skener ili skretnica isključe, tako da uređajem možete upravljati prema IP adresi.

Ova vrsta je pogodna za mrežu u kojoj se upravlja velikim brojem skenera, poput velike kancelarije ili škole.

Automatsko dodeljivanje pomoću funkcije DHCP:

Ispravna IP adresa biće automatski dodeljena kada komunikacija između skenera i skretnice koja podržava DHCP funkciju bude uspešna.

Ako je menjanje IP adrese određenog uređaja nezgodno, rezervišite IP adresu unapred, a zatim je dodelite.

DNS server i ovlašćeni server

Ako koristite uslugu pristupa internetu, konfigurišite DNS server. Ako ga ne konfigurišete, morate navesti IP adresu za pristup, pošto se može dogoditi da razrešavanje imena bude neuspešno.

Ovlašćeni server se nalazi na mrežnom prolazu između mreže i interneta i komunicira s računarom, skenerom i internetom (reverzni server) u ime svakog od njih. Reverzni server komunicira samo sa ovlašćenim serverom. Dakle, informacije o skeneru kao što su IP adresa i broj ulaza ne mogu se očitati, pa se očekuje povećana bezbednost.

Pomoću funkcije filtriranja možete zabraniti pristup određenoj URL adresi, pošto ovlašćeni server može da proveri sadržaj komunikacije.

Način podešavanja povezivanja na mrežu

Da biste podesili povezivanje na mrežu za IP adresu skenera, masku podmreže i podrazumevani mrežni prolaz, postupite na sledeći način.

Korišćenje kontrolne table:

Konfigurišite podešavanja za svaki skener pomoću kontrolne table skenera. Nakon što ste konfigurisali mrežna podešavanja skenera, priključite ga na mrežu.

Korišćenje čarobnjaka za instalaciju:

Ako se koristi čarobnjak za instalaciju, mreža skenera i računar klijent se podešavaju automatski. Podešavanje je moguće izvršiti prateći uputstva čarobnjaka za instalaciju čak i ako niste dobro upoznati s mrežom.

Korišćenje alatke:

Koristite alatku s administratorskog računara. Možete da otkrijete skener, a zatim ga podesite ili napravite SYLK datoteku kako biste izvršili grupna podešavanja skenera. Možete podesiti mnogo skenera, ali oni pre podešavanja moraju biti fizički povezani Ethernet kablom. Dakle, ovo se preporučuje ako možete da napravite Ethernet vezu za podešavanje.

Povezane informacije

➡ “Povezivanje na mrežu s kontrolne table” na strani 15

➡ “Povezivanje na mrežu pomoću čarobnjaka za instalaciju” na strani 19

➡ “Dodeljivanje IP adrese pomoću EpsonNet Config” na strani 56

Priključivanje

U ovom poglavlju opisano je okruženje ili postupak priključivanja skenera na mrežu.

Priključivanje na mrežu

Povezivanje na mrežu s kontrolne table

Priključite skener na mrežu pomoću kontrolne table skenera.

Za više informacija o kontrolnoj tabli skenera pogledajte *Korisnički vodič*.

Dodeljivanje IP adrese

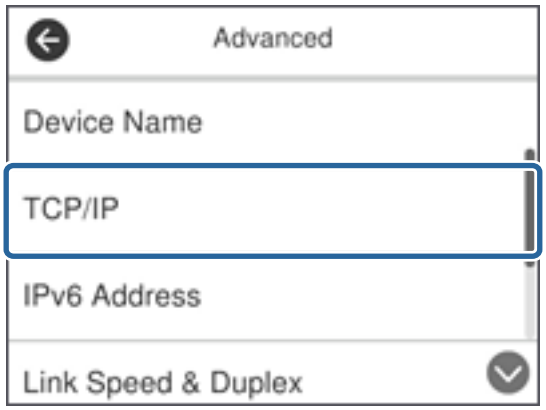
Podesite osnovne stavke, poput IP adresa, Maska podmreže i Podraz. mrež. prol..

1. Uključite skener.
2. Prevucite prstom nalevo preko kontrolne table skenera, a zatim dodirnite **Podešavanja**.

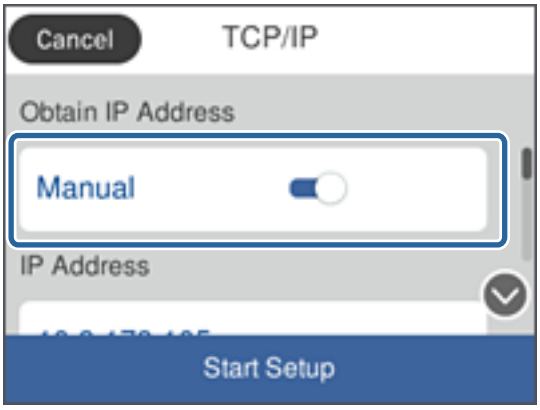
3. Dodirnite **Mrežne postavke** > **Promeni postavke**.

   Ako stavka ne bude prikazana, povucite prstom prema gore kako bi se pojavila.

4. Dodirnite **TCP/IP**.

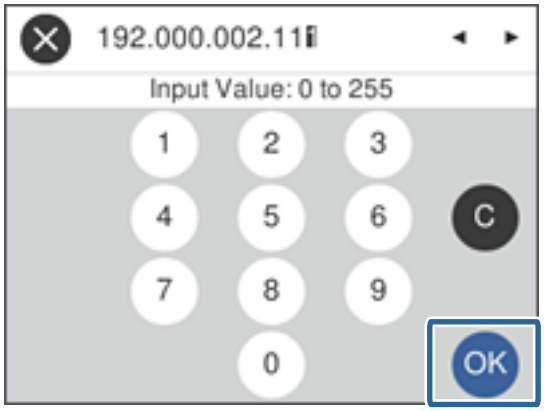


5. Izaberite **Ručno** za **Pribavi IP adresu**.



Napomena:
*Kada IP adresu podesite automatski pomoću DHCP funkcije rutera, odaberite **Automatski**. U tom slučaju **IP adresa**, **Maska podmreže**, i **Podraz. mrež. prol.** u koracima od 6 do 7 takođe budu automatski podešeni, tako da možete preći na korak 8.*

6. Dodirnite polje **IP adresa**, unesite IP adresu pomoću tastature prikazane na ekranu, a zatim dodirnite **U redu**.



Potvrdite vrednost prikazanu na prethodnom ekranu.

7. Podesite **Maska podmreže** i **Podraz. mrež. prol.**.

   Potvrdite vrednost prikazanu na prethodnom ekranu.

   Napomena:
   Ukoliko kombinacija stavki IP adresa, Maska podmreže i Podraz. mrež. prol. nije ispravna, stavka ***Počni podešavanje*** *je deaktivirana i ne može nastaviti s podešavanjima. Potvrdite da u unetim vrednostima nema grešaka.*

8. Dodirnite polje **Primarni DNS** za **DNS server**, unesite IP adresu za primarni DNS pomoću tastature prikazane na ekranu, a zatim dodirnite **U redu**.

   Potvrdite vrednost prikazanu na prethodnom ekranu.

   Napomena:
   Kada odaberete ***Automatski*** *za podešavanje dodeljivanja IP adrese, možete odabrati podešavanja za DNS server u* ***Ručno*** *ili* ***Automatski****. Ako ne možete automatski da dobijete adresu DNS servera, odaberite* ***Ručno*** *i unesite adresu DNS servera. Zatim direktno unesite adresu sekundarnog DNS servera. Ako odaberete* ***Automatski****, idite na korak 10.*

9. Dodirnite polje **Sekundarni DNS**, unesite IP adresu za sekundarni DNS server pomoću tastature prikazane na ekranu, a zatim dodirnite **U redu**.

   Potvrdite vrednost prikazanu na prethodnom ekranu.

10. Dodirnite **Počni podešavanje**.

11. Dodirnite **Zatvori** na ekranu za potvrdu.

    Ako ne dodirnete **Zatvori**, ekran se automatski zatvara posle određenog vremena.

Povezivanje na Ethernet

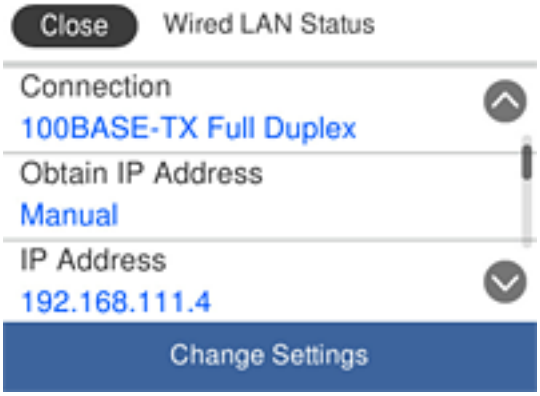
Priključite skener na mrežu pomoću Ethernet kabla i proverite vezu.

1. Priključite skener na čvorište (prekidač L2) pomoću Ethernet kabla.

   Ikona na početnom ekranu će se promeniti u  .

2. Dodirnite  na početnom ekranu.

3. Prevucite prstom prema gore, a zatim proverite da li su status veze i IP adresa tačni.



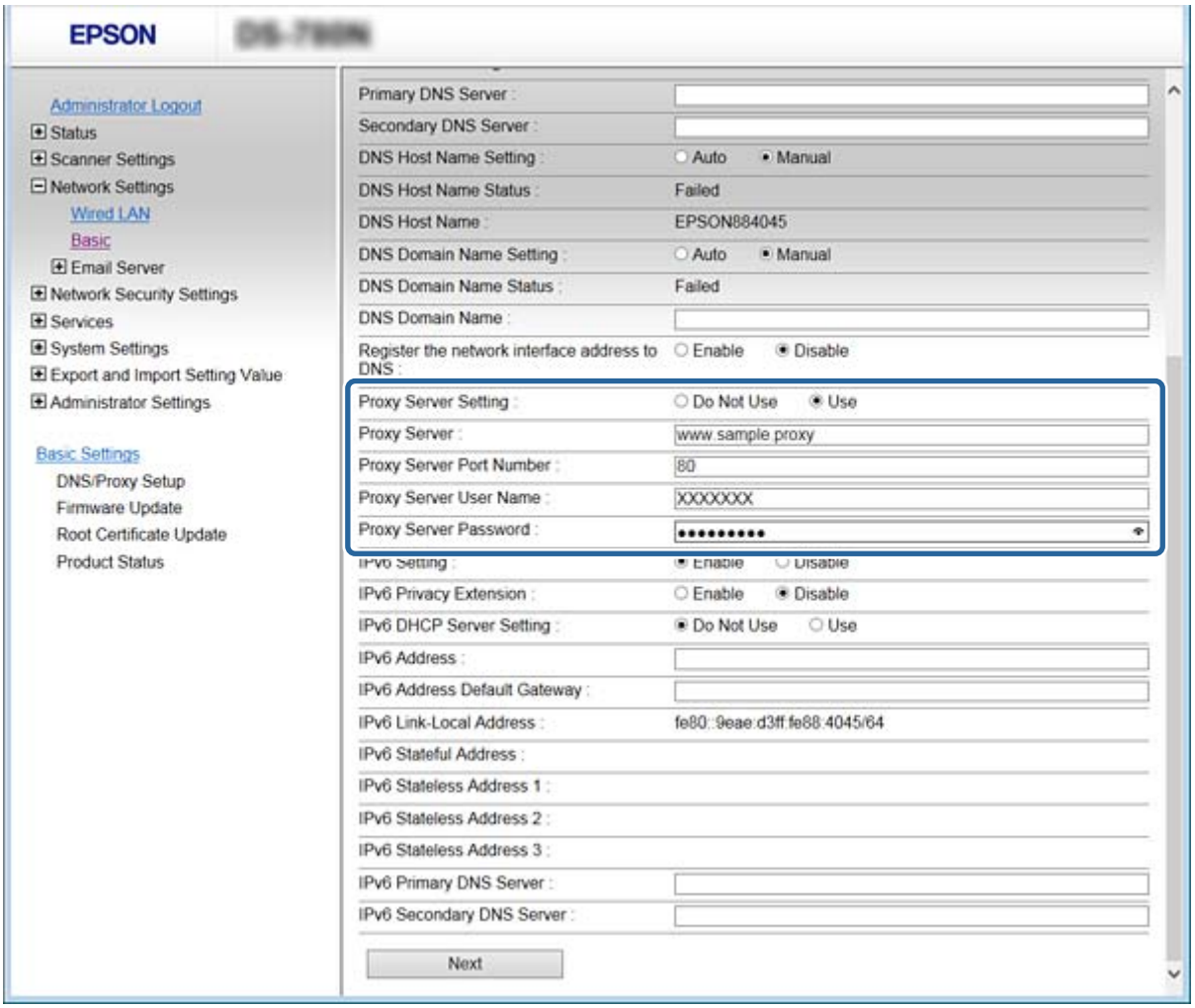
Podešavanje ovlašćenog servera

Ovlašćeni server se ne može podesiti na tabli. Konfigurišite pomoću Web Config.

1. Pristupite programu Web Config i odaberite **Network Settings** > **Basic**.
2. Izaberite **Use** u **Proxy Server Setting**.
3. Odredite ovlašćeni server u IPv4 adresi ili FQDN formatu u **Proksi server**, a zatim unesite broj ulaza u **Proxy Server Port Number**.

   Za ovlašćene servere koji zahtevaju proveru identiteta korisnika, unesite korisničko ime za proveru identiteta ovlašćenog servera i lozinku za proveru identiteta ovlašćenog servera.

4. Kliknite na dugme **Next**.



5. Potvrdite podešavanja, a zatim kliknite na **Podešavanja**.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Povezivanje na mrežu pomoću čarobnjaka za instalaciju

Preporučujemo korišćenje čarobnjaka za instalaciju prilikom povezivanja skenera s računarom. Čarobnjaka za instalaciju možete da pokrenete na jedan od sledećih načina.

❏ Podešavanjem uređaja sa veb-sajta

Pristupite sledećem veb-sajtu, a zatim unesite naziv proizvoda. Idite na **Podešavanje**, a zatim počnite sa podešavanjem.

http://epson.sn

❏ Podešavanjem uređaja pomoću diska sa softverom (samo za modele uz koji se isporučuje disk sa softverom i za korisnike koji imaju kompjutere s pogonom diska).

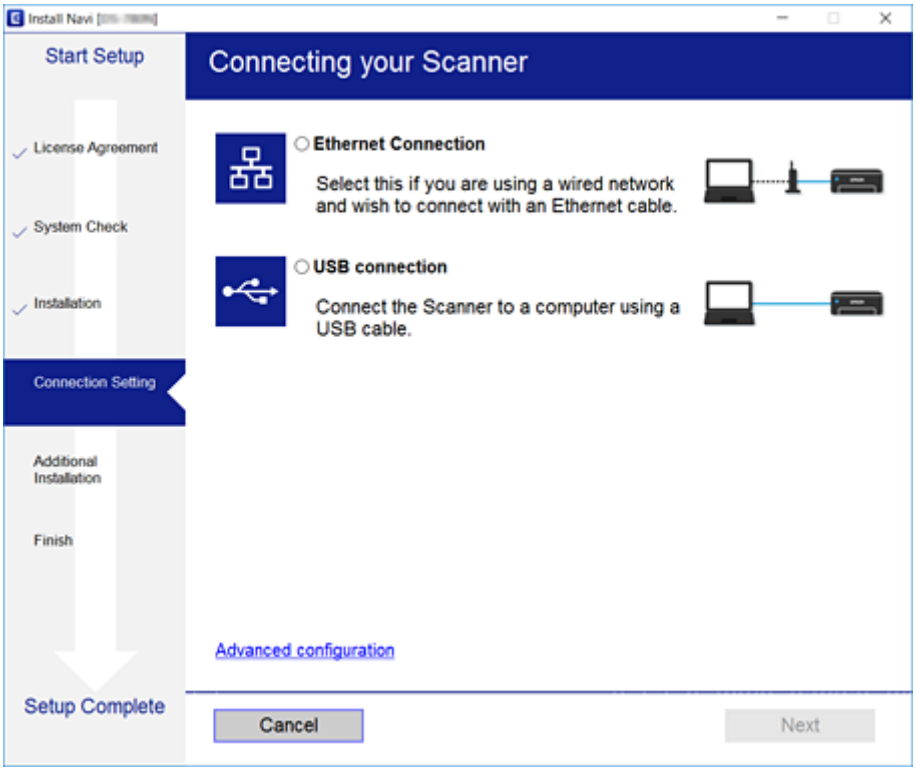
Ubacite disk sa softverom, a zatim sledite uputstva na ekranu.

Odabir načina povezivanja

Sledite uputstva na ekranu dok ne bude prikazan sledeći ekran, a zatim odaberite način povezivanja skenera s računarom.

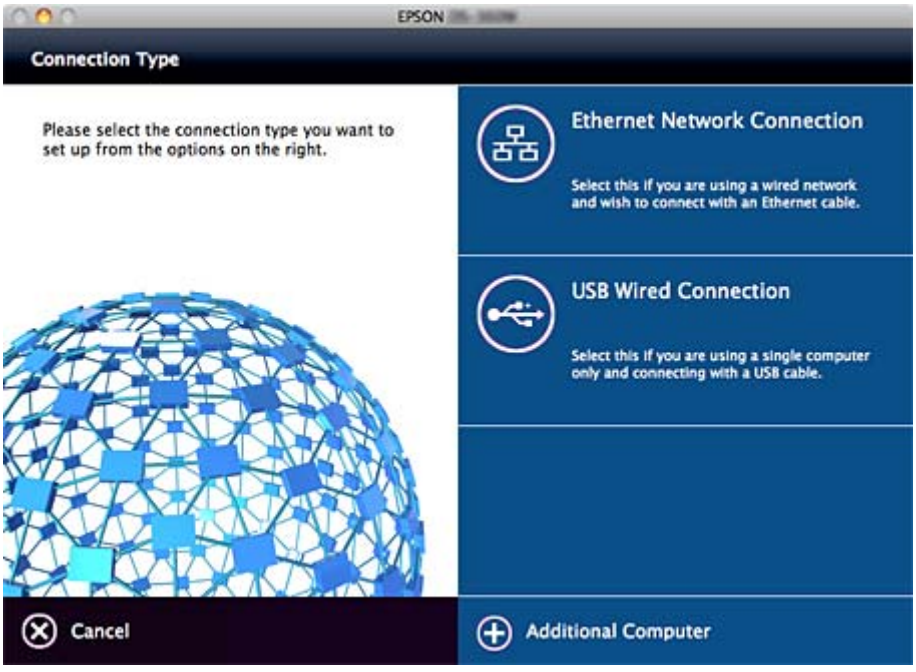
❏ Windows

Izaberite način povezivanja i kliknite na **Dalje**.



❏ Mac OS

Izaberite način povezivanja.



Priključivanje

Pratite uputstva na ekranu. Potreban softver je instaliran.

Podešavanje funkcija

U ovom poglavlju objašnjena su prva podešavanja koja treba napraviti kako bi se koristila svaka funkcija uređaja.

Softver za podešavanje

U ovom delu je objašnjen postupak za podešavanje s administratorskog računara pomoću Web Config.

Web Config (Veb-stranica za uređaj)

O aplikaciji Web Config

Web Config je aplikacija za podešavanje skenera koja se pokreće iz pregledača.

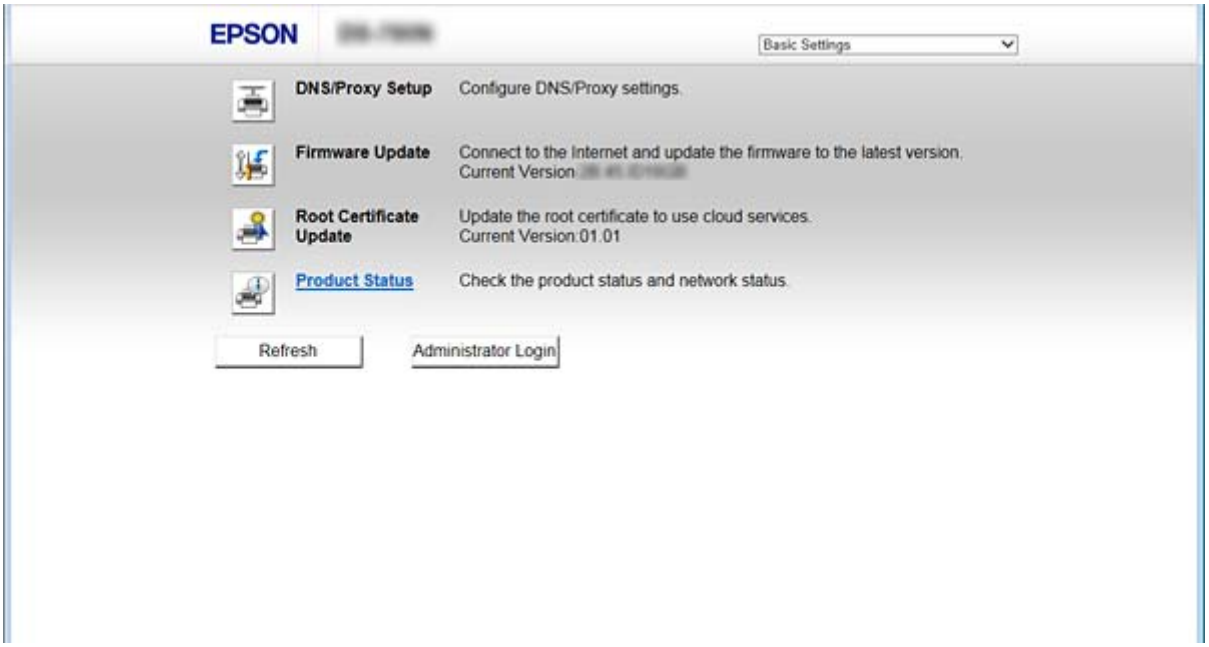
Da biste pristupili programu Web Config, potrebno je da prvo dodelite IP adresu skeneru.

Napomena:
Možete da zaključate postavke tako što ćete konfigurisati administratorsku lozinku za skener.

Postoje dve stranice za podešavanje, kao što je prikazano u produžetku.

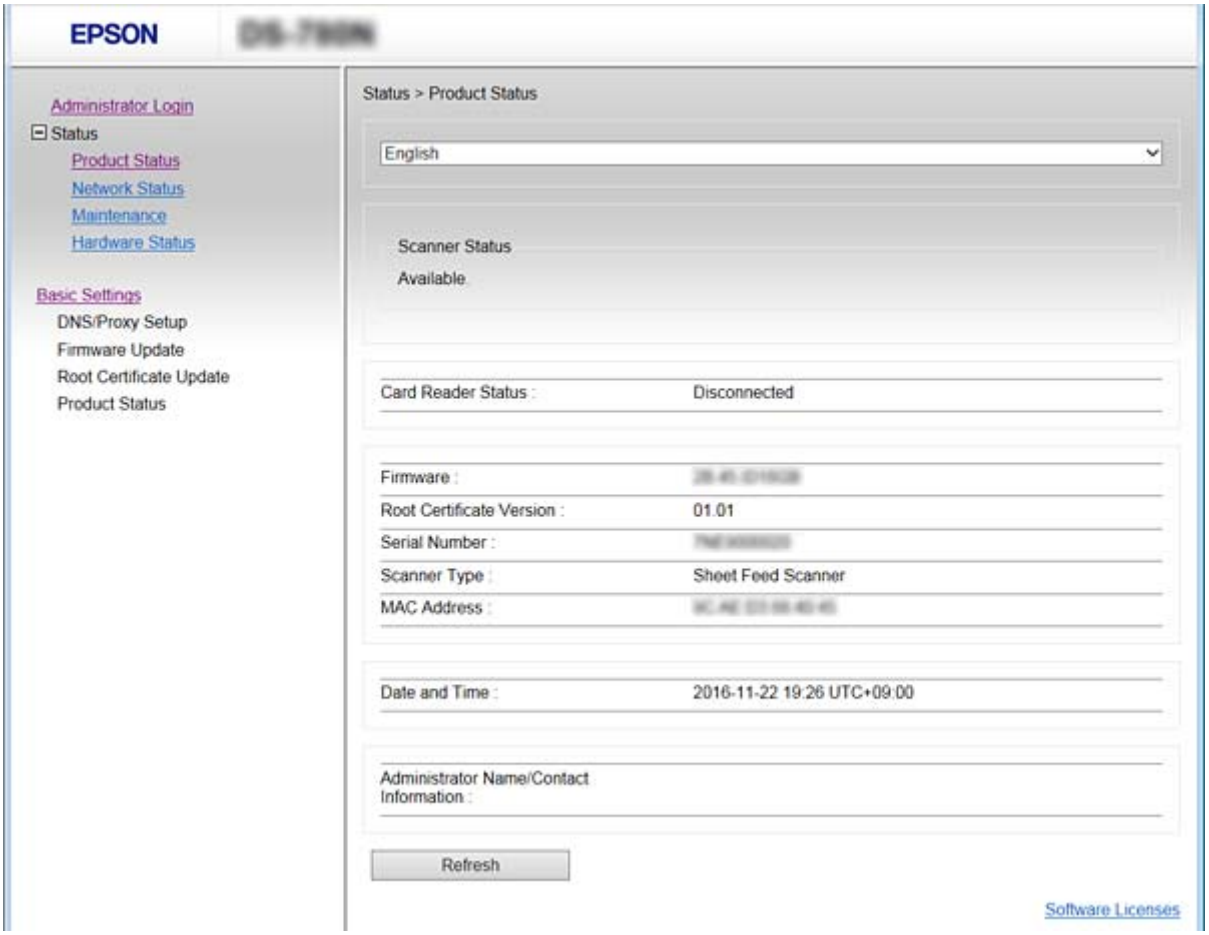
❏ **Basic Settings**

Možete da konfigurišete osnovne postavke skenera.



