

DS-790WN

Vodič za administratore

Potrebne postavke koje odgovaraju vašoj namjeni

Mrežne postavke

Potrebne postavke skeniranja

Osnovne postavke sigurnosti

Napredne sigurnosne postavke

Authentication Settings

AutorksaAutorska prava

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

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

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

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

© 2021 Seiko Epson Corporation

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

Zaštitni znakovi

- ❑ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION i njihovi logotipi registrirane su trgovačke oznake 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 registrirani su zaštitni znakovi tvrtke Sony Corporation.
- ❑ MIFARE je registrirani zaštitni znak tvrtke NXP Semiconductor Corporation.
- ❑ Opća napomena: svi ostali nazivi proizvoda iz vodiča koriste se samo za potrebe identifikacije i mogu biti zaštitni znakovi njihovih vlasnika. Epson se odriče bilo kakvih i svih prava na te zaštitne znakove.

Sadržaj

Autorska prava

Zaštitni znakovi

Uvod

Sadržaj ovog dokumenta.	7
Uporaba ovog vodiča.	7
Oznake i simboli.	7
Opisi koji se koriste u ovom priručniku.	7
Reference operativnog sustava.	8

Potrebne postavke koje odgovaraju vašoj namjeni

Potrebne postavke koje odgovaraju vašoj namjeni.	10
--	----

Mrežne postavke

Spajanje skenera na mrežu.	13
Prije odabira mrežne veze.	13
Povezivanje mreže na upravljačkoj ploči.	15
Dodavanje ili zamjena računala ili uređaja.	19
Spajanje na skener spojen na mrežu.	19
Izravno spajanje pametnog uređaja i skenera (Wi-Fi Direct).	21
Ponovno postavljanje mrežne veze.	23
Provjera statusa mrežne veze.	25
Provjera statusa mrežne veze s upravljačke ploče.	25
Mrežne specifikacije.	26
Specifikacije Wi-Fi veze.	26
Specifikacije Etherneta.	28
Mrežne funkcije i IPv4/IPv6.	28
Sigurnosni protokol.	28
Korištenje ulaza skenera.	29
Rješavanje problema.	30
Ne može se spojiti na mrežu.	30

Softver za postavljanje skenera

Web Config.	35
Pokretanje programa Web Config u internetskom pregledniku.	35
Pokretanje usluge Web Config u sustavu Windows.	35
Epson Device Admin.	36

Predložak konfiguracije.	36
----------------------------------	----

Potrebne postavke skeniranja

Konfiguriranje poslužitelja e-pošte.	41
Stavke postavljanja poslužitelja e-pošte.	41
Provjera veze s poslužiteljem e-pošte.	42
Postavljanje dijeljene mrežne mape.	44
Kreiranje zajedničke mape.	44
Omogućavanje dostupnosti kontakata.	61
Usporedba konfiguracije kontakata.	62
Registracija odredišta u kontaktima koristeći Web Config.	62
Registriranje odredišta kao grupe koristeći Web Config.	64
Sigurnosno kopiranje i uvoz kontakata.	65
Izvoz i skupna registracija kontakata koristeći alat.	66
Suradnja između LDAP-poslužitelja i korisnika.	68
Uporaba opcije Document Capture Pro Server.	71
Postavljanje načina poslužitelja.	71
Postavljanje značajke AirPrint.	71
Problemi kod pripremanja mrežnog skeniranja.	72
Savjeti za rješavanje problema.	72
Ne mogu pristupiti aplikaciji Web Config.	72

Prilagođavanje zaslona upravljačke ploče

Registriranje Postavke.	75
Mogućnosti izbornika Postavke.	76
Uređivanje početnog zaslona upravljačke ploče.	77
Promjena Izgled početnog zaslona.	77
Dodaj ikonu.	78
Ukloni ikonu.	79
Pomakni ikonu.	80

Osnovne postavke sigurnosti

Uvod u sigurnosne značajke proizvoda.	83
Administratorske postavke.	83
Konfiguriranje lozinke administratora.	83
Korištenje Postavka blokade za upravljačku ploču.	85
Prijava kao administrator s upravljačke ploče.	88
Onemogućavanje vanjskog sučelja.	89
Nadziranje daljinskog skenera.	90

Provjera informacija o daljinskom skeneru.	90
Primanje obavijesti o događajima putem e-pošte.	90
Rješavanje problema.	91
Zaboravili ste lozinku administratora.	91

Napredne sigurnosne postavke

Sigurnosne postavke i sprječavanje opasnosti.	93
Postavke sigurnosne značajke.	94
Upravljanje uporabom protokola.	94
Upravljanje protokolima.	94
Protokoli koje možete omogućiti ili onemogućiti.	94
Stavke postavljanja protokola.	95
Korištenje digitalnog certifikata.	97
O digitalnom certificiranju.	97
Konfiguriranje CA-signed Certificate.	97
Ažuriranje samopotpisanog certifikata.	101
Konfiguriranje CA Certificate.	101
SSL/TLS komunikacija sa skenerom.	102
Konfiguriranje osnovnih SSL/TLS postavki.	102
Konfiguriranje certifikata poslužitelja za skener.	103
Kriptirana komunikacija korištenjem IPsec/IP filtriranja.	104
O aplikaciji IPsec/IP Filtering.	104
Konfiguriranje zadanih pravila.	104
Konfiguriranje grupnih pravila.	108
Primjeri konfiguracije za IPsec/IP Filtering.	114
Konfiguriranje certifikata za IPsec/IP filtriranje.	115
Spajanje skenera s IEEE802.1X mrežom.	115
Konfiguriranje IEEE 802.1X mreže.	115
Konfiguriranje certifikata za IEEE 802.1X.	117
Rješavanje problema napredne sigurnosti.	117
Vraćanje sigurnosnih postavki.	117
Problemi s korištenjem sigurnosnih značajki mreže.	118
Problemi s korištenjem digitalnog certifikata.	120

Authentication Settings

O aplikaciji Authentication Settings.	125
Dostupne funkcije za Authentication Settings.	125
O aplikaciji Authentication Method.	126
Softver za postavljanje.	128
Ažuriranje firmvera skenera.	128
Povezivanje i konfiguriranje uređaja za provjeru autentičnosti.	128
Popis kompatibilnih čitača kartica.	128

Povezivanje uređaja za provjeru autentičnosti.	131
Postavke uređaja za provjeru autentičnosti.	132
Informacije o registraciji i postavkama.	133
Postavljanje značajke.	133
Omogućavanje provjere autentičnosti.	134
Authentication Settings.	134
Registriranje User Settings.	135
Sinkroniziranje s LDAP Server.	142
Postavljanje poslužitelja e-pošte.	145
Postavka Scan to My Folder.	146
Customize One-touch Functions.	148
Job History izvješća koristeći Epson Device Admin.	149
Stavke koje se mogu uključiti u Izvješće.	149
Prijava kao administrator s upravljačke ploče.	149
Onemogućite Authentication Settings.	149
Brisanje Authentication Settings informacija (Obnovi zadane postavke).	150
Rješavanje problema.	150
Nije moguće pročitati karticu za provjeru autentičnosti.	150

Održavanje

Čišćenje izvan skenera.	152
Čišćenje unutar skenera.	152
Zamjena kompleta sklopa valjka.	157
Kodovi kompleta za sklapanje valjka.	162
Resetiranje broja skenova.	162
Ušteda energije.	162
Transportiranje skenera.	163
Pomoć kod postavki.	164
Izvoz postavki.	164
Uvoz postavki.	165
Obnovi zadane postavke.	165
Ažuriranje aplikacija i upravljačkog programa.	166
Ažuriranje upravljačkog softvera skenera preko upravljačke ploče.	166
Ažuriranje firmvera koristeći Web Config.	167
Ažuriranje upravljačkog programa bez spajanja na internet.	167

Uvod

Sadržaj ovog dokumenta.	7
Uporaba ovog vodiča.	7

Sadržaj ovog dokumenta

Ovaj dokument pruža sljedeće informacije za administratore skenera.

- Mrežne postavke
- Priprema funkcije skeniranja
- Omogućavanje i upravljanje sigurnosnim postavkama
- Omogućiti i upravljati s Authentication Settings
- Svakodnevno održavanje

Za standardne metode korištenja skenera pogledajte *Korisnički vodič*.

Napomena:

Ovaj dokument objašnjava *Authentication Settings* koji pruža samostalnu provjeru autentičnosti bez potrebe za korištenjem poslužitelja za provjeru autentičnosti. Uz *Authentication Settings* uveden u ovom priručniku, također možete izgraditi sustav provjere autentičnosti s pomoću poslužitelja za provjeru autentičnosti. Za izradu sustava koristite *Document Capture Pro Server Authentication Edition* (skraćeni naziv je *Document Capture Pro Server AE*).

Više informacija saznajte u lokalnom uredu tvrtke Epson.

Uporaba ovog vodiča

Oznake i simboli



Pozor:

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



Važno:

Upute koje treba poštivati kako bi se izbjegla oštećenja na opremi.

Napomena:

Pružaju dodatne i referentne informacije.

Povezane informacije

➔ Poveznice s povezanim dijelovima.

Opisi koji se koriste u ovom priručniku

- Snimke zaslona za aplikacije su iz Windows 10 ili macOS High Sierra. Sadržaj prikazan na zaslonima ovisi o modelu i situaciji.
- Prikazi u ovom odjeljku služe samo kao referenca. Premda one mogu izgledati nešto drukčije od stvarnog proizvoda, načini rada su jednaki.

Reference operativnog sustava

Windows

U ovom priručniku se izrazi „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” koriste za sljedeće operativne sustave. Osim toga, „Windows” se koristi za sve verzije, a „Windows Server” se koristi za povezivanje sa sustavima „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012” i „Windows Server 2008 R2”.

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

Mac OS

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

Potrebne postavke koje odgovaraju vašoj namjeni

Potrebne postavke koje odgovaraju vašoj namjeni.10

Potrebne postavke koje odgovaraju vašoj namjeni

Pogledajte sljedeće kako biste podesili potrebne postavke koje odgovaraju vašoj namjeni.

Spajanje skenera na mrežu

Namjena	Potrebne postavke
Želim spojiti skener na mrežu.	Postavite svoj skener za mrežno skeniranje. "Spajanje skenera na mrežu" na strani 13
Želim spojiti skener na novo računalo.	Postavite mrežne postavke za svoj skener na novom računalu. "Dodavanje ili zamjena računala ili uređaja" na strani 19

Postavke za skeniranje

Namjena	Potrebne postavke
Želim poslati skenirane slike e-poštom. (Scan to Email)	1. Postavite poslužitelj e-pošte koji želite povezati. "Konfiguriranje poslužitelja e-pošte" na strani 41 2. Registrirajte adresu e-pošte primatelja Contacts (neobvezno). Nakon registracije adrese e-pošte, ne morate je unositi svaki put kada želite nešto poslati, možete je samo odabrati iz svojih kontakata. "Omogućavanje dostupnosti kontakata" na strani 61
Želim spremati skenirane slike u mapu na mreži. (Scan to Network Folder/FTP)	1. Napravite mapu na mreži u koju želite spremati slike. "Postavljanje dijeljene mrežne mape" na strani 44 2. Registrirajte putanju do mape u Contacts (neobvezno). Nakon registracije putanje do mape, ne morate je unositi svaki put kada želite nešto poslati, možete je jednostavno odabrati iz svojih kontakata. "Omogućavanje dostupnosti kontakata" na strani 61
Želim spremati skenirane slike na uslugu u oblaku. (Scan to Cloud)	Postavljanje Epson Connect. Pojednostavljeni postupak postavljanja potražite na internetskoj stranici portala Epson Connect. Prilikom postavljanja potreban vam je korisnički račun za uslugu pohrane na mreži s kojom se želite povezati. https://www.epsonconnect.com/ http://www.epsonconnect.eu (samo za Europu)

Prilagođavanje zaslona upravljačke ploče

Namjena	Potrebne postavke
Želim promijeniti stavke prikazane na upravljačkoj ploči skenera.	Postavite Postavke ili Uređivanje početnog zaslona . Svoje omiljene postavke skeniranja možete registrirati na upravljačkoj ploči i uređivati prikazane stavke. "Prilagođavanje zaslona upravljačke ploče" na strani 74

Postavljanje osnovnih sigurnosnih funkcija

Namjena	Potrebne postavke
Želim spriječiti bilo koga osim administratora da promijeni postavke skenera.	Postavite lozinku administratora za skener. “Administratorske postavke” na strani 83
Želim onemogućiti uporabu skenera s USB priključcima.	Onemogućite vanjsko sučelje. “Onemogućavanje vanjskog sučelja” na strani 89

Postavljanje naprednih sigurnosnih funkcija

Namjena	Potrebne postavke
Želim upravljati protokolima koje treba koristiti.	Omogućite ili onemogućite protokole. “Upravljanje uporabom protokola” na strani 94
Želim šifrirati komunikacijsku putanju.	1. Postavite svoj digitalni certifikat. “Korištenje digitalnog certifikata” na strani 97 2. Postavite SSL/TLS komunikaciju. “SSL/TLS komunikacija sa skenerom” na strani 102
Želim koristiti šifriranu komunikaciju (IPsec). Želim moći koristiti softver samo s određenog računala (IP filtriranje).	Postavite pravila za filtriranje prometa. “Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 104
Želim koristiti skener na mreži IEEE802.1X.	Postavite IEEE802.1X za skener. “Spajanje skenera s IEEE802.1X mrežom” na strani 115

Postavljanje funkcija za koje će skener provjeriti autentičnost

Namjena	Potrebne postavke
Želim omogućiti Authentication Settings.	Pogledajte sljedeće za više informacija o dostupnim Authentication Settings i Authentication Method. “O aplikaciji Authentication Settings” na strani 125 “O aplikaciji Authentication Method” na strani 126

Korištenje sustava za provjeru autentičnosti poslužitelja

Uz Document Capture Pro Server Authentication Edition (skraćeno od Document Capture Pro Server AE) možete izgraditi sustav provjere autentičnosti koji koristi poslužitelj za provjeru autentičnosti.

Više informacija saznajte u lokalnom uredu tvrtke Epson.

Mrežne postavke

Spajanje skenera na mrežu.	13
Dodavanje ili zamjena računala ili uređaja.	19
Provjera statusa mrežne veze.	25
Mrežne specifikacije.	26
Rješavanje problema.	30

Spajanje skenera na mrežu

Ovaj dio objašnjava spajanje skenera na mrežu koristeći upravljačku ploču skenera.

Napomena:

Ako su vaš skener i računalo u istom segmentu, možete se povezati i s pomoću instalacijskog programa.

Postavljanje s internetske stranice

Pristupite sljedećoj internetskoj stranici, a zatim unesite naziv proizvoda. Idite na **Postavljanje** i započnite s postavljanjem.

<http://epson.sn>

Postavljanje pomoću softverskog diska (samo za modele uz koje se isporučuje softverski disk i korisnike koji imaju Windows računala s diskovnim pogonom.)

Umetnite disk sa softverom u računalo, a zatim slijedite upute na zaslonu.

Prije odabira mrežne veze

Za spajanje na mrežu, unaprijed provjerite način povezivanja i informacije o postavci za povezivanje.

Prikupljanje informacija o postavci veze

Pripremite neophodne informacije postavki za spajanje. Unaprijed provjerite sljedeće informacije.

Odjeljenja	Stavke	Napomena
Način spajanja uređaja	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Odlučite kako želite povezati skener na mrežu. Za lokalnu žičanu mrežu spaja se preko LAN priključka. Za Wi-Fi spaja se na mrežu (SSID) pristupne točke.
Informacije o LAN vezi	<input type="checkbox"/> IP-adresa <input type="checkbox"/> Maska podmreže <input type="checkbox"/> Zadani pristupnik	Odlučite koju IP adresu dodijeliti skeneru. Kada dodijelite IP adresu statično, potrebne su sve vrijednosti. Kada dodijelite IP adresu dinamično pomoću funkcije DHCP, ova informacija nije potrebna jer se postavlja automatski.
Informacije o Wi-Fi vezi	<input type="checkbox"/> SSID <input type="checkbox"/> Lozinka	Ovo su SSID (naziv mreže) i lozinka pristupne točke na koju se skener spaja. Ako je postavljeno filtriranje MAC-adrese, unaprijed registrirajte MAC-adresu skenera kako biste registrirali skener. Pogledajte sljedeći dio s podržanim standardima. "Mrežne specifikacije" na strani 26
Informacije o DNS poslužitelju	<input type="checkbox"/> IP adresa primarnog DNS-a <input type="checkbox"/> IP adresa sekundarnog DNS-a	Oni su potrebni kod navođenja DNS poslužitelja. Sekundarni DNS postavlja se kada sustav ima pričuvnu konfiguraciju i postoji sekundarni DNS poslužitelj. Ako ste u maloj organizaciji i ne postavljate DNS poslužitelj, postavite IP adresu usmjernika.

Odjeljenja	Stavke	Napomena
Informacije o proxy poslužitelju	<input type="checkbox"/> Naziv proxy poslužitelja	Postavite ovo kada vaše mrežno okruženje koristi proxy poslužitelja za pristup internetu s intraneta te koristite funkciju kojom skener izravno pristupa internetu. Kod sljedećih funkcija skener se izravno spaja na internet. <input type="checkbox"/> Epson Connect Services <input type="checkbox"/> Usluge oblaka drugih tvrtki <input type="checkbox"/> Ažuriranje firmvera <input type="checkbox"/> Slanje skeniranih slika na SharePoint(WebDAV)
Informacije o broju ulaza	<input type="checkbox"/> Broj ulaza za oslobađanje	Provjerite broj ulaza koje koriste skener i računalo te prema potrebi oslobodite ulaz koji je blokirao vatrozid. Pogledajte sljedeći dio s brojem ulaza kojim se koristi skener. "Korištenje ulaza skenera" na strani 29

Dodjela IP adrese

U nastavku su navedeni načini dodjele IP adrese.

Statička IP adresa:

Ručno dodjeljivanje prethodno zadanu IP adrese skeneru (domaćinu).

Informacije o spajanju na mrežu (maska podmreže, zadani pristupnik, DNS poslužitelj itd.) trebaju se postaviti ručno.

IP adresa ne mijenja se ni nakon isključivanja uređaja, pa je korisna kada želite koristiti uređaje u okruženju u kojem ne možete mijenjati IP adresu ili ako želite koristiti uređaje koristeći IP adresu. Preporučujemo postavke za skener, poslužitelja, itd. kojima pristupa puno računala. Također, kod korištenja sigurnosnih značajki poput IPsec/IP filtriranja dodijelite fiksnu IP adresu tako da se IP adresa ne promijeni.

Automatska dodjela pomoću funkcije DHCP (dinamička IP adresa):

Automatski dodjeljuje IP adresu skeneru (domaćinu) pomoću funkcije DHCP na DHCP poslužitelju ili usmjerniku.

Informacije za spajanje na mrežu (maska podmreže, zadani pristupnik, DNS poslužitelj itd.) postavljene su automatski tako da uređaj možete jednostavno spojiti na mrežu.

Ako su uređaj ili usmjernik isključeni ili ovisi o postavkama DHCP poslužitelja, IP adresa će se možda promijeniti prilikom ponovnog spajanja.

Preporučujemo drugačije upravljanje uređajima osim IP adrese i komunikacije protokolima koji prate IP adresu.

Napomena:

Kada koristite funkciju zadržavanja IP adrese na DHCP-u, uređajima možete svaki put dodijeliti istu IP adresu.

DNS poslužitelj i proxy poslužitelj

DNS poslužitelj ima naziv domaćina, domene adrese e-pošte itd. koji je povezan s informacijom IP adrese.

Nije moguća komunikacija ako je druga strana opisana nazivom domaćina, domene itd. kada računalo ili skener provodi IP komunikaciju.

Upita DNS poslužitelja o toj informaciji i pribavlja IP adresu druge strane. Ovaj proces se zove razlučivanje naziva. Stoga uređaji kao što su računala i skeneri mogu komunicirati pomoću IP adrese.

razlučivanje naziva je neophodno kako bi skener komunicirao pomoću funkcije e-pošte i spajanja na internet.

Kada koristite neku od tih funkcija, uredite postavke DNS poslužitelja.

Kada dodjeljujete IP adresu skenera pomoću funkcije DHCP na DHCP poslužitelju ili usmjerniku, postavlja se automatski.

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

Kada se na internet spajate pomoću proxy poslužitelja, na skeneru konfigurirajte proxy poslužitelj.

Povezivanje mreže na upravljačkoj ploči

Povežite se na skener preko upravljačke ploče skenera.

Dodjela IP adrese

Postavite osnovne stavke poput adrese domaćina Maska podmreže, Zadani pristupnik.

Ovaj dio objašnjava proceduru postavljanja statičke IP adrese.

1. Uključite skener.
2. Odaberite **Postavke** na početnom zaslону na upravljačkoj ploči skenera.
3. Odaberite **Postavke mreže > Napredno > TCP/IP**.
4. Odaberite **Ručno** za **Dohvati IP adresu**.

Ako postavite automatski IP adresu korištenjem funkcije DHCP usmjernika, odaberite **Automatski**. U tom slučaju se **IP adresa**, **Maska podmreže**, i **Zadani pristupnik** u koraku 5 do 6 također automatski postavljaju, pa prijedite na korak 7.

5. Unesite IP adresu.

Fokus se pomiče na segment naprijed ili natrag odvojen točkom ako odaberete ◀ i ▶.

Potvrdite vrijednost prikazanu na prethodnom zaslону.

6. Podesite stavke **Maska podmreže** i **Zadani pristupnik**.

Potvrdite vrijednost prikazanu na prethodnom zaslону.



Važno:

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

7. Unesite IP adresu primarnog DNS poslužitelja.

Potvrdite vrijednost prikazanu na prethodnom zaslону.

Napomena:

Kada odaberete **Automatski** za postavke dodjele IP adrese, možete odabrati postavke DNS poslužitelja preko **Ručno** ili **Automatski**. Ako ne možete automatski pribaviti adresu DNS poslužitelja, odaberite **Ručno** i unesite adresu DNS poslužitelja. Zatim unesite izravno adresu sekundarnog DNS poslužitelja. Ako odaberete **Automatski**, idite na korak 9.

8. Unesite IP adresu sekundarnog DNS poslužitelja.
Potvrdite vrijednost prikazanu na prethodnom zaslonu.
9. Dodirnite **Početak postavke**.

Postavljanje proxy poslužitelja


Postavite proxy poslužitelj ako je oboje u nastavku točno.

- Proxy poslužitelj je izrađen za internetsko povezivanje.
- Kada koristite funkciju u kojoj se skener izravno spaja na internet kao što je usluga Epson Connect ili usluga oblaka drugih tvrtki.

1. Odaberite **Postavke** na početnom zaslonu.
Prilikom podešavanja postavki nakon postavki IP adrese, prikazuje se zaslon **Napredno**. Idite na korak 3.
2. Odaberite **Postavke mreže > Napredno**.
3. Odaberite **Proxy poslužitelj**.
4. Odaberite **Koristi za Postavke proxy poslužitelja**.
5. Unesite adresu proxy poslužitelja u IPv4 ili FQDN formatu.
Potvrdite vrijednost prikazanu na prethodnom zaslonu.
6. Unesite broj ulaza proxy poslužitelja.
Potvrdite vrijednost prikazanu na prethodnom zaslonu.
7. Dodirnite **Početak postavke**.

Spajanje na Ethernet

Spojite skener na mrežu koristeći LAN kabel i zatim provjerite vezu.

1. Spojite skener i koncentrator (sklopka LAN) LAN kabelom.
2. Odaberite  na početnom zaslonu.
3. Odaberite **Usmjerivač**.
4. Uvjerite se da su odabrane ispravne postavke Veza i IP adresa.
5. Dodirnite **Zatvori**.

Spajanje na bežični LAN (Wi-Fi)

Možete spojiti skener na bežični LAN (Wi-Fi) na nekoliko načina. Odaberite način povezivanja koji odgovara okruženju i uvjetima koje koristite.

Ako su vam poznati podaci za bežični usmjernik kao što su SSID i lozinka, postavke možete namjestiti ručno.

Ako bežični usmjernik podržava WPS, postavke možete namjestiti pomoću postavljanja gumba.

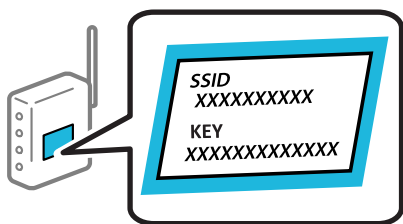
Nakon povezivanja skenera na mrežu, spojite na skener preko uređaja koji želite koristiti (računalo, pametni uređaj, tablet, itd.)

Odabir Wi-Fi postavki unosom SSID i lozinke

Možete postaviti Wi-Fi mrežu unosom informacija potrebnih za spajanje na bežični usmjernik preko upravljačke ploče skenera. Za postavljanje ovog načina treba vam SSID i lozinka za bežični usmjernik.

Napomena:

Ako koristite bežični usmjernik s njegovim zadanim postavkama, SSID i lozinka zapisani su na naljepnici. Ako ne znate SSID i lozinku, obratite se osobi koja je postavila bežični usmjernik ili provjerite dokumentaciju isporučenu uz bežični usmjernik.



1. Dodirnite  na početnom zaslonu.

2. Odaberite **Usmjerivač**.

3. Dodirnite **Pokreni postavu**.

Ako je mrežna veza već postavljena, prikazat će se pojednosti veze. Dodirnite **Promijenite na Wi-Fi vezu**, ili **Promijeni postavke** za promjenu postavki.

4. Odaberite **Čarobnjak za postavljanje Wi-Fi mreže**.

5. Slijedite upute na zaslonu za odabir SSID-a, unesite lozinku za bežični usmjernik i pokrenite postavljanje.

Ako želite provjeriti status mrežne veze skenera nakon dovršenog postavljanja, pojednosti potražite na donjoj poveznici povezanih informacija.

Napomena:

Ako ne znate SSID, provjerite je li zapisan na naljepnici bežičnog usmjernika. Ako koristite bežični usmjernik s njegovim zadanim postavkama, koristite SSID zapisan na naljepnici. Ako ne možete pronaći informacije, provjerite dokumentaciju isporučenu uz bežični usmjernik.

Lozinka razlikuje mala i velika slova.

Ako ne znate lozinku, provjerite jesu li informacije zapisane na naljepnici bežičnog usmjernika. Na naljepnici lozinka može sadržavati „Network Key”, „Wireless Password” itd. Ako koristite bežični usmjernik s njegovim zadanim postavkama, koristite lozinku zapisanu na naljepnici.

Povezane informacije

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

Postavljanje Wi-Fi postavki postavljanjem brzog gumba (WPS)

Možete automatski postaviti Wi-Fi mrežu tako da pritisnete gumb na bežičnom usmjerniku. Ako su zadovoljeni sljedeći uvjeti, moći ćete izvršiti postavljanje na ovaj način.

- Bežični usmjernik kompatibilan je s WPS-om (Wi-Fi Protected Setup).
- Aktualna Wi-Fi veza uspostavljena je pritiskom na gumb na bežičnom usmjerniku.

Napomena:

Ako ne možete pronaći gumb ili provodite postavljanje pomoću softvera, pogledajte dokumentaciju isporučenu s bežičnim usmjernikom.

1. Dodirnite  na početnom zaslonu.

2. Odaberite **Usmjerivač**.

3. Dodirnite **Pokreni postavu**.

Ako je mrežna veza već postavljena, prikazat će se pojedinosti veze. Dodirnite **Promijenite na Wi-Fi vezu**, ili **Promijeni postavke** za promjenu postavki.

4. Odaberite **Postavljanje pritisknog gumba (WPS)**.

5. Slijedite upute na zaslonu.

Ako želite provjeriti status mrežne veze skenera nakon dovršenog postavljanja, pojedinosti potražite na donjoj poveznici povezanih informacija.

Napomena:

Ako ne uspije povezivanje, ponovno pokrenite bežični usmjernik, približite ga skeneru i pokušajte ponovno.

Povezane informacije

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

Podršavanje postavki Wi-Fi veze postavljanjem PIN koda (WPS)

Možete se automatski spojiti na bežični usmjernik koristeći PIN kod. Na ovaj način možete odrediti je li bežični usmjernik kompatibilan s WPS-om (Wi-Fi Protected Setup). Upotrijebite računalo kako biste unijeli PIN-kod u bežični usmjernik.

1. Dodirnite  na početnom zaslonu.

2. Odaberite **Usmjerivač**.

3. Dodirnite **Pokreni postavu**.

Ako je mrežna veza već postavljena, prikazat će se pojedinosti veze. Dodirnite **Promijenite na Wi-Fi vezu**, ili **Promijeni postavke** za promjenu postavki.

4. Odaberite **Ostalo** > **Postavljanje PIN koda (WPS)**

5. Slijedite upute na zaslonu.

Ako želite provjeriti status mrežne veze skenera nakon dovršenog postavljanja, pojedino potražite na donjoj poveznici povezanih informacija.

Napomena:

Provjerite dokumentaciju isporučenu uz bežični usmjernik kako biste saznali više informacija o unosu PIN-koda.

Povezane informacije

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

Dodavanje ili zamjena računala ili uređaja

Spajanje na skener spojen na mrežu

Ako je skener već spojen na mrežu, možete spojiti računalo ili pametni uređaj na skener preko mreže.

Uporaba mrežnog skenera iz drugog računala

Preporučujemo da koristite program za instaliranje kako biste povezali skener s računalom. Program za instalaciju možete pokrenuti na jedan od sljedećih načina.

Postavljanje s internetske stranice

Pristupite sljedećoj internetskoj stranici, a zatim unesite naziv proizvoda. Idite na **Postavljanje** i započnite s postavljanjem.

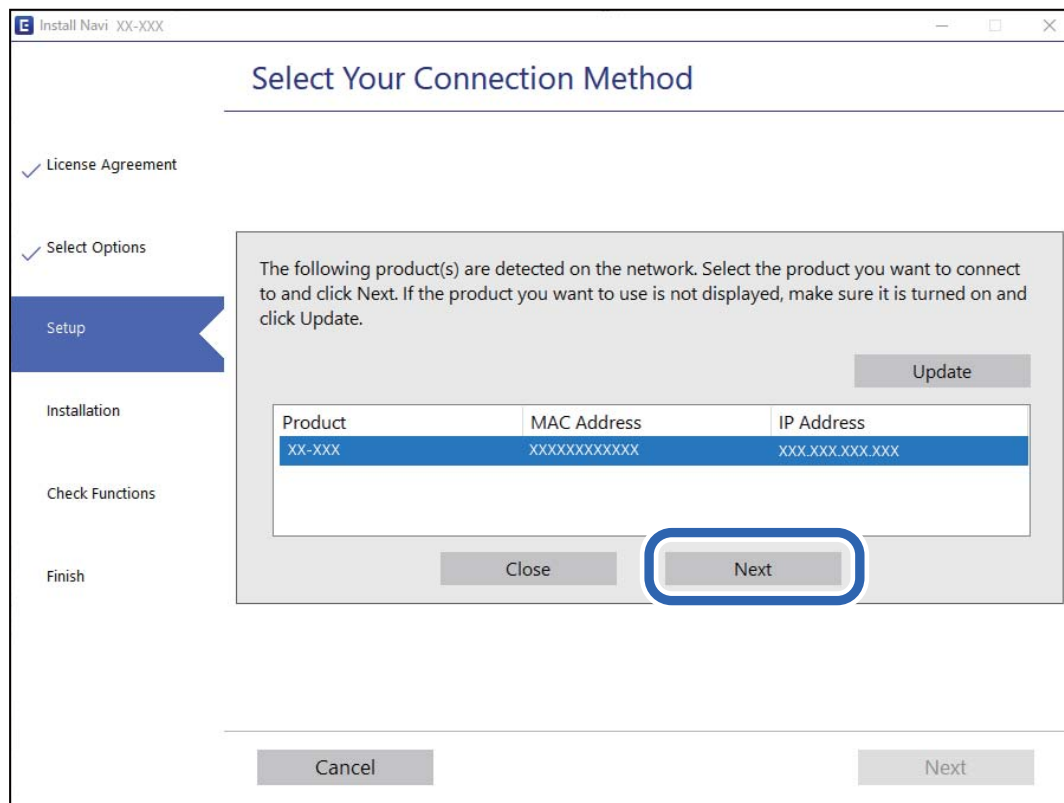
<http://epson.sn>

Postavljanje pomoću softverskog diska (samo za modele uz koje se isporučuje softverski disk i korisnike koji imaju Windows računala s diskovnim pogonom.)

Umetnite disk sa softverom u računalo, a zatim slijedite upute na zaslonu.

Odabir skenera

Slijedite upute sa zaslona dok se ne prikaže sljedeći zaslom, zatim odaberite naziv skenera na koji se želite spojiti i zatim kliknite na **Dalje**.



Slijedite upute na zaslону.

Korištenje mrežnog skenera preko pametnog uređaja

Možete spojiti pametni uređaj na skener koristeći jedan od sljedećih načina.

Spajanje preko bežičnog usmjernika

Spojite pametni uređaj na istu Wi-Fi mrežu (SSID) na kojoj je i skener.

Više pojedinosti potražite u nastavku.

[“Odabir postavki za spajanje na pametni uređaj” na strani 24](#)

Spajanje koristeći Wi-Fi Direct

Spojite pametni uređaj na skener izravno bez bežičnog usmjernika.

Više pojedinosti potražite u nastavku.

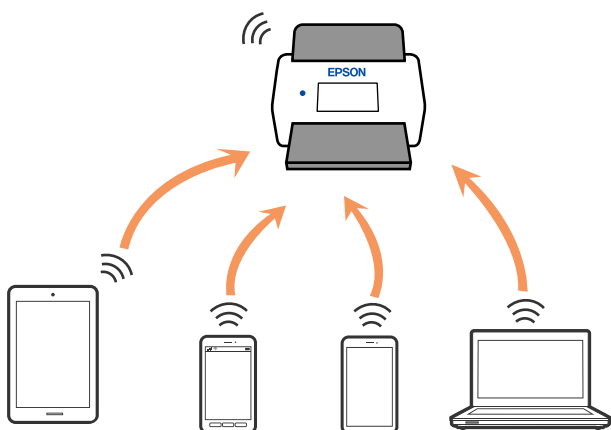
[“Izravno spajanje pametnog uređaja i skenera \(Wi-Fi Direct\)” na strani 21](#)

Izravno spajanje pametnog uređaja i skenera (Wi-Fi Direct)

Wi-Fi Direct (jednostavan način rada AP) omogućuje da spojite pametni uređaj izravno na skener bez bežičnog usmjernika te ispisujete s pametnog uređaja.

O aplikaciji Wi-Fi Direct


Ovaj način povezivanja koristite ako Wi-Fi ne koristite kod kuće ili u uredu ili ako želite izravno povezati skener i računalo ili pametni uređaj. U ovom načinu rada skener će se ponašati kao bežični usmjernič, a uređaje ćete sa skenerom moći povezati bez potrebe za korištenjem standardnog bežičnog usmjerniča. Međutim, uređaji koji su izravno povezani na skener ne mogu međusobno komunicirati preko skenera.



Skener možete istovremeno povezati putem Wi-Fi ili Ethernet veze te Wi-Fi Direct (jednostavan način rada AP). Međutim, ako mrežnu vezu pokrenete u načinu rada Wi-Fi Direct (jednostavan način rada AP) veze, kada je skener povezan putem Wi-Fi mreže, Wi-Fi će se privremeno odspojiti.

Povezivanje preko pametnog uređaja programom Wi-Fi Direct

Ovaj način omogućuje izravno povezivanje skenera s pametnim uređajima bez bežičnog usmjerniča.

1. Odaberite  na početnom zaslonu.
2. Odaberite **Wi-Fi Direct**.
3. Odaberite **Pokreni postavu**.
4. Pokrenite Epson Smart Panel na vašem pametnom uređaju.
5. Slijedite upute prikazane na Epson Smart Panel za spajanje na vaše skener.
Kada vaš pametni uređaj bude spojen na skener, prijedite na sljedeći korak.
6. Na upravljačkoj ploči skenera odaberite **Dovršeno**.

Isključivanje veze Wi-Fi Direct (jednostavan način rada AP)

Dostupna su dva načina deaktivacije veze Wi-Fi Direct (jednostavan način rada AP); možete deaktivirati sve veze koristeći upravljačku ploču skenera ili deaktivirajte svaku vezu iz računala ili pametnog telefona.

Kada želite onemogućiti sve veze, odaberite  > **Wi-Fi Direct** > **Pokreni postavu** > **Promjena** > **Onemogući Wi-Fi Direct**.



Važno:

Kada se onemogući Wi-Fi Direct (jednostavan način rada AP) veza, sva računala i pametni uređaji spojeni na skener Wi-Fi Direct (jednostavan način rada AP) vezom bit će odspojeni.

Napomena:

Ako želite odspojiti određeni uređaj, odspojite ga s uređaja umjesto skenera. Jednim od sljedećih načina isključite vezu Wi-Fi Direct (jednostavan način rada AP) iz uređaja.

- Isključite Wi-Fi vezu s mrežnim nazivom skenera (SSID).
- Spojite s drugim mrežnim nazivom (SSID).

Promjena postavki Wi-Fi Direct (jednostavni način rada AP) kao što je SSID

Kada je omogućeno Wi-Fi Direct (jednostavan način rada AP) povezivanje, postavke možete promijeniti u



> **Wi-Fi Direct** > **Pokreni postavu** > **Promjena**, a zatim se prikazuju sljedeće značajke izbornika.

Promijeni naziv mreže

Promijenite Wi-Fi Direct (jednostavan način rada AP) mrežni naziv (SSID) korišten za spajanje na skener s vašim arbitražnim imenom. Možete postaviti mrežni naziv (SSID) u ASCII znakovima koji su prikazani na tipkovnici softvera na upravljačkoj ploči. Možete unijeti do 22 znaka.

Kad mijenjate mrežni naziv (SSID), isključit će se svi povezani uređaji. Koristite novi mrežni naziv (SSID) želite li ponovno povezati uređaje koristite novu lozinku.

Promijeni lozinku

Promijenite Wi-Fi Direct (jednostavan način rada AP) lozinku za spajanje na skener na vašu arbitražnu vrijednost. Lozinku možete postaviti u ASCII znakovima koji su prikazani na tipkovnici softvera na upravljačkoj ploči. Možete unijeti od 8 do 22 znaka.

Kad mijenjate lozinku, isključit će se svi povezani uređaji. Ako želite ponovo povezati uređaje koristite novu lozinku.

Promijeni frekvencijski raspon

Promijenite raspon frekvencije za Wi-Fi Direct korišten za spajanje skenera. Možete odabrati 2,4 GHz ili 5 GHz.

Kod promjene raspona frekvencije isključit će se svi povezani uređaji. Ponovno spojite uređaj.

Imajte na umu da ne možete ponovno spojiti preko uređaja koji ne podržavaju raspon frekvencije od 5 GHz kod promjene na 5 GHz.

Ovisno o regiji, ova postavka možda neće biti prikazana.

Onemogućiti Wi-Fi Direct

Onemogućite Wi-Fi Direct (jednostavan način rada AP) postavke skenera. Kada ih onemogućite, svi uređaji povezani sa skenerom pomoću Wi-Fi Direct (jednostavan način rada AP) povezivanja su odspojeni.

Vrati zadane postavke

Vratite sve Wi-Fi Direct (jednostavan način rada AP) postavke na njihove zadane vrijednosti.

Izbrisane su Wi-Fi Direct (jednostavan način rada AP) informacije spajanja pametnog uređaja spremljene na skener.

Napomena:

Također možete postaviti iz kartice **Network** > **Wi-Fi Direct** na **Web Config** za sljedeće postavke.

- Omogućavanje ili onemogućavanje funkcije Wi-Fi Direct (jednostavan način rada AP)
- Promjena mrežnog naziva (SSID)
- Mijenjanje lozinke
- Promjena raspona frekvencije
Ovisno o regiji, ova postavka možda neće biti prikazana.
- Vraćanje postavki za Wi-Fi Direct (jednostavan način rada AP)

Ponovno postavljanje mrežne veze

Ovaj dio objašnjava način odabira postavki mrežne veze i promjenu načina povezivanja kod zamjene bežičnog usmjernika ili računala.

Kod zamjene bežičnog usmjernika

Kada zamijenite bežični usmjernik, odaberite postavke povezivanja računala ili pametnog uređaja i skenera.

Morate odabrati ove postavke ako, primjerice, promijenite pružatelja internetske usluge.

Odabir postavki za spajanje na računalo

Preporučujemo da koristite program za instaliranje kako biste povezali skener s računalom. Program za instalaciju možete pokrenuti na jedan od sljedećih načina.

- Postavljanje s internetske stranice
Pristupite sljedećoj internetskoj stranici, a zatim unesite naziv proizvoda. Idite na **Postavljanje** i započnite s postavljanjem.
<http://epson.sn>
- Postavljanje pomoću softverskog diska (samo za modele uz koje se isporučuje softverski disk i korisnike koji imaju Windows računala s diskovnim pogonom.)
Umetnite disk sa softverom u računalo, a zatim slijedite upute na zaslonu.

Odabir načina povezivanja

Slijedite upute na zaslonu. Na zaslonu **Odaberite postupak** odaberite **Ponovno postavljanje veze s Pisač (za novi mrežni usmjerivač ili promjenu USB-a na mrežu itd.)**, a zatim kliknite na **Dalje**.

