EPSON
EXCEED YOUR VISION

DS-790WN

Водич за администратори

NPD6726-00 MK

Авторски права

Трговски марки

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION и нивните логоа се регистрирани трговски марки или трговски марки на 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 и PaSoRi се регистрирани трговски марки на Sony Corporation.
- ❏ MIFARE е регистрирана трговска марка на NXP Semiconductor Corporation.
- ❏ Општо известување: останатите имиња на производи што се употребени овде се наменети само за идентификување и може да се трговски марки на нивните сопственици. Epson се одрекува од сите права врз овие марки.

Содржина

Основни безбедносни поставки

Напредни поставки за безбедност

Authentication Settings

Одржување

Вовед

Содржина на овој документ

Во овој документ се наведени следниве информации за администраторите на скенери.

❏ Мрежни поставки

❏ Подготовка на функцијата за скенирање

❏ Овозможување и управување со поставките за безбедност

❏ Овозможување и управување со Authentication Settings

❏ Вршење секојдневно одржување

Повеќе информации за стандардните начини на користење на скенерот се достапни во *Упатство за корисникот*.

Белешка:
Овој документ содржи објаснување за Authentication Settings кои нудат самостојна автентикација без да треба да користите сервер за автентикација. Покрај Authentication Settings наведени во овој прирачник, може и да создадете систем за автентикација користејќи сервер за автентикација. За да создадете систем за автентикација, користете Document Capture Pro Server Authentication Edition (скратено: Document Capture Pro Server AE).

За дополнителни информации, контактирајте со локалното претставништво на Epson.

Користење на овој прирачник

Ознаки и симболи

> ⚠ ***Внимание:***
> *Мора внимателно да ги следите упатствата за да не дојде до телесна повреда.*

> ***Важно:***
> *Мора да ги следите упатствата за да не дојде до оштетување на опремата.*

Белешка:
Дадени се дополнителни и референтни информации.

Поврзани информации

➡ Води кон поврзани делови.

Описи користени во овој прирачник

❏ Сликите од екран за апликациите се од Windows 10 или macOS High Sierra. Содржината прикажана на екраните се разликува во зависност од моделот и ситуацијата.

❏ Илустрациите користени во овој прирачник служат само за упатување. Иако илустрациите може да се делумно различни од конкретниот производ, начините на работа се исти.

Опфатени оперативни системи

Windows

Во овој прирачник, термините како што се „Windows 10", „Windows 8.1", „Windows 8", „Windows 7", „Windows Server 2019", „Windows Server 2016", „Windows Server 2012 R2", „Windows Server 2012" и „Windows Server 2008 R2" се однесуваат на следниве оперативни системи. Дополнително, „Windows" се однесува на сите верзии, а „Windows Server" се однесува на „Windows Server 2019", „Windows Server 2016", „Windows Server 2012 R2", „Windows Server 2012" и „Windows Server 2008 R2".

- ❏ Оперативен систем Microsoft® Windows® 10
- ❏ Оперативен систем Microsoft® Windows® 8.1
- ❏ Оперативен систем Microsoft® Windows® 8
- ❏ Оперативен систем Microsoft® Windows® 7
- ❏ Оперативен систем Microsoft® Windows Server® 2019
- ❏ Оперативен систем Microsoft® Windows Server® 2016
- ❏ Оперативен систем Microsoft® Windows Server® 2012 R2
- ❏ Оперативен систем Microsoft® Windows Server® 2012
- ❏ Оперативен систем Microsoft® Windows Server® 2008 R2

Mac OS

Во овој прирачник, „Mac OS" се однесува на macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan и OS X Yosemite.

Потребни поставки според намената

Потребни поставки според намената

Прочитајте ги долунаведените информации за да ги одредите потребните поставки според намената.

Поврзување на скенерот со мрежата

Намена	Потребни поставки
Сакам да го поврзам скенерот со мрежата.	Конфигурирајте го скенерот за мрежно скенирање. „Поврзување на скенерот со мрежата“ на страница 15
Сакам да го поврзам скенерот со нов компјутер.	Одредете ги мрежните поставки за вашиот скенер на новиот компјутер. „Додавање или менување на компјутерот или уредите“ на страница 22

Поставки за скенирање

Намена	Потребни поставки
Сакам да испратам скенирани слики по е-пошта. (Scan to Email)	1. Конфигурирајте го серверот за е-пошта што сакате да го поврзете. „Конфигурирање сервер за е-пошта“ на страница 45 2. Регистрирајте ја адресата на е-пошта на примачот во **Contacts** (изборно). Ако ја регистрирате адресата на е-пошта, нема да треба да ја внесувате секогаш кога сакате да испратите нешто, туку ќе може само да ја изберете од вашите контакти. „Побрз пристап до контактите“ на страница 67
Сакам да зачувам скенирани слики во папка на мрежата. (Scan to Network Folder/FTP)	1. Создајте папка на мрежата каде што сакате да ги зачувате сликите. „Поставување споделена мрежна папка“ на страница 48 2. Регистрирајте ја патеката на папката во **Contacts** (изборно). Ако ја регистрирате патеката на папката, нема да треба да ја внесувате секогаш кога сакате да испратите нешто, туку ќе може само да ја изберете од вашите контакти. „Побрз пристап до контактите“ на страница 67
Сакам да зачувам скенирани слики во услуга на облак. (Scan to Cloud)	Поставете ја Epson Connect. За повеќе информации околу поставувањето, посетете ја веб-локацијата за Epson Connect. При поставувањето, ќе ви треба корисничка сметка за услугата за онлајн складирање со која сакате да се поврзете. https://www.epsonconnect.com/ http://www.epsonconnect.eu (само за Европа)

Приспособување на приказот на контролната табла

Намена	Потребни поставки
Сакам да ги променам поставките прикажани на контролната табла на скенерот.	Поставете **Поч. пос.** или **Уреди Почеток**. Вашите претпочитани поставки за скенирање може да ги регистрирате на контролната табла и да ги изменувате прикажаните ставки. „Приспособување на приказот на контролната табла“ на страница 81

Поставување основни безбедносни функции

Намена	Потребни поставки
Сакам никој да не може да ги менува поставките на скенерот, освен администраторот.	Поставете администраторска лозинка за скенерот. „Администраторски поставки“ на страница 90
Сакам да ја оневозможам употребата на скенери со USB-врски.	Оневозможете го надворешниот интерфејс. „Оневозможување на надворешниот интерфејс“ на страница 96

Поставување напредни безбедносни функции

Намена	Потребни поставки
Сакам да контролирам кои протоколи може да се користат.	Овозможете или оневозможете ги протоколите. „Контролирање на користењето протоколи“ на страница 102
Сакам да ја шифрирам патеката за комуникација.	1. Конфигурирајте го вашиот дигитален сертификат. „Користење на дигитален сертификат“ на страница 105 2. Конфигурирајте SSL/TLS-комуникација. „SSL/TLS комуникација со скенер“ на страница 111
Сакам да користам шифрирана комуникација (IPsec). Сакам да можам да го користам софтверот само од одреден компјутер (IP-филтрирање).	Поставете правила за филтрирање сообраќај. „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 112
Сакам да користам скенер на IEEE802.1X-мрежа.	Конфигурирајте IEEE802.1X за скенерот. „Поврзување на скенерот на IEEE802.1X мрежа“ на страница 124

Поставување функции што треба да ги автентицира скенерот

Намена	Потребни поставки
Сакам да овозможам Authentication Settings.	Погледнете го следново за повеќе информации околу достапните Authentication Settings и Authentication Method. „За Authentication Settings“ на страница 134 „За Authentication Method“ на страница 135

Користење на системот за автентикација на серверот

Со Document Capture Pro Server Authentication Edition (скратено: Document Capture Pro Server AE), може да создадете систем за автентикација што користи сервер за автентикација.

За дополнителни информации, контактирајте со локалното претставништво на Epson.

Мрежни поставки

Поврзување на скенерот со мрежата

Во овој дел се објаснува постапката за поврзување на скенерот со мрежата користејќи ја контролната табла на скенерот.

Белешка:
Ако скенерот и компјутерот се во истиот сегмент, поврзувањето може да го извршите и со програмата за инсталирање.

❏ *Поставување од веб-локацијата*

*Одете на следнава веб-локација и внесете го името на производот. Одете на **Поставување**, а потоа започнете со поставување.*

http://epson.sn

❏ *Поставување со користење на дискот со софтвер (само за модели коишто доаѓаат со диск со софтвер и за корисници со компјутери со Windows со погони за диск.)*

Внесете го дискот со софтвер во компјутерот и следете ги инструкциите на екранот.

Пред воспоставување мрежна врска

За да се поврзете со мрежата, прво проверете го начинот на поврзување и информациите за поставките за врската.

Прибирање информации за поставките за поврзување

Подгответе ги потребните информации за поставките за поврзување. Проверете ги следниве информации однапред.

Одделни информации	Ставки	Забелешка
Начин на поврзување на уредот	❏ Етернет ❏ Wi-Fi	Одлучете како да го поврзете скенерот со мрежата. За жична LAN, се поврзува со LAN-преклопникот. За Wi-Fi, се поврзува со мрежата (SSID) на точката за пристап.
Информации за поврзување преку LAN	❏ IP-адреса ❏ Подмрежна маска ❏ Стандардна капија	Изберете IP-адреса за доделување на скенерот. Кога доделувате статична IP-адреса, треба да ги внесете сите вредности. Кога доделувате динамична IP-адреса користејќи ја функцијата DHCP, овие информации не се потребни бидејќи се поставуваат автоматски.
Информации за поврзување преку Wi-Fi	❏ SSID ❏ Лозинка	Ова се SSID (името на мрежата) и лозинката на точката за пристап со коишто се поврзува скенерот. Ако е поставено филтрирање MAC-адреси, регистрирајте ја MAC-адресата на скенерот однапред за да го регистрирате скенерот. Поддржаните стандарди се наведени овде. „Мрежни спецификации“ на страница 30

Одделни информации	Ставки	Забелешка
Информации за DNS-сервер	❏ IP-адреса за примарен DNS ❏ IP-адреса за секундарен DNS	Овие информации се потребни при одредување DNS-сервери. Секундарниот DNS се поставува кога системот има непотребна конфигурација и има секундарен DNS-сервер. Ако сте во мала организација и не го поставувате DNS-серверот, поставете ја IP-адресата на рутерот.
Информации за прокси-сервер	❏ Име на прокси-сервер	Поставете го ова кога мрежната околина го користи прокси-серверот за пристап до интернет преку интранет и кога користите функција за којашто скенерот пристапува директно до интернет. За следниве функции, скенерот се поврзува директно на интернет. ❏ Услуги Epson Connect ❏ Услуги во облак на други компании ❏ Ажурирање на фирмверот ❏ Испраќање скенирани слики во SharePoint (WebDAV)
Информации за број на порта	❏ Број на порта за отворање	Проверете го бројот на портата што ја користат скенерот и компјутерот и, ако е потребно, отворете ја портата што ја блокира заштитниот ѕид. Бројот на портата што ја користи скенерот е наведен овде. „Употреба на порта за скенерот“ на страница 32

Доделување IP-адреса

Следуваат типовите IP-адреси што може да се доделат.

Статична IP адреса:

Доделете ја претходно одредената IP-адреса на скенерот (хостот) рачно.

Информациите за поврзување со мрежата (подмрежна маска, стандарден мрежен премин, DNS-сервер итн.) треба да се постават рачно.

IP-адресата не се менува дури и кога уредот е исклучен, па ова е корисно кога сакате да управувате со уреди во околина каде што не може да ја менувате IP-адресата или каде што сакате да управувате со уредите користејќи ја IP-адресата. Препорачуваме поставки за скенерот, серверот итн., до коишто пристапуваат многу компјутери. Исто така, кога користите безбедносни функции како што се IPsec/IP-филтрирање, доделете фиксна IP-адреса за да не се менува IP-адресата.

Автоматско доделување користејќи ја функцијата DHCP (динамична IP-адреса):

Доделете ја IP-адресата на скенерот (хостот) автоматски, користејќи ја функцијата DHCP на DHCP-серверот или рутерот.

Информациите за поврзување со мрежата (подмрежна маска, стандарден мрежен премин, DNS-сервер итн.) се поставуваат автоматски, па уредот може лесно да го поврзете со мрежата.

IP-адресата може да се промени при следното поврзување, ако уредот или рутерот се исклучени или во зависност од поставките за DHCP-серверот.

Препорачуваме управување со уреди и комуникација со протоколи што може да ја следат IP-адресата.

Белешка:
Кога ја користите функцијата за резервирање IP-адреси на DHCP, може да ја доделите истата IP-адреса на уредите во секое време.

DNS сервер и Proxy сервер

DNS-серверот има име на хост, име на домен на адресата на е-пошта, итн. поврзани со информациите за IP-адресата.

Не е возможна комуникација ако другата страна е опишана со име на хост, име на домен, итн. кога компјутерот или скенерот врши IP-комуникација.

Ги бара тие информации од DNS-серверот и ја добива IP-адресата на другата страна. Овој процес се нарекува разрешување на имиња.

Затоа, уредите како што се компјутери и скенери може да комуницираат користејќи ја IP-адресата.

Разрешувањето на имиња е потребно за скенерот да комуницира користејќи ја функцијата за е-пошта или функцијата за интернет-врска.

Кога ги користите тие функции, одредете ги поставките за DNS-серверот.

Кога ја доделувате IP-адресата на скенерот користејќи ја DHCP-функцијата на DHCP-серверот или рутерот, таа се поставува автоматски.

Прокси-серверот е поставен на капијата меѓу мрежата и интернетот и комуницира со компјутерот, скенерот и интернетот (сервер од спротивната страна) во нивно име. Серверот од спротивната страна комуницира само со прокси-серверот. Затоа, информациите за скенерот како што се IP-адресата и бројот на портата не може да се прочитаат, па се очекува зголемена безбедност.

Кога се поврзувате на интернет преку прокси-сервер, конфигурирајте го прокси-серверот на скенерот.

Поврзување со мрежата преку контролната табла

Поврзете го скенерот со мрежата преку контролната табла на скенерот.

Доделување на IP-адресата

Поставете ги основните ставки како што се адреса на хост, Маска на подмрежа и Стандарден излез.

Во овој дел се објаснува постапката за поставување статична IP-адреса.

1. Вклучете го скенерот.
2. Изберете **Поставки** на почетниот екран на контролната табла на скенерот.
3. Изберете **Поставки за мрежа** > **Напредно** > **TCP/IP**.

4. Изберете **Рачно** за **Добиј IP Адреса**.

   Кога ја поставувате IP-адресата автоматски со DHCP-функцијата на рутерот, изберете **Автоматски**. Во тој случај, **IP адреса**, **Маска на подмрежа** и **Стандарден излез** од чекор 5 до 6 исто така се поставуваат автоматски, па одете на чекор 7.

5. Внесете ја IP-адресата.

   Фокусот се преместува до предниот или задниот сегмент одвоени со точка ако изберете ◀ и ▶.

   Потврдете ја вредноста прикажана на претходниот екран.

6. Поставете ги **Маска на подмрежа** и **Стандарден излез**.

   Потврдете ја вредноста прикажана на претходниот екран.

   > ***Важно:***
   >
   > *Ако комбинацијата од IP адреса, Маска на подмрежа и Стандарден излез е неточна,* ***Започни со поставување*** *е неактивно и не може да продолжи со поставките. Погрижете се да нема грешка во ставката.*

7. Внесете ја IP-адресата за примарниот DNS-сервер.

   Потврдете ја вредноста прикажана на претходниот екран.

   Белешка:
   Кога ќе изберете ***Автоматски*** *за поставките за доделување IP-адреса, може да ги изберете поставките за DNS-сервер од* ***Рачно*** *или од* ***Автоматски****. Ако не може автоматски да ја добиете адресата за DNS-сервер, изберете* ***Рачно*** *и внесете ја адресата за DNS-сервер. Потоа, директно внесете ја адресата за секундарниот DNS-сервер. Ако изберете* ***Автоматски****, одете на чекор 9.*

8. Внесете ја IP-адресата за секундарниот DNS-сервер.

   Потврдете ја вредноста прикажана на претходниот екран.

9. Допрете **Започни со поставување**.

Поставување прокси-сервер

Поставете го прокси-серверот ако е точно следново.

❏ Прокси-серверот е наменет за интернет-врска.

❏ Кога користите функција за којашто скенерот директно се поврзува на интернет, како што е услугата Epson Connect или услуги во облак на друга компанија.

1. Изберете **Поставки** на почетниот екран.

   Кога одредувате поставки откако ќе се постави IP-адреса, се прикажува екранот **Напредно**. Одете на чекор 3.

2. Изберете **Поставки за мрежа** > **Напредно**.

3. Изберете **Прокси-сервер**.

4. Изберете **Упот.** за **Поставки за прокси сервер**.

5. Внесете ја адресата за прокси-серверот во IPv4 или FQDN-формат.

   Потврдете ја вредноста прикажана на претходниот екран.

6. Внесете број на порта за прокси-серверот.

   Потврдете ја вредноста прикажана на претходниот екран.

7. Допрете **Започни со поставување**.

Поврзување со етернет

Поврзете го скенерот со мрежата користејќи LAN-кабел, па проверете ја врската.

1. Поврзете ги скенерот и хабот (LAN-преклопникот) користејќи LAN-кабел.

2. Изберете  на почетниот екран.

3. Изберете **Пренасочувач**.

4. Проверете дали се точни поставките за Конекција и IP адреса.

5. Допрете **Затвори**.

Поврзување со безжична LAN (Wi-Fi)

Скенерот може да го поврзете со безжична LAN (Wi-Fi) на неколку начини. Изберете начин на поврзување според околината и условите.

Ако ги знаете информациите за безжичниот рутер, како на пример SSID и лозинката, може рачно да ги одредите поставките.

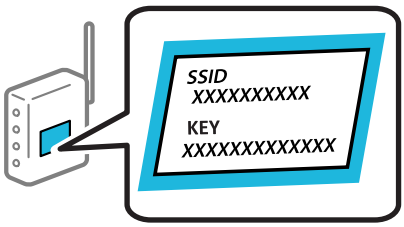
Ако безжичниот рутер поддржува WPS, може да ги одредите поставките со користење на поставувањето на копчето за притискање.

Откако ќе го поврзете скенерот со мрежата, поврзете го скенерот од уредот којшто сакате да го користите (компјутер, паметен уред, таблет итн.)

Одредување поставки за Wi-Fi со внесување SSID и лозинка

Може да поставите Wi-Fi мрежа со внесување на информациите потребни за поврзување со безжичен рутер од контролната табла на скенерот. За да извршите поставување со овој метод, ќе ви требаат SSID и лозинка за безжичен рутер.

Белешка:
Ако користите безжичен рутер со неговите стандардни поставки, SSID и лозинката се запишани на етикетата. Ако не ги знаете SSID и лозинката, контактирајте со лицето што го поставило безжичниот рутер или проверете ја документацијата приложена со безжичниот рутер.



1. Допрете  на почетниот екран.
2. Изберете **Пренасочувач**.
3. Допрете **Започни со поставување**.

   Ако мрежната врска е веќе поставена, се прикажуваат деталите за врската. Допрете **Промени во Wi-Fi конекција.** или **Промени поставки** за да ги промените поставките.
4. Изберете **Волшебник за поставување на Wi-Fi врска**.
5. Следете ги инструкциите на екранот за да изберете SSID, да ја внесете лозинката за безжичниот рутер и да го започнете поставувањето.

   Ако сакате да го проверите статусот на мрежната врска за скенерот откако ќе заврши поставувањето, погледнете го линкот со поврзани информации подолу.

   Белешка:
   - ❏ *Ако не ја знаете SSID, проверете дали е запишана на етикетата на безжичниот рутер. Ако го користите безжичниот рутер со неговите стандардни поставки, користете ја SSID запишана на етикетата. Ако не може да најдете информации, погледнете ја документацијата испорачана со безжичниот рутер.*
   - ❏ *Лозинката разликува големи и мали букви.*
   - ❏ *Ако не ја знаете лозинката, проверете дали е запишана на етикетата на безжичниот рутер. На етикетата, лозинката може да биде запишана како „Network Key", „Wireless Password" итн. Ако го користите безжичниот рутер со неговите стандардни поставки, внесете ја лозинката запишана на етикетата.*

Поврзани информации

➡ „Проверување на статусот на конекција на мрежа" на страница 28

Одредување поставки за Wi-Fi со поставување копче за притискање (WPS)

Може автоматски да поставите Wi-Fi-мрежа со притискање на копчето на безжичниот рутер. Ако следниве услови се исполнети, може да ја поставите на овој начин.

❏ Безжичниот рутер е компатибилен со WPS (Wi-Fi Protected Setup).

❏ Тековната Wi-Fi-врска е воспоставена со притискање копче на безжичниот рутер.

Белешка:
Ако не може да го најдете копчето или ако го вршите поставувањето со софтвер, погледнете ја документацијата испорачана со безжичниот рутер.

1. Допрете  на почетниот екран.
2. Изберете **Пренасочувач**.
3. Допрете **Започни со поставување**.

   Ако мрежната врска е веќе поставена, се прикажуваат деталите за врската. Допрете **Промени во Wi-Fi конекција.** или **Промени поставки** за да ги промените поставките.
4. Изберете **Поставка за копче за притискање (WPS)**.
5. Следете ги инструкциите на екранот.

   Ако сакате да го проверите статусот на мрежната врска за скенерот откако ќе заврши поставувањето, погледнете го линкот со поврзани информации подолу.

   Белешка:
   Ако поврзувањето не успева, рестартирајте го безжичниот рутер, поместете го поблизу до скенерот и обидете се повторно.

Поврзани информации

➡ „Проверување на статусот на конекција на мрежа“ на страница 28

Одредување поставки за Wi-Fi со поставување PIN-код (WPS)

Може автоматски да се поврзете со безжичен рутер користејќи PIN-код. Овој начин на поставување може да го користите ако безжичниот рутер поддржува WPS (Wi-Fi Protected Setup). Користете компјутер за да внесете PIN-код во безжичниот рутер.

1. Допрете  на почетниот екран.
2. Изберете **Пренасочувач**.
3. Допрете **Започни со поставување**.

   Ако мрежната врска е веќе поставена, се прикажуваат деталите за врската. Допрете **Промени во Wi-Fi конекција.** или **Промени поставки** за да ги промените поставките.
4. Изберете **Други** > **PIN шифра за пост. (WPS)**
5. Следете ги инструкциите на екранот.

   Ако сакате да го проверите статусот на мрежната врска за скенерот откако ќе заврши поставувањето, погледнете го линкот со поврзани информации подолу.

   Белешка:
   Погледнете ја документацијата испорачана со безжичниот рутер за детали за внесување PIN-код.

Поврзани информации

➡ „Проверување на статусот на конекција на мрежа“ на страница 28

Додавање или менување на компјутерот или уредите

Поврзување со скенер што веќе е поврзан со мрежата

Кога скенерот веќе е поврзан со мрежата, може да поврзете компјутер или паметен уред со скенерот преку мрежата.

Користење мрежен скенер од втор компјутер

Препорачуваме да ја користите програмата за инсталирање за да го поврзете скенерот со компјутер. Програмата за инсталирање може да ја стартувате на еден од следниве начини.

❏ Поставување од веб-локацијата

Одете на следнава веб-локација и внесете го името на производот. Одете во **Поставување** и започнете со поставување.

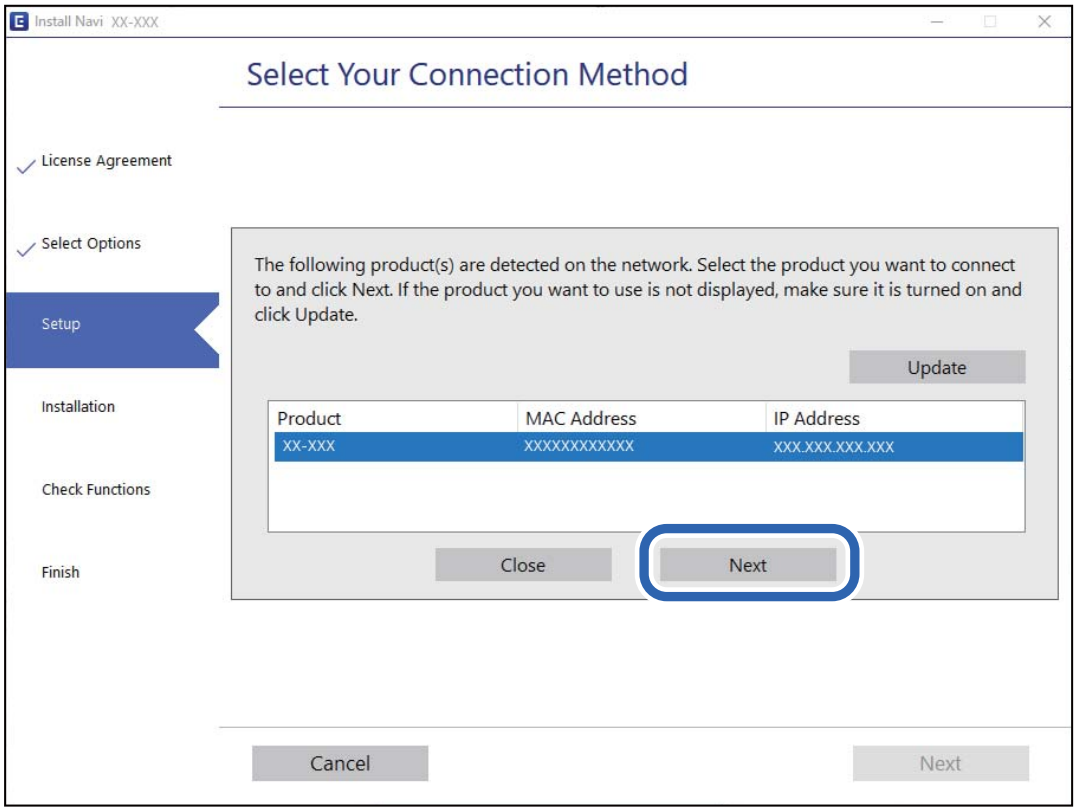
http://epson.sn

❏ Поставување со користење на дискот со софтвер (само за моделите коишто доаѓаат со диск со софтвер и за корисници со компјутери со Windows со погони за диск.)

Внесете го дискот со софтвер во компјутерот и следете ги инструкциите на екранот.

Изберете го скенерот

Следете ги инструкциите на екранот додека да се прикаже следниов екран, изберете го името на скенерот со којшто сакате да се поврзете, а потоа кликнете **Следно**.



Следете ги инструкциите на екранот.

Користење мрежен скенер од паметен уред

Може да поврзете паметен уред со скенерот на еден од следниве начини.

Поврзување преку безжичен рутер

Поврзете го паметниот уред со истата Wi-Fi мрежа (SSID) на којашто е поврзан скенерот.

За повеќе информации, погледнете го следново.

„Одредување поставки за поврзување со паметниот уред“ на страница 27

Поврзување преку Wi-Fi Direct

Поврзете го паметниот уред директно со скенерот, без безжичен рутер.

За повеќе информации, погледнете го следново.

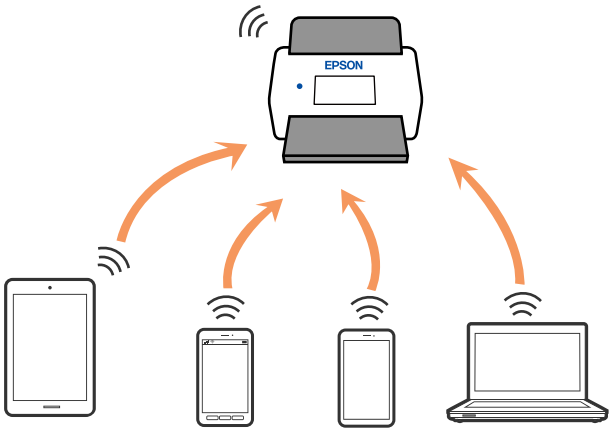
„Директно поврзување паметен уред и скенер (Wi-Fi Direct)“ на страница 24

Директно поврзување паметен уред и скенер (Wi-Fi Direct)

Wi-Fi Direct (едноставна AP) ви овозможува да поврзете паметен уред директно со скенерот без безжичен рутер и да скенирате од паметниот уред.

За Wi-Fi Direct

Користете го овој начин на поврзување кога не користите Wi-Fi во домашни услови или во канцеларија или кога сакате директно да ги поврзете скенерот и компјутерот или паметниот уред. Во овој режим, скенерот има улога на безжичен рутер и може да ги поврзете уредите со скенерот без да треба да користите стандарден безжичен рутер. Меѓутоа, уредите што се директно поврзани со скенерот, не може меѓусебно да комуницираат преку скенерот.



Скенерот може истовремено да биде поврзан преку Wi-Fi или етернет и Wi-Fi Direct (едноставна AP) врска. Меѓутоа, ако стартувате мрежна врска во Wi-Fi Direct (едноставна AP) врска кога скенерот е поврзан преку Wi-Fi, Wi-Fi е привремено исклучена.

Поврзување со паметен уред преку Wi-Fi Direct

Овој начин ви овозможува да го поврзувате скенерот директно со паметни уреди, без безжичен рутер.

1. Изберете  на почетниот екран.
2. Изберете **Wi-Fi Direct**.
3. Изберете **Започни со поставување**.
4. Стартувајте ја Epson Smart Panel на паметниот уред.
5. Следете ги инструкциите прикажани на Epson Smart Panel за да се поврзете со скенерот.
   Кога паметниот уред ќе се поврзе со скенерот, одете на следниот чекор.
6. На контролната табла на скенерот, изберете **Свршено**.

Прекинување Wi-Fi Direct (едноставна AP) врска

Има два начина за оневозможување Wi-Fi Direct (едноставна AP) врска; може да ги оневозможите сите врски користејќи ја контролната табла на скенерот или да ја оневозможите секоја врска од компјутерот или од паметниот уред.

Кога сакате да ги оневозможите сите врски, изберете  > **Wi-Fi Direct** > **Започни со поставување** > **Смени** > **Деактивирај Wi-Fi Direct**.

> ***Важно:***
> *Кога е оневозможена Wi-Fi Direct (едноставна AP) врска, се прекинува врската со сите компјутери и паметни уреди поврзани со скенерот во Wi-Fi Direct (едноставна AP) врска.*

Белешка:
Ако сакате да ја прекинете врската со одреден уред, прекинете ја од уредот наместо од скенерот. Wi-Fi Direct (едноставна AP) врска може да се прекине од уредот на еден од следниве начини.

- ❏ *Прекинете ја Wi-Fi врската со името на мрежата на скенерот (SSID).*
- ❏ *Поврзете се со друго име на мрежа (SSID).*

Менување на поставките за Wi-Fi Direct (едноставна AP) како на пр. SSID

Кога е овозможена врска Wi-Fi Direct (едноставна AP), може да ги менувате поставките од  > **Wi-Fi Direct** > **Започни со поставување** > **Смени**, каде што се прикажуваат следниве ставки од менито.

Промени име на мрежа

Сменете го името на мрежата (SSID) на Wi-Fi Direct (едноставна AP) што се користи за поврзување со скенерот, со име по ваш избор. Може да го поставите името на мрежата (SSID) во знаци ASCII што се прикажуваат на софтверската тастатура на контролната табла. Може да внесете до 22 знаци.

Кога го менувате името на мрежата (SSID), се прекинува врската со сите поврзани уреди. Користете го новото име на мрежата (SSID) ако сакате повторно да го поврзете уредот.

Промени лозинка

Сменете ја лозинката за Wi-Fi Direct (едноставна AP) со сопствена лозинка за поврзување со скенерот. Може да ја поставите лозинката во знаци ASCII што се прикажуваат на софтверската тастатура на контролната табла. Може да внесете од 8 до 22 знаци.

Кога ја менувате лозинката, се прекинува врската со сите поврзани уреди. Користете ја новата лозинка ако сакате повторно да го поврзете уредот.

Промени опсег на фреквенција

Менувајте го фреквентниот опсег на Wi-Fi Direct што се користи за поврзување со скенерот. Може да изберете 2,4 GHz или 5 GHz.

Кога го менувате фреквентниот опсег, се прекинува врската со сите поврзани уреди. Одново поврзете го уредот.

Имајте предвид дека кога менувате на 5 GHz, не може одново да се поврзувате од уреди што не го поддржуваат фреквентниот опсег 5 GHz.

Во зависност од регионот, оваа поставка може да не се прикажува.

Деактивирај Wi-Fi Direct

Оневозможете ги поставките за Wi-Fi Direct (едноставна AP) за скенерот. Кога ја оневозможувате врската Wi-Fi Direct (едноставна AP), се прекинува врската со сите уреди поврзани со скенерот.

Врати стандардни поставки

Вратете ги сите поставки за Wi-Fi Direct (едноставна AP) на нивните стандардни вредности.

Информациите за врската Wi-Fi Direct (едноставна AP) на паметниот уред зачувани во скенерот се бришат.

Белешка:
*Може да извршите поставување и од картичката **Network** > **Wi-Fi Direct** на Web Config за следниве поставки.*

- ❏ *Овозможување или оневозможување Wi-Fi Direct (едноставна AP)*
- ❏ *Менување на името на мрежата (SSID)*
- ❏ *Менување на лозинката*
- ❏ *Менување на фреквентниот опсег*

  Во зависност од регионот, оваа поставка може да не се прикажува.
- ❏ *Враќање на поставките за Wi-Fi Direct (едноставна AP)*

Ресетирање на мрежната врска

Во овој дел се објаснува како да ги одредите поставките за мрежната врска и да го промените начинот на поврзување кога го заменувате безжичниот рутер или компјутерот.

Кога го менувате безжичниот рутер

Кога го менувате безжичниот рутер, одредете ги поставките за врската меѓу компјутерот или паметниот уред и скенерот.

Овие поставки треба да ги одредите ако го смените интернет-операторот и сл.

Одредување поставки за поврзување со компјутерот

Препорачуваме да ја користите програмата за инсталирање за да го поврзете скенерот со компјутер. Програмата за инсталирање може да ја стартувате на еден од следниве начини.

- ❏ Поставување од веб-локацијата

  Одете на следнава веб-локација и внесете го името на производот. Одете во **Поставување** и започнете со поставување.

  http://epson.sn
- ❏ Поставување со користење на дискот со софтвер (само за моделите коишто доаѓаат со диск со софтвер и за корисници со компјутери со Windows со погони за диск.)

  Внесете го дискот со софтвер во компјутерот и следете ги инструкциите на екранот.

Избирање начини на поврзување

Следете ги инструкциите на екранот. На екранот **Изберете ја вашата операција**, изберете **Повторно постави поврзување на Печатач (за нов мрежен рутер или за менување на USB во мрежа, итн.)**, а потоа кликнете **Следно**.

Следете ги инструкциите на екранот за да го завршите поставувањето.

Ако не може да се поврзете, погледнете го следново за да се обидете да го решите проблемот.

„Не е можно поврзување на мрежа“ на страница 33

Одредување поставки за поврзување со паметниот уред

Може да го користите скенерот од паметен уред кога ќе го поврзете скенерот со истата Wi-Fi мрежа (SSID) со којашто е поврзан и паметниот уред. За да го користите скенерот од паметен уред, посетете ја следнава веб-локација, а потоа внесете го името на производот. Одете на **Поставување**, а потоа започнете со поставување.

http://epson.sn

Пристапете до веб-локацијата од паметниот уред што сакате да го поврзете со скенерот.

Кога го менувате компјутерот

Кога го менувате компјутерот, одредете ги поставките за врската меѓу компјутерот и скенерот.

Одредување поставки за поврзување со компјутерот

Препорачуваме да ја користите програмата за инсталирање за да го поврзете скенерот со компјутер. Програмата за инсталирање може да ја стартувате на следниов начин.

❏ Поставување од веб-локацијата

Одете на следнава веб-локација и внесете го името на производот. Одете на **Поставување**, а потоа започнете со поставување.

http://epson.sn

❏ Поставување со користење на дискот со софтвер (само за моделите коишто доаѓаат со диск со софтвер и за корисници со компјутери со Windows со погони за диск.)

Внесете го дискот со софтвер во компјутерот и следете ги инструкциите на екранот.

Следете ги инструкциите на екранот.

Менување на начинот на поврзување со компјутерот

Во овој дел се објаснува како да го промените начинот на поврзување кога компјутерот и скенерот се поврзани.

Менување на мрежната врска од етернет во Wi-Fi

Сменете ја етернет-врската во Wi-Fi врска од контролната табла на скенерот. Начинот на менување на врската е всушност ист како и во поставките за Wi-Fi врската.

Поврзани информации

➡ „Поврзување со безжична LAN (Wi-Fi)“ на страница 19

Менување на мрежната врска од Wi-Fi во етернет

Следете ги чекорите подолу за да ја промените врската од Wi-Fi врска во етернет-врска.

1. Изберете **Поставки** на почетниот екран.
2. Изберете **Поставки за мрежа** > **Поставување на жична LAN**.
3. Следете ги инструкциите на екранот.

Менување од USB-врска во мрежна врска

Со користење датотека за инсталирање и повторно поставување со различен начин на поврзување.

❏ Поставување од веб-локацијата

Одете на следнава веб-локација и внесете го името на производот. Одете во **Поставување** и започнете со поставување.

http://epson.sn

❏ Поставување со користење на дискот со софтвер (само за моделите коишто доаѓаат со диск со софтвер и за корисници со компјутери со Windows со погони за диск.)

Внесете го дискот со софтвер во компјутерот и следете ги инструкциите на екранот.

Изберете го начинот на поврзување

Следете ги инструкциите на екранот. На екранот **Изберете ја вашата операција**, изберете **Повторно постави поврзување на Печатач (за нов мрежен рутер или за менување на USB во мрежа, итн.)**, а потоа кликнете **Следно**.

Изберете ја мрежната врска што сакате да ја користите, **Поврзете се преку безжична мрежа (Wi-Fi)** или **Поврзи се преку жичан LAN (Ethernet)**, а потоа кликнете **Следно**.

Следете ги инструкциите на екранот за да го завршите поставувањето.

Проверување на статусот на конекција на мрежа

Може да го проверите статусот на мрежната конекција на следниов начин.

Проверка на статусот на мрежната врска од контролната табла

Статусот на мрежната врска може да го проверите со користење на иконата за мрежата или информациите за мрежата на контролната табла на скенерот.

Проверка на статусот на мрежната врска со користење на иконата за мрежата

Статусот на мрежната врска и јачината на радиобранот може да ги проверите со користење на иконата за мрежата на почетниот екран на скенерот.

	Го прикажува статусот на мрежната врска. Изберете ја иконата за да ги проверите и менувате тековните поставки. Ова е кратенката за следново мени. **Поставки** > **Поставки за мрежа** > **Wi-Fi поставување**	
		Скенерот не е поврзан со безжична (Wi-Fi) мрежа.
		Скенерот пребарува SSID, не е поставена IP-адреса или има проблем со безжична (Wi-Fi) мрежа.
		Скенерот е поврзан со безжична (Wi-Fi) мрежа. Бројот на линии ја покажува јачината на сигналот на врската. Колку повеќе линии има, толку е посилна врската.
		Скенерот не е поврзан со безжична (Wi-Fi) мрежа во режим Wi-Fi Direct (едноставна AP).
		Скенерот е поврзан со безжична (Wi-Fi) мрежа во режим Wi-Fi Direct (едноставна AP).
		Скенерот не е поврзан на жична (етернет) мрежа или не е поставен.
		Скенерот е поврзан на жична (етернет) мрежа.

Прикажување детални информации за мрежата на контролната табла

Кога скенерот е поврзан на мрежата, може да ги прегледате и останатите информации поврзани со мрежата со избирање на менијата за мрежа коишто сакате да ги проверите.

1. Изберете **Поставки** на почетниот екран.
2. Изберете **Поставки за мрежа** > **Статус на мрежа**.
3. За да ги проверите информациите, изберете ги менијата коишто сакате да ги проверите.
   - ❏ Статус на кабелска LAN/ Wi-Fi мрежа

     Ги прикажува информациите за мрежата (име на уред, врска, јачина на сигнал итн.) за етернет или Wi-Fi врски.

❏ Статус на Wi-Fi Direct

Прикажува дали Wi-Fi Direct е овозможено или оневозможено и SSID, лозинката итн. за Wi-Fi Direct врски.

❏ Статус на сервер за е-пошта

Прикажува информации за мрежа за сервер на е-пошта.

Мрежни спецификации

Спецификации за Wi-Fi

Следнава табела содржи спецификации за Wi-Fi.