❏ **Advanced Settings**

Možete da konfigurišete napredne postavke skenera. Ova stranica je uglavnom namenjena administratorima.



Pristup programu Web Config

Unesite IP adresu skenera u veb pregledač. JavaScript mora biti uključen. Kada pristupate programu Web Config putem HTTPS, u pregledaču će se pojaviti poruka upozorenja, jer se koristi nezavisni sertifikat, sačuvan u skeneru.

❏ Pristup preko protokola HTTPS

IPv4: https://<IP adresa skenera> (bez < >)

IPv6: https://[IP adresa skenera]/ (sa [ ])

❏ Pristup preko protokola HTTP

IPv4: http://<IP adresa skenera> (bez < >)

IPv6: http://[IP adresa skenera]/ (sa [ ])

Napomena:

❏ *Primeri*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Ako je ime skenera registrovano na DNS serveru, možete da koristite ime skenera umesto IP adrese.*

Povezane informacije

➡ "SSL/TLS komunikacija sa skenerom" na strani 63

➡ "O digitalnim sertifikatima" na strani 63

Korišćenje funkcija skeniranja

Zavisno od toga kako koristite skener, instalirajte sledeći softver i izvršiti podešavanja pomoću njega.

❏ **Skeniraj sa računara**

❏ Proverite rok važenja usluge skeniranja na mreži pomoću Web Config (rok pri isporuci iz fabrike).

❏ Instalirajte Epson Scan 2 na svoj računar i podesite IP adresu.

❏ Prilikom skeniranja uz korišćenje zadataka, instalirajte Document Capture Pro (Document Capture) i podesite postavke zadatka.

❏ **Skeniraj sa kontrolne table**

❏ Ako se koristi Document Capture Pro ili Document Capture Pro Server:

Instalirajte Document Capture Pro ili Document Capture Pro Server

DCP podešavanje (režim servera, režim klijenta).

❏ Ako se koristi WSD protokol:

Proverite rok važenja WSD protokola na Web Config ili kontrolnoj tabli (rok pri isporuci iz fabrike).

Dodatna podešavanja uređaja (Windows računar).

Skeniranje s računara

Instalirajte softver i proverite da li je omogućena usluga skeniranja na mreži da biste mogli da skenirate s računara putem mreže.

Povezane informacije

➡ "Softver koji treba instalirati" na strani 25

➡ "Omogućavanje skeniranja mreže" na strani 25

Softver koji treba instalirati

❏ Epson Scan 2

Ovo je upravljački program skenera. Ako koristite uređaj s računara, instalirajte upravljački program na svaki računar klijent. Ako je instaliran Document Capture Pro/Document Capture, možete vršiti radnje koje su dodeljene tasterima uređaja.

Upravljački programi štampača takođe se mogu distribuirati zajedno u paketima pomoću EpsonNet SetupManager.

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

Instalirajte na računar klijent. Možete s kontrolne table računara i skenera pozvati i izvršiti zadatak koji je registrovan na računaru uz pomoć Document Capture Pro/Document Capture koji je instaliran na mreži.

Takođe možete putem mreže skenirati sa računara. Za skeniranje je potreban Epson Scan 2.

Povezane informacije

➡ "EpsonNet SetupManager" na strani 56

Podesite IP adresu skenera na Epson Scan 2

Odredite IP adresu skenera tako da se skener može koristiti na mreži.

1. Pokrenite **Epson Scan 2 Utility** iz menija **Start** > **Svi programi** > **EPSON** > **Epson Scan 2**.

   Ako je već registrovan neki drugi skener, idite na korak 2.

   Ako nije registrovan, idite na korak 4.

2. Kliknite na ▼ na **Skener**.
3. Kliknite na **Podešavanja**.
4. Kliknite **Omogući uređivanje**, a zatim kliknite na **Dodaj**.
5. Izaberite naziv modela skenera iz menija **Model**.
6. Izaberite IP adresu skenera koji će se koristiti iz menija **Adresa** u **Pretraga mreža**.

   Kliknite na  i kliknite na  da biste ažurirali listu. Ako ne možete da nađete IP adresu skenera, izaberite **Unesite adresu** i unesite IP adresu.

7. Kliknite na **Dodaj**.
8. Kliknite na **U redu**.

Omogućavanje skeniranja mreže

Uslugu skeniranja mreže možete podesiti kada skenirate s kompjutera klijenta preko mreže. Podrazumevano podešavanje je omogućeno.

1. Pristupite programu Web Config i odaberite **Services** > **Network Scan**.

2. Proverite da li je odabrano **Enable scanning** u **EPSON Scan**.

   Ako je odabrano, ovaj zadatak je završen. Zatvorite Web Config.

   Ako nije obeleženo, izaberite ga i pređite na sledeći korak.

3. Kliknite na **Next**.

4. Kliknite na **OK**.

   Mreža se ponovo povezuje i podešavanja su nakon toga omogućena.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Skeniranje pomoću kontrolne table

Funkcija skeniranja u fasciklu i funkcija skeniranja u e-poruku pomoću kontrolne table skenera, kao i prenos rezultata skeniranja u e-poruku, fascikle itd. vrše se obavljanjem zadatka sa računara.

Prilikom prenosa rezultata skeniranja podesite zadatak pomoću Document Capture Pro Server ili Document Capture Pro.

Detalje o podešavanjima i postavljanju zadatka potražite u pomoći za Document Capture Pro Server ili Document Capture Pro.

Povezane informacije

➡ "Podešavanja Document Capture Pro Server/Document Capture Pro" na strani 26

➡ "Podešavanja servera i fascikli" na strani 27

Softver za instalaciju na računaru

❏ **Document Capture Pro Server**

Ovo je verzija servera Document Capture Pro. Instalirajte je na Windows server. Moguće je centralno upravljanje sa više uređaja i zadataka putem servera. Zadaci se mogu izvršiti istovremeno sa više skenera.

Koristeći sertifikovanu verziju Document Capture Pro Server, možete upravljati zadacima i analizirati istoriju povezanu sa korisnicima i grupama.

Radi detalja o Document Capture Pro Server obratite se lokalnom sedištu kompanije Epson.

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

Kao i u slučaju skeniranja s računara, možete s kontrolne table pozvati i izvršiti zadatke koji su registrovani na računaru. Nije moguće istovremeno pokrenuti zadatke na računaru sa više skenera.

Podešavanja Document Capture Pro Server/Document Capture Pro

Izvršite podešavanja za korišćenje funkcije skeniranja sa kontrolne table skenera.

1. Pristupite programu Web Config i odaberite **Services** > **Document Capture Pro**.

2. Izaberite **Režim rada**.

   ❏ Server Mode:

   Izaberite ga kada koristite Document Capture Pro Server ili kada koristite Document Capture Pro samo za zadatke koji su postavljeni za određeni računar.

   ❏ Client Mode:

   Postavite ga kada izaberete podešavanje zadatka Document Capture Pro (Document Capture) koje je instalirano na svakom računaru klijentu na mreži bez navođenja računara.

3. Podesite sledeće u skladu sa izabranim režimom.

   ❏ Server Mode:

   U **Server Address** odredite server na kom je instaliran Document Capture Pro Server. Može biti između 2 i 252 znakova u formatu IPv4, IPv6 ili FQDN ili naziv hosta. U formatu FQDN možete koristiti US-ASCII simbole, brojeve, slova i crtice (osim početnih i pratećih).

   ❏ Client Mode:

   Odredite **Group Settings** da biste koristili grupu skenera navedenu u Document Capture Pro (Document Capture).

4. Kliknite na **Podešavanja**.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Podešavanja servera i fascikli

Document Capture Pro i Document Capture Pro Server čuvaju skenirane podatke na serveru ili računaru klijentu jedanput i koriste funkciju prenosa da bi se izvršila funkcija skeniranja u fasciklu i funkciju skeniranja u e-poruku.

Potrebno vam je ovlašćenje i informacije za prenos sa računara na kom je instaliran Document Capture Pro, Document Capture Pro Server na računar ili u uslugu računarskog oblaka.

Pripremite informacije o funkciji koju ćete koristiti, a koje se odnose na sledeće.

Možete izvršiti podešavanja za ove funkcije pomoću Document Capture Pro ili Document Capture Pro Server. Detalje o podešavanjima potražite u dokumentaciji ili pomoći za Document Capture Pro Server ili Document Capture Pro.

Naziv	Podešavanja	Zahtev
Skeniranje u mrežnu fasciklu (eng. Scan to Network Folder) (SMB)	Napravite fasciklu za čuvanje dokumenata i podesite njeno deljenje	Administratorski korisnički nalog za računar koji kreira fascikle za čuvanje dokumenata.
	Odredište mrežne fascikle za čuvanje skeniranih dokumenata (SMB)	Korisničko ime i lozinka za prijavu na računar na kom se nalazi fascikla za čuvanje skeniranih dokumenata, kao i privilegija za ažuriranje te fascikle.
Skeniranje u mrežnu fasciklu (eng. Scan to Network Folder) (FTP)	Podešavanje prijavljivanja na FTP server	Informacije za prijavljivanje na FTP server i privilegija za ažuriranje fascikle za čuvanje skeniranih dokumenata.
Skeniranje u e-poruku (eng. Scan to Email)	Podešavanje servera za e-poštu	Podešavanje informacija o serveru za e-poštu

Naziv	Podešavanja	Zahtev
Skeniranje u Document Capture Pro (kada se koristi Document Capture Pro Server)	Podešavanje za prijavljivanje na usluge računarskog oblaka	Okruženje s pristupom internetu Registracija računa za usluge računarskog oblaka

Korišćenje WSD skeniranja (samo za Windows)

Ako računar koristi verziju Windows Vista ili kasniju, možete koristiti WSD skeniranje.

Kada se može koristiti WSD protokol, na kontrolnoj tabli skenera prikazaće se meni **Računar (WSD)**.

1. Pristupite programu Web Config i odaberite **Services** > **Protocol**.
2. Uverite se da je opcija **Enable WSD** zabeležena u **WSD Settings**.
   Ako je zabeležena, vaš zadatak je završen i možete da zatvorite Web Config.
   Ako nije zabeležena, uradite to i pređite na sledeći korak.
3. Kliknite na dugme **Next**.
4. Potvrdite podešavanja i kliknite na **Podešavanja**.

Vršenje sistemskih podešavanja

Vršenje sistemskih podešavanja na kontrolnoj tabli

Podešavanje osvetljenost ekrana

Podesite osvetljenost LCD ekrana.

1. Dodirnite **Podešavanja** na početnom ekranu.
2. Dodirnite **Uobičajena podešavanja** > **Osvetljenost LCD-a**.
3. Dodirnite  ili  da biste podesili osvetljenost.
   Možete podesiti od 1 do 9.
4. Dodirnite **U redu**.

Podešavanje zvuka

Podesite radni zvuk za tablu i zvuk za grešku.

1. Dodirnite **Podešavanja** na početnom ekranu.

2. Dodirnite **Uobičajena podešavanja** > **Zvuk**.
3. Podesite sledeće stavke po potrebi.
   - ❏ Radni zvuk
     Podesite jačinu radnog zvuka kontrolne table.
   - ❏ Zvuk za grešku
     Podesite jačinu zvuka za grešku.
4. Dodirnite **U redu**.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Prepoznavanje dvostrukog uvlačenja originala

Odredite funkciju za prepoznavanje dvostrukog uvlačenja dokumenta za skeniranje i za zaustavljanje skeniranja kada dođe do dvostrukog uvlačenja.

Da biste skenirali originale za koje se veruje da će doći do dvostrukog uvlačenja, kao što su koverte ili papir sa nalepnicama, odvojite ih.

Napomena:
To se može podisiti i iz Web Config ili Epson Scan 2.

1. Dodirnite **Podešavanja** na početnom ekranu.
2. Dodirnite **Spoljne Postavke skeniranja** > **Ultrasonic otkrivanje duplog uvlačenja**.
3. Dodirnite **Ultrasonic otkrivanje duplog uvlačenja** da biste uključili ili isključili tu opciju.
4. Dodirnite **Zatvori**.

Podešavanje režima sporog rada

Podesite skeniranje pri malim brzinama, tako da ne dolazi do zaglavljivanja papira prilikom skeniranja tankih originala poput ceduljica.

1. Dodirnite **Podešavanja** na početnom ekranu.
2. Dodirnite **Spoljne Postavke skeniranja** > **Sporo**.
3. Dodirnite **Sporo** da biste uključili ili isključili tu opciju.
4. Dodirnite **Zatvori**.

Vršenje sistemskih podešavanja pomoću Web Config

Podešavanja za uštedu energije tokom perioda neaktivnosti

Podesite uštedu energije za period neaktivnosti skenera. Vreme podesite u zavisnosti od okruženja u kom ga koristite.

Napomena:
Takođe možete izvršiti podešavanja za uštedu energije na kontrolnoj tabli skenera.

1. Pristupite programu Web Config i odaberite **System Settings** > **Power Saving**.
2. Unesite vreme u **Sleep Timer** kako bi se uređaj prebacio u režim uštede energije u periodu neaktivnosti.

   Možete podesiti trajanje do 240 minuta u minutama.
3. Podesite vreme isključivanja u **Power Off Timer**.
4. Kliknite na **OK**.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Podešavanje kontrolne table

Podešavanje kontrolne table skenera. Možete je podesiti na sledeći način.

1. Pristupite programu Web Config i odaberite **System Settings** > **Control Panel**.
2. Odredite sledeće stavke po potrebi.

   ❏ Language

   Izaberite jezik na kom će biti prikazana kontrolna tabla.

   ❏ Panel Lock

   Ako odaberete **ON**, biće potrebna administratorska lozinka kada vršite neku radnju koja zahteva administratorska ovlašćenja. Ako administratorska lozinka nije podešena, zaključavanje table je onemogućeno.

   ❏ Operation Timeout

   Ako odaberete **ON**, kada se prijavite kao administrator, bićete automatski odjavljeni i vraćeni na početni ekran ako tokom određenog perioda ne budete aktivni.

   Možete podesiti dužinu tog perioda od 10 sekundi do 240 minuta u sekundama.
3. Kliknite na **OK**.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Podešavanje ograničenja spoljašnjeg interfejsa

Možete ograničiti USB vezu s računara. Podesite je tako da ograničite skeniranje samo na skeniranje putem mreže.

1. Pristupite programu Web Config i odaberite **System Settings** > **External Interface**.
2. Izaberite **Enable** ili **Disable**.

   Da biste ograničili, izaberite **Disable**.
3. Dodirnite **OK**.

Sinhronizacija datuma i vremena sa serverom za vreme

Ako koristite CA sertifikat, možete sprečiti probleme s vremenom.

1. Pristupite programu Web Config i odaberite **System Settings** > **Date and Time** > **Time Server**.
2. Izaberite **Use** za **Use Time Server**.
3. Unesite adresu vremenskog servera u **Time Server Address**.

   Možete da koristite format IPv4, IPv6 ili FQDN. Unesite najviše 252 znaka. Ako ovo ne navodite, ostavite prazno.
4. Unesite **Update Interval (min)**.

   Možete podesiti trajanje do 10.800 minuta u minutama.
5. Kliknite na **OK**.

   Napomena:
   *Možete potvrditi status veze s vremenskim serverom u **Time Server Status**.*

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

Osnovne bezbednosne postavke

U ovom poglavlju objašnjene su osnovne bezbednosne postavke koje ne zahtevaju specijalno okruženje.

Predstavljanje osnovnih bezbednosnih funkcija

Predstavljamo osnovne bezbednosne funkcije Epson uređaja.

Naziv funkcije	Vrsta funkcije	Šta treba podesiti	Šta treba sprečiti
Postavljanje administratorske lozinke	Zaključajte podešavanja koja se odnose na sistem, kao što su podešavanja mreže i USB veze, tako da ih može promeniti samo administrator.	Administrator postavlja lozinku na uređaj. Konfigurisanje ili ažuriranje se mogu izvršiti iz bilo koje od sledećih stavki: Web Config, kontrolna tabla, Epson Device Admin, kao i EpsonNet Config.	Sprečava neovlašćeno očitavanje i menjanje informacija uskladištenih u uređaju, poput ID oznake, lozinke, mrežnih podešavanja i kontakata. Isto tako, smanjuje stepen širokog raspona bezbednosnih rizika, poput curenja informacija iz mrežnog okruženja ili bezbednosne smernice.
SSL/TLS komunikacije	Kada se Epsonovom serveru na internetu pristupa sa uređaja, poput komunikacije s računarom putem veb pregledača ili ažuriranja upravljačkog softvera, sadržaj komunikacije je šifrovan SSL/TLS protokolima.	Pribavite CA sertifikat, a zatim ga uvezite u skener.	Identifikacija uređaja pomoću CA sertifikata sprečava lažno predstavljanje i neovlašćeni pristup. Pored toga, sadržaj komunikacije putem SSL/TLS protokola je zaštićen i time se sprečava curenje sadržaja za štampanje i informacija o postavkama.
Protokoli kontrola	Protokoli kontrola koristi se za komunikaciju između uređaja i računara, i omogućava/onemogućava funkcije.	Protokol ili usluga koja važi za funkcije koje se dozvoljavaju ili zabranjuju na individualnoj osnovi.	Smanjenje bezbednosnih rizika koji se mogu javiti prilikom nenamerne upotrebe time što korisnici budu sprečeni da koriste nepotrebne funkcije.

Povezane informacije

➡ “O aplikaciji Web Config” na strani 22
➡ “EpsonNet Config” na strani 55
➡ “Epson Device Admin” na strani 55
➡ “Konfigurisanje administratorske lozinke” na strani 32
➡ “Kontrolisanje protokola” na strani 35

Konfigurisanje administratorske lozinke

Kada postavite administratorsku lozinku, korisnici koji nisu administratori neće moći da menjaju postavke za upravljanje sistemom. Administratorsku lozinku možete postaviti ili promeniti pomoću Web Config, kontrolne

table skenera ili softvera (Epson Device Admin ili EpsonNet Config). Kada koristite softver, pogledajte dokumentaciju za njega.

Povezane informacije

➡ "Konfigurisanje administratorske lozinke na kontrolnoj tabli" na strani 33
➡ "Konfigurisanje administratorske lozinke pomoću Web Config" na strani 33
➡ "EpsonNet Config" na strani 55
➡ "Epson Device Admin" na strani 55

Konfigurisanje administratorske lozinke na kontrolnoj tabli

Administratorsku lozinku možete postaviti na kontrolnoj tabli skenera.

1. Dodirnite **Podešavanja** na početnom ekranu.
2. Dodirnite **Administracija sistema** > **Administratorska podešavanja**.

   Ako stavka ne bude prikazana, povucite prstom prema gore kako bi se pojavila.
3. Dodirnite **Lozinka administratora** > **Registruj**.
4. Unesite novu lozinku, a zatim dodirnite **U redu**.
5. Ponovo unesite lozinku, a zatim dodirnite **U redu**.
6. Dodirnite **U redu** na ekranu za potvrdu.

   Prikazaće se ekran sa administratorskim postavkama.
7. Dodirnite **Zaključavanje podešavanja**, a zatim dodirnite **U redu** na ekranu za potvrdu.

   Zaključavanje podešavanja je postavljeno na **Uklj.**, a kada budete želeli da rukujete zaključanom stavkom na meniju biće vam potrebna administratorska lozinka.

Napomena:

❏ *Ako **Podešavanja** > **Uobičajena podešavanja** > **Vreme čekanja na radnju** postavite na **Uklj.**, skener će vas odjaviti nakon određenog perioda neaktivnosti na kontrolnoj tabli.*

❏ *Administratorsku lozinku možete da promenite ili izbrišete kada odaberete **Promeni** ili **Resetuj** na ekranu **Lozinka administratora** i unesete administratorsku lozinku.*

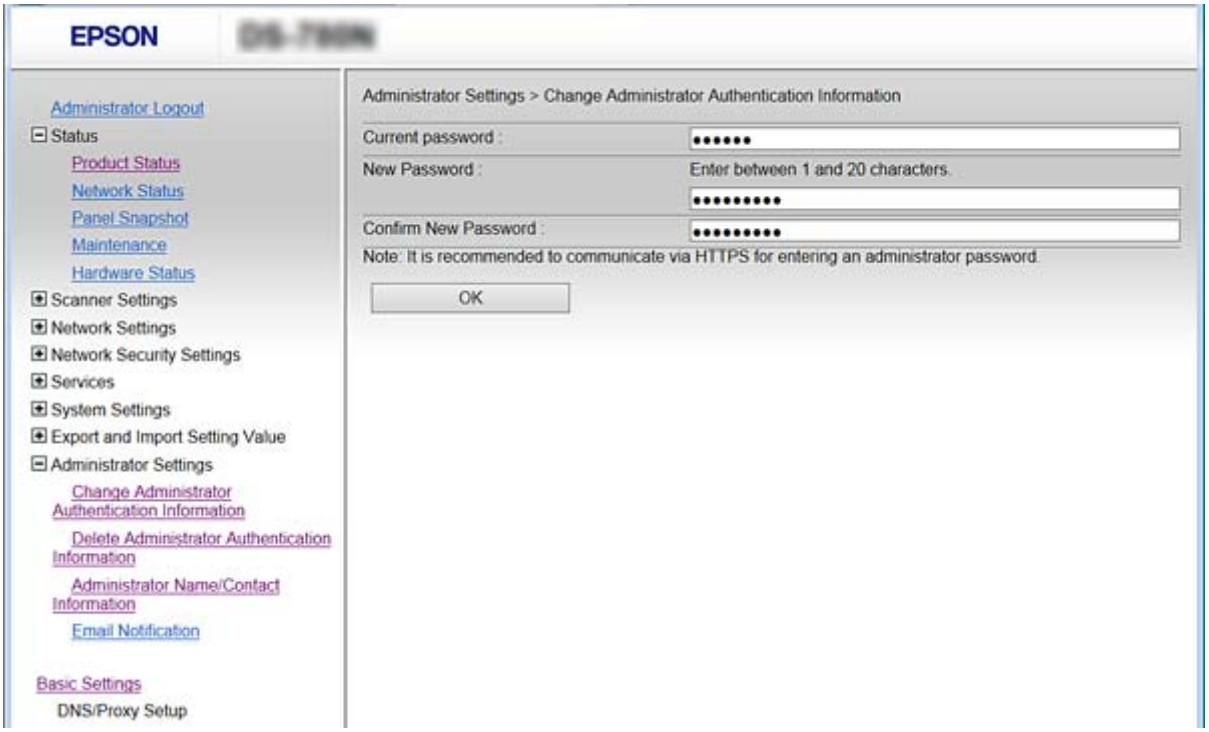
Konfigurisanje administratorske lozinke pomoću Web Config

Administratorsku lozinku možete postaviti pomoću Web Config.

