

DS-790WN

Vodič za administratore

Potrebna podešavanja koja odgovaraju nameni

Podešavanja mreže

Podešavanja potrebna za skeniranje

Osnovne bezbednosne postavke

Napredna bezbednosna podešavanja

Authentication Settings

Autorska prava

Nijedan deo ove publikacije ne sme se reprodukovati, uskladištiti u sistemu za preuzimanje ili prenositi u bilo kom obliku ili na bilo koji način: elektronski, mehanički, fotokopiranjem, snimanjem ili na drugi način, bez prethodne pismene dozvole korporacije Seiko Epson. Upotrebom informacija koje se nalaze u ovom dokumentu ne preuzima se nikakva odgovornost za patente. Ne preuzima se odgovornost ni za štete koje nastanu usled korišćenja informacija iz ovog dokumenta. Informacije navedene u ovom dokumentu su namenjene samo za upotrebu s ovim proizvodom kompanije Epson. Epson nije odgovoran za upotrebu ovih informacija s drugim proizvodima.

Korporacija Seiko Epson i njena povezana društva ne odgovaraju kupcu ovog proizvoda niti drugim licima za štetu, gubitke, potraživanja ili troškove nastale usled nezgode, nepravilne upotrebe ili zloupotrebe ovog proizvoda, neovlašćenih modifikacija, popravki ili izmena proizvoda i (osim u SAD) nedoslednog pridržavanja uputstava korporacije Seiko Epson za rad i održavanje proizvoda.

Korporacija Seiko Epson i njena povezana društva nisu odgovorni ni za kakvu štetu ili probleme nastale usled korišćenja opcionih ili potrošnih proizvoda koje korporacija Seiko Epson nije označila kao originalne Epsonove proizvode oznakom Original Epson Products ili odobrene Epsonove proizvode oznakom Epson Approved Products.

Korporacija Seiko Epson nije odgovorna ni za kakvu štetu nastalu usled elektromagnetnih smetnji do kojih dolazi zbog korišćenja interfejs kablova koje korporacija Seiko Epson nije označila kao odobrene Epsonove proizvode oznakom Epson Approved Products.

© 2021 Seiko Epson Corporation

Sadržaj ovog priručnika i specifikacije ovog proizvoda podložni su promenama bez prethodne najave.

Zaštitni znakovi

- ❑ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION i njihovi logotipi su zaštitni znakovi ili registrovani zaštitni znakovi kompanije Seiko Epson.
- ❑ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❑ Chrome is a trademark of Google LLC.
- ❑ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❑ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❑ FeliCa i PaSoRi predstavljaju registrovane žigove korporacije Sony.
- ❑ MIFARE predstavlja registrovani žig korporacije NXP Semiconductor.
- ❑ Opšta napomena: nazivi drugih proizvoda koji su ovde upotrebljeni služe isključivo u identifikacione svrhe i mogu biti zaštitni žigovi svojih vlasnika. Epson se odriče svih prava na te žigove.

Sadržaj

Autorska prava

Zaštitni znakovi

Uvod

Sadržaj ovog dokumenta.	7
Korišćenje ovog priručnika.	7
Oznake i simboli.	7
Opisi korišćeni u ovom priručniku.	7
Upućivanja na operativni sistem.	8

Potrebna podešavanja koja odgovaraju nameni

Potrebna podešavanja koja odgovaraju nameni.	10
--	----

Podešavanja mreže

Povezivanje skenera na mrežu.	13
Pre nego što napravite mrežnu vezu.	13
Povezivanje na mrežu sa kontrolne table.	15
Dodavanje ili zamena računara ili uređaja.	19
Povezivanje sa skenerom koji je povezan sa mrežom.	19
Direktno povezivanje pametnog uređaja i skenera (Wi-Fi Direct).	21
Resetovanje mrežne veze.	23
Provera statusa mrežne veze.	25
Provera statusa mrežnog povezivanja sa kontrolne table.	25
Specifikacije mreže.	27
Specifikacije bežične veze.	27
Specifikacije Ethernet mreže.	28
Mrežne funkcije i IPv4/IPv6.	28
Bezbednosni protokol.	29
Korišćenje ulaza za skener.	29
Rešavanje problema.	30
Ne možete da se povežete sa mrežom.	30

Softver za podešavanje skenera

Web Config.	35
Pokretanje Web Config u veb pregledaču.	35
Pokretanje aplikacije Web Config u operativnom sistemu Windows.	35
Epson Device Admin.	36

Šablon za konfiguraciju.	36
----------------------------------	----

Podešavanja potrebna za skeniranje

Konfigurisanje servera za poštu.	41
Stavke podešavanja servera za poštu.	41
Provera veze sa serverom e-pošte.	42
Podešavanje deljene mrežne fascikle.	44
Kreiranje deljene fascikle.	44
Dostupnost kontakata.	61
Poređenje konfiguracija kontakata.	62
Registrowanje odredišta u kontaktima pomoću Web Config.	62
Registrowanje odredišta kao grupe pomoću Web Config.	64
Izrada rezervne kopije i uvoz kontakata.	65
Izvoz i masovna registracija kontakata pomoću alata.	66
Saradnja između LDAP servera i korisnika.	68
Korišćenje funkcije Document Capture Pro Server.	71
Podešavanje režima servera.	71
Podešavanje funkcije AirPrint.	71
Problemi prilikom pripreme skeniranja preko mreže.	72
Napomene za rešavanje problema.	72
Pristup programu Web Config nije moguć.	72

Prilagođeno podešavanje prikaza kontrolne table

Registrowanje Un. pod. vr.	75
Opcije menija za Un. pod. vr.	76
Uređivanje početnog ekrana na kontrolnoj tabli.	77
Menjanje Raspored početnog ekrana.	77
Dodaj ikonu.	78
Ukloni ikonu.	79
Pomeri ikonu.	80

Osnovne bezbednosne postavke

Uvođenje funkcija sigurnosti proizvoda.	83
Podešavanja za administratore.	83
Konfigurisanje administratorske lozinke.	83
Upotreba Zaključavanje podešavanja sa kontrolne table štampača.	85
Prijavite se kao administrator sa kontrolne table štampača.	88

Onemogućavanje spoljnog interfejsa.	89
Upravljanje udaljenim skenerom.	90
Provera informacija za udaljeni skener.	90
Primanje obaveštenja o događajima e-poštom.	90
Rešavanje problema.	91
Zaboravili ste administratorsku lozinku.	91

Napredna bezbednosna podešavanja

Bezbednosna podešavanja i sprečavanje opasnosti.	93
Podešavanja bezbednosnih funkcija.	94
Kontrolisanje pomoću protokola.	94
Kontrolisanje protokola.	94
Protokoli koje možete da omogućite ili onemogućite.	94
Stavke podešavanja protokola.	95
Način korišćenja digitalnog sertifikata.	97
O digitalnim sertifikatima.	97
Konfigurisanje opcije CA-signed Certificate.	97
Ažuriranje nezavisnog sertifikata.	101
Konfigurisanje opcije CA Certificate.	101
SSL/TLS komunikacija sa skenerom.	102
Konfigurisanje osnovnih postavki SSL/TLS protokola.	102
Konfigurisanje sertifikata servera za skener.	103
Šifrovana komunikacija pomoću IPsec/IP filtriranja.	104
O aplikaciji IPsec/IP Filtering.	104
Konfigurisanje podrazumevane smernice.	104
Konfigurisanje smernica za grupe.	107
Primeri konfigurisanja opcije IPsec/IP Filtering.	113
Konfigurisanje sertifikata za IPsec/IP filtriranje.	114
Povezivanje skenera na IEEE802.1X mrežu.	114
Konfigurisanje IEEE 802.1X mreže.	114
Konfigurisanje sertifikata za IEEE 802.1X.	116
Rešavanje problema naprednih bezbednosnih postavki.	116
Vraćanje bezbednosnih podešavanja.	116
Problemi pri korišćenju funkcija za bezbednost na mreži.	117
Problemi pri korišćenju digitalnog sertifikata.	119

Authentication Settings

O aplikaciji Authentication Settings.	124
Dostupne funkcije za Authentication Settings.	124
O aplikaciji Authentication Method.	125
Softver za podešavanje.	127
Ažuriranje osnovnog softvera skenera.	127

Povezivanje i konfiguracija uređaja za autorizaciju.	127
Lista kompatibilnih čitača kartice.	127
Povezivanje sa uređajem za autorizaciju.	130
Podešavanja uređaja za autorizaciju.	131
Registrowanje i podešavanje podataka.	132
Podešavanja.	132
Omogućavanje autorizacije.	133
Authentication Settings.	133
Registrowanje User Settings.	134
Sinhronizacija s LDAP Server.	141
Podešavanje servera e-pošte.	144
Podešavanje režima Scan to My Folder.	145
Customize One-touch Functions.	147
Izveštaji Job History pomoću Epson Device Admin.	147
Stavke koje se mogu obuhvatiti izveštajem.	147
Prijavite se kao administrator sa kontrolne table štampača.	148
Onemogućavanje Authentication Settings.	148
Brisanje Authentication Settings informacija (Vrati podrazumevane postavke).	149
Rešavanje problema.	149
Ne možete da očitajte autorizacionu karticu.	149

Održavanje

Čišćenje spoljašnjosti skenera.	151
Čišćenje unutrašnjosti skenera.	151
Zamena sklopa valjaka.	156
Šifre sklopa valjaka.	161
Resetovanje broja skeniranja.	161
Ušteda energije.	161
Transportovanje skenera.	162
Pravljenje rezervne kopije podešavanja.	163
Izvoz podešavanja.	163
Uvoz podešavanja.	164
Vrati podrazumevane postavke.	164
Ažuriranje aplikacija i upravljačkog softvera.	165
Ažuriranje osnovnog softvera skenera pomoću kontrolne table.	165
Ažuriranje upravljačkog softvera pomoću aplikacije Web Config.	166
Ažuriranje upravljačkog softvera bez povezivanja sa internetom.	166



Uvod

Sadržaj ovog dokumenta. 7

Korišćenje ovog priručnika. 7

Sadržaj ovog dokumenta

Ovaj dokument pruža sledeće informacije za administratore skenera.

- Mrežne postavke
- Priprema funkcije skeniranja
- Omogućite i upravljajte bezbednosnim podešavanjima
- Omogućite i upravljajte Authentication Settings
- Obavljajte svakodnevno održavanje

Za standardne metode korišćenja skenera, pogledajte *Korisnički vodič*.

Napomena:

Ovaj dokument objašnjava Authentication Settings koja pružaju samostalnu autorizaciju, a da ne morate da koristite server za autorizaciju. Pored Authentication Settings navedenih u priručniku, takođe možete da napravite sistem za autorizaciju pomoću servera za autorizaciju. Da biste napravili sistem, koristite Document Capture Pro Server Authentication Edition (skraćeni naziv je Document Capture Pro Server AE).

Za više informacija obratite se lokalnom predstavništvu kompanije Epson.

Korišćenje ovog priručnika

Oznake i simboli



Oprez:

Uputstva koja se moraju pažljivo slediti da bi se izbegle fizičke povrede.



Važno:

Uputstva koja se moraju poštovati kako bi se izbegla oštećenja opreme.

Napomena:

Daje dodatne informacije i preporuke.

Povezane informacije

➔ Veze sa povezanim odeljcima.

Opisi korišćeni u ovom priručniku

- Snimci ekrana za aplikacije su iz operativnih sistema Windows 10 ili macOS High Sierra. Sadržaj prikazan na ekranima razlikuje se u zavisnosti od modela i situacije.
- Ilustracije korišćene u ovom priručniku su samo u informativne svrhe. Iako se mogu neznatno razlikovati u odnosu na stvarni proizvod, načini rada su isti.

Upućivanja na operativni sistem

Windows

U ovom priručniku, termini kao što su „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012”, i „Windows Server 2008 R2” odnose se na sledeće operativne sisteme. Pored toga, „Windows” se koristi za upućivanje na sve verzije a „Windows Server” se koristi za upućivanje na „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012”, i „Windows Server 2008 R2”.

- Operativni sistem Microsoft® Windows® 10
- Operativni sistem Microsoft® Windows® 8.1
- Operativni sistem Microsoft® Windows® 8
- Operativni sistem Microsoft® Windows® 7
- Operativni sistem Microsoft® Windows Server® 2019
- Operativni sistem Microsoft® Windows Server® 2016
- Operativni sistem Microsoft® Windows Server® 2012 R2
- Operativni sistem Microsoft® Windows Server® 2012
- Operativni sistem Microsoft® Windows Server® 2008 R2

Mac OS

U ovom priručniku, „Mac OS” se koristi za upućivanje na „macOS Big Sur”, „macOS Catalina”, „macOS Mojave”, „macOS High Sierra”, „macOS Sierra”, „OS X El Capitan” i „OS X Yosemite”.

Potrebna podešavanja koja odgovaraju nameni

Potrebna podešavanja koja odgovaraju nameni.10

Potrebna podešavanja koja odgovaraju nameni

Pogledajte sledeće da biste izvršili neophodna podešavanja koja odgovaraju nameni.

Povezivanje skenera na mrežu

Namena	Potrebna podešavanja
Želim da priključim skener na mrežu.	Podesite svoj skener za mrežno skeniranje. "Povezivanje skenera na mrežu" na strani 13
Želim da priključim skener na novi računar.	Podesite podešavanja mreže za skener na novom računaru. "Dodavanje ili zamena računara ili uređaja" na strani 19

Podešavanja za skeniranje

Namena	Potrebna podešavanja
Želim da pošaljem skeniranu sliku e-poštom. (Scan to Email)	1. Podesite server e-pošte koji želite da povežete. "Konfigurisanje servera za poštu" na strani 41 2. Registrujte adresu e-pošte primaoca u Contacts (opciono). Registrovanjem adrese e-pošte ne morate da je unosite svaki put kada želite nešto da pošaljete, možete je samo izabrati iz svojih kontakata. "Dostupnost kontakata" na strani 61
Želim da sačuvam skenirane slike u fascikli na mreži. (Scan to Network Folder/FTP)	1. Kreirajte fasciklu na mreži u koju želite da sačuvate slike. "Podešavanje deljene mrežne fascikle" na strani 44 2. Registrujte putanju do fascikle u Contacts (opciono). Registrovanjem putanje do fascikle ne morate da je unosite svaki put kada želite nešto da pošaljete, možete je samo izabrati iz svojih kontakata. "Dostupnost kontakata" na strani 61
Želim da sačuvam skenirane slike u računarski oblak. (Scan to Cloud)	Podešavanje Epson Connect. Više informacija o podešavanju potražite na internet stranici Epson Connect. Prilikom podešavanja, potreban vam je korisnički nalog za uslugu skladištenja na mreži na koju želite da se povežete. https://www.epsonconnect.com/ http://www.epsonconnect.eu (samo Evropa)

Prilagođeno podešavanje prikaza kontrolne table

Namena	Potrebna podešavanja
Želim da promenim stavke prikazane na kontrolnoj tabli skenera.	Podesite Un. pod. vr. ili Izmena početnog ekrana . Možete da registrujete svoja omiljena podešavanja skeniranja na kontrolnoj tabli i izmenite prikazane stavke. "Prilagođeno podešavanje prikaza kontrolne table" na strani 74

Postavljanje osnovnih bezbednosnih funkcija

Namena	Potrebna podešavanja
Želim da sprečim bilo koga osim administratora da menja podešavanja skenera.	Postavite administratorsku lozinku za skener. "Podešavanja za administratore" na strani 83
Želim da onemogućim upotrebu skenera sa USB priključcima.	Onemogućite spoljni interfejs. "Onemogućavanje spoljnog interfejsa" na strani 89

Postavljanje naprednih bezbednosnih funkcija

Namena	Potrebna podešavanja
Želim da kontrolišem koji protokoli se koriste.	Omogućite ili onemogućite protokole. "Kontrolisanje pomoću protokola" na strani 94
Želim da šifrujem putanju komunikacije.	1. Podesite svoj digitalni sertifikat. "Način korišćenja digitalnog sertifikata" na strani 97 2. Podesite SSL/TLS komunikaciju. "SSL/TLS komunikacija sa skenerom" na strani 102
Želim da koristim šifrovanu komunikaciju (IPsec). Želim da mogu da koristim softver samo sa određenog računara (IP filtriranje).	Podesite smernice za filtriranje saobraćaja. "Šifrovana komunikacija pomoću IPsec/IP filtriranja" na strani 104
Želim da koristim skener u IEEE802.1X mreži.	Podesite IEEE802.1X za skener. "Povezivanje skenera na IEEE802.1X mrežu" na strani 114

Podešavanje funkcija koje će skener potvrditi

Namena	Potrebna podešavanja
Želim da omogućim Authentication Settings.	Pogledajte sledeće radi detaljnijih informacija o dostupnim Authentication Settings i Authentication Method. "O aplikaciji Authentication Settings" na strani 124 "O aplikaciji Authentication Method" na strani 125

Korišćenje sistema za autorizaciju servera

Uz pomoć Document Capture Pro Server Authentication Edition (skraćena na Document Capture Pro Server AE), možete izgraditi sistem za autorizaciju koji koristi server za autorizaciju.

Za više informacija obratite se lokalnom predstavništvu kompanije Epson.

Podešavanja mreže

Povezivanje skenera na mrežu.	13
Dodavanje ili zamena računara ili uređaja.	19
Provera statusa mrežne veze.	25
Specifikacije mreže.	27
Rešavanje problema.	30

Povezivanje skenera na mrežu

Ovaj odeljak objašnjava kako da povežete skener na mrežu pomoću kontrolne table skenera.

Napomena:

Ako su vam skener i računar na istom segmentu, možete povezati koristeći program za instalaciju.

Podešavanje sa internet stranice

Pristupite sledećoj internet stranici i zatim unesite naziv proizvođača. Idite na **Podešavanje** a zatim započnite podešavanje.

<http://epson.sn>

Podešavanje pomoću diska sa softverom (samo za modele koji se isporučuju sa diskom sa softverom i korisnike sa Windows računarima sa diskom sa upravljačkim programima.)

Ubacite disk sa softverom u računar i zatim sledite uputstva na ekranu.

Pre nego što napravite mrežnu vezu

Da biste se povezali na mrežu, unapred proverite način povezivanja i informacije o podešavanju.

Prikupljanje informacija o podešavanju veze

Pripremite potrebne informacije po podešavanju radi povezivanja. Sledeće informacije proverite unapred.

Odeljak	Stavke	Napomena
Način povezivanja uređaja	<input type="checkbox"/> Ethernet <input type="checkbox"/> Bežična veza	Odlučite kako da priključite skener na mrežu. Za kablovsku LAN priključuje se na LAN prekidač. Za Wi-Fi priključuje se na mrežu (SSID) pristupne tačke.
Informacije o LAN vezi	<input type="checkbox"/> IP adresa <input type="checkbox"/> Maska podmreže <input type="checkbox"/> Podrazumevani mrežni prolaz	Odaberite IP adresu koju ćete dodeliti skeneru. Kada statično dodelite IP adresu, potrebne su sve vrednosti. Kada dinamično dodelite IP adresu pomoću DHCP funkcije, ove informacije nisu potrebne, jer se automatski podešava.
Informacije o bežičnoj vezi	<input type="checkbox"/> SSID <input type="checkbox"/> Lozinka	To su SSID (naziv mreže) i lozinka pristupne tačke na koju se skener povezuje. Ako je podešeno filtriranje MAC adrese, unapred registrujte MAC adresu skenera da biste registrovali skener. Pogledajte sledeće informacije u vezi sa podržanim standardima. "Specifikacije mreže" na strani 27
Informacije o DNS serveru	<input type="checkbox"/> IP adresa za primarni DNS <input type="checkbox"/> IP adresa za sekundarni DNS	Potrebne su prilikom određivanja DNS servera. Sekundarni DNS se podešava kada sistem ima suvišnu konfiguraciju i postoji sekundarni DNS server. Ako ste u maloj organizaciji i ne podesite DNS server, podesite IP adresu mrežnog usmerivača.

Odeljak	Stavke	Napomena
Informacije o ovlašćenom serveru	<input type="checkbox"/> Naziv ovlašćenog servera	<p>Podesite kada vaše mrežno okruženje koristi posrednički server za pristup internetu iz intraneta i kada koristite ovu funkciju da skener direktno pristupi internetu.</p> <p>Za sledeće funkcije, skener se direktno povezuje na internet.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Usluge Epson Connect <input type="checkbox"/> Usluge u računarskom oblaku drugih kompanija <input type="checkbox"/> Ažuriranje upravljačkog softvera <input type="checkbox"/> Slanje skeniranih slika u SharePoint (WebDAV)
Informacije o broju ulaza	<input type="checkbox"/> Broj ulaza za oslobađanje	<p>Proverite broj ulaza koje koriste skener i računar, zatim po potrebi oslobodite ulaz koji je blokiran zaštitnim zidom.</p> <p>Pogledajte sledeće informacije o broju ulaza koje skener koristi.</p> <p>“Korišćenje ulaza za skener” na strani 29</p>

Dodeljivanje IP adrese

Postoje sledeće vrste dodele IP adrese.

Statička IP adresa:

Ručno dodelite unapred određenu IP adresu skeneru (matičnom).

Informacije za povezivanje na mrežu (maska podmreže, podrazumevani mrežni prolaz, DNS server itd) treba da se podese ručno.

IP adresa se ne menja čak i kada je uređaj isključen, tako da je to korisno kada želite da upravljate uređajima u okruženju u kom ne možete da izmenite IP adresu ili želite da upravljate uređajima pomoću IP adrese. Preporučujemo da se podese skener, server itd. kojima mnogi računari pristupaju. Takođe, kada koristite bezbednosne funkcije kao što su IPsec/IP filtriranje, dodelite statičnu IP adresu, tako da se IP adresa ne menja.

Automatsko dodeljivanje pomoću funkcije DHCP (dinamičke IP adrese):

Automatski dodelite IP adresu skeneru (matičnom) pomoću DHCP funkcije DHCP servera ili mrežnog usmerivača.

Informacije za povezivanje na mrežu (maska podmreže, podrazumevani mrežni prolaz, DNS server itd) treba da se podese automatski, tako da možete jednostavno povezati uređaj sa mrežom.

Ako je uređaj ili mrežni usmerivač isključen, ili zavisno od podešavanja DHCP servera, IP adresa se može promeniti prilikom ponovnog povezivanja.

Preporučujemo da upravljate uređajima mimo IP adrese i da komunicirate sa protokolima koji mogu da prate IP adresu.

Napomena:

Kada koristite funkciju rezervacije IP adrese DHCP-a, možete dodeliti istu IP adresu uređajima u bilo kom trenutku.

DNS server i ovlašćeni server

DNS server ima naziv matičnog računara, naziv domena adrese e-pošte itd. u vezi sa informacijama o IP adresi.

Komunikacija nije moguća ako se druga strana opisuje pomoću naziva matičnog računara, naziva domena itd. kada računar ili skener vrši IP komunikaciju.

Šalje upit DNS serveru za tu informaciju i dobija IP adresu druge strane. Ovaj proces se zove razrešavanje imena.

Dakle, uređaji kao što su računari i skeneri mogu da komuniciraju pomoću IP adrese.

Razrešavanje imena je potrebno da bi skener komunicirao pomoću funkcije e-pošte i funkcije internet veze.

Kada koristite te funkcije, izvršite podešavanja DNS servera.

Kada dodelite IP adresu skeneru pomoću DHCP funkcije DHCP servera ili mrežnog usmerivača, ona se automatski podešava.

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

Kada se povežete na internet preko ovlašćenog servera, konfigurirate ovlašćeni server na skeneru.

Povezivanje na mrežu sa kontrolne table

Povežite skener na mrežu pomoću kontrolne table na skeneru.

Dodeljivanje IP adrese

Podesite osnovne stavke, poput adrese matičnog računara, Maska podmreže, Podraz. mrež. prol..

Ovo poglavlje opisuje postupak za podešavanje statičke IP adrese.

1. Uključite skener.
2. Izaberite **Podešavanja** na početnom ekranu na kontrolnoj tabli skenera.
3. Izaberite **Mrežne postavke > Napredno > TCP/IP**.
4. Izaberite **Ručno** za **Pribavi IP adresu**.

Kada IP adresu podesite automatski pomoću DHCP funkcije skretnice, odaberite **Automatski**. U tom slučaju **IP adresa**, **Maska podmreže**, i **Podraz. mrež. prol.** u koracima od 5 do 6 takođe budu automatski podešeni, tako da možete preći na korak 7.

5. Unesite IP adresu.

Fokus se pomera do prednjeg segmenta ili zadnjeg segmenta odvojenog tačkom ako izaberete ◀ i ▶.

Potvrdite vrednost prikazanu na prethodnom ekranu.

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

Potvrdite vrednost prikazanu na prethodnom ekranu.



Važno:

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

7. Unesite IP adresu primarnog DNS servera.
Potvrdite vrednost prikazanu na prethodnom ekranu.

Napomena:

*Kada izaberete **Automatski** za podešavanje dodeljivanja IP adrese, možete odabrati podešavanja za DNS server u **Ručno** ili **Automatski**. Ako ne možete automatski da dobijete adresu DNS servera, odaberite **Ručno** i unesite adresu DNS servera. Zatim direktno unesite adresu sekundarnog DNS servera. Ako odaberete **Automatski**, idite na korak 9.*

8. Unesite IP adresu sekundarnog DNS servera.
Potvrdite vrednost prikazanu na prethodnom ekranu.
9. Dodirnite **Počni podešavanje**.

Podešavanje ovlašćenog (proksi) servera


Podesite ovlašćeni server ako su zadovoljena oba sledeća uslova.

- Ovlašćeni server je napravljen za internet vezu.
- Kada koristite funkciju pri kojoj se skener direktno povezuje sa internetom, kao što je usluga Epson Connect ili usluge računarskog oblaka druge kompanije.

1. Na početnom ekranu izaberite **Podešavanja**.
Kada vršite podešavanja nakon podešavanja IP adrese, prikazuje se ekran **Napredno**. Pređite na korak 3.
2. Izaberite **Mrežne postavke > Napredno**.
3. Izaberite **Proksi server**.
4. Izaberite **Koristi za Postavke posredničkog servera**.
5. Unesite adresu ovlašćenog servera u formatu IPv4 ili FQDN.
Potvrdite vrednost prikazanu na prethodnom ekranu.
6. Unesite broj ulaza za ovlašćeni server.
Potvrdite vrednost prikazanu na prethodnom ekranu.
7. Dodirnite **Počni podešavanje**.

Povezivanje na Ethernet

Priključite skener na mrežu pomoću LAN kabla, a zatim proverite vezu.

1. Priključite skener na čvorište (prekidač LAN) pomoću LAN kabla.
2. Na početnom ekranu izaberite .
3. Izaberite **Ruter**.

4. Proverite da li su ispravna podešavanja Veza i IP adresa.
5. Dodirnite **Zatvori**.

Povezivanje na bežičnu LAN (Wi-Fi)

Možete povezati skener na bežičnu LAN (Wi-Fi) na nekoliko načina. Izaberite način povezivanja koji odgovara okruženju i uslovima koje koristite.

Ako znate informacije za bežični mrežni usmerivač, kao što su SSID i lozinka, možete ručno izvršiti podešavanja.

Ako bežični mrežni usmerivač podržava WPS, možete izvršiti podešavanja koristeći podešavanja pomoću tastera.

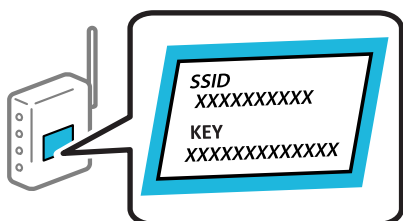
Nakon priključivanja skenera na mrežu, priključite skener sa uređaja koji želite da koristite (računar, pametni uređaj, tablet itd.)

Podešavanje bežične mreže pomoću unosa SSID i lozinke

Možete podesiti Wi-Fi mrežu pomoću unosa informacija koje su potrebne za bežični mrežni usmerivač sa kontrolne table skenera. Za podešavanje pomoću ovog načina potrebni su vam SSID i lozinka za bežični mrežni usmerivač.

Napomena:

Ako koristite bežični mrežni usmerivač sa njegovim standardnim podešavanjima, SSID i lozinka se nalaze na nalepnici. Ako ne znate SSID i lozinku, obratite se osobi koja je podesila bežični mrežni usmerivač, ili pogledajte dokumentaciju isporučenu sa bežičnim mrežnim usmerivačem.



1. Dodirnite  na početnom ekranu.

2. Izaberite **Ruter**.

3. Dodirnite **Pokreni podešavanje**.

Ako je mrežno povezivanje već podešeno, prikazuju se podaci o vezi. Dodirnite **Promenite na Wi-Fi vezu**, ili **Promeni postavke** da biste promenili podešavanja.

4. Izaberite **Čarobnjak za podešavanje Wi-Fi veze**.

5. Sledite uputstva na ekranu da biste izabrali SSID, unesite lozinku za bežični mrežni usmerivač i započnite podešavanje.

Ako želite da proverite status mrežnog povezivanja za skener nakon što se podešavanje završi, detalje potražite na sledećem linku za povezane informacije.

Napomena:

- Ako ne znate SSID, proverite da li je zapisan na nalepnici bežičnog mrežnog usmerivača. Ako koristite bežični ruter sa njegovim standardnim podešavanjima, koristite SSID koji se nalazi na nalepnici. Ako ne možete da pronađete nijednu informaciju, pogledajte dokumentaciju isporučenu sa bežičnim mrežnim usmerivačem.
- Lozinka je osetljiva na velika i mala slova.
- Ako ne znate lozinku, proverite da li je informacija zapisana na nalepnici bežičnog mrežnog usmerivača. Na nalepnici, lozinka može biti napisana kao „Network Key”, „Wireless Password” („Mrežni ključ”, „Bežična lozinka”) itd. Ako koristite bežični mrežni usmerivač sa njegovim standardnim podešavanjima, koristite lozinku koja je napisana na nalepnici.

Povezane informacije

➔ [“Provera statusa mrežne veze” na strani 25](#)

Vršenje podešavanja bežične mreže pomoću postavke tastera (WPS)

Wi-Fi mrežu možete automatski da podesite pritiskom na dugme na bežičnom mrežnom usmerivaču. Ako su ispunjeni sledeći uslovi, možete podesiti koristeći ovaj način.

- Bežični mrežni usmerivač je kompatibilan sa WPS (Wi-Fi Protected Setup).
- Trenutna Wi-Fi veza je uspostavljena pritiskom na dugme na bežičnom mrežnom usmerivaču.

Napomena:

Ako ne možete da nađete dugme ili ako obavljate podešavanje pomoću softvera, pogledajte dokumentaciju priloženu uz bežični ruter.

1. Dodirnite  na početnom ekranu.

2. Izaberite **Ruter**.

3. Dodirnite **Pokreni podešavanje**.

Ako je mrežno povezivanje već podešeno, prikazuju se podaci o vezi. Dodirnite **Promenite na Wi-Fi vezu**. ili **Promeni postavke** da biste promenili podešavanja.

4. Izaberite **Podešavanje tastera (WPS)**.

5. Pratite uputstva na ekranu.

Ako želite da proverite status mrežnog povezivanja za skener nakon što se podešavanje završi, detalje potražite na sledećem linku za povezane informacije.

Napomena:

Ako povezivanje ne uspe, restartujte bežični mrežni usmerivač, pomerite ga bliže skeneru i pokušajte ponovo.

Povezane informacije

➔ [“Provera statusa mrežne veze” na strani 25](#)

Vršenje podešavanja bežične mreže pomoću postavke PIN koda (WPS)

Možete automatski da se povežete na bežični ruter pomoću PIN koda. Možete koristiti ovaj način za podešavanje ako bežični ruter ima mogućnost WPS (Wi-Fi zaštićeno podešavanje). Pomoću računara unesite PIN kod u bežični ruter.

1. Dodirnite  na početnom ekranu.

2. Izaberite **Ruter**.

3. Dodirnite **Pokreni podešavanje**.

Ako je mrežno povezivanje već podešeno, prikazuju se podaci o vezi. Dodirnite **Promenite na Wi-Fi vezu** ili **Promeni postavke** da biste promenili podešavanja.

4. Izaberite **Drugo > Podešavanje PIN koda (WPS)**

5. Pratite uputstva na ekranu.

Ako želite da proverite status mrežnog povezivanja za skener nakon što se podešavanje završi, detalje potražite na sledećem linku za povezane informacije.

Napomena:

Detalje o unošenju PIN koda potražite u dokumentaciji priloženoj uz bežični ruter.

Povezane informacije

➔ [“Provera statusa mrežne veze” na strani 25](#)

Dodavanje ili zamena računara ili uređaja

Povezivanje sa skenerom koji je povezan sa mrežom

Kada je skener već povezan na mrežu, možete da povežete računar ili pametni uređaj sa skenerom preko mreže.

Korišćenje mrežnog skenera sa drugog računara

Preporučujemo da koristite alat za instalaciju da biste povezali skener sa računarom. Možete pokrenuti alat za instalaciju pomoću jednog od sledećih načina.

Podešavanje sa internet stranice

Pristupite sledećoj internet stranici i zatim unesite naziv proizvoda. Idite na **Podešavanje** a zatim započnite podešavanja.

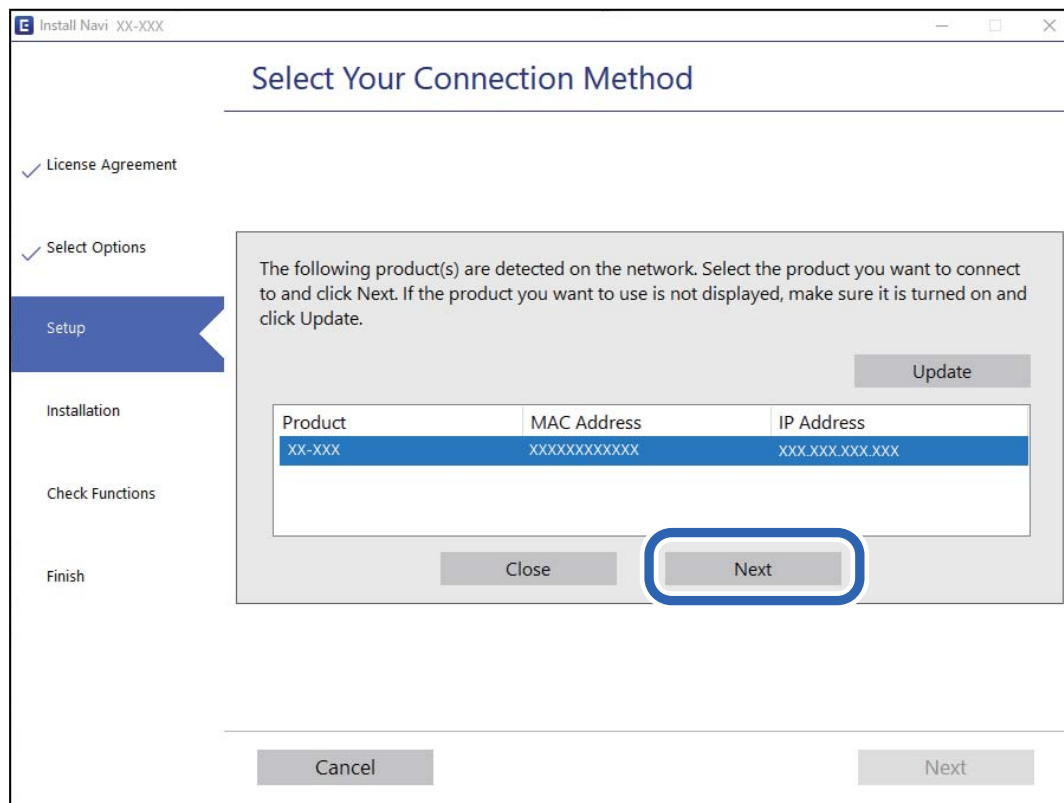
<http://epson.sn>

Podešavanje pomoću diska sa softverom (samo za modele koji se isporučuju sa diskom sa softverom i korisnike sa Windows računarima sa diskom sa upravljačkim programima).

Ubacite disk sa softverom u računar i zatim sledite uputstva na ekranu.

Izbor skenera

Sledite uputstva na ekranu dok se ne prikaže sledeći prozor, izaberite naziv skenera koji želite da priključite, a zatim kliknite na **Dalje**.



Pratite uputstva na ekranu.

Korišćenje mrežnog skenera sa pametnog uređaja

Pametni uređaj možete da povežete direktno na skener na jedan od sledećih načina.

Povezivanje preko bežičnog mrežnog usmerivača

Povežite pametni uređaj na istu bežičnu mrežu (SSID) kao skener.

Detaljnije informacije potražite u nastavku.

[“Vršenje podešavanja za povezivanje na pametni uređaj” na strani 24](#)

Povezivanje pomoću Wi-Fi Direct

Povežite pametni uređaj direktno sa skenerom bez bežičnog mrežnog usmerivača.

Detaljnije informacije potražite u nastavku.

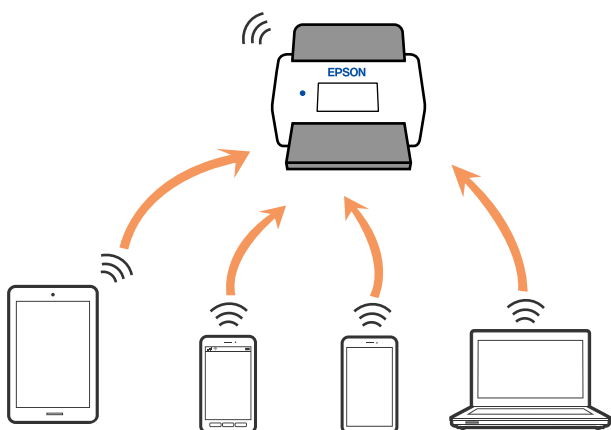
[“Direktno povezivanje pametnog uređaja i skenera \(Wi-Fi Direct\)” na strani 21](#)

Direktno povezivanje pametnog uređaja i skenera (Wi-Fi Direct)

Wi-Fi Direct (režim jednostavne pristupne tačke) vam omogućava da povežete skener sa pametnim uređajem bez bežičnog mrežnog usmerivača da biste skenirali sa pametnog uređaja.

O aplikaciji Wi-Fi Direct


Koristite ovaj način povezivanja kada ne koristite Wi-Fi kod kuće ili u kancelariji ili kada hoćete direktno da povežete skener i pametni uređaj. U ovom režimu skener se ponaša kao bežični mrežni usmerivač i možete da povežete uređaje sa skenerom, a da ne morate da koristite standardni bežični mrežni usmerivač. Međutim, uređaji koji su direktno povezani sa skenerom ne mogu međusobno komunicirati preko skenera.



Skener se može povezati pomoću Wi-Fi ili Ethernet veze i veze Wi-Fi Direct (režim jednostavne pristupne tačke) istovremeno. Međutim, ako pokrenete mrežno povezivanje u vezi Wi-Fi Direct (režim jednostavne pristupne tačke) kada je skener povezan putem Wi-Fi veze, Wi-Fi veza se privremeno prekida.

Povezivanje sa pametnim uređajem uz pomoć Wi-Fi Direct

Ovaj način vam omogućava da povežete skener direktno sa pametnim uređajima bez bežičnog mrežnog usmerivača.

1. Na početnom ekranu izaberite .
2. Izaberite **Wi-Fi Direct**.
3. Izaberite **Pokreni podešavanje**.
4. Pokrenite Epson Smart Panel na pametnom telefonu.
5. Pratite uputstva prikazana na Epson Smart Panel da biste se povezali na skener.
Kada je vaš pametni uređaj povezan sa skenerom, idite na sledeći korak.
6. Na kontrolnoj tabli skenera izaberite **Završeno**.

Prekid Wi-Fi Direct veze (režim jednostavne pristupne tačke)

Postoje dve metode za onemogućavanje Wi-Fi Direct (režim jednostavne pristupne tačke) veze; možete onemogućiti sve veze pomoću kontrolne table skenera, ili onemogućiti svaku vezu sa računara ili pametnog uređaja.

Kada želite da onemogućite sve veze, izaberite  > **Wi-Fi Direct** > **Pokreni podešavanje** > **Promeni** > **Onemogući Wi-Fi Direct**.



Važno:

Kada je veza Wi-Fi Direct (režim jednostavne pristupne tačke) onemogućena, svi računari i pametni uređaji priključeni na skener u Wi-Fi Direct (režim jednostavne pristupne tačke) nisu povezani.

Napomena:

Ako želite da prekinete vezu za određeni uređaj, prekinite je sa uređaja umesto skenera. Koristite jedan od sledećih načina da prekinete vezu Wi-Fi Direct (režim jednostavne pristupne tačke) sa uređaja.

- Isključite Wi-Fi vezu sa nazivom mreže skenera (SSID).*
- Povežete sa drugim nazivom mreže (SSID).*

Promena podešavanja za Wi-Fi Direct (režim jednostavne pristupne tačke) kao što su SSID

Kada je omogućena veza Wi-Fi Direct (režim jednostavne pristupne tačke), možete promeniti podešavanja iz



> **Wi-Fi Direct** > **Pokreni podešavanje** > **Promeni**, a zatim se prikazuju sledeće stavke menija.

Promeni naziv mreže

Promenite naziv mreže (SSID) za Wi-Fi Direct (režim jednostavne pristupne tačke) koji se koristi za povezivanje na skener na vaš proizvoljni naziv. Možete da podesite naziv mreže (SSID) u ASCII znakovima koji se prikazuju na softverskoj tastaturi na kontrolnoj tabli. Možete da unesete najviše 22 znaka.

Kada promenite naziv mreže (SSID), svi priključeni uređaji su isključeni. Koristite novi naziv mreže (SSID) ako želite da ponovo priključite uređaj.

Promeni lozinku

Promenite lozinku za Wi-Fi Direct (režim jednostavne pristupne tačke) za povezivanje na skener na vašu proizvoljnu vrednost. Možete da postavite lozinku u ASCII znakovima koji su prikazani na softverskoj tastaturi na kontrolnoj tabli. Možete da unesete od 8 do 22 znaka.

