

Vodič za administratore

Sadržaj

Autorska prava

Trgovačke marke

O ovom priručniku

Oznake i simboli.	6
Opisi korišteni u ovom priručniku.	6
Oznake operativnih sustava.	6

Uvod

Komponenta priručnika.	8
Objašnjenja izraza korištenih u ovom vodiču.	8

Priprema

Tijek postavki i upravljanja skenerom.	10
Primjer mrežnog okruženja.	11
Primjer postavke za uvođenje veze skenera.	11
Pripremanje povezivanja s mrežom.	12
Prikupljanje informacija o postavci veze.	12
Specifikacije skenera.	12
Korištenje broja ulaza.	13
Način dodjele IP adrese.	13
DNS poslužitelj i proxy poslužitelj.	13
Način postavljanja mrežne veze.	13

Povezivanje

Povezivanje s mrežom.	15
Povezivanje mreže na upravljačkoj ploči.	15
Povezivanje na mrežu preko instalacijskog programa.	19

Postavke funkcije

Softver za postavljanje.	22
Web Config (web-stranica uređaja).	22
Korištenje funkcijama skena.	24
Skeniranje putem računala.	24
Skeniranje preko upravljačke ploče.	26
Odabir postavki sustava.	28
Odabir postavki sustava preko upravljačke ploče.	28
Odabir postavki sustava koristeći Web Config.	30

Osnovne postavke sigurnosti

Uvod u osnovne sigurnosne značajke.	32
Konfiguriranje lozinke administratora.	32
Konfiguriranje lozinke administratora preko upravljačke ploče.	33
Konfiguriranje lozinke administratora koristeći Web Config.	33
Stavke koje treba zaključati preko lozinke administratora.	34
Upravljanje protokolima.	35
Protokoli koje možete omogućiti ili onemogućiti.	36
Stavke postavljanja protokola.	37

Postavke načina rada i upravljanja

Potvrda informacija o uređaju.	40
Upravljanje uređajima (Epson Device Admin).	40
Primanje obavijesti o događajima putem e-pošte.	41
O obavijestima e-poštom.	41
Konfiguriranje obavijesti e-poštom.	41
Konfiguriranje poslužitelja e-pošte.	42
Provjera veze s poslužiteljem e-pošte.	44
Ažuriranje firmvera.	46
Ažuriranje firmvera koristeći Web Config.	46
Ažuriranje firmvera koristeći Epson Firmware Updater.	46
Pomoć kod postavki.	47
Izvoz postavki.	47
Uvoz postavki.	47

Rješavanje problema

Savjeti za rješavanje problema.	49
Provjera zapisnika poslužitelja i mrežnog uređaja.	49
Inicijaliziranje mrežnih postavki.	49
Oporavak mrežnih postavki s upravljačke ploče pisača.	49
Provjera komunikacije između uređaja i računala.	49
Provjera povezivanja pomoću naredbe Ping — Windows.	49
Provjera povezivanja pomoću naredbe Ping — Mac OS.	51
Problemi s korištenjem mrežnog softvera.	52
Nije moguć pristup programu Web Config.	52

Naziv modela i/ili IP adrese se ne prikazuju
na EpsonNet Config. 53

Dodatak

Uvod u mrežni softver. 55
 Epson Device Admin. 55
 EpsonNet konfiguracija. 55
 EpsonNet SetupManager. 56
 Dodjeljivanje IP adrese koristeći EpsonNet Config. . 56
 Dodjela IP adrese korištenjem postavki serije. . . 56
 Dodjela IP adrese svakom uređaju. 59
 Korištenje ulaza skenera. 60

Napredne postavke sigurnosti za tvrtku

Sigurnosne postavke i sprječavanje opasnosti. . . . 62
 Postavke sigurnosne značajke. 63
 SSL/TLS komunikacija sa skenerom. 63
 O digitalnom certificiranju. 63
 Pribavljanje i uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA). 64
 Brisanje certifikata potpisanog od strane tijela za izdavanje certifikata (CA). 67
 Ažuriranje samopotpisanog certifikata. 68
 Konfigurirajte CA Certificate. 69
 Kriptirana komunikacija korištenjem IPsec/IP filtriranja. 71
 O aplikaciji IPsec/IP Filtering. 71
 Konfiguriranje stavke Default Policy. 72
 Konfiguriranje stavke Group Policy. 75
 Primjeri konfiguracije za IPsec/IP Filtering. . . . 81
 Konfiguriranje certifikata za IPsec/IP Filtering. . 82
 Upotreba SNMPv3 protokola. 83
 O protokolu SNMPv3. 83
 Konfiguriranje protokola SNMPv3. 83
 Spajanje skenera s IEEE802.1X mrežom. 85
 Konfiguriranje IEEE802.1X mreže. 85
 Konfiguriranje certifikata za IEEE802.1X. 86
 Rješavanje problema napredne sigurnosti. 87
 Vraćanje sigurnosnih postavki. 87
 Problemi s korištenjem sigurnosnih značajki mreže. 88
 Problemi s korištenjem digitalnog certifikata. . . . 90

AutorksaAutorska prava

Nije dopušteno reproducirati, pohraniti u sustavu za ponovno korištenje ili prenositi u bilo kojem obliku ili bilo kojim putem, elektroničkim ili mehaničkim, fotokopirano, snimljeno ili na bilo koji drugi način nijedan dio ovog izdanja bez prethodnog pismenog dopuštenja Seiko Epson Corporation. Ne podrazumijeva se nikakva odgovornost za patent u pogledu upotrebe ovdje sadržanih informacija. Ne prihvaća se nikakva odgovornost za štete proizašle iz upotrebe ovdje sadržanih informacija. Ovdje sadržane informacije namijenjene su isključivo za upotrebu s proizvodom Epson. Epson nije odgovoran za upotrebu ovih informacija i primjenu na drugim proizvodima.

Ni Seiko Epson Corporation, ni njezine pridružene tvrtke nisu odgovorne prema kupcu ovog proizvoda ili trećim stranama za štete, gubitke, troškove ili izdatke kupca ili treće strane kao posljedica nezgode, neispravne upotrebe ili zloupotrebe proizvoda ili izvođenja neovlaštenih promjena, popravaka ili izmjena na proizvodu, ili (što isključuje SAD) uslijed nepoštivanja uputa za upotrebu i održavanje koje navodi Seiko Epson Corporation.

Seiko Epson Corporation i njezine pridružene tvrtke nisu odgovorne za štete ili probleme nastale uslijed upotrebe bilo koje mogućnosti ili potrošačkog proizvoda koji nije označen kao originalan Epson proizvod ili odobreni Epson proizvod od strane Seiko Epson Corporation.

Seiko Epson Corporation nije odgovorna za bilo kakve štete nastale uslijed elektromagnetske interferencije koja se pojavljuje zbog upotrebe kabela koje Seiko Epson Corporation nije označila kao odobrene Epson proizvode.

©Seiko Epson Corporation 2016.

Sadržaj ovog priručnika i specifikacije proizvoda podliježu izmjenama bez prethodne najave.

Trgovačke marke

- ❑ EPSON® je registrirana trgovačka marka, a EPSON EXCEED YOUR VISION ili EXCEED YOUR VISION trgovačke su marke 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.
- ❑ Opća napomena: svi ostali nazivi proizvoda iz priručnika koriste se samo za potrebe identifikacije i mogu biti trgovačke marke njihovih vlasnika. Epson se odriče bilo kakvih i svih prava na te marke.

O ovom priručniku

Oznake i simboli



Pozor:

Upute koje se moraju pažljivo slijediti kako bi se izbjegle tjelesne ozljede.



Važno:

Upute koje se moraju slijediti kako bi se izbjeglo oštećivanje uređaja.

Napomena:

Upute koje sadrže korisne savjete i ograničenja rukovanja skenerom.

Povezane informacije

➔ Pritiskom ove ikone otvorit će se povezane informacije.

Opisi korišteni u ovom priručniku

- Snimke zaslona dijaloškog okvira upravljačkog programa skenera i upravljačkog programa skenera Epson Scan 2 potječu iz sustava Windows 10 ili OS X El Capitan. Sadržaj prikazan na zaslonima ovisi o modelu i situaciji.
- Ilustracije korištene u ovom priručniku samo su primjeri. Iako među modelima mogu postojati neznatne razlike, njihov način rada je isti.
- Neke stavke izbornika na LCD zaslonu variraju ovisno o modelu i postavkama.

Oznake operativnih sustava

Windows

U ovom priručniku, izrazi 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 sljedeće operativne sustave. Osim toga, pojam „Windows” odnosi se na sve verzije.

- Operativni sustav Microsoft® Windows® 10
- Operativni sustav Microsoft® Windows® 8.1
- Operativni sustav Microsoft® Windows® 8
- Operativni sustav Microsoft® Windows® 7
- Operativni sustav Microsoft® Windows Vista®
- Operativni sustav Microsoft® Windows® XP
- Operativni sustav Microsoft® Windows® XP Professional x64 Edition

O ovom priručniku

- Operativni sustav Microsoft® Windows Server® 2016
- Operativni sustav Microsoft® Windows Server® 2012 R2
- Operativni sustav Microsoft® Windows Server® 2012
- Operativni sustav Microsoft® Windows Server® 2008 R2
- Operativni sustav Microsoft® Windows Server® 2008
- Operativni sustav Microsoft® Windows Server® 2003 R2
- Operativni sustav Microsoft® Windows Server® 2003

Mac OS

U ovom priručniku, „Mac OS” se koristi za 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

Komponenta priručnika

Ovaj priručnik namijenjen je administratoru uređaja koji je odgovoran za spajanje pisača ili skenera na mrežu i sadrži informacije o odabiru postavki za uporabu tih funkcija.

Pogledajte *Korisnički vodič* s informacijama o korištenju funkcije.

Priprema

Objašnjava zadatke administratora, način postavljanja uređaja i softver za upravljanje.

Povezivanje

Objašnjava povezivanje uređaja na mrežu ili telefonsku liniju. Također objašnjava mrežno okruženje, primjerice korištenje ulaza za uređaj, informacije o DNS-u i proxy poslužitelju.

Postavke funkcije

Objašnjava postavke svake funkcije uređaja.

Osnovne postavke sigurnosti

Objašnjava postavke svake funkcije, kao što je ispisivanje, skeniranje i faksiranje.

Postavke načina rada i upravljanja

Objašnjava radnje nakon početka korištenja uređaja, poput provjera informacija i održavanja.

Rješavanje problema

Objašnjava inicijalizaciju postavki i rješavanje problema s mrežom.

Napredne postavke sigurnosti za tvrtku

Objašnjava način postavki za poboljšanje sigurnosti uređaja, poput korištenja CA certifikata, SSL/TLS komunikacije i IPsec/IP filtriranja.

Ovisno o modelu, neke funkcije u ovom poglavlju nisu podržane.

Objašnjenja izraza korištenih u ovom vodiču

U ovom vodiču korišteni su sljedeći izrazi.

Administrator

Osoba odgovorna za instaliranje i postavljanje uređaja ili mreže unutar ureda ili tvrtke. Kod manjih tvrtki ta osoba može biti zadužena za upravljanje uređajima i mrežom. Kod većih tvrtki administratori imaju ovlaštenje za mrežu ili uređaje skupine jedinica unutar odjela ili sektora, a administratori mreže odgovorni su za postavke komunikacije izvan tvrtke, primjerice za internet.

Uvod

Administrator mreže

Osoba zadužena za nadzor mrežne komunikacije. Osoba koja postavlja usmjernik, proxy poslužitelj, DNS poslužitelj i poslužitelj e-pošte radi nadzora komunikacije putem interneta ili mrežnog sustava.

Korisnik

Osoba koja koristi uređaje, kao što su pisači ili skeneri.

Web Config (web-stranica uređaja)

Web-poslužitelj koji je ugrađen u uređaj. Naziv mu je Web Config. Tamo možete provjeriti i promijeniti status uređaja.

Alat

Opći uvjet softvera za postavljanje i upravljanje uređajem, kao što je Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, itd.

Ubrzano skeniranje

Opći uvjet skeniranja s upravljačke ploče uređaja.

ASCII (američki standardni kod za razmjenu informacija)

Jedan od standardnih kodova znaka. 128 znakova definirano je uključujući znakove poput abecede (a–z, A–Z), arapskih brojki (0–9), simbola, praznih znakova i kontrolnih znakova. Kada je „ASCII” opisan u ovom vodiču, pokazuje 0x20–0x7E (heksadecimalni broj) naveden u nastavku i ne sadrži 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 praznog mjesta.

Unicode (UTF-8)

Međunarodni standardizirani kod koji pokriva glavne globalne jezike. Kada je „UTF-8” opisan u ovom vodiču, pokazuje kodne znakove u formatu UTF-8.

Priprema

Ovo poglavlje objašnjava ulogu administratora i pripremu prije odabira postavki.

Tijek postavki i upravljanja skenerom

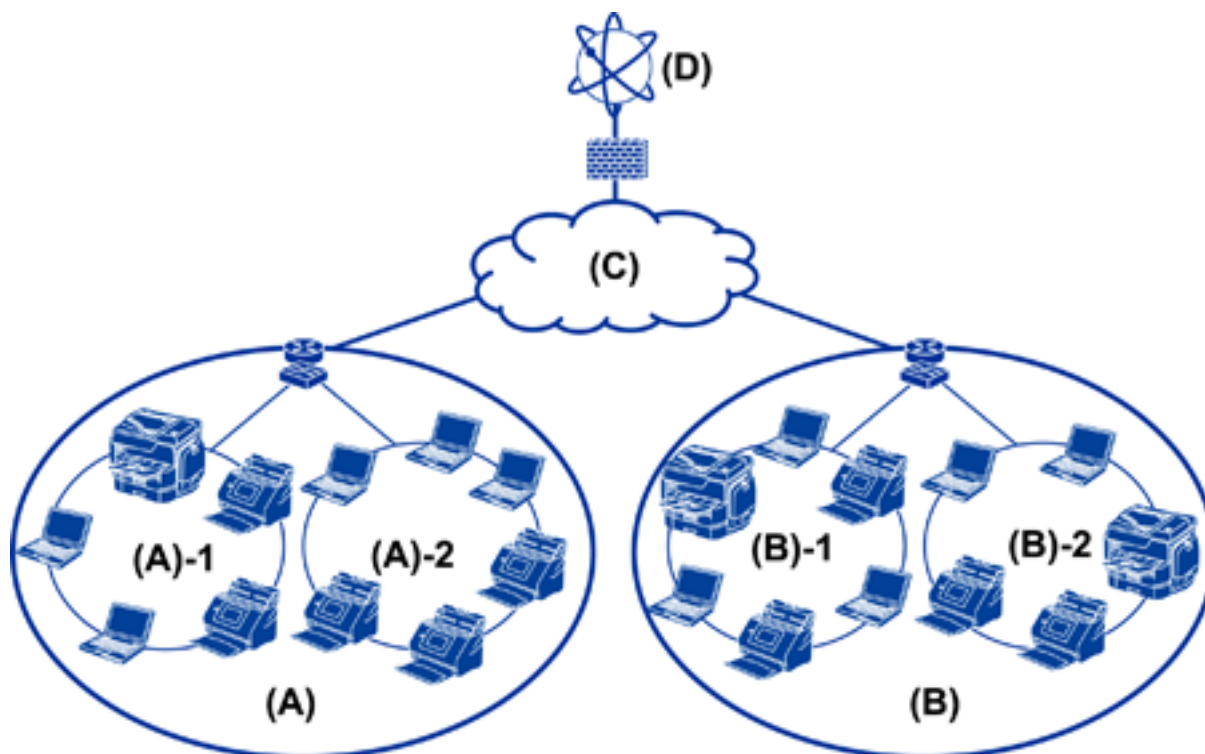
Administrator izvršava postavke mrežne veze, početnu konfiguraciju i održavanje skenera kako bi bile dostupne korisnicima.

1. Priprema
 - Prikupljanje informacija o postavci veze
 - Odluka o načinu povezivanja
2. Povezivanje
 - Mrežna veza s upravljačke ploče skenera
3. Postavljanje funkcija
 - Postavke upravljačkog programa skenera
 - Druge napredne postavke
4. Sigurnosne postavke
 - Administratorske postavke
 - SSL/TLS
 - Provjera protokola
 - Napredne sigurnosne postavke (opcija)
5. Rad i upravljanje
 - Provjera statusa uređaja
 - Reagiranje u hitnim slučajevima
 - Sigurnosna kopija postavki uređaja

Povezane informacije

- ➔ [“Priprema” na strani 10](#)
- ➔ [“Povezivanje” na strani 15](#)
- ➔ [“Postavke funkcije” na strani 22](#)
- ➔ [“Osnovne postavke sigurnosti” na strani 32](#)
- ➔ [“Postavke načina rada i upravljanja” na strani 40](#)

Primjer mrežnog okruženja



(A): ured 1

(A) – 1: LAN 1

(A) – 2: LAN 2

(B): ured 2

(B) – 1: LAN 1

(B) – 2: LAN 2

(C): WAN

(D): Internet

Primjer postavke za uvođenje veze skenera

Postoje dva osnovna tipa veze, ovisno o načinu uporabe skenera. Oba povezuju skener na mrežu s računalom preko koncentratora.

- Povezivanje poslužitelja/klijentskog računala (skenera koji koristi Windows poslužitelj, upravljanje zadacima)
- Veza P2P (izravno povezivanje preko klijentskog računala)

Povezane informacije

- ➔ [“Povezivanje Povezivanje poslužitelja/klijentskog računala” na strani 12](#)
- ➔ [“Veza tipa P2P” na strani 12](#)

Povezivanje Povezivanje poslužitelja/klijentskog računala

Upravljajte skenerom i zadacima s jednog mjesta koristeći Document Capture Pro Server instaliran na vašem poslužitelju. To je najprikladnije za zadatke u kojima se koristi više skenera za skeniranje velikog broja dokumenata određenog formata.

Povezane informacije

➔ [“Objašnjenja izraza korištenih u ovom vodiču” na strani 8](#)

Veza tipa P2P

Koristite jedan skener s upravljačkim programom skenera, kao što je Epson Scan 2, koji je instaliran na klijentsko računalo. Instaliranje programa Document Capture Pro (Document Capture) na klijentsko računalo omogućava pokretanje zadataka na pojedinačnim klijentskim računalima skenera.

Povezane informacije

➔ [“Objašnjenja izraza korištenih u ovom vodiču” na strani 8](#)

Pripremanje povezivanja s mrežom

Prikupljanje informacija o postavci veze

Trebate imati IP adresu, adresu pristupnika, itd. za mrežnu vezu. Unaprijed provjerite sljedeće.

Odjeljenja	Stavke	Napomena
Način spajanja uređaja	<input type="checkbox"/> Ethernet	Koristite STP (oklopljena uvijena parica) kategorije 5e ili više kao kabel za Ethernet vezu.
Informacije o LAN vezi	<input type="checkbox"/> IP adresa <input type="checkbox"/> Maska pod mreže <input type="checkbox"/> Zadani pristupnik	Neće biti potrebno ako automatski odredite IP adresu koristeći funkciju DHCP usmjernika.
Informacije o DNS poslužitelju	<input type="checkbox"/> IP adresa primarnog DNS-a <input type="checkbox"/> IP adresa sekundarnog DNS-a	Ako koristite statičku IP adresu kao IP adresu, konfigurirajte DNS poslužitelj. Konfigurirajte kod automatske dodjele koristeći funkciju DHCP i kada se DNS poslužitelj ne može dodijeliti automatski.
Informacije o proxy poslužitelju	<input type="checkbox"/> Naziv proxy poslužitelja <input type="checkbox"/> Broj ulaza	Konfigurirajte kod korištenja proxy poslužitelja za internetsku vezu i kod primjene usluge Epson Connect ili funkcije automatskog ažuriranja firmvera.

Specifikacije skenera

Specifikaciju koju skener podržava za standardni način rada ili povezivanje potražite u dokumentu *Korisnički vodič*.

Korištenje broja ulaza

Pogledajte „Dodatak” kako biste saznali broj ulaza kojim se koristi skener.

Povezane informacije

➔ [“Korištenje ulaza skenera” na strani 60](#)

Način dodjele IP adrese

Postoje dva načina dodjele IP adrese skeneru.

Statička IP adresa:

Dodijelite prethodno zadanu jedinstvenu IP adresu skeneru.

IP adresa nije promijenjena čak ni nakon isključivanja skenera ili usmjernika, pa možete upravljati IP adresom uređaja.

Ovaj način je prikladan za mrežu u kojoj se upravlja brojnim skenerima, poput velikih ureda ili škola.

Automatska dodjela preko funkcije DHCP:

Ispravna IP adresa automatski se dodjeljuje kada uspije komunikacija između skenera i usmjernika koja podržava funkciju DHCP.

Ako nije praktično promijeniti IP adresu određenog uređaja, rezervirajte IP adresu i zatim je dodijelite.

DNS poslužitelj i proxy poslužitelj

Ako koristite uslugu internetske veze, konfigurirajte DNS poslužitelj. Ako ga ne konfigurirate, trebate navesti IP adresu za pristup jer možda nećete otkriti naziv.

Proxy poslužitelj nalazi se na pristupniku između mreže i interneta te komunicira s računalom, skenerom i internetom (suprotan poslužitelj) u ime svakog od njih. Suprotan poslužitelj komunicira samo s poslužiteljem. Stoga se informacije o skeneru, kao što su IP adresa i broj ulaza, ne mogu pročitati te se očekuje veća sigurnost.

Možete zabraniti pristup određenoj URL adresi korištenjem funkcije filtriranja, jer proxy poslužitelj može provjeriti sadržaj komunikacije.

Način postavljanja mrežne veze

Za postavke veze IP adrese skenera, masku podmreže i zadani pristupnik učinite korake navedene u nastavku.

Korištenje upravljačke ploče:

Konfigurirajte postavke koristeći upravljačku ploču skenera za svaki skener. Spojite na mrežu nakon konfiguriranja postavki povezivanja skenera.

Korištenje instalacijskog programa:

Ako se koristi instalacijski program, automatski se postavljaju mreža skenera i klijentsko računalo. Postavka je dostupna prema sljedećim uputama instalacijskog programa, čak i ako nemate temeljito znanje o mreži.

Priprema

Korištenje alata:

Koristite alat iz računala administratora. Možete otkriti skener i zatim ga postaviti, ili kreirate SYLK datoteku kako biste odabrali skupne postavke za skener. Možete zadati mnogo skenera, no treba ih povezati fizički Ethernet kabelom prije odabira postavki. Stoga se preporučuje da instalirate Ethernet za postavku.

Povezane informacije

- ➔ [“Povezivanje mreže na upravljačkoj ploči” na strani 15](#)
- ➔ [“Povezivanje na mrežu preko instalacijskog programa” na strani 19](#)
- ➔ [“Dodjeljivanje IP adrese koristeći EpsonNet Config” na strani 56](#)

Povezivanje

Ovo poglavlje objašnjava okruženje ili postupak povezivanja skenera na mrežu.

Povezivanje s mrežom

Povezivanje mreže na upravljačkoj ploči

Povežite se na skener preko upravljačke ploče skenera.

Više o upravljačkoj ploči skenera pronađite u dokumentu *Korisnički vodič*.

Dodjela IP adrese

Postavite osnovne stavke poput IP adresa, Maska podmreže i Zadani pristupnik.