1. Pristupite programu Web Config i odaberite **Administrator Settings** > **Change Administrator Authentication Information**.

2. Unesite lozinku u polja **New Password** i **Confirm New Password**. Unesite korisničko ime ako je potrebno.

   Ako želite da zamenite lozinku novom, unesite aktuelnu lozinku.



3. Izaberite **OK**.

   Napomena:

   ❏ *Da biste postavili ili promenili stavke u zaključanom meniju, kliknite na **Administrator Login**, a zatim unesite administratorsku lozinku.*

   ❏ *Da biste izbrisali administratorsku lozinku, kliknite na **Administrator Settings** > **Delete Administrator Authentication Information**, a zatim unesite administratorsku lozinku.*

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Stavke koje mogu biti zaključane administratorskom lozinkom

Administratori imaju privilegije za podešavanje i menjanje postavki svih funkcija na uređajima.

Takođe, ako na uređaju postavite administratorsku lozinku, možete ga zaključati, tako da ne možete menjati stavke koje se odnose na upravljanje uređajem.

Stavke koje administrator može da kontroliše jesu sledeće.

Stavka	Opis
Podešavanje skenera	Podešavanje otkrivanja dvostrukog uvlačenja i režima sporog rada.

Osnovne bezbednosne postavke

Stavka	Opis
Podešavanja Ethernet veze	Promena naziva uređaja i IP adrese, postavljanje DNS servera ili proksi servera, kao i podešavanje promena u vezi s mrežnim povezivanjem.
Podešavanje korisničkih usluga	Postavke za kontrolisanje komunikacionih protokola ili usluga skeniranje mreže i Document Capture Pro.
Podešavanje servera e-pošte	Postavke servera e-pošte s kojim uređaji komuniciraju direktno.
Bezbednosno podešavanje	Podešavanja za bezbednost na mreži, poput SSL/TLS komunikacionih protokola, IPsec/IP filtriranja i IEEE802.1X.
Ažuriranje korenskog sertifikata	Ažuriranje korenskih sertifikata potrebno za autenfitikaciju Document Capture Pro Server i ažuriranje upravljačkog programa iz Web Config.
Ažuriranje upravljačkog softvera	Provera i ažuriranje upravljačkog softvera za uređaje.
Vreme, podešavanje sata	Vreme prelaska u pasivni režim, automatsko isključivanje, datum/vreme, sat za merenje neaktivnog vremena, druga podešavanja u vezi sa satom.
Vrati na podrazumevana podešavanja	Podešavanje vraćanja skenera na fabrička podešavanja.
Podešavanje za administratore	Podešavanje zaključavanja ili administratorske lozinke.
Podešavanje sertifikovanog uređaja	Podešavanje ID oznake uređaja za proveru identiteta. Podesite ovu stavku kada koristite skener u sistemu za proveru identiteta koji podržava uređaje za proveru identiteta.

Kontrolisanje protokola

Možete da skenirate pomoću raznih putanja i protokola. Takođe možete da koristite skeniranje mreže sa neograničenog broja mrežnih računara. Na primer, dozvoljeno je skeniranje samo uz pomoć određenh putanja i protokola. Možete da smanjite nenamerne bezbednosne rizike ograničavanjem na skeniranje sa određenih putanja ili kontrolisanjem dostupnih funkcija.

Konfigurišite podešavanja protokola.

1. Pristupite programu Web Config i odaberite **Services** > **Protocol**.
2. Konfigurišite svaku stavku.
3. Kliknite na **Next**.
4. Kliknite na **OK**.

   Podešavanja će biti primenjena na skener.

Povezane informacije

➡ “Pristup programu Web Config” na strani 23
➡ “Protokoli koje možete da omogućite ili onemogućite” na strani 36
➡ “Stavke podešavanja protokola” na strani 37

Protokoli koje možete da omogućite ili onemogućite

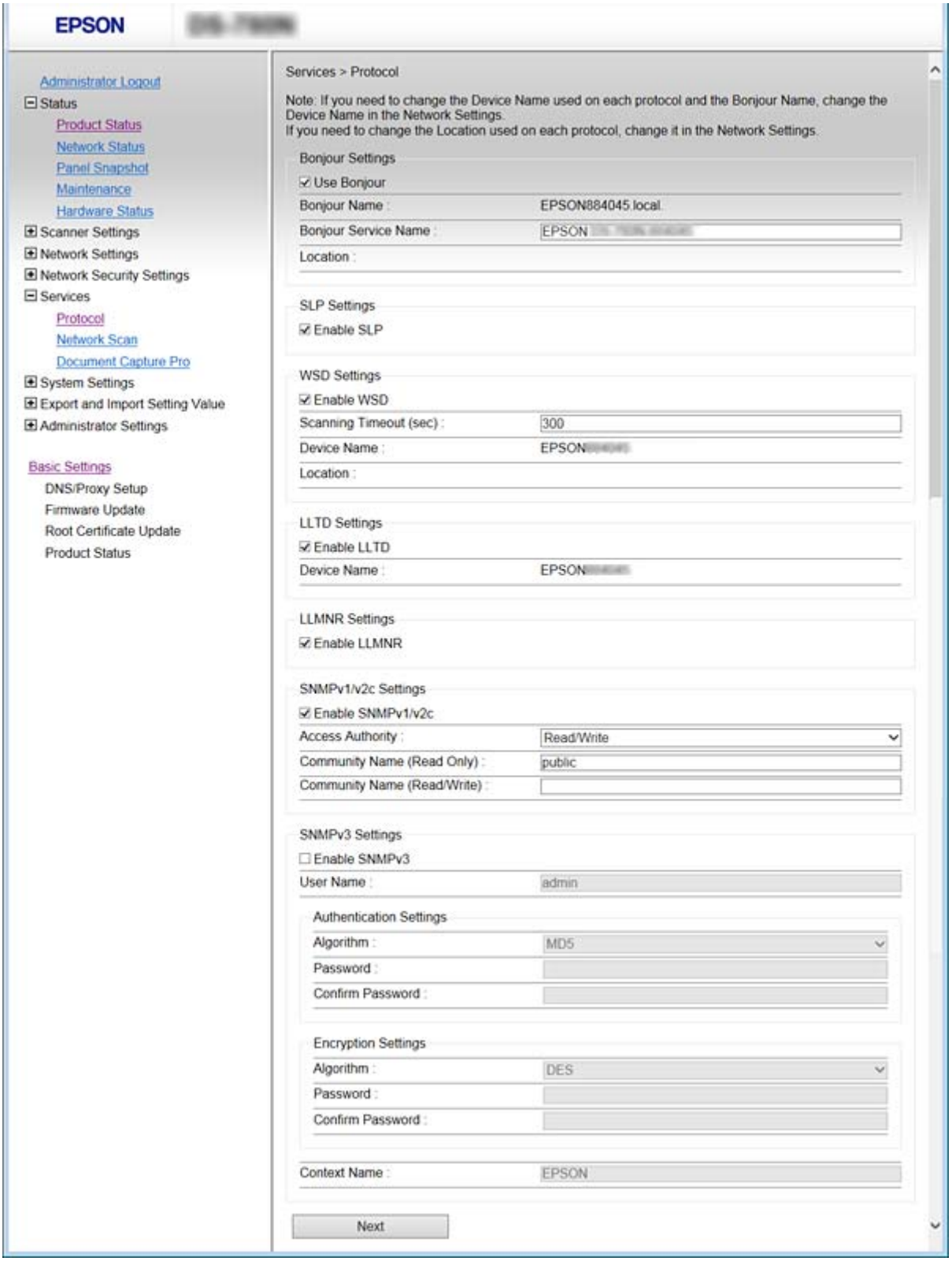
Protokol	Opis
Bonjour Settings	Možete da navedete želite li da koristite Bonjour. Bonjour se koristi za pronalaženje uređaja, skeniranje i tako dalje.
SLP Settings	Možete da omogućite ili onemogućite funkciju SLP. SLP se koristi za Epson Scan 2 i pretraživanje mreže u programu EpsonNet Config.
WSD Settings	Možete da omogućite ili onemogućite WSD funkciju. Kada je omogućena, možete da dodajete WSD uređaje ili skenirate sa WSD ulaza.
LLTD Settings	Možete da omogućite ili onemogućite funkciju LLTD. Kada je omogućena, biće prikazana Windows mapi mreže.
LLMNR Settings	Možete da omogućite ili onemogućite funkciju LLMNR. Kada je omogućena, možete da koristite razrešavanje imena bez NetBIOS čak i ako ne možete da koristite DNS.
SNMPv1/v2c Settings	Možete da navedete želite li ili ne da omogućite SNMPv1/v2c. Koristi se za podešavanje uređaja, nadgledanje i tako dalje.
SNMPv3 Settings	Možete da navedete želite li ili ne da omogućite SNMPv3. Koristi se za podešavanje šifrovanih uređaja, nadgledanje i tako dalje.

Povezane informacije

➡ “Kontrolisanje protokola” na strani 35

➡ “Stavke podešavanja protokola” na strani 37

Stavke podešavanja protokola



Stavke	Vrednost i opis podešavanja
Bonjour Settings	

Osnovne bezbednosne postavke

Stavke	Vrednost i opis podešavanja
Use Bonjour	Izaberite da biste potražili ili koristili uređaje kroz Bonjour.
Bonjour Name	Prikazuje Bonjour ime.
Bonjour Service Name	Možete prikazati i podesiti naziv usluge Bonjour.
Location	Prikazuje Bonjour ime lokacije.
SLP Settings	
Enable SLP	Izaberite ovo da biste omogućili SLP funkciju. Koristi se za otkrivanje mreže u Epson Scan 2 i EpsonNet Config.
WSD Settings	
Enable WSD	Izaberite ovo da biste omogućili dodavanje uređaja koristeći WSD, kao i štampanje i skeniranje sa WSD ulaza.
Scanning Timeout (sec)	Unesite vreme isteka komunikacije za WSD skeniranje vrednosti između 3 i 3600 sekundi.
Device Name	Prikazuje WSD ime uređaja.
Location	Prikazuje WSD ime lokacije.
LLTD Settings	
Enable LLTD	Izaberite ovo da biste omogućili LLTD. Skener je prikazan u Windows mapi mreže.
Device Name	Prikazuje LLTD ime uređaja.
LLMNR Settings	
Enable LLMNR	Izaberite ovo da biste omogućili LLMNR. Možete da koristite razrešavanje imena bez NetBIOS čak i ako ne možete da koristite DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Izaberite da biste omogućili SNMPv1/v2c. Prikazani su samo SNMPv3 skeneri.
Access Authority	Podesite pristupno telo kada je omogućen SNMPv1/v2c. Izaberite **Read Only** ili **Read/Write**.
Community Name (Read Only)	Unesite između 0 i 32 ASCII (od 0x20 do 0x7E) znaka.
Community Name (Read/Write)	Unesite između 0 i 32 ASCII (od 0x20 do 0x7E) znaka.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 je omogućen kada je polje obeleženo.
User Name	Unesite između 1 i 32 znaka koristeći znakove dužine jednog bajta.
Authentication Settings	
Algorithm	Odaberite algoritam za proveru identiteta za SNMPv3.

Osnovne bezbednosne postavke

Stavke	Vrednost i opis podešavanja
Password	Unesite lozinku za proveru identiteta za SNMPv3. Unesite između 8 i 32 znakova u formatu ASCII (0x20–0x7E). Ako ovo ne navodite, ostavite prazno.
Confirm Password	Kao potvrdu, unesite lozinku koju ste konfigurisali.
Encryption Settings	
Algorithm	Odaberite algoritam za šifrovanje za SNMPv3.
Password	Unesite lozinku za šifrovanje za SNMPv3. Unesite između 8 i 32 znakova u formatu ASCII (0x20–0x7E). Ako ovo ne navodite, ostavite prazno.
Confirm Password	Kao potvrdu, unesite lozinku koju ste konfigurisali.
Context Name	Unesite najviše 32 znaka u Unicode formatu (UTF-8). Ako ovo ne navodite, ostavite prazno. Broj znakova koji može biti unet zavisi od jezika.

Povezane informacije

➡ “Kontrolisanje protokola” na strani 35

➡ “Protokoli koje možete da omogućite ili onemogućite” na strani 36

Podešavanja u vezi s radom i upravljanjem

U ovom poglavlju objašnjene su stavke u vezi sa svakodnevnim radom uređaja i upravljanjem njime.

Potvrda informacija o uređaju

U stavki **Status**, pomoću Web Config, možete proveriti sledeće informacije o određenom uređaju.

❏ Product Status

Proverite jezik, status, broj proizvoda, MAC adresu itd.

❏ Network Status

Proverite informacije o statusu veze s mrežom, IP adresu, DNS server itd.

❏ Panel Snapshot

Prikažite sliku ekrana koji je prikazan na kontrolnoj tabli uređaja.

❏ Maintenance

Proverite datum početka, informacije o skeniranju itd.

❏ Hardware Status

Proverite status skenera.

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

Upravljanje uređajima (Epson Device Admin)

Koristeći Epson Device Admin, možete upravljati i rukovati mnogim uređajima. Epson Device Admin vam omogućava da upravljate uređajima koji se nalaze na drugoj mreži. U tekstu koji sledi dat je prikaz glavnih upravljačkih funkcija.

Više informacija o funkcijama i korišćenju softvera potražite u propratnoj dokumentaciji ili pomoći aplikacije Epson Device Admin.

❏ Otkrivanje uređaja

Možete otkriti uređaje na mreži, a zatim ih registrovati na spisak. Ako su Epson uređaji poput štampača i skenera priključeni na isti segment mreže kao i računar administratora, možete ih pronaći čak i ako im nije dodeljena IP adresa.

Možete takođe otkriti uređaje koji su priključeni na računare na mreži pomoću USB kablova. Treba da instalirate Epson Device USB Agent na kompjuter.

❏ Podešavanje uređaja

Možete da napravite šablon koji sadrži stavke podešavanja poput mrežnog interfejsa i izvora papira i primenite ih na druge uređaje kao deljene postavke. Kada je uređaj priključen na mrežu, možete dodeliti IP adresu uređaju kome IP adresa nije dodeljena.

❏ Nadgledanje uređaja

Možete redovno dobijati informacije o statusu, kao i detaljne informacije o uređajima na mreži. Možete takođe i nadgledati uređaje koji su priključeni na računare na mreži pomoću USB kablova, kao i uređaje iz drugih kompanija koji su registrovani na spisku uređaja. Da biste mogli da nadgledate uređaje priključene pomoću USB kablova, treba da instalirate Epson Device USB Agent.

❏ Upravljanje upozorenjima

Možete nadgledati upozorenja u vezi sa statusom uređaja i potrošnog materijala. Sistem automatski šalje administratoru obaveštenje putem e-pošte na osnovu postavljenih uslova.

❏ Upravljanje izveštajima

Možete praviti redovne izveštaje u skladu s tim kako sistem prikuplja podatke o korišćenju uređaja i potrošnih sredstava. Zatim možete da sačuvate te izveštaje i šaljete ih e-poštom.

Povezane informacije

➡ "Epson Device Admin" na strani 55

Primanje obaveštenja o događajima e-poštom

O obaveštenjima putem e-pošte

Možete da koristite ovu funkciju da biste dobili upozorenja putem e-pošte kada se događaj odigra. Možete registrovati do 5 elektronskih adresa i izabrati za koje događaje želite da dobijete obaveštenja.

Da bi se ova funkcija mogla koristiti, server za e-poštu mora biti konfigurisan.

Povezane informacije

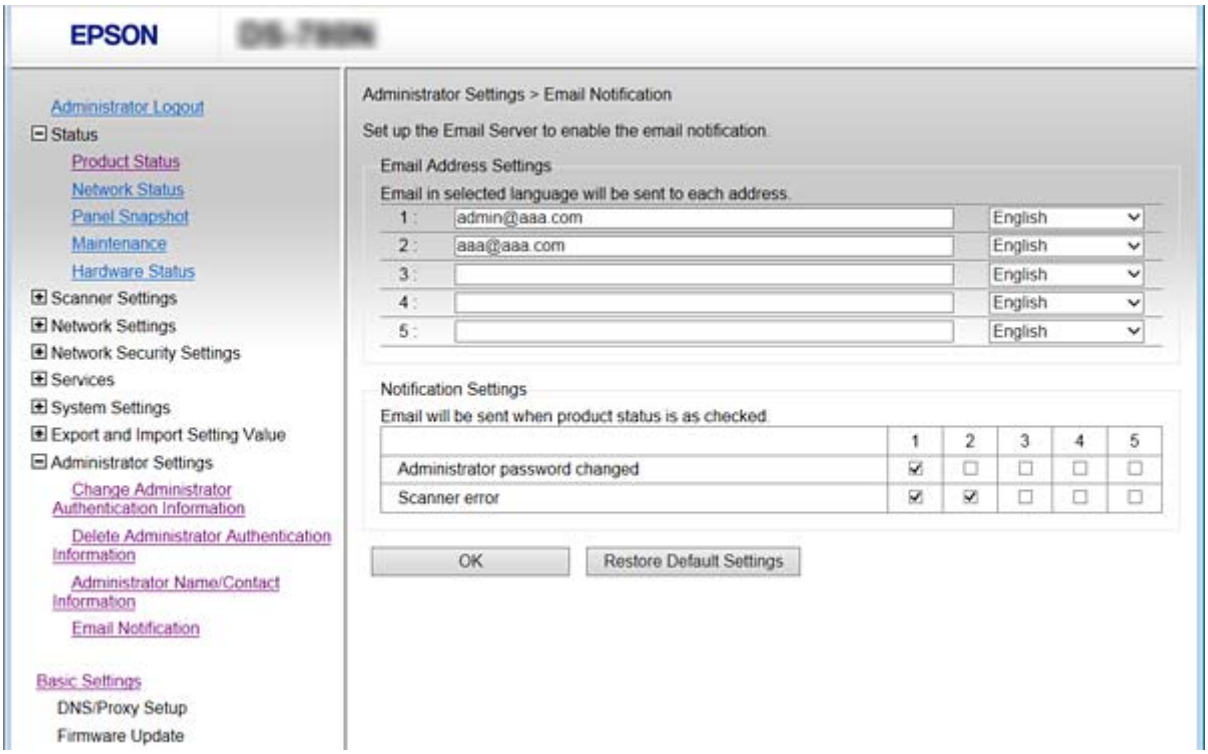
➡ "Konfigurisanje servera za poštu" na strani 42

Konfigurisanje obaveštenja putem e-pošte

Da biste mogli da koristite ovu funkciju, potrebno je da konfigurišete server za poštu.

1. Pristupite programu Web Config i izaberite **Administrator Settings** > **Email Notification**.
2. Unesite adresu e-pošte sa koje želite da dobijete obaveštenja.
3. Izaberite jezik za obaveštenja putem e-pošte.

4. Zabeležite polja za obaveštenja koja želite da dobijete.



5. Kliknite na **OK**.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23
➡ "Konfigurisanje servera za poštu" na strani 42

Konfigurisanje servera za poštu

Proverite sledeće pre konfigurisanja.

❏ Skener je povezan na mrežu.

❏ Informacije o serveru za e-poštu računara.

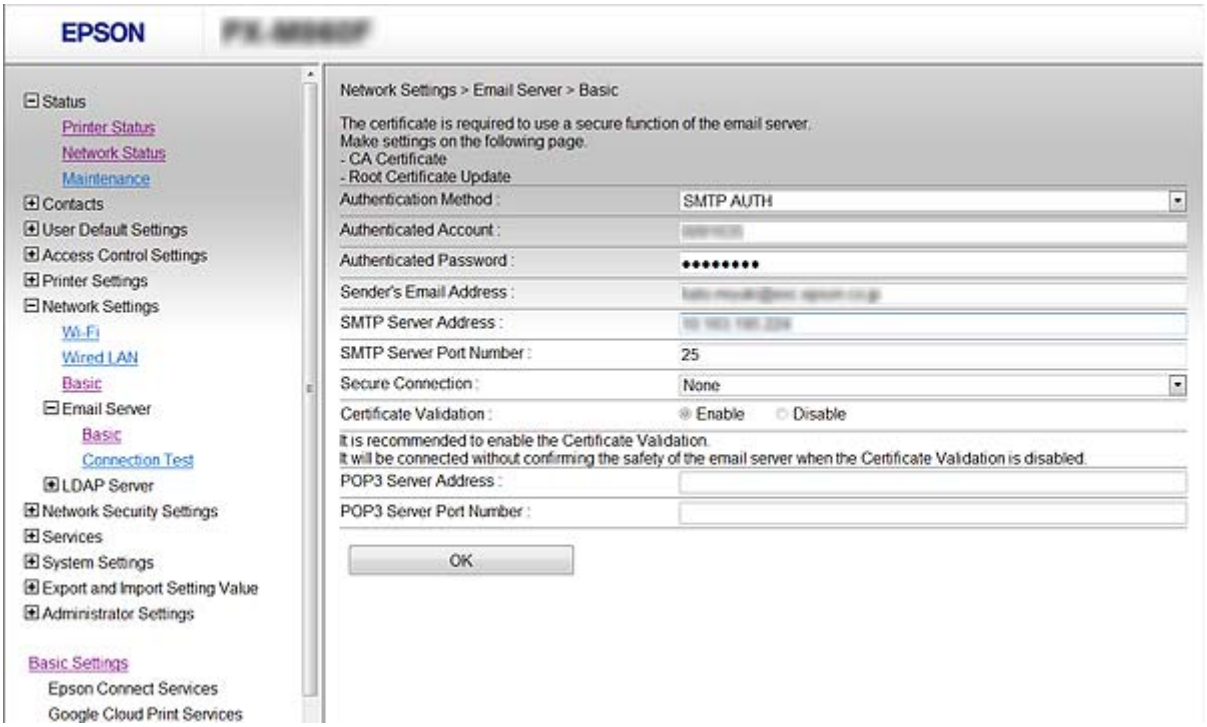
1. Pristupite programu Web Config i izaberite **Network Settings** > **Email Server** > **Basic**.
2. Izaberite jednu vrednost za svaku stavku.
3. Izaberite **OK**.

   Prikazaće se postavke koje ste izabrali.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23
➡ "Server za poštu — stavke podešavanja" na strani 43

Server za poštu — stavke podešavanja



Stavke	Podešavanja i objašnjenje	
Authentication Method	Navedite metod provere identiteta koji će se koristiti kada skener pristupa serveru za poštu.	
	Off	Autorizacija je onemogućena prilikom komunikacije sa serverom za poštu.
	SMTP AUTH	Zahteva da server za poštu podržava SMTP autorizaciju.
	POP before SMTP	Ako izaberete ovaj metod, konfigurišite POP3 server.
Authenticated Account	Ako izaberete **SMTP AUTH** ili **POP before SMTP** kao **Authentication Method**, unesite ime naloga za proveru identiteta dužine između 0 i 255 znakova u ASCII-ju (0x20 do 0x7E).	
Authenticated Password	Ako izaberete **SMTP AUTH** ili **POP before SMTP** kao **Authentication Method**, unesite autorizovanu lozinku između 0 i 20 znakova koristeći znakove A–Z, a–z i 0–9 i ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Unesite adresu e-pošte pošiljaoca. Unesite od 0 do 255 alfanumeričkih znakova u formatu ASCII (0x20–0x7E), osim : ( ) < > [ ] ; ¥. Tačka („.“) ne može da se nalazi na početnoj poziciji.	
SMTP Server Address	Unesite između 0 i 255 znakova koristeći znakove A–Z, a–z i 0–9. - . Možete da koristite format IPv4 ili FQDN.	
SMTP Server Port Number	Unesite broj između 1 i 65535.	