Slijedite upute za završetak postavljanja na zaslonu.

Ako ne možete spojiti, isprobajte sljedeće kako biste riješili problem.

[“Ne može se spojiti na mrežu” na strani 30](#)

Odabir postavki za spajanje na pametni uređaj

Možete koristiti skener preko pametnog uređaja kada spojite skener na istu Wi-Fi mrežu (SSID) kao i pametni uređaj. Za uporabu skenera preko pametnog uređaja, pristupite sljedećoj internetskoj stranici i zatim unesite naziv proizvođača. Idite na **Postavljanje** i započnite s postavljanjem.

<http://epson.sn>

Pristupite web-stranici preko pametnog uređaja koji želite spojiti na skener.

Kod punjenja računala

Kod punjenja računala odaberite postavke povezivanja računala i skenera.

Odabir postavki za spajanje na računalo

Preporučujemo da koristite program za instaliranje kako biste povezali skener s računalom. Možete pokrenuti program za instaliranje koristeći sljedeći način.

- Postavljanje s internetske stranice

Pristupite sljedećoj internetskoj stranici, a zatim unesite naziv proizvođača. Idite na **Postavljanje** i započnite s postavljanjem.

<http://epson.sn>

- Postavljanje pomoću softverskog diska (samo za modele uz koje se isporučuje softverski disk i korisnike koji imaju Windows računala s diskovnim pogonom.)

Umetnite disk sa softverom u računalo, a zatim slijedite upute na zaslonu.

Slijedite upute na zaslonu.

Promjena načina povezivanja s računalom

Ovaj dio objašnjava kako se može promijeniti način povezivanja kada su računalo i skener spojeni.

Promjena mrežne veze s Ethernet na Wi-Fi

Promijenite s Ethernet veze na Wi-Fi vezu s upravljačke ploče skenera. Način promjene veze u osnovi odgovara postavkama Wi-Fi veze.

Povezane informacije

➔ [“Spajanje na bežični LAN \(Wi-Fi\)” na strani 17](#)

Promjena mrežne veze s Wi-Fi na Ethernet

Slijedite donje korake za promjenu s Wi-Fi na Ethernet vezu.

1. Odaberite **Postavke** na početnom zaslonu.

2. Odaberite **Postavke mreže** > **Postava žičanog LAN-a**.
3. Slijedite upute na zaslonu.

Promjena s USB-a na mrežnu vezu

Koristeći program za instalaciju i ponovno postavljanje u drugom načinu povezivanja.

- Postavljanje s internetske stranice

Pristupite sljedećoj internetskoj stranici, a zatim unesite naziv proizvoda. Idite na **Postavljanje** i započnite s postavljanjem.

<http://epson.sn>

- Postavljanje pomoću softverskog diska (samo za modele uz koje se isporučuje softverski disk i korisnike koji imaju Windows računala s diskovnim pogonom.)

Umetnite disk sa softverom u računalo, a zatim slijedite upute na zaslonu.

Odabirom opcije za promjenu načina povezivanja

Slijedite upute na zaslonu. Na zaslonu **Odaberite postupak** odaberite **Ponovno postavljanje veze s Pisač (za novi mrežni usmjerivač ili promjenu USB-a na mrežu itd.)**, a zatim kliknite na **Dalje**.

Odaberite mrežnu vezu koju želite koristiti, **Poveži putem bežične mreže (Wi-Fi)** ili **Povezivanje putem kablenskog LAN-a (Ethernet)**, a zatim kliknite na **Dalje**.

Slijedite upute za završetak postavljanja na zaslonu.

Provjera statusa mrežne veze

Status mrežne veze možete provjeriti na sljedeći način.









Provjera statusa mrežne veze s upravljačke ploče

Možete provjeriti status mrežne veze pomoću ikone mreže ili podataka o mreži na upravljačkoj ploči skenera.

Provjera statusa mrežne veze pomoću ikone mreže

Pomoću ikone mreže na početnom zaslonu skenera možete provjeriti status mrežnog povezivanja i jačinu radiovala.



	<p>Prikazuje status mrežne veze.</p> <p>Odaberite ikonu kako biste provjerili ili promijenili aktualne postavke. To je prečac na sljedeći izbornik.</p> <p>Postavke > Postavke mreže > Postavljanje Wi-Fi veze</p>
	<p>Skener nije spojen na bežičnu (Wi-Fi) mrežu.</p>
	<p>Skener pretražuje SSID, uklonio je IP adresu ili ima poteškoća s bežičnom (Wi-Fi) mrežom.</p>
	<p>Skener je spojen na bežičnu (Wi-Fi) mrežu.</p> <p>Broj crtica označava jačinu mrežnog signala. Veći broj crtica znači i bolji mrežni signal.</p>
	<p>Skener nije spojen na bežičnu (Wi-Fi) mrežu u načinu Wi-Fi Direct (jednostavan način rada AP).</p>
	<p>Skener je spojen na bežičnu (Wi-Fi) mrežu u načinu Wi-Fi Direct (jednostavan način rada AP).</p>
	<p>Skener nije spojen na žičanu (Ethernet) mrežu ili je uklonio postavku.</p>
	<p>Skener je spojen na žičanu (Ethernet) mrežu.</p>

Prikaz detaljnih informacija o mreži na upravljačkoj ploči

Kada je vaš skener priključen na mrežu, možete vidjeti i druge informacije koje se odnose na mrežu odabiranjem izbornika mreže koju želite provjeriti.

1. Odaberite **Postavke** na početnom zaslonu.
2. Odaberite **Postavke mreže > Stanje mreže**.
3. Za provjeru informacija odaberite izbornike koje želite provjeriti.
 - Status ožičene LAN/Wi-Fi veze
Prikazuju se mrežni podaci (naziv uređaja, veza, jačina signala, itd.) za Ethernet ili Wi-Fi veze.
 - Wi-Fi Direct status
Prikazuje se je li značajka Wi-Fi Direct omogućena ili onemogućena te SSID, lozinka itd. za veze Wi-Fi Direct.
 - Status poslužitelja e-pošte
Prikazuju se mrežni podaci za poslužitelj e-pošte.

Mrežne specifikacije

Specifikacije Wi-Fi veze

Pogledajte sljedeću tablicu sa specifikacijama Wi-Fi veze.

Zemlje ili regije osim navedenih u nastavku	Tablica A
---	-----------

Australija Novi Zeland Tajvan Južna Koreja	Tablica B
---	-----------

Tablica A

Standardi	IEEE 802.11b/g/n*1
Frekvencijski opseg	2,4 GHz
Maksimalna prenesena radiofrekvencijska snaga	2400–2483,5 MHz: 20 dBm (EIRP)
Kanali	1/2/3/4/5/6/7/8/9/10/11/12/13
Načini povezivanja	Infrastruktura, Wi-Fi Direct (jednostavan način rada AP)*2*3
Sigurnosni protokoli*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Dostupno samo za HT20.

*2 Nije podržano za IEEE 802.11b.

*3 Istovremeno se mogu koristiti infrastruktura i Wi-Fi Direct modusi ili Ethernet veza.

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

*5 Udovoljava odredbi WPA2 s podrškom za WPA/WPA2 Personal.

Tablica B

Standardi	IEEE 802.11a/b/g/n*1/ac		
Rasponi frekvencije	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Kanali	Wi-Fi	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)
Načini povezivanja	Infrastruktura, Wi-Fi Direct (jednostavan način rada AP)*4, *5		
Sigurnosni protokoli*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Dostupno samo za HT20.

*2 Nije dostupno u Tajvanu.

*3 Dostupnost ovih kanala i uporaba proizvoda na otvorenom preko ova tri kanala ovisi o lokaciji. Više informacija potražite na <http://support.epson.net/wifi5ghz/>

- *4 Nije podržano za IEEE 802.11b.
- *5 Istovremeno se mogu koristiti infrastruktura i Wi-Fi Direct modusi ili Ethernet veza.
- *6 Wi-Fi Direct podržava samo WPA2-PSK (AES).
- *7 Udovoljava odredbi WPA2 s podrškom za WPA/WPA2 Personal.

Specifikacije Etherneta

Standardi	IEEE802.3i (10BASE-T)* ¹ IEEE802.3u (100BASE-TX)* ¹ IEEE802.3ab (1000BASE-T)* ¹ IEEE802.3az (energetski štedljivi Ethernet)* ²
Način komunikacije	Automatski, 10 Mbps potpuno dupleksni, 10 Mbps poludupleksni, 100 Mbps potpuno dupleksni, 100 Mbps poludupleksni
Spojnik	RJ-45

*1 Upotrijebite STP kabel (oklopljena upletena parica) kategorije 5e ili više kako biste spriječili opasnost od radijske interferencije.

*2 Spojeni uređaj treba udovoljavati standardima IEEE802.3az.

Mrežne funkcije i IPv4/IPv6

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

Sigurnosni protokol

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

* Trebate koristiti priključni uređaj koji ispunjava zahtjeve standarda IEEE802.1X.

Korištenje ulaza skenera

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

Kada je pošiljatelj (klijent) skener

Uporaba	Odredište (poslužitelj)	Protokol	Broj ulaza
Slanje datoteke (kada se preko skenera koristi skeniranje u mrežnu mapu)	FTP/FTPS poslužitelj	FTP/FTPS (TCP)	20
			21
	Poslužitelj datoteke	SMB (TCP)	445
		NetBIOS (UDP)	137
		NetBIOS (TCP)	138
	WebDAV poslužitelj	Protokol HTTP (TCP)	80
		Protokol HTTPS (TCP)	443
Slanje e-pošte (kada se preko skenera koristi skeniranje u e-poštu)	SMTP poslužitelj	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP prije SMTP veze (kada se preko skenera koristi skeniranje u e-poštu)	POP poslužitelj	POP3 (TCP)	110
Kada se koristi Epson Connect	Epson Connect poslužitelj	HTTPS	443
		XMPP	5222
Prikupljanje podataka o korisniku (koristi kontakte sa skenera)	LDAP poslužitelj	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Provjera autentičnosti korisnika kod prikupljanja podataka o korisniku (kada se koriste kontakti sa skenera) Provjera autentičnosti korisnika kod skeniranja u mrežnu mapu (SMB) sa skenera	KDC poslužitelj	Kerberos	88
Control WSD	Klijentsko računalo	WSD (TCP)	5357
Pretraživanje računala kod brzog skeniranja iz aplikacije	Klijentsko računalo	Otkrivanje brzog skeniranja preko mreže	2968

Kada je pošiljalatelj (klijent) računalo klijenta

Uporaba	Odredište (poslužitelj)	Protokol	Broj ulaza
Otkrijte skener iz aplikacije poput EpsonNet Config i upravljačkog programa skenera.	Skener	ENPC (UDP)	3289
Prikupite i postavite MIB informacije iz aplikacije poput EpsonNet Config i upravljačkog programa skenera.	Skener	SNMP (UDP)	161
Traženje WSD skenera	Skener	WS-Discovery (UDP)	3702
Prosljeđivanje podataka skena iz aplikacije	Skener	Mrežno skeniranje (TCP)	1865
Prikupljanje informacija o zadatku kod brzog skeniranja iz aplikacije	Skener	Brzo skeniranje preko mreže	2968
Web Config	Skener	HTTP (TCP)	80
		HTTPS (TCP)	443

Rješavanje problema

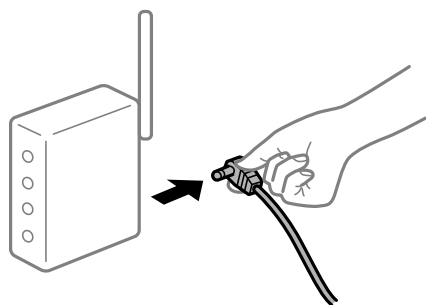
Ne može se spojiti na mrežu

Problem bi mogao biti jedan od sljedećih problema.

■ Nešto nije u radu s mrežnim uređajima za Wi-Fi vezu.

Rješenja

Isključite uređaje koje želite povezati s mrežom. Pričekajte otprilike 10 sekundi i potom uključite uređaje sljedećim redom: bežični usmjernik, računalo ili pametni uređaj i zatim skener. Približite skener i računalo ili pametni uređaj bežičnom usmjerniku kako biste pospješili komunikaciju radiovalovima i zatim ponovno pokušajte odabrati mrežne postavke.



■ Uređaji ne mogu primiti signale bežičnog adaptera jer su previše razmaknuti.

Rješenja

Nakon približavanja računala ili pametnog uređaja i skenera bežičnom usmjerniku, isključite bežični usmjernik i zatim ga ponovno uključite.

Kod promjene bežičnog usmjernika postavke ne odgovaraju novom usmjerniku.

Rješenja

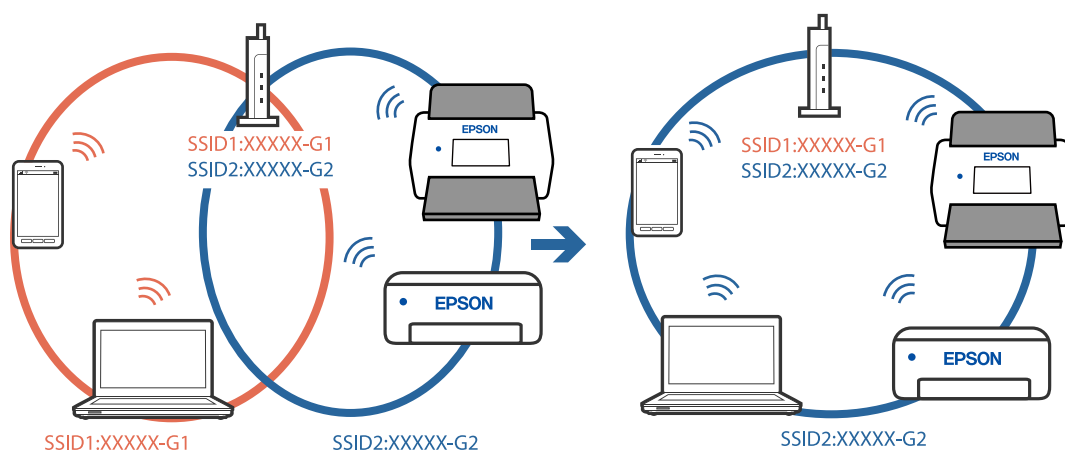
Ponovno odabiremo postavke veze kako bi odgovarale novom bežičnom usmjerniku.

Razlikuju se SSID-ovi spojeni preko računala ili pametnog uređaja.

Rješenja

Kada koristite više bežičnih usmjernika istovremeno ili kada bežični usmjernik ima više SSID-ova i uređaji se spoje na različite SSID-ove, ne možete se spojiti na bežični usmjernik.

Spojite računalo ili pametni uređaj na isti SSID na koji je spojen i skener.



Dostupan je odvajач privatnosti na bežičnom usmjerniku.

Rješenja

Većina bežičnih usmjernika ima značajku zaštite privatnosti koja blokira komunikaciju između povezanih uređaja. Ako ne možete komunicirati između skenera i računala ili pametnog uređaja čak i kada su spojeni na istu mrežu, onemogućite zaštitu privatnosti na bežičnom usmjerniku. Provjerite priručnik isporučen uz bežične usmjernike kako biste saznali više informacija.

IP adresa nije pravilno dodijeljena.

Rješenja

Skeneru je dodijeljena IP adresa 169.254.XXX.XXX uz podmrežnu masku 255.255.0.0; IP adresa možda nije ispravno dodijeljena.

Odaberite **Postavke > Postavke mreže > Napredno > TCP/IP** na upravljačkoj ploči skenera i zatim kliknite na IP adresu i podmrežnu masku dodijeljenu skeneru.

Ponovno pokrenite bežični pristupnik ili vratite mrežne postavke skenera na početne vrijednosti.

Postoji problem s mrežnim postavkama na računalu.

Rješenja

Pokušajte pristupiti web-stranici s vašeg računala kako biste se uvjerali da su ispravne mrežne postavke vašeg računala. Ako ne možete pristupiti web-stranicama, postoji problem s računalom.

Provjerite mrežnu vezu na računalu. Provjerite dokumentaciju isporučenu uz računalo kako biste saznali više informacija.

Skener je spojen Ethernetom koristeći uređaje koji podržavaju IEEE 802.3az (Energetski učinkoviti Ethernet).

Rješenja

Kada spojite skener preko Ethernet koristeći uređaje koji podržavaju IEEE 802.3az (Energetski učinkoviti Ethernet), mogu se pojaviti sljedeće poteškoće, ovisno o koncentratoru ili pristupniku koji koristite.

- Veza postaje nestabilna, a skener se uvijek iznova priključuje i isključuje.
- Ne može se spojiti na skener.
- Komunikacija se usporava.

Slijedite donje korake da biste onemogućili IEEE 802.3az za skener i zatim spojite.

1. Uklonite Ethernet kabel spojen na računalo i skener.
2. Kada je IEEE 802.3az aktiviran za računalo, deaktivirajte ga.
Provjerite dokumentaciju isporučenu uz računalo kako biste saznali više informacija.
3. Povežite računalo i skener izravno Ethernet kabelom.
4. Na skeneru provjerite mrežne postavke.
Odaberite **Postavke > Postavke mreže > Stanje mreže > Status ožičene LAN/Wi-Fi veze**.
5. Provjerite IP adresu skenera.
6. Na računalu pristupite dijelu Web Config.
Pokrenite web-preglednik, a zatim unesite IP adresu skenera.
[“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)
7. Odaberite karticu **Network > Wired LAN**.
8. Odaberite **OFF** za **IEEE 802.3az**.
9. Kliknite na **Next**.
10. Kliknite na **OK**.
11. Uklonite Ethernet kabel spojen na računalo i skener.
12. Ako ste deaktivirali IEEE 802.3az za računalo u koraku 2, aktivirajte ga.
13. Spojite Ethernet kabele koje ste uklonili u koraku 1 na računalo i skener.
Ako se problem i dalje javlja, uređaji osim skenera mogu uzrokovati problem.

Skener je isključen.

Rješenja

Provjerite je li skener uključen.

Pričekajte da lampica statusa prestane treptati što označava da je skener spreman za skeniranje.

Softver za postavljanje skenera

Web Config.	35
Epson Device Admin.	36

Web Config

Aplikacija Web Config se izvršava u web-preglednicima, kao što su Internet Explorer i Safari, na računalu. Možete potvrditi stanje skenera ili promijeniti postavke mrežne usluge i skenera. Budući da se skenerima pristupa i njima se upravlja izravno iz mreže, prikladan je za postavljanje jednog po jednog skenera. Za korištenje aplikacije Web Config potrebno je povezati računalo na istu mrežu na kojoj je skener.

Podržani su slijedeći preglednici.

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

* Koristite najnoviju inačicu.

Pokretanje programa Web Config u internetskom pregledniku

1. Provjerite IP adresu skenera.

Odaberite **Postavke > Postavke mreže > Stanje mreže** na upravljačkoj ploči skenera. Zatim odaberite aktivan status načina povezivanja (**Status ožičene LAN/Wi-Fi veze** ili **Wi-Fi Direct status**) da biste potvrdili IP adresu skenera.

2. Na računalu ili pametnom uređaju pokrenite web-preglednik i zatim unesite IP adresu skenera.

Format:

IPv4: http://IP adresa skenera/

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

Primjeri:

IPv4: http://192.168.100.201/

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

Napomena:

Budući da skener koristi samostalno potpisani certifikat kod pristupa HTTPS-u, u pregledniku je prikazano upozorenje kada pokrenete Web Config; to ne ukazuje na problem i stoga možete bezbrižno zanemariti.

3. Prijavite se kao administrator da biste promijenili postavke skeniranja.

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

Napomena:

- U nastavku se navode početne vrijednosti informacija Web Config administratora.

·Korisničko ime: nijedno (prazno)

·Lozinka: serijski broj skenera

Kako biste pronašli serijski broj, provjerite naljepnicu na stražnjoj strani skenera.

- Ako je **Administrator Logout** prikazan u gornjem desnom kutu zaslona, već ste se prijavili kao administrator.

Pokretanje usluge Web Config u sustavu Windows

Kod spajanja računala na skener pomoću WSD-a slijedite donje korake kako biste pokrenuli Web Config.

1. Otvorite popis skenera na računalu.

Windows 10

Kliknite na gumb Start i zatim odaberite **Windows sustav > Upravljačka ploča > Prikaz uređaja i pisača** pod stavkom **Hardver i zvuk**.

Windows 8.1/Windows 8

Odaberite **Radna površina > Postavke > Upravljačka ploča > Prikaz uređaja i pisača** pod stavkom **Hardver i zvuk** (ili **Hardver**).

Windows 7

Kliknite na gumb Start i odaberite **Upravljačka ploča > Prikaz uređaja i pisača** u postavci **Hardver i zvuk**.

2. Desnom tipkom miša kliknite na ikonu skenera i odaberite **Svojstva**.

3. Odaberite karticu **Web-servis** i kliknite na URL.

Budući da skener koristi samostalno potpisani certifikat kod pristupa HTTPS-u, u pregledniku je prikazano upozorenje kada pokrenete Web Config; to ne ukazuje na problem i stoga možete bezbrižno zanemariti.

Napomena:

U nastavku se navode početne vrijednosti informacija Web Config administratora.

·Korisničko ime: nijedno (prazno)

·Lozinka: serijski broj skenera

Kako biste pronašli serijski broj, provjerite naljepnicu na stražnjoj strani skenera.

Ako je **Administrator Logout** prikazan u gornjem desnom kutu zaslona, već ste se prijavili kao administrator.

Epson Device Admin

Epson Device Admin je višenamjenska aplikacija koja vam omogućuje upravljanje uređajima na mreži.

Možete koristiti predloške konfiguracije za primjenu objedinjenih postavki na više skenera na mreži, što ga čini prikladnim za instaliranje i upravljanje više skenera.

Možete preuzeti Epson Device Admin s mrežne stranice za podršku tvrtke Epson. Za pojedinosti o tome kako koristiti ovu aplikaciju, pogledajte dokumentaciju ili pomoć za Epson Device Admin.

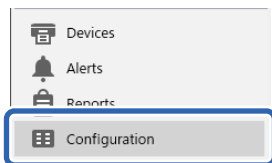
Predložak konfiguracije

Izrada predložka konfiguracije

Izradite novi predložak konfiguracije.

1. Pokrenite Epson Device Admin.

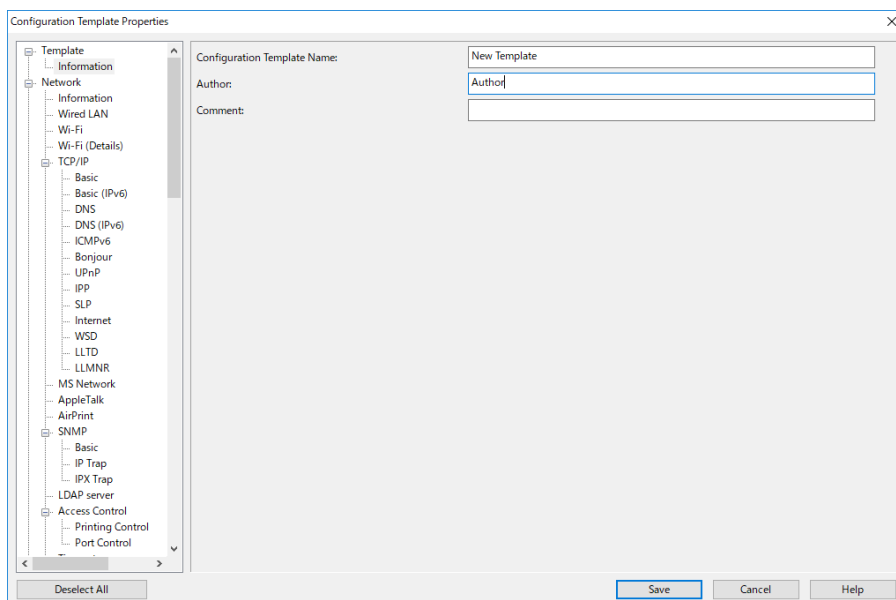
2. Odaberite **Configuration** na bočnoj traci izbornika zadatka.



3. Odaberite **New** u izborniku vrpce.



4. Postavite svaku stavku.



Stavka	Pojašnjenje
Configuration Template Name	Naziv predložka konfiguracije. Unesite maksimalno 1024 znakova u Unicode kodu (UTF-8).
Author	Podaci o kreatoru predložka. Unesite maksimalno 1024 znakova u Unicode kodu (UTF-8).
Comment	Unesite proizvoljne podatke. Unesite maksimalno 1024 znakova u Unicode kodu (UTF-8).

5. Odaberite stavke koje želite postaviti na lijevoj strani.

Napomena:

Kliknite stavke izbornika s lijeve strane da biste se prebacili na svaki zaslon. Postavljena vrijednost se zadržava ako promijenite zaslon, ali ne i ako ga poništite. Kada završite sa svim postavkama, kliknite **Save**.

Primjena predložka konfiguracije

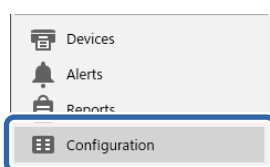
Primijenite spremljeni predložak konfiguracije na skener. Primijenjene su stavke odabrane na predlošku. Ako ciljni skener nema odgovarajuću funkciju, ona se ne primjenjuje.

Napomena:

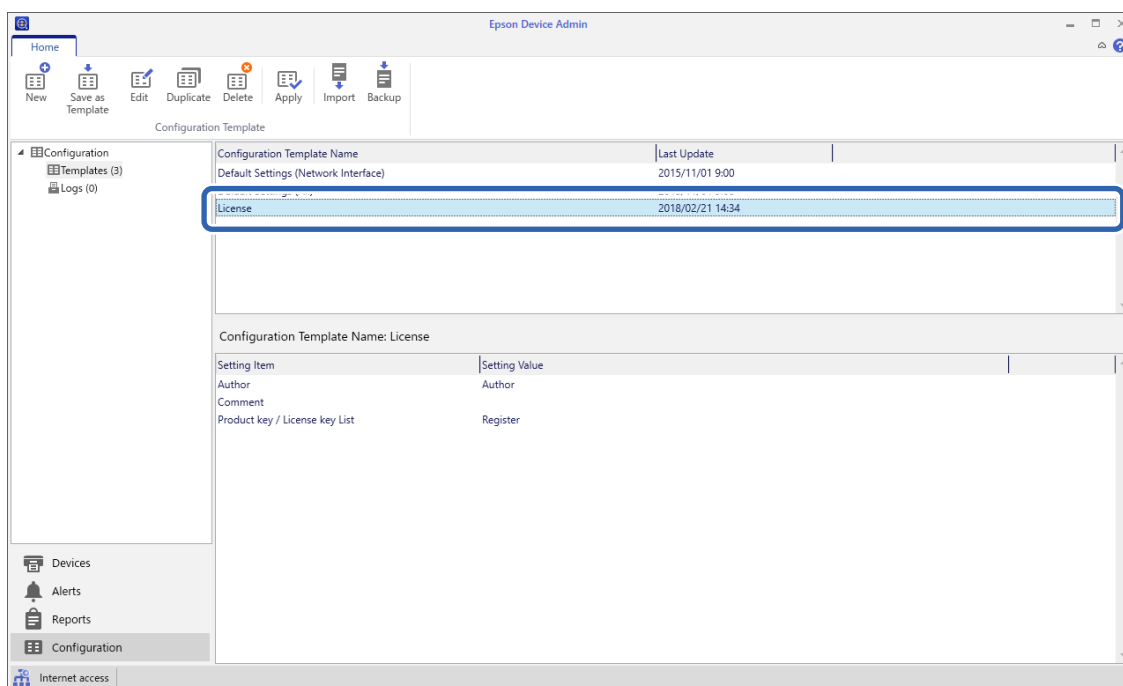
Kada je administratorska lozinka postavljena na skener, unaprijed konfigurirajte lozinku.

1. U izborniku vrpce na zaslonu Popis uređaja odaberite **Options** > **Password manager**.
2. Odaberite **Enable automatic password management** a zatim kliknite na **Password manager**.
3. Odaberite odgovarajući skener, a zatim kliknite **Edit**.
4. Unesite lozinku, a zatim kliknite na **OK**.

1. Odaberite **Configuration** na bočnoj traci izbornika zadatka.



2. Odaberite predložak konfiguracije iz kojeg se želite primijeniti **Configuration Template Name**.



3. Kliknite **Apply** u izborniku vrpce.
Prikazuje se zaslon za odabir uređaja.

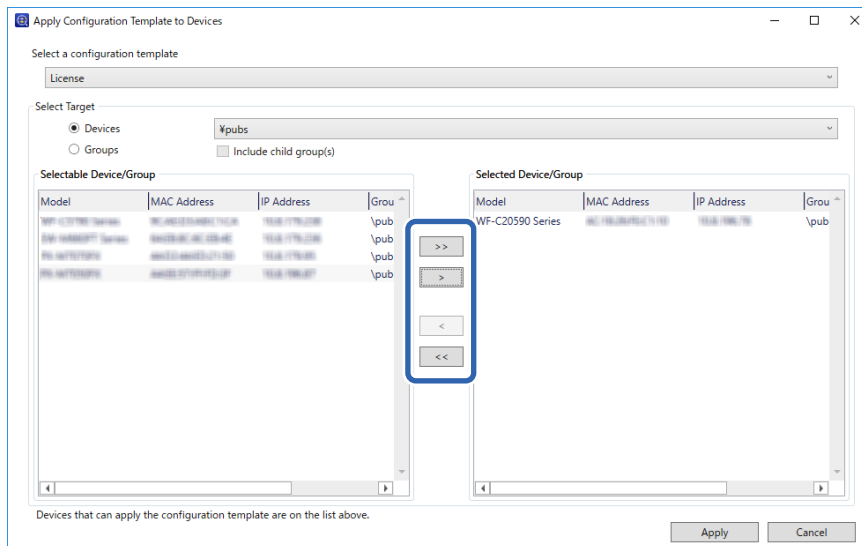


4. Odaberite predložak konfiguracije koji želite primijeniti.

Napomena:

- Kada odaberete **Devices** i grupe koje sadrže uređaje iz padajućeg izbornika, prikazan je svaki uređaj.
- Grupe se prikazuju kada odaberete **Groups**. Odaberite **Include child group(s)** za automatski odabir podređenih grupa unutar odabrane grupe.

5. Premjestite skener ili grupe na koje želite primijeniti predložak **Selected Device/Group**.



6. Kliknite na **Apply**.

Prikazuje se zaslon za potvrdu za konfiguracijski predložak koji treba primijeniti.

7. Kliknite na **OK** za primjenu predloška konfiguracije.

8. Kada se prikaže poruka koja vas obavještava da je postupak dovršen, kliknite **OK**.

9. Kliknite na **Details** i provjerite informacije.

Kada je prikazan u stavkama koje ste prijavili, aplikacija je uspješno dovršena.

10. Kliknite na **Close**.

Potrebne postavke skeniranja

Konfiguriranje poslužitelja e-pošte.	41
Postavljanje dijeljene mrežne mape.	44
Omogućavanje dostupnosti kontakata.	61
Uporaba opcije Document Capture Pro Server.	71
Postavljanje značajke AirPrint.	71
Problemi kod pripremanja mrežnog skeniranja.	72

Konfiguriranje poslužitelja e-pošte

Postavite poslužitelja e-pošte u aplikaciji Web Config.

Kada skener može slati e-poštu odabiranjem poslužitelja e-pošte, moguće je učiniti sljedeće.

- Prenijeti rezultate skeniranja pomoću e-pošte
- Primiti obavijest e-poštom sa skenera

Prije postavljanja provjerite u nastavku.

- Skener je povezan s mrežom koja ima pristup poslužitelju e-pošte.
- Informacije o postavljanju e-pošte na računalu koji koristi istog poslužitelja e-pošte kao skener.

Napomena:

- Kada koristite poslužitelj e-pošte na internetu provjerite informacije postavke preko pružatelja usluge ili web-stranice.
- Možete odrediti poslužitelja e-pošte na upravljačkoj ploči. Pristup je opisan u nastavku.

Postavke > Postavke mreže > Napredno > Poslužitelj za e-poštu > Postavke poslužitelja

1. Pristupite aplikaciji Web Config i odaberite karticu **Network > Email Server > Basic**.
2. Unesite vrijednost svake stavke.
3. Odaberite **OK**.
Prikazane su postavke koje ste odabrali.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Stavke postavljanja poslužitelja e-pošte

Stavke	Postavke i pojašnjenja	
Authentication Method	Odredite metodu autentifikacije za pristup skenera poslužitelju e-pošte.	
	Off	Autentifikacija je onemogućena prilikom komuniciranja s poslužiteljem e-pošte.
	SMTP AUTH	Zahtijeva se da poslužitelj e-pošte podržava SMTP autentifikaciju.
	POP before SMTP	Kod odabira ove metode konfigurirajte POP3 poslužitelj.
Authenticated Account	Ako ste odabrali SMTP AUTH ili POP before SMTP kao Authentication Method , unesite naziv autentificiranog računa sastavljenog od 0 do 255 znakova u ASCII kodu (0x20–0x7E).	
Authenticated Password	Ako ste odabrali SMTP AUTH ili POP before SMTP kao Authentication Method , unesite lozinku provjerene autentičnosti od 0 do 20 znakova u ASCII kodu (0x20–0x7E).	
Sender's Email Address	Unesite adresu e-pošte pošiljatelja. Unesite od 0 do 255 znakova u ASCII kodu (0x20–0x7E), osim : () < > [] ; ¥. Točka „.” ne može biti prvi znak.	

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

Provjera veze s poslužiteljem e-pošte

Možete provjeriti vezu s poslužiteljem e-pošte provođenjem provjere veze.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network > Email Server > Connection Test**.
2. Odaberite **Start**.

Započet će test veze s poslužiteljem pošte. Nakon provjere je prikazan izvještaj o provjeri.

Napomena:

Također možete odabrati vezu s poslužiteljem e-pošte na upravljačkoj ploči skenera. Pristup je opisan u nastavku.

Postavke > Postavke mreže > Napredno > Poslužitelj za e-poštu > Provjera veze

Reference testa veze s poslužiteljem e-pošte

Poruke	Uzrok
Connection test was successful.	Ova poruka pojavljuje se kod uspješnog povezivanja s poslužiteljem.
SMTP server communication error. Check the following. - Network Settings	Ova poruka pojavljuje se u sljedećem slučaju <ul style="list-style-type: none"> <input type="checkbox"/> Skener nije spojen na mrežu <input type="checkbox"/> Prekid rada poslužitelja SMTP <input type="checkbox"/> Mrežna veza je prekinuta tijekom komunikacije <input type="checkbox"/> Primljeni nepotpuni podaci

Poruke	Uzrok
POP3 server communication error. Check the following. - Network Settings	Ova poruka pojavljuje se u sljedećem slučaju <input type="checkbox"/> Skener nije spojen na mrežu <input type="checkbox"/> Prekid rada poslužitelja POP3 <input type="checkbox"/> Mrežna veza je prekinuta tijekom komunikacije <input type="checkbox"/> Primljeni nepotpuni podaci
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Ova poruka pojavljuje se u sljedećem slučaju <input type="checkbox"/> Nije uspjelo povezivanje na poslužitelj DNS <input type="checkbox"/> Pogrešna rezolucija naziva poslužitelja SMTP
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Ova poruka pojavljuje se u sljedećem slučaju <input type="checkbox"/> Nije uspjelo povezivanje na poslužitelj DNS <input type="checkbox"/> Pogrešna rezolucija naziva poslužitelja za POP3
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka pojavljuje se kod neuspjele provjere autentičnosti poslužitelja SMTP.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ova poruka pojavljuje se kod neuspjele provjere autentičnosti poslužitelja POP3.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Ova poruka pojavljuje se kada pokušavate komunicirati s nepodržanim protokolima.
Connection to SMTP server failed. Change Secure Connection to None.	Ova poruka pojavljuje se kod SMTP nepodudarnosti između poslužitelja i klijenskog računala ili kada poslužitelj ne podržava SMTP sigurnu vezu (SSL veza).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Ova poruka pojavljuje se kod SMTP nepodudarnosti između poslužitelja i klijenskog računala ili kada poslužitelj zatraži korištenje SSL/TLS veze za SMTP sigurnu vezu.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Ova poruka pojavljuje se kod SMTP nepodudarnosti između poslužitelja i klijenskog računala ili kada poslužitelj zatraži korištenje STARTTLS veze za SMTP sigurnu vezu.
The connection is untrusted. Check the following. - Date and Time	Ova poruka pojavljuje se ako je pogrešna postavka datuma i vremena skenera ili je istekao certifikat.
The connection is untrusted. Check the following. - CA Certificate	Ova poruka pojavljuje se kada skener nema korijenski certifikat koji odgovara poslužitelju ili ako nije uvezen CA Certificate.
The connection is not secured.	Ova poruka pojavljuje se kada je oštećen primljeni certifikat.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Ova poruka pojavljuje se u slučaju nepodudarnosti načina provjere autentičnosti između poslužitelja i klijenta. Poslužitelj podržava SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Ova poruka pojavljuje se u slučaju nepodudarnosti načina provjere autentičnosti između poslužitelja i klijenta. Poslužitelj ne podržava SMTP AUTH.

Poruke	Uzrok
Sender's Email Address is incorrect. Change to the email address for your email service.	Ova poruka pojavljuje se ako je navedena adresa e-pošte pogrešna.
Cannot access the product until processing is complete.	Ova poruka pojavljuje se kada je skener zauzet.

Postavljanje dijeljene mrežne mape

Odredite dijeljenu mrežnu mapu da biste spremili skeniranu sliku.

Kod spremanja datoteke u mapu, skener se prijavljuje kao korisnik računala na kojem je kreirana mapa.

Kreiranje zajedničke mape

Povezane informacije

- ➔ [“Prije kreiranja zajedničke mape” na strani 44](#)
- ➔ [“Provjera profila mreže” na strani 44](#)
- ➔ [“Lokacija na kojoj se izrađuje zajednička mapa i primjer sigurnosti” na strani 45](#)
- ➔ [“Dodavanje grupe ili korisnika kojima je odobren pristup” na strani 58](#)

Prije kreiranja zajedničke mape

Prije kreiranja zajedničke mape, provjerite sljedeće.

- Skener je spojen na mrežu gdje se može pristupiti računalu u kojem ćete kreirati zajedničku mapu.
- Znak s više bajtova nije uključen u ime računala u kojem će se kreirati zajednička mapa.



Važno:

Ako je u ime računala uključen znak s više bajta, možda neće uspjeti spremanje datoteke u zajedničku mapu.


U tome slučaju promijenite računalo na ono koje u imenu nema znak s više bajtova ili promijenite ime računala.

Ako mijenjate ime računala, pobrinite se da to unaprijed potvrdite s administratorom jer može utjecati na neke postavke, kao što su upravljanje računalom, pristup izvorima itd.

Provjera profila mreže

Na računalu na kojem će se izraditi zajednička mapa provjerite je li dostupno dijeljenje mape.

1. Prijavite se na računalo gdje će biti kreirana zajednička mapa preko korisničkog računa administratora.
2. Odaberite **Upravljačka ploča > Mreža i internet > Centar za mreže i zajedničko korištenje**.

3. Kliknite na **Promijeni napredne postavke dijeljenja** i zatim na  za profil dok je (**trenutačni profil**) u prikazanim mrežnim profilima.
4. Provjerite je li odabrano **Uključi zajedničko korištenje datoteka i pisača** u **Zajedničko korištenje datoteka i pisača**.
Ako je već odabrano, kliknite na **Otkazi** i zatvorite prozor.
Kada mijenjate postavke, kliknite na **Spremi promjene** i zatvorite prozor.

Lokacija na kojoj se izrađuje zajednička mapa i primjer sigurnosti

Ovisno o lokaciji gdje je izrađena zajednička mapa, razlikuje se sigurnost i praktičnost.

Kako biste zajedničkoj mapi upravljali preko skenera ili drugih računala, potrebna su sljedeće dozvole čitanja i mijenjanja mape.

Kartica **Dijeljenje > Napredno dijeljenje > Dozvole**

Time se upravlja dozvolom pristupu mreži zajedničke mape.

Pristupite dozvoli u kartici **Sigurnost**

Time se upravlja dozvolom pristupu mreži i lokalnom pristupu zajedničke mape.

Kada na zajedničkoj mapi koja je izrađena na radnoj površini postavite **Svi**, kao primjer izrade zajedničke mape, svi korisnici koji mogu pristupiti računalu imaju dozvolu pristupa.

Međutim, korisnik koji nema dozvolu ne može im pristupiti jer je radna površina (mapa) pod kontrolom korisničke mape te se sigurnosne postavke korisničke mape prenose na nju. Korisnik koji ima dozvolu pristupa na kartici **Sigurnost** (korisnik prijavljen i u ovom slučaju je administrator) može koristiti mapu.

U nastavku se navode upute za izradu točne lokacije.

Ovaj primjer odnosi se na kreiranje mape „scan_folder”.

Povezane informacije

- ➔ [“Primjer konfiguracije za poslužitelje datoteke” na strani 45](#)
- ➔ [“Primjer konfiguracije za osobno računalo” na strani 52](#)

Primjer konfiguracije za poslužitelje datoteke

Ovo objašnjenje je primjer izrade zajedničke mape u korijenu upravljačkog programa na zajedničkom računalu, kao što je poslužitelja datoteke pod određenim uvjetima.