1. Uključite skener.
2. Okrenite zaslon ulijevo na upravljačkoj ploči skenera i dodirnite **Postavke**.

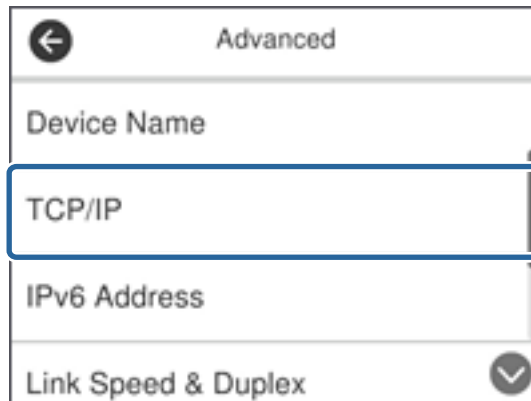


3. Dodirnite **Postavke mreže > Promijeni postavke**.

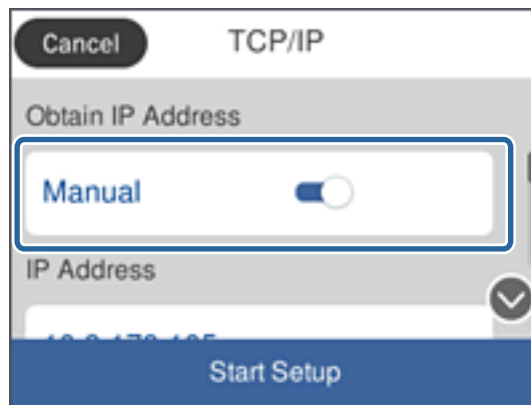
Ako stavka nije prikazana, pomaknite zaslon prema gore kako bi se pokazao.

Povezivanje

4. Dodirnite **TCP/IP**.



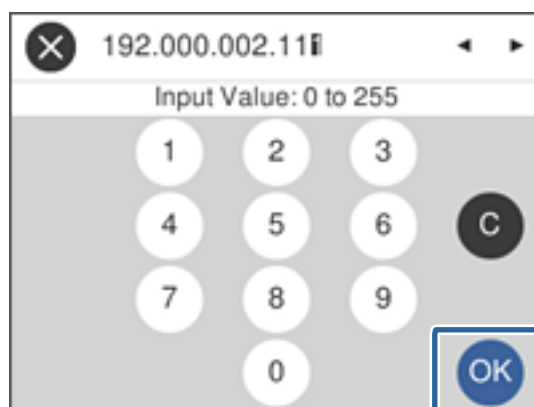
5. Odaberite **Ručno** za Dohvati IP adresu.



Napomena:

Ako postavite automatski IP adresu korištenjem funkcije DHCP usmjernika, odaberite **Automatski**. U tom slučaju se **IP adresa**, **Maska pod mreže**, i **Zadani pristupnik** u koraku 6 do 7 također automatski postavljaju, pa prijedite na korak 8.

6. Dodirnite polje **IP adresa**, unesite IP adresu preko zaslonske tipkovnice i zatim dodirnite **U redu**.



Potvrdite vrijednost prikazanu na prethodnom zaslonu.

Povezivanje

7. Podesite stavke **Maska pod mreže** i **Zadani pristupnik**.

Potvrdite vrijednost prikazanu na prethodnom zaslonu.

Napomena:

Ako kombinacija IP adresa, Maska pod mreže i Zadani pristupnik nije ispravna, **Početak postave** je neaktivan i ne može nastaviti s postavkama. Provjerite da nema greške u unosu.

8. Dodirnite polje **Primarni DNS za DNS poslužitelj**, unesite IP adresu za primarni DNS poslužitelj koristeći zaslonu tipkovnicu i zatim dodirnite **U redu**.

Potvrdite vrijednost prikazanu na prethodnom zaslonu.

Napomena:

Kada odaberete **Automatski** za postavke dodjele IP adrese, možete odabrati postavke DNS poslužitelja preko **Ručno** ili **Automatski**. Ako ne možete automatski pribaviti adresu DNS poslužitelja, odaberite **Ručno** i unesite adresu DNS poslužitelja. Zatim unesite izravno adresu sekundarnog DNS poslužitelja. Ako odaberete **Automatski**, idite na korak 10.

9. Dodirnite polje **Sekundarni DNS**, unesite IP adresu za primarni DNS poslužitelj koristeći zaslonu tipkovnicu i zatim dodirnite **U redu**.

Potvrdite vrijednost prikazanu na prethodnom zaslonu.

10. Dodirnite **Početak postave**.


11. Dodirnite **Zatvori** na zaslonu potvrde.

Zaslon se automatski zatvara ako određeno vrijeme ne dodirnete **Zatvori**.

Spajanje na Ethernet

Spojite skener na mrežu koristeći Ethernet kabel i provjerite vezu.

1. Spojite skener i koncentrador (sklopka L2) Ethernet kabelom.

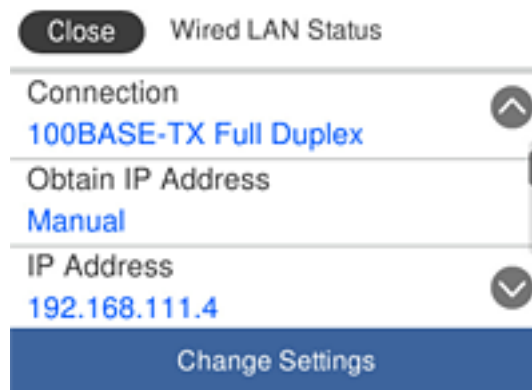
Ikona na početnom zaslonu prelazi u .

2. Dodirnite  na početnom zaslonu.



Povezivanje

3. Okrenite zaslon prema gore i uvjerite se da su ispravni status veze i IP adresa.



Postavljanje proxy poslužitelja

Proxy poslužitelj ne može biti odabran na ploči. Konfigurirajte koristeći Web Config.

1. Pristupite programu Web Config i odaberite **Network Settings > Basic**.
2. Odaberite **Use** pod **Proxy Server Setting**.
3. Odaberite proxy poslužitelj na IPv4 adresi ili FQDN format u dijelu **Proxy poslužitelj**, a zatim unesite broj ulaza u dijelu **Proxy Server Port Number**.

Kod proxy poslužitelja koji zahtijevaju provjeru autentičnosti, unesite korisničko ime proxy poslužitelja i lozinku za provjeru autentičnosti proxy poslužitelja.

Povezivanje

4. Kliknite na gumb **Next**.

The screenshot shows the EPSON Web Config interface for an ES-7000 printer. The left sidebar contains navigation options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Wired LAN', 'Basic', 'Email Server', 'Network Security Settings', 'Services', 'System Settings', 'Export and Import Setting Value', and 'Administrator Settings'. Under 'Basic Settings', 'DNS/Proxy Setup' is selected. The main content area displays various network configuration fields:

- Primary DNS Server : [text box]
- Secondary DNS Server : [text box]
- DNS Host Name Setting : Auto Manual
- DNS Host Name Status : Failed
- DNS Host Name : EPSON884045
- DNS Domain Name Setting : Auto Manual
- DNS Domain Name Status : Failed
- DNS Domain Name : [text box]
- Register the network interface address to DNS : Enable Disable
- Proxy Server Setting** : Do Not Use Use
- Proxy Server : www.sample.proxy
- Proxy Server Port Number : 80
- Proxy Server User Name : XXXXXXXX
- Proxy Server Password : [password field]
- IPv6 Setting : Enable Disable
- IPv6 Privacy Extension : Enable Disable
- IPv6 DHCP Server Setting : Do Not Use Use
- IPv6 Address : [text box]
- IPv6 Address Default Gateway : [text box]
- IPv6 Link-Local Address : fe80::9eae:d3ff:fe88:4045/64
- IPv6 Stateful Address : [text box]
- IPv6 Stateless Address 1 : [text box]
- IPv6 Stateless Address 2 : [text box]
- IPv6 Stateless Address 3 : [text box]
- IPv6 Primary DNS Server : [text box]
- IPv6 Secondary DNS Server : [text box]

A 'Next' button is located at the bottom of the configuration area.

5. Potvrdite postavke i zatim kliknite **Postavke**.

Povezane informacije

- ➔ “Pristup aplikaciji Web Config” na strani 23

Povezivanje na mrežu preko instalacijskog programa

Preporučujemo korištenje instalacijskog programa za povezivanje skenera s računalom. Možete pokrenuti instalacijski program koristeći jedan od sljedećih načina.

- Postavljanje preko web-stranice

Pristupite sljedećoj web-stranici i unesite naziv proizvoda. Idite na **Postavljanje** i zatim počnite s odabirom postavki.

<http://epson.sn>

- Postavljanje s diska softvera (samo za modele koji su isporučeni s diskom softvera i korisnicima računala s pogonima diska.)

Umetnite disk softvera u računalo i zatim slijedite upute prikazane na zaslonu.

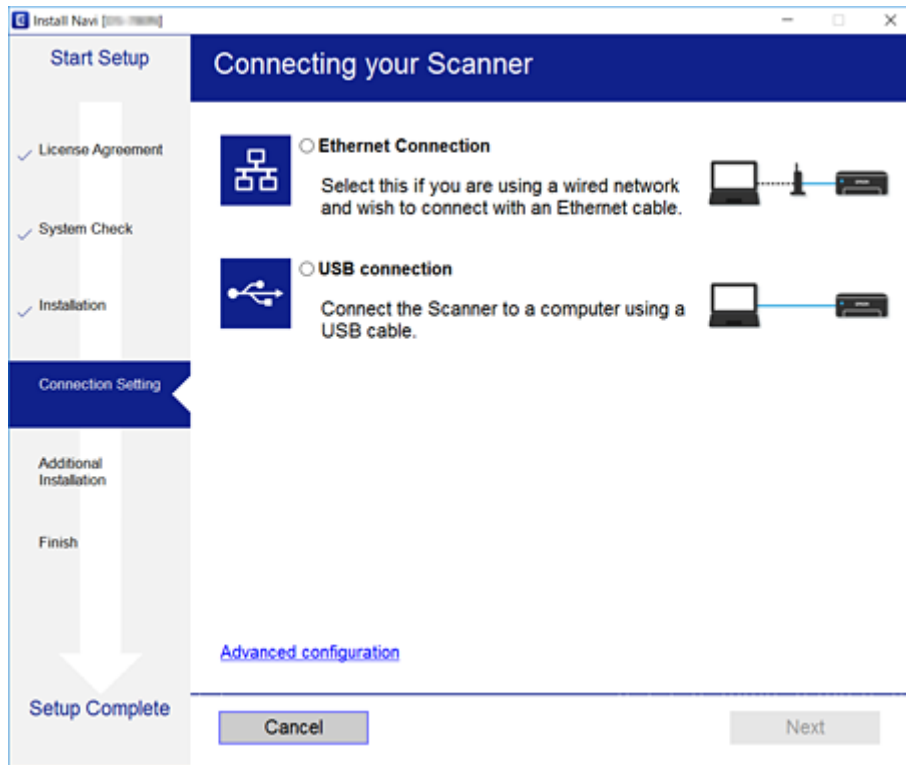
Povezivanje

Odabir načina povezivanja

Slijedite prikazane upute dok se ne prikaže sljedeći zaslon i zatim odaberite način povezivanja skenera s računalom.

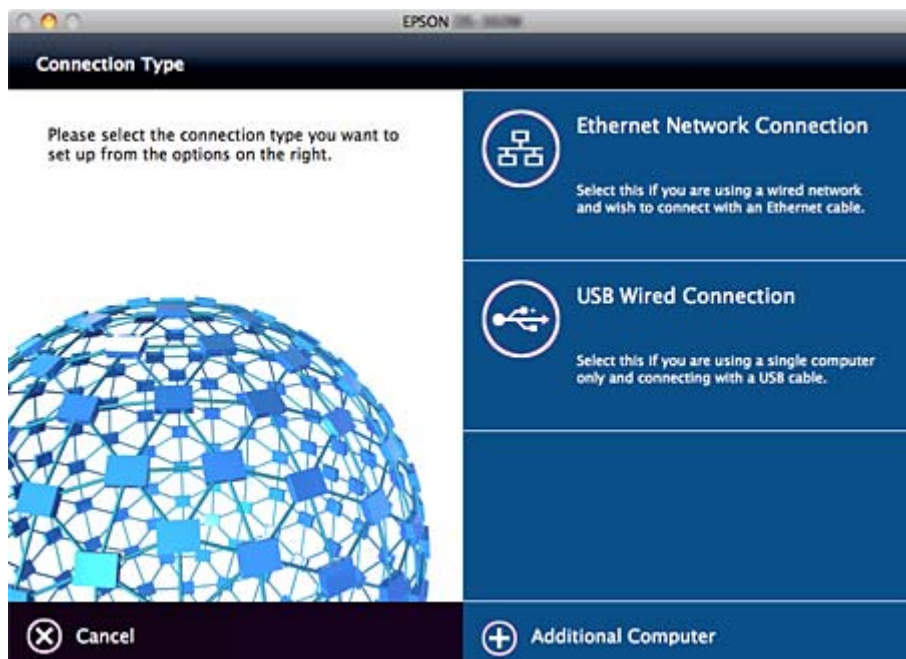
Windows

Odaberite način povezivanja, a zatim pritisnite **Dalje**.



Mac OS

Odaberite način povezivanja.



Povezivanje

Slijedite upute na zaslonu. Instaliran je potreban softver.

Postavke funkcije

Ovo poglavlje objašnjava prve potrebne postavke za korištenje svake funkcije uređaja.

Softver za postavljanje

U ovoj temi objašnjen je postupak odabira postavki s računala administrator koji koristi Web Config.

Web Config (web-stranica uređaja)

O aplikaciji Web Config

Web Config je web aplikacija za konfiguriranje postavki skenera.

Za pristup aplikaciji Web Config, najprije skeneru trebate dodijeliti IP adresu.

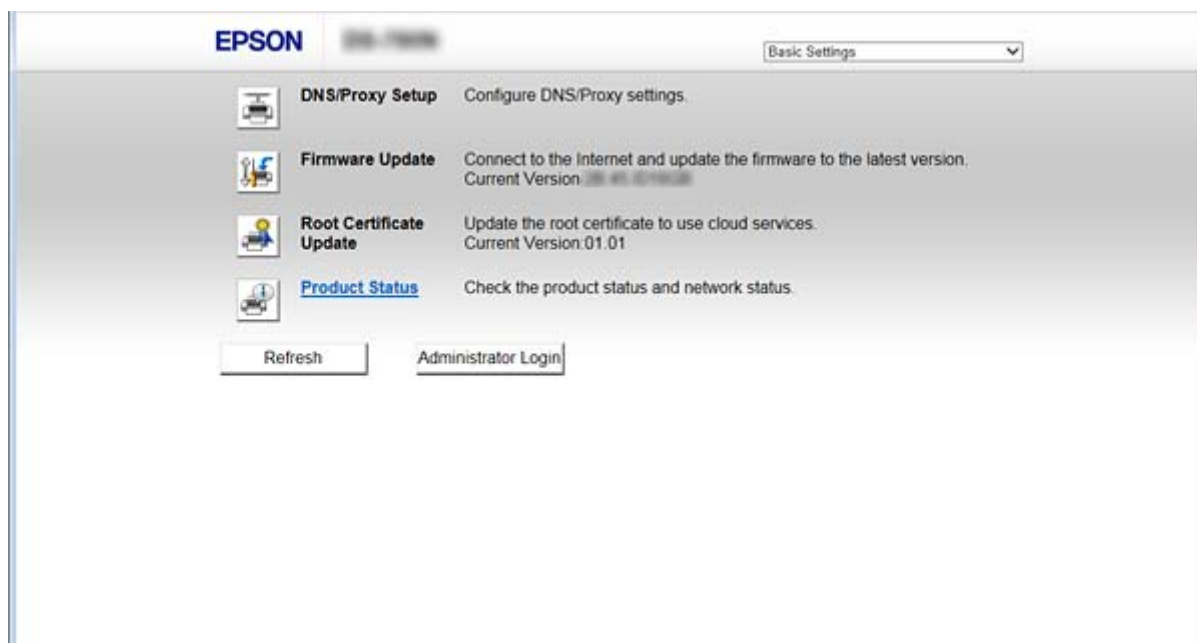
Napomena:

Postavke možete zaključati konfiguriranjem lozinke administratora za skener.

Postoje dvije stranice za postavke, kako je navedeno ispod.

Basic Settings

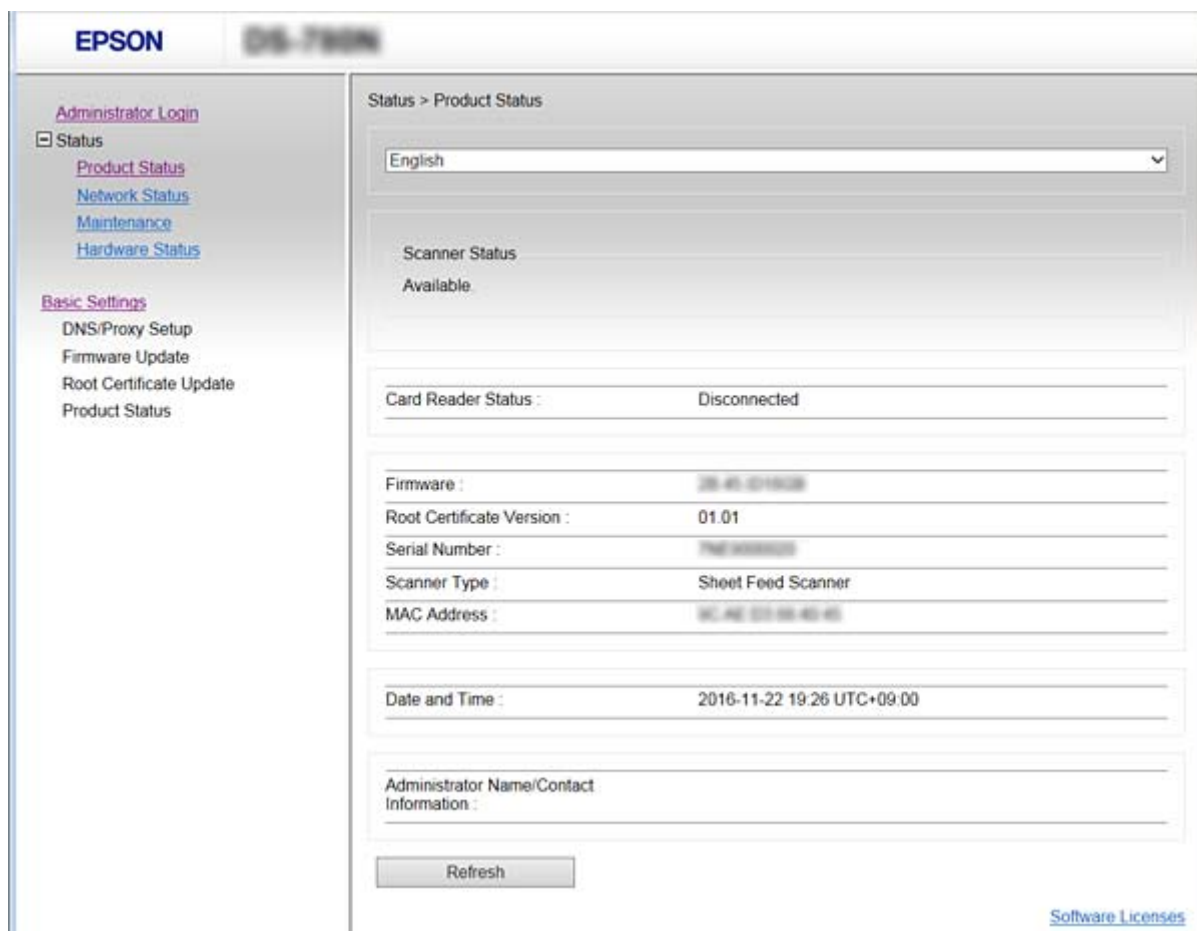
Ovdje možete konfigurirati osnovne postavke skenera.



Postavke funkcije

Advanced Settings

Ovdje možete konfigurirati napredne postavke skenera. Ova stranica je uglavnom namijenjena administratoru.



Pristup aplikaciji Web Config

Unesite IP adresu skenera u internetski preglednik. JavaScript mora biti omogućen. Prilikom pristupanja programu Web Config pomoću HTTPS-a, u pregledniku će se pojaviti poruka upozorenja zbog korištenja samopotpisanog certifikata pohranjenog u skeneru.

Pristup preko HTTPS-a

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

IPv6: [https://\[IP adresa skenera\]/](https://[IP adresa skenera]/) (s [])

Pristup preko HTTP-a

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

IPv6: [http://\[IP adresa skenera\]/](http://[IP adresa skenera]/) (s [])

Postavke funkcije

Napomena:

Primjeri

IPv4:

<https://192.0.2.111/>

<http://192.0.2.111/>

IPv6:

[https://\[2001:db8::1000:1\]/](https://[2001:db8::1000:1]/)

[http://\[2001:db8::1000:1\]/](http://[2001:db8::1000:1]/)

- Ako je naziv skenera registriran na DNS poslužitelju, možete koristiti naziv skenera umjesto njegove IP adrese.

Povezane informacije

- ➔ [“SSL/TLS komunikacija sa skenerom” na strani 63](#)
- ➔ [“O digitalnom certificiranju” na strani 63](#)

Korištenje funkcijama skena

Ovisno o načinu korištenja skenera, instalirajte sljedeći softver i preko njega odaberite postavke.

Skeniranje preko računala

- Provjerite valjanost usluge mrežnog skeniranja s programom Web Config (valjano pri tvorničkoj isporuci).
- Instalirajte Epson Scan 2 na vaše računalo i odredite IP adresu
- Kod skeniranja koristeći zadatke, instalirajte Document Capture Pro (Document Capture) i odaberite postavke zadatke.

Skenirajte s radne ploče

- Pri korištenju programa Document Capture Pro ili Document Capture Pro Server:
Instalirajte Document Capture Pro ili Document Capture Pro Server
Postavka DCP (modus poslužitelja, modus klijentskog računala).
- Pri korištenju protokola WSD:
Potvrdite valjanost WSD-a u programu Web Config ili na radnoj ploči (valjano pri tvorničkoj isporuci)
Dodatne postavke uređaja (računala sa sustavom Windows).

Skeniranje putem računala

Instalirajte softver i provjerite je li aktivirano mrežno skeniranje kako biste skenirali putem mreže s računala.

Povezane informacije

- ➔ [“Softver koji treba instalirati” na strani 25](#)
- ➔ [“Aktiviranje mrežnog skeniranja” na strani 25](#)

Postavke funkcije

Softver koji treba instalirati

Epson Scan 2

To je upravljački program skenera. Ako uređaj koristite preko računala, instalirajte upravljački program na svako klijentsko računalo. Ako se instalira Document Capture Pro/Document Capture, možete izvršiti radnje dodijeljene gumbima uređaja.

Preko usluge EpsonNet SetupManager upravljački programi pisača također se mogu distribuirati u paketu.

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

Instalirajte na klijentsko računalo. Možete zatražiti i izvršavati zadatke registrirane na računalu koristeći program Document Capture Pro/Document Capture instaliran na mreži preko računala i radne ploče skenera.

Također možete skenirati s računala putem mreže. Za skeniranje je potreban Epson Scan 2.

Povezane informacije

➔ [“EpsonNet SetupManager” na strani 56](#)

Postavite IP adresu skenera u programu Epson Scan 2

Navedite IP adresu skenera tako da se skener koristi na mreži.

1. Pokrenite **Epson Scan 2 Utility** u dijelu **Start > Svi programi > EPSON > Epson Scan 2**.

Ako je već registriran drugi skener, prijedite na korak 2.

Ako nije registriran, prijedite na korak 4.