Stavke	Podešavanja i objašnjenje	
Secure Connection	Navedite metod bezbedne veze za server e-pošte.	
	None	Ako izaberete **POP before SMTP** u **Authentication Method**, metod povezivanja će biti podešen na **None**.
	SSL/TLS	Ovo je dostupno kada je **Authentication Method** podešen na **Off** ili **SMTP AUTH**.
	STARTTLS	Ovo je dostupno kada je **Authentication Method** podešen na **Off** ili **SMTP AUTH**.
Certificate Validation	Sertifikat se potvrđuje kada se ovo omogući. Preporučujemo da podesite na **Enable**.	
POP3 Server Address	Ako izaberete **POP before SMTP** kao **Authentication Method**, unesite adresu POP3 servera između 0 i 255 znakova koristeći znakove A–Z, a–z i 0–9. - . Možete da koristite format IPv4 ili FQDN.	
POP3 Server Port Number	Ako izaberete **POP before SMTP** kao **Authentication Method**, unesite broj od 1 do 65535.	

Povezane informacije

➡ "Konfigurisanje servera za poštu" na strani 42

Provera veze sa serverom za poštu

1. Pristupite programu Web Config i izaberite **Network Settings** > **Email Server** > **Connection Test**.
2. Izaberite **Start**.

   Započeće provera veze sa serverom e-pošte. Po završetku testiranja prikazaće se izveštaj o proveri.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23
➡ "Reference testiranja veze sa serverom za poštu" na strani 44

Reference testiranja veze sa serverom za poštu

Poruke	Objašnjenje
Connection test was successful.	Ova poruka se pojavljuje kada se uspostavi veza sa serverom.
SMTP server communication error. Check the following. - Network Settings	Ova poruka se pojavljuje u sledećim slučajevima ❏ Skener nije povezan na mrežu ❏ SMTP server ne radi ❏ Mrežna veza je prekinuta tokom komunikacije ❏ Primljeni su nepotpuni podaci

Podešavanja u vezi s radom i upravljanjem

Poruke	Objašnjenje
POP3 server communication error. Check the following. - Network Settings	Ova poruka se pojavljuje u sledećim slučajevima ❏ Skener nije povezan na mrežu ❏ POP3 server ne radi ❏ Mrežna veza je prekinuta tokom komunikacije ❏ Primljeni su nepotpuni podaci
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Ova poruka se pojavljuje u sledećim slučajevima ❏ Povezivanje sa DNS serverom nije uspelo ❏ Razrešavanje imena za SMTP server nije uspelo
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Ova poruka se pojavljuje u sledećim slučajevima ❏ Povezivanje sa DNS serverom nije uspelo ❏ Razrešavanje imena za POP3 server nije uspelo
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka se pojavljuje kada provera identiteta SMTP servera nije uspela.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka se pojavljuje kada provera identiteta POP3 servera nije uspela.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Ova poruka se pojavljuje kada pokušate da komunicirate sa nepodržanim protokolima.
Connection to SMTP server failed. Change Secure Connection to None.	Ova poruka se pojavljuje kada dođe do SMTP neslaganja između servera i klijenta ili kada server ne podržava SMTP bezbednu vezu (SSL vezu).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Ova poruka se pojavljuje kada dođe do SMTP neslaganja između servera i klijenta ili kada server zahteva korišćenje SSL/TLS veze za SMTP bezbednu vezu.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Ova poruka se pojavljuje kada dođe do SMTP neslaganja između servera i klijenta ili kada server zahteva korišćenje STARTTLS veze za SMTP bezbednu vezu.
The connection is untrusted. Check the following. - Date and Time	Ova poruka se pojavljuje kada podešavanja datuma i vremena na skeneru nije tačno ili kada je sertifikat istekao.
The connection is untrusted. Check the following. - CA Certificate	Ova poruka se pojavljuje kada skener nema vrhovni sertifikat koji odgovara serveru ili CA Certificate nije uvezen.
The connection is not secured.	Ova poruka se pojavljuje kada je pribavljeni sertifikat oštećen.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Ova poruka se pojavljuje kada između servera i klijenta dođe do razlike u metodu provere identiteta. Server podržava SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Ova poruka se pojavljuje kada između servera i klijenta dođe do razlike u metodu provere identiteta. Server ne podržava SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	Ova poruka se pojavljuje kada navedena adresa e-pošte pošiljaoca nije tačna.

Poruke	Objašnjenje
Cannot access the product until processing is complete.	Ova poruka se pojavljuje kada je skener zauzet.

Povezane informacije

➡ “Provera veze sa serverom za poštu” na strani 44

Ažuriranje upravljačkog softvera

Ažuriranje upravljačkog softvera pomoću aplikacije Web Config

Ažuriranje upravljačkog softvera pomoću aplikacije Web Config. Uređaj mora biti povezan na internet.

1. Pristupite programu Web Config i odaberite **Basic Settings** > **Firmware Update**.
2. Kliknite na **Start**.

   Započinje potvrda upravljačkog softvera i prikazuju se informacije o njemu ukoliko postoji ažuriranje.
3. Kliknite na **Start**, a zatim sledite uputstva na ekranu.

Napomena:
Upravljački softver možete da ažurirate i pomoću Epson Device Admin. Možete vizuelno potvrditi informacije o upravljačkom softveru na listi uređaja. Ovo je korisno kada želite da ažurirate upravljački softver većeg broja uređaja. Više informacija potražite u priručniku ili na veb-sajtu Epson Device Admin.

Povezane informacije

➡ “Pristup programu Web Config” na strani 23
➡ “Epson Device Admin” na strani 55

Ažuriranje upravljačkog softvera pomoću aplikacije Epson Firmware Updater

Upravljački softver za uređaj možete preuzeti na računar s Epsonovog veb-sajta, a zatim povezati uređaj i računar pomoću USB kabla kako biste ažurirali upravljački softver. Ako ne možete da izvršite ažuriranje preko mreže, pokušajte to da uradite na sledeći način.

1. Pristupite Epsonovom veb-sajtu i preuzmite upravljački softver.
2. Računar na kom se nalazi preuzeti upravljački softver i uređaj povežite USB kablom.
3. Dvaput kliknite na preuzetu .exe datoteku.

   Epson Firmware Updater će se pokrenuti.
4. Pratite uputstva na ekranu.

Kopiranje podešavanja

Ukoliko izvezete stavke za podešavanja na Web Config, te stavke možete kopirati na druge skenere.

Izvoz podešavanja

Izvezite svako podešavanje za skener.

1. Pristupite programu Web Config i izaberite **Export and Import Setting Value** > **Export**.
2. Izaberite podešavanja koja želite da izvezete.

   Izaberite podešavanja koja želite da izvezete. Ako izaberete roditeljsku kategoriju, potkategorije će takođe biti izabrane. Ipak, potkategorije koje izazivaju greške dupliranjem unutar iste mreže (kao što su IP adrese i slično) ne mogu da budu izabrane.
3. Unesite lozinku kako biste šifrovali izvezenu datoteku.

   Potrebna vam je lozinka za uvoz datoteke. Ostavite ovo prazno ako ne želite da šifrujete datoteku.
4. Kliknite na **Export**.

> ***Važno:***
>
> *Ako želite da izvezete mrežna podešavanja skenera kao što su ime skenera i IP adresa, izaberite **Enable to select the individual settings of device** i izaberite još stavki. Koristite samo izabrane vrednosti za zamenski skener.*

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

Uvoz podešavanja

Uvezite izvezenu datoteku programa Web Config na skener.

> ***Važno:***
>
> *Kada uvozite vrednosti koje uključuju pojedinačne informacije kao što su ime skenera ili IP adresa, uverite se da ista IP adresa ne postoji na istoj mreži. Ako se IP adresa preklapa, skener ne odražava vrednost.*

1. Pristupite programu Web Config i izaberite **Export and Import Setting Value** > **Import**.
2. Izaberite izvezenu datoteku, a zatim unesite šifrovanu lozinku.
3. Kliknite na **Next**.
4. Izaberite podešavanja koja želite da uvezete, a zatim kliknite na **Next**.
5. Kliknite na **OK**.

Podešavanja će biti primenjena na skener.

Podešavanja u vezi s radom i upravljanjem

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

Otklanjanje problema

Saveti za otklanjanje problema

Više informacija možete pronaći u sledećem priručniku.

❏ Korisnički vodič

Sadrži uputstva za korišćenje skenera, održavanje i otklanjanje problema.

Provera evidencije za server i mrežni uređaj

U slučaju problema s povezivanjem na mrežu, možda ćete moći da utvrdite uzrok proverom evidencije za poštanski server, LDAP server itd, ili proverom statusa uz pomoć mrežne evidencije sistemske opreme i komandi, poput mrežnih skretnica.

Započinjanje mrežnih podešavanja

Vraćanje podešavanja mreže sa kontrolne table

Sve mrežne postavke možete da vratite na podrazumevane vrednosti.

1. Dodirnite **Podešavanja** na početnom ekranu.
2. Dodirnite **Administracija sistema** > **Vrati podrazumevana podešavanja** > **Mrežne postavke**.
3. Proverite poruku, a zatim dodirnite **Da**.
4. Kada se prikaže poruka o završetku, dodirnite **Zatvori**.

   Ako ne dodirnete **Zatvori**, ekran se automatski zatvara posle određenog vremena.

Provera komunikacije između uređaja i računara

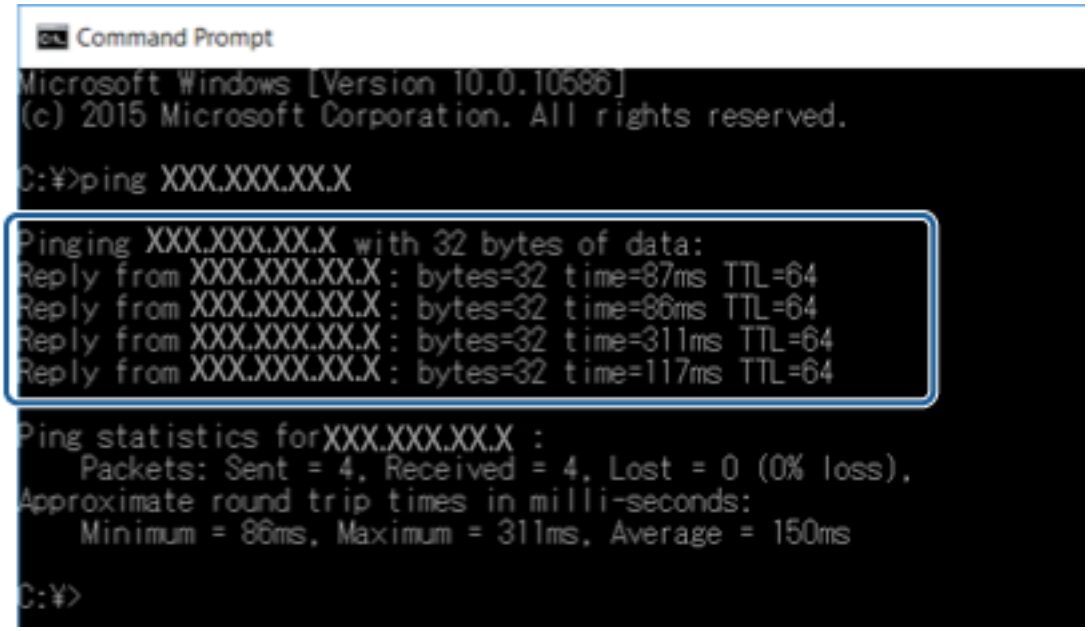
Provera priključka uz pomoć Ping komande — Windows

Možete koristiti Ping komandu da biste se uverili da li je računar priključen na skener. Sledite navedene korake da biste proverili priključak pomoću Ping komande.

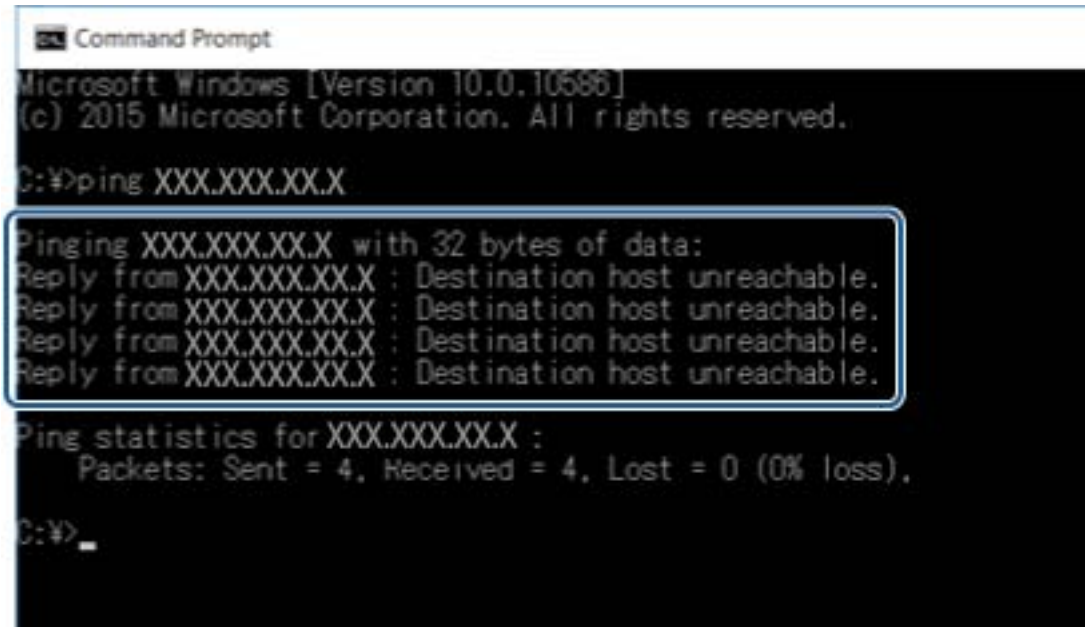
1. Proverite IP adresu skenera zbog priključka koji hoćete da proverite.

   Možete proveriti uz pomoć Epson Scan 2.

2. Prikažite ekran računara sa odzivnikom.
   - ❏ Windows 10
     Desni klik na dugme Start i držite ga, a zatim izaberite **Odzivnik**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Prikažite ekran aplikacije, a zatim izaberite **Odzivnik**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 ili ranije verzije
     Kliknite na dugme Start, izaberite **Svi programi** ili **Programi** > **Dodaci** > **Odzivnik**.
3. Unesite „ping xxx.xxx.xxx.xxx”, a zatim pritisnite taster Enter.
   Unesite IP adresu skenera za xxx.xxx.xxx.xxx.
4. Proverite status komunikacije.
   Ako postoji komunikacija između skenera i računara, prikazuje se sledeća poruka.



Ako ne postoji komunikacija između skenera i računara, prikazuje se sledeća poruka.



Provera veze pomoću komande za pingovanje — Mac OS

Možete koristiti Ping komandu da biste se uverili da li je računar priključen na skener. Sledite navedene korake da biste proverili priključak pomoću Ping komande.

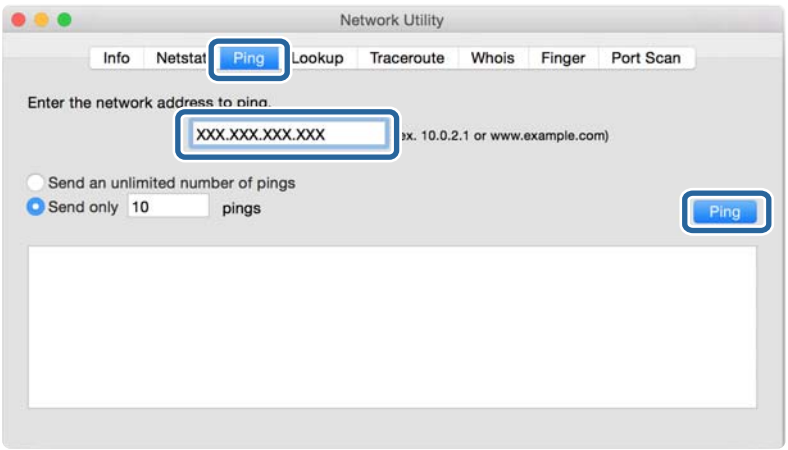
1. Proverite IP adresu skenera zbog priključka koji hoćete da proverite.

   Možete proveriti uz pomoć Epson Scan 2.

2. Pokrenite Network Utility.

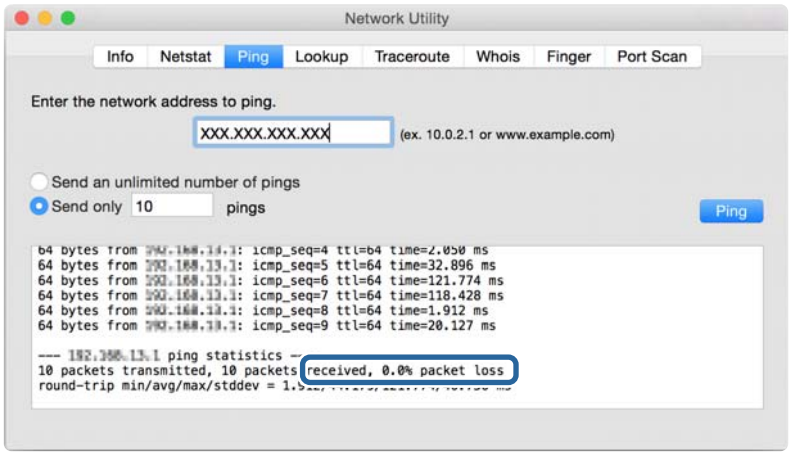
   Unesite „Network Utility“ u polje **Spotlight**.

3. Kliknite na karticu **Ping**, unesite IP adresu koju ste proverili u koraku 1 a zatim kliknite na **Ping**.

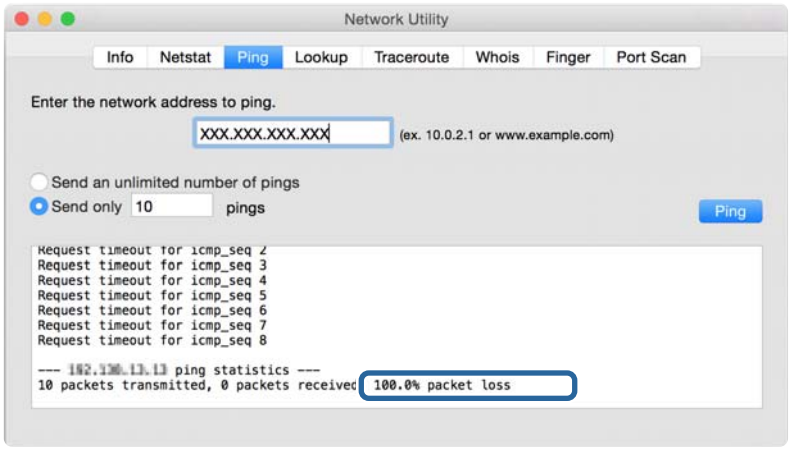


4. Proverite status komunikacije.

   Ako postoji komunikacija između skenera i računara, prikazuje se sledeća poruka.



   Ako ne postoji komunikacija između skenera i računara, prikazuje se sledeća poruka.



Problemi pri korišćenju mrežnih programa

Pristup programu Web Config nije moguć

Da li je uneta tačna IP adresa skenera?

Konfigurišite IP adresu koristeći Epson Device Admin ili EpsonNet Config.

Da li vaš pregledač podržava grupna šifrovanja za Encryption Strength za SSL/TLS?

Grupna šifrovanja za Encryption Strength za SSL/TLS su sledeća. Programu Web Config se može pristupiti samo u pregledaču koji podržava sledeća grupna šifrovanja. Proverite koje vrste šifrovanja vaš pregledač podržava.

❏ 80bitno: AES256/AES128/3DES

❏ 112bitno: AES256/AES128/3DES

❏ 128bitno: AES256/AES128

❏ 192bitno: AES256

❏ 256bitno AES256

Poruka „Isteklo“ se pojavljuje prilikom pokretanja programa Web Config preko SSL protokola (https).

Ako je sertifikat istekao, pribavite novi. Ako se poruka pojavi pre datuma isteka sertifikata, proverite da li je na skeneru podešen tačan datum.

Poruka „Naziv bezbednosnog sertifikata se ne podudara sa…“ se pojavljuje prilikom pokretanja programa Web Config preko SSL protokola (https).

IP adresa skenera koja je uneta u polje **Common Name** za kreiranje nezavisnog sertifikata ili CSR-a se ne podudara sa adresom unetom u pregledač. Ponovo pribavite i uvezite sertifikat ili promenite ime skenera.

Skeneru se pristupa preko ovlašćenog servera.

Ako za skener koristite ovlašćeni server, potrebno je da konfigurišete podešavanja ovlašćenog servera za skener.

❏ Windows:

Izaberite **Kontrolna tabla** > **Mreža i Internet** > **Internet opcije** > **Veze** > **Postavke LAN-a** > **Proksi server**, a zatim podesite proksi server tako da se ne koristi za lokalne adrese.

❏ Mac OS:

Izaberite **Željene postavke sistema** > **Mreža** > **Napredne postavke** > **Proksi serveri**, a zatim upišite lokalnu adresu u polje **Zaobiđi proksi postavke za ove matične računare i domene**.

Primer:

192.168.1.*: Lokalna mreža 192.168.1.XXX, maska podmreže 255.255.255.0

192.168.*.*: Lokalna mreža 192.168.XXX.XXX, maska podmreže 255.255.0.0

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

➡ “Dodeljivanje IP adrese” na strani 15

➡ “Dodeljivanje IP adrese pomoću EpsonNet Config” na strani 56

Naziv modela i/ili IP adresa se ne prikazuju u programu EpsonNet Config

Da li ste izabrali opciju Blokiraj, Otkaži, ili Isključi se kada se pojavio prozor Windows bezbednosti ili prozor zaštitnog zida?

Ako izaberete **Blokiraj**, **Otkaži** ili **Isključi se** , IP adresa i naziv modela se neće prikazivati u programu EpsonNet Config ili EpsonNet Setup.

Da biste to ispravili, registrujte EpsonNet Config kao izuzetak u Windows zaštitnom zidu i u komercijalnom programu za zaštitu. Ako koristite neki antivirus ili program za zaštitu, zatvorite ga i pokušajte da pokrenete EpsonNet Config.

Da li je podešeno premalo vremena za istek greške u komunikaciji?

Pokrenite program EpsonNet Config i izaberite **Tools** > **Options** > **Timeout**, a zatim povećajte vreme u opciji **Communication Error**. Imajte u vidu da takvo podešavanje može usporiti rad programa EpsonNet Config.

Povezane informacije

➡ “Pokretanje programa EpsonNet Config — Windows” na strani 56
➡ “Pokretanje programa EpsonNet Config — Mac OS” na strani 56

Dodatak

Predstavljanje mrežnog softvera

U tekstu koji sledi opisan je softver za konfigurisanje uređaja i upravljanje njima.

Epson Device Admin

Epson Device Admin je aplikacija koja vam omogućava da instalirate uređaje na mreži a zatim ih konfigurišete i upravljate njima. Možete da dobijete detaljne informacije o uređajima, poput statusa i stanja potrošnog materijala, da šaljete obaveštenja o upozorenjima i pravite izveštaje o korišćenju uređaja. Možete da napravite i predložak koji sadrži stavke za podešavanja i primenite ih na druge uređaje kao deljene postavke. Epson Device Admin možete da preuzmete na veb-lokaciji za podršku kompanije Epson. Više informacija potražite u propratnoj dokumentaciji ili pomoći aplikacije Epson Device Admin.

Pokretanje Epson Device Admin (samo Windows)

Odaberite **Svi programi** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Napomena:
Ako se pojavi upozorenje zaštitnog zida, omogućite pristup programu Epson Device Admin.