Kada promenite lozinku, svi priključeni uređaji su isključeni. Koristite novu lozinku ako želite da ponovo priključite uređaj.

Promeni frekventni opseg

Promenite frekventni opseg Wi-Fi Direct koji se koristi za povezivanje na skener. Možete izabrati 2,4 GHz ili 5 GHz.

Kada promenite frekventni opseg, svi priključeni uređaji su isključeni. Ponovo priključite uređaj.

Kada menjate frekventni opseg na 5 GHz, vodite računa da ne možete ponovo da se priključite sa uređaja koji ne podržava frekventni opseg od 5 GHz.

U zavisnosti od regiona ovo podešavanje možda neće biti prikazano.

Onemogućiti Wi-Fi Direct

Onemogućite Wi-Fi Direct (režim jednostavne pristupne tačke) podešavanje skenera. Kada ih onemogućite, svi uređaji koji su povezani sa skenerom u Wi-Fi Direct (režim jednostavne pristupne tačke) vezi su isključeni.

Vrati podrazumevana podešavanja

Vratite sva Wi-Fi Direct (režim jednostavne pristupne tačke) podešavanja na podrazumevane vrednosti.

Wi-Fi Direct (režim jednostavne pristupne tačke) informacije o povezivanju pametnog uređaja sačuvane na skeneru se brišu.

Napomena:

*Takođe možete podesiti sa kartice **Network** > **Wi-Fi Direct** na **Web Config** za sledeća podešavanja.*

- Omogućavanje ili onemogućavanje veze Wi-Fi Direct (režim jednostavne pristupne tačke)*
- Promena naziva mreže (SSID)*
- Promena lozinke*
- Menjanje frekventnog opsega*
U zavisnosti od regiona ovo podešavanje možda neće biti prikazano.
- Vraćanje podešavanja za Wi-Fi Direct (režim jednostavne pristupne tačke)*

Resetovanje mrežne veze

Ovaj odeljak objašnjava kako se vrše podešavanja mrežnog povezivanja i menja način povezivanja kada se menja bežični mrežni usmerivač ili računar.

Kada se menja bežični mrežni usmerivač

Kada menjate bežični mrežni usmerivač, izvršite podešavanja za povezivanje računara ili pametnog uređaja sa skenerom.

Potrebno je da odredite ova podešavanja ako želite da promenite pružaoca internet usluga itd.

Vršenje podešavanja za povezivanje na računar

Preporučujemo da koristite alat za instalaciju da biste povezali skener sa računarom. Možete pokrenuti alat za instalaciju pomoću jednog od sledećih načina.

- Podešavanje sa internet stranice**
Pristupite sledećoj internet stranici i zatim unesite naziv proizvoda. Idite na **Podešavanje** a zatim započnite podešavanja.
<http://epson.sn>
- Podešavanje pomoću diska sa softverom (samo za modele koji se isporučuju sa diskom sa softverom i korisnike sa Windows računarima sa diskom sa upravljačkim programima).**
Ubacite disk sa softverom u računar i zatim sledite uputstva na ekranu.

Izbor načina povezivanja

Pratite uputstva na ekranu. Na ekranu **Izaberite radnju** izaberite **Ponovo podesite vezu sa Štampač (u slučaju novog mrežnog rutera ili promene sa USB-a na mrežu itd.)**, a zatim kliknite na **Dalje**.

Sledite uputstva na ekranu da biste završili podešavanje.

Ako ne možete da se povežete, pogledajte sledeće kako biste rešili problem.

“Ne možete da se povežete sa mrežom” na strani 30

Vršenje podešavanja za povezivanje na pametni uređaj

Možete koristiti skener sa pametnog uređaja kada povežete skener na isti SSID bežične mreže kao i pametni uređaj. Da biste koristili skener sa pametnog uređaja, pristupite sledećoj internet stranici, a zatim unesite naziv proizvođača. Idite na **Podešavanje** a zatim započnite podešavanja.

<http://epson.sn>

Pristupite internet strani sa pametnog uređaja koji želite da povežete sa skenerom.

Kada menjate računar

Kada menjate računar, izvršite podešavanja veze između računara i skenera.

Vršenje podešavanja za povezivanje na računar

Preporučujemo da koristite alat za instalaciju da biste povezali skener sa računarom. Možete pokrenuti alat za instalaciju pomoću sledećeg načina.

Podešavanje sa internet stranice

Pristupite sledećoj internet stranici i zatim unesite naziv proizvođača. Idite na **Podešavanje** a zatim započnite podešavanja.

<http://epson.sn>

Podešavanje pomoću diska sa softverom (samo za modele koji se isporučuju sa diskom sa softverom i korisnike sa Windows računarima sa diskom sa upravljačkim programima).

Ubacite disk sa softverom u računar i zatim sledite uputstva na ekranu.

Pratite uputstva na ekranu.

Promena načina povezivanja sa računarom

Ovo poglavlje opisuje kako da promenite režim povezivanja kada su povezani računar i skener.

Promena mrežne veze iz režima Ethernet u bežičnu mrežu

Promena Ethernet veze u bežičnu mrežu sa kontrolne table skenera. Promena načina povezivanja u osnovi je ista kao podešavanje za povezivanje na bežičnu mrežu.

Povezane informacije

➔ “Povezivanje na bežičnu LAN (Wi-Fi)” na strani 17

Promena mrežne veze iz režima bežične mreže u Ethernet

Pratite korake u nastavku da biste promenili iz režima bežične mreže u Ethernet vezu.

1. Na početnom ekranu izaberite **Podešavanja**.
2. Izaberite **Mrežne postavke > Podešavanje ožičene lokalne mreže**.
3. Pratite uputstva na ekranu.

Promena povezivanja putem USB-a na mrežno povezivanje

Pomoću alata za instalaciju i resetovanje u različitom načinu povezivanja.

- Podešavanje sa internet stranice**

Pristupite sledećoj internet stranici i zatim unesite naziv proizvoda. Idite na **Podešavanje** a zatim započnite podešavanja.

<http://epson.sn>

- Podešavanje pomoću diska sa softverom (samo za modele koji se isporučuju sa diskom sa softverom i korisnike sa Windows računarima sa diskom sa upravljačkim programima).**

Ubacite disk sa softverom u računar i zatim sledite uputstva na ekranu.

Izbor Promene načina povezivanja

Pratite uputstva na ekranu. Na ekranu **Izaberite radnju** izaberite **Ponovo podesite vezu sa Štampač (u slučaju novog mrežnog rutera ili promene sa USB-a na mrežu itd.)**, a zatim kliknite na **Dalje**.

Izaberite mrežno povezivanje koje želite da koristite, **Povezivanje preko bežične mreže (Wi-Fi)** ili **Povežite koristeći ožičenu mrežu (Ethernet)**, a zatim kliknite na **Dalje**.

Sledite uputstva na ekranu da biste završili podešavanje.

Provera statusa mrežne veze

Možete proveriti status mrežnog povezivanja na sledeći način.









Provera statusa mrežnog povezivanja sa kontrolne table

Možete proveriti status mrežnog povezivanja uz pomoć ikone za mrežu ili informacija o mreži na kontrolnoj tabli skenera.

Provera statusa mrežnog povezivanja pomoću ikone za mrežu

Možete proveriti status mrežnog povezivanja i jačinu radio talasa uz pomoć ikone za mrežu na početnom ekranu skenera.



	<p>Prikazuje status mrežnog povezivanja.</p> <p>Izaberite ikonu da biste proverili i izmenili trenutna podešavanja. Ovo je prečica za sledeći meni.</p> <p>Podešavanja > Mrežne postavke > Podešavanje Wi-Fi-a</p>
	Skener nije povezan na bežičnu (Wi-Fi) mrežu.
	Skener traži SSID, resetovanu IP adresu, ili ima problem sa bežičnom (Wi-Fi) mrežom.
	Skener je povezan na bežičnu (Wi-Fi) mrežu. Broj podeljaka pokazuje jačinu signala veze. Što je više podeljaka popunjeno, veza je jača.
	Skener nije povezan na bežičnu (Wi-Fi) mrežu u Wi-Fi Direct (režim jednostavne pristupne tačke).
	Skener je povezan na bežičnu (Wi-Fi) mrežu u Wi-Fi Direct (jednostavna pristupna tačka) režimu.
	Skener nije povezan na ožičenu (Ethernet) mrežu ili ga resetujte.
	Skener je povezan na ožičenu (Ethernet) mrežu.

Prikazivanje detaljnih informacija o mreži na kontrolnoj tabli

Kad je skener povezan na mrežu, možete videti i ostale informacije u vezi sa mrežom izborom menija za mrežu koje želite da proverite.

1. Na početnom ekranu izaberite **Podešavanja**.
2. Izaberite **Mrežne postavke > Status mreže**.
3. Da biste pogledali informacije, izaberite menije koje želite da pogledate.
 - Status kablovske LAN/Wi-Fi mreže
Prikazuje informacije o mreži (naziv uređaja, vezu, jačinu signala itd) za Ethernet ili Wi-Fi veze.
 - Status Wi-Fi Direct
Prikazuje da li je Wi-Fi Direct omogućen ili onemogućen, SSID, lozinku itd. za Wi-Fi Direct veze.
 - Status servera e-pošte
Prikazuje informacije o mreži za server e-pošte.

Specifikacije mreže

Specifikacije bežične veze

Pogledajte sledeću tabelu radi specifikacija bežične veze.

Zemlje ili regioni osim ispod navedenih	Tabela A
Australija Novi Zeland Tajvan Južna Koreja	Tabela B

Tabela A

Standardi	IEEE 802.11b/g/n ^{*1}
Opseg frekvencije	2,4 GHz
Maksimalna prenesena snaga radio frekvencije	2.400–2.483,5 MHz: 20 dBm (EIRP)
Kanali	1/2/3/4/5/6/7/8/9/10/11/12/13
Režimi veze	Infrastruktura, Wi-Fi Direct (režim jednostavne pristupne tačke) ^{*2*3}
Bezbednosni protokoli ^{*4}	WEP (64/128bit), WPA2-PSK (AES) ^{*5} , WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Dostupno samo za HT20.

*2 Nije podržan za IEEE 802.11b.

*3 Infrastrukturni režim i Wi-Fi Direct režim ili Ethernet veza mogu se istovremeno koristiti.

*4 Wi-Fi Direct podržava samo WPA2-PSK (AES).

*5 Pridržava se standarda WPA2 sa podrškom za WPA/WPA2 Personal.

Tabela B

Standardi	IEEE 802.11a/b/g/n ^{*1} /ac
Frekventni opsezi	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz

Kanali	Bežična veza	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48) W58 (149/153/157/161/165)
Režimi veze	Infrastruktura, Wi-Fi Direct (režim jednostavne pristupne tačke) * ⁴ , * ⁵		
Bezbednosni protokoli* ⁶	WEP (64/128bit), WPA2-PSK (AES)* ⁷ , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Dostupno samo za HT20.

*2 Nije dostupno na Tajvanu.

*3 Dostupnost ovih kanala i upotreba proizvoda napolju preko ovih kanala zavisi od lokacije. Radi detaljnijih informacija pogledajte <http://support.epson.net/wifi5ghz/>

*4 Nije podržan za IEEE 802.11b.

*5 Infrastrukturni režim i Wi-Fi Direct režim ili Ethernet veza mogu se istovremeno koristiti.

*6 Wi-Fi Direct podržava samo WPA2-PSK (AES).

*7 Pridržava se standarda WPA2 sa podrškom za WPA/WPA2 Personal.

Specifikacije Ethernet mreže

Standardi	IEEE802.3i (10BASE-T)* ¹ IEEE802.3u (100BASE-TX)* ¹ IEEE802.3ab (1000BASE-T)* ¹ IEEE802.3az (Energetski efikasan Ethernet)* ²
Komunikacioni režim	Automatski, 10 Mbps puni dupleks, 10 Mbps poludupleks, 100 Mbps puni dupleks, 100 Mbps poludupleks
Priključak	RJ-45

*1 Koristite STP (kabl s upredenim paricama) kabl kategorije 5e ili više radi sprečavanja rizika od smetnji na radio talasima.

*2 Priključeni uređaj treba da je usaglašen sa standardima IEEE802.3az.

Mrežne funkcije i IPv4/IPv6

Funkcije	Podržano
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Funkcije	Podržano
Document Capture Pro Server	IPv4, IPv6

Bezbednosni protokol

IEEE802.1X*	
IPsec/IP filtriranje	
SSL/TLS	HTTPS server/klijent
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Morate koristiti uređaj za povezivanje koji je usaglašen s IEEE802.1X.

Korišćenje ulaza za skener

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

Kada je skener pošiljalac (klijent)

Upotreba	Odredište (server)	Protokol	Broj ulaza
Slanje datoteka (kada se sa skenera koristi funkcija skeniranja u mrežnu fasciklu)	FTP/FTPS server	FTP/FTPS (TCP)	20
			21
	Server za datoteku	SMB (TCP)	445
		NetBIOS (UDP)	137
		NetBIOS (TCP)	138
	WebDAV server	Protokol HTTP (TCP)	80
Protokol HTTPS(TCP)		443	
Slanje e-poštom (kada se sa skenera koristi funkcija skeniranja u e-poruku)	SMTP server	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
Povezivanje na POP pre povezivanja na SMTP (kada se sa skenera koristi funkcija skeniranja u e-poruku)	POP server	POP3 (TCP)	110
Kada se koristi usluga Epson Connect	Server Epson Connect	HTTPS	443
		XMPP	5222

Upotreba	Odredište (server)	Protokol	Broj ulaza
Prikupljanje informacija o korisniku (korišćenje kontakata iz skenera)	LDAP server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Provera identiteta korisnika prilikom prikupljanja informacija o korisnicima (kada se koriste kontakti sa skenera) Provera identiteta korisnika prilikom korišćenja skeniranja u mrežnu fasciklu (SMB) sa skenera	KDC server	Kerberos	88
Kontrolni WSD	Računar klijent	WSD (TCP)	5357
Pretraživanje računara prilikom skeniranja s uređaja pomoću aplikacije	Računar klijent	Otkrivanje na mreži za skeniranje s uređaja	2968

Kada je pošiljalac (klijent) računar klijent

Upotreba	Odredište (server)	Protokol	Broj ulaza
Otkrijte skener pomoću aplikacije kao što je EpsonNet Config i upravljački program skenera.	Skener	ENPC (UDP)	3289
Prikupite i podesite MIB informacije pomoću aplikacije kao što je EpsonNet Config i upravljački program skenera.	Skener	SNMP (UDP)	161
Traženje WSD skenera	Skener	Otkrivanje veb-servisa (UDP)	3702
Prosleđivanje skeniranih podataka iz aplikacije	Skener	Skeniranje mreže (TCP)	1865
Prikupljanje informacija o zadatku prilikom skeniranja s uređaja pomoću aplikacije	Skener	Skeniranje s uređaja na mreži	2968
Web Config	Skener	HTTP (TCP)	80
		HTTPS (TCP)	443

Rešavanje problema

Ne možete da se povežete sa mrežom

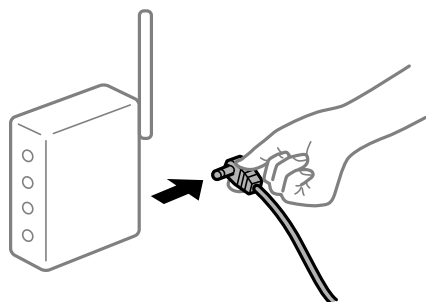
Problem bi mogao biti jedan od sledećih.

■ Nešto nije u redu sa mrežnim uređajima za bežičnu vezu.

Rešenja

Isključite uređaje koje želite da priključite na mrežu. Sačekajte oko 10 sekundi i zatim uključite uređaje sledećim redosledom: bežični mrežni usmerivač, računar ili pametni uređaj i zatim skener. Približite

skener i računar ili pametni uređaj bežičnom mrežnom usmerivaču da biste pomogli pri komunikaciji radio talasima, a zatim pokušajte da ponovo izvršite podešavanja mreže.



Uređaji ne mogu da prime signale sa bežičnog mrežnog usmerivača jer su previše udaljeni.

Rešenja

Nakon što približite računar ili pametni uređaj i skener bežičnom mrežnom usmerivaču, isključite bežični mrežni usmerivač i ponovo ga uključite.

Kada menjate bežični mrežni usmerivač, podešavanja ne odgovaraju novom mrežnom usmerivaču.

Rešenja

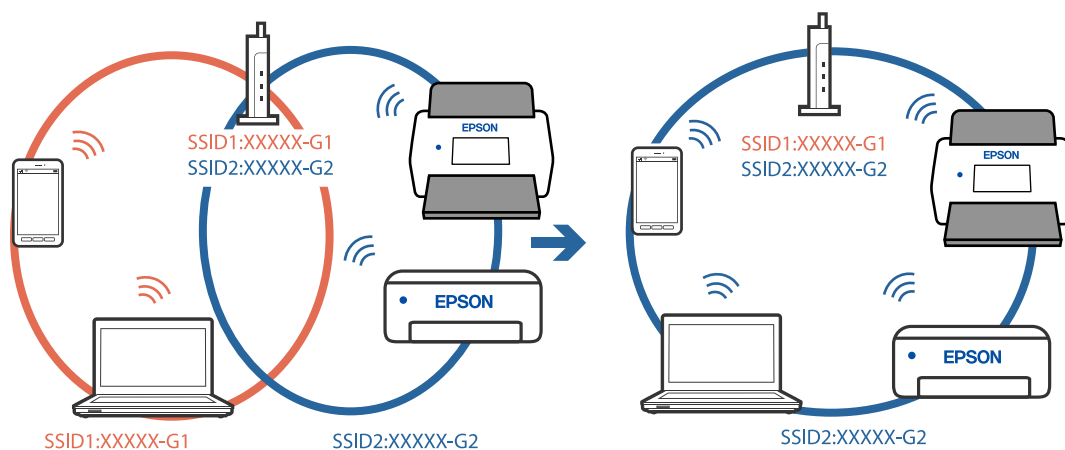
Ponovo izvršite podešavanja veze tako da odgovaraju novom bežičnom mrežnom usmerivaču.

SSID je drugačije povezan sa računara ili pametnog uređaja i računara.

Rešenja

Kada koristite više bežičnih mrežnih usmerivača u isto vreme ili bežični mrežni usmerivač ima više SSID-a ili uređaja povezanih na različite SSID-e, ne možete da se povežete na bežični mrežni usmerivač.

Priključite računar ili pametni uređaj na isti SSID kao i skener.



Dostupan je separator privatnosti na bežičnom mrežnom usmerivaču.

Rešenja

Većina bežičnih mrežnih usmerivača ima funkciju separatora privatnosti koja blokira komunikaciju između priključenih uređaja. Ako ne možete da komunicirate između skenera i računara ili pametnog uređaja, čak i ako su povezani na istu mrežu, onemogućite separator privatnosti na bežičnom mrežnom usmerivaču. Detalje potražite u priručniku priloženom uz bežični mrežni usmerivač.

■ IP adresa je nepravilno dodeljena.

Rešenja

Ako je skeneru dodeljena IP adresa 169.254.XXX.XXX, a podmrežna maska je 255.255.0.0, moguće je da IP adresa nije pravilno dodeljena.

Izaberite **Podešavanja > Mrežne postavke > Napredno > TCP/IP** na kontrolnoj tabli skenera, a zatim proverite IP adresu i podmrežnu masku dodeljenu skeneru.

Restartujte bežični mrežni usmerivač ili ponovo podesite mrežne postavke za skener.

■ Postoji problem sa mrežnim podešavanjima na računaru.

Rešenja

Pokušajte da pristupite nekom veb-sajtu sa svog računara da biste se uverili da su podešavanja mreže na vašem računaru tačna. Ako ne možete da pristupite nijednom veb-sajtu, postoji problem na računaru.

Proverite mrežno povezivanje računara. Detalje potražite u dokumentaciji priloženoj uz računar.

■ Skener je povezan preko Etherneta pomoću uređaja koji podržavaju IEEE 802.3az (Energetski efikasan Ethernet).

Rešenja

Kada povezujete skener preko Etherneta koristeći uređaje koji podržavaju IEEE 802.3az (Energetski efikasan Ethernet), mogu se pojaviti sledeći problemi zavisno od čvorišta ili bežičnog usmerivača koje koristite.

- Veza postaje nestabilna, skener se neprestano povezuje i prekida vezu.
- Ne možete da se povežete na skener.
- Brzina komunikacije postaje spora.

Sledite navedene korake da biste onemogućili IEEE 802.3az za skener a zatim se povežite.

1. Izvadite kabl za Ethernet koji je spojen sa računarom ili skenerom.
2. Kada je IEEE 802.3az za računar omogućen, onemogućite ga.
Detalje potražite u dokumentaciji priloženoj uz računar.
3. Povežite računar i skener direktno sa kablom za Ethernet.
4. Proverite podešavanja mreže na skeneru.
Izaberite **Podešavanja > Mrežne postavke > Status mreže > Status kablovske LAN/Wi-Fi mreže**.
5. Proverite IP adresu skenera.
6. Na računaru pristupite Web Config.
Pokrenite veb pregledač, a zatim unesite IP adresu skenera.
[“Pokretanje Web Config u veb pregledaču” na strani 35](#)
7. Izaberite karticu **Network > Wired LAN**.
8. Izaberite **OFF** za **IEEE 802.3az**.

9. Kliknite na **Next**.
10. Kliknite na **OK**.
11. Izvadite kabl za Ethernet koji je spojen sa računarom ili skenerom.
12. Ako ste onemogućili IEEE 802.3az za računar u drugom koraku, omogućite ga.
13. Povežite kablove za Ethernet koje ste skinuli u prvom koraku sa računarom ili skenerom.
Ako se problem i dalje pojavljuje, i drugi uređaji osim skenera mogu vam stvarati problem.

■ **Skener je isključen.**

Rešenja

Vodite računa da je skener uključen.

Takođe, sačekajte dok indikator statusa ne prestane da trepće pokazujući da je skener spreman da skenira.

Softver za podešavanje skenera

Web Config.	35
Epson Device Admin.	36

Web Config

Web Config je aplikacija koja radi u okviru veb pregledača kao što su Internet Explorer i Safari, na računaru. Možete potvrditi status skenera ili promeniti podešavanja mrežne usluge i skenera. S obzirom da skenerima pristupa i da se koriste direktno putem mreže, pogodno je za podešavanje skenera jednog po jednog. Da biste koristili Web Config, povežite računar na istu mrežu kao skener.

Podržani su sledeći pregledači.

Microsoft Edge, Windows Internet Explorer 8 ili noviji, Firefox*, Chrome*, Safari*

* Koristite najnoviju verziju.

Pokretanje Web Config u veb pregledaču

1. Proverite IP adresu skenera.

Izaberite **Podešavanja > Mrežne postavke > Status mreže** na kontrolnoj tabli skenera. A zatim izaberite aktivni način povezivanja (**Status kablovske LAN/Wi-Fi mreže** ili **Status Wi-Fi Direct**) da biste proverili IP adresu skenera.

2. Pokrenite mrežni pregledač sa računara ili pametnog uređaja i unesite IP adresu skenera.

Format:

IPv4: http://IP adresa skenera/

IPv6: http://[IP adresa skenera]/

Primeri:

IPv4: http://192.168.100.201/

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

Napomena:

S obzirom da skener koristi nezavisni sertifikat prilikom pristupanja HTTPS-u, u pregledaču se prikazuje upozorenje kada pokrenete Web Config; to ne ukazuje ni na kakav problem i može se bezbedno zanemariti.

3. Prijavite se kao administrator da izmenite podešavanja skenera.

Kliknite na **Administrator Login** u gornjem desnom delu ekrana. Unesite **User Name** i **Current password**, a zatim kliknite na **OK**.

Napomena:

- Sledeće stavke pružaju uvid u početne vrednosti za informacije o administratoru Web Config.

·Korisničko ime: ništa (prazno)

·Lozinka: serijski broj skenera

Da biste pronašli serijski broj, proverite nalepnicu na zadnjoj strani skenera.

- Ako se u gornjem desnom delu ekrana prikaže **Administrator Logout**, već ste se prijavili kao administrator.

Pokretanje aplikacije Web Config u operativnom sistemu Windows

Prilikom povezivanja računara na skener pomoću WSD, pratite korake u nastavku da biste pokrenuli Web Config.

1. Otvorite listu skenera na računaru.

Windows 10

Kliknite na dugme za početak i izaberite **Windows sistem > Kontrolna tabla > Prikaz uređaja i štampača u Hardver i zvuk**.

Windows 8.1/Windows 8

Izaberite **Radna površina > Podešavanja > Kontrolna tabla > Prikaz uređaja i štampača u Hardver i zvuk** (ili **Hardver**).

Windows 7

Kliknite na dugme Start i izaberite **Kontrolna tabla > Prikaz uređaja i štampača u Hardver i zvuk**.

2. Desnim tasterom miša kliknite na skener i izaberite **Svojstva**.

3. Izaberite karticu **Veb usluga** i kliknite na URL.

S obzirom da skener koristi nezavisni sertifikat prilikom pristupanja HTTPS-u, u pregledaču se prikazuje upozorenje kada pokrenete Web Config; to ne ukazuje ni na kakav problem i može se bezbedno zanemariti.

Napomena:

Sledeće stavke pružaju uvid u početne vrednosti za informacije o administratoru Web Config.

·Korisničko ime: ništa (prazno)

·Lozinka: serijski broj skenera

Da biste pronašli serijski broj, proverite nalepnicu na zadnjoj strani skenera.

*Ako se u gornjem desnom delu ekrana prikaže **Administrator Logout**, već ste se prijavili kao administrator.*

Epson Device Admin

Epson Device Admin je multifunkcionalna aplikacija koja vam omogućava da upravljate uređajima na mreži.

Možete da koristite šablone za konfiguraciju da biste primenili objedinjene postavke na više skenera na mreži, što je čini pogodnom za instaliranje i upravljanje više skenera.

Možete preuzeti Epson Device Admin sa Epsonove internet stranice za podršku. Za više detalja kako da koristite aplikaciju, pogledajte dokumentaciju ili pomoć za Epson Device Admin.

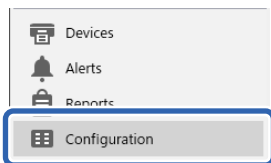
Šablon za konfiguraciju

Kreiranje šablona konfiguracije

Kreirajte novi šablon konfiguracije.

1. Pokrenite Epson Device Admin.

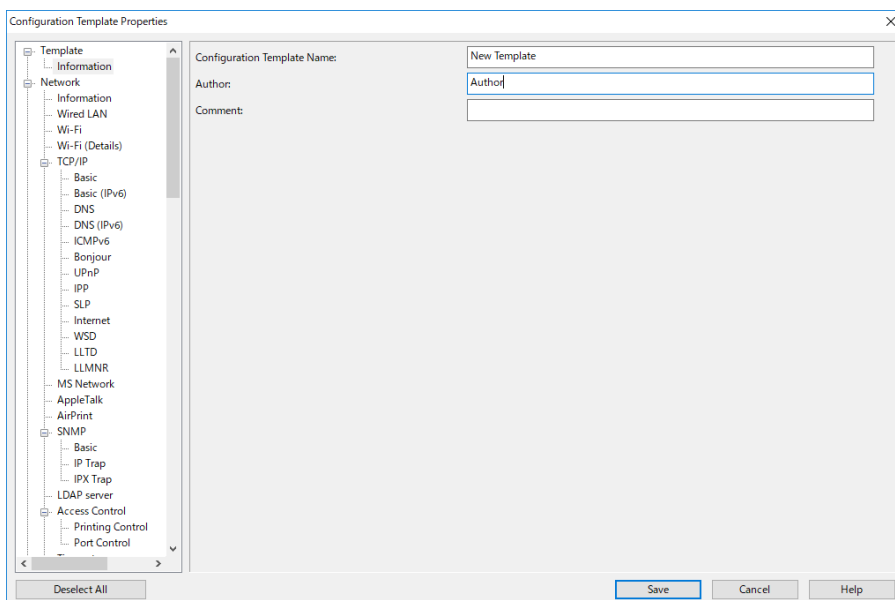
2. Izaberite **Configuration** u meniju zadataka na bočnoj traci.



3. Kliknite na **New** na trakastom meniju.



4. Podesite svaku stavku.



Stavka	Objašnjenje
Configuration Template Name	Naziv šablona za konfiguraciju. Unesite najviše 1024 znaka u formatu Unicode (UTF-8).
Author	Podaci o kreatoru šablona. Unesite najviše 1024 znaka u formatu Unicode (UTF-8).
Comment	Unesite proizvoljne podatke. Unesite najviše 1024 znaka u formatu Unicode (UTF-8).

5. Izaberite stavke koje želite da postaviti sa leve strane.

Napomena:

Kliknite na stavke menija sa leve strane da biste prešli na svaki ekran. Podešena vrednost se zadržava ako promenite ekran, ali ne i ako otkazete ekran. Kada završite sa svim podešavanjima, kliknite na **Save**.

Primena šablona za konfiguraciju

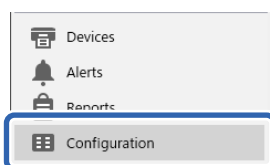
Primenite sačuvani šablon za konfiguraciju na skener. Primenjuju se stavke izabrane na šablonu. Ako ciljani skener nema odgovarajuće funkcije, neće se primeniti.

Napomena:

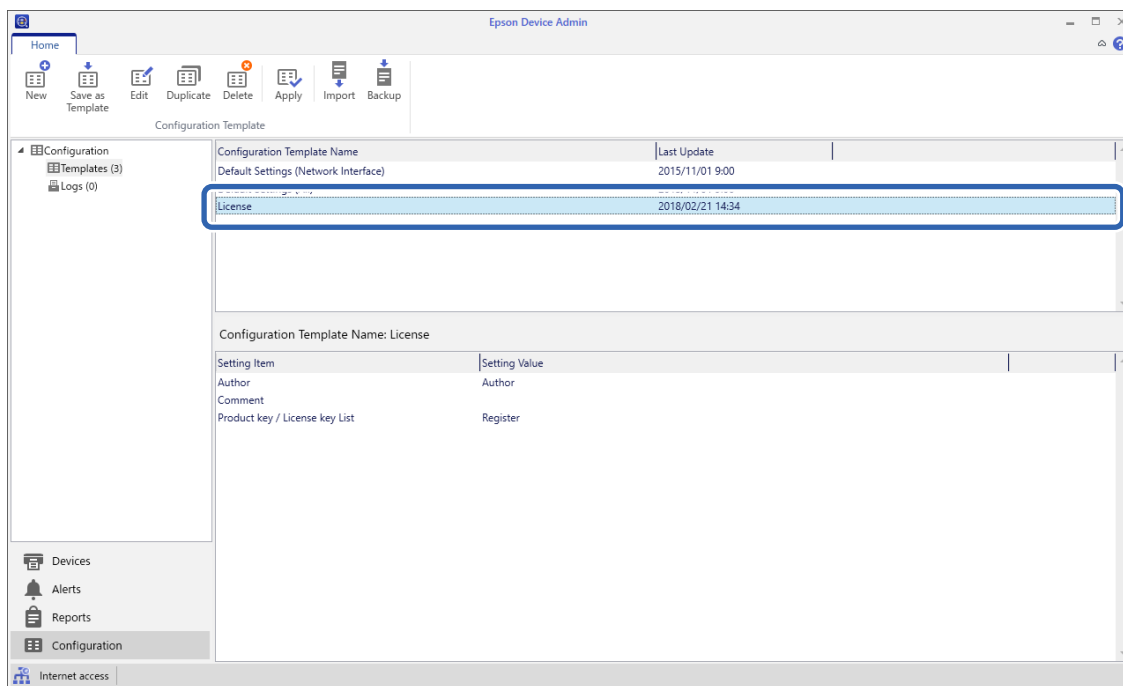
Kada je za skener podešena administratorska lozinka, unapred konfigurirajte lozinku.

1. Na trakastom meniju ekrana liste uređaja, izaberite **Options > Password manager**.
2. Izaberite **Enable automatic password management**, a zatim kliknite na **Password manager**.
3. Izaberite odgovarajući skener, a zatim kliknite na **Edit**.
4. Podesite lozinku, a zatim kliknite na **OK**.

1. Izaberite **Configuration** u meniju zadataka na bočnoj traci.



2. Izaberite šablon za konfiguraciju koji želite da primenite iz **Configuration Template Name**.



3. Kliknite **Apply** na trakastom meniju.
Prikazuje se ekran za izbor uređaja.

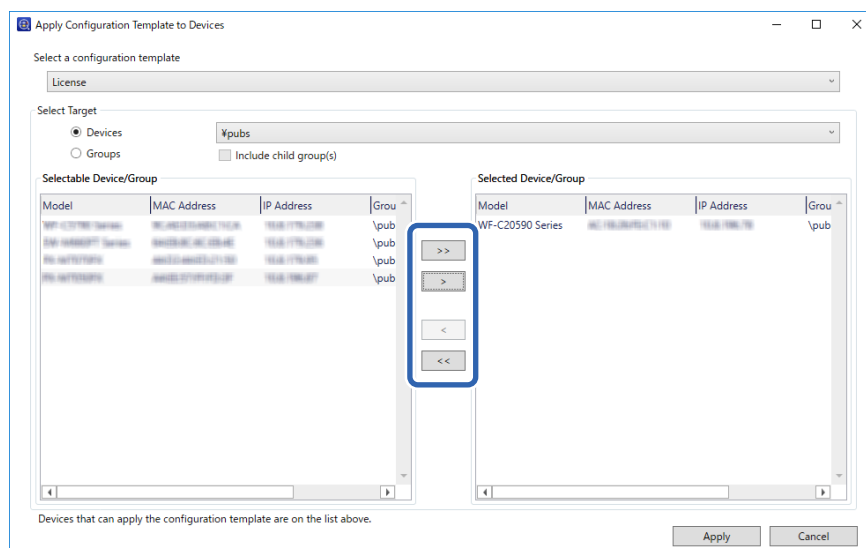


- Izaberite šablon za konfiguraciju koji želite da primenite.

Napomena:

- Kada izaberete **Devices** i grupe koje sadrže uređaje iz padajućeg menija, svaki uređaj se prikazuje.
- Prikazuju se grupe kada izaberete **Groups**. Izaberite **Include child group(s)** da biste automatski izabrali male grupe unutar izabrane grupe.

- Pomerite skener ili grupe na koje želite da primenite šablon **Selected Device/Group**.



- Kliknite na **Apply**.

Prikazuje se ekran za potvrdu šablona za konfiguraciju koji treba primeniti.

- Kliknite na **OK** da biste primenili šablon za konfiguraciju.

- Kada se prikaže poruka koja vas obaveštava da je postupak završen, kliknite na **OK**.

- Kliknite na **Details** i proverite informacije.

Kada se prikaže na stavkama koje ste primenili, aplikacija je uspešno završena.

- Kliknite na **Close**.

Podešavanja potrebna za skeniranje

Konfigurisanje servera za poštu.	41
Podešavanje deljene mrežne fascikle.	44
Dostupnost kontakata.	61
Korišćenje funkcije Document Capture Pro Server.	71
Podešavanje funkcije AirPrint.	71
Problemi prilikom pripreme skeniranja preko mreže.	72

Konfigurisanje servera za poštu

Podesite server za poštu iz Web Config.

Kada skener može da šalje e-poruke podešavanjem servera za poštu, moguće su sledeće situacije.

- Prenosi rezultate skeniranja pomoću e-pošte
- Prima obaveštanja elektronskom porukom sa skenera

Proverite sledeće pre podešavanja.

- Skener je povezan na mrežu koja može da pristupi serveru e-pošte.
- Informacije o podešavanju elektronske pošte na računaru koji koristi isti sever e-pošte kao i skener.

Napomena:

- Kada koristite server za e-poštu na mreži, potvrdite informacije o podešavanju od servisnog predstavnika ili sa veb-lokacije.
- Takođe možete podesiti server za e-poštu na kontrolnoj tabli skenera. Pristupite kao što je ispod opisano.

Podešavanja > Mrežne postavke > Napredno > Server za imejl > Postavke servera

1. Pristupite Web Config i izaberite karticu **Network > Email Server > Basic**.
2. Unesite vrednost za svaku stavku.
3. Izaberite **OK**.
Podešavanja koja ste izabrali su prikazana.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Stavke podešavanja servera za poštu

Stavke	Podešavanja i objašnjenje	
Authentication Method	Navedite metod provere identiteta koji će se koristiti kada skener pristupa serveru za poštu.	
	Off	Autorizacija je onemogućena prilikom komunikacije sa serverom za poštu.
	SMTP AUTH	Zahteva da server za poštu podržava SMTP autorizaciju.
	POP before SMTP	Ako izaberete ovaj metod, konfigurirate POP3 server.
Authenticated Account	Ako izaberete SMTP AUTH ili POP before SMTP kao Authentication Method , unesite ime naloga za proveru identiteta dužine između 0 i 255 znakova u ASCII-ju (0x20 do 0x7E).	
Authenticated Password	Ako izaberete SMTP AUTH ili POP before SMTP kao Authentication Method , unesite autorizovanu lozinku dužine između 0 i 20 znakova u ASCII formatu (0x20 do 0x7E).	
Sender's Email Address	Unesite adresu e-pošte pošiljaoca. Unesite od 0 do 255 alfanumeričkih znakova u formatu ASCII (0x20–0x7E), osim : () < > [] ; ¥. Tačka („.") ne može da se nalazi na početnoj poziciji.	

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

Provera veze sa serverom e-pošte

Možete da proverite vezu servera za poštu izvođenjem provere veze.

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

Zapoćeće provera veze sa serverom e-pošte. Nakon testa, prikazuje se izveštaj o proveri.

Napomena:

Takođe možete izvršiti proveru veze sa serverom e-pošte na kontrolnoj tabli. Pristupite kao što je ispod opisano.

Podešavanja > Mrežne postavke > Napredno > Server za imejl > Provera veze

Reference testiranja veze sa serverom za poštu

Poruke	Uzrok
Connection test was successful.	Ova poruka se prikazuje kada je veza sa serverom uspešna.
SMTP server communication error. Check the following. - Network Settings	<p>Ova poruka se prikazuje kad</p> <ul style="list-style-type: none"> <input type="checkbox"/> Skener nije povezan na mrežu <input type="checkbox"/> SMTP server ne radi <input type="checkbox"/> Veza se prekida u toku komunikacije <input type="checkbox"/> Primljeni su nepotpuni podaci

Poruke	Uzrok
POP3 server communication error. Check the following. - Network Settings	Ova poruka se prikazuje kad <ul style="list-style-type: none"> <input type="checkbox"/> Skener nije povezan na mrežu <input type="checkbox"/> POP3 server ne radi <input type="checkbox"/> Veza se prekida u toku komunikacije <input type="checkbox"/> Primljeni su nepotpuni podaci
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Ova poruka se prikazuje kad <ul style="list-style-type: none"> <input type="checkbox"/> Povezivanje sa DNS serverom nije uspelo <input type="checkbox"/> Rezolucija naziva za SMTP server nije uspela
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Ova poruka se prikazuje kad <ul style="list-style-type: none"> <input type="checkbox"/> Povezivanje sa DNS serverom nije uspelo <input type="checkbox"/> Rezolucija naziva za POP3 server nije uspela
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka se prikazuje kada SMTP provera identiteta ne uspe.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka se prikazuje kada POP3 provera identiteta ne uspe.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Ova poruka se prikazuje kada pokušate da komunicirate sa nepodržanim protokolima.
Connection to SMTP server failed. Change Secure Connection to None.	Ova poruka se prikazuje kada se ne poklapa SMTP između servera i klijenta, ili kada server ne podržava SMTP bezbednu vezu (SSL vezu).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Ova poruka se prikazuje kada se ne poklapa SMTP između servera i klijenta, ili kada server zatraži korišćenje SSL/TLS povezivanja za SMTP bezbednu vezu.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Ova poruka se prikazuje kada se ne poklapa SMTP između servera i klijenta, ili kada server zatraži korišćenje STARTTLS povezivanja za SMTP bezbednu vezu.
The connection is untrusted. Check the following. - Date and Time	Ova poruka se prikazuje kada je podešavanje datuma i vremena skenera neispravno ili ako je sertifikat istekao.
The connection is untrusted. Check the following. - CA Certificate	Ova poruka se prikazuje kada skener nema osnovni sertifikat koji odgovara serveru ili CA Certificate nije uvezen.
The connection is not secured.	Ova poruka se prikazuje kada je pribavljeni sertifikat oštećen.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Ova poruka se prikazuje kada se ne poklapa metoda provere identiteta između servera i klijenta. Server podržava SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Ova poruka se prikazuje kada se ne poklapa metoda provere identiteta između servera i klijenta. Server ne podržava SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	Ova poruka se prikazuje kada je adresa e-pošte određenog pošiljaoca pogrešna.

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

Podešavanje deljene mrežne fascikle

Podesite deljenu mrežnu fasciklu da biste sačuvali skeniranu sliku.

Kada čuvate datoteku u fasciklu, skener se prijavljuje kao korisnik računara na kom je fascikla kreirana.

Kreiranje deljene fascikle

Povezane informacije

- ➔ [“Pre nego što napravite deljenu fasciklu” na strani 44](#)
- ➔ [“Provera mrežnog profila” na strani 44](#)
- ➔ [“Mesto na kom je deljena fascikla napravljena i primer bezbednosti” na strani 45](#)
- ➔ [“Dodavanje grupe ili korisnika koji dozvoljava pristup” na strani 58](#)

Pre nego što napravite deljenu fasciklu

Pre nego što napravite deljenu fasciklu, proverite sledeće.

- Skener je povezan na mrežu preko koje ima pristup računaru gde će biti napravljena deljena fascikla.
- Višebajtni znakovi nisu uključeni u ime računara gde će biti napravljena deljena fascikla.



Važno:


Kada su višebajtni znakovi uključeni u ime računara, čuvanje datoteke u deljenu fasciklu možda neće uspeti.