Pristup korisnicima koje se može kontrolirati, kao što je netko tko ima istu domenu kao računalo za izradu zajedničke mape, mogu pristupiti zajedničkoj mapi.

Postavite ovu konfiguraciju kad dozvoljavate svim korisnicima da čitaju i pišu u zajedničkoj mapi na računalu, kao što je poslužitelj datoteke i zajedničko računalo.

- Mjesto za izradu zajedničke mape: korijen upravljačkog programa
- Staza mape: C:\scan_folder
- Dozvola pristupa preko mreže (dijeljene dozvole): svatko
- Dozvola pristupa na datotečnom sustavu (Sigurnost): autorizirani korisnici

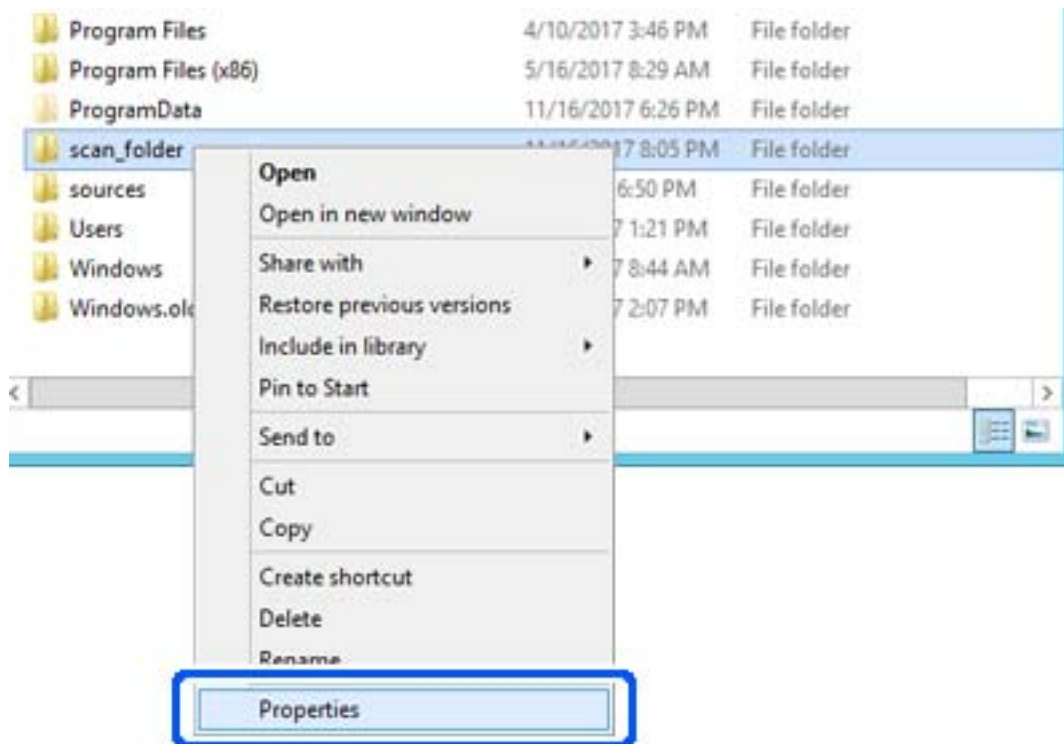
1. Prijavite se na računalo gdje će biti kreirana zajednička mapa preko korisničkog računa administratora.

2. Pokrenite Explorer.

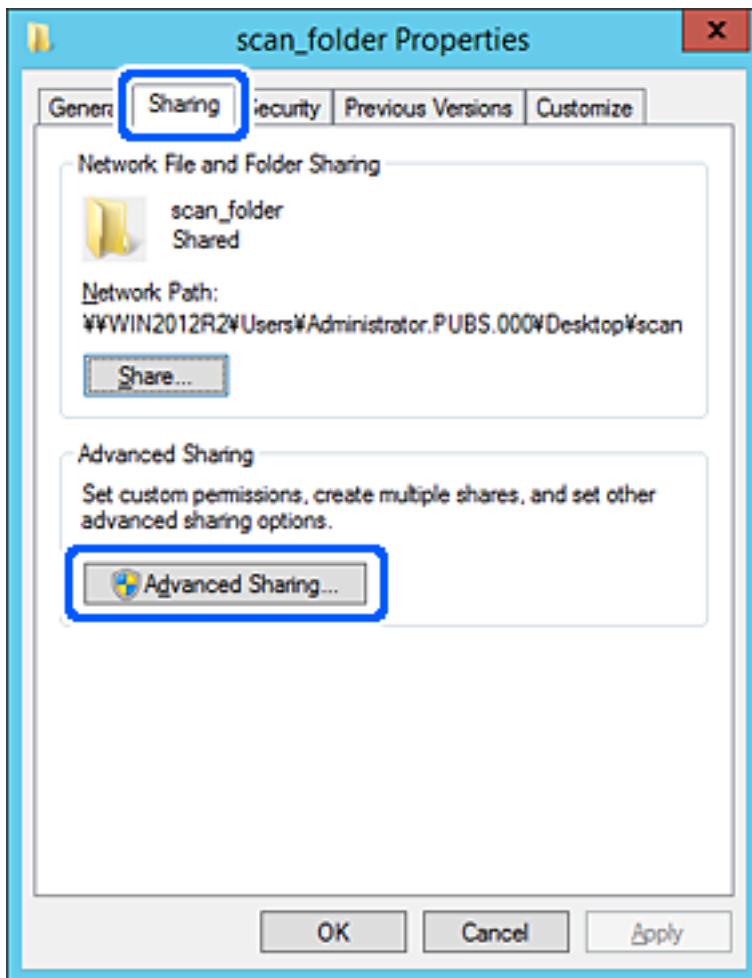
3. Izradite mapu na korijenu upravljačkog sustava i dajte joj naziv „scan_folder”.

Kod naziva mape unesite između 1 i 12 brojki i slova. Ako se prekorači ograničenje broja znakova u nazivu mape, možda joj nećete moći pristupiti normalno preko promijenjenog okruženja.

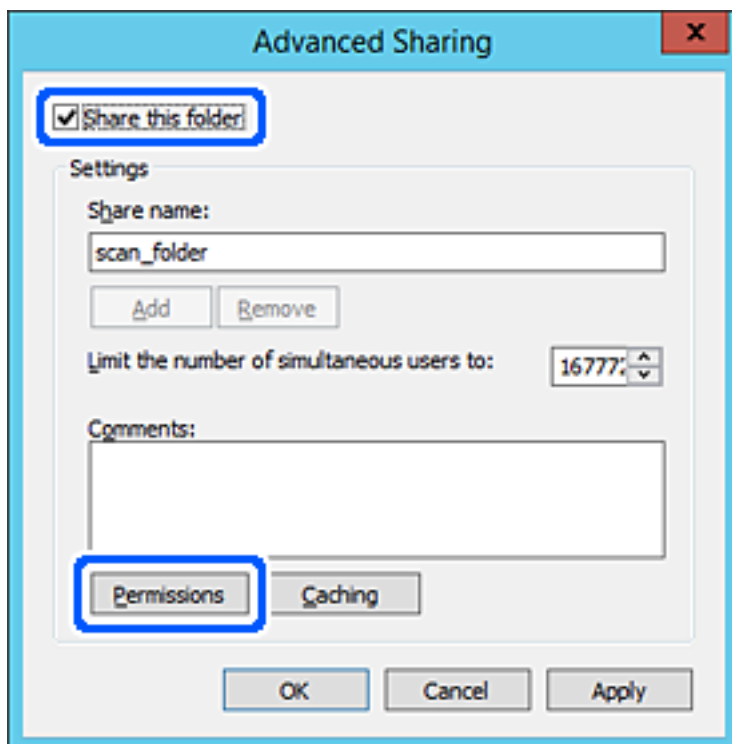
4. Desnim klikom kliknite na mapu i odaberite **Svojstva**.



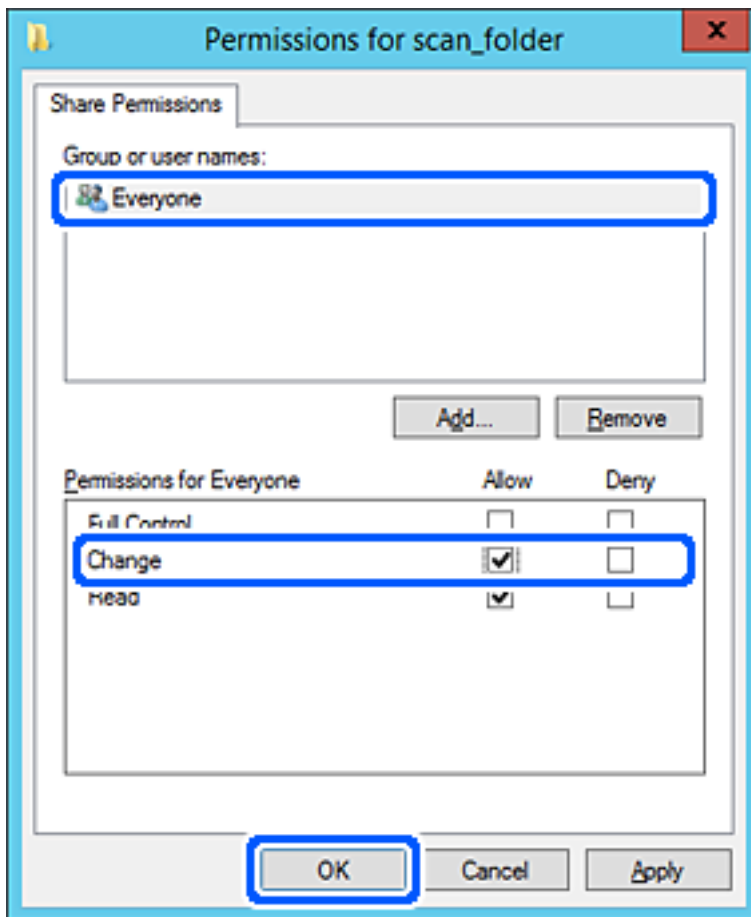
5. Kliknite na **Dodatno zajedničko korištenje** na kartici **Zajedničko korištenje**.



6. Odaberite **Dijeli ovu mapu**, a zatim kliknite na **Dozvole**.

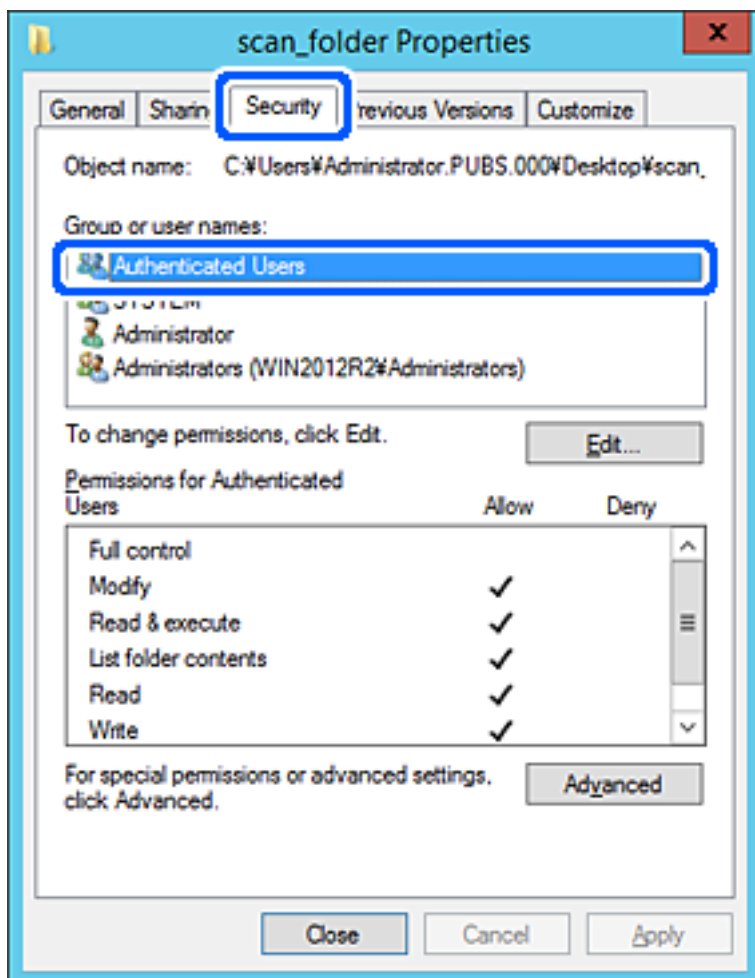


7. Odaberite skupinu **Svatko** pod **Nazivi grupe ili korisnička imena**, odaberite **Omogući** za **Promijeni** i zatim kliknite na **OK**.



8. Kliknite na **OK**.

9. Odaberite karticu **Sigurnost** i zatim **Autorizirani korisnici** pod **Nazivi grupe ili korisnička imena**.

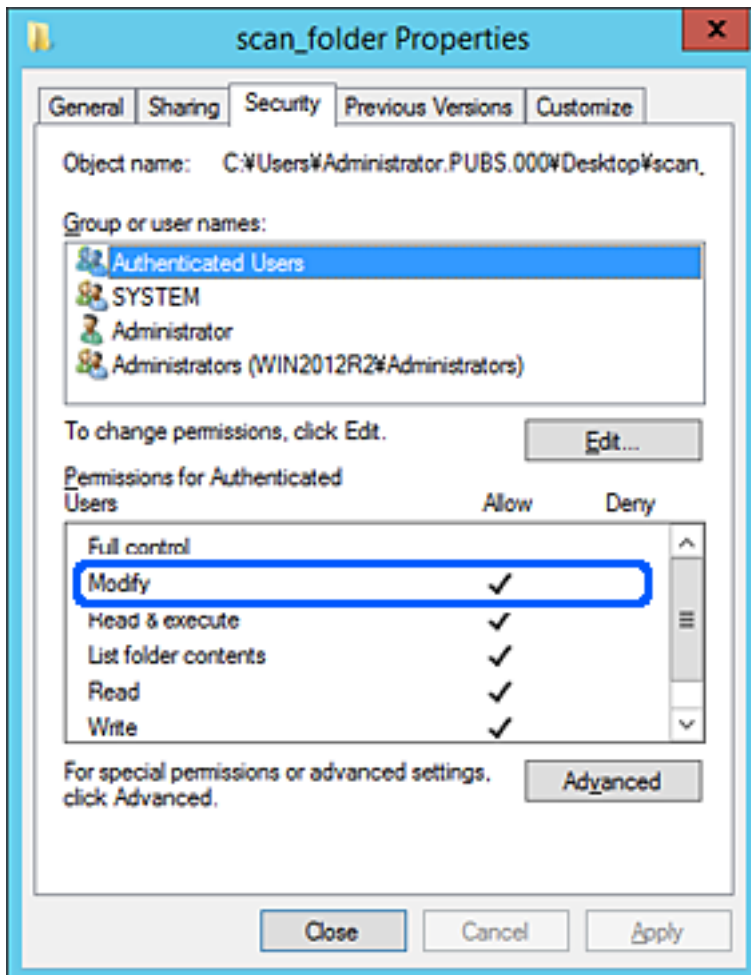


„Autorizirani korisnici” je posebna grupa koja uključuje sve korisnike koji se mogu prijaviti na domenu ili računalo. Ova grupa je prikazana samo kad je mapa izrađena odmah ispod korijenske mape.

Ako nije prikazana, možete je dodati klikanjem na **Uredi**. Za više pojedinosti pogledajte povezane informacije.

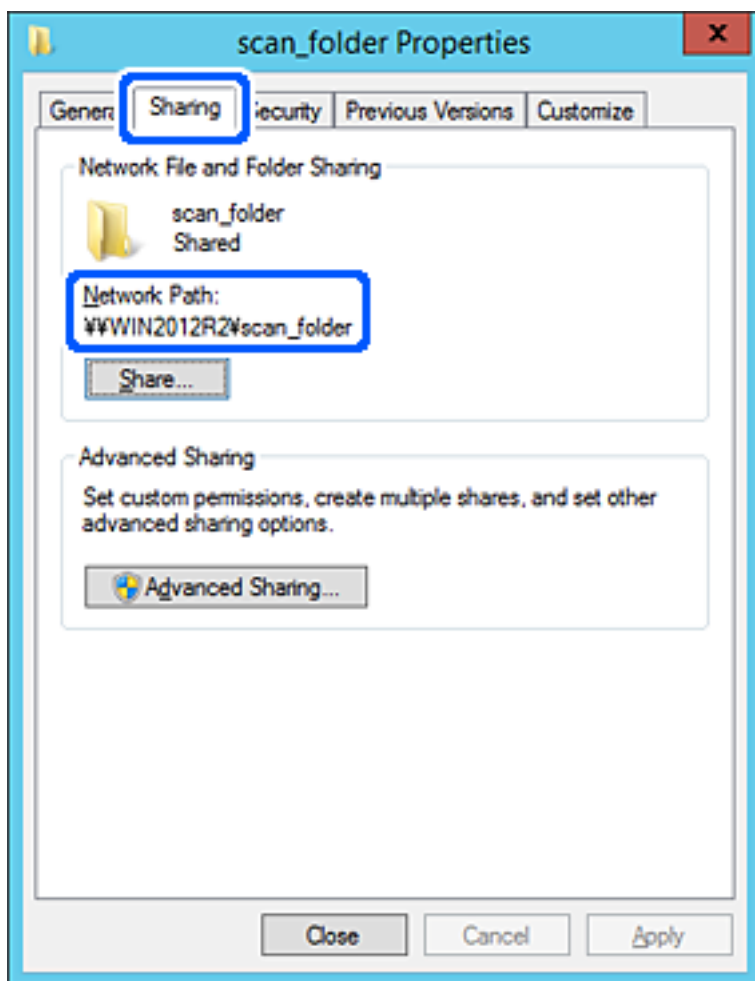
10. Provjerite je li odabrano **Dopusti** na **Izmijeni** u **Dozvole za autorizirane korisnike**.

Ako već niste, odaberite **Autorizirani korisnici**, kliknite na **Uredi**, odaberite **Dopusti** na **Izmijeni** u **Dozvole za autorizirane korisnike** i kliknite na **OK**.



11. Odaberite karticu **Dijeljenje**.

Prikazana je putanja mreže dijeljene mape. To se koristi prilikom registracije s kontaktima pisača. Zapišite je.



12. Kliknite na **OK** ili **Zatvori** kako biste zatvorili zaslon.

Provjerite ima li datoteka dozvolu za pisanje i čitanje na zajedničkoj mapi s računala na istoj domeni.

Povezane informacije

- ➔ “Dodavanje grupe ili korisnika kojima je odobren pristup” na strani 58
- ➔ “Registracija odredišta u kontaktima koristeći Web Config” na strani 62

Primjer konfiguracije za osobno računalo

Ovo objašnjenje je primjer izrade zajedničke mape na radnoj površini korisnika koji je trenutno prijavljen na računalu.

Korisnik koji se prijavljuje na računalo i ima administratorska prava može pristupiti mapi na radnoj površini i mapi s dokumentom koji se nalazi u mapi korisnika.

Postavite ovu konfiguraciju kada NE dozvoljavate čitanje i pisanje drugim korisnicima na zajedničkoj mapi na osobnom računalu.

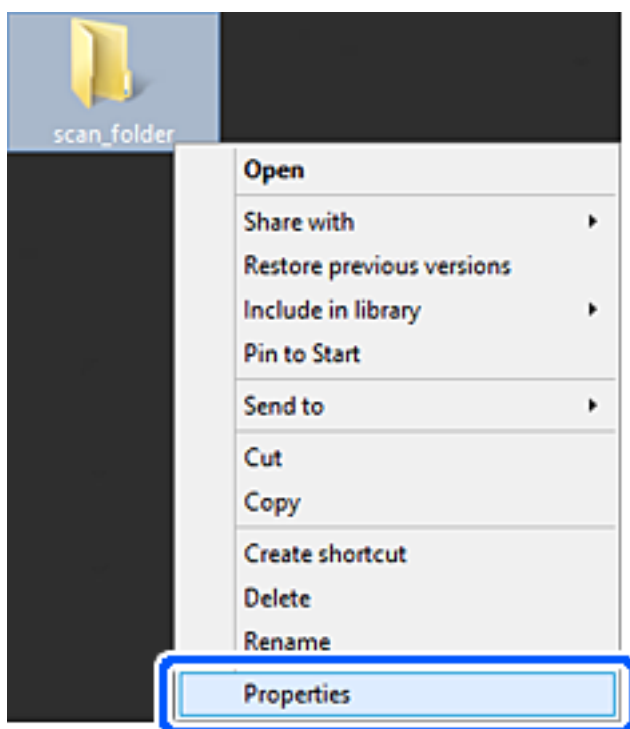
- Mjesto za izradu zajedničke mape: radna površina

- Putanja mape: C:\Users\xxxx\Desktop\scan_folder
- Dozvola pristupa preko mreže (dijeljene dozvole): svatko
- Dozvola pristupa na datotečnom sustavu (Sigurnost): nemojte dodavati ili dodavati imena Korisnika/Grupe za dozvolu pristupa

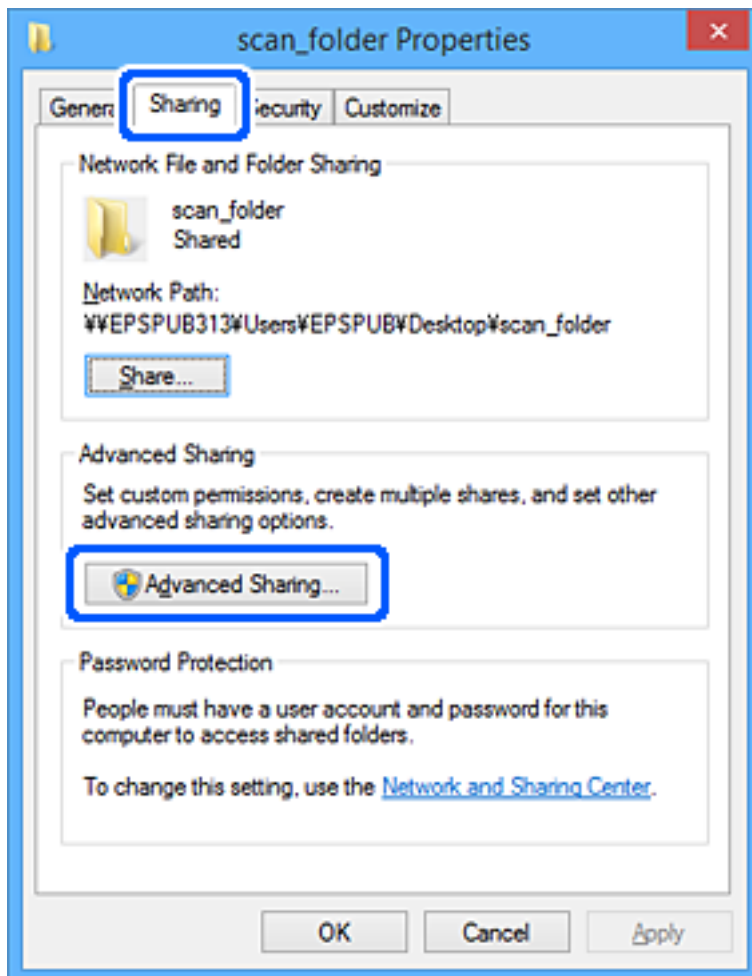
1. Prijavite se na računalo gdje će biti kreirana zajednička mapa preko korisničkog računa administratora.
2. Pokrenite Explorer.
3. Izradite mapu na radnoj površini i dajte joj ime „scan_folder”.

Kod naziva mape unesite između 1 i 12 brojki i slova. Ako se prekorači ograničenje broja znakova u nazivu mape, možda joj nećete moći pristupiti normalno preko promijenjenog okruženja.

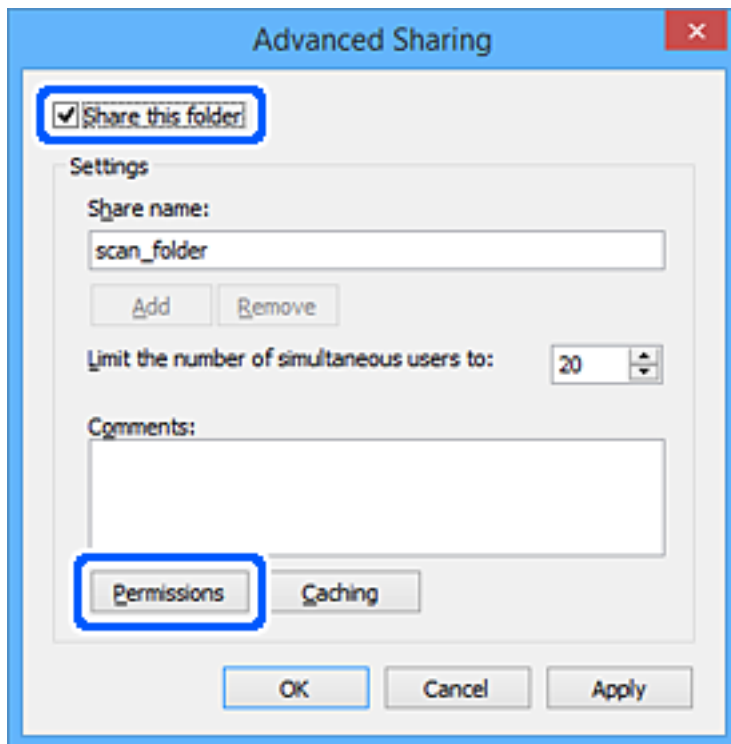
4. Desnim klikom kliknite na mapu i odaberite **Svojstva**.



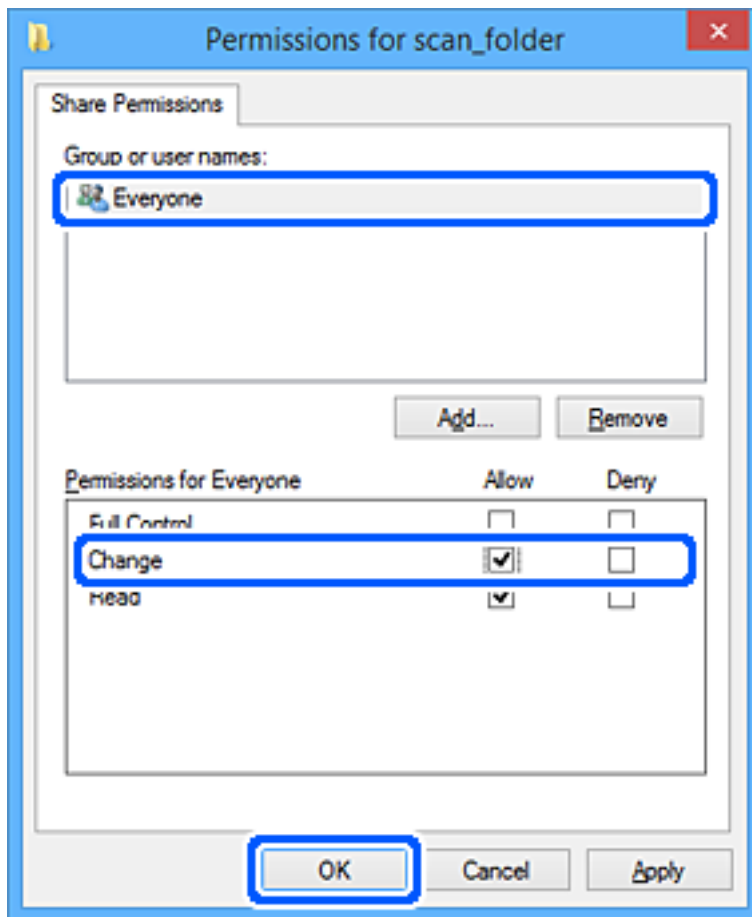
5. Kliknite na **Dodatno zajedničko korištenje** na kartici **Zajedničko korištenje**.



6. Odaberite **Dijeli ovu mapu**, a zatim kliknite na **Dozvole**.

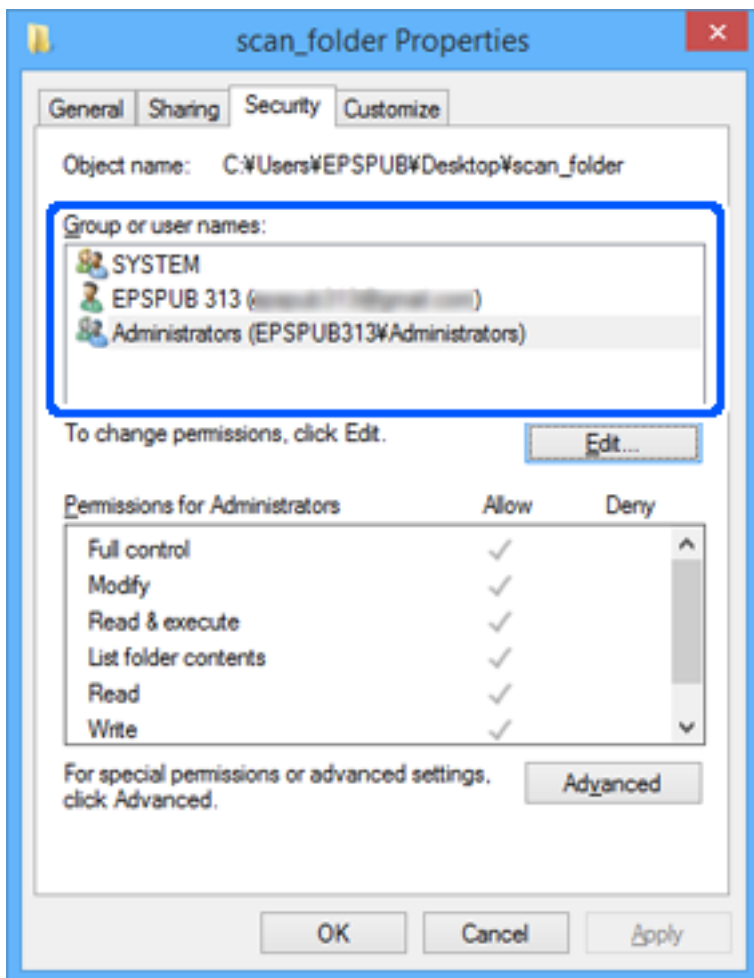


7. Odaberite skupinu **Svatko** pod **Nazivi grupe ili korisnička imena**, odaberite **Omogući** za **Promijeni** i zatim kliknite na **OK**.



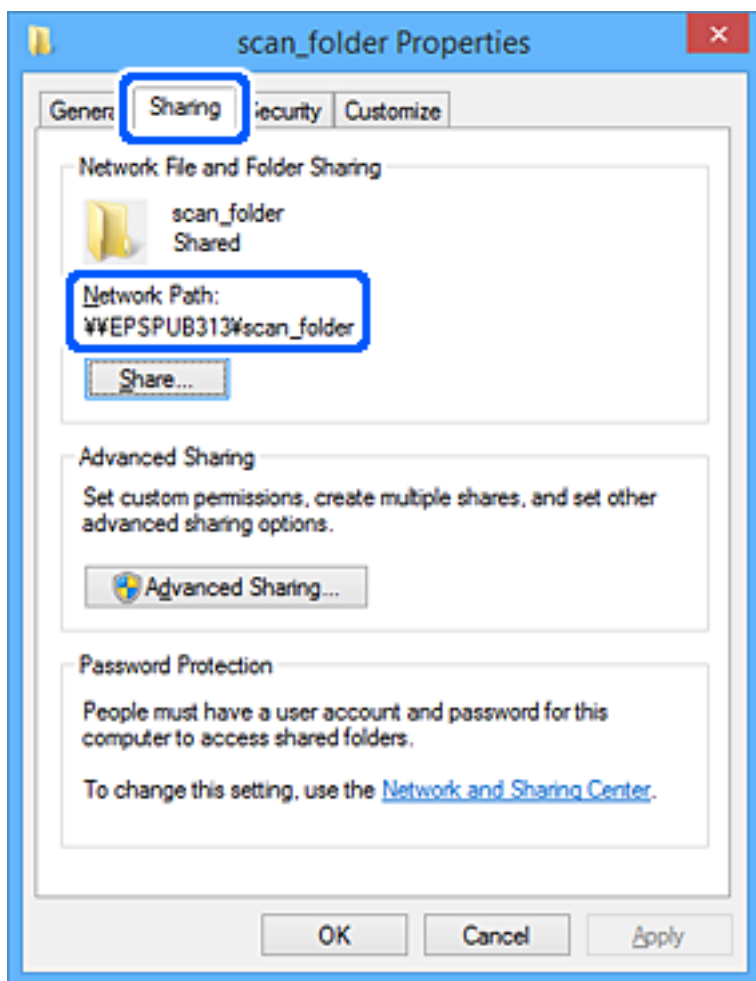
8. Kliknite na **OK**.
9. Odaberite karticu **Sigurnost**.
10. Provjerite grupu ili korisnika pod **Nazivi grupe ili korisnička imena**.
Grupa ili korisnik koji su tu prikazani mogu pristupiti zajedničkoj mapi.
U tom slučaju, korisnik koji se prijavi na ovo računalo i Administrator mogu pristupiti zajedničkoj mapi.

Ako je potrebno, dodajte dozvolu pristupa. Možete je dodati klikanjem na **Uredi**. Za više pojedinosti pogledajte povezane informacije.



11. Odaberite karticu **Dijeljenje**.

Prikazana je putanja mreže dijeljene mape. To se koristi prilikom registracije s kontaktima pisača. Zapišite je.



12. Kliknite na **OK** ili **Zatvori** kako biste zatvorili zaslon.

Provjerite ima li datoteka dozvolu za pisanje i čitanje na zajedničkoj mapi s računala korisnika ili grupa s dozvolom pristupa.

Povezane informacije

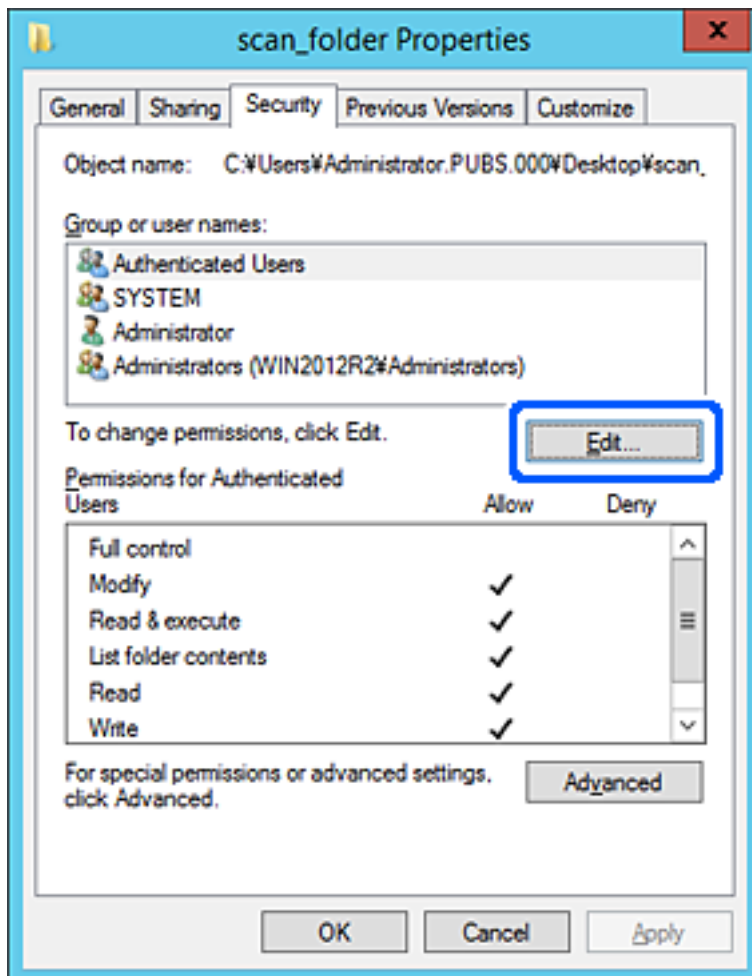
- ➔ “Dodavanje grupe ili korisnika kojima je odobren pristup” na strani 58
- ➔ “Registracija odredišta u kontaktima koristeći Web Config” na strani 62

Dodavanje grupe ili korisnika kojima je odobren pristup

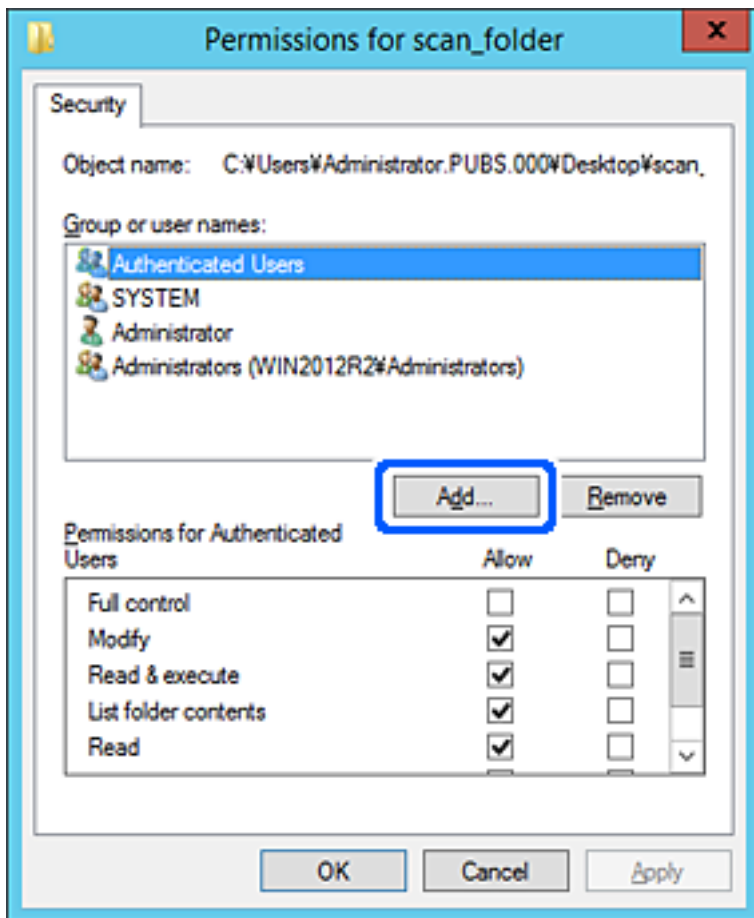
Možete dodati grupu ili korisnika kojima je odobren pristup.

1. Desnim klikom kliknite na mapu i odaberite **Svojstva**.
2. Odaberite karticu **Sigurnost**.

3. Kliknite **Uredi**.



4. Kliknite Dodaj pod Nazivi grupe ili korisnička imena.



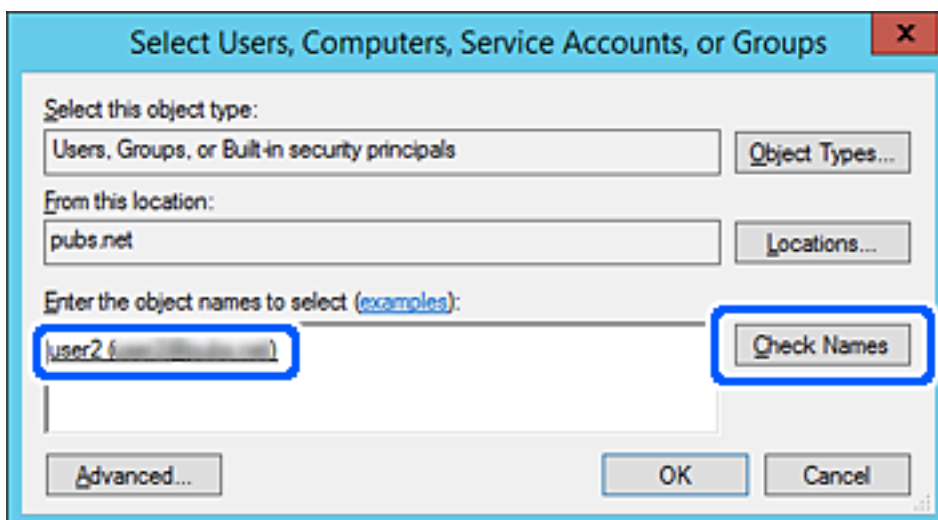
5. Unesite ime grupe ili korisnika kojima želite dozvoliti pristup i kliknite **Provjeri imena**.

Ime je potcrtano.