Земји или региони, освен долунаведените	Табела A
Австралија Нов Зеланд Тајван Јужна Кореја	Табела B

Табела A

Стандарди	IEEE 802.11b/g/n*1
Фреквентен опсег	2,4 GHz
Максимална радиофреквенција	2 400–2 483,5 MHz: 20 dBm (EIRP)
Канали	1/2/3/4/5/6/7/8/9/10/11/12/13
Режими на поврзување	Инфраструктурен, Wi-Fi Direct (едноставна AP)*2*3
Безбедносни протоколи*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Достапно само за HT20.

*2 Не е поддржано за IEEE 802.11b.

*3 Инфраструктурниот режим и режимот Wi-Fi Direct или етернет-врската може да се користат истовремено.

*4 Wi-Fi Direct поддржува само WPA2-PSK (AES).

*5 Во согласност со стандардите WPA2 со поддршка за WPA/WPA2 Personal.

Табела B

Стандарди	IEEE 802.11a/b/g/n*1/ac
Фреквентни опсези	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz

Канали	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)
Режими на поврзување	Инфраструктурен, Wi-Fi Direct (едноставна AP)*4, *5		
Безбедносни протоколи*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Достапно само за HT20.

*2 Не е достапно во Тајван.

*3 Достапноста на овие канали и користењето на производот на отворено преку овие канали варира според локацијата. За повеќе информации, погледнете http://support.epson.net/wifi5ghz/

*4 Не е поддржано за IEEE 802.11b.

*5 Инфраструктурниот режим и режимот Wi-Fi Direct или етернет-врската може да се користат истовремено.

*6 Wi-Fi Direct поддржува само WPA2-PSK (AES).

*7 Во согласност со стандардите WPA2 со поддршка за WPA/WPA2 Personal.

Спецификации за етернет

Стандарди	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energy Efficient Ethernet)*2
Режим на комуникација	Автоматски, 10 Mbps целосен дуплекс, 10 Mbps половина дуплекс, 100 Mbps целосен дуплекс, 100 Mbps половина дуплекс
Приклучок	RJ-45

*1 Користете кабел од категорија 5e или повисок STP (заштитен извиткан пар) за да спречите ризик од радио пречки.

*2 Поврзаниот уред треба да е усогласен со стандардите IEEE802.3az.

Мрежни функции и IPv4/IPv6

Функции	**Поддржано**
Epson Scan 2	IPv4, IPv6

Функции	Поддржано
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

Безбедносен протокол

IEEE802.1X*	
IPsec/IP филтрирање	
SSL/TLS	HTTPS сервер/клиент
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Треба да користите уред за поврзување што е во согласност со IEEE802.1X.

Употреба на порта за скенерот

Скенерот ја употребува следнава порта. По потреба, мрежниот администратор треба да дозволи овие порти да станат достапни.

Кога скенерот е испраќач (клиент)

Употреба	Дестинација (сервер)	Протокол	Број на порта
Испраќање датотеки (кога скенирањето во мрежна папка се користи од скенерот)	FTP/FTPS-сервер	FTP/FTPS (TCP)	20
			21
	Сервер за датотеки	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	WebDAV-сервер	HTTP-протокол (TCP)	80
		HTTPS-протокол (TCP)	443
Испраќање е-пораки (кога скенирањето во е-пошта се користи од скенерот)	SMTP-сервер	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP пред SMTP-врска (кога скенирањето во е-пошта се користи од скенерот)	POP-сервер	POP3 (TCP)	110

Употреба	Дестинација (сервер)	Протокол	Број на порта
Кога се користи Epson Connect	Сервер Epson Connect	HTTPS	443
		XMPP	5222
Прибирање податоци за корисници (се користат контактите од скенерот)	LDAP-сервер	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Автентикација на корисници при прибирање податоци за корисници (кога се користат контактите од скенерот) Автентикација на корисници кога се користи скенирање во мрежна папка (SMB) од скенерот	KDC-сервер	Kerberos	88
WSD-контрола	Клиентски компјутер	WSD (TCP)	5357
Пребарајте го компјутерот при push-скенирање од апликација	Клиентски компјутер	Откривање мрежно push-скенирање	2968

Кога клиентскиот компјутер е испраќач (клиент)

Употреба	Дестинација (сервер)	Протокол	Број на порта
Откријте го скенерот од апликација како што е EpsonNet Config и двигател за скенер.	Скенер	ENPC (UDP)	3289
Приберете и поставете ги MIB-информациите од апликација како што е EpsonNet Config и двигател за скенер.	Скенер	SNMP (UDP)	161
Пребарување WSD-скенер	Скенер	WS-откривање (UDP)	3702
Проследување на податоците од скенирањето од апликација	Скенер	Мрежно скенирање (TCP)	1865
Прибирање информации за задачата при push-скенирање од апликација	Скенер	Мрежно push-скенирање	2968
Web Config	Скенер	HTTP (TCP)	80
		HTTPS (TCP)	443

Решавање проблеми

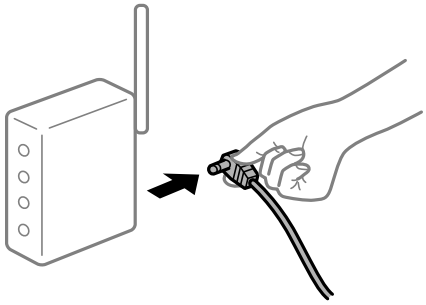
Не е можно поврзување на мрежа

Проблемот може да се јавува поради некоја од следниве причини.

Нешто не е во ред со мрежните уреди за Wi-Fi врска.

Решенија

Исклучете ги уредите коишто сакате да ги поврзете на мрежата. Почекајте околу 10 секунди, а потоа вклучете ги уредите во следниов редослед: безжичен рутер, компјутер или паметен уред и потоа скенерот. Поместете ги скенерот и компјутерот или паметниот уред поблизу до безжичниот рутер за да ја олесните комуникацијата со радиобранови, а потоа обидете се повторно да ги одредите мрежните поставки.



Уредите не можат да примаат сигнали од безжичниот рутер бидејќи се премногу раздалечени.

Решенија

Откако ќе ги доближите компјутерот или паметниот уред и скенерот до безжичниот рутер, исклучете го безжичниот рутер, па повторно вклучете го.

Кога го менувате безжичниот рутер, поставките не се соодветни за новиот рутер.

Решенија

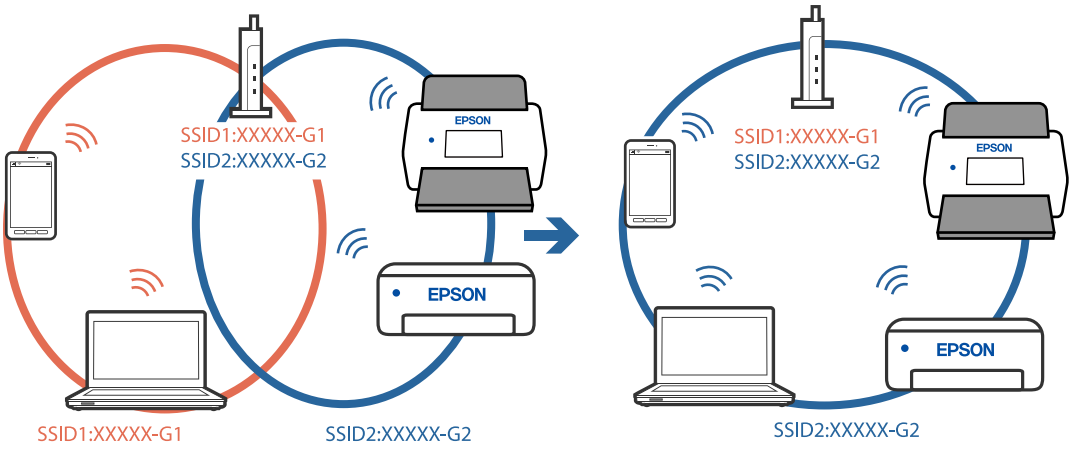
Одредете ги поставките за врската повторно, за да бидат соодветни за новиот безжичен рутер.

SSID поврзани од компјутерот или од паметниот уред и компјутерот се разликуваат.

Решенија

Кога истовремено користите повеќе безжични рутери или кога безжичниот рутер има повеќе SSID и уредите се поврзани со различни SSID, не може да се поврзете со безжичниот рутер.

Поврзете ги компјутерот или паметниот уред на истата SSID како и скенерот.



На безжичниот рутер е достапна функција за одделување за приватност.

Решенија

Повеќето безжични рутери имаат функција за одделување за приватност којашто ја блокира комуникацијата меѓу поврзаните уреди. Ако не може да се воспостави комуникација меѓу скенерот и компјутерот или паметниот уред дури и кога се поврзани на истата мрежа, оневозможете ја функцијата за одделување за приватност на безжичниот рутер. За детали, погледнете во прирачникот испорачан со безжичниот рутер.

IP-адресата не е правилно доделена.

Решенија

Ако IP-адресата доделена на скенерот е 169.254.XXX.XXX, а подмрежната маска е 255.255.0.0, IP-адресата може да не е правилно доделена.

Изберете **Поставки** > **Поставки за мрежа** > **Напредно** > **TCP/IP** на контролната табла на скенерот, а потоа проверете ги IP-адресата и подмрежната маска доделени на скенерот.

Рестартирајте го безжичниот рутер или ресетирајте ги мрежните поставки за скенерот.

Има проблем со мрежните поставки на компјутерот.

Решенија

Обидете се да ја отворите која било веб-локација од вашиот компјутер за да се уверите дека мрежните поставки на компјутерот се точни. Ако не може да отворите веб-локација, има проблем со компјутерот.

Проверете ја мрежната врска на компјутерот. За повеќе детали, погледнете ја документацијата приложена со компјутерот.

Скенерот е поврзан преку етернет користејќи уреди што поддржуваат IEEE 802.3az (енергетски ефикасен етернет).

Решенија

Кога го поврзувате скенерот преку етернет користејќи уреди што поддржуваат IEEE 802.3az (енергетски ефикасен етернет), во зависност од хабот или рутерот што го користите, може да се јават следниве проблеми.

- ❏ Врската со скенерот станува нестабилна, односно постојано се воспоставува и прекинува.
- ❏ Не е можно поврзување со скенерот.
- ❏ Бавна брзина на комуникацијата.

Следете ги чекорите подолу за да оневозможите IEEE 802.3az за скенерот, па да се поврзете.

1. Извадете го кабелот за етернет поврзан со компјутерот и скенерот.
2. Кога IEEE 802.3az е овозможен за компјутерот, оневозможете го.

   За повеќе детали, погледнете ја документацијата приложена со компјутерот.
3. Поврзете ги компјутерот и скенерот директно со кабел за етернет.
4. На скенерот, проверете ги мрежните поставки.

   Изберете **Поставки** > **Поставки за мрежа** > **Статус на мрежа** > **Статус на кабелска LAN/ Wi-Fi мрежа**.
5. Проверете ја IP-адресата на скенерот.
6. На компјутерот, одете на Web Config.

   Стартувајте веб-прелистувач, а потоа внесете ја IP-адресата на скенерот.

   „Извршување Web Config на веб-прелистувач“ на страница 38
7. Изберете ја картичката **Network** > **Wired LAN**.
8. Изберете **OFF** за **IEEE 802.3az**.
9. Кликнете **Next**.
10. Кликнете **OK**.
11. Извадете го кабелот за етернет поврзан со компјутерот и скенерот.
12. Ако сте оневозможиле IEEE 802.3az за компјутерот во чекор 2, овозможете го.
13. Поврзете го кабелот за етернет (што го извадивте во чекор 1) со компјутерот и скенерот.

Ако проблемот и понатаму се јавува, можно е да го предизвикуваат други уреди, а не скенерот.

Скенерот е исклучен.

Решенија

Погрижете се скенерот да биде вклучен.

Исто така, почекајте светлото за статус да престане да трепка, укажувајќи дека скенерот е подготвен за скенирање.

Софтвер за поставување на скенерот

Web Config

Web Config е апликација што се извршува во веб-прелистувачи како што се Internet Explorer и Safari на компјутер. Може да го проверите статусот на скенерот или да ги менувате поставките за скенерот и за мрежната услуга. Бидејќи до скенерите се пристапува и со нив се ракува директно преку мрежата, апликацијата е погодна за поединечно конфигурирање на секој скенер. За да ја користите Web Config, поврзете го компјутерот на истата мрежа како и скенерот.

Поддржани се следниве прелистувачи.

Microsoft Edge, Windows Internet Explorer 8 или понова верзија, Firefox*, Chrome* и Safari*

* Користете ја најновата верзија.

Извршување Web Config на веб-прелистувач

1. Проверете ја IP-адресата на скенерот.

   Изберете **Поставки** > **Поставки за мрежа** > **Статус на мрежа** на контролната табла на скенерот. Потоа, изберете го статусот на активниот начин на поврзување (**Статус на кабелска LAN/ Wi-Fi мрежа** или **Статус на Wi-Fi Direct**) за да ја потврдите IP-адресата на скенерот.

2. Стартувајте веб-прелистувач од компјутер или паметен уред, а потоа внесете ја IP-адресата на скенерот.

   Формат:

   IPv4: http://IP-адресата на скенерот/

   IPv6: http://[IP-адресата на скенерот]/

   Примери:

   IPv4: http://192.168.100.201/

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

   Белешка:
   Бидејќи скенерот користи само-потпишан сертификат при пристап до HTTPS, на прелистувачот се прикажува предупредување кога ќе ја стартувате Web Config; ова не укажува на проблем и може безбедно да се игнорира.

3. Најавете се како администратор за да ги менувате поставките за скенерот.

   Кликнете **Administrator Login** во горниот десен агол на екранот. Внесете **User Name** и **Current password**, а потоа кликнете **OK**.

   Белешка:
   - *Подолу се наведени почетните вредности за администраторските информации за Web Config.*

     ·Корисничко име: нема (празно)

     ·Лозинка: серискиот број на скенерот

     За да го најдете серискиот број, проверете ја етикетата залепена на задниот дел од скенерот.
   - *Ако **Administrator Logout** е прикажано во горниот десен агол на екранот, веќе сте се најавиле како администратор.*

Извршување Web Config на Windows

Кога поврзувате компјутер со скенерот користејќи WSD, следете ги чекорите подолу за да ја стартувате Web Config.

1. Отворете го списокот со скенери на компјутерот.
   - ❏ Windows 10

     Кликнете го копчето Старт, а потоа изберете **Систем на Windows** > **Контролна табла** > **Преглед на уреди и печатачи** во **Хардвер и звук**.
   - ❏ Windows 8.1/Windows 8

     Изберете **Работна површина** > **Поставки** > **Контролна табла** > **Преглед на уреди и печатачи** во **Хардвер и звук** (или **Хардвер**).
   - ❏ Windows 7

     Кликнете го копчето Старт, а потоа изберете **Контролна табла** > **Преглед на уреди и печатачи** во **Хардвер и звук**.
2. Кликнете со десното копче на вашиот скенер и изберете **Својства**.
3. Изберете ја картичката **Веб-услуга**, а потоа кликнете на URL-адресата.

   Бидејќи скенерот користи само-потпишан сертификат при пристап до HTTPS, на прелистувачот се прикажува предупредување кога ќе ја стартувате Web Config; ова не укажува на проблем и може безбедно да се игнорира.

   Белешка:
   - *Подолу се наведени почетните вредности за администраторските информации за Web Config.*

     ·Корисничко име: нема (празно)

     ·Лозинка: серискиот број на скенерот

     За да го најдете серискиот број, проверете ја етикетата залепена на задниот дел од скенерот.
   - *Ако **Administrator Logout** е прикажано во горниот десен агол на екранот, веќе сте се најавиле како администратор.*

Epson Device Admin

Epson Device Admin е мултифункционална апликација што ви овозможува да управувате со уреди на мрежа.

Може да користите шаблони за конфигурација за да применувате унифицирани поставки на повеќе скенери на одредена мрежа, а тоа е погодно за инсталирање и управување со повеќе скенери.

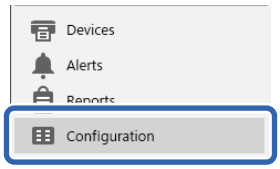
Epson Device Admin може да ја преземете од веб-локацијата за поддршка на Epson. За детали околу тоа како да ја користите оваа апликација, погледнете во документацијата или помошта за Epson Device Admin.

Шаблон за конфигурација

Создавање шаблон за конфигурација

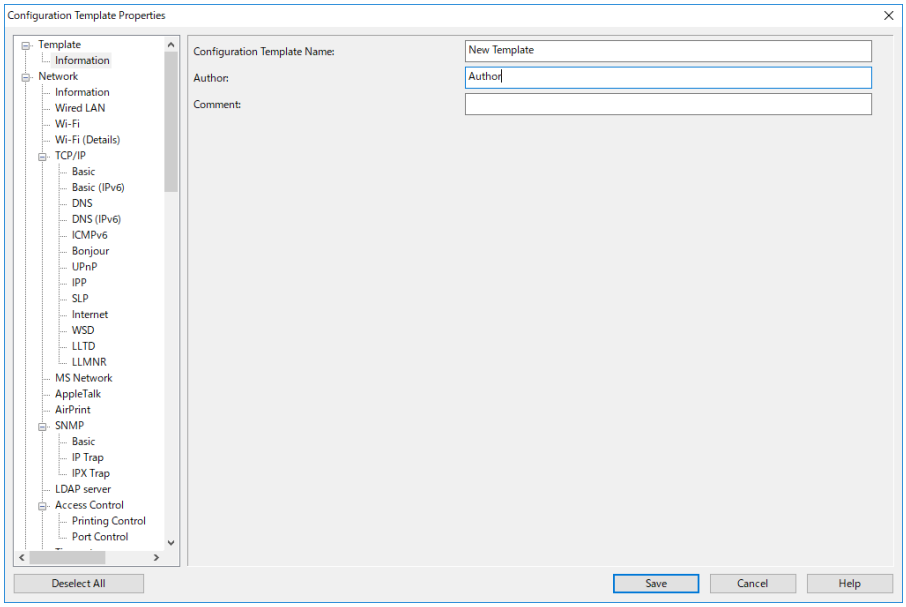
Создајте нов шаблон за конфигурација.

1. Стартувајте ја Epson Device Admin.
2. Изберете **Configuration** во менито со задачи на страничната лента.



3. Изберете **New** од менито со ленти.

4. Поставете ги сите ставки.



Ставка	Објаснување
Configuration Template Name	Име на шаблонот за конфигурација. Внесете до 1024 знаци во Unicode (UTF-8).
Author	Информации за создавачот на шаблонот. Внесете до 1024 знаци во Unicode (UTF-8).

Ставка	Објаснување
Comment	Внесете произволни информации. Внесете до 1024 знаци во Unicode (UTF-8).

5. Во левиот дел, изберете ги ставките што сакате да ги поставите.

   Белешка:
   *Во левиот дел, кликајте на ставките од менито за да го смените екранот. Поставената вредност се задржува ако го смените екранот, но не и ако го откажете екранот. Кога ќе го завршите одредувањето на поставките, кликнете **Save**.*

Примена на шаблонот за конфигурација

Применете го зачуваниот шаблон за конфигурација на скенерот. Се применуваат избраните ставки од шаблонот. Ако целниот скенер ја нема соодветната функција, таа нема да се примени.

Белешка:
Кога е поставена администраторска лозинка на скенерот, конфигурирајте ја лозинката однапред.

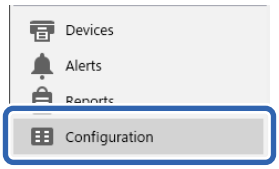
*1. Од менито со ленти во екранот „Список со уреди", изберете **Options** > **Password manager**.*

*2. Изберете **Enable automatic password management**, а потоа кликнете **Password manager**.*

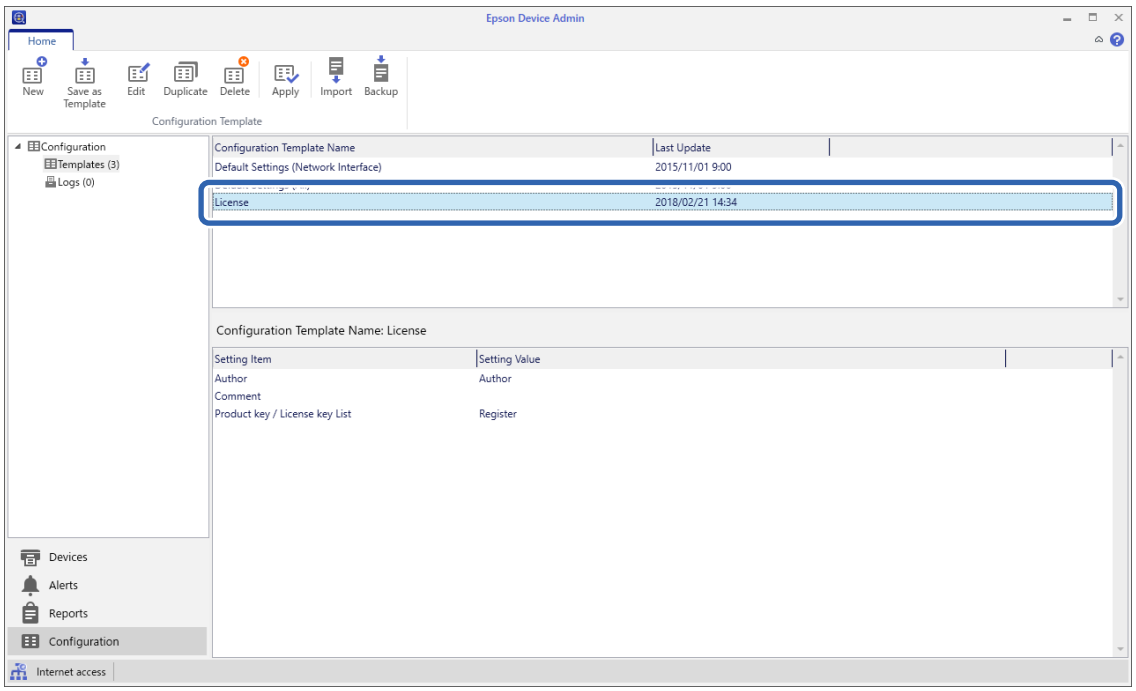
*3. Изберете го соодветниот скенер, а потоа кликнете **Edit**.*

*4. Поставете ја лозинката, а потоа кликнете **OK**.*

1. Изберете **Configuration** во менито со задачи на страничната лента.



2. Изберете го шаблонот за конфигурација што сакате да го примените од **Configuration Template Name**.



3. Кликнете **Apply** на менито со ленти.

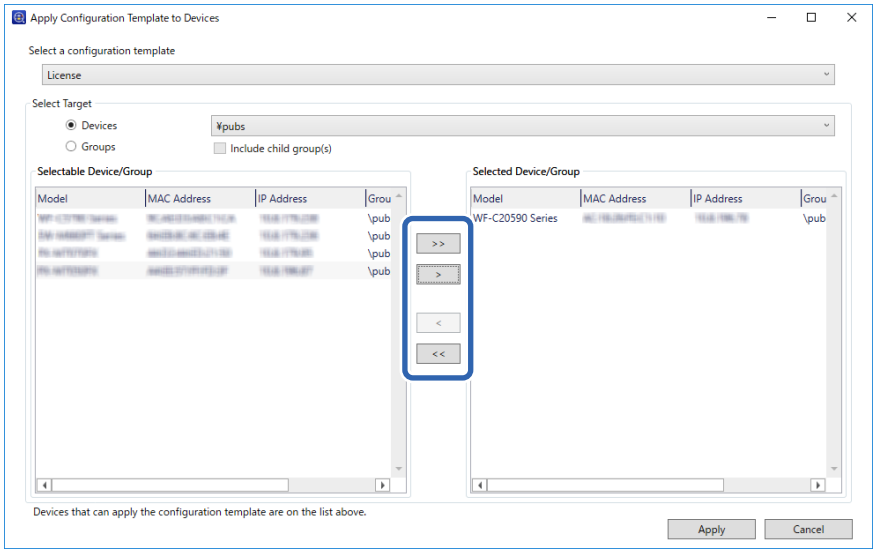
   Ќе се прикаже екранот за избирање уред.

4. Изберете го шаблонот за конфигурација што сакате да го примените.

Белешка:

- ❏ *Ако изберете **Devices** и групи што содржат уреди од паѓачкото мени, ќе се прикаже секој уред.*
- ❏ *Ако изберете **Groups**, ќе се прикажат групите. Изберете **Include child group(s)** за автоматско избирање детски групи во рамки на избраната група.*

5. Преместете ги скенерот или групите на кои сакате да го примените шаблонот во **Selected Device/Group**.



6. Кликнете **Apply**.

   Се прикажува екран за потврда за шаблонот за конфигурација што треба да се примени.

7. Кликнете **OK** за да го примените шаблонот за конфигурација.

8. Кога ќе се прикаже порака која ве информира дека постапката е завршена, кликнете **OK**.

9. Кликнете **Details** и проверете ги информациите.

   Кога на ставките што сте ги примениле се прикажува , тоа значи дека примената е успешно завршена.

10. Кликнете **Close**.

Задолжителни поставки за скенирање

Конфигурирање сервер за е-пошта

Поставете го серверот за е-пошта од Web Config.

Кога скенерот може да испраќа е-пошта со поставување на серверот за е-пошта, можно е следново.

❏ Испраќање на резултатите од скенирањето преку е-пошта

❏ Прием на известувањето од скенерот преку е-пошта

Проверете го следново пред да извршите поставување.

❏ Проверете дали скенерот е поврзан со мрежата што може да пристапува до серверот за е-пошта.

❏ Проверете ги информациите за поставки за е-пошта на компјутерот што го користи истиот сервер за е-пошта како и скенерот.

Белешка:

❏ *Кога го користите серверот за е-пошта на интернет, потврдете ги информациите за поставки од давателот на услугата или од веб-локацијата.*

❏ *Серверот за е-пошта може да го поставите и од контролната табла. Пристапете според инструкциите наведени подолу.*

Поставки > ***Поставки за мрежа*** > ***Напредно*** > ***Сервер за е-пошта*** > ***Поставки за сервер***

1. Одете на Web Config и изберете ја картичката **Network** > **Email Server** > **Basic**.
2. Внесете вредност за секоја ставка.
3. Изберете **OK**.

   Се прикажуваат поставките што ги избравте.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Ставки во поставка на сервер за е-пошта

Ставки	Поставки и објаснувања	
Authentication Method	Одредете го начинот на автентикација кога скенерот пристапува до серверот за е-пошта.	
	Off	Автентикацијата е оневозможена при комуникација со серверот за е-пошта.
	SMTP AUTH	Потребно е серверот за е-пошта да поддржува SMTP-автентикација.
	POP before SMTP	Конфигурирајте го POP3-серверот кога ќе го изберете овој начин.
Authenticated Account	Ако изберете **SMTP AUTH** или **POP before SMTP** како **Authentication Method**, внесете име на автентицирана сметка што содржи од 0 до 255 знаци во ASCII (0x20–0x7E).	

Ставки	Поставки и објаснувања	
Authenticated Password	Ако изберете **SMTP AUTH** или **POP before SMTP** како **Authentication Method**, внесете ја автентицираната лозинка што содржи од 0 до 20 знаци во ASCII (0x20–0x7E).	
Sender's Email Address	Внесете ја адресата на е-пошта на испраќачот. Внесете од 0 до 255 знаци во ASCII (0x20–0x7E) освен : ( ) < > [ ] ; ¥. Точката „.“ не може да биде првиот знак.	
SMTP Server Address	Внесете од 0 до 255 знаци со користење на A–Z a–z 0–9 . -. Може да користите IPv4 или FQDN формат.	
SMTP Server Port Number	Внесете број од 1 до 65535.	
Secure Connection	Одредете го начинот на безбедно поврзување за серверот за е-пошта.	
	None	Ако изберете **POP before SMTP** во **Authentication Method**, начинот на поврзување е поставен на **None**.
	SSL/TLS	Ова е достапно кога **Authentication Method** е поставен на **Off** или **SMTP AUTH**.
	STARTTLS	Ова е достапно кога **Authentication Method** е поставен на **Off** или **SMTP AUTH**.
Certificate Validation	Сертификатот е проверен кога ова е активирано. Препорачуваме ова да биде поставено на **Enable**.	
POP3 Server Address	Ако изберете **POP before SMTP** како **Authentication Method**, внесете ја адресата на POP3 серверот од 0 до 255 знаци со користење на A–Z a–z 0–9 . -. Може да користите IPv4 или FQDN формат.	
POP3 Server Port Number	Ако изберете **POP before SMTP** како **Authentication Method**, внесете број од 1 до 65535.	

Проверка на врската со серверот за е-пошта

Може да извршите проверка на врската со серверот за е-пошта.

1. Одете на Web Config и изберете ја картичката **Network** > **Email Server** > **Connection Test**.
2. Изберете **Start**.

   Започнува тестирањето на врската со серверот за е-пошта. По тестирањето, се прикажува извештај од тестирањето.

   Белешка:
   Врската со серверот за е-пошта може да ја проверите и од контролната табла. Пристапете според инструкциите наведени подолу.

   Поставки** > **Поставки за мрежа** > **Напредно** > **Сервер за е-пошта** > **Проверка на поврзување

Референци за тестирање на врската со серверот за е-пошта

Пораки	Причина
Connection test was successful.	Оваа порака се прикажува кога поврзувањето со серверот е успешно.
SMTP server communication error. Check the following. - Network Settings	Оваа порака се прикажува кога ❏ Скенерот не е поврзан на мрежа ❏ SMTP-серверот е исклучен ❏ Мрежната врска се прекинува при комуницирање ❏ Има прием на нецелосни податоци
POP3 server communication error. Check the following. - Network Settings	Оваа порака се прикажува кога ❏ Скенерот не е поврзан на мрежа ❏ POP3-серверот е исклучен ❏ Мрежната врска се прекинува при комуницирање ❏ Има прием на нецелосни податоци
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Оваа порака се прикажува кога ❏ Поврзувањето со DNS-сервер е неуспешно ❏ Разрешувањето на имиња за SMTP-сервер е неуспешно
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Оваа порака се прикажува кога ❏ Поврзувањето со DNS-сервер е неуспешно ❏ Разрешувањето на имиња за POP3-сервер е неуспешно
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Оваа порака се прикажува кога автентикацијата на SMTP-серверот е неуспешна.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Оваа порака се прикажува кога автентикацијата на POP3-серверот е неуспешна.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Оваа порака се прикажува кога се обидувате да комуницирате со несоодветни протоколи.
Connection to SMTP server failed. Change Secure Connection to None.	Оваа порака се прикажува кога не се совпаѓа SMTP на серверот и клиентот или кога серверот не поддржува безбедна врска SMTP (SSL-врска).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Оваа порака се прикажува кога настанува SMTP несовпаѓање помеѓу серверот и клиентот или кога серверот бара да користи SSL/TLS конекција за SMTP безбедна конекција.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Оваа порака се прикажува кога не се совпаѓа SMTP на серверот и клиентот или кога серверот бара да користи STARTTLS-врска за безбедна врска SMTP.

Пораки	Причина
The connection is untrusted. Check the following. - Date and Time	Оваа порака се прикажува кога поставката на датумот и времето на скенерот се неточни или кога сертификатот е застарен.
The connection is untrusted. Check the following. - CA Certificate	Оваа порака се прикажува кога скенерот нема коренов сертификат којшто одговара на серверот или CA Certificate не е увезен.
The connection is not secured.	Пораката се прикажува кога добиениот сертификат е оштетен.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Оваа порака се прикажува кога настанува несовпаѓање при методот на автентикација помеѓу серверот и клиентот. Серверот поддржува SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Оваа порака се прикажува кога настанува несовпаѓање при методот на автентикација помеѓу серверот и клиентот. Серверот не поддржува SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	Оваа порака се прикажува кога адресата на е-пошта на одредениот испраќач е погрешна.
Cannot access the product until processing is complete.	Пораката се прикажува кога скенерот е зафатен.

Поставување споделена мрежна папка

Поставете споделена мрежна папка за зачувување на скенираната слика.

Кога зачувувате датотека во папката, скенерот се најавува како корисник на компјутерот на кој била создадена папката.

Создавање на споделената папка

Поврзани информации

➡ „Пред создавање на споделената папка“ на страница 48
➡ „Проверка на мрежниот профил“ на страница 49
➡ „Локација каде што се создава споделената папка и пример за безбедноста“ на страница 49
➡ „Додавање група или корисник што дозволува пристап“ на страница 63

Пред создавање на споделената папка

Пред да ја создадете споделената папка, проверете го следново.

❏ Скенерот е поврзан на мрежата од каде што може да пристапи до компјутерот на кој ќе се создаде споделената папка.

❏ Во името на компјутерот на којшто ќе се создаде споделената папка нема знак составен од повеќе бајти.

Важно:

Кога во името на компјутерот има знак составен од повеќе бајти, зачувувањето на споделената папка можеби нема да успее.

Во тој случај, сменете го името на компјутерот или зачувајте на друг компјутер што не содржи знак со повеќе бајти во името.

Кога го менувате името на компјутерот, претходно консултирајте се со администраторот бидејќи тоа може да влијае врз одредени поставки, на пр. управување со компјутерот, пристап до ресурси итн.

Проверка на мрежниот профил

Проверете дали е достапно споделување папки на компјутерот каде што ќе се создаде споделената папка.

1. Најавете се на компјутерот каде што ќе се создаде споделената папка од страна на администраторската корисничка сметка.
2. Изберете **Контролна табла** > **Мрежа и интернет** > **Центар за мрежа и споделување**.
3. Кликнете **Променете ги напредните поставки за споделување**, а потоа кликнете за профилот со **(тековниот профил)** во прикажаните мрежни профили.
4. Проверете дали **Вклучете го споделувањето датотеки и печатачи** е избрано во **Споделување датотеки и печатачи**.

   Ако веќе е избрано, кликнете **Откажи** и затворете го прозорецот.

   Кога ќе ги промените поставките, кликнете **Зачувај ги промените** и затворете го прозорецот.

Локација каде што се создава споделената папка и пример за безбедноста

Во зависност од локацијата на создавање на споделената папка, безбедноста и погодноста варираат.

За да ракувате со споделената папка преку скенерите или другите компјутери, потребни се следниве дозволи за читање и менување на папката.

❏ Картичка **Споделување** > **Напредно споделување** > **Дозволи**

Ја контролира дозволата за мрежен пристап до споделената папка.

❏ Дозвола за пристап на картичката **Безбедност**

Ја контролира дозволата за мрежен пристап и локален пристап до споделената папка.

Кога ќе поставите **Сите** за споделената папка што се создава на работната површина, како пример за создавањето споделена папка, ќе им се дозволи пристап на сите корисници што имаат пристап до компјутерот.

Меѓутоа, корисникот што нема овластување не може да пристапува бидејќи работната површина (папката) е под контрола на корисничката папка, а потоа поставките за безбедност на корисничката папка се пренесени до неа. Корисникот на којшто му е дозволен пристап до

картичката **Безбедност** (корисник којшто е најавен и, во овој случај администратор) може да ракува со папката.

За создавање соодветна локација, видете подолу.

Ова е пример кога се создава папката „scan_folder".

Поврзани информации

➡ „Пример за конфигурација за датотечни сервери" на страница 50
➡ „Пример за конфигурација за персонален компјутер" на страница 57

Пример за конфигурација за датотечни сервери

Ова објаснување е пример за создавање споделена папка во почетниот директориум на дискот на споделениот компјутер, како што е датотечниот сервер, под следниов услов.

Корисници што може да го контролираат пристапот, како на пр. некој што има ист домен на компјутерот за создавање споделена папка, може да пристапуваат до споделената папка.

Поставете ја оваа конфигурација кога дозволувате сите корисници да читаат и да запишуваат во споделената папка на компјутерот, како што е датотечниот сервер и споделениот компјутер.

❏ Место за создавање споделена папка: почетен директориум на дискот

❏ Патека на папката: C:\scan_folder

❏ Дозвола за пристап преку мрежата (Дозволи за споделување): сите

❏ Дозвола за пристап на датотечен систем (Безбедност): Овластени корисници

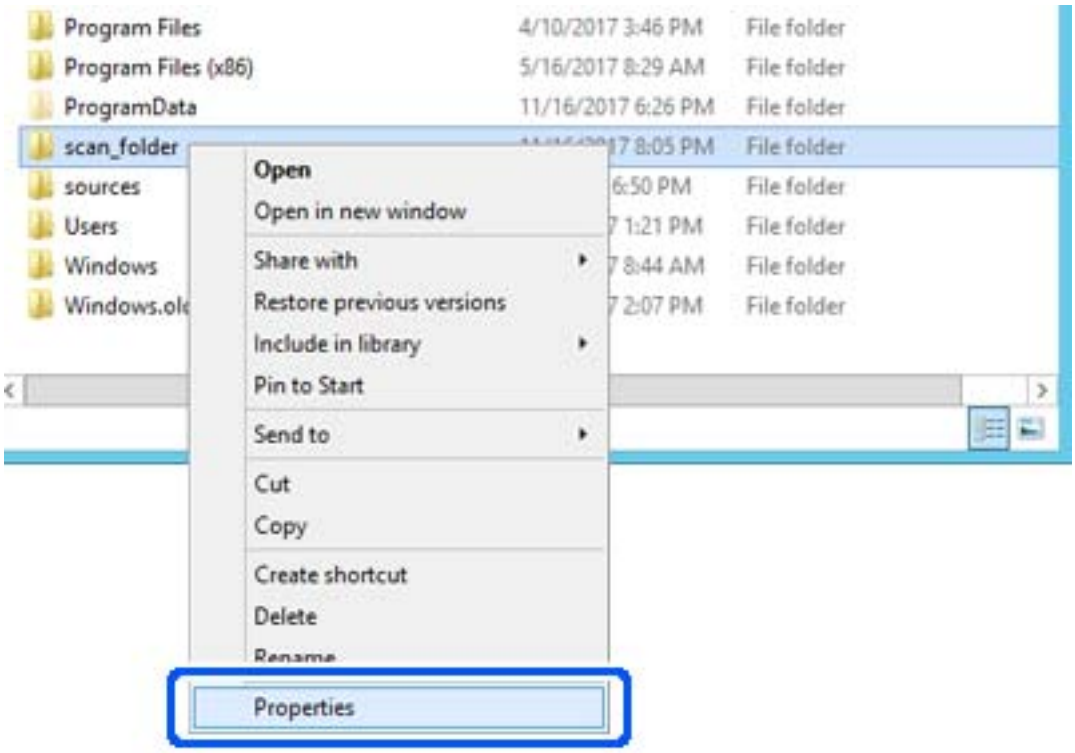
1. Најавете се на компјутерот каде што ќе се создаде споделената папка од страна на администраторската корисничка сметка.

2. Активирајте го истражувачот.

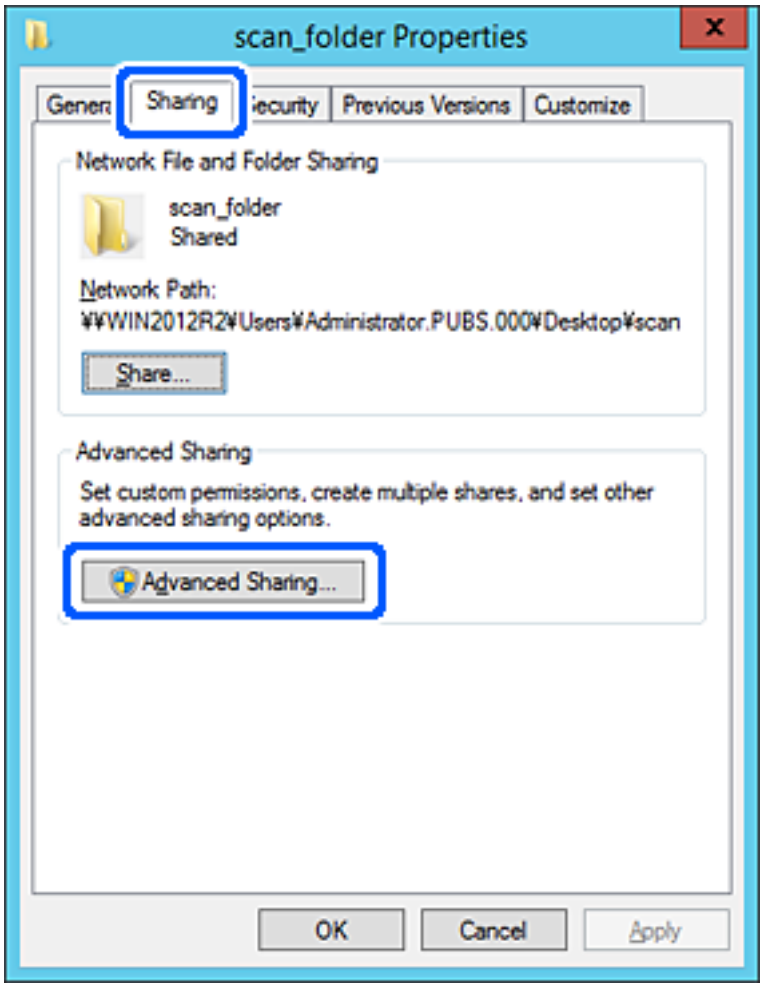
3. Создајте ја папката во почетниот директориум на дискот, а потоа именувајте ја како „scan_folder".