U tom slučaju, pređite na računar koji ne obuhvata višebajtnne znakove u imenu ili promenite ime računara.

Kada menjate ime računara, vodite računa da unapred proverite sa administratorom zato što to može uticati na neka podešavanja, kao što su upravljanje računarom, pristup resursima itd.

Provera mrežnog profila

Na računaru gde će biti napravljena deljena fascikla proverite da li je dostupna deljena fascikla.

1. Prijavite se na računar na kom će deljena fascikla biti kreirana uz pomoć korisničkog naloga sa nadležnošću administratora.
2. Izaberite **Kontrolnu tablu > Mreža i internet > Centar za mrežu i deljenje**.
3. Kliknite na **Promenite napredne postavke deljenja**, a zatim kliknite na  za profil sa **(trenutni profil)** u prikazanim mrežnim profilima.

4. Proverite da li je **Uključi deljenje datoteka i štampača** izabrano na **Deljenje datoteka i štampača**.

Ako je opcija već izabrana, kliknite na **Otkazi** i zatvorite prozor.

Kada menjate podešavanja, kliknite na **Sačuvaj izmene** i zatvorite prozor.

Mesto na kom je deljena fascikla napravljena i primer bezbednosti

Zavisno od mesta na kom je deljena fascikla napravljena, bezbednost i pogodnost mogu se razlikovati.

Radi upotrebe deljene fascikle sa skenera ili drugih računara potrebne su sledeće dozvole za čitanje i menjanje fascikle.

Kartica **Deljenje** > **Napredno deljenje** > **Dozvole**

Proverava dozvolu za mrežni pristup deljenoj fascikli.

Dozvola pristupa kartice **Bezbednost**

Upravlja dozvolom za mrežni pristup i lokalni pristup deljenoj fascikli.

Kada podesite **Svi** za deljenu fasciklu koja je napravljena na radnoj površini, kao primer kreiranja deljene fascikle, svim korisnicima koji mogu da pristupe računaru biće dozvoljen pristup.

Međutim, korisnik koji nema ovlašćenje ne može da im pristupi, jer radna površina (fascikla) je pod kontrolom korisničke fascikle, tako da joj se predaju bezbednosna podešavanja korisničke fascikle. Korisnik kojem je dozvoljen pristup na karticu **Bezbednost** (u ovom slučaju korisnik koji je prijavljen i koji je administrator) može da koristi fasciklu.

Pogledajte u nastavku kako kreirati pravilno mesto.

Ovo je primer kada se kreira „scan_folder”.

Povezane informacije

➔ [“Primer konfiguracije servera za datoteku” na strani 45](#)

➔ [“Primer konfiguracije za lični računar” na strani 52](#)

Primer konfiguracije servera za datoteku

Ovo objašnjenje je primer za kreiranje deljene fascikle u osnovnom direktorijumu diska na deljenom računaru, kao što je server za datoteku pod sledećim uslovima.

Pristup upravljivim korisnicima, kao što je neko ko ima isti domen računara za kreiranje deljene fascikle, može da pristupi deljenoj fascikli.

Podesite ovu konfiguraciju kada dozvoljavate bilo kom korisniku da čita ili piše u deljenu fasciklu na računaru, kao što je server za datoteku i deljeni računar.

Mesto za kreiranje deljene fascikle: osnovi direktorijum na disku

Putanja do fascikle: C:\scan_folder

Dozvolite pristup preko mreže (Dozvole za deljeni resurs): Svi

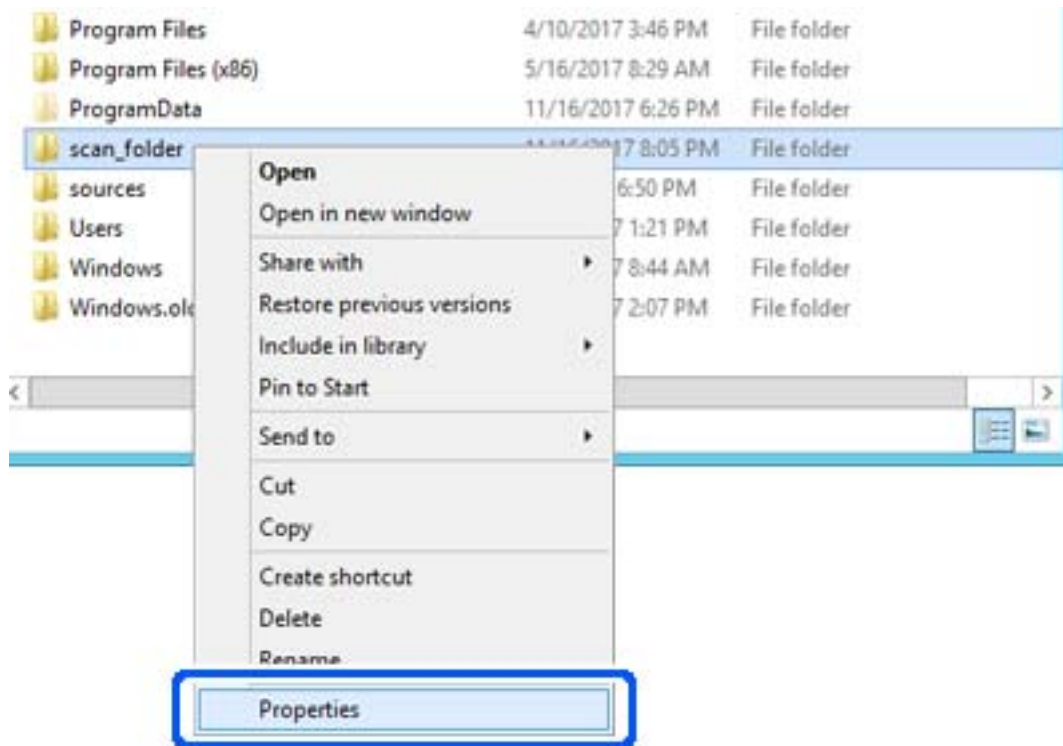
Dozvolite pristup sistemu datoteka (Bezbednost): Ovlašćeni korisnici

1. Prijavite se na računar na kom će deljena fascikla biti kreirana uz pomoć korisničkog naloga sa nadležnošću administratora.
2. Pokrenite pregledač.

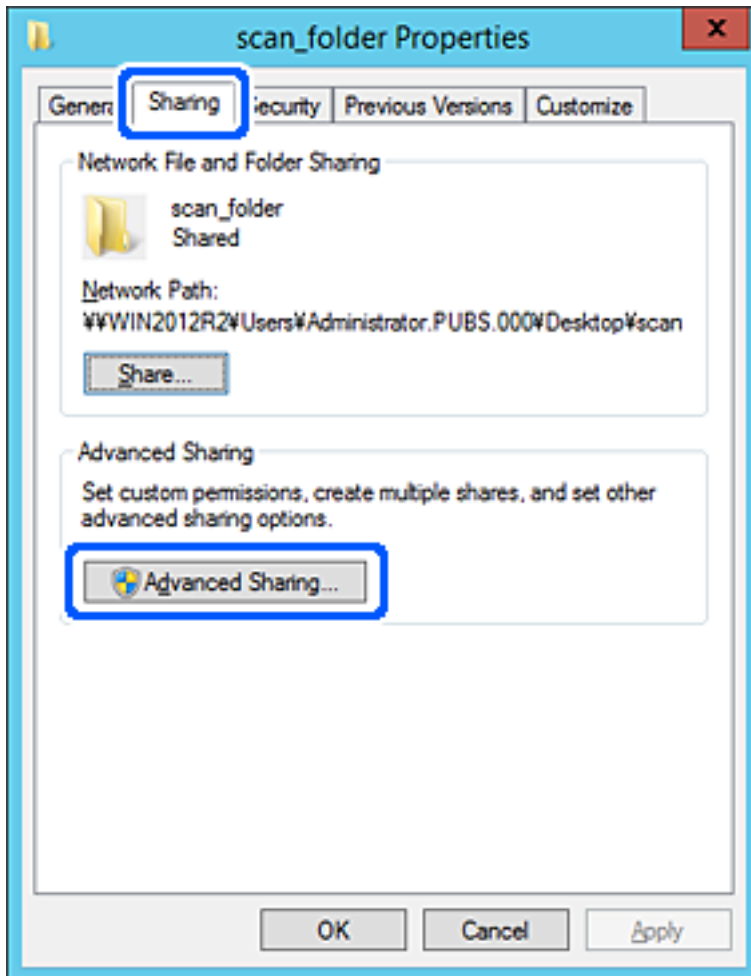
3. Kreirajte fasciklu u osnovnom direktorijumu na disku i nazovite je „scan_folder”.

Za naziv fascikle unesite od 1 do 12 alfanumeričkih znakova. Ako se prekorači ograničenje znakova naziva fascikle, možda nećete biti u mogućnosti da normalno pristupite pomoću promenljivog okruženja.

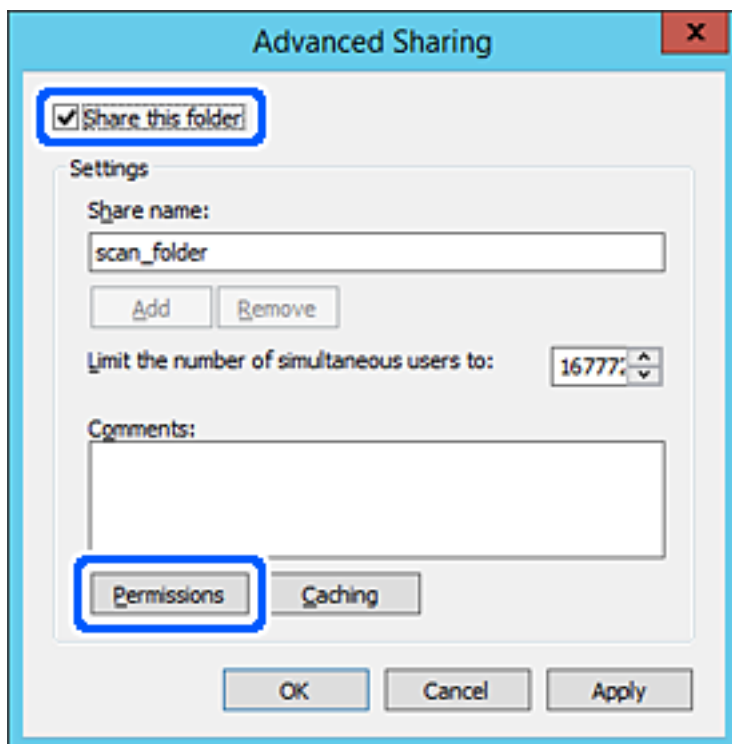
4. Kliknite desnim tasterom miša na fasciklu, a zatim izaberite **Svojstva**.



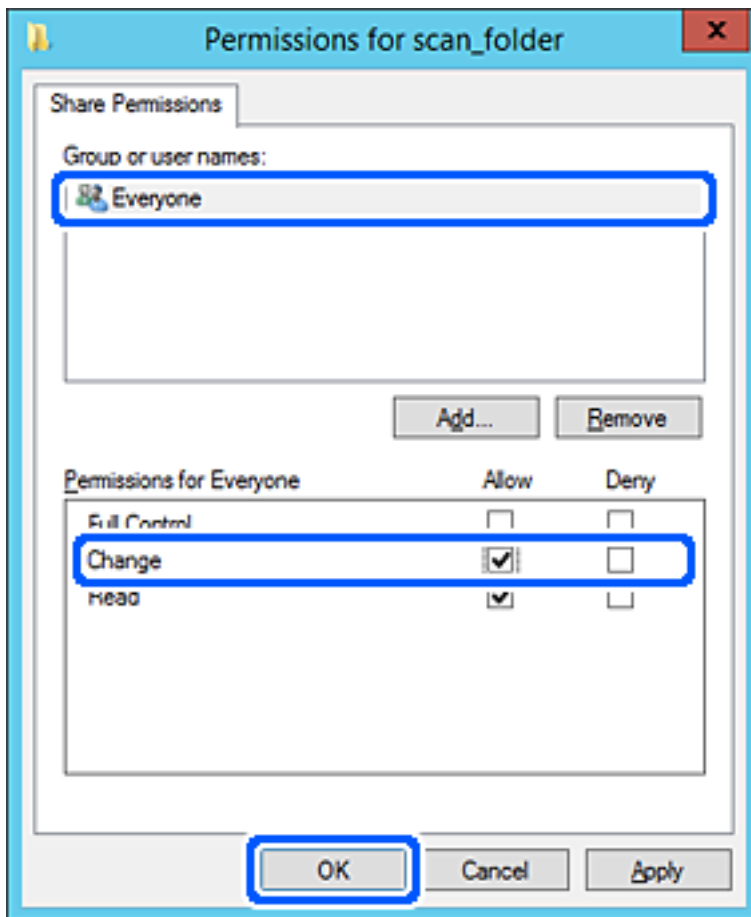
5. Kliknite na **Napredno deljenje** na kartici **Deljenje**.



- Izaberite **Deli ovu fasciklu**, a zatim kliknite na **Dozvole**.

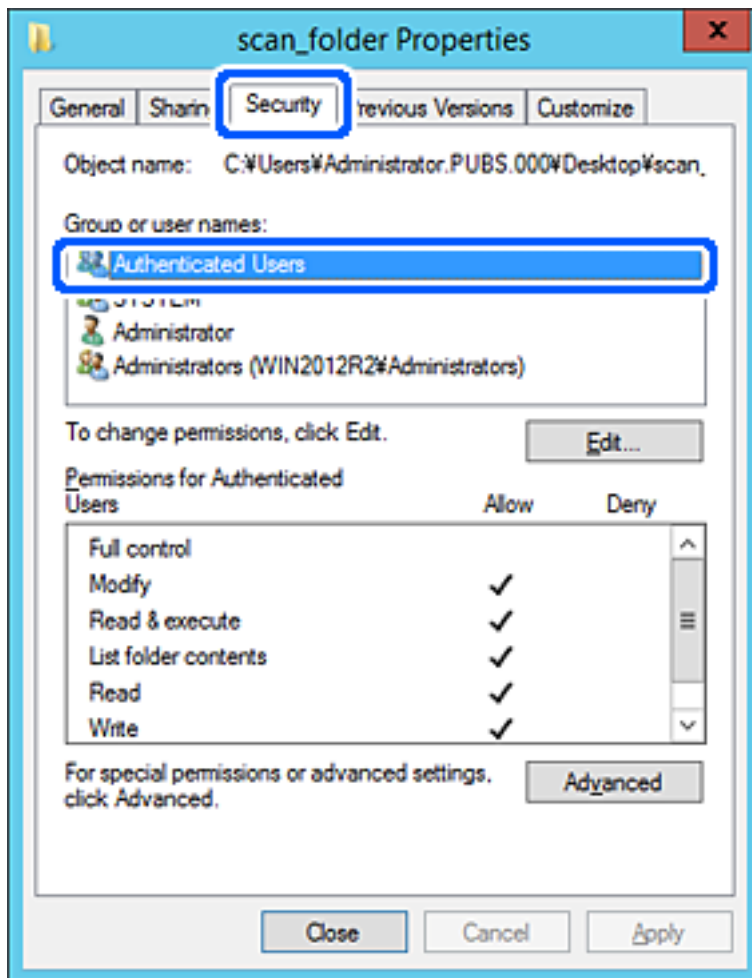


- Izaberite grupu **Svi** iz **Imena grupa ili korisnička imena**, izaberite **Omogući** pod **Promeni**, a zatim kliknite na **OK**.



- Kliknite na **OK**.

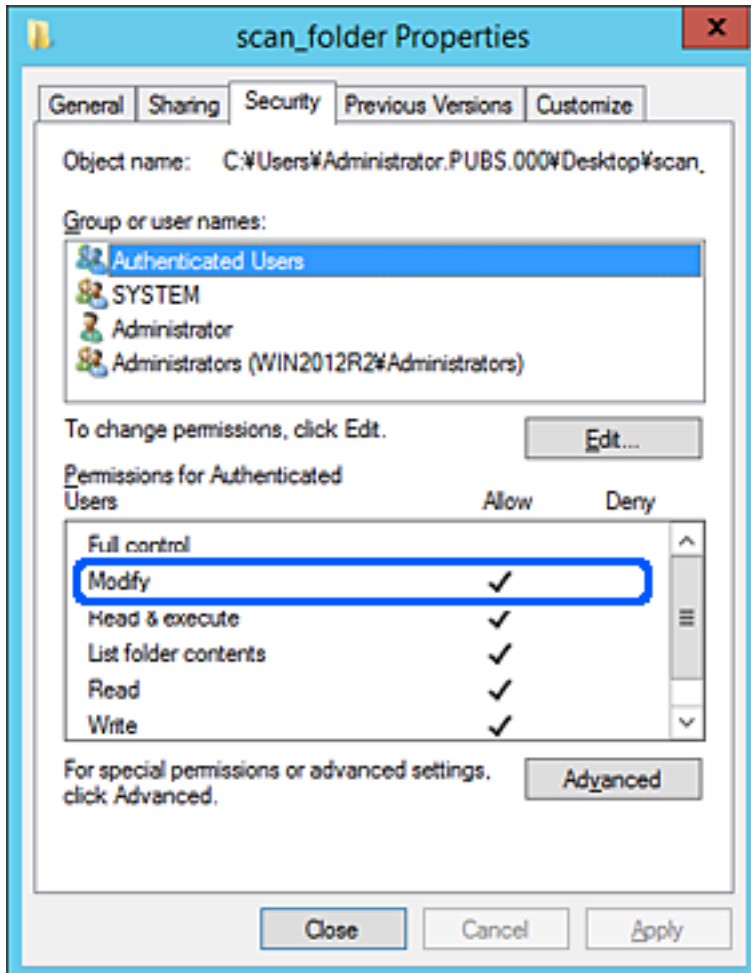
9. Izaberite karticu **Bezbednost**, a zatim izaberite **Ovlašćeni korisnici** pod **Imena grupa ili korisnička imena**.



„Ovlašćeni korisnici” je posebna grupa koja obuhvata sve korisnike koji mogu da se prijave na domen ili računar. Ova grupa se prikazuje samo kada je fascikla kreirana odmah ispod fascikle osnovnog direktorijuma. Ako se ne prikaže, možete je dodati klikom na **Uredi**. Više detalja potražite u povezanim informacijama.

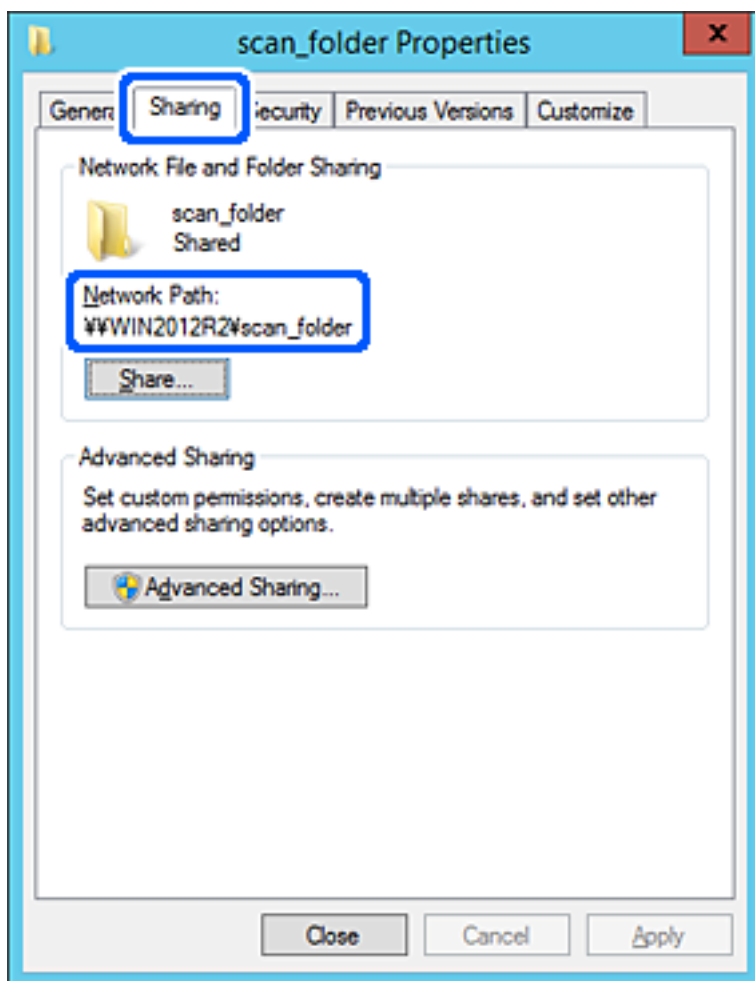
10. Proverite da li je **Omogući** na **Izmeni** izabrano u **Dozvole za ovlašćene korisnike**.

Ako nije izabrano, izaberite **Ovlašćeni korisnici**, kliknite na **Uredi**, izaberite **Omogući** na **Izmeni** u **Dozvole za ovlašćene korisnike**, a zatim kliknite na **OK**.



11. Izaberite karticu **Deljenje**.

Prikazuje se mrežna putanja deljene fascikle. Koristi se kada se registrujete na kontakte skenera. Zapišite je.



12. Kliknite na **OK** ili **Zatvori** da biste zatvorili ekran.

Proverite da li se u datoteku može upisivati ili čitati u deljenoj fascikli sa računara istog domena.

Povezane informacije

- ➔ “Dodavanje grupe ili korisnika koji dozvoljava pristup” na strani 58
- ➔ “Registrowanje odredišta u kontaktima pomoću Web Config” na strani 62

Primer konfiguracije za lični računar

Ovo objašnjenje je primer za kreiranje deljene fascikle na radnoj površini korisnika koji se trenutno prijavljuje na računar.

Korisnik koji se prijavi na računar i koji ima nadležnost administratora može da pristupi fascikli na radnoj površini i fascikli dokumenata koje se nalaze pod korisničkom fasciklom.

Podesite ovu konfiguraciju kada NE dozvoljavate drugom korisniku da čita ili piše po deljenoj fascikli na ličnom računaru.

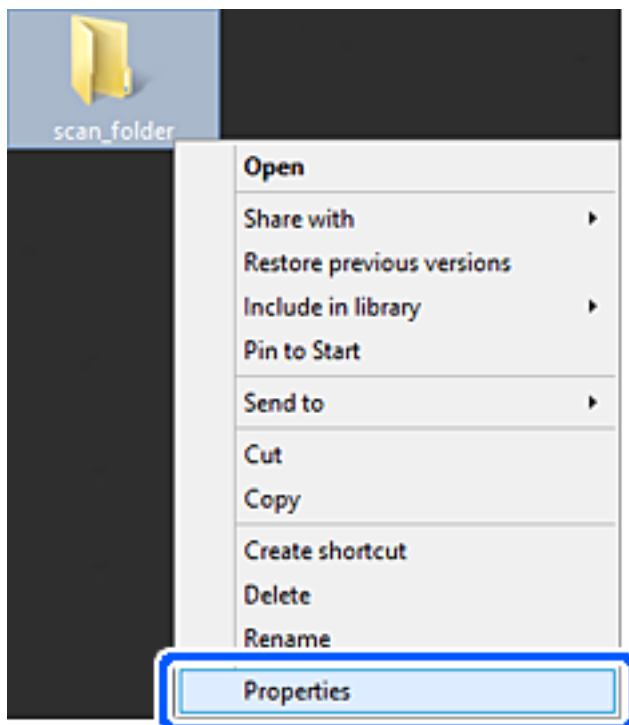
- Mesto za kreiranje deljene fascikle: radna površina

- Putanja do fascikle: C:\Users\xxxx\Desktop\scan_folder
- Dozvolite pristup preko mreže (Dozvole za deljeni resurs): Svi
- Dozvolite pristup sistemu datoteka (Bezbednost): nemojte dodavati ili dodajte ime korisnika/grupe da biste dozvolili pristup

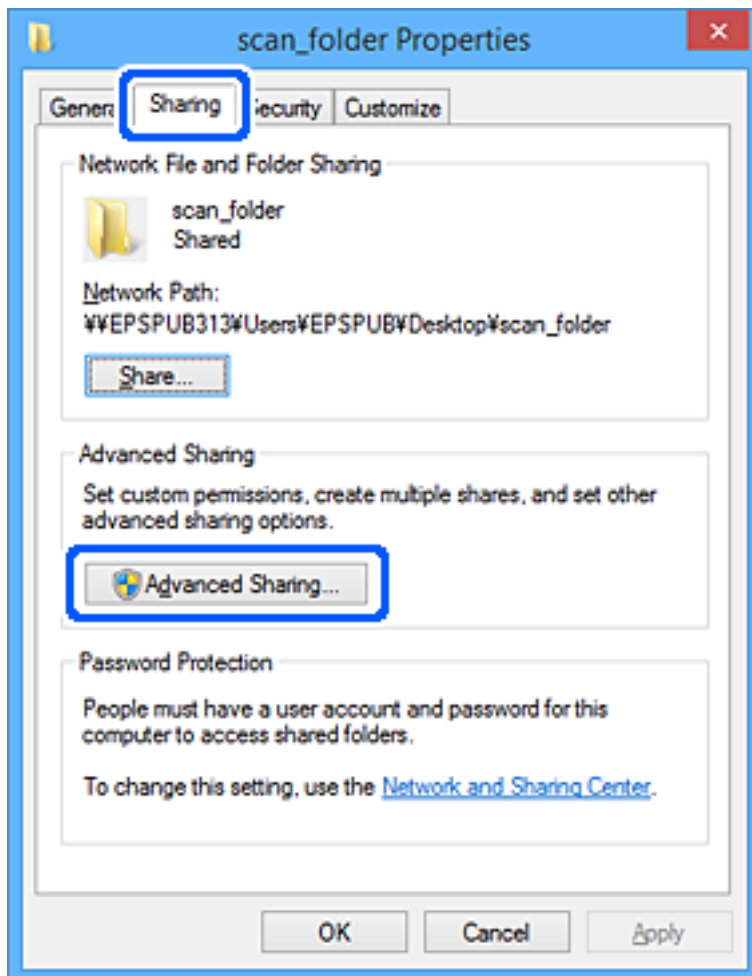
1. Prijavite se na računar na kom će deljena fascikla biti kreirana uz pomoć korisničkog naloga sa nadležnošću administratora.
2. Pokrenite pregledač.
3. Kreirajte fasciklu na radnoj površini i nazovite je „scan_folder”.

Za naziv fascikle unesite od 1 do 12 alfanumeričkih znakova. Ako se prekorači ograničenje znakova naziva fascikle, možda nećete biti u mogućnosti da normalno pristupite pomoću promenljivog okruženja.

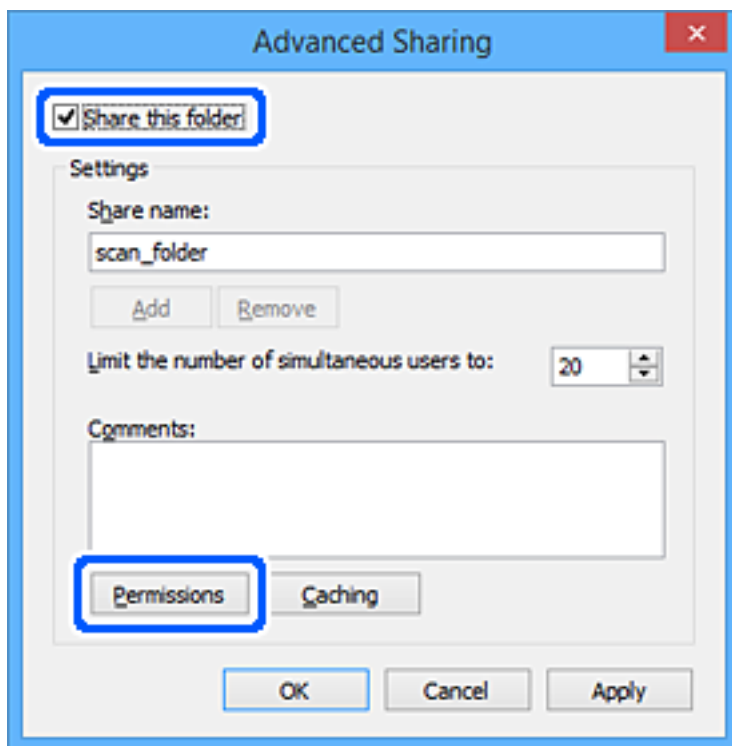
4. Kliknite desnim tasterom miša na fasciklu, a zatim izaberite **Svojstva**.



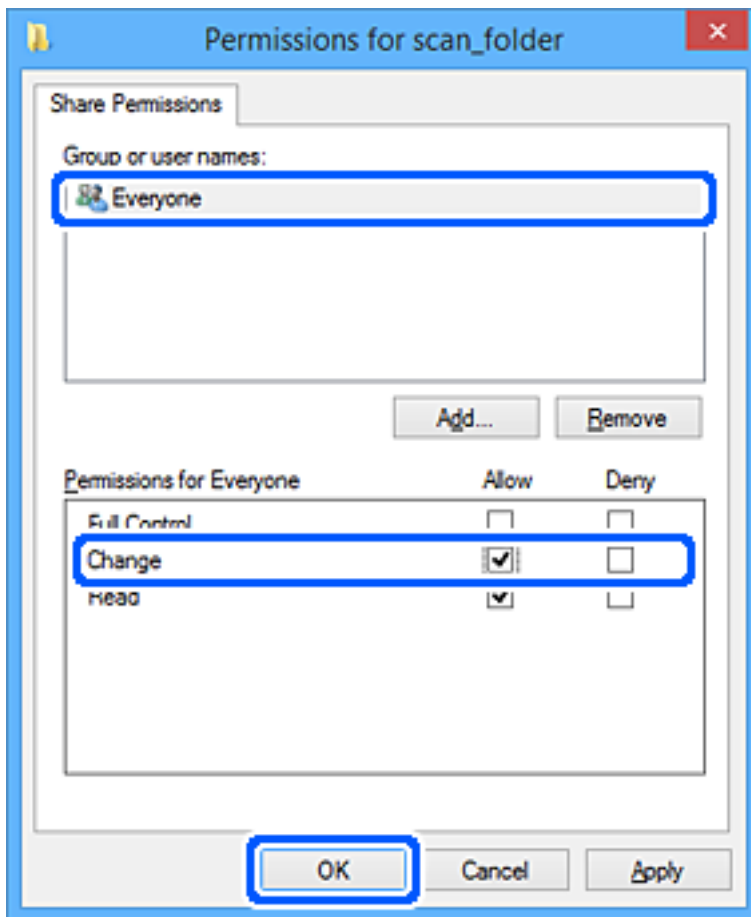
5. Kliknite na **Napredno deljenje** na kartici **Deljenje**.



- Izaberite **Deli ovu fasciklu**, a zatim kliknite na **Dozvole**.

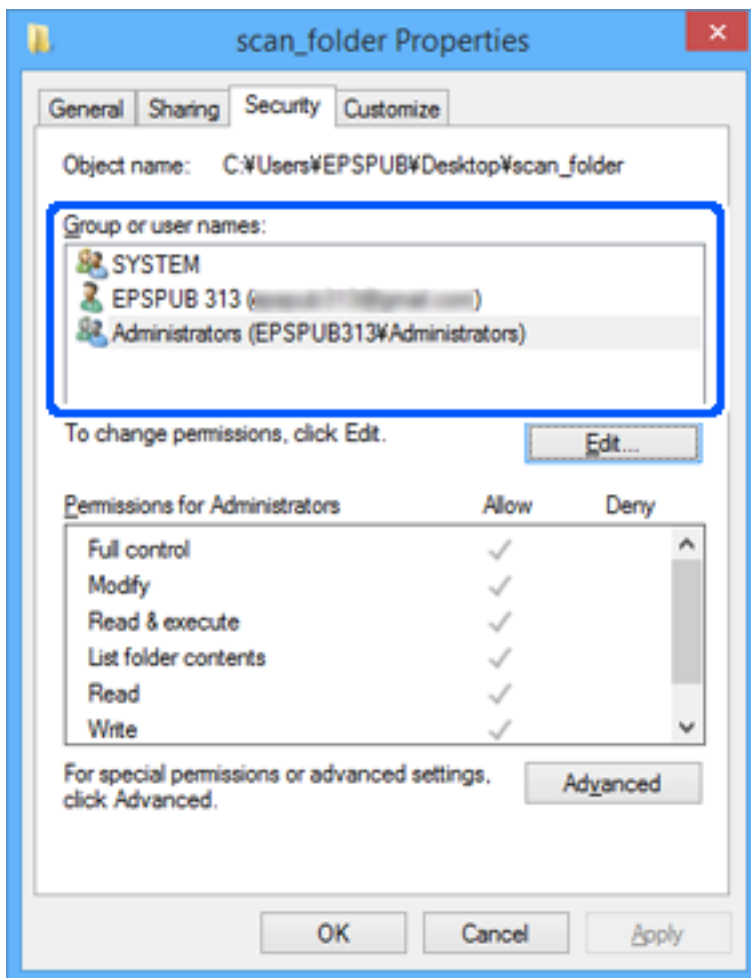


- Izaberite grupu **Svi** iz **Imena grupa ili korisnička imena**, izaberite **Omogući** pod **Promeni**, a zatim kliknite na **OK**.



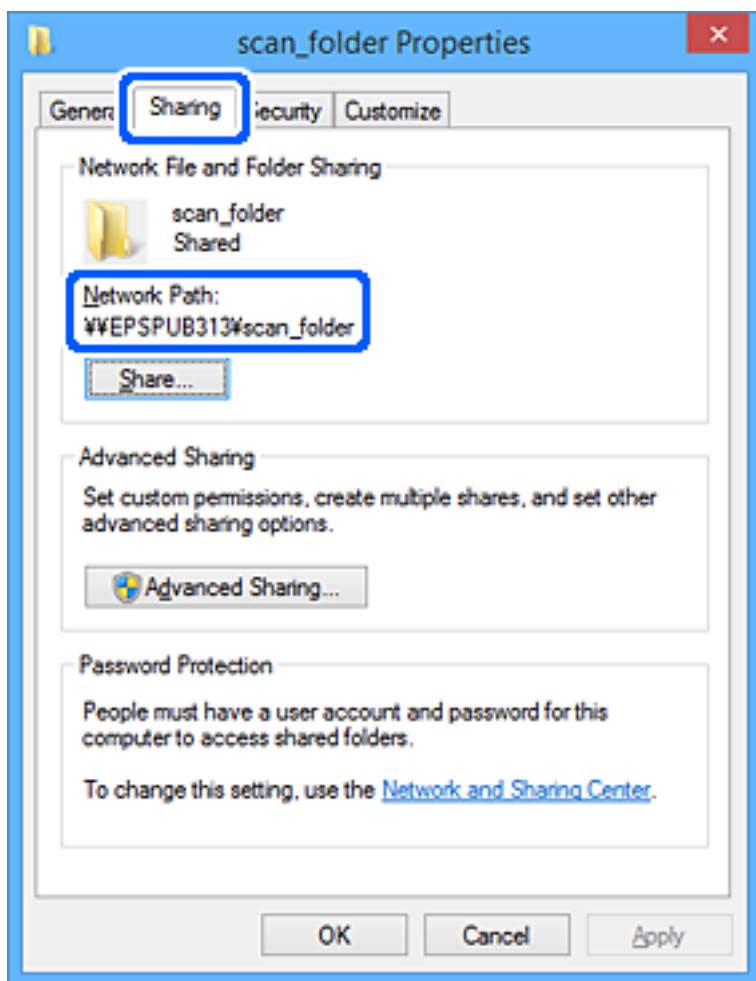
- Kliknite na **OK**.
- Izaberite karticu **Bezbednost**.
- Proverite grupu ili korisnika u **Imena grupa ili korisnička imena**.
Grupa ili korisnik koji se ovde prikaže može da pristupi deljenoj fascikli.
U ovom slučaju, korisnik koji se prijavi na ovaj računar i administrator mogu da pristupe deljenoj fascikli.

Ako treba, dodajte dozvolu pristupa. Možete ga dodati klikom na **Uredi**. Više detalja potražite u povezanim informacijama.



11. Izaberite karticu **Deljenje**.

Prikazuje se mrežna putanja deljene fascikle. Koristi se kada se registrujete na kontakte skenera. Zapišite je.



12. Kliknite na **OK** ili **Zatvori** da biste zatvorili ekran.

Proverite da li se u datoteku može upisivati ili čitati u deljenoj fascikli sa računara korisnika ili grupa sa dozvoljenim pristupom.

Povezane informacije

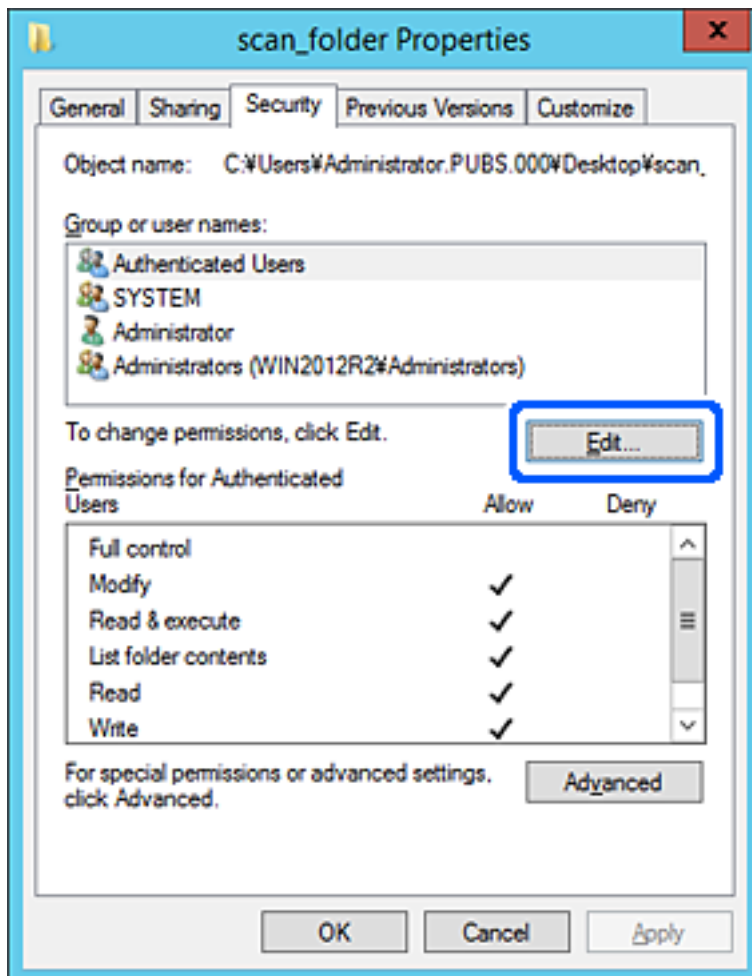
- ➔ “Dodavanje grupe ili korisnika koji dozvoljava pristup” na strani 58
- ➔ “Registrowanje odredišta u kontaktima pomoću Web Config” na strani 62

Dodavanje grupe ili korisnika koji dozvoljava pristup

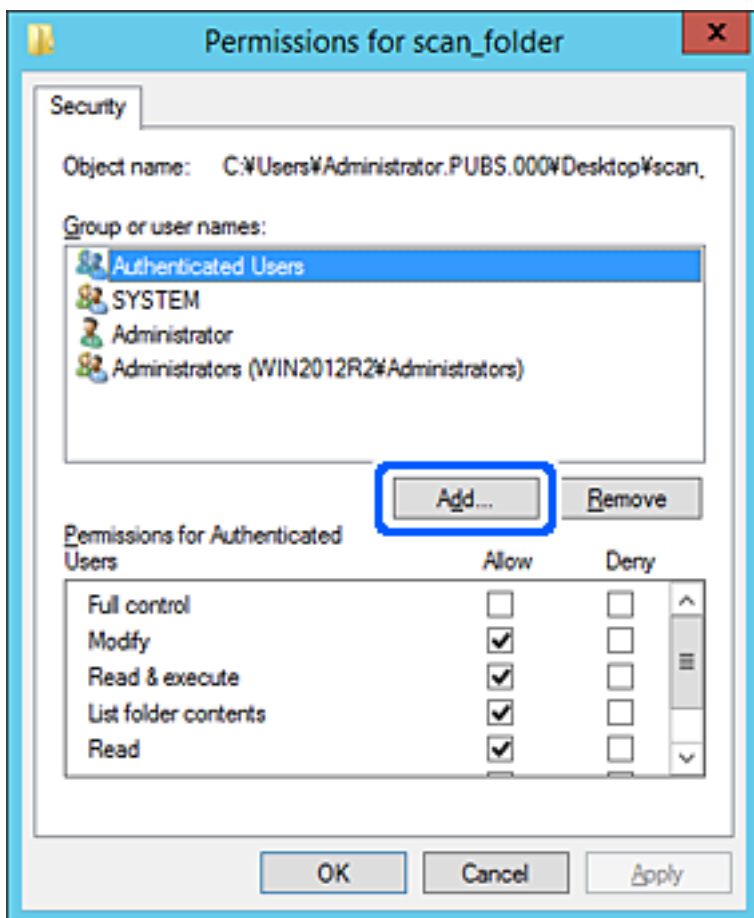
Možete da dodate grupu ili korisnika koji dozvoljava pristup.