2. Kliknite ▼ pod **Skener**.

3. Kliknite na **Postavke**.

4. Kliknite **Omogući uređivanje**, a zatim kliknite **Dodaj**.

5. Odaberite naziv modela skenera pod **Model**.

6. Odaberite IP adresu skenera koji će se koristiti na **Adresa** u dijelu **Traži mrežu**.

Kliknite  i zatim kliknite  kako biste ažurirali popis. Ako ne možete IP adresu skenera, odaberite **Unesite adresu** i zatim odaberite IP adresu.

7. Kliknite na **Dodaj**.

8. Kliknite na **U redu**.

Aktiviranje mrežnog skeniranja

Možete postaviti uslugu mrežnog skeniranja kada skenirate s računala klijenta preko mreže. Omogućena je zadana postavka.

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

Postavke funkcije

2. Uvjerite se da je odabrano **Enable scanning** pod **EPSON Scan**.
Ako je odabrana ta stavka, ovaj zadatak je završen. Zatvorite Web Config.
Ako je uklonjeno, odaberite i prijedite na sljedeći korak.
3. Kliknite na **Next**.
4. Kliknite na **OK**.
Mreža se ponovno povezuje i zatim se aktiviraju postavke.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Skeniranje preko upravljačke ploče

Funkcije skeniranja u mapu i skeniranja na e-poštu koristeći upravljačku ploču skenera, kao i prijenos rezultata skeniranja na e-poštu, u mape, itd. izvršavaju se putem zadatka s računala.

Kod prijenosa rezultata skenera, odaberite zadatak koristeći Document Capture Pro Server ili Document Capture Pro.

Pojedinosti o postavkama i konfiguriranju zadatka potražite u dokumentaciji ili pomoći u programu Document Capture Pro Server ili Document Capture Pro.

Povezane informacije

- ➔ [“Postavke programa Document Capture Pro Server/Document Capture Pro” na strani 26](#)
- ➔ [“Postavke poslužitelja i mapa” na strani 27](#)

Softver za instaliranje na računalu

Document Capture Pro Server

Ovo je verzija poslužitelja programa Document Capture Pro. Instalirajte na Windows poslužitelj. Poslužitelj može s jednog mjesta nadzirati više uređaja i zadataka. Zadaci se mogu izvršavati istovremeno preko više skenera.

Korištenjem certificirane verzije programa Document Capture Pro Server, možete upravljati zadacima i skenirati povijest povezanu s korisnicima i skupinama.

Više pojedinosti o programu Document Capture Pro Server saznajte od lokalnog predstavnika tvrtke Epson.

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

Kao i kod skeniranja preko računala, preko upravljačke ploče možete zatražiti zadatke registrirane na računalu te ih izvršiti. Zadaci računala ne mogu se pokrenuti istovremeno preko više skenera.

Postavke programa Document Capture Pro Server/Document Capture Pro

Odaberite postavke korištenja funkcije skeniranja preko radne ploče skenera.

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

Postavke funkcije

2. Odaberite **Način rada**.

Server Mode:

Odaberite kada koristite program Document Capture Pro Server ili Document Capture Pro samo za zadatke koji su postavljeni za određeno računalo.

Client Mode:

Odaberite kada odabirete postavku zadatka programa Document Capture Pro (Document Capture) instaliranog na svakom klijentskom računalu unutar mreže bez navođenja računala.

3. Odaberite sljedeće u skladu s odabranim načinom rada.

Server Mode:

Pod **Server Address** navedite poslužitelj na kojem je instaliran Document Capture Pro Server. Može sadržavati između 2 i 252 znakova u formatu IPv4, IPv6, naziv domaćina ili FQDN. U formatu FQDN mogu se koristiti znakovi sustava US-ASCII, brojke, slova i crtice (osim prednjih i stražnjih crtica).

Client Mode:

Odaberite **Group Settings** za korištenje skupine skenera koja se navodi u programu Document Capture Pro (Document Capture).

4. Kliknite na **Postavke**.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Postavke poslužitelja i mapa

Document Capture Pro i Document Capture Pro Server jednom spremaju skenirane podatke na poslužitelj ili klijentsko računalo te koriste funkciju prijenosa kako bi izvršili funkcije skeniranja u mapu i skeniranja na e-poštu.

Potrebni su vam ovlaštenje i informacije za prijenos s računala na kojem je instaliran program Document Capture Pro, Document Capture Pro Server na drugo računalo ili uslugu oblaka.

Pripremite informacije o funkciji koju ćete koristiti, uzimajući u obzir sljedeće.

Možete odabrati postavke ovih funkcija koristeći program Document Capture Pro ili Document Capture Pro Server. Pojediniosti o postavkama potražite u dokumentaciji ili pomoći u programu Document Capture Pro Server ili Document Capture Pro.

Naziv	Postavke	Zahtjev
Skeniraj u mrežnu mapu (SMB)	Kreiraj i postavi dijeljenje mape za spremanje	Administrativni korisnički račun za računalo koje kreira mape za spremanje.
	Odredište skeniranja u mrežnu mapu (SMB)	Korisničko ime i lozinka prijave na računalo s mapom za spremanje i privilegijom ažuriranja mape za spremanje.
Skeniraj u mrežnu mapu (FTP)	Postavljanje prijave FTP poslužitelja	Informacije za prijavu FTP poslužitelja i privilegija ažuriranja mape za spremanje.
Skeniraj u e-poštu	Postavljanje poslužitelja e-pošte	Informacije o postavljanju poslužitelja e-pošte

Postavke funkcije

Naziv	Postavke	Zahtjev
Skeniraj u dokument Capture Pro (kada se koristi Document Capture Pro Server)	Postavke prijave na usluge oblaka	Okruženje internetskog povezivanja Registracija računa za usluge oblaka

Koristite WSD sken (samo Windows)

Ako računalo koristi sustav Windows Vista ili noviju verziju, možete koristiti WSD sken.

Ako se može koristiti protokol WSD, izbornik **Računalo(WSD)** bit će prikazan na upravljačkoj ploči skenera.



1. Pristupite programu Web Config i odaberite **Services > Protocol**.
2. Potvrdite je li **Enable WSD** označen u dijelu **WSD Settings**.
Ako je označeno, vaš zadatak je završen i možete zatvoriti program Web Config.
Ako nije odabrano, označite i nastavite na sljedeći korak.
3. Kliknite na gumb **Next**.
4. Potvrdite postavke i kliknite **Postavke**.

Odabir postavki sustava

Odabir postavki sustava preko upravljačke ploče

Postavljanje svjetline zaslona

Postavite svjetlinu LCD zaslona.

1. Dodirnite **Postavke** na početnom zaslonu.
2. Dodirnite **Zajedničke postavke > Svjetlina LCD-a**.
3. Dodirnite  ili  kako biste prilagodili svjetlinu.
Možete prilagoditi razinu od 1 do 9.
4. Dodirnite **U redu**.

Postavljanje zvuka

Odaberite radni zvuk ploče i greške.

1. Dodirnite **Postavke** na početnom zaslonu.
2. Dodirnite **Zajedničke postavke > Zvuk**.

Postavke funkcije

3. Ako je to potrebno, odaberite sljedeće stavke.
 - Radni zvuk
Odaberite glasnoću radnog zvuka radne ploče.
 - Zvuk greške
Odaberite glasnoću zvuka greške.
4. Dodirnite **U redu**.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Otkrivanje dvostrukog umetanja izvornika

Odredite funkciju za otkrivanje dvostrukog umetanja dokumenta koji treba skenirati i zaustavljanja skeniranja u slučaju umetanja više listova.

Isključite te funkcije kada skenirate izvornike kod kojih bi se moglo registrirati višestruko umetanje, primjerice omotnice ili papir s naljepnicama.

Napomena:

Možete postaviti i preko programa Web Config ili Epson Scan 2.

1. Dodirnite **Postavke** na početnom zaslonu.
2. Dodirnite **Vanjske Postavke skeniranja > Ultrazvu. otkriv. dvostrukog uvlače.**
3. Dodirnite **Ultrazvu. otkriv. dvostrukog uvlače.** kako biste uključili ili isključili.
4. Dodirnite **Zatvori**.

Postavljanje sporog načina rada

Odaberite sporo skeniranje kako ne bi došlo do zaglavljivanja papira pri skeniranju tankih dokumenata, primjerice listića računa.

1. Dodirnite **Postavke** na početnom zaslonu.
2. Dodirnite **Vanjske Postavke skeniranja > Sporo.**
3. Dodirnite **Sporo** kako biste uključili ili isključili.
4. Dodirnite **Zatvori**.

Odabir postavki sustava koristeći Web Config

Postavke štednje energije tijekom neaktivnosti

Izvršite postavku štednje energije tijekom razdoblja neaktivnosti skenera. Odredite vrijeme ovisno o okruženju vašeg korištenja.

Napomena:

Možete odabrati postavke za uštedu energije na upravljačkoj ploči skenera.

1. Pristupite programu Web Config i odaberite **System Settings > Power Saving**.
2. Unesite vrijeme za **Sleep Timer** kako biste prebacili na način rada za uštedu energije u slučaju neaktivnosti. Možete odabrati do 240 minuta u minut.
3. Odaberite vrijeme isključivanja za **Power Off Timer**.
4. Kliknite na **OK**.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Postavljanje upravljačke ploče

Postavljanje upravljačke ploče skenera. Možete postaviti na sljedeći način.

1. Pristupite programu Web Config i odaberite **System Settings > Control Panel**.
2. Ako je to potrebno, postavite sljedeće stavke.
 - Language
Odaberite jezik prikaza na upravljačkoj ploči.
 - Panel Lock
Ako odaberete **ON**, administratorska lozinka zahtijeva se kada obavljate neku radnju za koju se traži ovlaštenje administratora. Ako se ne postavi lozinka administratora, bit će onemogućena blokada ploče.
 - Operation Timeout
Ako odaberete **ON** kada se prijavite kao administrator, automatski ćete biti odjavljeni i stoga prijeđite na početni zaslon ako neko vrijeme nema nikakvih aktivnosti.
Možete odabrati od 10 sekundi do 240 minuta, precizno u sekundu.
3. Kliknite na **OK**.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Postavke funkcije

Postavljanje ograničenja vanjskog sučelja

Možete ograničiti USB vezu preko računala. Postavite ograničeno skeniranje koje se ne obavlja preko mreže.

1. Pristupite programu Web Config i odaberite **System Settings > External Interface**.
2. Odaberite **Enable** ili **Disable**.
Za ograničavanje odaberite **Disable**.
3. Dodirnite **OK**.

Sinkroniziranje datuma i vremena s poslužiteljem vremena

Ako koristite CA certifikat, možete spriječiti problem s vremenom.

1. Pristupite programu Web Config i odaberite **System Settings > Date and Time > Time Server**.
2. Odaberite **Use** za **Use Time Server**.
3. Unesite adresu poslužitelja vremena za **Time Server Address**.
Možete koristiti IPv4, IPv6 ili FQDN format. Unesite najviše 252 znaka. Ako to ne navedete, ostavite prazno.
4. Unesite **Update Interval (min)**.
Možete odabrati do 10.800 minuta u minut.
5. Kliknite na **OK**.

Napomena:

*Možete potvrditi status veze preko poslužitelja vremena na **Time Server Status**.*

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Osnovne postavke sigurnosti

Ovo poglavlje objašnjava osnovne postavke sigurnosti koje ne zahtijevaju posebno okruženje.

Uvod u osnovne sigurnosne značajke

Predstavljamo osnovne sigurnosne značajke uređaja Epson.

Naziv značajke	Vrsta značajke	Što podesiti	Što spriječiti
Postavke lozinke administratora	Blokirajte postavke povezane sa sustavom, kao što su postavke mreže i USB veze, tako da ih može promijeniti samo administrator.	Administrator određuje lozinku uređaja. Konfiguracija ili ažuriranje dostupni su na svakom mjestu preko usluge Web Config, upravljačke ploče, Epson Device Admin i EpsonNet Config.	Spriječite neovlašteno čitanje i promjenu informacija pohranjenih na uređaju, kao što je ID, lozinka, mrežne postavke i kontakti. Također smanjuje široki spektar rizika, uključujući curenje informacija mrežnog okruženja ili sigurnosnih pravila.
SSL/TLS komunikacija	Kod pristupanja Epson poslužitelju ili Internetu preko uređaja, primjerice kod komunikacije s računalom putem preglednika ili ažuriranja firmvera, sadržaji komunikacije kriptirani su preko SSL/TLS komunikacije.	Pribavite CA-potpisani certifikat te ga uvezite na skener.	Uklanjanje identifikacije uređaja preko CA-potpisanog certifikata sprječava krađu identiteta i neovlašteni pristup. Također je zaštićen sadržaj komunikacije za SSL/TLS te sprječava curenje sadržaja za ispis podataka i informacija o postavkama.
Nadzire protokole	Nadzire protokole korištene za komunikaciju između uređaja i računala te aktivira ili deaktivira funkcije.	Protokol ili usluga koja se primjenjuje na sve značajke koje su zasebno odobrene ili zabranjene.	Smanjuje rizike koji se mogu pojaviti zbog neplanirane uporabe, sprječavajući korisnike da koriste nepotrebne funkcije.

Povezane informacije

- ➔ ["O aplikaciji Web Config" na strani 22](#)
- ➔ ["EpsonNet konfiguracija" na strani 55](#)
- ➔ ["Epson Device Admin" na strani 55](#)
- ➔ ["Konfiguriranje lozinke administratora" na strani 32](#)
- ➔ ["Upravljanje protokolima" na strani 35](#)

Konfiguriranje lozinke administratora

Kada postavite lozinku administratora, korisnici koji nisu administratori neće moći promijeniti postavke upravljanja sustavom. Možete postaviti i promijeniti lozinku administratora koristeći Web Config, upravljačku ploču skenera ili softver (Epson Device Admin ili EpsonNet Config). Pri korištenju softvera pogledajte dokumentaciju svakog softvera.

Osnovne postavke sigurnosti

Povezane informacije

- ➔ “Konfiguriranje lozinke administratora preko upravljačke ploče” na strani 33
- ➔ “Konfiguriranje lozinke administratora koristeći Web Config” na strani 33
- ➔ “EpsonNet konfiguracija” na strani 55
- ➔ “Epson Device Admin” na strani 55

Konfiguriranje lozinke administratora preko upravljačke ploče

Možete odrediti lozinku administratora na upravljačkoj ploči skenera.

1. Dodirnite **Postavke** na početnom zaslonu.
2. Dodirnite **Administracija sustava > Administratorske postavke**.
Ako stavka nije prikazana, pomaknite zaslon prema gore kako bi se pokazala.
3. Dodirnite **Lozinka administratora > Registracija**.
4. Unesite novu lozinku i dodirnite **U redu**.
5. Unesite ponovno lozinku i dodirnite **U redu**.
6. Dodirnite **U redu** na zaslonu potvrde.
Prikazan je zaslon postavki administratora.
7. Dodirnite **Postavka blokade**, a zatim dodirnite **U redu** za zaslonu potvrde.
Postavka blokade je postavljen na **Uklj.**, te će biti potrebna lozinka administratora kada koristite blokiranu stavku izbornika.

Napomena:

- Ako postavite **Postavke > Zajedničke postavke > Istek vremena za radnju na Uklj.** pisač će vas odjaviti nakon razdoblja neaktivnosti preko upravljačke ploče.
- Možete promijeniti ili izbrisati lozinku administratora kada odaberete **Promjena ili Ponovno postavi** na zaslonu **Lozinka administratora** i unesete lozinku administratora.

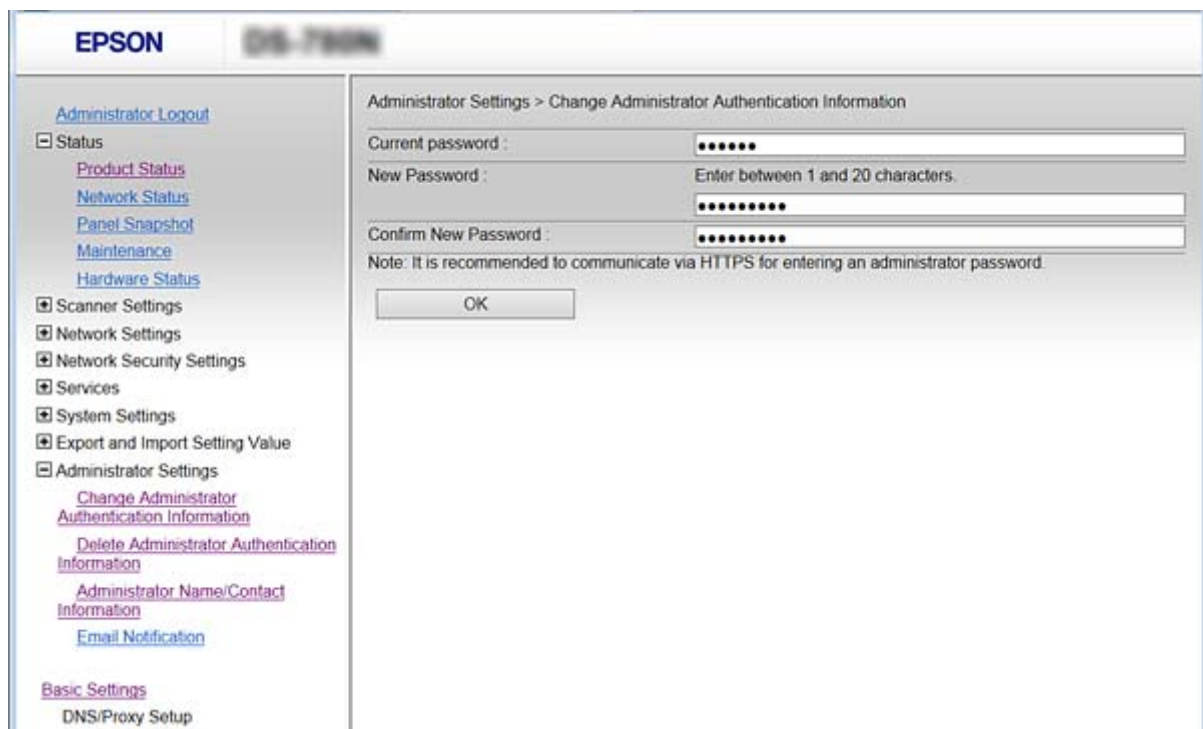
Konfiguriranje lozinke administratora koristeći Web Config

Možete postaviti lozinku administratora koristeći Web Config.

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

Osnovne postavke sigurnosti

- Unesite lozinku u **New Password** i **Confirm New Password**. Po potrebi unesite korisničko ime.
Ako želite zamijeniti lozinku novom, unesite trenutačnu lozinku.



- Odaberite **OK**.

Napomena:

- Kako biste postavili ili promijenili blokirane stavke izbornika, kliknite **Administrator Login**, a potom unesite lozinku administratora.
- Kako biste izbrisali lozinku administratora, kliknite **Administrator Settings > Delete Administrator Authentication Information**, a potom unesite lozinku administratora.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Stavke koje treba zaključati preko lozinke administratora

Administratori imaju privilegije za postavljanje i promjenu svih značajki na uređajima.

Pored toga, ako odaberete lozinku administratora na uređaju, možete ga zaključati tako da ne možete mijenjati stavke povezane s upravljanjem uređajem.

U nastavku su navedene značajke kojima administrator može upravljati.

Stavka	Opis
Postavke skenera	Postavke otkrivanja dvostrukog umetanja i sporog načina rada.

Osnovne postavke sigurnosti

Stavka	Opis
Postavke Ethernet veze	Mijenjanje naziva uređaja i IP adrese, postavke DNS ili proxy poslužitelja te postavljanje promjena povezanih s mrežnim vezama.
Postavke korisničkih usluga	Postavke za nadzor komunikacijskih protokola, mrežnog skeniranja i usluga Document Capture Pro.
Postavke poslužitelja e-pošte	Postavljanje poslužitelja e-pošte s kojim uređaj ima direktnu komunikaciju.
Postavke sigurnosti	Postavke za mrežnu sigurnost kao što je SSL/TLS komunikacija, IPsec/IP filtriranje i IEEE802.1X.
Ažuriranje korijenskog certifikata	Ažuriranje korijenskog certifikata potrebnog za provjeru autentičnosti programa Document Capture Pro Server i ažuriranje firmvera preko programa Web Config.
Ažuriranje firmvera	Provjera i ažuriranje firmvera uređaja.
Vrijeme, postavke vremenskog brojača	Vrijeme prijelaza u stanje mirovanja, automatsko isključivanje, datum/vrijeme, vremenski brojač za stanje bez rada i druge postavke povezane s vremenskim brojačem.
Vraćanje na zadane postavke	Postavke skenera koje treba vratiti na tvorničke postavke.
Postavke administratora	Postavke zaključavanja administratora ili lozinke administratora.
Postavke certificiranog uređaja	Postavke ID-a uređaja za provjeru autentičnosti. Postavljaju se prilikom uporabe skenera na sustavu provjere autentičnosti koji podržava uređaj za provjeru autentičnosti.

Upravljanje protokolima

Možete skenirati koristeći različite putanje i protokole. Možete koristiti i mrežno skeniranje preko nedefiniranog broja mrežnih računala. Primjerice, dozvoljeno je skeniranje samo navedenih putanja i protokola. Mogućnost pojave neželjenih sigurnosnih opasnosti možete smanjiti onemogućavanjem skeniranja preko određenih putanja ili upravljanjem dostupnim funkcijama.

Konfigurirajte postavke protokola.

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

Postavke će se primijeniti na skener.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Protokoli koje možete omogućiti ili onemogućiti” na strani 36](#)
- ➔ [“Stavke postavljanja protokola” na strani 37](#)

Osnovne postavke sigurnosti

Protokoli koje možete omogućiti ili onemogućiti

Protokol	Opis
Bonjour Settings	Možete odrediti hoćete li koristiti Bonjour. Bonjour se koristi za pretraživanje uređaja, skeniranje i drugo.
SLP Settings	Možete omogućiti ili onemogućiti funkciju SLP. SLP se koristi za program Epson Scan 2 i pretraživanje mreže u programu EpsonNet Config.
WSD Settings	Možete omogućiti ili onemogućiti funkciju WSD. Kada je to omogućeno, možete dodati WSD uređaje ili skenirati iz WSD ulaza.
LLTD Settings	Funkciju LLTD možete omogućiti i onemogućiti. Kada je ona omogućena, bit će prikazana u mapi mreže sustava Windows.
LLMNR Settings	Funkciju LLMNR možete omogućiti i onemogućiti. Kada je ona omogućena, možete koristiti razlučivanje naziva bez usluge NetBIOS, čak i ako ne možete koristiti DNS.
SNMPv1/v2c Settings	Možete odrediti hoće li biti omogućen protokol SNMPv1/v2c. On se koristi za postavljanje uređaja, praćenje itd.
SNMPv3 Settings	Možete odrediti hoće li biti omogućen protokol SNMPv3. Koristi se za postavljanje kriptiranih uređaja, nadziranje, itd.