   За името на папката, внесете од 1 до 12 алфанумерички знаци. Ако го надминете максималниот број знаци за името на папката, нема да може нормално да пристапувате до папката преку различни околини.

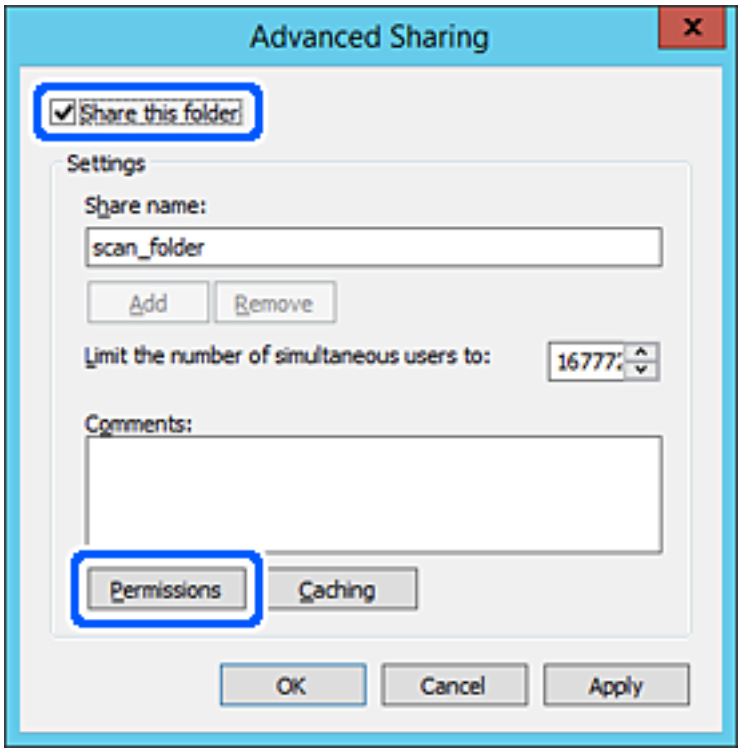
4. Кликнете со десното копче на папката и изберете **Својства**.



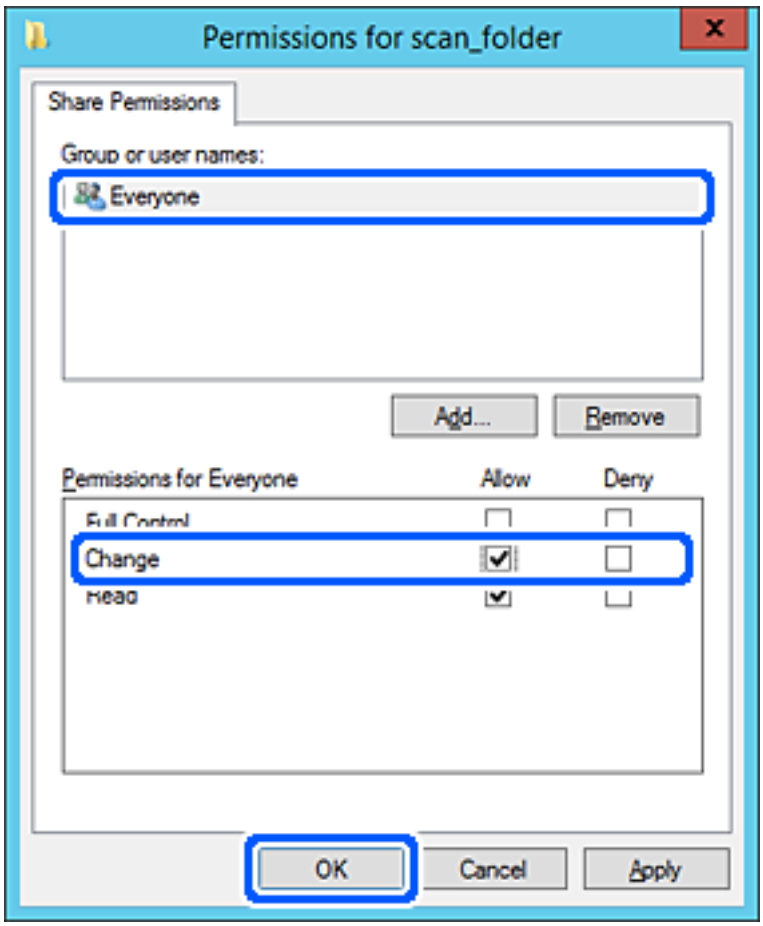
5. Кликнете на **Напредно споделување** на јазичето **Споделување**.



6. Изберете **Сподели ја оваа папка**, а потоа кликнете на **Дозволи**.

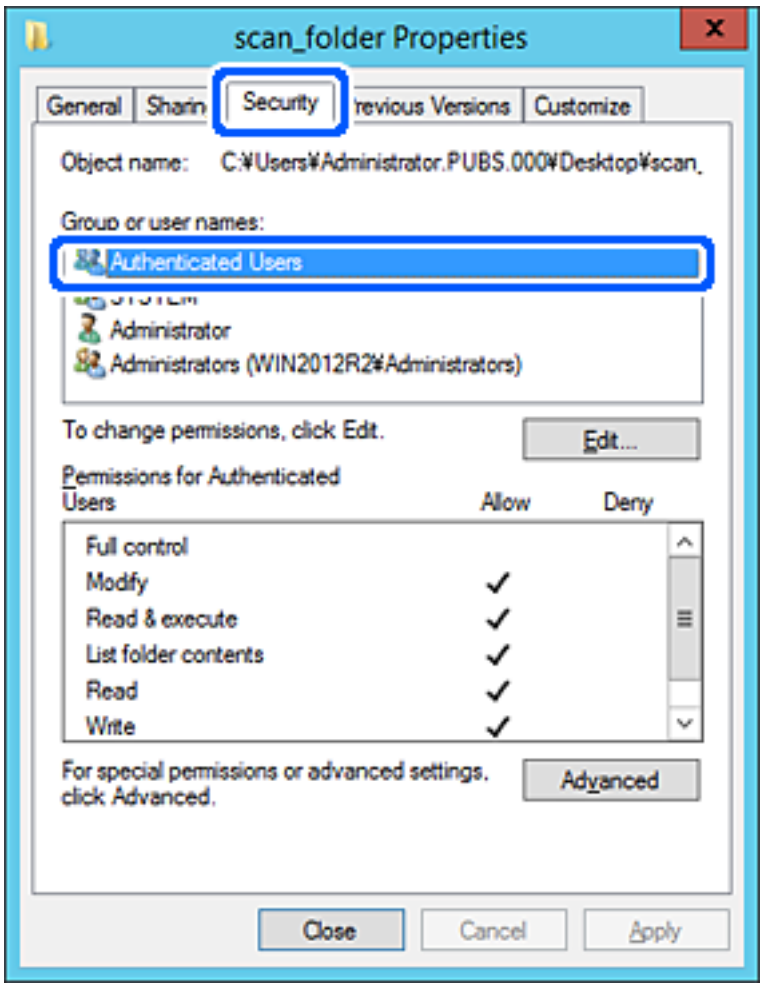


7. Изберете ја групата **Сите** од **Имиња на група или корисници**, изберете **Дозволи** на **Измени**, а потоа кликнете **OK**.



8. Кликнете на **Во ред**.

9. Изберете ја картичката **Безбедност**, а потоа изберете **Овластени корисници** на **Имиња на група или корисници**.

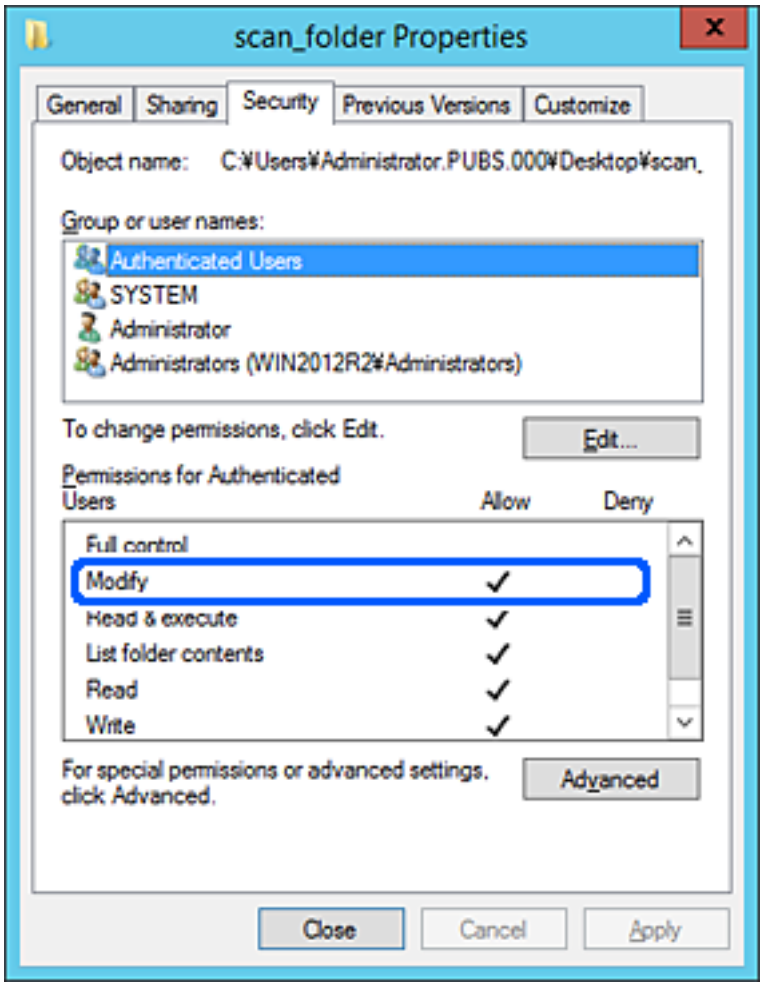


„Овластени корисници" е посебната група што ги вклучува сите корисници што може да се најават на доменот или на компјутерот. Оваа група се прикажува само кога папката се создава веднаш под почетната папка.

Ако не се прикажува, може да ја додадете кликнувајќи на **Уреди**. За повеќе детали, видете Поврзани информации.

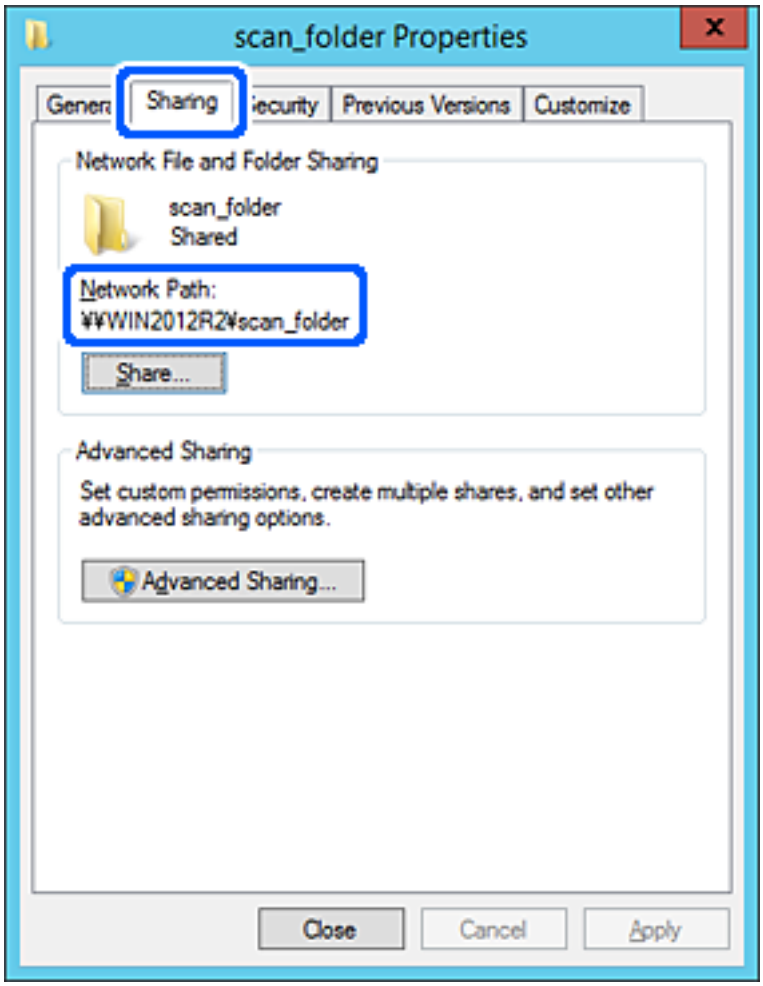
10. Уверете се дека **Дозволи** на **Измени** е избрано во **Дозволи за овластени корисници**.

    Ако не е избрано, изберете **Овластени корисници**, кликнете на **Уреди**, изберете **Дозволи** на **Измени** во **Дозволи за овластени корисници**, а потоа кликнете на **OK**.



11. Изберете ја картичката **Споделување**.

    Се прикажува мрежната патека на споделената папка. Таа се користи при регистрација во адресарот на скенерот. Запишете ја.



12. Кликнете на **Во ред** или **Затвори** за да го затворите екранот.

    Проверете дали датотеката може да се запишува или да се чита во споделената папка преку компјутерите на истиот домен.

Поврзани информации

➡ „Додавање група или корисник што дозволува пристап“ на страница 63
➡ „Регистрирање дестинација за контакти користејќи Web Config“ на страница 68

Пример за конфигурација за персонален компјутер

Ова објаснување е пример за создавање на споделената папка на десктоп-компјутерот ако корисникот во моментов се најавува на компјутерот.

Корисникот којшто се најавува на компјутерот и има администраторски овластувања може да пристапува до папката на работната површина и до папката со документи под папката Корисник.

Поставете ја конфигурацијава кога НЕ дозволувате читање и запишување на друг корисник во споделената папка на персоналниот компјутер.

- ❏ Место за создавање споделена папка: Desktop (работна површина)
- ❏ Патека на папката: C:\Users\xxxx\Desktop\scan_folder
- ❏ Дозвола за пристап преку мрежата (Дозволи за споделување): сите
- ❏ Дозвола за пристап до датотечен систем (Безбедност): не додавајте или додајте имиња на Корисник/Група за да дозволите пристап

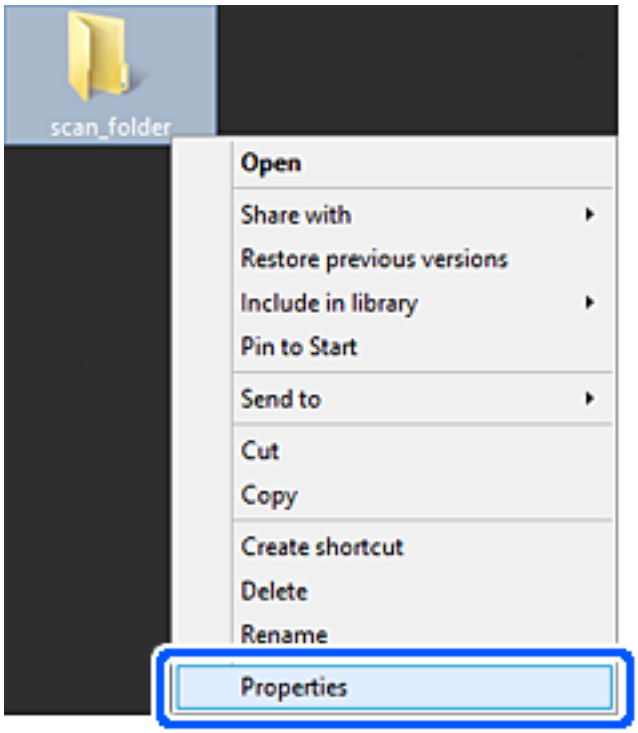
1. Најавете се на компјутерот каде што ќе се создаде споделената папка од страна на администраторската корисничка сметка.

2. Активирајте го истражувачот.

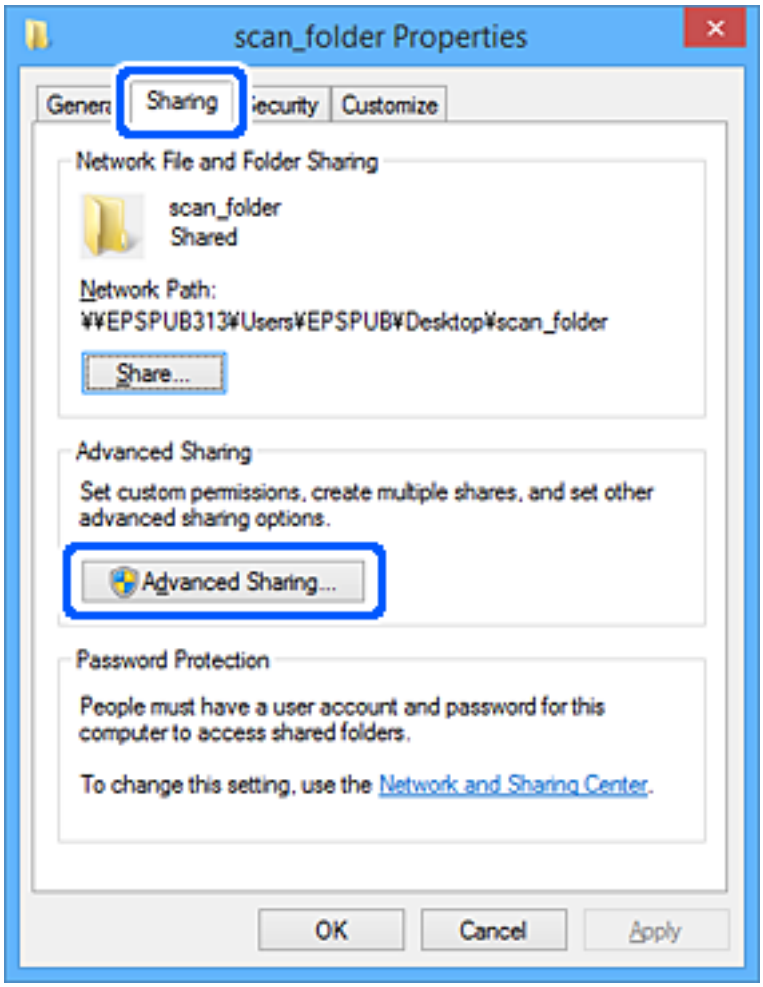
3. Создајте ја папката на работната површина, а потоа именувајте ја како „scan_folder".

   За името на папката, внесете од 1 до 12 алфанумерички знаци. Ако го надминете максималниот број знаци за името на папката, нема да може нормално да пристапувате до папката преку различни околини.

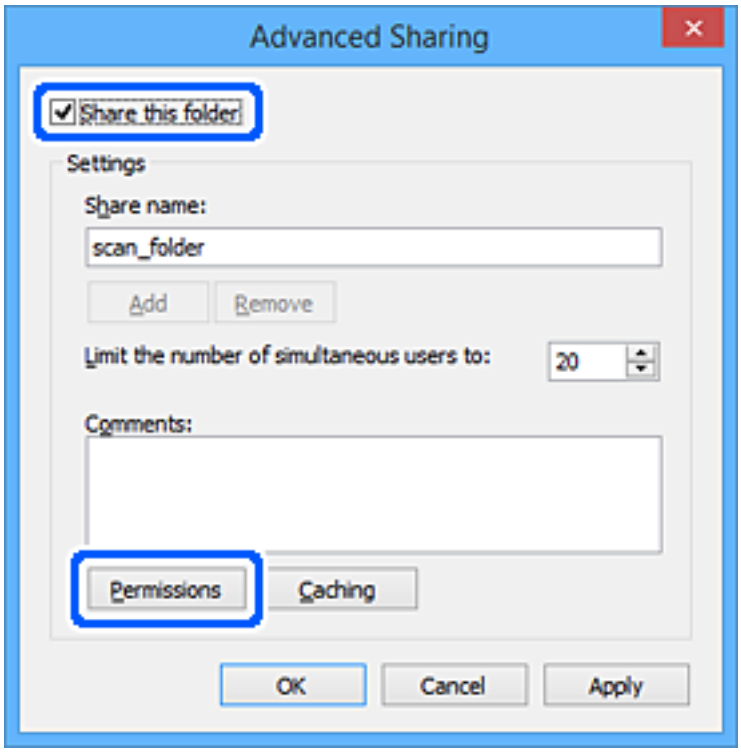
4. Кликнете со десното копче на папката и изберете **Својства**.



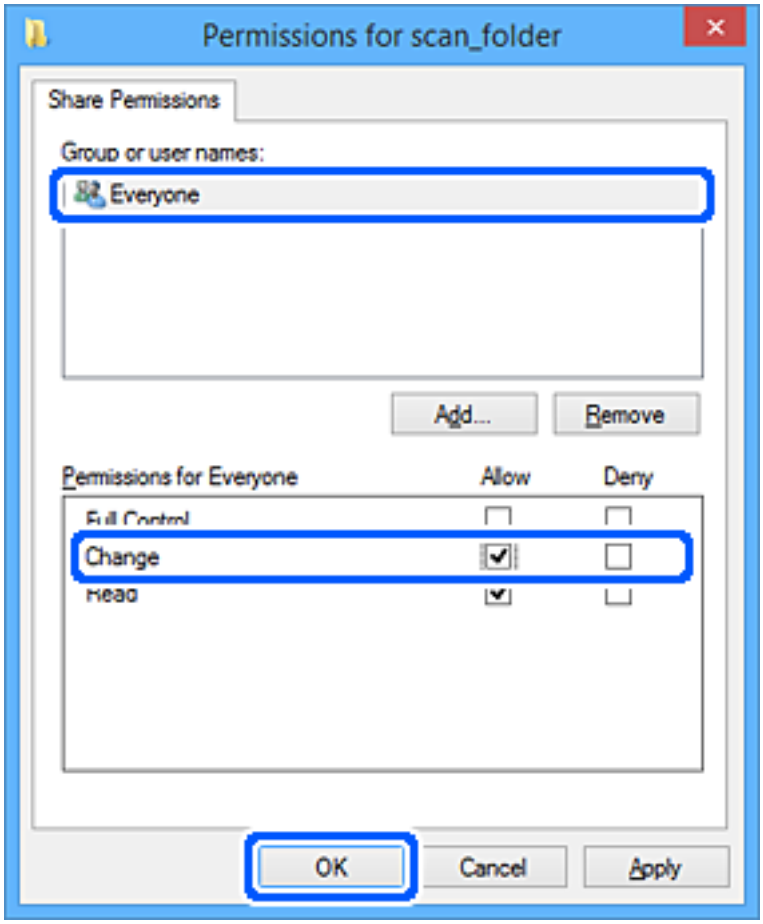
5. Кликнете на **Напредно споделување** на јазичето **Споделување**.



6. Изберете **Сподели ја оваа папка**, а потоа кликнете на **Дозволи**.



7. Изберете ја групата **Сите** од **Имиња на група или корисници**, изберете **Дозволи** на **Измени**, а потоа кликнете **OK**.



8. Кликнете на **Во ред**.

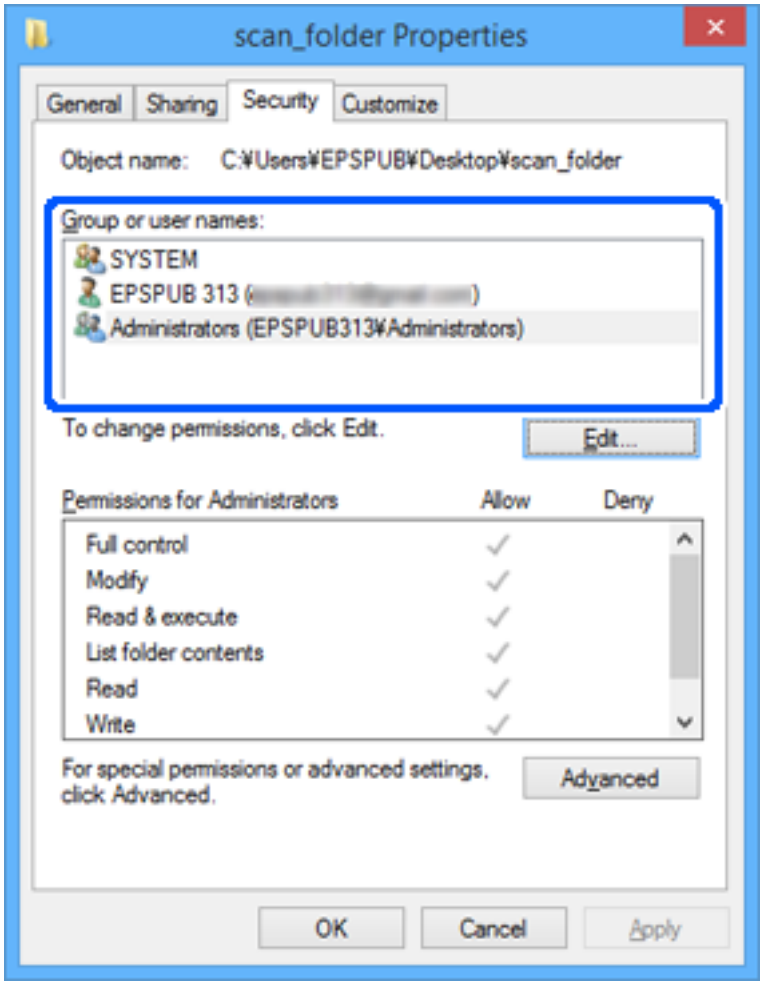
9. Изберете ја картичката **Безбедност**.

10. Проверете ги групата или корисникот во **Имиња на група или корисници**.

    Групата или корисникот што се прикажани овде може да пристапуваат до споделената папка.

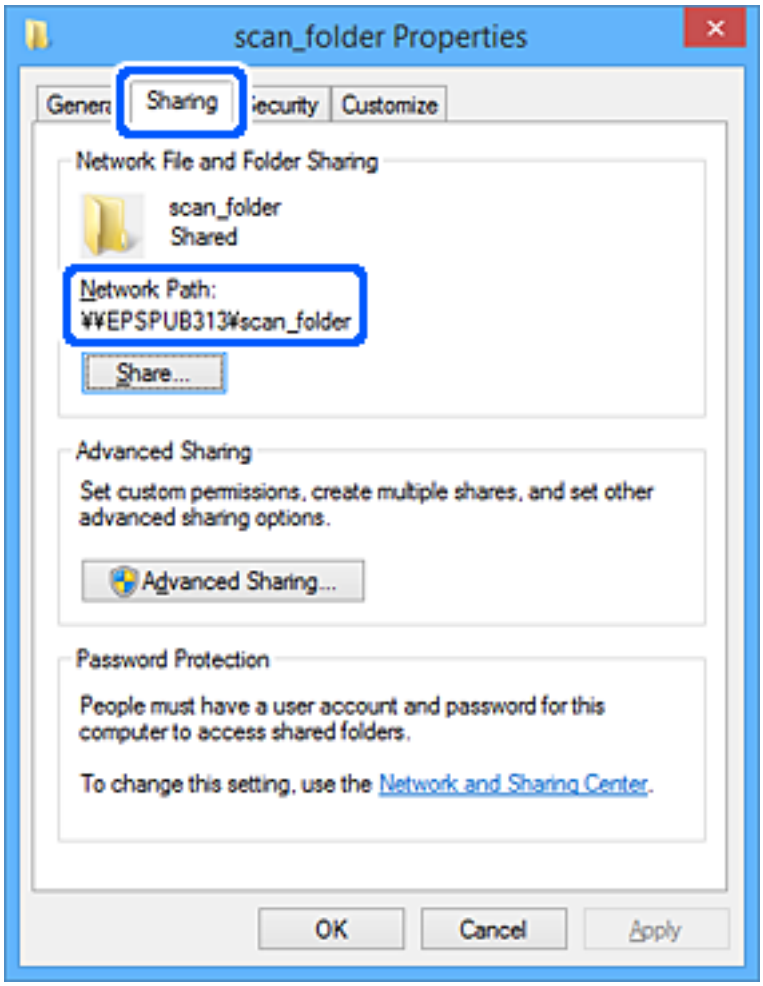
    Во овој случај, до споделената папка може да пристапуваат корисникот што се најавува на овој компјутер, како и администраторот.

Додајте дозвола за пристап, ако е потребно. Може да ја додадете кликнувајќи на **Уреди**. За повеќе детали, видете Поврзани информации.



11. Изберете ја картичката **Споделување**.

    Се прикажува мрежната патека на споделената папка. Таа се користи при регистрација во адресарот на скенерот. Запишете ја.



12. Кликнете на **Во ред** или **Затвори** за да го затворите екранот.

    Проверете дали датотеката може да се запишува или да се чита во споделената папка преку компјутерите на корисниците или на групите со дозвола за пристап.

Поврзани информации

➡ „Додавање група или корисник што дозволува пристап“ на страница 63
➡ „Регистрирање дестинација за контакти користејќи Web Config“ на страница 68

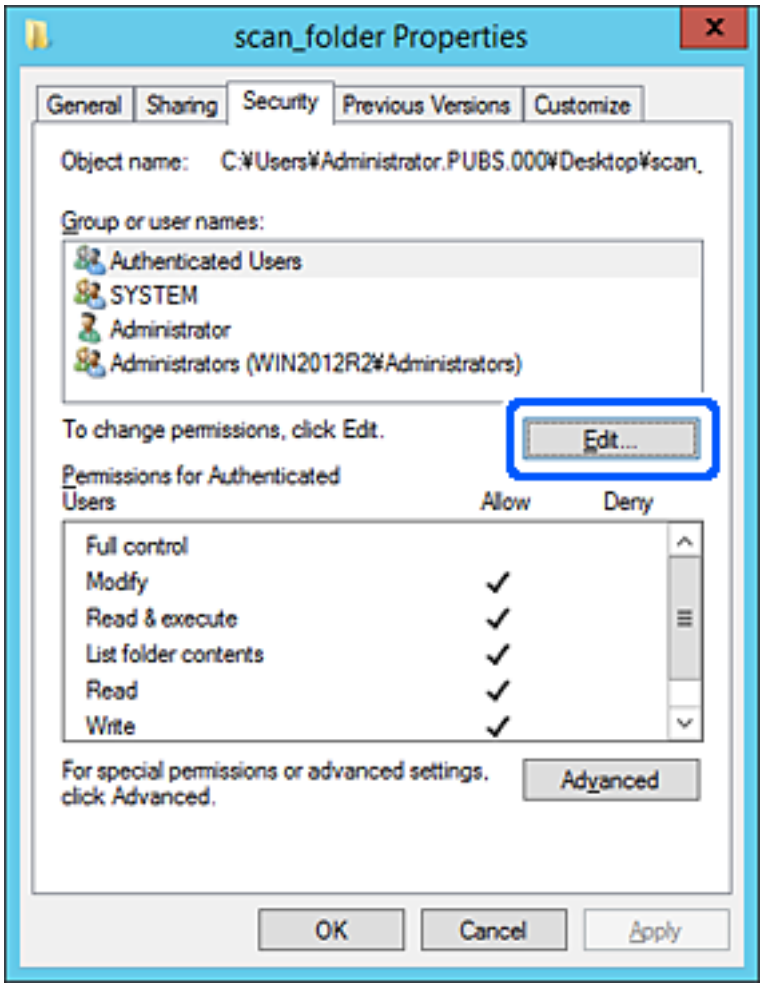
Додавање група или корисник што дозволува пристап

Може да додадете група или корисник што дозволува пристап.

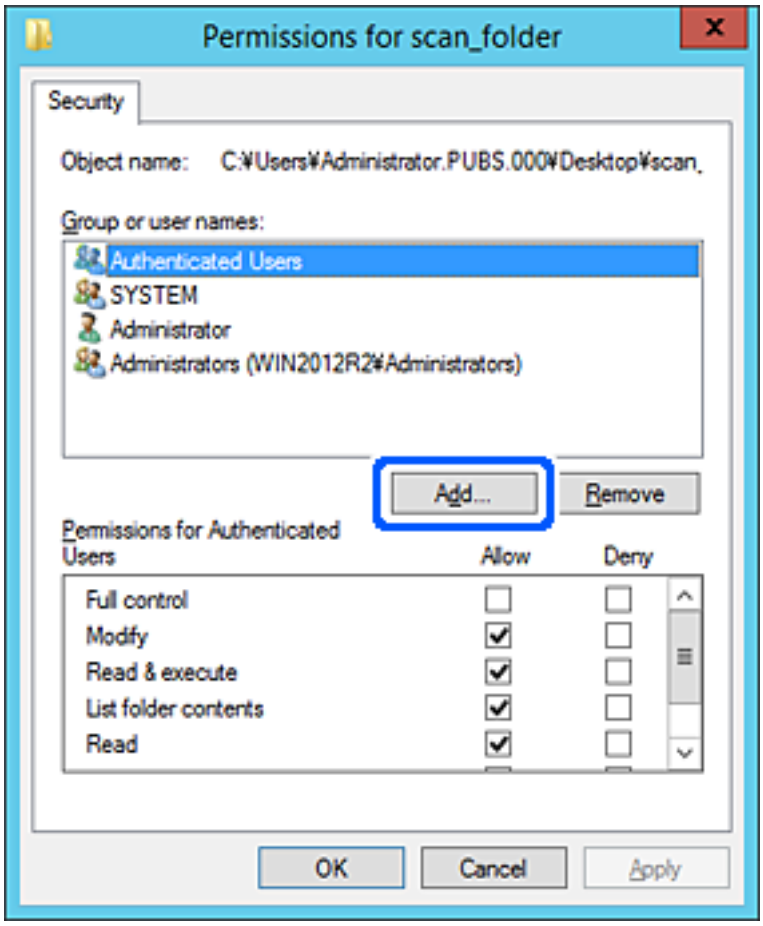
1. Кликнете со десното копче на папката и изберете **Својства**.

2. Изберете ја картичката **Безбедност**.

3. Кликнете на **Уреди**.



4. Кликнете на **Додај** под **Имиња на група или корисници**.

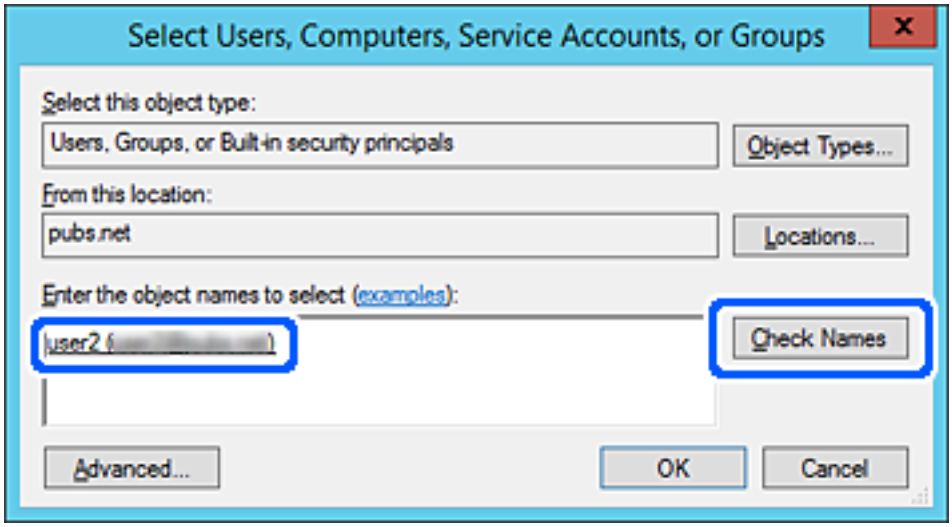


5. Внесете го името на група или корисник што сакате да дозволуваат пристап, а потоа кликнете **Провери имиња**.

   Името се подвлекува.

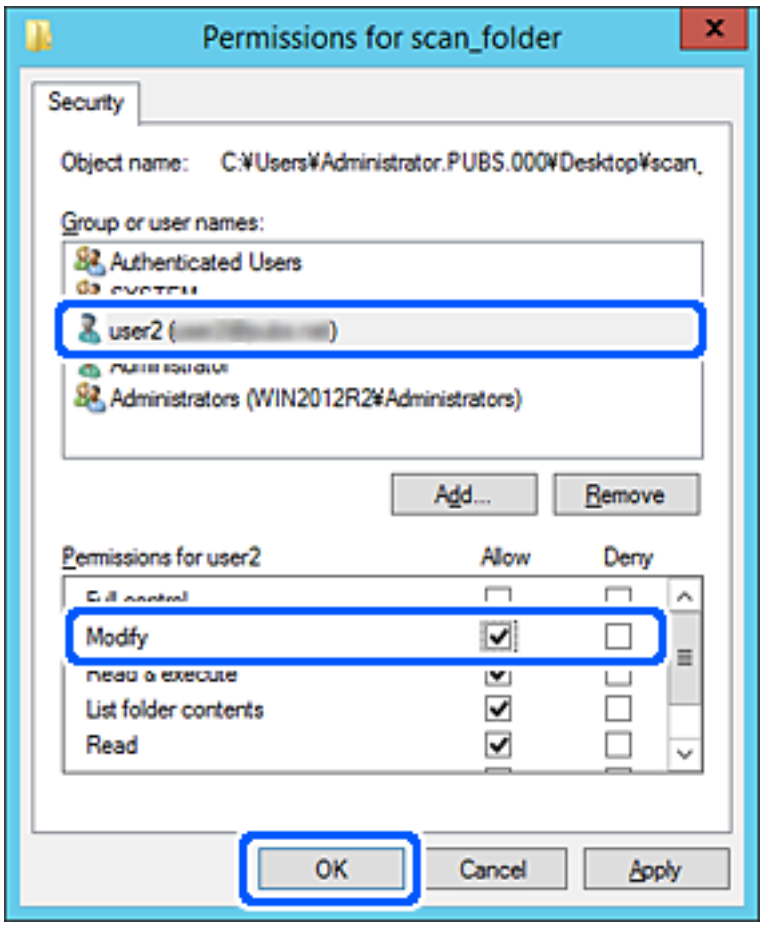
Белешка:
Ако не го знаете целото име на групата или корисникот, внесете дел од името, а потоа кликнете ***Провери имиња****. Се појавуваат имињата на групи или корисници што се совпаѓаат со дел од името, а потоа може да го изберете целото име од списокот.*

Ако се совпаѓа само едно име, целото подвлечено име се прикажува во ***Внесете го името на предметот за избирање****.*



6. Кликнете на **Во ред**.

7. Во екранот Дозвола, изберете го корисничкото име внесено во **Имиња на група или корисници**, изберете ја дозволата за пристап на **Модифицирај**, а потоа кликнете **Во ред**.



8. Кликнете на **Во ред** или **Затвори** за да го затворите екранот.

   Проверете дали датотеката може да се запишува или да се чита во споделената папка преку компјутерите на корисниците или на групите со дозвола за пристап.

Побрз пристап до контактите

Ако регистрирате дестинации во списокот со контакти на скенерот, лесно може да ја внесете дестинацијата кога скенирате.

Може да ги регистрирате следниве типови дестинации во списокот со контакти. Може да регистрирате најмногу 300 ставки.

Белешка:
За да ја внесете дестинацијата, може да го користите и LDAP-серверот (LDAP-пребарување).

Е-пошта	Дестинација за е-пошта. Претходно треба да ги конфигурирате поставките за серверот за е-пошта.
Мрежна папка	Дестинација за податоци од скенирање. Претходно треба да ја подготвите мрежната папка.

Поврзани информации

➡ „Соработка меѓу LDAP-серверот и корисниците“ на страница 74

Споредба на конфигурацијата на контакти

Постојат три алатки за конфигурирање на контактите на скенерот: Web Config, Epson Device Admin и контролната табла на скенерот. Разликите меѓу овие три алатки се наведени во табелата подолу.