1. Kliknite desnim tasterom miša na fasciklu i izaberite **Svojstva**.
2. Izaberite karticu **Bezbednost**.

3. Kliknite na Uredi.



4. Kliknite Dodaj pod Imena grupa ili korisnička imena.



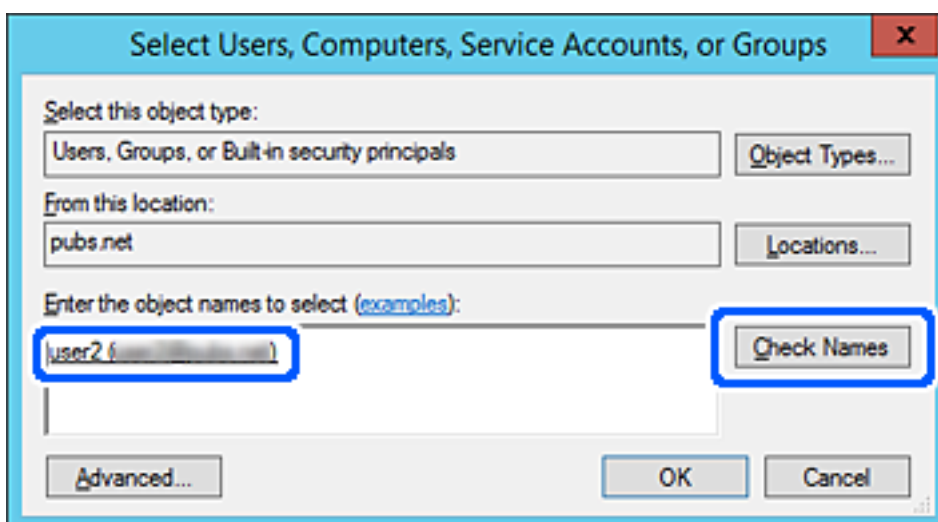
5. Unesite ime grupe ili korisničko ime kojem želite da dozvolite pristup, a zatim kliknite na **Proveri imena**.

Ime se podvlači.

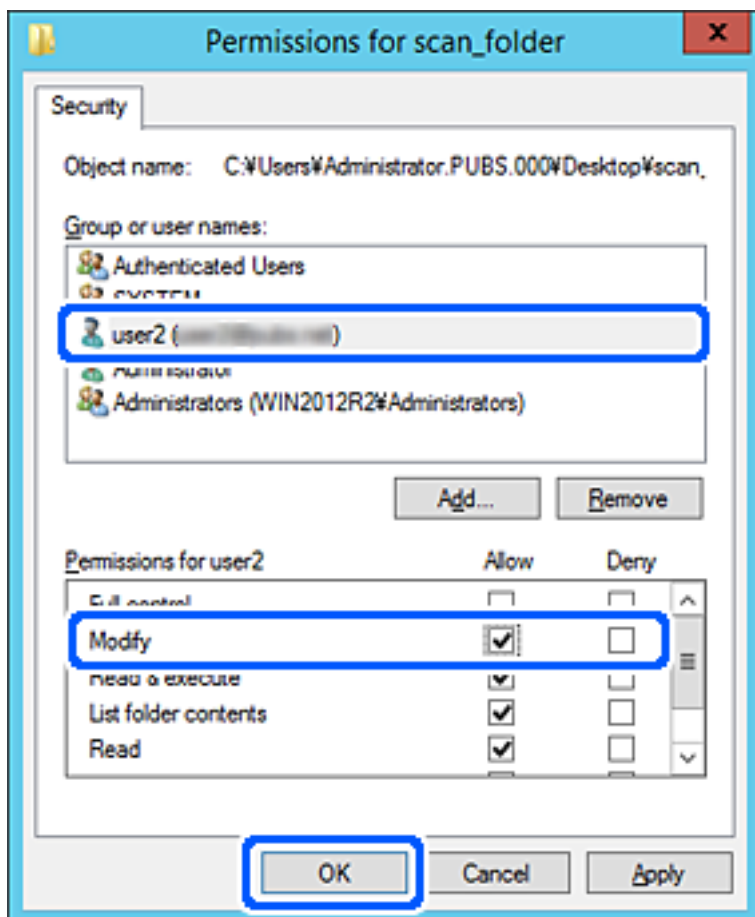
Napomena:

Ako ne znate celo ime grupe ili korisnika, unesite deo imena i zatim kliknite na **Proveri imena**. Navode se imena grupe ili korisnika koja odgovaraju delu imena, a zatim možete da izaberete celo ime sa liste.

Ako se podudara samo jedno ime, celo podvučeno ime se prikazuje u odeljku **Unesite ime objekta za izbor**.



6. Kliknite na **U redu**.
7. Na ekranu Dozvole izaberite korisničko ime koje je uneto u odeljku **Imena grupa ili korisnička imena**, izaberite dozvolu pristupa pod **Promeni**, a zatim kliknite na **U redu**.



8. Kliknite na **U redu** ili **Zatvori** da biste zatvorili ekran.
 Proverite da li se u datoteku može upisivati ili čitati u deljenoj fascikli sa računara korisnika ili grupa sa dozvoljenim pristupom.

Dostupnost kontakata

Registrowanje odredišta na listu kontakata skenera omogućava vam da lako uđete u odredište prilikom skeniranja.

Na listu kontakata možete da registrujete sledeće tipove odredišta. Možete da registrujete najviše 300 unosa.

Napomena:

Takođe možete da koristite LDAP server (LDAP pretraga) za ulazak u odredište.

E-pošta	Odredište za e-poštu. Morate prethodno da konfigurirate postavke servera e-pošte.
Mrežna fascikla	Odredište za skenirane podatke. Treba prethodno da podesite mrežnu fasciklu.

Povezane informacije

➔ [“Saradnja između LDAP servera i korisnika” na strani 68](#)

Poređenje konfiguracija kontakata

Postoje tri alatke kojima možete da konfigurirate kontakte u skeneru: Web Config, Epson Device Admin i kontrolna tabla skenera. Razlika između tri pomenute alatke je navedena u tabeli koja se nalazi u nastavku.

Funkcije	Web Config*	Epson Device Admin	Kontrolna tabla skenera
Registrovanje odredišta	✓	✓	✓
Izmena odredišta	✓	✓	✓
Dodavanje grupe	✓	✓	✓
Izmena grupe	✓	✓	✓
Brisanje odredišta ili grupa	✓	✓	✓
Brisanje svih odredišta	✓	✓	–
Uvoz datoteke	✓	✓	–
Izvoz u obliku datoteke	✓	✓	–

* Prijavite se kao administrator da biste izvršili podešavanja.

Registrovanje odredišta u kontaktima pomoću Web Config

Napomena:

Takođe možete registrovati podešavanja kontakata na kontrolnoj tabli skenera.

1. Pristupite Web Config i izaberite karticu **Scan > Contacts**.
2. Izaberite broj koji želite da registrujete, a zatim kliknite na **Edit**.
3. Unesite **Name** i **Index Word**.
4. Izaberite tip odredišta kao opciju **Type**.

Napomena:

*Ne možete izmeniti opciju **Type** nakon završene registracije. Ako želite da izmenite tip, izbrišite odredište i zatim ga ponovo registrujte.*

5. Unesite vrednost za svaku stavku, a zatim kliknite na **Apply**.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Stavke za podešavanje odredišta

Stavke	Podešavanja i objašnjenje
Opšta podešavanja	
Name	Unesite ime prikazano u kontaktima u dužini od najviše 30 znakova u Unicode formatu (UTF-8). Ako to ne odredite, ostavite prazno.
Index Word	Unesite ime koristeći 30 znakova ili manje u Unicode formatu (UTF-8) da biste pretražili kontakte na kontrolnoj tabli skenera. Ako to ne odredite, ostavite prazno.
Type	Izaberite tip adrese koji želite da registrujete.
Assign to Frequent Use	Izaberite da biste podesili registrovanu adresu kao često korišćenu adresu. Kada podešavate često korišćenu adresu, ona se prikazuje na vrhu ekrana za skeniranje, tako da možete da izaberete odredište bez prikazivanja kontakata.
Email	
Email Address	Unesite između 1 i 255 znakova koristeći znakove A–Z, a–z, 0–9, ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Network Folder (SMB)	
Save to	\\„Putanja do fascikle“ Unesite mesto na kom je željena fascikla smeštena od 1 do 253 znaka u Unicode formatu (UTF-8), bez „\“. Unesite mrežnu putanju prikazanu na ekranu sa svojstvima fascikle. Pogledajte sledeće podatke o podešavanjima mrežne putanje. “Primer konfiguracije za lični računar” na strani 52
User Name	Unesite korisničko ime za pristup mrežnoj fascikli u dužini od najviše 30 znakova u Unicode formatu (UTF-8). Međutim, izbegavajte korišćenje kontrolnih znakova (od 0x00 do 0x1F, 0x7F).
Password	Unesite lozinku za pristup mrežnoj fascikli u dužini od najviše 20 znakova u Unicode formatu (UTF-8). Međutim, izbegavajte korišćenje kontrolnih znakova (od 0x00 do 0x1F, 0x7F).
FTP	
Secure Connection	Izaberite FTP ili FTPS prema protokolu za prenos podataka koji podržava FTP server. Izaberite FTPS da biste dozvolili skeneru da komunicira sa bezbednosnim merama.
Save to	Unesite naziv servera od 1 do 253 znaka u ASCII formatu (0x20–0x7E), bez „ftp://“ ili „ftps://“.
User Name	Unesite korisničko ime za pristup FTP serveru u dužini od najviše 30 znakova u Unicode formatu (UTF-8). Međutim, izbegavajte korišćenje kontrolnih znakova (od 0x00 do 0x1F, 0x7F). Ako server dozvoljava anonimne veze, unesite korisničko ime kao što je Anonymous i FTP. Ako to ne odredite, ostavite prazno.
Password	Unesite lozinku za pristup FTP serveru dužine od najviše 20 znakova u Unicode formatu (UTF-8). Međutim, izbegavajte korišćenje kontrolnih znakova (od 0x00 do 0x1F, 0x7F). Ako to ne odredite, ostavite prazno.
Connection Mode	Izaberite način povezivanja iz menija. Ako između skenera i FTP servera postoji zaštitni zid, izaberite Passive Mode .

Stavke	Podešavanja i objašnjenje
Port Number	Unesite broj porta na FTP serveru između 1 i 65535.
Certificate Validation	Sertifikat FTP servera se potvrđuje kada se ovo omogući. Ova funkcija je dostupna kada je FTPS podešen na Secure Connection . Da biste podesili morate da uvezete CA Certificate na skener.
SharePoint(WebDAV)	
Secure Connection	Izaberite HTTP ili HTTPS prema protokolu za prenos podataka koji podržava server. Izaberite HTTPS da biste dozvolili skeneru da komunicira sa bezbednosnim merama.
Save to	Unesite naziv servera od 1 do 253 znaka u ASCII formatu (0x20–0x7E), bez „http://“ ili „https://“.
User Name	Unesite korisničko ime za pristup serveru u dužini od najviše 30 znakova u Unicode formatu (UTF-8). Međutim, izbegavajte korišćenje kontrolnih znakova (od 0x00 do 0x1F, 0x7F). Ako to ne odredite, ostavite prazno.
Password	Unesite lozinku za pristup serveru dužine od najviše 20 znakova u Unicode formatu (UTF-8). Međutim, izbegavajte korišćenje kontrolnih znakova (od 0x00 do 0x1F, 0x7F). Ako to ne odredite, ostavite prazno.
Certificate Validation	Sertifikat servera se potvrđuje kada se ovo omogući. Ova funkcija je dostupna kada je HTTPS podešen na Secure Connection . Da biste podesili morate da uvezete CA Certificate na skener.
Proxy Server	Izaberite da li želite da koristite ovlašćeni server ili ne.

Registrovanje odredišta kao grupe pomoću Web Config

Ako je tip odredišta podešen na **Email**, možete registrovati odredišta kao grupu.

1. Pristupite Web Config i izaberite karticu **Scan > Contacts**.
2. Izaberite broj koji želite da registrujete, a zatim kliknite na **Edit**.
3. Izaberite grupu iz **Type**.
4. Kliknite na **Select** za **Contact(s) for Group**.
Prikazuju se dostupna odredišta.
5. Izaberite odredište koje želite da registrujete u grupi, a zatim kliknite na **Select**.
6. Unesite **Name** i **Index Word**.
7. Izaberite da li želite da dodelite registrovanu grupu često korišćenoj grup ili ne.

Napomena:

Odredišta se mogu registrovati u više grupa.

8. Kliknite na **Apply**.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Izrada rezervne kopije i uvoz kontakata

Korišćenjem Web Config ili drugih alatki, možete da napravite rezervnu kopiju i uvezete kontakte.

Za Web Config, možete da napravite rezervnu kopiju kontakata pomoću izvoza podešavanja skenera koja obuhvataju kontakte. Izvezena datoteka ne može se uređivati zato što je izvezena kao binarna datoteka.

Kada uvezete podešavanja skenera na skener, kontakti bivaju zamenjeni.

Za Epson Device Admin, samo kontakti se mogu izvoziti sa ekrana sa svojstvima uređaja. Takođe, ako ne izvozite stavke povezane sa bezbednošću, možete da uređujete izvezeno kontakte i da ih uvezete zato što se mogu sačuvati kao SYLK datoteka ili CSV datoteka.

Uvoz kontakata pomoću Web Config

Ako imate skener koji omogućava pravljenje rezervnih kopija kontakata i kompatibilan je sa ovim skenerom, možete jednostavno registrovati kontakte tako što ćete uvesti datoteku rezervne kopije.

Napomena:

Radi uputstava o tome kako da napravite rezervnu kopiju kontakata skenera pogledajte priručnik isporučen uz skener.

Pratite sledeće korake za uvoz kontakata na ovaj skener.

1. Prispupite Web Config, izaberite karticu **Device Management > Export and Import Setting Value > Import**.
2. Izaberite datoteku rezervne kopije koju ste napravili u **File**, unesite lozinku i zatim kliknite na **Next**.
3. Izaberite polje **Contacts** a zatim kliknite na **Next**.

Pravljenje rezervne kopije kontakata pomoću Web Config

Podaci o kontaktima mogu biti izgubljeni usled neispravnog funkcionisanja skenera. Preporučujemo da napravite rezervnu kopiju podataka svaki put kada ih ažurirate. Epson neće biti odgovoran ni za kakav gubitak podataka niti za pravljenje rezervnih kopija ili vraćanje podataka i/ili podešavanja, čak ni tokom garantnog roka.

Koristeći Web Config možete da napravite rezervnu kopiju podataka o kontaktima uskladištenim u skeneru i sačuvate je na računaru.

1. Pristupite Web Config i zatim izaberite karticu **Device Management > Export and Import Setting Value > Export**.
2. Izaberite polje za potvrdu **Contacts** pod kategorijom **Scan**.
3. Unesite lozinku da biste šifrovali izvezenu datoteku.
Potrebna vam je lozinka da biste uvezli datoteku. Ostavite ovu opciju praznu ako ne želite da šifrujete datoteku.
4. Kliknite na **Export**.

Izvoz i masovna registracija kontakata pomoću alata

Ako koristite Epson Device Admin, možete da napravite rezervnu kopiju samo kontakata i uređujete izvezene datoteke, zatim da ih registrujete sve odjednom.

Korisno je ako želite da napravite rezervnu kopiju samo kontakata ili kada zamenite skener i želite da prenesete kontakte sa starog na novi.

Izvoz kontakata

Sačuvajte informacije o kontaktima u datoteku.

Možete da uređujete datoteke sačuvane u SYLK formatu ili csv formatu uz pomoć aplikacije za rad s tabelama ili uređivača teksta. Možete da registrujete sve odjednom nakon brisanja ili dodavanja informacija.

Informacije koje obuhvataju bezbednosne stavke kao što je lozinka i lične informacije mogu se sačuvati u binarnom formatu pomoću lozinke. Ne možete uređivati datoteku. Može se koristiti kao rezervna datoteka informacija koje obuhvataju bezbednosne stavke.

1. Pokrenite Epson Device Admin.
2. Izaberite **Devices** u meniju zadataka na bočnoj traci.
3. Izaberite uređaj koji želite da konfigurirate sa liste uređaja.
4. Kliknite na **Device Configuration** na kartici **Home** na trakastom meniju.
Kada je podešena administratorska lozinka, unesite lozinku i kliknite na **OK**.
5. Kliknite na **Common > Contacts**.
6. Izaberite format izvoza u **Export > Export items**.
 - All Items
Izvezite šifrovanu binarnu datoteku. Izaberite kada želite da obuhvatite bezbednosne stavke kao što su lozinka i lične informacije. Ne možete uređivati datoteku. Ako je izaberete, morate odrediti lozinku. Kliknite na **Configuration** i podesite lozinku dužine od 8 do 63 znaka u formatu ASCII. Ova lozinka je potrebna kada se uvozi binarna datoteka.
 - Items except Security Information
Izvezite datoteke u SYLK formatu ili csv formatu. Izaberite kada želite da uređujete informacije u izvezenoj datoteci.
7. Kliknite na **Export**.
8. Odredite mesto za čuvanje datoteke, izaberite vrstu datoteke i zatim kliknite na **Save**.
Prikažeće se poruka sa obaveštenjem o završetku.
9. Kliknite na **OK**.
Proverite da li je datoteka sačuvana na određenom mestu.

Uvoz kontakata

Uvezite informacije o kontaktima iz datoteke.

Možete da uvezete datoteke sačuvane u SYLK formatu ili csv formatu ili kopiranu binarnu datoteku koja obuhvata bezbednosne stavke.

1. Pokrenite Epson Device Admin.
2. Izaberite **Devices** u meniju zadataka na bočnoj traci.
3. Izaberite uređaj koji želite da konfigurirate sa liste uređaja.
4. Kliknite na **Device Configuration** na kartici **Home** na trakastom meniju.
Kada je podešena administratorska lozinka, unesite lozinku i kliknite na **OK**.
5. Kliknite na **Common > Contacts**.
6. Kliknite na **Browse** na **Import**.
7. Izaberite datoteku koju želite da uvezete, a zatim kliknite na **Open**.
Kada izaberete binarnu datoteku, u **Password** unesite lozinku koju ste podesili prilikom izvoza datoteke.
8. Kliknite na **Import**.
Prikazaće se ekran za potvrdu.
9. Kliknite na **OK**.
Prikazaće se rezultat provere važnosti.
 - Edit the information read
Kliknite kada pojedinačno želite da uredite informacije.
 - Read more file
Kliknite kada želite da uvezete više datoteka.
10. Kliknite na **Import**, a zatim kliknite na **OK** na ekranu za završetak uvoza.
Vratite se na ekran sa svojstvima uređaja.
11. Kliknite na **Transmit**.
12. Kliknite na **OK** na poruci za potvrdu.
Podešavanja se šalju skeneru.
13. Kliknite na **OK** na ekranu za završetak slanja.
Informacije o skeneru će biti ažurirane.
Otvorite kontakte iz Web Config ili sa kontrolne table skenera, a zatim proverite da li je kontakt ažuriran.

Saradnja između LDAP servera i korisnika

Kada saradujete s LDAP serverom, možete da koristite informacije o adresi registrovanoj na LDAP serveru kao odredište e-pošte.

Konfigurisanje LDAP servera

Da biste koristili informacije LDAP servera, registrujte ga na skeneru.

1. Pristupite Web Config i izaberite karticu **Network > LDAP Server > Basic**.
2. Unesite vrednost za svaku stavku.
3. Izaberite **OK**.
Podešavanja koja ste izabrali su prikazana.

Stavke za podešavanje LDAP servera

Stavke	Podešavanja i objašnjenje
Use LDAP Server	Izaberite Use ili Do Not Use .
LDAP Server Address	Unesite adresu LDAP servera. Unesite između 1 i 255 znakova u formatu IPv4, IPv6 ili FQDN. U slučaju formata FQDN, možete da koristite alfanumeričke znakove u formatu ASCII (0x20–0x7E) i „-“, osim na početnoj i krajnjoj poziciji adrese.
LDAP server Port Number	Unesite broj priključka LDAP servera od 1 do 65535.
Secure Connection	Navedite metod provere identiteta kada skener pristupa LDAP serveru.
Certificate Validation	Kada je omogućen, potvrđuje se sertifikat LDAP servera. Preporučujemo da podesite na Enable . Da biste podesili, CA Certificate treba da se uveze na skener.
Search Timeout (sec)	Podesite vreme trajanja pre nego što dođe do prekida u toku pretrage od 5 do 300.
Authentication Method	Izaberite jednu od metoda. Ako izaberete Kerberos Authentication , izaberite Kerberos Settings da biste izvršili podešavanja za Kerberos. Da biste izvršili Kerberos Authentication, potrebno je sledeće okruženje. <input type="checkbox"/> Skener i DNS server mogu da komuniciraju. <input type="checkbox"/> Sinhronizuje se vreme skenera, KDC servera i servera koji je potreban za proveru identiteta (LDAP server, SMTP server, server za datoteku). <input type="checkbox"/> Kada se radni server dodeli kao IP adresa, FQDN radnog servera se registruje na zonu povratnog pretraživanja DNS servera.
Kerberos Realm to be Used	Ako izaberete Kerberos Authentication za Authentication Method , unesite Kerberos domen koji želite da koristite.

Stavke	Podešavanja i objašnjenje
Administrator DN / User Name	Unesite korisničko ime za LDAP server u dužini od najviše 128 znakova u Unicode formatu (UTF-8). Nije moguće uneti kontrolne znakove, npr. 0x00–0x1F i 0X7F. Ova podešavanja se ne koriste kada je Anonymous Authentication izabrano kao Authentication Method . Ako to ne odredite, ostavite prazno.
Password	Unesite korisničko ime za proveru identiteta LDAP servera u dužini od najviše 128 znakova u Unicode formatu (UTF-8). Nije moguće uneti kontrolne znakove, npr. 0x00–0x1F i 0X7F. Ova podešavanja se ne koriste kada je Anonymous Authentication izabrano kao Authentication Method . Ako to ne odredite, ostavite prazno.

Podešavanja Kerberos protokola

Ako odaberete **Kerberos Authentication** kao **Authentication Method** za **LDAP Server > Basic**, izvršite sledeća podešavanja za Kerberos sa kartice **Network > Kerberos Settings**. Možete registrovati do 10 podešavanja za Kerberos.

Stavke	Podešavanja i objašnjenje
Realm (Domain)	Unesite područje Kerberos provere identiteta u dužini do 255 znakova u formatu ASCII (0x20–0x7E). Ako je ne registrujete, ostavite prazno.
KDC Address	Unesite adresu Kerberos servera za proveru identiteta. Unesite do 255 znakova u formatu IPv4, IPv6 ili FQDN. Ako je ne registrujete, ostavite prazno.
Port Number (Kerberos)	Unesite broj priključka Kerberos servera između 1 i 65535.

Konfiguracija podešavanja pretraživanja preko LDAP servera

Kada postavite podešavanja pretraživanja, možete da koristite adresu e-pošte registrovanu na LDAP serveru.

1. Pristupite Web Config i izaberite karticu **Network > LDAP Server > Search Settings**.
2. Unesite vrednost za svaku stavku.
3. Kliknite na **OK** da biste prikazali rezultat podešavanja.
Podešavanja koja ste izabrali su prikazana.

Pretraga preko LDAP servera — stavke podešavanja

Stavke	Podešavanja i objašnjenje
Search Base (Distinguished Name)	Ako želite da potražite proizvoljni domen, navedite naziv domena na LDAP serveru. Unesite između 0 i 128 znakova u formatu Unicode (UTF-8). Ako ne tražite proizvoljno svojstvo, ostavite ovo prazno. Primeri direktorijuma lokalnog servera: dc=server,dc=local
Number of search entries	Odredite broj unosa za pretraživanje od 5 do 500. Određeni broj unosa za pretraživanje se privremeno čuva i prikazuje. Čak i ako je broj unosa za pretraživanje veći od određenog broja i prikaže se poruka o grešci, pretraga se može dovršiti.

Stavke	Podešavanja i objašnjenje
User name Attribute	Odredite naziv svojstva koje ćete prikazati kada se traže korisnička imena. Unesite između 1 i 255 znakova u formatu Unicode (UTF-8). Prvi znak mora da bude a–z ili A–Z. Primer: cn, uid
User name Display Attribute	Odredite naziv svojstva koje ćete prikazati kao korisničko ime. Unesite između 0 i 255 znakova u formatu Unicode (UTF-8). Prvi znak mora da bude a–z ili A–Z. Primer: cn, sn
Email Address Attribute	Odredite naziv svojstva koje ćete prikazati kada se traže e-adrese. Unesite kombinaciju znakova u dužini od 1 do 255 znakova, koristeći znakove A–Z, a–z, 0–9 i -. Prvi znak mora da bude a–z ili A–Z. Primer: pošta
Arbitrary Attribute 1 - Arbitrary Attribute 4	Možete odrediti ostala proizvoljna svojstva za pretragu. Unesite između 0 i 255 znakova u formatu Unicode (UTF-8). Prvi znak mora da bude a–z ili A–Z. Ako ne želite da pretražujete proizvoljne atribute, nemojte popunjavati ovo polje. Primer: o, ou

Provera veze sa LDAP serverom

Vrši proveru veze sa LDAP serverom uz pomoć parametra podešenog na **LDAP Server > Search Settings**.

1. Pristupite Web Config i izaberite karticu **Network > LDAP Server > Connection Test**.
2. Izaberite **Start**.

Test veze se pokreće. Nakon testa, prikazuje se izveštaj o proveri.

Reference testiranja veze sa LDAP serverom

Poruke	Objašnjenje
Connection test was successful.	Ova poruka se prikazuje kada je veza sa serverom uspešna.
Connection test failed. Check the settings.	Ova poruka se prikazuje iz sledećih razloga: <input type="checkbox"/> Adresa LDAP servera ili broj porta nije tačan. <input type="checkbox"/> Došlo je do prekida. <input type="checkbox"/> Do Not Use je izabrano kao Use LDAP Server . <input type="checkbox"/> Ako je Kerberos Authentication izabrano kao Authentication Method , podešavanja kao Realm (Domain) , KDC Address i Port Number (Kerberos) su neispravna.
Connection test failed. Check the date and time on your product or server.	Ova poruka se pojavljuje kada se veza ne ostvari jer nije podešeno isto vreme za skener i za LDAP server.

Poruke	Objašnjenje
Authentication failed. Check the settings.	Ova poruka se prikazuje iz sledećih razloga: <input type="checkbox"/> User Name i/ili Password su neispravni. <input type="checkbox"/> Ako je izabrano Kerberos Authentication kao Authentication Method , vreme/datum se možda neće konfigurisati.
Cannot access the product until processing is complete.	Ova poruka se prikazuje kada je skener zauzet.

Korišćenje funkcije Document Capture Pro Server

Pomoću aplikacije Document Capture Pro Server, možete da upravljate načinom razvrstavanja, formatom u kom se čuvaju, kao i odredištem za prosleđivanje dokumenata skeniranih s kontrolne table skenera. Možete s kontrolne table skenera pozvati i izvršiti zadatak koji je prethodno registrovan na serveru.

Instalirajte je na serverski računar.

Radi detaljnijih informacija o Document Capture Pro Server obratite se svom lokalnom predstavništvu kompanije Epson.

Podešavanje režima servera

Da biste koristili Document Capture Pro Server, izvršite sledeća podešavanja.

1. Pristupite Web Config i izaberite karticu **Scan > Document Capture Pro**.
2. Izaberite **Server Mode** za **Mode**.
3. Unesite adresu servera Document Capture Pro Server instaliranog na njemu u stavku **Server Address**.
Unesite između 2 i 255 znakova u formatu IPv4, IPv6 ili FQDN ili naziv hosta. U slučaju formata FQDN, možete da koristite alfanumeričke znakove u formatu ASCII (0x20–0x7E) i „-“, osim na početnoj i krajnjoj poziciji adrese.
4. Kliknite na **OK**.
Mreža se ponovo povezuje i podešavanja su nakon toga omogućena.

Podešavanje funkcije AirPrint

Pristupite Web Config, izaberite karticu **Network**, a zatim izaberite **AirPrint Setup**.

Stavke	Objašnjenje
Bonjour Service Name	Unesite naziv usluge Bonjour, koristeći ASCII format (0x20–0x7E) i najviše 41 znak.
Bonjour Location	Unesite opis lokacije skenera pomoću Unicode (UTF-8) formata i najviše 127 bajtova.

Stavke	Objašnjenje
Wide-Area Bonjour	Podesite da li će širokopojasni Bonjour biti korišćen ili ne. Ako ga koristite, skener mora biti registrovan na DNS serveru da bi se pretraživao skener preko segmenta.
Enable AirPrint	Bonjour i AirPrint (usluga skeniranja) su omogućeni.

Problemi prilikom pripreme skeniranja preko mreže

Napomene za rešavanje problema

Proveravanje poruke o grešci

Kada se pojavi problem, prvo proverite ima li poruka na kontrolnoj tabli skenera ili upravljačkom ekranu. Ako ste podesili obaveštenja putem e-pošte u slučaju odigravanja događaja, možete brzo saznati status.

Provera statusa komunikacije

Proverite status komunikacije serverskog računara ili klijentskog računara pomoću komande kao što je ping i ipconfig.

Provera veze

Da biste proverili vezu između skenera i servera za poštu, izvršite proveru veze sa skenera. Takođe proverite vezu od klijentskog računara do servera kako biste proverili status komunikacije.

Započinjanje mrežnih podešavanja

Ako se ne prikaže problem u vezi sa podešavanjima i statusom komunikacije, problemi se mogu rešiti onemogućavanjem ili započinjanjem mrežnih podešavanja skenera, a zatim ponovnim postavljanjem.

Pristup programu Web Config nije moguć

Skeneru nije dodeljena IP adresa.

Rešenja

Moguće je da važeća IP adresa nije pravilno dodeljena skeneru. Konfigurirajte IP adresu pomoću kontrolne table skenera. Informacije o trenutnom podešavanju možete da potvrdite preko kontrolne table skenera.

Veb pregledač ne podržava jačinu šifrovanja za SSL/TLS.

Rešenja

SSL/TLS ima Encryption Strength. Možete otvoriti Web Config uz pomoć veb pregledača koji podržava grupna šifrovanja kao što je ispod navedeno. Proverite da li koristite podržani pregledač.

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

CA-signed Certificate je istekao.

Rešenja

Ako postoji problem sa isteklim sertifikatom, prikazuje se poruka „Sertifikat je istekao” prilikom povezivanja na Web Config preko protokola SSL/TLS (https). Ako se poruka pojavi pre datuma isteka sertifikata, proverite da li je na skeneru podešen tačan datum.

Opšti naziv sertifikata i skenera se ne podudaraju.

Rešenja

Ako se opšti naziv sertifikata i skenera ne podudaraju, prikazuje se poruka „Naziv bezbednosnog sertifikata se ne podudara...” prilikom pokretanja Web Config preko SSL/TLS protokola (https). Ovo se dešava zato što se sledeće IP adrese ne podudaraju.

- IP adresa skenera se unosi u opšti naziv za kreiranje Self-signed Certificate ili CSR
- IP adresa se unosi u pregledač kada pokrećete Web Config

Za Self-signed Certificate, ažurirajte sertifikat.

Za CA-signed Certificate ponovo uzmite sertifikat za skener.

Podešavanje ovlašćenog servera za lokalnu adresu nije podešeno na veb pregledaču.

Rešenja

Kada je skener podešen da koristi ovlašćeni server, konfigurirate veb pregledač tako da se ne povezuje na lokalnu adresu preko ovlašćenog servera.

- Windows:

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

- Mac OS:

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

Primer:

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

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

DHCP server je onemogućen u podešavanjima računara.

Rešenja

Ako je DHCP server za automatsko pribavljanje IP adrese onemogućen na računaru, ne možete pristupiti Web Config. Omogućite DHCP.

Primer za operativni sistem Windows 10:

Otvorite kontrolnu tablu i kliknite na **Mreža i internet > Centar za mrežu i deljenje > Promeni podešavanja adaptera**. Otvorite ekran sa svojstvima povezivanja koje koristite, a zatim otvorite ekran sa svojstvima za **Internet protokol verzija 4 (TCP/IPv4)** ili **Internet protokol verzija 6 (TCP/IPv6)**.

Proverite da je izabrano **Automatsko pribavljanje IP adrese** na prikazanom ekranu.


Prilagođeno podešavanje prikaza kontrolne table

Registrovanje Un. pod. vr.	75
Uređivanje početnog ekrana na kontrolnoj tabli.	77

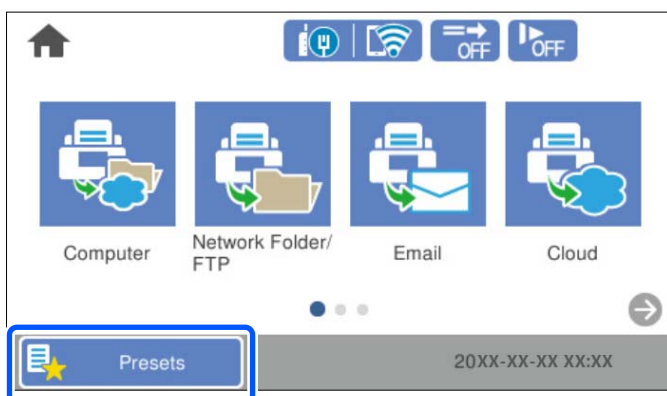
Registrovanje Un. pod. vr.


Možete registrovati često korišćeno podešavanje skeniranja kao **Un. pod. vr.**. Možete registrovati najviše 48 unapred određenih podešavanja.

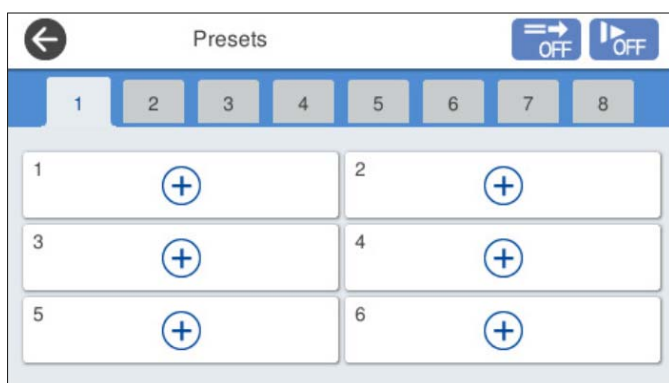
Napomena:

- Možete registrovati aktuelna podešavanja tako što ćete izabrati  na ekranu za započinjanje skeniranja.
- Takođe možete registrovati **Presets** u *Web Config*.
Izaberite karticu **Scan** > **Presets**.
- Ako prilikom registracije izaberete **Skeniraj na računar**, možete da registrujete zadatak kreiran u *Document Capture Pro* kao **Presets**. Ovo je dostupno samo za računare koji su povezani preko mreže. Unapred registrujte zadatak u *Document Capture Pro*.
- Ako je omogućeno podešavanje provere identiteta, samo administrator može da registruje **Presets**.

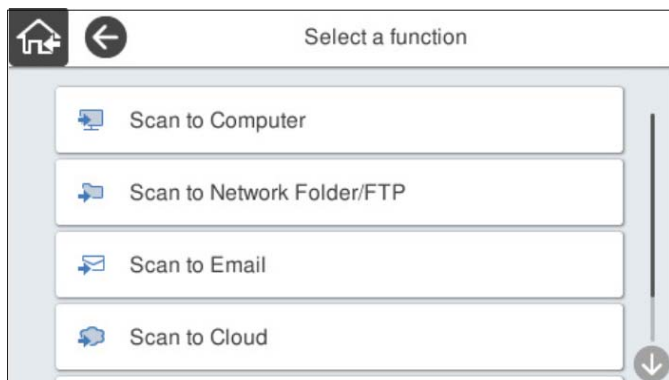
1. Izaberite **Un. pod. vr.** na početnom ekranu na kontrolnoj tabli skenera.



2. Izaberite .



3. Izaberite meni koji želite da koristite da registrujete unapred određenih podešavanja.



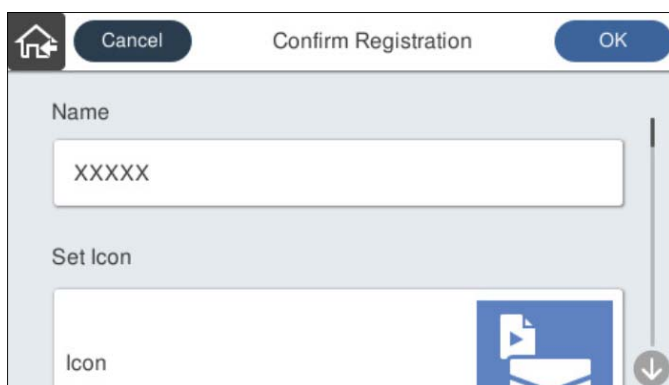
4. Podesite svaku stavku, a zatim izaberite .

Napomena:

Kada izaberete **Skeniraj na računar**, izaberite računar na kom je instaliran Document Capture Pro, a zatim izaberite registrovani zadatak. Ovo je dostupno samo za računare koji su povezani preko mreže.


5. Izvršite unapred određena podešavanja.

- Ime:** Podesite naziv.
- Podesi ikonu:** Podesite sliku i boju ikone koju želite da prikažete.
- Postavke brzog slanja:** Odmah započinje skeniranje bez potvrde kada je izabrana zadata postavka.
Kada koristite Document Capture Pro Server, čak i ako podesite softver da potvrdi sadržaj zadatka pre skeniranja, **Postavke brzog slanja** na unapred određenim podešavanjima skenera ima prednost nad softverom.
- Sadržaj:** Proverite podešavanja skeniranja.



6. Izaberite **OK**.

Opcije menija za Un. pod. vr.

Možete da promene podešavanja zadate postavke ako izaberete  u svakoj zadatoj postavci.

Promeni ime:

Menja naziv zadate postavke.

Promeni ikonu:

Menja sliku ikone i boju zadate postavke.

Postavke brzog slanja:

Odmah započinje skeniranje bez potvrde kada je izabrana zadata postavka.

Promeni položaj:

Menja redosled prikaza zadatih postavki.

Izbriši:

Briše zadate postavke.

Dodaj ili ukloni ikonu na početnom ekranu:

Dodaje ili briše ikonu zadate postavke sa početnog ekrana.

Potvrdi detalje:

Prikazuje podešavanja zadate postavke. Možete da učitate zadate postavke tako što ćete izabrati **Koristi ovu postavku**.

Uređivanje početnog ekrana na kontrolnoj tabli

Možete da prilagodite početni ekran tako što ćete izabrati **Podešavanja > Izmena početnog ekrana** na kontrolnoj tabli skenera.

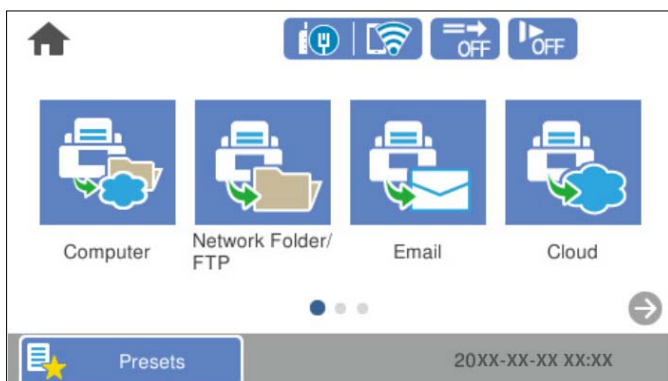
- Raspored: Menja način prikaza ikona menija.
[“Menjanje Raspored početnog ekrana” na strani 77](#)
- Dodaj ikonu: Dodaje ikone u **Un. pod. vr.** podešavanje koje ste izvršili ili vraća ikone koje ste sklonili sa ekrana.
[“Dodaj ikonu” na strani 78](#)
- Ukloni ikonu: Uklanja ikone sa početnog ekrana.
[“Ukloni ikonu” na strani 79](#)
- Pomeri ikonu: Menja redosled prikaza datoteka.
[“Pomeri ikonu” na strani 80](#)
- Vraćanje podrazumevanog prikaza ikona: Vraća standardna podešavanja prikaza za početni ekran.
- Pozadina: promenite boju pozadine početnog ekrana.

Menjanje Raspored početnog ekrana

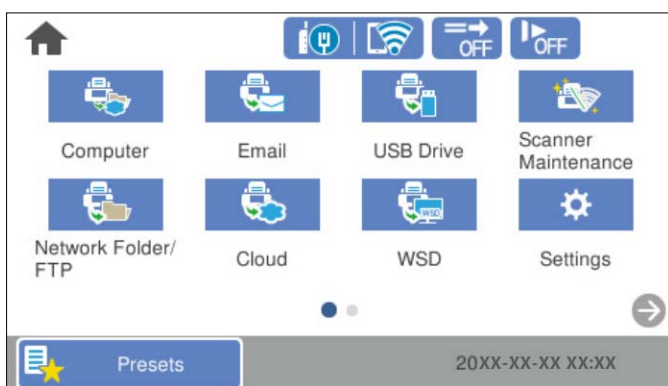
1. Izaberite **Podešavanja > Izmena početnog ekrana > Raspored** na kontrolnoj tabli skenera.


- Izaberite **Linija** ili **Matrica**.

Linija:



Matrica:

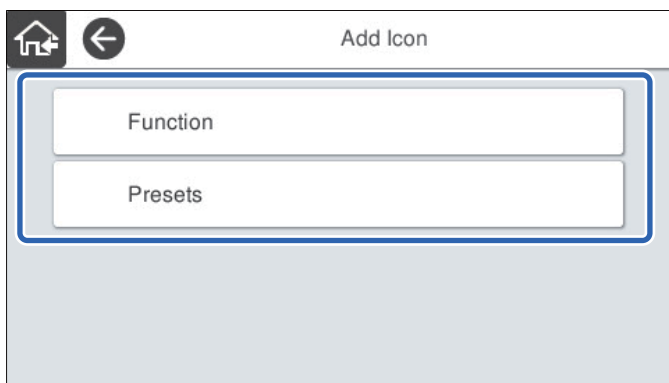


- Izaberite  da biste se vratili i proverili početni ekran.

