EPSON
EXCEED YOUR VISION

DS-790WN

Administratora rokasgrāmata

NPD6726-00 LV

Autortiesības

Preču zīmes

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION un to logotipi ir reģistrētas preču zīmes vai uzņēmuma „Seiko Epson" preču zīmes.
- ❏ 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 un PaSoRi ir uzņēmuma „Sony Corporation" reģistrētas preču zīmes.
- ❏ MIFARE ir uzņēmuma „NXP Semiconductor Corporation" reģistrēta preču zīme.
- ❏ Vispārīga norāde. Citi šeit izmantotie produktu nosaukumi ir paredzēti tikai identificēšanai, un tie var būt to attiecīgo īpašnieku preču zīmes. Epson nepretendē uz jebkādām šo preču zīmju tiesībām.

Satura rādītājs

Tīkla drošības iestatījumi

Authentication Settings

Apkope

Ievads

Šī dokumenta saturs

Šis dokuments skenera administratoriem sniedz turpmāk minēto informāciju.

❏ Tīkla iestatījumi

❏ Skenēšanas funkciju sagatavošana

❏ Drošības iestatījumu iespējošana un pārvaldība

❏ Authentication Settings iespējošana un pārvaldība

❏ Ikdienas apkopes veikšana

Lai iegūtu informāciju par standarta skenera izmantošanas metodēm, skatiet *Lietotāja rokasgrāmata*.

Piezīme:
Šis dokuments izskaidro Authentication Settings, kas sniedz atsevišķu autentifikāciju bez autentifikācijas servera izmantošanas. Papildus šajā rokasgrāmatā izskaidrotajiem Authentication Settings, jūs varat izveidot autentifikācijas sistēmu, izmantojot autentifikācijas serveri. Lai izveidotu sistēmu, izmantojiet Document Capture Pro Server Authentication Edition (saīsinātais nosaukums ir Document Capture Pro Server AE).

Lai iegūtu plašāku informāciju, sazinieties ar vietējo Epson biroju.

Šīs pamācības izmantošana

Zīmes un simboli

> ***Brīdinājums:***
> *Instrukcijas, kas stingri jāievēro, lai izvairītos no fiziskām traumām.*

> ***Svarīga informācija:***
> *Instrukcijas, kas jāievēro, lai nepieļautu aparatūras bojājumus.*

Piezīme:
Sniedz papildinformāciju un informāciju uzziņām.

Saistītā informācija

➡ Saites uz saistītajām sadaļām.

Šajā rokasgrāmatā lietotie apraksti

❏ Lietotņu ekrānuzņēmumi iegūti no Windows 10 vai macOS High Sierra. Ekrānos redzamais saturs var atšķirties atkarībā no modeļa un situācijas.

❏ Šajā rokasgrāmatā izmantotie attēli paredzēti tikai atsaucei. Lai gan tie var nedaudz atšķirties no faktiskās ierīces, darba paņēmieni ir tādi paši.

Atsauces uz operētājsistēmām

Windows

Šajā rokasgrāmatā izmantotie termini, piemēram „Windows 10", „Windows 8.1", Windows 8", „Windows 7", „Windows Server 2019", „Windows Server 2016", „Windows Server 2012 R2", „Windows Server 2012", un „Windows Server 2008 R2" attiecas uz turpmāk norādītajām operētājsistēmām. Turklāt „Windows" lietots attiecībā uz visām versijām, bet „Windows Server" attiecas uz Windows Server 2019„Windows Server 2016", „Windows Server 2012 R2", „Windows Server 2012", un „Windows Server 2008 R2".

❏ Operētājsistēma Microsoft® Windows® 10

❏ Operētājsistēma Microsoft® Windows® 8.1

❏ Operētājsistēma Microsoft® Windows® 8

❏ Operētājsistēma Microsoft® Windows® 7

❏ Operētājsistēma Microsoft® Windows Server® 2019

❏ Operētājsistēma Microsoft® Windows Server® 2016

❏ Operētājsistēma Microsoft® Windows Server® 2012 R2

❏ Operētājsistēma Microsoft® Windows Server® 2012

❏ Operētājsistēma Microsoft® Windows Server® 2008 R2

Mac OS

Termins „Mac OS" tiek lietots kā atsauce uz „macOS Big Sur", „macOS Catalina", „macOS Mojave", „macOS High Sierra", „macOS Sierra", „OS X El Capitan" un „OS X Yosemite".

Jūsu nolūkiem nepieciešamie iestatījumi

Jūsu nolūkiem nepieciešamie iestatījumi

Skatiet turpmāko informāciju, lai uzstādītu jūsu nolūkiem nepieciešamos iestatījumus.

Skenera savienošana ar tīklu

Nolūks	Nepieciešamie iestatījumi
Vēlos pievienot skeneri tīklam.	Iestatiet skeneri tīkla skenēšanai. "Skenera savienošana ar tīklu" 13. lpp.
Vēlos pievienot skeneri jaunam datoram.	Iestatiet skenera tīkla iestatījumus jaunajā datorā. "Datora vai ierīču pievienošana vai nomaiņa" 19. lpp.

Skenēšanas iestatījumi

Nolūks	Nepieciešamie iestatījumi
Vēlos sūtīt skenētos attēlus uz e-pastu. (Scan to Email)	1. Iestatiet e-pasta serveri, ko vēlaties saistīt. "Pasta servera konfigurēšana" 41. lpp. 2. Reģistrējiet saņēmēja e-pasta adresi **Contacts** (izvēles). Reģistrējot e-pasta adresi, jums tā nebūs jāievada katru reizi, kad vēlēsities kaut ko nosūtīt. Varēsit to izvēlēties no Kontaktiem. "Kontaktpersonu pieejamības sniegšana" 62. lpp.
Vēlos saglabāt skenētos attēlus tīkla mapē. (Scan to Network Folder/FTP)	1. Izveidojiet tīkla mapi, kurā vēlaties saglabāt attēlus. "Koplietošanas tīkla mapes iestatīšana" 44. lpp. 2. Reģistrējiet ceļu uz mapi **Contacts** (izvēles). Reģistrējot mapes ceļu, jums tas nebūs jāievada katru reizi, kad vēlēsities kaut ko nosūtīt. Varēsit to izvēlēties no Kontaktiem. "Kontaktpersonu pieejamības sniegšana" 62. lpp.
Vēlos saglabāt skenētos attēlus mākoņpakalpojumā. (Scan to Cloud)	Iestatiet Epson Connect. Lai iegūtu detalizētu informāciju par iestatīšanu, skatiet Epson Connect portāla tīmekļa vietni. Iestatot, jums nepieciešams lietotāja konts tiešsaistes krātuves pakalpojumā ar kuru vēlaties saistīt. https://www.epsonconnect.com/ http://www.epsonconnect.eu (tikai Eiropā)

Vadības paneļa displeja pielāgošana

Nolūks	Nepieciešamie iestatījumi
Vēlos mainīt skenera vadības panelī attēlotos vienumus.	Iestatiet **Priekšiestat.** vai **Sākumlapas rediģēšana**. Vadības panelī varat reģistrēt savus iecienītākos skenēšanas iestatījumus un rediģēt attēlotos vienumus. "Vadības paneļa displeja pielāgošana" 75. lpp.

Pamata drošības funkciju iestatīšana

Nolūks	Nepieciešamie iestatījumi
Vēlos novērst, ka skenera iestatījumus maina kāds cits nevis administrators.	Iestatiet skenera administratora paroli. "Administratora iestatījumi" 84. lpp.
Vēlos atspējot skeneru izmantošanu ar USB savienojumiem.	Atspējojiet ārējo saskarni. "Ārējās saskarnes atspējošana" 90. lpp.

Papildu drošības funkciju iestatīšana

Nolūks	Nepieciešamie iestatījumi
Vēlos kontrolēt kādus protokolus izmantot.	Iespējojiet vai atspējojiet protokolus. "Vadība, izmantojot protokolus" 95. lpp.
Vēlos šifrēt sakaru ceļu.	1. Iestatiet savu digitālo sertifikātu. "Ciparsertifikāta lietošana" 98. lpp. 2. Iestatiet SSL/TLS sakarus. "SSL/TLS sakari ar skeneri" 103. lpp.
Vēlos izmantot šifrētus sakarus (IPsec). Vēlos izmantot programmatūru tikai no konkrēta datora (IP filtrēšana).	Iestatiet trafika filtrēšanas politikas. "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 105. lpp.
Vēlos izmantot skeneri IEEE802.1X tīklā.	Iestatiet IEEE802.1X skenerī. "Skenera pievienošana IEEE802.1X tīklam" 115. lpp.

Funkciju iestatīšana, lai autentificētos skenerī

Nolūks	Nepieciešamie iestatījumi
Vēlos iespējot Authentication Settings.	Skatiet turpmāk minēto papildinformācijai par pieejamajiem Authentication Settings un Authentication Method. "Par Authentication Settings" 125. lpp. "Par Authentication Method" 126. lpp.

Servera autentifikācijas sistēmas izmantošana

Izmantojot Document Capture Pro Server Authentication Edition (saīsinājumā Document Capture Pro Server AE), varat izveidot autentifikācijas sistēmu, kas autentifikācijai izmanto serveri.

Lai iegūtu plašāku informāciju, sazinieties ar vietējo Epson biroju.

Tīkla iestatījumi

Skenera savienošana ar tīklu

Šajā sadaļā tiek paskaidrots, kā savienot skeneri ar tīklu, izmantojot skenera vadības paneli.

Piezīme:
Ja jūsu skeneris un dators ir vienā segmentā, varat arī tos savienot, izmantojot instalētāju.

❏ *Iestatīšana no tīmekļa vietnes*

Atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties ***Iestatīšana*** *un sāciet iestatīšanu.*

http://epson.sn

❏ *Iestatīšana, izmantojot programmatūras disku (tikai modeļiem, kuru komplektā iekļauts programmatūras disks, un lietotājiem, kuru datoros ir operētājsistēma Windows un diskdziņi).*

Ievietojiet programmatūras disku datorā un izpildiet ekrānā sniegtās instrukcijas.

Pirms tīkla savienojuma izveides

Lai izveidotu savienojumu ar tīklu, pirms tam pārbaudiet savienojuma metodi un savienojuma iestatījumu informāciju.

Informācijas apkopošana savienojuma iestatīšanai

Sagatavojiet nepieciešamo iestatījumu informāciju, lai izveidotu savienojumu. Iepriekš pārbaudiet tālāk norādīto informāciju.

Sadaļas	Posms	Piezīme
Ierīces savienojuma metode	❏ Ethernet ❏ Wi-Fi	Izlemj, kā pievienot skeneri tīklam. Vadu lokālā tīkla gadījumā savieno ar lokālā tīkla komutatoru. Wi-Fi gadījumā savieno ar piekļuves punkta tīklu (SSID).
Lokālā tīkla savienojuma informācija	❏ IP adrese ❏ Apakštīkla maska ❏ Noklusējuma vārteja	Izlemiet, kādu IP adresi piešķirt skenerim. Piešķirot statisku IP adresi, nepieciešams norādīt visas vērtības. Piešķirot dinamisku IP adresi, izmantojot DHCP funkciju, šī informācija nav nepieciešama, jo tā tiek iestatīta automātiski.
Wi-Fi savienojuma informācija	❏ SSID ❏ Parole	Šis ir SSID (tīkla nosaukums) un parole piekļuves punktam, ar kuru savienojas skeneris. Ja ir iestatīta MAC adreses filtrēšana, iepriekš reģistrējiet skenera MAC adresi, lai reģistrētu skeneri. Lai iegūtu informāciju par atbalstītajiem standartiem, skatiet tālāk norādīto informāciju. "Tīkla specifikācijas" 27. lpp.
DNS servera informācija	❏ Primārā DNS servera IP adrese ❏ Sekundārā DNS servera IP adrese	Tās ir nepieciešamas, norādot DNS serverus. Sekundārais DNS tiek iestatīts, kad sistēmai ir rezerves konfigurācija un eksistē sekundārs DNS serveris. Ja jums ir neliela organizācija un neiestatāt DNS serveri, iestatiet maršrutētāja IP adresi.

Sadaļas	Posms	Piezīme
Starpniekservera informācija	❏ Starpniekservera nosaukums	Izveidojiet šos iestatījumus, kad jūsu tīkla vidē starpniekserveris tiek izmantots, lai piekļūtu internetam no iekštīkla, un jūs izmantojat funkciju, kuras lietošanai skeneris tieši piekļūst internetam. Lai izmantotu tālāk norādītās funkcijas, skeneris izveido tiešu savienojumu ar internetu. ❏ Epson Connect pakalpojumi ❏ Citu uzņēmumu mākoņpakalpojumi ❏ Aparātprogrammatūras atjaunināšana ❏ Skenēto attēlu sūtīšana, izmantojot SharePoint(WebDAV)
Porta numura informācija	❏ Izlaižamais porta numurs	Pārbaudiet skenera un datora izmantoto porta numuru, pēc tam nepieciešamības gadījumā atveriet portu, ko nobloķējis ugunsmūris. Skatiet tālāk norādīto, lai iegūtu porta numuru, kuru izmanto skeneris. "Porta izmantošana skenerim" 29. lpp.

IP adreses piešķiršana

Tālāk norādīti IP adreses piešķiršanas veidi.

Statiska IP adrese:

Manuāli piešķiriet skenerim (resursdatoram) iepriekš noteiktu IP adresi.

Informācija, kas nepieciešama, lai izveidotu savienojumu ar tīklu (apakštīkla maska, noklusējuma vārteja utt.), jāiestata manuāli.

IP adrese nemainās pat tad, ja ierīce ir izslēgta, tāpēc tas ir noderīgi, kad vēlaties pārvaldīt ierīces vidē, kur nevarat mainīt IP adresi, vai vēlaties pārvaldīt ierīces, izmantojot IP adresi. Šie iestatījumi ieteicami skenerim, serverim un citām ierīcēm, kurām piekļūst daudz datoru. Tāpat, izmantojot tādas drošības funkcijas kā IPsec/IP filtrēšana, piešķiriet fiksētu IP adresi, lai IP adrese nemainītos.

Automātiska piešķiršana, izmantojot DHCP funkciju (dinamiska IP adrese):

Automātiski piešķiriet skenerim (resursdatoram) IP adresi, izmantojot DHCP servera vai maršrutētāja DHCP funkciju.

Informācija, kas nepieciešama, lai izveidotu savienojumu ar tīklu (apakštīkla maska, noklusējuma vārteja, DNS serveris utt.) tiek iestatīta automātiski, lai jūs varētu viegli savienot ierīci ar tīklu.

Ja ierīce vai maršrutētājs ir izslēgts, atkarībā no DHCP servera iestatījumiem IP adrese var mainīties, atkārtoti izveidojot savienojumu.

Iesakām pārvaldīt ierīces, izņemot IP adresi un saziņu ar protokoliem, kas var sekot IP adresei.

Piezīme:
Izmantojot DHCP IP adreses rezervācijas funkciju, to pašu IP adresi var jebkurā brīdī piešķirt ierīcēm.

DNS serveris un starpniekserveris

DNS serverim ir resursdatora nosaukums, e-pasta adreses domēna nosaukums u. c. saistībā ar IP adreses informāciju.

Sakarus nevar izveidot, ja otru pusi raksturo resursdatora nosaukums, domēna nosaukums u. c., kad dators vai skeneris veido IP sakarus.

Vaicā šo informāciju DNS serverim un iegūst otras puses IP adresi. Šo procesu dēvē par nosaukuma atpazīšanu.

Tā rezultātā ierīces, piemēram, datori un skeneri, var veidot sakarus, izmantojot IP adresi.

Nosaukuma atpazīšana ir nepieciešama, lai skeneris varētu veidot sakarus, izmantojot e-pasta funkciju vai interneta savienojuma funkciju.

Izmantojot šīs funkcijas, izveidojiet DNS servera iestatījumus.

Piešķirot skenera IP adresi, izmantojot DHCP servera vai maršrutētāja DHCP funkciju, tā tiek iestatīta automātiski.

Starpniekserveris atrodas vārtejā starp tīklu un internetu, un tas sazinās ar datoru, skeneri un internetu (pretējo serveri) šo ierīču vietā. Pretējais serveris sazinās tikai ar starpniekserveri. Tādēļ nevar nolasīt tādu skenera informāciju kā IP adrese un porta numurs, un nepieciešama uzlabota drošība.

Izveidojot interneta savienojumu caur starpniekserveri, konfigurējiet skenera starpniekserveri.

Savienošana ar tīklu, izmantojot vadības paneli

Pievienojiet skeneri tīklam, izmantojot skenera vadības paneli.

IP adreses piešķiršana

Iestatiet tādus pamata vienumus kā Apakštīkla maska, Noklusējuma vārteja.

Šajā sadaļā aprakstīta statiskas IP adreses iestatīšanas procedūra.

1. Ieslēdziet skeneri.
2. Skenera vadības paneļa sākuma ekrānā atlasiet **Iestatījumi**.
3. Atlasiet **Tīkla iestatījumi** > **Papildu** > **TCP/IP**.
4. Iestatījumam **Manuāli** atlasiet **Iegūt IP adresi**.

   Ja IP adrese iestatīta automātiski, izmantojot maršrutētāja DHCP funkciju, atlasiet **Auto**. Šādā gadījumā 5. un 6. darbībā norādītie vienumi **IP adrese**, **Apakštīkla maska** un **Noklusējuma vārteja** arī tiek iestatīti automātiski, tāpēc pārejiet uz 7. darbību.
5. Ievadiet IP adresi.

   Fokuss pārvietojas uz nākamo segmentu vai iepriekšējo segmentu, kas atdalīti ar punktu, ja atlasāt ◀ un ▶.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.
6. Iestatiet vienumu **Apakštīkla maska** un **Noklusējuma vārteja**.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

> ***Svarīga informācija:***
>
> *Ja iestatījumu IP adrese, Apakštīkla maska un Noklusējuma vārteja kombinācija nav pareiza,* ***Sākt iestatīšanu*** *nav aktīvs, un iestatīšanu nevar turpināt. Pārbaudiet, vai ievadītajos datos nav kļūdu.*

7. Ievadiet primārā DNS servera IP adresi.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

   Piezīme:
   *IP adreses piešķiršanas iestatījumos atlasot vienumu **Auto**, iespējams DNS servera iestatījumiem atlasīt režīmu **Manuāli** vai **Auto**. Ja DNS servera adresi nevar iegūt automātiski, atlasiet vienumu **Manuāli** un ievadiet DNS servera adresi. Pēc tam ievadiet sekundārā DNS servera adresi. Ja atlasīts vienums **Auto**, turpiniet ar 9. darbību.*

8. Ievadiet sekundārā DNS servera IP adresi.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

9. Pieskarieties **Sākt iestatīšanu**.

Starpniekservera iestatīšana

Iestatiet starpniekserveri, ja ir izpildīti abi tālāk minētie nosacījumi.

❏ Starpniekserveris ir paredzēts savienošanai ar internetu.

❏ Tiek izmantota funkcija, ar kuras palīdzību skeneris tieši savienojas ar internetu, piemēram, Epson Connect pakalpojums vai cita uzņēmuma mākoņpakalpojumi.

1. Sākuma ekrānā izvēlieties **Iestatījumi**.

   Izvēloties iestatījumus pēc IP adreses iestatīšanas, tiek rādīts ekrāns **Papildu**. Pārejiet uz 3. darbību.

2. Atlasiet **Tīkla iestatījumi** > **Papildu**.

3. Izvēlieties **Starpniekserveris**.

4. Iestatījumam **Lietot** atlasiet **Starpniekservera iestatījumi**.

5. Ievadiet starpniekservera adresi IPv4 vai FQDN formātā.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

6. Ievadiet starpniekservera porta numuru.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

7. Pieskarieties **Sākt iestatīšanu**.

Ethernet savienojums

Savienojiet skeneri ar tīklu, izmantojot LAN vadu, un pēc tam pārbaudiet savienojumu.

1. Savienojiet skeneri ar centrmezglu (lokālā tīkla komutatoru), izmantojot LAN vadu.

2. Sākuma ekrānā izvēlieties  .

3. Atlasiet **Maršrutētājs**.

4. Pārliecinieties, ka Savienojums un IP adrese iestatījumi ir pareizi.

5. Pieskarieties **Aizvērt**.

Savienojums ar bezvadu lokālo tīklu (Wi-Fi)

Skeneri var savienot ar bezvadu LAN (Wi-Fi) vairākos veidos. Izvēlieties videi un jūsu apstākļiem atbilstošu savienojuma metodi.

Ja jums ir zināma bezvadu maršrutētāja informācija, piemēram, SSID un parole, varat iestatījumus norādīt manuāli.

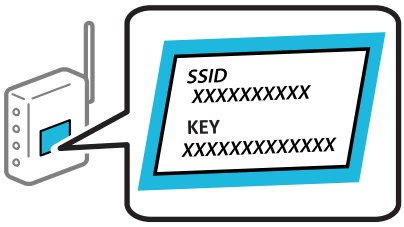
Ja bezvadu maršrutētājs atbalsta WPS, varat veikt iestatīšanu, izmantojot pogu.

Pēc skenera savienošanas ar tīklu izveidojiet savienojumu ar skeneri no ierīces, kuru vēlaties izmantot (datora, viedierīces, planšetes utt.)

Wi-Fi iestatījumu izveide, ievadot SSID un paroli

Jūs varat iestatīt Wi-Fi tīklu skenera vadības panelī, ievadot informāciju, kas nepieciešama, lai savienotu ar bezvadu maršrutētāju. Lai iestatītu, izmantojot šo metodi, jums nepieciešams bezvadu maršrutētāja SSID un parole.

Piezīme:
Ja izmantojat bezvadu maršrutētāju ar noklusējuma iestatījumiem, SSID un parole ir norādīti uz uzlīmes. Ja nezināt SSID un paroli, sazinieties ar personu, kas veica bezvadu maršrutētāja iestatīšanu, vai arī skatiet bezvadu maršrutētājam pievienoto dokumentāciju.



1. Sākuma ekrānā pieskarieties  .

2. Izvēlieties **Maršrutētājs**.

3. Pieskarieties **Sākt iestatīšanu**.

   Ja tīkla savienojums jau ir iestatīts, tiks parādīta savienojuma informācija. Pieskarieties pie **Mainīt uz Wi-Fi savienojumu.** vai **Mainīt iestatījumus**, lai mainītu iestatījumus.

4. Atlasiet **Wi-Fi iestatīšanas vednis**.

5. Izpildiet ekrānā redzamos norādījumus, lai atlasītu SSID, ievadītu bezvadu maršrutētāja paroli un sāktu iestatīšanu.

   Ja vēlaties pārbaudīt skenera tīkla savienojuma statusu pēc iestatīšanas, skatiet papildinformāciju tālāk norādītajā saitē.

Piezīme:

- ❏ *Ja nezināt SSID, apskatieties, vai tas nav norādīts uz uzlīmes, kas atrodas uz bezvadu maršrutētāja. Ja izmantojat bezvadu maršrutētāju ar noklusējuma iestatījumiem, izmantojiet uz uzlīmes norādīto SSID. Ja nevarat atrast informāciju, skatiet bezvadu maršrutētājam pievienoto dokumentāciju.*
- ❏ *Parole ir reģistrjutīga.*
- ❏ *Ja nezināt paroli, apskatieties, vai tā nav norādīta uz uzlīmes, kas atrodas uz bezvadu maršrutētāja. Parole uz uzlīmes var būt norādīta kā „Network Key", „Wireless Password", u.c. Ja izmantojat bezvadu maršrutētāju ar noklusējuma iestatījumiem, izmantojiet uz uzlīmes norādīto paroli.*

Saistītā informācija

➡ "Tīkla savienojuma statusa pārbaude" 25. lpp.

Wi-Fi iestatījumu izvēle, veicot iestatīšanu ar spiedpogu (WPS)

Wi-Fi tīklu var iestatīt automātiski, nospiežot pogu uz bezvadu maršrutētāja. Ja ir ievēroti turpmāk norādītie nosacījumi, varat iestatīt tīklu šādā veidā.

- ❏ Bezvadu maršrutētājs ir saderīgs ar WPS (Wi-Fi Protected Setup).
- ❏ Pašreizējais Wi-Fi savienojums izveidots, nospiežot pogu uz bezvadu maršrutētāja.

Piezīme:
Ja nevarat atrast pogu vai iestatīšanai izmantojat programmatūru, skatiet bezvadu maršrutētājam pievienoto dokumentāciju.

1. Sākuma ekrānā pieskarieties  .
2. Izvēlieties **Maršrutētājs**.
3. Pieskarieties **Sākt iestatīšanu**.

   Ja tīkla savienojums jau ir iestatīts, tiks parādīta savienojuma informācija. Pieskarieties pie **Mainīt uz Wi-Fi savienojumu.** vai **Mainīt iestatījumus**, lai mainītu iestatījumus.
4. Izvēlieties **Iestatīšana ar spiedpogu (WPS)**.
5. Izpildiet ekrānā sniegtos norādījumus.

   Ja vēlaties pārbaudīt skenera tīkla savienojuma statusu pēc iestatīšanas, skatiet papildinformāciju tālāk norādītajā saitē.

   Piezīme:
   Ja neizdodas izveidot savienojumu, pārstartējiet bezvadu maršrutētāju, pārvietojiet to tuvāk skenerim un mēģiniet vēlreiz.

Saistītā informācija

➡ "Tīkla savienojuma statusa pārbaude" 25. lpp.

Wi-Fi iestatījumu izvēle, veicot PIN koda iestatīšanu (WPS)

Varat automātiski izveidot savienojumu ar bezvadu maršrutētāju, izmantojot PIN kodu. Šo metodi iestatīšanai var izmantot, ja bezvadu maršrutētājs nodrošina WPS (Wi-Fi aizsargāto iestatīšanu). Izmantojiet datoru, lai bezvadu maršrutētājā ievadītu PIN kodu.

1. Sākuma ekrānā pieskarieties  .
2. Izvēlieties **Maršrutētājs**.
3. Pieskarieties **Sākt iestatīšanu**.

   Ja tīkla savienojums jau ir iestatīts, tiks parādīta savienojuma informācija. Pieskarieties pie **Mainīt uz Wi-Fi savienojumu.** vai **Mainīt iestatījumus**, lai mainītu iestatījumus.
4. Atlasiet **Citi** > **PIN koda iestatīšana (WPS)**
5. Izpildiet ekrānā sniegtos norādījumus.