EpsonNet Config

Program EpsonNet Config omogućava administratoru da konfiguriše mrežne postavke skenera, na primer da dodeli IP adresu i da promeni režim povezivanja. Funkcija grupnog podešavanja je podržana u operativnom sistemu Windows. Više informacija potražite u propratnoj dokumentaciji ili pomoći aplikacije EpsonNet Config.

Pokretanje programa EpsonNet Config — Windows

Odaberite **Svi programi** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Napomena:
Ako se pojavi upozorenje zaštitnog zida, omogućite pristup programu EpsonNet Config.

Pokretanje programa EpsonNet Config — Mac OS

Izaberite **Kreni** > **Aplikacije** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager je program koji služi za kreiranje paketa za jednostavno podešavanje skenera, u koje spadaju instaliranje upravljačkog programa za skener, instaliranje programa Document Capture Pro. Ovaj program omogućava administratoru da kreira jedinstvene pakete programa i da ih distribuira različitim grupama.

Više informacija potražite na regionalnoj veb lokaciji kompanije Epson.

Dodeljivanje IP adrese pomoću EpsonNet Config

Možete dodeliti IP adresu skeneru pomoću EpsonNet Config. EpsonNet Config vam omogućava da dodelite IP adresu skeneru kom ona nije dodeljena nakon povezivanja pomoću Ethernet kabla.

Dodeljivanje IP adresa pomoću grupnih podešavanja

Pravljenje datoteke za grupna podešavanja

Koristeći MAC adresu i naziv modela kao ključeve, možete da napravite novu SYLK datoteku kako biste podesili IP adresu.

1. Otvorite aplikaciju za rad s tabelama (poput programa Microsoft Excel) ili uređivač teksta.

2. U prvi red unesite „Info_MACAddress“, „Info_ModelName“, i „TCPIP_IPAddress“ kao nazive stavki podešavanja.

   Unesite stavke podešavanja za sledeće tekstualne nizove. Kod razlikovanja velikih i malih slova i znakova od dva bajta/jednog bajta, ako je samo jedan znak drugačiji, stavka neće biti prepoznata.

   Naziv stavke podešavanja unesite onako kako je opisano ispod; u protivnom, EpsonNet Config neće moći da prepozna stavke podešavanja.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Unesite MAC adresu, naziv modela i IP adresu za svaki mrežni interfejs.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

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

4. Unesite naziv datoteke i sačuvajte je kao SYLK datoteku (*.slk).

Vršenje grupnih podešavanja pomoću datoteke za konfiguraciju

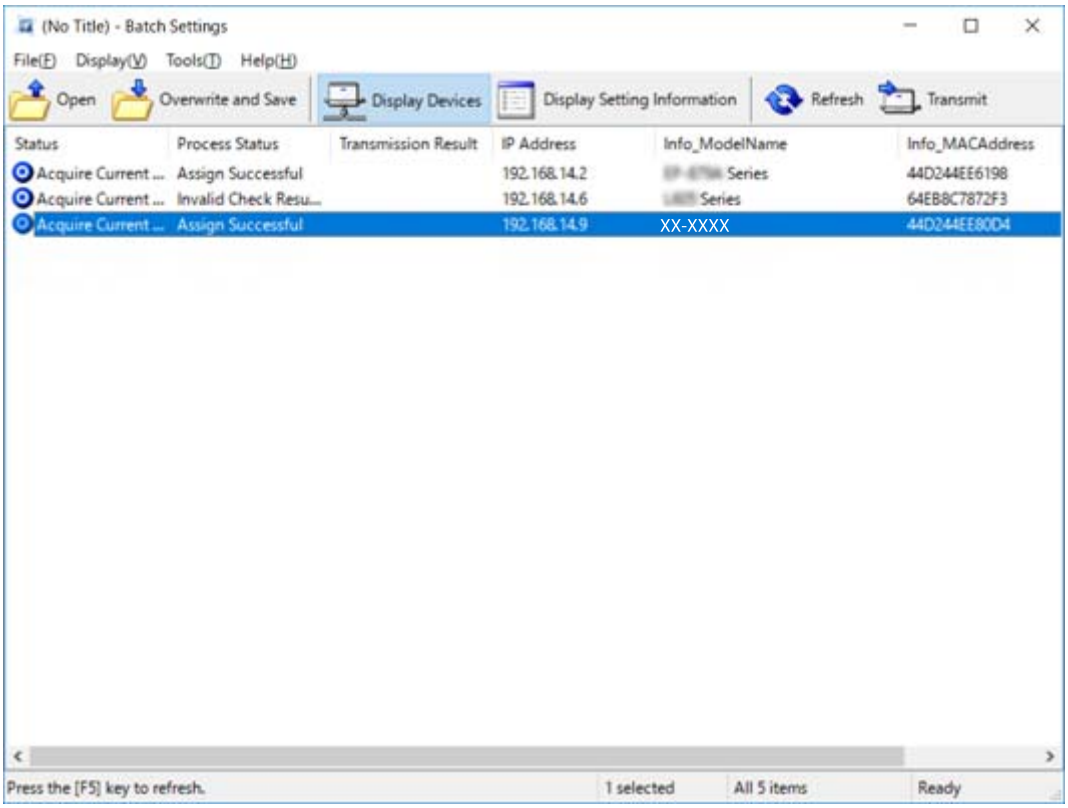
Dodelite IP adrese u datoteci za konfiguraciju (SYLK datoteci) u isto vreme. Treba da napravite datoteku za konfiguraciju pre dodeljivanja adresa.

1. Priključite sve uređaje na mrežu pomoću Ethernet kablova.
2. Uključite skener.
3. Pokrenite EpsonNet Config.

   Biće prikazan spisak skenera na mreži. Moguće je da će biti potrebno malo vremena da se pojave svi skeneri.
4. Kliknite na **Tools** > **Batch Settings**.
5. Kliknite na **Open**.
6. Na ekranu za odabir datoteke odaberite SYLK datoteku (*.slk) u kojoj se nalaze podešavanja, a zatim kliknite na **Open**.

7. Odaberite uređaje za koje želite da izvršite grupna podešavanja s kolonom **Status** postavljenom na **Unassigned** i sa **Process Status** postavljenim na **Assign Successful**.

   Prilikom vršenja višestrukog odabira, pritisnite taster Ctrl ili Shift i kliknite ili prevucite mišem.



8. Kliknite na **Transmit**.

9. Kada se prikaže ekran za unos lozinke, unesite lozinku, a zatim kliknite na **OK**.

   Pošaljite podešavanja.

   Napomena:
   Informacije se šalju na mrežni interfejs dok se traka napredovanja ne popuni. Nemojte iskljućivati uređaj ili bežični adapter i nemojte slati nikakve podatke uređaju.

10. Na ekranu **Transmitting Settings** kliknite na **OK**.

11. Proverite status uređaja koji ste podesili.

    Za uređaje na kojima bude prikazano  ili  , proverite sadržaj datoteke za podešavanja ili da li je ponovno pokretanje uređaja proteklo u redu.

Ikona	Status	Process Status	Objašnjenje
	Setup Complete	Setup Successful	Podešavanje završeno bez problema.
	Setup Complete	Rebooting	Kada informacije budu poslane, svaki uređaj treba ponovo pokrenuti kako bi podešavanja bila omogućena. Provera se vrši da bi se utvrdilo da li se nakon ponovnog pokretanja na uređaj može priključiti ili ne.
	Setup Complete	Reboot Failed	Nakon prenošenja podataka uređaj ne može biti potvrđen. Proverite da li je uređaj uključen i da li je ponovno pokretanje proteklo u redu.
	Setup Complete	Searching	Traženje uređaja navedenog u datoteci s podešavanjima.*
	Setup Complete	Search Failed	Uređaji koji su već podešeni ne mogu biti provereni. Proverite da li je uređaj uključen ili da li je ponovno pokretanje proteklo u redu.*

    * Samo kad su informacije o podešavanjima prikazane.

Povezane informacije

➡ "Pokretanje programa EpsonNet Config — Windows" na strani 56
➡ "Pokretanje programa EpsonNet Config — Mac OS" na strani 56

Dodeljivanje IP adrese svakom uređaju

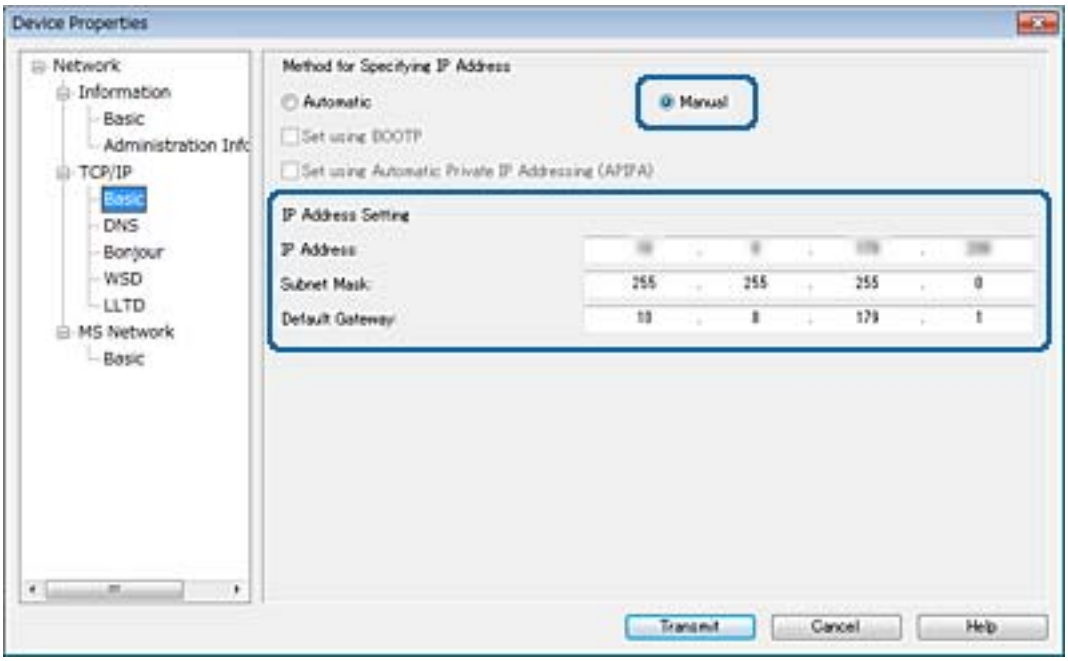
Dodelite IP adresu skeneru koristeći EpsonNet Config.

1. Uključite skener.
2. Povežite skener na mrežu pomoću Ethernet kabla.
3. Pokrenite EpsonNet Config.

   Biće prikazan spisak skenera na mreži. Moguće je da će biti potrebno malo vremena da se pojave svi skeneri.
4. Dvaput kliknite na skener kom želite da dodelite IP adresu.

   Napomena:
   Ako ste povezali više skenera istog modela, željeni skener možete identifikovati korišćenjem MAC adrese.
5. Izaberite **Network** > **TCP/IP** > **Basic**.

6. Unesite adrese za **IP Address**, **Subnet Mask**, i **Default Gateway**.



Napomena:
Unesite statičku adresu kad priključite skener na bezbednu mrežu.

7. Kliknite na **Transmit**.

   Prikazuje se ekran za potvrdu prenosa informacija.

8. Kliknite na **OK**.

   Prikazaće se ekran za završetak prenosa.

   Napomena:
   Informacije se prenose na uređaj, a zatim se prikazuje poruka „Konfiguracija uspešno završena“. Nemojte isključivati uređaj i nemojte slati nikakve podatke usluzi.

9. Kliknite na **OK**.

Povezane informacije

➡ “Pokretanje programa EpsonNet Config — Windows” na strani 56
➡ “Pokretanje programa EpsonNet Config — Mac OS” na strani 56

Korišćenje ulaza za skener

Skener koristi sledeći ulaz. Administrator treba po potrebi da dozvoli mreži da omogući ove ulaze.

Dodatak

Pošiljalac (klijent)	Upotreba	Odredište (server)	Protokol	Broj ulaza
Skener	Slanje e-poštom (obaveštenja putem e-pošte)	SMTP server	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	Povezivanje na POP pre povezivanja na SMTP (obaveštenja putem e-pošte)	POP server	POP3 (TCP)	110
	Kontrolni WSD	Računar klijent	WSD (TCP)	5357
	Pretraživanje računara prilikom skeniranja s uređaja pomoću aplikacije Document Capture Pro	Računar klijent	Otkrivanje na mreži za skeniranje s uređaja	2968
	Prikupljanje informacija o zadatku prilikom skeniranja s uređaja pomoću aplikacije Document Capture Pro	Računar klijent	Skeniranje s uređaja na mreži	2968
Računar klijent	Otkrijte skener pomoću aplikacije kao što je EpsonNet Config i upravljački program skenera.	Skener	ENPC (UDP)	3289
	Prikupite i podesite MIB informacije pomoću aplikacije kao što je EpsonNet Config i upravljački program skenera.	Skener	SNMP (UDP)	161
	Traženje WSD skenera	Skener	Otkrivanje veb-servisa (UDP)	3702
	Prosleđivanje skeniranih podataka iz aplikacije Document Capture Pro	Skener	Skeniranje mreže (TCP)	1865

Napredne bezbednosne postavke za Enterprise

U ovom poglavlju opisane su napredne bezbednosne funkcije.

Bezbednosna podešavanja i sprečavanje opasnosti

Kada je uređaj priključen na mrežu, možete mu pristupiti s udaljene lokacije. Pored toga, mnogi ljudi mogu da dele taj uređaj, što pomaže da se unapredi efikasnost i udobnost rada. Međutim, rizici kao što su nezakoniti pristup, nezakonita upotreba i neovlašćeno menjanje podataka se povećavaju. Ako koristite uređaj u okruženju u kom imate pristup internetu, rizici su još veći.

Kako bi ovaj rizik bio izbegnut, kod Epson uređaja se primenjuju razne bezbednosne tehnologije.

Podesite uređaj prema potrebi, u zavisnosti od uslova okruženja koji su uspostavljeni pomoću informacija o klijentovom okruženju.

Naziv	Vrsta funkcije	Šta treba podesiti	Šta treba sprečiti
SSL/TLS komunikacija	Komunikaciona putanja računara i uređaja je šifrovana pomoću SSL/TLS protokola. Sadržaj komunikacije je zaštićen preko pregledača.	Podesite CA sertifikat uređaja za server koji ima potpisan CA (Sertifikaciono telo, eng. Certificate Authority) sertifikat.	Sprečite curenje podataka o podešavanjima i sadržaju podataka koji se šalju skeneru na štampanje s računara. Pristup Epsonovom serveru na internetu sa uređaja može biti zaštićen i ažuriranjem upravljačkog softvera itd.
IPsec/IP filtriranje	Možete podesiti da dozvolite odvajanje ili odsecanje podataka koji dolaze od određenog klijenta ili su određenog tipa. Pošto IPsec štiti podatke po jedinici IP paketa (šifrovanje i provera identiteta), možete bezbedno prenositi neobezbeđeni protokol za skeniranje.	Napravite osnovne smernice i individualne smernice da biste podesili klijenta ili vrstu podataka koji mogu da pristupe uređaju.	Zaštitite uređaj od neovlašćenog pristupa, kao i od neovlašćenog menjanja i presretanja podataka koji se šalju uređaju.
SNMPv3	Dodate su funkcije kao što su nadgledanje uređaja priključenih na mrežu, integritet podataka koji se šalju SNMP protokolu za kontrolu, šifrovanje, proveru identiteta korisnika itd.	Omogućite SNMPv3, a zatim podesite način provere identiteta i šifrovanja.	Obezbedite promene podešavanja putem mreže, kao i poverljivost u nadgledanju stanja.
IEEE802.1X	Povezivanje je dozvoljeno samo korisniku čiji je identitet proveren za korišćenje Ethernet mreže. Uređaj može da koristi samo onaj korisnik kome je to dozvoljeno.	Podešavanje provere identiteta za RADIUS server (server za proveru identiteta).	Zaštitite uređaj od neovlašćenog pristupa i korišćenja.

Napredne bezbednosne postavke za Enterprise

Naziv	Vrsta funkcije	Šta treba podesiti	Šta treba sprečiti
Očitavanje ID kartice	Uređaj možete koristiti tako što ćete držati ID karticu iznad identifikovanog priključenog uređaja. Možete ograničiti dobijanje evidencije za svakog korisnika i uređaj, kao i ograničiti dostupnost uređaja i funkcija na njima za svakog korisnika ili grupu.	Priključite uređaj za proveru identiteta na uređaj, a zatim podesite informacije o korisniku u sistemu za proveru identiteta.	Sprečite neovlašćenu upotrebu uređaja i prevare.

Povezane informacije

➡ "SSL/TLS komunikacija sa skenerom" na strani 63

➡ "Šifrovana komunikacija pomoću IPsec/IP filtriranja" na strani 71

➡ "Upotreba SNMPv3 protokola" na strani 82

➡ "Povezivanje skenera na IEEE802.1X mrežu" na strani 84

Podešavanje bezbednosne funkcije

Prilikom podešavanja IPsec/IP filtriranja ili funkcije IEEE802.1X, preporučuje se da pristupite alatki Web Config koristeći SSL/TLS za prenos informacija kako biste smanjili bezbednosne rizike kao što su neovlašćeno menjanje ili presretanje.

SSL/TLS komunikacija sa skenerom

Kada je sertifikat servera za skener podešen pomoću protokola SSL/TLS (Sloj sigurnih utičnica/Bezbednost transportnog sloja), možete šifrovati komunikacionu putanju između računara. Ovo uradite ako želite da sprečite neovlašćeni pristup i pristup na daljinu.

O digitalnim sertifikatima

❏ Sertifikat koji je odobrilo neko sertifikaciono telo (CA)

Sertifikat koji potpisuje neko sertifikaciono telo (CA) pribavlja se od datog sertifikacionog tela. Komunikaciju možete da zaštitite korišćenjem CA sertifikata. CA sertifikat možete da koristite za svaku bezbednosnu funkciju.

❏ CA sertifikat

CA sertifikat označava da je treća strana potvrdila identitet servera. On predstavlja ključnu komponentu zaštite koja garantuje bezbednost na internetu. Potrebno je da pribavite CA sertifikat za proveru identiteta servera od sertifikacionog tela koje ih izdaje.

❏ Nezavisni sertifikat

Nezavisni sertifikat je sertifikat koji skener sam izdaje i potpisuje. Taj sertifikat nije pouzdan i ne može da spreči prevare. Ako koristite taj sertifikat kao SSL/TLS sertifikat, u pregledaču će se možda pojaviti bezbednosno upozorenje. Taj sertifikat možete da koristite samo za SSL/TLS komunikaciju.

Povezane informacije

➡ “Pribavljanje i uvoz CA sertifikata” na strani 64
➡ “Brisanje CA sertifikata” na strani 67
➡ “Ažuriranje nezavisnog sertifikata” na strani 68

Pribavljanje i uvoz CA sertifikata

Pribavljanje CA sertifikata

Da biste pribavili CA sertifikat, kreirajte CSR (zahtev za potpisivanje sertifikata) i pošaljite ga sertifikacionom telu. CSR možete da kreirate uz pomoć programa Web Config i računara.

Pratite uputstva za kreiranje CSR-a i pribavite CA sertifikat koristeći Web Config. Prilikom kreiranja CSR-a uz pomoć programa Web Config, sertifikat je u formatu PEM/DER.

1. Pristupite programu Web Config i izaberite **Network Security Settings**. Zatim izaberite **SSL/TLS** > **Certificate** ili **IPsec/IP Filtering** > **Client Certificate** ili **IEEE802.1X** > **Client Certificate**.

2. Kliknite na **Generate** kod **CSR**.

   Otvoriće se stranica za kreiranje CSR-a.

3. Izaberite jednu vrednost za svaku stavku.

   Napomena:
   Dostupna dužina šifre i skraćenice se mogu razlikovati u zavisnosti od sertifikacionog tela. Poštujte pravila datog sertifikacionog tela prilikom kreiranja zahteva.

4. Kliknite na **OK**.

   Prikazaće se poruka sa obaveštenjem o završetku.

5. Izaberite **Network Security Settings**. Zatim izaberite **SSL/TLS** > **Certificate**, ili **IPsec/IP Filtering** > **Client Certificate** ili **IEEE802.1X** > **Client Certificate**.

6. CSR preuzmite na računar tako što ćete kliknuti na jedno od dugmadi za preuzimanje koju sadrži **CSR**, u formatu koji zahteva dato sertifikaciono telo.

   > ***Važno:***
   > *Nemojte ponovo da generišete CSR. Ako to uradite, možda nećete moći da uvezete izdati CA-signed Certificate.*

7. Pošaljite CSR sertifikacionom telu i dobavite CA-signed Certificate.

   Poštujte pravila datog sertifikacionog tela koja se odnose na način slanja i formular.

8. Sačuvajte izdati CA-signed Certificate na računaru koji je povezan sa skenerom.

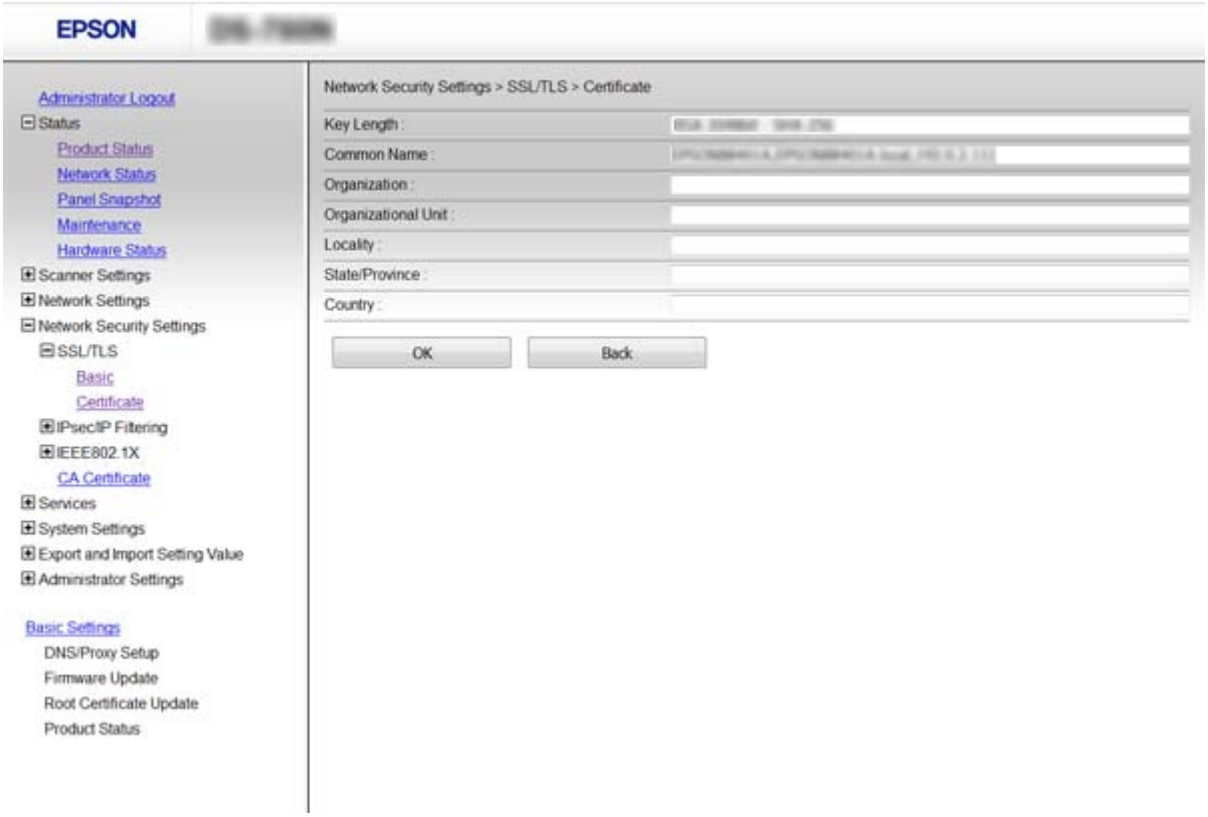
   Postupak dobijanja CA-signed Certificate se smatra gotovim kada sertifikat snimite na odredišnu lokaciju.