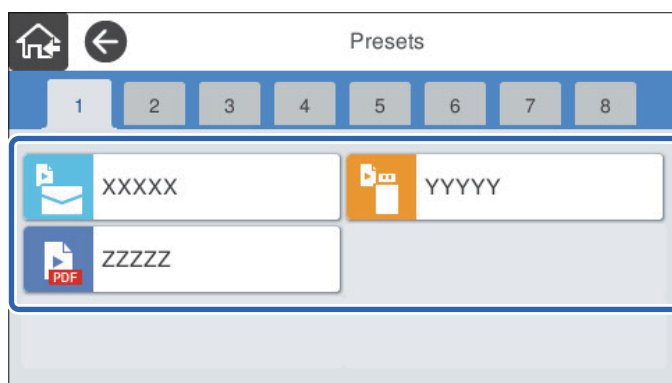
Dodaj ikonu

- Izaberite **Podešavanja** > **Izmena početnog ekrana** > **Dodaj ikonu** na kontrolnoj tabli skenera.
- Izaberite **Funkcija** ili **Un. pod. vr.**
 - Funkcija: Prikazuje standardne funkcije prikazane na početnom ekranu.

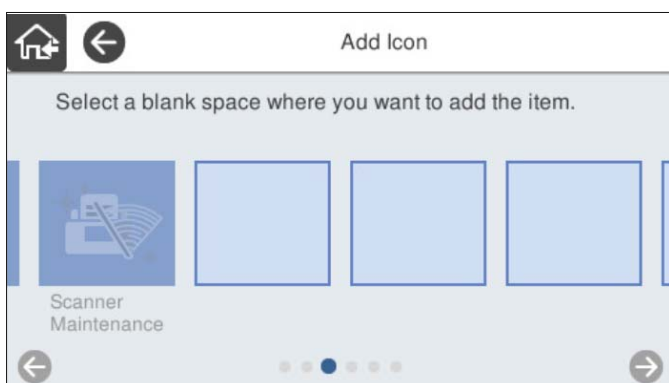
- Un. pod. vr.: Prikazuje registrovana unapred određena podešavanja.




3. Izaberite stavku koju želite da dodate početnom ekranu.



4. Izaberite prazan prostor gde želite da dodate stavku.
Ako želite da dodate više ikona, ponovite korake 3 do 4.

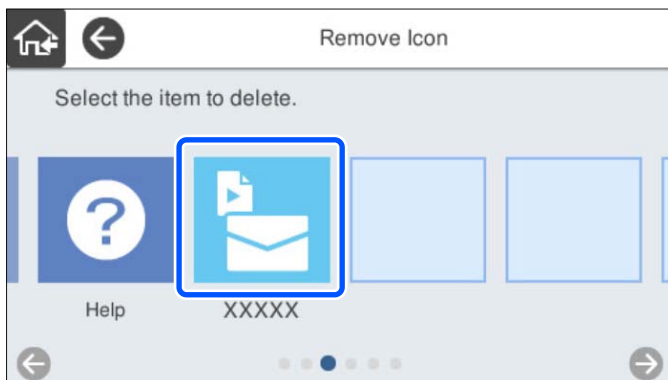


5. Izaberite  da biste se vratili i proverili početni ekran.


Ukloni ikonu

1. Izaberite **Podešavanja > Izmena početnog ekrana > Ukloni ikonu** na kontrolnoj tabli skenera.

2. Izaberite ikonu koju želite da uklonite.

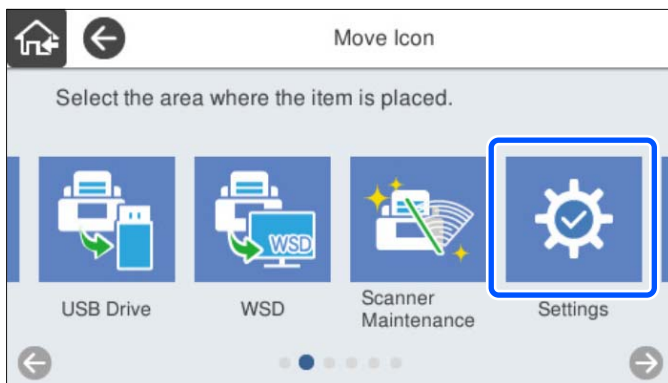


3. Da biste završili, izaberite **Da**.
Ako želite da uklonite više ikona, ponovite postupke 2 do 3.

4. Izaberite  da biste se vratili i proverili početni ekran.

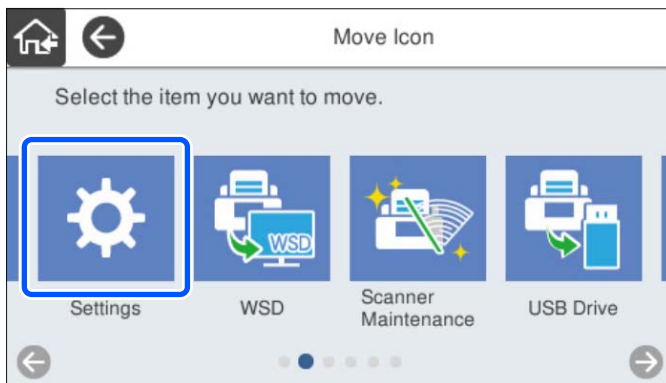
Pomeri ikonu


1. Izaberite **Podešavanja** > **Izmena početnog ekrana** > **Pomeri ikonu** na kontrolnoj tabli skenera.
2. Izaberite ikonu koju želite da pomerite.



3. Izaberite okvir odredišta.

Ako se u odredišnom okviru već nalazi druga ikona, ikone se zamenjuju.



4. Izaberite  da biste se vratili i proverili početni ekran.

Osnovne bezbednosne postavke

Uvođenje funkcija sigurnosti proizvoda.	83
Podešavanja za administratore.	83
Onemogućavanje spoljnog interfejsa.	89
Upravljanje udaljenim skenerom.	90
Rešavanje problema.	91

Uvođenje funkcija sigurnosti proizvoda

Ovaj odeljak uvodi sigurnosnu funkciju za Epson uređaje.

Naziv funkcije	Vrsta funkcije	Šta podesiti	Šta sprečiti
Podešavanje lozinke administratora	Zaključava postavke sistema, kao što su postavke za povezivanje za mrežu ili USB.	Administrator podešava lozinku na uređaj. Možete podesiti ili promeniti i iz Web Config i sa kontrolne table skenera.	Sprečava neovlašćeno očitavanje i menjanje informacija uskladištenih u uređaju, poput ID oznake, lozinke, mrežnih podešavanja itd. Takođe smanjite širok spektar bezbednosnih rizika kao što je curenje informacija za mrežno okruženje ili politiku bezbednosti.
Postavka za spoljni interfejs	Kontroliše interfejs koji se priključuje na uređaj.	Omogućite ili onemogućite USB povezivanje sa računarom.	USB veza računara: Sprečava neovlašćenu upotrebu uređaja zabranom skeniranja bez prolaska kroz mrežu.

Povezane informacije

- ➔ [“Konfigurisanje administratorske lozinke” na strani 83](#)
- ➔ [“Onemogućavanje spoljnog interfejsa” na strani 89](#)

Podešavanja za administratore

Konfigurisanje administratorske lozinke

Kada postavite administratorsku lozinku, možete sprečiti korisnike da menjaju podešavanja upravljanja sistemom. Podrazumevane vrednosti su podešene od vremena kupovine. Po potrebi ih promenite.

Napomena:

Sledeće stavke pružaju uvid u podrazumevane vrednosti za informacije o administratoru.

- Korisničko ime (koristi se samo za Web Config): ništa (prazno)*
- Lozinka: serijski broj skenera*

Da biste pronašli serijski broj, proverite nalepnicu na zadnjoj strani skenera.

Možete da promenite administratorsku lozinku ili pomoću Web Config, kontrolne table skenera ili Epson Device Admin. Kada koristite Epson Device Admin, pogledajte uputstvo za upotrebu ili pomoć za Epson Device Admin.

Promena administratorske lozinke pomoću Web Config

Promenite lozinku za administratora u Web Config.

1. Pristupite Web Config i izaberite karticu **Product Security > Change Administrator Password**.

2. Unesite neophodne informacije u **Current password**, **User Name**, **New Password** i **Confirm New Password**.
Unesite bar jedan znak za novu lozinku.

Napomena:

Sledeće stavke pružaju uvid u podrazumevane vrednosti za informacije o administratoru.

- Korisničko ime: ništa (prazno)
- Lozinka: serijski broj skenera

Da biste pronašli serijski broj, proverite nalepnicu na zadnjoj strani skenera.



Važno:

Vodite računa da zapamtite administratorsku lozinku koju ste podesili. Ako zaboravite svoju lozinku, nećete biti u mogućnosti da je ponovo postavite i moraćete da zatražite pomoć od tehničkog osoblja.

3. Izaberite **OK**.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Promena administratorske lozinke na kontrolnoj tabli

Možete da promenite administratorsku lozinku s kontrolne table skenera.

1. Izaberite **Podešavanja** na kontrolnoj tabli skenera.
2. Izaberite **Administracija sistema > Administratorska podešavanja**.
3. Izaberite **Lozinka administratora > Promeni**.
4. Unesite vašu trenutnu lozinku.

Napomena:

Podešavanje u vreme kupovine (podrazumevana vrednost) za administratorsku lozinku je serijski broj skenera.

Da biste pronašli serijski broj, proverite nalepnicu na zadnjoj strani skenera.

5. Unesite vašu novu lozinku.

Morate uneti bar jedan znak.



Važno:

Vodite računa da zapamtite administratorsku lozinku koju ste podesili. Ako zaboravite svoju lozinku, nećete biti u mogućnosti da je ponovo postavite i moraćete da zatražite pomoć od tehničkog osoblja.

6. Ponovo unesite novu lozinku za potvrdu.

Prikazaće se poruka sa obaveštenjem o završetku.

Upotreba Zaključavanje podešavanja sa kontrolne table štampača


Možete koristiti Zaključavanje podešavanja da zaključate kontrolnu tablu kako biste sprečili korisnike da menjaju stavke koje se odnose na podešavanja sistema.

Napomena:

Ako omogućite *Authentication Settings* na skeneru, *Zaključavanje podešavanja* je omogućen i za kontrolnu tablu. Kontrolna tabla se ne može otključati kada je omogućen *Authentication Settings*.

Čak i ako onemogućite *Authentication Settings*, opcija *Zaključavanje podešavanja* ostaje omogućena. Ako želite da je onemogućite, možete izvršiti podešavanja sa kontrolne table ili *Web Config*.

Podešavanje Zaključavanje podešavanja sa kontrolne table

1. Ako želite da otkazete **Zaključavanje podešavanja** nakon što ga omogućite, dodirnite  u gornjem desnom uglu na početnom ekranu da biste se prijavili kao administrator.

Opcija  nije prikazana kada je onemogućeno **Zaključavanje podešavanja**. Ukoliko želite omogućite ovo podešavanje, idite na sledeći korak.

2. Izaberite **Podešavanja**.
3. Izaberite **Administracija sistema > Administratorska podešavanja**.
4. Izaberite **Uklj. ili Isklj. za Zaključavanje podešavanja**.

Podešavanje Zaključavanje podešavanja iz Web Config

1. Izaberite karticu **Device Management > Control Panel**.
2. Izaberite **ON** ili **OFF** za **Panel Lock**.
3. Kliknite na **OK**.

Povezane informacije

➔ “Pokretanje *Web Config* u veb pregledaču” na strani 35

Stavke Zaključavanje podešavanja na meniju Podešavanja

Ovo je lista stavki koje su zaključane u meniju **Podešavanja** na kontrolnoj tabli pomoću *Zaključavanje podešavanja*.

✓: treba da se zaključa.

- : ne treba da se zaključa.

Meni Podešavanja	Zaključavanje podešavanja
Osn. podešavanja	-

Meni Podešavanja		Zaključavanje podešavanja
	Osvetljenost LCD-a	-
	Zvukovi	-
	Tajmer za spavanje	✓
	Merač vremena za isključivanje	✓
	Podešavanja za datum/vreme	✓
	Jezik/Language	✓/-*
	Tastatura (U zavisnosti od modela i regiona, ova funkcija možda neće biti dostupna.)	-
	Vreme za radnju je isteklo	✓
	Veza sa računarnom preko USB-a	✓
	Direktno napajanje uklj.	✓
Podešavanja skenera		-
	Sporo	-
	Vreme zaustavlj. dvostrukog uvlač.	✓
	DFDS funkcija	-
	Zaštita papira	✓
	Otkrivanje prljavštine na staklu	✓
	Ultrasonic otkrivanje duplog uvlačenja	✓
	Istek vremena za Režim automatskog uvlačenja	✓
	Potvrdi primaoca	✓
Izmena početnog ekrana		✓
	Raspored	✓
	Dodaj ikonu	✓
	Ukloni ikonu	✓
	Pomeri ikonu	✓
	Vraćanje podrazumevanog prikaza ikona	✓
	Pozadina	✓
Korisničke postavke		✓


Meni Podešavanja		Zaključavanje podešavanja
	Mrežni direktorijum/FTP	✓
	Imejl	✓
	Oblak	✓
	USB disk	✓
Mrežne postavke		✓
	Podešavanje Wi-Fi-a	✓
	Podešavanje ožičene lokalne mreže	✓
	Status mreže	✓
	Napredno	✓
Postavke veb usluge		✓
	Epson Connect usluge	✓
Document Capture Pro		-
	Promeni postavke	✓
Menadžer kontakata		-
	Registruj/izbriši	✓/-*
	Često	-
	Opcije prikaza	-
	Opcije pretrage	-
Administracija sistema		✓
	Menadžer kontakata	✓
	Administratorska podešavanja	✓
	Ograničenja	✓
	Šifrovanje lozinke	✓
	Istraživanje korisnika	✓
	Postavke WSD-a	✓
	Vrati podrazumevane postavke	✓
	Ažuriranje firmvera	✓
Informacije o uređaju		-

Meni Podešavanja		Zaključavanje podešavanja
	Serijski broj	-
	Trenutna verzija	-
	Ukupan broj skeniranja	-
	Broj 1-stranih skeniranja	-
	Broj 2-stranih skeniranja	-
	Broj skeniranja nosećeg lista	-
	Broj skeniranja nakon zamene valjka	-
	Broj skeniranja nakon redovnog čišćenja	-
	Resetuj broj skeniranja	✓
Održavanje skenera		-
	Čišćenje valjka	-
	Zamena valjka	-
	Resetuj broj skeniranja	✓
	Način zamene	-
	Redovno čišćenje	-
	Resetuj broj skeniranja	✓
	Uputstvo za čišćenje	-
	Čišćenje stakla	-
Podešavanje upozorenja za zamenu valjka		✓
	Podeš. broja upozorenja	✓
Podešavanja upozorenja za redovno čišćenje		✓
	Podešavanje upozorenja	✓
	Podeš. broja upozorenja	✓

* Možete da podesite da li želite da dozvolite promene u **Administracija sistema > Ograničenja**.

Prijavite se kao administrator sa kontrolne table štampača

Možete koristiti bilo koji od sledećih metoda da se prijavite kao administrator sa kontrolne table skenera.

1. Dodirnite  u gornjem desnom delu ekrana.
 - Kada su omogućene Authentication Settings, prikazuje se ikona na ekranu **Dobro došli** (ekran pripravnosti za autorizaciju).
 - Kada je omogućeno Authentication Settings, prikazuje se ikona na početnom ekranu.

2. Dodirnite **Da** kada se prikaže ekran za potvrdu.
3. Unesite lozinku za administratora.
Prikazuje se poruka o završetku prijave, a zatim se prikazuje početni ekran na kontrolnoj tabli.

Da biste se prijavili, dodirnite  u gornjem desnom delu ekrana.

Onemogućavanje spoljnog interfejsa

Možete onemogućiti interfejs koji se koristi za povezivanje uređaja sa skenerom. Podesite ograničenja da biste ograničili skeniranje samo na skeniranje putem mreže.

Napomena:

Takođe možete izvršiti podešavanja ograničenja na kontrolnoj tabli skenera.

*Veza sa računarom preko USB-a: **Podešavanja** > **Osn. podešavanja** > **Veza sa računarom preko USB-a***

1. Pristupite Web Config i izaberite karticu **Product Security** > **External Interface**.
2. Izaberite **Disable** za funkcije koje želite da podesite.
Izaberite **Enable** kada želite da poništite upravljanje.
Veza sa računarom preko USB-a
Možete ograničiti upotrebu USB veze sa računara. Ako želite da je ograničite, izaberite **Disable**.
3. Kliknite na **OK**.
4. Uverite se da se onemogućeni ulaz ne može koristiti.
Veza sa računarom preko USB-a
Ako je na računaru instaliran upravljački program
Povežite skener i računar pomoću USB kabla, a zatim se uverite da skener ne skenira.
Ako na računaru nije instaliran upravljački program
Operativni sistem Windows:
Otvorite menadžer uređaja i zadržite ga, povežite skener i računar pomoću USB kabla, a zatim se uverite da prikazani sadržaj menadžera uređaja ostaje nepromenjen.
Operativni sistem Mac OS:
Povežite skener i računar pomoću USB kabla, a zatim se uverite da ne možete dodati skenier iz **Štampači i skeneri**.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Upravljanje udaljenim skenerom

Provera informacija za udaljeni skener

U stavci **Status** pomoću Web Config možete proveriti sledeće informacije o određenom skeneru.

- Product Status
Proverite status, uslugu u računarskom oblaku, broj proizvoda, MAC adresu itd.
- Network Status
Proverite informacije o statusu veze s mrežom, IP adresu, DNS server itd.
- Usage Status
Proverite prvi dan skeniranja, broj skeniranih dokumenata itd.
- Hardware Status
Proverite status svake funkcije skenera.
- Panel Snapshot
Prikazuje sliku ekrana prikazanog na kontrolnoj tabli skenera.

Primanje obaveštenja o događajima e-poštom

O obaveštenjima putem e-pošte

Ovo je funkcija obaveštavanja koja, kada događaj kao što je prestanak skeniranja i pojava greške skenera, šalje e-poruku na navedenu adresu.

Možete registrovati najviše pet odredišta i postaviti podešavanja obaveštenja za svako odredište.

Da bi se ova funkcija mogla koristiti, treba da podesite server e-pošte pre podešavanja obaveštenja.

Povezane informacije

➔ [“Konfigurisanje servera za poštu” na strani 41](#)

Konfigurisanje obaveštenja putem e-pošte

Konfigurirate obaveštenja putem e-pošte pomoću Web Config.

1. Pristupite Web Config i izaberite karticu **Device Management > Email Notification**.
2. Podesite predmet obaveštenja putem e-pošte.
Izaberite sadržaj koji je prikazan o predmetu iz dva padajuća menija.
 - Izabrani sadržaji su prikazani odmah pored **Subject**.
 - Ne možete isti sadržaj postaviti i sa leve i sa desne strane.
 - Kada broj znakova u **Location** prelazi 32 bajta, znakovi koji prelaze 32 bajta se izostavljaju.

- Unesite adresu e-pošte za slanje obaveštenja putem e-pošte.
Koristite A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @, i unesite između 1 i 255 znakova.
- Izaberite jezik za obaveštenja putem e-pošte.
- Izaberite polje za potvrdu događaja za koji želite da primite obaveštenje.
Broj **Notification Settings** je povezan sa brojem odredišta **Email Address Settings**.
Primer:
Ako želite da se obaveštenje pošalje na adresu e-pošte podešenu za broj 1 u **Email Address Settings** kad se promeni lozinka administratora, izaberite polje za kolonu **1** u redu **Administrator password changed**.
- Kliknite na **OK**.
Potvrdite da će obaveštenje putem e-pošte biti poslato izazvanim događajem.
Na primer: Promenjena je administratorska lozinka.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Stavke za obaveštenje putem e-pošte

Stavke	Podešavanja i objašnjenje
Administrator password changed	Obratite pažnju kada je administratorska lozinka promenjena.
Scanner error	Obratite pažnju kada se pojavi greška skenera.
Greška Wi-Fi	Obaveštenje kada se pojavi greška bežičnog LAN interfejsa.

Rešavanje problema

Zaboravili ste administratorsku lozinku

Potrebna vam je pomoć tehničkog osoblja. Obratite se svom lokalnom prodavcu.

Napomena:

Sledeće stavke pružaju uvid u početne vrednosti za administratora Web Config.

- Korisničko ime: ništa (prazno)
- Lozinka: serijski broj skenera

Da biste pronašli serijski broj, proverite nalepnicu na zadnjoj strani skenera. Ako vratite podrazumevana podešavanja za lozinku administratora, vraćaju se na početne vrednosti.

Napredna bezbednosna podešavanja

Bezbednosna podešavanja i sprečavanje opasnosti.	93
Kontrolisanje pomoću protokola.	94
Način korišćenja digitalnog sertifikata.	97
SSL/TLS komunikacija sa skenerom.	102
Šifrovana komunikacija pomoću IPsec/IP filtriranja.	104
Povezivanje skenera na IEEE802.1X mrežu.	114
Rešavanje problema naprednih bezbednosnih postavki.	116

Bezbednosna podešavanja i sprečavanje opasnosti

Kada je skener priključen na mrežu, možete mu pristupiti sa udaljene lokacije. Pored toga, mnogi ljudi mogu zajednički da koriste skener, što je korisno u poboljšavanju radne efikasnosti i praktičnosti. Međutim, rizici kao što su nezakoniti pristup, nezakonita upotreba i neovlašćeno menjanje podataka se povećavaju. Ako koristite skener u okruženju u kom imate pristup internetu, rizici su još veći.

Za skenere koji nemaju zaštitu od spoljašnjeg pristupa, sa interneta će se moći pročitati kontakti koji su sačuvani na skeneru.

Kako bi se izbegao ovaj rizik, Eposonovi skeneri imaju niz bezbednosnih tehnika.

Podesite skener po potrebi u skladu sa uslovima okruženja koje je utemeljeno na informacijama o korisnikovom okruženju.

Naziv	Vrsta funkcije	Šta podesiti	Šta sprečiti
Kontrola protokola	Kontroliše protokole i usluge koje se koriste za komunikaciju između skenera i računara i omogućava i onemogućava funkcije.	Protokol ili usluga koja važi za funkcije koje se dozvoljavaju ili zabranjuju na individualnoj osnovi.	Smanjenje bezbednosnih rizika koji se mogu javiti prilikom nenamerne upotrebe time što korisnici budu sprečeni da koriste nepotrebne funkcije.
SSL/TLS komunikacija	Sadržaj komunikacija se šifruje SSL/TLS komunikacijom prilikom pristupa Epson serveru na Internetu sa skenera, kao što je komunikacija sa računarom preko veb pregledača, korišćenjem Epson Connect i ažuriranjem osnovnog softvera.	Pribavite CA sertifikat, a zatim ga uvezite u skener.	Brisanjem identifikacije skenera uz pomoć CA sertifikata sprečava se lažno predstavljanje i neovlašćen pristup. Pored toga, zaštićeni su komunikacijski sadržaji SSL/TLS i time se sprečava curenje sadržaja za podatke o skeniranju i informacije o podešavanju.
IPsec/IP filtriranje	Možete podesiti da dozvolite odvajanje ili odsecanje podataka koji dolaze od određenog klijenta ili su određenog tipa. Pošto IPsec štiti podatke po jedinici IP paketa (šifrovanje i provera identiteta), možete bezbedno prenositi neobezbeđeni protokol.	Kreirajte osnovne smernice i pojedinačne smernice da biste podesili klijenta ili vrstu podataka koji mogu pristupiti skeneru.	Sprečite neovlašćen pristup, falsifikovanje i presretanje komunikacijskih podataka na skeneru.
IEEE 802.1X	Omogućava da se samo autentifikovani korisnici povežu na mrežu. Omogućava samo dozvoljenom korisniku da koristi skener.	Podešavanje provere identiteta za RADIUS server (server za proveru identiteta).	Zaštite skener od neovlašćenog pristupa i korišćenja.

Povezane informacije

- ➔ [“Kontrolisanje pomoću protokola” na strani 94](#)
- ➔ [“SSL/TLS komunikacija sa skenerom” na strani 102](#)
- ➔ [“Šifrovana komunikacija pomoću IPsec/IP filtriranja” na strani 104](#)
- ➔ [“Povezivanje skenera na IEEE802.1X mrežu” na strani 114](#)

Podešavanja bezbednosnih funkcija

Kada podešavate IPsec/IP filtriranje ili IEEE 802.1X, preporučuje se da pristupite Web Config pomoću SSL/TLS za prenošenje informacija o podešavanju kako bi se umanjili bezbednosni rizici kao što su greška ili prekid.

Vodite računa da konfigurišete lozinku administratora pre podešavanja IPsec/IP filtriranja ili IEEE 802.1X.

Kontrolisanje pomoću protokola

Možete da skenirate pomoću raznih putanja i protokola. Takođe možete da koristite skeniranje mreže sa neograničenog broja mrežnih računara.

Možete da smanjite nenamerne bezbednosne rizike ograničavanjem na skeniranje sa određenih putanja ili kontrolisanjem dostupnih funkcija.

Kontrolisanje protokola

Konfigurišite podešavanja protokola koja skener podržava.

1. Pristupite Web Config i zatim izaberite karticu **Network Security** tab > **Protocol**.
2. Konfigurišite svaku stavku.
3. Kliknite na **Next**.
4. Kliknite na **OK**.

Podešavanja će biti primenjena na skener.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Protokoli koje možete da omogućite ili onemogućite

Protokol	Opis
Bonjour Settings	Možete da navedete želite li da koristite Bonjour. Bonjour se koristi za pronalaženje uređaja, skeniranje, i tako dalje.
SLP Settings	Možete da omogućite ili onemogućite funkciju SLP. SLP se koristi za skeniranje s uređaja i pretraživanje mreže u programu EpsonNet Config.
WSD Settings	Možete da omogućite ili onemogućite funkciju WSD. Kada je omogućena, možete da dodate WSD uređaje i skenirate sa WSD ulaza.
LLTD Settings	Možete da omogućite ili onemogućite funkciju LLTD. Kada je omogućena, biće prikazana Windows mapi mreže.
LLMNR Settings	Možete da omogućite ili onemogućite funkciju LLMNR. Kada je omogućena, možete da koristite razrešavanje imena bez NetBIOS čak i ako ne možete da koristite DNS.

Protokol	Opis
SNMPv1/v2c Settings	Možete da navedete želite li ili ne da omogućite SNMPv1/v2c. Koristi se za podešavanje uređaja, nadgledanje i tako dalje.
SNMPv3 Settings	Možete da navedete želite li ili ne da omogućite SNMPv3. Koristi se za podešavanje šifrovanih uređaja, nadgledanje i tako dalje.

Stavke podešavanja protokola

Bonjour Settings

Stavke	Vrednost i opis podešavanja
Use Bonjour	Izaberite da biste potražili ili koristili uređaje kroz Bonjour.
Bonjour Name	Prikazuje Bonjour ime.
Bonjour Service Name	Prikazuje Bonjour ime usluge.
Location	Prikazuje Bonjour ime lokacije.
Wide-Area Bonjour	Podesite da li će se koristiti Wide-Area Bonjour.

SLP Settings

Stavke	Vrednost i opis podešavanja
Enable SLP	Izaberite ovo da biste omogućili SLP funkciju. Ovo se koristi kao mrežno podešavanje u EpsonNet Config.

WSD Settings

Stavke	Vrednost i opis podešavanja
Enable WSD	Izaberite ovo da biste omogućili dodavanje uređaja koristeći WSD i skenirajte sa WSD ulaza.
Scanning Timeout (sec)	Unesite vreme isteka komunikacije za WSD skeniranje vrednosti između 3 i 3.600 sekundi.
Device Name	Prikazuje WSD ime uređaja.
Location	Prikazuje WSD ime lokacije.

LLTD Settings

Stavke	Vrednost i opis podešavanja
Enable LLTD	Izaberite ovo da biste omogućili LLTD. Skener je prikazan u Windows mapi mreže.
Device Name	Prikazuje LLTD ime uređaja.

LLMNR Settings

Stavke	Vrednost i opis podešavanja
Enable LLMNR	Izaberite ovo da biste omogućili LLMNR. Možete da koristite razrešavanje imena bez NetBIOS čak i ako ne možete da koristite DNS.

SNMPv1/v2c Settings

Stavke	Vrednost i opis podešavanja
Enable SNMPv1/v2c	Izaberite da biste omogućili SNMPv1/v2c.
Access Authority	Podesite pristupno telo kada je omogućen SNMPv1/v2c. Izaberite Read Only ili Read/Write .
Community Name (Read Only)	Unesite između 0 i 32 ASCII (od 0x20 do 0x7E) znaka.
Community Name (Read/Write)	Unesite između 0 i 32 ASCII (od 0x20 do 0x7E) znaka.

SNMPv3 Settings

Stavke	Vrednost i opis podešavanja
Enable SNMPv3	SNMPv3 je omogućen kada je polje štiklirano.
User Name	Unesite između 1 i 32 znaka koristeći znakove dužine jednog bajta.
Authentication Settings	
Algorithm	Odaberite algoritam za proveru identiteta za SNMPv3.
Password	Unesite lozinku za proveru identiteta za SNMPv3. Unesite između 8 i 32 znakova u formatu ASCII (0x20–0x7E). Ako to ne odredite, ostavite prazno.
Confirm Password	Kao potvrdu, unesite lozinku koju ste konfigurisali.
Encryption Settings	
Algorithm	Odaberite algoritam za šifrovanje za SNMPv3.
Password	Unesite lozinku za šifrovanje za SNMPv3. Unesite između 8 i 32 znakova u formatu ASCII (0x20–0x7E). Ako to ne odredite, ostavite prazno.
Confirm Password	Kao potvrdu, unesite lozinku koju ste konfigurisali.
Context Name	Unesite najviše 32 znaka u Unicode formatu (UTF-8). Ako to ne odredite, ostavite prazno. Broj znakova koji može biti unet zavisi od jezika.

Način korišćenja digitalnog sertifikata

O digitalnim sertifikatima

CA-signed Certificate

To je sertifikat koji je potpisalo sertifikaciono telo (CA — Certificate Authority). Možete ga pribaviti ako pošaljete zahtev sertifikacionom telu. Ovaj sertifikat potvrđuje postojanje skenera i koristi se za SSL/TLS komunikaciju, tako da možete da osigurate bezbednost prenosa podataka.

Kada se koristi za SSL/TLS komunikaciju, koristi se kao serverski sertifikat.

Kada je podešen na IPsec/IP filtriranje ili IEEE 802.1X komunikaciju, koristi se kao klijentski sertifikat.

CA sertifikat

To je sertifikat koji se nalazi u nizu CA-signed Certificate, koji se naziva i prelazni CA sertifikat. Veb pregledač ga koristi za proveru putanje do sertifikata skenera prilikom pristupa serveru druge strane ili Web Config.

Za CA sertifikat, podesite kada treba da proverite putanju do sertifikata servera za pristup sa skenera. Za skener, podesite da potvrđuje putanju CA-signed Certificate za SSL/TLS vezu.

Možete dobiti CA sertifikat skenera od sertifikacionog tela kod kog je izdat CA sertifikat.

Takođe možete pribaviti CA sertifikat koji se koristi za proveru servera druge strane od sertifikacionog tela koje je izdalo CA-signed Certificate drugog servera.

Self-signed Certificate

To je sertifikat koji skener sam potpisuje i izdaje. Takođe se naziva korenski sertifikat. S obzirom da izdavalac sam sebe sertifikuje, nije pouzdan i ne može sprečiti lažno predstavljanje.

Koristite ga kada vršite bezbednosna podešavanja i jednostavnu SSL/TLS komunikaciju bez CA-signed Certificate.

Ako koristite taj sertifikat za SSL/TLS komunikaciju, u pregledaču će se možda pojaviti bezbednosno upozorenje, jer sertifikat nije registrovan u pregledaču. Možete da koristite Self-signed Certificate samo za SSL/TLS komunikaciju.

Povezane informacije

- ➔ [“Konfigurisanje opcije CA-signed Certificate” na strani 97](#)
- ➔ [“Ažuriranje nezavisnog sertifikata” na strani 101](#)
- ➔ [“Konfigurisanje opcije CA Certificate” na strani 101](#)

Konfigurisanje opcije CA-signed Certificate

Pribavljanje CA sertifikata

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

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

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

Šta god da izaberete, možete pribaviti isti sertifikat i koristiti ga zajednički.

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

Otvoriće se stranica za kreiranje CSR-a.

3. Unesite vrednost za svaku stavku.

Napomena:

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

4. Kliknite na **OK**.

Prikažaće se poruka sa obaveštenjem o završetku.

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

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



Važno:

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

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

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

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

Postupak dobijanja CA-signed Certificate se smatra gotovim kada sertifikat snimate na određenu lokaciju.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Stavke podešavanja CSR-a

Stavke	Podešavanja i objašnjenje
Key Length	Izaberite dužinu šifre za CSR.

Stavke	Podešavanja i objašnjenje
Common Name	<p>Možete uneti između 1 i 128 znakova. Ako se radi o IP adresi, potrebno je da bude statička. Možete da unesete 1 do 5 IPv4 adresa, IPv6 adresa, naziv matičnog računara, FQDNs odvojiti ih zarezima.</p> <p>Prvi element se čuva u opštem nazivu, a ostali elementi se čuvaju u polju za druge nazive predmeta sertifikata.</p> <p>Primer:</p> <p>IP adresa skenera: 192.0.2.123, Naziv skenera: EPSONA1B2C3 Common Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123</p>
Organization/ Organizational Unit/ Locality/ State/Province	Možete da unesete između 0 i 64 znaka u formatu ASCII (0x20–0x7E). Pojedinačne nazive možete da razdvojite zarezima.
Country	Unesite dvocifrenu šifru zemlje u skladu sa standardom ISO-3166.
Sender's Email Address	Možete uneti elektronsku adresu pošiljaoca radi podešavanja severa za poštu. Unesite istu elektronsku adresu kao što je Sender's Email Address za karticu Network > Email Server > Basic .

Uvoz CA sertifikata

Uvezite dobijeni CA-signed Certificate na skener.



Važno:

- Proverite da li su na skeneru podešeni tačno vreme i datum. Moguće je da sertifikat ne važi.
- Ako ste sertifikat dobili na osnovu CSR formulara iz programa Web Config, sertifikat možete da uvezete jednom.

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

2. Kliknite na **Import**

Otvoriće se stranica za uvoz sertifikata.

3. Unesite vrednost za svaku stavku. Podesite **CA Certificate 1** i **CA Certificate 2** prilikom provere putanju sertifikata na veb pregledaču koji pristupa skeneru.

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

- Sertifikat u formatu PEM/DER dobijen iz programa Web Config
 - Private Key:** Nemojte konfigurisati ovu stavku jer skener sadrži privatni ključ.
 - Password:** Nemojte je konfigurisati.
 - CA Certificate 1/CA Certificate 2:** opciono
- Sertifikat u formatu PEM/DER dobijen sa računara
 - Private Key:** Podesite ovu stavku.
 - Password:** Nemojte je konfigurisati.
 - CA Certificate 1/CA Certificate 2:** opciono

- Sertifikat u formatu PKCS#12 dobijen sa računara
 - Private Key:** Nemojte je konfigurisati.
 - Password:** opciono
 - CA Certificate 1/CA Certificate 2:** Nemojte je konfigurisati.

4. Kliknite na **OK**.

Prikazaće se poruka sa obaveštenjem o završetku.

Napomena:

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

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Stavke za podešavanja uvoza CA sertifikata

Stavka	Podešavanja i objašnjenje
Server Certificate ili Client Certificate	Izaberite format sertifikata. Za SSL/TLS protokol prikazuje se Server Certificate. Za IPsec/IP filtriranje ili IEEE 802.1X, prikazuje se Client Certificate.
Private Key	Ako dobijete sertifikat u formatu PEM/DER pomoću CSR-a napravljenog sa računara, odredite datoteku sa privatnim ključem koja odgovara sertifikatu.
Password	Ako je format Certificate with Private Key (PKCS#12) , unesite lozinku za šifrovanje privatnog ključa koji je podešen kada dobijete sertifikat.
CA Certificate 1	Ako je format vašeg sertifikata Certificate (PEM/DER) , uvezite sertifikat sertifikacionog tela koje izdaje CA-signed Certificate koji se koristi kao sertifikat servera. Ako je potrebno, odredite datoteku.
CA Certificate 2	Ako je format vašeg sertifikata Certificate (PEM/DER) , uvezite sertifikat sertifikacionog tela koje izdaje CA Certificate 1. Ako je potrebno, odredite datoteku.

Brisanje CA sertifikata

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



Važno:

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

1. Pristupite opciji Web Config, i onda odaberite karticu **Network Security**. Zatim izaberite **SSL/TLS > Certificate** ili **IPsec/IP Filtering > Client Certificate** ili **IEEE802.1X > Client Certificate**.
2. Kliknite na **Delete**.

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

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Ažuriranje nezavisnog sertifikata

S obzirom da skener izdaje Self-signed Certificate, možete ga ažurirati kada istekne ili kada se opisani sadržaj promeni.

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

Možete uneti najviše 5 IPv4 adresa, IPv6 adresa, naziva matičnog računara, FQDN-ova od 1 do 128 znakova tako što ćete ih odvojiti zarezima. Prvi parametar se čuva pod zajedničkim imenom, a ostali se čuvaju u drugom polju predmeta sertifikata.

Primer:

IP adresa skenera: 192.0.2.123, Naziv skenera: EPSONA1B2C3

Zajedničko ime: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Navedite rok važenja sertifikata.
5. Kliknite na **Next**.
Prikazaće se poruka sa potvrdom.
6. Kliknite na **OK**.
Skener će biti ažuriran.

Napomena:

*Podatke o sertifikatu možete proveriti sa kartice **Network Security** > **SSL/TLS** > **Certificate** > **Self-signed Certificate** i kliknuti na **Confirm**.*

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Konfigurisanje opcije CA Certificate

Kada podesite CA Certificate, možete proveriti putanju do CA sertifikata servera kojem skener pristupa. Time može da se spreči lažno predstavljanje.

Možete pribaviti CA Certificate od sertifikacionog tela u kom se CA-signed Certificate izdaje.

Uvoz CA Certificate

Uvezite CA Certificate na skener.

1. Pristupite opciji Web Config, a zatim izaberite karticu **Network Security > CA Certificate**.
2. Kliknite na **Import**.
3. Navedite CA Certificate koji želite da uvezete.
4. Kliknite na **OK**.

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

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Brisanje CA Certificate

Možete da izbrišete uvezeni CA Certificate.

1. Pristupite Web Config a zatim izaberite karticu **Network Security > CA Certificate**.
2. Kliknite **Delete** pored CA Certificate koji želite da izbrišete.
3. Potvrdite da želite da izbrišete sertifikat u prikazanoj poruci.
4. Kliknite **Reboot Network**, a zatim proverite da je izbrisan CA sertifikat nije naveden na ažuriranom ekranu.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

SSL/TLS komunikacija sa skenerom

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

Konfigurisanje osnovnih postavki SSL/TLS protokola

Ako skener podržava funkciju HTTPS servera, možete da koristite SSL/TLS protokol da šifrujete komunikaciju. Možete da konfigurirate skener i da njime upravljate pomoću programa Web Config, uz zagarantovanu zaštitu.

Konfigurirate jačinu šifrovanja i funkciju preusmeravanja.

1. Pristupite Web Config i izaberite karticu **Network Security > > SSL/TLS > Basic**.

- Izaberite po jednu vrednost za svaku stavku.
 - Encryption Strength
Izaberite nivo jačine šifrovanja.
 - Redirect HTTP to HTTPS
Preusmeravanje na HTTPS kada se pristupi HTTP-u.
- Kliknite na **Next**.
Prikazaće se poruka sa potvrdom.
- Kliknite na **OK**.
Skener će biti ažuriran.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Konfigurisanje sertifikata servera za skener

- Pristupite Web Config i izaberite karticu **Network Security** > **SSL/TLS** > **Certificate**.
- Odredite koji sertifikat će se koristiti pod opcijom **Server Certificate**.
 - Self-signed Certificate
Skener je generisao nezavisni sertifikat. Izaberite ovu stavku ako niste pribavili CA sertifikat.
 - CA-signed Certificate
Izaberite ovu stavku ako ste unapred pribavili i uvezli CA sertifikat.
- Kliknite na **Next**.
Prikazaće se poruka sa potvrdom.
- Kliknite na **OK**.
Skener će biti ažuriran.

Povezane informacije

- ➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)
- ➔ [“Konfigurisanje opcije CA-signed Certificate” na strani 97](#)
- ➔ [“Konfigurisanje opcije CA Certificate” na strani 101](#)

Šifrovana komunikacija pomoću IPsec/IP filtriranja

O aplikaciji IPsec/IP Filtering

Uz pomoć funkcije IPsec/IP filtriranja možete da filtrirate saobraćaj na osnovu IP adrese, servisa i porta. Kombinovanjem filtera možete da konfigurirate skener tako da prihvata ili blokira određene klijente i određene podatke. Uz to, možete da povećate bezbednost tako što ćete koristiti IPsec.

Napomena:

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

Konfigurisanje podrazumevane smernice

Da bi filtriranje saobraćaja bilo aktivno, konfigurirate podrazumevanu smernicu. Podrazumevane smernice važe za sve korisnike i grupe koje se povezuju sa skenerom. Ako želite da preciznije kontrolišete korisnike i grupe korisnika, konfigurirate smernice za grupe.

1. Pristupite Web Config i zatim izaberite karticu **Network Security > IPsec/IP Filtering > Basic**.
2. Unesite vrednost za svaku stavku.
3. Kliknite na **Next**.
Prikazaće se poruka sa potvrdom.
4. Kliknite na **OK**.
Skener će biti ažuriran.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Default Policy — stavke podešavanja

Default Policy

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

Access Control

Konfigurirate način kontrole saobraćaja IP paketa.

Stavke	Podešavanja i objašnjenje
Permit Access	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IP paketima.
Refuse Access	Izaberite ovu stavku ako želite da zabranite prolaz definisanim IP paketima.
IPsec	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IPsec paketima.

IKE Version

Izaberite IKEv1 ili IKEv2 za IKE Version. Izaberite jednu od njih na osnovu uređaja s kojim je skener povezan.

IKEv1

Kada odaberete IKEv1 kao IKE Version, biće prikazane sledeće stavke.