   Ja vēlaties pārbaudīt skenera tīkla savienojuma statusu pēc iestatīšanas, skatiet papildinformāciju tālāk norādītajā saitē.

   Piezīme:
   Detalizētu informāciju par PIN koda ievadi skatiet bezvadu maršrutētājam pievienotajā dokumentācijā.

Saistītā informācija

➡ "Tīkla savienojuma statusa pārbaude" 25. lpp.

Datora vai ierīču pievienošana vai nomaiņa

Savienojuma izveide ar skeneri, kas ir bijis savienots ar tīklu

Ja skeneris jau ir savienots ar tīklu, datoru vai viedierīci varat savienot ar skeneri šajā tīklā.

Tīkla skenera izmantošana no otra datora

Skenera savienošanai ar datoru ieteicams izmantot instalētāju. Instalētāju var palaist ar kādu no turpmāk aprakstītajām metodēm.

❏ Iestatīšana no tīmekļa vietnes

Atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

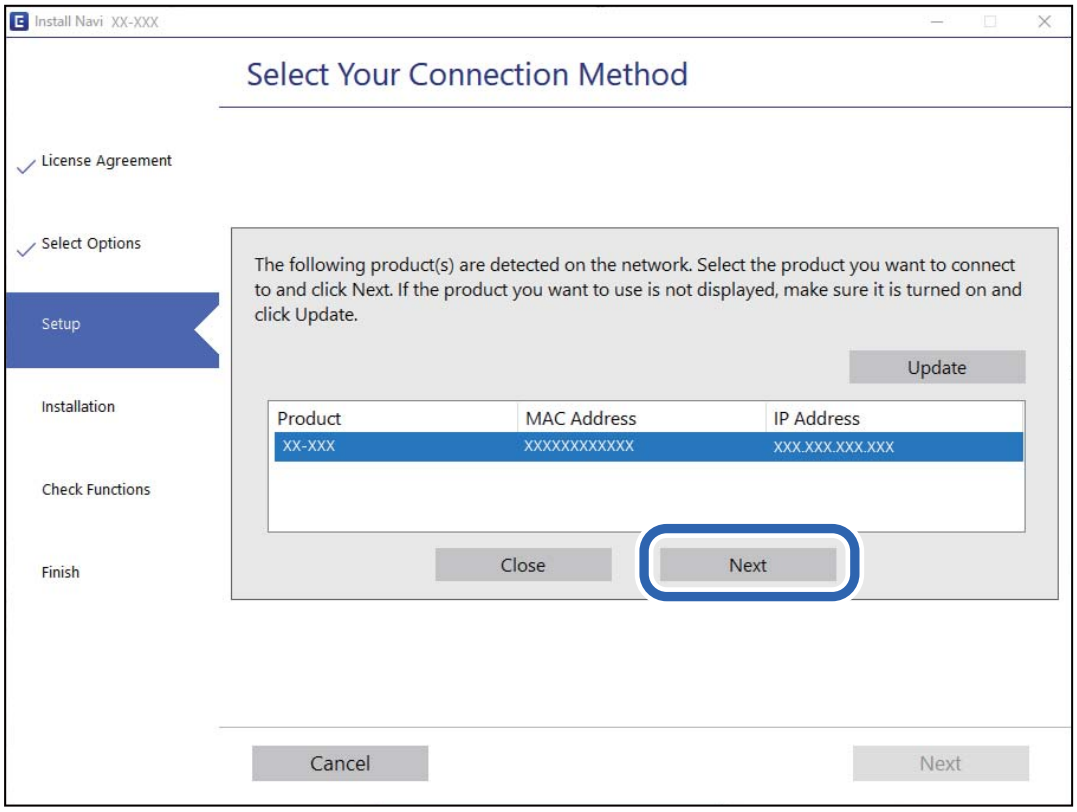
http://epson.sn

❏ Iestatīšana, izmantojot programmatūras disku (tikai modeļiem, kuru komplektā iekļauts programmatūras disks, un lietotājiem, kuru datoros ir operētājsistēma Windows un diskdziņi).

Ievietojiet programmatūras disku datorā un izpildiet ekrānā sniegtās instrukcijas.

Skenera izvēle

Izpildiet ekrānā redzamos norādījumus, līdz tiek parādīts turpmāk redzamais ekrāns, tad atlasiet tā skenera nosaukumu, ar kuru vēlaties izveidot savienojumu, un pēc tam noklikšķiniet uz **Tālāk**.



Izpildiet ekrānā sniegtos norādījumus.

Tīkla skenera lietošana no viedierīces

Skeneri ir iespējams savienot ar viedierīci, izmantojot kādu no turpmāk aprakstītajām metodēm.

Savienojuma izveide caur bezvadu maršrutētāju

Savienojiet viedierīci ar to pašu Wi-Fi tīklu (SSID), ar kuru ir savienots skeneris.

Lai uzzinātu vairāk, skatiet zemāk sniegto informāciju.

"Iestatījumu veikšana savienojuma izveidei ar viedierīci" 24. lpp.

Savienojuma izveide, izmantojot Wi-Fi Direct

Pievienojiet viedierīci tieši pie skenera, neizmantojot bezvadu maršrutētāju.

Lai uzzinātu vairāk, skatiet zemāk sniegto informāciju.

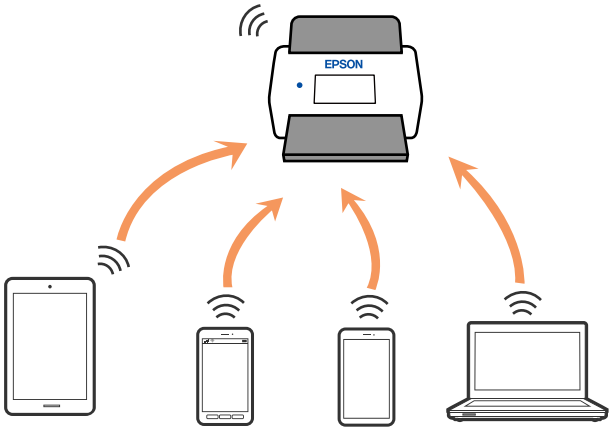
"Tieši savienojiet viedierīci un skeneri (Wi-Fi Direct)" 21. lpp.

Tieši savienojiet viedierīci un skeneri (Wi-Fi Direct)

Wi-Fi Direct (vienkāršā PP) ļauj tieši savienot viedierīci ar skeneri, neizmantojot bezvadu maršrutētāju, un skenēt no viedierīces.

Par Wi-Fi Direct

Izmantojiet šo savienojuma metodi, kad mājās vai birojā neizmantojat Wi-Fi vai kad tiešā veidā vēlaties savstarpēji savienot skeneri un datoru vai viedierīci. Šajā režīmā skeneris veic bezvadu maršrutētāja funkciju, un ar skeneri ir iespējams savienot ierīces, neizmantojot standarta bezvadu maršrutētāju. Tomēr ierīces, kas ir savienotas ar skeneri tiešā veidā, nevar izveidot savstarpējus sakarus ar skenera starpniecību.



Skenerim vienlaikus var būt Wi-Fi vai Ethernet savienojums un Wi-Fi Direct (vienkāršā PP) savienojums. Tomēr, ja tīkla savienojumu startē Wi-Fi Direct (vienkāršā PP) savienojuma brīdī, kad skenerim ir Wi-Fi savienojums, Wi-Fi savienojums īslaicīgi tiek pārtraukts.

Savienošana ar viedierīci, izmantojot Wi-Fi Direct

Šo metodi var izmantot, lai tiešā veidā savienotu skeneri ar viedierīcēm, neizmantojot bezvadu maršrutētāju.

1. Sākuma ekrānā izvēlieties  .
2. Izvēlieties **Wi-Fi Direct**.
3. Izvēlieties **Sākt iestatīšanu**.
4. Instalējiet viedierīcē programmu Epson Smart Panel.
5. Sekojiet instrukcijām uz Epson Smart Panel, lai savienotu to ar skeneri.

   Kad jūsu viedierīce ir savienota ar skeneri, dodieties uz nākamo soli.
6. Skenera vadības panelī atlasiet **Pabeigts**.

Wi-Fi Direct (vienkāršā PP) savienojuma pārtraukšana

Ir pieejamas divas metodes, kā atspējot Wi-Fi Direct (vienkāršā PP) savienojumu; varat atspējot visus savienojumus, izmantojot skenera vadības paneli, vai atspējot katru savienojumu, izmantojot datoru vai viedierīci.

Ja vēlaties atspējot visus savienojumus, atlasiet **Wi-Fi Direct** > **Sākt iestatīšanu** > **Mainīt** > **Atspējot Wi-Fi Direct**.

> ***Svarīga informācija:***
> *Kad tiek atspējots Wi-Fi Direct (vienkāršā PP) savienojums, visi datori un viedierīces, kas ir savienotas ar skeneri Wi-Fi Direct (vienkāršā PP) režīmā, tiek atvienotas.*

Piezīme:
Ja vēlaties atvienot noteiktu ierīci, dariet to, izmantojot ierīci, nevis skeneri. Izmantojiet kādu no sekojošām metodēm, lai atvienoju Wi-Fi Direct (vienkāršā PP) savienojumu, lietojot ierīci.

❏ *Atvienojiet Wi-Fi savienojumu ar skenera tīkla nosaukumu (SSID).*

❏ *Izveidojiet savienojumu ar citu tīkla nosaukumu (SSID).*

Wi-Fi Direct (vienkāršā PP) iestatījumu, piemēram, SSID maiņa

Ja Wi-Fi Direct (vienkāršā PP) savienojums ir iespējots, jūs varat nomainīt iestatījumus dodoties uz > **Wi-Fi Direct** > **Sākt iestatīšanu** > **Mainīt** un pēc tam tiek parādīti sekojoši izvēlnes vienumi.

Tīkla nosaukuma maiņa

Mainiet Wi-Fi Direct (vienkāršā PP) tīkla nosaukumu (SSID), kas tiek izmantots, veidojot savienojumu ar skeneri. Tīkla nosaukumu (SSID) var iestatīt, ar vadības paneļa programmatūras tastatūru ievadot ASCII rakstzīmes. Varat ievadīt līdz pat 22 rakstzīmēm.

Mainot tīkla nosaukumu (SSID), tiek atvienotas visas pievienotās ierīces. Ja vēlaties atjaunot ierīces savienojumu, izmantojiet jauno tīkla nosaukumu (SSID).

Nomainiet paroli

Mainiet savienojuma ar skeneri izveidei izmantoto Wi-Fi Direct (vienkāršā PP) paroli uz savu brīvi noteiktu vērtību. Paroli var iestatīt ar ASCII rakstzīmēm, kas redzamas vadības paneļa programmatūras tastatūrā. Varat ievadīt no 8 līdz 22 rakstzīmēm.

Mainot paroli, tiek atvienotas visas pievienotās ierīces. Ja vēlaties atkārtoti savienot ierīci, izmantojiet jauno paroli.

Frekvences diapazona maiņa

Nomainiet Wi-Fi Direct frekvenču diapazonu, kas tiek lietots savienojuma izveidei ar skeneri. Jūs varat izvēlēties starp 2,4 GHz un 5 GHz.

Nomainot frekvenču diapazonu, tiek atvienotas visas savienotās ierīces. Atkārtoti izveidojiet savienojumu ar ierīci.

Ņemiet vērā, ka, nomainot diapazonu uz 5 GHz, savienojumu nav iespējams atjaunot no ierīcēm, kas neatbalsta 5 GHz frekvenču diapazonu.

Atkarībā no reģiona šis iestatījums, iespējams, netiks parādīts.

Atspējot Wi-Fi Direct

Atspējojiet skenera Wi-Fi Direct (vienkāršā PP) iestatījumus. Veicot atspējošanu, visas ierīces, kas savienotas ar skeneri, izmantojot Wi-Fi Direct (vienkāršā PP) savienojumu, tiek atvienotas.

Atjaunot noklusējuma iestatījumus

Atjaunojiet visu Wi-Fi Direct (vienkāršā PP) iestatījumu noklusējuma vērtības.

Skenerī saglabātā viedierīces Wi-Fi Direct (vienkāršā PP) savienojuma informācija tiek dzēsta.

Piezīme:
*Cilnē **Network** > **Wi-Fi Direct** programmā Web Config var iestatīt arī sekojošus iestatījumus.*

- ❏ *Wi-Fi Direct (vienkāršā PP) iespējošana vai atspējošana*
- ❏ *Tīkla nosaukuma (SSID) mainīšana*
- ❏ *Paroles mainīšana*
- ❏ *Frekvenču diapazona maiņa*

  Atkarībā no reģiona šis iestatījums, iespējams, netiks parādīts.
- ❏ *Wi-Fi Direct (vienkāršā PP) iestatījumu atjaunošana*

Tīkla savienojuma atiestatīšana

Šajā sadaļā ir izskaidrots, kā veikt tīkla savienojuma iestatījumus un mainīt savienojuma metodi, kad nomainât bezvadu maršrutētāju vai datoru.

Nomainot bezvadu maršrutētāju

Ja nomainât bezvadu maršrutētāju, veiciet iestatījumus savienojumam starp datoru vai viedierīci un skeneri.

Jums jāizveido šie iestatījumi arī tad, ja mainât interneta pakalpojumu nodrošinātāju un tamlīdzīgos gadījumos.

Iestatījumu veikšana savienojuma izveidei ar datoru

Skenera savienošanai ar datoru ieteicams izmantot instalētāju. Instalētāju var palaist ar kādu no turpmāk aprakstītajām metodēm.

- ❏ Iestatīšana no tīmekļa vietnes

  Atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

  http://epson.sn
- ❏ Iestatīšana, izmantojot programmatūras disku (tikai modeļiem, kuru komplektā iekļauts programmatūras disks, un lietotājiem, kuru datoros ir operētājsistēma Windows un diskdziņi).

  Ievietojiet programmatūras disku datorā un izpildiet ekrānā sniegtās instrukcijas.

Savienojuma veida izvēle

Izpildiet ekrānā sniegtos norādījumus. Ekrānā **Atlasīt darbību** atlasiet iestatījumu **Iestatīt Printeris savienojumu vēlreiz (jaunam tīkla maršrutētājam vai mainot USB uz tīklu utt.)** un pēc tam noklikšķiniet uz **Tālāk**.

Lai pabeigtu iestatīšanu, izpildiet ekrānā redzamos norādījumus.

Ja nevarat izveidot savienojumu, skatiet turpmāk norādīto informāciju, lai mēģinātu atrisināt problēmu.

"Nevar izveidot savienojumu ar tīklu" 30. lpp.

Iestatījumu veikšana savienojuma izveidei ar viedierīci

Ja skeneri savieno ar to pašu Wi-Fi tīklu (SSID), ar kuru ir savienota viedierīce, iespējams skeneri izmantot no viedierīces. Lai izmantotu skeneri no viedierīces, dodieties uz tālāk norādīto tīmekļa vietni un ievadiet produkta nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

http://epson.sn

Piekļūstiet vietnei viedierīcē, kuru vēlaties savienot ar skeneri.

Nomainot datoru

Ja nomainiet datoru, veiciet iestatījumus savienojumam starp datoru un skeneri.

Iestatījumu veikšana savienojuma izveidei ar datoru

Skenera savienošanai ar datoru ieteicams izmantot instalētāju. Instalētāju var palaist ar šo metodi.

❏ Iestatīšana no tīmekļa vietnes

Atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

http://epson.sn

❏ Iestatīšana, izmantojot programmatūras disku (tikai modeļiem, kuru komplektā iekļauts programmatūras disks, un lietotājiem, kuru datoros ir operētājsistēma Windows un diskdziņi).

Ievietojiet programmatūras disku datorā un izpildiet ekrānā sniegtās instrukcijas.

Izpildiet ekrānā sniegtos norādījumus.

Metodes savienojumam ar datoru maiņa

Šajā sadaļā ir paskaidrots, kā izmainīt metodi, kādā tiek izveidots savienojums starp datoru un skeneri.

Tīkla savienojuma izmainīšana no Ethernet uz Wi-Fi

Skenera vadības panelī nomainiet savienojuma veidu no Ethernet uz Wi-Fi. Savienojuma metode principā ir tāda pati kā Wi-Fi savienojuma izveides metode.

Saistītā informācija

➡ "Savienojums ar bezvadu lokālo tīklu (Wi-Fi)" 17. lpp.

Tīkla savienojuma izmainīšana no Wi-Fi uz Ethernet

Izpildiet tālāk norādītās darbības, lai savienojuma veidu izmainītu no Wi-Fi uz Ehternet.

1. Sākuma ekrānā izvēlieties **Iestatījumi**.
2. Atlasiet **Tīkla iestatījumi** > **Vadu LAN iestatīšana**.

3. Izpildiet ekrānā sniegtos norādījumus.

Savienojuma maiņa no USB uz tīkla savienojumu

Instalētāja izmantošana un cita savienojuma veida iestatīšana.

❏ Iestatīšana no tīmekļa vietnes

Atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

http://epson.sn

❏ Iestatīšana, izmantojot programmatūras disku (tikai modeļiem, kuru komplektā iekļauts programmatūras disks, un lietotājiem, kuru datoros ir operētājsistēma Windows un diskdziņi).

Ievietojiet programmatūras disku datorā un izpildiet ekrānā sniegtās instrukcijas.

Savienojuma veida maiņa

Izpildiet ekrānā sniegtos norādījumus. Ekrānā **Atlasīt darbību** atlasiet iestatījumu **Iestatīt Printeris savienojumu vēlreiz (jaunam tīkla maršrutētājam vai mainot USB uz tīklu utt.)** un pēc tam noklikšķiniet uz **Tālāk**.

Izvēlēties tīkla savienojumu, kas jāizmanto: **Izveidot savienojumu, izmantojot bezvadu tīklu (Wi-Fi)** vai **Izveidot savienojumu, izmantojot vadu LAN (Ethernet)** un tad noklikšķiniet uz **Tālāk**.

Lai pabeigtu iestatīšanu, izpildiet ekrānā redzamos norādījumus.

Tīkla savienojuma statusa pārbaude

Tīkla savienojuma statusu var pārbaudīt turpmāk aprakstītajā veidā.

Tīkla savienojuma statusa pārbaude, izmantojot vadības paneli

Tīkla savienojuma statusu varat pārbaudīt, apskatot tīkla ikonu vai tīkla informāciju skenera vadības panelī.

Tīkla savienojuma statusa pārbaude, apskatot tīkla ikonu

Varat pārbaudīt tīkla savienojuma statusu un radioviļņa stiprumu, apskatot tīkla ikonu, kas redzama skenera sākuma ekrānā.

	Parāda tīkla savienojuma statusu. Atlasiet ikonu, lai pārbaudītu un mainītu pašreizējos iestatījumus. Šī ir saīsne, lai atvērtu tālāk norādīto izvēlni. **Iestatījumi** > **Tīkla iestatījumi** > **Wi-Fi iestatīšana**	
		Skeneris nav savienots ar bezvadu (Wi-Fi) tīklu.
		Skeneris meklē SSID, noņemts IP adreses iestatījums, vai radusies problēma ar bezvadu (Wi-Fi) tīklu.
		Skeneris ir savienots ar bezvadu (Wi-Fi) tīklu. Stabiņu skaits norāda savienojuma signāla stiprumu. Jo vairāk stabiņu redzams, jo stiprāks savienojums.
		Skeneris nav savienots ar bezvadu (Wi-Fi) tīklu Wi-Fi Direct (vienkāršā PP) režīmā.
		Skeneris ir savienots ar bezvadu (Wi-Fi) tīklu Wi-Fi Direct (vienkāršā PP) režīmā.
		Skeneris nav savienots ar vadu (Ethernet) tīklu vai ir atvienots.
		Skeneris ir savienots ar vadu (Ethernet) tīklu.

Detalizētas tīkla informācijas attēlošana vadības panelī

Kad jūsu skenerim ir izveidots savienojums ar tīklu, iespējams apskatīt arī citu ar tīklu saistītu informāciju, atlasot tīkla izvēlnes, kuras vēlaties pārbaudīt.

1. Sākuma ekrānā izvēlieties **Iestatījumi**.
2. Atlasiet **Tīkla iestatījumi** > **Tīkla statuss**.
3. Lai pārbaudītu informāciju, atlasiet izvēlnes, ko vēlaties pārbaudīt.
   - ❏ Vadu LAN/Wi-Fi statuss

     Parāda tīkla informāciju (ierīces nosaukumu, savienojumu, signāla stiprumu utt.) Ethernet vai Wi-Fi savienojumiem.
   - ❏ Wi-Fi Direct statuss

     Parāda, vai ir iespējots vai atspējots Wi-Fi Direct, kā arī SSID, paroli un citus datus Wi-Fi Direct savienojumiem.
   - ❏ E-pasta servera statuss

     Parāda e-pasta servera tīkla informāciju.

Tīkla specifikācijas

Wi-Fi specifikācijas

Wi-Fi specifikācijas skatiet zemāk norādītajā tabulā.

Valstis vai reģioni, izņemot zemāk norādītos	A tabula
Austrālija Jaunzēlande Taivāna Dienvidkoreja	B tabula

A tabula

Standarti	IEEE 802.11b/g/n*1
Frekvenču diapazons	2,4 GHz
Maksimālā raidītā radiofrekvenču signāla jauda	2 400–2 483,5 MHz: 20 dBm (EIRP)
Kanāli	1/2/3/4/5/6/7/8/9/10/11/12/13
Savienojuma režīmi	Infrastruktūras, Wi-Fi Direct (vienkāršā PP)*2*3
Drošības protokoli*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Pieejams tikai HT20 ierīcēs.

*2 Netiek atbalstīts standartam IEEE 802.11b.

*3 Infrastruktūras un Wi-Fi Direct režīmus vai Ethernet savienojumu var izmantot vienlaikus.

*4 Wi-Fi Direct atbalsta tikai WPA2-PSK (AES).

*5 Atbilst WPA2 standartiem ar WPA/WPA2 Personal atbalstu.

B tabula

Standarti	IEEE 802.11a/b/g/n*1/ac
Frekvences diapazoni	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz

Kanāli	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)
Savienojuma režīmi	Infrastruktūras, Wi-Fi Direct (vienkāršā PP)*4, *5		
Drošības protokoli*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Pieejams tikai HT20 ierīcēs.

*2 Nav pieejams Taivānā.

*3 Šo kanālu pieejamība un izstrādājuma lietošana ārpus telpām, izmantojot šos kanālus, mainās atkarībā no atrašanās vietas. Papildinformācijai skatiet šeit: http://support.epson.net/wifi5ghz/

*4 Netiek atbalstīts standartam IEEE 802.11b.

*5 Infrastruktūras un Wi-Fi Direct režīmus vai Ethernet savienojumu var izmantot vienlaikus.

*6 Wi-Fi Direct atbalsta tikai WPA2-PSK (AES).

*7 Atbilst WPA2 standartiem ar WPA/WPA2 Personal atbalstu.

Ethernet tehniskie dati

Standarti	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (energoefektīvs Ethernet)*2
Sakaru režīms	Automātisks, 10 Mb/s pilnduplekss, 10 Mb/s pusduplekss, 100 Mb/s pilnduplekss, 100 Mb/s pusduplekss
Savienotājs	RJ-45

*1 Lietojiet 5e vai augstākas kategorijas ekranētu vītā pāra kabeli, lai novērstu radio traucējumu risku.

*2 Pievienotajai ierīcei jāatbilst IEEE802.3az standartiem.

Tīkla funkcijas un IPv4/IPv6

Funkcijas	Atbalstītas
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Funkcijas	Atbalstītas
Document Capture Pro Server	IPv4, IPv6

Drošības protokols

IEEE802.1X*	
IPsec/IP filtrēšana	
SSL/TLS	HTTPS serveris/klients
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Savienojumam jāizmanto standartam IEEE802.1X atbilstoša ierīce.

Porta izmantošana skenerim

Skeneris izmanto turpmāk norādītos portus. Tīkla administratoram jānodrošina šo portu pieejamība atkarībā no vajadzībām.

Kad sūtītājs (klients) ir skeneris

Lietošana	Mērķis (serveris)	Protokols	Porta numurs
Failu sūtīšana (skenerī izmantojot skenēšanu uz tīkla mapi)	FTP/FTPS serveris	FTP/FTPS (TCP)	20
			21
	Failu serveris	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	WebDAV serveris	Protokols HTTP (TCP)	80
		Protokols HTTPS (TCP)	443
E-pasta sūtīšana (skenerī izmantojot skenēšanu uz e-pastu)	SMTP serveris	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
Savienojums „POP pirms SMTP" (skenerī izmantojot skenēšanu uz e-pastu)	POP serveris	POP3 (TCP)	110
Kad tiek izmantots pakalpojums Epson Connect	Epson Connect Server	HTTPS	443
		XMPP	5222

Lietošana	Mērķis (serveris)	Protokols	Porta numurs
Lietotāju informācijas vākšana (izmantojot kontaktpersonas skenerī)	LDAP serveris	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Lietotāju autentificēšana, vācot lietotāju informāciju (izmantojot kontaktpersonas skenerī) Lietotāju autentificēšana, izmantojot skenēšanu uz tīkla mapi (SMB) no skenera	KDC serveris	Kerberos	88
WSD vadība	Klientdators	WSD (TCP)	5357
Meklēšana datorā, veicot pašpiegādes skenēšanu no lietotnes	Klientdators	Tīkla pašpiegādes skenēšanas noteikšana	2968

Kad sūtītājs (klients) ir Klienta dators

Lietošana	Mērķis (serveris)	Protokols	Porta numurs
Atrodiet skeneri, izmantojot programmu, piemēram, EpsonNet Config un skenera draiveri.	Skeneris	ENPC (UDP)	3289
Apkopojiet un iestatiet MIB informāciju, izmantojot programmu, piemēram, EpsonNet Config un skenera draiveri.	Skeneris	SNMP (UDP)	161
WSD skenera meklēšana	Skeneris	WS-Discovery (UDP)	3702
Skenēto datu pārsūtīšana no lietotnes	Skeneris	Network Scan (TCP)	1865
Darba informācijas ieguve, veicot pašpiegādes skenēšanu no lietotnes	Skeneris	Tīkla pašpiegādes skenēšana	2968
Web Config	Skeneris	HTTP (TCP)	80
		HTTPS (TCP)	443

Problēmu risināšana

Nevar izveidot savienojumu ar tīklu

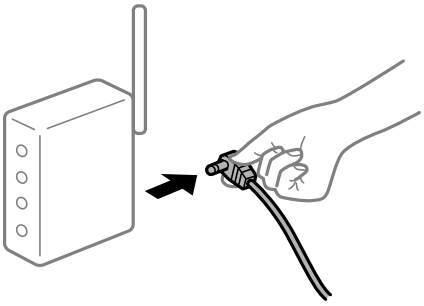
Šo problēmu var radīt kāds no tālāk norādītajiem cēloņiem.