Povezane informacije

- ➔ [“Upravljanje protokolima” na strani 35](#)
- ➔ [“Stavke postavljanja protokola” na strani 37](#)

Osnovne postavke sigurnosti

Stavke postavljanja protokola

The screenshot shows the 'Services > Protocol' configuration page in the EPSON control panel. The left sidebar contains navigation links for various settings, including 'Protocol' under the 'Services' section. The main content area is titled 'Services > Protocol' and includes a note about changing device and Bonjour names. Below the note are several sections for enabling and configuring different protocols:

- Bonjour Settings:** Includes a checked 'Use Bonjour' checkbox, a 'Bonjour Name' field with 'EPSON884045.local', a 'Bonjour Service Name' field with 'EPSON', and an empty 'Location' field.
- SLP Settings:** Includes a checked 'Enable SLP' checkbox.
- WSD Settings:** Includes a checked 'Enable WSD' checkbox, a 'Scanning Timeout (sec)' field with '300', a 'Device Name' field with 'EPSON', and an empty 'Location' field.
- LLTD Settings:** Includes a checked 'Enable LLTD' checkbox and a 'Device Name' field with 'EPSON'.
- LLMNR Settings:** Includes a checked 'Enable LLMNR' checkbox.
- SNMPv1/v2c Settings:** Includes a checked 'Enable SNMPv1/v2c' checkbox, an 'Access Authority' dropdown menu set to 'Read/Write', a 'Community Name (Read Only)' field with 'public', and an empty 'Community Name (Read/Write)' field.
- SNMPv3 Settings:** Includes an unchecked 'Enable SNMPv3' checkbox, a 'User Name' field with 'admin', and sub-sections for 'Authentication Settings' (Algorithm: MD5, Password and Confirm Password fields) and 'Encryption Settings' (Algorithm: DES, Password and Confirm Password fields).

At the bottom of the main content area, there is a 'Context Name' field with 'EPSON' and a 'Next' button.

Stavke

Postavljanje vrijednosti i opisa

Bonjour Settings

Osnovne postavke sigurnosti

Stavke	Postavljanje vrijednosti i opisa
Use Bonjour	Označite ovu stavku ako želite pretraživanje ili korištenje uređaja pomoću usluge Bonjour.
Bonjour Name	Prikazuje naziv za Bonjour.
Bonjour Service Name	Možete prikazati i odabrati naziv usluge Bonjour.
Location	Prikazuje naziv Bonjour lokacije.
SLP Settings	
Enable SLP	Odaberite ovu stavku ako želite omogućiti funkciju SLP. Ako se koristi za otkrivanje mreže u programu Epson Scan 2 ili EpsonNet Config.
WSD Settings	
Enable WSD	Odaberite ovu stavku ako želite omogućiti dodavanje uređaja pomoću značajke WSD te ispis i skeniranje preko ulaza WSD.
Scanning Timeout (sec)	Unesite vrijednost isteka vremena komunikacije za WSD skeniranje, između 3 i 3.600 sekundi.
Device Name	Prikazuje naziv WSD uređaja.
Location	Prikazuje naziv WSD lokacije.
LLTD Settings	
Enable LLTD	Odabirom ove stavke omogućit ćete LLTD. Skener se prikazuje u mapi mreže sustava Windows.
Device Name	Prikazuje naziv LLTD uređaja.
LLMNR Settings	
Enable LLMNR	Odabirom ove stavke omogućit ćete LLMNR. Razlučivanje naziva možete koristiti bez značajke NetBIOS čak i ako ne možete koristiti DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Odaberite ako želite omogućiti SNMPv1/v2c. Prikazat će se samo skeneri koji podržavaju SNMPv3.
Access Authority	Postavite ovlašteno tijelo za pristup kada je omogućen protokol SNMPv1/v2c. Odaberite Read Only ili Read/Write .
Community Name (Read Only)	Unesite 0 do 32 znaka ASCII koda (0x20 do 0x7E).
Community Name (Read/Write)	Unesite 0 do 32 znaka ASCII koda (0x20 do 0x7E).
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 je aktiviran kada je označen potvrdni kvadratić.
User Name	Unesite između 1 i 32 znaka koristeći 1-bitne znakove.
Authentication Settings	
Algorithm	Odaberite algoritam za provjeru autentičnosti za SNMPv3.

Osnovne postavke sigurnosti

Stavke	Postavljanje vrijednosti i opisa
Password	Odaberite lozinku za provjeru autentičnosti za SNMPv3. Unesite od 8 do 32 znaka u ASCII kodu (0x20–0x7E). Ako to ne navedete, ostavite prazno.
Confirm Password	Za potvrdu unesite lozinku koju ste postavili.
Encryption Settings	
Algorithm	Odaberite algoritam enkripcije za SNMPv3.
Password	Odaberite lozinku enkripcije za SNMPv3. Unesite od 8 do 32 znaka u ASCII kodu (0x20–0x7E). Ako to ne navedete, ostavite prazno.
Confirm Password	Za potvrdu unesite lozinku koju ste postavili.
Context Name	Unesite najviše 32 znaka Unicode (UTF-8). Ako to ne navedete, ostavite prazno. Broj znakova koji se mogu unijeti razlikuje se ovisno o jeziku.

Povezane informacije

- ➔ [“Upravljanje protokolima” na strani 35](#)
- ➔ [“Protokoli koje možete omogućiti ili onemogućiti” na strani 36](#)

Postavke načina rada i upravljanja

Ovo poglavlje objašnjava stavke povezane sa svakodnevnim radnim koracima i upravljanjem uređajem.

Potvrda informacija o uređaju

Možete provjeriti sljedeće informacije o uređaju preko **Status** koristeći Web Config.

- Product Status
Provjerite jezik, status, broj proizvoda, MAC adresu, itd.
- Network Status
Provjerite informacije o statusu mrežne veze, IP adresu, DNS poslužitelj, itd.
- Panel Snapshot
Pregledajte snimku zaslona prikazanu na upravljačkoj ploči uređaja.
- Maintenance
Provjerite datum početka, informacije o skeniranju, itd.
- Hardware Status
Provjerite status skenera.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Upravljanje uređajima (Epson Device Admin)

Možete upravljati i koristiti mnoge uređaje s programom Epson Device Admin. Epson Device Admin omogućava upravljanje uređajima koji se nalaze na različitoj mreži. U nastavku se ističu glavne značajke upravljanja.

Više informacija o funkcijama i korištenju softvera potražite u dokumentaciji ili pomoći programa Epson Device Admin.

- Otkrivanje uređaja
Možete otkriti uređaje na mreži i zatim ih prijaviti na popis. Ako se Epson uređaji poput pisača i skenera spoje na isti dio mreže na kojem se nalazi računalo administratora, možete ih pronaći čak i ako nemaju dodijeljenu IP adresu.
Također možete otkriti uređaje koji su spojeni na računala na mreži preko USB kabela. Trebate instalirati Epson Device USB Agent na računalo.
- Postavljanje uređaja
Možete napraviti predložak koji sadrži elemente postavki kao što je mrežno sučelje i papirnati izvor te ga primijeniti na druge uređaje kao dijeljene postavke. Kada se spoji na mrežu, možete dodijeliti IP adresu na uređaju kojem nije dodijeljena IP adresa.
- Nadziranje uređaja
Možete redovito pribaviti status i detaljne informacije za uređaje na mreži. Također možete nadzirati uređaje spojene na računalo na mreži preko USB kabela i uređaja drugih tvrtki koje su prijavljene na popisu uređaja. Kod nadzora uređaja povezanih USB kabelima trebate instalirati Epson Device USB Agent.

Postavke načina rada i upravljanja

Upravljanje alarmima

Možete nadzirati alarme statusa uređaja i potrošnog materijala. Sustav automatski šalje e-poruke obavijesti administratoru na temelju zadanih uvjeta.

Upravljanje izvješćima

Možete kreirati standardna izvješća dok sustav prikuplja podatke o korištenju uređaja i potrošnog materijala. Zatim možete spremiti ta kreirana izvješća i pošaljite ih e-poštom.

Povezane informacije

➔ [“Epson Device Admin” na strani 55](#)

Primanje obavijesti o događajima putem e-pošte

O obavijestima e-poštom

Ovu značajku možete koristiti kako biste primali upozorenja e-poštom kada se pojavi neki događaj. Možete registrirati do 5 adresa e-pošte i odabrati za koje događaje želite primati obavijesti.

Poslužitelj e-pošte mora biti konfiguriran za korištenje ove funkcije.

Povezane informacije

➔ [“Konfiguriranje poslužitelja e-pošte” na strani 42](#)

Konfiguriranje obavijesti e-poštom

Kako biste koristili ovu funkciju, morate konfigurirati poslužitelj e-pošte.

1. Pristupite programu Web Config i odaberite **Administrator Settings > Email Notification**.
2. Unesite adresu e-pošte na koju želite primati obavijesti.
3. Odaberite jezik za obavijesti e-poštom.

Postavke načina rada i upravljanja

4. Označite okvire za obavijesti koje želite primati.

Administrator Settings > Email Notification

Set up the Email Server to enable the email notification.

Email Address Settings

Email in selected language will be sent to each address.

1:	admin@aaa.com	English
2:	aaa@aaa.com	English
3:		English
4:		English
5:		English

Notification Settings

Email will be sent when product status is as checked.

	1	2	3	4	5
Administrator password changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scanner error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Restore Default Settings

5. Pritisnite OK.

Povezane informacije

- ➔ “Pristup aplikaciji Web Config” na strani 23
- ➔ “Konfiguriranje poslužitelja e-pošte” na strani 42

Konfiguriranje poslužitelja e-pošte

Prije konfiguriranja provjerite sljedeće.

- Je li skener povezan s mrežom.
- Podaci poslužitelja e-pošte za računalo.

1. Pristupite programu Web Config i odaberite **Network Settings > Email Server > Basic**.
2. Unesite vrijednost za svaku stavku.
3. Odaberite **OK**.

Prikazuju se postavke koje ste odabrali.

Povezane informacije

- ➔ “Pristup aplikaciji Web Config” na strani 23
- ➔ “Stavke postavljanja poslužitelja e-pošte” na strani 43

Postavke načina rada i upravljanja

Stavke postavljanja poslužitelja e-pošte

The screenshot shows the Epson printer's web interface for configuring the Email Server. The left sidebar contains a navigation menu with options like Status, Contacts, Network Settings, and Email Server. The main area is titled 'Network Settings > Email Server > Basic'. It contains a warning about certificates and several configuration fields: Authentication Method (SMTP AUTH), Authenticated Account, Authenticated Password (masked), Sender's Email Address, SMTP Server Address, SMTP Server Port Number (25), Secure Connection (None), and Certificate Validation (Enable). There is also a note about certificate validation and fields for POP3 Server Address and POP3 Server Port Number.

Stavke	Postavke i objašnjenje						
Authentication Method	<p>Odredite metodu autentifikacije za pristup skenera poslužitelju e-pošte.</p> <table border="1"> <tr> <td>Off</td> <td>Autentikacija je onemogućena prilikom komuniciranja s poslužiteljem e-pošte.</td> </tr> <tr> <td>SMTP AUTH</td> <td>Zahtijeva se da poslužitelj e-pošte podržava SMTP autentikaciju.</td> </tr> <tr> <td>POP before SMTP</td> <td>Kod odabira ove metode konfigurirajte POP3 poslužitelj.</td> </tr> </table>	Off	Autentikacija je onemogućena prilikom komuniciranja s poslužiteljem e-pošte.	SMTP AUTH	Zahtijeva se da poslužitelj e-pošte podržava SMTP autentikaciju.	POP before SMTP	Kod odabira ove metode konfigurirajte POP3 poslužitelj.
Off	Autentikacija je onemogućena prilikom komuniciranja s poslužiteljem e-pošte.						
SMTP AUTH	Zahtijeva se da poslužitelj e-pošte podržava SMTP autentikaciju.						
POP before SMTP	Kod odabira ove metode konfigurirajte POP3 poslužitelj.						
Authenticated Account	Ako ste odabrali SMTP AUTH ili POP before SMTP kao Authentication Method , unesite naziv autentificiranog računa sastavljenog od 0 do 255 znakova u ASCII kodu (0x20–0x7E).						
Authenticated Password	Ako ste odabrali SMTP AUTH ili POP before SMTP kao Authentication Method , unesite autentificiranu lozinku sastavljenu od 0 do 20 znakova koristeći znakove A–Z a–z 0–9! # \$ % & ' * + - . / = ? ^ _ { } ~ @.						
Sender's Email Address	Unesite adresu e-pošte pošiljatelja. Unesite od 0 do 255 znakova u ASCII kodu (0x20–0x7E), osim : () < > [] ; ¥. Točka "." ne može biti prvi znak.						
SMTP Server Address	Unesite između 0 i 255 znaka pomoću znakova A–Z a–z 0–9. - . . Možete koristiti IPv4 ili FQDN format.						
SMTP Server Port Number	Unesite broj između 1 i 65535.						

Postavke načina rada i upravljanja

Stavke	Postavke i objašnjenje	
Secure Connection	Odredite način sigurne veze za poslužitelj e-pošte.	
	None	Ako ste odabrali POP before SMTP u Authentication Method , način povezivanja će biti podešen na None .
	SSL/TLS	To će biti dostupno ako Authentication Method namjestite na Off ili SMTP AUTH .
	STARTTLS	To će biti dostupno ako Authentication Method namjestite na Off ili SMTP AUTH .
Certificate Validation	Valjanost certifikat će biti provjerena ako je to omogućeno. Preporučamo da to namjestite na Enable .	
POP3 Server Address	Ako odaberete POP before SMTP kao Authentication Method , unesite adresu POP3 poslužitelja sastavljenu od 0 do 255 znakova koristeći znakove A–Z a–z 0–9, - . Možete koristiti IPv4 ili FQDN format.	
POP3 Server Port Number	Ako odaberete POP before SMTP za Authentication Method , unesite broj između 1 i 65535.	

Povezane informacije

➔ [“Konfiguriranje poslužitelja e-pošte” na strani 42](#)

Provjera veze s poslužiteljem e-pošte

1. Pristupite programu Web Config i odaberite **Network Settings > Email Server > Connection Test**.
2. Odaberite **Start**.
Započet će test veze s poslužiteljem pošte. Nakon testa se prikazuje izvješće provjere.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
➔ [“Reference testa veze s poslužiteljem e-pošte” na strani 44](#)

Reference testa veze s poslužiteljem e-pošte

Poruke	Objašnjenje
Connection test was successful.	Ova poruka se pojavljuje ako je veza s poslužiteljem uspješna.
SMTP server communication error. Check the following. - Network Settings	Ova poruka pojavljuje se ako <ul style="list-style-type: none"> <input type="checkbox"/> Skener nije povezan s mrežom <input type="checkbox"/> SMTP poslužitelj je neaktivan <input type="checkbox"/> Veza s mrežom je prekinuta za vrijeme komunikacije <input type="checkbox"/> Primljeni si nepotpuni podaci

Postavke načina rada i upravljanja

Poruke	Objašnjenje
POP3 server communication error. Check the following. - Network Settings	Ova poruka pojavljuje se ako <ul style="list-style-type: none"> <input type="checkbox"/> Skener nije povezan s mrežom <input type="checkbox"/> POP3 poslužitelj je neaktivan <input type="checkbox"/> Veza s mrežom je prekinuta za vrijeme komunikacije <input type="checkbox"/> Primljeni si nepotpuni podaci
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Ova poruka pojavljuje se ako <ul style="list-style-type: none"> <input type="checkbox"/> Povezivanje sa DNS poslužiteljem nije uspjelo <input type="checkbox"/> Nije uspjelo razlučivanje naziva za SMTP poslužitelj
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Ova poruka pojavljuje se ako <ul style="list-style-type: none"> <input type="checkbox"/> Povezivanje sa DNS poslužiteljem nije uspjelo <input type="checkbox"/> Nije uspjelo razlučivanje naziva za POP3 poslužitelj
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka pojavljuje se u slučaju neuspješne autentifikacije SMTP poslužitelja.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka pojavljuje se u slučaju neuspješne autentifikacije POP3 poslužitelja.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Ova poruka pojavljuje se kada pokušavate komunicirati s nepodržanim protokolima.
Connection to SMTP server failed. Change Secure Connection to None.	Ova poruka pojavljuje se u slučaju nepodudaranja SMTP između poslužitelja i klijenta ili ako poslužitelj na podržava SMTP sigurnu vezu (SSL vezu).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Ova poruka pojavljuje se u slučaju nepodudaranja SMTP između poslužitelja i klijenta ili ako poslužitelja zatraži korištenje SSL/TLS veze za SMTP sigurnu vezu.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Ova poruka pojavljuje se u slučaju nepodudaranja SMTP između poslužitelja i klijenta ili ako poslužitelja zatraži korištenje STARTTLS veze za SMTP sigurnu vezu.
The connection is untrusted. Check the following. - Date and Time	Ova poruka pojavljuje se ako je netočna postavka datuma i vremena skenera ili ako je istekao certifikat.
The connection is untrusted. Check the following. - CA Certificate	Ova poruka se pojavljuje ako skener nema korijenski certifikat koji se podudara s poslužiteljem ili ako CA Certificate nije uvezen.
The connection is not secured.	Ova poruka pojavljuje se ako je pribavljeni certifikat oštećen.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Ova poruka pojavljuje se ako dođe do nepodudaranja načina autentifikacije između poslužitelja i klijenta. Poslužitelj podržava SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Ova poruka pojavljuje se ako dođe do nepodudaranja načina autentifikacije između poslužitelja i klijenta. Poslužitelj ne podržava SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	Ova poruka pojavljuje se ako je zadana adresa e-pošte pošiljatelja netočna.

Postavke načina rada i upravljanja

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

Povezane informacije

- ➔ [“Provjera veze s poslužiteljem e-pošte” na strani 44](#)

Ažuriranje firmvera

Ažuriranje firmvera koristeći Web Config

Ažurirajte firmver koristeći Web Config. Uređaj mora biti povezan s internetom.

1. Pristupite programu Web Config i odaberite **Basic Settings > Firmware Update**.
2. Kliknite na **Start**.
Pokreće se potvrda firmvera te se informacije o firmveru prikazuju ako postoji ažurirani firmver.
3. Kliknite **Start** i slijedite upute na zaslону.

Napomena:

Također možete ažurirati firmver koristeći *Epson Device Admin*. Možete vizualno potvrditi informacije o firmveru na popisu uređaja. Korisno je kada želite ažurirati firmver više uređaja. Saznajte više u vodiču ili pomoći za *Epson Device Admin*.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Epson Device Admin” na strani 55](#)

Ažuriranje firmvera koristeći Epson Firmware Updater

Možete preuzeti firmver uređaja s Epsonove internetske stranice na računalo, a zatim spojite uređaj i računalo USB kabelom kako biste ažurirali firmver. Ako ne možete ažurirati preko mreže, isprobajte ovaj način.

1. Pristupite Epsonovoj internetskoj stranici i preuzmite firmver.
2. Spojite računalo koji sadrži preuzeti firmver na uređaj preko USB kabela.
3. Dvaput kliknite preuzetu datoteku nastavka .exe.
Pokrenut će se aplikacija Epson Firmware Updater.
4. Slijedite upute na zaslону.

Pomoć kod postavki

Izvozom postavki na Web Config možete kopirati stavke na druge skenere.

Izvoz postavki

Izvoz svake postavke za skener.

1. Pristupite programu Web Config i odaberite **Export and Import Setting Value > Export**.
2. Odaberite postavke koji želite izvesti.
Odaberite postavke koje želite izvesti. Ako odaberete nadređenu kategoriju, odabrat će se i podkategorije. Međutim, podkategorije koje uzrokuju greške dupliranjem unutar isti mreže (kao što su IP adrese i sl.) ne mogu se odabrati.
3. Unesite lozinku za kriptiranje izvezene datoteke.
Za uvoz datoteke potrebna vam je lozinka. Ostavite ovo praznim ako ne želite kriptirati datoteku.
4. Pritisnite **Export**.

**Važno:**

*Ako želite izvesti mrežne postavke skenera, kao što su naziv pisača i IP adresa, odaberite **Enable to select the individual settings of device** i odaberite više stavki. Koristite samo odabrane vrijednosti za zamjenski skener.*

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Uvoz postavki

U skener uvezite izvezenu Web Config datoteku.

**Važno:**

Prilikom uvoza vrijednosti koje sadrže pojedine podatke, kao što su naziv skenera, IP adresa, pazite da ista IP adresa ne postoji na istoj mreži. Ako se IP adrese preklapaju, na skener se neće primijeniti vrijednost.

1. Pristupite programu Web Config i odaberite **Export and Import Setting Value > Import**.
2. Odaberite izvezenu datoteku pa unesite kriptiranu lozinku.
3. Pritisnite **Next**.
4. Odaberite postavke koje želite uvesti i zatim kliknite na **Next**.
5. Pritisnite **OK**.

Postavke će se primijeniti na skener.

Postavke načina rada i upravljanja

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Rješavanje problema

Savjeti za rješavanje problema

Više informacija možete pronaći u sljedećim priručnicima.

Korisnički vodič

Pružaju upute o korištenju skenera, održavanju i rješavanju problema.

Provjera zapisnika poslužitelja i mrežnog uređaja

U slučaju problema s mrežnom vezom, možda će biti potrebno otkriti uzrok potvrđivanjem zapisnika poslužitelja e-pošte ili poslužitelja LDAP, provjerom statusa korištenjem mrežnog zapisa na temelju zapisnika i naredbi opreme sustava, primjerice usmjerivača.

Inicijaliziranje mrežnih postavki

Oporavak mrežnih postavki s upravljačke ploče pisača

Možete vratiti sve mrežne postavke na njihove zadane vrijednosti.

1. Dodirnite **Postavke** na početnom zaslonu.
 2. Dodirnite **Administracija sustava > Vрати zadane postavke > Postavke mreže**.
 3. Provjerite poruku i dodirnite **Da**.
 4. Kada se prikaže poruka o dovršetku, dodirnite **Zatvori**.
Zaslon se automatski zatvara ako određeno vrijeme ne dodirnete **Zatvori**.
-

Provjera komunikacije između uređaja i računala

Provjera povezivanja pomoću naredbe Ping — Windows

Pomoću naredbe Ping možete provjeriti je li računalo povezano sa skenerom. Slijedite korake navedene u nastavku kako biste provjerili povezanost pomoću naredbe Ping.

1. Provjerite IP adresu skenera za vezu koju želite provjeriti.
Možete je provjeriti pomoću programa Epson Scan 2.

Rješavanje problema

2. Prikažite zaslon unosa naredbe računala.

Windows 10

Desnom tipkom kliknite na gumb Start ili pritisnite i zadržite ga i zatim odaberite **Unos naredbe**.

Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

Prikažite zaslon aplikacije i potom odaberite **Unos naredbe**.

Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 ili starija inačica

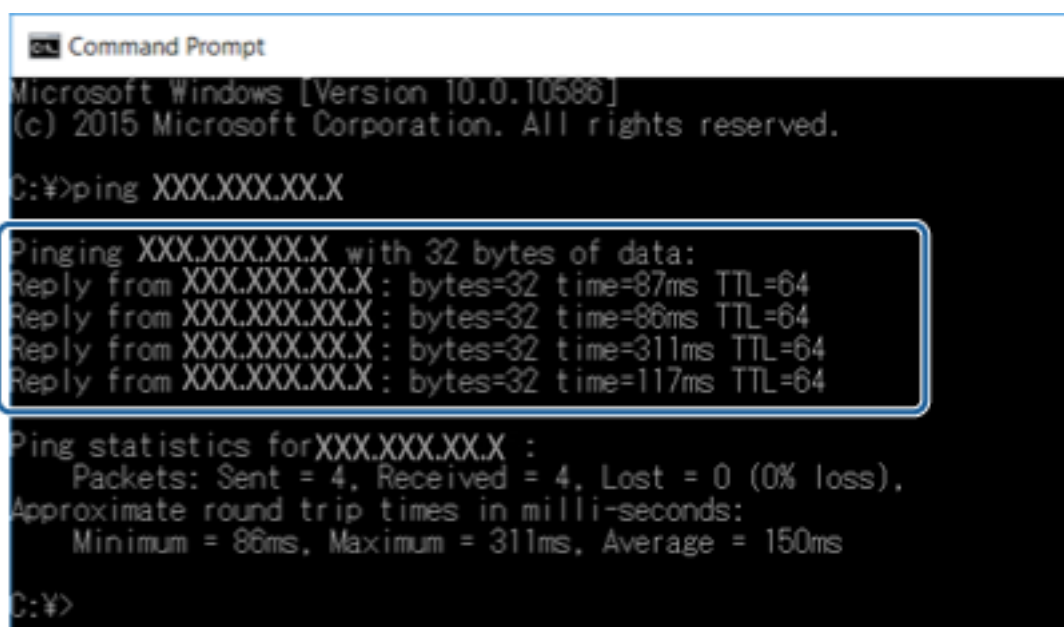
Kliknite gumb Start, odaberite **Svi programi** ili **Programi** > **Dodatna oprema** > **Unos naredbe**.