Stavke	Podešavanja i objašnjenje
Authentication Method	Da biste mogli da izaberete Certificate , potrebno je da unapred dobijete i uvezete CA sertifikat.
Pre-Shared Key	Ako izaberete Pre-Shared Key za Authentication Method , unesite preliminarno deljenu šifru od 1 do 127 znakova.
Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.

IKEv2

Kada odaberete IKEv2 kao IKE Version, biće prikazane sledeće stavke.

Stavke	Podešavanja i objašnjenje	
Local	Authentication Method	Da biste mogli da izaberete Certificate , potrebno je da unapred dobijete i uvezete CA sertifikat.
	ID Type	Ako odaberete Pre-Shared Key za Authentication Method , izaberite vrstu ID oznake za skener.
	ID	Unesite ID skenera koji odgovara vrsti ID oznake. Kao prvi znak ne možete upotrebiti „@“, „#“, i „=“. Distinguished Name: Unesite između 1 i 255 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „=“. IP Address: Unesite format IPv4 ili IPv6. FQDN: Unesite kombinaciju znakova dužine od 1 do 255 znakova, koristeći znakove A–Z, a–z, 0–9, „-“ i tačku (.). Email Address: Unesite između 1 i 255 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „@“. Key ID: Unesite između 1 i 255 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.
	Pre-Shared Key	Ako izaberete Pre-Shared Key za Authentication Method , unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.

Stavke		Podešavanja i objašnjenje
Remote	Authentication Method	Da biste mogli da izaberete Certificate , potrebno je da unapred dobijete i uvezete CA sertifikat.
	ID Type	Ako odaberete Pre-Shared Key za Authentication Method , izaberite vrstu ID oznake za uređaj čiji identitet želite da proverite.
	ID	Unesite ID skenera koji odgovara vrsti ID oznake. Kao prvi znak ne možete upotrebiti „@“, „#“, i „=“. Distinguished Name: Unesite između 1 i 255 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „=“. IP Address: Unesite format IPv4 ili IPv6. FQDN: Unesite kombinaciju znakova dužine od 1 do 255 znakova, koristeći znakove A–Z, a–z, 0–9, „-“ i tačku (.). Email Address: Unesite između 1 i 255 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Potrebno je da uključite „@“. Key ID: Unesite između 1 i 255 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.
	Pre-Shared Key	Ako izaberete Pre-Shared Key za Authentication Method , unesite preliminarno deljenu šifru od 1 do 127 znakova.
	Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.

Encapsulation

Ako izaberete **IPsec** za **Access Control**, potrebno je da konfigurirate režim enkapsulacije.

Stavke	Podešavanja i objašnjenje
Transport Mode	Izaberite ovu opciju ako skener uvek koristite na istoj LAN mreži. IP paketi sloja 4 i viših slojeva se šifruju.
Tunnel Mode	Ako koristite skener na mreži sa mogućnošću priključenja na internet, kao što je IPsec-VPN, izaberite ovu opciju. Zaglavlje i podaci o IP paketima se šifruju. Remote Gateway(Tunnel Mode): Ako izaberete Tunnel Mode za Encapsulation , unesite adresu mrežnog prolaza od 1 do 39 znakova.

Security Protocol

Ako izaberete **IPsec** za **Access Control**, izaberite neku opciju.

Stavke	Podešavanja i objašnjenje
ESP	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka i kako biste šifrovali podatke.
AH	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka. Čak i ako je šifrovanje podataka zabranjeno, možete da koristite IPsec.

❑ Algorithm Settings

Preporučuje se da izaberete **Any** za sva podešavanja ili da izaberete stavku osim **Any** svako podešavanje. Ako izaberete **Any** za neka od podešavanja i izaberete stavku osim **Any** za ostala podešavanja, možda neće postojati komunikacija s uređajem, zavisno od drugog uređaja koji želite da proverite.

Stavke		Podešavanja i objašnjenje
IKE	Encryption	Odaberite algoritam za šifrovanje za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.
	Authentication	Odaberite algoritam za proveru identiteta za IKE.
	Key Exchange	Odaberite algoritam za razmenu ključeva za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.
ESP	Encryption	Odaberite algoritam za šifrovanje za ESP. Ova funkcija je dostupna kada je ESP podešen na Security Protocol .
	Authentication	Odaberite algoritam za proveru identiteta za ESP. Ova funkcija je dostupna kada je ESP podešen na Security Protocol .
AH	Authentication	Odaberite algoritam za šifrovanje za AH. Ova funkcija je dostupna kada je AH podešen na Security Protocol .

Konfigurisanje smernica za grupe

Smernice za grupu su jedno ili više pravila koja se primenjuju na korisnika ili grupu korisnika. Skener kontroliše IP pakete koji odgovaraju konfigurisanim smernicama. Proverava se identitet IP paketa u odnosu na smernice za grupu redosledom od 1 do 10, a zatim u odnosu na podrazumevanu smernicu.

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

Group Policy — stavke podešavanja

Stavke	Podešavanja i objašnjenje
Enable this Group Policy	Možete da omogućite ili onemogućite smernicu za grupu.

Access Control

Konfigurirate način kontrole saobraćaja IP paketa.

Stavke	Podešavanja i objašnjenje
Permit Access	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IP paketima.
Refuse Access	Izaberite ovu stavku ako želite da zabranite prolaz definisanim IP paketima.
IPsec	Izaberite ovu stavku ako želite da dozvolite prolaz definisanim IPsec paketima.

Local Address (Scanner)

Izaberite IPv4 adresu ili IPv6 adresu koja odgovara vašem mrežnom okruženju. Ako se IP adresa dodeli automatski, možete izabrati **Use auto-obtained IPv4 address**.

Napomena:

Ako je IPv6 adresa automatski dodeljena, povezivanje možda neće biti moguće. Konfigurirate statičku IPv6 adresu.

Remote Address(Host)

Unesite IP adresu uređaja da biste mogli da upravljate pristupom. IP adresa mora biti dužine do 43 znaka. Ako ne unesete IP adresu, kontrolisaće se sve adrese.

Napomena:

Ako je IP adresa automatski dodeljena (npr. ako ju je dodelio DHCP), povezivanje možda neće biti moguće. Konfigurirate statičku IP adresu.

Method of Choosing Port

Izaberite način određivanja portova.

Service Name

Ako izaberete **Service Name** za **Method of Choosing Port**, izaberite neku opciju.

Transport Protocol

Ako izaberete **Port Number** za **Method of Choosing Port**, potrebno je da konfigurirate režim enkapsulacije.

Stavke	Podešavanja i objašnjenje
Any Protocol	Izaberite ovu stavku kako biste upravljali vrstama protokola.
TCP	Izaberite ovu stavku kako biste upravljali podacima za unicast.
UDP	Izaberite ovu stavku kako biste upravljali podacima za broadcast i multicast.
ICMPv4	Izaberite ovu stavku kako biste upravljali komandom za ping.

Local Port

Ako izaberete **Port Number** za **Method of Choosing Port** i ako izaberete **TCP** ili **UDP** za **Transport Protocol**, unesite brojeve portova za upravljanje prijemom paketa, odvojene zarezima. Možete da unesete najviše 10 brojeva portova.

Primer: 20,80,119,5220

Ako ne unesete broj porta, kontrolisaće se svi portovi.

Remote Port

Ako izaberete **Port Number** za **Method of Choosing Port** i ako izaberete **TCP** ili **UDP** za **Transport Protocol**, unesite brojeve portova za upravljanje slanjem paketa, odvojene zarezima. Možete da unesete najviše 10 brojeva portova.

Primer: 25,80,143,5220

Ako ne unesete broj porta, kontrolisaće se svi portovi.

IKE Version

Izaberite **IKEv1** ili **IKEv2** za **IKE Version**. Izaberite jednu od njih na osnovu uređaja s kojim je skener povezan.

IKEv1

Kada odaberete **IKEv1** kao **IKE Version**, biće prikazane sledeće stavke.

Stavke	Podešavanja i objašnjenje
Authentication Method	Ako izaberete IPsec za Access Control , izaberite neku opciju. Za podrazumevanu smernicu uobičajen je korišćeni sertifikat.
Pre-Shared Key	Ako izaberete Pre-Shared Key za Authentication Method , unesite preliminarno deljenu šifru od 1 do 127 znakova.
Confirm Pre-Shared Key	Kao potvrdu, unesite šifru koju ste konfigurisali.

❑ IKEv2

Kada odaberete **IKEv2** kao **IKE Version**, biće prikazane sledeće stavke.

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

Encapsulation

Ako izaberete **IPsec** za **Access Control**, potrebno je da konfigurirate režim enkapsulacije.

Stavke	Podešavanja i objašnjenje
Transport Mode	Izaberite ovu opciju ako skener uvek koristite na istoj LAN mreži. IP paketi sloja 4 i viših slojeva se šifruju.
Tunnel Mode	Ako koristite skener na mreži sa mogućnošću priključenja na internet, kao što je IPsec-VPN, izaberite ovu opciju. Zaglavlje i podaci o IP paketima se šifruju. Remote Gateway(Tunnel Mode): Ako izaberete Tunnel Mode za Encapsulation , unesite adresu mrežnog prolaza od 1 do 39 znakova.

Security Protocol

Ako izaberete IPsec za Access Control, izaberite neku opciju.

Stavke	Podešavanja i objašnjenje
ESP	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka i kako biste šifrovali podatke.
AH	Izaberite ovu stavku kako biste obezbedili integritet provere identiteta i podataka. Čak i ako je šifrovanje podataka zabranjeno, možete da koristite IPsec.

Algorithm Settings

Preporučuje se da izaberete **Any** za sva podešavanja ili da izaberete stavku osim **Any** svako podešavanje. Ako izaberete **Any** za neka od podešavanja i izaberete stavku osim **Any** za ostala podešavanja, možda neće postojati komunikacija s uređajem, zavisno od drugog uređaja koji želite da proverite.

Stavke	Podešavanja i objašnjenje	
IKE	Encryption	Odaberite algoritam za šifrovanje za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.
	Authentication	Odaberite algoritam za proveru identiteta za IKE.
	Key Exchange	Odaberite algoritam za razmenu ključeva za IKE. Stavke se razlikuju u zavisnosti od IKE verzije.
ESP	Encryption	Odaberite algoritam za šifrovanje za ESP. Ova funkcija je dostupna kada je ESP podešen na Security Protocol .
	Authentication	Odaberite algoritam za proveru identiteta za ESP. Ova funkcija je dostupna kada je ESP podešen na Security Protocol .
AH	Authentication	Odaberite algoritam za šifrovanje za AH. Ova funkcija je dostupna kada je AH podešen na Security Protocol .

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

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

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

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

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

*3 Osim za lokalne adrese IPv6 linka.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Reference naziva usluge u smernicama za grupe

Napomena:

Nedostupne usluge su prikazane, ali se ne mogu izabrati.

Naziv usluge	Tip protokola	Broj lokalnog izlaza	Broj udaljenog izlaza	Funkcije koje se kontrolišu
Any	–	–	–	Sve usluge
ENPC	UDP	3289	Bilo koji izlaz	Traženje skenera iz aplikacije kao što je Epson Device Admin i upravljačkog programa skenera
SNMP	UDP	161	Bilo koji izlaz	Preuzimanje i konfigurisanje MIB iz aplikacije kao što je Epson Device Admin i Epson upravljačkog programa skenera
WSD	TCP	Bilo koji izlaz	5357	Kontrolni WSD
WS-Discovery	UDP	3702	Bilo koji izlaz	Traženje za WSD skenere
Network Scan	TCP	1865	Bilo koji izlaz	Prosleđivanje skeniranih podataka iz aplikacije Document Capture Pro
Network Push Scan	TCP	Bilo koji izlaz	2968	Preuzimanje informacija o zadatku skeniranja s uređaja iz aplikacije Document Capture Pro
Network Push Scan Discovery	UDP	2968	Bilo koji izlaz	Traženje računara sa skenera
FTP Data (Remote)	TCP	Bilo koji izlaz	20	FTP klijent (prosleđivanje skeniranih podataka) Međutim, to može da kontroliše samo FTP server koji koristi udaljeni izlaz broj 20.
FTP Control (Remote)	TCP	Bilo koji izlaz	21	FTP klijent (kontrola prosleđenih skeniranih podataka)

Naziv usluge	Tip protokola	Broj lokalnog izlaza	Broj udaljenog izlaza	Funkcije koje se kontrolišu
CIFS (Remote)	TCP	Bilo koji izlaz	445	CIFS klijent (prosleđivanje skeniranih podataka u fasciklu)
NetBIOS Name Service (Remote)	UDP	Bilo koji izlaz	137	CIFS klijent (prosleđivanje skeniranih podataka u fasciklu)
NetBIOS Datagram Service (Remote)	UDP	Bilo koji izlaz	138	
NetBIOS Session Service (Remote)	TCP	Bilo koji izlaz	139	
HTTP (Local)	TCP	80	Bilo koji izlaz	HTTP(S) server (prosleđivanje podataka o Web Config i WSD)
HTTPS (Local)	TCP	443	Bilo koji izlaz	
HTTP (Remote)	TCP	Bilo koji izlaz	80	HTTP(S) klijent (ažuriranje osnovnog softvera i ažuriranje osnovnog sertifikata)
HTTPS (Remote)	TCP	Bilo koji izlaz	443	

Primeri konfigurisanja opcije IPsec/IP Filtering

Prijem samo IPsec paketa

Ovaj primer služi samo za konfigurisanje podrazumevane smernice.

Default Policy:

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

Group Policy: Nemojte je konfigurisati.

Prihvatanje podataka za skeniranje i postavki skenera

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

Default Policy:

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

Group Policy:

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

Prihvatanje pristupa samo sa određene IP adrese

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

Default Policy:

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

Group Policy:

- Enable this Group Policy: Štiklirajte ovo polje.
- Access Control: Permit Access
- Remote Address(Host): IP adresa klijenta administratora

Napomena:

Bez obzira na konfiguraciju smernice, klijent će moći da pristupi skeneru i da ga konfigurira.

Konfigurisanje sertifikata za IPsec/IP filtriranje

Konfigurirate klijentski sertifikat za IPsec/IP filtriranje. Kada ga podesite, možete koristiti sertifikat kao metod provere identiteta za IPsec/IP filtriranje. Ako želite da konfigurirate sertifikaciono telo, idite u **CA Certificate**.

1. Pristupite Web Config i zatim izaberite karticu **Network Security > IPsec/IP Filtering > Client Certificate**.
2. Uvezite sertifikat u **Client Certificate**.

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

Povezane informacije

- ➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)
- ➔ [“Konfigurisanje opcije CA-signed Certificate” na strani 97](#)
- ➔ [“Konfigurisanje opcije CA Certificate” na strani 101](#)

Povezivanje skenera na IEEE802.1X mrežu

Konfigurisanje IEEE 802.1X mreže

Kada podesite IEEE 802.1X mrežu na skeneru, možete da je koristite na mreži povezanoj sa RADIUS serverom, LAN prekidačem sa funkcijom provere identiteta ili pristupnom tačkom.

1. Pristupite Web Config i zatim izaberite karticu **Network Security > IEEE802.1X > Basic**.
2. Unesite vrednost za svaku stavku.

Ako želite da koristite skener na bežičnoj mreži, kliknite na **Wi-Fi Setup** i izaberite ili unesite SSID.

Napomena:

Možete deliti postavke između mreža Ethernet i Wi-Fi.

3. Kliknite na **Next**.
Prikazaće se poruka sa potvrdom.
4. Kliknite na **OK**.
Skener će biti ažuriran.

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

IEEE 802.1X mreža — stavke podešavanja

Stavke	Podešavanja i objašnjenje	
IEEE802.1X (Wired LAN)	Možete da omogućite ili onemogućite podešavanja stranice (IEEE802.1X > Basic) za IEEE802.1X (ožičena LAN mreža).	
IEEE802.1X (Wi-Fi)	Prikazaće se status veze za IEEE802.1X (Wi-Fi).	
Connection Method	Prikazan je način povezivanja trenutno aktivne mreže.	
EAP Type	Izaberite metod provere identiteta između skenera i RADIUS servera.	
	EAP-TLS	Morate pribaviti i uvesti CA sertifikat.
	PEAP-TLS	
	PEAP/MSCHAPv2	Morate konfigurisati lozinku.
	EAP-TTLS	
User ID	Konfigurirajte ID koji će se koristiti za proveru identiteta RADIUS servera. Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.	
Password	Konfigurirajte lozinku kojom će se proveravati identitet skenera. Unesite između 1 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta. Ako koristite a Windows server kao RADIUS server, možete da unesete do 127 znakova.	
Confirm Password	Kao potvrdu, unesite lozinku koju ste konfigurisali.	
Server ID	Možete da konfigurirate ID na serveru kojim će se proveravati vaš identitet na RADIUS serveru. Čvorište koje proverava identitet će proveriti da li je ID servera sadržan u polju subject/subjectAltName u sertifikatu servera koji je poslat sa RADIUS servera. Unesite između 0 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.	
Certificate Validation	Možete da podesite validaciju sertifikata bez obzira na metod provere identiteta. Uvezite sertifikat u CA Certificate .	
Anonymous Name	Ako izaberete PEAP-TLS ili PEAP/MSCHAPv2 kao EAP Type , možete da konfigurirate anonimno ime umesto korisničkog ID-a za fazu 1 PEAP provere identiteta. Unesite između 0 i 128 ASCII znakova (od 0x20 do 0x7E) veličine jednog bajta.	

Stavke	Podešavanja i objašnjenje	
Encryption Strength	Možete da izaberete jednu od sledećih stavki.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Konfigurisanje sertifikata za IEEE 802.1X

Konfigurirate klijentski sertifikat za IEEE802.1X. Kada ga podesite, možete koristiti **EAP-TLS** i **PEAP-TLS** kao metod provere identiteta za IEEE 802.1X. Ako želite da konfigurirate sertifikat sertifikacionog tela, idite u **CA Certificate**.

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

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

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Rešavanje problema naprednih bezbednosnih postavki

Vraćanje bezbednosnih podešavanja

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

Onemogućavanje bezbednosne funkcije pomoću Web Config

Možete da onemogućite IPsec/IP Filtering pomoću Web Config.

1. Pristupite Web Config i izaberite karticu **Network Security > IPsec/IP Filtering > Basic**.
2. Onemogućite **IPsec/IP Filtering**.

Problemi pri korišćenju funkcija za bezbednost na mreži

Ako zaboravite preliminarno deljenu šifru

Ponovo konfigurirate preliminarno deljenu šifru.

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

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

Povezane informacije

- ➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)
- ➔ [“Šifrovana komunikacija pomoću IPsec/IP filtriranja” na strani 104](#)

Komunikacija preko IPsec protokola nije moguća

Odredite algoritam koji skener ili računar ne podržavaju.

Skener podržava sledeće algoritme. Proverite podešavanja računara.

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

* Dostupan samo za IKEv2

Povezane informacije

- ➔ [“Šifrovana komunikacija pomoću IPsec/IP filtriranja” na strani 104](#)

Komunikacija je naglo prekinuta

IP adresa skenera je promenjena ili se ne može koristiti.

Kada je IP adresa registrovana na lokalnu adresu na Group Policy promenjena ili se ne može koristiti, IPsec komunikacija ne može da se izvrši. Onemogućite IPsec preko kontrolne table skenera.

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

Unesite statičku IP adresu.

IP adresa računara je promenjena ili se ne može koristiti.

Kada je IP adresa registrovana na udaljenu adresu na Group Policy promenjena ili se ne može koristiti, IPsec komunikacija ne može da se izvrši.

Onemogućite IPsec preko kontrolne table skenera.

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

Unesite statičku IP adresu.

Povezane informacije

- ➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)
- ➔ [“Šifrovana komunikacija pomoću IPsec/IP filtriranja” na strani 104](#)

Povezivanje nakon konfigurisanja IPsec/IP filtriranja nije moguće

Podešavanja IPsec/IP filtriranja nisu tačna.

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

Povezane informacije

- ➔ [“Šifrovana komunikacija pomoću IPsec/IP filtriranja” na strani 104](#)

Ne možete pristupiti skeneru nakon konfigurisanja IEEE 802.1X

Podešavanja IEEE 802.1X nisu tačna.

Onemogućite IEEE 802.1X i Wi-Fi sa kontrolne table skenera. Povežite skener i računar, a zatim ponovo konfigurirate IEEE 802.1X.

Povežite skener i računar, a zatim ponovo konfigurirate IEEE 802.1X.

Povezane informacije

- ➔ [“Konfigurisanje IEEE 802.1X mreže” na strani 114](#)

Problemi pri korišćenju digitalnog sertifikata

Ne možete da uvezete CA-signed Certificate

CA-signed Certificate i informacije o CSR -u se ne podudaraju.

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

- Da li pokušavate da uvezete sertifikat na uređaj koji ne sadrži iste informacije?
Proverite informacije u CSR-u, pa uvezite sertifikat na uređaj koji sadrži iste informacije.
- Da li ste zamenili CSR sačuvan na skeneru nakon slanja CSR-a sertifikacionom telu?
Ponovo pribavite CA sertifikat uz pomoć CSR-a.

CA-signed Certificate ima više od 5 KB.

Ne možete da uvezete CA-signed Certificate ako ima više od 5 KB.

Lozinka za uvoz sertifikata nije tačna.

Unesite tačnu lozinku. Ako zaboravite lozinku, nećete moći da uvezete sertifikat. Ponovo pribaviti CA-signed Certificate.

Povezane informacije

➔ [“Uvoz CA sertifikata” na strani 99](#)

Nezavisni sertifikat nije moguće ažurirati

Nije uneseno Common Name.

Potrebno je uneti Common Name.

Nepodržani znakovi su uneti u Common Name.

Unesite između 1 i 128 znakova u formatu IPv4, IPv6, kao naziv matičnog računara ili u formatu FQDN u obliku ASCII (0x20–0x7E).

Razmak ili zarez su uključeni u opšti naziv.

Ako unesete zarez, Common Name se deli na tom mestu. Ako se unese samo razmak pre ili posle zareza, pojaviće se greška.

Povezane informacije

➔ [“Ažuriranje nezavisnog sertifikata” na strani 101](#)

Nije moguće kreirati CSR

Nije uneseno Common Name.

Potrebno je uneti Common Name.

Nepodržani znakovi su uneti u Common Name, Organization, Organizational Unit, Locality, i State/Province.

Unesite znakove u formatu IPv4, IPv6, kao naziva matičnog računara ili u formatu FQDN u obliku ASCII (0x20–0x7E).

Razmak ili zarez su uključeni u Common Name.

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

Povezane informacije

➔ [“Pribavljanje CA sertifikata” na strani 97](#)

Pojavljuje se upozorenje koje se odnosi na digitalni sertifikat

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

Poruke	Uzrok/lek
Invalid file.	<p>Uzrok:</p> <p>Ne uvozite sertifikat u formatu datoteke X509.</p> <p>Lek:</p> <p>Proverite da li ste izabrali odgovarajući sertifikat koji vam je poslalo pouzdano sertifikaciono telo.</p>
	<p>Uzrok:</p> <p>Datoteka koju ste uvezli je prevelika. Maksimalna veličina datoteke je 5 KB.</p> <p>Lek:</p> <p>Ako izaberete odgovarajuću datoteku, sertifikat je možda oštećen ili lažan.</p>
	<p>Uzrok:</p> <p>Lanac u sertifikatu nije ispravan.</p> <p>Lek:</p> <p>Više informacija o sertifikatu potražite na veb lokaciji sertifikacionog tela.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p>Uzrok:</p> <p>Sertifikat u formatu datoteke PKCS#12 sadrži više od 3 CA sertifikata.</p> <p>Lek:</p> <p>Svaki sertifikat uvezite nakon konvertovanja iz formata PKCS#12 u format PEM ili uvezite sertifikat u formatu datoteke PKCS#12 koji sadrži do 2 CA sertifikata.</p>
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p>Uzrok:</p> <p>Sertifikat je istekao.</p> <p>Lek:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ako je sertifikat istekao, pribavite i uvezite novi. <input type="checkbox"/> Ako sertifikat nije istekao, proverite da li su u skeneru podešeni tačno vreme i datum.
Private key is required.	<p>Uzrok:</p> <p>Sa sertifikatom nije uparen nijedan privatni ključ.</p> <p>Lek:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ako je sertifikat u formatu PEM/DER i ako je dobijen na osnovu CSR-a preko računara, navedite datoteku sa privatnim ključem. <input type="checkbox"/> Ako je sertifikat u formatu PKCS#12 i ako je dobijen na osnovu CSR-a preko računara, navedite datoteku sa privatnim ključem.
	<p>Uzrok:</p> <p>Ponovo ste uvezli PEM/DER sertifikat dobijen na osnovu CSR-a pomoću programa Web Config.</p> <p>Lek:</p> <p>Ako je sertifikat u formatu PEM/DER i ako je dobijen na osnovu CSR-a pomoću programa Web Config, možete da ga uvezete samo jednom.</p>

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

Povezane informacije

➔ [“O digitalnim sertifikatima” na strani 97](#)

Greškom ste izbrisali CA sertifikat

Ne postoji rezervna kopija datoteke CA sertifikata.

Ako imate rezervnu kopiju datoteke, ponovo uvezite sertifikat.

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

Povezane informacije

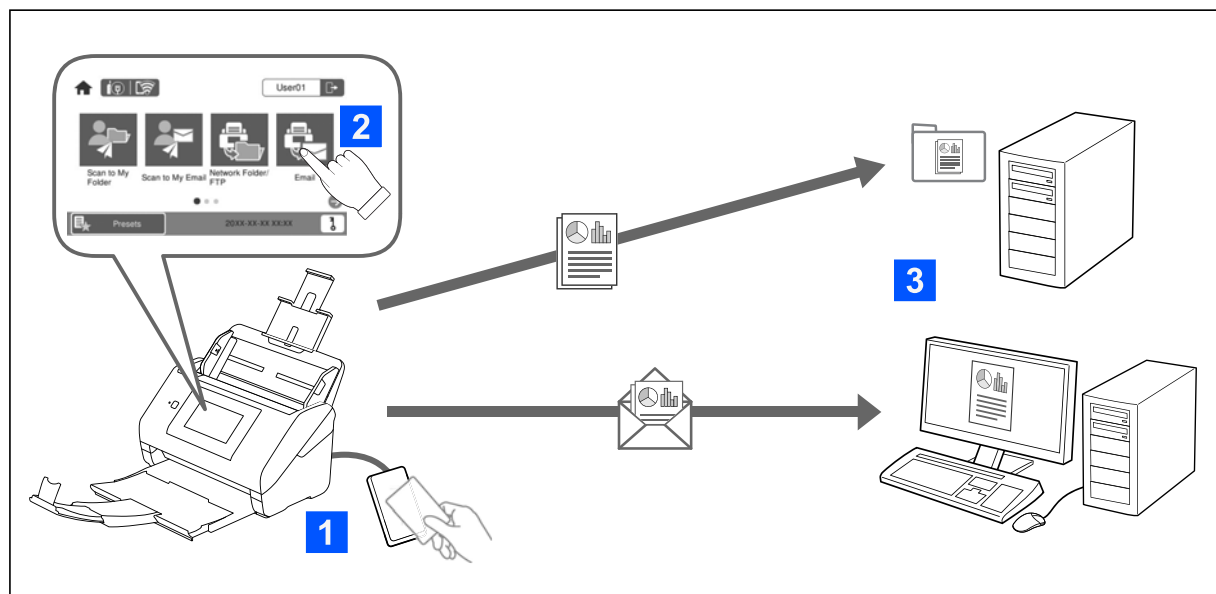
➔ [“Uvoz CA sertifikata” na strani 99](#)

➔ [“Brisanje CA sertifikata” na strani 100](#)

Authentication Settings

O aplikaciji Authentication Settings.	124
O aplikaciji Authentication Method.	125
Softver za podešavanje.	127
Ažuriranje osnovnog softvera skenera.	127
Povezivanje i konfiguracija uređaja za autorizaciju.	127
Registrowanje i podešavanje podataka.	132
Izveštaji Job History pomoću Epson Device Admin.	147
Prijavite se kao administrator sa kontrolne table štampača.	148
Onemogućavanje Authentication Settings.	148
Brisanje Authentication Settings informacija (Vrati podrazumevane postavke).	149
Rešavanje problema.	149

O aplikaciji Authentication Settings



Kada je omogućeno Authentication Settings, neophodna je provera identiteta korisnika. Možete da podesite načine skeniranja koje svaki korisnik može da koristi i sprečite slučajna pokretanja.

Možete da navedete adresu e-pošte ovlašćenog korisnika kao odredište skeniranja (Scan to My Email), ili sačuvate podatke svakog korisnika u ličnu fasciklu (Scan to My Folder). Takođe možete da odredite ostale načine skeniranja.

Napomena:

- Ne možete da skenirate sa računara ili pametnog uređaja kada je omogućena opcija Authentication Settings.
- Pored Authentication Settings navedenih u priručniku, takođe možete da napravite sistem za autorizaciju pomoću servera za autorizaciju. Da biste napravili sistem, koristite Document Capture Pro Server Authentication Edition (skraćeni naziv je Document Capture Pro Server AE). Za više informacija obratite se lokalnom predstavništvu kompanije Epson.

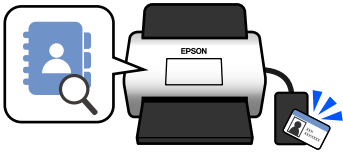
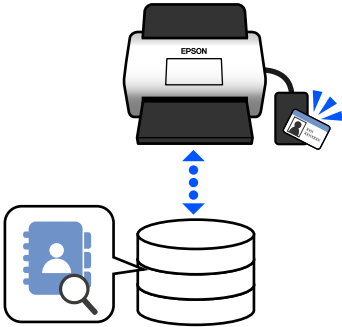
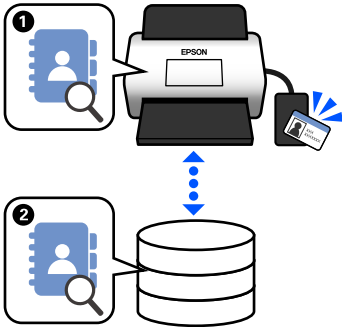
Dostupne funkcije za Authentication Settings

Funkcije skeniranja na kontrolnoj tabli	Authentication Settings	
	Kada je omogućeno	Kada je onemogućeno
Skeniraj u moju fasciklu Čuva slike u fascikli dodeljenoj ovlašćenom korisniku.	✓	-
Skeniraj u moj imejl Šalje slike na adresu e-pošte dodeljenu ovlašćenom korisniku.	✓	-
Skeniraj na mrežni direktorijum/FTP Čuva slike u fascikli na mreži.	✓	✓

Funkcije skeniranja na kontrolnoj tabli	Authentication Settings	
	Kada je omogućeno	Kada je onemogućeno
<p>Skeniraj na računar</p> <p>Čuva slike na povezani računar pomoću zadatka napravljenog u Document Capture Pro (Windows)/Document Capture (Mac OS).</p> <p>* Kada je omogućeno Authentication Settings, možete da koristite samo zadatke koji su registrovani u Un. pod. vr.</p>	✓*	✓
<p>Skeniraj na imejl</p> <p>Šalje slike na adresu e-pošte koju ste podesili.</p>	✓	✓
<p>Skeniraj u oblak</p> <p>Šalje slike u računarski oblak koji ste podesili.</p>	✓	✓
<p>Skeniraj na USB disk</p> <p>Čuva slike na USB disk koji je povezan na skener. Ovo je dostupno samo ako je uređaj za proveru identiteta povezan sa skenerom.</p>	✓	✓
<p>Skenirajte na WSD</p> <p>Čuva slike na povezani računar pomoću WSD funkcije.</p>	-	✓
<p>Un. pod. vr.</p> <p>Možete registrovati najviše 48 podrazumevanih funkcija skeniranja.</p> <p>Možete dodeliti najviše pet Un. pod. vr. korisnicima registrovanim u Local DB. Dodeljena Un. pod. vr. su dostupna samo za tog korisnika. Un. pod. vr. koja nisu dodeljena nijednom korisniku mogu da koriste svi ostali korisnici.</p>	✓	✓

O aplikaciji Authentication Method

Ovaj skener pruža autorizaciju pomoću sledećih načina bez obaveznog pravljenja servera za autorizaciju.

	Local DB	LDAP	Local DB and LDAP
Informacije o lokaciji korisnika	<p>Memorija skenera</p> <p>Metod autorizacije proverava informacije korisnika koji je registrovan na skener i upoređuje ih sa korisnikom koji koristi funkcije skeniranja.</p>	<p>LDAP server*</p> <p>Metod autorizacije proverava informacije korisnika LDAP servera sinhronizovanog sa skenerom. S obzirom da se 300 stavki korisničkih informacija sa LDAP servera može privremeno čuvati u skeneru kao skrivena memorija, autorizacija se može izvršiti pomoću skrivene memorije ako LDAP server prestane da radi.</p> <p>* Server koji pruža usluge direktorijuma koji može da komunicira sa LDAP.</p>	<p>Memorija skenera i LDAP server</p> <p>Prvo proverite informacije korisnika registrovanih u skeneru (1), i ako ih nema puno, proverite informacije korisnika u odnosu na LDAP server (2).</p>
			
Broj registrovanih korisnika	50 (memorija skenera)	Neograničeno (LDAP server)	50 (memorija skenera) Neograničeno (LDAP server)
Skrivena memorija skenera	-	300	Maks. 300 (50 proširenja skrivene memorije dele User Settings u Local DB)
Metod prijave	<p>Možete da koristite bilo koji od sledećih načina.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Podignite autorizacionu karticu, ili unesite User ID i Password <input type="checkbox"/> Podignite autorizacionu karticu, ili unesite ID Number <input type="checkbox"/> Unesite User ID i Password <input type="checkbox"/> Unesite User ID <input type="checkbox"/> Unesite ID Number 		
Ograničenja funkcije „Skeniraj na“	Podesite pojedinačno za svakog korisnika	Ista podešavanja za sve korisnike LDAP	Local DB korisnici: podesite pojedinačno LDAP korisnici: ista podešavanja za sve korisnike
Dodeljena Un. pod. vr. korisnicima	Najviše 5 po korisniku	- (ne može se podesiti pojedinačno)	Local DB korisnici: najviše 5 po korisniku LDAP korisnici: -

Softver za podešavanje

Podesite pomoću Web Config ili Epson Device Admin.

- Kada koristite Web Config, možete da podesite skener samo pomoću veb pregledača.
[“Web Config” na strani 35](#)
- Kada koristite Epson Device Admin, možete istovremeno podesiti više skenera pomoću šablona za konfiguraciju.
[“Epson Device Admin” na strani 36](#)

Ažuriranje osnovnog softvera skenera

Pre omogućavanja Authentication Settings, ažurirajte osnovni softver skenera na najnoviju verziju. Prethodno povežite skener na internet.



Važno:

Za vreme ažuriranja nemojte isključivati računar ili skener.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Device Management > Firmware Update**, a zatim pratite uputstva na ekranu kako biste ažurirali osnovni softver.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Home > Firmware > Update** na ekranu liste uređaja, a zatim pratite uputstva na ekranu kako biste ažurirali osnovni softver.

Napomena:

Ako je već instaliran najnoviji osnovni softver, ne treba da ga ažurirate.

Povezivanje i konfiguracija uređaja za autorizaciju

Ako želite da povežete i koristite uređaj za autorizaciju, kao što je čitač IC kartice, prvo morate da konfigurirate uređaj. To nije neophodno ako ne koristite uređaj za autorizaciju.

Povezane informacije

- ➔ [“Povezivanje sa uređajem za autorizaciju” na strani 130](#)
- ➔ [“Podešavanja uređaja za autorizaciju” na strani 131](#)

Lista kompatibilnih čitača kartice

Ova lista ne garantuje rad čitača kartica na listi.

Da: kompatibilan (ID informacije se mogu očitati pomoću standardnih podešavanja čitača kartice.)

Ne: nije kompatibilan

Proizvođač	Model	Model proizvoda	Autorizacijska kartica							Režim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
RF IDE-AS	pcProx Plus	RDR-80081AKU	Da	Da*1	Da*1	Da*1	Ne	Ne	Ne	Tastatura
RF IDE-AS	pcProx	RDR-7081BKU	Da*1	Ne	Da	Da	Ne	Ne	Ne	Tastatura
RF IDE-AS	pcProx	RDR-7581AKU	Da	Ne	Da*1	Da*1	Ne	Ne	Ne	Tastatura
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Ne	Ne	Da	Da	Ne	Ne	Ne	Tastatura
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Da	Ne	Da	Da	Da	Da	Da	Tastatura
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Da	Da	Da	Da	Da	Da	Da	Tastatura
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Da	Da	Da	Da	Da	Da	Da	Tastatura
ELATEC	TWN4 Slim	T4QC-FC3B7	Da	Da	Da	Da	Da	Da	Da	Tastatura
HID Global	OMNI-KEY 5427	OMNI-KEY5427CK OMNI-KEY5427CK gen2	Da	Da	Da	Da	Da	Ne	Da	Tastatura*1
ACS	ACR122U	ACR122U	Ne	Ne	Da*2	Da*2	Da	Ne	Da*2	PC/SC

Proizvođač	Model	Model proizvođača	Autorizacijska kartica							Režim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
ACS	ACR1252	ACR1252	Ne	Ne	Da*2	Da*2	Da	Da	Da*2	PC/SC
Sony	PaSoRi	RC-S330/S	Ne	Ne	Da*2	Da*2	Da*2	Da*2	Da*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Ne	Ne	Da*2	Da*2	Da*2	Da*2	Da*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Da	Da	Da	Da	Da	Da	Da	Tastatura
DMZ	Leitor RFID Multi-125	DMZ087	Ne	Da	Ne	Ne	Ne	Ne	Ne	Tastatura
DMZ	Leitor RFID Mifare	DMZ088	Ne	Ne	Da	Da	Ne	Ne	Ne	Tastatura
DMZ	Biometric & RFID Reader	DMZ073	Ne	Da	Ne	Ne	Ne	Ne	Ne	Tastatura
inepro	SCR708	SCR708	Da*1	Da*1	Da*1	Da*1	Da*1	Da*1	Da*1	Tastatura
Y Soft	YU03088001	MU0388	Da	Da	Da	Da	Da	Da	Da	Tastatura
Cardadis	TCM3 Cardadis MiFare Card Reader	ZTCM3-MIFARE	Ne	Ne	Da	Da	Ne	Ne	Da	Tastatura
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Ne	Ne	Da	Da	Ne	Ne	Da	Tastatura

Proizvođač	Model	Model proizvoda	Autorizaciona kartica							Režim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
NT-wa-re	MiCard Multi-Tech4-PI	T4DT-FB4WU F-PI	Da	Da	Da	Da	Da	Da	Da	Tastatura
NT-wa-re	MiCard Plus-2-V2	RDR-80 081AG U-NT2-20	Da*1	Da*1	Da*1	Da*1	Ne	Ne	Ne	Tastatura
NT-wa-re	MiCard V3 Multi	MiCard V3 Multi	Da	Da	Da	Da	Da	Da	Ne	Tastatura

*1 Treba da promenite podešavanja čitača kartice pomoću vlasničkog softvera priloženog od strane proizvođača čitača kartice.

*2 Ako želite da koristite podatke u određenom delu kartice osim standardnog ID-a kartice kao ID za autorizaciju tako što ćete konfigurisati podešavanja proizvoda, obratite se svom partneru ili lokalnom predstavniku kompanije Epson radi detaljnijih informacija o načinu podešavanja proizvoda.

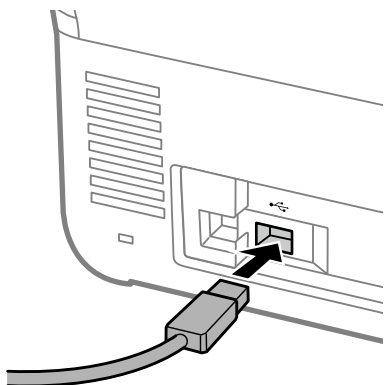
Povezivanje sa uređajem za autorizaciju



Važno:

Kada povežete uređaj za autorizaciju na više skenera, koristite proizvod sa istim brojem modela.

Povežite USB kabl čitača kartica sa USB ulazom spoljnog interfejsa na skeneru.



Provera rada uređaja za autorizaciju

Možete proveriti status povezivanja i prepoznavanje autorizacione kartice za uređaj za autorizaciju sa kontrolne table skenera.

Prikazuje se informacija ako izaberete **Podešavanja > Informacije o uređaju > Status uređaja za proveru identiteta**.

Podešavanja uređaja za autorizaciju

Podesite format čitanja za informacije za autorizaciju primljene sa autorizacione kartice.

Možete podesiti sledeći način čitanja za uređaj za autorizaciju.

- Pročitajte određenu oblast autorizacione kartice, kao što je broj zaposlenog ili lični broj.
- Koristite informacije sa autorizacione kartice osim za UID (informacije sa autorizacione kartice kao što je serijski broj).

Možete da koristite alatku za generisanje operativnih parametara. Obratite se svom dobavljači radi detaljnih informacija.

Napomena:

Upotreba autorizacionih kartica od različitih proizvođača:

Kada koristite UID informacije sa kartice (informacije o broju kartice, kao što je serijski broj), možete koristiti kombinaciju različitih vrsta autorizacionih kartica. To ne može da se kombinuje kada koristite informacije sa druge kartice.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Device Management > Card Reader**.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Administrator Settings > Authentication Settings > Card Reader** iz šablona za konfiguraciju.