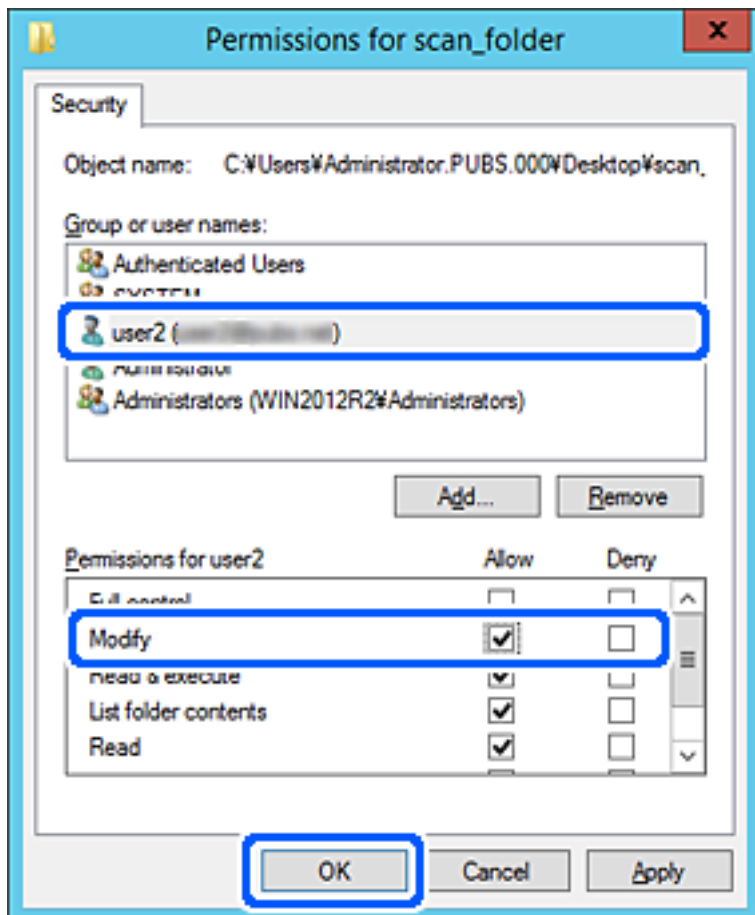
Napomena:

Ako ne znate puno ime grupe ili korisnika, unesite dio imena i kliknite **Provjeri imena**. Prikazuju se imena grupe ili korisnika koji odgovaraju dijelu imena i zatim s popisa možete odabrati puno ime.

Ako odgovara samo jedno ime, u dijelu **Unesite ime predmeta za odabir** bit će prikazano potcrtano puno ime.



- Kliknite **U redu**.
- Na zaslonu Dozvole odaberite korisničko ime uneseno pod **Nazivi grupe ili korisnička imena**, odaberite dozvolu pristupa pod **Izmijeni** i kliknite **U redu**.



- Kliknite **U redu** ili **Zatvori** kako biste zatvorili zaslon.
Provjerite ima li datoteka dozvolu za pisanje i čitanje na zajedničkoj mapi s računala korisnika ili grupa s dozvolom pristupa.

Omogućavanje dostupnosti kontakata

Registriranje odredišta na popisu kontakata skenera omogućava vam jednostavan unos odredišta kod skeniranja.

Možete registrirati sljedeće tipove odredišta na popisu kontakata. Možete registrirati ukupno 300 unosa.

Napomena:

Također možete koristiti LDAP poslužitelj (LDAP pretraživanje) za unos odredišta.

E-pošta	Odredište e-pošte. Prethodno trebate konfigurirati postavke poslužitelja e-pošte.
Mrežna mapa	Odredište podataka skeniranja. Prethodno trebate pripremiti mrežnu mapu.

Povezane informacije

➔ [“Suradnja između LDAP-poslužitelja i korisnika” na strani 68](#)

Usporedba konfiguracije kontakata

Postoje tri alata za konfiguriranje kontakata skenera: Web Config, Epson Device Admin i kontrolna ploča skenera. Razlike između ta tri alata navedene su u tablici ispod.

Značajke	Web Config*	Epson Device Admin	Upravljačka ploča skenera
Registriranje odredišta	✓	✓	✓
Uređivanje odredišta	✓	✓	✓
Dodavanje grupe	✓	✓	✓
Uređivanje grupe	✓	✓	✓
Brisanje odredišta ili grupa	✓	✓	✓
Brisanje svih odredišta	✓	✓	–
Uvoz datoteke	✓	✓	–
Izvoz u datoteku	✓	✓	–

* Prijavite se kao administrator da biste birali postavke.

Registracija odredišta u kontaktima koristeći Web Config

Napomena:

Možete registrirati i kontakte na upravljačkoj ploči skenera.

1. Pristupite aplikaciji Web Config i odaberite karticu **Scan > Contacts**.
2. Odaberite broj koji želite registrirati i kliknite na **Edit**.
3. Unesite **Name** i **Index Word**.
4. Odaberite vrstu odredišta kao opciju **Type**.

Napomena:

Ne možete promijeniti opciju **Type** nakon izvršene registracije. Ako želite promijeniti vrstu, izbrišite odredište i zatim ponovno registrirajte.

5. Unesite vrijednost za svaku stavku i zatim kliknite na **Apply**.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Postavke odredišta

Stavke	Postavke i pojašnjenja
Standardne postavke	
Name	Unesite naziv prikazan u kontaktima s najviše 30 znakova Unicode (UTF-8). Ako to ne navedete, ostavite prazno polje.
Index Word	Unesite naziv koristeći 30 znakova ili manje u Unicode sustavu (UTF-8) da biste pretražili kontakte na upravljačkoj ploči skenera. Ako to ne navedete, ostavite prazno polje.
Type	Odaberite vrstu adrese koju želite registrirati.
Assign to Frequent Use	Odaberite za definiranje registrirane adrese kao često korištene adrese. Kada se definira kao često korištena adresa, prikazuje se u gornjem zaslonu skeniranja i možete navesti odredište bez prikazivanja kontakata.
Email	
Email Address	Unesite između 1 i 255 znaka pomoću znakova A-Z a-z 0-9! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Network Folder (SMB)	
Save to	\\„Putanja mape“ Unesite lokaciju na kojoj se nalazi ciljna mapa, između 1 i 253 znakova Unicode (UTF-8), bez „\\“. Unesite mrežnu putanju prikazanu na zaslonu svojstava mape. Pogledajte sljedeće u vezi s pojedinostima o postavljanju mrežne putanje. “Primjer konfiguracije za osobno računalo” na strani 52
User Name	Unesite korisničko ime za pristup mrežnoj mapi s najviše 30 znakova Unicode (UTF-8). Međutim, ne koristite upravljačke znakove (0x00 do 0x1F, 0x7F).
Password	Unesite lozinku za pristup mrežnoj mapi s najviše 20 znakova Unicode (UTF-8). Međutim, ne koristite upravljačke znakove (0x00 do 0x1F, 0x7F).
FTP	
Secure Connection	Odaberite FTP ili FTPS u skladu s protokolom prijenosa datoteke koji podržava FTP poslužitelj. Odaberite FTPS da biste skeneru omogućili komunikaciju sa sigurnosnim mjerama.
Save to	Unesite naziv poslužitelja koristeći između 1 i 253 znaka koda ASCII (0x20–0x7E), izuzev „ftp://“ ili „ftps://“.
User Name	Unesite korisničko ime za pristup FTP poslužitelju s najviše 30 znakova Unicode (UTF-8). Međutim, ne koristite upravljačke znakove (0x00 do 0x1F, 0x7F). Ako poslužitelj omogućava anonimne veze, unesite korisničko ime, recimo Anonimno, te FTP. Ako to ne navedete, ostavite prazno polje.
Password	Unesite lozinku za pristup FTP poslužitelju s najviše 20 znakova Unicode (UTF-8). Međutim, ne koristite upravljačke znakove (0x00 do 0x1F, 0x7F). Ako to ne navedete, ostavite prazno polje.
Connection Mode	Odaberite način povezivanja preko izbornika. Ako se postavi vatrozid između pisača i FTP poslužitelja, odaberite Passive Mode .
Port Number	Unesite broj ulaza FTP poslužitelja između 1 i 65535.

Stavke	Postavke i pojašnjenja
Certificate Validation	Valjanost FTP certifikata bit će provjerena ako je to omogućeno. To će biti dostupno kada FTPS bude odabran za Secure Connection . Za postavljanje trebate uvesti CA Certificate na skener.
SharePoint(WebDAV)	
Secure Connection	Odaberite HTTP ili HTTPS u skladu s protokolom prijenosa datoteke koji podržava poslužitelj. Odaberite HTTPS da biste skeneru omogućili komunikaciju sa sigurnosnim mjerama.
Save to	Unesite naziv poslužitelja koristeći između 1 i 253 znaka koda ASCII (0x20–0x7E), izuzev „http://” ili „https://”.
User Name	Unesite korisničko ime za pristup poslužitelju s najviše 30 znakova Unicode (UTF-8). Međutim, ne koristite upravljačke znakove (0x00 do 0x1F, 0x7F). Ako to ne navedete, ostavite prazno polje.
Password	Unesite lozinku za pristup poslužitelju s najviše 20 znakova Unicode (UTF-8). Međutim, ne koristite upravljačke znakove (0x00 do 0x1F, 0x7F). Ako to ne navedete, ostavite prazno polje.
Certificate Validation	Valjanost certifikata bit će provjerena ako je to omogućeno. To će biti dostupno kada HTTPS bude odabran za Secure Connection . Za postavljanje trebate uvesti CA Certificate na skener.
Proxy Server	Odaberite želite li koristiti proxy poslužitelj.

Registriranje odredišta kao grupe koristeći Web Config

Ako je vrsta odredišta postavljena na **Email**, možete registrirati odredišta kao grupu.

1. Pristupite aplikaciji Web Config i odaberite karticu **Scan > Contacts**.
2. Odaberite broj koji želite registrirati i kliknite na **Edit**.
3. Odaberite skupinu pod stavkom **Type**.
4. Kliknite na **Select** za **Contact(s) for Group**.
Prikazana su dostupna odredišta.
5. Odaberite odredište koje želite registrirati za skupinu i zatim kliknite na **Select**.
6. Unesite **Name** i **Index Word**.
7. Odaberite hoćete li dodijeliti registriranu skupinu često korištenoj skupini.
***Napomena:**
Odredišta se mogu registrirati za više skupina.*
8. Kliknite na **Apply**.

Povezane informacije

➔ “Pokretanje programa Web Config u internetskom pregledniku” na strani 35

Sigurnosno kopiranje i uvoz kontakata

Koristeći Web Config ili druge alate možete sigurnosno kopirati i uvoziti kontakte.

Za Web Config možete izraditi sigurnosnu kopiju kontakata izvozom postavki skenera s kontaktima. Izvezena datoteka ne može se uređivati jer je izvezena u binarnom obliku.

Kod uvoza postavki skenera na skener dolazi do zamjene starih kontakata novima.

Kod programa Epson Device Admin mogu se izvoziti samo kontakti sa zaslona uređaja. Također, ako ne izvozite sigurnosne stavke, možete urediti izvezene stavke i uvoziti ih jer se to može spremirati kao SYLK ili CSV datoteka.

Uvoz kontakata koristeći Web Config

Ako imate skener koji vam omogućava sigurnosno kopiranje kontakata i koji je kompatibilan s ovim skenerom, možete lako registrirati kontakte tako da uvezete datoteku sigurnosne kopije.

Napomena:

Upute o načinu sigurnosnog kopiranja kontakata potražite u priručniku isporučenom uz skener.

Slijedite korake navedene u nastavku za uvoz kontakata na ovaj skener.

1. Pristupite aplikaciji Web Config, odaberite karticu **Device Management** > **Export and Import Setting Value** > **Import**.
2. Odaberite datoteku sigurnosne kopije koju ste kreirali u **File**, unesite lozinku i zatim kliknite na **Next**.
3. Odaberite potvrdni okvir **Contacts** i zatim kliknite na **Next**.

Sigurnosna kopija kontakata koristeći Web Config

Podaci o kontaktima mogu se izgubiti zbog kvara skenera. Preporučujemo vam da svaki puta kada ažurirate podatke stvorite sigurnosnu kopiju. Epson ne preuzima nikakvu odgovornost za gubitak podataka niti za izradu sigurnosne kopije podataka i/ili postavki, čak ni tijekom jamstvenog roka.

Pomoću programa Web Config na računalu možete načiniti sigurnosnu kopiju podataka pohranjenih na skener.

1. Pristupite aplikaciji Web Config i odaberite karticu **Device Management** > **Export and Import Setting Value** > **Export**.
2. Odaberite potvrdni kvadratić **Contacts** pod kategorijom **Scan**.
3. Unesite lozinku kako biste šifrirali izvezenu datoteku.
Za uvoz datoteke potrebna vam je lozinka. Ostavite ovo mjesto prazno ako ne želite šifrirati datoteku.
4. Kliknite na **Export**.

Izvoz i skupna registracija kontakata koristeći alat

Ako koristite Epson Device Admin, možete sigurnosno kopirati samo kontakte i urediti izvezene datoteke, a zatim ih registrirati sve odjednom.

Korisno je želite li izraditi sigurnosnu kopiju samo kontakata ili kada zamijenite skener i želite prenijeti kontakte sa starog na novi.

Izvoz kontakata

Spremite informacije o kontaktima u datoteku.

Možete uređivati datoteke spremljene u SYLK ili CSV formatu pomoću aplikacije za proračunske tablice ili programa za uređivanje teksta. Možete sve odjednom registrirati nakon brisanja ili dodavanja informacija.

Informacije koje sadrže sigurnosne stavke kao što su lozinke i osobne informacije mogu se spremiti u binarnom formatu s lozinkom. Ne možete urediti datoteku. Ovo se može koristiti kao sigurnosna kopija informacija uključujući sigurnosne stavke.

1. Pokrenite Epson Device Admin.
2. Odaberite **Devices** na bočnoj traci izbornika zadatka.
3. Odaberite uređaj koji želite konfigurirati s popisa uređaja.
4. Kliknite na **Device Configuration** na kartici **Home** na trakastom izborniku.
Kada je postavljena lozinka administratora, unesite lozinku i kliknite na **OK**.
5. Kliknite na **Common > Contacts**.
6. Odaberite format za izvoz iz **Export > Export items**.
 - All Items
Izvezite šifriranu binarnu datoteku. Odaberite kada želite uključiti sigurnosne stavke kao što su lozinka i osobne informacije. Ne možete urediti datoteku. Ako to odaberete, morate postaviti lozinku. Kliknite na **Configuration** i postavite lozinku dugu između 8 i 63 znakova u ASCII. Ova lozinka će biti potrebna prilikom uvoza binarne datoteke.
 - Items except Security Information
Izvezite datoteke u SYLK ili CSV formatu. Odaberite želite li urediti informacije na izvezenoj datoteci.
7. Kliknite na **Export**.
8. Naznačite mjesto za spremanje datoteke, vrstu datoteke i zatim kliknite na **Save**.
Prikazuje se poruka o dovršetku.
9. Kliknite na **OK**.
Provjerite je li datoteka spremljena na naznačeno mjesto.

Uvoz kontakata

Uvoz informacije o kontaktima iz datoteke.

Možete uvesti datoteke spremljene u SYLK ili CSV formatu ili sigurnosnu kopiju binarne datoteke koja uključuje sigurnosne stavke.

1. Pokrenite Epson Device Admin.
2. Odaberite **Devices** na bočnoj traci izbornika zadatka.
3. Odaberite uređaj koji želite konfigurirati s popisa uređaja.
4. Kliknite na **Device Configuration** na kartici **Home** na trakastom izborniku.
Kada je postavljena lozinka administratora, unesite lozinku i kliknite na **OK**.
5. Kliknite na **Common > Contacts**.
6. Kliknite na **Browse** pod **Import**.
7. Odaberite datoteku koju želite uvesti i zatim kliknite na **Open**.
Kad odaberete binarnu datoteku u **Password** unesite lozinku koju ste postavili prilikom izvoza datoteke.
8. Kliknite na **Import**.
Prikazuje se zaslon potvrde.
9. Kliknite na **OK**.
Prikazuje se rezultat potvrđivanja.
 - Edit the information read
Kliknite kada želite pojedinačno urediti informacije.
 - Read more file
Kliknite kada želite uvesti više datoteka.
10. Kliknite na **Import** i zatim na **OK** na zaslonu dovršetka uvoza.
Vratite se na zaslon svojstva uređaja.
11. Kliknite na **Transmit**.
12. Kliknite na **OK** na poruci potvrde.
Postavke su poslane skeneru.
13. Na zaslonu dovršetka slanja kliknite na **OK**.
Informacije o skeneru su ažurirane.
Otvorite kontakte u aplikaciji Web Config ili upravljačkoj ploči skenera i zatim provjerite jesu li kontakti ažurirani.

Suradnja između LDAP-poslužitelja i korisnika

Kod suradnje s LDAP poslužiteljem, možete koristiti adresne informacije registrirane na LDAP poslužitelji kao odredište e-pošte.

Konfiguriranje LDAP poslužitelja

Kako biste iskoristili informacije o LDAP poslužitelju, registrirajte ih na skeneru.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network > LDAP Server > Basic**.
2. Unesite vrijednost svake stavke.
3. Odaberite **OK**.
Prikazane su postavke koje ste odabrali.

Stavke postavljanja LDAP poslužitelja

Stavke	Postavke i pojašnjenja
Use LDAP Server	Odaberite Use ili Do Not Use .
LDAP Server Address	Unesite adresu LDAP poslužitelja. Unesite između 1 i 255 znakova u formatu IPv4, IPv6 ili FQDN. Za FQDN format možete koristiti alfanumeričke znakove u ASCII kodu (0x20–0x7E) i „-“, osim na početku i na kraju adrese.
LDAP server Port Number	Unesite broj ulaza poslužitelja LDAP, između 1 i 65535.
Secure Connection	Odredite metodu potvrđivanja autentičnosti kada skener pristupa LDAP poslužitelju.
Certificate Validation	Kad je omogućeno, potvrđen je certifikat za LDAP poslužitelja. Preporučamo da to namjestite na Enable . Kako bi bio postavljen CA Certificate treba biti uvezen u skener.
Search Timeout (sec)	Odredite trajanje pretraživanja prije isteka vremena, između 5 i 300.
Authentication Method	Odaberite jedan od načina. Ako odaberete Kerberos Authentication , odaberite Kerberos Settings kako biste odabrali postavke za Kerberos. Za provođenje Kerberos Authentication potrebno je sljedeće okruženje. <input type="checkbox"/> Skener i DNS poslužitelj mogu komunicirati. <input type="checkbox"/> Vrijeme na skeneru, KDC poslužitelju i poslužitelju potrebnom za potvrđivanje autentičnosti (LDAP poslužitelj, SMTP poslužitelj, poslužitelj datoteke) trebaju biti sinkronizirani. <input type="checkbox"/> Kada je poslužitelj usluge dodijeljen kao IP adresa, FQDN poslužitelja usluge je registriran na zoni obrnutog pretraživanja DNS poslužitelja.
Kerberos Realm to be Used	Ako odaberete Kerberos Authentication za Authentication Method , odaberite Kerberos područje koje želite koristiti.

Stavke	Postavke i pojašnjenja
Administrator DN / User Name	Unesite korisničko ime za poslužitelj LDAP s najviše 128 znakova Unicode (UTF-8). Ne možete koristiti kontrolne znakove, kao što su 0x00–0x1F i 0x7F. Ova postavka se ne koristi kada je Anonymous Authentication odabran kao Authentication Method . Ako to ne navedete, ostavite prazno polje.
Password	Unesite lozinku za autentikaciju poslužitelja LDAP s najviše 128 znakova Unicode (UTF-8). Ne možete koristiti kontrolne znakove, kao što su 0x00–0x1F i 0x7F. Ova postavka se ne koristi kada je Anonymous Authentication odabran kao Authentication Method . Ako to ne navedete, ostavite prazno polje.

Kerberos postavke

Ako odaberete **Kerberos Authentication** za **Authentication Method** od **LDAP Server > Basic**, izvršite sljedeće Kerberos postavke u kartici **Network > Kerberos Settings**. Možete registrirati do 10 postavki Kerberos.

Stavke	Postavke i pojašnjenja
Realm (Domain)	Unesite područje Kerberos autentikacije s najviše 255 znakova u ASCII kodu (0x20–0x7E). Ako ne registrirate, ostavite prazno polje.
KDC Address	Unesite adresu poslužitelja za Kerberos autentikaciju. Unesite najviše 255 znakova u formatu IPv4, IPv6 ili FQDN. Ako ne registrirate, ostavite prazno polje.
Port Number (Kerberos)	Unesite broj ulaza Kerberos poslužitelja, između 1 i 65535.

Konfiguriranje postavki pretraživanja LDAP poslužitelja

Kada odaberete postavke pretraživanja, možete koristiti adresu e-pošte registriranu na LDAP poslužitelju.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network > LDAP Server > Search Settings**.
2. Unesite vrijednost svake stavke.
3. Kliknite na **OK** za prikaz rezultata postavljanja.
Prikazane su postavke koje ste odabrali.

Stavke postavljanja pretraživanja LDAP poslužitelja

Stavke	Postavke i pojašnjenja
Search Base (Distinguished Name)	Ako želite tražiti proizvoljnu domenu, navedite naziv domene LDAP poslužitelja. Unesite između 0 i 128 znakova u Unicode kodu (UTF-8). Ako ne tražite arbitražno svojstvo, ostavite ovo polje prazno. Primjer direktorija lokalnog poslužitelja: dc=server,dc=local
Number of search entries	Navedite broj unosa za pretraživanje između 5 i 500. Navedeni broj unosa za pretraživanje je spremljen i privremeno prikazano. Pretraživanje se može izvršiti čak i kada je broj unosa za pretraživanje veći od navedenog broja te se pojavi poruka greške.

Stavke	Postavke i pojašnjenja
User name Attribute	Navedite naziv svojstva koji će biti prikazan kod pretraživanja korisničkih imena. Unesite između 1 i 255 znakova u Unicode kodu (UTF-8). Prvi znak treba biti a–z ili A–Z. Primjer: cn, uid
User name Display Attribute	Navedite naziv svojstva koji će biti prikazan kao korisničko ime. Unesite između 0 i 255 znakova u Unicode kodu (UTF-8). Prvi znak treba biti a–z ili A–Z. Primjer: cn, sn
Email Address Attribute	Navedite naziv svojstva koji će biti prikazan kod pretraživanja adresa e-pošte. Unesite kombinaciju između 1 i 255 znakova pomoću znakova A–Z, a–z, 0–9 i -. Prvi znak treba biti a–z ili A–Z. Primjer: mail
Arbitrary Attribute 1 - Arbitrary Attribute 4	Možete navesti druga arbitražna svojstva koja treba potražiti. Unesite između 0 i 255 znakova u Unicode kodu (UTF-8). Prvi znak treba biti a–z ili A–Z. Ako ne želite tražiti proizvoljne atribute, ostavite ovo polje prazno. Primjer: o, ou

Provjera veze s LDAP poslužiteljem

Izvršava provjeru veze LDAP poslužitelja koristeći parametre zadane pod **LDAP Server > Search Settings**.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network > LDAP Server > Connection Test**.
2. Odaberite **Start**.
Pokrenuta je provjera veze. Nakon provjere je prikazan izvještaj o provjeri.

Reference testa veze s LDAP poslužiteljem

Poruke	Pojašnjenje
Connection test was successful.	Ova poruka pojavljuje se kod uspješnog povezivanja s poslužiteljem.
Connection test failed. Check the settings.	Ova poruka pojavljuje se iz sljedećih razloga: <ul style="list-style-type: none"> <input type="checkbox"/> Adresa LDAP poslužitelja ili broj porta je netočan. <input type="checkbox"/> Došlo je do isteka vremena. <input type="checkbox"/> Do Not Use je odabrano kao Use LDAP Server. <input type="checkbox"/> Ako je Kerberos Authentication odabran kao Authentication Method, postavke poput Realm (Domain), KDC Address i Port Number (Kerberos) nisu točne.
Connection test failed. Check the date and time on your product or server.	Ova poruka pojavljuje se kada veza ne uspije zbog nepodudaranja vremenskih postavki skenera i LDAP poslužitelja.

Poruke	Pojašnjenje
Authentication failed. Check the settings.	Ova poruka pojavljuje se iz sljedećih razloga: <input type="checkbox"/> Stavka User Name i/ili Password nije točna. <input type="checkbox"/> Ako se Kerberos Authentication odabere za Authentication Method , možda se neće konfigurirati vrijeme/datum.
Cannot access the product until processing is complete.	Ova poruka pojavljuje se kada je skener zauzet.

Uporaba opcije Document Capture Pro Server

Koristeći Document Capture Pro Server možete upravljati načinom sortiranja, spremanjem formata i prosljeđivanjem odredišta rezultata skeniranja koje je izvršeno s upravljačke ploče skenera. Možete pozvati i izvršiti zadatak koji je prethodno prijavljen na poslužitelj preko upravljačke ploče skenera.

Instalirajte ga na računalo poslužitelja.

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

Postavljanje načina poslužitelja

Kako biste koristili Document Capture Pro Server, odaberite sljedeće postavke.

1. Pristupite aplikaciji Web Config i odaberite karticu **Scan > Document Capture Pro**.
2. Odaberite **Server Mode** za **Mode**.
3. Unesite adresu poslužitelja s programom Document Capture Pro Server instaliranim na njemu za **Server Address**.
Unesite između 2 i 255 znakova u formatu IPv4, IPv6, naziv domaćina ili FQDN. Za FQDN format možete koristiti alfanumeričke znakove u ASCII kodu (0x20–0x7E) i „-“, osim na početku i na kraju adrese.
4. Kliknite na **OK**.
Mreža se ponovno povezuje i zatim se aktiviraju postavke.

Postavljanje značajke AirPrint

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

Stavke	Pojašnjenje
Bonjour Service Name	Unesite naziv usluge Bonjour, koristeći ASCII tekst (0x20 – 0x7E) i do 41 znak.
Bonjour Location	Unesite opis lokacije skenera, koristeći Unicode (UTF-8) tekst i do 127 bajtova.
Wide-Area Bonjour	Odredite hoćete li koristiti Wide-Area Bonjour. Ako ga koristite, skener mora biti registriran na DNS poslužitelju kako biste mogli potražiti skener preko segmenta.

Stavke	Pojašnjenje
Enable AirPrint	Omogućeni su Bonjour i AirPrint (usluga skeniranja).

Problemi kod pripremanja mrežnog skeniranja

Savjeti za rješavanje problema

Provjera poruke greške

Kada dođe do problema, najprije provjerite ima li kakva poruka na upravljačkoj ploči skenera ili zaslonu upravljačkog programa. Ako set postavili obavijest e-poštom nakon događaja, možete odmah vidjeti status.

Provjera statusa komunikacije

Provjerite status komunikacije poslužitelja računala ili klijentskog računala uporabom naredbi kao što su ping ili ipconfig.

Testiranje povezivanja

Za provjeru vezu između skenera i poslužitelja e-pošte provedite provjeru veze na skeneru. Također provjerite povezivanje s klijentskog računala na poslužitelja kako biste provjerili status komunikacije.

Inicijaliziranje postavki

Ako postavke i status komunikacije ne pokazuju nikakav problem, možda se problem može riješiti onemogućavanjem ili inicijaliziranjem mrežnih postavki na skeneru i zatim njihovim ponovnim postavljanjem.

Ne mogu pristupiti aplikaciji Web Config

Skeneru nije dodijeljena IP-adresa.

Rješenja

Skeneru možda nije dodijeljena valjana IP-adresa. Konfigurirajte IP adresu pomoću upravljačke ploče skenera. Možete potvrditi trenutačne informacije o postavkama preko upravljačke ploče skenera.

Web-preglednik ne podržava snagu sustava za šifriranje za SSL/TLS.

Rješenja

SSL/TLS ima Encryption Strength. Možete otvoriti Web Config s pomoću web-preglednika koji podržava skupna šifriranja na način opisan u nastavku. Provjerite koristite li podržani preglednik.

80-bitni: AES256/AES128/3DES

112-bitni: AES256/AES128/3DES

128-bitni: AES256/AES128

192-bitni: AES256

256-bitni: AES256

Istekao je CA-signed Certificate.

Rješenja

Ako postoji problem s datumom isteka certifikata, prikazat će se poruka „Certifikat je istekao” kod spajanja na Web Config koristeći SSL/TLS komunikaciju (https). Ako se poruka pojavi prije isteka certifikata, provjerite je li datum skenera ispravno konfiguriran.

Uobičajeno ime certifikata i skenera se ne podudaraju.

Rješenja

Ako se uobičajeno ime certifikata i skenera se ne podudaraju, prikazuje se poruka „Naziv sigurnosnog certifikata se ne podudara...” kada pristupate aplikaciji Web Config pomoću SSL/TLS komunikacije (https). Do toga je došlo zato što se ne podudaraju sljedeće IP adrese.

- IP adresa skenera unesena u uobičajeno ime za izradu Self-signed Certificate ili CSR
- IP adresa unesena u web-preglednik dok je pokrenuta aplikacija Web Config

Za Self-signed Certificate ažurirajte certifikat.

Za CA-signed Certificate ponovo uzmite certifikat za skener.

Postavka Proxy poslužitelja lokalne adrese nije postavljena za web-preglednik.

Rješenja

Kada je skener postavljen za primjenu Proxy poslužitelja, konfigurirajte web-preglednik kako se lokalna adresa ne bi povezala preko Proxy poslužitelja.

- Windows:

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

- Mac OS:

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

Primjer:

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

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

DHCP je onemogućen u postavkama računala.

Rješenja

Ako DHCP za pribavljanje IP adrese automatski je onemogućen na računalu, ne možete pristupiti programu Web Config. Omogućite DHCP.

Primjer za Windows 10:

Otvorite upravljačku ploču i zatim kliknite **Mreža i Internet > Mreža i centar za dijeljenje > Promjena postavki adaptera**. Otvorite zaslon Svojstva za veze kojima se koristite i zatim otvorite zaslon svojstva za **Internetski protokol verzija 4 (TCP/IPv4)** ili **Internetski protokol verzija 6 (TCP/IPv6)**. Provjerite da je na prikazanom zaslonu odabrano **Automatski pribavi IP adresu**.


Prilagođavanje zaslona upravljačke ploče

Registriranje Postavke.	75
Uređivanje početnog zaslona upravljačke ploče.	77

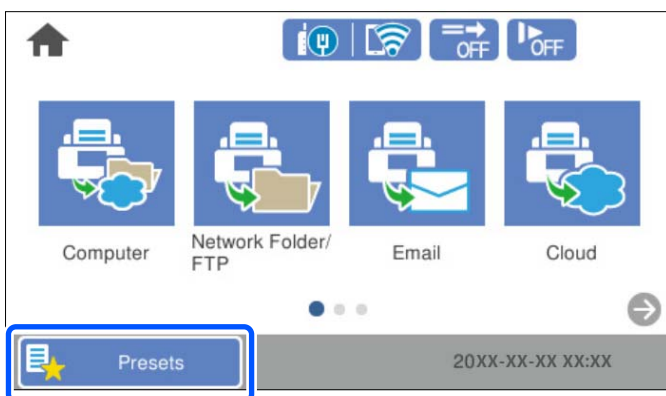
Registriranje Postavke


Možete registrirati često korištenu postavku skeniranja kao **Postavke**. Možete registrirati do 48 početnih postavki.

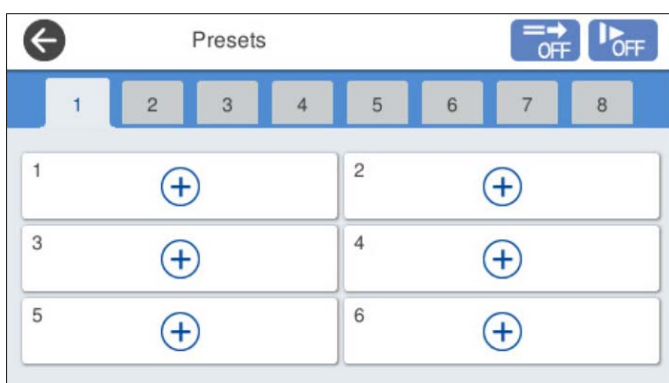
Napomena:

- Možete registrirati trenutačne postavke odabirom  na zaslonu početka skeniranja.
- Također možete registrirati **Presets** u Web Config.
Odaberite karticu **Scan** > **Presets**.
- Ako odaberete **Skeniraj u računalo** prilikom registriranja, možete registrirati zadatak kreiran u programu Document Capture Pro kao **Presets**. To je dostupno samo za računala spojena preko mreže. Unaprijed registrirajte zadatak u programu Document Capture Pro.
- Ako se omogući funkcija autentikacije, samo administrator može registrirati **Presets**.

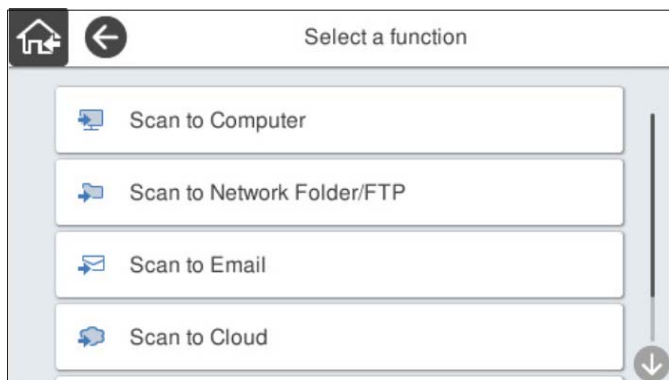
1. Odaberite **Postavke** na početnom zaslonu na upravljačkoj ploči skenera.



2. Odaberite .



3. Odaberite izbornik koji želite koristiti za registriranje zadane postavke.



4. Odaberite svaku stavku, a zatim odaberite .

Napomena:

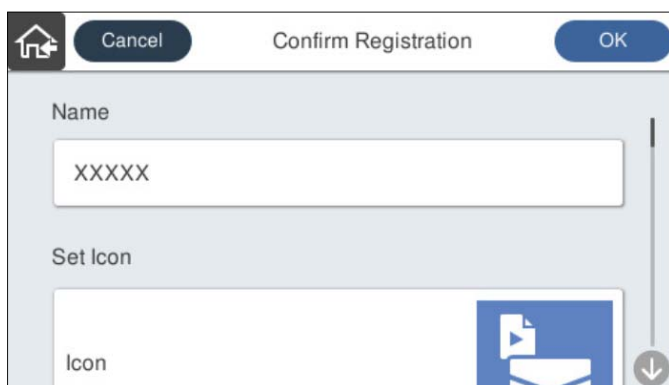
Kada odaberete **Skeniraj u računalo**, odaberite računalo na kojem je instaliran Document Capture Pro i zatim odaberite registrirani zadatak. To je dostupno samo za računala spojena preko mreže.

5. Odaberite zadane postavke.

- Naziv:** postavite naziv.
- Postavite ikonu:** postavite sliku i boju ikone za prikaz.
- Postavka Brzo slanje:** odmah pokreće skeniranje bez potvrde kada se odabere zadana postavka.


Kada koristite Document Capture Pro Server, čak i kada postavite softver da potvrdi sadržaj zadatka prije skeniranja, **Postavka Brzo slanje** u početnim postavkama skenera ima prednost u odnosu na softver.

- Sadržaj:** provjerite postavke skeniranja.



6. Odaberite **OK**.

Mogućnosti izbornika Postavke

Možete promijeniti postavke odabirom  u svakoj zadanoj postavci.

Promijenite Naziv:

Mijenja naziv zadane postavke.

Promijenite ikonu:

Mijenja sliku ikone i boju zadane postavke.

Postavka Brzo slanje:

Odmah pokreće skeniranje bez potvrde kada se odabere zadana postavka.

Promijenite položaj:

Mijenja redoslijed prikaza zadanih postavki.

Izbriši:

Briše zadanu postavku.

Dodajte ili uklonite ikonu na početnom zaslonu:

Dodaje ili briše ikonu zadane postavke s početnog zaslona.

Potvrdite Pojediniosti:

Prikaz zadanih postavki. Možete učitati zadanu postavku odabirom opcije **Koristi ovu postavku**.

Uređivanje početnog zaslona upravljačke ploče

Možete prilagoditi početni zaslon odabirom **Postavke > Uređivanje početnog zaslona** na upravljačkoj ploči skenera.

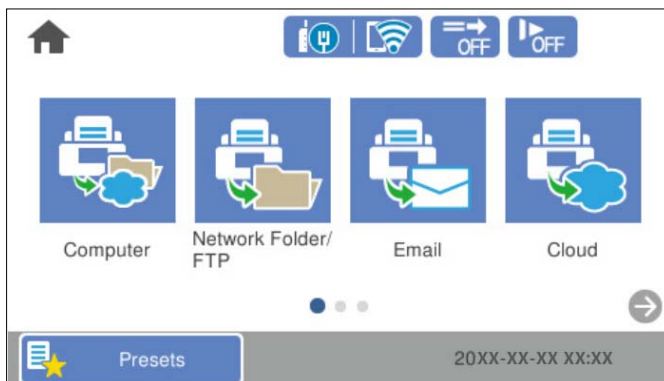
- Izgled: mijenja način prikaza ikona izbornika.
[“Promjena Izgled početnog zaslona” na strani 77](#)
- Dodaj ikonu: dodaje ikone postavkama **Postavke** koje ste odabrali ili vraća ikone koje su uklonjene sa zaslona.
[“Dodaj ikonu” na strani 78](#)
- Ukloni ikonu: uklanja ikone s početnog zaslona.
[“Ukloni ikonu” na strani 79](#)
- Pomakni ikonu: mijenja redoslijed prikaza ikona.
[“Pomakni ikonu” na strani 80](#)
- Vraćanje zadanog prikaza ikone: vraća zadane postavke prikaza za početni zaslon.
- Podloga: promijenite boju pozadine početnog zaslona.

Promjena Izgled početnog zaslona

1. Odaberite **Postavke > Uređivanje početnog zaslona > Izgled** na upravljačkoj ploči skenera.


2. Odaberite **Linija** ili **Matrica**.

Linija:



Matrica:

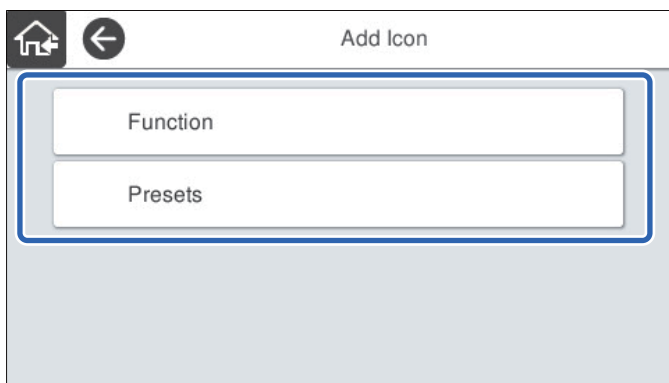


3. Odaberite  za povratak i provjeru početnog zaslona.

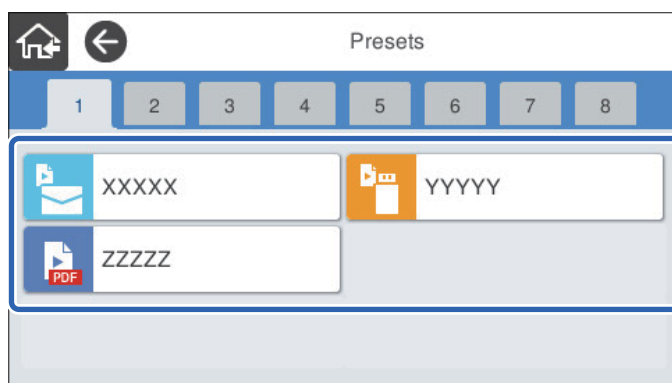
Dodaj ikonu

1. Odaberite **Postavke** > **Uređivanje početnog zaslona** > **Dodaj ikonu** na upravljačkoj ploči skenera.
2. Odaberite **Funkcija** ili **Postavke**.
 - Funkcija: prikazuje zadane funkcije pokazane na početnom zaslonu.

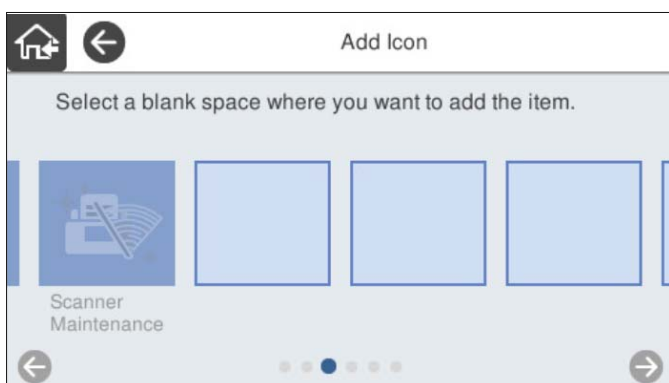
- ❑ Postavke: prikazuje registrirane postavke.