Tīkla ierīcēm ir radušās problēmas izveidot Wi-Fi savienojumu.

Risinājumi

Izslēdziet ierīces, kuras vēlaties savienot ar tīklu. Apmēram 10 sekundes uzgaidiet un pēc tam ieslēdziet ierīces šādā secībā: bezvadu maršrutētājs, dators vai viedierīce un pēc tam skeneris. Pārvietojiet skeneri

un datoru vai viedierīci tuvāk bezvadu maršrutētājam, lai uzlabotu radioviļņu sakarus, un pēc tam mēģiniet atkārtoti veikt tīkla iestatīšanu.



Ierīce nespēj saņemt signālus no bezvadu maršrutētāja, jo tie atrodas pārāk tālu viens no otra.

Risinājumi

Pēc datora, viedierīces un skenera pārvietošanas tuvāk bezvadu maršrutētājam, izslēdziet un pēc tam atkal ieslēdziet bezvadu maršrutētāju.

Ja tiek nomainīts bezvadu maršrutētājs, iestatījumi neatbildīs jaunajam maršrutētājam.

Risinājumi

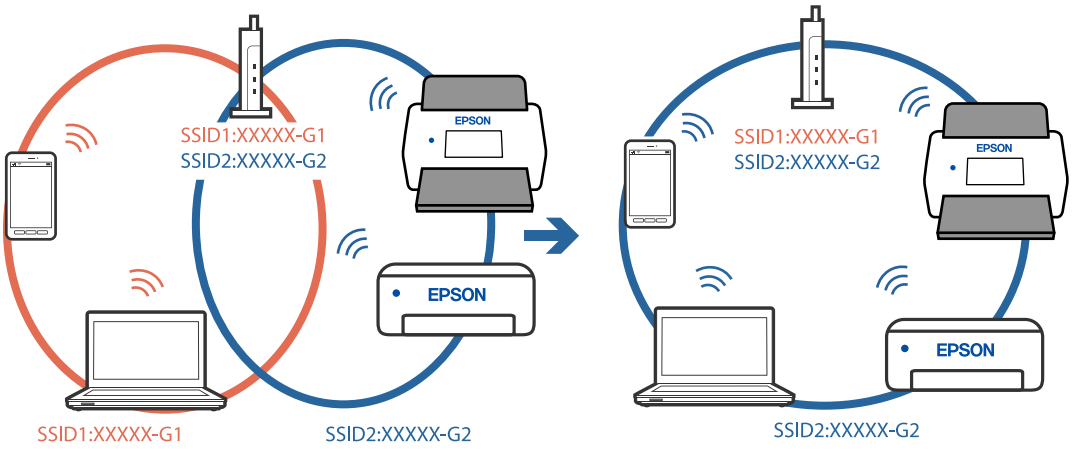
Vēlreiz veiciet savienojuma iestatījumus, lai tie atbilstu jaunajam bezvadu maršrutētājam.

SSID, kas pievienoti no datora vai viedierīces un datora, atšķiras.

Risinājumi

Ja vienlaicīgi izmantojat vairākus bezvadu maršrutētājus vai bezvadu maršrutētājam ir vairāki SSID un ierīces ir pievienotas dažādiem SSID, jūs nevarat izveidot savienojumu ar bezvadu maršrutētāju.

Savienojiet datoru vai viedierīci ar to pašu SSID, ar kuru ir savienots skeneris.



Bezvadu maršrutētājā ir pieejams privātuma atdalītājs.

Risinājumi

Lielākai daļai bezvadu maršrutētāju ir privātuma atdalītājs, kas bloķē saziņu starp pievienotām ierīcēm. Ja saziņa starp skeneri un datoru vai viedierīci neizdodas pat tad, ja tie ir savienoti vienā un tajā pašā tīklā, bezvadu maršrutētājā atspējojiet privātuma atdalītāju. Papildinformāciju skatiet bezvadu maršrutētāja rokasgrāmatā.

IP adrese nav pareizi piešķirta.

Risinājumi

Ja skenerim piešķirtā IP adrese ir 169.254.XXX.XXX un apakštīkla maska ir 255.255.0.0, IP adrese var nebūt piešķirta pareizi.

Skenera vadības panelī atlasiet **Iestatījumi** > **Tīkla iestatījumi** > **Papildu** > **TCP/IP** un pēc tam pārbaudiet skenerim piešķirto IP adresi un apakštīkla masku.

Restartējiet bezvadu maršrutētāju vai atiestatiet skenera tīkla iestatījumus.

Datorā radušās problēmas ar tīkla iestatījumiem.

Risinājumi

Mēģiniet no datora piekļūt jebkurai tīmekļa vietnei, lai pārbaudītu, vai datorā ir pareizi tīkla iestatījumi. Ja nevar piekļūt nevienai vietnei, tātad problēma ir datorā.

Pārbaudiet tīkla savienojumu datorā. Detalizētu informāciju skatiet datoram pievienotajā dokumentācijā.

Skeneris ir savienots ar Ethernet, izmantojot ierīces, kas atbalsta IEEE 802.3az (energoefektīvs Ethernet).

Risinājumi

Ja skenera savienojums ar Ethernet tiek izveidots, izmantojot ierīces, kas atbalsta IEEE 802.3az (energoefektīvs Ethernet), var rasties tālāk norādītās problēmas, atkarībā no izmantotā centrmezgla vai maršrutētāja.

- ❏ Savienojums kļūst nestabils, skenera savienojums tiek atkārtoti izveidots un pārtraukts.
- ❏ Nevar izveidot savienojumu ar skeneri.
- ❏ Sakaru ātrums kļūst lēns.

Sekojiet tālāk norādītajiem soļiem, lai skenerim atspējotu IEEE 802.3az un pēc tam izveidotu savienojumu.

1. Atvienojiet Ethernet kabeli, kas ir savienots ar datoru un skeneri.
2. Ja datoram ir iespējots IEEE 802.3az, atspējojiet to.

   Detalizētu informāciju skatiet datoram pievienotajā dokumentācijā.
3. Izveidojiet tiešu savienojumu starp datoru un skeneri ar Ethernet kabeli.
4. Pārbaudiet tīkla iestatījumus skenerī.

   Atlasiet **Iestatījumi** > **Tīkla iestatījumi** > **Tīkla statuss** > **Vadu LAN/Wi-Fi statuss**.
5. Pārbaudiet skenera IP adresi.
6. Datorā piekļūstiet Web Config.

   Palaidiet tīmekļa pārlūkprogrammu un pēc tam ievadiet skenera IP adresi.

   "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.
7. Atlasiet cilni **Network** > **Wired LAN**.

8. Iestatījumam **OFF** atlasiet **IEEE 802.3az**.
9. Noklikšķiniet uz **Next**.
10. Noklikšķiniet uz **OK**.
11. Atvienojiet Ethernet kabeli, kas ir savienots ar datoru un skeneri.
12. Ja datoram atspējojāt IEEE 802.3az, kā norādīts 2. solī, iespējojiet to.
13. Savienojiet Ethernet kabeļus, ko 1. solī atvienojāt no datora un skenera.

Ja problēma joprojām pastāv, to, iespējams, izraisa kādas citas ierīces, nevis skeneris.

Skeneris ir izslēgts.

Risinājumi

Pārliecinieties, ka skeneris ir ieslēgts.

Uzgaidiet, līdz statusa indikators pārtrauc mirgot, norādot, ka skeneris ir gatavs skenēšanai.

Programmatūra skenera iestatīšanai

Web Config

Web Config ir programma, kas darbojas tīmekļa pārlūkos, piemēram, Internet Explorer un Safari datorā. Var skatīt skenera statusu vai mainīt tīkla pakalpojuma un skenera iestatījumus. Tā kā skeneriem piekļūst un tie darbojas tieši no tīkla, tad ieteicams vienlaicīgi iestatīt vienu skeneri. Lai izmantotu Web Config, savienojiet savu datoru un skeneri ar vienu un to pašu tīklu.

Tiek atbalstītas šādas pārlūkprogrammas.

Microsoft Edge, Windows Internet Explorer 8 vai jaunāka versija, Firefox*, Chrome*, Safari*

* Lietojiet jaunāko versiju.

Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā

1. Pārbaudiet skenera IP adresi.

   Skenera vadības panelī atlasiet **Iestatījumi** > **Tīkla iestatījumi** > **Tīkla statuss**. Tad atlasiet aktīvā savienojuma metodes statusu (**Vadu LAN/Wi-Fi statuss** vai **Wi-Fi Direct statuss**), lai apstiprinātu skenera IP adresi.

2. Datorā vai viedierīcē palaidiet tīmekļa pārlūkprogrammu un ievadiet skenera IP adresi.

   Formāts:

   IPv4: http://skenera IP adrese/

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

   Piemēri:

   IPv4: http://192.168.100.201/

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

   Piezīme:
   Tā kā skeneris izmanto pašparakstītu sertifikātu, lai piekļūtu HTTPS serveriem, palaižot Web Config, pārlūkprogrammā parādīsies brīdinājuma paziņojums, taču tas nenorāda uz problēmu un to var droši ignorēt.

3. Lai mainītu skenera iestatījumus, piesakieties kā administrators.

   Ekrāna augšējā labajā pusē noklikšķiniet uz **Administrator Login**. Ievadiet **User Name** un **Current password**, un pēc tam noklikšķiniet **OK**.

   Piezīme:
   ❏ *Tālāk sniegtas Web Config sākotnējās vērtības administratora informācijai.*

   ·Lietotājvārds: nav (tukšs)

   ·Parole: skenera sērijas numurs

   Lai iegūtu sērijas numuru, apskatiet etiķeti, kas uzlīmēta skenera aizmugurē.

   ❏ *Ja ekrāna augšējā labajā pusē tiek parādīts **Administrator Logout**, tad jūs jau esat pieteicies kā administrators.*

Web Config palaišana operētājsistēmā Windows

Ja savienojat datoru ar skeneri, lietojot WSD, izpildiet turpmāk norādītās darbības, lai palaistu Web Config.

1. Datorā atveriet skenera sarakstu.

   ❏ Windows 10

   Noklikšķiniet uz pogas Sākums un pēc tam sadaļā **Aparatūra un skaņa** atlasiet **Sistēma Windows** > **Vadības panelis** > **Skatīt ierīces un printerus**.

   ❏ Windows 8.1/Windows 8

   Atlasiet **Darbvirsma** > **Iestatījumi** > **Vadības panelis** > **Skatīt ierīces un printerus** no **Aparatūra un skaņa** (vai **Aparatūra**).

   ❏ Windows 7

   Noklikšķiniet uz pogas Start un sadaļā **Aparatūra un skaņa** atlasiet **Vadības panelis** > **Skatīt ierīces un printerus**.

2. Ar peles labo pogu noklikšķiniet uz skenera un atlasiet **Rekvizīti**.

3. Atlasiet cilni **Tīmekļa pakalpojums** un noklikšķiniet uz URL.

   Tā kā skeneris izmanto pašparakstītu sertifikātu, lai piekļūtu HTTPS serveriem, palaižot Web Config, pārlūkprogrammā parādīsies brīdinājuma paziņojums, taču tas nenorāda uz problēmu un to var droši ignorēt.

   Piezīme:

   ❏ *Tālāk sniegtas Web Config sākotnējās vērtības administratora informācijai.*

   ·Lietotājvārds: nav (tukšs)

   ·Parole: skenera sērijas numurs

   Lai iegūtu sērijas numuru, apskatiet etiķeti, kas uzlīmēta skenera aizmugurē.

   ❏ *Ja ekrāna augšējā labajā pusē tiek parādīts **Administrator Logout**, tad jūs jau esat pieteicies kā administrators.*

Epson Device Admin

Epson Device Admin ir daudzfunkcionāla lietojumprogramma, kas ļauj pārvaldīt tīklā esošās ierīces.

Varat izmantot konfigurācijas veidnes, lai piemērotu vienotos iestatījumus vairākiem tīklā esošajiem skeneriem, padarot vairāku skeneru iestatīšanu un pārvaldīšanu piemērotu.

Varat lejupielādēt Epson Device Admin no Epson atbalsta tīmekļa vietnes. Papildinformāciju par to, kā izmantot šo lietojumprogrammu, skatiet Epson Device Admin dokumentācijā vai palīdzības sadaļā.

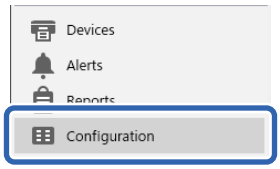
Konfigurācijas veidne

Konfigurācijas veidnes izveidošana

No jauna izveidojiet konfigurācijas veidni.

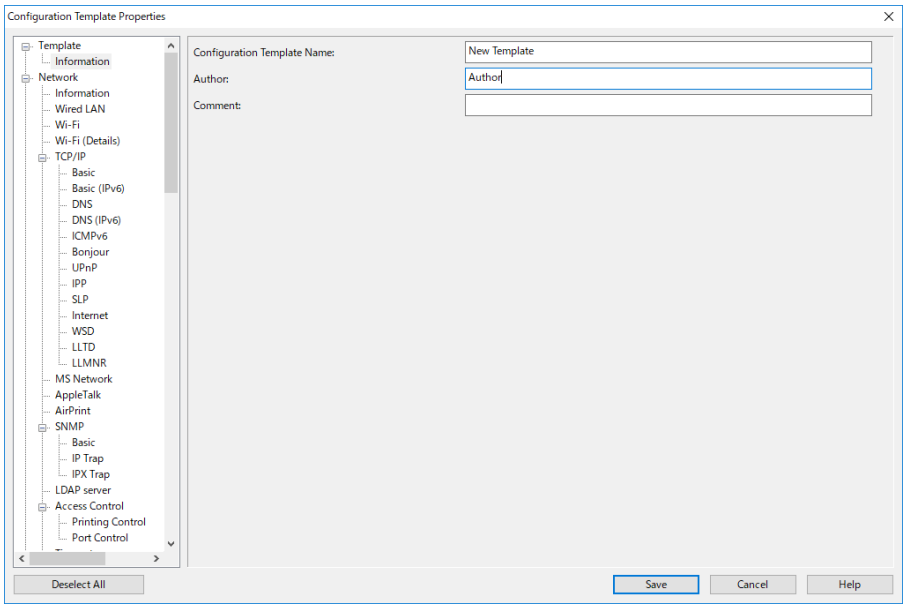
1. Palaidiet Epson Device Admin.

2. Sānu joslas uzdevumu izvēlnē atlasiet **Configuration**.



3. Lentes izvēlnē atlasiet **New**.

4. Iestatiet katru vienumu.



Vienums	Skaidrojums
Configuration Template Name	Konfigurācijas veidnes nosaukums. Ievadiet līdz 1024 rakstzīmēm Unicode formātā (UTF-8).
Author	Informācija par veidnes izveidotāju. Ievadiet līdz 1024 rakstzīmēm Unicode formātā (UTF-8).
Comment	Ievadiet pieņemtu informāciju. Ievadiet līdz 1024 rakstzīmēm Unicode formātā (UTF-8).

5. Kreisajā pusē atlasiet vienumus, ko vēlaties iestatīt.

Piezīme:
*Noklikšķiniet izvēlnes vienumus kreisajā pusē, lai pārslēgtos uz katru ekrānu. Iestatītā vērtība tiek saglabāta, ja pārslēdzat ekrānu, bet ne tad, ja atceļat ekrānu. Kad visi iestatījumi pabeigti, noklikšķiniet **Save**.*

Konfigurācijas veidnes lietošana

Lietojiet saglabāto konfigurācijas veidni skenerim. Tiek lietoti veidnē atlasītie vienumi. Jā mērķa skenerim nav piemērotas funkcijas, tā netiek lietota.

Piezīme:
Ja skenerim iestatīta administratora parole, konfigurējiet paroli pirms tam.

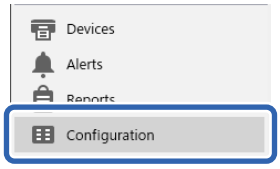
*1. Ierīces saraksta ekrāna lentes izvēlnē atlasiet **Options** > **Password manager**.*

*2. Izvēlieties **Enable automatic password management** un pēc tam noklikšķiniet uz **Password manager**.*

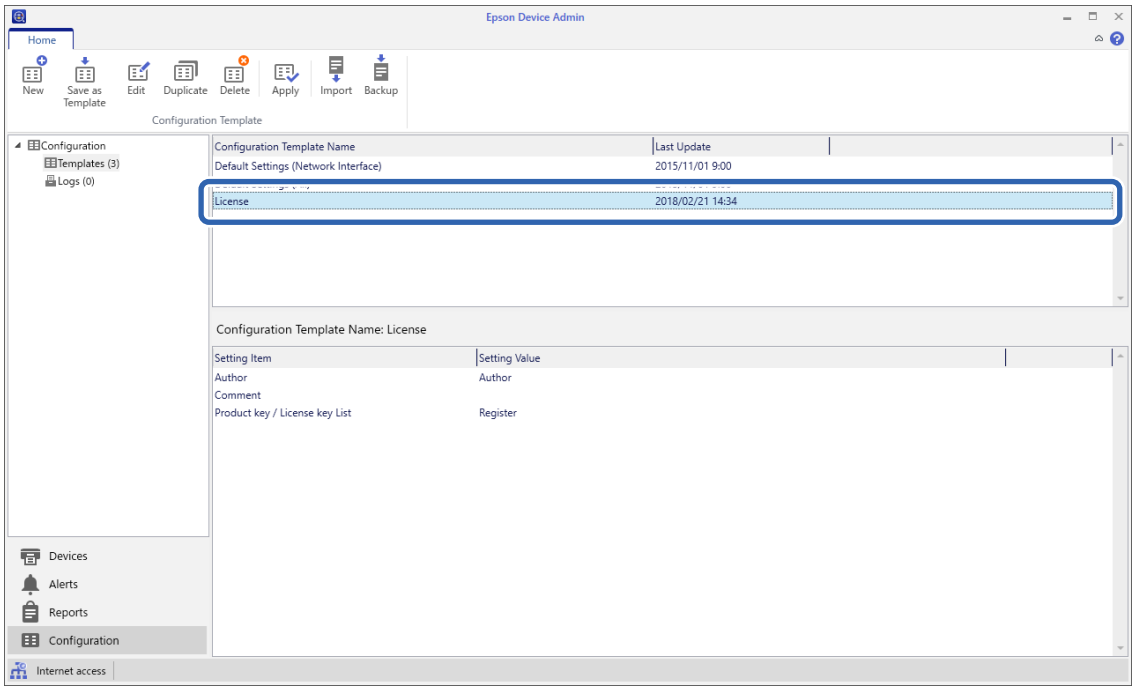
*3. Atlasiet atbilstošo skeneri un pēc tam noklikšķiniet uz **Edit**.*

*4. Iestatiet paroli un noklikšķiniet uz **OK**.*

1. Sānu joslas uzdevumu izvēlnē atlasiet **Configuration**.



2. Sadaļā **Configuration Template Name** atlasiet konfigurācijas veidni, ko vēlaties lietot.



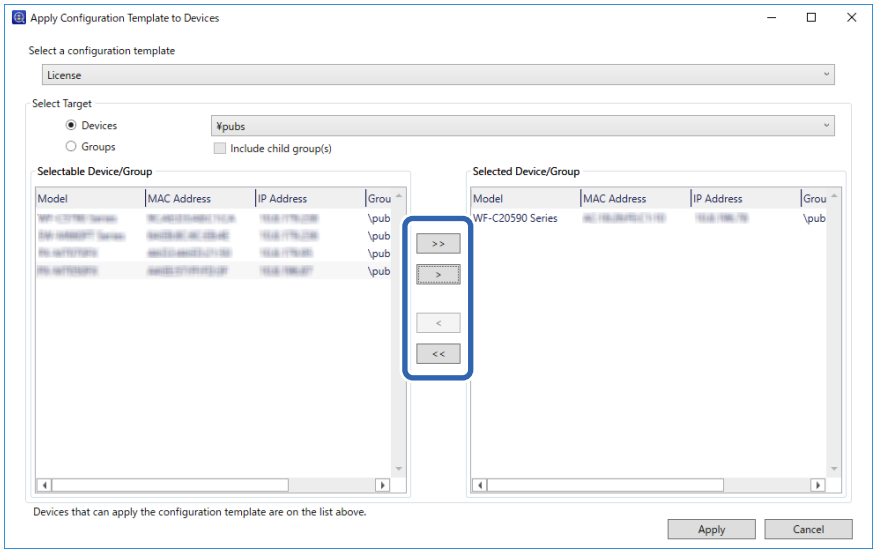
3. Lentes izvēlnē noklikšķiniet uz **Apply**.

   Tiek parādīts ierīces atlases ekrāns.

4. Atlasiet konfigurācijas veidni, ko vēlaties lietot.

   Piezīme:
   - ❏ *Kad izvelkamā izvēlnē atlasiet **Devices** un grupas, kas satur ierīces, tiek parādīta katra ierīce.*
   - ❏ *Atlasot **Groups**, tiek rādītas grupas. Atlasiet **Include child group(s)**, lai automātiski atlasītu bērnu grupas atlasītajā grupā.*

5. Pārvietojiet skeneri vai grupas, kurām vēlaties piemērot veidni uz **Selected Device/Group**.



6. Noklikšķiniet uz **Apply**.

   Tiek parādīts apstiprinājuma ekrāns lietotajai konfigurācijas veidnei.

7. Noklikšķiniet uz **OK**, lai lietotu konfigurācijas veidni.

8. Kad tiek parādīts ziņojums ar informāciju par to, ka procedūra ir pabeigta, noklikšķiniet uz **OK**.

9. Noklikšķiniet uz **Details** un pārbaudiet informāciju.

   Kad lietotajiem vienumiem tiek parādīts , piemērošana ir veiksmīgi pabeigta.

10. Noklikšķiniet uz **Close**.

Nepieciešamie skenēšanas iestatījumi

Pasta servera konfigurēšana

Iestatiet pasta serveri, izmantojot programmu Web Config.

Kad skeneris var nosūtīt e-pasta ziņu, iestatot pasta serveri, iespējams veikt tālāk norādītās darbības.

❏ Pārsūta skenēšanas rezultātus, izmantojot e-pastu

❏ Saņem e-pasta paziņojumu no skenera

Pirms iestatīšanas pārbaudiet tālāk norādīto.

❏ Skeneris ir savienots ar tīklu, kas var piekļūt pasta serverim.

❏ Pārbaudiet e-pasta iestatījumus datoram, kas izmanto to pašu pasta serveri, ko skeneris.

Piezīme:

❏ *Izmantojot pasta serveri internetā, pārbaudiet iestatījumu informāciju, sazinoties ar pakalpojumu sniedzēju, vai tīmekļa vietnē.*

❏ *Pasta serveri var arī iestatīt, izmantojot skenera vadības paneli. Piekļūstiet iestatījumiem, kā norādīts tālāk.*

Iestatījumi > ***Tīkla iestatījumi*** > ***Papildu*** > ***E-pasta serveris*** > ***Servera iestatījumi***

1. Atveriet programmu Web Config un atlasiet cilni **Network** > **Email Server** > **Basic**.
2. Ievadiet vērtību katram vienumam.
3. Atlasiet **OK**.

   Tiks parādīti atlasītie iestatījumi.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Pasta servera vienumu iestatīšana

Posms	Iestatījumi un skaidrojums	
Authentication Method	Norādiet autentifikācijas metodi, kuru skeneris izmantos piekļuvei e-pasta serverim.	
	Off	Sazinoties ar pasta serveri, autentifikācija ir atspējota.
	SMTP AUTH	Nepieciešams, lai pasta serveris atbalstītu SMTP autentifikāciju.
	POP before SMTP	Atlasot šo metodi, konfigurējiet POP3 serveri.
Authenticated Account	Atlasot **SMTP AUTH** vai **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet autentifikācijas konta nosaukumu, kas sastāv no 0 līdz 255 ASCII rakstzīmēm (0x20–0x7E).	
Authenticated Password	Atlasot **SMTP AUTH** vai **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet autentifikācijas paroli, kurā jābūt no 0 līdz 20 ASCII rakstzīmēm (0x20–0x7E).	
Sender's Email Address	Ievadiet sūtītāja e-pasta adresi. Ievadiet no 0 līdz 255 ASCII rakstzīmēm (0x20–0x7E), izņemot šīs : ( ) < > [ ] ; ¥. Pirmā rakstzīme nedrīkst būt punkts (.).	
SMTP Server Address	Ievadiet no 0 līdz 255 rakstzīmēm A–Z a–z 0–9 . -. Var izmantot IPv4 vai FQDN formātu.	

Posms	Iestatījumi un skaidrojums	
SMTP Server Port Number	Ievadiet skaitli no 1 līdz 65 535.	
Secure Connection	Norādiet e-pasta servera drošā savienojuma metodi.	
	None	Atlasot **POP before SMTP** kā **Authentication Method** iestatījumu, savienojuma metode tiek iestatīta kā **None**.
	SSL/TLS	Tas ir pieejams, kad **Authentication Method** ir iestatīta kā **Off** vai „**SMTP AUTH**".
	STARTTLS	Tas ir pieejams, kad **Authentication Method** ir iestatīta kā **Off** vai „**SMTP AUTH**".
Certificate Validation	Iespējojot šo funkciju, sertifikāts tiek validēts. Ieteicams to iestatīt kā **Enable**.	
POP3 Server Address	Atlasot **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet POP3 servera adresi, kas sastāv no 0 līdz 255 rakstzīmēm A–Z a–z 0–9 . -. Var izmantot IPv4 vai FQDN formātu.	
POP3 Server Port Number	Atlasot **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet skaitli no 1 līdz 65535.	