3. Unesite "ping xxx.xxx.xxx.xxx" i zatim pritisnite tipku Enter.

Unesite IP adresu skenera za xxx.xxx.xxx.xxx.

4. Provjerite status komunikacije.

Ako pisac i računalo komuniciraju, prikazat će se sljedeća poruka.



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

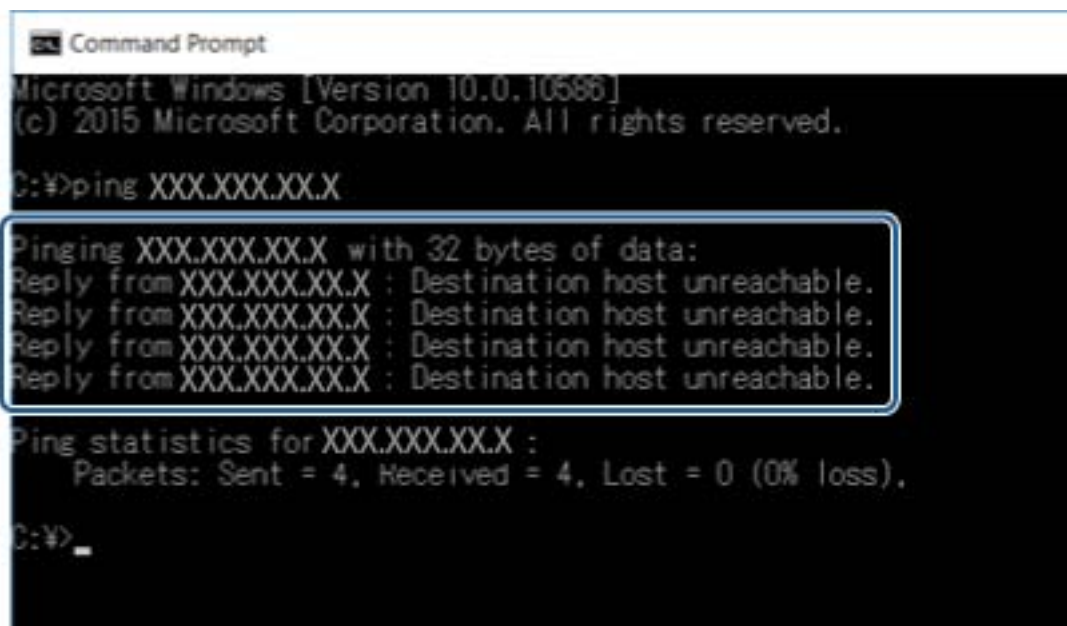
Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X: bytes=32 time=87ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=86ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=311ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=117ms TTL=64

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 86ms, Maximum = 311ms, Average = 150ms

C:\>
```

Rješavanje problema

Ako pišač i računalo ne komuniciraju, prikazat će se sljedeća poruka.



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.

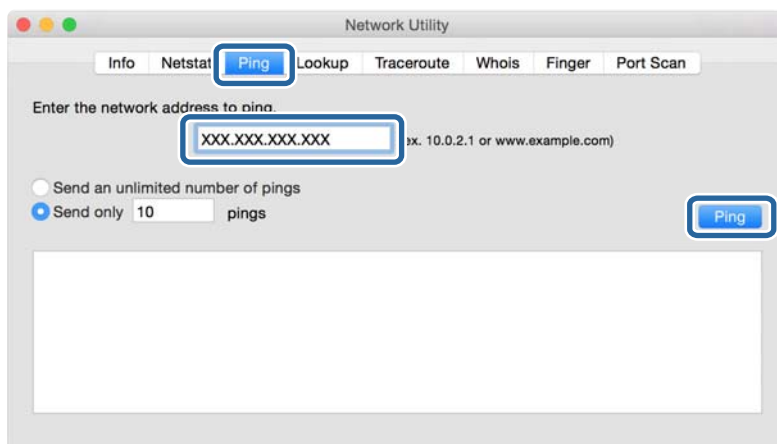
Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>_
```

Provjera povezivanja pomoću naredbe Ping — Mac OS

Pomoću naredbe Ping možete provjeriti je li računalo povezano sa skenerom. Slijedite korake navedene u nastavku kako biste provjerili povezanost pomoću naredbe Ping.

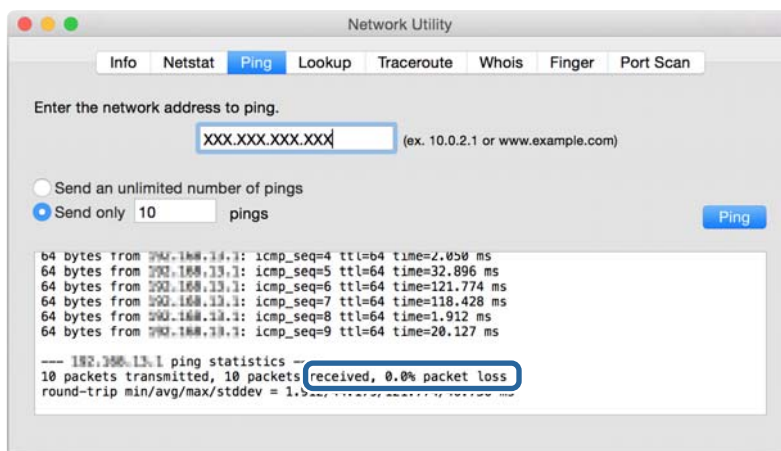
1. Provjerite IP adresu skenera za vezu koju želite provjeriti.
Možete je provjerite pomoću programa Epson Scan 2.
2. Pokrenite mrežni uslužni program.
Unesite „Network Utility” u **Spotlight**.
3. Kliknite karticu **Ping**, unesite IP adresu koju ste provjerili u koraku 1 i potom kliknite **Ping**.



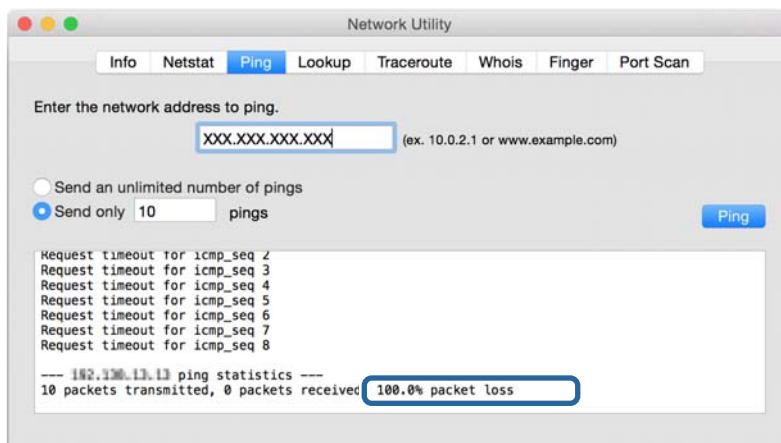
Rješavanje problema

4. Provjerite status komunikacije.

Ako pisar i računalo komuniciraju, prikazat će se sljedeća poruka.



Ako pisar i računalo ne komuniciraju, prikazat će se sljedeća poruka.



Problemi s korištenjem mrežnog softvera

Nije moguć pristup programu Web Config

Je li IP adresa skenera ispravno konfigurirana?

Konfigurirajte IP adresu pomoću programa Epson Device Admin ili EpsonNet Config.

Podržava li vaš preglednik masovno šifriranje za Encryption Strength za SSL/TLS?

Masovno šifriranje za Encryption Strength za SSL/TLS je sljedeće. Aplikaciji Web Config može se pristupiti samo pomoću preglednika koji podržava sljedeće masovno šifriranje. Provjerite koju vrstu kriptiranja koristi vaš preglednik.

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

Rješavanje problema

- 192bit: AES256
- 256bit: AES256

Poruka „Isteklo” pojavljuje se kod pristupanja aplikaciji Web Config pomoću SSL komunikacije (https-a).

Ako je certifikat istekao, pribavite ga ponovno. Ako se poruka pojavi prije isteka certifikata, provjerite je li datum skenera ispravno konfiguriran.

Kod pristupanja aplikaciji Web Config pomoću SSL komunikacije (https-a) pojavljuje se poruka „Naziv sigurnosnog certifikata ne odgovara...”.

IP adresa skenera unesena za **Common Name** za izradu samopotpisanog certifikata ili zahtjeva za potpisivanje certifikata ne podudara se s adresom unesenom u preglednik. Ponovno pribavite i uvezite certifikat ili promijenite naziv skenera.

Skeneru se pristupa preko proxy poslužitelja.

Ako koristite proxy poslužitelj sa skenerom, trebate konfigurirati proxy postavke preglednika.

Windows:

Odaberite **Upravljačka ploča > Mreža i internet > Internetske opcije > Veze > LAN postavke > Proxy poslužitelj**, a zatim konfigurirajte da se za lokalne adrese ne koristi proxy poslužitelj.

Mac OS:

Odaberite **Postavke sustava > Mreža > Napredno > Proxy**, a zatim registrirajte lokalnu adresu za **Zaobiđi proxy postavke za ove hostove i domene**.

Primjer:

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

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

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Dodjela IP adrese” na strani 15](#)
- ➔ [“Dodjeljivanje IP adrese koristeći EpsonNet Config” na strani 56](#)

Naziv modela i/ili IP adrese se ne prikazuju na EpsonNet Config

Jeste li odabrali Blokiraj, Odustani ili Isključi računalo kada se prikazao Windows zaslon za sigurnost ili vatrozid?

Ako odaberete **Blokiraj**, **Odustani** ili **Isključi**, IP adresa i naziv modela se neće prikazivati na EpsonNet Config ili EpsonNet Setup.

Kako biste to ispravili, registrirajte EpsonNet Config kao iznimku preko Windows vatrozida i komercijalnog sigurnosnog softvera. Ako koristite antivirusni program ili sigurnosni program, zatvorite ga, a zatim pokušajte koristiti EpsonNet Config.

Je li postavka za istek u slučaju pogreške u komunikaciji prekratka?

Pokrenite EpsonNet Config i odaberite **Tools > Options > Timeout**, a zatim povećajte vrijeme za postavku **Communication Error**. Napominjemo da u tom slučaju EpsonNet Config može raditi sporije.

Rješavanje problema

Povezane informacije

- ➔ [“Pokretanje aplikacije EpsonNet Config — Windows” na strani 56](#)
- ➔ [“Pokretanje aplikacije EpsonNet Config — Mac OS” na strani 56](#)

Dodatak

Uvod u mrežni softver

U nastavku se opisuje softver koji konfigurira i upravlja uređajima.

Epson Device Admin

Epson Device Admin je aplikacija koja vam omogućuje instaliranje uređaja na mrežu, a zatim konfiguriranje i upravljanje uređajima. Možete pribaviti detaljne informacije o uređajima, poput statusa i potrošnog materijala, slati obavijesti i upozorenja te kreirati izvješća za potrebe korištenja uređaja. Također možete napraviti predložak koji sadrži postavke te ga primijeniti na druge uređaje kao dijeljene postavke. Epson Device Admin možete preuzeti sa web-mjesta za podršku Epson. Za više informacija pogledajte dokumentaciju ili datoteke pomoći aplikacije Epson Device Admin.

Pokretanje programa Epson Device Admin (samo sustav Windows)

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

Napomena:

Ako se pojavi upozorenje vatrozida, dopustite pristup za Epson Device Admin.

EpsonNet konfiguracija

EpsonNet Config omogućava administratoru konfiguriranje mrežnih postavki skenera, kao što su dodjela IP adrese i promjena načina spajanja. Značajka skupnog postavljanja podržana je u operativnom sustavu Windows. Za više informacija pogledajte dokumentaciju ili datoteke pomoći aplikacije EpsonNet Config.



Pokretanje aplikacije EpsonNet Config — Windows

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

Napomena:

Ako se pojavi upozorenje vatrozida, dopustite pristup za EpsonNet Config.

Pokretanje aplikacije EpsonNet Config — Mac OS

Odaberite **Idi > Aplikacije > Epson Software > EpsonNet > EpsonNet Config SE > EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager je softver za izradu paketa za jednostavnu instalaciju skenera, poput instaliranja upravljačkog programa skenera i instaliranje programa Document Capture Pro. Ovaj softver administratoru omogućuje stvaranje jedinstvenih softverskih paketa i njihovo distribuiranje među grupama.

Kako biste saznali više, posjetite naše regionalno Epson web-mjesto.

Dodjeljivanje IP adrese koristeći EpsonNet Config

Možete dodijeliti IP adresu skeneru koristeći EpsonNet Config. EpsonNet Config omogućava dodjelu IP adrese skeneru kojemu nije dodijeljena nakon povezivanja Ethernet kabelom.

Dodjela IP adrese korištenjem postavki serije

Kreiranje datoteke za postavke serije

Koristeći MAC adresu i naziv modela kao ključeve, možete kreirati novu SYLK datoteku za postavljanje IP adrese.

1. Otvorite aplikaciju za proračunske tablice (kao što je Microsoft Excel) ili program za uređivanje teksta.
2. Unesite „Info_MACAddress”, „Info_ModelName” i „TCPIP_IPAddress” u prvi red kao nazive elementa postavke.

Unesite elemente postavke za sljedeće tekstualne nizove. Za razlikovanje velikih/malih slova i znakova s jednim/dvostrukim bajtom, ako se razlikuje samo jedan znak, stavka neće biti prepoznata.

Unesite naziv elementa postavke kako je opisano u nastavku; u protivnom, EpsonNet Config neće moći prepoznati elemente postavke.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Unesite MAC adresu, naziv modela i IP adresu svakog mrežnog sučelja.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

Dodatak

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

4. Unesite naziv i spremite kao SYLK datoteku (*.slk).

Odabir skupnih postavki koristeći konfiguracijsku datoteku

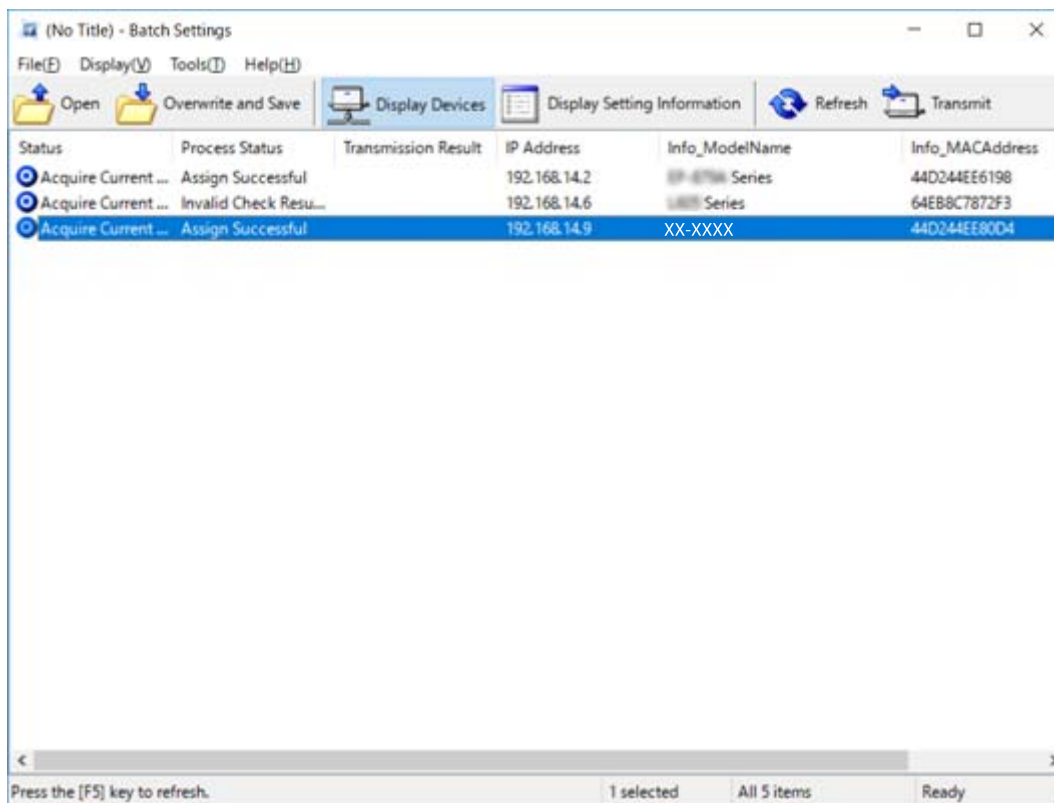
Istovremeno dodijelite IP adrese u konfiguracijsku datoteku (SYLK). Trebate kreirati konfiguracijsku datoteku prije dodjeljivanja.

1. Spojite sve uređaje na mrežu koristeći Ethernet kabele.
2. Uključite skener.
3. Pokrenite EpsonNet Config.
Prikazan je popis skenera na mreži. Može proći neko vrijeme prije nego budu prikazani.
4. Kliknite **Tools > Batch Settings**.
5. Kliknite na **Open**.
6. Na zaslону odabira datoteke odaberite datoteku SYLK (*.slk) koja sadrži postavke, a zatim kliknite **Open**.

Dodatak

7. Odaberite uređaje za koje želite izvršiti skupne postavke koristeći stupac **Status** postavljen na **Unassigned**, a **Process Status** postavljen na **Assign Successful**.

Kod višestrukog odabira pritisnite Ctrl ili Shift te kliknite ili povucite mišem.



8. Kliknite na **Transmit**.
9. Kada se prikaže zaslon za unos lozinke, unesite lozinku i kliknite **OK**.

Prenesite postavke.

Napomena:



Informacije se prenose na mrežno sučelje dok se ne završi napredovanje procesa. Nemojte isključivati uređaj ni bežični adapter i nemojte slati nikakve podatke na uređaj.






10. Na zaslonu **Transmitting Settings** kliknite **OK**.



Dodatak

11. Provjerite status uređaja koji postavljate.

Za uređaje koji pokazuju  ili  provjerite sadržaj datoteke postavki ili provjerite normalno pokretanje uređaja.

Ikona	Status	Process Status	Objašnjenje
	Setup Complete	Setup Successful	Postavljanje je izvršeno normalno.
	Setup Complete	Rebooting	Kada se prenose informacije, svaki uređaj treba se ponovno pokrenuti kako bi se aktivirale postavke. Provjera se provodi kako bi se ustanovilo može li se spajati na uređaj nakon novog pokretanja.
	Setup Complete	Reboot Failed	Ne može se potvrditi uređaj nakon prijenosa postavki. Provjerite je li uređaj uključen ili se ponovno pokrenuo na normalan način.
	Setup Complete	Searching	Pretraživanje uređaja navedenog u datoteci postavki.*
	Setup Complete	Search Failed	Ne mogu se provjeriti uređaji koji su već konfigurirani. Provjerite je li uređaj uključen ili se ponovno pokrenuo na normalan način.*

* Samo kada su prikazane informacije o postavci.

Povezane informacije

- ➔ [“Pokretanje aplikacije EpsonNet Config — Windows” na strani 56](#)
- ➔ [“Pokretanje aplikacije EpsonNet Config — Mac OS” na strani 56](#)

Dodjela IP adrese svakom uređaju

Dodijelite IP adresu skeneru koristeći EpsonNet Config.

1. Uključite skener.
2. Spojite skener na mrežu koristeći Ethernet kabel.
3. Pokrenite EpsonNet Config.

Prikazan je popis skenera na mreži. Može proći neko vrijeme prije nego budu prikazani.

4. Dvaput pritisnite na skener koji želite dodijeliti.

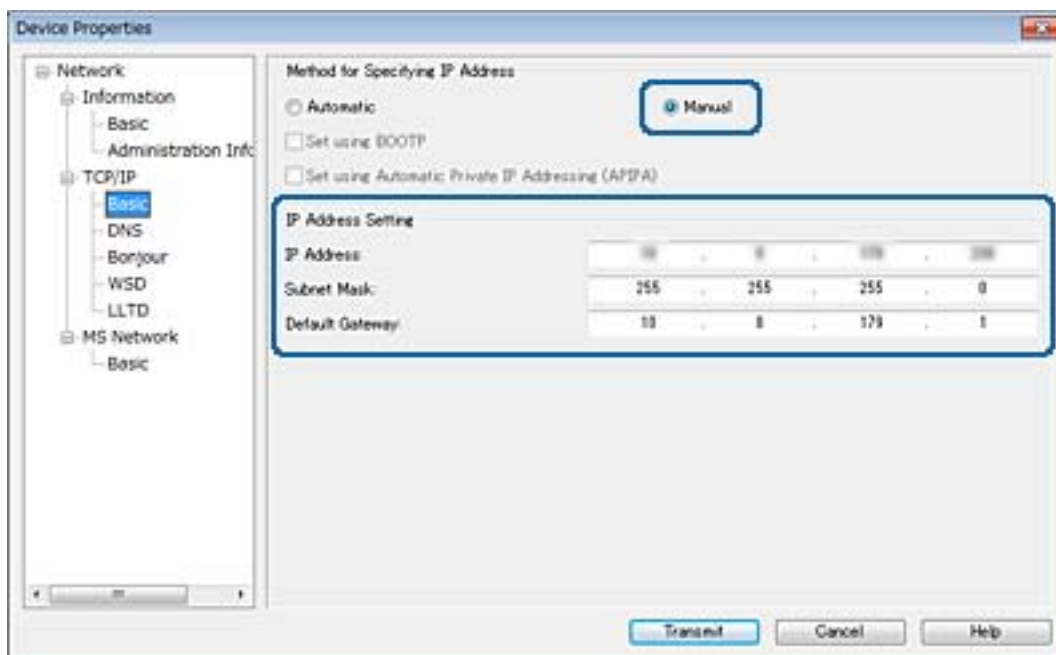
Napomena:

Ako se spojili više skenera istog modela, možete identificirati skener koristeći MAC adresu.

5. Odaberite **Network > TCP/IP > Basic**.

Dodatak

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

**Napomena:**

Unesite statičku adresu kada spojite skener na sigurnu mrežu.

7. Kliknite na **Transmit**.

Prikazan je zaslon koji potvrđuje prijenos informacija.

8. Kliknite na **OK**.

Prikazan je zaslon koji prikazuje završetak prijenosa.

Napomena:

Informacije se prenose uređaju, a zatim se prikazuje poruka „Konfiguracija je uspješno završena”. Nemojte isključivati uređaj i nemojte slati nikakve podatke servisnom odjelu.

9. Kliknite na **OK**.

Povezane informacije

- ➔ “Pokretanje aplikacije EpsonNet Config — Windows” na strani 56
- ➔ “Pokretanje aplikacije EpsonNet Config — Mac OS” na strani 56

Korištenje ulaza skenera

Skener koristi sljedeći ulaz. Ovi ulazi trebaju biti odobreni kako bi ih po potrebi omogućio administrator mreže.