3. Odaberite stavku koju želite dodati na početnom zaslonu.



4. Odaberite prazninu gdje želite dodati stavku.
Ako želite dodati višestruke ikone, ponovite korake 3 do 4.

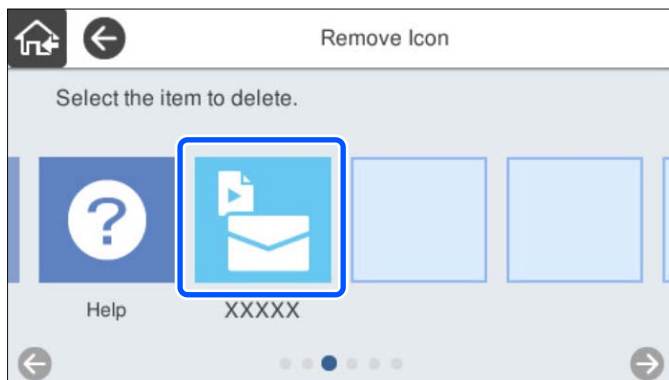



5. Odaberite  za povratak i provjeru početnog zaslona.

Ukloni ikonu

1. Odaberite **Postavke** > **Uređivanje početnog zaslona** > **Ukloni ikonu** na upravljačkoj ploči skenera.

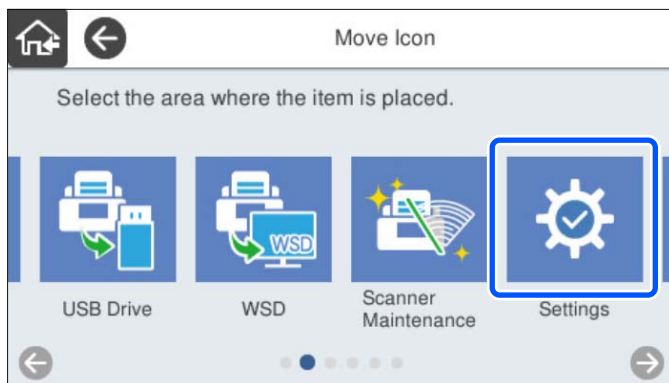
2. Odaberite ikonu koju želite ukloniti.



3. Odaberite **Da** za završetak.
Ako želite ukloniti višestruke ikone, ponovite postupak 2 do 3.
4. Odaberite  za povratak i provjeru početnog zaslona.

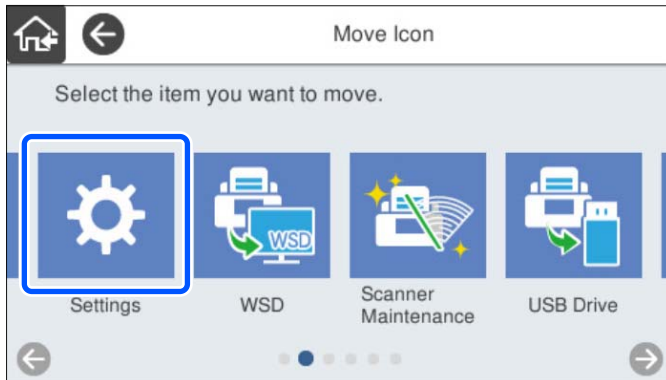
Pomakni ikonu


1. Odaberite **Postavke** > **Uređivanje početnog zaslona** > **Pomakni ikonu** na upravljačkoj ploči skenera.
2. Odaberite ikonu koju želite premjestiti.



3. Odaberite okvir odredišta.

Ako se već postavi druga ikona u ciljni okvir, ikone će biti zamijenjene.



4. Odaberite  za povratak i provjeru početnog zaslona.

Osnovne postavke sigurnosti

Uvod u sigurnosne značajke proizvoda.	83
Administratorske postavke.	83
Onemogućavanje vanjskog sučelja.	89
Nadziranje daljinskog skenera.	90
Rješavanje problema.	91

Uvod u sigurnosne značajke proizvoda

Ovaj dio vas uvodi u sigurnosne funkcije Epson uređaja.

Naziv značajke	Vrsta značajke	Što podesiti	Što spriječiti
Postavke lozinke administratora	Blokira postavke sustava, poput konfiguracije veze za mrežu ili USB.	Administrator određuje lozinku uređaja. Možete odrediti ili promijeniti preko aplikacije Web Config te na upravljačkoj ploči skenera.	Spriječite neovlašteno čitanje i promjenu informacija pohranjenih na uređaju, kao što je ID, lozinka, mrežne postavke i sl. Također smanjuje široki spektar rizika, uključujući curenje informacija mrežnog okruženja ili sigurnosnih pravila.
Postavke za vanjsko sučelje	Upravlja sučeljem koji se spaja na uređaj.	Omogućite ili onemogućite USB povezivanje s računalom.	USB spajanje na računalo: sprječava neovlaštenu uporabu uređaja tako što zabranjuje skeniranje bez spajanja na mrežu.

Povezane informacije

- ➔ [“Konfiguriranje lozinke administratora” na strani 83](#)
- ➔ [“Onemogućavanje vanjskog sučelja” na strani 89](#)

Administratorske postavke

Konfiguriranje lozinke administratora

Kada odaberete lozinku administratora, možete spriječiti da korisnici promijene postavke upravljanja sustavom. Zadane vrijednosti postavljene su u trenutku kupnje. Promijenite ih po potrebi.

Napomena:

U nastavku se navode zadane vrijednosti informacija o administratoru.

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

Kako biste pronašli serijski broj, provjerite naljepnicu na stražnjoj strani skenera.

Možete promijeniti lozinku administratora koristeći Web Config, upravljačku ploču skenera ili Epson Device Admin. Kod primjene programa Epson Device Admin, pogledajte vodič Epson Device Admin ili pomoć.

Promjena lozinke administratora koristeći Web Config

Promijenite lozinku administratora pod Web Config.

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

2. Unesite potrebne podatke u **Current password**, **User Name**, **New Password**, i **Confirm New Password**.
Unesite barem jedan znak za novu lozinku.

Napomena:

U nastavku se navode zadane vrijednosti informacija o administratoru.

Korisničko ime: nijedno (prazno)

Lozinka: serijski broj skenera

Kako biste pronašli serijski broj, provjerite naljepnicu na stražnjoj strani skenera.



Važno:

Obvezno zapamtite administratorsku lozinku koju ste postavili. Ako zaboravite lozinku, nećete je moći resetirati i morat ćete zatražiti pomoć od servisera.

3. Odaberite **OK**.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Promjena lozinke administratora preko upravljačke ploče

Možete promijeniti lozinku administratora na upravljačkoj ploči skenera.

1. Odaberite **Postavke** na upravljačkoj ploči skenera.
2. Odaberite **Administracija sustava > Administratorske postavke**.
3. Odaberite **Lozinka administratora > Promjena**.
4. Unesite trenutачnu lozinku.

Napomena:

Postavka u trenutku kupnje (zadana vrijednost) za lozinku administratora je serijski broj skenera.

Kako biste pronašli serijski broj, provjerite naljepnicu na stražnjoj strani skenera.

5. Unesite novu lozinku.

Unesite barem jedan znak.



Važno:

Obvezno zapamtite administratorsku lozinku koju ste postavili. Ako zaboravite lozinku, nećete je moći resetirati i morat ćete zatražiti pomoć od servisera.

6. Ponovno unesite novu lozinku za potvrdu.

Prikazuje se poruka o dovršetku.

Korištenje Postavka blokade za upravljačku ploču


Možete koristiti Postavka blokade za zaključavanje upravljačke ploče kako biste spriječili korisnike da mijenjaju stavke povezane s postavkama sustava.

Napomena:

Ako omogućite *Authentication Settings* na skeneru, Postavka blokade je također omogućen za upravljačku ploču. Upravljačka ploča ne može se otključati kada se onemogući *Authentication Settings*.

Čak i ako onemogućite *Authentication Settings*, Postavka blokade ostaje omogućeno. Ako želite onemogućiti, možete odabrati postavke preko upravljačke ploče ili programa *Web Config*.

Postavljanje Postavka blokade s upravljačke ploče

1. Ako želite otkazati **Postavka blokade** nakon što se omogući, dodirnite  u gornjem desnom kutu početnog zaslona kako biste se prijavili kao administrator.



se ne prikazuje kada je onemogućeno **Postavka blokade**. Ako želite omogućiti ovu postavku, prijedite na sljedeći korak.

2. Odaberite **Postavke**.
3. Odaberite **Administracija sustava > Administratorske postavke**.
4. Odaberite **Uklj.** ili **Isklj.** kao **Postavka blokade**.

Postavka Postavka blokade preko Web Config

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

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Postavka blokade stavke u izborniku Postavke

Ovo je popis stavki koje su zaključane u izborniku **Postavke** na upravljačkoj ploči preko Postavka blokade.

✓: treba blokirati.

- : ne treba blokirati.

Izbornik Postavke	Postavka blokade
Osnovne postavke	-

Izbornik Postavke		Postavka blokade
	Svjetlina LCD-a	-
	Zvukovi	-
	Tajmer za mirovanje	✓
	Isključi mjerač vremena	✓
	Postavke datuma/vremena	✓
	Jezik/Language	✓/-*
	Tipkovnica (Ova značajka možda neće biti dostupna u vašoj regiji.)	-
	Prekid rada	✓
	Povezivanje s računalom preko USB	✓
	Izr. napajanje uklj.	✓
Postavke skenera		-
	Sporo	-
	Vrijeme zaust. dvostrukog ulaganja	✓
	Funkcija DFDS	-
	Zaštita papira	✓
	Otkrivanje prljavog stakla	✓
	Ultrazvu. otkriv. dvostrukog uvlače.	✓
	Način automatskog uvlačenja je istekao	✓
	Potvrdi primatelja	✓
Uređivanje početnog zaslona		✓
	Izgled	✓
	Dodaj ikonu	✓
	Ukloni ikonu	✓
	Pomakni ikonu	✓
	Vraćanje zadanog prikaza ikone	✓
	Podloga	✓
Korisničke postavke		✓
	Mrežna mapa/FTP	✓
	E-pošta	✓
	Oblak	✓
	USB pogon	✓


Izbornik Postavke		Postavka blokade
Postavke mreže		✓
	Postavljanje Wi-Fi veze	✓
	Postava žičanog LAN-a	✓
	Stanje mreže	✓
	Napredno	✓
Postavke web usluge		✓
	Usluge Epson Connect	✓
Document Capture Pro		-
	Promijeni postavke	✓
Upravitelj Kontaktima		-
	Registriranje/izbriši	✓/-*
	Često	-
	Prikaži mogućnosti	-
	Mogućnosti pretraživanja	-
Administracija sustava		✓
	Upravitelj Kontaktima	✓
	Administratorske postavke	✓
	Ograničenja	✓
	Šifriranje lozinke	✓
	Istraživanje kupaca	✓
	Postavke za WSD	✓
	Obnovi zadane postavke	✓
	Ažuriranje firmvera	✓
Podaci o uređaju		-

Izbornik Postavke		Postavka blokade
	Serijski broj	-
	Trenutna verzija	-
	Ukupan broj skeniranja	-
	Broj 1-stranih skeniranja	-
	Broj 2-stranih skeniranja	-
	Broj skeniranja nosivih listova	-
	Broj skenova nakon zamjene valjka	-
	Broj skenova nakon redovitog čišćenja	-
	Resetiraj broj skeniranja	✓
Održavanje skenera		-
	Čišćenje valjka	-
	Zamjena valjka	-
	Resetiraj broj skeniranja	✓
	Kako zamijeniti	-
	Redovito čišćenje	-
	Resetiraj broj skeniranja	✓
	Kako se čisti	-
	Čišćenje stakla	-
Postavka upozorenja za zamjenu valjka		✓
	Postav. upoz. o broju	✓
Postavke upozorenja za redovito čišćenje		✓
	Postavka obavijesti upozorenja	✓
	Postav. upoz. o broju	✓


* Možete postaviti želite li dopustiti promjene u **Administracija sustava > Ograničenja**.

Prijava kao administrator s upravljačke ploče

Možete koristiti bilo koju od sljedećih metoda za prijavu kao administrator s upravljačke ploče skenera.

1. Dodirnite  u gornjem desnom dijelu zaslona.
 - Kada se omogući Authentication Settings, ikona se prikazuje na zaslonu **Dobro došli** (zaslon u stanju pripravnosti za provjeru autentičnosti).
 - Kada se onemogući Authentication Settings, ikona se prikazuje na početnom zaslonu.

2. Dodirnite **Da** kada se prikaže zaslon za potvrdu.
3. Unesite administratorsku lozinku.
Prikazuje se poruka dovršene prijave, a zatim se prikazuje početni zaslon na upravljačkoj ploči.

Za odjavu dodirnite  u gornjem desnom kutu početnog zaslona.

Onemogućavanje vanjskog sučelja

Možete onemogućiti sučelje koje se koristi za spajanje uređaja na skener. Podesite postavke zabrane kako biste zabranili skeniranje osim preko mreže.

Napomena:

Možete podesiti postavke zabrane na upravljačkoj ploči skenera.

Povezivanje s računalom preko USB: **Postavke > Osnovne postavke > Povezivanje s računalom preko USB**

1. Pristupite aplikaciji Web Config i odaberite karticu **Product Security > External Interface**.
2. Odaberite **Disable** na funkcijama koje želite postaviti.
Odaberite **Enable** kada želite otkazati nadzor.
Povezivanje s računalom preko USB
Možete ograničiti korištenje USB veze preko računala. Ako želite ograničiti, odaberite **Disable**.
3. Kliknite na **OK**.
4. Provjerite može li se koristiti onemogućeni ulaz.
Povezivanje s računalom preko USB
Ako je upravljački program instaliran na računalu
Priključite skener na računalo putem USB kabela, a zatim provjerite ispisuje li skener.
Ako upravljački program nije instaliran na računalu
Windows:
Otvorite upravitelj uređaja i zadržite, spojite skener na računalo pomoću USB kabela i zatim potvrdite da sadržaj prikaza upravitelja uređaja ostaje nepromijenjen.
Mac OS:
Priključite skener na računalo putem USB kabela, a zatim provjerite možete li dodati skener u dijelu **Pisači i skeneri**.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Nadziranje daljinskog skenera

Provjera informacija o daljinskom skeneru

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

Product Status

Provjerite status, uslugu u oblaku, broj proizvoda, MAC adresu, itd.

Network Status

Provjerite informacije o statusu mrežne veze, IP-adresu, DNS poslužitelj, itd.

Usage Status

Provjerite prvi dan skeniranja, broj skeniranja, itd.

Hardware Status

Provjerite status svake funkcije skenera.

Panel Snapshot

Prikazuje fotografiju zaslona prikazanu na upravljačkoj ploči skenera.

Primanje obavijesti o događajima putem e-pošte

O obavijestima e-poštom

Ovo je funkcija obavijesti koja će poslati e-poštu na navedenu adresu ako se pojave događaji poput prekida skeniranja i greška skenera.

Možete registrirati do pet odredišta i zadati postavke obavijesti za svako odredište.

Za uporabu ove funkcije trebate postaviti poslužitelj e-pošte prije postavljanja obavijesti.

Povezane informacije

➔ [“Konfiguriranje poslužitelja e-pošte” na strani 41](#)

Konfiguriranje obavijesti e-poštom

Konfigurirajte obavijesti e-poštom pomoću aplikacije Web Config.

1. Pristupite aplikaciji Web Config i odaberite karticu **Device Management > Email Notification**.
2. Zadajte predmet obavijesti e-poštom.

U padajućim izbornicima odaberite sadržaj koji će biti prikazan u predmetu.

 - Odabrani sadržaj prikazuje se pored **Subject**.
 - Isti sadržaj ne može biti prikazan s lijeve i s desne strane.
 - Kad broj znakova u **Location** prekoračuje 32 bita, znakovi koji premašuju 32 bita se izostavljaju.

- Unesite adresu e-pošte za slanje obavijesti e-poštom.
Koristite A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @ i unesite između 1 i 255 znakova.
- Odaberite jezik za obavijesti e-poštom.
- Odaberite potvrdni okvir za događaj za koji želite primiti obavijest.
Broj **Notification Settings** povezan je s brojem odredišta u **Email Address Settings**.
Primjer:
Ako želite poslati obavijest na adresu e-pošte postavljenu za broj 1 pod **Email Address Settings** kada se promijeni lozinka administratora, odaberite potvrdni okvir za stupac **1** u retku **Administrator password changed**.
- Kliknite na **OK**.
Provjerite hoće li obavijest e-poštom biti poslana nakon izazvanog događaja.
Primjer: lozinka administratora je promijenjena.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Stavke za obavijest e-poštom

Stavke	Postavke i pojašnjenja
Administrator password changed	Obavijest kada se promijeni lozinka administratora.
Scanner error	Obavijest kada je došlo do pogreške skenera.
Wi-Fi greška	Obavijest kada se pojavi greška bežičnog LAN sučelja.

Rješavanje problema

Zaboravili ste lozinku administratora

Trebate pomoć servisnog osoblja. Obratite se lokalnom zastupniku.

Napomena:

U nastavku se navode početne vrijednosti Web Config administratora.

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

Kako biste pronašli serijski broj, provjerite naljepnicu na stražnjoj strani skenera. Ako vratite zadane postavke lozinke administratora, resetira se na početne vrijednosti.

Napredne sigurnosne postavke

Sigurnosne postavke i sprječavanje opasnosti.	93
Upravljanje uporabom protokola.	94
Korištenje digitalnog certifikata.	97
SSL/TLS komunikacija sa skenerom.	102
Kriptirana komunikacija korištenjem IPsec/IP filtriranja.	104
Spajanje skenera s IEEE802.1X mrežom.	115
Rješavanje problema napredne sigurnosti.	117

Sigurnosne postavke i sprječavanje opasnosti

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

Za skenere koji nemaju zaštitu pristupa izvana moguće je preko interneta iščitati zapisnike kontakata koji su spremljeni u skeneru.

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

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

Naziv	Vrsta značajke	Što podesiti	Što spriječiti
Nadzor protokola	Nadzire protokol i usluge namijenjene komunikaciji između skenera i računala, a također aktivira i deaktivira značajke.	Protokol ili usluga koja se primjenjuje na sve značajke koje su zasebno odobrene ili zabranjene.	Smanjuje rizike koji se mogu pojaviti zbog neplanirane uporabe, sprječavajući korisnike da koriste nepotrebne funkcije.
SSL/TLS komunikacija	Sadržaj komunikacije kriptiran pomoću SSL/TLS komunikacija prilikom pristupanja Epson poslužitelju na Internetu sa skenera, primjerice pri komunikaciji s računalom preko web-preglednika koristeći Epson Connect i firmver za ažuriranje.	Pribavite CA-potpisani certifikat te ga uvezite na skener.	Uklanjanje identifikacije skenera preko CA-potpisanog certifikata sprječava krađu identiteta i neovlašteni pristup. Također je zaštićen sadržaj komunikacije za SSL/TLS te sprječava curenje sadržaja za skeniranje podataka i informacija o postavkama.
IPsec/IP filtriranje	Možete postaviti dozvolu prekidanja i rezanja podataka određenog klijenta ili vrste. S obzirom da IPsec štiti podatke preko IP paketne jedinice (kriptiranje i provjera autentičnosti), možete sigurno komunicirati neosiguranim protokolom.	Kreirajte osnovno i individualno pravilo za postavljanje klijenta ili vrste podataka koji mogu pristupiti skeneru.	Zaštite od neovlaštenog pristupa, falsificiranja i presretanja komunikacijskih podataka prema skeneru.
IEEE 802.1X	Omogućava samo odobrenim korisnicima povezivanje s mrežom. Dozvoljava uporabu skenera samo korisniku koji ima dozvolu.	Postavke provjere autentičnosti na RADIUS poslužitelju (poslužitelj za provjeru autentičnosti).	Štiti od neovlaštenog pristupa i zlouporabe skenera.

Povezane informacije

- ➔ [“Upravljanje uporabom protokola” na strani 94](#)
- ➔ [“SSL/TLS komunikacija sa skenerom” na strani 102](#)
- ➔ [“Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 104](#)
- ➔ [“Spajanje skenera s IEEE802.1X mrežom” na strani 115](#)

Postavke sigurnosne značajke

Kod postavljanja IPsec/IP filtriranja ili IEEE 802.1X preporučuje se da pristupite programu Web Config koristeći SSL/TLS za prijenos informacija o postavkama kako bi se smanjili sigurnosni rizici poput falsificiranja ili presretanja komunikacije.

Obvezno konfigurirajte lozinku administratora prije postavljanja IPsec/IP filtriranja ili IEEE 802.1X.

Upravljanje uporabom protokola

Možete skenirati koristeći različite putanje i protokole. Također možete koristiti mrežno skeniranje preko nedefiniranog broja mrežnih računala.

Mogućnost pojave neželjenih sigurnosnih opasnosti možete smanjiti onemogućavanjem skeniranja preko određenih putanja ili upravljanjem dostupnim funkcijama.

Upravljanje protokolima

Konfigurirajte postavke protokola koje podržava skener.

1. Pristupite aplikaciji Web Config, a zatim odaberite karticu **Network Security** tab > **Protocol**.
2. Konfigurirajte svaku stavku.
3. Kliknite na **Next**.
4. Kliknite na **OK**.
Postavke će se primijeniti na skener.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Protokoli koje možete omogućiti ili onemogućiti

Protokol	Opis
Bonjour Settings	Možete odrediti hoćete li koristiti Bonjour. Bonjour se koristi za pretraživanje uređaja, skeniranja i tako dalje.
SLP Settings	Funkciju SLP možete omogućiti i onemogućiti. SLP se koristi za skeniranje sa slanjem i pretraživanje mreže u programu EpsonNet Config.
WSD Settings	Funkciju WSD možete omogućiti i onemogućiti. Kada se omogući, možete dodati WSD uređaje ili skenirati preko WSD ulaza.
LLTD Settings	Funkciju LLTD možete omogućiti i onemogućiti. Kada je ona omogućena, bit će prikazana u mapi mreže sustava Windows.
LLMNR Settings	Funkciju LLMNR možete omogućiti i onemogućiti. Kada je ona omogućena, možete koristiti razlučivanje naziva bez usluge NetBIOS, čak i ako ne možete koristiti DNS.

Protokol	Opis
SNMPv1/v2c Settings	Možete odrediti hoće li biti omogućen protokol SNMPv1/v2c. On se koristi za postavljanje uređaja, praćenje itd.
SNMPv3 Settings	Možete odrediti hoće li biti omogućen protokol SNMPv3. Koristi se za postavljanje kriptiranih uređaja, nadziranje, itd.

Stavke postavljanja protokola

Bonjour Settings

Stavke	Postavljanje vrijednosti i opisa
Use Bonjour	Označite ovu stavku ako želite pretraživanje ili korištenje uređaja pomoću usluge Bonjour.
Bonjour Name	Prikazuje naziv za Bonjour.
Bonjour Service Name	Prikazuje naziv usluge Bonjour.
Location	Prikazuje naziv Bonjour lokacije.
Wide-Area Bonjour	Postavite ako želite koristiti Wide-Area Bonjour.

SLP Settings

Stavke	Postavljanje vrijednosti i opisa
Enable SLP	Odaberite ovu stavku ako želite omogućiti funkciju SLP. To se koristi kod pretraživanja mreže u aplikaciji EpsonNet Config.

WSD Settings

Stavke	Postavljanje vrijednosti i opisa
Enable WSD	Odaberite ovu stavku ako želite omogućiti dodavanje uređaja koristeći WSD te ispisivati preko ulaza WSD.
Scanning Timeout (sec)	Unesite vrijednost isteka vremena komunikacije za WSD skeniranje, između 3 i 3 600 sekundi.
Device Name	Prikazuje naziv WSD uređaja.
Location	Prikazuje naziv WSD lokacije.

LLTD Settings

Stavke	Postavljanje vrijednosti i opisa
Enable LLTD	Odabirom ove stavke omogućit ćete LLTD. Skener se prikazuje u mapi mreže sustava Windows.
Device Name	Prikazuje naziv LLTD uređaja.

LLMNR Settings

Stavke	Postavljanje vrijednosti i opisa
Enable LLMNR	Odabirom ove stavke omogućit ćete LLMNR. Razlučivanje naziva možete koristiti bez značajke NetBIOS čak i ako ne možete koristiti DNS.

SNMPv1/v2c Settings

Stavke	Postavljanje vrijednosti i opisa
Enable SNMPv1/v2c	Odaberite ako želite omogućiti SNMPv1/v2c.
Access Authority	Postavite ovlašteno tijelo za pristup kada je omogućen protokol SNMPv1/v2c. Odaberite Read Only ili Read/Write .
Community Name (Read Only)	Unesite 0 do 32 znaka ASCII koda (0x20 do 0x7E).
Community Name (Read/Write)	Unesite 0 do 32 znaka ASCII koda (0x20 do 0x7E).

SNMPv3 Settings

Stavke	Postavljanje vrijednosti i opisa
Enable SNMPv3	SNMPv3 je aktiviran kada je označen potvrdni kvadratić.
User Name	Unesite između 1 i 32 znaka koristeći 1-bitne znakove.
Authentication Settings	
Algorithm	Odaberite algoritam za autentikaciju za SNMPv3.
Password	Odaberite lozinku za autentikaciju za SNMPv3. Unesite od 8 do 32 znaka u ASCII kodu (0x20–0x7E). Ako to ne navedete, ostavite prazno polje.
Confirm Password	Za potvrdu unesite lozinku koju ste postavili.
Encryption Settings	
Algorithm	Odaberite algoritam za enkripciju za SNMPv3.
Password	Odaberite lozinku za enkripciju za SNMPv3. Unesite od 8 do 32 znaka u ASCII kodu (0x20–0x7E). Ako to ne navedete, ostavite prazno polje.
Confirm Password	Za potvrdu unesite lozinku koju ste postavili.
Context Name	Unesite najviše 32 znaka Unicode (UTF-8). Ako to ne navedete, ostavite prazno polje. Broj znakova koji se mogu unijeti razlikuje se ovisno o jeziku.

Korištenje digitalnog certifikata

O digitalnom certificiranju

CA-signed Certificate

Ovo je certifikat koje je izdalo tijelo koje izdaje digitalne certifikate (CA) Možete ga pribaviti tako da ga zatražite od tijela koje izdaje digitalne certifikate. Ovaj certifikat potvrđuje prisutnost skenera i koristit se za SSL/TLS komunikaciju tako da možete osigurati sigurnost podatkovne komunikacije.

Kada se koristi za SSL/TLS komunikaciju, koristi se kao certifikat poslužitelja.

Kada je postavljen za IPsec/IP filtriranje ili IEEE 802.1X komunikaciju, koristi se kao certifikat klijenta.

CA certifikat

To je certifikat koji je u lancu s CA-signed Certificate i naziva se i srednji CA certifikat. Koristi ga web-preglednik za odobrenje putanje certifikata skenera prilikom pristupa poslužitelju druge strane ili aplikaciji Web Config.

Za CA certifikat odredite kada ćete odobriti putanju certifikatu poslužitelja kojem se pristupa preko skenera. Kod skenera postavite za potvrđivanje putanje CA-signed Certificate za SSL/TLS vezu.

Možete dobiti CA certifikat skenera od tijela koje izdaje digitalne certifikate.

Nadalje, možete pribaviti CA certifikat koji se koristi za potvrđivanje poslužitelja druge strane od tijela koje izdaje CA-signed Certificate drugih poslužitelja.

Self-signed Certificate

Ovaj certifikat skener sam potpisuje i izdaje. Još se naziva i korijenski certifikat. Budući da izdavatelj sam sebe certificira, nije pouzdan i ne može spriječiti krađu identiteta.

Koristite ga prilikom određivanja sigurnosnih postavki i provođenja jednostavne SSL/TLS komunikacije bez CA-signed Certificate.

Ako koristite ovaj certifikat za SSL/TLS komunikaciju, u pregledniku će se možda prikazati sigurnosno upozorenje jer certifikat nije registriran na web-pregledniku. Self-signed Certificate možete koristiti samo za SSL/TLS komunikaciju.

Povezane informacije

- ➔ [“Konfiguriranje CA-signed Certificate” na strani 97](#)
- ➔ [“Ažuriranje samopotpisanog certifikata” na strani 101](#)
- ➔ [“Konfiguriranje CA Certificate” na strani 101](#)

Konfiguriranje CA-signed Certificate

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

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

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

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

Što god odabrali možete pribaviti isti certifikat i koristiti ga uobičajeno.

2. Pritisnite **Generate** u **CSR**.

Otvara se stranica za izradu zahtjeva za potpisivanje certifikata.

3. Unesite vrijednost svake stavke.

Napomena:

Dostupne duljine ključeva i kratica ovise o tijelu koje izdaje digitalni certifikat. Izradite zahtjev prema pravilima pojedinog tijela.

4. Kliknite na **OK**.

Prikazuje se poruka o dovršetku.

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

6. Pritisnite gumbe za preuzimanje u **CSR** prema formatu određenom od strane tijela za izdavanje digitalnih certifikata kako biste zahtjev za potpisivanje certifikata preuzeli na računalo.



Važno:

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

7. Pošaljite CSR tijelu za izdavanje certifikata i pribavite CA-signed Certificate.

Slijedite pravila svakog tijela za izdavanje certifikata u vezi sa načinom slanja i formularom.

8. Spremite izdani CA-signed Certificate na računalo povezano sa skenerom.

Pribavljanje CA-signed Certificate je dovršeno kada certifikat spremite na odredište.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Stavke postavljanja zahtjeva za potpisivanje certifikata

Stavke	Postavke i pojašnjenja
Key Length	Odaberite duljinu ključa za zahtjev za potpisivanje certifikata.

Stavke	Postavke i pojašnjenja
Common Name	<p>Možete unijeti između 1 i 128 znakova. Ako se radi o IP adresi, to mora biti statična IP adresa. Možete unijeti od 1 do 5 IPv4 adresa, IPv6 adresa, naziva domaćina, FQDN-ova odvojenih zarezom.</p> <p>Prvi element je spremljen kao zajednički naziv, a drugi elementi su spremljeni u polje pseudonima subjekta certifikata.</p> <p>Primjer:</p> <p>IP adresa skenera: 192.0.2.123, Naziv skenera: EPSONA1B2C3</p> <p>Common Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123</p>
Organization/ Organizational Unit/ Locality/ State/Province	Možete unijeti od 0 do 64 znaka u ASCII kodu (0x20–0x7E). Nazive možete odvojiti zarezima.
Country	Unesite dvoznamenkasti broj šifre zemlje određen standardom ISO-3166.
Sender's Email Address	Možete unijeti adresu e-pošte pošiljatelja za postavku poslužitelja e-pošte. Unesite istu adresu e-pošte kao Sender's Email Address za karticu Network > Email Server > Basic .

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

Uvezite pribavljeni CA-signed Certificate na skener.



Važno:

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

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

2. Kliknite na **Import**

Otvora se stranica za uvoz certifikata.

3. Unesite vrijednost svake stavke. Postavite **CA Certificate 1** i **CA Certificate 2** kada potvrđujete putanju certifikata na web-pregledniku kojim pristupate skeneru.

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

- Certifikat u PEM/DER formatu dobiven od strane Web Config
 - Private Key:** nemojte konfigurirati, jer skener sadrži privatni ključ.
 - Password:** nemojte konfigurirati.
 - CA Certificate 1/CA Certificate 2:** dodatno
- Certifikat u PEM/DER formatu dobiven s računala
 - Private Key:** trebete postaviti.
 - Password:** nemojte konfigurirati.
 - CA Certificate 1/CA Certificate 2:** dodatno

- Certifikat u PKCS#12 formatu dobiven s računala
 - Private Key**: nemojte konfigurirati.
 - Password**: dodatno
 - CA Certificate 1/CA Certificate 2**: nemojte konfigurirati.

4. Kliknite na OK.

Prikazuje se poruka o dovršetku.

Napomena:

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

Povezane informacije

➔ “Pokretanje programa Web Config u internetskom pregledniku” na strani 35

Postavljanje stavki za uvoz certifikata koji je potpisalo tijelo za izdavanje digitalnih certifikata (CA)

Stavke	Postavke i pojašnjenja
Server Certificate ili Client Certificate	Odaberite format certifikata. Za SSL/TLS vezu prikazan je Server Certificate. Za IPsec/IP filtriranje ili IEEE 802.1X prikazan je Client Certificate.
Private Key	Ako možete dobiti certifikat PEM/DER formata pomoću zahtjeva za potpisivanje certifikata (CSR) izrađenog na računalu, navedite datoteku privatnog ključa koja se podudara s certifikatom.
Password	Ako je format datoteke Certificate with Private Key (PKCS#12) , unesite lozinku za šifriranje privatnog ključa koji je postavljen kada pribavite certifikat.
CA Certificate 1	Ako je format certifikata Certificate (PEM/DER) , unesite certifikat CA-signed Certificate koji izdaje tijelo za certifikate koji se koristi kao certifikat za poslužitelj. Odredite datoteku ako je to potrebno.
CA Certificate 2	Ako je format certifikata Certificate (PEM/DER) , uvezite certifikat koji izdaje tijelo za certifikate CA Certificate 1. Odredite datoteku ako je to potrebno.

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

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



Važno:

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

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

2. Kliknite na **Delete**.
3. U prikazanoj poruci potvrdite da želite izbrisati certifikat.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Ažuriranje samopotpisanog certifikata

Self-signed Certificate izdaje skener i stoga ga možete ažurirati kada istekne ili kada se promijeni opis sadržaj.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network Security** tab > **SSL/TLS** > **Certificate**.

2. Kliknite na **Update**.

3. Unesite **Common Name**.

Možete unijeti do 5 IPv4 adresa, IPv6 adresa, naziva glavnog računala, FQDN-ovi od 1 do 128 znakova i odvajanjem zarezom. Prvi parametar pohranjen je za standardni naziv, a ostali su pohranjeni za polje pseudonima predmeta certifikata.

Primjer:

IP adresa skenera: 192.0.2.123, Naziv skenera: EPSONA1B2C3

Standardni naziv: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Odredite razdoblje valjanosti certifikata.

5. Kliknite na **Next**.

Prikazuje se poruka potvrde.

6. Kliknite na **OK**.

Skener se ažurira.

Napomena:

Možete provjeriti informacije certifikata iz kartice **Network Security** > **SSL/TLS** > **Certificate** > **Self-signed Certificate** i kliknite **Confirm**.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Konfiguriranje CA Certificate

Kada odredite CA Certificate, možete provjeriti putanju CA certifikata poslužitelja kojem pristupa skener. To može spriječiti krađu identiteta.

Možete nabaviti CA Certificate preko dijela za ovlaštenje certifikata koji izdaje CA-signed Certificate.

Uvoz CA Certificate

Uvezite CA Certificate na skener.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network Security > CA Certificate**.
2. Kliknite na **Import**.
3. Odredite CA Certificate koji želite uvesti.
4. Kliknite na **OK**.

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

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Brisanje CA Certificate

Možete izbrisati uvezeni CA Certificate.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network Security > CA Certificate**.
2. Kliknite na **Delete** pored CA Certificate kojeg želite izbrisati.
3. U prikazanoj poruci potvrdite da želite izbrisati certifikat.
4. Kliknite na **Reboot Network**, a zatim provjerite je li izbrisani CA certifikat naveden na ažuriranom zaslonu.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

SSL/TLS komunikacija sa skenerom

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

Konfiguriranje osnovnih SSL/TLS postavki

Ako skener podržava značajku HTTPS, možete koristiti SSL/TLS komunikaciju za kriptiranje komunikacije. Možete konfigurirati i upravljati skenerom pomoću softvera Web Config dok u isto vrijeme osiguravate sigurnost.

Konfigurirajte jačinu kriptiranja i značajku preusmjerenja.

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

2. Odaberite vrijednost za svaki stavku.
 - Encryption Strength
Odaberite jačinu kriptiranja.
 - Redirect HTTP to HTTPS
Preusmjeri na HTTPS u slučaju pristupa HTTP-u.
3. Kliknite na **Next**.
Prikazuje se poruka potvrde.
4. Kliknite na **OK**.
Skener se ažurira.

Povezane informacije

- ➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Konfiguriranje certifikata poslužitelja za skener

1. Pristupite aplikaciji Web Config i odaberite karticu **Network Security > SSL/TLS > Certificate**.
2. Navedite certifikat koji će se koristiti za **Server Certificate**.
 - Self-signed Certificate
Za skener je generiran samopotpisani certifikat. Ako nemate certifikat koji je potpisan od strane tijela za izdavanje certifikata (CA), odaberite ovo.
 - CA-signed Certificate
Ako unaprijed dobijete i uvezete certifikat koji je potpisalo tijelo za izdavanje certifikata (CA), možete odrediti ovo.
3. Kliknite na **Next**.
Prikazuje se poruka potvrde.
4. Kliknite na **OK**.
Skener se ažurira.

Povezane informacije

- ➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)
- ➔ [“Konfiguriranje CA-signed Certificate” na strani 97](#)
- ➔ [“Konfiguriranje CA Certificate” na strani 101](#)

Kriptirana komunikacija korištenjem IPsec/IP filtriranja

O aplikaciji IPsec/IP Filtering

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

Napomena:

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

Konfiguriranje zadanih pravila

Za filtriranje prometa konfigurirajte zadana pravila. Zadana pravila primjenjuju se na svakog korisnika ili grupu koja se spaja na skener. Za finije kontrole korisnika i grupa korisnika konfigurirajte grupna pravila.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network Security > IPsec/IP Filtering > Basic**.
2. Unesite vrijednost svake stavke.
3. Kliknite na **Next**.
Prikazuje se poruka potvrde.
4. Kliknite na **OK**.
Skener se ažurira.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Postavljanje stavki za Default Policy

Default Policy

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

Access Control

Konfigurirajte metodu kontrole prometa za IP pakete.

Stavke	Postavke i pojašnjenja
Permit Access	Odaberite ovo za dopuštenje prolaza konfiguriranim IP paketima.
Refuse Access	Odaberite ovo za odbijanje prolaza konfiguriranim IP paketima.
IPsec	Odaberite ovo za dopuštenje prolaza konfiguriranim IPsec paketima.

IKE Version

Odaberite **IKEv1** ili **IKEv2** za **IKE Version**. Odaberite jedan njih sukladno uređaju na koji je spojen skener.

IKEv1

Sljedeće stavke prikazane su ako odaberete **IKEv1** za **IKE Version**.

Stavke	Postavke i pojašnjenja
Authentication Method	Kako biste mogli odabrati Certificate , trebate unaprijed nabaviti i uvesti certifikat koji je potpisalo tijelo za izdavanje certifikata (CA).
Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.

IKEv2

Sljedeće stavke prikazane su ako odaberete **IKEv2** za **IKE Version**.

Stavke	Postavke i pojašnjenja	
Local	Authentication Method	Kako biste mogli odabrati Certificate , trebate unaprijed nabaviti i uvesti certifikat koji je potpisalo tijelo za izdavanje certifikata (CA).
	ID Type	Ako odaberete Pre-Shared Key za Authentication Method , odaberite vrstu identifikacije za skener.
	ID	Unesite ID skenera koji odgovara vrsti ID-a. Ne možete koristiti „@“, „#“ i „=“ kao prvi znak. Distinguished Name: unesite 1 do 255 jednobajtnih ASCII (0x20 do 0x7E) znakova. Trebate uključiti „=“. IP Address: unesite IPv4 ili IPv6 format. FQDN: unesite kombinaciju između 1 i 255 znakova koristeći A–Z, a–z, 0–9, „-“ i točku (.). Email Address: unesite 1 do 255 jednobajtnih ASCII (0x20 do 0x7E) znakova. Trebate uključiti „@“. Key ID: unesite 1 do 255 jednobajtnih ASCII (0x20 do 0x7E) znakova.
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.

Stavke		Postavke i pojašnjenja
Remote	Authentication Method	Kako biste mogli odabrati Certificate , trebate unaprijed nabaviti i uvesti certifikat koji je potpisalo tijelo za izdavanje certifikata (CA).
	ID Type	Ako odaberete Pre-Shared Key za Authentication Method , odaberite vrstu identifikacije za uređaj kojem želite provjeriti autentičnost.
	ID	Unesite ID skenera koji odgovara vrsti ID-a. Ne možete koristiti „@“, „#“ i „=“ kao prvi znak. Distinguished Name: unesite 1 do 255 jednobajtnih ASCII (0x20 do 0x7E) znakova. Trebate uključiti „=“. IP Address: unesite IPv4 ili IPv6 format. FQDN: unesite kombinaciju između 1 i 255 znakova koristeći A–Z, a–z, 0–9, „-“ i točku (.). Email Address: unesite 1 do 255 jednobajtnih ASCII (0x20 do 0x7E) znakova. Trebate uključiti „@“. Key ID: unesite 1 do 255 jednobajtnih ASCII (0x20 do 0x7E) znakova.
	Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
	Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.

Encapsulation

Ako odaberete **IPsec** za **Access Control**, trebate konfigurirati način skrivanja podataka („encapsulation”).

Stavke	Postavke i pojašnjenja
Transport Mode	Ako koristite samo skener u istoj LAN mreži, odaberite ovo. IP paketi sloja 4 ili kasniji su kriptirani.
Tunnel Mode	Ako koristite skener na mreži s pristupom internetu, kao što je IPsec-VPN, odaberite ovu opciju. Zaglavlje („header”) i podaci IP paketa su kriptirani. Remote Gateway(Tunnel Mode): ako odaberete Tunnel Mode za Encapsulation , unesite adresu pristupnika duljine od 1 do 39 znakova.

Security Protocol

Ako odaberete **IPsec** za **Access Control**, odaberite opciju.

Stavke	Postavke i pojašnjenja
ESP	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka te kako biste kriptirali podatke.
AH	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka. Čak i ako je kriptiranje podataka zabranjeno, možete koristiti IPsec.

❑ Algorithm Settings

Preporučujemo da odaberete **Any** za sve postavke ili odaberite drugu stavku osim **Any** za svaku postavku. Ako odaberete **Any** za neku od postavki i odaberete drugu stavku osim **Any** za druge postavke, uređaj možda neće imati komunikaciju ovisno o drugim uređajima kojima želite provjeriti autentičnost.