Stavka	Objašnjenje
Vendor ID	Podesite ID dobavljača uređaja za autorizaciju koji ograničava upotrebu od 0000 do FFFF koristeći 4 alfanumerička znaka. Ako ne želite da je ograničite, unesite 0000.
Product ID	Podesite ID uređaja za autorizaciju koji ograničava upotrebu od 0000 do FFFF koristeći 4 alfanumerička znaka. Ako ne želite da je ograničite, unesite 0000.
Operational parameter	Podesite radni parametar uređaja za autorizaciju između 0 i 8192 znaka. Dostupni su A~Z, a~z, 0~9, +, /, =, razmak i komandu za prelazak u novi red.
Card Reader	Izaberite format pretvaranje za uređaj za autorizaciju. Možete da proverite detalje formata. Pogledajte link u opisu artikla.
Authentication Card ID save format	Izaberite format pretvaranje za informacije o autorizaciji identifikacione kartice. Možete da proverite detalje formata. Pogledajte link u opisu artikla.
Set card ID range	Omogućite specifikacije za položaj čitanja.
Text Start Position	Odredite početni položaj teksta za čitanje informacija identifikacione kartice. Možete odrediti između 1 i 4096.
Number of Characters	Odredite broj znakova koji se čitaju od početnog položaja informacija identifikacione kartice. Možete odrediti između 1 i 4096.

Registrovanje i podešavanje podataka

Podešavanja

Izvršite potrebna podešavanja u zavisnosti od Authentication Method i metoda skeniranja koji koristite.



Važno:

Pre početka podešavanja, proverite da li je podešavanje vremena za skener tačno.

Ako je podešeno vreme netačno, prikazuje se poruka o grešci „Licenca je istekla“, što može dovesti do neuspelog podešavanja skenera. Takođe, da biste koristili bezbednosne funkcije kao što su SSL/TLS komunikacija ili IPsec, mora se podesiti tačno vreme. Možete podesiti vreme na sledeći način.

Kartica Web Config: **Device Management > Date and Time > Date and Time.**

Kontrolna tabla skenera: **Podešavanja > Osn. podešavanja > Podešavanja za datum/vreme.**

Podešavanje	Local DB	LDAP	Local DB and LDAP
Omogućavanje autorizacije Treba da omogućite autorizaciju pre nego što izvršite podešavanja autorizacije. "Omogućavanje autorizacije" na strani 133	✓	✓	✓
Authentication Settings Podešavanje Authentication Method i kako da proverite identitet korisnika. "Authentication Settings" na strani 133	✓	✓	✓
Registrovanje User Settings Registrujte podešavanja za svakog korisnika. Takođe možete da registrujete korisnike zajedno pomoću CSV datoteke. "Registrovanje User Settings" na strani 134	✓	–	✓
Sinhronizacija s LDAP Server Izvršite sinhronizaciju podešavanja LDAP servera. "Sinhronizacija s LDAP Server" na strani 141	–	✓	✓
Podešavanje Email Server Postavite podešavanja servera e-pošte. Podesite ovo kada koristite funkcije koje zahtevaju podešavanja servera e-pošte, kao što je Scan to My Email. "Podešavanje servera e-pošte" na strani 144	✓	✓	✓
Podešavanje Scan to My Folder Podesite odredišne fascikle. Podesite ovo kada koristite funkciju Scan to My Folder. "Podešavanje režima Scan to My Folder" na strani 145	✓	✓	✓

Podešavanje	Local DB	LDAP	Local DB and LDAP
<p>Customize One-touch Functions</p> <p>Podesite ovo kada menjate stavke prikazane na kontrolnoj tabli skenera. Možete da prikazete samo ikone koje su vam potrebne na kontrolnoj tabli ili promenite redosled ikona.</p> <p>"Customize One-touch Functions" na strani 147</p>	✓	✓	✓

Omogućavanje autorizacije

Treba da omogućite autorizaciju pre nego što izvršite podešavanja autorizacije.

Prilikom podešavanja iz Web Config:

Izaberite **Uključeno (uređaj/LDAP server)** na kartici **Product Security > Basic > Authentication**.

Prilikom podešavanja iz Epson Device Admin:

Na šablonu za konfiguraciju, izaberite **Uključeno (uređaj/LDAP server)** iz **Administrator Settings > Authentication Settings > Basic > Authentication**.

Napomena:

Ako omogućite Authentication Settings na skeneru, Zaključavanje podešavanja je omogućen i za kontrolnu tablu. Kontrolna tabla se ne može otključati kada je omogućen Authentication Settings.

Čak i ako onemogućite Authentication Settings, opcija Zaključavanje podešavanja ostaje omogućena. Ako želite da je onemogućite, možete izvršiti podešavanja sa kontrolne table ili Web Config.

Povezane informacije

- ➔ ["Podešavanje Zaključavanje podešavanja sa kontrolne table" na strani 85](#)
- ➔ ["Podešavanje Zaključavanje podešavanja iz Web Config" na strani 85](#)

Authentication Settings

Podešavanje Authentication Method i kako da proverite identitet korisnika.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Product Security > Authentication Settings**.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Administrator Settings > Authentication Settings > Authentication Settings** iz šablona za konfiguraciju.

Stavka	Objašnjenje
Authentication Method	<p>Izaberite Authentication Method.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Local DB Provera identiteta pomoću User Settings registrovanih na skeneru. Neophodno je da registrujete korisnika na skener. <input type="checkbox"/> LDAP Proverite identitet pomoću informacija o korisniku LDAP servera sinhronizovanih sa skenerom. Morate prethodno da konfigurirate postavke LDAP servera. <input type="checkbox"/> Local DB and LDAP Proverite identitet pomoću informacija o korisniku registrovanih na skener ili LDAP server sinhronizovanih sa skenerom. Morate da registrujete korisnika na skener i podesite LDAP server.
How to Authenticate User	<p>Izaberite kako da proverite identitet korisnika.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Card or User ID and Password Koristite autorizacionu karticu da biste proverili identitet korisnika. Takođe možete da koristite ID korisnika i lozinku za proveru identiteta. <input type="checkbox"/> User ID and Password Koristite ID korisnika i lozinku za proveru identiteta. Kada izaberete ovu funkciju, ne možete da koristite autorizacionu karticu za autorizaciju. <input type="checkbox"/> User ID Koristite samo ID korisnika za autorizaciju. Treba da podesite lozinku. <input type="checkbox"/> Card or ID Number Koristite autorizacionu karticu da biste proverili identitet korisnika. Takođe možete da koristite ID Number. <input type="checkbox"/> ID Number Koristite samo ID broj za proveru identiteta korisnika.
Allow users to register authentication cards	<p>Omogućite ga ako dozvoljavate korisnicima da registruju autorizacionu karticu u sistemu.</p> <p>Ako izaberete LDAP kao Authentication Method, ne možete ga podesiti.</p> <p>Za više informacije o tome kako korisnici mogu da registruju svoje autorizacione kartice, pogledajte „Registrovanje autorizacione kartice“ u <i>Korisnički vodič</i>.</p>
The Minimum Digit Number of ID Number	<p>Izaberite minimalni broj cifara za ID broj.</p>
Caching for LDAP authenticated users	<p>Kada koristite LDAP server za proveru identiteta, možete podesiti da li ćete koristiti keširanje za korisničke informacije.</p>
Use user information in SMTP authentication	<p>Kada koristite ID korisnika i lozinku za autorizaciju, možete podesiti da li ćete koristiti informacije korisnika za SMTP autorizaciju. Sistem koristi poslednji ID korisnika i lozinku koji su bili prijavljeni.</p>
Restrictions for LDAP authenticated users	<p>Ako koristite LDAP, možete da podesite funkcije koje su dostupne za korisnika.</p>

Registrovanje User Settings

Registrujte User Settings koja se koriste za autorizaciju korisnika. Možete registrovati koristeći bilo koji od sledećih načina.

- Registrovanje User Settings jedno po jedno (Web Config)

- Registrovanje više User Settings kao grupe pomoću CSV datoteke (Web Config)
- Registrovanje User Settings na više skenera kao grupe pomoću šablona za konfiguraciju (Epson Device Admin)

Povezane informacije

- ➔ [“Pojedinačno registrovanje User Settings \(Web Config\)” na strani 135](#)
- ➔ [“Registrovanje više User Settings pomoću CSV datoteke \(Web Config\)” na strani 136](#)
- ➔ [“Registrovanje User Settings na više skenera kao grupe \(Epson Device Admin\)” na strani 139](#)

Pojedinačno registrovanje User Settings (Web Config)

Pristupite Web Config i izaberite karticu **Product Security > User Settings > Add**, a zatim unesite User Settings.

Stavka	Objašnjenje
User ID	Unesite korisnički ID koji želite da koristite za autorizaciju u opsegu od 1 do 83 bajta koji se može izraziti u Unicode (UTF-8) formatu. Pošto korisnički ID ne razlikuje velika i mala slova, možete se prijaviti koristeći velika ili mala slova.
User name Display	Unesite korisničko ime prikazano na kontrolnoj tabli skenera koristeći najviše 32 znaka koje se može izraziti u Unicode (UTF-16) formatu. Možete ostaviti prazno.
Password	Unesite lozinku koju želite da koristite za autorizaciju sa najviše 32 znaka u ASCII formatu. U lozinki se razlikuju velika i mala slova. Ostavite prazno ako izaberete User ID za How to Authenticate User .
Authentication Card ID	Unesite ID autorizacione kartice sa 116 znakova u ASCII formatu. Možete ostaviti prazno. Kada odobrite Allow users to register authentication cards za Authentication Settings , preslikava se rezultat registrovan od strane korisnika.
ID Number	Ova stavka se prikazuje kada su Card or ID Number ili ID Number izabrani u Authentication Settings > How to Authenticate User . Unesite broj koji pada negde između broja koji je podešen u Authentication Settings > The Minimum Digit Number of ID Number i do 8 cifara.
Auto Generate	Ova stavka se prikazuje kada su Card or ID Number ili ID Number izabrani u Authentication Settings > How to Authenticate User . Kliknite na automatski generisani ID broj sa istim brojem cifara koji ste izabrali u The Minimum Digit Number of ID Number .
Department	Unesite naziv odeljenja i sve što identifikuje korisnika sa najviše 40 znakova koji se mogu izraziti u Unicode (UTF-16) formatu. Možete ostaviti prazno.
Email Address	Unesite e-adresu korisnika sa 200 znakova u ASCII formatu. Koristi se kao odredište za Scan to My Email . Možete ostaviti prazno.
Scan to My Folder	Podesite da biste pojedinačno sačuvali odredište kada izaberete Individual u Scan to My Folder > Setting Type . Pogledajte sledeće radi detaljnijih informacija o stavkama podešavanja. “Podešavanje režima Scan to My Folder” na strani 145

Stavka	Objašnjenje
Restrictions	Možete da ograničite funkcije za svakog korisnika. Izaberite funkciju koju dozvoljavate da koristite.
Presets	<p>Možete postaviti najviše pet unapred određenih podešavanja koja su dostupna samo izabranom korisniku iz unapred registrovanih Presets.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Presets koja su dodeljena korisniku može da koristi samo korisnik. Presets koja nisu dodeljena nijednom korisniku mogu da koriste svi ostali korisnici. <input type="checkbox"/> Ako korisnik ima dostupna samo jedna Presets, automatski se učitavaju nakon autorizacije. Ako je dostupno više Presets, nakon autorizacije se prikazuje lista Presets. <input type="checkbox"/> Ne možete da kreirate ili prikazete Presets koja koriste funkcije ograničene u Restrictions.

Registrovanje više User Settings pomoću CSV datoteke (Web Config)

Unesite podešavanja za svakog korisnika u CSV datoteku i registrujte ih kao grupu.

Kreiranje CSV datoteke

Kreirajte CSV datoteku za uvoz User Settings.

Napomena:

Ako unapred registrujete jedno ili više User Settings, a zatim izvozite formatiranu datoteku (CSV datoteku), možete da koristite registrovana podešavanja kao referencu za unos stavki podešavanja.

1. Pristupite Web Config i izaberite karticu **Product Security > User Settings**.
2. Kliknite na **Export**.
3. Izaberite format datoteke za **File Format**.

Izaberite na osnovu sledećeg uputstva.

Stavka	Objašnjenje
CSV UTF-16 (Tab delimited)	<p>Izaberite kada uređujete datoteku pomoću Microsoft Excel.</p> <p>Svaki parametar je zatvoren sa „[]” (zagradama). Unesite parametre u „[]”.</p> <p>Kada ažurirate datoteke, preporučujemo da zamenite datoteku. Ako ste nedavno sačuvali datoteku, izaberite Unicode tekst (*.txt) za format datoteke.</p>
CSV UTF-8 (Comma delimited)	<p>Izaberite kada želite da uredite datoteku pomoću uređivača teksta ili makro naredbe bez Microsoft Excel.</p>
CSV UTF-8 (Semicolon delimited)	

4. Kliknite na **Export**.

5. Uredite i sačuvajte ovu CSV datoteku u aplikaciji za rad s tabelama kao što je Microsoft Excel ili u uređivaču teksta.



Važno:

Kada uređujete datoteku, nemojte menjati šifrovanje i podatke u zaglavlju.

Stavke za podešavanje CSV datoteke

Stavka	Podešavanja i objašnjenje
UserID	Unesite korisnički ID da biste koristili autorizaciju između 1 i 83 bajta u Unicode.
UserName	Unesite korisničko ime prikazano na kontrolnoj tabli skenera koristeći najviše 32 znaka u Unicode formatu. Možete ostaviti prazno.
Password	Unesite lozinku za autorizaciju sa najviše 32 znaka u ASCII formatu. Kada uvozite, podešena je kao lozinka umesto EncPassword . Ostavite prazno ako izaberete User ID za How to Authenticate User . Kada izvozite, uvek je prazno.
AuthenticationCardID	Podesite rezultate očitavanja autorizacione kartice. Kada odobrite Allow users to register authentication cards u Authentication Settings , preslikava se rezultat registrovan od strane korisnika. Unesite najviše 116 znakova u ASCII formatu. Možete ostaviti prazno.
IDNumber	Ova stavka se prikazuje kada su Card or ID Number ili ID Number izabrani u Authentication Settings > How to Authenticate User . Unesite broj koji pada negde između broja koji je podešen u Authentication Settings > The Minimum Digit Number of ID Number i do 8 cifara. ID broj ne možete duplirati. Ako je dupliran, bićete upozoreni na grešku prilikom uvoza datoteke. Kada se ostavi prazno, automatski mu se dodeljuje broj.
Department	Proizvoljno unesite naziv odeljenja da biste razlikovali korisnike. Unesite najviše 40 znakova u Unicode formatu. Možete ostaviti prazno.
MailAddress	Postavite adresu e pošte za korisnike. Koristi se kao odredište za Scan to My Email . Možete da koristite A-Z, a-z, 0-9, !#%&'*+-. /=?^_{}~@. Unesite najviše 200 znakova. Ne možete da upotrebite „,“ (zarez) kao prvi znak. Možete ostaviti prazno.
FolderProtocol	Podesite tip funkcije Scan to My Folder. Mrežna fascikla/FTP (SMB): 0 FTP: 1
FolderPath	Postavite odredište za čuvanje za funkciju Scan to My Folder.
FolderUserName	Postavite korisničko ime za funkciju Scan to My Folder.
FolderPassword	Postavite lozinku da biste potvrdili autentičnost odredišne fascikle za funkciju Scan to My Folder koristeći najviše 32 ASCII znaka. Kada uvozite, podešena je kao lozinka umesto EncPassword . Kada izvozite, uvek je prazno.
FtpPassive	Podesite dugme za režim povezivanja za FTP server kada je FTP izabran kao Type za funkciju Scan to My Folder. Aktivni režim: 0, Pasivni režim: 1

Stavka	Podešavanja i objašnjenje
FtpPort	Podesite broj ulaza za slanje skeniranih podataka za FTP server od 0 do 65535, kada je izabran FTP kao Type za funkciju Scan to My Folder.
ScanToMemory	Podesite ograničenja za Scan to USB Drive. Nije dozvoljeno: 0, Dozvoljeno: 1
ScanToMail	Podesite ograničenja za Scan to Email. Možete podesiti Skeniraj u moj imejl samo kada je omogućena opcija Scan to Email . Nije dozvoljeno: 0, Dozvoljeno: 1
ScanToFolder	Podesite ograničenja za Scan to Network Folder/FTP. Možete podesiti Skeniraj u moju fasciklu samo kada je omogućena opcija Scan to Network Folder/FTP . Nije dozvoljeno: 0, Dozvoljeno: 1
ScanToCloud	Podesite ograničenja za Scan to Cloud. Nije dozvoljeno: 0, Dozvoljeno: 1
ScanToComputer	Podesite ograničenja za Skeniraj na računar. Nije dozvoljeno: 0, Dozvoljeno: 1
PresetIndex	Podesite Presets koja želite da povežete sa korisnikom. Možete da postavite najviše pet Presets registrovanih brojeva razdvojenih zarezima.
EncPassword	Kada izvozite korisničke postavke, parametar podešen za Password je šifrovan, onda je vrednost šifrovana pomoću BASE64 i izlazom. Kada uvozite uz novu lozinku za Password , ova vrednost se ignoriše. Ako je Password prazna, koristi se ova vrednost a lozinka ostaje ista kao i pre izvoza.
EncFolderPassword	Kada izvozite, parametar podešen za FolderPassword je šifrovan, onda je vrednost šifrovana pomoću BASE64 i izlazom. Kada uvozite uz novu lozinku za FolderPassword , ova vrednost se ignoriše. Ako je FolderPassword prazna, koristi se ova vrednost a lozinka ostaje ista kao i pre izvoza.

Uvoz CSV datoteke

1. Pristupite Web Config i izaberite karticu **Product Security** > **User Settings**.
2. Kliknite na **Import**.
3. Izaberite datoteku koju želite da uvezete.
4. Kliknite na **Import**.
5. Nakon provere prikazanih podataka, kliknite na **OK**.

Registrovanje User Settings na više skenera kao grupe (Epson Device Admin)

Možete da registrujete User Settings koja se koriste u Local DB kao grupu pomoću LDAP servera ili CSV/ENE datoteke.

Napomena:

ENE datoteka je binarna datoteka koju pruža kompanija Epson a koja šifrjuje i čuva podatke za **Contacts** kao što su lični podaci User Settings. Može se izvesti iz Epson Device Admin i možete podesiti lozinku. Korisno je kada želite da uvezete User Settings iz rezervne kopije.

Uvoz iz CSV/ENE datoteke

1. Izaberite **Administrator Settings > Authentication Settings > User Settings** iz šablona za konfiguraciju.
2. Kliknite na **Import**.
3. Izaberite **CSV or ENE File** iz **Import Source**.
4. Kliknite na **Browse**.
Prikazuje se ekran za izbor datoteke.
5. Izaberite datoteku koju želite da uvezete da biste je otvorili.
6. Izaberite način uvoza.
 - Overwrite and Add:** zamenjuje ako postoji isti korisnički ID, dodaje novi ID ako ne postoji.
 - Replace All:** zamenjuje sve sa korisničkim podešavanjima koje želite da uvezete.
7. Kliknite na **Import**.
Prikazaće se ekran za potvrdu podešavanja.
8. Kliknite na **OK**.
Prikazuje se rezultat provere validacije.
Napomena:
 - Ako broj uvezenih korisničkih podešavanja premašuje broj koji se može uvesti, pojaviće se poruka da izbrišete neka korisnička podešavanja. Pre uvoza izbrišite sva dodatna korisnička podešavanja.*
 - Izaberite korisnička podešavanja koja želite da izbrišete pre uvoza, a zatim kliknite na **Delete**.*
9. Kliknite na **Import**.
Korisnička podešavanja se uvoze u šablon za konfiguraciju.

Uvoz iz LDAP servera

1. Izaberite **Administrator Settings > Authentication Settings > User Settings** iz šablona za konfiguraciju.
2. Kliknite na **Import**.
3. Izaberite **LDAP** iz **Import Source**.

4. Kliknite na **Settings**.

Prikazuju se podešavanja **LDAP Server**.

Napomena:

Ovo podešavanje LDAP servera je za uvoz korisničkih podešavanja sa LDAP servera. Uvezena (kopirana) korisnička podešavanja se koriste za proveru identiteta korisnika pomoću samog skenera.

*S druge strane, kada izaberete **LDAP** ili **Local DB and LDAP** kao metod autorizacije, identitet korisnika se proverava pomoću LDAP servera.*

5. Podesite svaku stavku.

Kada uvozite korisničke postavke sa LDAP servera, možete unapred da konfigurirate sledeća podešavanja pored LDAP podešavanja.

Ostale stavke potražite u povezanim informacijama.

Stavka		Objašnjenje	
LDAP Server Settings	LDAP Server Type	Omogućava vam da izaberete tip LDAP servera.	
Search Settings	Search Filter	Možete podesiti tekst koji se koristi za LDAP filter za pretragu. Izaberite Custom da izmenite tekst za pretragu.	
	Options	Type	Možete da podesite tip odredišta za čuvanje za Scan To My Folder .
	Connection Mode	Kada je podešen Type na FTP , možete da podesite režim FTP veze.	
	Port Number	Kada je podešen Type na FTP , možete podesiti broj ulaza koji želite da koristite.	

6. Po potrebi izvršite proveru veze klikom na **Connection Test**.

Pribavlja i prikazuje 10 korisničkih podešavanja sa LDAP servera.

7. Kliknite na **OK**.

8. Izaberite način uvoza.

Overwrite and Add: zamenjuje ako postoji isti korisnički ID, dodaje novi ID ako ne postoji.

Replace All: zamenjuje sve sa korisničkim podešavanjima koje želite da uvezete.

9. Kliknite na **Import**.

Prikazaće se ekran za potvrdu podešavanja.

10. Kliknite na **OK**.

Prikazuje se rezultat provere validacije.

11. Kliknite na **Import**.

Korisnička podešavanja se uvoze u šablon za konfiguraciju.

Povezane informacije

➔ [“Konfigurisanje LDAP servera” na strani 141](#)

➔ “Konfiguracija podešavanja pretraživanja preko LDAP servera” na strani 142

Sinhronizacija s LDAP Server

Izvršite LDAP Server podešavanja za skener.

Po potrebi izvršite podešavanja za primarni i sekundarni server.

Napomena:

Podešavanja za LDAP Server su zajednička sa **Contacts**.

Dostupne usluge

Podržane su sledeće usluge direktorijuma.

Naziv usluge	Verzija
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Konfigurisanje LDAP servera

Da biste koristili LDAP server, prvo treba da konfigurirate LDAP server.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Network > LDAP Server > Basic (Primary Server)** ili **Basic (Secondary Server)**.

Ako izaberete **Kerberos Authentication** kao **Authentication Method**, izaberite **Network > Kerberos Settings** da biste izvršili podešavanja za Kerberos.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Network > LDAP server > Server Settings (Primary Server)** ili **Server Settings (Secondary Server)** iz šablona za konfiguraciju.

Ako izaberete **Kerberos Authentication** kao **Authentication Method**, izaberite **Network — Security > Kerberos Settings** da biste izvršili podešavanja za Kerberos.

Stavka	Podešavanja i objašnjenje
Use LDAP Server	Izaberite Use ili Do Not Use .
LDAP Server Address	Unesite adresu LDAP servera. Unesite između 1 i 255 znakova u formatu IPv4, IPv6 ili FQDN. Za FQDN format možete koristiti alfanumeričke znakove u ASCII (0x20–0x7E) i crtice, osim na početku ili na kraju adrese.
LDAP server Port Number (Port number)	Unesite broj ulaza LDAP servera od 1 do 65535.
Secure Connection	Navedite metod autorizacije koji će se koristiti kada skener pristupa LDAP serveru.
Certificate Validation	Sertifikat LDAP servera se potvrđuje kada se ovo omogući. Preporučujemo da se ovo podesi na Enable . Da biste podesili, CA Certificate treba da se uveze na skener.

Stavka	Podešavanja i objašnjenje
Search Timeout (sec)	Podesite vreme trajanja pre nego što dođe do prekida u toku pretrage od 5 do 300 sekundi.
Authentication Method	Izaberite metod autorizacije. Ako izaberete Kerberos Authentication , unapred izvršite podešavanja za Kerberos. Da biste izvršili Kerberos Authentication, potrebno je sledeće okruženje. <input type="checkbox"/> Skener i DNS server mogu da komuniciraju. <input type="checkbox"/> Sinhronizuje se vreme skenera, KDC servera i servera koji je potreban za autorizaciju (LDAP server, SMTP server, server za datoteku). <input type="checkbox"/> Kada se radni server dodeli kao IP adresa, FQDN radnog servera se registruje na zonu povratnog pretraživanja DNS servera.
Kerberos Realm to be Used	Ako izaberete Kerberos Authentication za Authentication Method , unesite Kerberos domen koji želite da koristite.
Administrator DN / User Name	Unesite korisničko ime za LDAP server u dužini od najviše 128 znakova u Unicode formatu (UTF-8). Nije moguće uneti kontrolne znakove, npr. 0x00 do 0x1F i 0X7F. Ova podešavanja se ne koriste kada je Anonymous Authentication izabrano kao Authentication Method . Ako želite da odredite, ostavite prazno.
Password	Unesite korisničko ime za autorizaciju LDAP servera u dužini od najviše 128 znakova u Unicode formatu (UTF-8). Nije moguće uneti kontrolne znakove, npr. 0x00 do 0x1F i 0X7F. Ova podešavanja se ne koriste kada je Anonymous Authentication izabrano kao Authentication Method . Ako želite da odredite, ostavite prazno.

Podešavanja Kerberos protokola

Ako izaberete **Kerberos Authentication** kao **Authentication Method**, potrebno je da izvršite podešavanja za Kerberos. Možete registrovati najviše 10 podešavanja za Kerberos.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Network > Kerberos Settings**.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Network > Security > Kerberos Settings** iz šablona za konfiguraciju.

Stavka	Podešavanja i objašnjenje
Realm (Domain)	Unesite područje Kerberos autorizacije u dužini do 255 znakova u formatu ASCII (0x20–0x7E). Ako želite da registrujete, ostavite prazno.
KDC Address	Unesite adresu Kerberos servera za autorizaciju. Unesite do 255 znakova u formatu IPv4, IPv6 ili FQDN. Ako želite da registrujete, ostavite prazno.
Port Number (Kerberos)	Unesite broj priključka Kerberos servera između 1 i 65535.

Konfiguracija podešavanja pretraživanja preko LDAP servera

Postavlja attribute pretrage za korisnička podešavanja.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Network > LDAP Server > Search Settings (Authentication)**.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Administrator Settings > Authentication Settings > LDAP server > Search Settings (Authentication)** iz šablona za konfiguraciju.

Stavka	Podešavanja i objašnjenje
Search Base (Distinguished Name)	Odredite početnu poziciju kada tražite korisničke informacije sa LDAP servera. Unesite između 0 i 128 znakova u formatu Unicode (UTF-8). Ako ne tražite proizvoljno svojstvo, ostavite ovo prazno. Primeri direktorijuma lokalnog servera: dc=server,dc=local
User ID Attribute	Odredite naziv svojstva koje ćete prikazati kada se traži ID broj. Unesite između 1 i 255 znakova u formatu ASCII. Prvi znak mora da bude a-z ili A-Z. Primer: cn, uid
User name Display Attribute	Odredite naziv svojstva koje ćete prikazati kao korisničko ime. Unesite između 0 i 255 znakova u formatu ASCII. Prvi znak mora da bude a-z ili A-Z. Nemojte popunjavati ovo polje. Primer: cn, name
Authentication Card ID Attribute	Odredite naziv svojstva koje ćete prikazati kao ID autorizacione kartice. Unesite između 0 i 255 znakova u formatu ASCII. Prvi znak mora da bude a-z ili A-Z. Nemojte popunjavati ovo polje. Primer: cn, sn
ID Number Attribute	Odredite naziv svojstva koje ćete prikazati kada se traži ID broj. Unesite između 1 i 255 znakova u formatu ASCII. Prvi znak mora da bude a-z ili A-Z. Primer: cn, id
Department Attribute	Odredite naziv svojstva koje ćete prikazati kao naziv odeljenja. Unesite između 0 i 255 znakova u formatu ASCII. Prvi znak mora da bude a-z ili A-Z. Nemojte popunjavati ovo polje. Primer: ou, ou-cl
Email Address Attribute	Odredite naziv svojstva koje ćete prikazati kada se traže e-adrese. Unesite između 1 i 255 znakova u formatu ASCII. Prvi znak mora da bude a-z ili A-Z. Primer: mail
Save To Attribute	Odredite naziv svojstva koji ukazuje na odredište za Scan To My Folder. Unesite između 0 i 255 znakova u formatu ASCII. Na primer: homeDirectory

Provera veze sa LDAP serverom

Vrši proveru veze sa LDAP serverom uz pomoć parametra podešenog na **LDAP Server > Search Settings**.

1. Pristupite Web Config i izaberite karticu **Network > LDAP Server > Connection Test**.
2. Izaberite **Start**.
Test veze se pokreće. Nakon testa, prikazuje se izveštaj o proveru.

Reference testiranja veze sa LDAP serverom

Poruke	Objašnjenje
Connection test was successful.	Ova poruka se prikazuje kada je veza sa serverom uspešna.
Connection test failed. Check the settings.	Ova poruka se prikazuje iz sledećih razloga: <ul style="list-style-type: none"> <input type="checkbox"/> Adresa LDAP servera ili broj porta nije tačan. <input type="checkbox"/> Došlo je do prekida. <input type="checkbox"/> Do Not Use je izabrano kao Use LDAP Server. <input type="checkbox"/> Ako je Kerberos Authentication izabrano kao Authentication Method, podešavanja kao Realm (Domain), KDC Address i Port Number (Kerberos) su neispravna.
Connection test failed. Check the date and time on your product or server.	Ova poruka se pojavljuje kada se veza ne ostvari jer nije podešeno isto vreme za skener i za LDAP server.
Authentication failed. Check the settings.	Ova poruka se prikazuje iz sledećih razloga: <ul style="list-style-type: none"> <input type="checkbox"/> User Name i/ili Password su neispravni. <input type="checkbox"/> Ako je izabrano Kerberos Authentication kao Authentication Method, vreme/datum se možda neće konfigurisati.
Cannot access the product until processing is complete.	Ova poruka se prikazuje kada je skener zauzet.

Podešavanje servera e-pošte

Kada koristite **Scan to My Email**, podesite server e-pošte.

Napomena:

Možete podesiti **Scan to My Email** samo kada je omogućena opcija **Scan to Email**.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Network > Email Server > Basic**.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Common > Email Server > Mail Server Settings** iz šablona za konfiguraciju.

Stavka	Podešavanja i objašnjenje	
Authentication Method	Navedite metod autorizacije koji će se koristiti kada skener pristupa serveru za poštu.	
	Off	Autorizacija je onemogućena prilikom komunikacije sa serverom za poštu.
	SMTP AUTH	Server za e-poštu treba da podržava SMTP autorizaciju.
	POP before SMTP	Kada izaberete ovu stavku, podesite POP3 server.
Authenticated Account	Ako izaberete SMTP AUTH ili POP before SMTP kao Authentication Method , unesite naziv naloga za autorizaciju. Unesite između 0 i 255 znakova u formatu ASCII (0x20–0x7E).	
Authenticated Password	Ako izaberete SMTP AUTH ili POP before SMTP kao Authentication Method , unesite potvrđenu lozinku. Unesite između 0 i 20 znakova u formatu ASCII (0x20–0x7E).	

Stavka	Podešavanja i objašnjenje	
Sender's Email Address	Unesite adresu e-pošte pošiljaoca. Unesite od 0 do 255 alfanumeričkih znakova u formatu ASCII (0x20–0x7E), osim : () < > [] ; ¥. Tačka („.") ne može da se nalazi na početnoj poziciji.	
SMTP Server Address	Unesite između 0 i 255 znakova koristeći znakove A–Z a–z 0–9 . - . Možete da koristite format IPv4 ili FQDN.	
SMTP Server Port Number	Unesite broj između 1 i 65535.	
Secure Connection	Navedite metod bezbedne veze za server e-pošte.	
	None	Ako izaberete POP before SMTP u Authentication Method , metod povezivanja će biti podešen na None .
	SSL/TLS	Ovo je dostupno kada je Authentication Method podešen na Off ili SMTP AUTH .
	STARTTLS	Ovo je dostupno kada je Authentication Method podešen na Off ili SMTP AUTH .
Certificate Validation	Sertifikat se potvrđuje kada se ovo omogući. Preporučujemo da se ovo podesi na Enable .	
POP3 Server Address	Ako izaberete POP before SMTP kao Authentication Method , unesite adresu POP3 servera. Možete da unesete između 0 i 255 znakova koristeći znakove A–Z a–z 0–9. Možete da koristite format IPv4 ili FQDN.	
POP3 Server Port Number	Ako izaberete POP before SMTP kao Authentication Method , odredite broj ulaza. Unesite broj između 1 i 65535.	

Podešavanje režima Scan to My Folder

Čuvaju se skenirane slike u fascikl dodeljenoj svakom korisniku. Možete postaviti sledeće kao dodeljenu fasciklu.

Napomena:

Možete podesiti *Scan To My Folder* samo kada je omogućena opcija *Scan to Network Folder/FTP*.

Podešavanje Sačuvaj na računaru	Authentication Method	Lokacija podešavanja putanje do fascikle
Navedite jednu mrežnu fasciklu za sve Authentication Settings da biste automatski kreirali ličnu fasciklu ispod navedene fascikle koristeći ime korisničkog ID-a.	<input type="checkbox"/> Local DB <input type="checkbox"/> LDAP <input type="checkbox"/> Local DB and LDAP	Skener (podešavanje Scan to My Folder)
Svakom korisniku pojedinačno dodelite različite mrežne fascikle.	Local DB	Skener (User Settings)
	LDAP	LDAP svojstva
	Local DB and LDAP	Skener (User Settings) ili LDAP svojstva

Prilikom podešavanja iz Web Config:

Izaberite karticu **Product Security** > **Scan to Network Folder/FTP**.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Administrator Settings** > **Authentication Settings** > **Scan to Network Folder/FTP** > **Scan to My Folder** iz šablona za konfiguraciju.

Stavka		Objašnjenje
Save To Setting	Setting Type	<input type="checkbox"/> Shared: Automatski kreira fasciklu nazvanu prema ID-u korisnika ispod putanje fascikle ili URL adrese navedene u Save to , i čuva skenirane slike u ovoj fascikli. <input type="checkbox"/> Individual: Podesite odredište za čuvanje rezultata skeniranja za svakog korisnika. Local DB korisnici se mogu podesiti u korisničkim podešavanjima. LDAP korisnici koriste lokaciju za skladištenje dobijenu iz svojstva pretrage LDAP servera.
	Type	Izaberite protokol prenosa u skladu sa izlaznim odredištem skeniranja. Za mrežnu fasciklu: Network Folder (SMB) Za FTP server: FTP
	Save to	Navedite putanju ili URL izlazne putanje. Unesite najviše 160 znakova u formatu Unicode (UTF-16).
	Connection Mode	Podesite kada izaberete FTP u Type . Izaberite režim povezivanja na FTP server.
	Port Number	Podesite kada izaberete FTP u Type . Unesite broj ulaza da biste poslali skenirane podatke na FTP server između 0 i 65535.
Authentication Settings	Setting Type	Podesite kada izaberete Individual kao Setting Type u Save To Setting . Podesite „User Name“ i „Password“ da biste pristupili fascikli. <input type="checkbox"/> Shared: Koristite zajedničko User Name i Password za sve korisnike. <input type="checkbox"/> Individual: Za korisnike Local DB, podesite User Name i Password pojedinačno u Korisničke postavke . LDAP korisnici se nemogu pojedinačno konfigurirati. User Name i Password postavljeni ovom stavkom se koriste kao grupa.
	User Name	Unesite korisničko ime da biste pristupili izlaznoj odredišnoj fascikli skeniranja. Unesite najviše 30 znakova u formatu Unicode (UTF-16). Podesite ovo kada koristite Shared ili LDAP server.
	Password	Unesite lozinku koja odgovara User Name . Unesite najviše 20 znakova u formatu Unicode (UTF-16). Podesite ovo kada koristite Shared ili LDAP server.

Zabranite promenu odredišta za Scan to Network Folder/FTP

Stavka	Objašnjenje
Prohibit manual entry of destination	Kada je omogućeno, korisnik ne može da promeni podrazumevano odredište.

Customize One-touch Functions

Možete da prikazete samo neophodne ikone tako što ćete urediti raspored ikona prikazanih na početnom ekranu kontrolne table.

Prilikom podešavanja iz Web Config:

Izaberite karticu **Product Security > Customize One-touch Functions**.

Prilikom podešavanja iz Epson Device Admin:

Izaberite **Administrator Settings > Authentication Settings > Customize One-touch Functions** iz šablona za konfiguraciju.

Napomena:

U sledećim slučajevima ikone za određenu funkciju nisu prikazane na početnom ekranu.

- Kada izaberete funkcije koje nisu dozvoljene zbog **Restrictions**.*
- Kada adresa e-pošte za prijavljenog korisnika nije registrovana. (Scan to My Email)*
- Kada nije podešena određena fascikla. (Scan to My Folder)*

Stavka	Objašnjenje
Maximum functions per screen	Izaberite raspored ikona prikazanih na kontrolnoj tabli. Slika se menja prema izabranom rasporedu.
Screen(s)	Izaberite broj stranica.
Number	Izaberite funkcije koje želite da prikazete za svako numerisano mesto.

Izveštaji Job History pomoću Epson Device Admin

Možete da kreirate izveštaj Job History za svakog korisnika pomoću Epson Device Admin. Možete sačuvati najviše 3000 primeraka istorije upotrebe skenera. Izveštaj možete kreirati tako što ćete navesti period ili postaviti redovan raspored.

Da biste izvezli Job History kao izveštaj, izaberite **Options > Epson Print Admin Serverless/Authentication Settings > Manage the Epson Print Admin Serverless/Authentication compatible devices** iz trakastog menija na ekranu liste uređaja.

Radi detaljnijih informacija kako da kreirate izveštaj o korisniku pogledajte dokumentaciju ili pomoć za Epson Device Admin.


Stavke koje se mogu obuhvatiti izveštajem

U izveštaju o korisniku možete izneti sledeće stavke.

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

Prijavite se kao administrator sa kontrolne table štampača

Možete koristiti bilo koji od sledećih metoda da se prijavite kao administrator sa kontrolne table skenera.

1. Dodirnite  u gornjem desnom delu ekrana.
 - Kada su omogućene Authentication Settings, prikazuje se ikona na ekranu **Dobro došli** (ekran pripravnosti za autorizaciju).
 - Kada je omogućeno Authentication Settings, prikazuje se ikona na početnom ekranu.
2. Dodirnite **Da** kada se prikaže ekran za potvrdu.
3. Unesite lozinku za administratora.
Prikazuje se poruka o završetku prijave, a zatim se prikazuje početni ekran na kontrolnoj tabli.

Da biste se prijavili, dodirnite  u gornjem desnom delu ekrana.

Onemogućavanje Authentication Settings

Možete da onemogućite Authentication Settings pomoću Web Config.

Napomena:

User Settings registrovana na skeneru biće sačuvana iako su onemogućena Authentication Settings. Možete ih ukloniti vraćanjem skenera na podrazumevana podešavanja.

1. Otvorite Web Config.
2. Izaberite karticu **Product Security > Basic > Authentication**.
3. Izaberite **OFF**.
4. Kliknite na **Next**.
5. Kliknite na **OK**.

Napomena:

Čak i ako onemogućite Authentication Settings, opcija Zaključavanje podešavanja ostaje omogućena. Ako želite da je onemogućite, možete izvršiti podešavanja sa kontrolne table ili Web Config.

Povezane informacije

- ➔ [“Podešavanje Zaključavanje podešavanja sa kontrolne table” na strani 85](#)
- ➔ [“Podešavanje Zaključavanje podešavanja iz Web Config” na strani 85](#)

Brisanje Authentication Settings informacija (Vrati podrazumevane postavke)

Da biste izbrisali Authentication Settings podatke (Card Reader, Authentication Method, User Settings, i tako dalje), vratite sva podešavanja skenera na podrazumevana podešavanja u trenutku kupovine.

Izaberite **Podešavanja > Administracija sistema > Vrati podrazumevane postavke > Sve postavke** na kontrolnoj tabli.



Važno:

Svi kontakti i ostala mrežna podešavanja će biti izbrisana. Izbrisana podešavanja ne mogu da se vrate.

Rešavanje problema

Ne možete da očitajte autorizacionu karticu

Proverite sledeće.

- Proverite da li je uređaj za autorizaciju pravilno povezan na skener.
Povežite uređaj za autorizaciju na USB priključak spoljnog interfejsa sa zadnje strane skenera.
- Proverite da li su podržani uređaj za autorizaciju i autorizaciona kartica.

Održavanje

Čišćenje spoljašnjosti skenera.	151
Čišćenje unutrašnjosti skenera.	151
Zamena sklopa valjaka.	156
Resetovanje broja skeniranja.	161
Ušteda energije.	161
Transportovanje skenera.	162
Pravljenje rezervne kopije podešavanja.	163
Vrati podrazumevane postavke.	164
Ažuriranje aplikacija i upravljačkog softvera.	165


Čišćenje spoljašnjosti skenera

Obrišite mrlje na spoljašnjem kućištu pomoću suve krpe ili krpe navlažene rastvorom blagog deterdženta i vode.



Važno:

- Nikada ne koristite alkohol, razređivač ili korozivan rastvor za čišćenje skenera. Može doći do izobličenja ili promene boje.*
- Nemojte dozvoliti da voda uđe u proizvod. To može dovesti do neispravnog rada.*
- Ni u kom slučaju ne otvarajte kućište skenera.*

1. Pritisnite dugme  da biste isključili skener.
2. Isključite adapter naizmjenične struje iz skenera.
3. Očistite spoljni deo kućišta krpom navlaženom rastvorom blagog deterdženta i vode.

Napomena:

Ekran osetljiv na dodir obrišite mekom, suvom krpom.

Čišćenje unutrašnjosti skenera

Nakon što se skener koristi izvesno vreme, papir i sobna prašina na valjku ili staklenom delu unutar skenera mogu izazvati probleme sa uvlačenjem papira ili kvalitetom slike. Očistite unutrašnjost skenera nakon svakih 5,000 skeniranja.


Najnoviji broj skeniranja možete proveriti na kontrolnoj tabli ili u uslužnom programu Epson Scan 2 Utility.