Функции	Web Config*	Epson Device Admin	Контролна табла на скенерот
Регистрирање дестинација	✓	✓	✓
Изменување дестинација	✓	✓	✓
Додавање група	✓	✓	✓
Изменување група	✓	✓	✓
Бришење дестинација или групи	✓	✓	✓
Бришење на сите дестинации	✓	✓	–
Увезување датотека	✓	✓	–
Извезување во датотека	✓	✓	–

* За да одредувате поставки, најавете се како администратор.

Регистрирање дестинација за контакти користејќи Web Config

Белешка:
Контактите може да ги регистрирате и преку контролната табла на скенерот.

1. Одете на Web Config и изберете ја картичката **Scan** > **Contacts**.
2. Изберете го бројот што сакате да го регистрирате, а потоа кликнете **Edit**.
3. Внесете **Name** и **Index Word**.
4. Изберете го типот на дестинација како **Type** опција.

   Белешка:
   *Не може да ја промените **Type** опцијата откако ќе завршите со регистрацијата. Ако сакате да го промените типот, избришете ја дестинацијата и повторно регистрирајте.*
5. Внесете вредност за секоја ставка и кликнете на **Apply**.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Поставки за дестинација

Ставки	Поставки и објаснувања
Вообичаени поставки	
Name	Внесете име прикажано во контактите од 30 знаци или помалку во Unicode (UTF-8). Во спротивно, оставете го полево празно.
Index Word	За да пребарувате контакти преку контролната табла на скенерот, внесете име користејќи 30 знаци или помалку во Unicode (UTF-8). Во спротивно, оставете го полево празно.
Type	Изберете го типот на адреса што сакате да ја регистрирате.
Assign to Frequent Use	Изберете за да се постави регистрираната адреса како често употребувана. Кога ја поставувате како често користена адреса, таа се прикажува во горниот дел на екранот за скенирање и може да ја одредите дестинацијата без да се прикажуваат контактите.
Email	
Email Address	Внесете од 1 до 255 знаци користејќи A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Network Folder (SMB)	
Save to	\\„Патека за папката“ Внесете локација каде што целната папка е лоцирана од 1 до 253 знаци во Unicode (UTF-8), не внесувајќи го „\\“. Внесете ја мрежната патека прикажана на екранот со својства на папката. Погледнете го следново за детали во врска со поставувањето на мрежната патека. „Пример за конфигурација за персонален компјутер“ на страница 57
User Name	Внесете корисничко име од 30 знаци или помалку во Unicode (UTF-8) за да пристапите до мрежна папка. Меѓутоа, не користете контролни знаци (0x00 до 0x1F, 0x7F).
Password	Внесете лозинка од 20 знаци или помалку во Unicode (UTF-8) за да пристапите до мрежна папка. Меѓутоа, не користете контролни знаци (0x00 до 0x1F, 0x7F).
FTP	
Secure Connection	Изберете FTP или FTPS според протоколот за пренос на датотеки што го поддржува FTP-серверот. Изберете **FTPS** за да овозможите скенерот да комуницира со безбедносни мерки.
Save to	Внесете го името на серверот од 1 до 253 знаци во ASCII (0x20-0x7E), не внесувајќи „ftp://“ или „ftps://“.

Ставки	Поставки и објаснувања
User Name	Внесете корисничко име за да пристапите до FTP-сервер од 30 знаци или помалку во Unicode (UTF-8). Меѓутоа, не користете контролни знаци (0x00 до 0x1F, 0x7F). Ако серверот дозволува анонимни врски, внесете го корисничкото име, како на пример Анонимно и FTP. Во спротивно, оставете го полево празно.
Password	Внесете лозинка од 20 знаци или помалку во Unicode (UTF-8) за да пристапите до FTP-сервер. Меѓутоа, не користете контролни знаци (0x00 до 0x1F, 0x7F). Во спротивно, оставете го полево празно.
Connection Mode	Изберете режим на поврзување од менито. Ако е поставен заштитен ѕид меѓу скенерот и FTP-серверот, изберете **Passive Mode**.
Port Number	Внесете го бројот на портата на FTP-серверот од 1 до 65535.
Certificate Validation	Сертификатот на FTP-серверот се потврдува кога ова е овозможено. Ова е достапно кога **FTPS** е избрано за **Secure Connection**. За да извршите поставување, треба да увезете CA Certificate во скенерот.
SharePoint(WebDAV)	
Secure Connection	Изберете HTTP или HTTPS според протоколот за пренос на датотеки што го поддржува серверот. Изберете **HTTPS** за да овозможите скенерот да комуницира со безбедносни мерки.
Save to	Внесете го името на серверот од 1 до 253 знаци во ASCII (0x20-0x7E), не внесувајќи „http://" или „https://".
User Name	За да пристапите до сервер, внесете корисничко име што содржи до 30 знаци во Unicode (UTF-8). Меѓутоа, не користете контролни знаци (0x00 до 0x1F, 0x7F). Во спротивно, оставете го полево празно.
Password	За да пристапите до сервер, внесете лозинка што содржи до 20 знаци во Unicode (UTF-8). Меѓутоа, не користете контролни знаци (0x00 до 0x1F, 0x7F). Во спротивно, оставете го полево празно.
Certificate Validation	Сертификатот на серверот се потврдува кога ова е овозможено. Ова е достапно кога **HTTPS** е избрано за **Secure Connection**. За да извршите поставување, треба да увезете CA Certificate во скенерот.
Proxy Server	Изберете дали сакате да користите прокси-сервер.

Регистрирање дестинации како група користејќи Web Config

Ако типот на дестинацијата е поставен на **Email**, може да ги регистрирате дестинациите како група.

1. Одете на Web Config и изберете ја картичката **Scan** > **Contacts**.
2. Изберете го бројот што сакате да го регистрирате, а потоа кликнете **Edit**.
3. Изберете група од **Type**.

4. Кликнете на **Select** за **Contact(s) for Group**.

   Се прикажуваат достапните дестинации.

5. Изберете ја дестинацијата којашто сакате да ја регистрирате во групата и потоа кликнете на **Select**.

6. Внесете **Name** и **Index Word**.

7. Изберете дали ќе ја назначите регистрираната група во често користената група.

   Белешка:
   Дестинациите може да се регистрираат во повеќе групи.

8. Кликнете **Apply**.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Увезување и правење резервна копија од контакти

Може да увезувате контакти и да правите резервна копија од контактите со Web Config или со други алатки.

Со Web Config, може да правите резервна копија од контактите извезувајќи ги поставките за скенерот што содржат контакти. Извезената датотека не може да се изменува бидејќи е извезена како бинарна датотека.

Кога во скенерот ги увезувате поставките за скенерот, контактите се заменуваат со други.

Со Epson Device Admin, од екранот со својства на уредот може да се извезуваат само контакти. Исто така, ако не ги извезувате ставките поврзани со безбедност, може да ги изменувате извезените контакти и да ги увезувате бидејќи може да се зачуваат како датотека SYLK или датотека CSV.

Увезување контакти користејќи Web Config

Ако имате скенер што ви овозможува да направите резервна копија од контактите и е компатибилен со овој скенер, може лесно да ги регистрирате контактите со увезување на датотеката со резервна копија.

Белешка:
За инструкции околу тоа како да направите резервна копија од контактите на скенерот, погледнете во прирачникот приложен со печатачот.

Следете ги чекорите подолу за да ги увезете контактите во овој скенер.

1. Одете на Web Config, изберете ја картичката **Device Management** > **Export and Import Setting Value** > **Import**.

2. Изберете ја датотеката со резервна копија што ја создадовте во **File**, внесете ја лозинката, а потоа кликнете **Next**.

3. Изберете го полето за избор **Contacts**, а потоа кликнете **Next**.

Правење резервна копија од контактите со Web Config

Податоците за контактите може да се изгубат поради дефект на скенерот. Ви препорачуваме да правите резервна копија од податоците секогаш кога ќе ги ажурирате. Epson не одговара за губење податоци, за правење резервни копии или враќање податоци и/или поставки дури и во гарантниот период.

Со Web Config може да направите резервна копија во компјутерот од податоците за контакти зачувани во скенерот.

1. Одете на Web Config, а потоа изберете ја картичката **Device Management** > **Export and Import Setting Value** > **Export**.
2. Изберете го полето за избор **Contacts** во категоријата **Scan**.
3. Внесете лозинка за да ја шифрирате извезената датотека.

   Лозинката ќе ви треба за да ја увезете датотеката. Оставете го ова празно ако не сакате да ја шифрирате датотеката.
4. Кликнете **Export**.

Користење алатка за извезување и групна регистрација на контактите

Ако користите Epson Device Admin, може да направите резервна копија само од контактите и да ги изменувате извезените датотеки, а потоа да ги регистрирате сите одеднаш.

Ова е корисно ако сакате да направите резервна копија само од контактите или кога го менувате скенерот и сакате да ги префрлите контактите од стариот во новиот скенер.

Извезување контакти

Зачувајте ги информациите за контактите во датотеката.

Може да ги уредувате датотеките зачувани во SYLK-формат или CSV-формат користејќи апликација за табеларни пресметки или уредувач за текст. Може да ги регистрирате сите одеднаш, откако ќе ги избришете или додадете информациите.

Информациите што содржат безбедносни ставки, како што се лозинка и лични податоци, може да се зачуваат во бинарен формат со лозинка. Не може да ја уредувате датотеката. Може да се користи како резервна датотека на информациите што ги содржат безбедносните ставки.

1. Стартувајте ја Epson Device Admin.
2. Изберете **Devices** во менито со задачи на страничната лента.
3. Од списокот со уреди, изберете го уредот што сакате да го конфигурирате.
4. Кликнете **Device Configuration** на картичката **Home** од менито со ленти.

   Кога е поставена лозинката за администратор, внесете ја лозинката и кликнете на **OK**.
5. Кликнете **Common** > **Contacts**.

6. Изберете го форматот за извезување од **Export** > **Export items**.
   - ❏ All Items

     Извезете ја шифрираната бинарна датотека. Изберете кога сакате да вклучите безбедносни ставки, како што се лозинки и лични податоци. Не може да ја уредувате датотеката. Ако ја изберете, мора да поставите лозинка. Кликнете **Configuration** и поставете лозинка од 8 до 63 знаци во ASCII. Оваа лозинка се бара при увезување на бинарната датотека.
   - ❏ Items except Security Information

     Извезете ги датотеките во SYLK-формат или во CSV-формат. Изберете кога сакате да ги уредувате информациите на извезената датотека.
7. Кликнете **Export**.
8. Одредете го местото за зачувување на датотеката, изберете го типот датотека, а потоа кликнете **Save**.

   Се прикажува пораката за завршување.
9. Кликнете **OK**.

   Уверете се дека датотеката е зачувана во одреденото место.

Увезување контакти

Увезете ги информациите за контакти од датотеката.

Може да ги увезете датотеките зачувани во SYLK-формат или CSV-формат или резервната бинарна датотека што ги содржи безбедносните ставки.

1. Стартувајте ја Epson Device Admin.
2. Изберете **Devices** во менито со задачи на страничната лента.
3. Од списокот со уреди, изберете го уредот што сакате да го конфигурирате.
4. Кликнете **Device Configuration** на картичката **Home** од менито со ленти.

   Кога е поставена лозинката за администратор, внесете ја лозинката и кликнете на **OK**.
5. Кликнете **Common** > **Contacts**.
6. Кликнете на **Browse** на **Import**.
7. Изберете ја датотеката што сакате да ја увезете, а потоа кликнете **Open**.

   Кога ќе ја изберете бинарната датотека, во **Password**, при извезување на датотеката внесете ја лозинката што сте ја поставиле.
8. Кликнете **Import**.

   Се прикажува екранот за потврда.

9. Кликнете **OK**.

   Се прикажува резултатот од потврдувањето.

   ❏ Edit the information read

   Кликнете кога сакате да ги уредувате информациите поединечно.

   ❏ Read more file

   Кликнете кога сакате да увезувате повеќе датотеки.

10. Кликнете на **Import**, а потоа кликнете на **OK** во екранот за завршување на увезувањето.

    Вратете се во екранот за својства на уредот.

11. Кликнете **Transmit**.

12. Кликнете на **OK** на пораката за потврда.

    Поставките се испраќаат до скенерот.

13. На екранот за завршување на испраќањето, кликнете на **OK**.

    Информациите на скенерот се ажурираат.

    Отворете ги контактите од Web Config или од контролната табла на скенерот, а потоа проверете дали контактот е ажуриран.

Соработка меѓу LDAP-серверот и корисниците

При соработка со LDAP-серверот, може да ги користите информациите за адреса регистрирани на LDAP-серверот како дестинација за е-пошта.

Конфигурирање на LDAP-серверот

За да ги користите информациите на LDAP-серверот, регистрирајте го на скенерот.

1. Одете на Web Config и изберете ја картичката **Network** > **LDAP Server** > **Basic**.

2. Внесете вредност за секоја ставка.

3. Изберете **OK**.

   Се прикажуваат поставките што ги избравте.

Ставки за поставка на LDAP серверот

Ставки	Поставки и објаснувања
Use LDAP Server	Изберете **Use** или **Do Not Use**.
LDAP Server Address	Внесете адреса на LDAP серверот. Внесете од 1 до 255 знака од IPv4, IPv6 или FQDN формат. За FQDN-форматот, може да користите алфанумерички знаци во ASCII (0x20–0x7E) и „-" освен за почетокот и крајот на адресата.

Ставки	Поставки и објаснувања
LDAP server Port Number	Внесете го бројот на портата на LDAP-серверот (од 1 до 65535).
Secure Connection	Одредете го начинот на автентикација кога скенерот пристапува до LDAP-серверот.
Certificate Validation	Кога ова е овозможено, се потврдува сертификатот на LDAP-серверот. Препорачуваме ова да биде поставено на **Enable**. За да се постави, **CA Certificate** треба да се увезе во скенерот.
Search Timeout (sec)	Одредете ја должината на времето за пребарување пред да настане прекинот од 5 до 300.
Authentication Method	Изберете еден од начините. Ако изберете **Kerberos Authentication**, изберете **Kerberos Settings** за да ги одредите поставките за Kerberos. За да извршите Kerberos Authentication, потребна е следнава околина. ❏ Скенерот и DNS-серверот може да комуницираат. ❏ Времето на скенерот, на KDC-серверот и на потребниот сервер за автентикација (LDAP-сервер, SMTP-сервер, датотечен сервер) се синхронизирани. ❏ Кога серверот за услуги е назначен како IP-адреса, FQDN на серверот за услуги е регистрирано во зоната за обратно пребарување на DNS-серверот.
Kerberos Realm to be Used	Ако изберете **Kerberos Authentication** како **Authentication Method**, изберете го доменот на Kerberos што сакате да го користите.
Administrator DN / User Name	Внесете го корисничкото име за LDAP сервер од 128 знаци или помалку во Unicode (UTF-8). Не може да ги користите контролните знаци, како на пример 0x00–0x1F и 0x7F. Поставката не се користи кога е избрано **Anonymous Authentication** како **Authentication Method**. Во спротивно, оставете го полево празно.
Password	Внесете ја лозинката за автентикација на LDAP сервер од 128 знаци или помалку во Unicode (UTF-8). Не може да ги користите контролните знаци, како на пример 0x00–0x1F и 0x7F. Поставката не се користи кога е избрано **Anonymous Authentication** како **Authentication Method**. Во спротивно, оставете го полево празно.

Поставки за Kerberos

Ако изберете **Kerberos Authentication** за **Authentication Method** од **LDAP Server** > **Basic**, направете ги следните поставки за Kerberos од јазичето **Network** > **Kerberos Settings**. Може да регистрирате до 10 поставки за Kerberos.

Ставки	Поставки и објаснувања
Realm (Domain)	Внесете го доменот на Kerberos автентикацијата од 255 знаци или помалку во ASCII (0x20–0x7E). Ако не го регистрирате, оставете го празно.
KDC Address	Внесете адреса на Kerberos серверот за автентикација. Внесете 255 знаци или помалку од IPv4, IPv6 или FQDN формат. Ако не го регистрирате, оставете го празно.

Ставки	Поставки и објаснувања
Port Number (Kerberos)	Внесете го бројот на портата на Kerberos серверот од 1 до 65535.

Конфигурирање на поставките за пребарување на LDAP-серверот

Кога ги одредувате поставките за пребарување, може да ја користите адресата на е-пошта регистрирана на LDAP-серверот.

1. Одете на Web Config и изберете ја картичката **Network** > **LDAP Server** > **Search Settings**.
2. Внесете вредност за секоја ставка.
3. Кликнете **OK** за да се прикаже резултатот за поставката.

   Се прикажуваат поставките што ги избравте.

Ставки за поставка за пребарување на LDAP серверот

Ставки	Поставки и објаснувања
Search Base (Distinguished Name)	Ако сакате да пребарувате арбитрарен домен, одредете го името на доменот на LDAP серверот. Внесете од 0 до 128 знаци во Unicode (UTF-8). Ако не пребарувате артибрарни атрибути, оставете го ова празно. Пример за именик на локален сервер: dc=server,dc=local
Number of search entries	Одредете го бројот на записи на пребарувања од 5 до 500. Одредениот број на записите на пребарувања привремено се зачувува и прикажува. Дури и ако бројот на записи на пребарувања е над одредениот број и се прикаже порака за грешка, пребарувањето може да заврши.
User name Attribute	Одредете го името на атрибутот за да се прикаже при пребарување на имиња на корисник. Внесете од 1 до 255 знаци во Unicode (UTF-8). Првиот знак треба да биде a–z или A–Z. Пример: cn, uid
User name Display Attribute	Одредете го името на атрибутот за да се прикаже како корисничко име. Внесете од 0 до 255 знаци во Unicode (UTF-8). Првиот знак треба да биде a–z или A–Z. Пример: cn, sn
Email Address Attribute	Одредете го името на атрибутот за да се прикаже при пребарување на адреси на е-пошта. Внесете комбинација од 1 до 255 знаци со користење на A–Z a–z 0–9 и -. Првиот знак треба да биде a–z или A–Z. Пример: пошта
Arbitrary Attribute 1 - Arbitrary Attribute 4	Може да го одредите другите арбитрарни атрибути за пребарување. Внесете од 0 до 255 знаци во Unicode (UTF-8). Првиот знак треба да биде a–z или A–Z. Ако не сакате да пребарувате за арбитрарни атрибути, оставете го ова празно. Пример: o, ou

Проверка на врската со LDAP-серверот

Врши тестирање на врската со LDAP-серверот користејќи го параметарот поставен на **LDAP Server** > **Search Settings**.

1. Одете на Web Config и изберете ја картичката **Network** > **LDAP Server** > **Connection Test**.
2. Изберете **Start**.

   Започнува тестирањето на врската. По тестирањето, се прикажува извештај од тестирањето.

Пробни референции за конекција на LDAP сервер

Пораки	Објаснување
Connection test was successful.	Оваа порака се прикажува кога поврзувањето со серверот е успешно.
Connection test failed. Check the settings.	Оваа порака се прикажува од следниве причини: ❏ Адресата на LDAP серверот или бројот на порти е неточен. ❏ Настанал прекин. ❏ **Do Not Use** е избрано како **Use LDAP Server**. ❏ Ако **Kerberos Authentication** е избрано како **Authentication Method**, поставките како на пример **Realm (Domain)**, **KDC Address** и **Port Number (Kerberos)** се неточни.
Connection test failed. Check the date and time on your product or server.	Оваа порака се појавува кога поврзувањето не успева бидејќи поставките за време за скенерот и за LDAP-серверот се неусогласени.
Authentication failed. Check the settings.	Оваа порака се прикажува од следниве причини: ❏ **User Name** и/или **Password** се неточни. ❏ Ако **Kerberos Authentication** е избран како **Authentication Method**, времето/датумот можно е да не може да се конфигурира.
Cannot access the product until processing is complete.	Пораката се прикажува кога скенерот е зафатен.

Користење Document Capture Pro Server

Со помош на Document Capture Pro Server, може да управувате со начинот на подредување, форматот на зачувување и дестинацијата за проследување на резултатот од скенирањето, извршени од контролната табла на скенерот. Од контролната табла на скенерот може да повикате и да извршите задача којашто била претходно регистрирана на серверот.

Инсталирајте ја на компјутерот што служи како сервер.

За повеќе информации околу Document Capture Pro Server, контактирајте со локалното претставништво на Epson.

Поставување режим за сервер

За да употребувате Document Capture Pro Server, направете го поставувањето на следниот начин.

1. Одете на Web Config и изберете ја картичката **Scan** > **Document Capture Pro**.
2. Изберете **Server Mode** за **Mode**.
3. Внесете ја адресата на серверот со Document Capture Pro Server инсталиран на него за **Server Address**.

   Внесете помеѓу 2 и 255 знаци од IPv4, IPv6, име на хост или FQDN формат. За FQDN форматот, може да користите алфанумерички знаци во ASCII (0x20–0x7E) и „- " освен за почетокот и крајот на адресата.
4. Кликнете **OK**.

   Мрежата се поврзува повторно и потоа поставките се овозможени.

Поставување на AirPrint

Одете на Web Config, изберете ја картичката **Network**, а потоа изберете **AirPrint Setup**.

Ставки	Објаснување
Bonjour Service Name	Внесете име на услугата Bonjour, користејќи ASCII-текст (0x20 – 0x7E) и до 41 знак.
Bonjour Location	Внесете опис на локацијата на скенерот, користејќи текст во Unicode (UTF-8) и до 127 бајти.
Wide-Area Bonjour	Поставете дали да се користи Wide-Area Bonjour. Ако се користи, скенерот мора да биде регистриран на DNS-серверот за да може да се пребарува скенерот низ сегментот.
Enable AirPrint	Bonjour и AirPrint (услуга за скенирање) се овозможени.

Проблеми при подготовка на мрежното скенирање

Совети за решавање проблеми

❏ Проверка на пораката за грешка

Кога ќе се појави проблем, прво проверете дали има пораки на контролната табла на скенерот или на екранот на двигателот. Ако имате поставено известување преку е-пошта кога се случуваат настаните, може веднаш да го дознаете статусот.

❏ Проверка на статусот на комуникација

Проверете го статусот на комуникација на серверот или клиентскиот компјутер користејќи команди како што се „ping" и „ipconfig".

❏ Тест на врската

За да ја проверите врската меѓу скенерот и серверот за е-пошта, извршете тест на врската од скенерот. Исто така, проверете ја врската од клиентскиот компјутер до серверот за да го проверите статусот на комуникацијата.

❏ Активирање на поставките

Ако поставките и статусот на комуникацијата не покажуваат проблем, проблемите може да се решат со оневозможување или активирање на мрежните поставки за скенерот и со повторно поставување.

Не може да пристапите до Web Config

IP-адресата не е доделена на скенерот.

Решенија

Можеби не е доделена важечка IP-адреса на скенерот. Конфигурирајте ја IP-адресата користејќи ја контролната табла на скенерот. Информациите за тековната поставка може да ги проверите преку контролната табла на скенерот.

Веб-прелистувачот не ја поддржува јачината на шифрирање за SSL/TLS.

Решенија

SSL/TLS има Encryption Strength. Web Config може да се отвори со веб-прелистувач што ги поддржува групните шифрирања прикажани подолу. Проверете дали користите поддржан веб-прелистувач.

❏ 80 bit: AES256/AES128/3DES

❏ 112 bit: AES256/AES128/3DES

❏ 128 bit: AES256/AES128

❏ 192 bit: AES256

❏ 256 bit: AES256

CA-signed Certificate е истечен.

Решенија

Ако има проблем со датумот на истекување на сертификатот, се прикажува „Сертификатот е истечен" кога се поврзувате на Web Config со комуникација SSL/TLS (https). Ако пораката се прикажува пред датумот на истекување на сертификатот, проверете дали датумот на скенерот е правилно конфигуриран.

Заедничките имиња на сертификатот и на скенерот не се совпаѓаат.

Решенија

Ако заедничките имиња на сертификатот и на скенерот не се совпаѓаат, пораката „Името на безбедносниот сертификат не се совпаѓа…" се прикажува кога пристапувате до Web Config со комуникација SSL/TLS (https). Ова се случува бидејќи следниве IP-адреси не се совпаѓаат.

❏ IP-адресата на скенерот внесена во заедничкото име, за создавање Self-signed Certificate или CSR

❏ IP-адресата внесена во веб-прелистувачот кога е активна Web Config

За Self-signed Certificate, ажурирајте го сертификатот.

За CA-signed Certificate, земете го сертификатот за скенерот повторно.

Поставката за прокси-сервер за локална адреса не е поставена за веб-прелистувач.

Решенија

Кога скенерот е поставен да користи прокси-сервер, конфигурирајте го веб-прелистувачот да не се поврзува на локалната адреса преку прокси-серверот.

❏ Windows:

Изберете **Контролна табла** > **Мрежа и интернет** > **Опции за интернет** > **Врски** > **Поставки за LAN** > **Прокси-сервер**, а потоа конфигурирајте да не се користи прокси-серверот за LAN (локални адреси).

❏ Mac OS:

Изберете **Системски претпочитани вредности** > **Мрежа** > **Напредно** > **Прокси-сервери**, а потоа регистрирајте ја локалната адреса за **Заобиколи поставки за прокси за овие хостови и домени**.

Пример:

192.168.1.*: Локална адреса 192.168.1.XXX, подмрежна маска 255.255.255.0

192.168.*.*: Локална адреса 192.168.XXX.XXX, подмрежна маска 255.255.0.0

DHCP е оневозможено во поставките за компјутерот.

Решенија

Ако DHCP за автоматско добивање IP-адреса е оневозможено на компјутерот, не може да пристапите до Web Config. Овозможете DHCP.

Пример за Windows 10:

Отворете ја контролната табла, а потоа кликнете **Мрежа и интернет** > **Центар за мрежа и споделување** > **Измени ги параметрите за адаптерот**. Отворете го екранот „Својства" на врската што ја користите, а потоа отворете го екранот „Својства" за **Верзија на интернет-протокол 4 (TCP/IPv4)** или **Верзија на интернет-протокол 6 (TCP/IPv6)**. Погрижете се **Автоматско добивање IP-адреса** да биде избрано на прикажаниот екран.

Приспособување на приказот на контролната табла

Регистрирање Поч. пос.

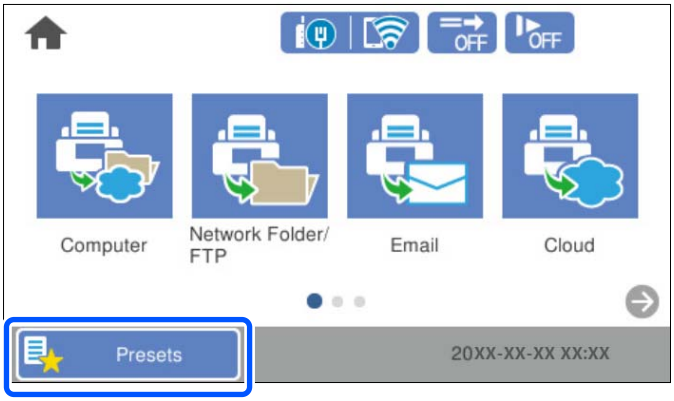
Често користените поставки за скенирање може да ги регистрирате како **Поч. пос.**. Може да регистрирате најмногу 48 однапред поставени поставки.

Белешка:

- *За да ги регистрирате тековните поставки, изберете* ☆ *на екранот за започнување со скенирањето.*
- *Може да регистрирате **Presets** и во Web Config.*

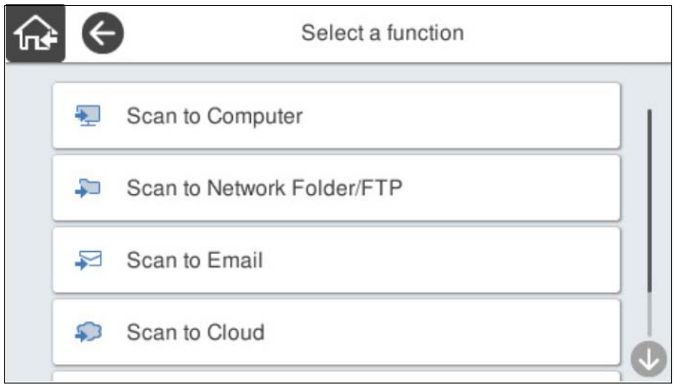
  *Изберете ја картичката **Scan** > **Presets**.*
- *Ако изберете **Скенирај на компјутер** при регистрирањето, може да ја регистрирате задачата создадена во Document Capture Pro како **Presets**. Ова е достапно само за компјутери поврзани на мрежа. Регистрирајте ја задачата во Document Capture Pro однапред.*
- *Ако е овозможена функцијата за автентикација, само администраторот може да регистрира **Presets**.*

1. Изберете **Поч. пос.** на почетниот екран на контролната табла на скенерот.



2. Изберете ⊕.

3. Изберете го менито што сакате да го користите за регистрирање однапред поставена поставка.



4. Одредете ја секоја ставка, а потоа изберете ☆+.

Белешка:
*Кога ќе изберете **Скенирај на компјутер**, изберете го компјутерот на којшто е инсталирана Document Capture Pro, а потоа изберете регистрирана задача. Ова е достапно само за компјутери поврзани на мрежа.*

5. Одредете ги поставките за однапред поставените поставки.
   - ❏ **Име**: поставете го името.
   - ❏ **Постави Икона**: поставете ги сликата и бојата на иконата што ќе се прикажува.
   - ❏ **Поставка за Брзо испраќање**: веднаш го започнува скенирањето без да бара потврда, бидејќи е избрана однапред поставената поставка.

     Кога користите Document Capture Pro Server, дури и ако поставите софтверот да ги потврдува содржините на задачата пред скенирањето, **Поставка за Брзо испраќање** во однапред поставената поставка на скенерот има приоритет над софтверот.
   - ❏ **Содржина**: проверете ги поставките за скенирање.

6. Изберете **OK**.

Опции на менито за Поч. пос.

Поставките за однапред поставена поставка може да ги промените ако изберете › во однапред поставената поставка.

Промени Име:

Го менува името на однапред поставената поставка.

Промени Икона:

Ги менува сликата за иконата и бојата на однапред поставената поставка.

Поставка за Брзо испраќање:

Веднаш го започнува скенирањето без да бара потврда, бидејќи е избрана однапред поставената поставка.

Промени положба:

Го менува редоследот на прикажување на однапред поставените поставки.

Избриши:

Ја брише однапред поставената поставка.

Додај или Отстрани Икона на Почетен:

Ја додава или отстранува иконата за однапред поставената поставка од почетниот екран.

Потврдете Детали:

Прегледајте ги поставките за однапред поставената поставка. Може да ја вчитате однапред поставената поставка ако изберете **Користи ја поставкава**.

Изменување на почетниот екран на контролната табла

За да го приспособувате почетниот екран, изберете **Поставки** > **Уреди Почеток** на контролната табла на скенерот.

- Приказ: го менува начинот на прикажување на иконите на менито.
  „Менување Приказ на почетниот екран“ на страница 85
- Додади икона: додава икони на **Поч. пос.** што сте ги одредиле или ги враќа иконите што сте ги отстраниле од екранот.
  „Додади икона“ на страница 85
- Отстрани икона: отстранува икони од почетниот екран.
  „Отстрани икона“ на страница 86
- Премести икона: го менува редоследот на прикажување на иконите.
  „Премести икона“ на страница 87
- Обнови стандарден приказ на икони: ги враќа стандардните поставки за прикажување за почетниот екран.

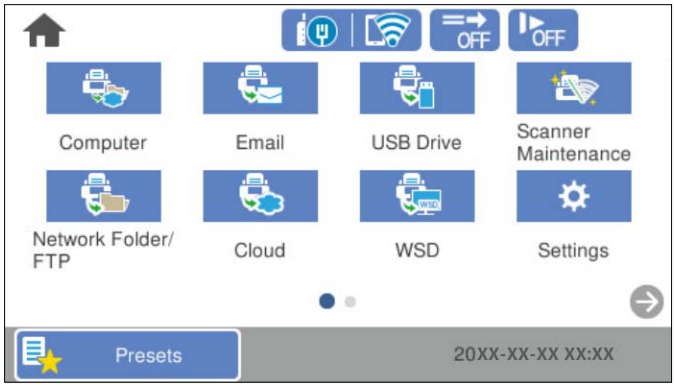
❏ Тапет: променете ја бојата на тапетот за почетниот екран.

Менување Приказ на почетниот екран

1. Изберете **Поставки** > **Уреди Почеток** > **Приказ** на контролната табла на скенерот.
2. Изберете **Линија** или **Матрица**.

   Линија:

   Матрица:



3. Изберете за да се вратите и да го проверите почетниот екран.

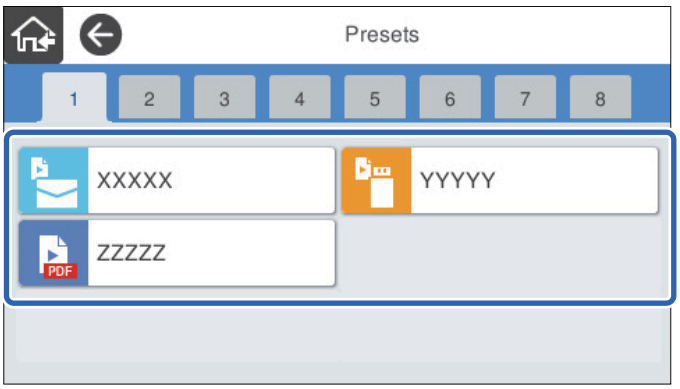
Додади икона

1. Изберете **Поставки** > **Уреди Почеток** > **Додади икона** на контролната табла на скенерот.
2. Изберете **Функција** или **Поч. пос.**.

   ❏ Функција: ги прикажува стандардните функции што се појавуваат на почетниот екран.

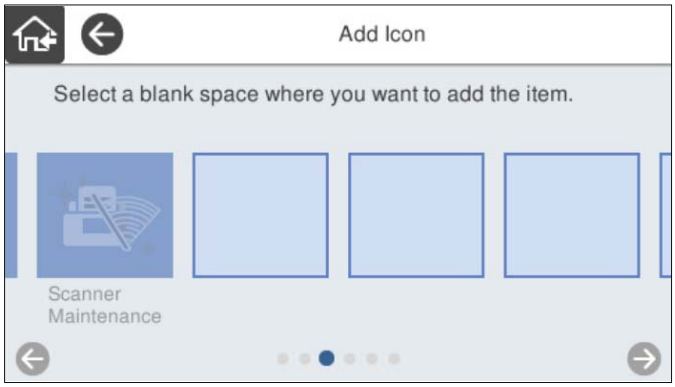
❏ Поч. пос.: ги прикажува регистрираните однапред поставени поставки.

3. Изберете ја ставката што сакате да ја додадете на почетниот екран.



4. Изберете го празниот простор каде што сакате да ја додадете ставката.

   Ако сакате да додадете повеќе икони, повторете ги чекорите од 3 до 4.

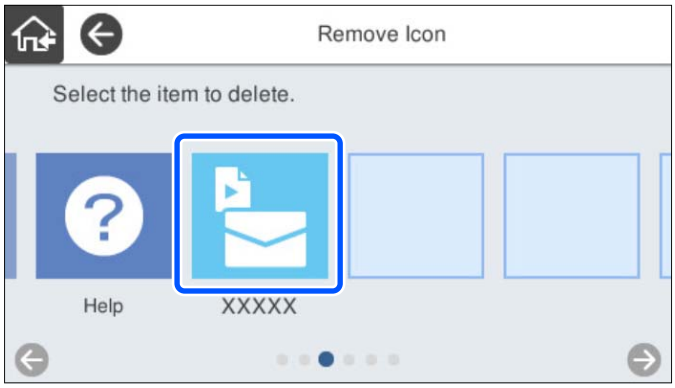


5. Изберете  за да се вратите и да го проверите почетниот екран.

Отстрани икона

1. Изберете **Поставки** > **Уреди Почеток** > **Отстрани икона** на контролната табла на скенерот.

2. Изберете ја иконата што сакате да ја отстраните.



3. Изберете **Да** за да завршите.

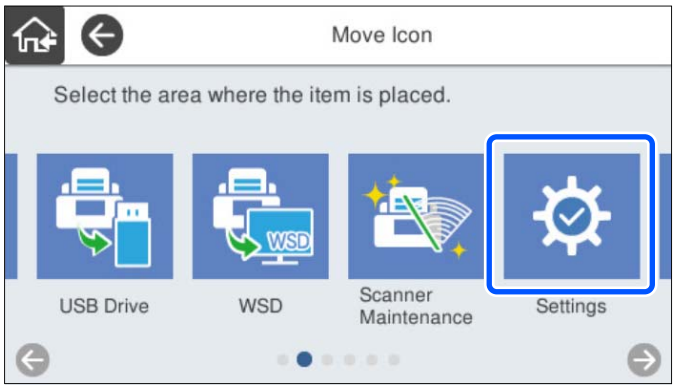
   Ако сакате да отстраните повеќе икони, повторете ги чекорите 2 и 3.

4. Изберете за да се вратите и да го проверите почетниот екран.

Премести икона

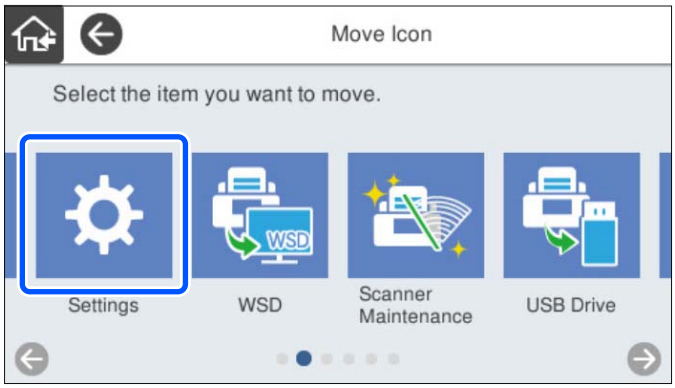
1. Изберете **Поставки** > **Уреди Почеток** > **Премести икона** на контролната табла на скенерот.

2. Изберете ја иконата што сакате да ја преместите.



3. Изберете ја рамката за дестинација.

   Ако друга икона е веќе поставена во рамката за дестинација, иконите се заменуваат.



4. Изберете за да се вратите и да го проверите почетниот екран.

Основни безбедносни поставки

Вовед во безбедносните функции на производот

Во овој дел се претставуваат безбедносните функции на уредите Epson.

Име на функцијата	Тип на функцијата	Што да поставите	Што да спречите
Поставување за администраторската лозинка	Ги заклучува системските поставки, како што е поставувањето врска за мрежа или за USB.	Администраторот поставува лозинка за уредот. Може да ја поставите или да ја смените преку Web Config или преку контролната табла на скенерот.	Спречува недозволено читање и менување на информациите складирани во уредот, како што се ID, лозинка, мрежни поставки итн. Исто така, намалува голем број безбедносни ризици, како на пр. протекување на информации за мрежната околина или за правилото за безбедност.
Поставување за надворешен интерфејс	Го контролира интерфејсот што се поврзува со уредот.	Овозможете или оневозможете USB-врска со компјутерот.	USB-врска на компјутерот: спречува неовластена употреба на уредот забранувајќи скенирање што не се одвива преку мрежата.

Поврзани информации

➡ „Конфигурирање на администраторската лозинка“ на страница 90
➡ „Оневозможување на надворешниот интерфејс“ на страница 96

Администраторски поставки

Конфигурирање на администраторската лозинка

Ако поставите администраторска лозинка, може да спречите корисниците да ги менуваат поставките за управување со системот. Стандардните вредности се поставени при купувањето. Менувајте ги по потреба.

Белешка:
Подолу се наведени стандардните вредности за администраторските информации.

❏ *Корисничко име (се користи само за Web Config): нема (празно)*

❏ *Лозинка: серискиот број на скенерот*

За да го најдете серискиот број, проверете ја етикетата залепена на задниот дел од скенерот.

Може да ја смените администраторската лозинка со Web Config, преку контролната табла на скенерот или со Epson Device Admin. Кога користите Epson Device Admin, погледнете го водичот или помошта за Epson Device Admin.

Менување на администраторската лозинка со Web Config

Администраторската лозинка може да ја промените во Web Config.

1. Одете на Web Config и изберете ја картичката **Product Security** > **Change Administrator Password**.
2. Внесете ги потребните информации во **Current password**, **User Name**, **New Password** и **Confirm New Password**.

   Внесете барем еден знак за новата лозинка.

   Белешка:
   Подолу се наведени стандардните вредности за администраторските информации.