Stavke		Postavke i pojašnjenja
IKE	Encryption	Odaberite algoritam enkripcije za IKE. Stavke se razlikuju ovisno o verziji IKE-a.
	Authentication	Odaberite algoritam za provjeru autentičnosti za IKE.
	Key Exchange	Odaberite algoritam zamjene ključa za IKE. Stavke se razlikuju ovisno o verziji IKE-a.
ESP	Encryption	Odaberite algoritam enkripcije za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
	Authentication	Odaberite algoritam autentikacije za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
AH	Authentication	Odaberite algoritam enkripcije za AH. To će biti dostupno kada AH bude odabran za Security Protocol .

Konfiguriranje grupnih pravila

Grupna pravila su jedno ili više pravila koja se primjenjuju za korisnika ili grupu korisnika. Skener kontrolira IP pakete koji se podudaraju s konfiguriranim pravilima. IP paketi su autentificirani u poretku grupnih pravila 1 do 10, zatim u poretku zadanih pravila.

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

Postavljanje stavki za Group Policy

Stavke	Postavke i pojašnjenja
Enable this Group Policy	Možete omogućiti ili onemogućiti grupna pravila.

Access Control

Konfigurirajte metodu kontrole prometa za IP pakete.

Stavke	Postavke i pojašnjenja
Permit Access	Odaberite ovo za dopuštenje prolaza konfiguriranim IP paketima.
Refuse Access	Odaberite ovo za odbijanje prolaza konfiguriranim IP paketima.
IPsec	Odaberite ovo za dopuštenje prolaza konfiguriranim IPsec paketima.

Local Address (Scanner)

Odaberite IPv4 ili IPv6 adresu koja odgovara okruženju vaše mreže. Ako je IP adresa dodijeljena automatski, možete odabrati **Use auto-obtained IPv4 address**.

Napomena:

Ako je IPv6 adresa dodijeljena automatski, veza možda neće biti dostupna. Konfigurirajte statičnu IPv6 adresu.

Remote Address(Host)

Unesite IP adresu uređaja za kontrolu pristupa. IP adresa mora sadržavati najviše 43 znaka. Ako ne unesete IP adresu, sve će se adrese kontrolirati.

Napomena:

Ako je IP adresa dodijeljena automatski (npr. ako ju je dodijelio DHCP), veza možda neće biti dostupna. Konfigurirajte statičnu IP adresu.

Method of Choosing Port

Odaberite način određivanja ulaza.

Service Name

Ako odaberete **Service Name** za **Method of Choosing Port**, odaberite opciju.

Transport Protocol

Ako odaberete **Port Number** za **Method of Choosing Port**, trebate konfigurirati način skrivanja podataka („encapsulation”).

Stavke	Postavke i pojašnjenja
Any Protocol	Odaberite ovo za kontroliranje svih vrsta protokola.
TCP	Odaberite ovo za kontroliranje podataka za jednosmjerni prijenos („unicast”).
UDP	Odaberite ovo za kontrolu podataka za emitiranje („broadcast”) i ciljano emitiranje („multicast”).
ICMPv4	Odaberite ovo za kontrolu ping naredbe.

Local Port

Ako odaberete **Port Number** za **Method of Choosing Port** i ako odaberete **TCP** ili **UDP** za **Transport Protocol**, unesite brojeve ulaza za provjeru primanja paketa i odvojite ih zarezima. Možete unijeti maksimalno 10 brojeva ulaza.

Primjer: 20,80,119,5220

Ako ne unesete broj ulaza, svi ulazi se kontroliraju.

Remote Port

Ako odaberete **Port Number** za **Method of Choosing Port** i ako odaberete **TCP** ili **UDP** za **Transport Protocol**, unesite brojeve ulaza za provjeru slanja paketa i odvojite ih zarezima. Možete unijeti maksimalno 10 brojeva ulaza.

Primjer: 25,80,143,5220

Ako ne unesete broj ulaza, svi ulazi se kontroliraju.

IKE Version

Odaberite **IKEv1** ili **IKEv2** za **IKE Version**. Odaberite jedan njih sukladno uređaju na koji je spojen skener.

IKEv1

Sljedeće stavke prikazane su ako odaberete **IKEv1** za **IKE Version**.

Stavke	Postavke i pojašnjenja
Authentication Method	Ako odaberete IPsec za Access Control , odaberite opciju. Korišteni certifikat je uobičajen sa zadanim pravilima.
Pre-Shared Key	Ako odaberete Pre-Shared Key za Authentication Method , unesite unaprijed postavljeni zajednički ključ duljine od 1 do 127 znakova.
Confirm Pre-Shared Key	Za potvrdu unesite konfigurirani ključ.

IKEv2

Sljedeće stavke prikazane su ako odaberete **IKEv2** za **IKE Version**.

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

Encapsulation

Ako odaberete **IPsec** za **Access Control**, trebate konfigurirati način skrivanja podataka („encapsulation”).

Stavke	Postavke i pojašnjenja
Transport Mode	Ako koristite samo skener u istoj LAN mreži, odaberite ovo. IP paketi sloja 4 ili kasniji su kriptirani.
Tunnel Mode	Ako koristite skener na mreži s pristupom internetu, kao što je IPsec-VPN, odaberite ovu opciju. Zaglavlje („header“) i podaci IP paketa su kriptirani. Remote Gateway(Tunnel Mode): ako odaberete Tunnel Mode za Encapsulation , unesite adresu pristupnika duljine od 1 do 39 znakova.

Security Protocol

Ako odaberete **IPsec** za **Access Control**, odaberite opciju.

Stavke	Postavke i pojašnjenja
ESP	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka te kako biste kriptirali podatke.
AH	Odaberite kako biste osigurali integritet provjere autentičnosti i podataka. Čak i ako je kriptiranje podataka zabranjeno, možete koristiti IPsec.

Algorithm Settings

Preporučujemo da odaberete **Any** za sve postavke ili odaberite drugu stavku osim **Any** za svaku postavku. Ako odaberete **Any** za neku od postavki i odaberete drugu stavku osim **Any** za druge postavke, uređaj možda neće imati komunikaciju ovisno o drugim uređajima kojima želite provjeriti autentičnost.

Stavke	Postavke i pojašnjenja	
IKE	Encryption	Odaberite algoritam enkripcije za IKE. Stavke se razlikuju ovisno o verziji IKE-a.
	Authentication	Odaberite algoritam za provjeru autentičnosti za IKE.
	Key Exchange	Odaberite algoritam zamjene ključa za IKE. Stavke se razlikuju ovisno o verziji IKE-a.
ESP	Encryption	Odaberite algoritam enkripcije za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
	Authentication	Odaberite algoritam autentikacije za ESP. To će biti dostupno kada ESP bude odabran za Security Protocol .
AH	Authentication	Odaberite algoritam enkripcije za AH. To će biti dostupno kada AH bude odabran za Security Protocol .

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

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

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

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

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

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

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Reference naziva usluga na značajci Pravila grupe

Napomena:

Nedostupne usluge prikazuju se, no ne mogu se odabrati.

Naziv usluge	Vrsta protokola	Broj lokalnog priključka	Broj udaljenog priključka	Kontrolirane značajke
Any	–	–	–	Sve usluge
ENPC	UDP	3289	Bilo koji ulaz	Pretraživanje skenera iz aplikacija kao što je Epson Device Admin i upravljačkog programa skenera
SNMP	UDP	161	Bilo koji ulaz	Dobivanje i konfiguriranje MIB-a iz aplikacija kao što je Epson Device Admin i Epson upravljačkog programa skenera
WSD	TCP	Bilo koji ulaz	5357	Kontroliranje WSD-a
WS-Discovery	UDP	3702	Bilo koji ulaz	Traženje WSD skenera
Network Scan	TCP	1865	Bilo koji ulaz	Preusmjeravanje skeniranih podataka iz Document Capture Pro
Network Push Scan	TCP	Bilo koji ulaz	2968	Prikupljanje informacija za prosljeđivanje skeniranih stranica iz Document Capture Pro
Network Push Scan Discovery	UDP	2968	Bilo koji ulaz	Traženje računala preko skenera
FTP Data (Remote)	TCP	Bilo koji ulaz	20	FTP klijent (prosljeđivanje skeniranih podataka) Međutim, ovime se može kontrolirati samo FTP poslužitelj koji koristi udaljeni ulaz broj 20.
FTP Control (Remote)	TCP	Bilo koji ulaz	21	FTP klijent (provjera prosljeđivanja skeniranih podataka)

Naziv usluge	Vrsta protokola	Broj lokalnog priključka	Broj udaljenog priključka	Kontrolirane značajke
CIFS (Remote)	TCP	Bilo koji ulaz	445	CIFS klijent (prosljeđivanje skeniranih podataka u mapu)
NetBIOS Name Service (Remote)	UDP	Bilo koji ulaz	137	CIFS klijent (prosljeđivanje skeniranih podataka u mapu)
NetBIOS Datagram Service (Remote)	UDP	Bilo koji ulaz	138	
NetBIOS Session Service (Remote)	TCP	Bilo koji ulaz	139	
HTTP (Local)	TCP	80	Bilo koji ulaz	HTTP(S) poslužitelj (preusmjeravanje podataka aplikacije Web Config i WSD)
HTTPS (Local)	TCP	443	Bilo koji ulaz	
HTTP (Remote)	TCP	Bilo koji ulaz	80	HTTP(S) klijent (ažuriranje firmvera i korijenskog certifikata)
HTTPS (Remote)	TCP	Bilo koji ulaz	443	

Primjeri konfiguracije za IPsec/IP Filtering

Samo za dolazne IPsec pakete

Ovaj primjer je samo za konfiguriranje zadanih pravila.

Default Policy:

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

Group Policy: nemojte konfigurirati.

Primanje podataka o skeniranju i postavke skenera

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

Default Policy:

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

Group Policy:

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

Dobivanje pristupa samo s određene IP adrese

Ovaj primjer određenoj IP adresi omogućuje pristup skeneru.

Default Policy:

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

Group Policy:

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

Napomena:

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

Konfiguriranje certifikata za IPsec/IP filtriranje

Konfigurirajte certifikat klijenta za IPsec/IP filtriranje. Kada postavite, možete koristiti certifikat kao način provjere autentičnosti za IPsec/IP filtriranje. Ako želite konfigurirati tijelo za izdavanje certifikata, uđite u **CA Certificate**.

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

Ako ste već uvezli certifikat kojeg je izdalo tijelo za izdavanje certifikata, možete kopirati certifikat i koristiti ga s funkcijom IPsec/IP filtriranje. Za kopiranje odaberite certifikat u **Copy From** pa kliknite **Copy**.

Povezane informacije

- ➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)
- ➔ [“Konfiguriranje CA-signed Certificate” na strani 97](#)
- ➔ [“Konfiguriranje CA Certificate” na strani 101](#)

Spajanje skenera s IEEE802.1X mrežom

Konfiguriranje IEEE 802.1X mreže

Kada na skeneru postavite IEEE 802.1X, možete ga koristiti na mreži spojenoj na RADIUS poslužitelja, LAN priključak s funkcijom potvrđivanja autentičnosti ili na pristupnu točku.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network Security > IEEE802.1X > Basic**.
2. Unesite vrijednost svake stavke.

Ako želite koristiti skener na Wi-Fi mreži, kliknite na **Wi-Fi Setup** i odaberite ili unesite SSID.

Napomena:

Možete primijeniti iste postavke za Ethernet i Wi-Fi.

3. Kliknite na **Next**.
Prikazuje se poruka potvrde.
4. Kliknite na **OK**.
Skener se ažurira.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Stavke za postavljanje IEEE 802.1X mreže

Stavke	Postavke i pojašnjenja
IEEE802.1X (Wired LAN)	Možete omogućiti ili onemogućiti postavke stranice (IEEE802.1X > Basic) za IEEE802.1X (žičani LAN).
IEEE802.1X (Wi-Fi)	Prikazat će se status veze za IEEE802.1X (Wi-Fi).
Connection Method	Prikazana je metoda povezivanja trenutne mreže.
EAP Type	Odaberite opciju za način provjere autentičnosti između skenera i RADIUS poslužitelja.
EAP-TLS	Trebate pribaviti i uvesti certifikat s potpisom CA.
PEAP-TLS	
PEAP/MSCHAPv2	Trebate postaviti lozinku.
EAP-TTLS	
User ID	Konfigurirajte ID za korištenje autentifikacije RADIUS poslužitelja. Unesite 1 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova.
Password	Konfigurirajte lozinku za provjeru autentičnosti skenera. Unesite 1 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova. Ako Windows poslužitelj koristite kao RADIUS poslužitelj, moći ćete unijeti do 127 znakova.
Confirm Password	Za potvrdu unesite lozinku koju ste postavili.
Server ID	Možete konfigurirati ID poslužitelja za autentifikaciju s određenim RADIUS poslužiteljem. Autentifikator potvrđuje sadrži li polje subject/subjectAltName certifikata poslužitelja ID poslužitelja poslan s RADIUS poslužitelja. Unesite 0 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova.
Certificate Validation	Provjeru valjanosti certifikata možete postaviti neovisno o načinu provjere autentičnosti. Uvezite certifikat u CA Certificate .
Anonymous Name	Ako odaberete PEAP-TLS ili PEAP/MSCHAPv2 za EAP Type , možete postaviti anonimno ime umjesto korisničkog ID-a za fazu 1 PEAP provjere autentičnosti. Unesite 0 do 128 jednobajtnih ASCII (0x20 do 0x7E) znakova.

Stavke	Postavke i pojašnjenja	
Encryption Strength	Možete odabrati nešto od sljedećeg.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Konfiguriranje certifikata za IEEE 802.1X

Konfigurirajte certifikat klijenta za IEEE802.1X. Kada postavite, možete koristiti **EAP-TLS** i **PEAP-TLS** kao način provjere autentičnosti za IEEE 802.1X. Ako želite konfigurirati tijelo za izdavanje certifikata, uđite u **CA Certificate**.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network Security > IEEE802.1X > Client Certificate**.
2. Certifikat unesite u **Client Certificate**.

Ako ste već uvezli certifikat kojeg je izdalo tijelo za izdavanje certifikata, možete kopirati certifikat i koristiti ga u IEEE802.1X. Za kopiranje odaberite certifikat u **Copy From** pa kliknite **Copy**.

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Rješavanje problema napredne sigurnosti

Vraćanje sigurnosnih postavki

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

Onemogućavanje sigurnosne funkcije koristeći Web Config

Možete onemogućiti IPsec/IP Filtering koristeći Web Config.

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

Problemi s korištenjem sigurnosnih značajki mreže

Zaboravljen je unaprijed postavljeni zajednički ključ

Ponovno konfigurirajte unaprijed postavljeni zajednički ključ.

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

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

Povezane informacije

- ➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)
- ➔ [“Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 104](#)

Ne mogu komunicirati s IPsec komunikacijom

Naznačite algoritam koji skener ili računalo ne podržavaju.

Skener podržava sljedeće algoritme. Provjerite postavke računala.

Sigurnosne metode	Algoritmi
IKE algoritam enkripcije	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE algoritam za provjeru autentičnosti	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE algoritam zamjene tipke	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP algoritam enkripcije	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP algoritam za provjeru autentičnosti	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH algoritam za provjeru autentičnosti	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Dostupno samo za IKEv2

Povezane informacije

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

Iznenadna nemogućnost komunikacije

IP adresa skenera je promijenjena ili se ne može koristiti.

Kad je promijenjena IP adresa registrirana za lokalnu adresu u Group Policy ili se ne može koristiti, nije moguće provesti IPsec komunikaciju. Onemogućite IPsec preko upravljačke ploče skenera.

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

Koristite statičnu IP adresu.

IP adresa računala je promijenjena ili se ne može koristiti.

Kad je promijenjena IP adresa registrirana za adrese udaljene lokacije u Group Policy ili se ne može koristiti, nije moguće provesti IPsec komunikaciju.

Onemogućite IPsec preko upravljačke ploče skenera.

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

Koristite statičnu IP adresu.

Povezane informacije

- ➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)
- ➔ [“Kriptirana komunikacija korištenjem IPsec/IP filtriranja” na strani 104](#)

Nije moguće povezivanje nakon konfiguriranja IPsec/IP filtriranja

Postavke IPsec/IP filtriranja nisu točne.

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

Povezane informacije

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

Pristup skeneru nije moguć nakon konfiguriranja mreže IEEE 802.1X

Postavke IEEE 802.1X nisu točne.

Onemogućite IEEE 802.1X i Wi-Fi na upravljačkoj ploči skenera. Povežite skener i računalo, a zatim ponovno konfigurirajte IEEE 802.1X.

Povežite skener i računalo, a zatim ponovno konfigurirajte IEEE 802.1X.

Povezane informacije

- ➔ [“Konfiguriranje IEEE 802.1X mreže” na strani 115](#)

Problemi s korištenjem digitalnog certifikata

Nije moguće uvesti CA-signed Certificate

CA-signed Certificate i informacije na zahtjevu za potpisivanje certifikata se ne podudaraju.

Ako CA-signed Certificate i zahtjev za potpisivanje certifikata ne sadrže iste informacije, zahtjev za potpisivanje certifikata se ne može uvesti. Označite sljedeće:

- Pokušavate li uvesti certifikat na uređaj koji nema iste informacije?
Provjerite informacije na zahtjevu za potpisivanje certifikata, a zatim uvezite certifikat na uređaj koji sadrži iste informacije.
- Jeste li izbrisali zahtjev za potpisivanje certifikata pohranjen na skeneru nakon što ste ga poslali tijelu za izdavanje digitalnih certifikata?
Ponovno pribavite certifikat potpisan od strane tijela za izdavanje certifikata pomoću zahtjeva za potpisivanje certifikata.

CA-signed Certificate ima više od 5KB.

Ne možete uvesti CA-signed Certificate koji je veći od 5 KB.

Lozinka za uvoz certifikata nije ispravna.

Unesite ispravnu lozinku. Ako zaboravite lozinku, ne možete uvesti certifikat. Ponovo pribavite CA-signed Certificate.

Povezane informacije

➔ [“Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 99](#)

Ažuriranje samopotpisanog certifikata nije moguće

Nije unesen Common Name.

Common Name mora biti unesen.

Nepodržani znakovi uneseni su pod Common Name.

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

Standardni naziv sadrži zarez ili prazno mjesto.

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

Povezane informacije

➔ [“Ažuriranje samopotpisanog certifikata” na strani 101](#)

Izrada zahtjeva za potpisivanje certifikata nije moguća

Nije unesen Common Name.

Common Name mora biti unesen.

Nepodržani znakovi uneseni su pod Common Name, Organization, Organizational Unit, Locality i State/Province.

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

Common Name sadrži zarez ili prazno mjesto.

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

Povezane informacije

➔ [“Pribavljanje certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 97](#)

Pojavljuje se upozorenje u vezi s digitalnim certifikatom

Poruke	Uzrok/što napraviti
Enter a Server Certificate.	<p>Uzrok: Niste odabrali datoteku za uvoz.</p> <p>Što napraviti: Odaberite datoteku i pritisnite Import.</p>
CA Certificate 1 is not entered.	<p>Uzrok: CA certifikat 1 nije unesen; unesen je samo certifikat CA 2.</p> <p>Što napraviti: Najprije unesite CA certifikat 1.</p>
Invalid value below.	<p>Uzrok: Lokacija datoteke i/ili lozinka sadrži znakove koji nisu podržani.</p> <p>Što napraviti: Provjerite jesu li za stavku znakovi ispravno uneseni.</p>
Invalid date and time.	<p>Uzrok: Datum i vrijeme za skener nisu postavljeni.</p> <p>Što napraviti: Postavite datum i vrijeme pomoću Web Config ili EpsonNet Config.</p>
Invalid password.	<p>Uzrok: Lozinka unesena za CA certifikat i unesena lozinka se ne podudaraju.</p> <p>Što napraviti: Unesite ispravnu lozinku.</p>

Poruke	Uzrok/što napraviti
Invalid file.	<p>Uzrok:</p> <p>Ne uvozite datoteku certifikata u formatu X509.</p> <p>Što napraviti:</p> <p>Provjerite odabirete li ispravan certifikat poslan od strane pouzdanog tijela za izdavanje certifikata.</p>
	<p>Uzrok:</p> <p>Datoteka koju ste uvezli je prevelika. Maksimalna veličina datoteke je 5 KB.</p> <p>Što napraviti:</p> <p>Ako ste odabrali ispravnu datoteku, certifikat je možda oštećen ili krivotvoren.</p>
	<p>Uzrok:</p> <p>Lanac u certifikatu nije valjan.</p> <p>Što napraviti:</p> <p>Dodatne informacije o certifikatu potražite na internetskoj stranici tijela koje izdaje digitalne certifikate.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p>Uzrok:</p> <p>Datoteka certifikata u formatu PKCS#12 sadrži više od 3 CA certifikata.</p> <p>Što napraviti:</p> <p>Uvezite svaki certifikat konvertiran iz PKCS#12 formata u PEM format ili uvezite datoteku certifikata u PKCS#12 formatu koja sadrži najviše 2 CA certifikata.</p>
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p>Uzrok:</p> <p>Certifikat je istekao.</p> <p>Što napraviti:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ako je certifikat istekao, pribavite i uvezite novi. <input type="checkbox"/> Ako je certifikat istekao, provjerite jesu li datum i vrijeme skenera ispravno postavljeni.
Private key is required.	<p>Uzrok:</p> <p>Nema privatnog ključa uparenog s certifikatom.</p> <p>Što napraviti:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ako je format certifikata PEM/DER i dobili ste ga preko zahtjeva za potpisivanje certifikata pomoću računala, navedite datoteku privatnog ključa. <input type="checkbox"/> Ako je format certifikata PKCS#12 i dobili ste ga preko zahtjeva za potpisivanje certifikata pomoću računala, izradite datoteku koja sadrži privatni ključ.
	<p>Uzrok:</p> <p>Ponovno ste uvezli PEM/DER certifikat dobiven preko zahtjeva za potpisivanje certifikata pomoću aplikacije Web Config.</p> <p>Što napraviti:</p> <p>Ako je format certifikata PEM/DER i dobili ste ga preko zahtjeva za potpisivanje certifikata pomoću aplikacije Web Config, možete ga uvesti samo jednom.</p>

Poruke	Uzrok/što napraviti
Setup failed.	<p>Uzrok:</p> <p>Konfiguriranje se ne može dovršiti, jer komunikacija između skenera i računala nije uspjela ili se datoteka ne može pročitati zbog pogrešaka.</p> <p>Što napraviti:</p> <p>Nakon što provjerite navedenu datoteku i komunikaciju, ponovno uvezite datoteku.</p>

Povezane informacije

➔ [“O digitalnom certificiranju” na strani 97](#)

Slučajno ste izbrisali certifikat potpisan od strane tijela za izdavanje certifikata

Nema datoteke sigurnosne kopije za CA-certifikat.

Ako imate sigurnosnu kopiju, ponovno uvezite certifikat.

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

Povezane informacije

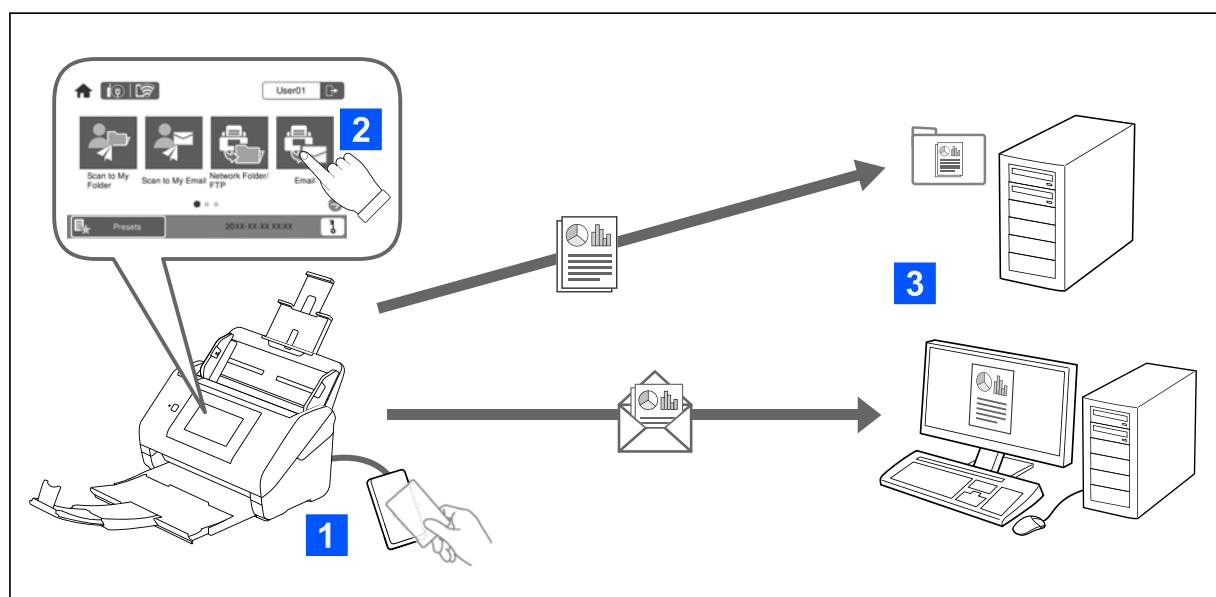
➔ [“Uvoz certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 99](#)

➔ [“Brisanje certifikata potpisanog od strane tijela za izdavanje certifikata \(CA\)” na strani 100](#)

Authentication Settings

O aplikaciji Authentication Settings.	125
O aplikaciji Authentication Method.	126
Softver za postavljanje.	128
Ažuriranje firmvera skenera.	128
Povezivanje i konfiguriranje uređaja za provjeru autentičnosti.	128
Informacije o registraciji i postavkama.	133
Job History izvješća koristeći Epson Device Admin.	149
Prijava kao administrator s upravljačke ploče.	149
Onemogućite Authentication Settings.	149
Brisanje Authentication Settings informacija (Obnovi zadane postavke).	150
Rješavanje problema.	150

O aplikaciji Authentication Settings



Kada se omogući Authentication Settings, za početak skeniranja potrebna je provjera autentičnosti korisnika. Možete postaviti metode skeniranja koje može koristiti svaki korisnik i spriječiti slučajne radnje.

Možete odrediti adresu e-pošte provjerenog korisnika kao odredište skeniranja (Scan to My Email) ili spremiti podatke svakog korisnika u osobnu mapu (Scan to My Folder). Također možete odrediti druge metode skeniranja.

Napomena:

- Ne možete skenirati iz računala ili pametnog uređaja kada se omogući Authentication Settings.
- Uz Authentication Settings uveden u ovom priručniku, također možete izgraditi sustav provjere autentičnosti s pomoću poslužitelja za provjeru autentičnosti. Za izradu sustava koristite Document Capture Pro Server Authentication Edition (skraćeni naziv je Document Capture Pro Server AE). Više informacija saznajte u lokalnom uredu tvrtke Epson.

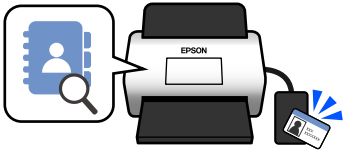
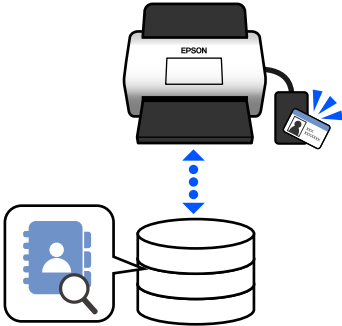
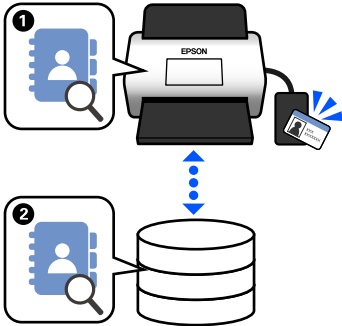
Dostupne funkcije za Authentication Settings

Funkcija skeniranja na upravljačkoj ploči	Authentication Settings	
	Kada se omogući	Kada se onemogući
Skeniraj u moju mapu Sprema slike u mapu koja je dodijeljena provjerenom korisniku.	✓	-
Skeniraj u moju e-poštu Šalje slike na adresu e-pošte provjerenog korisnika.	✓	-
Skeniraj u mrežnu mapu/FTP Sprema slike u mapu na mreži.	✓	✓

Funkcija skeniranja na upravljačkoj ploči	Authentication Settings	
	Kada se omogući	Kada se onemogući
<p>Skeniraj u računalo</p> <p>Sprema slike na povezano računalo s pomoću zadataka kreiranih u Document Capture Pro (Windows)/Document Capture (Mac OS).</p> <p>* Kada je omogućen Authentication Settings, možete koristiti samo zadatke koji su prijavljeni u Postavke.</p>	✓*	✓
<p>Skeniraj u e-poštu</p> <p>Šalje slike na adresu e-pošte koju ste postavili.</p>	✓	✓
<p>Skeniraj u oblak</p> <p>Šalje slike na uslugu u oblaku koju ste postavili.</p>	✓	✓
<p>Skeniraj na USB pogon</p> <p>Sprema slike na USB pogon spojen na skener. To je dostupno samo kada nijedan uređaj za provjeru autentičnosti nije povezan sa skenerom.</p>	✓	✓
<p>Skeniraj u WSD</p> <p>Sprema slike na povezano računalo s pomoću WSD značajke.</p>	-	✓
<p>Postavke</p> <p>Možete registrirati do 48 unaprijed postavljenih funkcija skeniranja.</p> <p>Možete dodijeliti do pet Postavke korisnicima registriranim u Local DB. Dodijeljeni Postavke dostupni su samo tom korisniku. Postavke koji nisu dodijeljeni nijednom korisniku mogu koristiti svi korisnici.</p>	✓	✓

O aplikaciji Authentication Method

Ovaj skener može osigurati provjeru autentičnosti pomoću sljedećih metoda bez potrebe za izgradnjom poslužitelja za provjeru autentičnosti.

	Local DB	LDAP	Local DB and LDAP
Lokacija podataka o korisniku	<p>Memorija skenera</p> <p>Ova metoda provjere autentičnosti provjerava korisničke podatke registrirane na skeneru i uspoređuje ih s korisnikom koji koristi funkciju skeniranja.</p>	<p>LDAP poslužitelj*</p> <p>Ova metoda provjere autentičnosti provjerava korisničke podatke LDAP poslužitelja sinkroniziranog sa skenerom. Budući da se do 300 stavki korisničkih informacija s LDAP poslužitelja može privremeno pohraniti u skener kao predmemorija, provjeru autentičnosti može se izvesti s pomoću predmemorije ako LDAP poslužitelj prestane s radom.</p> <p>* Poslužitelj koji pruža uslugu imenika koja može komunicirati s LDAP-om.</p>	<p>Memorija skenera i LDAP poslužitelj</p> <p>Prvo provjerite korisničke podatke registrirane u skeneru (1), a ako nema podudaranja, provjerite podatke korisnika u odnosu na LDAP poslužitelj (2).</p>
			
Broj registriranih korisnika	50 (memorija skenera)	Neograničeno (LDAP poslužitelj)	50 (f50 (memorija skenera) Neograničeno (LDAP poslužitelj)
Predmemorija skenera	-	300	Najviše 300 (50 utora za predmemoriju dijeli se sa User Settings u Local DB)
Načini prijave	<p>Možete koristiti bilo koji od sljedećih načina.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Držite karticu za provjeru autentičnosti ili unesite User ID i Password <input type="checkbox"/> Držite karticu za provjeru autentičnosti 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 značajke „Skeniraj u“	Postavlja se pojedinačno za svakog korisnika	Iste postavke za sve LDAP korisnike	Local DB korisnici: postavite pojedinačno LDAP korisnici: iste postavke za sve korisnike
Dodjela Postavke korisnicima	Do 5 po korisniku	- (Ne može se postaviti pojedinačno)	Local DB korisnici: do 5 po korisniku LDAP korisnici: -

Softver za postavljanje

Postavite s pomoću Web Config ili Epson Device Admin.

- Kada koristite Web Config, možete postaviti skener samo s pomoću web preglednika.
[“Web Config” na strani 35](#)
- Kada koristite Epson Device Admin, možete postaviti više skenera odjednom s pomoću predloška konfiguracije.
[“Epson Device Admin” na strani 36](#)

Ažuriranje firmvera skenera

Prije omogućavanja Authentication Settings, ažurirajte firmver skenera na najnoviju verziju. Unaprijed povežite skener s internetom.



Važno:

Ne isključujte računalo ili skener dok traje ažuriranje.

Prilikom postavljanja iz Web Config:

Odaberite karticu **Device Management** > **Firmware Update**, a zatim slijedite upute na zaslonu za ažuriranje firmvera.

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Home** > **Firmware** > **Update** na zaslonu s popisom uređaja, a zatim slijedite upute na zaslonu za ažuriranje firmvera.

Napomena:

Ako je najnoviji firmware već instaliran, ne morate ga ažurirati.

Povezivanje i konfiguriranje uređaja za provjeru autentičnosti

Ako želite spojiti i koristiti uređaj za provjeru autentičnosti kao što je čitač IC kartica, prvo morate konfigurirati uređaj. To nije potrebno ako ne koristite uređaj za provjeru autentičnosti.

Povezane informacije

- ➔ [“Povezivanje uređaja za provjeru autentičnosti” na strani 131](#)
- ➔ [“Postavke uređaja za provjeru autentičnosti” na strani 132](#)

Popis kompatibilnih čitača kartica

Ovaj popis ne jamči rad čitača kartica na popisu.

Da: podržano (Informacije ID-a mogu se čitati sa standardnim postavkama čitača kartica.)

Ne: nije kompatibilno

Izrađivač	Model	Broj modela	Kartica za provjeru autentičnosti							Način rada
			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	Tipkovnica
RF IDE-AS	pcProx	RDR-7081BKU	Da*1	Ne	Da	Da	Ne	Ne	Ne	Tipkovnica
RF IDE-AS	pcProx	RDR-7581AKU	Da	Ne	Da*1	Da*1	Ne	Ne	Ne	Tipkovnica
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Ne	Ne	Da	Da	Ne	Ne	Ne	Tipkovnica
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Da	Ne	Da	Da	Da	Da	Da	Tipkovnica
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Da	Da	Da	Da	Da	Da	Da	Tipkovnica
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Da	Da	Da	Da	Da	Da	Da	Tipkovnica
ELATEC	TWN4 Slim	T4QC-FC3B7	Da	Da	Da	Da	Da	Da	Da	Tipkovnica
HID Global	OMNI-KEY 5427	OMNI-KEY5427CK OMNI-KEY5427CK gen2	Da	Da	Da	Da	Da	Ne	Da	Tipkovnica*1
ACS	ACR122U	ACR122U	Ne	Ne	Da*2	Da*2	Da	Ne	Da*2	PC/SC

Izrađivač	Model	Broj modela	Kartica za provjeru autentičnosti							Način rada
			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	Tipkovnica
DMZ	Leitor RFID Multi-125	DMZ087	Ne	Da	Ne	Ne	Ne	Ne	Ne	Tipkovnica
DMZ	Leitor RFID Mifare	DMZ088	Ne	Ne	Da	Da	Ne	Ne	Ne	Tipkovnica
DMZ	Biometric & RFID Reader	DMZ073	Ne	Da	Ne	Ne	Ne	Ne	Ne	Tipkovnica
inepro	SCR708	SCR708	Da*1	Da*1	Da*1	Da*1	Da*1	Da*1	Da*1	Tipkovnica
Y Soft	YU03088001	MU0388	Da	Da	Da	Da	Da	Da	Da	Tipkovnica
Cardadis	TCM3 Cardadis MiFare Card Reader	ZTCM3-MIFARE	Ne	Ne	Da	Da	Ne	Ne	Da	Tipkovnica
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Ne	Ne	Da	Da	Ne	Ne	Da	Tipkovnica

Izrađivač	Model	Broj modela	Kartica za provjeru autentičnosti							Način rada
			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	Tipkov-nica
NT-wa-re	MiCard Plus-2-V2	RDR-80 081AG U-NT2-20	Da*1	Da*1	Da*1	Da*1	Ne	Ne	Ne	Tipkov-nica
NT-wa-re	MiCard V3 Multi	MiCard V3 Multi	Da	Da	Da	Da	Da	Da	Ne	Tipkov-nica

*1 Morate promijeniti postavke čitača kartica korištenjem vlasničkog softvera koji ste primili od proizvođača čitača kartica.

*2 Ako trebate koristiti podatke u određenom području na kartici osim standardnog ID-a kartice kao ID za provjeru autentičnosti konfiguriranjem postavki proizvoda, obratite se svom Epson partneru ili lokalnom predstavniku za više informacija o načinu postavljanja proizvoda.

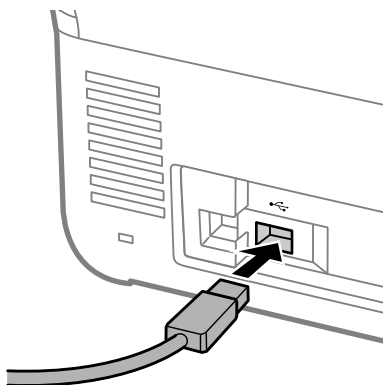
Povezivanje uređaja za provjeru autentičnosti



Važno:

Kada povežete uređaj za provjeru autentičnosti na više skenera, koristite proizvod s istim brojem modela.

Spojite USB kabel čitača kartica na USB priključak vanjskog sučelja na skeneru.



Provjera rada uređaja za provjeru autentičnosti

Na upravljačkoj ploči skenera možete provjeriti status veze i prepoznavanje kartice za provjeru autentičnosti za uređaj za provjeru autentičnosti.

Informacije se prikazuju ako odaberete **Postavke > Podaci o uređaju > Status uređaja za provjeru autentičnosti**.

Postavke uređaja za provjeru autentičnosti

Postavite format čitanja za podatke provjere autentičnosti primljene s kartice za provjeru autentičnosti.

Možete postaviti sljedeći način čitanja za uređaj za provjeru autentičnosti.

- Pročitajte određeno područje kartice za provjeru autentičnosti, kao što je broj zaposlenika ili osobni ID.
- Koristite podatke kartice za provjeru autentičnosti osim UID-a (podaci o kartici za provjeru autentičnosti kao što je serijski broj.)

Možete koristiti alat za generiranje radnih parametara. Pitajte svog prodavača za pojedinosti.

Napomena:

Korištenje kartica za provjeru autentičnosti različitih proizvođača:

Kada koristite podatke o UID kartici (podaci o ID-u kartice kao što je serijski broj), možete koristiti kombinaciju vrsta kartica za provjeru autentičnosti. To se ne može mijesati kada koristite druge podatke o kartici.

Prilikom postavljanja iz Web Config:

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

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Administrator Settings > Authentication Settings > Card Reader** u predlošku konfiguracije.

Stavka	Pojašnjenje
Vendor ID	Postavite ID dobavljača uređaja za provjeru autentičnosti koji ograničava uporabu od 0000 do FFFF s pomoću 4 alfanumerička znaka. Ako ne želite ograničiti, postavite na 0000.
Product ID	Postavite ID proizvoda uređaja za provjeru autentičnosti koja ograničava uporabu s 0000 na FFFF s pomoću 4 alfanumerička znaka. Ako ne želite ograničiti, postavite na 0000.
Operational parameter	Postavite parametar rada uređaja za provjeru autentičnosti između 0 i 8192 znaka. Dostupni su A~Z, a~z, 0~9, +, /, =, razmak i pomak reda.
Card Reader	Odaberite format pretvorbe za uređaj za provjeru autentičnosti. Možete provjeriti pojedinosti o formatu. Pogledajte poveznicu navedenu u opisu stavke.
Authentication Card ID save format	Odaberite format pretvorbe za podatke za provjeru autentičnosti osobne iskaznice. Možete provjeriti pojedinosti o formatu. Pogledajte poveznicu navedenu u opisu stavke.
Set card ID range	Omogućite specifikaciju položaja čitanja.
Text Start Position	Odredite početni položaj teksta za čitanje ID informacija. Možete navesti između 1 i 4096.
Number of Characters	Odredite broj znakova koji se čitaju od početnog položaja ID informacija. Možete navesti između 1 i 4096.

Informacije o registraciji i postavkama

Postavljanje značajke

Napravite potrebne postavke ovisno o Authentication Method i načinu skeniranja koju koristite.



Važno:

Prije početka postavljanja provjerite je li postavka vremena za skener ispravna.

Ako je postavka vremena netočna, prikazuje se poruka o pogrešci „Licenca je istekla“, što može dovesti do neuspjeha u postavljanju skenera. Također, za korištenje sigurnosne funkcije kao što je SSL/TLS komunikacija ili IPsec, potrebno je postaviti točno vrijeme. Vrijeme možete postaviti na sljedeći način.

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

Upravljačka ploča skenera: **Postavke** > **Osnovne postavke** > **Postavke datuma/vremena**.