Dodatak

Pošiljatelj (klijent)	Uporaba	Odredište (poslužitelj)	Protokol	Broj ulaza
Skener	Slanje e-pošte (obavijest putem e-pošte)	SMTP poslužitelj	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP prije SMTP veze (obavijest putem e-pošte)	POP poslužitelj	POP3 (TCP)	110
	Control WSD	Klijentsko računalo	WSD (TCP)	5357
	Pretraživanje računala kod brzog skeniranja iz aplikacije Document Capture Pro	Klijentsko računalo	Otkrivanje brzog skeniranja preko mreže	2968
Prikupljanje informacija kod brzog skeniranja iz aplikacije Document Capture Pro	Klijentsko računalo	Brzo skeniranje preko mreže	2968	
Klijentsko računalo	Otkrijte skener iz aplikacije poput EpsonNet Config i upravljačkog programa skenera.	Skener	ENPC (UDP)	3289
	Prikupite i postavite MIB informacije iz aplikacije poput EpsonNet Config i upravljačkog programa skenera.	Skener	SNMP (UDP)	161
	Traženje WSD skenera	Skener	WS-Discovery (UDP)	3702
	Preusmjeravanje skeniranih podataka iz Document Capture Pro	Skener	Mrežno skeniranje (TCP)	1865

Napredne postavke sigurnosti za tvrtku

U ovom poglavlju opisujemo napredne sigurnosne značajke.

Sigurnosne postavke i sprječavanje opasnosti

Kad je uređaj spojen na mrežu, možete mu pristupiti s udaljene lokacije. Mnogo ljudi može dijeliti uređaj, što je veoma korisno za poboljšanje radne učinkovitosti i praktičnosti. Međutim, time se povećava i opasnost od nedozvoljenog pristupa, uporabe i neovlaštenog mijenjanja podataka. Ako uređaj koristite na mjestu s pristupom internetu, rizik je još veći.

Kako biste izbjegli taj rizik, uređaji tvrtke Epson imaju razne vrste sigurnosnih tehnologija.

Uređaj podesite prema potrebi u skladu s uvjetima lokacije koji su razvijeni na temelju informacija klijenta o lokaciji.

Naziv	Vrsta značajke	Što podesiti	Što spriječiti
SSL/TLS komunikacija	Komunikacijska staza između računala i uređaja kriptirana je putem SSL/TLS komunikacije. Zaštićen je sadržaj komunikacije preko preglednika.	Postavite CA certifikat za poslužitelj koji je certifikat s potpisom CA (Certificate Authority) za uređaj.	Spriječite curenje informacija i sadržaja prenesenih podataka s računala na skener. Pristup Epson poslužitelju na internetu preko uređaja možete zaštititi ažuriranjem firmvera, i sl.
IPsec/IP filtriranje	Možete postaviti dozvolu prekidanja i rezanja podataka određenog klijenta ili vrste. S obzirom da IPsec štiti podatke preko IP paketne jedinice (kriptiranje i provjera autentičnosti), možete sigurno komunicirati između neosiguranog skeniranja.	Kreirajte osnovno i individualno pravilo za postavljanje klijenta ili vrste podataka koji mogu pristupiti uređaju.	Zaštite od neovlaštenog pristupa, falsificiranja i presretanja komunikacijskih podataka prema uređaju.
SNMPv3	Dodane su značajke kao što je nadzor spojenih uređaja na mreži, integritet podataka na SNMP nadzornom protokolu, kriptiranje, provjera autentičnosti korisnika, itd.	Aktivirajte SNMPv3 i zatim postavite način provjere autentičnosti i enkripcije.	Osigurajte postavke promjene preko mreže, nadzor statusa povjerljivosti.
IEEE802.1X	Dozvoljava spajanje samo korisniku koji ima odobrenje za Ethernet. Dozvoljava uporabu uređaja samo korisniku koji ima dozvolu.	Postavke provjere autentičnosti na RADIUS poslužitelju (poslužitelj za provjeru autentičnosti).	Štiti od neovlaštenog pristupa i zlouporabe uređaja.

Napredne postavke sigurnosti za tvrtku

Naziv	Vrsta značajke	Što podesiti	Što spriječiti
Očitavanje identifikacijske kartice	Ovaj uređaj možete koristiti tako da držite identifikacijsku karticu iznad spojenog uređaja za provjeru autentičnosti. Možete ograničiti dobivanje zapisnika za svakog korisnika i svaki uređaj te ograničiti dostupnu uporabu uređaja i dostupne značajke za svakog korisnika i grupu.	Spojite uređaj za provjeru autentičnosti na uređaj, a u sustavu provjere autentičnosti navedite informacije o korisniku.	Spriječite neovlašteno korištenje i zlouporabu uređaja.

Povezane informacije

- ➔ [“SSL/TLS komunikacija sa skenerom” na strani 63](#)
- ➔ [“Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 71](#)
- ➔ [“Upotreba SNMPv3 protokola” na strani 83](#)
- ➔ [“Spajanje skenera s IEEE802.1X mrežom” na strani 85](#)

Postavke sigurnosne značajke

Kod postavljanja IPsec/IP filtriranja ili IEEE802.1X preporučuje se da pristupite programu Web Config koristeći SSL/TLS za prijenos informacija o postavkama kako bi se smanjili sigurnosni rizici poput falsificiranja ili presretanja komunikacije.

SSL/TLS komunikacija sa skenerom

Kada se certifikat poslužitelja koji koristi SSL/TLS (Secure Sockets Layer/Transport Layer Security) komunikaciju sa skenerom, možete kriptirati komunikacijsku stazu između računala. Učinite to ako želite spriječiti daljinski i neovlašteni pristup.

O digitalnom certificiranju

- Certifikat koji je potpisalo tijelo koje izdaje digitalne certifikate (CA)

Certifikat koji je potpisalo CA (tijelo koje izdaje digitalne certifikate) morate dobiti od tijela koje izdaje certifikate. Sigurnu komunikaciju možete osigurati korištenjem certifikata koji je potpisalo tijelo koje izdaje digitalne certifikate (CA). Možete koristiti certifikat koje je potpisalo tijelo koje izdaje digitalne certifikate (CA) za svaku sigurnosnu značajku.
- Certifikat koje je izdalo tijelo koje izdaje digitalne certifikate (CA)

Certifikat koje je izdalo tijelo koje izdaje digitalne certifikate (CA) označava da je treća strana potvrdila identitet poslužitelja. Ovo je ključna komponenta “web-of-trust” sigurnosti. CA certifikat za autentifikaciju poslužitelja morate dobiti od tijela koje izdaje digitalne certifikate.
- Samopotpisani certifikat

Samopotpisani certifikat je certifikat koji izdaje i potpisuje sam skener. Ovaj certifikat je nepouzdan i ne može spriječiti “spoofing”. Ako koristite ovaj certifikat za SSL/TLS certifikat, u pregledniku će se možda prikazati sigurnosno upozorenje. Ovaj certifikat možete koristiti samo za SSL/TLS komunikaciju.

Napredne postavke sigurnosti za tvrtku

Povezane informacije

- ➔ “Pribavljanje i uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA)” na strani 64
- ➔ “Brisanje certifikata potpisanog od strane tijela za izdavanje certifikata (CA)” na strani 67
- ➔ “Ažuriranje samopotpisanog certifikata” na strani 68

Pribavljanje i uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA)

Pribavljanje certifikata potpisanog od strane tijela za izdavanje certifikata (CA)

Za pribavljanje certifikata koje je potpisalo tijelo za izdavanje digitalnih certifikata, izradite CSR (zahtjev za potpisivanje certifikata) i podnesite ga tijelu za izdavanje digitalnih certifikata. Zahtjev za potpisivanje certifikata možete izraditi pomoću aplikacije Web Config i računala.

Slijedite korake za izradu zahtjeva i pribavite certifikat koji je potpisalo tijelo za izdavanje digitalnih certifikata pomoću aplikacije Web Config. Kada izrađujete zahtjev za potpisivanje certifikata pomoću aplikacije Web Config, certifikat će biti u PEM/DER formatu.

1. Pristupite programu Web Config i odaberite **Network Security Settings**. Zatim odaberite **SSL/TLS > Certificate** ili **IPsec/IP Filtering > Client Certificate** ili **IEEE802.1X > Client Certificate**.
2. Pritisnite **Generate** u **CSR**.
Otvora se stranica za izradu zahtjeva za potpisivanje certifikata.
3. Unesite vrijednost za svaku stavku.
Napomena:
Dostupne duljine ključeva i kratica ovise o tijelu koje izdaje digitalni certifikat. Izradite zahtjev prema pravilima pojedinog tijela.
4. Pritisnite **OK**.
Prikazuje se poruka o dovršetku.
5. Odaberite **Network Security Settings**. Zatim odaberite **SSL/TLS > Certificate** ili **IPsec/IP Filtering > Client Certificate** ili **IEEE802.1X > Client Certificate**.
6. Pritisnite gumb za preuzimanje u **CSR** prema formatu određenom od strane tijela za izdavanje digitalnih certifikata kako biste zahtjev za potpisivanje certifikata preuzeli na računalo.



Važno:

Nemojte ponovno generirati CSR. Ako to učinite, nećete moći uvesti izdani CA-signed Certificate.

7. Pošaljite CSR tijelu za izdavanje certifikata i pribavite CA-signed Certificate.
Slijedite pravila svakog tijela za izdavanje certifikata u vezi sa načinom slanja i formularom.
8. Spremite izdani CA-signed Certificate na računalo povezano sa skenerom.
Pribavljanje CA-signed Certificate je dovršeno kada certifikat spremite na odredište.

Napredne postavke sigurnosti za tvrtku

Povezane informacije

- ➔ “Pristup aplikaciji Web Config” na strani 23
- ➔ “Stavke postavljanja zahtjeva za potpisivanje certifikata” na strani 65
- ➔ “Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA)” na strani 66

Stavke postavljanja zahtjeva za potpisivanje certifikata

The screenshot shows the 'Certificate' configuration page in the EPSON network security settings. The left sidebar contains a navigation menu with options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Network Security Settings', 'SSL/TLS', 'IPsec/IP Filtering', 'IEEE802.1X', 'Services', 'System Settings', 'Export and Import Setting Value', 'Administrator Settings', and 'Basic Settings'. The main content area is titled 'Network Security Settings > SSL/TLS > Certificate' and contains the following fields:

- Key Length: [Input field]
- Common Name: [Input field]
- Organization: [Input field]
- Organizational Unit: [Input field]
- Locality: [Input field]
- State/Province: [Input field]
- Country: [Input field]

At the bottom of the form are two buttons: 'OK' and 'Back'.

Stavke	Postavke i objašnjenje
Key Length	Odaberite duljinu ključa za zahtjev za potpisivanje certifikata.
Common Name	Možete unijeti između 1 i 128 znakova. Ako se radi o IP adresi, to mora biti statična IP adresa. Primjer: URL za pristup aplikaciji Web Config: https://10.152.12.225 Zajednički naziv: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Možete unijeti od 0 do 64 znaka u ASCII kodu (0x20–0x7E). Nazive možete odvojiti zarezima.
Country	Unesite dvoznamenkasti broj šifre zemlje određen standardom ISO-3166.

Povezane informacije

- ➔ “Pribavljanje certifikata potpisanog od strane tijela za izdavanje certifikata (CA)” na strani 64

Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA)



Važno:

- Provjerite jesu li datum i vrijeme skenera ispravno postavljeni.
- Ako certifikat dobijete pomoću zahtjeva za potpisivanje certifikata izrađenog u aplikaciji Web Config, certifikat možete uvesti jednom.

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

2. Pritisnite **Import**.

Otvara se stranica za uvoz certifikata.

3. Unesite vrijednost za svaku stavku.

Ovisno o tome gdje izrađujete zahtjev za potpisivanje certifikata i formatu datoteke certifikata, potrebne postavke mogu se razlikovati. Unesite vrijednosti potrebnih stavki prema sljedećem.

- Certifikat u PEM/DER formatu dobiven od strane Web Config
 - Private Key:** Nemojte konfigurirati, jer skener sadrži privatni ključ.
 - Password:** Nemojte konfigurirati.
 - CA Certificate 1/CA Certificate 2:** Dodatno
- Certifikat u PEM/DER formatu dobiven s računala
 - Private Key:** Trebate postaviti.
 - Password:** Nemojte konfigurirati.
 - CA Certificate 1/CA Certificate 2:** Dodatno
- Certifikat u PKCS#12 formatu dobiven s računala
 - Private Key:** Nemojte konfigurirati.
 - Password:** Dodatno
 - CA Certificate 1/CA Certificate 2:** Nemojte konfigurirati.

4. Pritisnite **OK**.

Prikazuje se poruka o dovršetku.

Napomena:

Pritisnite **Confirm** za potvrđivanje informacija o certifikatu.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Postavljanje stavki za uvoz certifikata koji je potpisalo tijelo za izdavanje digitalnih certifikata” na strani 67](#)

Napredne postavke sigurnosti za tvrtku

Postavljanje stavki za uvoz certifikata koji je potpisalo tijelo za izdavanje digitalnih certifikata

EPSON

Administrator Logout

- Status
 - Product Status
 - Network Status
 - Panel Snapshot
 - Maintenance
 - Hardware Status
- Scanner Settings
- Network Settings
- Network Security Settings
 - SSL/TLS
 - Basic
 - Certificate
 - IPsec/IP Filtering
 - IEEE802.1X
 - CA Certificate
- Services
- System Settings
- Export and Import Setting Value
- Administrator Settings

Basic Settings

- DNS/Proxy Setup
- Firmware Update
- Root Certificate Update
- Product Status

Network Security Settings > SSL/TLS > Certificate

Server Certificate : Certificate (PEM/DER)
Browse... [file selection]

Private Key : Browse... [file selection]

Password : [text input]

CA Certificate 1 : Browse... [file selection]

CA Certificate 2 : Browse... [file selection]

Note: It is recommended to communicate via HTTPS for importing a certificate.

OK Back

Stavke	Postavke i objašnjenje
Server Certificate ili Client Certificate	Odaberite format certifikata.
Private Key	Ako možete dobiti certifikat PEM/DER formata pomoću zahtjeva za potpisivanje certifikata izrađenog na računalu, navedite datoteku privatnog ključa koja se podudara s certifikatom.
Password	Unesite lozinku za kriptiranje privatnog ključa.
CA Certificate 1	Ako je format certifikata Certificate (PEM/DER) , unesite certifikat koji izdaje tijelo za certifikate za poslužitelje. Odredite datoteku ako je to potrebno.
CA Certificate 2	Ako je format certifikata Certificate (PEM/DER) , uvezite certifikat koji izdaje tijelo za certifikate CA Certificate 1 . Odredite datoteku ako je to potrebno.

Povezane informacije

➔ “Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA)” na strani 66

Brisanje certifikata potpisanog od strane tijela za izdavanje certifikata (CA)

Možete izbrisati uvezeni certifikat ako istekne ili ako kriptirana veza više nije potrebna.

Napredne postavke sigurnosti za tvrtku



Važno:

Ako certifikat dobijete pomoću zahtjeva za potpisivanje certifikata izrađenog u aplikaciji Web Config, izbrisani certifikat ne možete više uvesti. U tom slučaju, izradite zahtjev za potpisivanje certifikata i ponovno pribavite certifikat.

1. Pristupite programu Web Config i odaberite **Network Security Settings**. Zatim odaberite **SSL/TLS > Certificate** ili **IPsec/IP Filtering > Client Certificate** ili **IEEE802.1X > Client Certificate**.
2. Kliknite na **Delete**.
3. U prikazanoj poruci potvrdite da želite izbrisati certifikat.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Ažuriranje samopotpisanog certifikata

Ako skener podržava značajku HTTPS, možete ažurirati samopotpisani certifikat. Kada pristupate aplikaciji Web Config pomoću samopotpisanog certifikata, pojavljuje se poruka upozorenja.

Samopotpisani certifikat koristite privremeno, dok ne pribavite i uvezete certifikat koji je potpisalo tijelo za izdavanje certifikata.

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

Unesite IP adresu ili identifikator, kao što je FQDN naziv skenera. Možete unijeti između 1 i 128 znakova.

Napomena:

Ime (CN) možete odvojiti zarezom.

Napredne postavke sigurnosti za tvrtku

4. Odredite razdoblje valjanosti certifikata.

EPSON

Administrator Logout

- Status
 - Product Status
 - Network Status
 - Panel Snapshot
 - Maintenance
 - Hardware Status
- Scanner Settings
- Network Settings
- Network Security Settings
 - SSL/TLS
 - Basic
 - Certificate
 - IPsec/IP Filtering
 - IEEE802.1X
 - CA Certificate
- Services
- System Settings
- Export and Import Setting Value
- Administrator Settings

Basic Settings

- DNS/Proxy Setup
- Firmware Update
- Root Certificate Update
- Product Status

Network Security Settings > SSL/TLS > Certificate

Key Length :	2048
Common Name :	SEIKO EPSON CORP
Organization :	SEIKO EPSON CORP
Valid Date (UTC) :	2016-11-24 02:49:09 UTC
Certificate Validity (year) :	10

Next Back

5. Kliknite na **Next**.

Prikazuje se poruka potvrde.

6. Kliknite na **OK**.

Skener se ažurira.

Napomena:

Pritisnite **Confirm** za potvrđivanje informacija o certifikatu.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Konfigurirajte CA Certificate

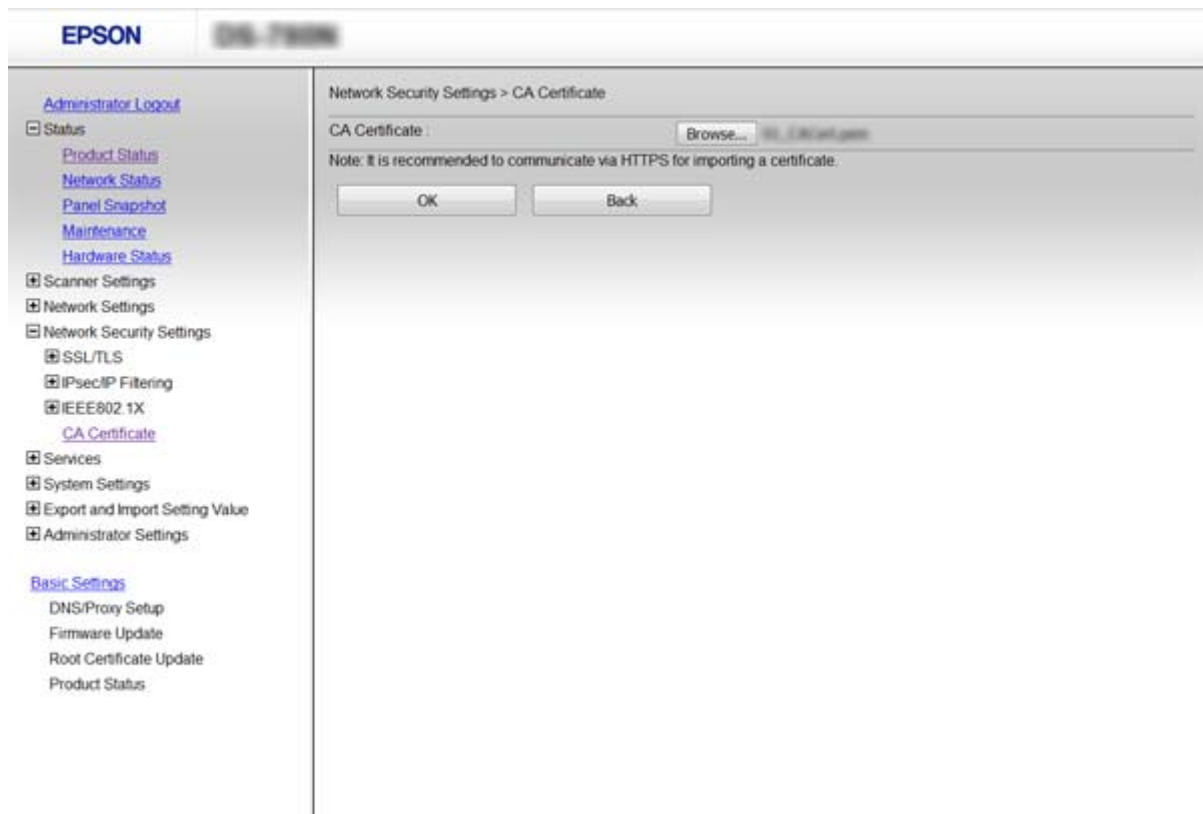
Možete uvesti, prikazati, izbrisati CA Certificate.

Uvoz CA Certificate

1. Pristupite programu Web Config i odaberite **Network Security Settings > CA Certificate**.
2. Pritisnite **Import**.

Napredne postavke sigurnosti za tvrtku

3. Odredite CA Certificate koji želite uvesti.



4. Pritisnite **OK**.

Po dovršetku uvoza, vratit ćete se na zaslon **CA Certificate** i prikazat će se uvezeni CA Certificate.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

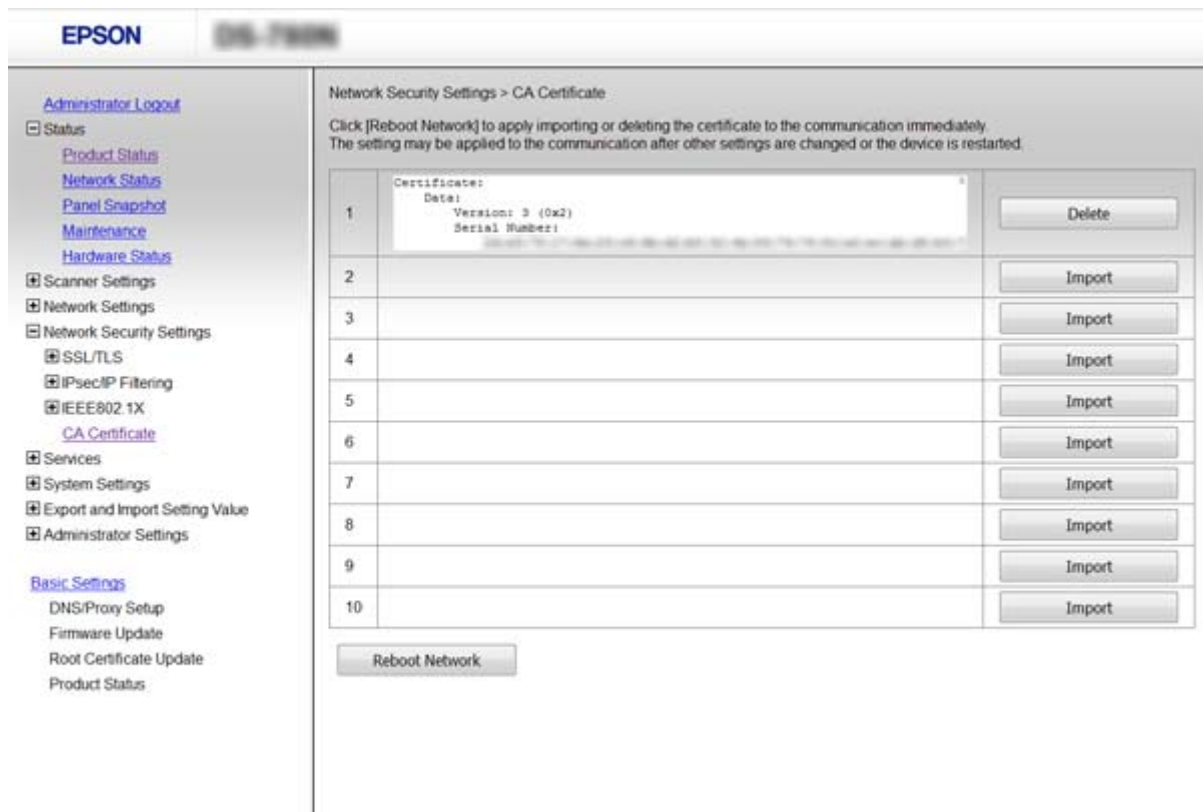
Brisanje CA Certificate

Možete izbrisati uvezeni CA Certificate.