   - ❏ *Корисничко име: нема (празно)*
   - ❏ *Лозинка: серискиот број на скенерот*

   За да го најдете серискиот број, проверете ја етикетата залепена на задниот дел од скенерот.

   > ***Важно:***
   > *Запомнете ја администраторската лозинка што ќе ја поставите. Ако ја заборавите лозинката, нема да може да ја ресетирате и ќе треба да побарате помош од сервисен персонал.*

3. Изберете **OK**.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Менување на администраторската лозинка од контролната табла

Администраторската лозинка може да ја промените од контролната табла на скенерот.

1. Изберете **Поставки** од контролната табла на скенерот.
2. Изберете **Администрир. на систем** > **Администраторски поставки**.
3. Изберете **Лозинка на администраторот** > **Промени**.
4. Внесете ја тековната лозинка.

   Белешка:
   Поставката при купувањето (стандардната вредност) за администраторската лозинка е серискиот број на скенерот.

   За да го најдете серискиот број, проверете ја етикетата залепена на задниот дел од скенерот.

5. Внесете ја новата лозинка.

   Внесете барем еден знак.

> ***Важно:***
>
> *Запомнете ја администраторската лозинка што ќе ја поставите. Ако ја заборавите лозинката, нема да може да ја ресетирате и ќе треба да побарате помош од сервисен персонал.*

6. За да ја потврдите, внесете ја новата лозинка уште еднаш.

Се прикажува порака за завршување.

Користење Поставка за заклучување за контролната табла

Може да користите Поставка за заклучување за да ја заклучите контролната табла и да спречите корисниците да менуваат ставки поврзани со системските поставки.

Белешка:
Ако овозможите Authentication Settings на скенерот, ќе се овозможи и Поставка за заклучување за контролната табла. Контролната табла не може да се отклучи кога е овозможено Authentication Settings.

Дури и ако оневозможите Authentication Settings, Поставка за заклучување останува овозможено. Ако сакате да го оневозможите, може да одредите поставки преку контролната табла или преку Web Config.

Поставување Поставка за заклучување од контролната табла

1. Ако сакате да ја откажете **Поставка за заклучување** откако ќе биде овозможена, допрете  во горниот десен агол на почетниот екран за да се најавите како администратор.

    не се прикажува кога **Поставка за заклучување** е оневозможена. Ако сакате да ја овозможите оваа поставка, одете на следниот чекор.

2. Изберете **Поставки**.

3. Изберете **Администрир. на систем** > **Администраторски поставки**.

4. Изберете **Вкл.** или **Иск.** за **Поставка за заклучување**.

Поставување Поставка за заклучување преку Web Config

1. Изберете ја картичката **Device Management** > **Control Panel**.

2. Изберете **ON** или **OFF** за **Panel Lock**.

3. Кликнете **OK**.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Ставки со Поставка за заклучување во менито Поставки

Ова е список со ставките што се заклучени со Поставка за заклучување во менито **Поставки** на контролната табла.

✓: да биде заклучено.

- : да биде незаклучено.

Мени Поставки		Поставка за заклучување
Осн поставки		-
	ЛЦД осветленост	-
	Звуци	-
	Тајмер за спиење	✓
	Мерач на времето за исклучување	✓
	Поставки за датум/време	✓
	Јазик/Language	✓/-*
	Тастатура (Оваа функција може да не биде достапна во зависност од регионот.)	-
	Прекин во функционирање	✓
	Врска со компјутер преку USB	✓
	Директно вклучување	✓
Поставки на скенерот		-
	Бавно	-
	Време за запирање на двој. внес.	✓
	Функција DFDS	-
	Зашт. на хартија	✓
	Открив. нечистотија на стаклото	✓
	Ултрасо. откр. на двојно ставање	✓
	Истекување на Режимот за автоматско внесување	✓
	Потврди примач	✓
Уреди Почеток		✓

Мени Поставки		**Поставка за заклучување**
	Приказ	✓
	Додади икона	✓
	Отстрани икона	✓
	Премести икона	✓
	Обнови стандарден приказ на икони	✓
	Тапет	✓
Кориснички поставки		✓
	Мрежна папка/ФТП	✓
	E-пошта	✓
	Облак	✓
	USB-диск	✓
Поставки за мрежа		✓
	Wi-Fi поставување	✓
	Поставување на жична LAN	✓
	Статус на мрежа	✓
	Напредно	✓
Поставки за веб услуга		✓
	Услуги на Epson Connect	✓
Document Capture Pro		-
	Промени поставки	✓
Управник со Контакти		-
	Регистрирај/Избриши	✓/-*
	Чести	-
	Прегледај опции	-
	Опции за пребарување	-
Администрир. на систем		✓

Мени Поставки			**Поставка за заклучување**
	Управник со Контакти		✓
	Администраторски поставки		✓
	Ограничувања		✓
	Енкрипција на лозинка		✓
	Истражување на клиентите		✓
	Поставки WSD		✓
	Врати ги стандардните поставки		✓
	Ажурирање на фирмвер		✓
Информации за уред			-
	Сериски број		-
	Тековна верзија		-
	Вкупен број на скенирања		-
	Бр. на едностр. скенирања		-
	Бр. на двострани скенирања		-
	Бр. на скен. од Носач на листови		-
	Бр. на ск. по зам. на валјакот		-
	Бр. на ск. по Редовно чистење		-
	Ресетирајте го бројот на скенирања		✓
Одржување на скенер			-
	Чистење на валјак		-
	Замена на валјак за одржување		-
		Ресетирајте го бројот на скенирања	✓
		Како да замените	-
	Редовно чистење		-
		Ресетирајте го бројот на скенирања	✓
		Како да се чисти	-
	Чистење на Стакло		-
Поставка за предупредување за замена на валјакот			✓
	Пост. за бр. на предупр		✓
Поставки за предупредување за Редовно чистење			✓

Мени Поставки		Поставка за заклучување
	Поставка за предупредување	✓
	Пост. за бр. на предупр	✓

* Може да одредите дали да се дозволуваат измени во **Администрир. на систем** > **Ограничувања**.

Најавете се како администратор од контролната табла

Може да користите кој било од следниве начини за да се најавите како администратор од контролната табла на скенерот.

1. Допрете  во горниот десен агол на екранот.
   - ❏ Кога Authentication Settings е овозможено, иконата се прикажува на екранот **Добредојдовте** (екранот во мирување за автентикација).
   - ❏ Кога Authentication Settings е оневозможено, иконата се прикажува на почетниот екран.
2. Допрете **Да** кога ќе се прикаже екранот за потврда.
3. Внесете ја администраторската лозинка.

   Се прикажува порака што ве известува дека најавувањето е извршено, а потоа се прикажува почетниот екран на контролната табла.

За да се одјавите, допрете  во горниот десен агол на почетниот екран.

Оневозможување на надворешниот интерфејс

Може да го оневозможите интерфејсот што се користи за поврзување на уредот со скенерот. Одредете ги поставките за ограничување, за да спречите скенирање што не се одвива преку мрежа.

Белешка:
Поставките за ограничување може да ги одредите и преку контролната табла на скенерот.

*Врска со компјутер преку USB : **Поставки** > **Осн поставки** > **Врска со компјутер преку USB***

1. Одете на Web Config и изберете ја картичката **Product Security** > **External Interface**.
2. Изберете **Disable** на функциите што сакате да ги поставите.

   Изберете **Enable** кога сакате да го откажете контролирањето.

   Врска со компјутер преку USB

   Може да ја ограничите употребата на USB-врската од компјутерот. Ако сакате да ја ограничите, изберете **Disable**.

3. Кликнете **OK**.

4. Уверете се дека оневозможената порта не може да се користи.

   Врска со компјутер преку USB

   Ако двигателот бил инсталиран на компјутерот

   Поврзете го скенерот со компјутерот користејќи USB-кабел, а потоа потврдете дека скенерот не скенира.

   Ако двигателот не бил инсталиран на компјутерот

   Windows:

   Отворете го управникот со уреди и оставете го отворен, поврзете го скенерот со компјутерот користејќи USB-кабел, а потоа проверете дали содржините прикажани во управникот со уреди остануваат непроменети.

   Mac OS:

   Поврзете го скенерот со компјутерот користејќи USB-кабел, а потоа потврдете дека не може да го додадете скенерот од **Печатачи и скенери**.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Надгледување далечински скенер

Проверување информации за далечински скенер

Следниве информации за скенерот што работи може да ги проверите преку **Status** со Web Config.

- ❏ Product Status

  Проверете ги статусот, услугата во облак, бројот на производот, MAC-адресата итн.

- ❏ Network Status

  Проверете ги информациите за статусот на мрежната врска, IP-адресата, DNS-серверот итн.

- ❏ Usage Status

  Проверете ги скенирањата, бројот на скенирања итн., за првиот ден.

- ❏ Hardware Status

  Проверете го статусот на секоја функција на скенерот.

- ❏ Panel Snapshot

  Прикажува слика од екранот прикажана на контролната табла на скенерот.

Примање на известувања на е-пошта кога ќе има настани

Во врска со известувањата на е-пошта

Ова е функцијата за известување што испраќа е-порака до наведената адреса при настани како што се прекинување на скенирањето и грешка на скенерот.

Може да регистрирате до пет одредишта и да ги поставите поставките за известување за секое одредиште.

За да ја користите функцијава, треба да го поставите серверот за пошта пред да ги поставувате известувањата.

Поврзани информации

➡ „Конфигурирање сервер за е-пошта“ на страница 45

Конфигурирање известување преку е-пошта

Конфигурирајте го известувањето преку е-пошта користејќи Web Config.

1. Одете на Web Config и изберете ја картичката **Device Management** > **Email Notification**.
2. Наведете го предметот на известувањето преку е-пошта.

   Изберете ги содржините за прикажување во предметот од двете паѓачки менија.

   - ❏ Избраните содржини се прикажуваат до **Subject**.
   - ❏ Истите содржини не може да се поставуваат одлево и оддесно.
   - ❏ Кога бројот на знаци во **Location** надминува 32 бајти, знаците што надминуваат 32 бајти се изземаат.
3. Внесете ја адресата на е-пошта за испраќање на известувањето преку е-пошта.

   Користете A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @, и внесете од 1 до 255 знаци.
4. Изберете го јазикот за известувањата преку е-пошта.
5. Изберете го полето за избор на настанот за којшто сакате да добиете известување.

   Бројот на **Notification Settings** е поврзан со бројот на дестинации во **Email Address Settings**.

   Пример:

   Ако сакате да се испрати известување до адресата на е-пошта поставена за бројот 1 во **Email Address Settings** кога администраторската лозинка е променета, изберете го полето за избор за колоната **1** во редот **Administrator password changed**.
6. Кликнете **OK**.

   Потврдете дека сакате да се испрати известување преку е-пошта за одреден настан.

   На пример: администраторската лозинка е променета.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Ставки за известување преку е-порака

Ставки	Поставки и објаснувања
Administrator password changed	Известување кога администраторската лозинка е променета.
Scanner error	Известување кога се јавува грешка на скенерот.
Грешка на Wi-Fi	Известување кога се јавува грешка на безжичниот LAN-интерфејс.

Решавање проблеми

Ја заборавивте администраторската лозинка

Ви треба помош од сервисен персонал. Контактирајте со локалниот дистрибутер.

Белешка:
Подолу се наведени почетните вредности за администраторот на Web Config.

❏ *Корисничко име: нема (празно)*

❏ *Лозинка: серискиот број на скенерот*

За да го најдете серискиот број, проверете ја етикетата залепена на задниот дел од скенерот. Ако ги вратите стандардните вредности за администраторската лозинка, таа ќе се ресетира на почетните вредности.

Напредни поставки за безбедност

Безбедносни поставки и спречување опасност

Кога скенер е поврзан со мрежа, може да му пристапите од оддалечена локација. Покрај тоа, многу луѓе може да го споделуваат скенерот, што е корисно за подобрувањето на оперативната ефикасност и погодност. Меѓутоа, така се зголемуваат ризиците како што се незаконски пристап, незаконска употреба и неовластени измени на податоците. Ако го користите скенерот во средина каде што може да пристапувате до интернет, ризиците се уште поголеми.

Ако скенерот нема заштита од надворешен пристап, ќе биде можно преку интернет да се читаат контактите зачувани во скенерот.

За да се избегне овој ризик, скенерите Epson имаат разни безбедносни технологии.

Поставете го скенерот како што е потребно, според условите на средината одредени согласно информациите за средината на клиентот.

Име	Тип на функцијата	Што да поставите	Што да спречите
Контрола на протоколи	Ги контролира протоколите и услугите што треба да се користат за комуникација меѓу скенери и компјутери и овозможува и оневозможува функции.	Протокол или услуга што се применува за одделно дозволени или забранети функции.	Ги намалува безбедносните ризици што може да настанат со ненамерна употреба, спречувајќи ги корисниците да употребуваат непотребни функции.
SSL/TLS-комуникации	Комуникациските содржини се шифрирани со SSL/TLS-комуникации кога се пристапува до серверот Epson на интернет од скенерот, на пр. при комуницирањето со компјутер преку веб-прелистувач со помош на Epson Connect и при ажурирањето на фирмверот.	Стекнете се со CA потпишан сертификат и потоа импортирајте го во скенерот.	Со одобрувањето на идентификацијата на скенерот преку сертификатот потпишан од CA се спречува лажно претставување и неовластен пристап. Покрај тоа, комуникациските содржини на SSL/TLS се заштитени и се спречува упад во податоците од скенирањето и поставувањето.
IPsec/IP-филтрирање	Може да поставите да биде дозволено одвојувањето и прекинувањето на податоците што се од одреден клиент или од одреден вид. Бидејќи IPsec ги заштитува податоците преку единица со IP-пакет (шифрирање и автентикација), може безбедно да комуницирате небезбеден протокол.	Создајте основно правило и поединечно правило за да ги одредите клиентот или типот податоци што може да пристапуваат до скенерот.	Спречете неовластен пристап, менување и пресретнување на комуникациските податоци до скенерот.

Име	Тип на функцијата	Што да поставите	Што да спречите
IEEE 802.1X	Дозволува само автентицирани корисници да се поврзуваат на мрежата. Дозволува само одобрен корисник да го користи скенерот.	Поставка за автентикација за RADIUS-сервер (сервер за автентикација).	Спречува неовластен пристап и употреба на скенерот.

Поврзани информации

- „Контролирање на користењето протоколи“ на страница 102
- „SSL/TLS комуникација со скенер“ на страница 111
- „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 112
- „Поврзување на скенерот на IEEE802.1X мрежа“ на страница 124

Поставки за безбедносни функции

Кога поставувате IPsec/IP-филтрирање или IEEE 802.1X, се препорачува да пристапите до Web Config користејќи SSL/TLS за пренесување на информациите за поставките со цел да се намалат безбедносните ризици, како што се неовластени измени или пресретнување на податоците.

Погрижете се да ја конфигурирате администраторската лозинка пред да поставите IPsec/IP-филтрирање или IEEE 802.1X.

Контролирање на користењето протоколи

Може да скенирате со користење на разни патеки и протоколи. Исто така, може да користите мрежно скенирање од неодреден број компјутери на мрежата.

Може да ги намалите ненамерните безбедносни ризици со ограничување на скенирањето од одредени патеки или со контролирање на достапните функции.

Контрола на протоколи

Конфигурирајте ги поставките за протоколи поддржани од скенерот.

1. Одете на Web Config, а потоа изберете ја картичката **Network Security** tab > **Protocol**.
2. Конфигурирајте ги сите ставки.
3. Кликнете **Next**.
4. Кликнете **OK**.

   Поставките се увезуваат во скенерот.

Поврзани информации

- „Извршување Web Config на веб-прелистувач“ на страница 38

Протоколи што може да ги овозможите или оневозможите

Протокол	Опис
Bonjour Settings	Може да одредите дали да се користи Bonjour. Bonjour се користи за уреди, скенирање итн.
SLP Settings	Може да ја овозможите или оневозможите функцијата SLP. SLP се користи за push-скенирање и мрежно пребарување во EpsonNet Config.
WSD Settings	Може да ја овозможите или оневозможите функцијата WSD. Кога ова е овозможено, може да додавате уреди со WSD и да скенирате од WSD-портата.
LLTD Settings	Може да ја овозможите или оневозможите функцијата LLTD. Кога ова е овозможено, се прикажува на мрежната карта на Windows.
LLMNR Settings	Може да ја овозможите или оневозможите функцијата LLMNR. Кога ова е овозможено, може да користите разрешување на имиња без NetBIOS, дури и ако не може да користите DNS.
SNMPv1/v2c Settings	Може да одредите дали да се овозможи SNMPv1/v2c. Ова се користи за поставување уреди, надгледување итн.
SNMPv3 Settings	Може да одредите дали да се овозможи SNMPv3. Ова се користи за поставување шифрирани уреди, надгледување итн.

Поставки за протокол

Bonjour Settings

Ставки	Вредност за поставката и опис
Use Bonjour	Изберете го ова за да пребарувате или да користите уреди преку Bonjour.
Bonjour Name	Го прикажува името Bonjour.
Bonjour Service Name	Го прикажува името на услугата Bonjour.
Location	Го прикажува името на локацијата Bonjour.
Wide-Area Bonjour	Поставете дали да се користи Wide-Area Bonjour.

SLP Settings

Ставки	Вредност за поставката и опис
Enable SLP	Изберете го ова за да се овозможи функцијата SLP. Ова се користи за мрежно пребарување во EpsonNet Config.

WSD Settings

Ставки	Вредност за поставката и опис
Enable WSD	Изберете го ова за да овозможите додавање уреди со WSD, како и скенирање од WSD-портата.
Scanning Timeout (sec)	Внесете ја вредноста за истекот на времето за комуникација за WSD-скенирање (од 3 до 3.600 секунди).
Device Name	Го прикажува името на WSD-уредот.
Location	Го прикажува името на локацијата WSD.

LLTD Settings

Ставки	Вредност за поставката и опис
Enable LLTD	Изберете го ова за да овозможите LLTD. Скенерот е прикажан во Windows мапата на мрежа.
Device Name	Го прикажува името на LLTD-уредот.

LLMNR Settings

Ставки	Вредност за поставката и опис
Enable LLMNR	Изберете го ова за да овозможите LLMNR. Може да користите разрешување на имиња без NetBIOS, дури и ако не може да користите DNS.

SNMPv1/v2c Settings

Ставки	Вредност за поставката и опис
Enable SNMPv1/v2c	Изберете за да овозможите SNMPv1/v2c.
Access Authority	Поставете го издавачот на пристап кога е овозможено SNMPv1/v2c. Изберете **Read Only** или **Read/Write**.
Community Name (Read Only)	Внесете од 0 до 32 ASCII (од 0x20 до 0x7E) знаци.
Community Name (Read/Write)	Внесете од 0 до 32 ASCII (од 0x20 до 0x7E) знаци.

SNMPv3 Settings

Ставки	Вредност за поставката и опис
Enable SNMPv3	SNMPv3 е овозможено кога полето е штиклирано.
User Name	Внесете од 1 до 32 знаци користејќи 1-бајтни знаци.
Authentication Settings	

Ставки		Вредност за поставката и опис
	Algorithm	Изберете алгоритам за автентикација за SNMPv3.
	Password	Внесете ја лозинката за автентикација за SNMPv3. Внесете од 8 до 32 знаци во ASCII (0x20–0x7E). Во спротивно, оставете го полево празно.
	Confirm Password	За да потврдите, внесете ја лозинката што ја конфигуриравте.
Encryption Settings		
	Algorithm	Изберете алгоритам за шифрирање за SNMPv3.
	Password	Внесете ја лозинката за шифрирање за SNMPv3. Внесете од 8 до 32 знаци во ASCII (0x20–0x7E). Во спротивно, оставете го полево празно.
	Confirm Password	За да потврдите, внесете ја лозинката што ја конфигуриравте.
Context Name		Внесете до 32 знаци или помалку во Unicode (UTF-8). Во спротивно, оставете го полево празно. Бројот на знаци што може да се внесат варира зависно од јазикот.

Користење на дигитален сертификат

За дигиталната сертификација

❏ CA-signed Certificate

Ова е сертификат потпишан од CA (Издавач на сертификати). Може да го добиете за да аплицирате до Издавачот на сертификати. Сертификатот го потврдува постоењето на скенерот и се користи за комуникација SSL/TLS, за да се овозможи безбедност на податочните комуникации.

Кога се користи за комуникација SSL/TLS, се користи како сертификат на сервер.

Кога е поставен на филтрирање IPsec/IP или комуникација IEEE 802.1x, се користи како сертификат за клиент.

❏ Сертификат од CA

Ова е сертификат во рамки на CA-signed Certificate, исто така наречен среден сертификат од CA. Се користи од веб-прелистувачот за да се потврди патеката на сертификатот на скенерот кога се пристапува до серверот на другата страна или до Web Config.

За сертификатот од CA, поставете кога да се потврди патеката на сертификатот на серверот при пристапување од скенерот. За скенерот, поставете да се потврди патеката на CA-signed Certificate за врска SSL/TLS.

Може да го добиете сертификатот од CA на скенерот од Издавачот на сертификати (CA) каде што е издаден сертификат од CA.

Исто така, може да го добиете сертификатот од CA што се користи за потврдување на серверот на другата страна од Издавачот на сертификати што издал CA-signed Certificate на другиот сервер.

❏ Self-signed Certificate

Ова е сертификат што го потпишува и издава самиот скенер. Се нарекува и основен сертификат. Бидејќи издавачот се потврдува себеси, тоа не е веродостојно и не може да спречи лажно претставување.

Користете го кога ја одредувате поставката за безбедност и при едноставна комуникација SSL/TLS без CA-signed Certificate.

Ако го користите овој сертификат за комуникација SSL/TLS, може да се прикаже безбедносно предупредување на прелистувачот бидејќи сертификатот не е регистриран на прелистувач. Може да користите Self-signed Certificate само за комуникација SSL/TLS.

Поврзани информации

➡ „Конфигурирање CA-signed Certificate“ на страница 106
➡ „Ажурирање самопотпишан сертификат“ на страница 109
➡ „Конфигурирање CA Certificate“ на страница 110

Конфигурирање CA-signed Certificate

Добивање на ИС потпишан сертификат

За да добиете ИС потпишан сертификат, креирајте CSR (Барање за потпишување на сертификат) и применете го на издавачот на сертификати. Може да креирате CSR со користење на Web Config и компјутерот.

Следете ги чекорите за да креирате CSR и за да добиете ИС потпишан сертификат со користење на Web Config. Кога креирате CSR со користење на Web Config, сертификатот е во PEM/DER формат.

1. Пристапете до Web Config, а потоа изберете го јазичето **Network Security**. Следно, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.

   Што и да изберете, може да го добиете истиот сертификат и да го користите како заеднички.

2. Кликнете на **Generate** од **CSR**.

   Се отвора страница за креирање на CSR.

3. Внесете вредност за секоја ставка.

   Белешка:
   Достапните должина на клуч и кратенките се разликуваат во зависност од издавачот на сертификати. Креирајте барање во согласност со правилата на секој издавач на сертификати.

4. Кликнете на **OK**.

   Се прикажува порака за комплетирање.

5. Изберете ја картичката **Network Security**. Следно, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.

6. Кликнете на едно од копчињата за преземање на **CSR** според одредениот формат од секој издавач на сертификати за да го преземете CSR на компјутер.

> ***Важно:***
>
> *Не генерирајте го CSR повторно. Ако го направите тоа, можно е да не може да го увезете издадениот CA-signed Certificate.*

7. Испратете го CSR на издавач на сертификати и добијте CA-signed Certificate.

   Следете ги правилата на секој издавач на сертификати за методот и формата на испраќање.

8. Зачувајте го издадениот CA-signed Certificate на компјутер поврзан на скенер.

   Добивањето на CA-signed Certificate е комплетирано кога ќе го зачувате сертификатот во дестинација.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Поставки за CSR

Ставки	Поставки и објаснувања
Key Length	Изберете должина на клучот за CSR.
Common Name	Може да внесете од 1 до 128 знаци. Ако ова е IP-адреса, треба да биде статична IP-адреса. Може да внесете од една до пет IPv4-адреси, IPv6-адреси, имиња на хостови и FQDN-и, одделувајќи ги со запирки. Првиот елемент се зачувува во заедничкото име, а другите елементи се зачувуваат во полето за алијас на предметот на сертификатот. Пример: IP-адреса на скенерот: 192.0.2.123, име на скенерот: EPSONA1B2C3 Common Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organization/ Organizational Unit/ Locality/ State/Province	Може да внесете од 0 до 64 знаци во ASCII (0x20–0x7E). Може да ги одвојувате различните имиња со запирки.
Country	Внесете код за земја со двоцифрен број одреден од ISO-3166.
Sender's Email Address	Може да ја внесете адресата на е-пошта на испраќачот во поставката за серверот за е-пошта. Внесете ја истата адреса на е-пошта како **Sender's Email Address** во картичката **Network** > **Email Server** > **Basic**.

Увезување сертификат потпишан од CA

Увезете го добиениот CA-signed Certificate во скенерот.

Важно:

- *Погрижете се дека датумот и времето на скенерот се точно поставени. Сертификатот може да е неважечки.*
- *Ако добивате сертификат користејќи CSR создадено од Web Config, може да го увезете сертификатот само еднаш.*

1. Одете на Web Config, а потоа изберете ја картичката **Network Security**. Потоа, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.

2. Кликнете **Import**

   Се отвора страница за увезување сертификат.

3. Внесете вредност за секоја ставка. Поставете **CA Certificate 1** и **CA Certificate 2** кога ја потврдувате патеката на сертификатот на веб-прелистувачот што пристапува до скенерот.

   Во зависност од тоа каде создавате CSR и од форматот на датотеката на сертификатот, потребните поставки може да се разликуваат. Внесете вредности за потребните ставки според следново.

   - Сертификат во формат PEM/DER добиен од Web Config
     - **Private Key**: не конфигурирајте затоа што скенерот содржи приватен клуч.
     - **Password**: не конфигурирајте.
     - **CA Certificate 1**/**CA Certificate 2**: Изборно
   - Сертификат во формат PEM/DER добиен од компјутер
     - **Private Key**: треба да го поставите.
     - **Password**: не конфигурирајте.
     - **CA Certificate 1**/**CA Certificate 2**: Изборно
   - Сертификат во формат PKCS#12 добиен од компјутер
     - **Private Key**: не конфигурирајте.
     - **Password**: изборно
     - **CA Certificate 1**/**CA Certificate 2**: Не конфигурирајте.

4. Кликнете **OK**.

   Се прикажува порака за завршување.

Белешка:
*Кликнете **Confirm** за потврдување на информациите на сертификатот.*

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Поставки за увезување сертификат потпишан од CA

Ставки	Поставки и објаснувања
Server Certificate или Client Certificate	Изберете формат на сертификат. За врска SSL/TLS, се прикажува Server Certificate. За IPsec/IP-филтрирање или IEEE 802.1X, се прикажува Client Certificate.
Private Key	Ако добивате сертификат во формат PEM/DER користејќи CSR создадено од компјутер, одредете соодветна датотека со приватен клуч за сертификатот.
Password	Ако форматот на датотеката е **Certificate with Private Key (PKCS#12)**, внесете ја лозинката за шифрирање на приватниот клуч што се поставува кога го добивате сертификатот.
CA Certificate 1	Ако форматот на сертификатот е **Certificate (PEM/DER)**, увезете сертификат од издавач на сертификати што издава CA-signed Certificate користен како сертификат за сервер. Ако е потребно, одредете датотека.
CA Certificate 2	Ако форматот на сертификатот е **Certificate (PEM/DER)**, увезете сертификат од издавач на сертификати што издава CA Certificate 1. Ако е потребно, одредете датотека.

Бришење на ИС потпишан сертификат

Може да избришете внесен сертификат ако сертификатот е застарен или кога шифрираната конекција повеќе не е потребна.

Важно:

Ако добиете сертификат со користење на CSR креиран од Web Config, не може повторно да го внесете избришаниот сертификат.Во овој случај, креирајте CSR и повторно добијте го сертификатот.

1. Пристапете до Web Config, а потоа изберете го јазичето **Network Security**.Следно, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.
2. Кликнете **Delete**.
3. Потврдете дека сакате да го избришете сертификатот во прикажаната порака.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Ажурирање самопотпишан сертификат

Бидејќи Self-signed Certificate се издава од скенерот, може да го ажурирате кога ќе истече или кога опишаната содржина ќе се промени.

1. Одете на Web Config и изберете ја картичката **Network Security** tab > **SSL/TLS** > **Certificate**.
2. Кликнете **Update**.
3. Внесете **Common Name**.

   Може да внесете до 5 адреси IPv4, адреси IPv6, имиња на хост, FQDN-и што содржат од 1 до 128 знаци, одделувајќи ги со запирки. Првиот параметар се зачувува во заедничкото име, а другите се зачувуваат во полето за алијас на предметот на сертификатот.

   Пример:

   IP-адреса на скенерот: 192.0.2.123, име на скенерот: EPSONA1B2C3

   Заедничко име: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Одредете период на важност за сертификатот.
5. Кликнете **Next**.

   Се прикажува порака за потврда.
6. Кликнете **OK**.

   Скенерот е ажуриран.

Белешка:
*Информациите за сертификатот може да ги проверите преку картичката **Network Security** > **SSL/TLS** > **Certificate** > **Self-signed Certificate**, а потоа да кликнете на **Confirm**.*

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Конфигурирање CA Certificate

Кога ќе поставите CA Certificate, може да ја потврдите патеката до сертификатот од CA на серверот до којшто пристапува скенерот. Така може да спречите лажно претставување.

Може да добиете CA Certificate од издавачот на сертификати каде што е издаден CA-signed Certificate.

Увезување CA Certificate

Увезете CA Certificate во скенерот.

1. Одете на Web Config, а потоа изберете ја картичката **Network Security** > **CA Certificate**.
2. Кликнете **Import**.
3. Одредете CA Certificate што сакате да го увезете.
4. Кликнете **OK**.

Кога ќе заврши увезувањето, се прикажува екранот **CA Certificate** и увезениот CA Certificate.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Бришење CA Certificate

Може да го избришете увезениот CA Certificate.

1. Одете на Web Config, а потоа изберете ја картичката **Network Security** > **CA Certificate**.
2. Кликнете **Delete** до CA Certificate што сакате да го избришете.
3. Во прикажаната порака, потврдете дека сакате да го избришете сертификатот.
4. Кликнете **Reboot Network**, а потоа уверете се дека избришаниот сертификат од CA не е наведен во ажурираниот екран.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

SSL/TLS комуникација со скенер

Кога сертификатот на серверот е поставен со SSL/TLS (Secure Sockets Layer/Transport Layer Security) комуникација со скенерот, можете да ја шифрирате патеката на комуникација меѓу компјутерите. Направете го ова ако сакате да спречите далечински и неавторизиран пристап.

Конфигурирање основни поставки за SSL/TLS

Ако скенерот поддржува функција за HTTPS-сервер, може да користите SSL/TLS-комуникација за да шифрирате комуникации. Може да го конфигурирате и да управувате со скенерот користејќи Web Config, истовремено овозможувајќи безбедност.

Конфигурирајте ги јачината на шифрирањето и функцијата за пренасочување.

1. Одете на Web Config и изберете ја картичката **Network Security** > **SSL/TLS** > **Basic**.
2. Изберете вредност за секоја ставка.
   - ❏ Encryption Strength
     Изберете ниво на јачината на шифрирањето.
   - ❏ Redirect HTTP to HTTPS
     Пренасочувајте кон HTTPS кога ќе се пристапи до HTTP.
3. Кликнете **Next**.
   Се прикажува порака за потврда.

4. Кликнете **OK**.

   Скенерот е ажуриран.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач" на страница 38

Конфигурирање сертификат на сервер за скенерот

1. Одете на Web Config и изберете ја картичката **Network Security** > **SSL/TLS** > **Certificate**.
2. Одредете сертификат за употреба на **Server Certificate**.
   - ❏ Self-signed Certificate

     Скенерот создава самопотпишан сертификат. Ако не добиете сертификат потпишан од CA, изберете го овој сертификат.
   - ❏ CA-signed Certificate

     Ако однапред добиете и увезете сертификат потпишан од CA, може да го одредите овој сертификат.
3. Кликнете **Next**.

   Се прикажува порака за потврда.
4. Кликнете **OK**.

   Скенерот е ажуриран.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач" на страница 38
➡ „Конфигурирање CA-signed Certificate" на страница 106
➡ „Конфигурирање CA Certificate" на страница 110

Комуникација со енкрипција со помош на IPsec/IP филтрирање

Во врска со IPsec/IP Filtering

Може да филтрирате сообраќај според IP-адреси, услуги и порта, со помош на функцијата за филтрирање IPsec/IP. Со комбинирање на филтрирањето може да го конфигурирате скенерот за да ги прифатите или да ги блокирате одредените клиенти или одредените податоци. Покрај тоа, може да го подобрите нивото на безбедност со користење на IPsec.

Белешка:
Компјутерите коишто имаат Windows Vista или понова верзија или Windows Server 2008 или понова верзија на поддршка за IPsec.

Конфигурирање на стандардната политика

За да филтрирате сообраќај, конфигурирајте ја стандардната политика. Стандардната политика се применува на секој корисник или група поврзана на скенерот. За подетална контрола над корисниците или групите на корисници конфигурирајте ги политиките на групата.

1. Пристапете до Web Config, а потоа изберете го јазичето **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Внесете вредност за секоја ставка.
3. Кликнете на **Next**.

   Се прикажува порака за потврда.
4. Кликнете на **OK**.

   Скенерот е ажуриран.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Поставки за Default Policy

Default Policy

Ставки	Поставки и објаснувања
IPsec/IP Filtering	Може да ја овозможите или оневозможите функцијата IPsec/IP-филтрирање.

❑ Access Control

Конфигурирајте начин на контрола за сообраќајот на IP-пакетите.

Ставки	Поставки и објаснувања
Permit Access	Изберете го ова за да дозволите да поминуваат конфигурирани IP-пакети.
Refuse Access	Изберете го ова за да одбиете да поминуваат конфигурирани IP-пакети.
IPsec	Изберете го ова за да дозволите да поминуваат конфигурирани IPsec-пакети.

❏ **IKE Version**

Изберете **IKEv1** или **IKEv2** за **IKE Version**. Изберете една од нив според уредот со кој е поврзан скенерот.

❏ IKEv1

Следниве ставки се прикажуваат кога ќе изберете **IKEv1** за **IKE Version**.

Ставки	**Поставки и објаснувања**
Authentication Method	За да изберете **Certificate**, треба претходно да добиете и увезете сертификат потпишан од CA.
Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете претходно споделен клуч што содржи од 1 до 127 знаци.
Confirm Pre-Shared Key	За да потврдите, внесете го клучот што го конфигуриравте.

❏ IKEv2

Следниве ставки се прикажуваат кога ќе изберете **IKEv2** за **IKE Version**.

Ставки		**Поставки и објаснувања**
Local	Authentication Method	За да изберете **Certificate**, треба претходно да добиете и увезете сертификат потпишан од CA.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете го типот на ID за скенерот.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не може да користите „@", „#" и „=" за првиот знак. **Distinguished Name**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „=". **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 до 255 знаци користејќи A–Z, a–z, 0–9, „-" и точка (.). **Email Address**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „@". **Key ID**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E).
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете претходно споделен клуч што содржи од 1 до 127 знаци.
	Confirm Pre-Shared Key	За да потврдите, внесете го клучот што го конфигуриравте.

Ставки		Поставки и објаснувања
Remote	Authentication Method	За да изберете **Certificate**, треба претходно да добиете и увезете сертификат потпишан од CA.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете го типот на ID за уредот за којшто сакате да извршите автентикација.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не може да користите „@", „#" и „=" за првиот знак. **Distinguished Name**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „=". **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 до 255 знаци користејќи A–Z, a–z, 0–9, „-" и точка (.). **Email Address**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „@". **Key ID**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E).
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете претходно споделен клуч што содржи од 1 до 127 знаци.
	Confirm Pre-Shared Key	За да потврдите, внесете го клучот што го конфигуриравте.

❑ Encapsulation

Ако изберете **IPsec** за **Access Control**, треба да конфигурирате режим на енкапсулација.

Ставки	Поставки и објаснувања
Transport Mode	Ако го користите скенерот само на иста LAN, изберете го ова. IP-пакетите од слојот 4 или од понов слој се шифрирани.
Tunnel Mode	Ако го користите скенерот на мрежа што поддржува интернет, како што е IPsec-VPN, изберете ја оваа опција. Заглавјето и податоците на IP-пакетите се шифрирани. **Remote Gateway(Tunnel Mode)**: ако изберете **Tunnel Mode** за **Encapsulation**, внесете адреса на капијата од 1 до 39 знаци.

❑ Security Protocol

Ако изберете **IPsec** за **Access Control**, изберете опција.

Ставки	Поставки и објаснувања
ESP	Изберете го ова за да се обезбеди интегритет на автентикацијата и податоците и за да ги шифрирате податоците.
AH	Изберете го ова за да се обезбеди интегритет на автентикацијата и податоците. Дури и ако шифрирањето на податоците е забрането, може да користите IPsec.

❑ **Algorithm Settings**

Се препорачува да изберете **Any** за сите поставки или да изберете друга ставка освен **Any** за секоја поставка. Ако изберете **Any** за некоја од поставките и изберете ставка поинаква од **Any** за другите поставки, уредот може да не комуницира во зависност од другиот уред за којшто сакате да извршите автентикација.

Ставки		Поставки и објаснувања
IKE	Encryption	Изберете го алгоритамот за шифрирање за IKE. Ставките се разликуваат во зависност од верзијата на IKE.
	Authentication	Изберете го алгоритамот за автентикација за IKE.
	Key Exchange	Изберете го алгоритамот за размена на клучеви за IKE. Ставките се разликуваат во зависност од верзијата на IKE.
ESP	Encryption	Изберете го алгоритамот за шифрирање за ESP. Ова е достапно кога **ESP** е избрано за **Security Protocol**.
	Authentication	Изберете го алгоритамот за автентикација за ESP. Ова е достапно кога **ESP** е избрано за **Security Protocol**.
AH	Authentication	Изберете го алгоритамот за шифрирање за AH. Ова е достапно кога **AH** е избрано за **Security Protocol**.

Конфигурирање на политиката на Групацијата

Политика на групата претставува едно или повеќе правила коишто се применуваат на корисник или на група на корисници. Скенерот ги контролира IP пакетите коишто се совпаѓаат со конфигурираните политики. IP пакетите се автентицираат според редоследот на политиката на групата од 1 до 10, а потоа според стандардната политика.

1. Пристапете до Web Config, а потоа изберете го јазичето **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Кликнете на нумерираното јазиче коешто сакате да го конфигурирате.
3. Внесете вредност за секоја ставка.
4. Кликнете на **Next**.

   Се прикажува порака за потврда.
5. Кликнете на **OK**.

   Скенерот е ажуриран.

Поставки за Group Policy

Ставки	Поставки и објаснувања
Enable this Group Policy	Може да овозможите или оневозможите правила за група.

Access Control

Конфигурирајте начин на контрола за сообраќајот на IP-пакетите.

Ставки	Поставки и објаснувања
Permit Access	Изберете го ова за да дозволите да поминуваат конфигурирани IP-пакети.
Refuse Access	Изберете го ова за да одбиете да поминуваат конфигурирани IP-пакети.
IPsec	Изберете го ова за да дозволите да поминуваат конфигурирани IPsec-пакети.

Local Address (Scanner)

Изберете IPv4-адреса или IPv6-адреса што соодветствува со вашата мрежна околина. Ако IP-адресата е доделена автоматски, може да изберете **Use auto-obtained IPv4 address**.

Белешка:
Ако IPv6-адресата е доделена автоматски, врската може да биде недостапна. Конфигурирајте статична IPv6-адреса.

Remote Address(Host)

Внесете ја IP-адресата на уредот за да го контролирате пристапот. IP-адресата мора да има 43 знаци или помалку. Ако не внесете IP-адреса, сите адреси се контролирани.

Белешка:
Ако IP-адресата е доделена автоматски (на пр. доделена од DHCP), врската може да биде недостапна. Конфигурирајте статична IP-адреса.

Method of Choosing Port

Изберете начин на одредување на портите.

❏ Service Name

Ако изберете **Service Name** за **Method of Choosing Port**, изберете опција.

❏ Transport Protocol

Ако изберете **Port Number** за **Method of Choosing Port**, треба да конфигурирате режим на енкапсулација.