Postavke	Local DB	LDAP	Local DB and LDAP
<p>Omogućavanje provjere autentičnosti</p> <p>Morate omogućiti provjeru autentičnosti prije postavljanja postavki provjere autentičnosti.</p> <p>"Omogućavanje provjere autentičnosti" na strani 134</p>	✓	✓	✓
<p>Authentication Settings</p> <p>Postavljanje Authentication Method i kako provjeriti autentičnost korisnika.</p> <p>"Authentication Settings" na strani 134</p>	✓	✓	✓
<p>Registriranje User Settings</p> <p>Registrirajte postavke za svakog korisnika. Također možete skupno registrirati korisnike s pomoću CSV datoteke.</p> <p>"Registriranje User Settings" na strani 135</p>	✓	–	✓
<p>Sinkroniziranje s LDAP Server</p> <p>Napravite postavke sinkronizacije LDAP poslužitelja.</p> <p>"Sinkroniziranje s LDAP Server" na strani 142</p>	–	✓	✓
<p>Postavljanje Email Server</p> <p>Postavite postavke poslužitelja e-pošte. Postavite ovo kada koristite funkcije koje zahtijevaju postavke poslužitelja e-pošte kao što je Scan to My Email.</p> <p>"Postavljanje poslužitelja e-pošte" na strani 145</p>	✓	✓	✓
<p>Postavka Scan to My Folder</p> <p>Postavite odredišne mape. Postavite to kada koristite funkciju Scan to My Folder.</p> <p>"Postavka Scan to My Folder" na strani 146</p>	✓	✓	✓

Postavke	Local DB	LDAP	Local DB and LDAP
<p>Customize One-touch Functions</p> <p>Postavite ovo kada mijenjate stavke prikazane na upravljačkoj ploči skenera. Na upravljačkoj ploči možete prikazati samo ikone koje trebate ili promijenite redoslijed ikona.</p> <p>"Customize One-touch Functions" na strani 148</p>	✓	✓	✓

Omogućavanje provjere autentičnosti

Morate omogućiti provjeru autentičnosti prije postavljanja postavki provjere autentičnosti.

Prilikom postavljanja iz Web Config:

Odaberite **Uključeno (uređaj/LDAP poslužitelj)** na kartici **Product Security > Basic > Authentication**.

Prilikom postavljanja iz Epson Device Admin:

Na predlošku konfiguracije odaberite **Uključeno (uređaj/LDAP poslužitelj)** iz **Administrator Settings > Authentication Settings > Basic > Authentication**.

Napomena:

Ako omogućite Authentication Settings na skeneru, Postavka blokade je također omogućen za upravljačku ploču. Upravljačka ploča ne može se otključati kada se onemogući Authentication Settings.

Čak i ako onemogućite Authentication Settings, Postavka blokade ostaje omogućeno. Ako želite onemogućiti, možete odabrati postavke preko upravljačke ploče ili programa Web Config.

Povezane informacije

- ➔ ["Postavljanje Postavka blokade s upravljačke ploče" na strani 85](#)
- ➔ ["Postavka Postavka blokade preko Web Config" na strani 85](#)

Authentication Settings

Postavljanje Authentication Method i kako provjeriti autentičnost korisnika.

Prilikom postavljanja iz Web Config:

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

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Administrator Settings > Authentication Settings > Authentication Settings** u predlošku konfiguracije.

Stavka	Pojašnjenje
Authentication Method	<p>Odaberite Authentication Method.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Local DB Provjerite autentičnost koristeći User Settings registrirane na skeneru. Potrebno je registrirati korisnika na skeneru. <input type="checkbox"/> LDAP Provjerite autentičnost s pomoću korisničkih informacija na LDAP poslužitelju sinkroniziranom sa skenerom. Prethodno trebate konfigurirati postavke poslužitelja LDAP. <input type="checkbox"/> Local DB and LDAP Provjerite autentičnost s pomoću korisničkih podataka registriranih na skeneru ili LDAP poslužitelju sinkroniziranom sa skenerom. Morate registrirati korisnika na skeneru i postaviti LDAP poslužitelj.
How to Authenticate User	<p>Odaberite način provjere autentičnosti korisnika.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Card or User ID and Password Koristite karticu za provjeru autentičnosti za provjeru autentičnosti korisnika. Također možete koristiti korisnički ID i lozinku za provjeru autentičnosti. <input type="checkbox"/> User ID and Password Koristite korisnički ID i lozinku za provjeru autentičnosti korisnika. Kada odaberete ovu funkciju, ne možete koristiti karticu za provjeru autentičnosti. <input type="checkbox"/> User ID Koristite samo korisnički ID za provjeru autentičnosti korisnika. Ne morate postavljati lozinku. <input type="checkbox"/> Card or ID Number Koristite karticu za provjeru autentičnosti za provjeru autentičnosti korisnika. Također možete koristiti ID Number. <input type="checkbox"/> ID Number Koristite samo ID broj za provjeru autentičnosti korisnika.
Allow users to register authentication cards	<p>Omogućite ga ako dopustite korisnicima da registriraju karticu za provjeru autentičnosti u sustavu. Ako odaberete LDAP za Authentication Method, ne možete ga postaviti.</p> <p>Za više informacija o tome kako korisnici mogu registrirati svoje kartice za provjeru autentičnosti pogledajte dio „Registriranje kartice za provjeru autentičnosti“ u <i>Korisnički vodič</i>.</p>
The Minimum Digit Number of ID Number	<p>Odaberite minimalni broj znamenki za ID broj.</p>
Caching for LDAP authenticated users	<p>Prilikom korištenja provjere autentičnosti poslužitelja LDAP možete postaviti želite li koristiti predmemoriju za korisničke podatke.</p>
Use user information in SMTP authentication	<p>Kada koristite korisnički ID i lozinku za provjeru autentičnosti, možete postaviti želite li koristiti korisničke podatke za SMTP provjeru autentičnosti. Sustav koristi posljednji korisnički ID i lozinku koji su bili prijavljeni.</p>
Restrictions for LDAP authenticated users	<p>Ako koristite LDAP, možete postaviti funkcije koje su dostupne korisniku.</p>

Registriranje User Settings

Registrirajte User Settings koji se koristi za provjeru autentičnosti korisnika. Registrirati se možete na bilo koji od sljedećih načina.

- Registriranje User Settings Jedan po jedan (Web Config)
- Registriranje višestrukih User Settings kao skup s pomoću CSV datoteke (Web Config)
- Registriranje User Settings na više skenera kao skup s pomoću predložka konfiguracije (Epson Device Admin)

Povezane informacije

- ➔ “Registriranje User Settings pojedinačno (Web Config)” na strani 136
- ➔ “Registriranje višestrukih User Settings korištenjem CSV datoteke (Web Config)” na strani 137
- ➔ “Registriranje User Settings na više skenera kao skup (Epson Device Admin)” na strani 140

Registriranje User Settings pojedinačno (Web Config)

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

Stavka	Pojašnjenje
User ID	Unesite korisnički ID koji želite koristiti za provjeru autentičnosti u rasponu od 1 do 83 bajta koji se mogu izraziti koristeći Unicode (UTF-8). Budući da ID korisnika ne razlikuje velika ili mala slova, možete se prijaviti pomoću velikih ili malih slova.
User name Display	Unesite korisničko ime prikazano na upravljačkoj ploči skenera unutar 32 znaka koji se mogu izraziti koristeći Unicode (UTF-16). To možete ostaviti prazno.
Password	Unesite lozinku koju želite koristiti za provjeru autentičnosti unutar 32 znaka u ASCII kodu. Lozinka razlikuje mala i velika slova. Ostavite ovo prazno ako odaberete User ID za How to Authenticate User .
Authentication Card ID	Unesite ID kartice za provjeru autentičnosti s najviše 116 znakova u ASCII kodu. To možete ostaviti prazno. Kad dopustite Allow users to register authentication cards za Authentication Settings , odražava se rezultat koji su registrirali korisnici.
ID Number	Ova stavka prikazuje se kada se Card or ID Number ili ID Number odabere u Authentication Settings > How to Authenticate User . Unesite broj negdje između postavljenog broja Authentication Settings > The Minimum Digit Number of ID Number te sadrži do 8 znamenki.
Auto Generate	Ova stavka prikazuje se kada se Card or ID Number ili ID Number odabere u Authentication Settings > How to Authenticate User . Kliknite da biste automatski generirali ID broj s istim brojem znamenki koji ste odabrali The Minimum Digit Number of ID Number .
Department	Unesite naziv odjela itd. koji identificira korisnika unutar 40 znakova koji se mogu izraziti kodom Unicode (UTF-16). To možete ostaviti prazno.
Email Address	Unesite adresu e-pošte korisnika s najviše 200 znakova u ASCII kodu. Ovo se koristi kao odredište za Scan to My Email . To možete ostaviti prazno.

Stavka	Pojašnjenje
Scan to My Folder	Postavite odredišta spremanja pojedinačno kada odaberete Individual u Scan to My Folder > Setting Type . Pogledajte sljedeće za više informacija o stavkama podešavanja. "Postavka Scan to My Folder" na strani 146
Restrictions	Možete ograničiti funkcije za svakog korisnika. Odaberite funkciju čiju uporabu želite dozvoliti.
Presets	Možete postaviti do pet unaprijed postavljenih postavki koje su dostupne samo odabranom korisniku iz Presets registriranom u skeneru. <input type="checkbox"/> Presets koje su dodijeljene korisniku može koristiti samo taj korisnik. Presets koji nisu dodijeljeni nijednom korisniku mogu koristiti svi korisnici. <input type="checkbox"/> Ako korisnik ima samo jednu dostupnu Presets, koja se automatski učitava nakon provjere autentičnosti. Ako je dostupno više Presets, popis Presets prikazuje se nakon provjere autentičnosti. <input type="checkbox"/> Ne možete kreirati ili prikazati Presets koji koriste funkcije ograničene u Restrictions .

Registriranje višestrukih User Settings korištenjem CSV datoteke (Web Config)

Unesite postavke za svakog korisnika u CSV datoteku i registrirajte ih skupno.

Izrada CSV datoteke

Izradite CSV datoteku za uvoz User Settings.

Napomena:

Ako registrirate jednu ili više njih User Settings unaprijed, a zatim izvezite formatiranu datoteku (CSV datoteku), registriranu postavku možete koristiti kao referencu za unos stavki postavki.

1. Pristupite aplikaciji Web Config i odaberite karticu **Product Security > User Settings**.
2. Kliknite na **Export**.
3. Odaberite format datoteke za **File Format**.
Odaberite ga upućivanjem u nastavku.

Stavka	Pojašnjenje
CSV UTF-16 (Tab delimited)	Odaberite kada uređujete datoteku pomoću Microsoft Excel. Svaki parametar zatvara se s „[]” (zagrada). Unesite parametre u „[]”. Kada ažurirate datoteku, preporučujemo da je zamijenite novom. Ako ste nedavno spremili datoteku, odaberite Unicode tekst (*.txt) za format datoteke.
CSV UTF-8 (Comma delimited)	Odaberite kada uređujete datoteku s pomoću uređivača teksta ili makronaredbe bez Microsoft Excel.
CSV UTF-8 (Semicolon delimited)	

4. Kliknite na **Export**.

5. Uredite i spremite ovu CSV datoteku u aplikaciju za proračunske tablice kao što je Microsoft Excel ili u uređivaču teksta.



Važno:

Prilikom uređivanja datoteke nemojte mijenjati podatke o kodiranju i zaglavlju.

Stavke postavljanja CSV datoteke

Stavka	Postavke i pojašnjenja
UserID	Unesite korisnički ID za korištenje provjere autentičnosti između 1 i 83 bajta Unicode.
UserName	Unesite korisničko ime prikazano na upravljačkoj ploči skenera s najviše 32 znaka Unicode. To možete ostaviti prazno.
Password	Unesite lozinku koju ćete koristiti za provjeru autentičnosti s najviše 32 znaka u ASCII kodu. Prilikom uvoza, ovo se postavlja kao lozinka umjesto EncPassword . Ostavite ovo prazno ako odaberete User ID za How to Authenticate User . Prilikom izvoza, ovo je uvijek prazno.
AuthenticationCardID	Postavite rezultat čitanja kartice za provjeru autentičnosti. Kada dopustite Allow users to register authentication cards u Authentication Settings , prikazan je rezultat koji su registrirali korisnici. Unesite s najviše 116 znakova u ASCII kodu. To možete ostaviti prazno.
IDNumber	Ova stavka prikazuje se kada se Card or ID Number ili ID Number odabere u Authentication Settings > How to Authenticate User . Unesite broj negdje između postavljenog broja Authentication Settings > The Minimum Digit Number of ID Number te sadrži do 8 znamenki. ID broj ne može se duplicirati. Ako je dupliciran, bit ćete upozoreni na pogrešku prilikom uvoza datoteke. Kada se ostavi prazno, automatski mu se dodjeljuje broj.
Department	Unesite proizvoljan naziv odjela kako biste razlikovali korisnike. Unesite do 40 znakova u Unicode. To možete ostaviti prazno.
MailAddress	Postavite adresu e-pošte za korisnike. Ovo se koristi kao odredište za Scan to My Email . Možete koristiti A-Z, a-z, 0-9, !#%&*' +-. / = ? ^ _ { } ~ @. Unesite najviše 200 znaka. Ne možete koristiti „,“ (zarez) kao prvi znak. To možete ostaviti prazno.
FolderProtocol	Postavite vrstu funkcije Scan to My Folder. Mrežna mapa/FTP (SMB): 0, FTP: 1
FolderPath	Postavite odredište za spremanje za funkciju Scan to My Folder.
FolderUserName	Postavite korisničko ime za funkciju Scan to My Folder.
FolderPassword	Postavite lozinku za provjeru autentičnosti odredišne mape za funkciju Scan to My Folder s najviše 32 znaka ASCII koda. Prilikom uvoza, ovo se postavlja kao lozinka umjesto EncPassword . Prilikom izvoza, ovo je uvijek prazno.

Stavka	Postavke i pojašnjenja
FtpPassive	Postavite način povezivanja za FTP poslužitelj kada se FTP odabere kao Type za funkciju Scan to My Folder. Aktivni način rada: 0, pasivni način rada: 1
FtpPort	Postavite broj porta za slanje skeniranih podataka na FTP poslužitelj od 0 do 65535 kada se FTP odabere kao Type za funkciju Scan to My Folder.
ScanToMemory	Postavite ograničenja za Scan to USB Drive. Nije dopušteno: 0, Dopušteno: 1
ScanToMail	Postavite ograničenja za Scan to Email. Možete postaviti Skeniraj u moju e-poštu samo kada se omogući Scan to Email . Nije dopušteno: 0, Dopušteno: 1
ScanToFolder	Postavite ograničenja za Scan to Network Folder/FTP. Možete postaviti Skeniraj u moju mapu samo kada se omogući Scan to Network Folder/FTP . Nije dopušteno: 0, Dopušteno: 1
ScanToCloud	Postavite ograničenja za Scan to Cloud. Nije dopušteno: 0, Dopušteno: 1
ScanToComputer	Postavite ograničenja za Skeniraj u računalo. Nije dopušteno: 0, Dopušteno: 1
PresetIndex	Postavite Presets koje želite povezati s korisnikom. Možete postaviti do pet Presets registracijskih brojeva odvojenih zarezima.
EncPassword	Prilikom izvoza korisničkih postavki, parametar postavljen za Password je šifriran i tada je vrijednost kodirana koristeći BASE64 i izlaz. Prilikom uvoza s novom lozinkom za Password , ova vrijednost se zanemaruje. Ako je Password prazno, ova vrijednost se koristi, a lozinka ostaje ista kao prije izvoza.
EncFolderPassword	Prilikom šifriranog izvoza skupa parametara za FolderPassword , vrijednost se kodira koristeći BASE64 i izlaz. Prilikom uvoza s novom lozinkom za FolderPassword , ova vrijednost se zanemaruje. Ako je FolderPassword prazno, ova vrijednost se koristi, a lozinka ostaje ista kao prije izvoza.

Uvoz CSV datoteke

1. Pristupite aplikaciji Web Config i odaberite karticu **Product Security > User Settings**.
2. Kliknite na **Import**.
3. Odaberite datoteku koju želite uvesti.
4. Kliknite na **Import**.
5. Nakon što provjerite prikazane informacije, kliknite **OK**.

Registriranje User Settings na više skenera kao skup (Epson Device Admin)

Možete se registrirati User Settings korišteno u Local DB kao skup pomoću LDAP poslužitelja ili CSV/ENE datoteke.

Napomena:

ENE datoteka je binarna datoteka koju omogućava Epson koja šifrira i sprema informacije za **Contacts** kao što su osobni podaci i User Settings. Može se izvoziti iz Epson Device Admin i možete postaviti lozinku. Korisno je kada želite uvesti User Settings iz sigurnosne kopije datoteke.

Uvoz iz datoteke CSV/ENE

1. Odaberite **Administrator Settings > Authentication Settings > User Settings** u predlošku konfiguracije.
2. Kliknite na **Import**.
3. Odaberite **CSV or ENE File** pod **Import Source**.
4. Kliknite na **Browse**.
Prikazuje se zaslon za odabir datoteke.
5. Odaberite datoteku koju želite uvesti da biste je otvorili.
6. Odaberite način uvoza.
 - Overwrite and Add:** zamjenjuje postojeće ako postoji isti korisnički ID; dodaje novi ID ako ne postoji.
 - Replace All:** zamjenjuje sve s korisničkim postavkama koje želite uvesti.
7. Kliknite na **Import**.
Prikazuje se zaslon potvrde postavke.
8. Kliknite na **OK**.
Prikazuje se rezultat potvrđivanja.
Napomena:
 - Ako broj uvezenih korisničkih postavki premašuje broj koji se može uvesti, pojavit će se poruka od vas da izbrišete neke korisničke postavke. Izbrišite sve dodatne korisničke postavke prije uvoza.*
 - Odaberite korisničke postavke koje želite izbrisati prije uvoza, a zatim kliknite **Delete**.*
9. Kliknite na **Import**.
Korisničke postavke uvoze se u predložak konfiguracije.

Uvoz iz LDAP poslužitelja

1. Odaberite **Administrator Settings > Authentication Settings > User Settings** u predlošku konfiguracije.
2. Kliknite na **Import**.
3. Odaberite **LDAP** pod **Import Source**.

4. Kliknite na **Settings**.

Prikazane su postavke **LDAP Server**.

Napomena:

Ova postavka LDAP poslužitelja služi za uvoz korisničkih postavki s LDAP poslužitelja. Uvezene (kopirane) korisničke postavke koriste se za provjeru autentičnosti korisnika s pomoću samog skenera.

S druge strane, kada odaberete **LDAP** ili **Local DB and LDAP** kao metodu provjere autentičnosti, korisnici se provjeravaju komunikacijom s LDAP poslužiteljem.

5. Postavite svaku stavku.

Prilikom uvoza korisničkih postavki iz LDAP poslužitelja, osim LDAP postavki možete konfigurirati i sljedeće postavke.

Za ostale stavke pogledajte Povezane informacije.

Stavka		Pojašnjenje	
LDAP Server Settings	LDAP Server Type	Omogućuje odabir vrste LDAP poslužitelja.	
Search Settings	Search Filter	Možete postaviti tekst koji se koristi za LDAP filter pretraživanja. Odaberite Custom za uređivanje teksta pretraživanja.	
	Options	Type	Možete postaviti vrstu odredišta za spremanje za Scan To My Folder .
		Connection Mode	Kada se Type postavi na FTP , možete postaviti način FTP veze.
	Port Number	Kada se Type postavi na FTP , možete postaviti broj porta koji želite koristiti.	

6. Po potrebi izvršite provjeru veze klikanjem na **Connection Test**.

Pribavlja i prikazuje 10 korisničkih postavki iz LDAP poslužitelja.

7. Kliknite na **OK**.

8. Odaberite način uvoza.

- Overwrite and Add:** zamjenjuje postojeće ako postoji isti korisnički ID; dodaje novi ID ako ne postoji.
- Replace All:** zamjenjuje sve s korisničkim postavkama koje želite uvesti.

9. Kliknite na **Import**.

Prikazuje se zaslon potvrde postavke.

10. Kliknite na **OK**.

Prikazuje se rezultat potvrđivanja.

11. Kliknite na **Import**.

Korisničke postavke uvoze se u predložak konfiguracije.

Povezane informacije

- ➔ “Konfiguriranje LDAP poslužitelja” na strani 142
- ➔ “Konfiguriranje postavki pretraživanja LDAP poslužitelja” na strani 144

Sinkroniziranje s LDAP Server

Odaberite postavke LDAP Server za vaš skener.

Po potrebi izvršite postavke za primarni i sekundarni poslužitelj.

Napomena:

Postavke za **LDAP Server** dijele se s **Contacts**.

Dostupne usluge

Podržane su sljedeće usluge imenika.

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

Konfiguriranje LDAP poslužitelja

Da biste koristili LDAP poslužitelj, prvo morate konfigurirati LDAP poslužitelj.

Prilikom postavljanja iz Web Config:

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

Ako odaberete **Kerberos Authentication** kao **Authentication Method**, odaberite **Network > Kerberos Settings** za postavljanje postavki za Kerberos.

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Network > LDAP server > Server Settings (Primary Server)** ili **Server Settings (Secondary Server)** u predlošku konfiguracije.

Ako odaberete **Kerberos Authentication** kao **Authentication Method**, odaberite **Network — Security > Kerberos Settings** za postavljanje postavki za Kerberos.

Stavka	Postavke i pojašnjenja
Use LDAP Server	Odaberite Use ili Do Not Use .
LDAP Server Address	Unesite adresu LDAP poslužitelja. Unesite između 1 i 255 znakova u formatu IPv4, IPv6 ili FQDN. Za format FQDN možete koristiti alfanumeričke znakove u ASCII kodu (0x20 – 0x7E) i crte, osim na početku i kraju adrese.
LDAP server Port Number (Port number)	Unesite broj ulaza poslužitelja LDAP, između 1 i 65535.
Secure Connection	Odredite način provjere autentičnosti za pristup skenera poslužitelju LDAP.

Stavka	Postavke i pojašnjenja
Certificate Validation	Valjanost certifikata poslužitelja LDAP bit će provjerena ako je to omogućeno. Preporučujemo da ovo postavite na Enable . Kako bi bio postavljen CA Certificate treba biti uvezen u skener.
Search Timeout (sec)	Odredite trajanje pretraživanja prije isteka vremena, između 5 i 300 sekundi.
Authentication Method	Odabir načina provjere autentičnosti. Ako odaberete Kerberos Authentication , unaprijed odaberite postavke za Kerberos. Za provođenje Kerberos Authentication potrebno je sljedeće okruženje. <input type="checkbox"/> Skener i DNS poslužitelj mogu komunicirati. <input type="checkbox"/> Vrijeme na skeneru, KDC poslužitelju i poslužitelju potrebnom za potvrđivanje autentičnosti (LDAP poslužitelj, SMTP poslužitelj, poslužitelj datoteke) trebaju biti sinkronizirani. <input type="checkbox"/> Kada je poslužitelj usluge dodijeljen kao IP adresa, FQDN poslužitelja usluge je registriran na zoni obrnutog pretraživanja DNS poslužitelja.
Kerberos Realm to be Used	Ako odaberete Kerberos Authentication za Authentication Method , odaberite Kerberos područje koje želite koristiti.
Administrator DN / User Name	Unesite korisničko ime za poslužitelj LDAP s najviše 128 znakova Unicode (UTF-8). Ne možete koristiti kontrolne znakove, kao što su 0x00 – 0x1F i 0x7F. Ova postavka se ne koristi kada je Anonymous Authentication odabran kao Authentication Method . Ako to ne navedete, ostavite prazno polje.
Password	Unesite lozinku za provjeru autentičnosti poslužitelja LDAP s najviše 128 znakova Unicode (UTF-8). Ne možete koristiti kontrolne znakove, kao što su 0x00 – 0x1F i 0x7F. Ova postavka se ne koristi kada je Anonymous Authentication odabran kao Authentication Method . Ako to ne navedete, ostavite prazno polje.

Kerberos postavke

Ako odaberete **Kerberos Authentication** kao **Authentication Method**, morate odabrati Kerberos postavke. Možete registrirati do 10 Kerberos postavki.

Prilikom postavljanja iz Web Config:

Odaberite karticu **Network > Kerberos Settings**.

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Network > Security > Kerberos Settings** u predlošku konfiguracije.

Stavka	Postavke i pojašnjenja
Realm (Domain)	Unesite područje Kerberos provjere autentičnosti s najviše 255 znakova u ASCII kodu (0x20 – 0x7E). Ako to ne registrirate, ostavite prazno polje.
KDC Address	Unesite adresu poslužitelja za Kerberos provjeru autentičnosti. Unesite najviše 255 znakova u formatu IPv4, IPv6 ili FQDN. Ako to ne registrirate, ostavite prazno polje.
Port Number (Kerberos)	Unesite broj ulaza Kerberos poslužitelja, između 1 i 65535.

Konfiguriranje postavki pretraživanja LDAP poslužitelja

Postavlja attribute pretraživanja za korisničke postavke.

Prilikom postavljanja iz Web Config:

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

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Administrator Settings > Authentication Settings > LDAP server > Search Settings (Authentication)** u predlošku konfiguracije.

Stavka	Postavke i pojašnjenja
Search Base (Distinguished Name)	Odredite početni položaj kada tražite korisničke podatke iz LDAP poslužitelja. Unesite između 0 i 128 znakova Unicode (UTF-8). Ako ne tražite arbitražno svojstvo, ostavite ovo polje prazno. Primjer direktorija lokalnog poslužitelja: dc=server,dc=local
User ID Attribute	Navedite naziv atributa koji će se prikazivati kod pretraživanja ID brojeva. Unesite od 1 do 255 znaka u ASCII kodu. Prvi znak treba biti a – z ili A – Z. Primjer: cn, uid
User name Display Attribute	Navedite naziv svojstva koji će biti prikazan kao korisničko ime. Unesite od 0 do 255 znaka u ASCII kodu. Prvi znak treba biti a – z ili A – Z. Njega možete ostaviti praznim. Primjer: cn, name
Authentication Card ID Attribute	Odredite naziv atributa koji će se prikazati kao ID kartice za provjeru autentičnosti. Unesite od 0 do 255 znaka u ASCII kodu. Prvi znak treba biti a – z ili A – Z. Njega možete ostaviti praznim. Primjer: cn, sn
ID Number Attribute	Navedite naziv atributa koji će se prikazivati kod pretraživanja ID brojeva. Unesite od 1 do 255 znaka u ASCII kodu. Prvi znak treba biti a – z ili A – Z. Primjer: cn, id
Department Attribute	Navedite naziv svojstva koji će biti prikazan kao naziv odjela. Unesite od 0 do 255 znaka u ASCII kodu. Prvi znak treba biti a – z ili A – Z. Njega možete ostaviti praznim. Primjer: ou, ou-cl
Email Address Attribute	Navedite naziv svojstva koji će biti prikazan kod pretraživanja adresa e-pošte. Unesite od 1 do 255 znaka u ASCII kodu. Prvi znak treba biti a – z ili A – Z. Primjer: mail
Save To Attribute	Odredite naziv atributa koji ukazuje na određite za Scan To My Folder. Unesite od 0 do 255 znaka u ASCII kodu. Primjer: homeDirectory

Provjera veze s LDAP poslužiteljem

Izvršava provjeru veze LDAP poslužitelja koristeći parametre zadane pod **LDAP Server > Search Settings**.

1. Pristupite aplikaciji Web Config i odaberite karticu **Network > LDAP Server > Connection Test**.

2. Odaberite **Start**.

Pokrenuta je provjera veze. Nakon provjere je prikazan izvještaj o provjeri.

Reference testa veze s LDAP poslužiteljem

Poruke	Pojašnjenje
Connection test was successful.	Ova poruka pojavljuje se kod uspješnog povezivanja s poslužiteljem.
Connection test failed. Check the settings.	Ova poruka pojavljuje se iz sljedećih razloga: <input type="checkbox"/> Adresa LDAP poslužitelja ili broj porta je netočan. <input type="checkbox"/> Došlo je do isteka vremena. <input type="checkbox"/> Do Not Use je odabrano kao Use LDAP Server . <input type="checkbox"/> Ako je Kerberos Authentication odabran kao Authentication Method , postavke poput Realm (Domain) , KDC Address i Port Number (Kerberos) nisu točne.
Connection test failed. Check the date and time on your product or server.	Ova poruka pojavljuje se kada veza ne uspije zbog nepodudaranja vremenskih postavki skenera i LDAP poslužitelja.
Authentication failed. Check the settings.	Ova poruka pojavljuje se iz sljedećih razloga: <input type="checkbox"/> Stavka User Name i/ili Password nije točna. <input type="checkbox"/> Ako se Kerberos Authentication odabere za Authentication Method , možda se neće konfigurirati vrijeme/datum.
Cannot access the product until processing is complete.	Ova poruka pojavljuje se kada je skener zauzet.

Postavljanje poslužitelja e-pošte

Kada koristite **Scan to My Email**, postavite poslužitelj e-pošte.

Napomena:

Možete postaviti **Scan to My Email** samo kada se omogući **Scan to Email**.

Prilikom postavljanja iz Web Config:

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

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Common > Email Server > Mail Server Settings** u predlošku konfiguracije.

Stavka	Postavke i pojašnjenja	
Authentication Method	Odredite način provjere autentičnosti za pristup skenera poslužitelju e-pošte.	
	Off	Provjera autentičnosti onemogućena je prilikom komuniciranja s poslužiteljem e-pošte.
	SMTP AUTH	Poslužitelj e-pošte treba podržavati potvrđivanje autentičnosti SMTP.
	POP before SMTP	Ako odaberete ovu stavku, postavite POP3 poslužitelja.
Authenticated Account	Ako odaberete SMTP AUTH ili POP before SMTP kao Authentication Method , unesite naziv računa za koji je provjerena autentičnost. Unesite od 0 do 255 znaka u ASCII kodu (0x20 – 0x7E).	
Authenticated Password	Ako odaberete SMTP AUTH ili POP before SMTP kao Authentication Method , unesite provjerenu lozinku. Unesite od 0 do 20 znaka u ASCII kodu (0x20 – 0x7E).	
Sender's Email Address	Unesite adresu e-pošte pošiljatelja. Unesite od 0 do 255 znakova u ASCII kodu (0x20 – 0x7E), osim : () < > [] ; ¥. Točka „.” ne može biti prvi znak.	
SMTP Server Address	Unesite između 0 i 255 znaka pomoću znakova A – Z a – z 0 – 9 . -. Možete koristiti IPv4 ili FQDN format.	
SMTP Server Port Number	Unesite broj između 1 i 65535.	
Secure Connection	Odredite način sigurne veze za poslužitelj e-pošte.	
	None	Ako ste odabrali POP before SMTP u Authentication Method , način povezivanja će biti podešen na None .
	SSL/TLS	To će biti dostupno ako Authentication Method namjestite na Off ili SMTP AUTH .
	STARTTLS	To će biti dostupno ako Authentication Method namjestite na Off ili SMTP AUTH .
Certificate Validation	Valjanost certifikata bit će provjerena ako je to omogućeno. Preporučujemo da ovo postavite na Enable .	
POP3 Server Address	Ako odaberete POP before SMTP kao Authentication Method , unesite POP3 adresu poslužitelja. Unesite između 0 i 255 znakova koristeći A – Z, a – z, 0 – 9. Možete koristiti IPv4 ili FQDN format.	
POP3 Server Port Number	Ako odaberete POP before SMTP kao Authentication Method , navedite broj porta. Unesite broj između 1 i 65535.	

Postavka Scan to My Folder

Sprema skenirane slike u mapu dodijeljenu svakom korisniku. Možete postaviti sljedeće kao dodijeljenu mapu.

Napomena:

Možete postaviti **Scan To My Folder** samo kada se omogući **Scan to Network Folder/FTP**.

Postavka Spremi na	Authentication Method	Mjesto postavljanja putanje mape
Navedite jednu mrežnu mapu za sve Authentication Settings da automatski kreirate osobnu mapu ispod navedene mape koristeći naziv korisničkog ID-a.	<input type="checkbox"/> Local DB <input type="checkbox"/> LDAP <input type="checkbox"/> Local DB and LDAP	Skener (postavka Scan to My Folder)
Dodijelite različite mrežne mape zasebno svakom korisniku.	Local DB	Skener (User Settings)
	LDAP	Atributi LDAP-a
	Local DB and LDAP	Atributi skenera (User Settings) ili LDAP-a

Prilikom postavljanja iz Web Config:

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

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Administrator Settings** > **Authentication Settings** > **Scan to Network Folder/FTP** > **Scan to My Folder** u predlošku konfiguracije.

Stavka	Stavka	Pojашnjenje
Save To Setting	Setting Type	<input type="checkbox"/> Shared: Automatski kreira mapu nazvanu prema ID-u korisnika ispod putanje mape ili URL-a navedenog u Save to i sprema skenirane slike u ovu mapu. <input type="checkbox"/> Individual: Postavite odredište spremanja za rezultate skeniranja za svakog korisnika. Local DB korisnici mogu se postaviti u korisničkim postavkama. LDAP korisnici koriste lokaciju za pohranu dobivenu iz atributa pretraživanja LDAP poslužitelja.
	Type	Odaberite protokol prijenosa u skladu s odredištem izlaza skeniranja. Za mrežnu mapu: Network Folder (SMB) Za FTP poslužitelj: FTP
	Save to	Navedite put ili URL izlazne putanje. Unesite do 160 znakova u Unicode (UTF-16).
	Connection Mode	Postavite kada odaberete FTP u Type . Odaberite način povezivanja s FTP poslužiteljem.
	Port Number	Postavite kada odaberete FTP u Type . Unesite broj porta za slanje skeniranih podataka na FTP poslužitelj između 0 i 65535.

Stavka		Pojašnjenje
Authentication Settings	Setting Type	<p>Postavite kada odaberete Individual kao Setting Type u Save To Setting.</p> <p>Postavite „User Name“ i „Password“ za pristup mapi.</p> <p><input type="checkbox"/> Shared: Koristite zajednički User Name i Password za sve korisnike.</p> <p><input type="checkbox"/> Individual: Za Local DB korisnika, postavite User Name i Password pojedinačno u Korisničke postavke. LDAP korisnici ne mogu se konfigurirati pojedinačno. User Name i Password postavljene ovom stavkom koriste se kao serija.</p>
	User Name	<p>Unesite korisničko ime za pristup određenoj mapi za izlaz skeniranja.</p> <p>Unesite do 30 znakova u Unicode (UTF-16). Postavite ovo kada koristite Shared ili LDAP poslužitelj.</p>
	Password	<p>Unesite lozinku koja odgovara User Name.</p> <p>Unesite do 20 znakova u Unicode (UTF-16). Postavite ovo kada koristite Shared ili LDAP poslužitelj.</p>

Zabrana promjene odredišta za Scan to Network Folder/FTP

Stavka	Pojašnjenje
Prohibit manual entry of destination	Kada je omogućeno, korisnik ne može promijeniti zadano odredište.

Customize One-touch Functions

Možete prikazati samo potrebne ikone uređivanjem izgleda ikona prikazanog na početnom zaslonu za upravljačku ploču.

Prilikom postavljanja iz Web Config:

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

Prilikom postavljanja iz Epson Device Admin:

Odaberite **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** u predlošku konfiguracije.

Napomena:

U sljedećim slučajevima ikone za navedene funkcije nisu prikazane na početnom zaslonu.

- Kada odaberete funkcije koje nisu dopuštene zbog **Restrictions**.
- Kada nije registrirana adresa e-pošte za prijavljenog korisnika. (Scan to My Email)
- Kada odredišna mapa nije postavljena. (Scan to My Folder)

Stavka	Pojašnjenje
Maximum functions per screen	Odaberite raspored ikona prikazanih na upravljačkoj ploči. Slika se mijenja prema odabranom rasporedu.
Screen(s)	Odaberite broj stranica.

Stavka	Pojašnjenje
Number	Odaberite funkcije koje želite prikazati za svaki položaj označen brojem.

Job History izvješća koristeći Epson Device Admin

Možete kreirati Job History izvješće za svaku grupu i svakog korisnika koristeći Epson Device Admin. Na skener možete spremiti do 3000 primjera povijesti korištenja. Izvješće možete izraditi navođenjem razdoblja ili postavljanjem uobičajenog rasporeda.

Za izlaz Job History kao izvješće odaberite **Options > Epson Print Admin Serverless/Authentication Settings > Manage the Epson Print Admin Serverless/Authentication compatible devices** u izborniku vrpce na zaslonu Popis uređaja.

Za pojedinosti o izradi korisničkog izvješća pogledajte dokumentaciju za Epson Device Admin.


Stavke koje se mogu uključiti u Izvješće

U korisničkom izvješću možete ispisati sljedeće 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

Prijava kao administrator s upravljačke ploče

Možete koristiti bilo koju od sljedećih metoda za prijavu kao administrator s upravljačke ploče skenera.

1. Dodirnite  u gornjem desnom dijelu zaslona.
 - Kada se omogući Authentication Settings, ikona se prikazuje na zaslonu **Dobro došli** (zaslon u stanju pripravnosti za provjeru autentičnosti).
 - Kada se onemogući Authentication Settings, ikona se prikazuje na početnom zaslonu.
2. Dodirnite **Da** kada se prikaže zaslon za potvrdu.
3. Unesite administratorsku lozinku.

Prikazuje se poruka dovršene prijave, a zatim se prikazuje početni zaslon na upravljačkoj ploči.

Za odjavu dodirnite  u gornjem desnom kutu početnog zaslona.

Onemogućite Authentication Settings

Možete onemogućiti Authentication Settings koristeći Web Config.

Napomena:

User Settings registrirani na skeneru bit će spremljeni čak i ako je onemogućeno Authentication Settings. Možete ih ukloniti vraćanjem skenera na zadane postavke.

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

Napomena:

Čak i ako onemogućite Authentication Settings, Postavka blokade ostaje omogućeno. Ako želite onemogućiti, možete odabrati postavke preko upravljačke ploče ili programa Web Config.

Povezane informacije

- ➔ [“Postavljanje Postavka blokade s upravljačke ploče” na strani 85](#)
- ➔ [“Postavka Postavka blokade preko Web Config” na strani 85](#)

Brisanje Authentication Settings informacija (Obnovi zadane postavke)

Za brisanje svih Authentication Settings informacija (Card Reader, Authentication Method, User Settings, i tako dalje), vratite sve postavke skenera na zadane postavke u trenutku kupnje.

Odaberite **Postavke > Administracija sustava > Obnovi zadane postavke > Sve postavke** na upravljačkoj ploči.



Važno:

Svi kontakti i druge mrežne postavke također će biti izbrisani. Izbrisane postavke nije moguće vratiti.

Rješavanje problema

Nije moguće pročitati karticu za provjeru autentičnosti

Provjerite sljedeće.

- Provjerite je li uređaj za provjeru autentičnosti ispravno spojen na skener.
Spojite uređaj za provjeru autentičnosti na USB port vanjskog sučelja na stražnjoj strani skenera.
- Provjerite jesu li podržani uređaj i kartica za provjeru autentičnosti.

Održavanje

Čišćenje izvan skenera.	152
Čišćenje unutar skenera.	152
Zamjena kompleta sklopa valjka.	157
Resetiranje broja skenova.	162
Ušteda energije.	162
Transportiranje skenera.	163
Pomoć kod postavki.	164
Obnovi zadane postavke.	165
Ažuriranje aplikacija i upravljačkog programa.	166


Čišćenje izvan skenera

Obrišite sve mrlje na vanjskom kućištu suhom krpom ili krpom namočenom blagim deterdžentom i vodom.



Važno:

- Nikada ne koristite alkohol, razrjeđivač ili bilo kakvo korozivno otapalo za čišćenje skenera. Može doći do izobličenja ili promjene boje.*
- Ne dopustite da voda proдре unutar proizvoda. To bi moglo uzrokovati kvar.*
- Nikad ne otvarajte kućište skenera.*

1. Pritisnite gumb  kako biste isključili skener.
2. Iskopčajte AC prilagodnik iz skenera.
3. Očistite vanjsko kućište krpom navlaženom blagim deterdžentom i vodom.

Napomena:

Obrišite dodirni zaslon mekanom, suhom krpom.

Čišćenje unutar skenera

Nakon korištenja skenera neko vrijeme, papirna i okolna prašina na valjcima ili staklenom dijelu unutar skenera može uzrokovati probleme s umetanjem papira ili kvalitetom skenirane slike. Očistite unutrašnjost skenera svakih 5,000 skenova.


Možete provjeriti aktualni broj skenova na upravljačkoj ploči ili u programu Epson Scan 2 Utility.

Ako je površina zaprljana materijalom koji se teško uklanja, upotrijebite originalni Epsonov komplet za čišćenje kako biste uklonili mrlje. Upotrijebite malu količinu sredstva za čišćenje na krpi za čišćenje kako biste uklonili mrlje.