Pasta servera savienojuma pārbaude

Savienojumu ar pasta serveri var pārbaudīt, veicot savienojuma pārbaudi.

1. Atveriet programmu Web Config un atlasiet cilni **Network** > **Email Server** > **Connection Test**.

2. Izvēlieties **Start**.

   Tiek sākts pasta servera savienojuma tests. Pēc pārbaudes tiks parādīta pārbaudes atskaite.

   Piezīme:
   Savienojumu ar pasta serveri var arī pārbaudīt, izmantojot skenera vadības paneli. Piekļūstiet iestatījumiem, kā norādīts tālāk.

   Iestatījumi** > **Tīkla iestatījumi** > **Papildu** > **E-pasta serveris** > **Savienojuma pārbaude

Pasta servera savienojuma testēšanas atsauces

Ziņojumi	Cēlonis
Connection test was successful.	Šis ziņojums tiek parādīts tad, ja savienojuma izveide ar serveri ir veiksmīga.
SMTP server communication error. Check the following. - Network Settings	Šis ziņojums tiek parādīts, ja ❏ Skeneris nav savienots ar tīklu ❏ Ir notikusi servera SMTP atteice ❏ Sakaru laikā tiek pārtraukts tīkla savienojums ❏ Saņemti nepilnīgi dati

Ziņojumi	Cēlonis
POP3 server communication error. Check the following. - Network Settings	Šis ziņojums tiek parādīts, ja ❏ Skeneris nav savienots ar tīklu ❏ Ir notikusi servera POP3 atteice ❏ Sakaru laikā tiek pārtraukts tīkla savienojums ❏ Saņemti nepilnīgi dati
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Šis ziņojums tiek parādīts, ja ❏ Neizdodas savienojums ar DNS serveri ❏ Neizdodas atpazīt SMTP servera nosaukumu
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Šis ziņojums tiek parādīts, ja ❏ Neizdodas savienojums ar DNS serveri ❏ Neizdodas atpazīt POP3 servera nosaukumu
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Šis ziņojums tiek parādīts, ja neizdodas SMTP servera autentifikācija.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Šis ziņojums tiek parādīts, ja neizdodas POP3 servera autentifikācija.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Šis ziņojums tiek parādīts, ja mēģināt sazināties, izmantojot neatbalstītus protokolus.
Connection to SMTP server failed. Change Secure Connection to None.	Šis ziņojums tiek parādīts, ja rodas SMTP neatbilstība starp serveri un klientu vai arī serveris neatbalsta SMTP drošo savienojumu (SSL savienojums).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Šis ziņojums tiek parādīts, ja rodas SMTP neatbilstība starp serveri un klientu vai arī serveris pieprasa izmantot SMTP drošajam savienojumam SSL/TLS savienojuma iespēju.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Šis ziņojums tiek parādīts, ja rodas SMTP neatbilstība starp serveri un klientu vai arī serveris pieprasa SMTP drošajam savienojumam izmantot STARTTLS savienojuma iespēju.
The connection is untrusted. Check the following. - Date and Time	Šis ziņojums tiek parādīts, ja skenera datuma un laika iestatījums nav pareizs vai sertifikātam ir beidzies derīguma termiņš.
The connection is untrusted. Check the following. - CA Certificate	Šis ziņojums tiek parādīts, ja skenerim nav saknes sertifikāta, kas atbilst serverim, vai arī nav importēts CA Certificate.
The connection is not secured.	Šis ziņojums tiek parādīts, ja iegūtais sertifikāts ir bojāts.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Šis ziņojums tiek parādīts, ja rodas neatbilstība starp servera un klienta autentifikācijas metodi. Serveris atbalsta SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Šis ziņojums tiek parādīts, ja rodas neatbilstība starp servera un klienta autentifikācijas metodi. Serveris neatbalsta SMTP AUTH.

Ziņojumi	Cēlonis
Sender's Email Address is incorrect. Change to the email address for your email service.	Šis ziņojums tiek parādīts, ja norādītā sūtītāja e-pasta adrese nav pareiza.
Cannot access the product until processing is complete.	Šis ziņojums tiek parādīts, ja skeneris ir aizņemts.

Koplietošanas tīkla mapes iestatīšana

Iestatiet koplietotu tīkla mapi, kurā saglabāt skenēto attēlu.

Saglabājot mapē failu, skeneris piesakās kā datora, kurā mape tika izveidota, lietotājs.

Koplietotas mapes izveide

Saistītā informācija

➡ "Pirms koplietotas mapes izveides" 44. lpp.

➡ "Tīkla profila pārbaude" 44. lpp.

➡ "Koplietotās mapes izveides vieta un drošības piemērs" 45. lpp.

➡ "Grupas vai lietotāja pievienošana, atļaujot piekļuvi" 58. lpp.

Pirms koplietotas mapes izveides

Pirms koplietotas mapes izveides pārbaudiet tālāk norādīto.

❏ Skeneris ir savienots ar tīklu, kurā tas var piekļūt koplietoto mapi izveidojušam datoram.

❏ Koplietoto mapi izveidojušā datora nosaukumā netiek ietverta vairākbaitu rakstzīme.

Svarīga informācija:

Kad datora nosaukumā netiek ietverta vairākbaitu rakstzīme, faila saglabāšana koplietotajā mapē var neizdoties.

Tādā gadījumā izmantojiet datoru, kas nosaukumā neietver vairākbaitu rakstzīmi, vai nomainiet datora nosaukumu.

Ja izlemjat mainīt datora nosaukumu, iepriekš saskaņojiet to ar administratoru, jo nosaukuma maiņa var ietekmēt noteiktus iestatījumus, piemēram, datora pārvaldību, piekļuvi resursiem u. c.

Tīkla profila pārbaude

Datorā, kurā tiks izveidota koplietotā mape, pārbaudiet, vai koplietotā mape ir pieejama.

1. Piesakieties datorā, kurā tiks izveidota koplietotā mape, izmantojot lietotāja kontu ar administratora atļaujām.

2. Atlasiet **Vadības panelis** > **Tīkls un internets** > **Tīkla un koplietošanas centrs**.

3. Noklikšķiniet uz **Papildu koplietošanas iestatījumi** un pēc tam parādītajā tīkla profilu saturā noklikšķiniet uz blakus profilam ar uzrakstu **(pašreizējais profils)**.

4. Pārbaudiet, vai opcija **Ieslēgt failu un printeru koplietošanu** ir atlasīta sadaļā **Failu un printeru koplietošana**.

   Ja opcija jau ir atlasīta, noklikšķiniet uz **Atcelt** un aizveriet logu.

   Kad iestatījumi ir nomainīti, noklikšķiniet uz **Saglabāt izmaiņas** un aizveriet logu.

Koplietotās mapes izveides vieta un drošības piemērs

Atkarībā no koplietotās mapes izveides vietas atšķiras tās drošības un lietošanas ērtības pakāpe.

Lai izmantotu koplietoto mapi skeneros vai citos datoros, nepieciešamas tālāk norādītās mapes lasīšanas un izmaiņu veikšanas atļaujas.

❏ Cilne **Koplietošana** > **Papildu koplietošana** > **Atļaujas**

Pārvalda koplietotās mapes tīkla piekļuves atļauju.

❏ Cilnes **Drošība** piekļuves atļauja

Pārvalda koplietotās mapes tīkla piekļuves un lokālās piekļuves atļauju.

Piemēram, izveidojot koplietotu mapi un iestatot **Visi** uz darbvirsmas izveidotai koplietotajai mapei, piekļuve būs atļauta visiem lietotājiem, kuriem ir piekļuve datoram.

Tomēr lietotājs, kam nav tiesību, nevar piekļūt mapei, jo darbvirsmu (mapi) pārvalda lietotāja mape, un tādā gadījumā darbvirsmai tiek nodoti lietotāja mapes drošības iestatījumi. Lietotājs, kuram cilnē **Drošība** atļauta piekļuve (šajā gadījumā — pieteicies lietotājs un administrators) var veikt darbības mapē.

Skatiet tālāk norādīto informāciju, lai izveidotu attiecīgu atrašanās vietu.

Šis piemērs attiecas uz mapes „scan_folder” izveidi.

Saistītā informācija

➡ "Failu serveru konfigurācijas piemērs" 45. lpp.

➡ "Personālā datora konfigurācijas piemērs" 52. lpp.

Failu serveru konfigurācijas piemērs

Šajā paskaidrojumā sniegts piemērs, kā izveidot koplietotu mapi koplietotā datora diska saknes direktorijā, piemēram, failu serverī, ievērojot tālāk norādīto nosacījumu.

Koplietotajai mapei var piekļūt lietotāji ar piekļuves vadību, piemēram, persona, kurai ir tāds pats domēns kā datoram, kurā izveidota koplietotā mape.

Iestatiet šo konfigurāciju, ja vēlaties atļaut visiem lietotājiem lasīt un rakstīt saturu koplietotajā mapē, kas atrodas datorā, piemēram, failu serverī un koplietotajā datorā.

❏ Koplietotās mapes izveides vieta: diska saknes direktorijs

❏ Mapes ceļš: C:\scan_folder

❏ Atļauja piekļuvei tīklā (koplietošanas pilnvaras): visiem

❏ Atļauja piekļuvei failu sistēmā (drošība): autentificētiem lietotājiem

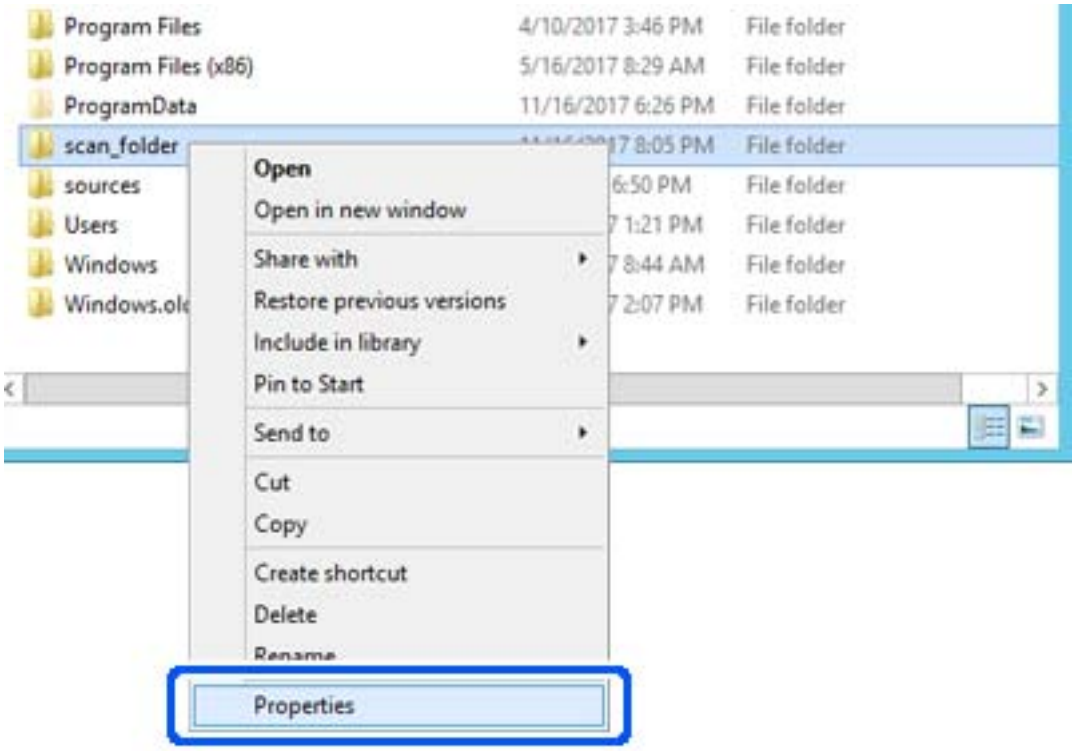
1. Piesakieties datorā, kurā tiks izveidota koplietotā mape, izmantojot lietotāja kontu ar administratora atļaujām.

2. Palaidiet pārlūku.

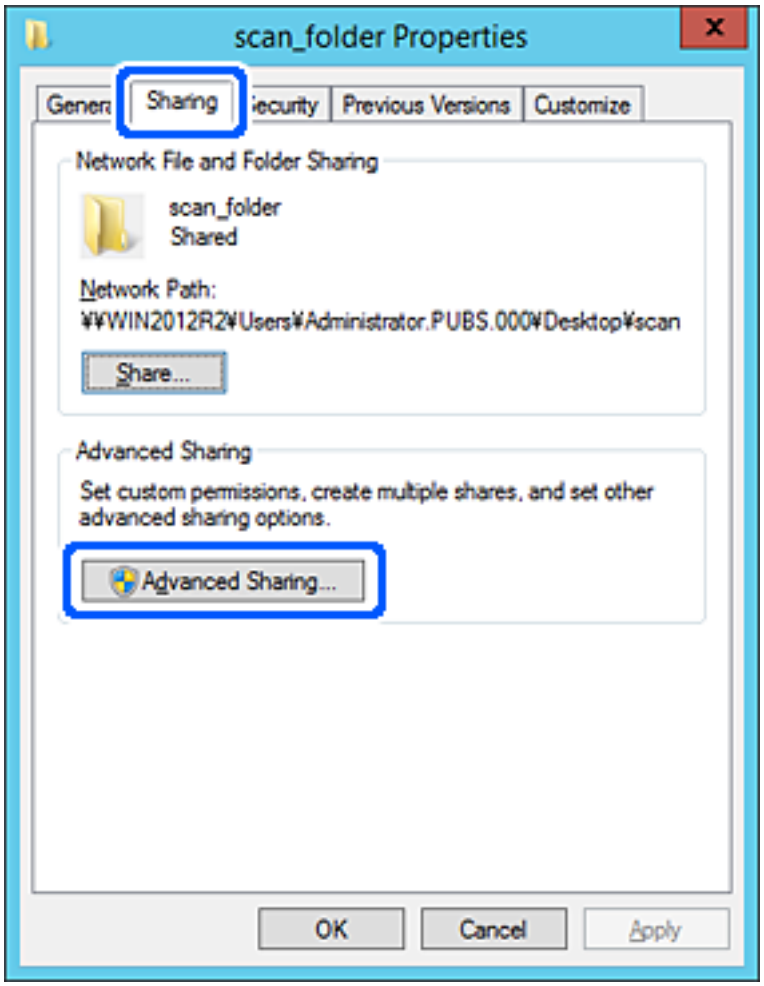
3. Diska saknes direktorijā izveidojiet mapi un piešķiriet tai nosaukumu „scan_folder”.

   Ievadiet 1–12 burtciparu rakstzīmes garu mapes nosaukumu. Pārsniedzot mapes nosaukuma rakstzīmju ierobežojumu, atkarībā no vides jūs, iespējams, nevarēsiet piekļūt mapei ierastajā veidā.

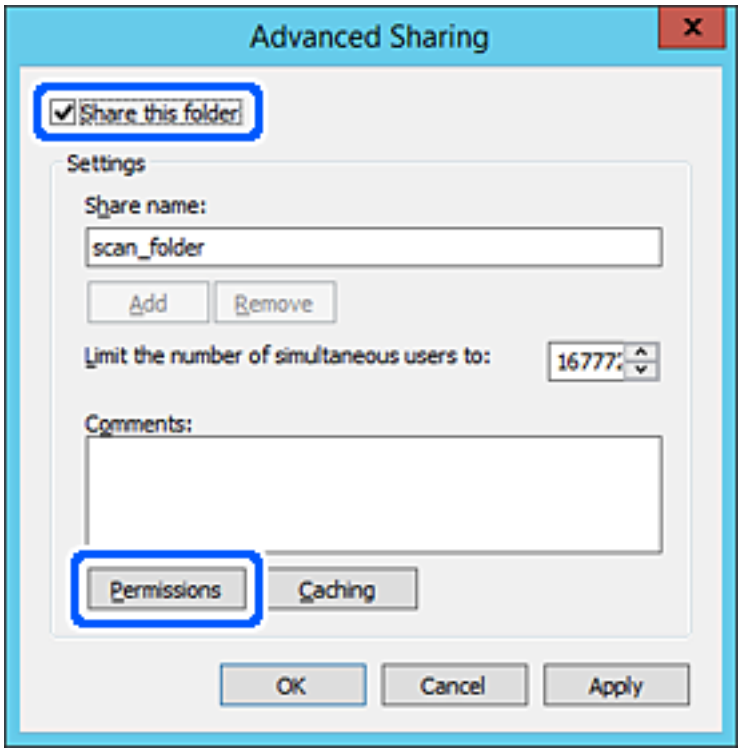
4. Ar peles labo pogu noklikšķiniet uz mapes un tad atlasiet **Rekvizīti**.



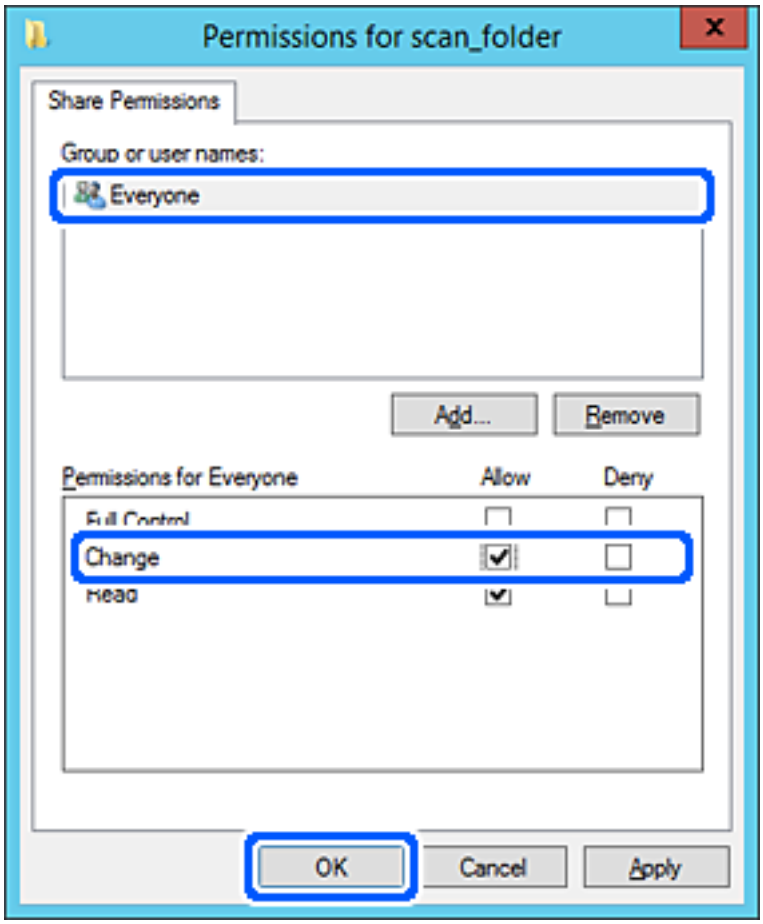
5. Noklikšķiniet uz **Papildu koplietošana** cilnē **Koplietošana**.



6. Atlasiet **Koplietot šo mapi** un tad noklikšķiniet uz **Atļaujas**.

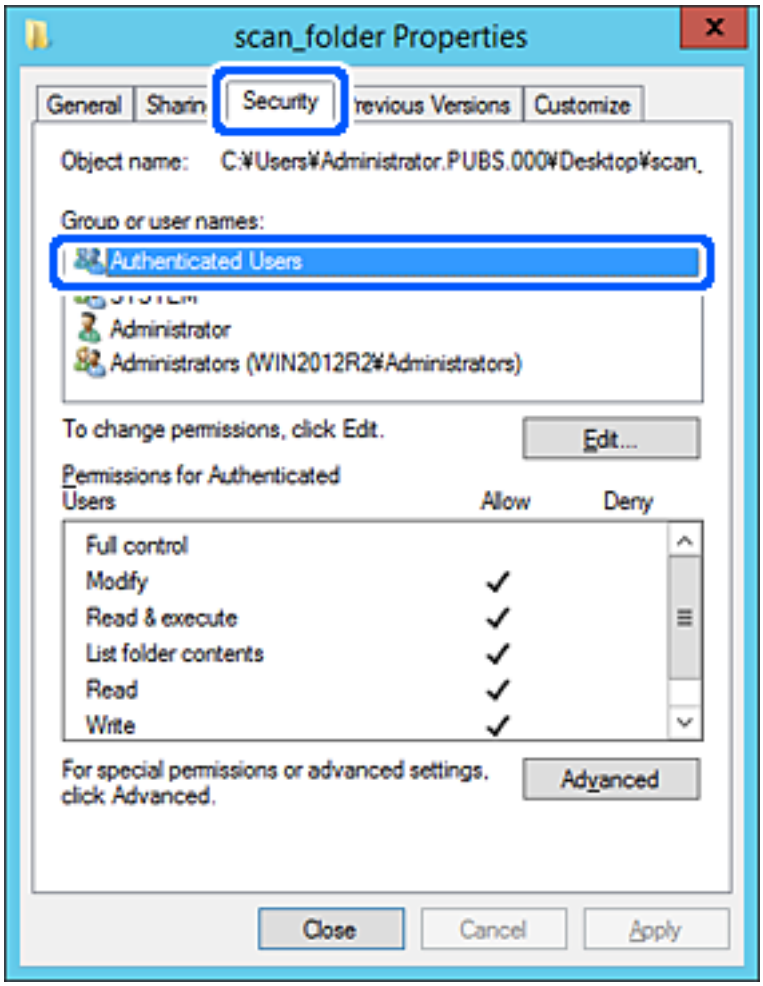


7. Atlasiet grupu **Visi** sadaļā **Grupu nosaukumi vai lietotājvārdi**, sadaļā **Mainīt** atlasiet **Atļaut** un tad noklikšķiniet uz **Labi**.



8. Noklikšķiniet uz **Labi**.

9. Atlasiet cilni **Drošība** un pēc tam atlasiet **Autentificētie lietotāji** sadaļā **Grupu nosaukumi vai lietotājvārdi**.

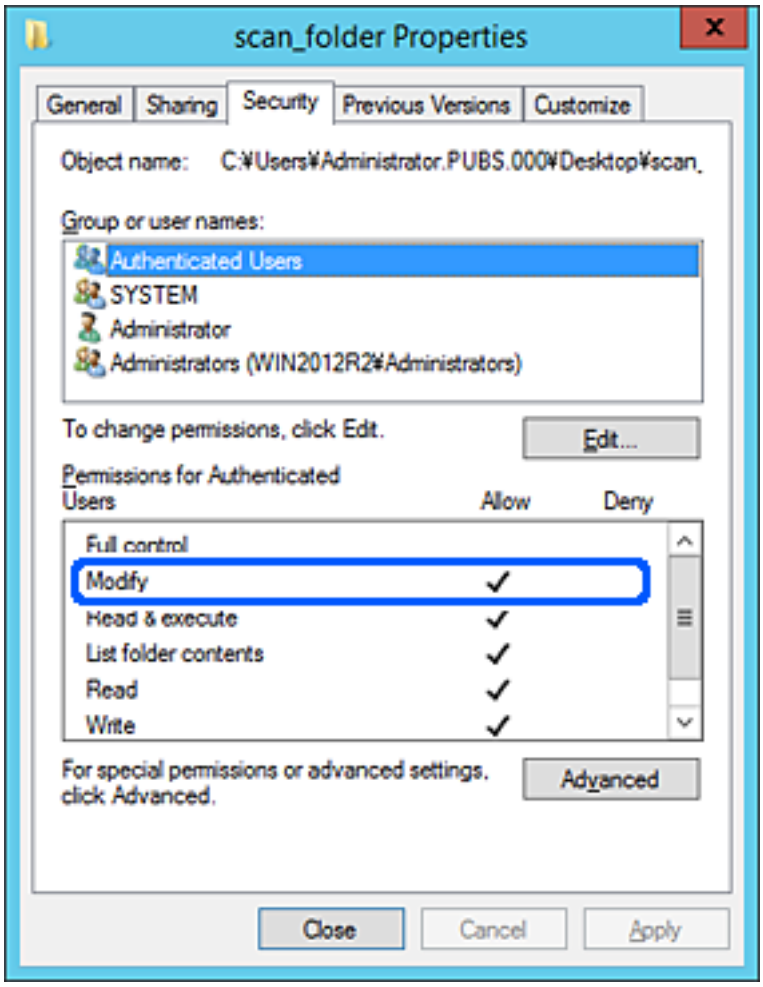


„Autentificētie lietotāji" ir īpaša grupa, un tā ietver visus lietotājus, kas var pieteikties domēnā vai datorā. Šī grupa tiek rādīta tikai tad, ja mape ir izveidota uzreiz zem saknes mapes.

Ja grupa netiek rādīta, varat to pievienot, noklikšķinot uz **Rediģēt**. Papildinformāciju skatiet sadaļā „Saistītā informācija".