Ставки	Поставки и објаснувања
Any Protocol	Изберете го ова за да ги контролирате сите типови протоколи.
TCP	Изберете го ова за да ги контролирате податоците за unicast.
UDP	Изберете го ова за да ги контролирате податоците за broadcast и multicast.
ICMPv4	Изберете го ова за да ја контролирате ping-наредбата.

❏ Local Port

Ако изберете **Port Number** за **Method of Choosing Port** и ако изберете **TCP** или **UDP** за **Transport Protocol**, внесете ги броевите на портите за да го контролирате приемот на пакети, одвојувајќи ги со запирки. Може да внесете најмногу 10 броеви на порти.

Пример: 20,80,119,5220

Ако не внесете број на порта, сите порти се контролирани.

❏ Remote Port

Ако изберете **Port Number** за **Method of Choosing Port** и ако изберете **TCP** или **UDP** за **Transport Protocol**, внесете ги броевите на портите за да го контролирате испраќањето на пакети, одвојувајќи ги со запирки. Може да внесете најмногу 10 броеви на порти.

Пример: 25,80,143,5220

Ако не внесете број на порта, сите порти се контролирани.

IKE Version

Изберете **IKEv1** или **IKEv2** за **IKE Version**. Изберете една од нив според уредот со кој е поврзан скенерот.

❏ IKEv1

Следниве ставки се прикажуваат кога ќе изберете **IKEv1** за **IKE Version**.

Ставки	Поставки и објаснувања
Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опција. Користениот сертификат е вообичаен со стандардно правило.
Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете претходно споделен клуч што содржи од 1 до 127 знаци.
Confirm Pre-Shared Key	За да потврдите, внесете го клучот што го конфигуриравте.

❏ IKEv2

Следниве ставки се прикажуваат кога ќе изберете **IKEv2** за **IKE Version**.

Ставки		**Поставки и објаснувања**
Local	Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опција. Користениот сертификат е вообичаен со стандардно правило.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете го типот на ID за скенерот.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не може да користите „@", „#" и „=" за првиот знак. **Distinguished Name**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „=". **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 до 255 знаци користејќи A–Z, a–z, 0–9, „-" и точка (.). **Email Address**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „@". **Key ID**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E).
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете претходно споделен клуч што содржи од 1 до 127 знаци.
	Confirm Pre-Shared Key	За да потврдите, внесете го клучот што го конфигуриравте.
Remote	Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опција. Користениот сертификат е вообичаен со стандардно правило.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете го типот на ID за уредот за којшто сакате да извршите автентикација.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не може да користите „@", „#" и „=" за првиот знак. **Distinguished Name**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „=". **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 до 255 знаци користејќи A–Z, a–z, 0–9, „-" и точка (.). **Email Address**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E). Треба да вклучите „@". **Key ID**: Внесете од 1 до 255 1-бајтни знаци ASCII (од 0x20 до 0x7E).
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете претходно споделен клуч што содржи од 1 до 127 знаци.
	Confirm Pre-Shared Key	За да потврдите, внесете го клучот што го конфигуриравте.

Encapsulation

Ако изберете **IPsec** за **Access Control**, треба да конфигурирате режим на енкапсулација.

Ставки	Поставки и објаснувања
Transport Mode	Ако го користите скенерот само на иста LAN, изберете го ова. IP-пакетите од слојот 4 или од понов слој се шифрирани.
Tunnel Mode	Ако го користите скенерот на мрежа што поддржува интернет, како што е IPsec-VPN, изберете ја оваа опција. Заглавјето и податоците на IP-пакетите се шифрирани. **Remote Gateway(Tunnel Mode)**: ако изберете **Tunnel Mode** за **Encapsulation**, внесете адреса на капијата од 1 до 39 знаци.

Security Protocol

Ако изберете **IPsec** за **Access Control**, изберете опција.

Ставки	Поставки и објаснувања
ESP	Изберете го ова за да се обезбеди интегритет на автентикацијата и податоците и за да ги шифрирате податоците.
AH	Изберете го ова за да се обезбеди интегритет на автентикацијата и податоците. Дури и ако шифрирањето на податоците е забрането, може да користите IPsec.

Algorithm Settings

Се препорачува да изберете **Any** за сите поставки или да изберете друга ставка освен **Any** за секоја поставка. Ако изберете **Any** за некоја од поставките и изберете ставка поинаква од **Any** за другите поставки, уредот може да не комуницира во зависност од другиот уред за којшто сакате да извршите автентикација.

Ставки		Поставки и објаснувања
IKE	Encryption	Изберете го алгоритамот за шифрирање за IKE. Ставките се разликуваат во зависност од верзијата на IKE.
	Authentication	Изберете го алгоритамот за автентикација за IKE.
	Key Exchange	Изберете го алгоритамот за размена на клучеви за IKE. Ставките се разликуваат во зависност од верзијата на IKE.
ESP	Encryption	Изберете го алгоритамот за шифрирање за ESP. Ова е достапно кога **ESP** е избрано за **Security Protocol**.
	Authentication	Изберете го алгоритамот за автентикација за ESP. Ова е достапно кога **ESP** е избрано за **Security Protocol**.
AH	Authentication	Изберете го алгоритамот за шифрирање за AH. Ова е достапно кога **AH** е избрано за **Security Protocol**.

Комбинација на Local Address (Scanner) и Remote Address(Host) на Group Policy

		Поставување на Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Поставување на Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Празно место	✓	✓	✓

*1 Ако е избрано **IPsec** за **Access Control**, не може да одредите во должина на префикс.

*2 Ако е избрано **IPsec** за **Access Control**, може да изберете линк-локална адреса (fe80::), но политиката на групата ќе биде оневозможена.

*3 Освен IPv6 линк локални адреси.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Имиња на услуги во правила за група

Белешка:
Недостапните услуги се прикажани, но не може да се изберат.

Име на услугата	Тип протокол	Број на локална порта	Број на далечинска порта	Контролирани функции
Any	–	–	–	Сите услуги
ENPC	UDP	3289	Која било порта	Пребарување скенер од апликации како што се Epson Device Admin и двигател за скенер
SNMP	UDP	161	Која било порта	Вчитување и конфигурирање MIB од апликации како што се Epson Device Admin и двигателот за скенерот Epson
WSD	TCP	Која било порта	5357	Контролирање WSD
WS-Discovery	UDP	3702	Која било порта	Пребарување WSD-скенери
Network Scan	TCP	1865	Која било порта	Проследување скенирани податоци од Document Capture Pro
Network Push Scan	TCP	Која било порта	2968	Вчитување информации за задача за push-скенирање од Document Capture Pro
Network Push Scan Discovery	UDP	2968	Која било порта	Пребарување компјутер од скенерот

Име на услугата	Тип протокол	Број на локална порта	Број на далечинска порта	Контролирани функции
FTP Data (Remote)	TCP	Која било порта	20	FTP-клиент (проследување скенирани податоци) Меѓутоа, ова може да контролира само FTP-сервер што користи далечинска порта со број 20.
FTP Control (Remote)	TCP	Која било порта	21	FTP-клиент (контролирање на проследувањето скенирани податоци)
CIFS (Remote)	TCP	Која било порта	445	CIFS-клиент (проследување скенирани податоци во папка)
NetBIOS Name Service (Remote)	UDP	Која било порта	137	CIFS-клиент (проследување скенирани податоци во папка)
NetBIOS Datagram Service (Remote)	UDP	Која било порта	138	
NetBIOS Session Service (Remote)	TCP	Која било порта	139	
HTTP (Local)	TCP	80	Која било порта	HTTP(S)-сервер (проследување податоци од Web Config и WSD)
HTTPS (Local)	TCP	443	Која било порта	
HTTP (Remote)	TCP	Која било порта	80	HTTP(S)-клиент (ажурирање на фирмверот и коренскиот сертификат)
HTTPS (Remote)	TCP	Која било порта	443	

Примери за конфигурирање IPsec/IP Filtering

Примање само IPsec-пакети

Овој пример служи само за конфигурирање на стандардното правило.

Default Policy:

- ❏ **IPsec/IP Filtering**: **Enable**
- ❏ **Access Control**: **IPsec**
- ❏ **Authentication Method**: **Pre-Shared Key**
- ❏ **Pre-Shared Key**: внесете до 127 знаци.

Group Policy: не конфигурирајте.

Примање податоци за скенирање и поставки за скенерот

Овој пример овозможува пренос на податоци за скенирање и конфигурација на скенер од одредени услуги.

Default Policy:

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

Group Policy:

- **Enable this Group Policy**: изберете го полето.
- **Access Control**: **Permit Access**
- **Remote Address(Host)**: IP-адреса на клиент
- **Method of Choosing Port**: **Service Name**
- **Service Name**: изберете го полето на **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)** и **Network Scan**.

Пристап само од одредена IP-адреса

Овој пример дозволува одредена IP-адреса да пристапува до скенерот.

Default Policy:

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

Group Policy:

- **Enable this Group Policy**: изберете го полето.
- **Access Control**: **Permit Access**
- **Remote Address(Host)**: IP-адреса на клиент на администратор

Белешка:
Без оглед на конфигурацијата на правилото, клиентот ќе може да пристапува до скенерот и да го конфигурира.

Конфигурирање сертификат за IPsec/IP-филтрирање

Конфигурирајте го сертификатот на клиентот за IPsec/IP-филтрирање. Кога ќе го поставите сертификатот, може да го користите како метод за автентикација за IPsec/IP-филтрирање. Ако сакате да го конфигурирате издавачот на сертификати, одете на **CA Certificate**.

1. Одете на Web Config, а потоа изберете ја картичката **Network Security** > **IPsec/IP Filtering** > **Client Certificate**.

2. Увезете го сертификатот во **Client Certificate**.

   Ако веќе имате увезено сертификат објавен од издавач на сертификати, може да го копирате сертификатот и да го употребите во IPsec/IP-филтрирање. За да го копирате, изберете го сертификатот од **Copy From**, а потоа кликнете **Copy**.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38
➡ „Конфигурирање CA-signed Certificate“ на страница 106
➡ „Конфигурирање CA Certificate“ на страница 110

Поврзување на скенерот на IEEE802.1X мрежа

Конфигурирање на IEEE 802.1X мрежа

Кога ќе поставите IEEE 802.1X за скенерот, може да го користите на мрежата поврзана со RADIUS-сервер, на LAN-преклопник со функција за автентикација или точка за пристап.

1. Пристапете до Web Config, а потоа изберете го јазичето **Network Security** > **IEEE802.1X** > **Basic**.

2. Внесете вредност за секоја ставка.

   Ако сакате да го користите скенерот на Wi-Fi мрежа, кликнете на **Wi-Fi Setup** и изберете или внесете SSID.

   Белешка:
   Може да споделувате поставки помеѓу Ethernet и Wi-Fi.

3. Кликнете на **Next**.

   Се прикажува порака за потврда.

4. Кликнете на **OK**.

   Скенерот е ажуриран.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Поставки за мрежа со IEEE 802.1X

Ставки	Поставки и објаснувања
IEEE802.1X (Wired LAN)	Може да ги овозможувате или оневозможувате поставките на страницата (**IEEE802.1X** > **Basic**) за IEEE802.1X (жична LAN).
IEEE802.1X (Wi-Fi)	Се прикажува статусот за врската на IEEE802.1X (Wi-Fi).
Connection Method	Се прикажува начинот на поврзување на тековната мрежа.

Ставки	Поставки и објаснувања	
EAP Type	Изберете опција за начин на автентикација меѓу скенерот и RADIUS-сервер.	
	EAP-TLS	Треба да добиете и увезете сертификат потпишан од CA.
	PEAP-TLS	
	PEAP/MSCHAPv2	Треба да конфигурирате лозинка.
	EAP-TTLS	
User ID	Конфигурирајте ID за користење за автентикација на RADIUS-сервер. Внесете од 1 до 128 1-бајтни знаци ASCII (од 0x20 до 0x7E).	
Password	Конфигурирајте лозинка за автентикација на скенерот. Внесете од 1 до 128 1-бајтни знаци ASCII (од 0x20 до 0x7E). Ако користите Windows-сервер како RADIUS-сервер, може да внесете до 127 знаци.	
Confirm Password	За да потврдите, внесете ја лозинката што ја конфигуриравте.	
Server ID	Може да конфигурирате ID на серверот за да се изврши автентикација со одреден RADIUS-сервер. Authenticator проверува дали има ID на сервер во полето subject/subjectAltName во сертификатот на сервер што се испраќа од RADIUS-сервер. Внесете од 0 до 128 1-бајтни знаци ASCII (од 0x20 до 0x7E).	
Certificate Validation	Може да поставите проверка на сертификатот без оглед на начинот на автентикација. Увезете го сертификатот во **CA Certificate**.	
Anonymous Name	Ако изберете **PEAP-TLS** или **PEAP/MSCHAPv2** за **EAP Type**, може да конфигурирате анонимно име наместо ID на корисник за фаза 1 од автентикација PEAP. Внесете од 0 до 128 1-бајтни знаци ASCII (од 0x20 до 0x7E).	
Encryption Strength	Може да изберете од следново.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Конфигурирање сертификат за IEEE 802.1X

Конфигурирајте го сертификатот на клиент за IEEE802.1X. Кога ќе го поставите, може да користите **EAP-TLS** и **PEAP-TLS** како метод за автентикација на IEEE 802.1X. Ако сакате да го конфигурирате сертификатот од издавачот на сертификати, одете на **CA Certificate**.

1. Одете на Web Config, а потоа изберете ја картичката **Network Security** > **IEEE802.1X** > **Client Certificate**.

2. Внесете сертификат во **Client Certificate**.

   Ако веќе имате увезено сертификат објавен од издавач на сертификати, може да го копирате сертификатот и да го употребите во IEEE802.1X. За да го копирате, изберете го сертификатот од **Copy From**, а потоа кликнете **Copy**.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

Решавање проблеми за напредна безбедност

Враќање на безбедносните поставки

Кога ќе воспоставите безбедна средина како што е IPsec/IP-филтрирање, можеби нема да може да комуницирате со уредите поради неправилни поставки или проблеми со уредот или серверот. Во тој случај, вратете ги безбедносните поставки за повторно да ги одредите поставките за уредот или за да ви се дозволи привремена употреба.

Оневозможување на безбедносната функција користејќи Web Config

Може да оневозможите IPsec/IP Filtering користејќи Web Config.

1. Одете на Web Config и изберете ја картичката **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Оневозможете **IPsec/IP Filtering**.

Проблеми со користење на функциите за безбедност на мрежа

Сте го заборавиле претходно споделениот клуч

Реконфигурирајте претходно споделен клуч.

За промена на клучот, пристапете на Web Config и изберете го јазичето **Network Security** > **IPsec/IP Filtering** > **Basic** > **Default Policy** или **Group Policy**.

Кога го менувате споделениот клуч, конфигурирајте го споделениот клуч за компјутери.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38
➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 112

Не може да комуницирате со IPsec-комуникација

Наведете го алгоритамот што скенерот или компјутерот не го поддржуваат.

Скенерот ги поддржува следниве алгоритми. Проверете ги поставките на компјутерот.

Безбедносни методи	Алгоритми
IKE-алгоритам за шифрирање	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-алгоритам за автентикација	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE-алгоритам за размена на клучеви	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-алгоритам за шифрирање	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-алгоритам за автентикација	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-алгоритам за автентикација	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* достапно само за IKEv2

Поврзани информации

➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 112

Одненадеж не може да комуницирате

IP-адресата на скенерот е сменета или не може да се користи.

Кога IP-адресата регистрирана на локалната адреса на Group Policy е сменета или не може да се користи, не може да се врши комуникација IPsec. Оневозможете го IPsec од контролната табла на скенерот.

Ако DHCP е застарен, рестартирањето или IPv6 адресата е застарена или не е добиена, тогаш IP адресата регистрирана за скенерот Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) може да не биде пронајдена.

Користете статична IP адреса.

IP-адресата на компјутерот е сменета или не може да се користи.

Кога IP-адресата регистрирана на далечинската адреса на Group Policy е сменета или не може да се користи, не може да се врши комуникација IPsec.

Оневозможете го IPsec од контролната табла на скенерот.

Ако DHCP е застарен, рестартирањето или IPv6 адресата е застарена или не е добиена, тогаш IP адресата регистрирана за скенерот Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) може да не биде пронајдена.

Користете статична IP адреса.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач“ на страница 38

➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 112

Не може да се поврзете откако ќе го конфигурирате IPsec/IP филтрирањето

Поставките за IPsec/IP филтрирање се погрешни.

Оневозможете го IPsec/IP филтрирањето од контролната табла на скенерот. Поврзете ги скенерот и компјутерот и повторно направете ги поставките за IPsec/IP филтрирање.

Поврзани информации

➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 112

Не може да го конфигурирате скенерот по конфигурирање на IEEE 802.1X

Поставките за IEEE 802.1X се погрешни.

Оневозможете ги IEEE 802.1X и Wi-Fi од контролната табла на скенерот. Поврзете ги скенерот и компјутерот и повторно конфигурирајте ја IEEE 802.1X.

Поврзете ги скенерот и компјутерот и повторно конфигурирајте ја IEEE 802.1X.

Поврзани информации

➡ „Конфигурирање на IEEE 802.1X мрежа“ на страница 124

Проблеми со користење на дигитален сертификат

Не може да се увезе CA-signed Certificate

CA-signed Certificate и информациите на CSR не се совпаѓаат.

Ако CA-signed Certificate и CSR ги немаат истите информации, не може да го увезете CSR. Проверете го следново:

❏ Дали се обидувате да увезете сертификат на уред којшто ги нема истите информации?

Проверете ги информациите на CSR па потоа увезете го сертификатот на уредот којшто ги има истите информации.

❏ Дали сте го презапишале CSR зачуван во скенерот откако сте го испратиле CSR на издавачите на сертификати?

Повторно добијте потпишан ИС сертификат со CSR.

CA-signed Certificate има повеќе од 5 KB.

Не може да увезете CA-signed Certificate што има повеќе од 5 KB.

Лозинката за увезување на сертификатот е погрешна.

Внесете ја точната лозинка. Ако сте ја заборавиле лозинката, не може да го увезете сертификатот. Добијте повторно CA-signed Certificate.

Поврзани информации

➡ „Увезување сертификат потпишан од CA“ на страница 107

Не може да го ажурирате самопотпишаниот сертификат

Не е внесено Common Name.

Мора да внесете **Common Name**.

Внесени се неподдржани знаци за Common Name.

Внесете од 1 до 128 знака од IPv4, IPv6, име на главен компјутер или FQDN формат во ASCII (0x20–0x7E).

Има запирка или празно место во заедничкото име.

Ако има запирка, **Common Name** е одделено од таа точка. Ако има само празно место пред или по запирката, настанува грешка.

Поврзани информации

➡ „Ажурирање самопотпишан сертификат“ на страница 109

Не може да креирате CSR

Не е внесено Common Name.

Мора да внесете **Common Name**.

Внесени се неподдржани знаци за Common Name, Organization, Organizational Unit, Locality и State/Province.

Внесете знаци од IPv4, IPv6, име на главен компјутер или FQDN формат во ASCII (0x20–0x7E).

Има запирка или празно место во Common Name.

Ако има запирка, **Common Name** е одделено од таа точка. Ако има само празно место пред или по запирката, настанува грешка.

Поврзани информации

➡ „Добивање на ИС потпишан сертификат“ на страница 106

Се прикажува предупредување во врска со дигитален сертификат

Пораки	Причина/Што да направите
Enter a Server Certificate.	**Причина:** Не сте избрале датотека за увезување. **Што да направите:** Изберете датотека и кликнете на **Import**.
CA Certificate 1 is not entered.	**Причина:** ИС сертификат 1 не е внесен и внесен е само ИС сертификат 2. **Што да направите:** Првин внесете го ИС сертификат 1.
Invalid value below.	**Причина:** Има несоодветни знаци во патеката на датотеката и/или лозинката. **Што да направите:** Погрижете се знаците да бидат внесени правилно за ставката.
Invalid date and time.	**Причина:** Датумот и времето на скенерот не се поставени. **Што да направите:** Поставете ги датумот и времето со користење на Web Config или EpsonNet Config.
Invalid password.	**Причина:** Одредената лозинка за ИС сертификатот и внесената лозинка не се совпаѓаат. **Што да направите:** Внесете ја точната лозинка.

Пораки	Причина/Што да направите
Invalid file.	**Причина:** Не внесувате датотека за сертификат во X509 формат. **Што да направите:** Осигурете се дека сте го избрале точниот сертификат од проверен издавач на сертификати.
	Причина: Датотеката којашто сте ја внеле е премногу долга. Максималната големина на датотеката е 5 KB. **Што да направите:** Ако ја изберете точната датотека, сертификатот може да биде корумпиран или произведен.
	Причина: Синџирот којшто се содржи во сертификатот е неважечки. **Што да направите:** За повеќе информации за сертификатот, погледнете ја интернет страницата за издавачот на сертификати.
Cannot use the Server Certificates that include more than three CA certificates.	**Причина:** Датотеката на сертификатот во PKCS#12 формат содржи повеќе од 3 ИС сертификати. **Што да направите:** Увезете ги сите сертификати конвертирајќи ги од PKCS#12 формат во PEM формат или увезете ја датотеката на сертификатот во PKCS#12 формат којашто содржи до 2 ИС сертификати.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Причина:** ИС сертификатот е застерен. **Што да направите:** ❏ Ако сертификатот е застарен, добијте го и увезете го новиот сертификат. ❏ Ако сертификатот е застарен, погрижете се датумот и времето на скенерот да бидат поставени правилно.

Пораки	Причина/Што да направите
Private key is required.	**Причина:** Нема спарен приватен клуч со сертификат. **Што да направите:** ❏ Ако сертификатот е во PEM/DER формат и е добиен од CSR со користење на компјутер, назначете ја датотеката за приватен клуч. ❏ Ако сертификатот е во PKCS#12 формат и е добиен од CSR со користење на компјутер, креирајте датотека којашто содржи приватен клуч.
	Причина: Повторно сте го увезле PEM/DER сертификатот добиен од CSR со користење на Web Config. **Што да направите:** Ако сертификатот е во PEM/DER формат и е добиен од CSR со користење на Web Config, може да го увезете само еднаш.
Setup failed.	**Причина:** Не може да ја завршите конфигурацијата затоа што комуникацијата помеѓу скенерот и компјутерот е неуспешна или датотеката не може да биде прочитани поради одредени грешки. **Што да направите:** Откако ќе ја проверите одредената датотека и комуникацијата, повторно увезете ја датотеката.

Поврзани информации

➡ „За дигиталната сертификација“ на страница 105

Сте го избришале ИС потпишаниот сертификат по грешка

Нема резервна датотека со сертификатот потпишан од ИС.

Ако имате резервна датотека, повторно внесете го сертификатот.

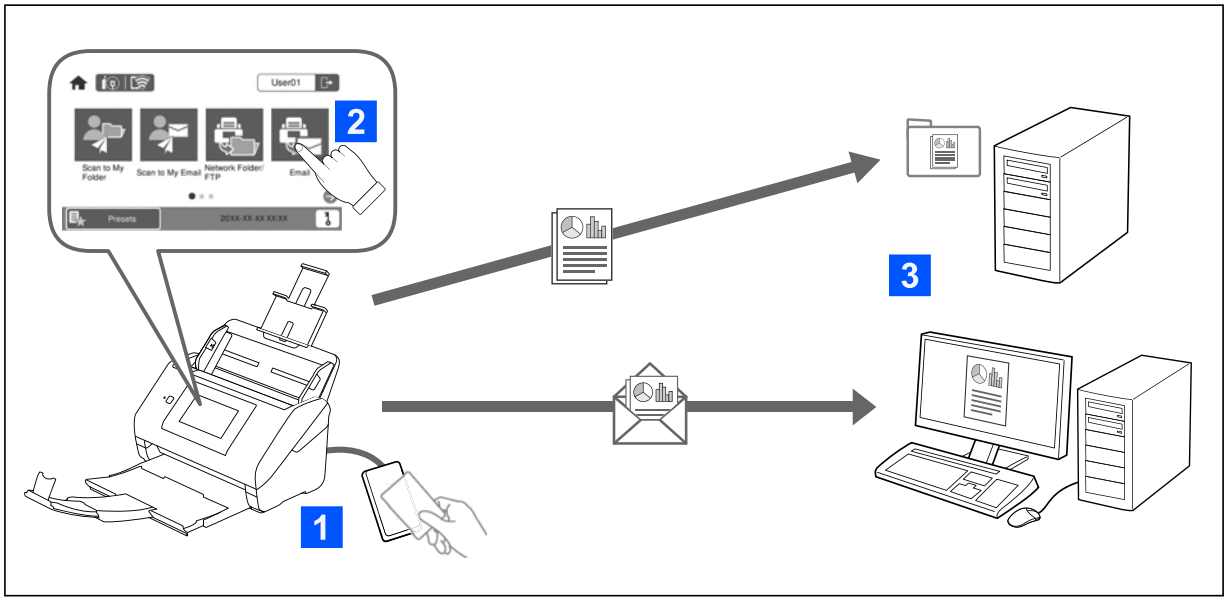
Ако добиете сертификат со користење на CSR креиран од Web Config, не може повторно да го внесете избришаниот сертификат. Креирајте CSR и добијте нов сертификат.

Поврзани информации

➡ „Увезување сертификат потпишан од CA“ на страница 107
➡ „Бришење на ИС потпишан сертификат“ на страница 109

Authentication Settings

За Authentication Settings



Кога е овозможено Authentication Settings, потребно е да се изврши автентикација на корисникот за да започне скенирањето. Може да ги поставите начините на скенирање што може да ги користи секој корисник и да спречите случајни дејства.

Може да ја одредите адресата на е-пошта на автентицираниот корисник како дестинација за скенирање (Scan to My Email) или да ги зачувате податоците на секој корисник во лична папка (Scan to My Folder). Може и да одредите други начини на скенирање.

Белешка:

- *Кога е овозможено Authentication Settings, не може да скенирате од компјутер или паметен уред.*
- *Покрај Authentication Settings наведени во овој прирачник, може и да создадете систем за автентикација користејќи сервер за автентикација. За да создадете систем за автентикација, користете Document Capture Pro Server Authentication Edition (скратено: Document Capture Pro Server AE). За дополнителни информации, контактирајте со локалното претставништво на Epson.*

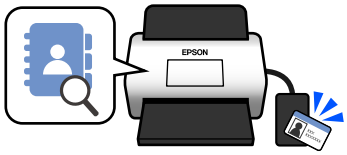
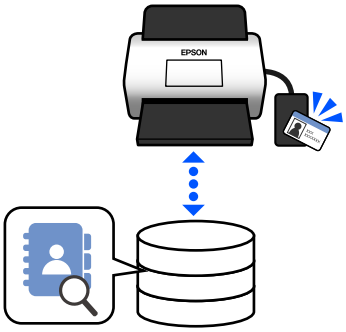
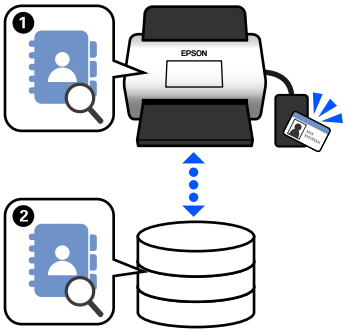
Достапни функции за Authentication Settings

Функција за скенирање на контролната табла	Authentication Settings	
	Кога е овозможено	Кога е оневозможено
Скен. во Моја папка Зачувува слики во папката назначена на автентицираниот корисник.	✓	-
Скен. во Моја е-пошта Испраќа слики до адресата на е-пошта на автентицираниот корисник.	✓	-
Скенирај во мрежна папка/ФТП Зачувува слики во папка на мрежата.	✓	✓

Функција за скенирање на контролната табла	Authentication Settings	
	Кога е овозможено	Кога е оневозможено
Скенирај на компјутер Зачувува слики на поврзан компјутер користејќи задачи создадени во Document Capture Pro (Windows)/Document Capture (Mac OS). * Кога Authentication Settings е овозможено, може да користите само задачи регистрирани во **Поч. пос.**.	✓*	✓
Скенирај во е-пошта Испраќа слики до адресата на е-пошта што сте ја поставиле.	✓	✓
Скенирај во облак Испраќа слики до услугата во облак што сте ја поставиле.	✓	✓
Скен. во USB-диск Зачувува слики во USB-уред поврзан со скенерот. Ова е достапно само кога на скенерот не е поврзан уред за автентикација.	✓	✓
Скенирај во WSD Зачувува слики на поврзан компјутер користејќи ја функцијата WSD.	-	✓
Поч. пос. Може да регистрирате најмногу 48 однапред поставени функции за скенирање. Може да доделите до пет Поч. пос. на корисници регистрирани во Local DB. Доделените Поч. пос. се достапни само за тој корисник. Оние Поч. пос. што не се доделени на ниту еден корисник може да ги користат сите корисници.	✓	✓

За Authentication Method

Овој скенер може да обезбеди автентикација користејќи ги следниве начини без да мора да се создаде сервер за автентикација.

	Local DB	LDAP	Local DB and LDAP
Локација на корисничките податоци	**Меморија на скенерот** Со овој начин на автентикација се проверуваат корисничките податоци регистрирани на скенерот и се споредуваат со податоците на корисникот кој ја користи функцијата за скенирање.	**LDAP-сервер*** Со овој начин на автентикација се проверуваат корисничките податоци на LDAP-серверот синхронизиран со скенерот. Бидејќи до 300 ставки кориснички податоци од LDAP-серверот може привремено да се складираат во скенерот како кеш-меморија, автентикацијата може да се изврши со кеш-меморијата ако LDAP-серверот е недостапен. * Сервер кој обезбедува услуга за директориум што може да комуницира со LDAP.	**Меморија на скенерот и LDAP-сервер** Прво проверете ги корисничките податоци регистрирани во скенерот (❶), па ако нема совпаѓање, споредете ги корисничките податоци со оние на LDAP-серверот (❷).
			
Број на регистрирани корисници	50 (меморија на скенерот)	Неограничено (LDAP-сервер)	50 (меморија на скенерот) Неограничено (LDAP-сервер)
Кеш-меморија на скенерот	-	300	Максимум 300 (50 ставки од кеш-меморијата се споделуваат со User Settings во Local DB)
Начини на најавување	Може да користите некој од следниве начини. ❏ Доближете картичка за автентикација или внесете **User ID** и **Password** ❏ Доближете картичка за автентикација или внесете **ID Number** ❏ Внесете **User ID** и **Password** ❏ Внесете **User ID** ❏ Внесете **ID Number**		
Ограничувања на функцијата „Скенирај во“	Поставете поединечно за секој корисник	Исти поставки за сите корисници на LDAP	Корисници на Local DB: поставете поединечно Корисници на LDAP: исти поставки за сите корисници

	Local DB	LDAP	Local DB and LDAP
Доделување Поч. пос. на корисниците	До 5 по корисник	- (Не може да се постави поединечно)	Корисници на Local DB: до 5 по корисник Корисници на LDAP: -

Софтвер за поставување

Поставување со Web Config или Epson Device Admin.

❏ Кога користите Web Config, може да го поставите скенерот користејќи само веб-прелистувач.

„Web Config“ на страница 38

❏ Кога користите Epson Device Admin, може да поставите повеќе скенери одеднаш користејќи шаблон за конфигурација.

„Epson Device Admin“ на страница 39

Ажурирање на фирмверот на скенерот

Пред да овозможите Authentication Settings, ажурирајте го фирмверот на скенерот на најновата верзија. Претходно, поврзете го скенерот на интернет.

Важно:

Не исклучувајте ги компјутерот или скенерот додека трае ажурирањето.

При поставување од Web Config:

Изберете ја картичката **Device Management** > **Firmware Update**, а потоа следете ги инструкциите на екранот за да го ажурирате фирмверот.

При поставување од Epson Device Admin:

Изберете **Home** > **Firmware** > **Update** на екранот со списокот со уреди, а потоа следете ги инструкциите на екранот за да го ажурирате фирмверот.

Белешка:

Ако најновиот фирмвер е веќе инсталиран, нема потреба да ажурирате.

Поврзување и конфигурирање уред за автентикација

Ако сакате да поврзете и да користите уред за автентикација како што е читач за IC-картички, прво треба да го конфигурирате уредот. Ова не е потребно ако не користите уред за автентикација.

Поврзани информации

➡ „Поврзување на уредот за автентикација“ на страница 140
➡ „Поставки за уредот за автентикација“ на страница 141

Список со компатибилни читачи за картички

Овој список не ги гарантира дејствата на читачите за картички во списокот.

Да: поддржан (ID-информациите може да се прочитаат со стандардни поставки за читачот за картички.)

Не: не е компатибилен

Производител	Модел	Број на модел	Картичка за автентикација							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Да	Да*1	Да*1	Да*1	Не	Не	Не	Тастатура
RF IDEAS	pcProx	RDR-7081BKU	Да*1	Не	Да	Да	Не	Не	Не	Тастатура
RF IDEAS	pcProx	RDR-7581AKU	Да	Не	Да*1	Да*1	Не	Не	Не	Тастатура
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Не	Не	Да	Да	Не	Не	Не	Тастатура
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Да	Не	Да	Да	Да	Да	Да	Тастатура
ELATEC	TWN4 MULTITECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Да	Да	Да	Да	Да	Да	Да	Тастатура

Производител	Модел	Број на модел	Картичка за автентикација							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ELATEC	TWN4 MultiTech 2 BLE-PI	T4LK-FB4BLZ-PI	Да	Да	Да	Да	Да	Да	Да	Тастатура
ELATEC	TWN4 Slim	T4QC-FC3B7	Да	Да	Да	Да	Да	Да	Да	Тастатура
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Да	Да	Да	Да	Да	Не	Да	Тастатура*1
ACS	ACR122U	ACR122U	Не	Не	Да*2	Да*2	Да	Не	Да*2	PC/SC
ACS	ACR1252	ACR1252	Не	Не	Да*2	Да*2	Да	Да	Да*2	PC/SC
Sony	PaSoRi	RC-S330/S	Не	Не	Да*2	Да*2	Да*2	Да*2	Да*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Не	Не	Да*2	Да*2	Да*2	Да*2	Да*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Да	Да	Да	Да	Да	Да	Да	Тастатура
DMZ	Leitor RFID Multi-125	DMZ087	Не	Да	Не	Не	Не	Не	Не	Тастатура
DMZ	Leitor RFID Mifare	DMZ088	Не	Не	Да	Да	Не	Не	Не	Тастатура
DMZ	Biometric & RFID Reader	DMZ073	Не	Да	Не	Не	Не	Не	Не	Тастатура

Производител	Модел	Број на модел	Картичка за автентикација							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
inepro	SCR708	SCR708	Да*1	Да*1	Да*1	Да*1	Да*1	Да*1	Да*1	Тастатура
Y Soft	YU03088 001	MU0388	Да	Да	Да	Да	Да	Да	Да	Тастатура
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Не	Не	Да	Да	Не	Не	Да	Тастатура
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Не	Не	Да	Да	Не	Не	Да	Тастатура
NT-ware	MiCard MultiTech4-PI	T4DT-FB4WUF-PI	Да	Да	Да	Да	Да	Да	Да	Тастатура
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Да*1	Да*1	Да*1	Да*1	Не	Не	Не	Тастатура
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Да	Да	Да	Да	Да	Да	Не	Тастатура

*1 Треба да ги промените поставките за читачот за картички со користење на заштитениот софтвер обезбеден од производителот на читачот за картички.

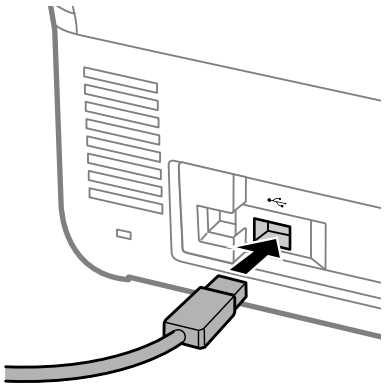
*2 Ако треба да користите податоци во одреден дел на картичката освен стандардниот ID на картичката како ID за автентикација со конфигурирање на поставките за производот, контактирајте со локалниот претставник или партнер на Epson за повеќе информации околу начинот на конфигурирање на производот.

Поврзување на уредот за автентикација

Важно:

Кога ќе го поврзете уредот за автентикација со повеќе скенери, користете производ со ист број на модел.

Поврзете го USB-кабелот на читачот за картички со USB-портата за надворешен интерфејс на скенерот.



Проверка на статусот на уредот за автентикација

Статусот на врската на уредот за автентикација, како и неговото препознавање на картичката за автентикација може да ги проверите преку контролната табла на скенерот.

Информациите ќе се прикажат ако изберете **Поставки** > **Информации за уред** > **Статус на уредот за автентикација**.

Поставки за уредот за автентикација

Поставете го форматот за читање на информациите за автентикација добиени од картичката за автентикација.

Може да го поставите следниов начин на читање за уредот за автентикација.

- ❏ Читање одредена област од картичката за автентикација, на пр. број на вработен или личен ID.
- ❏ Користење на информациите од картичката за автентикација, освен UID (информации за картичката за автентикација, на пр. нејзиниот сериски број.)

  Може да користите алатка за генерирање на оперативните параметри. За детали, обратете се до дистрибутерот.

Белешка:
Користење картички за автентикација од различни производители:

Кога се користат UID-информации за картичките (информации за ID на картичката, како што е серискиот број), може да користите мешавина од различни типови картички за автентикација. Ова не може да се меша кога се користат други информации од картичките.

При поставување од Web Config:

Изберете ја картичката **Device Management** > **Card Reader**.

При поставување од Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Card Reader** од шаблонот за конфигурација.

Ставка	Објаснување
Vendor ID	Поставете го ID на продавачот на уредот за автентикација што го ограничува користењето од 0000 до FFFF со 4 алфанумерички знаци. Ако не сакате да го ограничите, поставете го на 0000.
Product ID	Поставете го ID на производот на уредот за автентикација што го ограничува користењето од 0000 до FFFF со 4 алфанумерички знаци. Ако не сакате да го ограничите, поставете го на 0000.
Operational parameter	Поставете го оперативниот параметар на уредот за автентикација од 0 до 8192 знаци. Достапни се A~Z, a~z, 0~9, +, /, =, празно место и нов ред.
Card Reader	Изберете го форматот на конверзија за уредот за автентикација. Може да ги проверите деталите за форматот. Погледнете го линкот наведен во описот на ставката.
Authentication Card ID save format	Изберете го форматот на конверзија за информациите за автентикација од ID-картичката. Може да ги проверите деталите за форматот. Погледнете го линкот наведен во описот на ставката.
Set card ID range	Овозможете спецификација на позицијата за читање.
Text Start Position	Одредете ја почетната позиција во текстот за читање на информациите за ID. Може да одредите од 1 до 4096.
Number of Characters	Одредете го бројот на знаци што треба да се читаат од почетната позиција на информациите за ID. Може да одредите од 1 до 4096.

Информации за регистрирање поставки

Поставување

Одредете ги потребните поставки во зависност од Authentication Method и начинот на скенирање што го користите.

Важно:

Пред да започнете со поставувањето, проверете дали поставката за време за скенерот е точна.

Ако поставката за време е неточна, ќе се прикаже пораката за грешка „Лиценцата е истечена", па можеби нема да може да го довршите поставувањето на скенерот. Мора да се постави точно време и за да може да се користи безбедносна функција како SSL/TLS-комуникација или IPsec. Времето може да го поставите на следниов начин.

- *Web Config: картичка **Device Management** > **Date and Time** > **Date and Time**.*
- *Контролна табла на скенерот: **Поставки** > **Осн поставки** > **Поставки за датум/време**.*

Поставки	Local DB	LDAP	Local DB and LDAP
Овозможување автентикација Пред да ги одредите поставките за автентикација, треба да овозможите автентикација. „Овозможување автентикација“ на страница 143	✓	✓	✓
Authentication Settings Поставување Authentication Method и како да се изврши автентикација на корисникот. „Authentication Settings“ на страница 144	✓	✓	✓
Регистрирање User Settings Регистрирајте ги поставките за секој корисник. Може и групно да регистрирате корисници со CSV-датотека. „Регистрирање User Settings“ на страница 145	✓	–	✓
Синхронизирање со LDAP Server Одредете ги поставките за синхронизација на LDAP-серверот. „Синхронизирање со LDAP Server“ на страница 152	–	✓	✓
Поставување Email Server Одредете ги поставките за серверот за е-пошта. Поставете го ова кога користите функции за кои се потребни поставки за сервер за е-пошта, како на пр. Scan to My Email. „Поставување на серверот за е-пошта“ на страница 156	✓	✓	✓
Поставување Scan to My Folder Поставете ги дестинациските папки. Поставете го ова кога ја користите функцијата Scan to My Folder. „Поставување на Scan to My Folder“ на страница 157	✓	✓	✓
Customize One-touch Functions Поставете го ова кога ги менувате ставките што се прикажуваат на контролната табла на скенерот. Може да поставите на контролната табла да се прикажуваат само иконите што ви се потребни, или пак, да го промените нивниот редослед. „Customize One-touch Functions“ на страница 159	✓	✓	✓

Овозможување автентикација

Пред да ги одредите поставките за автентикација, треба да овозможите автентикација.