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

➡ “CSR — stavke podešavanja” na strani 65
➡ “Uvoz CA sertifikata” na strani 66

CSR — stavke podešavanja



Stavke	Podešavanja i objašnjenje
Key Length	Izaberite dužinu šifre za CSR.
Common Name	Možete uneti između 1 i 128 znakova. Ako se radi o IP adresi, potrebno je da bude statička. Primer: URL adresa za pristup programu Web Config: https://10.152.12.225 Opšte ime: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Možete da unesete između 0 i 64 znaka u formatu ASCII (0x20–0x7E). Pojedinačna imena možete da razdvojite zapetama.
Country	Unesite dvocifrenu šifru zemlje u skladu sa standardom ISO-3166.

Povezane informacije

➡ “Pribavljanje CA sertifikata” na strani 64

Uvoz CA sertifikata

Važno:

❏ *Proverite da li su na skeneru podešeni tačno vreme i datum.*

❏ *Ako ste sertifikat dobili na osnovu CSR formulara iz programa Web Config, sertifikat možete da uvezete jednom.*

1. Pristupite programu Web Config i izaberite **Network Security Settings**. Zatim izaberite **SSL/TLS** > **Certificate**, ili **IPsec/IP Filtering** > **Client Certificate** ili **IEEE802.1X** > **Client Certificate**.

2. Kliknite na **Import**.

   Otvoriće se stranica za uvoz sertifikata.

3. Izaberite jednu vrednost za svaku stavku.

   Postavke mogu da se razlikuju u zavisnosti od toga gde kreirate CSR i od formata datoteke sertifikata. Unesite vrednosti u obavezna polja u skladu sa sledećim stavkama.

   ❏ Sertifikat u formatu PEM/DER dobijen iz programa Web Config

   ❏ **Private Key**: Nemojte konfigurisati ovu stavku jer skener sadrži privatni ključ.

   ❏ **Password**: Nemojte je konfigurisati.

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

   ❏ Sertifikat u formatu PEM/DER dobijen sa računara

   ❏ **Private Key**: Podesite ovu stavku.

   ❏ **Password**: Nemojte je konfigurisati.

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

   ❏ Sertifikat u formatu PKCS#12 dobijen sa računara

   ❏ **Private Key**: Nemojte je konfigurisati.

   ❏ **Password**: Opcionalno

   ❏ **CA Certificate 1**/**CA Certificate 2**: Nemojte je konfigurisati.

4. Kliknite na **OK**.

   Prikazaće se poruka sa obaveštenjem o završetku.

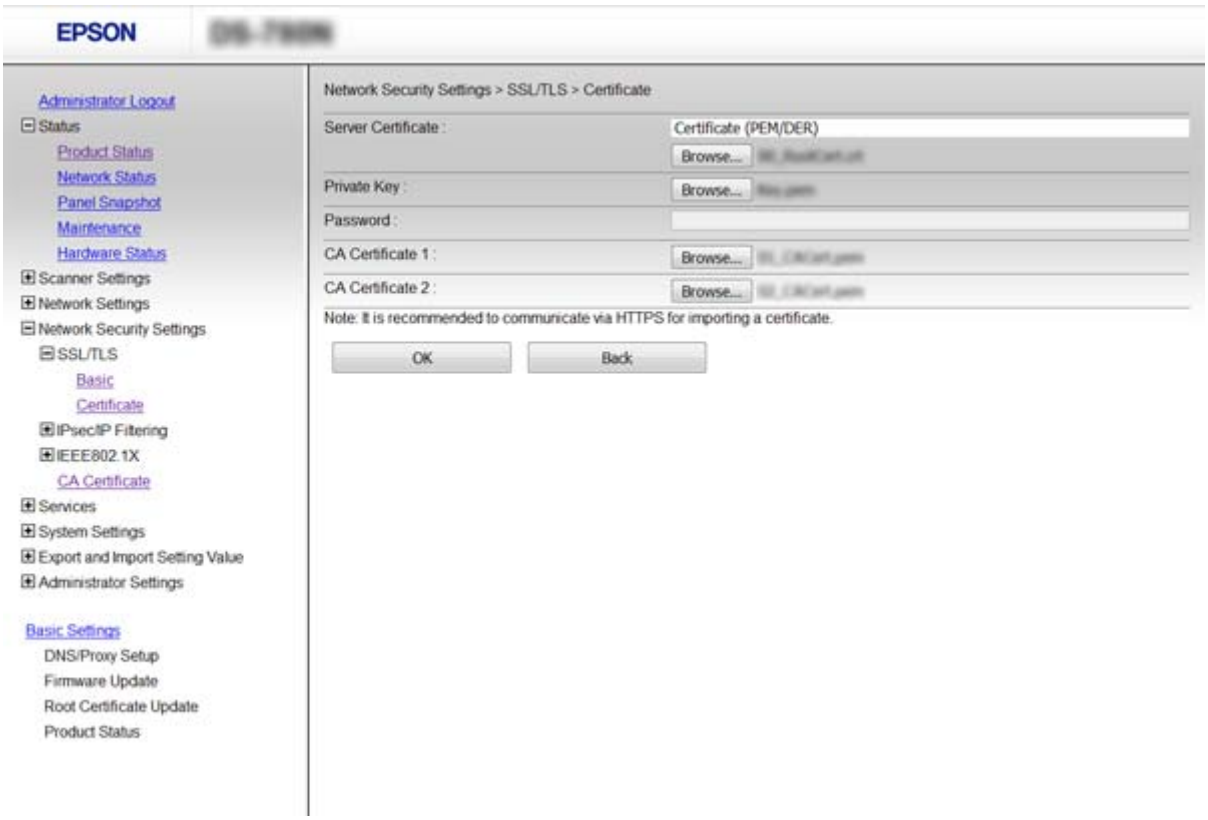
Napomena:
Kliknite na ***Confirm*** *da biste proverili informacije u sertifikatu.*

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

➡ “Uvoz CA sertifikata – stavke podešavanja” na strani 67

Uvoz CA sertifikata – stavke podešavanja



Stavke	Postavke i objašnjenja
Server Certificate ili Client Certificate	Izaberite format sertifikata.
Private Key	Ako ste sertifikat dobili u formatu PEM/DER koristeći CSR kreiran na računaru, navedite datoteku sa privatnim ključem koja odgovara sertifikatu.
Password	Unesite lozinku kako biste šifrovali privatni ključ.
CA Certificate 1	Ako je format sertifikata **Certificate (PEM/DER)**, uvezite sertifikat od sertifikacionog tela koje je izdalo sertifikat za server. Ako je potrebno, navedite datoteku.
CA Certificate 2	Ako je format sertifikata **Certificate (PEM/DER)**, uvezite sertifikat od sertifikacionog tela koje je izdalo **CA Certificate 1**. Ako je potrebno, navedite datoteku.

Povezane informacije

➡ “Uvoz CA sertifikata” na strani 66

Brisanje CA sertifikata

Možete da izbrišete uvezeni sertifikat kada istekne ili kada više ne postoji potreba za šifrovanjem veze.

> ***Važno:***
> *Ako ste sertifikat dobili na osnovu CSR formulara iz programa Web Config, ne možete ponovo da uvezete izbrisani sertifikat. U tom slučaju, kreirajte CSR i ponovo pribavite sertifikat.*

1. Pristupite programu Web Config, a zatim izaberite **Network Security Settings**. Zatim izaberite **SSL/TLS** > **Certificate** ili **IPsec/IP Filtering** > **Client Certificate** ili **IEEE802.1X** > **Client Certificate**.
2. Kliknite na **Delete**.
3. Potvrdite da želite da izbrišete sertifikat u prikazanoj poruci.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Ažuriranje nezavisnog sertifikata

Ako skener podržava funkciju HTTPS servera, možete da ažurirate nezavisni sertifikat. Prilikom otvaranja programa Web Config uz pomoć nezavisnog sertifikata pojavljuje se poruka sa upozorenjem.

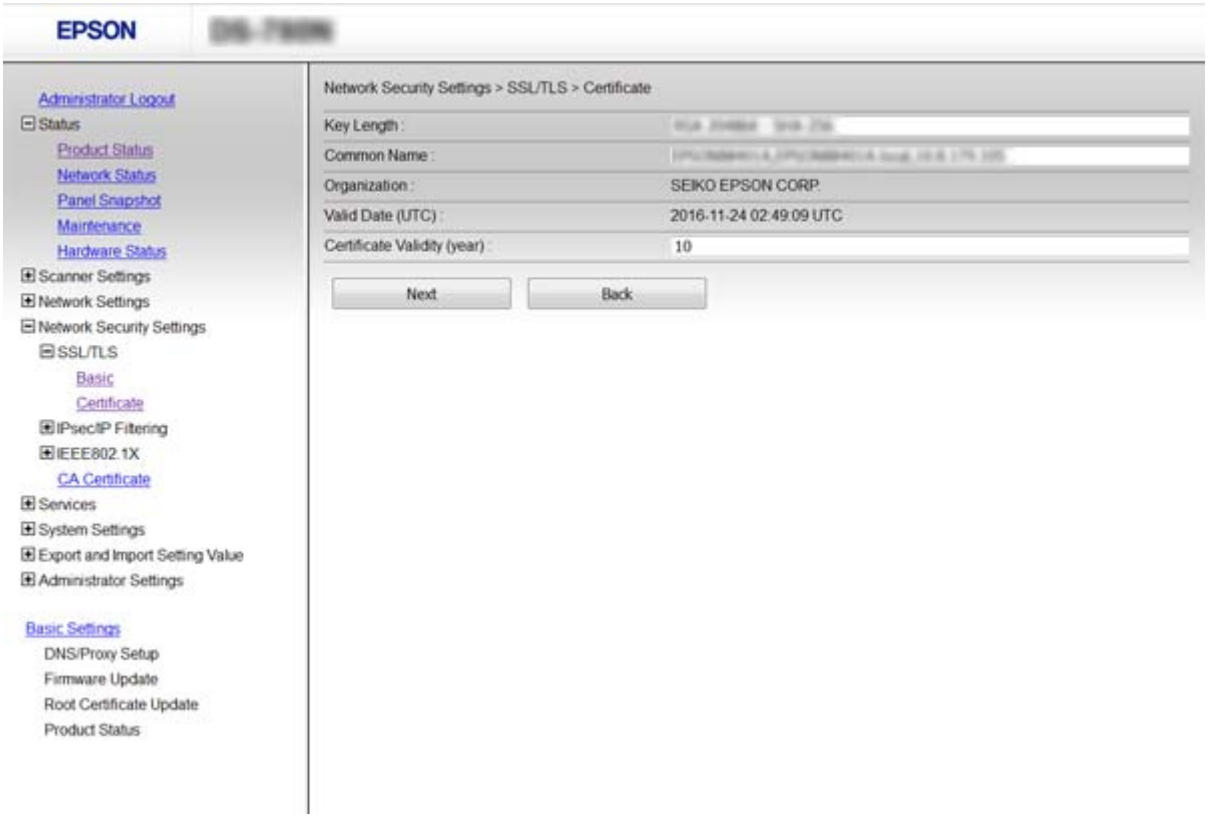
Nezavisni sertifikat koristite privremeno dok ne dobijete i uvezete CA sertifikat.

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Kliknite na **Update**.
3. Unesite **Common Name**.

   Unesite IP adresu ili neki identifikator poput FQDN naziva skenera. Možete uneti između 1 i 128 znakova.

   Napomena:
   Pojedinačna imena (CN) možete da razdvojite zapetama.

4. Navedite rok važenja sertifikata.



5. Kliknite na **Next**.

   Prikazaće se poruka sa potvrdom.

6. Kliknite na **OK**.

   Skener će biti ažuriran.

Napomena:
*Kliknite na **Confirm** da biste proverili informacije u sertifikatu.*

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Konfigurisanje CA Certificate

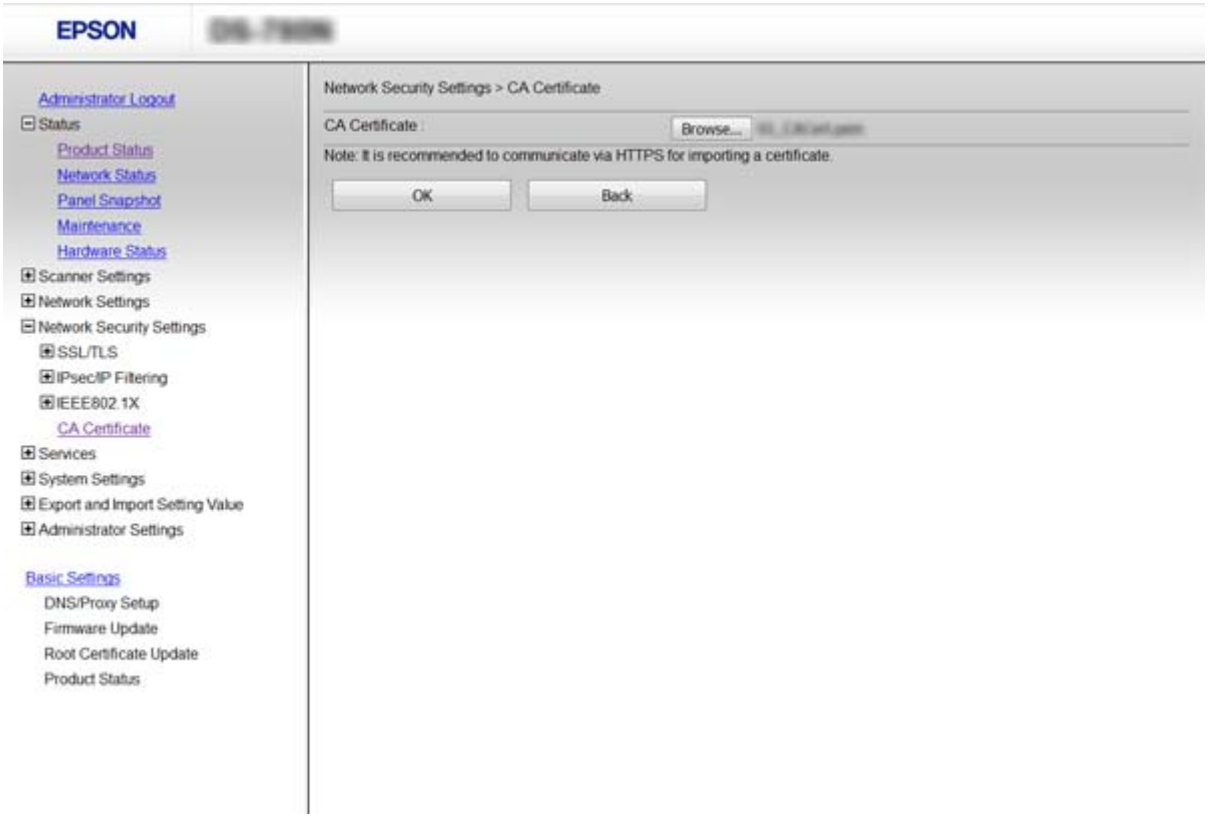
Možete da uvezete, prikažete i izbrišete CA Certificate.

Uvoz CA Certificate

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **CA Certificate**.

2. Kliknite na **Import**.

3. Navedite CA Certificate koji želite da uvezete.



4. Kliknite na **OK**.

Kada se uvoz završi, bićete vraćeni na ekran **CA Certificate** i uvezeni CA Certificate će se prikazati.

Povezane informacije

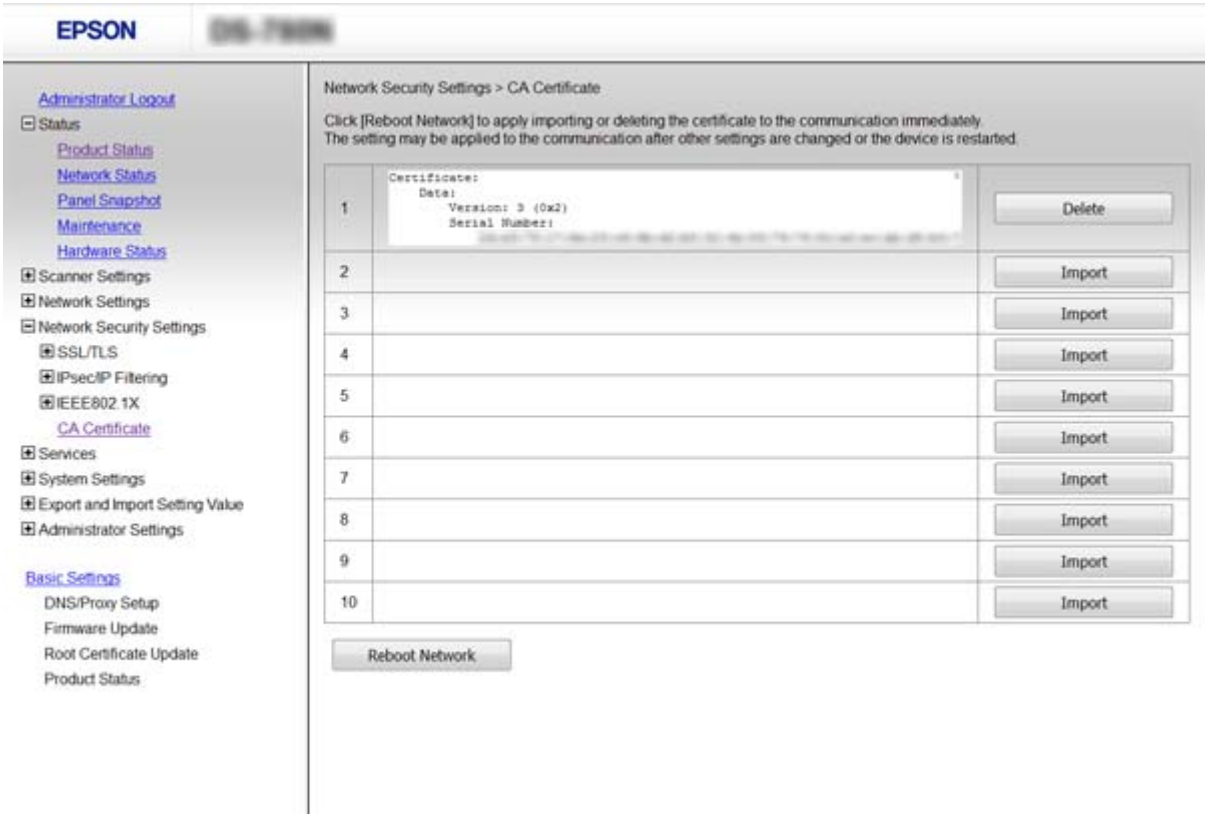
➡ "Pristup programu Web Config" na strani 23

Brisanje CA Certificate

Možete da izbrišete uvezeni CA Certificate.

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **CA Certificate**.

2. Kliknite na **Delete** pored CA Certificate koji želite da izbrišete.



3. Potvrdite da želite da izbrišete sertifikat u prikazanoj poruci.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Šifrovana komunikacija pomoću IPsec/IP filtriranja

O aplikaciji IPsec/IP Filtering

Ako skener podržava IPsec/IP filtriranje, možete da konfigurišete saobraćaj na osnovu IP adrese, servisa i porta. Kombinovanjem filtera, možete da konfigurišete skener tako da prihvata ili blokira određene klijente i određene podatke. Uz to, možete da povećate bezbednost tako što ćete koristiti IPsec.

Da bi filtriranje saobraćaja bilo aktivno, konfigurišite podrazumevanu smernicu. Podrazumevane smernice važe za sve korisnike i grupe koje se povezuju sa skenerom. Ako želite da preciznije kontrolišete korisnike i grupe korisnika, konfigurišite smernice za grupe. Smernice za grupu su jedno ili više pravila koja se primenjuju na korisnika ili grupu korisnika. Skener kontroliše IP pakete koji odgovaraju konfigurisanim smernicama. Proverava se identitet IP paketa u odnosu na smernice za grupu redosledom od 1 do 10, a zatim u odnosu na podrazumevanu smernicu.

Napomena:
Računari koji koriste Windows Vista ili novije verzije, ili Windows Server 2008 ili novije verzije podržavaju IPsec.

Konfigurisanje opcije Default Policy

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Izaberite jednu vrednost za svaku stavku.
3. Kliknite na **Next**.

   Prikazaće se poruka sa potvrdom.
4. Kliknite na **OK**.

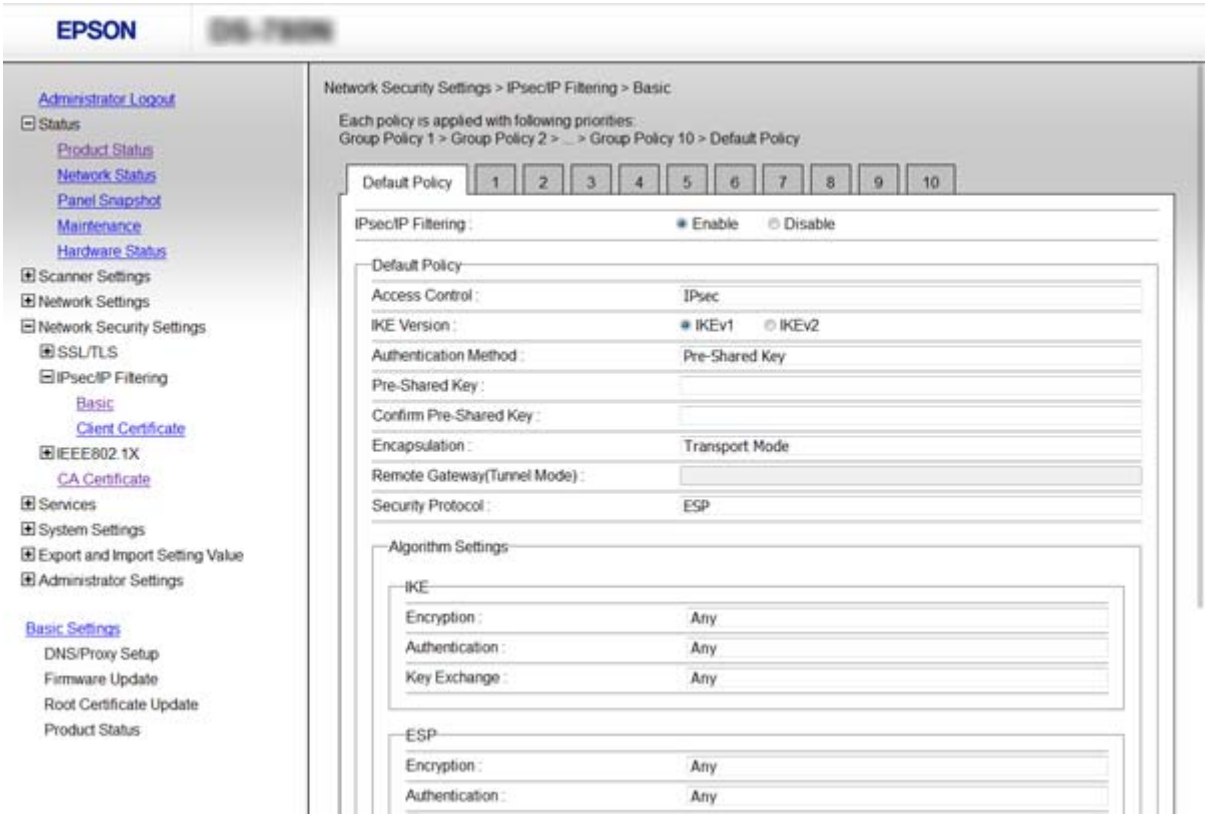
   Skener će biti ažuriran.

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

➡ “Default Policy — stavke podešavanja” na strani 72

Default Policy — stavke podešavanja



Stavke	Podešavanja i objašnjenje
IPsec/IP Filtering	Možete da omogućite ili onemogućite funkciju IPsec/IP filtriranja.