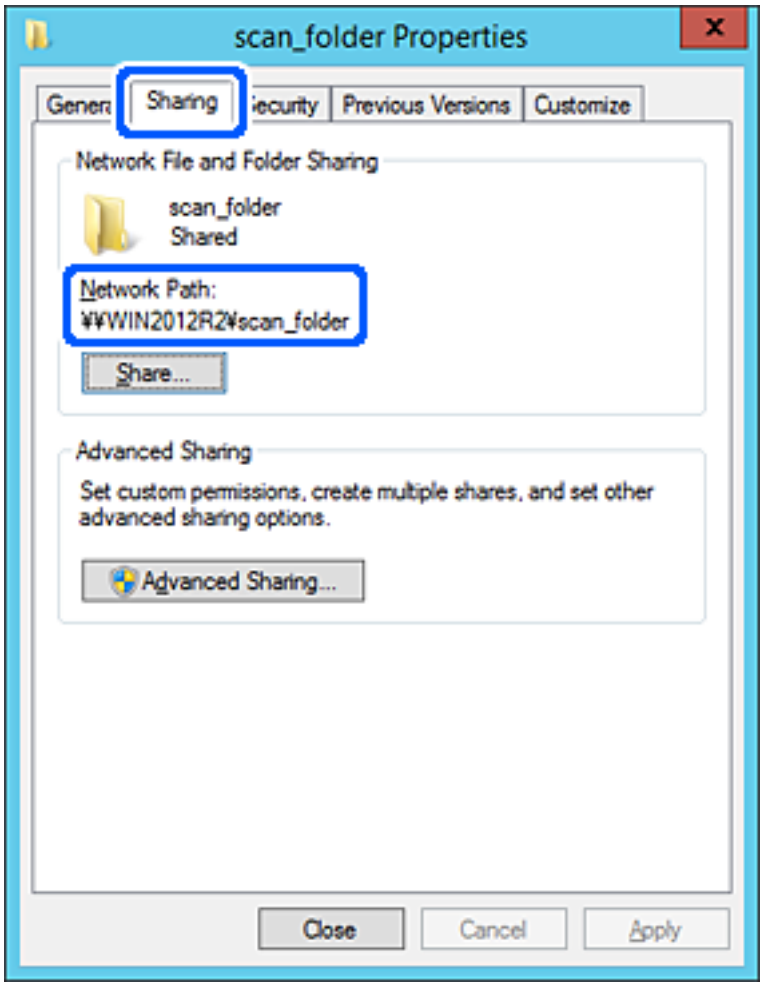
10. Pārbaudiet, vai opcija **Atļaut** ir atlasīta izvēlnes **Autentificēto lietotāju atļaujas** sadaļā **Modificēt**.

    Ja opcija nav atlasīta, atlasiet **Autentificētie lietotāji**, noklikšķiniet uz **Rediģēt**, atlasiet **Atļaut** izvēlnes **Autentificēto lietotāju atļaujas** sadaļā **Modificēt** un pēc tam noklikšķiniet uz **Labi**.



11. Atlasiet cilni **Koplietošana**.

    Tiek parādīts koplietošanas mapes tīkla ceļš. Tas tiek izmantots, veicot reģistrāciju skenera kontaktpersonu sarakstā. Lūdzu, pierakstiet to.



12. Noklikšķiniet uz **Labi** vai **Aizvērt**, lai aizvērtu ekrānu.

    Pārbaudiet, vai failu var ierakstīt vai nolasīt koplietotajā mapē, izmantojot tā paša domēna datorus.

Saistītā informācija

➡ "Grupas vai lietotāja pievienošana, atļaujot piekļuvi" 58. lpp.
➡ "Mērķa reģistrēšana kontaktpersonu sadaļā, izmantojot Web Config" 63. lpp.

Personālā datora konfigurācijas piemērs

Šajā paskaidrojumā sniegts piemērs koplietotās mapes izveidei tā lietotāja darbvirsmā, kas pašreiz pieteicies datorā.

Lietotājs, kas piesakās datorā un kuram ir administratora tiesības, var piekļūt darbvirsmas mapei un dokumentu mapei, kas atrodas mapē Lietotājs.

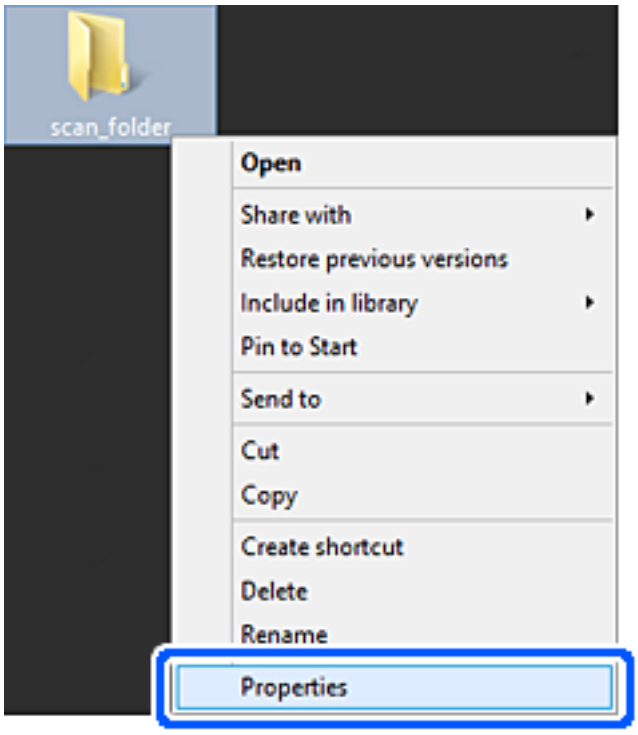
Iestatiet šo konfigurāciju, ja NEVĒLATIES citam lietotājam atļaut personālajā datorā esošas koplietotās mapes satura lasīšanu un rakstīšanu tajā.

❏ Koplietotās mapes izveides vieta: darbvirsma

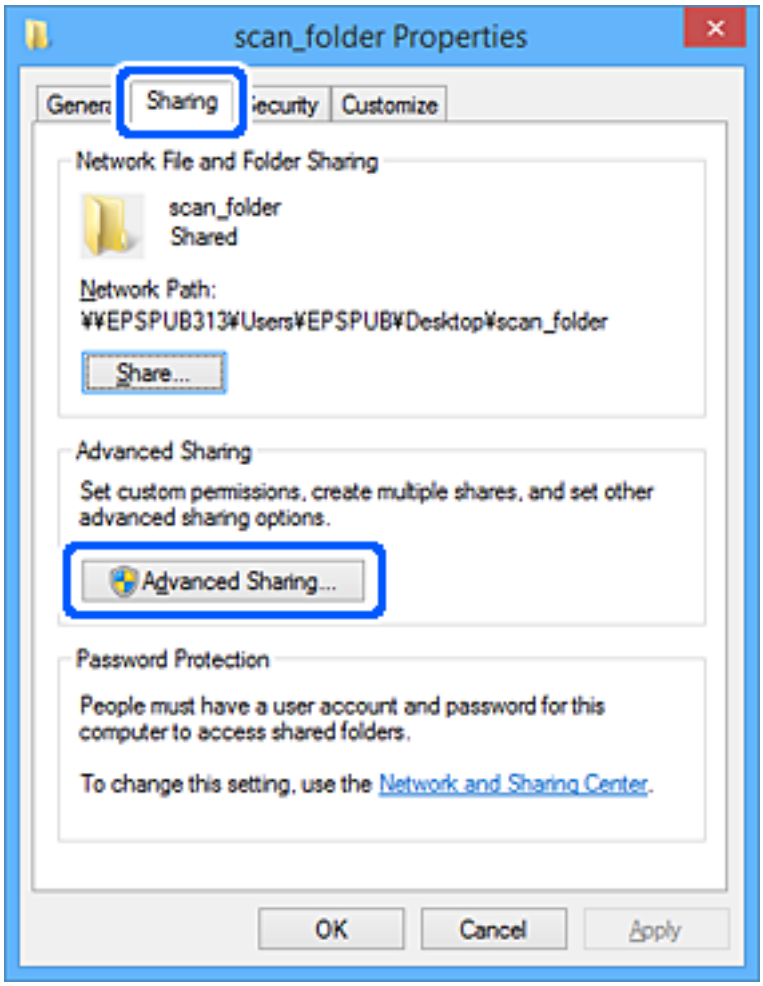
- ❏ Mapes ceļš: C:\Users\xxxx\Desktop\scan_folder
- ❏ Atļauja piekļuvei tīklā (koplietošanas pilnvaras): visiem
- ❏ Atļauja piekļuvei failu sistēmā (drošība): nepievienojiet vai pievienojiet lietotājvārdus/grupu nosaukumus, lai atļautu piekļuvi

1. Piesakieties datorā, kurā tiks izveidota koplietotā mape, izmantojot lietotāja kontu ar administratora atļaujām.
2. Palaidiet pārlūku.
3. Darbvirsmā izveidojiet mapi un piešķiriet tai nosaukumu „scan_folder”.

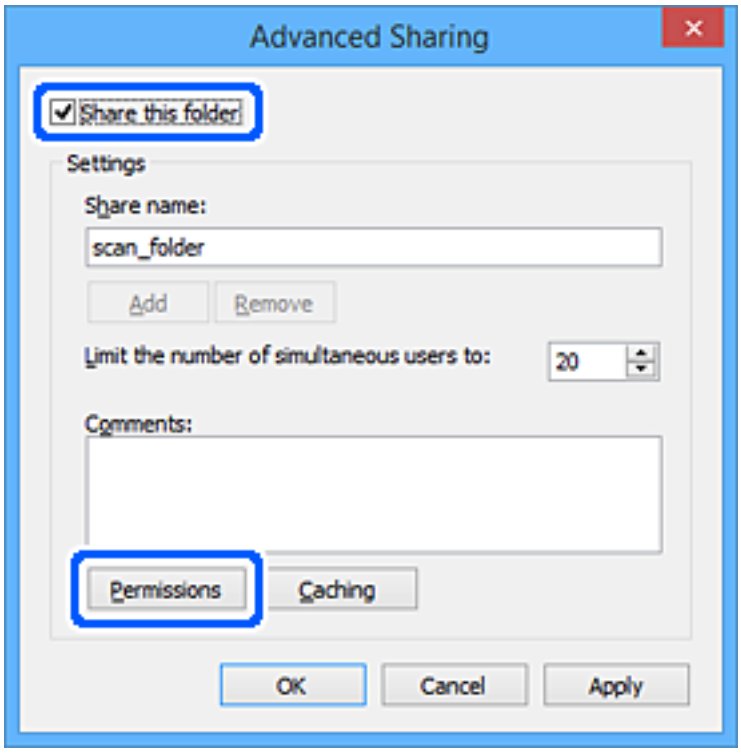
   Ievadiet 1–12 burtciparu rakstzīmes garu mapes nosaukumu. Pārsniedzot mapes nosaukuma rakstzīmju ierobežojumu, atkarībā no vides jūs, iespējams, nevarēsiet piekļūt mapei ierastajā veidā.
4. Ar peles labo pogu noklikšķiniet uz mapes un tad atlasiet **Rekvizīti**.



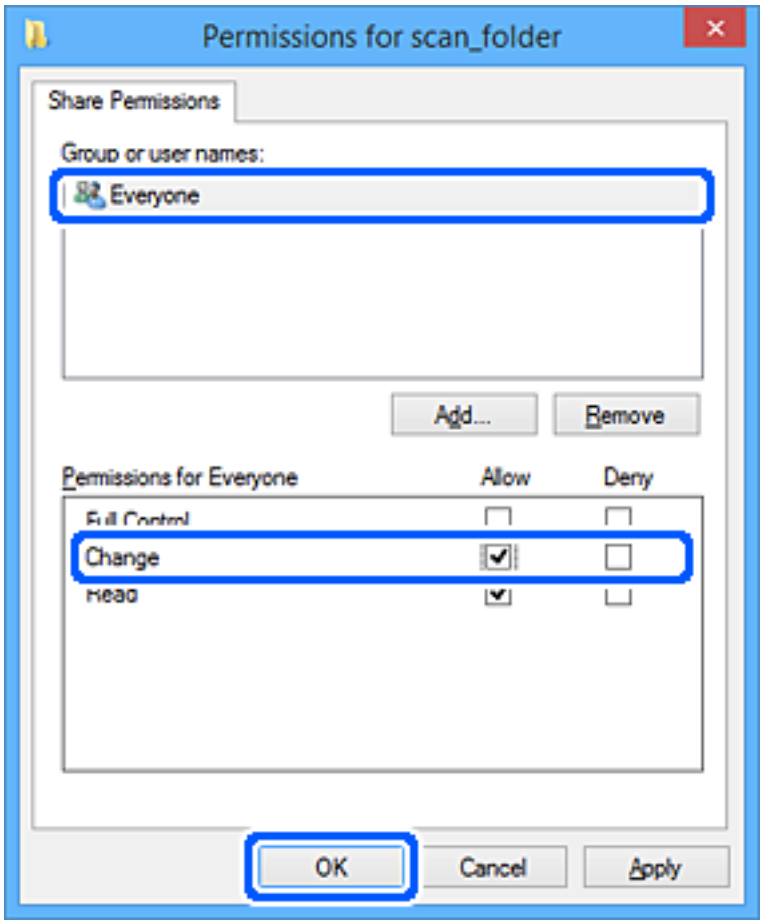
5. Noklikšķiniet uz **Papildu koplietošana** cilnē **Koplietošana**.



6. Atlasiet **Koplietot šo mapi** un tad noklikšķiniet uz **Atļaujas**.



7. Atlasiet grupu **Visi** sadaļā **Grupu nosaukumi vai lietotājvārdi**, sadaļā **Mainīt** atlasiet **Atļaut** un tad noklikšķiniet uz **Labi**.



8. Noklikšķiniet uz **Labi**.

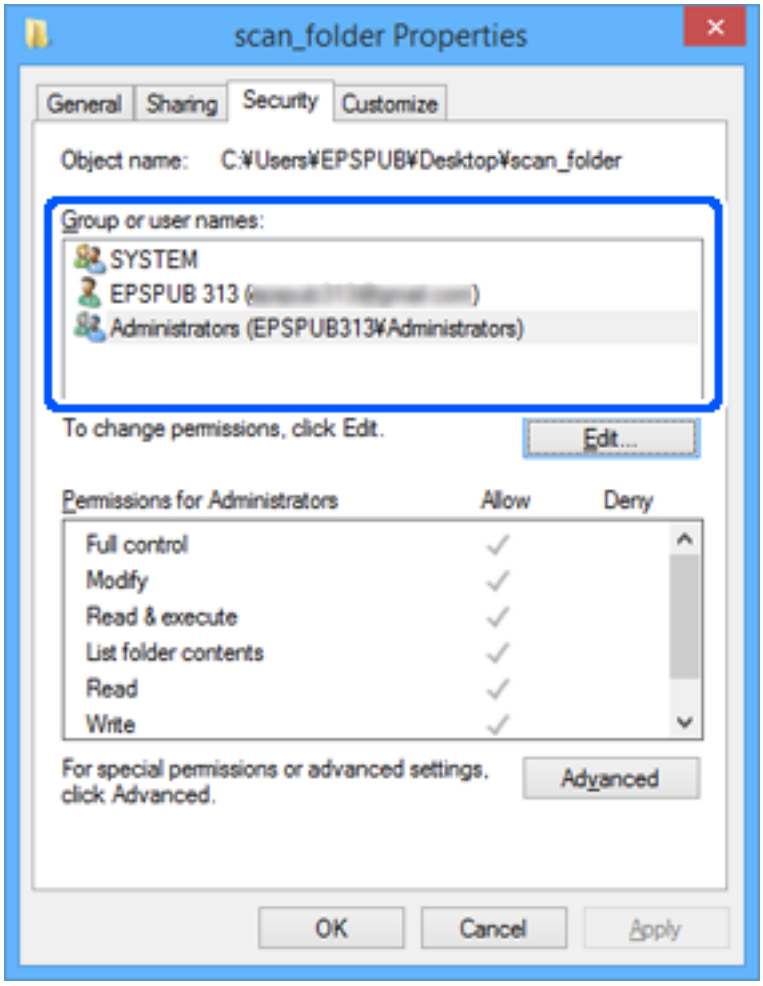
9. Atlasiet cilni **Drošība**.

10. Pārbaudiet grupu vai lietotāju sadaļā **Grupu nosaukumi vai lietotājvārdi**.

    Šajā sadaļā redzamā grupa vai lietotājs var piekļūt koplietotajai mapei.

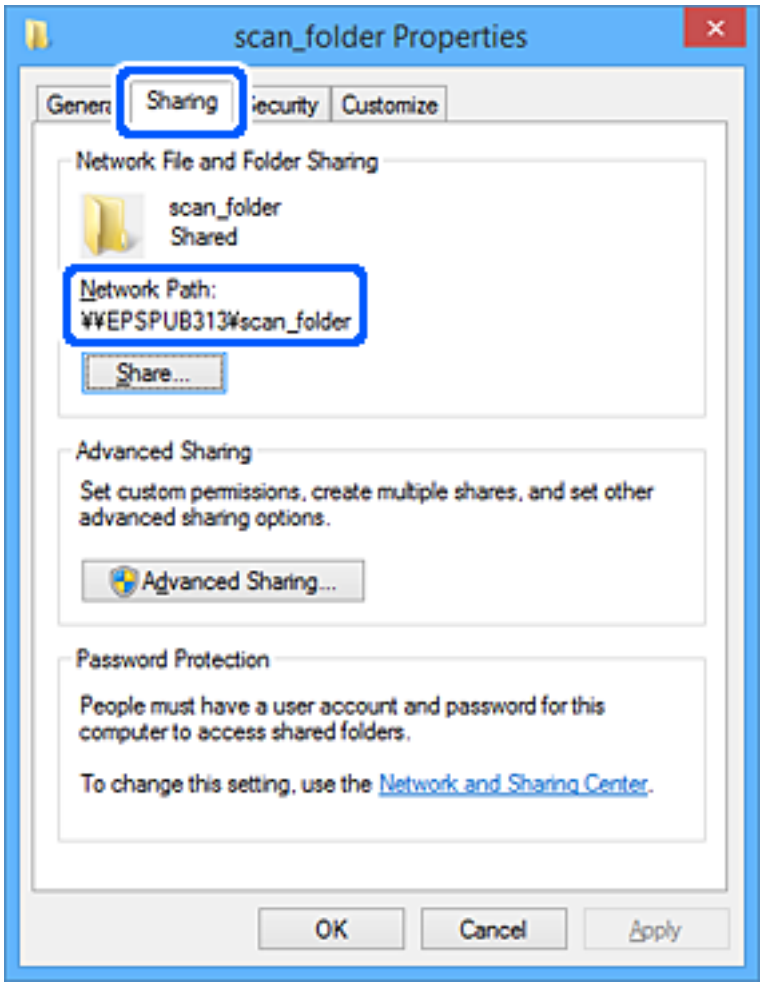
    Šajā gadījumā koplietotajai mapei var piekļūt lietotājs, kas piesakās šajā datorā, un administrators.

Ja nepieciešams, pievienojiet piekļuves atļauju. To var pievienot, noklikšķinot uz **Rediģēt**. Papildinformāciju skatiet sadaļā „Saistītā informācija”.



11. Atlasiet cilni **Koplietošana**.

    Tiek parādīts koplietošanas mapes tīkla ceļš. Tas tiek izmantots, veicot reģistrāciju skenera kontaktpersonu sarakstā. Lūdzu, pierakstiet to.



12. Noklikšķiniet uz **Labi** vai **Aizvērt**, lai aizvērtu ekrānu.

    Pārbaudiet, vai failu var ierakstīt vai nolasīt koplietotajā mapē, izmantojot to lietotāju vai grupu datorus, kam piešķirta piekļuves atļauja.

Saistītā informācija

➡ "Grupas vai lietotāja pievienošana, atļaujot piekļuvi" 58. lpp.

➡ "Mērķa reģistrēšana kontaktpersonu sadaļā, izmantojot Web Config" 63. lpp.

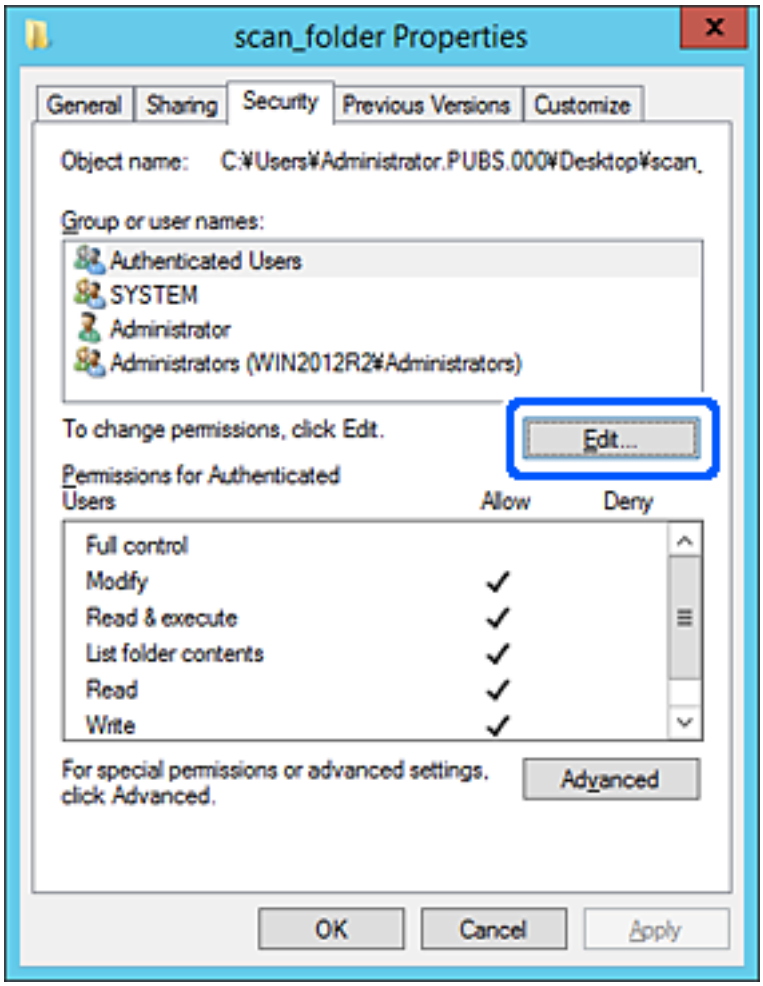
Grupas vai lietotāja pievienošana, atļaujot piekļuvi

Varat pievienot grupu vai lietotāju, tādējādi atļaujot piekļuvi.

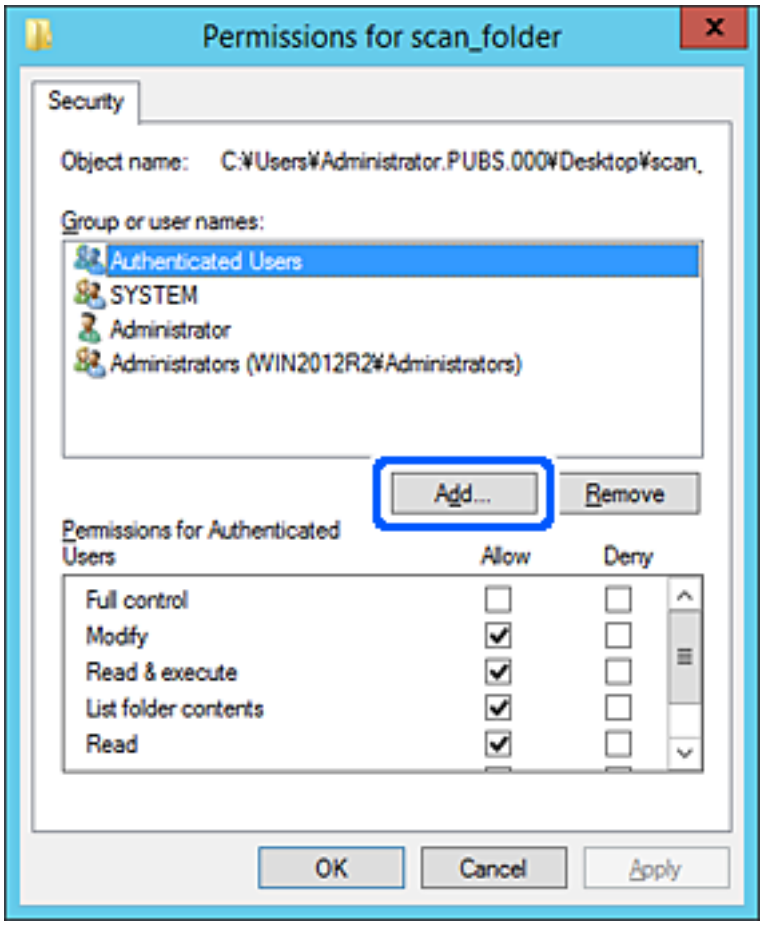
1. Ar peles labo pogu noklikšķiniet uz mapes un atlasiet **Rekvizīti**.

2. Atlasiet cilni **Drošība**.

3. Noklikšķiniet uz **Rediģēt**.



4. Noklikšķiniet uz **Pievienot** sadaļā **Grupu nosaukumi vai lietotājvārdi**.

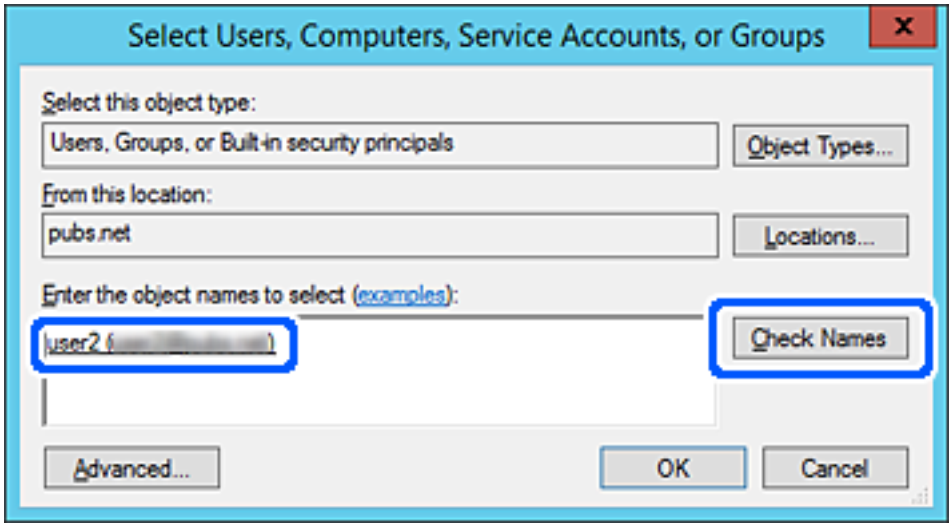


5. Ievadiet grupas nosaukumu vai lietotājvārdu, kam vēlaties atļaut piekļuvi, un pēc tam noklikšķiniet uz **Pārbaudīt vārdus**.

   Nosaukums/vārds tiek pasvītrots.