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

Napredne postavke sigurnosti za tvrtku

- Kliknite **Delete** pored CA Certificate kojeg želite izbrisati.



- U prikazanoj poruci potvrdite da želite izbrisati certifikat.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Kriptirana komunikacija korištenjem IPsec/IP filtriranja

O aplikaciji IPsec/IP Filtering

Ako skener podržava IPsec/IP filtriranje, možete filtrirati promet na temelju IP adresa, usluga i porta. Kombiniranjem filtriranja možete konfigurirati skener tako da prihvati ili blokira određene klijente i podatke. Osim toga, možete poboljšati razinu sigurnosti korištenjem IPsec-a.

Za filtriranje prometa konfigurirajte zadana pravila. Zadana pravila primjenjuju se na svakog korisnika ili grupu koja se spaja na skener. Za finije kontrole korisnika i grupa korisnika konfigurirajte grupna pravila. Grupna pravila su jedno ili više pravila koja se primjenjuju za korisnika ili grupu korisnika. Skener kontrolira IP pakete koji se podudaraju s konfiguriranim pravilima. IP paketi su autentificirani u poretku grupnih pravila 1 do 10, zatim u poretku zadanih pravila.

Napomena:

Računala s operativnim sustavom Windows Vista ili novijim ili Windows Server 2008 ili novijim podržavaju IPsec.

Konfiguriranje stavke Default Policy

1. Pristupite programu Web Config i odaberite **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Unesite vrijednost za svaku stavku.
3. Pritisnite **Next**.
Prikazuje se poruka potvrde.
4. Pritisnite **OK**.
Skener se ažurira.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Postavljanje stavki za Default Policy” na strani 72](#)

Postavljanje stavki za Default Policy

The screenshot shows the Epson Web Config interface. The breadcrumb navigation is **Network Security Settings > IPsec/IP Filtering > Basic**. Below the breadcrumb, it states: "Each policy is applied with following priorities: Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy". There are 10 tabs labeled 1 through 10, with "Default Policy" selected. The main configuration area is titled "Default Policy" and includes the following settings:

- IPsec/IP Filtering:** Enable Disable
- Default Policy:**
 - Access Control:** IPsec
 - IKE Version:** IKEv1 IKEv2
 - Authentication Method:** Pre-Shared Key
 - Pre-Shared Key:** [Text input field]
 - Confirm Pre-Shared Key:** [Text input field]
 - Encapsulation:** Transport Mode
 - Remote Gateway(Tunnel Mode):** [Text input field]
 - Security Protocol:** ESP
- Algorithm Settings:**
 - IKE:**
 - Encryption:** Any
 - Authentication:** Any
 - Key Exchange:** Any
 - ESP:**
 - Encryption:** Any
 - Authentication:** Any

Stavke	Postavke i objašnjenje
IPsec/IP Filtering	Možete omogućiti ili onemogućiti značajku IPsec/IP filtriranja.

Napredne postavke sigurnosti za tvrtku

Stavke	Postavke i objašnjenje	
Access Control	Konfigurirajte metodu kontrole prometa za IP pakete.	
	Permit Access	Odaberite ovo za dopuštenje prolaza konfiguriranim IP paketima.
	Refuse Access	Odaberite ovo za odbijanje prolaza konfiguriranim IP paketima.
	IPsec	Odaberite ovo za dopuštenje prolaza konfiguriranim IPsec paketima.
IKE Version	Odaberite IKEv1 ili IKEv2 za IKE verziju. Odaberite jedan njih sukladno uređaju na koji je spojen skener.	
IKEv1	Sljedeće stavke prikazane su ako odaberete IKEv1 za IKE Version .	
	Authentication Method	Kako biste mogli odabrati Certificate , trebate unaprijed nabaviti i uvesti certifikat koji je potpisalo tijelo za izdavanje certifikata (CA).
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.
IKEv2	Sljedeće stavke prikazane su ako odaberete IKEv2 za IKE Version .	
Local	Authentication Method	Kako biste mogli odabrati Certificate , trebate unaprijed nabaviti i uvesti certifikat koji je potpisalo tijelo za izdavanje certifikata (CA).
	ID Type	Odaberite tip ID-a skenera.
	ID	Unesite ID skenera koji odgovara vrsti ID-a. Ne možete koristiti „@“, „#“ i „=“ kao prvi znak. Distinguished Name: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „=“. IP Address: unesite IPv4 ili IPv6 format. FQDN: unesite kombinaciju između 1 i 255 znakova koristeći A–Z, a–z, 0–9, „-“ i točku (.). Email Address: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „@“. Key ID: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka.
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.

Napredne postavke sigurnosti za tvrtku

Stavke	Postavke i objašnjenje	
Remote	Authentication Method	Kako biste mogli odabrati Certificate , trebate unaprijed nabaviti i uvesti certifikat koji je potpisalo tijelo za izdavanje certifikata (CA).
	ID Type	Odaberite vrstu ID-a za uređaj koji želite provjeriti.
	ID	Unesite ID skenera koji odgovara vrsti ID-a. Ne možete koristiti „@“, „#“ i „=“ kao prvi znak. Distinguished Name: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „=“. IP Address: unesite IPv4 ili IPv6 format. FQDN: unesite kombinaciju između 1 i 255 znakova koristeći A–Z, a–z, 0–9, „-“ i točku (.). Email Address: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „@“. Key ID: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka.
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.
Encapsulation	Ako odaberete IPsec za Access Control , trebate konfigurirati način skrivanja podataka („encapsulation“).	
	Transport Mode	Ako koristite samo skener u istoj LAN mreži, odaberite ovo. IP paketi sloja 4 ili kasniji su kriptirani.
	Tunnel Mode	Ako koristite skener na mreži s pristupom internetu, kao što je IPsec-VPN, odaberite ovu opciju. Zaglavlje („header“) i podaci IP paketa su kriptirani.
Remote Gateway(Tunnel Mode)	Ako odaberete Tunnel Mode za Encapsulation , unesite adresu pristupnika duljine od 1 do 39 znakova.	
Security Protocol	IPsec za Access Control , odaberite opciju.	
	ESP	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka te kako biste kriptirali podatke.
	AH	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka. Čak i ako je kriptiranje podataka zabranjeno, možete koristiti IPsec.
Algorithm Settings		
IKE	Encryption	Odaberite algoritam enkripcije za IKE. Stavke se razlikuju ovisno o verziji IKE-a.
	Authentication	Odaberite algoritam za provjeru autentičnosti za IKE.
	Key Exchange	Odaberite algoritam zamjene ključa za IKE. Stavke se razlikuju ovisno o verziji IKE-a.

Napredne postavke sigurnosti za tvrtku

Stavke	Postavke i objašnjenje	
ESP	Encryption	Odaberite algoritam enkripcije za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
	Authentication	Odaberite algoritam za provjeru autentičnosti za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
AH	Authentication	Odaberite algoritam enkripcije za AH. To će biti dostupno kada AH bude odabran za Security Protocol .

Povezane informacije

➔ [“Konfiguriranje stavke Default Policy” na strani 72](#)

Konfiguriranje stavke Group Policy

1. Pristupite programu Web Config i odaberite **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Kliknite na karticu označenu brojem koju želite konfigurirati.
3. Unesite vrijednost za svaku stavku.
4. Pritisnite **Next**.
Prikazuje se poruka potvrde.
5. Pritisnite **OK**.
Skener se ažurira.

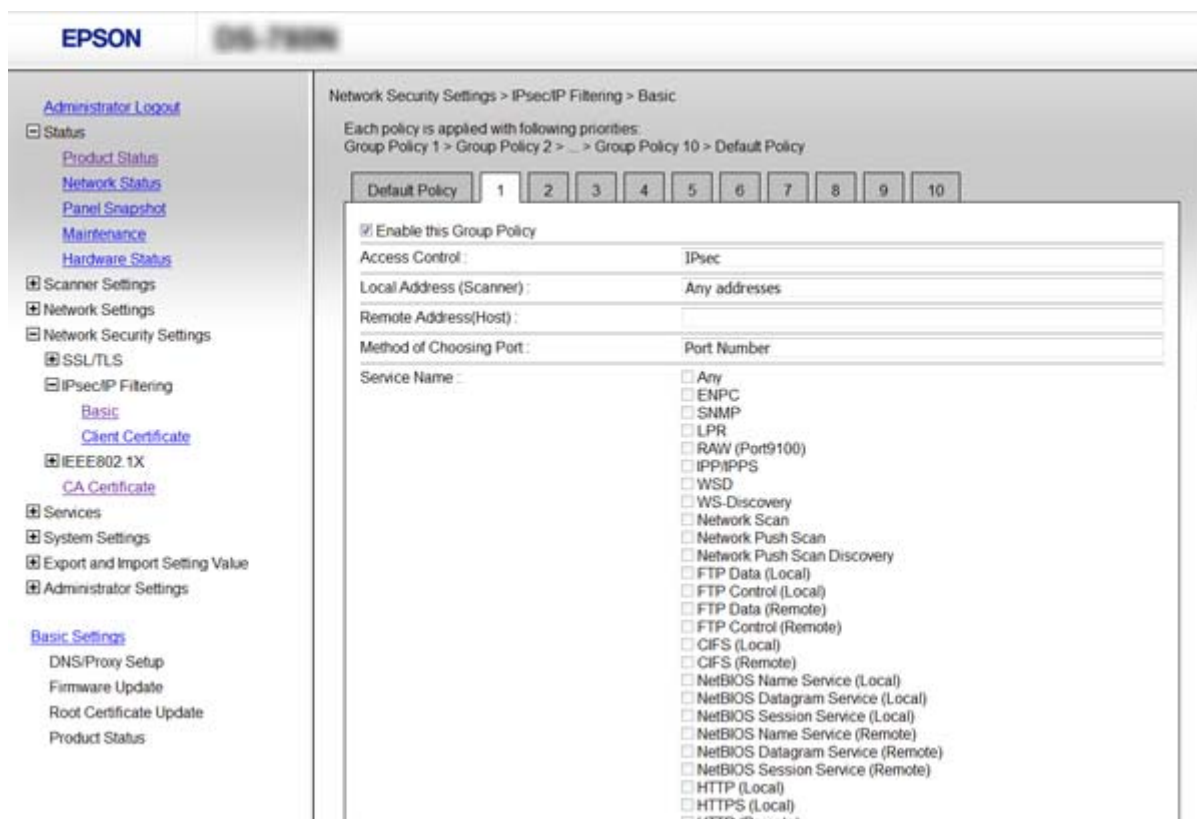
Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

➔ [“Postavljanje stavki za Group Policy” na strani 76](#)

Napredne postavke sigurnosti za tvrtku

Postavljanje stavki za Group Policy



Stavke	Postavke i objašnjenje	
Enable this Group Policy	Možete omogućiti ili onemogućiti grupna pravila.	
Access Control	Konfigurirajte metodu kontrole prometa za IP pakete.	
	Permit Access	Odaberite ovo za dopuštenje prolaza konfiguriranim IP paketima.
	Refuse Access	Odaberite ovo za odbijanje prolaza konfiguriranim IP paketima.
	IPsec	Odaberite ovo za dopuštenje prolaza konfiguriranim IPsec paketima.
Local Address (Scanner)	Odaberite IPv4 ili IPv6 adresu koja odgovara okruženju vaše mreže. Ako je IP adresa dodijeljena automatski, možete odabrati Use auto-obtained IPv4 address .	
Remote Address(Host)	Unesite IP adresu uređaja za kontrolu pristupa. IP adresa mora sadržavati najviše 43 znaka. Ako ne unesete IP adresu, sve će se adrese kontrolirati. Napomena: Ako je IP adresa dodijeljena automatski (npr. ako ju je dodijelio DHCP), veza možda neće biti dostupna. Konfigurirajte statičnu IP adresu.	
Method of Choosing Port	Odaberite način određivanja ulaza.	
Service Name	Ako odaberete Service Name za Method of Choosing Port , odaberite opciju.	

Napredne postavke sigurnosti za tvrtku

Stavke	Postavke i objašnjenje	
Transport Protocol	Ako odaberete Port Number za Method of Choosing Port , trebate konfigurirati način skrivanja podataka („encapsulation“).	
	Any Protocol	Odaberite ovo za kontroliranje svih vrsta protokola.
	TCP	Odaberite ovo za kontroliranje podataka za jednosmjerni prijenos („unicast“).
	UDP	Odaberite ovo za kontrolu podataka za emitiranje („broadcast“) i ciljano emitiranje („multicast“).
ICMPv4	Odaberite ovo za kontrolu ping naredbe.	
Local Port	Ako odaberete Port Number za Method of Choosing Port i ako odaberete TCP ili UDP za Transport Protocol , unesite brojeve ulaza za provjeru primanja paketa i odvojite ih zarezima. Možete unijeti maksimalno 10 brojeva ulaza. Primjer: 20,80,119,5220 Ako ne unesete broj ulaza, svi ulazi se kontroliraju.	
Remote Port	Ako odaberete Port Number za Method of Choosing Port i ako odaberete TCP ili UDP za Transport Protocol , unesite brojeve ulaza za provjeru slanja paketa i odvojite ih zarezima. Možete unijeti maksimalno 10 brojeva ulaza. Primjer: 25,80,143,5220 Ako ne unesete broj ulaza, svi ulazi se kontroliraju.	
IKE Version	Odaberite IKEv1 ili IKEv2 za IKE verziju. Odaberite jedan njih sukladno uređaju na koji je spojen skener.	
IKEv1	Sljedeće stavke prikazane su ako odaberete IKEv1 za IKE Version .	
	Authentication Method	Ako odaberete IPsec za Access Control , odaberite opciju. Korišteni certifikat je uobičajen sa zadanim pravilima.
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.
IKEv2	Sljedeće stavke prikazane su ako odaberete IKEv2 za IKE Version .	

Napredne postavke sigurnosti za tvrtku

Stavke	Postavke i objašnjenje	
Local	Authentication Method	Ako odaberete IPsec za Access Control , odaberite opciju. Korišteni certifikat je uobičajen sa zadanim pravilima.
	ID Type	Odaberite tip ID-a skenera.
	ID	<p>Unesite ID skenera koji odgovara vrsti ID-a.</p> <p>Ne možete koristiti „@“, „#“ i „=“ kao prvi znak.</p> <p>Distinguished Name: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „=“.</p> <p>IP Address: unesite IPv4 ili IPv6 format.</p> <p>FQDN: unesite kombinaciju između 1 i 255 znakova koristeći A–Z, a–z, 0–9, „-“ i točku (.).</p> <p>Email Address: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „@“.</p> <p>Key ID: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka.</p>
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.
Remote	Authentication Method	Ako odaberete IPsec za Access Control , odaberite opciju. Korišteni certifikat je uobičajen sa zadanim pravilima.
	ID Type	Odaberite vrstu ID-a za uređaj koji želite provjeriti.
	ID	<p>Unesite ID skenera koji odgovara vrsti ID-a.</p> <p>Ne možete koristiti „@“, „#“ i „=“ kao prvi znak.</p> <p>Distinguished Name: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „=“.</p> <p>IP Address: unesite IPv4 ili IPv6 format.</p> <p>FQDN: unesite kombinaciju između 1 i 255 znakova koristeći A–Z, a–z, 0–9, „-“ i točku (.).</p> <p>Email Address: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka. Trebate uključiti „@“.</p> <p>Key ID: unesite 1 do 128 1-bajtna ASCII (0x20 do 0x7E) znaka.</p>
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.

Napredne postavke sigurnosti za tvrtku

Stavke	Postavke i objašnjenje	
Encapsulation	Ako odaberete IPsec za Access Control , trebate konfigurirati način skrivanja podataka („encapsulation“).	
	Transport Mode	Ako koristite samo skener u istoj LAN mreži, odaberite ovo. IP paketi sloja 4 ili kasniji su kriptirani.
	Tunnel Mode	Ako koristite skener na mreži s pristupom internetu, kao što je IPsec-VPN, odaberite ovu opciju. Zaglavlje („header“) i podaci IP paketa su kriptirani.
Remote Gateway(Tunnel Mode)	Ako odaberete Tunnel Mode za Encapsulation , unesite adresu pristupnika duljine od 1 do 39 znakova.	
Security Protocol	Ako odaberete IPsec za Access Control , odaberite opciju.	
	ESP	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka te kako biste kriptirali podatke.
	AH	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka. Čak i ako je kriptiranje podataka zabranjeno, možete koristiti IPsec.
Algorithm Settings		
IKE	Encryption	Odaberite algoritam enkripcije za IKE. Stavke se razlikuju ovisno o verziji IKE-a.
	Authentication	Odaberite algoritam za provjeru autentičnosti za IKE.
	Key Exchange	Odaberite algoritam zamjene ključa za IKE. Stavke se razlikuju ovisno o verziji IKE-a.
ESP	Encryption	Odaberite algoritam enkripcije za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
	Authentication	Odaberite algoritam za provjeru autentičnosti za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
AH	Authentication	Odaberite algoritam za provjeru autentičnosti za AH. To će biti dostupno kada AH bude odabran za Security Protocol .

Povezane informacije

- ➔ [“Konfiguriranje stavke Group Policy” na strani 75](#)
- ➔ [“Kombinacija stavki Local Address \(Scanner\) i Remote Address\(Host\) na opciji Group Policy” na strani 80](#)
- ➔ [“Reference naziva usluga na značajci Group Policy \(Pravila grupe\)” na strani 80](#)

Napredne postavke sigurnosti za tvrtku

Kombinacija stavki Local Address (Scanner) i Remote Address(Host) na opciji Group Policy

		Postavljanje stavke Local Address (Scanner)		
		IPv4	IPv6* ²	Any addresses* ³
Postavljanje stavke Remote Address(Host)	IPv4* ¹	✓	–	✓
	IPv6* ¹ , * ²	–	✓	✓
	Prazno	✓	✓	✓

*1 Ako se odabere **IPsec za Access Control**, nije moguće specificirati duljinu prefiksa.

*2 Ako se odabere **IPsec za Access Control**, moguće je odabrati lokalnu adresu na razini poveznice (fe80::), no pravila grupe bit će onemogućena.

*3 To ne vrijedi samo za IPv6 lokalne adrese na razini poveznice.

Reference naziva usluga na značajki Group Policy (Pravila grupe)

Napomena:

Nedostupne usluge prikazuju se, no ne mogu se odabrati.

Naziv usluge	Vrsta protokola	Broj lokalnog priključka	Broj udaljenog priključka	Kontrolirane značajke
Any	–	–	–	Sve usluge
ENPC	UDP	3289	Bilo koji ulaz	Pretraživanje skenera iz aplikacija kao što je EpsonNet Config i upravljačkog programa skenera
SNMP	UDP	161	Bilo koji ulaz	Dobivanje i konfiguriranje MIB-a iz aplikacija kao što je EpsonNet Config i Epson upravljačkog programa skenera
WSD	TCP	Bilo koji ulaz	5357	Kontroliranje WSD-a
WS-Discovery	UDP	3702	Bilo koji ulaz	Pretraživanje skenera iz WSD-a
Network Scan	TCP	1865	Bilo koji ulaz	Preusmjeravanje skeniranih podataka iz Document Capture Pro
Network Push Scan Discovery	UDP	2968	Bilo koji ulaz	Traženje računala preko skenera.
Network Push Scan	TCP	Bilo koji ulaz	2968	Informacije o postupku zaprimanja brzog skeniranja iz aplikacije Document Capture Pro ili Document Capture
HTTP (Local)	TCP	80	Bilo koji ulaz	HTTP(S) poslužitelj (preusmjeravanje podataka aplikacije Web Config i WSD)
HTTPS (Local)	TCP	443	Bilo koji ulaz	

Napredne postavke sigurnosti za tvrtku

Naziv usluge	Vrsta protokola	Broj lokalnog priključka	Broj udaljenog priključka	Kontrolirane značajke
HTTP (Remote)	TCP	Bilo koji ulaz	80	HTTP(S) klijent (komunikacija između ažuriranja firmvera i ažuriranja korijenskog certifikata)
HTTPS (Remote)	TCP	Bilo koji ulaz	443	

Primjeri konfiguracije za IPsec/IP Filtering

Samo za dolazne IPsec pakete

Ovaj primjer je samo za konfiguriranje zadanih pravila.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: IPsec
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: Unesite najviše 127 znakova.

Group Policy:

Nemojte konfigurirati.

Prihvatanje skena koristeći Epson Scan 2 i postavke skenera

Ovaj primjer omogućava komunikaciju podataka o skeniranju i konfiguracije skenera s određenih usluga.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Označite okvir.
- Access Control: Permit Access
- Remote Address(Host): IP adresa klijenta
- Method of Choosing Port: Service Name
- Service Name: Označite okvir za ENPC, SNMP, Network Scan, HTTP (Local) i HTTPS (Local).

Dobivanje pristupa samo s određene IP adrese

Ovaj primjer određenoj IP adresi omogućuje pristup skeneru.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Označite okvir.
- Access Control: Permit Access
- Remote Address(Host): IP adresa klijenta administratora

Napredne postavke sigurnosti za tvrtku

Napomena:

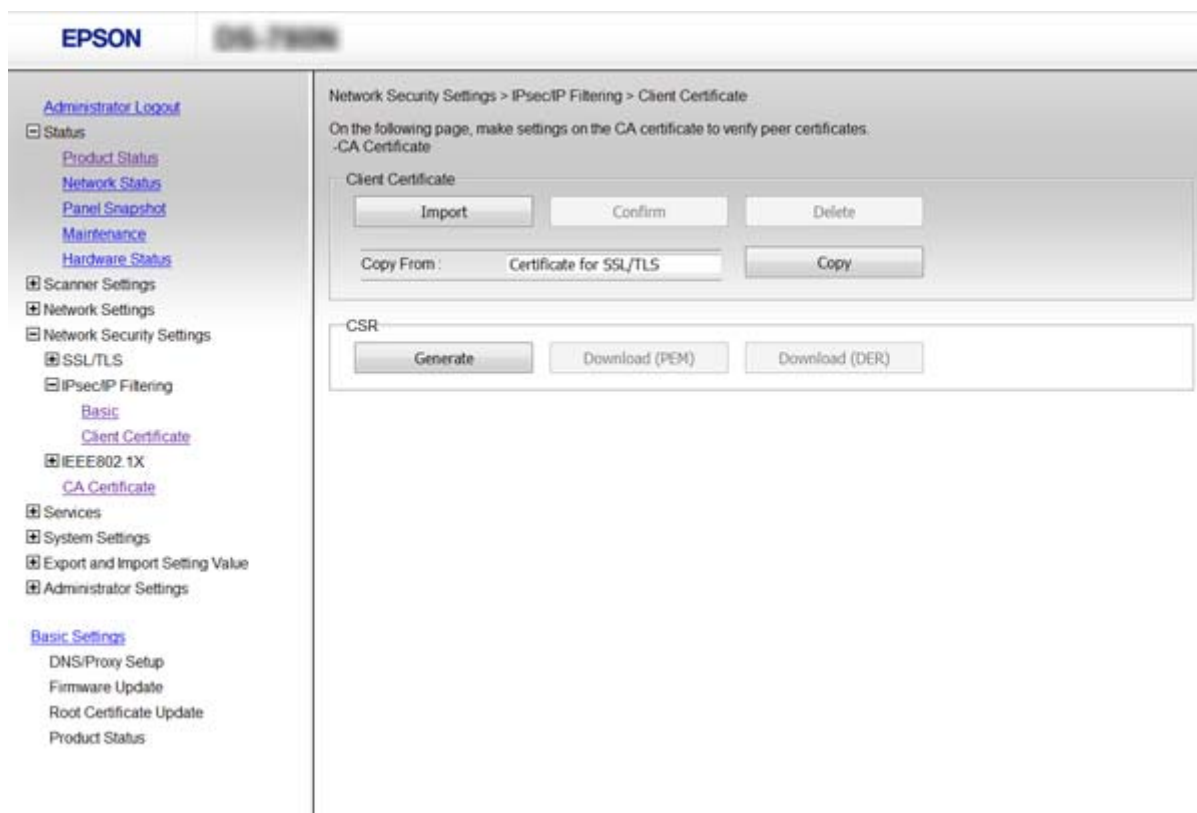
Bez obzira na konfiguraciju pravila, klijent će moći pristupiti skeneru i konfigurirati ga.