Napredne bezbednosne postavke za Enterprise

Stavke	Podešavanja i objašnjenje	
Access Control	Konfigurišite način kontrole saobraćaja IP paketa.	
	Permit Access	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IP paketima.
	Refuse Access	Izaberite ovu stavku ako želite da zabranite prolaz definisanim IP paketima.
	IPsec	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IPsec paketima.
IKE Version	Kao IKE verziju izaberite IKEv1 ili IKEv2. Izaberite jednu od njih na osnovu uređaja s kojim je skener povezan.	
IKEv1	Kada odaberete **IKEv1** kao **IKE Version**, biće prikazane sledeće stavke.	
	Authentication Method	Da biste mogli da izaberete **Certificate**, potrebno je da unapred dobijete i uvezete CA sertifikat.
	Pre-Shared Key	Ako izaberete **Pre-Shared Key** za **Authentication Method**, unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.
IKEv2	Kada odaberete **IKEv2** kao **IKE Version**, biće prikazane sledeće stavke.	
Local	Authentication Method	Da biste mogli da izaberete **Certificate**, potrebno je da unapred dobijete i uvezete CA sertifikat.
	ID Type	Izaberite vrstu ID oznake za skener.
	ID	Unesite ID skenera koji odgovara vrsti ID oznake. Kao prvi znak ne možete upotrebiti „@“, „#“, i „=“. **Distinguished Name**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „=“. **IP Address**: Unesite format IPv4 ili IPv6. **FQDN**: Unesite kombinaciju znakova dužine od 1 do 255 znakova, koristeći znakove A–Z, a–z, 0–9, „-“ i tačku (.). **Email Address**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „@“. **Key ID**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.
	Pre-Shared Key	Ako izaberete **Pre-Shared Key** za **Authentication Method**, unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.

Napredne bezbednosne postavke za Enterprise

Stavke	Podešavanja i objašnjenje	
Remote	Authentication Method	Da biste mogli da izaberete **Certificate**, potrebno je da unapred dobijete i uvezete CA sertifikat.
	ID Type	Izaberite vrstu ID oznake za uređaj čiji identitet želite da proverite.
	ID	Unesite ID skenera koji odgovara vrsti ID oznake. Kao prvi znak ne možete upotrebiti „@“, „#“, i „=“. **Distinguished Name**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „=“. **IP Address**: Unesite format IPv4 ili IPv6. **FQDN**: Unesite kombinaciju znakova dužine od 1 do 255 znakova, koristeći znakove A–Z, a–z, 0–9, „-“ i tačku (.). **Email Address**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „@“. **Key ID**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.
	Pre-Shared Key	Ako izaberete **Pre-Shared Key** za **Authentication Method**, unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.
Encapsulation	Ako izaberete **IPsec** za **Access Control**, potrebno je da konfigurišete režim enkapsulacije.	
	Transport Mode	Izaberite ovu opciju ako skener uvek koristite na istoj LAN mreži. IP paketi sloja 4 i viših slojeva se šifruju.
	Tunnel Mode	Ako koristite skener na mreži sa mogućnošću priključenja na internet, kao što je IPsec-VPN, izaberite ovu opciju. Zaglavlje i podaci o IP paketima se šifruju.
Remote Gateway(Tunnel Mode)	Ako izaberete **Tunnel Mode** za **Encapsulation**, unesite adresu mrežnog prolaza od 1 do 39 znakova.	
Security Protocol	**IPsec** za **Access Control**, odaberite jednu opciju.	
	ESP	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka i kako biste šifrovali podatke.
	AH	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka. Čak i ako je šifrovanje podataka zabranjeno, možete da koristite IPsec.
Algorithm Settings		
IKE	Encryption	Odaberite algoritam za šifrovanje za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.
	Authentication	Odaberite algoritam za proveru identiteta za IKE.
	Key Exchange	Odaberite algoritam za razmenu ključeva za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.

Stavke	Podešavanja i objašnjenje	
ESP	Encryption	Odaberite algoritam za šifrovanje za ESP. Ova funkcija je dostupna kada je **ESP** podešen na **Security Protocol**.
	Authentication	Odaberite algoritam za proveru identiteta za ESP. Ova funkcija je dostupna kada je **ESP** podešen na **Security Protocol**.
AH	Authentication	Odaberite algoritam za šifrovanje za AH. Ova funkcija je dostupna kada je **AH** podešen na **Security Protocol**.

Povezane informacije

➡ "Konfigurisanje opcije Default Policy" na strani 72

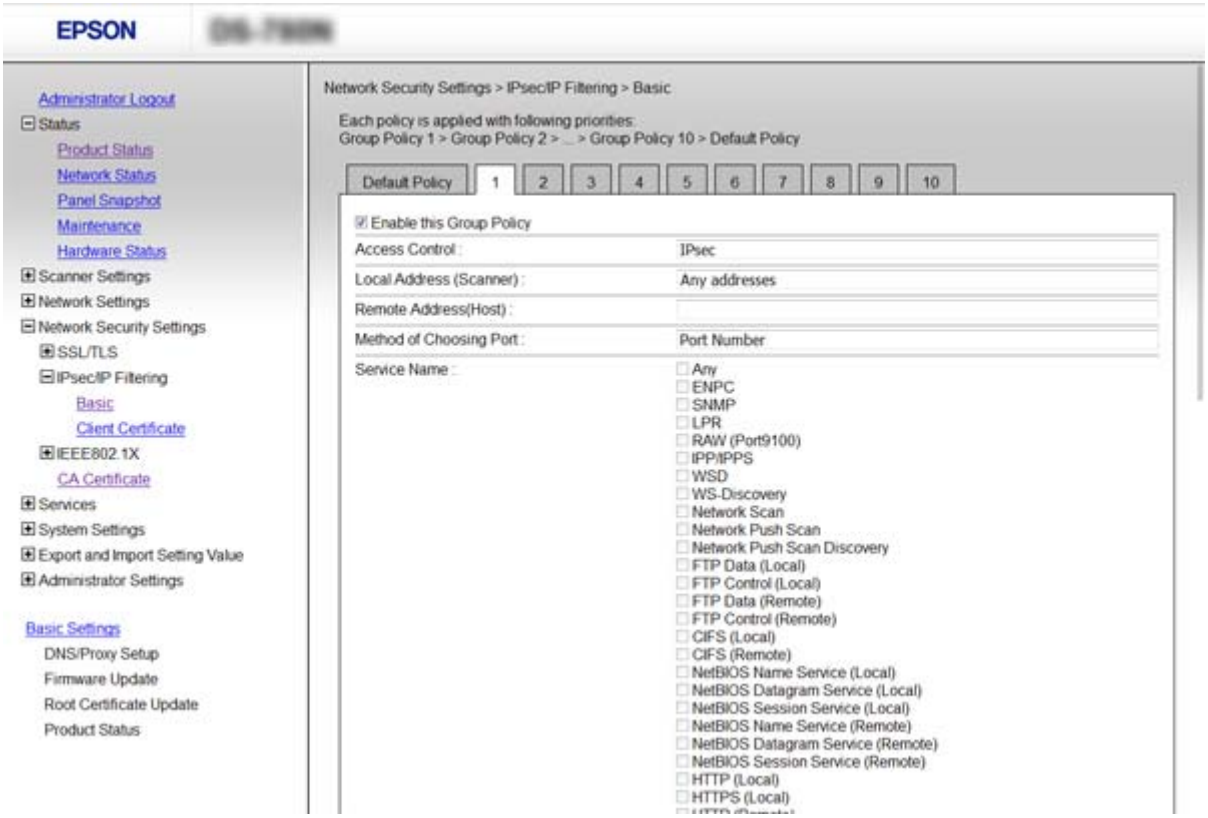
Konfigurisanje opcije Group Policy

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Kliknite na brojčanu karticu koju želite da konfigurišete.
3. Izaberite jednu vrednost za svaku stavku.
4. Kliknite na **Next**.
   Prikazaće se poruka sa potvrdom.
5. Kliknite na **OK**.
   Skener će biti ažuriran.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23
➡ "Group Policy — stavke podešavanja" na strani 76

Group Policy — stavke podešavanja



Stavke	Podešavanja i objašnjenje	
Enable this Group Policy	Možete da omogućite ili onemogućite smernicu za grupu.	
Access Control	Konfigurišite način kontrole saobraćaja IP paketa.	
	Permit Access	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IP paketima.
	Refuse Access	Izaberite ovu stavku ako želite da zabranite prolaz definisanim IP paketima.
	IPsec	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IPsec paketima.
Local Address (Scanner)	Izaberite IPv4 adresu ili IPv6 adresu koja odgovara vašem mrežnom okruženju. Ako se IP adresa dodeli automatski, možete izabrati **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Unesite IP adresu uređaja da biste mogli da upravljate pristupom. IP adresa mora biti dužine do 43 znaka. Ako ne unesete IP adresu, kontrolisaće se sve adrese. ***Napomena:*** *Ako je IP adresa automatski dodeljena (npr. ako ju je dodelio DHCP), povezivanje možda neće biti moguće. Konfigurišite statičku IP adresu.*	
Method of Choosing Port	Izaberite način određivanja portova.	
Service Name	Ako izaberete **Service Name** za **Method of Choosing Port**, izaberite neku opciju.	

Napredne bezbednosne postavke za Enterprise

Stavke	Podešavanja i objašnjenje	
Transport Protocol	Ako izaberete **Port Number** za **Method of Choosing Port**, potrebno je da konfigurišete režim enkapsulacije.	
	Any Protocol	Izaberite ovu stavku kako biste upravljali vrstama protokola.
	TCP	Izaberite ovu stavku kako biste upravljali podacima za unicast.
	UDP	Izaberite ovu stavku kako biste upravljali podacima za broadcast i multicast.
	ICMPv4	Izaberite ovu stavku kako biste upravljali komandom za ping.
Local Port	Ako izaberete **Port Number** za **Method of Choosing Port** i ako izaberete **TCP** ili **UDP** za **Transport Protocol**, unesite brojeve portova za upravljanje prijemom paketa, odvojene zapetama. Možete da unesete najviše 10 brojeva portova. Primer: 20,80,119,5220 Ako ne unesete broj porta, kontrolisaće se svi portovi.	
Remote Port	Ako izaberete **Port Number** za **Method of Choosing Port** i ako izaberete **TCP** ili **UDP** za **Transport Protocol**, unesite brojeve portova za upravljanje slanjem paketa, odvojene zapetama. Možete da unesete najviše 10 brojeva portova. Primer: 25,80,143,5220 Ako ne unesete broj porta, kontrolisaće se svi portovi.	
IKE Version	Kao IKE verziju izaberite IKEv1 ili IKEv2. Izaberite jednu od njih na osnovu uređaja s kojim je skener povezan.	
IKEv1	Kada odaberete **IKEv1** kao **IKE Version**, biće prikazane sledeće stavke.	
	Authentication Method	Ako izaberete **IPsec** za **Access Control**, izaberite neku opciju. Za podrazumevanu smernicu uobičajen je korišćeni sertifikat.
	Pre-Shared Key	Ako izaberete **Pre-Shared Key** za **Authentication Method**, unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.
IKEv2	Kada odaberete **IKEv2** kao **IKE Version**, biće prikazane sledeće stavke.	

Napredne bezbednosne postavke za Enterprise

Stavke	Podešavanja i objašnjenje	
Local	Authentication Method	Ako izaberete **IPsec** za **Access Control**, izaberite neku opciju. Za podrazumevanu smernicu uobičajen je korišćeni sertifikat.
	ID Type	Izaberite vrstu ID oznake za skener.
	ID	Unesite ID skenera koji odgovara vrsti ID oznake. Kao prvi znak ne možete upotrebiti „@“, „#“, i „=“. **Distinguished Name**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „=“. **IP Address**: Unesite format IPv4 ili IPv6. **FQDN**: Unesite kombinaciju znakova dužine od 1 do 255 znakova, koristeći znakove A–Z, a–z, 0–9, „-“ i tačku (.). **Email Address**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „@“. **Key ID**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.
	Pre-Shared Key	Ako izaberete **Pre-Shared Key** za **Authentication Method**, unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.
Remote	Authentication Method	Ako izaberete **IPsec** za **Access Control**, izaberite neku opciju. Za podrazumevanu smernicu uobičajen je korišćeni sertifikat.
	ID Type	Izaberite vrstu ID oznake za uređaj čiji identitet želite da proverite.
	ID	Unesite ID skenera koji odgovara vrsti ID oznake. Kao prvi znak ne možete upotrebiti „@“, „#“, i „=“. **Distinguished Name**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „=“. **IP Address**: Unesite format IPv4 ili IPv6. **FQDN**: Unesite kombinaciju znakova dužine od 1 do 255 znakova, koristeći znakove A–Z, a–z, 0–9, „-“ i tačku (.). **Email Address**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „@“. **Key ID**: Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.
	Pre-Shared Key	Ako izaberete **Pre-Shared Key** za **Authentication Method**, unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.

Napredne bezbednosne postavke za Enterprise

Stavke	Podešavanja i objašnjenje	
Encapsulation	Ako izaberete **IPsec** za **Access Control**, potrebno je da konfigurišete režim enkapsulacije.	
	Transport Mode	Izaberite ovu opciju ako skener uvek koristite na istoj LAN mreži. IP paketi sloja 4 i viših slojeva se šifruju.
	Tunnel Mode	Ako koristite skener na mreži sa mogućnošću priključenja na internet, kao što je IPsec-VPN, izaberite ovu opciju. Zaglavlje i podaci o IP paketima se šifruju.
Remote Gateway(Tunnel Mode)	Ako izaberete **Tunnel Mode** za **Encapsulation**, unesite adresu mrežnog prolaza od 1 do 39 znakova.	
Security Protocol	Ako izaberete **IPsec** za **Access Control**, izaberite neku opciju.	
	ESP	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka i kako biste šifrovali podatke.
	AH	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka. Čak i ako je šifrovanje podataka zabranjeno, možete da koristite IPsec.
Algorithm Settings		
IKE	Encryption	Odaberite algoritam za šifrovanje za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.
	Authentication	Odaberite algoritam za proveru identiteta za IKE.
	Key Exchange	Odaberite algoritam za razmenu ključeva za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.
ESP	Encryption	Odaberite algoritam za šifrovanje za ESP. Ova funkcija je dostupna kada je **ESP** podešen na **Security Protocol**.
	Authentication	Odaberite algoritam za proveru identiteta za ESP. Ova funkcija je dostupna kada je **ESP** podešen na **Security Protocol**.
AH	Authentication	Odaberite algoritam za proveru identiteta za AH. Ova funkcija je dostupna kada je **AH** podešen na **Security Protocol**.

Povezane informacije

➡ “Konfigurisanje opcije Group Policy” na strani 75

➡ “Kombinacija Local Address (Scanner) i Remote Address(Host) on Group Policy” na strani 79

➡ “Reference naziva usluge u smernicama za grupe” na strani 80

Kombinacija Local Address (Scanner) i Remote Address(Host) on Group Policy

	Podešavanje Local Address (Scanner)		
	IPv4	IPv6*2	Any addresses*3

Podešavanje Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Prazno	✓	✓	✓

*1 Ako je izabrano **IPsec** za **Access Control**, ne možete odrediti u unapred definisanoj dužini.

*2 Ako je izabrano **IPsec** za **Access Control**, možete izabrati vezu sa lokalnom mrežom (fe80::), ali smernice za grupe će biti onemogućene.

*3 Osim za lokalne adrese IPv6 linka.

Reference naziva usluge u smernicama za grupe

Napomena:
Nedostupne usluge su prikazane, ali se ne mogu izabrati.

Naziv usluge	Tip protokola	Broj lokalnog porta	Broj udaljenog porta	Funkcije koje se kontrolišu
Any	–	–	–	Sve usluge
ENPC	UDP	3289	Bilo koji port	Traženje skenera iz aplikacije kao što je EpsonNet Config i upravljačkog programa skenera
SNMP	UDP	161	Bilo koji port	Preuzimanje i konfigurisanje MIB iz aplikacije kao što je EpsonNet Config i Epson upravljačkog programa skenera
WSD	TCP	Bilo koji port	5357	Kontrolni WSD
WS-Discovery	UDP	3702	Bilo koji port	Traženje skenera iz WSD
Network Scan	TCP	1865	Bilo koji port	Prosleđivanje skeniranih podataka iz aplikacije Document Capture Pro
Network Push Scan Discovery	UDP	2968	Bilo koji port	Traženje računara sa skenera
Network Push Scan	TCP	Bilo koji port	2968	Preuzimanje informacija o zadatku skeniranja s uređaja iz aplikacije Document Capture Pro ili Document Capture
HTTP (Local)	TCP	80	Bilo koji port	HTTP(S) server (prosleđivanje podataka o Web Config i WSD)
HTTPS (Local)	TCP	443	Bilo koji port	
HTTP (Remote)	TCP	Bilo koji port	80	HTTP(S) klijent (komunikacija između ažuriranja upravljačkog softvera i ažuriranje korenskog sertifikata)
HTTPS (Remote)	TCP	Bilo koji port	443	

Primeri konfigurisanja opcije IPsec/IP Filtering

Prijem samo IPsec paketa

Ovaj primer služi samo za konfigurisanje podrazumevane smernice.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: Unesite najviše 127 znakova.

Group Policy:

Nemojte je konfigurisati.

Prihvatanje skeniranja uz pomoć Epson Scan 2 i podešavanja skenera

Primer pokazuje komunikacije podataka za skeniranje i konfiguracije skenera sa navedenih usluga.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Štiklirajte ovo polje.

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

❏ **Remote Address(Host)**: IP adresa klijenta

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

❏ **Service Name**: Zabeležite polje **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** i **HTTPS (Local)**.

Prihvatanje pristupa samo sa određene IP adrese

U ovom primeru pristup skeneru se dozvoljava samo određenim IP adresama.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Štiklirajte ovo polje.

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

❏ **Remote Address(Host)**: IP adresa klijenta administratora

Napomena:
Bez obzira na konfiguraciju smernice, klijent će moći da pristupi skeneru i da ga konfiguriše.

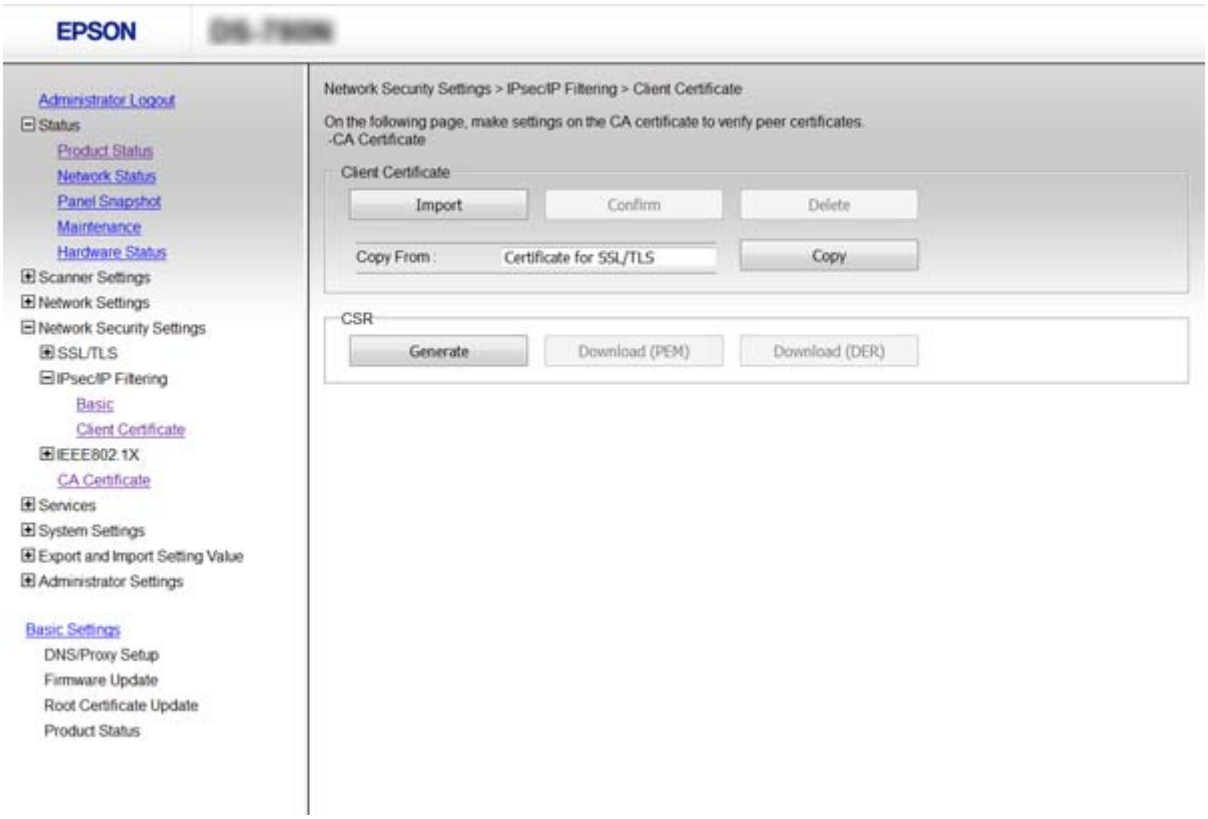
Konfigurisanje sertifikata za IPsec/IP Filtering

Konfigurišite klijentski sertifikat za IPsec/IP filtriranje. Ako želite da konfigurišete sertifikaciono telo, idite u **CA Certificate**.

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Uvezite sertifikat u **Client Certificate**.

   Ako ste već uvezli sertifikat objavljen od strane sertifikacionog tela u IEEE802.1X u SSL/TLS, možete da kopirate sertifikat i koristite ga u IPsec/IP filtriranju. Da biste kopirali, izaberite sertifikat u **Copy From**, a zatim kliknite na **Copy**.



Povezane informacije

➡ “Pristup programu Web Config” na strani 23

➡ “Pribavljanje i uvoz CA sertifikata” na strani 64

Upotreba SNMPv3 protokola

O protokolu SNMPv3

SNMP je protokol koji vrši praćenje i kontrolu kako bi prikupio informacije od uređaja koji su priključeni na mrežu. SNMPv3 je verzija funkcije upravljanja bezbednošću koja je unapređena.

Prilikom korišćenja protokola SNMPv3, praćenje stanja i promene postavki komunikacionog (paketa) SNMP mogu biti šifrovane i zahtevati proveru identiteta kako bi komunikacioni (paket) SNMP bio zaštićen od rizika na mreži, poput prisluškivanja, lažnog predstavljanja i neovlašćenih izmena.

Konfigurisanje SNMPv3

Ako skener podržava SNMPv3 protokol, možete da nadgledate i upravljate pristupom skeneru.

1. Pristupite programu Web Config i izaberite **Services** > **Protocol**.
2. Izaberite jednu vrednost za svaku stavku na meniju **SNMPv3 Settings**.
3. Kliknite na **Next**.