При поставување од Web Config:

Изберете **Вклучено (уред/LDAP сервер)** од картичката **Product Security** > **Basic** > **Authentication**.

При поставување од Epson Device Admin:

Во шаблонот за конфигурација, изберете **Вклучено (уред/LDAP сервер)** од **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Белешка:
Ако овозможите Authentication Settings на скенерот, ќе се овозможи и Поставка за заклучување за контролната табла. Контролната табла не може да се отклучи кога е овозможено Authentication Settings.

Дури и ако оневозможите Authentication Settings, Поставка за заклучување останува овозможено. Ако сакате да го оневозможите, може да одредите поставки преку контролната табла или преку Web Config.

Поврзани информации

➡ „Поставување Поставка за заклучување од контролната табла“ на страница 92
➡ „Поставување Поставка за заклучување преку Web Config“ на страница 92

Authentication Settings

Поставување Authentication Method и како да се изврши автентикација на корисникот.

При поставување од Web Config:

Изберете ја картичката **Product Security** > **Authentication Settings**.

При поставување од Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Authentication Settings** од шаблонот за конфигурација.

Ставка	Објаснување
Authentication Method	Изберете Authentication Method. ❏ Local DB Извршете автентикација со User Settings регистрирани на скенерот. Неопходно е да го регистрирате корисникот на скенерот. ❏ LDAP Извршете автентикација користејќи ги корисничките податоци на LDAP-серверот синхронизиран со скенерот. Претходно, треба да ги конфигурирате поставките за LDAP-серверот. ❏ Local DB and LDAP Извршете автентикација користејќи ги корисничките податоци регистрирани на скенерот или на LDAP-серверот синхронизиран со скенерот. Треба да го регистрирате корисникот на скенерот и да го поставите LDAP-серверот.

Ставка	Објаснување
How to Authenticate User	Изберете како да се изврши автентикација на корисникот. ❏ Card or User ID and Password За да вршите автентикација на корисниците, користете картичка за автентикација. За автентикација може да користите и ID на корисник и лозинка. ❏ User ID and Password За да вршите автентикација на корисниците, користете ID на корисник и лозинка. Ако ја изберете функцијава, нема да може да користите картичка за автентикација за да вршите автентикација. ❏ User ID За да вршите автентикација на корисниците, користете само ID на корисник. Нема потреба да поставите лозинка. ❏ Card or ID Number За да вршите автентикација на корисниците, користете картичка за автентикација. Може да користите и ID Number. ❏ ID Number Користете само ID-број за да вршите автентикација на корисниците.
Allow users to register authentication cards	Овозможете ја функцијава ако им дозволувате на корисниците да ја регистрираат картичката за автентикација на системот. Ако изберете **LDAP** како **Authentication Method**, не може да се постави. За повеќе информации околу тоа како корисниците може да ги регистрираат своите картички за автентикација, видете „Регистрирање картичка за автентикација" во *Упатство за корисникот*.
The Minimum Digit Number of ID Number	Изберете го минималниот број на цифри за ID-бројот.
Caching for LDAP authenticated users	Ако користите автентикација со LDAP-сервер, може да поставите дали да се врши складирање на корисничките податоци во кеш-меморијата.
Use user information in SMTP authentication	Ако користите ID на корисник и лозинка за автентикација, може да поставите дали корисничките податоци да се користат за SMTP-автентикација. Системот ги користи последните ID на корисник и лозинка што биле најавени.
Restrictions for LDAP authenticated users	Ако користите LDAP, може да поставите кои функции да бидат достапни за корисникот.

Регистрирање User Settings

Регистрирајте User Settings што се користат за автентикација на корисници. Може да ги регистрирате на некој од следниве начини.

❏ Регистрирање User Settings една по една (Web Config)

❏ Регистрирање повеќе User Settings како група, користејќи CSV-датотека (Web Config)

❏ Регистрирање User Settings на повеќе скенери како група, користејќи шаблон за конфигурација (Epson Device Admin)

Поврзани информации

➡ „Регистрирање User Settings поединечно (Web Config)“ на страница 146
➡ „Регистрирање повеќе User Settings користејќи CSV-датотека (Web Config)“ на страница 147
➡ „Регистрирање User Settings на повеќе скенери како група (Epson Device Admin)“ на страница 150

Регистрирање User Settings поединечно (Web Config)

Одете на Web Config и изберете ја картичката **Product Security** > **User Settings** > **Add**, а потоа отворете User Settings.

Ставка	Објаснување
User ID	Внесете го ID на корисник што сакате да го користите за автентикација, во опсег од 1 до 83 бајти што може да се изразат во Unicode (UTF-8). Бидејќи за ID на корисник не се разликуваат мали од големи букви, може да се најавите со големи или мали букви.
User name Display	Внесете го корисничкото име прикажано на контролната табла на скенерот, до 32 знаци што може да се изразат во Unicode (UTF-16). Ова може да го оставите празно.
Password	Внесете ја лозинката што сакате да ја користите за автентикација, до 32 знаци во ASCII. Лозинката разликува големи и мали букви. Оставете го ова празно ако сте избрале **User ID** за **How to Authenticate User**.
Authentication Card ID	Внесете го ID на картичката за автентикација, до 116 знаци во ASCII. Ова може да го оставите празно. Кога ќе овозможите **Allow users to register authentication cards** за **Authentication Settings**, се одразува резултатот регистриран од корисниците.
ID Number	Оваа ставка се прикажува кога **Card or ID Number** или **ID Number** е избрано во **Authentication Settings** > **How to Authenticate User**. Внесете број што е во рамките на бројот поставен во **Authentication Settings** > **The Minimum Digit Number of ID Number** и содржи до 8 цифри.
Auto Generate	Оваа ставка се прикажува кога **Card or ID Number** или **ID Number** е избрано во **Authentication Settings** > **How to Authenticate User**. Кликнете за автоматски да се генерира ID-број со истиот број на цифри што сте го избрале во **The Minimum Digit Number of ID Number**.
Department	Внесете го името на одделот и сл., што го идентификува корисникот, користејќи до 40 знаци што може да се изразат во Unicode (UTF-16). Ова може да го оставите празно.
Email Address	Внесете ја адресата на е-пошта на корисникот, до 200 знаци во ASCII. Ова се користи како дестинација за **Scan to My Email**. Ова може да го оставите празно.

Ставка	Објаснување
Scan to My Folder	Дестинациите за зачувување може да ги поставите поединечно ако изберете **Individual** во **Scan to My Folder** > **Setting Type**. Погледнете го следново за повеќе информации околу поставките. „Поставување на Scan to My Folder“ на страница 157
Restrictions	Може да ги ограничите функциите за секој корисник. Изберете ја функцијата што дозволувате да се користи.
Presets	Од Presets регистрирани во скенерот, може да одредите до пет однапред поставени поставки што ќе бидат достапни само за одреден корисник. ❏ Оние Presets што се доделени на одреден корисник може да ги користи само тој корисник. Оние Presets што не се доделени на ниту еден корисник може да ги користат сите корисници. ❏ Ако за корисникот е достапна само една од Presets, таа автоматски ќе се примени по автентикацијата. Ако се достапни повеќе Presets, по автентикацијата ќе се прикаже список со Presets. ❏ Не може да создавате или да се прикажуваат Presets што користат функции што се ограничени во **Restrictions**.

Регистрирање повеќе User Settings користејќи CSV-датотека (Web Config)

Внесете ги поставките за секој корисник во CSV-датотека и регистрирајте ги како група.

Создавање CSV-датотека

Создајте CSV-датотека за да увезете User Settings.

Белешка:
Ако регистрирате една или повеќе User Settings однапред, а потоа извезете форматирана датотека (CSV-датотека), може да ја користите регистрираната поставка како референца за внесување поставки.

1. Одете на Web Config и изберете ја картичката **Product Security** > **User Settings**.
2. Кликнете **Export**.
3. Изберете формат на датотеката во **File Format**.

   Изберете го според инструкциите подолу.

Ставка	Објаснување
CSV UTF-16 (Tab delimited)	Како да го изберете форматот кога ќе ја изменувате датотеката користејќи Microsoft Excel. Секој параметар е опкружен со „[ ]“ (загради). Внесете ги параметрите во „[ ]“. Кога ќе ја изменувате датотеката, препорачуваме да ја замените со нејзината понова верзија. Ако за првпат ја зачувувате датотеката, изберете „Unicode text (*.txt)“ како формат на датотеката.

Ставка	Објаснување
CSV UTF-8 (Comma delimited)	Како да го изберете форматот кога ќе ја изменувате датотеката користејќи уредувач за текст или макро без Microsoft Excel.
CSV UTF-8 (Semicolon delimited)	

4. Кликнете **Export**.

5. Изменете ја и зачувајте ја оваа CSV-датотека во апликација за табеларни пресметки како што е Microsoft Excel или во уредувач за текст.

> ***Важно:***
> *Кога ја изменувате датотеката, не менувајте ги информациите за кодирањето и заглавието.*

Поставки за CSV-датотека

Ставка	Поставки и објаснување
UserID	Внесете ID на корисник што ќе се користи за автентикација, од 1 до 83 бајти во Unicode.
UserName	Внесете го корисничкото име прикажано на контролната табла на скенерот, до 32 знаци во Unicode. Ова може да го оставите празно.
Password	Внесете ја лозинката што ќе се користи за автентикација, до 32 знаци во ASCII. При увезувањето, ова е поставено како лозинка наместо **EncPassword**. Оставете го ова празно ако сте избрале **User ID** за **How to Authenticate User**. При извезувањето, ова е секогаш празно.
AuthenticationCardID	Одредете поставки за резултатот од читањето на картичката за автентикација. Кога ќе овозможите **Allow users to register authentication cards** во **Authentication Settings**, се одразува резултатот регистриран од корисниците. Внесете до 116 знаци во ASCII. Ова може да го оставите празно.
IDNumber	Оваа ставка се прикажува кога **Card or ID Number** или **ID Number** е избрано во **Authentication Settings** > **How to Authenticate User**. Внесете број што е во рамките на бројот поставен во **Authentication Settings** > **The Minimum Digit Number of ID Number** и содржи до 8 цифри. ID-бројот не може да се дуплира. Ако е дуплиран, ќе добиете предупредување за грешка при увезувањето на датотеката. Кога е оставено празно, автоматски му се доделува број.
Department	Внесете произволно име на одделот за да се разликуваат корисниците. Внесете до 40 знаци во Unicode. Ова може да го оставите празно.
MailAddress	Поставете ја адресата на е-пошта за корисниците. Ова се користи како дестинација за **Scan to My Email**. Може да користите A-Z, a-z, 0-9, !#’%&’*+-./=?^_{|}~@. Внесете до 200 знаци. Не може да користите „‟ (запирка) за првиот знак. Ова може да го оставите празно.

Ставка	Поставки и објаснување
FolderProtocol	Одредете тип на функцијата Scan to My Folder. Мрежна папка/FTP (SMB): 0, FTP: 1
FolderPath	Поставете ја дестинацијата за зачувување за функцијата Scan to My Folder.
FolderUserName	Поставете го корисничкото име за функцијата Scan to My Folder.
FolderPassword	Поставете лозинка што содржи до 32 знаци во ASCII за автентикација на дестинациската папка за функцијата Scan to My Folder. При увезувањето, ова е поставено како лозинка наместо **EncPassword**. При извезувањето, ова е секогаш празно.
FtpPassive	Поставете го режимот за поврзување за FTP-серверот кога **FTP** е избрано како **Type** за функцијата Scan to My Folder. Активен режим: 0, Пасивен режим: 1
FtpPort	Поставете го бројот на портата за испраќање скенирани податоци до FTP-серверот од 0 до 65535 кога **FTP** е избрано како **Type** за функцијата Scan to My Folder.
ScanToMemory	Поставете ги ограничувањата за Scan to USB Drive. Не е дозволено: 0, Дозволено: 1
ScanToMail	Поставете ги ограничувањата за Scan to Email. Може да поставите **Скен. во Моја е-пошта** само кога **Scan to Email** е овозможено. Не е дозволено: 0, Дозволено: 1
ScanToFolder	Поставете ги ограничувањата за Scan to Network Folder/FTP. Може да поставите **Скен. во Моја папка** само кога **Scan to Network Folder/FTP** е овозможено. Не е дозволено: 0, Дозволено: 1
ScanToCloud	Поставете ги ограничувањата за Scan to Cloud. Не е дозволено: 0, Дозволено: 1
ScanToComputer	Поставете ги ограничувањата за Скенирај на компјутер. Не е дозволено: 0, Дозволено: 1
PresetIndex	Поставете Presets коишто сакате да ги назначите за корисникот. Може да поставите до пет Presets со регистарски броеви одделени со запирки.
EncPassword	При извезувањето на кориснички поставки, параметарот поставен за **Password** се шифрира, а потоа вредноста се кодира со BASE64 и се извезува. При увезувањето со новата лозинка за **Password**, оваа вредност се игнорира. Ако полето за **Password** е празно, се користи оваа вредност и лозинката останува каква што била пред извезувањето.

Ставка	Поставки и објаснување
EncFolderPassword	При извезувањето, параметарот поставен за **FolderPassword** се шифрира, а потоа вредноста се кодира со BASE64 и се извезува. При увезувањето со новата лозинка за **FolderPassword**, оваа вредност се игнорира. Ако полето за **FolderPassword** е празно, се користи оваа вредност и лозинката останува каква што била пред извезувањето.

Увезување CSV-датотека

1. Одете на Web Config и изберете ја картичката **Product Security** > **User Settings**.
2. Кликнете **Import**.
3. Изберете ја датотеката што сакате да ја увезете.
4. Кликнете **Import**.
5. Откако ќе ги проверите прикажаните информации, кликнете **OK**.

Регистрирање User Settings на повеќе скенери како група (Epson Device Admin)

Може да регистрирате User Settings што се користат во Local DB како група, користејќи LDAP-сервер или CSV/ENE-датотека.

Белешка:
ENE-датотеката е бинарна датотека обезбедена од Epson којашто шифрира и зачувува податоци за ***Contacts****, како што се лични податоци и User Settings. Може да се извезе од Epson Device Admin и може да поставите лозинка. Корисна е кога сакате да увезете User Settings од резервна датотека.*

Увезување од CSV/ENE-датотека

1. Изберете **Administrator Settings** > **Authentication Settings** > **User Settings** од шаблонот за конфигурација.
2. Кликнете **Import**.
3. Изберете **CSV or ENE File** од **Import Source**.
4. Кликнете **Browse**.

   Се прикажува екранот за избирање на датотеката.
5. Изберете ја датотеката што сакате да ја увезете за да ја отворите.

6. Изберете начин на увезување.
   - ❏ Overwrite and Add: презапишува ако постои ист ID на корисник; додава нов ID ако не постои.
   - ❏ Replace All: заменува сè со корисничките поставки што сакате да ги увезете.
7. Кликнете **Import**.

   Се прикажува екранот за потврдување на поставката.
8. Кликнете **OK**.

   Се прикажува резултатот од потврдувањето.

   Белешка:
   - ❏ *Ако бројот на кориснички поставки за увезување го надминува бројот на поставки што може да се увезат, ќе се прикаже порака што ве известува дека треба да избришете дел од корисничките поставки. Пред увезувањето, избришете го вишокот кориснички поставки.*
   - ❏ *Пред увезувањето, изберете ги корисничките поставки што сакате да ги избришете, а потоа кликнете **Delete**.*
9. Кликнете **Import**.

   Корисничките поставки ќе се увезат во шаблонот за конфигурација.

Увезување од LDAP-серверот

1. Изберете **Administrator Settings** > **Authentication Settings** > **User Settings** од шаблонот за конфигурација.
2. Кликнете **Import**.
3. Изберете **LDAP** од **Import Source**.
4. Кликнете **Settings**.

   Се прикажуваат поставките за **LDAP Server**.

   Белешка:
   Оваа поставка за LDAP-серверот служи за увезување на корисничките поставки од LDAP-серверот. Увезените (копирани) кориснички поставки се користат за автентикација на корисниците со самиот скенер.

   *Од друга страна, ако изберете **LDAP** или **Local DB and LDAP** како начин на автентикација, корисниците се автентицираат преку комуникација со LDAP-серверот.*
5. Поставете ги сите ставки.

   При увезувањето кориснички поставки од LDAP-сервер, покрај поставките за LDAP може да ги конфигурирате и следниве поставки.

   За други ставки, погледнете во „Поврзани информации".

Ставка		Објаснување
LDAP Server Settings	LDAP Server Type	Ви овозможува да го изберете типот LDAP-сервер.

Ставка			Објаснување
Search Settings	Search Filter		Може да го одредите текстот што ќе се користи за филтерот за пребарување за LDAP. Изберете **Custom** за да го измените текстот за пребарување.
	Options	Type	Може да го поставите типот на дестинацијата за зачувување за **Scan To My Folder**.
		Connection Mode	Кога **Type** е поставен на **FTP**, може да го поставите режимот за поврзување преку FTP.
		Port Number	Кога **Type** е поставен на **FTP**, може да го поставите бројот на портата што сакате да ја користите.

6. По потреба, извршете тест на врската со кликнување **Connection Test**.

   Вчитува и прикажува 10 кориснички поставки од LDAP-серверот.

7. Кликнете **OK**.

8. Изберете начин на увезување.

   ❏ Overwrite and Add: презапишува ако постои ист ID на корисник; додава нов ID ако не постои.

   ❏ Replace All: заменува сè со корисничките поставки што сакате да ги увезете.

9. Кликнете **Import**.

   Се прикажува екранот за потврдување на поставката.

10. Кликнете **OK**.

    Се прикажува резултатот од потврдувањето.

11. Кликнете **Import**.

    Корисничките поставки ќе се увезат во шаблонот за конфигурација.

Поврзани информации

➡ „Конфигурирање LDAP-сервер“ на страница 153
➡ „Конфигурирање на поставките за пребарување на LDAP-серверот“ на страница 155

Синхронизирање со LDAP Server

Одредете ги поставките за LDAP Server за скенерот.

По потреба, одредете поставки и за примарниот и за секундарниот сервер.

Белешка:
*Поставките за **LDAP Server** се споделуваат со **Contacts**.*

Достапни услуги

Поддржани се следниве услуги за директориуми.

Име на услугата	Верзија
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

Конфигурирање LDAP-сервер

За да користите LDAP-сервер, прво треба да го конфигурирате.

При поставување од Web Config:

Изберете ја картичката **Network** > **LDAP Server** > **Basic (Primary Server)** или **Basic (Secondary Server)**.

Ако изберете **Kerberos Authentication** како **Authentication Method**, изберете **Network** > **Kerberos Settings** за да одредите поставки за Kerberos.

При поставување од Epson Device Admin:

Изберете **Network** > **LDAP server** > **Server Settings (Primary Server)** или **Server Settings (Secondary Server)** од шаблонот за конфигурација.

Ако изберете **Kerberos Authentication** како **Authentication Method**, изберете **Network** — **Security** > **Kerberos Settings** за да одредите поставки за Kerberos.

Ставка	Поставки и објаснување
Use LDAP Server	Изберете **Use** или **Do Not Use**.
LDAP Server Address	Внесете ја адресата на LDAP-серверот. Внесете од 1 до 255 знаци во IPv4, IPv6 или FQDN-формат. За FQDN-форматот, може да користите алфанумерички знаци во ASCII (0x20 – 0x7E) и цртички, освен на почетокот и крајот на адресата.
LDAP server Port Number (Port number)	Внесете го бројот на портата на LDAP-серверот (од 1 до 65535).
Secure Connection	Одредете го начинот на автентикација кога скенерот пристапува до LDAP-серверот.
Certificate Validation	Кога ова е овозможено, се врши автентикација на сертификатот на LDAP-серверот. Препорачуваме да го поставите ова на **Enable**. За да се постави, **CA Certificate** треба да се увезе во скенерот.
Search Timeout (sec)	Поставете ја должината на времето за пребарување (од 5 до 300 секунди).

Ставка	Поставки и објаснување
Authentication Method	Изберете го начинот на автентикација. Ако изберете **Kerberos Authentication**, одредете ги поставките за Kerberos однапред. За да извршите Kerberos Authentication, потребна е следнава околина. ❏ Скенерот и DNS-серверот може да комуницираат. ❏ Времето за скенерот, за KDC-серверот и за потребниот сервер за автентикација (LDAP-сервер, SMTP-сервер, датотечен сервер) се синхронизирани. ❏ Кога серверот за услуги е назначен како IP-адреса, FQDN за серверот за услуги е регистрирано во зоната за обратно пребарување на DNS-серверот.
Kerberos Realm to be Used	Ако изберете **Kerberos Authentication** како **Authentication Method**, изберете го доменот на Kerberos што сакате да го користите.
Administrator DN / User Name	Внесете го корисничкото име за LDAP сервер од 128 знаци или помалку во Unicode (UTF-8). Не може да користите контролни знаци, како што се 0x00 до 0x1F и 0x7F. Поставката не се користи кога е избрано **Anonymous Authentication** како **Authentication Method**. Ако не сакате да го наведете ова, оставете го празно.
Password	Внесете ја лозинката за автентикација на LDAP сервер од 128 знаци или помалку во Unicode (UTF-8). Не може да користите контролни знаци, како што се 0x00 до 0x1F и 0x7F. Поставката не се користи кога е избрано **Anonymous Authentication** како **Authentication Method**. Ако не сакате да го наведете ова, оставете го празно.

Поставки за Kerberos

Ако изберете **Kerberos Authentication** како **Authentication Method**, треба да одредите поставки за Kerberos. Може да регистрирате најмногу 10 поставки за Kerberos.

При поставување од Web Config:

Изберете ја картичката **Network** > **Kerberos Settings**.

При поставување од Epson Device Admin:

Изберете **Network** > **Security** > **Kerberos Settings** од шаблонот за конфигурација.

Ставка	Поставки и објаснување
Realm (Domain)	Внесете го доменот на автентикацијата со Kerberos користејќи до 255 знаци во ASCII (0x20 – 0x7E). Ако не сакате да го регистрирате ова, оставете го празно.
KDC Address	Внесете адреса на Kerberos серверот за автентикација. Внесете до 255 знаци во IPv4, IPv6 или FQDN-формат. Ако не сакате да го регистрирате ова, оставете го празно.
Port Number (Kerberos)	Внесете го бројот на портата за серверот Kerberos (од 1 до 65535).

Конфигурирање на поставките за пребарување на LDAP-серверот

Ги поставува атрибутите за пребарување за корисничките поставки.

При поставување од Web Config:

Изберете ја картичката **Network** > **LDAP Server** > **Search Settings (Authentication)**.

При поставување од Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** од шаблонот за конфигурација.

Ставка	Поставки и објаснување
Search Base (Distinguished Name)	Наведете ја почетната позиција кога барате кориснички податоци од LDAP-серверот. Внесете од 0 до 128 знаци во Unicode (UTF-8). Ако не пребарувате произволен атрибут, оставете го ова празно. Пример за директориум на локален сервер: dc=server,dc=local
User ID Attribute	Наведете го името на атрибутот што ќе се прикажува кога се пребарува ID-бројот. Внесете од 1 до 255 знаци во ASCII. Првиот знак треба да биде a – z или A – Z. Пример: cn, uid
User name Display Attribute	Наведете го името на атрибутот што ќе се прикажува како корисничко име. Внесете од 0 до 255 знаци во ASCII. Првиот знак треба да биде a – z или A – Z. Ова може да го оставите празно. Пример: cn, name
Authentication Card ID Attribute	Наведете го името на атрибутот што ќе се прикажува како ID на картичката за автентикација. Внесете од 0 до 255 знаци во ASCII. Првиот знак треба да биде a – z или A – Z. Ова може да го оставите празно. Пример: cn, sn
ID Number Attribute	Наведете го името на атрибутот што ќе се прикажува кога се пребарува ID-бројот. Внесете од 1 до 255 знаци во ASCII. Првиот знак треба да биде a – z или A – Z. Пример: cn, id
Department Attribute	Наведете го името на атрибутот што ќе се прикажува како име на одделот. Внесете од 0 до 255 знаци во ASCII. Првиот знак треба да биде a – z или A – Z. Ова може да го оставите празно. Пример: ou, ou-cl
Email Address Attribute	Наведете го името на атрибутот што ќе се прикажува кога се пребаруваат адреси на е-пошта. Внесете од 1 до 255 знаци во ASCII. Првиот знак треба да биде a – z или A – Z. Пример: mail
Save To Attribute	Наведете го името на атрибутот што ќе укажува на дестинацијата за Scan To My Folder. Внесете од 0 до 255 знаци во ASCII. Пример: homeDirectory

Проверка на врската со LDAP-серверот

Врши тестирање на врската со LDAP-серверот користејќи го параметарот поставен на **LDAP Server** > **Search Settings**.

1. Одете на Web Config и изберете ја картичката **Network** > **LDAP Server** > **Connection Test**.
2. Изберете **Start**.

   Започнува тестирањето на врската. По тестирањето, се прикажува извештај од тестирањето.

Пробни референции за конекција на LDAP сервер

Пораки	Објаснување
Connection test was successful.	Оваа порака се прикажува кога поврзувањето со серверот е успешно.
Connection test failed. Check the settings.	Оваа порака се прикажува од следниве причини: ❏ Адресата на LDAP серверот или бројот на порти е неточен. ❏ Настанал прекин. ❏ **Do Not Use** е избрано како **Use LDAP Server**. ❏ Ако **Kerberos Authentication** е избрано како **Authentication Method**, поставките како на пример **Realm (Domain)**, **KDC Address** и **Port Number (Kerberos)** се неточни.
Connection test failed. Check the date and time on your product or server.	Оваа порака се појавува кога поврзувањето не успева бидејќи поставките за време за скенерот и за LDAP-серверот се неусогласени.
Authentication failed. Check the settings.	Оваа порака се прикажува од следниве причини: ❏ **User Name** и/или **Password** се неточни. ❏ Ако **Kerberos Authentication** е избран како **Authentication Method**, времето/датумот можно е да не може да се конфигурира.
Cannot access the product until processing is complete.	Пораката се прикажува кога скенерот е зафатен.

Поставување на серверот за е-пошта

Кога користите **Scan to My Email**, поставете го серверот за е-пошта.

Белешка:
*Може да поставите **Scan to My Email** само кога **Scan to Email** е овозможено.*

При поставување од Web Config:

Изберете ја картичката **Network** > **Email Server** > **Basic**.

При поставување од Epson Device Admin:

Изберете **Common** > **Email Server** > **Mail Server Settings** од шаблонот за конфигурација.

Ставка	Поставки и објаснување	
Authentication Method	Одредете го начинот на автентикација кога скенерот пристапува до серверот за е-пошта.	
	Off	Автентикацијата е оневозможена при комуникација со серверот за е-пошта.
	SMTP AUTH	Серверот за е-пошта треба да поддржува SMTP-автентикација.
	POP before SMTP	Ако ја изберете оваа ставка, поставете POP3-сервер.
Authenticated Account	Ако изберете **SMTP AUTH** или **POP before SMTP** како **Authentication Method**, внесете го името на автентицираната сметка. Внесете од 0 до 255 знаци во ASCII (0x20 – 0x7E).	
Authenticated Password	Ако изберете **SMTP AUTH** или **POP before SMTP** како **Authentication Method**, внесете ја автентицираната лозинка. Внесете од 0 до 20 знаци во ASCII (0x20 – 0x7E).	
Sender's Email Address	Внесете ја адресата на е-пошта на испраќачот. Внесете од 0 до 255 знаци во ASCII (0x20 – 0x7E) освен : ( ) < > [ ] ; ¥. Точка „.“ не може да биде првиот знак.	
SMTP Server Address	Внесете од 0 до 255 знаци користејќи A – Z a – z 0 – 9 . -. Може да користите IPv4 или FQDN-формат.	
SMTP Server Port Number	Внесете број од 1 до 65535.	
Secure Connection	Одредете го начинот на безбедно поврзување за серверот за е-пошта.	
	None	Ако изберете **POP before SMTP** во **Authentication Method**, начинот на поврзување е поставен на **None**.
	SSL/TLS	Ова е достапно кога **Authentication Method** е поставен на **Off** или **SMTP AUTH**.
	STARTTLS	Ова е достапно кога **Authentication Method** е поставен на **Off** или **SMTP AUTH**.
Certificate Validation	Кога ова е овозможено, се врши автентикација на сертификатот. Препорачуваме да го поставите ова на **Enable**.	
POP3 Server Address	Ако изберете **POP before SMTP** како **Authentication Method**, внесете ја адресата на POP3-серверот. Внесете од 0 до 255 знаци користејќи A – Z a – z 0 – 9. Може да користите IPv4 или FQDN-формат.	
POP3 Server Port Number	Ако изберете **POP before SMTP** како **Authentication Method**, наведете го бројот на портата. Внесете број од 1 до 65535.	

Поставување на Scan to My Folder

Ги зачувува скенираните слики во папката назначена за секој корисник. Користете го следниов начин за да одредите назначена папка.

Белешка:
*Може да поставите **Scan To My Folder** само кога **Scan to Network Folder/FTP** е овозможено.*

Поставка „Зачувај во“	Authentication Method	Локација на поставката за патеката на папката
Одредете една мрежна папка за сите Authentication Settings, за да може автоматски да се создаде лична папка под одредената папка именувана по ID на корисникот.	❏ Local DB ❏ LDAP ❏ Local DB and LDAP	Скенер (поставка Scan to My Folder)
Назначете различни мрежни папки, посебно за секој корисник.	Local DB	Скенер (User Settings)
	LDAP	LDAP-атрибути
	Local DB and LDAP	Скенер (User Settings) или LDAP-атрибути

При поставување од Web Config:

Изберете ја картичката **Product Security** > **Scan to Network Folder/FTP**.

При поставување од Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Scan to Network Folder/FTP** > **Scan to My Folder** од шаблонот за конфигурација.

Ставка		Објаснување
Save To Setting	Setting Type	❏ **Shared**: Автоматски создава папка именувана по ID на корисникот под патеката на папката или URL-адресата одредена во **Save to** и ги зачувува скенираните слики во оваа папка. ❏ **Individual**: Поставете ја дестинацијата за зачувување на резултатите од скенирањето за секој корисник. Корисниците на Local DB може да се постават во корисничките поставки. Корисниците на LDAP ја користат локацијата за складирање добиена од атрибутите за пребарување на LDAP-серверот.
	Type	Изберете го протоколот за пренос според излезната дестинација за скенирањето. За мрежна папка: **Network Folder (SMB)** За FTP-сервер: **FTP**
	Save to	Наведете ја патеката или URL-адресата на излезната патека. Внесете до 160 знаци во Unicode (UTF-16).
	Connection Mode	Поставете го кога ќе изберете **FTP** во **Type**. Изберете режим на поврзување со FTP-серверот.
	Port Number	Поставете го кога ќе изберете **FTP** во **Type**. Внесете го бројот на портата (од 0 до 65535) за испраќање на скенираните податоци до FTP-сервер.

Ставка		Објаснување
Authentication Settings	Setting Type	Поставете го кога ќе изберете **Individual** како **Setting Type** во **Save To Setting**. Поставете „User Name" и „Password" за пристап до папката. ❏ **Shared**: Користете заедничко **User Name** и **Password** за сите корисници. ❏ **Individual**: За корисници на Local DB, поставете **User Name** и **Password** поединечно во **Кориснички поставки**. Корисниците на LDAP не може да се конфигурираат поединечно. **User Name** и **Password** поставени во оваа ставка се користат заедно.
	User Name	Внесете го корисничкото име за пристап до дестинациската папка со резултатите од скенирањето. Внесете до 30 знаци во Unicode (UTF-16). Поставете го ова кога користите **Shared** или LDAP-сервер.
	Password	Внесете ја лозинката за соодветното **User Name**. Внесете до 20 знаци во Unicode (UTF-16). Поставете го ова кога користите **Shared** или LDAP-сервер.

Забрана за менување на дестинацијата за Scan to Network Folder/FTP

Ставка	Објаснување
Prohibit manual entry of destination	Кога е овозможено, корисникот не може да ја промени стандардната дестинација.

Customize One-touch Functions

Може да изберете да се прикажуваат само потребните икони така што ќе го измените распоредот на иконите прикажан на почетниот екран за контролната табла.

При поставување од Web Config:

Изберете ја картичката **Product Security** > **Customize One-touch Functions**.

При поставување од Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** од шаблонот за конфигурација.

Белешка:
Во следниве случаи, иконите за наведените функции не се прикажуваат на почетниот екран.

❏ *Ако изберете функции што не се дозволени поради **Restrictions**.*

❏ *Ако адресата на е-пошта за најавен корисник не е регистрирана. (Scan to My Email)*

❏ *Кога дестинациската папка не е поставена. (Scan to My Folder)*

Ставка	Објаснување
Maximum functions per screen	Изберете го распоредот на иконите што се прикажуваат на контролната табла. Сликата се менува според избраниот распоред.
Screen(s)	Изберете го бројот на страници.
Number	Изберете ги функциите што сакате да се прикажуваат за секоја нумерирана позиција.

Извештаи со Job History преку Epson Device Admin

Може да создадете извештај со Job History за секоја група и секој корисник преку Epson Device Admin. Може да зачувате до 3000 ставки со историја на користење во скенерот. Извештајот може да го создадете така што ќе одредите период или ќе поставите редовен распоред.

За да создадете извештај со Job History, изберете **Options** > **Epson Print Admin Serverless/ Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** од менито со ленти на екранот со списокот со уреди.

За детали околу тоа како да создадете кориснички извештај, погледнете во документацијата за Epson Device Admin.

Ставки што може да бидат вклучени во извештајот

Може да ги вклучите следниве ставки во корисничкиот извештај.

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

Најавете се како администратор од контролната табла

Може да користите кој било од следниве начини за да се најавите како администратор од контролната табла на скенерот.

1. Допрете  во горниот десен агол на екранот.
   - ❏ Кога Authentication Settings е овозможено, иконата се прикажува на екранот **Добредојдовте** (екранот во мирување за автентикација).
   - ❏ Кога Authentication Settings е оневозможено, иконата се прикажува на почетниот екран.
2. Допрете **Да** кога ќе се прикаже екранот за потврда.

3. Внесете ја администраторската лозинка.

   Се прикажува порака што ве известува дека најавувањето е извршено, а потоа се прикажува почетниот екран на контролната табла.

За да се одјавите, допрете  во горниот десен агол на почетниот екран.

Оневозможување Authentication Settings

Може да оневозможите Authentication Settings преку Web Config.

Белешка:
User Settings регистрирани на скенерот ќе бидат зачувани дури и ако Authentication Settings е оневозможено. Може да ги отстраните така што ќе го вратите скенерот на неговите стандардни поставки.

1. Одете на Web Config.
2. Изберете ја картичката **Product Security** > **Basic** > **Authentication**.
3. Изберете **OFF**.
4. Кликнете **Next**.
5. Кликнете **OK**.

Белешка:
Дури и ако оневозможите Authentication Settings, Поставка за заклучување останува овозможено. Ако сакате да го оневозможите, може да одредите поставки преку контролната табла или преку Web Config.

Поврзани информации

➡ „Поставување Поставка за заклучување од контролната табла“ на страница 92
➡ „Поставување Поставка за заклучување преку Web Config“ на страница 92

Бришење информации за Authentication Settings (Врати ги стандардните поставки)

За да ги избришете сите информации за Authentication Settings (Card Reader, Authentication Method, User Settings итн.), вратете ги сите поставки за скенерот на стандардните поставки.

Изберете **Поставки** > **Администрир. на систем** > **Врати ги стандардните поставки** > **Сите поставки** на контролната табла.

Важно:
Ќе се избришат и сите контакти и други мрежни поставки. Избришаните поставки не може да се вратат.

Решавање проблеми

Картичката за автентикација не може да се прочита

Проверете го следново.

❏ Проверете дали уредот за автентикација е правилно поврзан со скенерот.

Поврзете го уредот за автентикација со USB-портата за надворешен интерфејс на задната страна на скенерот.

❏ Проверете дали се поддржани уредот за автентикација и картичката за автентикација.

Одржување

Чистење на надворешноста на скенерот

Исчистете ги дамките на надворешната површина на куќиштето со сува крпа или со крпа навлажнета со благ детергент и вода.

Важно:

- *Не користете алкохол, разредувач или корозивен растворувач за да го чистите скенерот. Може да дојде до деформација или промена на бојата.*
- *Не дозволувајте да навлезе вода во производот. Тоа може да предизвика дефект.*
- *Не отворајте го куќиштето на скенерот.*

1. Притиснете го копчето ⏻ за да го исклучите скенерот.
2. Исклучете го адаптерот за наизменична струја од скенерот.
3. Чистете ја надворешната површина на куќиштето со крпа навлажнета со благ детергент и вода.

   Белешка:
   Избришете го екранот на допир со мека, сува крпа.

Чистење на внатрешноста на скенерот

Откако ќе го користите скенерот одредено време, хартијата и прашината од просторијата на валјакот или на стаклениот дел во внатрешноста на скенерот може да предизвикаат проблеми со внесувањето на хартијата или со квалитетот на скенираните слики. Чистете ја внатрешноста на скенерот на секои 5,000 скенирања.

Може да го проверите последниот број на скенирања на контролната табла или во Epson Scan 2 Utility.

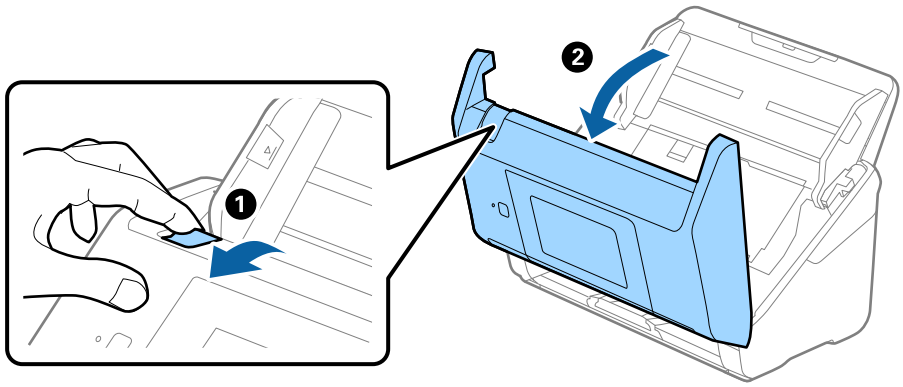
Ако некоја површина има дамки од материјал што тешко се отстранува, користете оригинална опрема за чистење на Epson за да ги отстраните дамките. Користете мало количество средство за чистење на крпата за чистење за да ги отстраните дамките.

Важно:

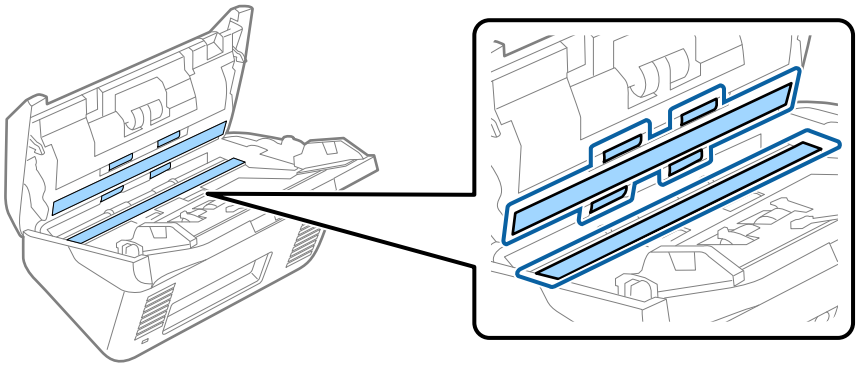
- *Не користете алкохол, разредувач или корозивен растворувач за да го чистите скенерот. Може да дојде до деформација или промена на бојата.*
- *Не распрскувајте течности или подмачкувачи врз скенерот. Оштетувањето на опремата или струјните кола може да предизвика неправилно функционирање.*
- *Не отворајте го куќиштето на скенерот.*

1. Притиснете го копчето ⏻ за да го исклучите скенерот.
2. Исклучете го адаптерот за наизменична струја од скенерот.