Konfiguriranje certifikata za IPsec/IP Filtering

Konfigurirajte certifikat klijenta za IPsec/IP filtriranje. Ako želite konfigurirati tijelo za izdavanje certifikata, uđite u **CA Certificate**.

1. Pristupite programu Web Config i odaberite **Network Security Settings > IPsec/IP Filtering > Client Certificate**.
2. Uvezite certifikat u **Client Certificate**.

Ako ste već uvezli certifikat kojeg je izdalo tijelo za izdavanje certifikata u IEEE802.1X ili SSL/TLS, moći ćete kopirati certifikat i koristiti ga u IPsec/IP filtriranju. Za kopiranje odaberite certifikat u **Copy From** pa kliknite **Copy**.



Povezane informacije

- ➔ “Pristup aplikaciji Web Config” na strani 23
- ➔ “Pribavljanje i uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA)” na strani 64

Upotreba SNMPv3 protokola

O protokolu SNMPv3

SNMP je protokol koji izvršava nadzor i upravljanje u svrhu prikupljanja informacija o uređajima povezanim s mrežom. SNMPv3 je poboljšana verzija sigurnosne značajke upravljačkog sustava.

Pri korištenju protokola SNMPv3, nadziranje stanja i promjene postavki SNMP komunikacije (paketa) mogu se odobriti i kriptirati radi zaštite SNMP komunikacije (paketa) od mrežnih opasnosti, kao što su nadziranje komunikacije, lažno predstavljanje i falsificiranje.

Konfiguriranje protokola SNMPv3

Ako skener podržava protokol SNMPv3, možete nadgledati i upravljati pristupom skeneru.

1. Pristupite programu Web Config i odaberite **Services > Protocol**.
2. Unesite vrijednost za svaku stavku opcije **SNMPv3 Settings**.
3. Pritisnite **Next**.
Prikazuje se poruka potvrde.
4. Pritisnite **OK**.
Skener se ažurira.

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Stavke podešavanja za SNMPv3” na strani 84](#)

Napredne postavke sigurnosti za tvrtku

Stavke podešavanja za SNMPv3

The screenshot shows the 'SNMPv3 Settings' section of the EPSON network security configuration. It includes the following fields and options:

- Enable SNMPv3:** Checked.
- User Name:** admin
- Authentication Settings:**
 - Algorithm: MD5
 - Password: [empty]
 - Confirm Password: [empty]
- Encryption Settings:**
 - Algorithm: DES
 - Password: [empty]
 - Confirm Password: [empty]
- Context Name:** EPSON

Stavke	Postavke i objašnjenje
Enable SNMPv3	SNMPv3 će biti omogućeno kada se označi potvrdni okvir.
User Name	Unesite između 1 i 32 znaka pomoću znakova od 1 bajta.
Authentication Settings	
Algorithm	Odaberite algoritam za provjeru autentičnosti.
Password	Unesite između 8 i 32 znakova u ASCII (0x20-0x7E).
Confirm Password	Unesite konfiguriranu lozinku za potvrdu.
Encryption Settings	
Algorithm	Odaberite algoritam za šifriranje.
Password	Unesite između 8 i 32 znakova u ASCII (0x20-0x7E).
Confirm Password	Unesite konfiguriranu lozinku za potvrdu.
Context Name	Unesite između 1 i 32 znaka pomoću znakova od 1 bajta.

Povezane informacije

➔ [“Konfiguriranje protokola SNMPv3” na strani 83](#)

Spajanje skenera s IEEE802.1X mrežom

Konfiguriranje IEEE802.1X mreže

Ako skener podržava IEEE802.1X, možete ga koristiti u mreži s provjerom autentičnosti koja je spojena s RADIUS poslužiteljem i čvorištem kao jedinicom za provjeru autentičnosti.

1. Pristupite programu Web Config i odaberite **Network Security Settings > IEEE802.1X > Basic**.
2. Unesite vrijednost za svaku stavku.
3. Kliknite na **Next**.
Prikazuje se poruka potvrde.
4. Kliknite na **OK**.
Skener se ažurira.

Povezane informacije

- ➔ “Pristup aplikaciji Web Config” na strani 23
- ➔ “Stavke za postavljanje IEEE802.1X mreže” na strani 85
- ➔ “Pristup pisaču ili skeneru nije moguć nakon konfiguriranja mreže IEEE802.1X” na strani 90

Stavke za postavljanje IEEE802.1X mreže

The screenshot shows the Epson Web Config interface for configuring IEEE802.1X settings. The left sidebar contains a navigation menu with options like Administrator Logout, Status, Product Status, Network Status, Panel Snapshot, Maintenance, Hardware Status, Scanner Settings, Network Settings, Network Security Settings (expanded), SSL/TLS, IPsec/IP Filtering, IEEE802.1X (expanded), Basic (selected), Client Certificate, CA Certificate, Services, System Settings, Export and Import Setting Value, and Administrator Settings. Under Basic Settings, there are links for DNS/Proxy Setup, Firmware Update, Root Certificate Update, and Product Status.

The main content area is titled "Network Security Settings > IEEE802.1X > Basic". It contains the following configuration options:

- IEEE802.1X (Wired LAN): Enable Disable
- EAP Type: EAP-TLS
- User ID: [Text Input Field]
- Password: [Text Input Field]
- Confirm Password: [Text Input Field]
- Server ID: [Text Input Field]
- Certificate Validation: Enable Disable
- Anonymous Name: [Text Input Field]
- Encryption Strength: Middle

At the bottom of the configuration area, there is a "Next" button.

Napredne postavke sigurnosti za tvrtku

Stavke	Postavke i objašnjenje	
IEEE802.1X (Wired LAN)	Možete omogućiti ili onemogućiti postavke stranice (IEEE802.1X > Basic) za IEEE802.1X (žičani LAN).	
EAP Type	Odaberite opciju za način provjere autentičnosti između skenera i RADIUS poslužitelja.	
	EAP-TLS	Trebate pribaviti i uvesti certifikat s potpisom CA.
	PEAP-TLS	
	PEAP/MSCHAPv2	Trebate postaviti lozinku.
User ID	Konfigurirajte ID za korištenje provjere autentičnosti poslužitelja RADIUS. Unesite 1 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova.	
Password	Konfigurirajte lozinku za provjeru autentičnosti skenera. Unesite 1 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova. Ako Windows poslužitelj koristite kao RADIUS poslužitelj, moći ćete unijeti do 127 znakova.	
Confirm Password	Za potvrdu unesite lozinku koju ste postavili.	
Server ID	Možete konfigurirati ID poslužitelja za provjeru autentičnosti s određenim poslužiteljem RADIUS. Jedinica za provjeru autentičnosti potvrđuje sadrži li polje subject/subjectAltName certifikata poslužitelja ID poslužitelja poslan s poslužitelja RADIUS. Unesite 0 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova.	
Certificate Validation	Provjeru valjanosti certifikata možete postaviti neovisno o načinu provjere autentičnosti. Uvezite certifikat u CA Certificate .	
Anonymous Name	Ako odaberete PEAP-TLS ili PEAP/MSCHAPv2 za Authentication Method , možete postaviti anonimno ime umjesto korisničkog ID-a za fazu 1 PEAP provjere autentičnosti. Unesite 0 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova.	
Encryption Strength	Možete odabrati nešto od sljedećeg.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Povezane informacije

➔ [“Konfiguriranje IEEE802.1X mreže” na strani 85](#)

Konfiguriranje certifikata za IEEE802.1X

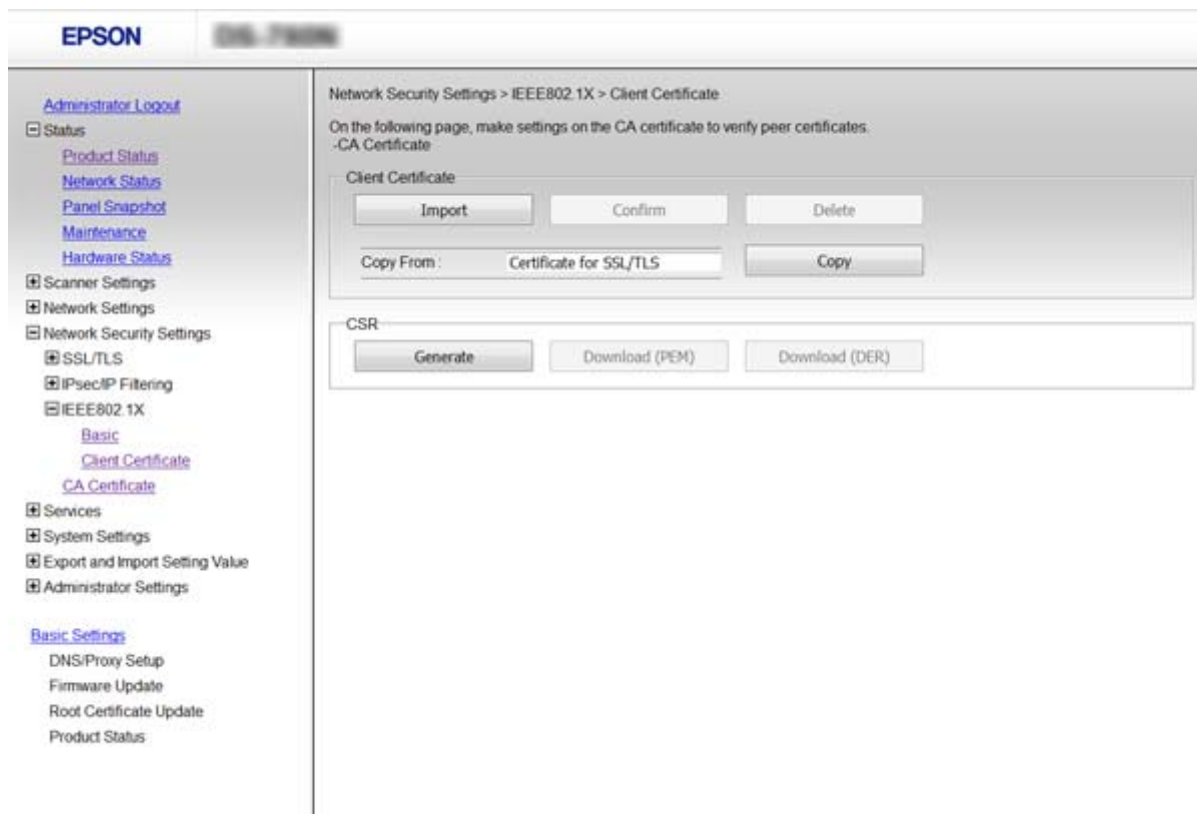
Konfigurirajte certifikat klijenta za IEEE802.1X. Ako želite konfigurirati tijelo za izdavanje certifikata, udite u **CA Certificate**.

1. Pristupite programu Web Config i odaberite **Network Security Settings > IEEE802.1X > Client Certificate**.

Napredne postavke sigurnosti za tvrtku

2. Certifikat unesite u **Client Certificate**.

Certifikat možete kopirati ako ga je izdalo tijelo za izdavanje certifikata. Za kopiranje odaberite certifikat u **Copy From** pa kliknite **Copy**.



Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Pribavljanje i uvoz certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 64](#)

Rješavanje problema napredne sigurnosti

Vraćanje sigurnosnih postavki

Kada uspostavite vrlo sigurno okruženje kao što je IPsec/IP filtriranje ili IEEE802.1X, možda nećete moći komunicirati s uređajima zbog neispravnih postavki ili problema s uređajem ili poslužiteljem. U tom slučaju, vratite sigurnosne postavke kako biste ponovno odabrali postavke uređaja ili kako biste ga mogli privremeno koristiti.

Onemogućavanje sigurnosne funkcije preko upravljačke ploče

Možete onemogućiti IPsec/IP filtriranje ili IEEE802.1X preko upravljačke ploče skenera.

1. Dodirnite **Postavke > Postavke mreže**.

Napredne postavke sigurnosti za tvrtku

2. Dodirnite **Promijeni postavke**.
3. Dodirnite stavke koje želite onemogućiti.
 - IPsec/IP filtriranje
 - IEEE802.1X
4. Kada se prikaže poruka o dovršetku, dodirnite **Nastavi**.

Vraćanje sigurnosne funkcije korištenjem programa Web Config

Za protokol IEEE802.1X uređaji možda neće biti prepoznati na mreži. U tom slučaju onemogućite funkciju putem upravljačke ploče skenera.

Kod IPsec/IP filtriranja možete onemogućiti funkciju ako možete pristupiti uređaju preko računala.

Onemogućavanje IPsec/IP filtriranja koristeći funkciju Web Config

1. Pristupite programu Web Config i odaberite **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Odaberite **Disable** za **IPsec/IP Filtering** pod stavkom **Default Policy**.
3. Kliknite **Next** i zatim uklonite **Enable this Group Policy** za sva skupna pravila.
4. Kliknite na **OK**.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Problemi s korištenjem sigurnosnih značajki mreže

Zaboravljen je unaprijed postavljeni zajednički ključ

Ponovno konfigurirajte ključ pomoću aplikacije Web Config.

Kako biste promijenili ključ, pristupite programu Web Config i odaberite **Network Security Settings > IPsec/IP Filtering > Basic > Default Policy** ili **Group Policy**.

Ako promijenite prethodno otkriveni ključ, konfigurirajte prethodno otkriveni ključ za računala.

Povezane informacije

➔ [“Pristup aplikaciji Web Config” na strani 23](#)

Ne mogu komunicirati s IPsec komunikacijom

Koristite li za postavke računala algoritam koji nije podržan?

Skener podržava sljedeće algoritme.

Sigurnosne metode	Algoritmi
IKE algoritam enkripcije	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE algoritam za provjeru autentičnosti	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE algoritam zamjene tipke	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 enkripcije	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP algoritam za provjeru autentičnosti	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH algoritam za provjeru autentičnosti	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* dostupno samo za IKEv2

Povezane informacije

➔ [“Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 71](#)

Iznenadna nemogućnost komunikacije

Je li IP adresa skenera neispravna ili izmijenjena?

Onemogućite IPsec preko upravljačke ploče skenera.

Ako je DHCP zastario, kod ponovnog pokretanja ili je IPv6 adresa zastarjela ili nije pribavljena, IP adresa prijavljena za program skenera Web Config (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Local Address (Scanner)**).

Koristite statičnu IP adresu.

Je li IP adresa računala valjana ili izmijenjena?

Onemogućite IPsec preko upravljačke ploče skenera.

Ako je DHCP zastario, kod ponovnog pokretanja ili je IPv6 adresa zastarjela ili nije pribavljena, IP adresa prijavljena za program skenera Web Config (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Remote Address(Host)**).

Koristite statičnu IP adresu.

Napredne postavke sigurnosti za tvrtku

Povezane informacije

- ➔ [“Pristup aplikaciji Web Config” na strani 23](#)
- ➔ [“Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 71](#)

Nije moguće povezivanje nakon konfiguriranja IPsec/IP filtriranja

Postavljena vrijednost možda je netočna.

Onemogućite IPsec/IP filtriranje na upravljačkoj ploči skenera. Povežite skener i računalo pa ponovno podesite postavke za IPsec/IP filtriranje.

Povezane informacije

- ➔ [“Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 71](#)

Pristup pisaču ili skeneru nije moguć nakon konfiguriranja mreže IEEE802.1X

Postavke možda nisu ispravne.

Onemogućite IEEE802.1X na upravljačkoj ploči skenera. Povežite skener i računalo, a zatim ponovno konfigurirajte IEEE802.1X.

Povezane informacije

- ➔ [“Konfiguriranje IEEE802.1X mreže” na strani 85](#)

Problemi s korištenjem digitalnog certifikata

Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata (CA) nije moguć

Podudaraju li se certifikat potpisan od strane tijela za izdavanje digitalnih certifikata (CA) i informacije na zahtjevu za potpisivanje certifikata?

Ako certifikat potpisan od strane tijela za izdavanje digitalnih certifikata i zahtjev za potpisivanje certifikata ne sadrže iste informacije, zahtjev za potpisivanje certifikata se ne može uvesti. Označite sljedeće:

- Pokušavate li uvesti certifikat na uređaj koji nema iste informacije?

Provjerite informacije na zahtjevu za potpisivanje certifikata, a zatim uvezite certifikat na uređaj koji sadrži iste informacije.

- Jeste li izbrisali zahtjev za potpisivanje certifikata pohranjen na skeneru nakon što ste ga poslali tijelu za izdavanje digitalnih certifikata?

Ponovno pribavite certifikat potpisan od strane tijela za izdavanje certifikata pomoću zahtjeva za potpisivanje certifikata.

Je li certifikat potpisan od strane tijela za izdavanje certifikata veći od 5 KB?

Ne možete uvesti certifikat potpisan od strane tijela za izdavanje certifikata koji je veći od 5 KB.

Napredne postavke sigurnosti za tvrtku

Je li lozinka za uvoz certifikata ispravna?

Ako zaboravite lozinku, ne možete uvesti certifikat.

Povezane informacije

➔ [“Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 66](#)

Ažuriranje samopotpisanog certifikata nije moguće

Je li unesen Common Name?

Common Name mora biti unesen.

Jesu li za Common Name uneseni znakovi koji nisu podržani? Na primjer, japanski nije podržan.

Unesite između 1 i 128 znakova u formatu IPv4, IPv6, naziva poslužitelja ili FQDN u ASCII kodu (0x20-0x7E).

Sadrži li Common Name zarez ili razmak?

Ako sadrži zarez, Common Name se na tom mjestu dijeli. Ako se unese samo razmak prije ili nakon zareza, dolazi do pogreške.

Povezane informacije

➔ [“Ažuriranje samopotpisanog certifikata” na strani 68](#)

Izrada zahtjeva za potpisivanje certifikata nije moguća

Je li unesen Common Name?

Common Name mora biti unesen.

Jesu li za Common Name, Organization, Organizational Unit, Locality, State/Province uneseni znakovi koji nisu podržani? Na primjer, japanski nije podržan.

Unesite znakove u formatu IPv4, IPv6, naziva poslužitelja ili FQDN u ASCII kodu (0x20-0x7E).

Sadrži li Common Name zarez ili razmak?

Ako sadrži zarez, Common Name se na tom mjestu dijeli. Ako se unese samo razmak prije ili nakon zareza, dolazi do pogreške.

Povezane informacije

➔ [“Pribavljanje certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 64](#)

Napredne postavke sigurnosti za tvrtku

Pojavljuje se upozorenje u vezi s digitalnim certifikatom

Poruke	Uzrok/što napraviti
Enter a Server Certificate.	<p>Uzrok: Niste odabrali datoteku za uvoz.</p> <p>Što napraviti: Odaberite datoteku i pritisnite Import.</p>
CA Certificate 1 is not entered.	<p>Uzrok: CA certifikat 1 nije unesen; unesen je samo certifikat CA 2.</p> <p>Što napraviti: Najprije unesite CA certifikat 1.</p>
Invalid value below.	<p>Uzrok: Lokacija datoteke i/ili lozinka sadrži znakove koji nisu podržani.</p> <p>Što napraviti: Provjerite jesu li za stavku znakovi ispravno uneseni.</p>
Invalid date and time.	<p>Uzrok: Datum i vrijeme za skener nisu postavljeni.</p> <p>Što napraviti: Postavite datum i vrijeme pomoću Web Config ili EpsonNet Config.</p>
Invalid password.	<p>Uzrok: Lozinka unesena za CA certifikat i unesena lozinka se ne podudaraju.</p> <p>Što napraviti: Unesite ispravnu lozinku.</p>
Invalid file.	<p>Uzrok: Ne uvozite datoteku certifikata u formatu X509.</p> <p>Što napraviti: Provjerite odabirete li ispravan certifikat poslan od strane pouzdanog tijela za izdavanje certifikata.</p>
	<p>Uzrok: Datoteka koju ste uvezli je prevelika. Maksimalna veličina datoteke je 5 KB.</p> <p>Što napraviti: Ako ste odabrali ispravnu datoteku, certifikat je možda oštećen ili krivotvoren.</p>
	<p>Uzrok: Lanac u certifikatu nije valjan.</p> <p>Što napraviti: Dodatne informacije o certifikatu potražite na internetskoj stranici tijela koje izdaje digitalne certifikate.</p>

Napredne postavke sigurnosti za tvrtku

Poruke	Uzrok/što napraviti
Cannot use the Server Certificates that include more than three CA certificates.	<p>Uzrok: Datoteka certifikata u formatu PKCS#12 sadrži više od 3 CA certifikata.</p> <p>Što napraviti: Uvezite svaki certifikat konvertiran iz PKCS#12 formata u PEM format ili uvezite datoteku certifikata u PKCS#12 formatu koja sadrži najviše 2 CA certifikata.</p>
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p>Uzrok: Certifikat je istekao.</p> <p>Što napraviti:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ako je certifikat istekao, pribavite i uvezite novi. <input type="checkbox"/> Ako je certifikat istekao, provjerite jesu li datum i vrijeme skenera ispravno postavljeni.
Private key is required.	<p>Uzrok: Nema privatnog ključa uparenog s certifikatom.</p> <p>Što napraviti:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ako je format certifikata PEM/DER i dobili ste ga preko zahtjeva za potpisivanje certifikata pomoću računala, navedite datoteku privatnog ključa. <input type="checkbox"/> Ako je format certifikata PKCS#12 i dobili ste ga preko zahtjeva za potpisivanje certifikata pomoću računala, izradite datoteku koja sadrži privatni ključ.
	<p>Uzrok: Ponovno ste uvezli PEM/DER certifikat dobiven preko zahtjeva za potpisivanje certifikata pomoću aplikacije Web Config.</p> <p>Što napraviti: Ako je format certifikata PEM/DER i dobili ste ga preko zahtjeva za potpisivanje certifikata pomoću aplikacije Web Config, možete ga uvesti samo jednom.</p>
Setup failed.	<p>Uzrok: Konfiguriranje se ne može dovršiti, jer komunikacija između skenera i računala nije uspjela ili se datoteka ne može pročitati zbog pogrešaka.</p> <p>Što napraviti: Nakon što provjerite navedenu datoteku i komunikaciju, ponovno uvezite datoteku.</p>

Povezane informacije

➔ [“O digitalnom certificiranju” na strani 63](#)

Slučajno ste izbrisali certifikat potpisan od strane tijela za izdavanje certifikata

Postoji li sigurnosna kopija certifikata?

Ako imate sigurnosnu kopiju, ponovno uvezite certifikat.

Ako certifikat dobijete pomoću zahtjeva za potpisivanje certifikata izrađenog u aplikaciji Web Config, izbrisani certifikat ne možete više uvesti. Izradite zahtjev za potpisivanje certifikata ili pribavite novi certifikat.

Napredne postavke sigurnosti za tvrtku

Povezane informacije

- ➔ [“Brisanje certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 67](#)
- ➔ [“Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 66](#)