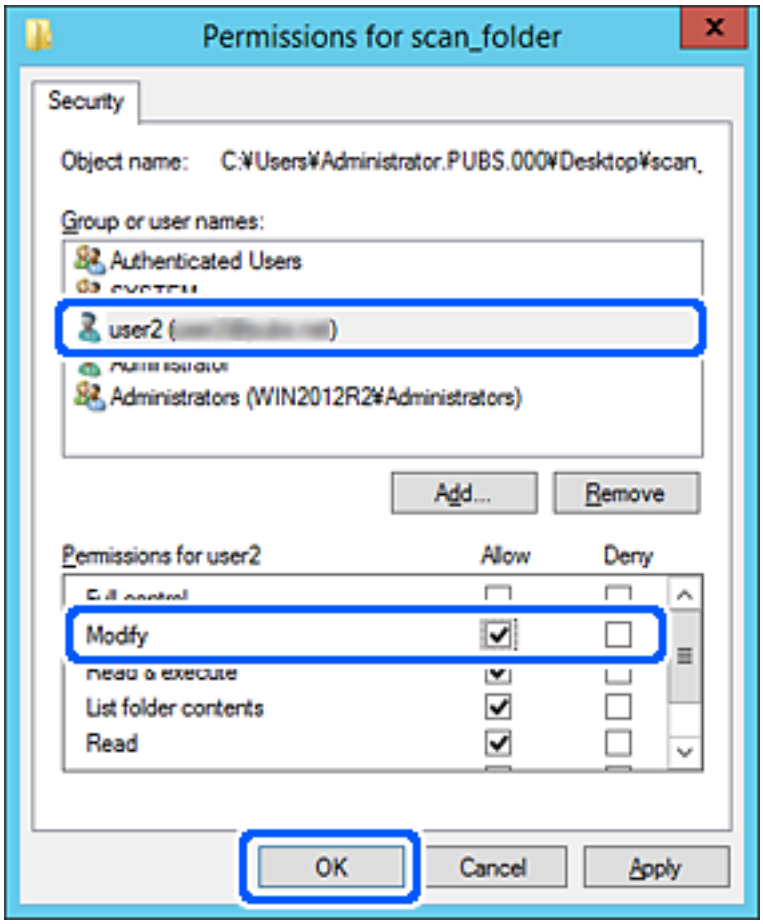
Piezīme:
Ja nezināt pilno grupas nosaukumu vai lietotājvārdu, ievadiet tā daļu un noklikšķiniet uz ***Pārbaudīt vārdus****. Tiks parādīti grupu nosaukumi vai lietotājvārdi, kas atbilst vārda daļai, un pēc tam sarakstā varat atlasīt pilno nosaukumu/vārdu.*

Ja atbilst tikai viens nosaukums/vārds, pilnais nosaukums/vārds ar pasvītrojumu tiek parādīts laukā ***Ievadiet atlasāmā objekta nosaukumu****.*



6. Noklikšķiniet uz **Labi**.

7. Ekrānā Atļaujas atlasiet sadaļā **Grupu nosaukumi vai lietotājvārdi** ievadīto lietotājvārdu, piešķiriet atļauju **Modificēt**, pēc tam noklikšķiniet uz **Labi**.



8. Noklikšķiniet uz **Labi** vai **Aizvērt**, lai aizvērtu ekrānu.

   Pārbaudiet, vai failu var ierakstīt vai nolasīt koplietotajā mapē, izmantojot to lietotāju vai grupu datorus, kam piešķirta piekļuves atļauja.

Kontaktpersonu pieejamības sniegšana

Adresātu reģistrēšana skenera kontaktpersonu sarakstā, skenējot ļauj viegli ievadīt adresātu.

Kontaktpersonu sarakstā var reģistrēt tālāk norādītu veidu adresātus. Kopā var reģistrēt līdz 300 ierakstiem.

Piezīme:
Adresātu var ievadīt, izmantojot arī LDAP serveri (LDAP meklēšana).

E-pasts	E-pasta adresāts. Vispirms jākonfigurē e-pasta servera iestatījumi.
Tīkla mape	Skenēšanas datu adresāts. Pirms skenēšanas jāsagatavo tīkla mape.

Saistītā informācija

➡ "LDAP servera un lietotāju mijiedarbība" 69. lpp.

Kontaktu konfigurācijas salīdzinājums

Pieejami trīs skenera kontaktpersonu konfigurēšanas rīki: Web Config, Epson Device Admin un printera vadības panelis. Tabulā turpmāk norādītas šo rīku atšķirības.

Funkcijas	Web Config*	Epson Device Admin	Skenera vadības panelis
Galamērķa reģistrēšana	✓	✓	✓
Galamērķa rediģēšana	✓	✓	✓
Grupas pievienošana	✓	✓	✓
Grupas rediģēšana	✓	✓	✓
Galamērķu vai grupu dzēšana	✓	✓	✓
Visu galamērķu dzēšana	✓	✓	–
Faila importēšana	✓	✓	–
Eksportēšana uz failu	✓	✓	–

* Piesakieties kā administrators, lai veiktu iestatījumus.

Mērķa reģistrēšana kontaktpersonu sadaļā, izmantojot Web Config

Piezīme:
Kontaktpersonas var reģistrēt arī skenera vadības panelī.

1. Atveriet programmu Web Config un atlasiet cilni **Scan** > **Contacts**.
2. Izvēlēties reģistrējamo numuru un tad noklikšķiniet uz **Edit**.
3. Ievadiet **Name** un **Index Word**.
4. Atlasiet adresāta veidu kā **Type**.

   Piezīme:
   *Pēc reģistrēšanas iespēju **Type** vairs nevarēs mainīt. Ja vēlaties mainīt veidu, izdzēsiet adresātu un tad vēlreiz reģistrējiet.*
5. Ievadiet katra vienuma vērtību un tad noklikšķiniet uz **Apply**.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Adresāta iestatīšanas vienumi

Posms	Iestatījumi un skaidrojums
Parastie iestatījumi	
Name	Izmantojot unikoda (UTF-8) rakstzīmes, ievadiet vārdu un uzvārdu, ne vairāk par 30 rakstzīmēm, kas būs redzams pie kontaktpersonām. Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Index Word	Ievadiet nosaukumu, kas satur 30 rakstzīmes vai mazāk Unicode (UTF-8), lai meklētu kontaktpersonas skenera vadības panelī. Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Type	Atlasiet adreses veidu, ko vēlaties reģistrēt.
Assign to Frequent Use	Atlasiet, lai reģistrētu adresi iestatītu, kā bieži izmantotu adresi. Iestatot adresi kā bieži izmantotu adresi, tā tiks parādīta skenēšanas ekrāna augšdaļā un adresātu varēs norādīt, neatverot kontaktpersonu sarakstu.
Email	
Email Address	Ievadiet 1–255 rakstzīmes: A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Network Folder (SMB)	
Save to	\\„Mapes ceļš” Ievadiet mērķa mapes atrašanās vietu — no 1 līdz 253 unikoda (UTF-8) rakstzīmēm, izlaižot daļu „\\”. Ievadiet tīkla ceļu, kas attēlots mapes rekvizītu ekrānā. Papildinformāciju par tīkla ceļa iestatīšanu skatiet tālāk. "Personālā datora konfigurācijas piemērs" 52. lpp.
User Name	Lai piekļūtu tīkla mapei, ievadiet lietotājvārdu, ne garāku par 30 unikoda (UTF-8) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F).
Password	Lai piekļūtu tīkla mapei, ievadiet paroli, ne garāku par 20 unikoda (UTF-8) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F).
FTP	
Secure Connection	Atlasiet FTP vai FTPS atbilstoši faila pārsūtīšanas protokolam, kuru atbalsta FTP serveris. Atlasiet **FTPS**, lai ļautu skenerim sazināties, izmantojot drošības pasākumus.
Save to	Ievadiet servera nosaukumu diapazonā no 1 līdz 253 rakstzīmēm, izmantojot ASCII (0x20–0x7E) un izlaižot „ftp://” vai ftps://”.
User Name	Lai piekļūtu FTP serverim, ievadiet lietotājvārdu, ne garāku par 30 unikoda (UTF-8) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F). Ja serveris atļauj anonīmus savienojumus, ievadiet lietotājvārdu Anonīms un FTP. Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Password	Lai piekļūtu FTP serverim, ievadiet paroli, ne garāku par 20 unikoda (UTF-8) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F). Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Connection Mode	Izvēlnē atlasiet savienojuma režīmu. Ja starp skeneri un FTP serveri atrodas ugunsmūris, atlasiet **Passive Mode**.
Port Number	Ievadiet FTP servera porta numuru — skaitli no 1 līdz 65535.

Posms	Iestatījumi un skaidrojums
Certificate Validation	FTP servera sertifikāts tiek apstiprināts, kas tas ir iespējots. Tas ir pieejams, kad **FTPS** ir izvēlēts kā **Secure Connection** iestatījums. Lai veiktu iestatīšanu, CA Certificate jāimportē skenerī.
SharePoint(WebDAV)	
Secure Connection	Atlasiet HTTP vai HTTPS atbilstoši faila pārsūtīšanas protokolam, kuru atbalsta serveris. Atlasiet **HTTPS**, lai ļautu skenerim sazināties, izmantojot drošības pasākumus.
Save to	Ievadiet servera nosaukumu diapazonā no 1 līdz 253 rakstzīmēm, izmantojot ASCII (0x20–0x7E) un izlaižot „http://" vai https://".
User Name	Lai piekļūtu serverim, ievadiet lietotājvārdu, ne garāku par 30 unikoda (UTF-8) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F). Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Password	Lai piekļūtu serverim, ievadiet paroli, ne garāku par 20 unikoda (UTF-8) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F). Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Certificate Validation	Servera sertifikāts tiek apstiprināts, kad tas ir iespējots. Tas ir pieejams, kad **HTTPS** ir izvēlēts kā **Secure Connection** iestatījums. Lai veiktu iestatīšanu, CA Certificate jāimportē skenerī.
Proxy Server	Izvēlieties, vai jāizmanto starpniekserveris.

Mērķa kā grupas reģistrēšana, izmantojot Web Config

Ja mērķu veida iestatījums ir **Email**, mērķus var reģistrēt kā grupu.

1. Atveriet programmu Web Config un atlasiet cilni **Scan** > **Contacts**.
2. Izvēlēties reģistrējamo numuru un tad noklikšķiniet uz **Edit**.
3. Sadaļā **Type** atlasiet grupu.
4. Noklikšķiniet uz **Select**, lai atvērtu sadaļu **Contact(s) for Group**.
   Tiks parādīti pieejamie adresāti.
5. Atlasiet adresātu, ko vēlaties reģistrēt grupā, un tad noklikšķiniet uz **Select**.
6. Atveriet **Name** un **Index Word**.
7. Atlasiet, vai piešķirt reģistrēto grupu bieži izmantotajai grupai.
   Piezīme:
   Adresātus var reģistrēt vairākās grupās.
8. Noklikšķiniet uz **Apply**.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Kontaktpersonu dublēšana un importēšana

Izmantojot programmu Web Config vai citus rīkus, varat dublēt un importēt kontaktpersonas.

Programmai Web Config varat dublēt kontaktpersonas, eksportējot kontaktpersonas ietverošus skenera iestatījumus. Eksportēto failu nevar rediģēt, jo tas ir eksportēts kā binārais fails.

Importējot skenera iestatījumus skenerī, kontaktpersonas tiek pārrakstītas.

Programmai Epson Device Admin no ierīces rekvizītu ekrāna var eksportēt tikai kontaktpersonas. Tāpat, ja nevēlaties eksportēt ar drošību saistītos vienumus, varat rediģēt eksportētās kontaktpersonas un importēt tās, jo tās var saglabāt kā SYLK vai CSV failu.

Kontaktpersonu importēšana, izmantojot Web Config

Ja jums ir skeneris, kas ļauj dublēt kontaktpersonas, un tas ir saderīgs ar šo skeneri, jūs varat viegli reģistrēt kontaktpersonas importējot dublējuma failu.

Piezīme:
Instrukcijas par skenera kontaktpersonu dublēšanu skatiet skenerī pievienotajā rokasgrāmatā.

Izpildiet tālāk norādītās darbības, lai šajā skenerī importētu kontaktpersonas.

1. Piekļūstiet Web Config, atlasiet cilni **Device Management** > **Export and Import Setting Value** > **Import**.
2. Izvēlieties dublējuma failu, kas izveidots **File**, ievadiet paroli un noklikšķiniet **Next**.
3. Atlasiet izvēles rūtiņu **Contacts** un pēc tam noklikšķiniet **Next**.

Kontaktpersonu dublēšana, izmantojot Web Config

Kontaktpersonu dati var tikt zaudēti skenera disfunkcijas dēļ. Ieteicams izveidot datu dublējumkopiju pēc katras datu atjaunināšanas reizes. Epson neuzņemas atbildību par jebkādiem zaudētiem datiem, kā arī par datu un/vai iestatījumu dublēšanu un atjaunošanu pat garantijas perioda laikā.

Izmantojot Web Config, varat datorā dublēt skenerī saglabātos kontaktpersonu datus.

1. Atveriet programmu Web Config un tad atlasiet cilni **Device Management** > **Export and Import Setting Value** > **Export**.
2. Atlasiet **Contacts** izvēles rūtiņu kategorijā **Scan**.
3. Ievadiet paroli, lai šifrētu eksportēto failu.

   Faila importēšanai nepieciešama parole. Ja nevēlaties šifrēt failu, atstājiet šo lauku tukšu.
4. Noklikšķiniet uz **Export**.

Liela kontaktpersonu apjoma eksportēšana un reģistrācija, izmantojot rīku

Izmantojot programmu Epson Device Admin, varat dublēt tikai kontaktpersonas un rediģēt eksportētos failus, kā arī pēc tam tos vienlaicīgi reģistrēt.

Tas ir noderīgi, ja vēlaties dublēt tikai kontaktpersonas vai maināt skeneri un vēlaties pārsūtīt kontaktpersonas no vecā skenera uz jauno.

Kontaktpersonu eksportēšana

Saglabājiet kontaktpersonu informāciju failā.

Varat rediģēt SYLK vai csv formātā saglabātos failus, izmantojot izklājlapu lietojumprogrammu vai teksta redaktoru. Pēc informācijas dzēšanas vai pievienošanas visu informāciju var vienlaicīgi reģistrēt.

Informāciju, kas ietver drošības vienumus, piemēram, paroli un personas informāciju, var saglabāt binārā formātā un aizsargāt ar paroli. Jūs nevarat rediģēt failu. To var izmantot kā informācijas dublējuma failu, ietverot drošības vienumus.

1. Palaidiet Epson Device Admin.
2. Sānu joslas uzdevumu izvēlnē atlasiet **Devices**.
3. Ierīču sarakstā atlasiet ierīci, kuru vēlaties konfigurēt.
4. Noklikšķiniet uz **Device Configuration** lentes izvēlnes cilnē **Home**.

   Ja ir iestatīta administratora parole, ievadiet paroli un noklikšķiniet uz **OK**.
5. Noklikšķiniet uz **Common** > **Contacts**.
6. Atlasiet eksportēšanas formātu sadaļā **Export** > **Export items**.
   - ❏ All Items

     Eksportējiet šifrēto bināro failu. Atlasiet, ja vēlaties ietvert drošības vienumus, piemēram, paroli un personas informāciju. Jūs nevarat rediģēt failu. Ja to atlasāt, jums jāiestata parole. Noklikšķiniet uz **Configuration** un iestatiet 8–63 rakstzīmes garu paroli ASCII formātā. Šī parole tiek prasīta, importējot bināro failu.
   - ❏ Items except Security Information

     Eksportējiet SYLK vai csv formāta failus. Atlasiet, ja vēlaties rediģēt eksportētā faila informāciju.
7. Noklikšķiniet uz **Export**.
8. Norādiet faila saglabāšanas vietu, atlasiet faila tipu un noklikšķiniet uz **Save**.

   Tiek parādīts ziņojums par pabeigšanu.
9. Noklikšķiniet uz **OK**.

   Pārbaudiet, vai fails ir saglabāts norādītajā vietā.

Kontaktpersonu importēšana

Importējiet kontaktpersonu informāciju no faila.

Varat importēt SYLK vai csv formātā saglabātus failus vai dublētu bināro failu, kas ietver drošības vienumus.

1. Palaidiet Epson Device Admin.
2. Sānu joslas uzdevumu izvēlnē atlasiet **Devices**.
3. Ierīču sarakstā atlasiet ierīci, kuru vēlaties konfigurēt.
4. Noklikšķiniet uz **Device Configuration** lentes izvēlnes cilnē **Home**.

   Ja ir iestatīta administratora parole, ievadiet paroli un noklikšķiniet uz **OK**.
5. Noklikšķiniet uz **Common** > **Contacts**.
6. Noklikšķiniet uz **Browse** sadaļā **Import**.
7. Atlasiet importējamo failu un noklikšķiniet uz **Open**.

   Atlasot bināro failu, sadaļā **Password** ievadiet paroli, ko iestatījāt, eksportējot failu.
8. Noklikšķiniet uz **Import**.

   Tiek parādīts apstiprinājuma ekrāns.
9. Noklikšķiniet uz **OK**.

   Tiek parādīts validācijas rezultāts.

   ❏ Edit the information read

   Noklikšķiniet, kad vēlaties atsevišķi rediģēt informāciju.

   ❏ Read more file

   Noklikšķiniet, kad vēlaties importēt vairākus failus.
10. Noklikšķiniet uz **Import**, tad importēšanas pabeigšanas ekrānā noklikšķiniet uz **OK**.

    Atgriezieties ierīces rekvizītu ekrānā.
11. Noklikšķiniet uz **Transmit**.
12. Apstiprinājuma ziņojumā noklikšķiniet uz **OK**.

    Iestatījumi tiek nosūtīti skenerim.
13. Sūtīšanas pabeigšanas ekrānā noklikšķiniet uz **OK**.

    Skenera informācija tiek atjaunināta.

    Atveriet kontaktpersonu sarakstu programmā Web Config vai skenera vadības panelī un tad pārbaudiet, vai kontaktpersonas informācija ir atjaunināta.

LDAP servera un lietotāju mijiedarbība

Mijiedarbojoties ar LDAP serveri, adreses informāciju, kas reģistrēta LDAP serverī, varat izmantot kā e-pasta mērķi.

LDAP servera konfigurēšana

Lai izmantotu LDAP servera informāciju, reģistrējiet to skenerī.

1. Atveriet programmu Web Config un atlasiet cilni **Network** > **LDAP Server** > **Basic**.
2. Ievadiet vērtību katram vienumam.
3. Izvēlieties **OK**.

   Tiks parādīti atlasītie iestatījumi.

LDAP servera vienumu iestatīšana

Posms	Iestatījumi un skaidrojums
Use LDAP Server	Atlasiet **Use** vai **Do Not Use**.
LDAP Server Address	Ievadiet LDAP servera adresi. Ievadiet 1–255 rakstzīmes IPv4, IPv6 vai FQDN formātā. FQDN formātā var izmantot burtciparu rakstzīmes ASCII (0x20–0x7E) kodējumā un „-", izņemot adreses sākumu un beigas.
LDAP server Port Number	Ievadiet LDAP servera porta numuru — skaitli no 1 līdz 65535.
Secure Connection	Norādiet autentifikācijas metodi, kas tiks izmantota, kad skeneris piekļūs LDAP serverim.
Certificate Validation	Iespējojot šo funkciju, tiek validēts LDAP servera sertifikāts. Ieteicams to iestatīt kā **Enable**. Lai veiktu iestatīšanu, **CA Certificate** jāimportē skenerī.
Search Timeout (sec)	Iestatiet meklēšanas laiku, pirms iestājas noildze: diapazonā no 5 līdz 300.
Authentication Method	Atlasiet kādu no metodēm. Atlasot **Kerberos Authentication**, Kerberos iestatījumu veikšanai izvēlieties **Kerberos Settings**. Lai veiktu Kerberos Authentication, nepieciešama tālāk norādītā vide. ❏ Skeneris un DNS serveris var veikt saziņu. ❏ Skenera, KDC servera un autentifikācijai nepieciešamā servera (LDAP servera, SMTP servera, failu servera) laiks tiek sinhronizēts. ❏ Kad pakalpojumu serveris tiek piešķirts kā IP adrese, pakalpojumu servera FQDN tiek reģistrēts DNS servera reversās uzmeklēšanas apgabalā.
Kerberos Realm to be Used	Atlasot **Authentication Method** iespēju **Kerberos Authentication**, izvēlieties izmantojamo Kerberos nozarojumu.

Posms	Iestatījumi un skaidrojums
Administrator DN / User Name	Ievadiet lietotājvārdu LDAP serverim, ne garāku par 128 unikoda (UTF-8) rakstzīmēm. Nevar izmantot kontroles rakstzīmes, piemēram, 0x00–0x1F un 0x7F. Šis iestatījums netiek izmantots, ja ir atlasīta **Anonymous Authentication** iespēja **Authentication Method**. Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Password	Ievadiet paroli autentifikācijai LDAP serverī, ne garāku par 128 unikoda (UTF-8) rakstzīmēm. Nevar izmantot kontroles rakstzīmes, piemēram, 0x00–0x1F un 0x7F. Šis iestatījums netiek izmantots, ja ir atlasīta **Anonymous Authentication** iespēja **Authentication Method**. Ja nevēlaties to darīt, atstājiet šo lauku tukšu.

Kerberos iestatījumi

Ja atlasāt **Kerberos Authentication** iestatījumam **Authentication Method** sadaļā **LDAP Server** > **Basic**, izvēlieties tālāk norādītos Kerberos iestatījumus cilnē **Network** > **Kerberos Settings**. Var reģistrēt līdz 10 Kerberos iestatījumiem.

Posms	Iestatījumi un skaidrojums
Realm (Domain)	Ievadiet Kerberos autentifikācijas apgabalu, ne vairāk kā 255 ASCII rakstzīmes (0x20–0x7E). Ja nevēlaties to reģistrēt, atstājiet šo lauku tukšu.
KDC Address	Ievadiet Kerberos autentifikācijas servera adresi. Ievadiet ne vairāk kā 255 rakstzīmes IPv4, IPv6 vai FQDN formātā. Ja nevēlaties to reģistrēt, atstājiet šo lauku tukšu.
Port Number (Kerberos)	Ievadiet Kerberos servera porta numuru diapazonā no 1 līdz 65535.

LDAP servera meklēšanas iestatījumu konfigurēšana

Izveidojot meklēšanas iestatījumus, jūs varat izmantot LDAP serverī reģistrēto e-pasta adresi.

1. Atveriet programmu Web Config un atlasiet cilni **Network** > **LDAP Server** > **Search Settings**.
2. Ievadiet vērtību katram vienumam.
3. Noklikšķiniet uz **OK**, lai tiktu parādīts iestatīšanas rezultāts.

   Tiks parādīti atlasītie iestatījumi.

LDAP servera meklēšanas vienumu iestatīšana

Posms	Iestatījumi un skaidrojums
Search Base (Distinguished Name)	Ja vēlaties meklēt patvaļīgu domēnu, norādiet LDAP servera domēna nosaukumu. Ievadiet 0–128 unikoda rakstzīmes (UTF-8). Ja nevēlaties meklēt brīvi noteiktu atribūtu, atstājiet šo lauku tukšu. Lokālā servera direktorija piemērs: dc=server,dc=local
Number of search entries	Norādiet meklēšanas ierakstu skaitu diapazonā no 5 līdz 500. Norādītais meklēšanas ierakstu skaits tiks saglabāts un īslaicīgi parādīts. Pat ja meklēšanas ierakstu skaits pārsniedz norādīto un tiek parādīts kļūdas ziņojums, meklēšanu tomēr var veikt.

Posms	Iestatījumi un skaidrojums
User name Attribute	Norādiet atribūta nosaukumu, kas jāparāda, meklējot lietotājvārdus. Ievadiet līdz 1–255 unikoda rakstzīmes (UTF-8). Pirmajai rakstzīmei jābūt a–z vai A–Z. Piemērs: cn, uid
User name Display Attribute	Norādiet atribūta nosaukumu, kas jāparāda kā lietotājvārds. Ievadiet līdz 0–255 unikoda rakstzīmes (UTF-8). Pirmajai rakstzīmei jābūt a–z vai A–Z. Piemērs: cn, sn
Email Address Attribute	Norādiet atribūta nosaukumu, kas jāparāda, meklējot e-pasta adreses. Ievadiet 1–255 rakstzīmju kombināciju, izmantojot A–Z, a–z, 0–9, un -. Pirmajai rakstzīmei jābūt a–z vai A–Z. Piemērs: pasts
Arbitrary Attribute 1 - Arbitrary Attribute 4	Lai veiktu meklēšanu, var norādīt arī citus brīvi noteiktus atribūtus. Ievadiet līdz 0–255 unikoda rakstzīmes (UTF-8). Pirmajai rakstzīmei jābūt a–z vai A–Z. Ja nevēlaties meklēt patvaļīgus atribūtus, atstājiet šo lauku tukšu. Piemērs: o, ou

LDAP servera savienojuma pārbaude

Veic LDAP servera savienojuma pārbaudi, izmantojot parametru, kas iestatīts sadaļā **LDAP Server** > **Search Settings**.

1. Atveriet programmu Web Config un atlasiet cilni **Network** > **LDAP Server** > **Connection Test**.
2. Izvēlieties **Start**.

   Tiek sākta savienojuma pārbaude. Pēc pārbaudes tiks parādīta pārbaudes atskaite.

LDAP servera savienojuma testēšanas atsauces

Ziņojumi	Skaidrojums
Connection test was successful.	Šis ziņojums tiek parādīts tad, ja savienojuma izveide ar serveri ir veiksmīga.
Connection test failed. Check the settings.	Šis ziņojums tiek parādīts tālāk norādīto iemeslu dēļ: ❏ Nepareiza LDAP servera adrese vai porta numurs. ❏ Ir iestājusies noildze. ❏ Iespēja **Do Not Use** ir atlasīta kā **Use LDAP Server**. ❏ Ja iespēja **Kerberos Authentication** ir atlasīta kā **Authentication Method**, iestatījums **Realm (Domain)**, **KDC Address** un **Port Number (Kerberos)** nav pareizs.
Connection test failed. Check the date and time on your product or server.	Šis ziņojums tiek parādīts, ja savienojuma izveide nav izdevusies, jo nesakrīt skenera un LDAP servera laika iestatījumi.