Ako je površina zamrljana supstancom koja se teško uklanja, za uklanjanje mrlja upotrebite originalni Epsonov pribor za čišćenje. Koristite malu količinu sredstva za čišćenje nanesenog na krpom za čišćenje da biste uklonili mrlje.

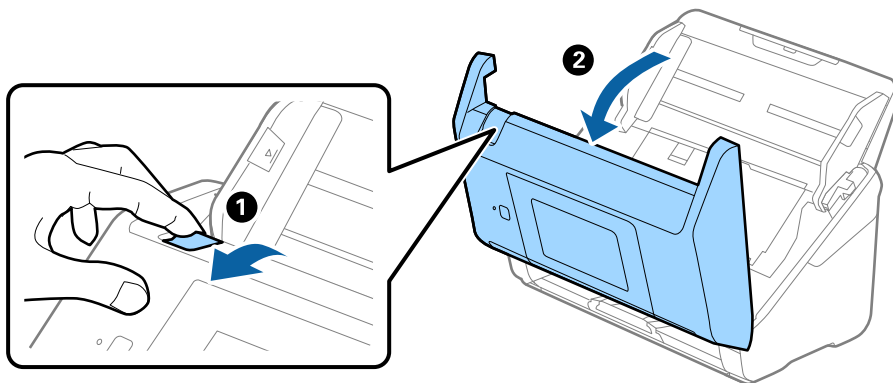


Važno:

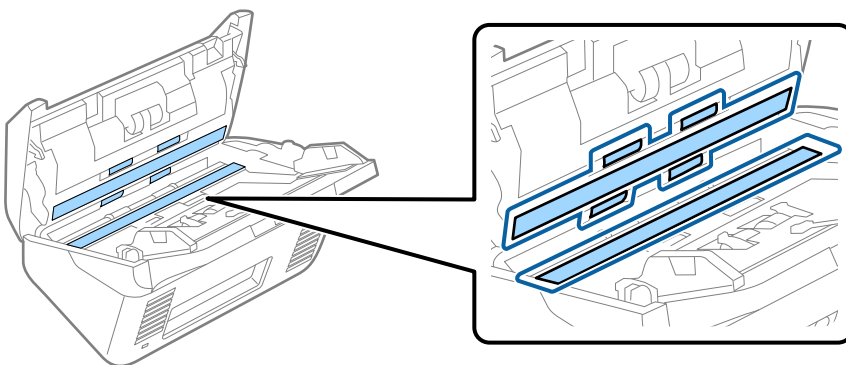
- Nikada ne koristite alkohol, razređivač ili korozivan rastvor za čišćenje skenera. Može doći do izobličenja ili promene boje.*
- Nikada ne prskajte bilo kakvu tečnost ili mazivo na skener. Oštećenje opreme ili kola može dovesti do nepravilnog rada.*
- Ni u kom slučaju ne otvarajte kućište skenera.*

1. Pritisnite dugme  da biste isključili skener.
2. Isključite adapter naizmjenične struje iz skenera.

3. Povucite polugu i otvorite poklopac skenera.



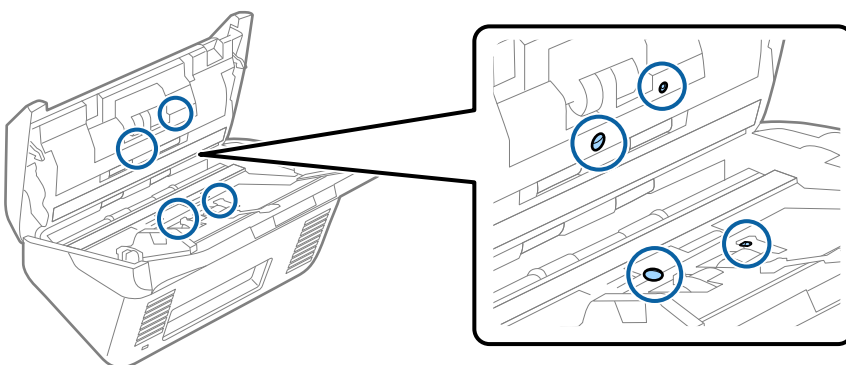
4. Obrišite mrlje na plastičnom valjku i staklenoj površini na dnu unutar poklopca skenera pomoću meke krpe ili originalnog Epsonovog pribora za čišćenje.



Važno:

- Nemojte previše pritiskati površinu stakla skenera.
- Nemojte koristiti četku ili tvrd alat. Sve ogrebotine na staklu mogu uticati na kvalitet skeniranja.
- Nemojte raspršivati sredstvo za čišćenje direktno na površinu stakla skenera.

5. Obrišite sve mrlje na sensorima pomoću pamučnog brisača.

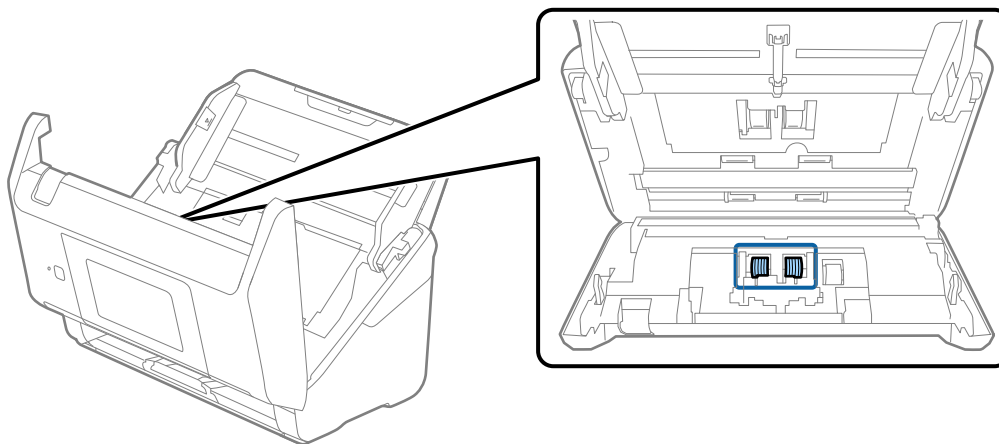




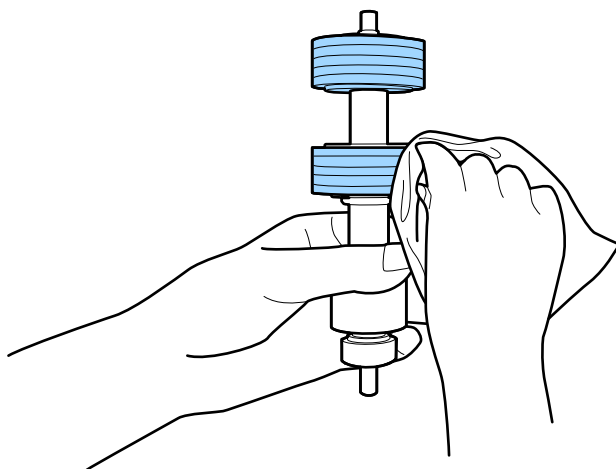
Važno:

Nemojte koristiti tečnost poput sredstva za čišćenje na pamučnom brisaču.

6. Otvorite poklopac i zatim izvadite valjak za razdvajanje.
Pogledajte „Zamenu sklopa valjaka” radi detaljnijih podataka.



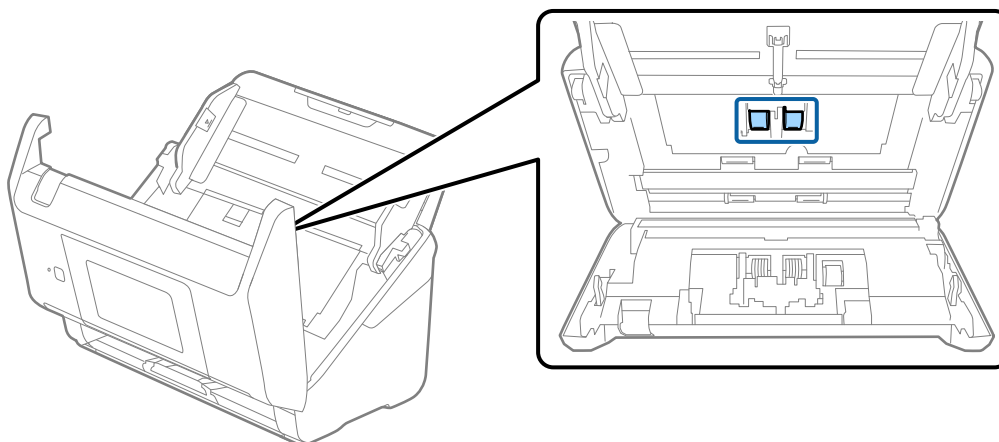
7. Obrišite prašinu ili nečistoće na valjku za razdvajanje pomoću originalnog Epsonovog pribora za čišćenje ili meke, vlažne krpe.



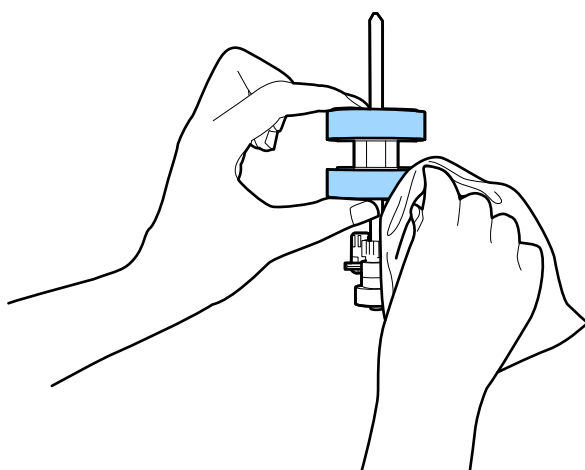
Važno:

Za čišćenje valjka koristite samo originalan Epsonov pribor za čišćenje ili meku, vlažnu krpku. Upotreba suve krpe može oštetiti površinu valjka.

8. Otvorite poklopac i zatim izvadite prijemni valjak.
Pogledajte „Zamenu sklopa valjaka” radi detaljnijih podataka.



9. Obrišite prašinu ili nečistoće na prijemnom valjku pomoću originalnog Epsonovog pribora za čišćenje ili meke, vlažne krpe.

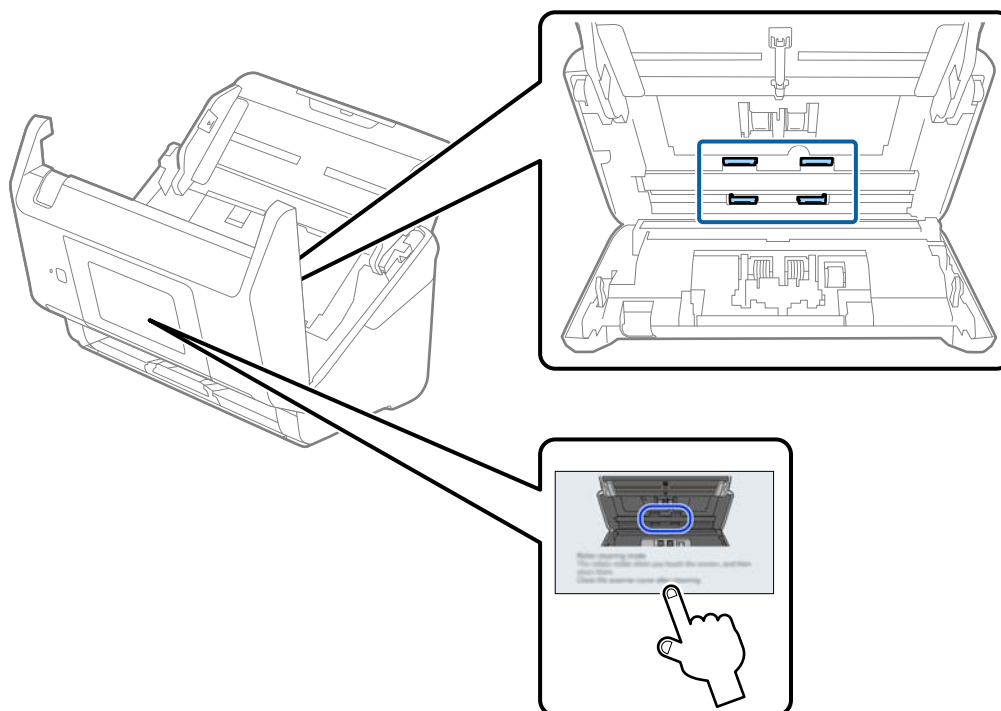


Važno:

Za čišćenje valjka koristite samo originalan Epsonov pribor za čišćenje ili meku, vlažnu krpu. Upotreba suve krpe može oštetiti površinu valjka.

10. Zatvorite poklopac skenera.
11. Uključite adapter naizmjenične struje i uključite skener.
12. Na početnom ekranu izaberite **Održavanje skenera**.
13. Na ekranu **Održavanje skenera** izaberite **Čišćenje valjka**.
14. Povucite polugu da otvorite poklopac skenera.
Skener ulazi u režim čišćenja valjaka.

- Polako okrećite valjke na dnu dodirivanjem bilo gde po LCD ekranu. Obrisite površinu valjaka pomoću originalnog Epsonovog pribora za čišćenje ili meke krpe navlažene vodom. Ponavljajte ovaj postupak dok valjci ne budu čisti.



Oprez:

Vodite računa da mehanizam ne zahvati vaše ruke ili kosu kada pokrećete valjak. To može dovesti do povreda.

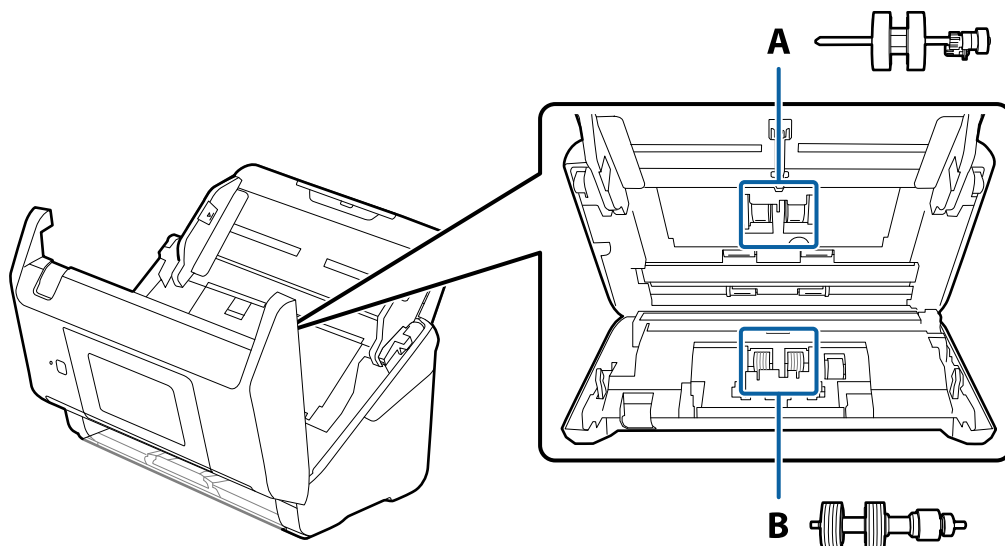
- Zatvorite poklopac skenera.
Skener izlazi iz režima čišćenja valjaka.

Povezane informacije


➔ [“Zamena sklopa valjaka” na strani 156](#)

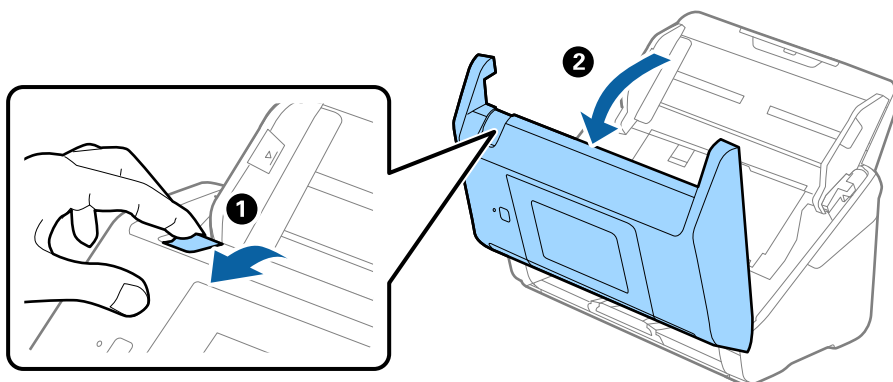
Zamena sklopa valjaka

Sklop valjaka (valjak za uvlačenje papira i valjak za razdvajanje) treba da se zameni kada broj skeniranja prekorači vek trajanja valjaka. Kada se na kontrolnoj tabli ili ekranu vašeg računara prikaže poruka o zameni, sledite navedene korake kako biste ga zamenili.

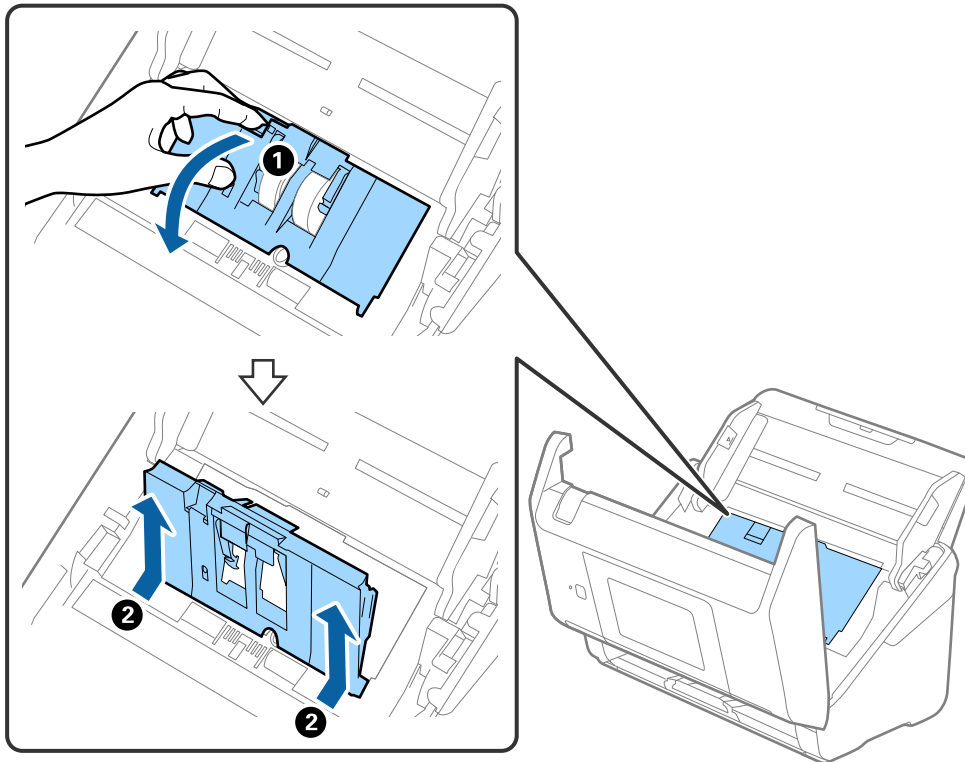


A: valjak za uvlačenje papira, B: valjak za razdvajanje

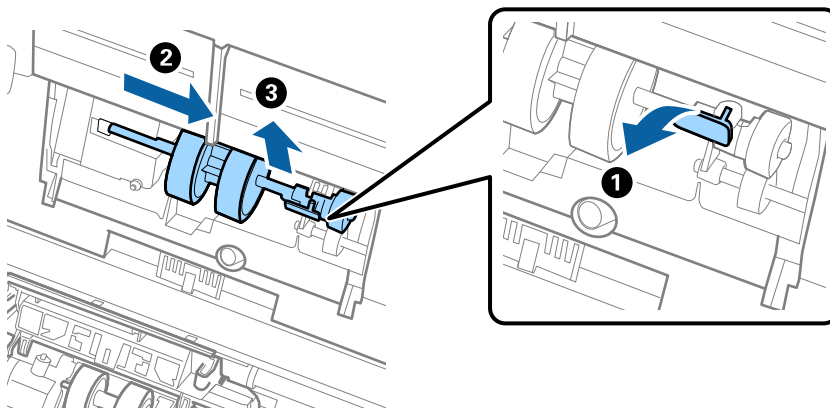
1. Pritisnite dugme  da biste isključili skener.
2. Isključite adapter naizmenične struje iz skenera.
3. Povucite polugu i otvorite poklopac skenera.



4. Otvorite poklopac prijemnog valjka, a zatim ga gurnite i izvadite.



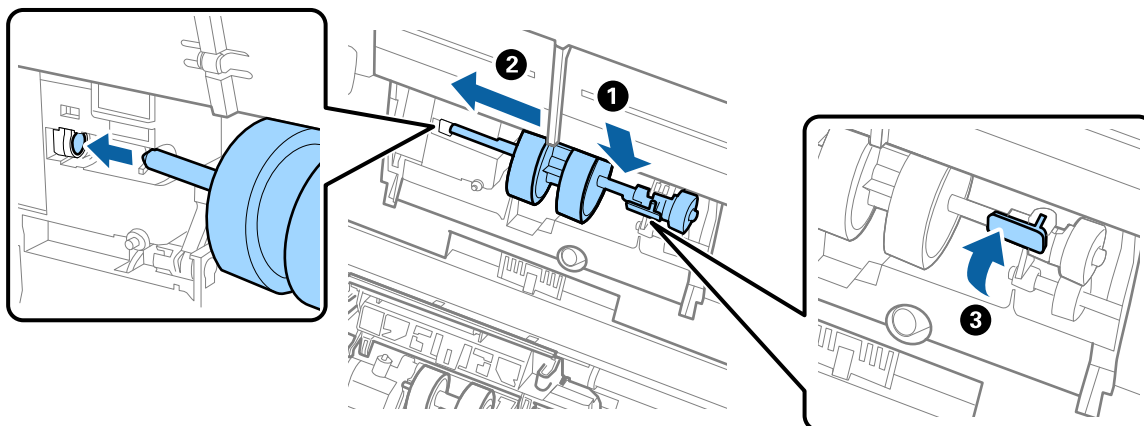
5. Pritisnite deo za učvršćivanje osovine valjka, a zatim gurnite i izvadite montirane prijemne valjke.



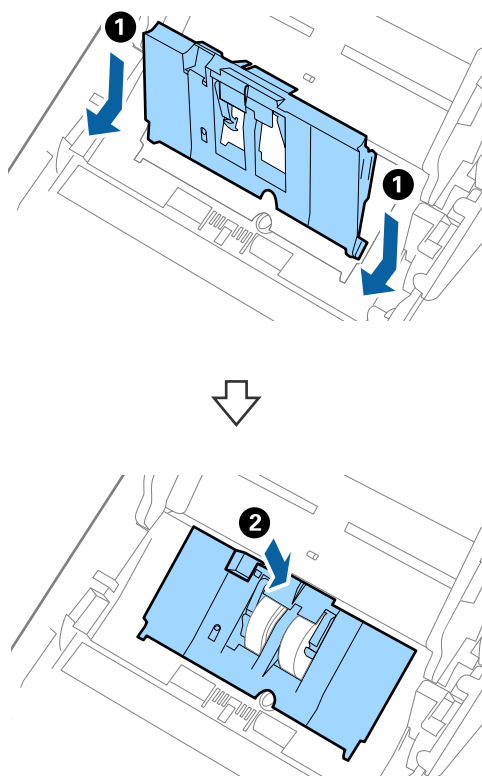
Važno:

Nemojte silom izvlačiti prijemni valjak. Na taj način biste mogli oštetiti unutrašnjost skenera.

6. Dok držite deo za pričvršćivanje, gurnite novi prijemni valjak u levu stranu i umetnite ga u otvor u skeneru. Pritisnite deo za pričvršćivanje da biste ga učvrstili.

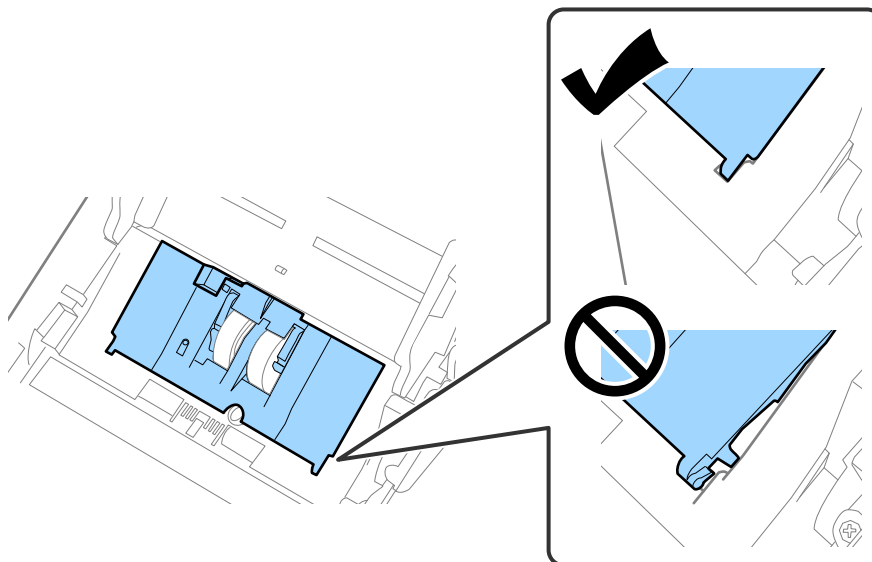


7. Stavite ivicu poklopca prijemnog valjka u žleb i gurnite ga. Čvrsto zatvorite poklopac.

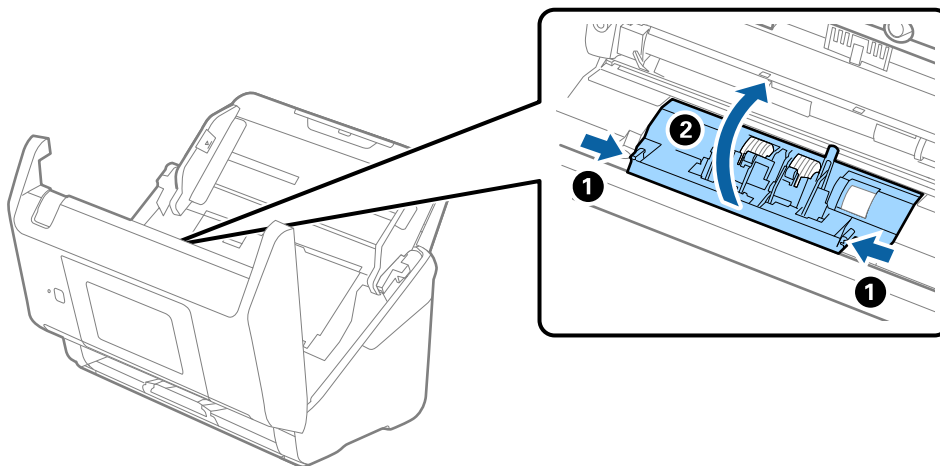


! **Važno:**

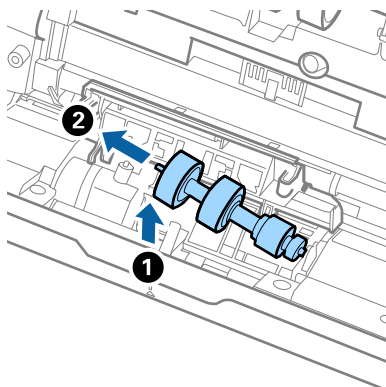
- ❑ *Vodite računa da poklopac prijemnog valjka bude pravilno zatvoren.*
- ❑ *Vodite računa da valjci za uvlačenje papira budu pravilno montirani ako se poklopac teško zatvara.*
- ❑ *Nemojte postavljati poklopac dok je podignut.*



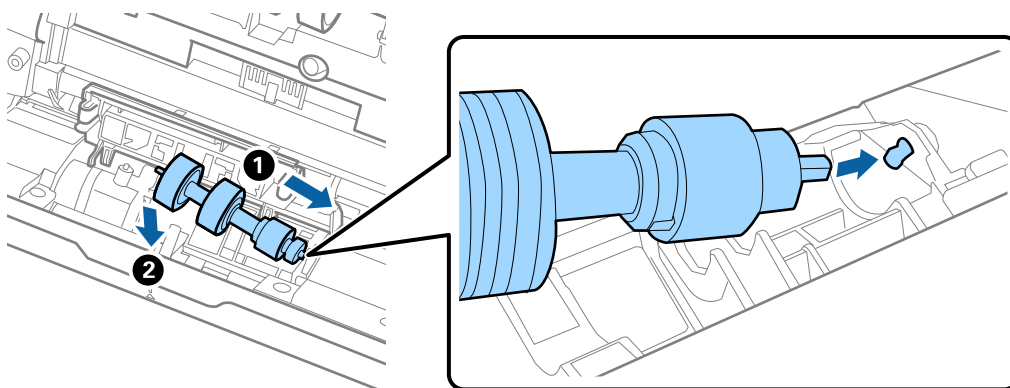
8. Gurnite hvatače na oba kraja poklopca valjka za razdvajanje da biste otvorili poklopac.



- Podignite levu stranu valjka za razdvajanje, a zatim gurnite i izvadite montirane valjke za razdvajanje.



- Ubacite osovinu novog valjka za razdvajanje u otvor sa desne strane, a zatim spustite valjak.



- Zatvorite poklopac valjka za razdvajanje.



Važno:

Ako se poklopac teško zatvara, proverite da li ste pravilno postavili valjke za razdvajanje.

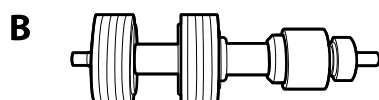
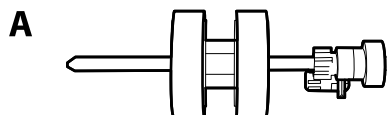
- Zatvorite poklopac skenera.
- Uključite adapter naizmenične struje i uključite skener.
- Resetujte broj skeniranja pomoću kontrolne table.

Napomena:

Odložite prijemni valjak i valjak za razdvajanje poštujući pravila i propise u svojoj lokalnoj zajednici. Nemojte ih rastavljati.

Šifre sklopa valjaka

Delovi (prijemni valjak i valjak za razdvajanje) treba da se zamene kada broj skeniranja prekorači radni broj. Najnoviji broj skeniranja možete proveriti na kontrolnoj tabli ili uslužnom programu Epson Scan 2.



A: prijemi valjak, B: valjak za razdvajanje

Naziv dela	Šifre	Vek trajanja
Sklop valjaka	B12B819671 B12B819681 (samo Indija)	200,000*

* Ovaj broj je dostignut uzastopnim skeniranjem pomoću originalnih papira za Epsonov test i predstavlja vodič za ciklus zamene. Ciklus zamene može varirati zavisno od tipova papira, kao što je papir koji stvara mnogo papirne prašine ili papir s grubom površinom koji može skratiti vek trajanja.

Resetovanje broja skeniranja

Resetuje broj skeniranja nakon zamene sklopa valjaka.

1. Na početnom ekranu izaberite **Podešavanja > Informacije o uređaju > Resetuj broj skeniranja > Broj skeniranja nakon zamene valjka**.
2. Dodirnite **Da**.

Povezane informacije

➔ [“Zamena sklopa valjaka” na strani 156](#)

Ušteda energije

Možete štedeti energiju ako koristite režim mirovanja ili režim automatskog gašenja kada skener ne izvršava nikakve operacije. Možete podesiti vremenski period pre nego što skener uđe u režim mirovanja i automatski se isključi. Svako povećanje će uticati na energetska efikasnost proizvoda. Razmislite o uticaju na životnu sredinu pre vršenja bilo kakvih izmena.

1. Na početnom ekranu izaberite **Podešavanja**.
2. Izaberite **Osn. podešavanja**.


3. Izaberite **Pod. isključivanja**, a zatim odredite podešavanja.

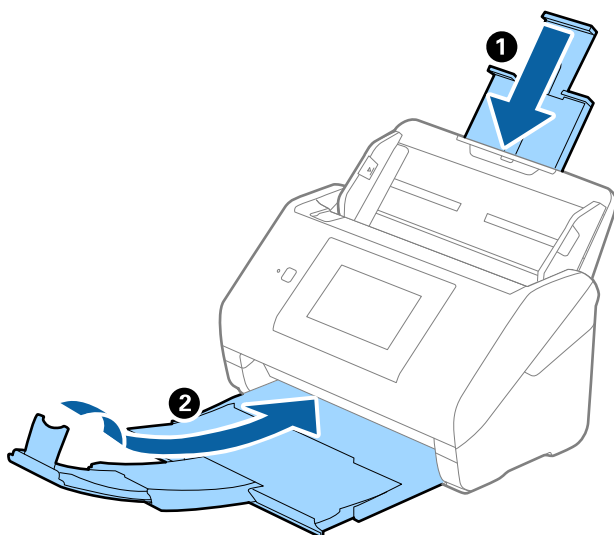
Napomena:

Dostupne funkcije mogu se razlikovati u zavisnosti od lokacije kupovine.

Transportovanje skenera

Ako je potrebno da transportujete skener radi preseljenja ili popravke, pratite korake u nastavku da biste spakovali skener.

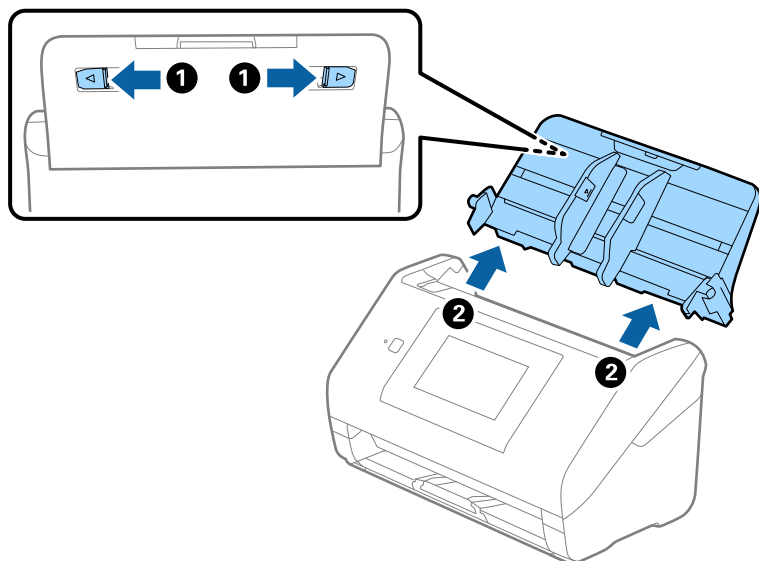
1. Pritisnite dugme  da biste isključili skener.
2. Isključite adapter naizmjenične struje iz napajanja.
3. Uklonite kablove i uređaje.
4. Zatvorite ulaznu fioku i izlaznu fioku.



Važno:

Vodite računa da dobro zatvorite izlaznu fioku; u suprotnom, može se oštetiti tokom transporta.

5. Otvorite ulaznu fioku.



6. Spojite ambalažu u kojoj je bio spakovan skener, zatim spakujte skener u njegovu originalnu kutiju ili u neku tvrdi kutiju.

Pravljenje rezervne kopije podešavanja

Možete da izvezete vrednost postavki podešenih u Web Config u datoteku. Možete je koristiti za izradu rezervnih kopija kontakata, vrednosti postavki, zamene skenera itd.

Izvezena datoteka ne može se uređivati zato što je izvezena kao binarna datoteka.

Izvoz podešavanja

Izvezite podešavanje za skener.

1. Pristupite Web Config i zatim izaberite karticu **Device Management > Export and Import Setting Value > Export**.

2. Izaberite podešavanja koja želite da izvezete.

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

3. Unesite lozinku da biste šifrovali izvezenu datoteku.

Potrebna vam je lozinka da biste uvezli datoteku. Ostavite ovu opciju praznu ako ne želite da šifrujete datoteku.

4. Kliknite na **Export**.



Važno:

Ako želite da izvezete mrežna podešavanja skenera kao što su ime uređaja i IPv6 adresa, izaberite **Enable to select the individual settings of device** i izaberite još stavki. Koristite samo izabrane vrednosti za zamenski skener.

Povezane informacije

- ➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Uvoz podešavanja

Uvezite izvezenu datoteku programa Web Config na skener.



Važno:

Kada uvozite vrednosti koje uključuju pojedinačne informacije kao što su ime skenera ili IP adresa, uverite se da ista IP adresa ne postoji na istoj mreži.

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

Podešavanja će biti primenjena na skener.

Povezane informacije

- ➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Vрати podrazumevane postavke

Na kontrolnoj tabli, izaberite **Podešavanja > Administracija sistema > Vрати podrazumevane postavke**, a zatim izaberite stavke koje želite da vratite na podrazumevane vrednosti.

- Mrežne postavke: vratite postavke u vezi s mrežnim podešavanjima na početne vrednosti.
- Sve izuzev mrežnih postavki: vratite ostale postavke na početne vrednosti osim postavki za mrežna podešavanja.
- Sve postavke: sve postavke vratite na fabrička podešavanja.



Važno:

Ako izaberete i pokrenete **Sve postavke**, biće obrisani svi podaci o podešavanjima registrovani na skeneru, uključujući kontakte i podešavanja za proveru identiteta korisnika. Izbrisana podešavanja ne mogu da se vrate.

Ažuriranje aplikacija i upravljačkog softvera

Ažuriranjem aplikacija i upravljačkog softvera možete da rešite određene probleme i unapredite ili dodate funkcije. Proverite da li koristite najnoviju verziju aplikacija i upravljačkog softvera.



Važno:

Za vreme ažuriranja nemojte isključivati računar ili skener.

Napomena:

Ako se skener može povezati na internet, možete ažurirati osnovni softver štampača iz Web Config. Izaberite karticu **Device Management > Firmware Update**, proverite prikazanu poruku, a zatim kliknite na **Start**.

1. Proverite da li je skener povezan s računarom i da li je računar povezan sa internetom.
2. Pokrenite aplikaciju EPSON Software Updater i ažurirajte aplikacije ili upravljački softver.

Napomena:

Operativni sistemi Windows Server nisu podržani.

- Operativni sistem Windows 10

Kliknite na dugme za početak i zatim izaberite **Epson Software > EPSON Software Updater**.

- Operativni sistem Windows 8.1/Windows 8

Unesite naziv aplikacije u polje za pretragu, a zatim izaberite prikazanu ikonu.

- Operativni sistem Windows 7

Kliknite na dugme za početak i zatim izaberite **Svi programi ili Programi > Epson Software > EPSON Software Updater**.

- Operativni sistem Mac OS

Izaberite **Nalazač > Kreni > Aplikacije > Epson Software > EPSON Software Updater**.

Napomena:

Ako na listi ne možete da nađete aplikaciju koju želite da ažurirate, to znači da ta aplikacija ne može da se ažurira preko funkcije EPSON Software Updater. Proverite najnovije verzije aplikacija na lokalnoj internet stranici kompanije Epson.

<http://www.epson.com>

Ažuriranje osnovnog softvera skenera pomoću kontrolne table

Ako se skener može povezati na internet, možete ažurirati osnovni softver skenera pomoću kontrolne table. Takođe možete podesiti da skener redovno proverava ažurirane verzije osnovnog softvera i obavesti vas ako ima dostupnih.

1. Na početnom ekranu izaberite **Podešavanja**.

- Izaberite **Administracija sistema > Ažuriranje firmvera > Ažuriraj**.

Napomena:

Izaberite **Obaveštenje > Uklj.** da biste podesili da skener redovno proverava dostupne ažurirane verzije osnovnog softvera.

- Proverite poruku prikazanu na ekranu i započnite traženje dostupnih ažuriranih verzija.
- Ako je na LCD ekranu prikazana poruka koja vas obaveštava da je dostupna ažurirana verzija osnovnog softvera, sledite uputstva na ekranu da biste pokrenuli ažuriranje.



Važno:

- Nemojte da isključujete kabl skenera niti da isključujete skener dok se ažuriranje ne završi; u suprotnom skener može nepravilno da radi.
- Ako ažuriranje osnovnog softvera nije završeno ili je neuspešno, skener se ne pokreće uobičajeno i prikazuje se „Recovery Mode” na LCD ekranu sledeći put kada se skener uključi. U tom slučaju treba ponovo da ažurirate osnovni softver pomoću računara. Povežite skener na računar pomoću USB kabla. Kada je na skeneru prikazano „Recovery Mode“, ne možete ažurirati osnovni softver preko mrežnog povezivanja. Pristupite Epsonovoj lokalnoj internet stranici sa računara i zatim preuzmite najnoviji osnovni softver skenera. Pogledajte uputstva na veb-sajtu radi sledećih koraka.

Ažuriranje upravljačkog softvera pomoću aplikacije Web Config

Ako se skener može povezati na internet, možete ažurirati osnovni softver štampača iz Web Config.

- Pristupite Web Config i izaberite karticu **Device Management > Firmware Update**.
- Izaberite **Start** a zatim sledite uputstva na ekranu.

Započinje potvrda upravljačkog softvera i prikazuju se informacije o njemu ukoliko postoji ažuriranje.

Napomena:

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

Povezane informacije

➔ [“Pokretanje Web Config u veb pregledaču” na strani 35](#)

Ažuriranje upravljačkog softvera bez povezivanja sa internetom

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

Napomena:

Pre ažuriranja proverite da li je upravljački program skenera Epson Scan 2 instaliran na vašem računaru. Ako aplikacija Epson Scan 2 nije instalirana, instalirajte je.

- Proverite Epsonovu internet stranicu radi najnovijih izdanja ažuriranja za upravljački softver.

<http://www.epson.com>

- Ako postoji upravljački program za skener, preuzmite ga i idite na sledeći korak.
 - Ako na internet stranici ne postoje informacije o upravljačkom programu, već koristite najnoviji upravljački program.
2. Računar na kom se nalazi preuzeti upravljački softver i skener povežite USB kablom.
 3. Dvaput kliknite na preuzetu .exe datoteku.
Epson Firmware Updater će se pokrenuti.
 4. Pratite uputstva na ekranu.