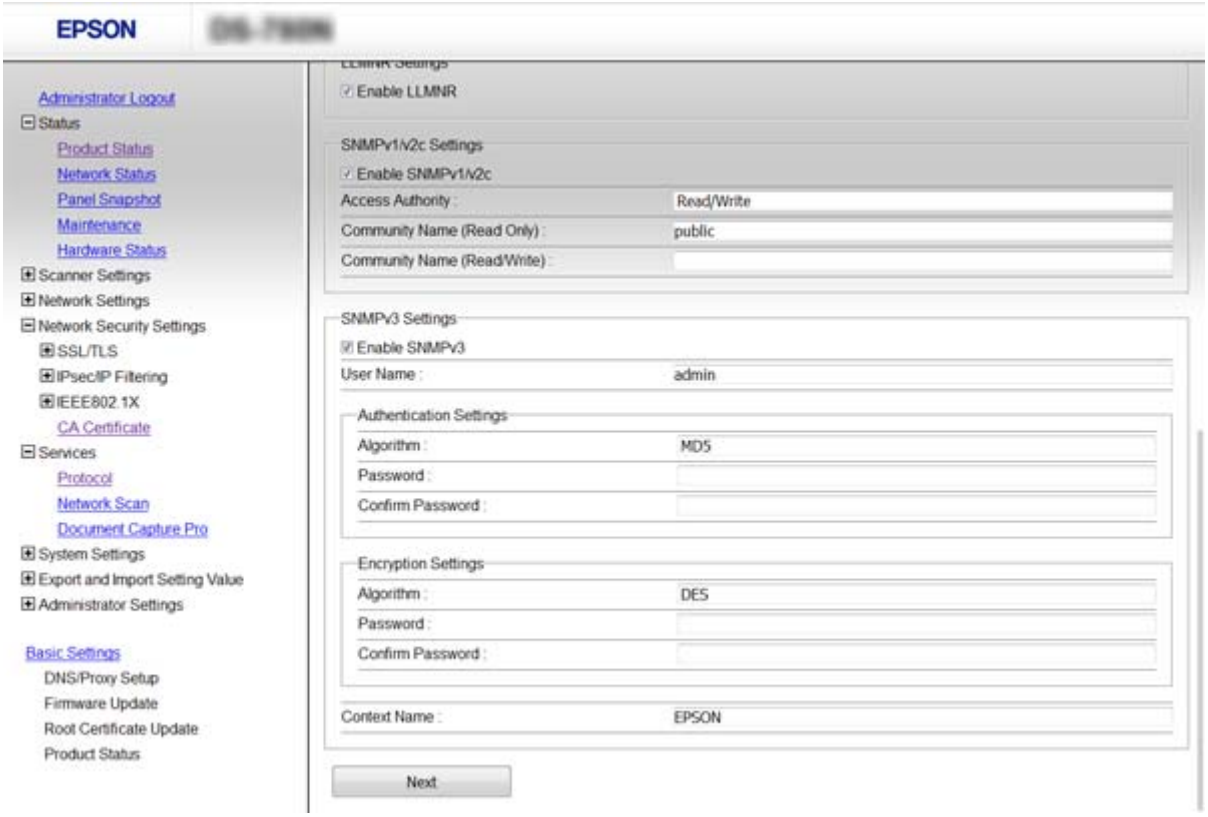
   Prikazaće se poruka sa potvrdom.
4. Kliknite na **OK**.

   Skener će biti ažuriran.

Povezane informacije

➡ “Pristup programu Web Config” na strani 23
➡ “Postavke za SNMPv3” na strani 83

Postavke za SNMPv3



Napredne bezbednosne postavke za Enterprise

Stavke	Postavke i objašnjenja
Enable SNMPv3	SNMPv3 protokol je omogućen kada je polje štiklirano.
User Name	Unesite između 1 i 32 znakova koristeći znake od 1 bajta.
Authentication Settings	
Algorithm	Izaberite algoritam za proveru identiteta.
Password	Unesite između 8 i 32 znakova u formatu ASCII (0x20-0x7E).
Confirm Password	Unesite lozinku koju ste konfigurisali radi potvrde.
Encryption Settings	
Algorithm	Izaberite algoritam za šifrovanje.
Password	Unesite između 8 i 32 znakova u formatu ASCII (0x20-0x7E).
Confirm Password	Unesite lozinku koju ste konfigurisali radi potvrde.
Context Name	Unesite između 1 i 32 znakova koristeći znake od 1 bajta.

Povezane informacije

➡ "Konfigurisanje SNMPv3" na strani 83

Povezivanje skenera na IEEE802.1X mrežu

Konfigurisanje IEEE802.1X mreže

Ako skener podržava IEEE802.1X, možete da ga koristite na mreži sa proverom identiteta koja je povezana sa RADIUS serverom i čvorištem koje proverava identitet.

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Izaberite jednu vrednost za svaku stavku.
3. Kliknite na **Next**.

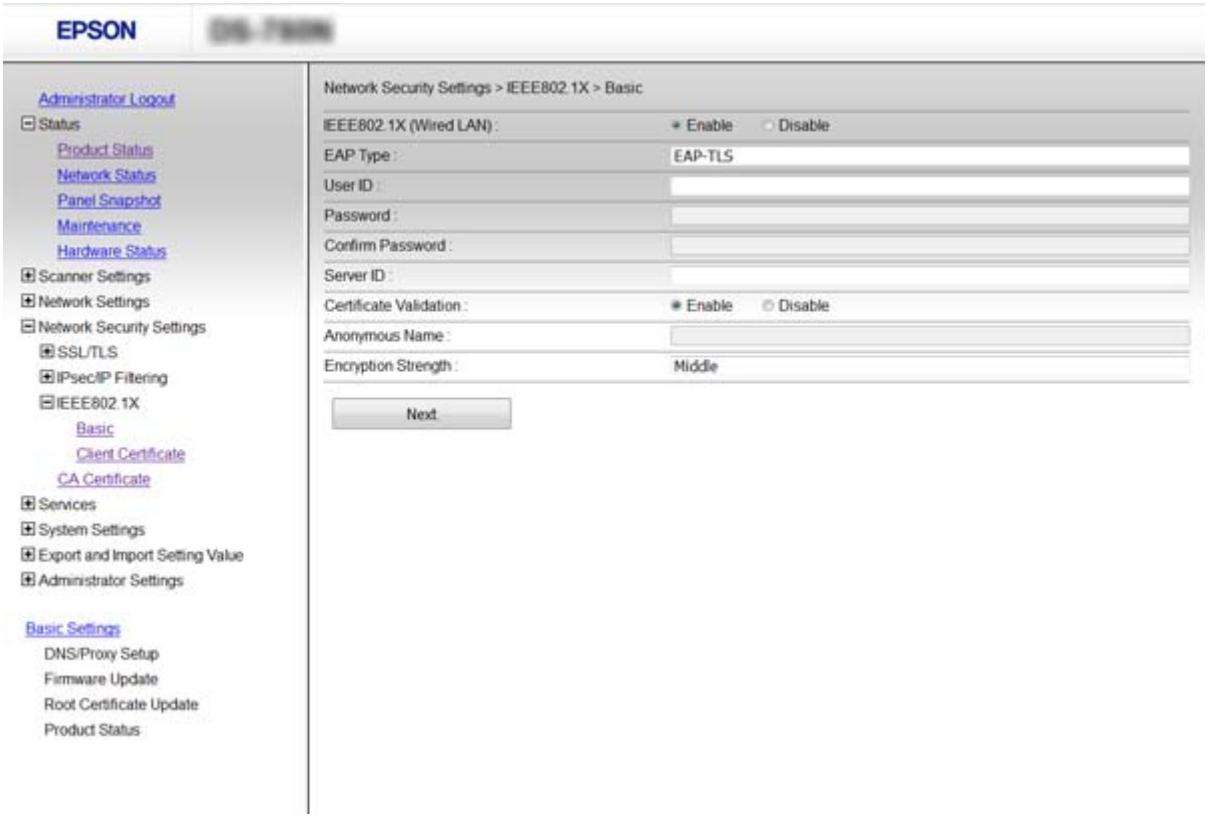
   Prikazaće se poruka sa potvrdom.
4. Kliknite na **OK**.

   Skener će biti ažuriran.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23
➡ "IEEE802.1X mreža — stavke podešavanja" na strani 85
➡ "Ne možete pristupiti štampaču ili skeneru nakon konfigurisanja IEEE802.1X" na strani 89

IEEE802.1X mreža — stavke podešavanja



Stavke	Podešavanja i objašnjenje	
IEEE802.1X (Wired LAN)	Možete da omogućite ili onemogućite podešavanja stranice (**IEEE802.1X** > **Basic**) za IEEE802.1X (ožičena LAN mreža).	
EAP Type	Izaberite metod provere identiteta između skenera i RADIUS servera.	
	EAP-TLS	Morate pribaviti i uvesti CA sertifikat.
	PEAP-TLS	
	PEAP/MSCHAPv2	Morate konfigurisati lozinku.
User ID	Konfigurišite ID koji će se koristiti za proveru identiteta RADIUS servera. Unesite između 1 i 128 1-bitnih ASCII (od 0x20 do 0x7E) znakova.	
Password	Konfigurišite lozinku kojom će se proveravati identitet skenera. Unesite između 1 i 128 1-bitnih ASCII (od 0x20 do 0x7E) znakova. Ako koristite a Windows server kao RADIUS server, možete da unesete do 127 znakova.	
Confirm Password	Kao potvrdu, unesite lozinku koju ste konfigurisali.	
Server ID	Možete da konfigurišete ID na serveru kojim će se proveravati vaš identitet na RADIUS serveru. Čvorište koje proverava identitet će proveriti da li je ID servera sadržan u polju subject/subjectAltName u sertifikatu servera koji je poslat sa RADIUS servera. Unesite između 0 i 128 1-bitnih ASCII (od 0x20 do 0x7E) znakova.	
Certificate Validation	Možete da podesite validaciju sertifikata bez obzira na metod provere identiteta. Uvezite sertifikat u **CA Certificate**.	

Stavke	Podešavanja i objašnjenje	
Anonymous Name	Ako izaberete **PEAP-TLS** ili **PEAP/MSCHAPv2** kao **Authentication Method**, možete da konfigurišete anonimno ime umesto korisničkog ID-a za fazu 1 PEAP provere identiteta. Unesite između 0 i 128 1-bitnih ASCII (od 0x20 do 0x7E) znakova.	
Encryption Strength	Možete da izaberete jednu od sledećih stavki.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Povezane informacije

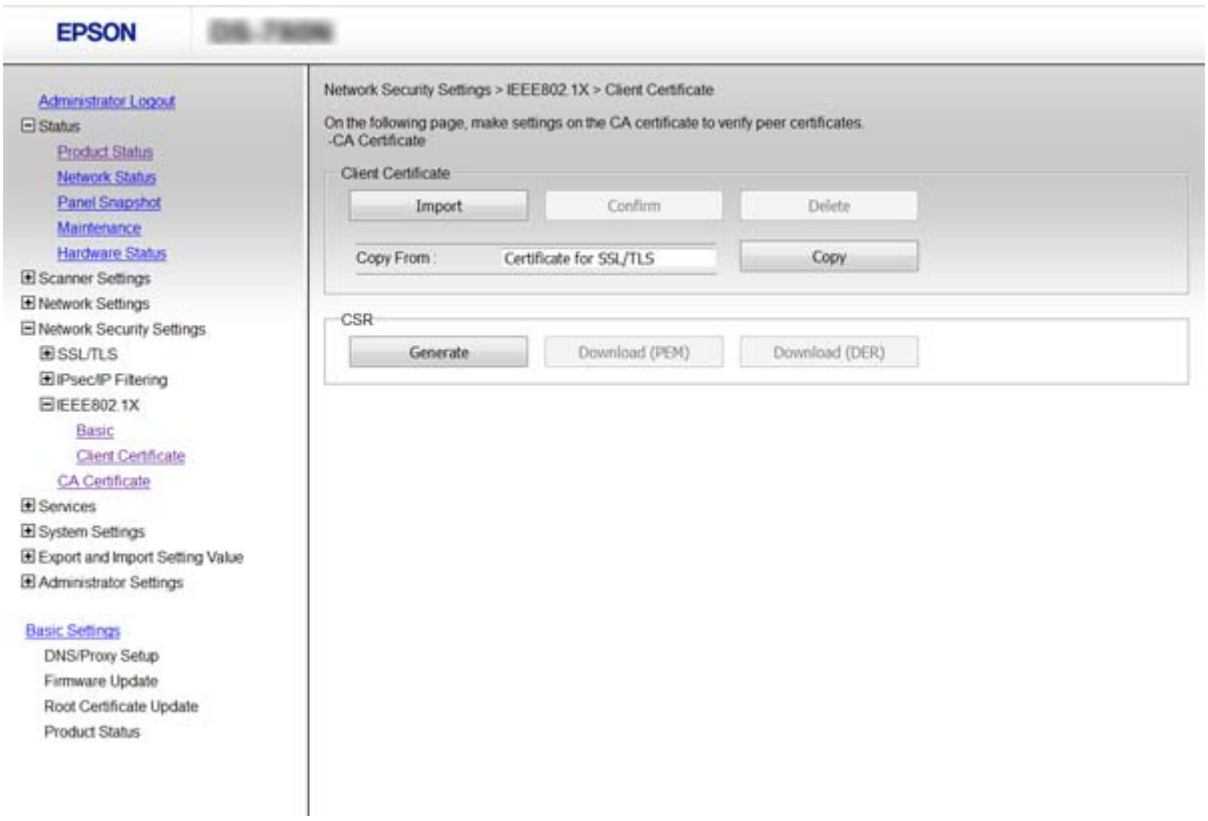
➡ "Konfigurisanje IEEE802.1X mreže" na strani 84

Konfigurisanje sertifikata za IEEE802.1X

Konfigurišite klijentski sertifikat za IEEE802.1X. Ako želite da konfigurišete sertifikat sertifikacionog tela, idite u **CA Certificate**.

1. Pristupite programu Web Config i izaberite **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Unesite sertifikat u polje **Client Certificate**.

   Možete da kopirate sertifikat ako je objavljen od strane sertifikacionog tela. Da biste kopirali, izaberite sertifikat u **Copy From**, a zatim kliknite na **Copy**.



Povezane informacije

➡ “Pristup programu Web Config” na strani 23

➡ “Pribavljanje i uvoz CA sertifikata” na strani 64

Rešavanje problema naprednih bezbednosnih postavki

Vraćanje bezbednosnih podešavanja

Kada uspostavite izuzetno bezbedno okruženje, kao što su IPsec/IP filtriranje ili IEEE802.1X, moguće je da nećete moći da komunicirate s uređajima zbog neispravnih podešavanja ili problema s uređajem ili serverom. U tom slučaju vratite bezbednosna podešavanja kako biste ponovo podesili uređaj ili kako biste mogli privremeno da ga koristite.

Onemogućavanje bezbednosne funkcije pomoću kontrolne table

IPsec/IP filtriranje ili IEEE802.1X možete da onemogućite pomoću kontrolne table skenera.

1. Dodirnite **Podešavanja** > **Mrežne postavke**.
2. Dodirnite **Promeni postavke**.
3. Odaberite stavke koje želite da onemogućite.
   - ❏ **IPsec/IP filtriranje**
   - ❏ **IEEE802.1X**
4. Kada se prikaže poruka o završetku, dodirnite **Nastavi**.

Vraćanje bezbednosne funkcije pomoću alatke Web Config

Kod funkcije IEEE802.1X postoji mogućnost da uređaji ne budu prepoznati na mreži. U tom slučaju onemogućite tu funkciju pomoću kontrolne table skenera.

Kod IPsec/IP filtriranja funkciju možete onemogućiti ako možete da pristupite uređaju s računara.

Onemogućavanje IPsec/IP filtriranja pomoću Web Config

1. Pristupite programu Web Config i odaberite **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Izaberite **Disable** za **IPsec/IP Filtering** u **Default Policy**.
3. Kliknite na **Next**, a zatim isključite **Enable this Group Policy** za sve grupne smernice.
4. Kliknite na **OK**.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Problemi pri korišćenju funkcija za bezbednost na mreži

Ako zaboravite preliminarno deljenu šifru

Ponovo konfigurišite šifru uz pomoć programa Web Config.

Da biste promenili šifru, pristupite Web Config i izaberite **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** ili **Group Policy**.

Kada promenite preliminarno deljenu šifru, konfigurišite preliminarno deljenu šifru za računare.

Povezane informacije

➡ "Pristup programu Web Config" na strani 23

Komunikacija preko IPsec protokola nije moguća

Da li koristite nepodržani algoritam za postavke računara?

Skener podržava sledeće algoritme.

Načini zaštite	Algoritmi
IKE algoritam za šifrovanje	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE algoritam za proveru identiteta	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE algoritam za razmenu ključeva	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP algoritam za šifrovanje	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP algoritam za proveru identiteta	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH algoritam za proveru identiteta	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Dostupan samo za IKEv2

Povezane informacije

➡ "Šifrovana komunikacija pomoću IPsec/IP filtriranja" na strani 71

Komunikacija je naglo prekinuta

Da li je IP adresa skenera netačna ili se promenila?

Onemogućite IPsec preko kontrolne table skenera.

Ako je DHCP istekao, ponovo se pokreće ili je IPv6 adresa istekla ili nije pribavljena, tada se može dogoditi da IP adresa registrovana za Web Config skenera (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) ne bude pronađena.

Unesite statičku IP adresu.

Da li je IP adresa računara netačna ili se promenila?

Onemogućite IPsec preko kontrolne table skenera.

Ako je DHCP istekao, ponovo se pokreće ili je IPv6 adresa istekla ili nije pribavljena, tada se može dogoditi da IP adresa registrovana za Web Config skenera (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) ne bude pronađena.

Unesite statičku IP adresu.

Povezane informacije

➡ “Pristup programu Web Config” na strani 23

➡ “Šifrovana komunikacija pomoću IPsec/IP filtriranja” na strani 71

Povezivanje nakon konfigurisanja IPsec/IP filtriranja nije moguće

Podešena vrednost možda nije tačna.

Onemogućite IPsec/IP filtriranje na kontrolnoj tabli skenera. Povežite skener i računar i ponovo podesite IPsec/IP filtriranje.

Povezane informacije

➡ “Šifrovana komunikacija pomoću IPsec/IP filtriranja” na strani 71

Ne možete pristupiti štampaču ili skeneru nakon konfigurisanja IEEE802.1X

Moguće je da su postavke netačne.

Onemogućite IEEE802.1X sa kontrolne table skenera. Povežite skener i računar, a zatim ponovo konfigurišite IEEE802.1X.

Povezane informacije

➡ “Konfigurisanje IEEE802.1X mreže” na strani 84

Problemi pri korišćenju digitalnog sertifikata

CA sertifikat ne može da se uveze

Da li se CA sertifikat i informacije u CSR-u podudaraju?

Ako CA sertifikat i CSR ne sadrže iste informacije, CSR ne može da se uveze. Proverite sledeće stavke:

❏ Da li pokušate da uvezete sertifikat na uređaj koji ne sadrži iste informacije?
Proverite informacije u CSR-u, pa uvezite sertifikat na uređaj koji sadrži iste informacije.

❏ Da li ste zamenili CSR sačuvan na skeneru nakon slanja CSR-a sertifikacionom telu?
Ponovo pribavite CA sertifikat sa CSR-om.

Da li je CA sertifikat veći od 5 KB?

CA sertifikat veći od 5 KB ne može da se uveze.

Da li je lozinka za uvoz sertifikata tačna?

Ako zaboravite lozinku, nećete moći da uvezete sertifikat.

Povezane informacije

➡ “Uvoz CA sertifikata” na strani 66

Nezavisni sertifikat nije moguće ažurirati

Da li je uneto Common Name?

Potrebno je uneti **Common Name**.

Da li su u polje Common Name uneti neki znakovi koji nisu podržani? Na primer, japanski jezik nije podržan.

Unesite između 1 i 128 znakova u formatu IPv4, IPv6, kao ime hosta ili u formatu FQDN u obliku ASCII (0x20-0x7E).

Da li Common Name sadrži razmak ili zapetu?

Ako unesete zapetu, **Common Name** se deli na tom mestu. Ako se unese samo razmak pre ili posle zapete, pojaviće se greška.

Povezane informacije

➡ “Ažuriranje nezavisnog sertifikata” na strani 68

Nije moguće kreirati CSR

Da li je uneto Common Name?

Potrebno je uneti **Common Name**.

Da li su u polja Common Name, Organization, Organizational Unit, Locality, State/Province uneti neki znakovi koji nisu podržani? Na primer, japanski jezik nije podržan.

Unesite znakove u formatu IPv4, IPv6, kao ime hosta ili u formatu FQDN u obliku ASCII (0x20-0x7E).

Da li Common Name sadrži razmak ili zapetu?

Ako unesete zapetu, **Common Name** se deli na tom mestu. Ako se unese samo razmak pre ili posle zapete, pojaviće se greška.

Povezane informacije

➡ "Pribavljanje CA sertifikata" na strani 64

Pojavljuje se upozorenje koje se odnosi na digitalni sertifikat

Poruke	Uzrok/lek
Enter a Server Certificate.	**Uzrok:** Niste izabrali datoteku za uvoz. **Lek:** Izaberite jednu datoteku i kliknite na **Import**.
CA Certificate 1 is not entered.	**Uzrok:** CA sertifikat 1 nije unet, već je unet samo CA sertifikat 2. **Lek:** Prvo uvezite CA sertifikat 1.
Invalid value below.	**Uzrok:** Putanja datoteke i/ili lozinka sadrži nepodržane znakove. **Lek:** Proverite da li se stavka sastoji iz odgovarajućih znakova.
Invalid date and time.	**Uzrok:** U skeneru nisu podešeni vreme i datum. **Lek:** Podesite vreme i datum pomoću programa Web Config ili EpsonNet Config.
Invalid password.	**Uzrok:** Lozinka podešena za CA sertifikat i uneta lozinka se ne podudaraju. **Lek:** Unesite tačno lozinku.

Napredne bezbednosne postavke za Enterprise

Poruke	Uzrok/lek
Invalid file.	**Uzrok:** Ne uvozite sertifikat u formatu datoteke X509. **Lek:** Proverite da li ste izabrali odgovarajući sertifikat koji vam je poslalo pouzdano sertifikaciono telo.
	Uzrok: Datoteka koju ste uvezli je prevelika. Maksimalna veličina datoteke je 5 KB. **Lek:** Ako izaberete odgovarajuću datoteku, sertifikat je možda oštećen ili lažan.
	Uzrok: Lanac u sertifikatu nije ispravan. **Lek:** Više informacija o sertifikatu potražite na veb lokaciji sertifikacionog tela.
Cannot use the Server Certificates that include more than three CA certificates.	**Uzrok:** Sertifikat u formatu datoteke PKCS#12 sadrži više od 3 CA sertifikata. **Lek:** Svaki sertifikat uvezite nakon konvertovanja iz formata PKCS#12 u format PEM ili uvezite sertifikat u formatu datoteke PKCS#12 koji sadrži do 2 CA sertifikata.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Uzrok:** Sertifikat je istekao. **Lek:** ❏ Ako je sertifikat istekao, pribavite i uvezite novi. ❏ Ako sertifikat nije istekao, proverite da li su u skeneru podešeni tačno vreme i datum.
Private key is required.	**Uzrok:** Sa sertifikatom nije uparen nijedan privatni ključ. **Lek:** ❏ Ako je sertifikat u formatu PEM/DER i ako je dobijen na osnovu CSR-a preko računara, navedite datoteku sa privatnim ključem. ❏ Ako je sertifikat u formatu PKCS#12 i ako je dobijen na osnovu CSR-a preko računara, navedite datoteku sa privatnim ključem.
	Uzrok: Ponovo ste uvezli PEM/DER sertifikat dobijen na osnovu CSR-a pomoću programa Web Config. **Lek:** Ako je sertifikat u formatu PEM/DER i ako je dobijen na osnovu CSR-a pomoću programa Web Config, možete da ga uvezete samo jednom.

Poruke	Uzrok/lek
Setup failed.	**Uzrok:** Konfigurisanje nije moguće dovršiti jer ne postoji komunikacija između skenera i računara ili ako datoteku nije moguće pročitati jer sadrži greške. **Lek:** Nakon provere navedene datoteke i komunikacije, ponovo uvezite datoteku.

Povezane informacije

➡ "O digitalnim sertifikatima" na strani 63

Greškom ste izbrisali CA sertifikat

Postoji li rezervna kopija datoteke sertifikata?

Ako imate rezervnu kopiju datoteke, ponovo uvezite sertifikat.

Ako ste sertifikat dobili na osnovu CSR formulara iz programa Web Config, ne možete ponovo da uvezete izbrisani sertifikat. Kreirajte CSR i pribavite novi sertifikat.

Povezane informacije

➡ "Brisanje CA sertifikata" na strani 67

➡ "Uvoz CA sertifikata" na strani 66