Ziņojumi	Skaidrojums
Authentication failed. Check the settings.	Šis ziņojums tiek parādīts tālāk norādīto iemeslu dēļ: ❏ Laukā **User Name** un/vai **Password** nav ievadīta pareiza informācija. ❏ Ja iespēja **Kerberos Authentication** ir atlasīta kā **Authentication Method**, laiks un datums var netikt konfigurēts.
Cannot access the product until processing is complete.	Šis ziņojums tiek parādīts, ja skeneris ir aizņemts.

Programmatūras Document Capture Pro Server lietošana

Izmantojot Document Capture Pro Server, var noteikt kārtošanas metodi, saglabāšanas formātu un pārsūtīšanas mērķi skenēšanas rezultātam, kas iegūts, izmantojot skenera vadības paneli. Izmantojot skenera vadības paneli, var izsaukt un izpildīt iepriekš serverī reģistrētu uzdevumu.

Instalējiet to servera datorā.

Lai iegūtu plašāku informāciju par Document Capture Pro Server, sazinieties ar vietējo Epson biroju.

Servera režīma iestatīšana

Lai izmantotu programmu Document Capture Pro Server, veiciet turpmāk norādītos iestatījumus.

1. Atveriet programmu Web Config un atlasiet cilni **Scan** > **Document Capture Pro**.
2. Iestatījumam **Server Mode** atlasiet **Mode**.
3. Laukā Document Capture Pro Server ievadiet servera, kurā ir instalēta programma **Server Address** adresi.

   Ievadiet no 2 līdz 255 rakstzīmēm IPv4, IPv6, resursdatora nosaukuma vai FQDN formātā. FQDN formātā var izmantot burtciparu rakstzīmes ASCII (0x20–0x7E) kodējumā un „-”, izņemot adreses sākumu un beigas.
4. Noklikšķiniet uz **OK**.

   Tīkla savienojums tiek atjaunots, un pēc tam tiek iespējoti iestatījumi.

Funkcijas AirPrint iestatīšana

Atveriet Web Config, atlasiet cilni **Network**, pēc tam atlasiet **AirPrint Setup**.

Posms	Skaidrojums
Bonjour Service Name	Ievadiet Bonjour pakalpojuma nosaukumu, izmantojot ASCII teksta formātu (0x20–0x7E) un ne vairāk kā 41 rakstzīmi.
Bonjour Location	Ievadiet skenera atrašanās vietas aprakstu, izmantojot Unicode (UTF-8) teksta formātu un ne vairāk kā 127 baiti.

Posms	Skaidrojums
Wide-Area Bonjour	Iestatiet, vai tiks izmantots plaša apgabala Bonjour pakalpojums. Ja to izmantosit, skeneri jāreģistrē DNS serverī, lai skeneri varētu meklēt segmenta ietvaros.
Enable AirPrint	Bonjour pakalpojums un AirPrint (Skenēšanas pakalpojums) ir iespējoti.

Problēmas sagatavot tīkla skenēšanu

Problēmu risināšanas padomi

❏ Kļūdas ziņojuma pārbaude

Ja radusies problēma, vispirms pārbaudiet, vai skenera vadības panelī vai draivera ekrānā nav ziņojumu. Ja ir iestatīts paziņojuma e-pasts, norisinoties notikumiem, varat ātri uzzināt statusu.

❏ Sakaru statusa pārbaude

Pārbaudiet servera datora vai klienta datora sakaru statusu, izmantojot komandu, piemēram, ping un ipconfig.

❏ Savienojuma pārbaude

Lai pārbaudītu skenera un pasta servera savienojumu, veiciet savienojuma pārbaudi skenerī. Lai noskaidrotu sakaru statusu, pārbaudiet arī klienta datora savienojumu ar serveri.

❏ Iestatījumu inicializēšana

Ja iestatījumi un sakaru statuss neparāda problēmas, tās var atrisināt, atspējojot vai inicializējot skenera tīkla iestatījumus un atkal tos aktivizējot.

Nevar piekļūt Web Config

IP adrese nav piešķirta skenerim.

Risinājumi

Derīgu IP adresi neizdodas piešķirt skenerim. Konfigurējiet IP adresi, izmantojot skenera vadības paneli. Pašreizējo iestatījumu informāciju var pārbaudīt skenera vadības panelī.

Tīmekļa pārlūkprogramma neatbalsta SSL/TLS šifrēšanas pakāpi.

Risinājumi

SSL/TLS ir Encryption Strength. Varat atvērt Web Config, izmantojot tīmekļa pārlūkprogrammu, kas atbalsta lielapjoma šifrēšanu, kā norādīts tālāk. Pārbaudiet, vai izmantojat atbalstītu pārlūkprogrammu.

❏ 80 bitu: AES256/AES128/3DES

❏ 112 bitu: AES256/AES128/3DES

❏ 128 bitu: AES256/AES128

❏ 192 bitu: AES256

❏ 256 bitu: AES256

CA-signed Certificate ir beidzies derīguma termiņš.

Risinājumi

Ja radusies problēma ar sertifikāta derīguma termiņa datumu, izveidojot savienojumu ar Web Config, lietojot SSL/TLS sakarus (https), tiek parādīts ziņojums „Beidzies sertifikāta derīguma termiņš". Ja ziņojums tiek parādīts tieši pirms derīguma termiņa beigu datuma, pārliecinieties, ka skenera datums ir konfigurēts pareizi.

Sertifikāta un skenera kopējais nosaukums nesakrīt.

Risinājumi

Ja sertifikāta un skenera kopējais nosaukums nesakrīt, piekļūstot programmai Web Config ar SSL/TLS sakariem (https), parādās paziņojums „Neatbilstošs drošības sertifikāta nosaukums···". Tas notiek tāpēc, ka tālāk norādītās IP adreses nesakrīt.

❏ Skenera IP adrese, kas ievadīta kopējam nosaukumam, lai izveidotuSelf-signed Certificate vai CSR

❏ Tīmekļa pārlūkā ievadītā IP adrese, kad ir palaista programma Web Config

Self-signed Certificate gadījumā, atjauniniet sertifikātu.

Izvēloties CA-signed Certificate, vēlreiz iegūstiet skenera sertifikātu.

Tīmekļa pārlūkprogrammā nav iestatīts starpniekservera lokālās adreses iestatījums.

Risinājumi

Ja skeneris ir iestatīts izmantot starpniekserveri, konfigurējiet tīmekļa pārlūkprogrammu neizveidot savienojumu ar lokālo adresi, izmantojot starpniekserveri.

❏ Windows:

Atlasiet **Vadības panelis** > **Tīkls un internets** > **Interneta opcijas** > **Savienojumi** > **LAN iestatījumi** > **Starpniekserveris** un pēc tam konfigurējiet neizmantot starpniekserveri LAN (lokālām adresēm).

❏ Mac OS:

Atlasiet **Sistēmas preferences** > **Tīkls** > **Papildus** > **Starpniekserveri** un pēc tam reģistrējiet **Apiet starpnieka iestatījumus šiem viesotājiem un domēniem** lokālo adresi.

Piemērs:

192.168.1.*: Lokālā adrese 192.168.1.XXX, apakštīkla maska 255.255.255.0

192.168.*.*: Lokālā adrese 192.168.XXX.XXX, apakštīkla maska 255.255.0.0

Datora iestatījumos DHCP ir atspējots.

Risinājumi

Ja DHCP IP adreses iegūšanai datorā ir automātiski atspējots, jūs nevarat piekļūt Web Config. Iespējot DHCP.

Piemērs operētājsistēmā Windows 10:

Atveriet Vadības paneli un noklikšķiniet **Tīkls un internets** > **Tīkls un koplietošanas centrs** > **Mainīt adaptera iestatījumus**. Atveriet jūsu izmantotā savienojuma Rekvizītu ekrānu un atveriet **Interneta protokola 4. versijas (TCP/IPv4)** vai **Interneta protokola 6. versijas (TCP/IPv6)** rekvizītus. Pārbaudiet, vai **Iegūt IP adresi automātiski** ir atlasīts uz parādītā ekrāna.

Vadības paneļa displeja pielāgošana

Priekšiestat. reģistrēšana

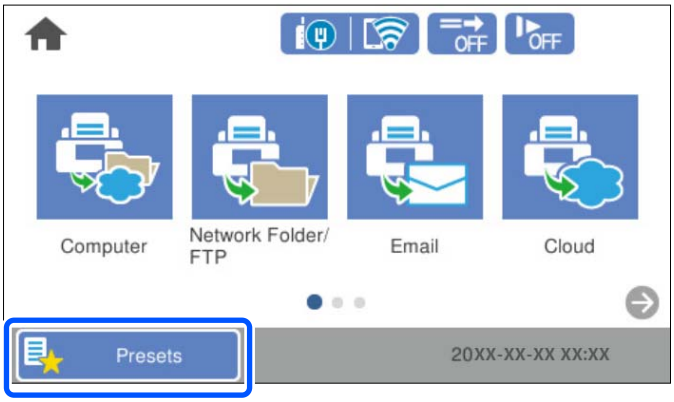
Varat reģistrēt bieži lietotos skenēšanas iestatījumus kā **Priekšiestat.**. Ir iespējams reģistrēt līdz 48 priekšietstatījumus.

Piezīme:

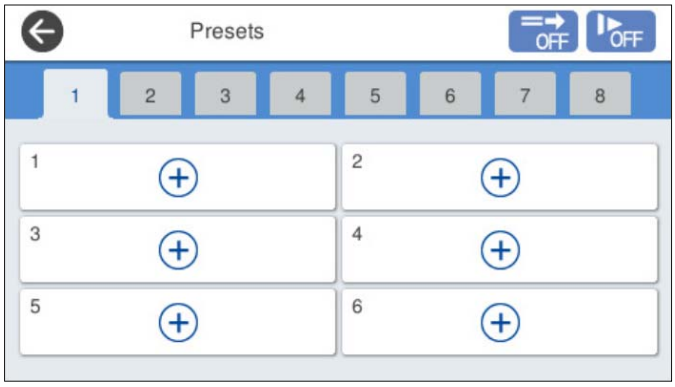
- *Varat reģistrēt esošos iestatījumus, skenēšanas iestatījumu sākuma ekrānā atlasot* ☆.
- ***Presets** varat reģistrēt arī Web Config.*

  *Atlasiet cilni **Scan** > **Presets**.*
- *Ja izvēlaties **Skenēt uz datoru** reģistrējoties, jūs varat reģistrēt uzdevumu, kas izveidots Document Capture Pro kā **Presets**. Tas ir pieejams tikai datoriem, kas pieslēgti tīklā. Reģistrējiet uzdevumu Document Capture Pro iepriekš.*
- *Ja autentifikācijas funkcija ir iespējota, tikai administrators var reģistrēt **Presets**.*

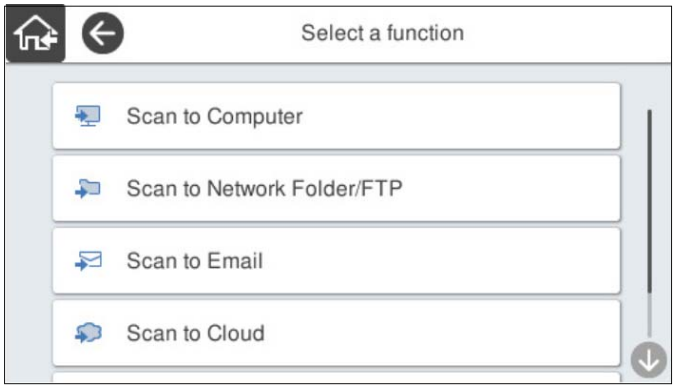
1. Skenera vadības paneļa sākuma ekrānā atlasiet **Priekšiestat.**.



2. Atlasiet ⊕.



3. Atlasiet vēlamo izvēlni, lai reģistrētu sākotnējo iestatījumu.



4. Iestatiet katru vienumu un pēc tam atlasiet ☆+.

Piezīme:
*Atlasot **Skenēt uz datoru**, atlasiet datoru, kurā ir instalēts Document Capture Pro, un atlasiet reģistrēto uzdevumu. Tas ir pieejams tikai datoriem, kas pieslēgti tīklā.*

5. Veiciet sākotnējos iestatījumus.
   - ❏ **Nosaukums**: Iestata nosaukumu.
   - ❏ **Iestatīt ikonu**: Iestata ikonas attēlu un krāsu.
   - ❏ **Iestatījums Ātrā sūtīšana**: sāk skenēšanu bez apstiprinājuma, kad izvēlēts šis sākotnējais iestatījums.

     Izmantojot Document Capture Pro Server, pat ja jūs iestatāt programmatūru, kas pirms skenēšanas apstiprina uzdevuma saturu, **Iestatījums Ātrā sūtīšana** skenera priekšiestatījumos ir prioritārs pār programmatūru.
   - ❏ **Saturs**: pārbauda skenēšanas iestatījumus.

6. Atlasiet **OK**.

Izvēlnes opcijas Priekšiestat.

Varat mainīt priekšiestatījumu iestatījumus, katrā priekšiestatījumā atlasot ›.

Mainīt nosaukums:

Maina priekšiestatījuma nosaukumu.

Mainīt ikonu:

Maina priekšiestatījuma ikonas attēlu un krāsu.

Iestatījums Ātrā sūtīšana:

Nekavējoties sāk skenēšanu bez apstiprinājuma, ja izvēlēts šis priekšiestatījums.

Mainīt pozīciju:

Maina priekšiestatījumu attēlošanas kārtību.

Dzēst:

Dzēš priekšiestatījumu.

Pievienot vai noņemt ikonu izvēlnē Sākums:

Pievieno vai dzēš priekšiestatījuma ikonu sākuma ekrānā.

Apstiprināt detalizētu informāc.:

Parāda priekšiestatījuma iestatījumus. Priekšiestatījumu var ielādēt, atlasot **Lietot šo iestatījumu**.

Vadības paneļa sākuma ekrāna rediģēšana

Varat pielāgot sākuma ekrānu, skenera vadības panelī atlasot **Iestatījumi** > **Sākumlapas rediģēšana**.

❏ Izkārtojums: maina izvēlnes ikonu attēlošanas metodi.

"Mainīt Izkārtojums sākuma ekrānā" 78. lpp.

❏ Pievienot ikonu: pievieno ikonas iestatītajiem **Priekšiestat.** vai atgriež ikonas, kuras pirms tām noņēmāt no ekrāna.

"Pievienot ikonu" 79. lpp.

❏ Noņemt ikonu: noņem ikonu no sākuma ekrāna.

"Noņemt ikonu" 80. lpp.

❏ Pārvietot ikonu: maina ikonu attēlošanas kārtību.

"Pārvietot ikonu" 81. lpp.

❏ Atjaunot noklus. ikonu attēlojumu: atjauno sākuma ekrāna displeja noklusējuma iestatījumus.

❏ Tapete: maina sākuma ekrāna fona tapetes krāsu.

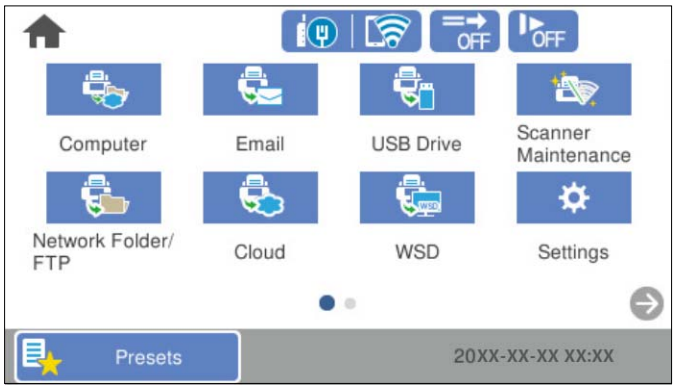
Mainīt Izkārtojums sākuma ekrānā

1. Skenera vadības panelī atlasiet **Iestatījumi** > **Sākumlapas rediģēšana** > **Izkārtojums**.

2. Atlasiet **Līnija** vai **Matrica**.

Līnija:

Matrica:



3. Atlasiet , lai atgrieztu un pārbaudītu sākuma ekrānu.

Pievienot ikonu

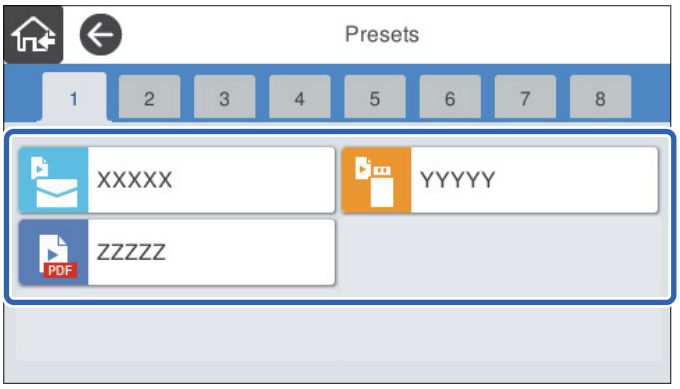
1. Skenera vadības panelī atlasiet **Iestatījumi** > **Sākumlapas rediģēšana** > **Pievienot ikonu**.

2. Atlasiet **Funkcija** vai **Priekšiestat.**.

❏ Funkcija: parāda sākuma ekrāna displeja noklusējuma iestatījumus.

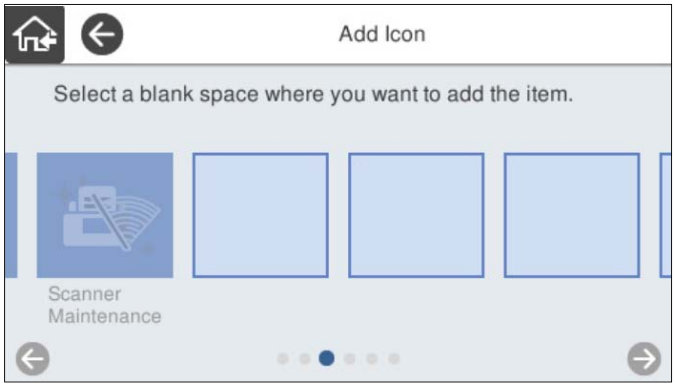
❏ Priekšiestat.: parāda reģistrētos sākotnējos iestatījumus.

3. Sākuma ekrānā atlasiet vienumu, ko izmantosit.



4. Atlasiet tukšo vietu, kurā vēlaties pievienot vienumu.

   Ja vēlaties pievienot vairākas ikonas, atkārtojiet 3. un 4. soli.

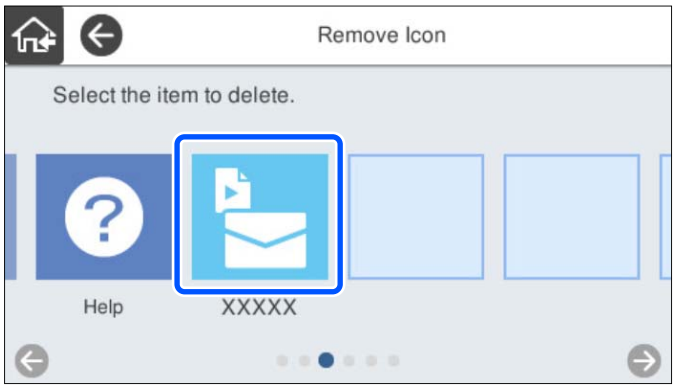


5. Atlasiet , lai atgrieztu un pārbaudītu sākuma ekrānu.

Noņemt ikonu

1. Skenera vadības panelī atlasiet **Iestatījumi** > **Sākumlapas rediģēšana** > **Noņemt ikonu**.

2. Atlasiet ikonu, kuru vēlaties noņemt.



3. Atlasiet **Jā**, lai pabeigtu procedūru.

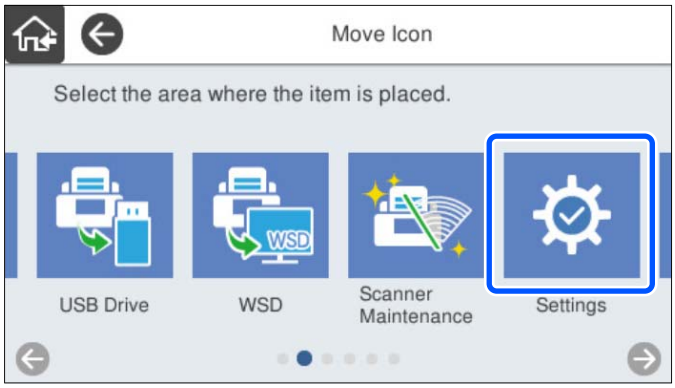
   Ja vēlaties noņemt vairākas ikonas, atkārtojiet 2 un 3 soli.

4. Atlasiet , lai atgrieztu un pārbaudītu sākuma ekrānu.

Pārvietot ikonu

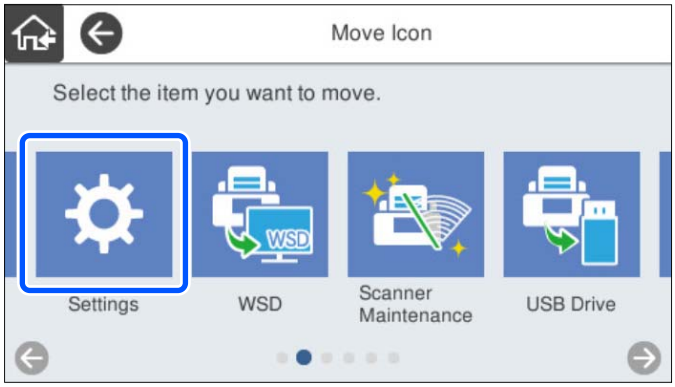
1. Skenera vadības panelī atlasiet **Iestatījumi** > **Sākumlapas rediģēšana** > **Pārvietot ikonu**.

2. Atlasiet ikonu, kuru vēlaties pārvietot.



3. Vēlreiz atlasiet mērķa rāmi.

   Ja mērķa rāmī ir iestatīta cita ikona, ikonas tiek aizvietotas.



4. Atlasiet , lai atgrieztu un pārbaudītu sākuma ekrānu.

Pamata drošības iestatījumi

Ierīces drošības funkciju vispārējs apraksts

Šajā sadaļā ir aprakstītas Epson ierīču drošības funkcijas.

Funkcijas nosaukums	Funkcijas veids	Kas jāiestata	Kas jānovērš
Administratora paroles iestatīšana	Bloķē sistēmas iestatījumus, piemēram, tīkla vai USB savienojuma iestatījumus.	Administrators iestata ierīces paroli. Iestatījumus var izveidot vai mainīt gan programmā Web Config, gan skenera vadības panelī.	Novērš neatļautu ierīcē saglabātās informācijas, piemēram, ID, paroles, tīkla iestatījumu utt., skatīšanu un mainīšanu. Papildus mazina arī dažādus drošības riskus, piemēram, tīkla vides vai drošības politikas informācijas noplūdi.
Ārējās saskarnes iestatīšana	Saskarnes, ko izmanto savienojumam ar ierīci, vadība.	Iespējo vai atspējo USB savienojumu ar datoru.	Datora USB savienojums: novērš nesankcionētu ierīces lietošanu, atļaujot skenēt tikai tīklā.

Saistītā informācija

➡ "Administratora paroles konfigurēšana" 84. lpp.
➡ "Ārējās saskarnes atspējošana" 90. lpp.

Administratora iestatījumi

Administratora paroles konfigurēšana

Iestatot administratora paroli, jūs varat neļaut lietotājiem mainīt sistēmas pārvaldības iestatījumus. Pirkšanās brīdī ir iestatītas noklusējuma vērtības. Mainiet tās pēc nepieciešamības.

Piezīme:
Tālāk sniegtas noklusējuma vērtības administratora informācijai.

❏ *Lietotājvārds (izmanto tikai Web Config): nav (tukšs)*

❏ *Parole: skenera sērijas numurs*

Lai iegūtu sērijas numuru, apskatiet etiķeti, kas uzlīmēta skenera aizmugurē.

Administratora paroli varat mainīt, izmantojot gan Web Config, gan skenera vadības paneli, gan Epson Device Admin. Ja izmantojat Epson Device Admin, skatiet Epson Device Admin pamācību vai palīdzības sadaļu.

Administratora paroles mainīšana, izmantojot Web Config

Mainiet administratora paroli sadaļā Web Config.

1. Atveriet programmu Web Config un atlasiet cilni **Product Security** > **Change Administrator Password**.

2. Ievadiet nepieciešamo informāciju **Current password**, **User Name**, **New Password** un **Confirm New Password**.

   Ievadiet vismaz vienu rakstzīmi jaunajai parolei.

   Piezīme:
   Tālāk sniegtas noklusējuma vērtības administratora informācijai.

   ❏ *Lietotājvārds: nav (tukšs)*

   ❏ *Parole: skenera sērijas numurs*

   Lai iegūtu sērijas numuru, apskatiet etiķeti, kas uzlīmēta skenera aizmugurē.

   > ***Svarīga informācija:***
   > *Pārliecinieties, ka atceraties iestatīto administratora paroli. Ja aizmirstat paroli, jūs nevarēsit to atiestatīt un jums būs jālūdz apkalpojošā personāla palīdzība.*

3. Atlasiet **OK**.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Administratora paroles mainīšana, izmantojot vadības paneli

Administratora paroli var mainīt, izmantojot skenera vadības paneli.

1. Skenera vadības panelī izvēlieties **Iestatījumi**.

2. Atlasiet **Sistēmas administrēšana** > **Administratora iestatījumi**.

3. Atlasiet **Admin. parole** > **Mainīt**.

4. Ievadiet pašreizējo paroli.

   Piezīme:
   Pirkuma brīdī (noklusējuma vērtība) administratora parole ir skenera sērijas numurs.

   Lai iegūtu sērijas numuru, apskatiet etiķeti, kas uzlīmēta skenera aizmugurē.

5. Ievadiet jauno paroli.

   Ievadiet vismaz vienu rakstzīmi.

   > ***Svarīga informācija:***
   > *Pārliecinieties, ka atceraties iestatīto administratora paroli. Ja aizmirstat paroli, jūs nevarēsit to atiestatīt un jums būs jālūdz apkalpojošā personāla palīdzība.*

6. Lai apstiprinātu, ievadiet jauno paroli.

Tiek parādīts ziņojums par pabeigšanu.