3. Повлечете ја рачката и отворете го капакот за скенерот.



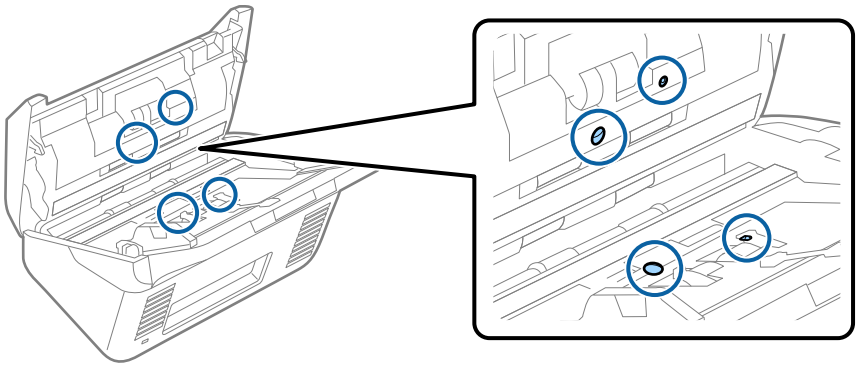
4. Избришете ги дамките на пластичниот валјак и на стаклената површина на дното на внатрешноста на капакот за скенерот со мека крпа или со оригинална опрема за чистење на Epson.



Важно:

- ❏ *Не притискајте премногу на стаклената површина.*
- ❏ *Не користете четка или тврда алатка. Гребаници на стаклото може да влијаат врз квалитетот на скенирањето.*
- ❏ *Не прскајте средство за чистење директно на стаклената површина.*

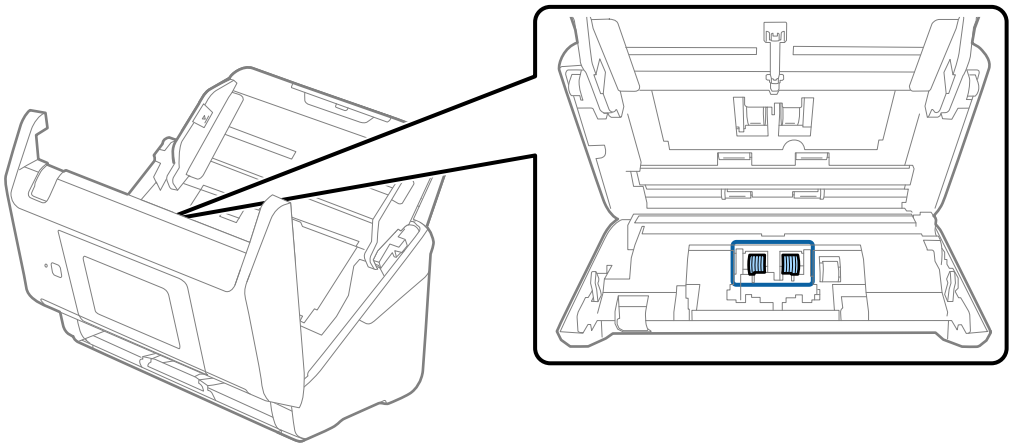
5. Избришете ги дамките на сензорите со памучна чепкалка за уши.



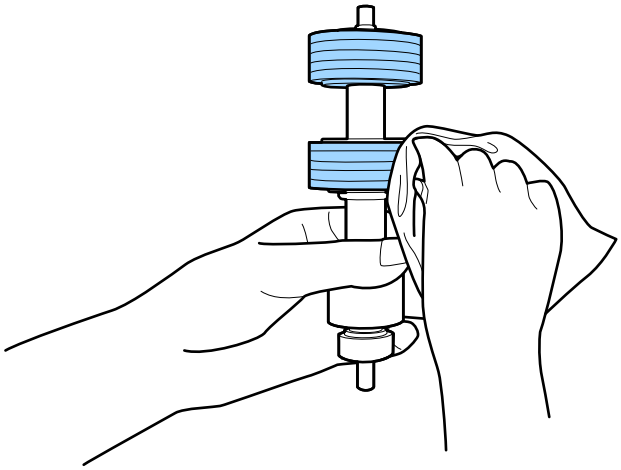
> ***Важно:***
>
> *Не нанесувајте течност како што е средство за чистење на чепкалката за уши.*

6. Отворете го капакот, а потоа извадете го валјакот за одвојување хартија.

   За повеќе детали, погледнете во „Заменување на склопот со валјаци".



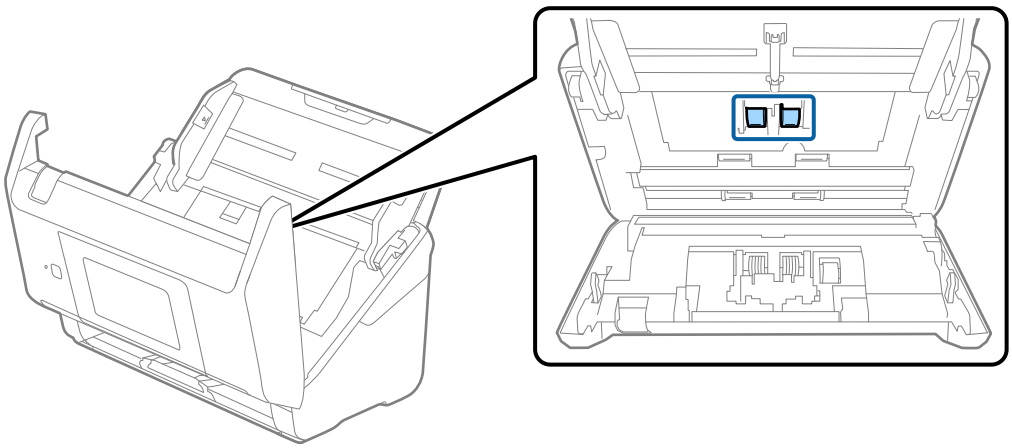
7. Избришете ја прашината или нечистотијата на валјакот за одвојување хартија користејќи оригинална опрема за чистење на Epson или мека, влажна крпа.



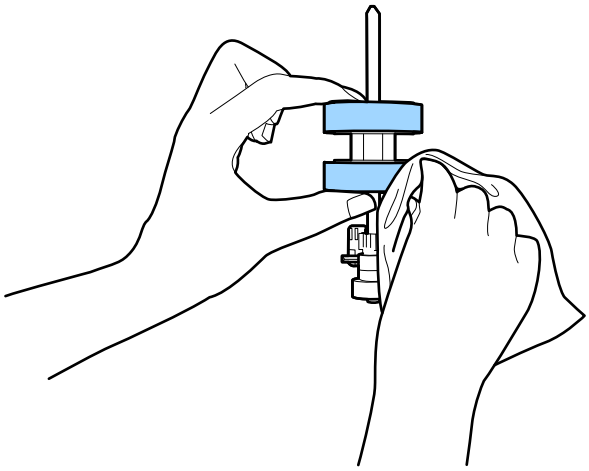
> ***Важно:***
>
> *Користете само оригинална опрема за чистење на Epson или мека, влажна крпа за да го исчистите валјакот. Користењето сува крпа може да доведе до оштетување на површината на валјакот.*

8. Отворете го капакот, а потоа извадете го валјакот за земање хартија.

   За повеќе детали, погледнете во „Заменување на склопот со валјаци".



9. Избришете ја прашината или нечистотијата на валјакот за земање хартија користејќи оригинална опрема за чистење на Epson или мека, влажна крпа.



> ***Важно:***
>
> *Користете само оригинална опрема за чистење на Epson или мека, влажна крпа за да го исчистите валјакот. Користењето сува крпа може да доведе до оштетување на површината на валјакот.*

10. Затворете го капакот за скенерот.

11. Приклучете го адаптерот за наизменична струја, а потоа вклучете го скенерот.

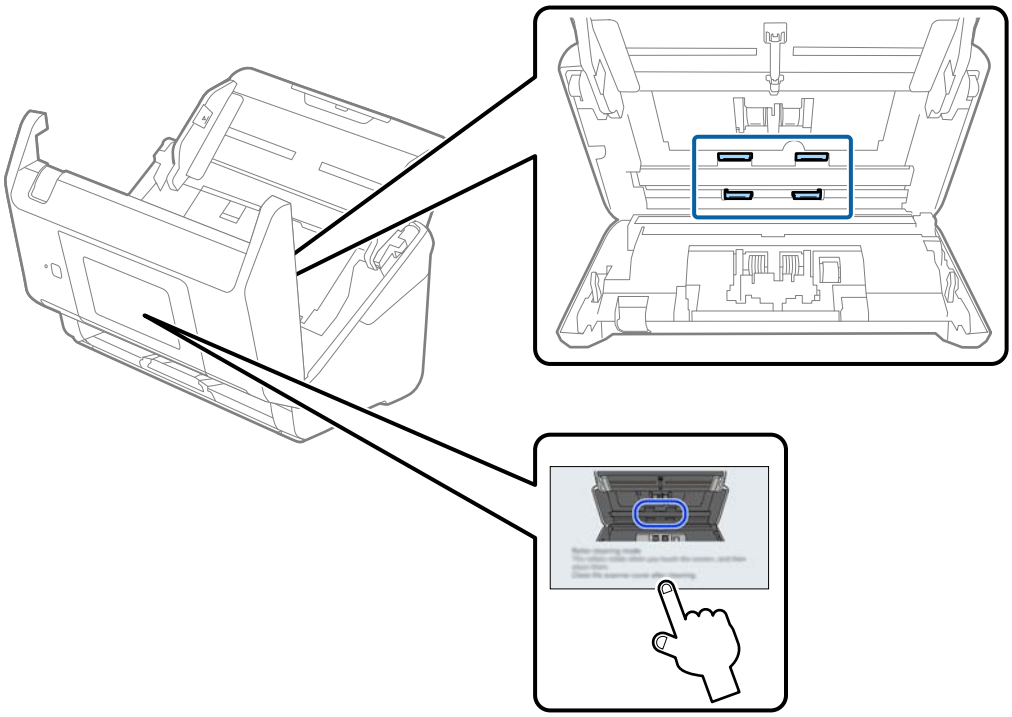
12. Изберете **Одржување на скенер** од почетниот екран.

13. На екранот **Одржување на скенер** изберете **Чистење на валјак**.

14. Повлечете ја рачката за да го отворите капакот за скенерот.

    Скенерот влегува во режимот за чистење валјаци.

15. Бавно вртете ги валјаците на долниот дел допирајќи на кој било дел од LCD. Избришете ја површината на валјаците користејќи оригинална опрема за чистење на Epson или мека крпа навлажнета со вода. Повторувајте го ова додека не ги исчистите валјаците.



> ***Внимание:***
>
> *Внимавајте да не ги фатите дланките или косата во механизмот кога ракувате со валјакот. Тоа може да предизвика повреда.*

16. Затворете го капакот за скенерот.

    Скенерот излегува од режимот за чистење валјаци.

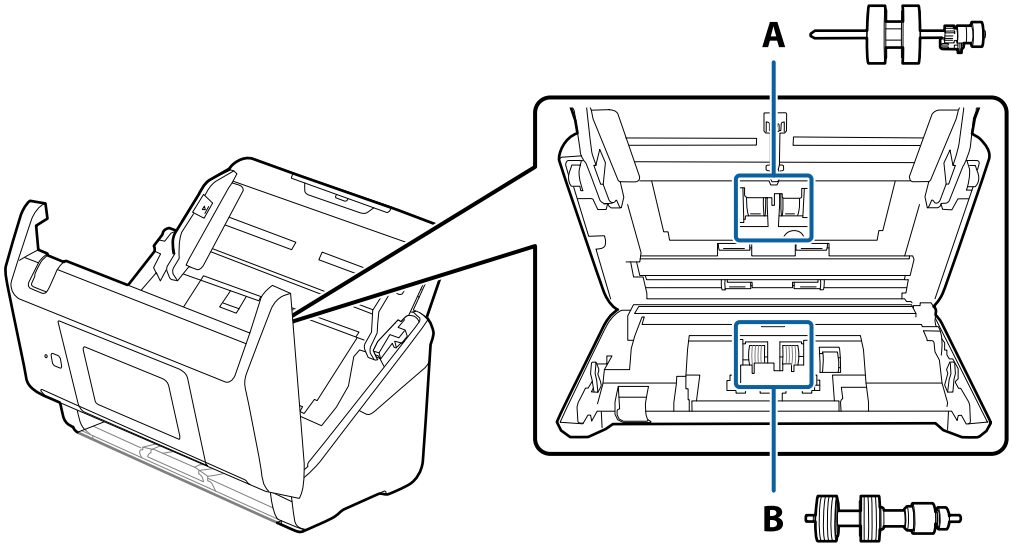
Поврзани информации

➡ „Замена на склопот со валјаци“ на страница 168

Замена на склопот со валјаци

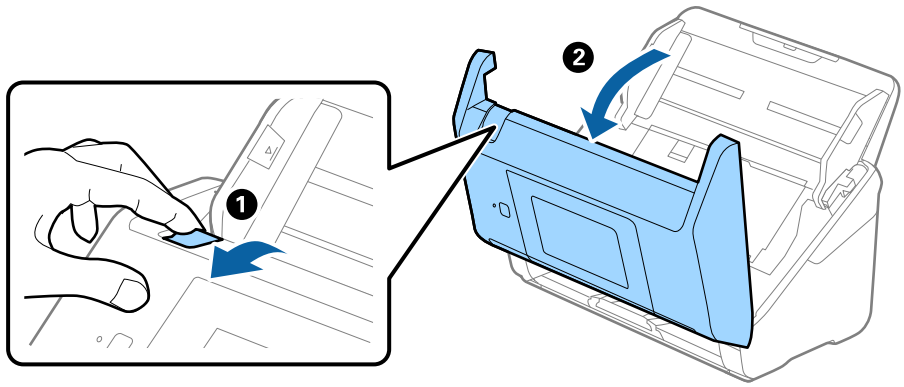
Треба да го замените склопот со валјаци (валјакот за земање хартија и валјакот за одвојување хартија) кога бројот на скенирања ќе го надмине работниот век на валјаците. Кога на

контролната табла или на екранот на компјутерот ќе се прикаже пораката за замена, следете ги чекорите подолу и извршете замена.

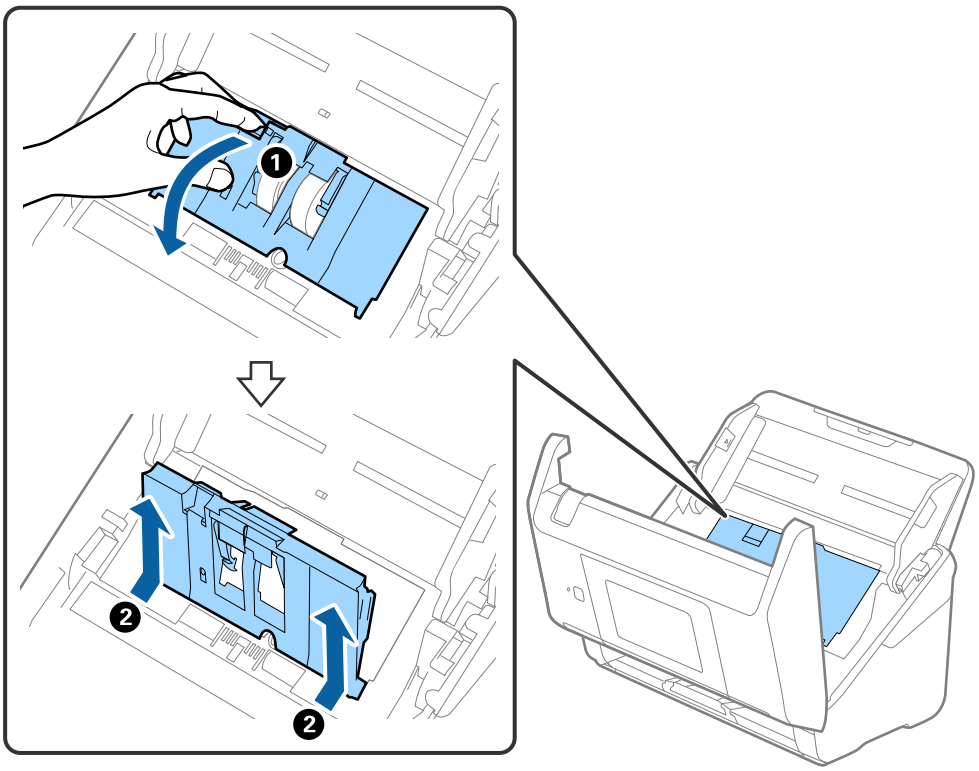


A: валјак за земање хартија, B: валјак за одвојување хартија

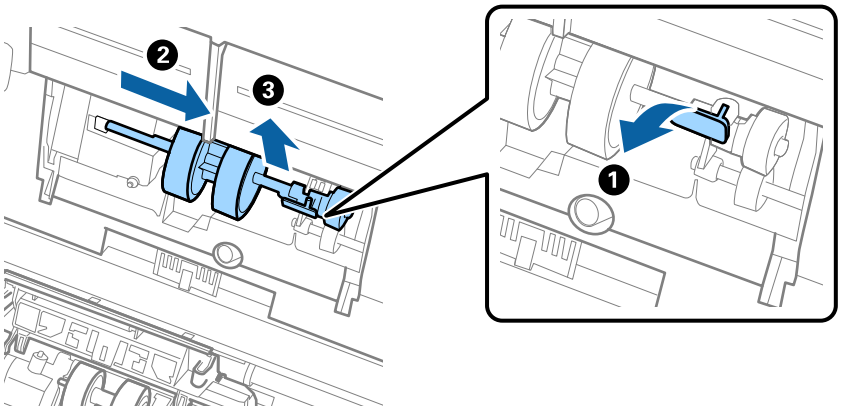
1. Притиснете го копчето ⏻ за да го исклучите скенерот.
2. Исклучете го адаптерот за наизменична струја од скенерот.
3. Повлечете ја рачката и отворете го капакот за скенерот.



4. Отворете го капакот за валјакот за земање хартија, па повлечете го и извадете го.

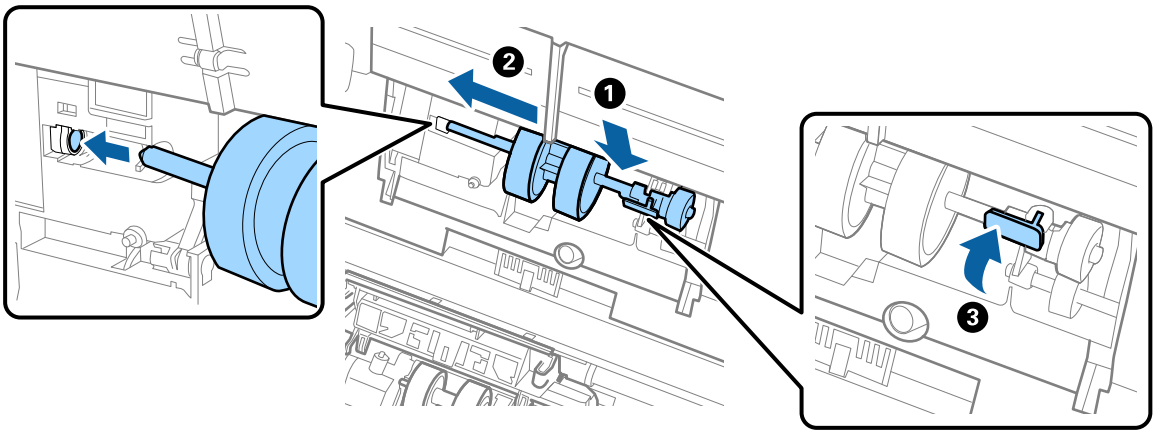


5. Повлечете го надолу елементот на оската за валјакот, а потоа повлечете го и извадете го инсталираниот валјак за земање хартија.

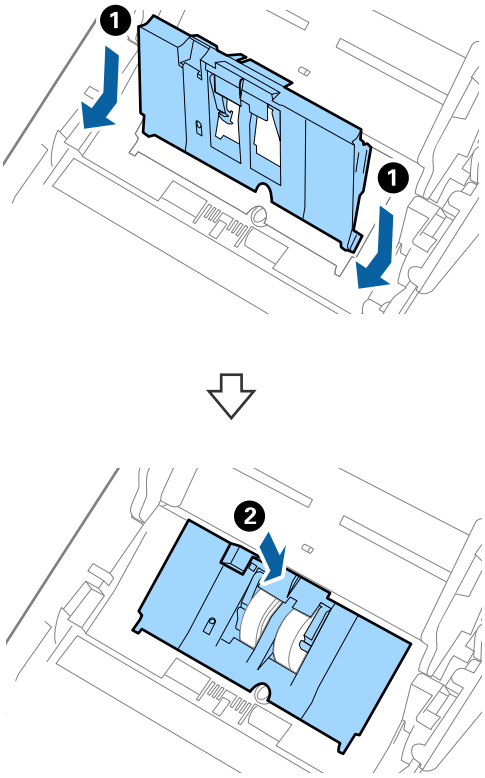


> ***Важно:***
>
> *Не извлекувајте го валјакот за земање хартија со прекумерна сила. Така може да се оштети внатрешноста на скенерот.*

6. Додека го држите елементот надолу, повлечете го новиот валјак за земање хартија налево и вметнете го во дупката во скенерот. Притиснете го елементот за да го фиксирате.

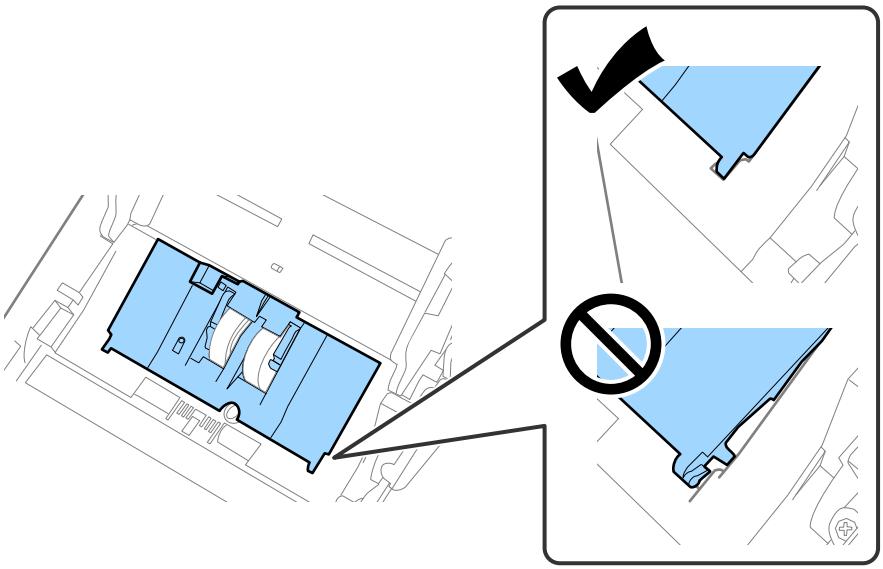


7. Ставете го работ на капакот за валјакот за земање хартија во вдлабнатината и провлечете го. Добро затворете го капакот.

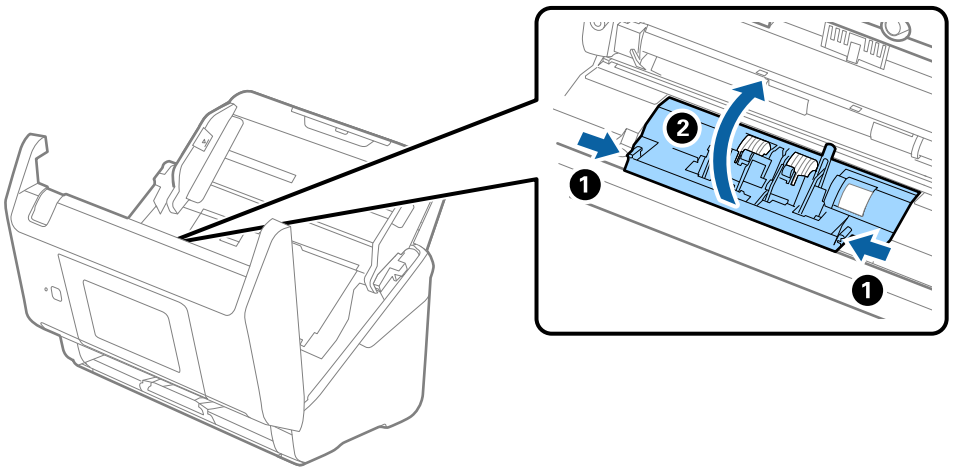


Важно:

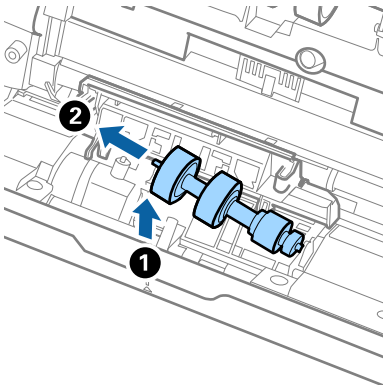
- ❏ *Погрижете се капакот да биде правилно затворен.*
- ❏ *Ако капакот тешко се затвора, проверете дали валјакот за земање хартија е инсталиран правилно.*
- ❏ *Не инсталирајте го капакот додека е подигнат.*



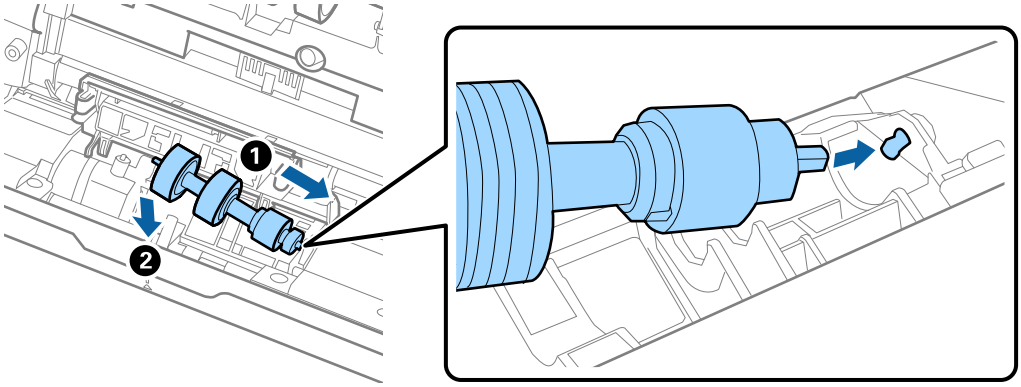
8. За да го отворите капакот, турнете ги куките на двата краја од капакот за валјакот за одвојување хартија.



9. Подигнете ја левата страна на валјакот за одвојување хартија, па повлечете го и извадете го инсталираниот валјак за одвојување хартија.



10. Вметнете ја оската на новиот валјак за одвојување хартија во дупката на десната страна и спуштете го валјакот.



11. Затворете го капакот за валјакот за одвојување хартија.

> ***Важно:***
>
> *Ако капакот тешко се затвора, проверете дали валјакот за одвојување хартија е инсталиран правилно.*

12. Затворете го капакот за скенерот.

13. Приклучете го адаптерот за наизменична струја, а потоа вклучете го скенерот.

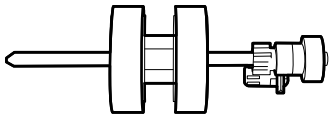
14. Ресетирајте го бројот на скенирања на контролната табла.

Белешка:
Депонирајте ги валјакот за земање хартија и валјакот за одвојување хартија согласно правилата и прописите на локалните власти. Не расклопувајте ги.

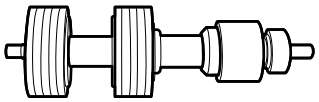
Кодови за склопот со валјаци

Кога бројот на скенирања ќе го надмине сервисниот број, треба да ги замените деловите (валјакот за земање хартија и валјакот за одвојување хартија). Тековниот број на скенирања може да го видите на контролната табла или во Epson Scan 2 Utility.

A



B



A: валјак за земање хартија, B: валјак за одвојување хартија

Име на дел	Кодови	Работен век
Склоп со валјаци	B12B819671 B12B819681 (само за Индија)	200,000*

* Овој број е добиен со последователно скенирање со оригинална хартија на Epson за тестирање и претставува водич за циклусот за замена. Циклусот за замена може да варира во зависност од различните типови хартија, на пр. хартија што генерира многу прашина или хартија со груба површина што може да го скрати работниот век.

Ресетирање на бројот на скенирања

Ресетирајте го бројот на скенирања откако ќе го замените склопот со валјаци.

1. Изберете **Поставки** > **Информации за уред** > **Ресетирајте го бројот на скенирања** > **Бр. на ск. по зам. на валјакот** од почетниот екран.
2. Допрете **Да**.

Поврзани информации

➡ „Замена на склопот со валјаци“ на страница 168

Штедење енергија

Кога скенерот не извршува задачи, може да штедите енергија со користење на режимот на спиење или режимот за автоматско исклучување. Може да поставите временски период за скенерот да влезе во режимот на спиење и да се исклучи автоматски. Секое зголемување ќе влијае врз енергетската ефикасност на производот. Имајте ја предвид животната средина пред да вршите промени.

1. Изберете **Поставки** на почетниот екран.

2. Изберете **Осн поставки**.

3. Изберете **Поставки за искл.**, а потоа одредете ги поставките.

   Белешка:
   Достапните функции може да се разликуваат во зависност од локацијата на набавка.

Пренесување на скенерот

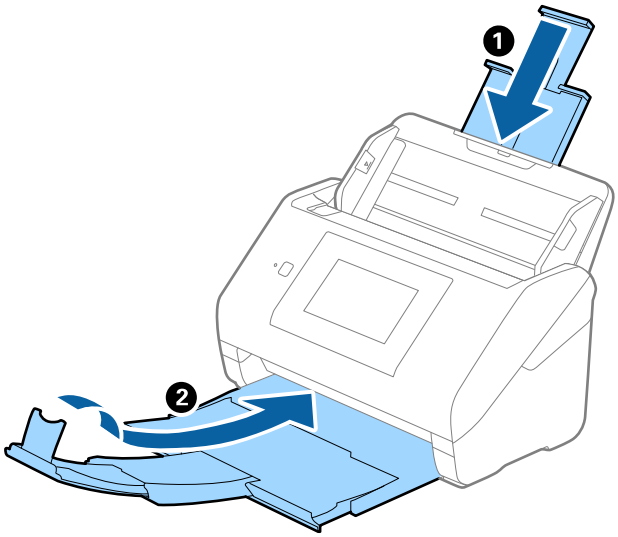
Кога треба да го пренесете скенерот за да го преместите или за поправка, следете ги чекорите дадени подолу за пакување на скенерот.

1. Притиснете на копчето ⏻ за да го исклучите скенерот.

2. Исклучете го струјниот адаптер.

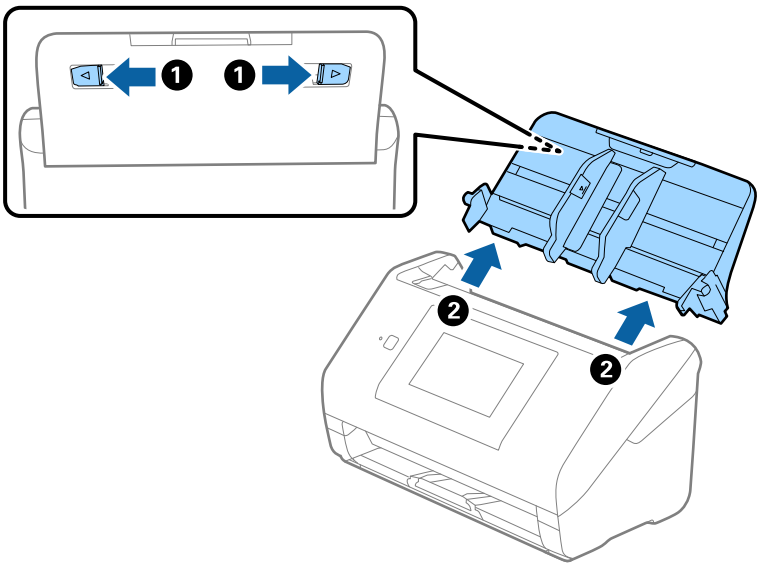
3. Извадете ги каблите и уредот.

4. Затворете ги издолжувањето на влезната фиока и излезната фиока.



> ***Важно:***
> *Погрижете се добро да ја затворите излезната фиока; во спротивно може да се оштети за време на пренесувањето.*

5. Отстранете ја влезната фиока.



6. Ставете ги материјалите за пакување што се испорачани со скенерот, потоа препакувајте го скенерот во неговата оригинална кутија или во цврста кутија.

Правење резервна копија на поставките

Може да ја извезете вредноста на поставката поставена од Web Config во датотеката. Може да ја користите за правење резервна копија од контактите, вредности на поставките, замена на скенерот итн.

Извезената датотека не може да се уредува бидејќи е извезена како бинарна датотека.

Извезете ги поставките

Извезете ја поставката за скенерот.

1. Пристапете до Web Config, а потоа изберете го јазичето **Device Management** > **Export and Import Setting Value** > **Export**.

2. Изберете ги поставките коишто сакате да ги извезете.

   Изберете ги поставките коишто сакате да ги извезете. Ако изберете слична категорија, избрани се и поткатегориите. Меѓутоа, не може да ги изберете поткатегориите коишто предизвикуваат грешки со удвојување во рамките на истата мрежа (како на пример IP адреса итн.).

3. Внесете лозинка за да ја шифрирате извезената датотека.

   Потребна ви е лозинка за да ја увезете датотеката. Оставете го ова празно ако не сакате да ја шифрирате датотеката.

4. Кликнете на **Export**.

> ***Важно:***
>
> *Ако сакате да ги извезете мрежните поставки за скенерот, како на пример името на уредот и IPv6 адресата, изберете **Enable to select the individual settings of device** и изберете уште ставки. Користете ги избраните вредности само за скенерот за замена.*

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач" на страница 38

Увезување поставки

Увезете ја извезената датотека од Web Config во скенерот.

> ***Важно:***
>
> *Кога увезувате вредности што вклучуваат поединечни информации, како што се име на скенер или IP-адреса, погрижете се да нема иста IP-адреса на истата мрежа.*

1. Одете на Web Config, а потоа изберете ја картичката **Device Management** > **Export and Import Setting Value** > **Import**.
2. Изберете ја изнесената датотека и внесете ја шифрираната лозинка.
3. Кликнете **Next**.
4. Изберете ги поставките што сакате да ги увезете, а потоа кликнете **Next**.
5. Кликнете **OK**.

Поставките се увезуваат во скенерот.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач" на страница 38

Врати ги стандардните поставки

На контролната табла, изберете **Поставки** > **Администрир. на систем** > **Врати ги стандардните поставки**, а потоа изберете ги ставките што сакате да ги вратите на стандардните вредности.

- ❏ Поставки за мрежа: вратете ги мрежните поставки на нивниот почетен статус.
- ❏ Се освен Поставки за мрежа: вратете ги другите поставки на нивниот почетен статус, освен мрежните поставки.
- ❏ Сите поставки: вратете ги сите поставки на нивниот почетен статус што важел при купувањето.

Важно:

*Ако изберете и извршите **Сите поставки**, ќе се избришат сите податоци за поставките регистрирани во скенерот, вклучително и поставките за контактите и автентикацијата на корисници. Избришаните поставки не може да се вратат.*

Ажурирање на апликациите и фирмверот

Со ажурирањето на апликациите и фирмверот можно е да отстраните одредени проблеми и да подобрите или додадете функции. Проверете дали ги користите најновите верзии на апликациите и фирмверот.

Важно:

❏ *Не исклучувајте ги компјутерот или скенерот додека трае ажурирањето.*

Белешка:

*Кога скенерот може да се поврзе на интернет, може да го ажурирате фирмверот преку Web Config. Изберете ја картичката **Device Management** > **Firmware Update**, проверете ја прикажаната порака, а потоа кликнете **Start**.*

1. Проверете дали скенерот е поврзан со компјутерот и дали компјутерот е поврзан на интернет.

2. Вклучете ја EPSON Software Updater и ажурирајте ги апликациите или фирмверот.

   Белешка:

   Windows Server оперативните системи не се поддржани.

   ❏ Windows 10

   Кликнете го копчето Старт, а потоа изберете **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Внесете го името на апликацијата во полето за пребарување, а потоа изберете ја прикажаната икона.

   ❏ Windows 7

   Кликнете го копчето Старт, а потоа изберете **Сите програми** или **Програми** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Изберете **Finder** > **Оди** > **Апликации** > **Epson Software** > **EPSON Software Updater**.

Белешка:

Ако во списокот не можете да ја најдете апликацијата што сакате да ја ажурирате, нема да може да извршите ажурирање со помош на EPSON Software Updater. Проверете дали се достапни најнови верзии од апликациите на веб-локацијата на локалното претставништво на Epson.

http://www.epson.com

Ажурирање на фирмверот на скенерот користејќи ја контролната табла

Ако скенерот може да се поврзе на интернет, може да го ажурирате фирмверот на скенерот користејќи ја контролната табла. Може и да поставите скенерот редовно да проверува дали има ажурирања за фирмверот и да ве известува ако се достапни.

1. Изберете **Поставки** на почетниот екран.

2. Изберете **Администрир. на систем** > **Ажурирање на фирмвер** > **Ажурирај**.

   Белешка:
   *Изберете **Известување** > **Вкл.** за да поставите скенерот редовно да проверува дали се достапни ажурирања за фирмверот.*

3. Проверете ја пораката прикажана на екранот и започнете да пребарувате достапни ажурирања.

4. Ако пораката се прикаже на LCD екранот и ве извести дека е достапно ажурирање за фирмвер, следете ги упатствата на екранот за да започнете со ажурирање.

   Важно:
   - *Не исклучувајте го скенерот и не вадете го неговиот кабел за напојување пред да заврши ажурирањето; во спротивно, скенерот може да не работи правилно.*
   - *Ако ажурирањето на фирмверот не е завршено или е неуспешно, скенерот нема да стартува како вообичаено и на LCD-екранот ќе се прикаже „Recovery Mode" при следното вклучување на скенерот. Во оваа ситуација, потребно е повторно да го ажурирате фирмверот со користење на компјутер. Поврзете го скенерот со компјутерот користејќи USB-кабел. Кога на скенерот се прикажува „Recovery Mode", не може да го ажурирате фирмверот преку мрежна врска. На компјутерот, отворете ја веб-локацијата на локалното претставништво на Epson и преземете ја најновата верзија на фирмверот за скенерот. Погледнете ги упатствата на интернет страницата за следни чекори.*

Ажурирање на фирмверот преку Web Config

Кога скенерот може да се поврзе на интернет, може да го ажурирате фирмверот преку Web Config.

1. Одете на Web Config и изберете ја картичката **Device Management** > **Firmware Update**.

2. Кликнете **Start**, а потоа следете ги инструкциите на екранот.

   Започнува потврдувањето на фирмверот, а информациите за фирмверот се прикажуваат ако постои ажуриран фирмвер.

Белешка:
Може да го ажурирате фирмверот и преку Epson Device Admin. Информациите за фирмверот може визуелно да ги потврдите во списокот со уреди. Тоа е корисно кога сакате да ажурирате фирмвер на повеќе уреди. За повеќе информации, погледнете во водичот или помошта за Epson Device Admin.

Поврзани информации

➡ „Извршување Web Config на веб-прелистувач" на страница 38

Ажурирање фирмвер без поврзување на интернет

Можете да го преземете фирмверот за уредот од веб-страницата на Epson директно на компјутер и потоа да го поврзете уредот и компјутерот преку USB кабел за да го ажурирате фирмверот. Ако не можете да го ажурирате преку мрежата, обидете се со овој метод.

Белешка:
Пред да ажурирате, погрижете се двигателот за скенерот Epson Scan 2 да биде инсталиран на компјутерот. Ако Epson Scan 2 не е инсталирана, инсталирајте ја.

1. Посетете ја веб-локацијата на Epson за да проверите дали се достапни ажурирања за фирмверот.

   http://www.epson.com

   ❏ Ако има фирмвер за вашиот скенер, преземете го и одете на следниот чекор.

   ❏ Ако на веб-локацијата нема информации за фирмвер, тоа значи дека веќе го користите најновиот фирмвер.

2. Поврзете го компјутерот којшто го содржи преземениот фирмвер со скенерот преку USB-кабел.

3. Кликнете двапати на преземената .exe датотека.

   Epson Firmware Updater се вклучува.

4. Следете ги упатствата на екранот.