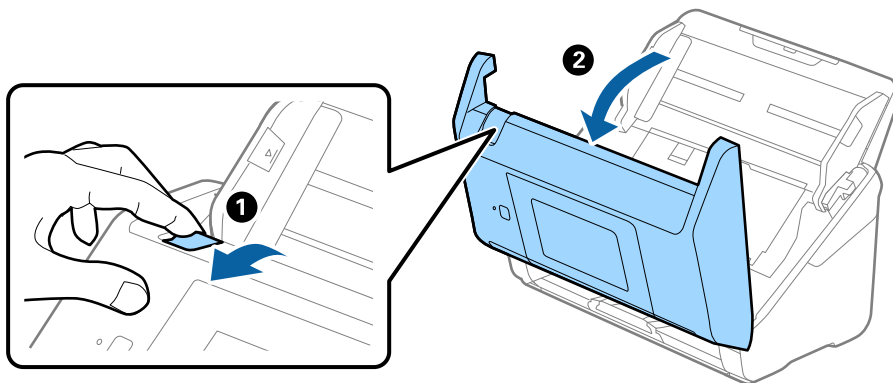


Važno:

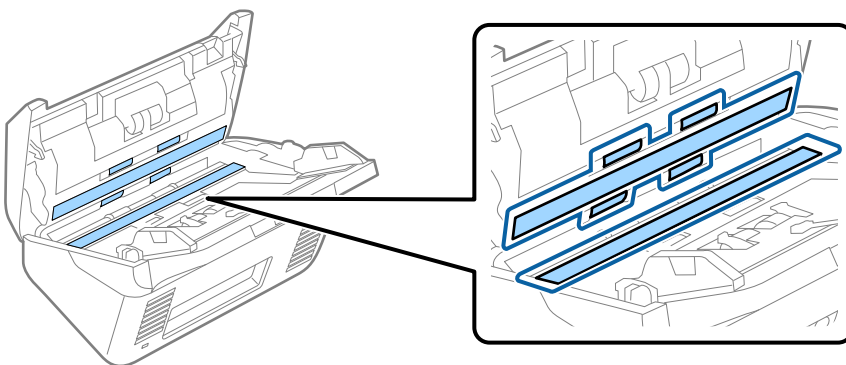
- Nikada ne koristite alkohol, razrjeđivač ili bilo kakvo korozivno otapalo za čišćenje skenera. Može doći do izobličenja ili promjene boje.*
- Nikada ne prskajte tekućinu ili lubrikant po skeneru. Oštećenje opreme ili sklopovlja može uzrokovati neispravan rad.*
- Nikad ne otvarajte kućište skenera.*

1. Pritisnite gumb  kako biste isključili skener.
2. Iskopčajte AC prilagodnik iz skenera.

3. Povucite ručicu i otvorite poklopac skenera.



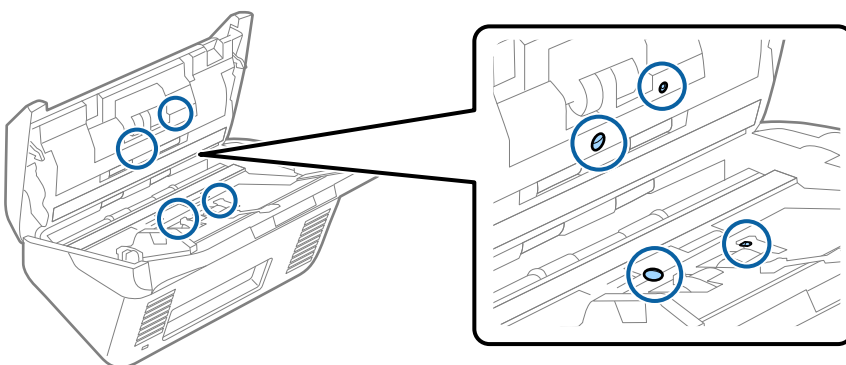
4. Obrišite sve mrlje s plastičnog valjka i staklene površine na dnu unutar poklopca skenera koristeći mekanu krpu ili originalni Epsonov komplet za čišćenje.



Važno:

- Ne pritiskajte prejako staklenu površinu.
- Nemojte koristiti četku ni tvrdi alat. Ogrebotine stakla mogu utjecati na kvalitetu skeniranja.
- Ne prskajte sredstvo za čišćenje izravno na staklenu površinu.

5. Obrišite sve mrlje sa senzora pomoću pamučnim štapićem.

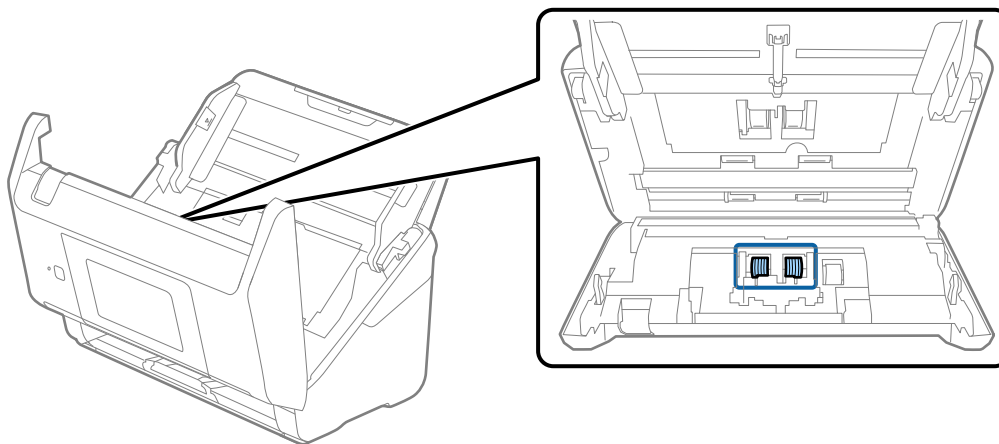




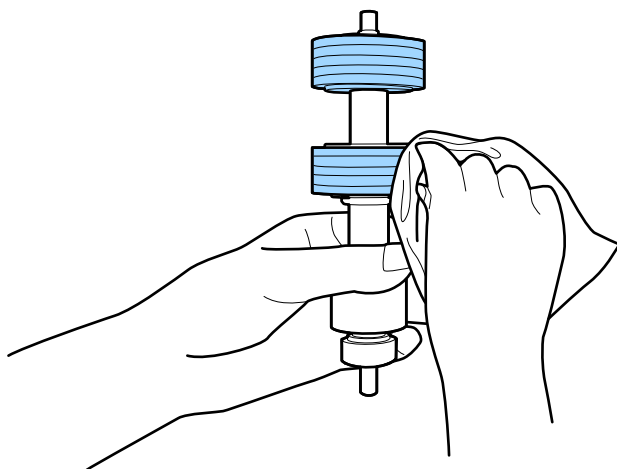
Važno:

Nemojte koristiti tekućinu, primjerice sredstvo za čišćenje, na pamučnom štapiću.

6. Otvorite poklopac i zatim uklonite valjak za odvajanje.
Saznajte više u dijelu “Zamjena kompleta sklopa valjka”.



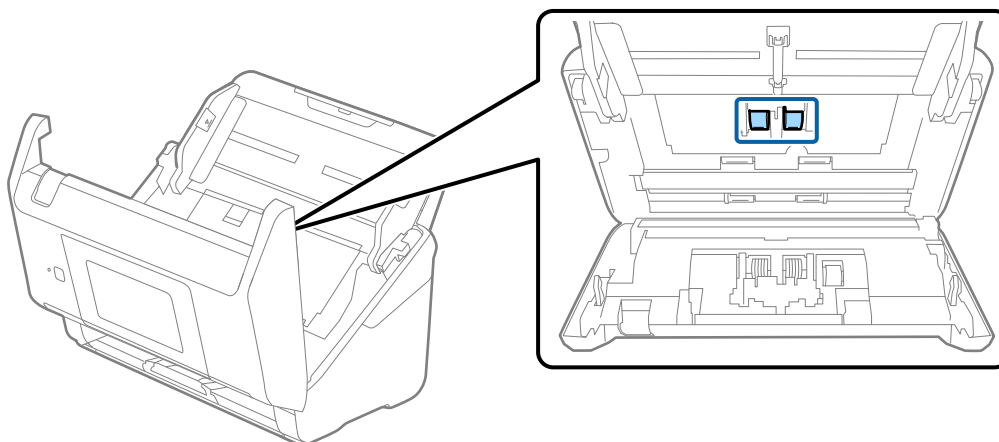
7. Obrišite svu prašinu ili prljavštinu s valjka za odvajanje koristeći originalni Epsonov set za čišćenje ili mekanu, navlaženu krpku.



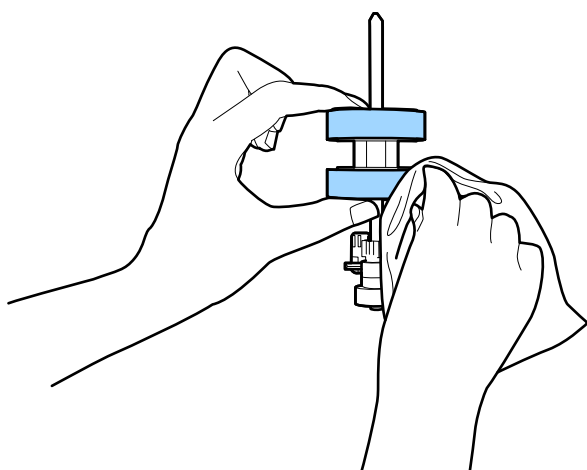
Važno:

Upotrijebite originalni Epsonov set za čišćenje ili mekanu, navlaženu krpku kako biste očistili valjak. Korištenje suhe krpe može oštetiti površinu valjka.

8. Otvorite poklopac i zatim uklonite valjak za preuzimanje.
Saznajte više u dijelu “Zamjena kompleta sklopa valjka”.



9. Obrišite svu prašinu ili prljavštinu s valjka za preuzimanje koristeći originalni Epsonov set za čišćenje ili mekanu, navlaženu krpku.

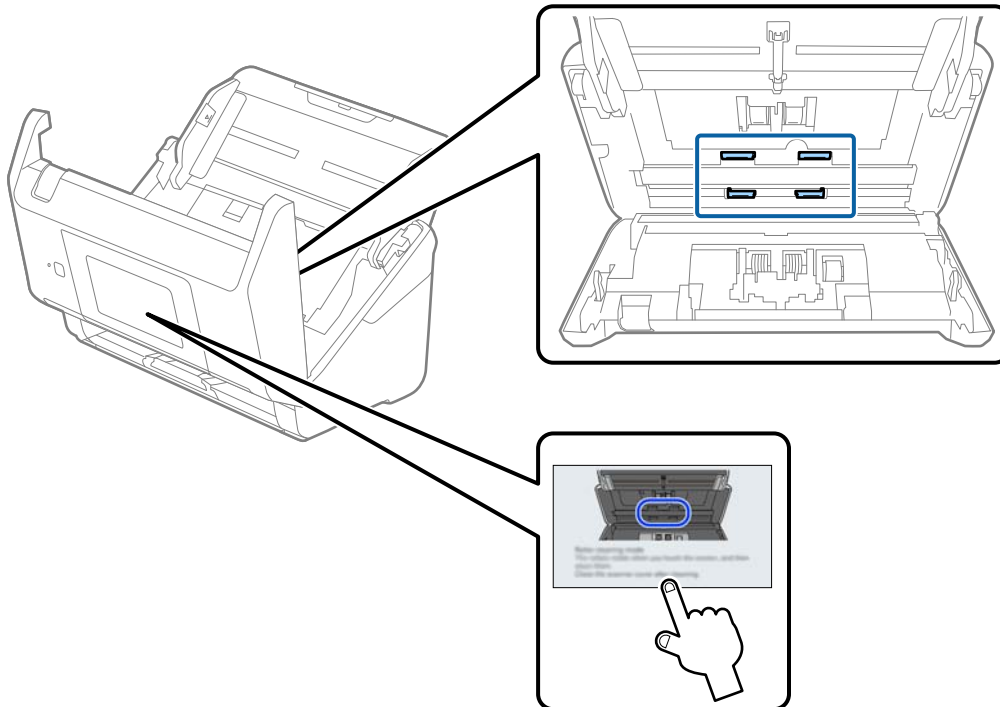


Važno:

Upotrijebite originalni Epsonov set za čišćenje ili mekanu, navlaženu krpku kako biste očistili valjak. Korištenje suhe krpe može oštetiti površinu valjka.

10. Zatvorite poklopac skenera.
11. Ukopčajte AC prilagodnik i uključite skener.
12. Odaberite **Održavanje skenera** iz početnog zaslona.
13. Na zaslonu **Održavanje skenera** odaberite **Čišćenje valjka**.
14. Povucite ručicu da biste otvorili poklopac skenera.
Skener pokreće način rada za čišćenje valjka.

- Polako okrećite valjke na dnu dodirivanjem bilo kojeg mjesta na LCD-zaslonu. Obrišite površinu valjaka koristeći originalni Epsonov set za čišćenje ili mekanu krpu natopljenu vodom. Ponovite ovo dok valjci ne budu čisti.



Pozor:

Pazite da vaše ruke ili kosu ne uhvati mehanizam tijekom okretanja valjka. To bi moglo izazvati ozljedu.

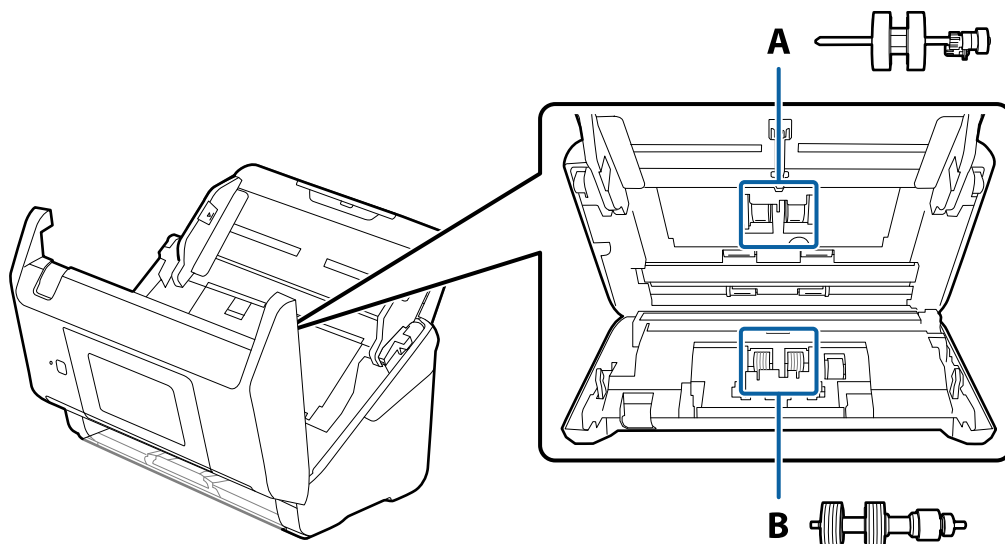
- Zatvorite poklopac skenera.
Skener izlazi iz načina rada za čišćenje valjka.

Povezane informacije


➔ [“Zamjena kompleta sklopa valjka” na strani 157](#)

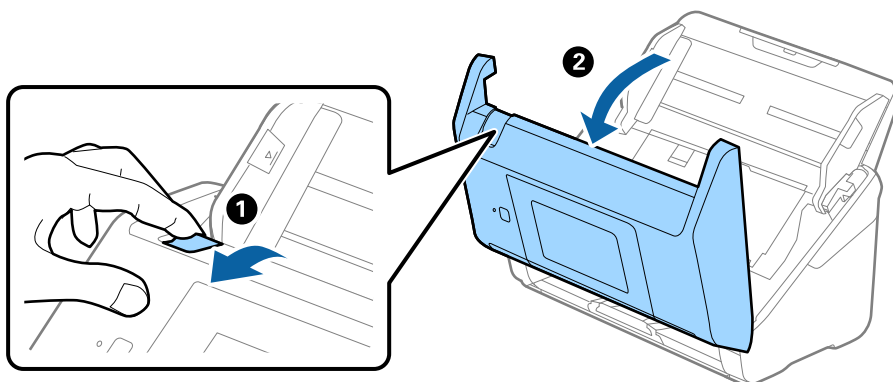
Zamjena kompleta sklopa valjka

Komplet sklopa valjka (valjak za preuzimanje i valjak za odvajanje) treba zamijeniti kada nekoliko skenova prekorači životni ciklus valjaka. Kada se poruka zamjene prikaže na upravljačkoj ploči ili zaslonu računala, slijedite donje korake za zamjenu.

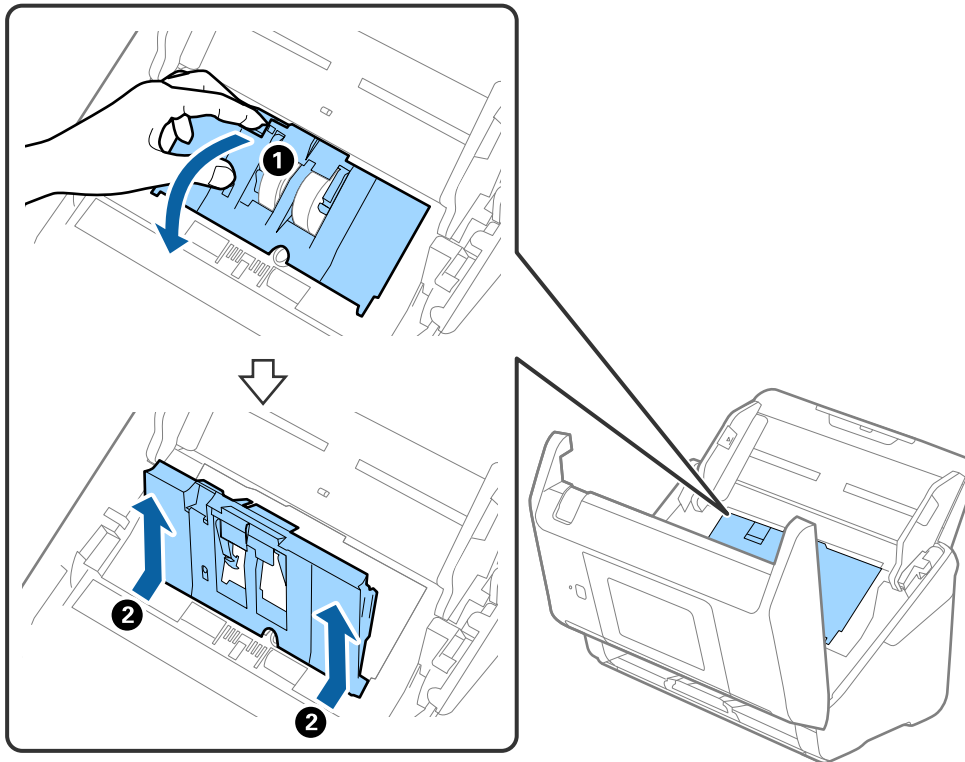


A: valjak za preuzimanje, B: valjak za odvajanje

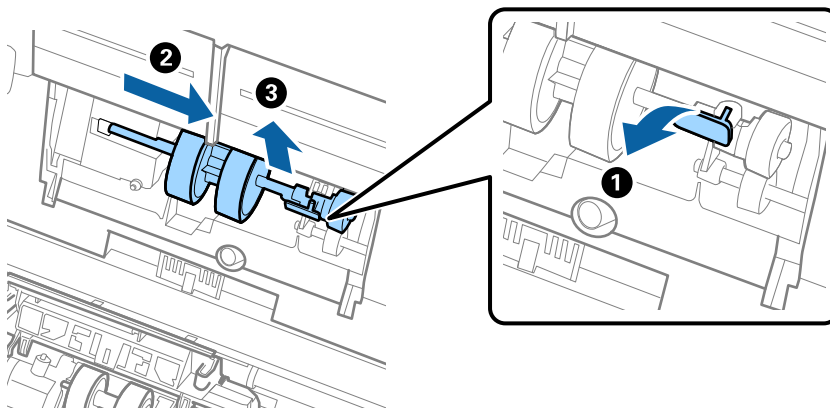
1. Pritisnite gumb  kako biste isključili skener.
2. Iskopčajte AC prilagodnik iz skenera.
3. Povucite ručicu i otvorite poklopac skenera.



4. Otvorite poklopac valjka za preuzimanje, gurnite ga i uklonite.



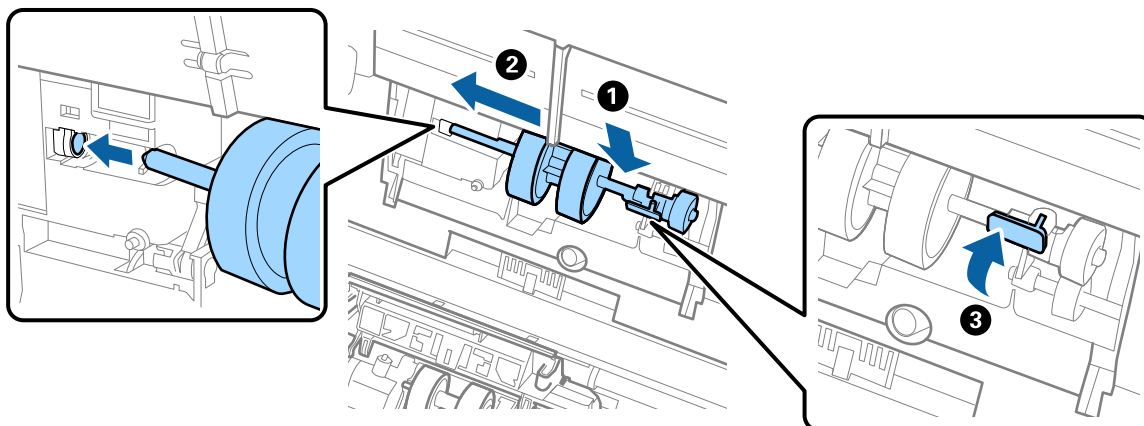
5. Povucite učvršćenje osovinnice valjka i zatim gurnite i uklonite valjke za preuzimanje.



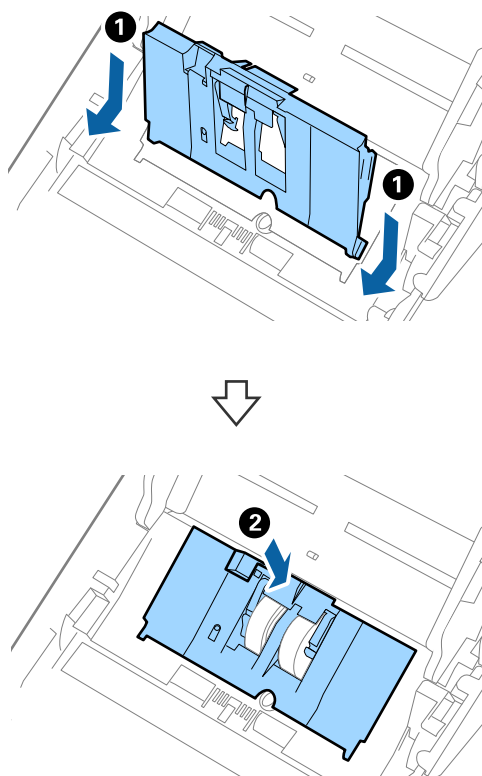
Važno:

Nemojte snažno izvlačiti valjak za preuzimanje. To bi moglo oštetiti unutrašnjost skenera.

6. Pridržavajući učvršćenje, gurnite novi valjak za preuzimanje ulijevo i umetnite ga u otvor skenera. Pritisnite učvršćenje kao biste ga osigurali.

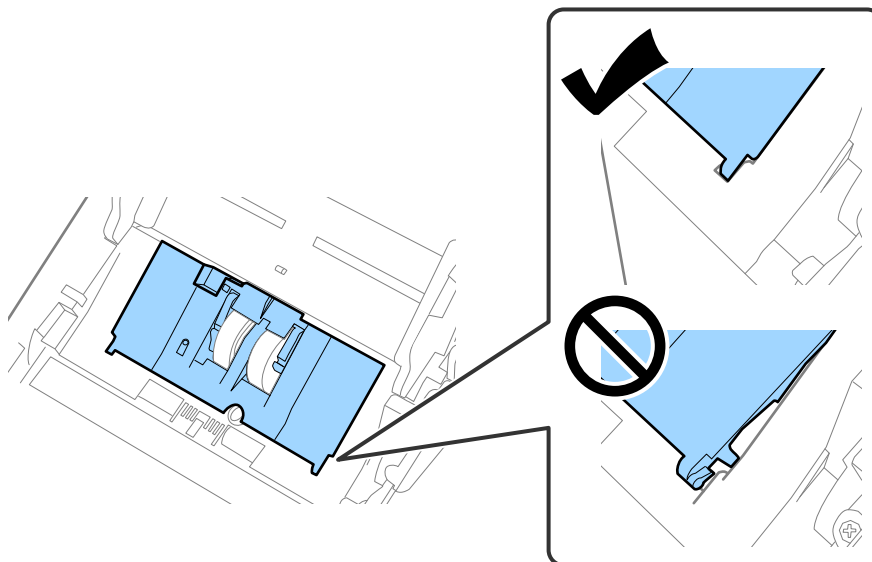


7. Rub poklopca valjka za preuzimanje umetnite u žlijeb i gurnite ga. Čvrsto zatvorite poklopac.

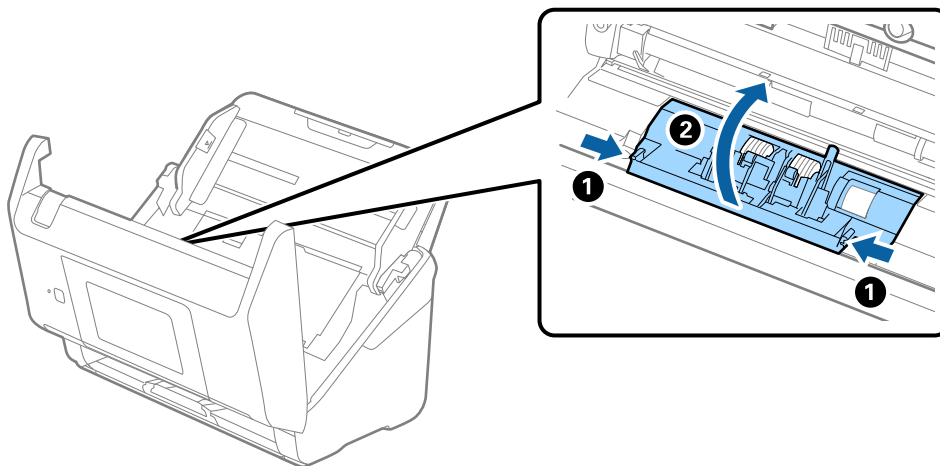


! **Važno:**

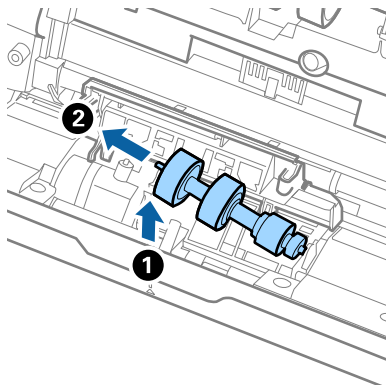
- ❑ Uvjerite se da je poklopac jedinice za preuzimanje pravilno zatvoren.
- ❑ Uvjerite se da su valjci za uvlačenje pravilno postavljeni ako se poklopac otežano zatvara.
- ❑ Nemojte postavljati poklopac dok je podignut.



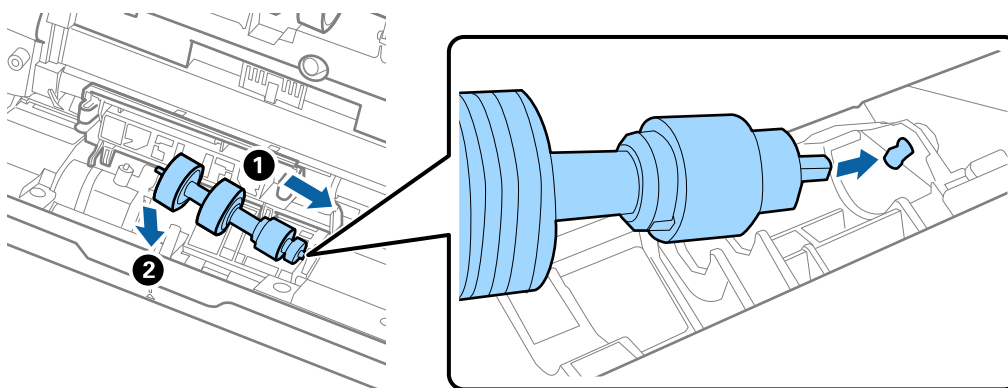
8. Gurnite kukice na krajevima poklopca valjka za odvajanje kako bi se otvorio poklopac.



9. Podignite lijevu stranu valjka za odvajanje, a zatim gurnite i uklonite ugrađene valjke za razdvajanje.



10. Umetnite novu osovinicu valjka za odvajanje u desnu rupu i zatim spustite valjak.



11. Zatvorite poklopac valjka za odvajanje.



Važno:

Ako se poklopac ne može zatvoriti, provjerite jesu li valjci za odvajanje pravilno instalirani.

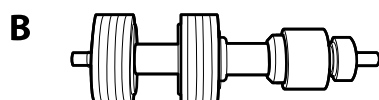
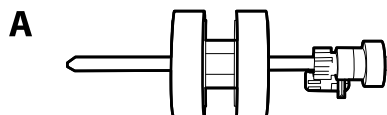
12. Zatvorite poklopac skenera.
13. Ukopčajte AC prilagodnik i uključite skener.
14. Resetirajte broj skenova na upravljačkoj ploči.

Napomena:

Zbrinite valjak za preuzimanje i valjak za odvajanje poštujući pravila i propise lokalnih nadležnih tijela. Nemojte ih rastavljati.

Kodovi kompleta za sklapanje valjka

Dijelovi (valjak za preuzimanje i valjak za odvajanje) se trebaju zamijeniti kada broj skenova prekorači servisni broj. Možete provjeriti najnoviji broj skenova na upravljačkoj ploči ili u programu Epson Scan 2 Utility.



A: valjak za preuzimanje, B: valjak za odvajanje

Naziv dijela	Kodovi	Životni ciklus
Komplet za sklapanje valjka	B12B819671 B12B819681 (samo Indija)	200,000*

* Ovaj broj je dostignut uzastopnim skeniranjem koristeći originalne probne Epson papire te je smjernica za ciklus zamjene. Ciklus zamjene može se mijenjati ovisno o različitim tipovima papira, kao što je papir koji stvara mnogo prašine papira ili papir hrapave površine koji može skratiti životni ciklus.

Resetiranje broja skenova

Resetira broj skenova nakon zamjene kompleta za sklapanje valjka.

1. Odaberite **Postavke > Podaci o uređaju > Resetiraj broj skeniranja > Broj skenova nakon zamjene valjka s početnog zaslona**.
2. Dodirnite **Da**.

Povezane informacije

➔ [“Zamjena kompleta sklopa valjka” na strani 157](#)

Ušteda energije

Možete uštedjeti energiju primjenom načina mirovanja ili automatskog isključivanja kada računalo ne izvršava nikakvu radnju. Možete postaviti razdoblje prije nego skener uđe u način mirovanja i automatski se isključi. Svako povećanje utjecat će na energetski učinak proizvoda. Prije bilo kakvih promjena, uzmite u obzir zaštitu okoliša.

1. Odaberite **Postavke** na početnom zaslonu.
2. Odaberite **Osnovne postavke**.


3. Odaberite **Postavke za isklj.** i podesite ih.

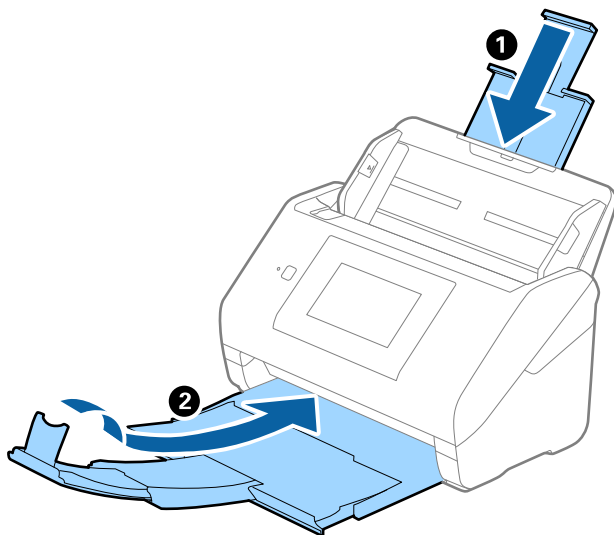
Napomena:

Dostupne značajke mogu se razlikovati ovisno o mjestu kupnje.

Transportiranje skenera

Ako trebate prenositi skener radi premještanja ili popravaka, slijedite korake u nastavku kako biste zapakirali skener.

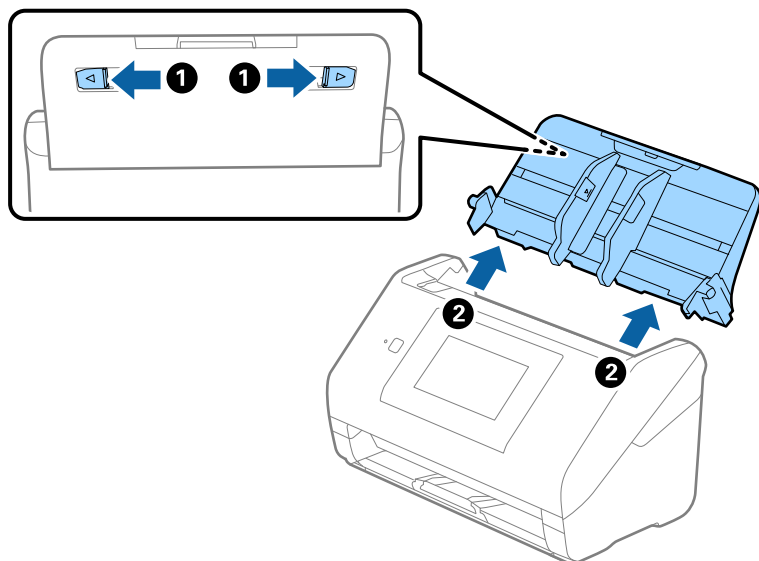
1. Pritisnite gumb  kako biste isključili skener.
2. Iskopčajte AC adapter.
3. Uklonite kabele i uređaje.
4. Zatvorite produžetak ulaznog pretinca i izlazni pretinac.



Važno:

Pobrinite se da je izlazni pretinac sigurno zatvoren, jer bi se u protivnom mogao oštetiti tijekom transporta.

- Uklonite ulazni pretinac.



- Zapakirajte skener u materijale za pakiranje koje ste dobili sa skenerom te ponovno zapakirajte skener u originalnu kutiju.

Pomoć kod postavki

Možete izvesti vrijednost postavke iz Web Config u datoteku. Možete je koristiti za sigurnosno kopiranje kontakata, odabir vrijednosti, zamjenu skenera, itd.

Izvezena datoteka ne može se uređivati jer je izvezena u binarnom obliku.

Izvoz postavki

Izvezite postavke skenera.

- Pristupite aplikaciji Web Config i odaberite karticu **Device Management > Export and Import Setting Value > Export**.
- Odaberite postavke koji želite izvesti.
Odaberite postavke koje želite izvesti. Ako odaberete nadređenu kategoriju, odabrat će se i potkategorije. Međutim, potkategorije koje uzrokuju greške dupliciranjem unutar isti mreže (kao što su IP adrese i sl.) ne mogu se odabrati.
- Unesite lozinku kako biste šifrirali izvezenu datoteku.
Za uvoz datoteke potrebna vam je lozinka. Ostavite ovo mjesto prazno ako ne želite šifrirati datoteku.

4. Kliknite na **Export**.



Važno:

Ako želite izvesti mrežne postavke skenera, kao što su naziv uređaja i IPv6 adresa, odaberite **Enable to select the individual settings of device** i odaberite više stavki. Koristite samo odabrane vrijednosti za zamjenski skener.

Povezane informacije

- ➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Uvoz postavki

U skener uvezite izvezenu Web Config datoteku.



Važno:

Prilikom uvoza vrijednosti koje sadrže pojedine podatke, kao što su naziv skenera, IP adresa, pazite da ista IP adresa ne postoji na istoj mreži.

1. Pristupite aplikaciji Web Config i odaberite karticu **Device Management > Export and Import Setting Value > Import**.
2. Odaberite izvezenu datoteku i zatim unesite šifriranu lozinku.
3. Kliknite na **Next**.
4. Odaberite postavke koje želite uvesti i zatim kliknite na **Next**.
5. Kliknite na **OK**.

Postavke će se primijeniti na skener.

Povezane informacije

- ➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Obnovi zadane postavke

Na upravljačkoj ploči odaberite **Postavke > Administracija sustava > Obnovi zadane postavke**, a zatim odaberite stavke koje želite vratiti na zadane vrijednosti.

- Postavke mreže: vratite mrežne postavke na njihov početni status.
- Sve osim Postavke mreže: vratite druge postavke na njihov početni status izuzev mrežnih postavki.
- Sve postavke: vratite sve postavke na njihov početni status nakon kupnje.



Važno:

Ako odaberete i pokrenete **Sve postavke**, svi podaci postavki registriranih za skener, uključujući kontakte i postavke provjere autentičnosti korisnika, bit će izbrisani. Izbrisane postavke nije moguće vratiti.

Ažuriranje aplikacija i upravljačkog programa

Riješite određene probleme i poboljšajte ili dodajte funkcije ažuriranjem aplikacija ili upravljačkog programa. Koristite najnoviju verziju aplikacija i upravljačkog programa.



Važno:

Ne isključujte računalo ili skener dok traje ažuriranje.

Napomena:

Kada se skener može spojiti na internet, možete ažurirati upravljački program koristeći Web Config. Odaberite karticu **Device Management > Firmware Update**, provjerite prikazanu poruku i zatim kliknite na **Start**.

1. Pobrinite se da skener i računalo budu međusobno povezani i da je računalo spojeno na internet.
2. Pokrenite EPSON Software Updater kako biste ažurirali aplikacije ili upravljački program.

Napomena:

Nisu podržani operativni sustavi poslužitelja sustava Windows.

Windows 10

Kliknite na gumb Start i odaberite **Epson Software > EPSON Software Updater**.

Windows 8.1/Windows 8

Unesite naziv aplikacije u gumbić za pretraživanje i zatim odaberite prikazanu ikonu.

Windows 7

Kliknite na gumb Start i odaberite **Svi programi ili Programi > Epson Software > EPSON Software Updater**.

Mac OS

Odaberite **Alat za traženje > Idi > Aplikacije > Epson Software > EPSON Software Updater**.

Napomena:

Ako ne možete pronaći aplikaciju koju želite ažurirati na popisu aplikacija, tada postupak ažuriranja ne možete izvršiti korištenjem programa EPSON Software Updater. Potražite najnovije verzije aplikacija na lokalnoj mrežnoj Epsonovoj stranici.

<http://www.epson.com>

Ažuriranje upravljačkog softvera skenera preko upravljačke ploče

Ako je skener spojen na Internet, možete ažurirati firmver skenera preko upravljačke ploče. Također možete postaviti skener da redovito provjerava ažuriranja upravljačkog softvera i obavijesti vas kada budu dostupna.

1. Odaberite **Postavke** na početnom zaslonu.

2. Odaberite **Administracija sustava > Ažuriranje firmvera > Ažuriraj**.

Napomena:

Odaberite **Obavijest > Uklj.** kako biste postavili skener da redovito provjerava dostupna ažuriranja upravljačkog softvera.

3. Pročitajte poruku prikazanu na zaslonu i počnite pretraživati raspoloživa ažuriranja.
4. Ako je na LCD zaslonu prikazana poruka koja vas obavještava da je dostupno ažuriranje upravljačkog softvera, slijedite prikazane upute kako biste pokrenuli ažuriranje.



Važno:

- Nemojte isključivati ni odspajati skener dok se ne izvrši ažuriranje, jer bi moglo doći do kvara skenera.
- Ako se ažuriranje upravljačkog softvera ne izvrši uspješno, skener se neće normalno pokrenuti te će kod sljedećeg uključivanja skenera na LCD zaslonu biti prikazano „Recovery Mode”. U toj situaciji ponovno trebate ažurirati upravljački softver koristeći računalo. Spojite skener na računalo koristeći USB kabel. Dok je na skeneru prikazano „Recovery Mode”, ne možete ažurirati upravljački softver preko mrežne veze. Na računalo pristupite lokalnoj Epson web-stranici i zatim preuzmite najnoviji upravljački softver skenera. Sljedeći koraci navedeni su na web-stranici.

Ažuriranje firmvera koristeći Web Config

Kada se skener može spojiti na internet, možete ažurirati upravljački program koristeći Web Config.

1. Pristupite aplikaciji Web Config i odaberite karticu **Device Management > Firmware Update**.
2. Kliknite na **Start** i slijedite upute na zaslonu.

Pokreće se potvrda firmvera te se informacije o firmveru prikazuju ako postoji ažurirani firmver.

Napomena:

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

Povezane informacije

➔ [“Pokretanje programa Web Config u internetskom pregledniku” na strani 35](#)

Ažuriranje upravljačkog programa bez spajanja na internet

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

Napomena:

Prije ažuriranja provjerite je li upravljački program skenera *Epson Scan 2* instaliran na vašem računalo. Ako nije instalirana aplikacija *Epson Scan 2*, instalirajte je.

1. Provjerite Epson internetsku stranicu s najnovijim izdanjima ažuriranja firmvera.

<http://www.epson.com>

- Ako postoji firmver za vaš skener, preuzmite ga i prijedite na sljedeći korak.

- Ako na internetskoj stranici nema informacija o firmveru, već koristite najnoviji firmver.
- 2. Spojite računalo koji sadrži preuzeti firmver na skener preko USB kabela.
- 3. Dvaput kliknite na preuzetu datoteku nastavka .exe.
Pokrenut će se aplikacija Epson Firmware Updater.
- 4. Slijedite upute na zaslonu.