Bloķēšanas iestatījums izmantošana vadības panelim

Varat izmantot, Bloķēšanas iestatījums lai bloķētu vadības paneli, novēršot lietotāju veiktu ar sistēmas iestatījumiem saistītu vienumu maiņu.

Piezīme:
Ja skenerī iespējosiet Authentication Settings, vadības panelim arī tiks iespējots Bloķēšanas iestatījums. Vadības paneli nevar atbloķēt, kad Authentication Settings ir iespējoti.

Pat, ja atspējosit Authentication Settings, Bloķēšanas iestatījums paliek iespējoti. Ja vēlaties tos atspējot, šos iestatījumus varat veikt no vadības paneļa vai Web Config.

Bloķēšanas iestatījums iestatīšana, izmantojot vadības paneli

1. Ja vēlaties atcelt **Bloķēšanas iestatījums** pēc tam, kad tas iespējots, tad sākuma ekrāna augšējā labajā stūrī pieskarieties  un piesakieties kā administrators.

    nav redzams, kad **Bloķēšanas iestatījums** ir atspējots. Ja vēlaties iespējot šo iestatījumu, dodieties uz nākamo soli.

2. Atlasiet **Iestatījumi**.

3. Atlasiet **Sistēmas administrēšana** > **Administratora iestatījumi**.

4. Atlasiet **Iesl** vai **Izsl** kā **Bloķēšanas iestatījums**.

Bloķēšanas iestatījums iestatīšana, izmantojot Web Config

1. Atlasiet cilni **Device Management** > **Control Panel**.

2. Atlasiet **ON** vai **OFF** kā iestatījumu sadaļā **Panel Lock**.

3. Noklikšķiniet uz **OK**.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Bloķēšanas iestatījums vienumus izvēlnē Iestatījumi

Šis ir vienumu saraksts, ko vadības paneļa izvēlnē **Iestatījumi** bloķē Bloķēšanas iestatījums.

✓: jābloķē.

- : netiek bloķēts.

Izvēlne Iestatījumi	Bloķēšanas iestatījums
Pamatiestatījumi	-

Izvēlne Iestatījumi		Bloķēšanas iestatījums
	LCD spilgtums	-
	Skaņas	-
	Iemidzināšanas taimeris	✓
	Izslēgšanās taimeris	✓
	Datuma/laika iestatījumi	✓
	Valoda/Language	✓/-*
	Tastatūra (Šī funkcija var nebūt pieejama atkarībā no reģiona.)	-
	Darbības taimauts	✓
	Datora pievienošana ar USB	✓
	Tieša ieslēgšana	✓
Skenera iestatījumi		-
	Lēni	-
	Dubultās padeves apturēšanas laiks	✓
	DFDS funkcija	-
	Papīra aizsardzība	✓
	Stikla netīrumu noteikšana	✓
	Dubultas ievades not. ar ultrask.	✓
	Automātiskās padeves režīms taimauts	✓
	Apstiprināt saņēmēju	✓
Sākumlapas rediģēšana		✓
	Izkārtojums	✓
	Pievienot ikonu	✓
	Noņemt ikonu	✓
	Pārvietot ikonu	✓
	Atjaunot noklus. ikonu attēlojumu	✓
	Tapete	✓
Lietotāja iestatījumi		✓

Izvēlne Iestatījumi		Bloķēšanas iestatījums
	Tīkla mape/FTP	✓
	E-pasts	✓
	Mākonis	✓
	USB disks	✓
Tīkla iestatījumi		✓
	Wi-Fi iestatīšana	✓
	Vadu LAN iestatīšana	✓
	Tīkla statuss	✓
	Papildu	✓
Tīkla pakalpojumu iestatījumi		✓
	Epson Connect pakalpojumi	✓
Document Capture Pro		-
	Mainīt iestatījumus	✓
Kontaktpersonu pārvaldnieks		-
	Reģistrēt/Dzēst	✓/-*
	Bieži izmantoti	-
	Aplūkot opcijas	-
	Meklēšanas opcijas	-
Sistēmas administrēšana		✓
	Kontaktpersonu pārvaldnieks	✓
	Administratora iestatījumi	✓
	Ierobežojumi	✓
	Paroles šifrēšana	✓
	Klientu izpēte	✓
	WSD iestatījumi	✓
	Atjaunot noklusējuma iestatījumus	✓
	Aparātprogramatūras atjauninājums	✓
Ierīces informācija		-

Izvēlne Iestatījumi			Bloķēšanas iestatījums
	Sērijas numurs		-
	Pašreizējā versija		-
	Kopējais ieskenēto lapu skaits		-
	Vienpusēju skenējumu skaits		-
	Divpusēju skenējumu skaits		-
	Nesējloksnes skenējumu skaits		-
	Skenējumu skaits pēc apkopes ruļļa nomaiņas		-
	Skenējumu skaits pēc parastās tīrīšanas		-
	Atiestatiet skenējumu skaitu		✓
Skenera apkope			-
	Ruļļu tīrīšana		-
	Apkopes ruļļa nomaiņa		-
		Atiestatiet skenējumu skaitu	✓
		Nomaiņa	-
	Parasta tīrīšana		-
		Atiestatiet skenējumu skaitu	✓
		Tīrīšana	-
	Stikla tīrīšana		-
Veltniša nomaiņas brīdinājuma iestatījums			✓
	Brīdin. skaita iestat.		✓
Parastās tīrīšanas brīdinājuma iestatījumi			✓
	Brīdinājuma iestatījums		✓
	Brīdin. skaita iestat.		✓

* Var iestatīt, vai atļaut vai neatļaut izmaiņas **Sistēmas administrēšana** > **Ierobežojumi**.

Pieteikšanās kā administratoram, izmantojot vadības paneli

Varat izmantot turpmāk norādītās metodes, lai pieteiktos kā administrators, izmantojot skenera vadības paneli.

1. Ekrāna augšējā labajā pusē pieskarieties pie  .
   - ❏ Kad iespējoti Authentication Settings ekrānā **Laipni lūdzam!** ir redzama ikona (autentifikācijas gaidstāves ekrāns).
   - ❏ Kad atspējoti Authentication Settings, sākuma ekrānā redzama ikona.

2. Pieskarieties **Jā**, kad redzams apstiprinājuma ekrāns.

3. Ievadiet administratora paroli.

   Parādās paziņojums, ka pieteikšanās ir pabeigta, un pēc tam vadības panelī redzams sākuma ekrāns.

Lai atteiktos, ekrāna augšējā labajā pusē pieskarieties pie  .

Ārējās saskarnes atspējošana

Saskarni, ko izmanto ierīces savienošanai ar skeneri, var atspējot. Lai ierobežotu skenēšanu bez tīkla izmantošanas, izvēlieties ierobežojošos iestatījumus.

Piezīme:
Ierobežojošos iestatījumus var veikt arī skenera vadības panelī.

Datora pievienošana ar USB: ***Iestatījumi*** > ***Pamatiestatījumi*** > ***Datora pievienošana ar USB***

1. Atveriet programmu Web Config un atlasiet cilni **Product Security** > **External Interface**.

2. Atlasiet **Disable** pie funkcijām, ko vēlaties iestatīt.

   Atlasiet **Enable**, ja vēlaties atcelt kontroli.

   Datora pievienošana ar USB

   Pastāv iespēja aizliegt USB savienojuma lietošanu no datora. Ja vēlaties to aizliegt, izvēlieties **Disable**.

3. Noklikšķiniet uz **OK**.

4. Pārbaudiet, vai var lietot atspējoto portu.

   Datora pievienošana ar USB

   Ja datorā ir instalēts draiveris

   Savienojiet skeneri ar datoru, izmantojot USB kabeli, un pēc tam pārliecinieties, vai skeneris neveic drukāšanu.

   Ja datorā nav instalēts draiveris

   Windows:

   Atveriet ierīču pārvaldnieku un atstājiet to atvērtu, savienojiet skeneri ar datoru, izmantojot USB kabeli, un pēc tam pārliecinieties, vai ierīču pārvaldnieka displeja saturs paliek nemainīgs.

   Mac OS:

   Savienojiet skeneri ar datoru, izmantojot USB kabeli, un pēc tam pārliecinieties, ka nevarat pievienot skeneri no **Printeri un skeneri**.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Attāla skenera kontrole

Attāla skenera informācijas pārbaudīšana

Ekrānā **Status** programmā Web Config var pārbaudīt tālāk norādīto izmantotā skenera informāciju.

❏ Product Status

Pārbaudiet statusu, mākoņpakalpojumu, produkta numuru, MAC adresi u. c.

❏ Network Status

Pārbaudīt tīkla savienojuma statusu, IP adresi, DNS serveri utt.

❏ Usage Status

Pārbaudiet pirmo dienu, kad sākta skenēšana, skenēšanas reižu skaitu utt.

❏ Hardware Status

Pārbaudiet katra skenera funkcijas statusu.

❏ Panel Snapshot

Parāda ekrānšāviņu, kas redzams skenera vadības panelī.

E-pasta ziņojumu saņemšana notikumu gadījumā

Par e-pasta paziņojumiem

Tā ir paziņojumu funkcija, kas, norisinoties tādiem notikumiem kā skenēšanas pārtraukšana un skenera kļūda, nosūta e-pasta ziņu uz norādīto adresi.

Varat reģistrēt līdz pieciem mērķiem un izveidot katra mērķa paziņojumu iestatījumus.

Lai izmantotu šo funkciju, pirms paziņojumu iestatīšanas jāiestata pasta serveris.

Saistītā informācija

➡ "Pasta servera konfigurēšana" 41. lpp.

E-pasta paziņojumu konfigurēšana

Konfigurējiet e-pasta paziņojumu, izmantojot programmu Web Config.

1. Atveriet programmu Web Config un atlasiet cilni **Device Management** > **Email Notification**.
2. Iestatiet e-pasta paziņojuma tēmu.

   Divās izvelkamajās izvēlnēs atlasiet par tēmu parādīto saturu.

   ❏ Atlasītais saturs tiek rādīts blakus laukam **Subject**.

   ❏ To pašu saturu nevar iestatīt gan kreisajā, gan labajā pusē.

   ❏ Kad lauka **Location** rakstzīmju skaits pārsniedz 32 baitus, 32 baitus pārsniedzošās rakstzīmes netiek iekļautas.

3. Ievadiet e-pasta adresi, uz kuru nosūtīt paziņojuma e-pastu.

   Izmantojiet rakstzīmes A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @ un ievadiet no 1 līdz 255 rakstzīmēm.

4. Izvēlieties e-pasta paziņojumu valodu.

5. Atlasiet izvēles rūtiņu blakus notikumam, par kuru vēlaties saņemt paziņojumu.

   Sadaļas **Notification Settings** numurs ir saistīts ar sadaļas **Email Address Settings** mērķa numuru.

   Piemērs:

   Ja vēlaties, lai paziņojums tiktu nosūtīts uz e-pasta adresi, kas iestatīta numuram 1 sadaļā **Email Address Settings**, kad mainīta administratora parole, atlasiet izvēles rūtiņas kolonnu **1** rindā **Administrator password changed**.

6. Noklikšķiniet uz **OK**.

   Pārliecinieties, vai e-pasta ziņojums tiek nosūtīts, izraisot notikumu.

   Piemērs: ir mainīta administratora parole.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Vienumi e-pasta paziņojumiem

Posms	Iestatījumi un skaidrojums
Administrator password changed	Paziņojums, kad ir mainīta administratora parole.
Scanner error	Paziņojums, kad radusies skenera kļūda.
Wi-Fi kļūme	Paziņojums, kad radusies bezvadu lokālā tīkla saskarnes kļūda.

Problēmu risināšana

Aizmirsta administratora parole

Nepieciešama apkopes personāla palīdzība. Sazinieties ar vietējo izplatītāju.

Piezīme:
Tālāk sniegtas Web Config sākotnējās vērtības administratoram.

❏ *Lietotājvārds: nav (tukšs)*

❏ *Parole: skenera sērijas numurs*

Lai iegūtu sērijas numuru, apskatiet etiķeti, kas uzlīmēta skenera aizmugurē. Ja atjaunojat administratora paroles noklusējuma iestatījumus, tā tiek atiestatīta ar sākotnējām vērtībām.

Tīkla drošības iestatījumi

Drošības iestatījumi un bīstamības novēršana

Kad skeneris ir pievienots tīklam, varat tam piekļūt attālināti. Turklāt skeneri var koplietot vairāki cilvēki, kas palīdz uzlabot darba efektivitāti un padara to ērtāku. Tomēr pieaug dažādi riski, piemēram, neatļauta piekļuve, lietošana un manipulācijas ar datiem. Ja izmantojat skeneri vidē ar piekļuvi internetam, risks ir vēl lielāks.

Skeneris kuri nav aizsargāti pret piekļuvi no ārpuses, iespējama nesankcionēta skenerī saglabāto kontaktu nolasīšana, izmantojot internetu.

Lai novērstu šo risku, Epson skeneri ir aprīkoti ar dažādām drošības tehnoloģijām.

Veiciet skenerī nepieciešamos iestatījumus atbilstoši klienta informācijas vides apstākļiem.

Nosaukums	Funkcijas veids	Kas jāiestata	Kas jānovērš
Protokola pārvaldība	Kontrolē protokolus un pakalpojumus, ko izmanto sakariem starp skeneriem un datoriem, iespējo un atspējo dažādas funkcijas.	Protokols vai pakalpojums, kuru izmanto atsevišķu funkciju atļaušanai vai aizliegšanai.	Netīšu drošības risku mazināšana, aizliedzot lietotājiem nevajadzīgu funkciju izmantošanu.
SSL/TLS sakaru sistēma	Piekļūstot Epson serverim internetā no skenera, sakaru saturs tiek šifrēts, izmantojot SSL/TLS protokolu — piemēram, ar programmas Epson Connect palīdzību veidojot savienojumu ar datoru tīmekļa pārlūkprogrammā un atjauninot aparātprogrammatūru.	Iegūstiet sertificēšanas iestādes parakstītu sertifikātu un tad importējiet to skenerī.	Skenera identifikācija, izmantojot CA parakstītus sertifikātus, novērš uzdošanos par citu personu un neatļautu piekļuvi. Turklāt tiek aizsargāts SSL/TLS sakaru saturs un novērsta skenējamā satura un iestatījumu informācijas noplūde.
IPsec/IP filtrēšana	Varat iestatījumos atļaut no noteikta klienta saņemtu vai noteikta veida datu atdalīšanu. Tā kā IPsec aizsargā datus pa IP pakešu vienībām (šifrēšana un autentificēšana), varat droši veidot sakarus, izmantojot nedrošu protokolu.	Izveidojiet pamata politiku un individuālu politiku, lai iestatītu klientu vai datu veidu, kas var piekļūt skenerim.	Nodrošiniet aizsardzību pret nesankcionētu piekļuvi, manipulācijām ar datiem, kas tiek pārsūtīti uz skeneri, un to pārtveršanu.
IEEE 802.1X	Ļauj tīklam pievienoties tikai autentificētiem lietotājiem. Atļauj tikai pilnvarotiem lietotājiem izmantot skeneri.	Autentificēšanas iestatījumi RADIUS serverī (autentificēšanas serverī).	Aizsardzība pret nesankcionētu piekļuvi un skenera izmantošanu.

Saistītā informācija

➡ "Vadība, izmantojot protokolus" 95. lpp.

➡ "SSL/TLS sakari ar skeneri" 103. lpp.

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 105. lpp.

➡ "Skenera pievienošana IEEE802.1X tīklam" 115. lpp.

Drošības funkciju iestatījumi

Iestatot IPsec/IP filtrēšanu vai IEEE 802.1X, lai sniegtu iestatījumu informāciju iesakām piekļūt Web Config, izmantojot SSL/TLS, lai mazinātu drošības riskus, piemēram, sagrozīšanu vai pārtveršanu.

Pirms IPsec/IP filtrēšanas vai IEEE 802.1X iestatīšanas, pārliecinieties, ka iestatāt administratora paroli.

Vadība, izmantojot protokolus

Skenēšanai var izmantot dažādus ceļus un protokolus. Tīkla skenēšanas funkciju var izmantot arī no nenoteikta skaita tīklam pieslēgtiem datoriem.

Netīšus drošības riskus var samazināt, ierobežojot skenēšanu no noteiktiem ceļiem vai kontrolējot pieejamās funkcijas.

Protokolu vadība

Konfigurē skenera atbalstītos protokola iestatījumus.

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security** tab > **Protocol**.
2. Konfigurējiet katru vienumu.
3. Noklikšķiniet uz **Next**.
4. Noklikšķiniet uz **OK**.

   Skenerim tiek piemēroti iestatījumi.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Protokoli, kurus var iespējot vai atspējot

Protokols	Apraksts
Bonjour Settings	Var norādīt, vai lietot Bonjour. Bonjour lieto, lai meklētu ierīces, skenētu u.t.t.
SLP Settings	Var iespējot vai atspējot SLP funkciju. SLP funkciju lieto, lai veiktu pašpiegādes skenēšanu un meklētu tīklu programmatūras elementā EpsonNet Config.
WSD Settings	Var iespējot vai atspējot WSD funkciju. Iespējojot šo funkciju, var pievienot WSD ierīces un skenēt no WSD porta.
LLTD Settings	Var iespējot vai atspējot LLTD funkciju. Iespējojot šo funkciju, tas tiek parādīts Windows tīkla kartē.
LLMNR Settings	Var iespējot vai atspējot LLMNR funkciju. Iespējojot šo funkciju, var lietot nosaukumu atpazīšanu bez NetBIOS pat tad, ja nevar lietot DNS.
SNMPv1/v2c Settings	Var norādīt, vai iespējot SNMPv1/v2c. To izmanto ierīču iestatīšanai, pārraudzībai u.t.t.

Protokols	Apraksts
SNMPv3 Settings	Var norādīt, vai iespējot SNMPv3. To izmanto šifrētu ierīču iestatīšanai, pārraudzībai utt.

Protokolu iestatīšanas vienumi

Bonjour Settings

Posms	Vērtības iestatīšana un apraksts
Use Bonjour	Atlasiet šo iespēju, lai meklētu vai lietotu ierīces, izmantojot Bonjour.
Bonjour Name	Tiek parādīts Bonjour nosaukums.
Bonjour Service Name	Tiek parādīts Bonjour pakalpojuma nosaukums.
Location	Tiek parādīts Bonjour vietas nosaukums.
Wide-Area Bonjour	Iestatiet, vai izmantot Wide-Area Bonjour.

SLP Settings

Posms	Vērtības iestatīšana un apraksts
Enable SLP	Atlasiet šo iespēju, lai iespējotu SLP funkciju. To lieto, piemēram, tīkla meklēšanai programmā EpsonNet Config.

WSD Settings

Posms	Vērtības iestatīšana un apraksts
Enable WSD	Atlasiet šo iespēju, lai iespējotu ierīču pievienošanu, izmantojot WSD, un skenētu no WSD porta.
Scanning Timeout (sec)	Ievadiet sakaru taimauta vērtību WSD skenēšanai no 3 līdz 3600 sekundēm.
Device Name	Tiek parādīts WSD ierīces nosaukums.
Location	Tiek parādīts WSD vietas nosaukums.

LLTD Settings

Posms	Vērtības iestatīšana un apraksts
Enable LLTD	Atlasiet šo iespēju, lai iespējotu LLTD. Skeneris tiek parādīts Windows tīkla mapē.
Device Name	Tiek parādīts LLTD ierīces nosaukums.

LLMNR Settings

Posms	Vērtības iestatīšana un apraksts
Enable LLMNR	Atlasiet šo iespēju, lai iespējotu LLMNR. Var lietot nosaukumu atpazīšanu bez NetBIOS pat tad, ja nevar lietot DNS.

SNMPv1/v2c Settings

Posms	Vērtības iestatīšana un apraksts
Enable SNMPv1/v2c	Atlasiet, lai iespējotu SNMPv1/v2c.
Access Authority	Iestatiet piekļuves pilnvaras, kad ir iespējots SNMPv1/v2c. Atlasiet **Read Only** vai **Read/Write**.
Community Name (Read Only)	Ievadiet no 0 līdz 32 ASCII (0x20–0x7E) rakstzīmēm.
Community Name (Read/Write)	Ievadiet no 0 līdz 32 ASCII (0x20–0x7E) rakstzīmēm.

SNMPv3 Settings

Posms		Vērtības iestatīšana un apraksts
Enable SNMPv3		Atzīmējot izvēles rūtiņu, tiek iespējots SNMPv3.
User Name		Ievadiet no 1 līdz 32 vienbaita rakstzīmēm.
Authentication Settings		
	Algorithm	Atlasiet SNMPv3 autentificēšanas algoritmu.
	Password	Atlasiet SNMPv3 autentificēšanas paroli. Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E). Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
	Confirm Password	Lai apstiprinātu, ievadiet konfigurēto paroli.
Encryption Settings		
	Algorithm	Atlasiet SNMPv3 šifrēšanas algoritmu.
	Password	Atlasiet SNMPv3 šifrēšanas paroli. Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E). Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
	Confirm Password	Lai apstiprinātu, ievadiet konfigurēto paroli.
Context Name		Ievadiet 32 unikoda (UTF-8) rakstzīmes vai mazāku rakstzīmju skaitu. Ja nevēlaties to darīt, atstājiet šo lauku tukšu. Rakstzīmju skaits, ko var ievadīt, ir atkarīgs no valodas.

Ciparsertifikāta lietošana

Par ciparsertifikātiem

❏ CA-signed Certificate

Šo sertifikātu parakstījusi CA (Certificate Authority — sertificēšanas iestāde). To var iegūt un iesniegt sertificēšanas iestādē. Šis sertifikāts apstiprina skenera eksistenci un tiek izmantots SSL/TLS sakariem, lai jūs varētu garantēt datu sakaru drošību.

Lietojot sertifikātu SSL/TLS sakariem, tas tiek izmantots kā servera sertifikāts.

Ja ir iestatīta IPsec/IP filtrēšana vai IEEE 802.1X sakari, tas tiek izmantots kā klienta sertifikāts.

❏ CA sertifikāts

Šis sertifikāts ir CA-signed Certificate ķēdē — to dēvē arī par sertificēšanas starpniekiestādes sertifikātu. Tīmekļa pārlūks to izmanto, lai validētu skenera sertifikāta ceļu, piekļūstot otras puses serverim vai programmai Web Config.

CA sertifikātam iestatiet, kad validēt servera sertifikāta ceļu, piekļūstot no skenera. Skenerim iestatiet CA-signed Certificate ceļa apstiprināšanu SSL/TLS savienojuma gadījumā.

Skenera CA sertifikātu varat iegūt no sertificēšanas iestādes, kas izsniegusi attiecīgo CA sertifikātu.

Varat iegūt arī otras puses servera validēšanai izmantoto CA sertifikātu no sertificēšanas iestādes, kas izsniegusi otra servera CA-signed Certificate.

❏ Self-signed Certificate

Šis ir sertifikāts, kuru paraksta un izsniedz pats skeneris. To dēvē arī par saknes sertifikātu. Tā kā izdevējs sertificē pats sevi, šis sertifikāts nav uzticams un nevar novērst uzdošanos par kādu citu.

Izmantojiet to, nosakot drošības iestatījumus un veidojot vienkāršus SSL/TLS sakarus bez CA-signed Certificate.

Ja izmantojat šo sertifikātu SSL/TLS sakariem, tīmekļa pārlūkprogrammā var parādīties drošības brīdinājums, jo sertifikāts nav reģistrēts tīmekļa pārlūkprogrammā. Self-signed Certificate var izmantot tikai SSL/TLS sakariem.

Saistītā informācija

➡ "CA-signed Certificate konfigurēšana" 98. lpp.

➡ "Pašparakstīta sertifikāta atjaunināšana" 102. lpp.

➡ "CA Certificate konfigurēšana" 102. lpp.

CA-signed Certificate konfigurēšana

CA parakstīta sertifikāta iegūšana

Lai iegūtu CA parakstītu sertifikātu, izveidojiet sertifikāta parakstīšanas pieprasījumu (CSR — Certificate Signing Request) un iesniedziet to sertificēšanas iestādē. CSR var izveidot, izmantojot lietojumprogrammu Web Config un datoru.

Lai izveidotu CSR un iegūtu CA parakstītu sertifikātu, izmantojot Web Config, veiciet turpmāk norādītās darbības. CSR izveidei izmantojot Web Config, sertifikāta formāts ir PEM/DER.

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security**. Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.

   Lai ko jūs izvēlētos, jūs varat iegūt to pašu sertifikātu un izmantot to vienoti.

2. Sadaļā **Generate** noklikšķiniet uz **CSR**.

   Tiek atvērta CSR izveides lapa.

3. Ievadiet vērtību katram vienumam.

   Piezīme:
   Pieejamais atslēgas garums un saīsinājumi atšķiras atkarībā no sertifikācijas iestādes. Izveidojiet pieprasījumu atbilstīgi katras sertificēšanas iestādes noteikumiem.

4. Noklikšķiniet uz **OK**.

   Tiek parādīts ziņojums par pabeigšanu.

5. Atlasiet cilni **Network Security**. Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.

6. Lai lejupielādētu CSR datorā, noklikšķiniet uz sertificēšanas iestādes attiecīgā formāta **CSR** sertifikāta lejupielādes pogas.

   > ***Svarīga informācija:***
   > *Neģenerējiet CSR no jauna. Ja tā izdarāt, iespējams, nevarēs importēt izsniegtu CA-signed Certificate.*

7. Nosūtiet CSR sertificēšanas iestādei un iegūstiet CA-signed Certificate.

   Ievērojiet katras sertificēšanas iestādes nosūtīšanas un formas noteikumus.

8. Saglabājiet izsniegto CA-signed Certificate datorā, kas pievienots skenerim.

   Kad sertifikāts tiek saglabāts galamērķī, CA-signed Certificate iegūšana ir pabeigta.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

CSR vienumu iestatīšana

Posms	Iestatījumi un skaidrojums
Key Length	Atlasiet CSR atslēgas garumu.

Posms	Iestatījumi un skaidrojums
Common Name	Var ievadīt no 1 līdz 128 rakstzīmēm. Ja tā ir IP adrese, tai jābūt statiskai IP adresi. Jūs varat ievadīt 1–5 IPv4 adreses, IPv6 adreses, resursdatoru nosaukumus, FQDN, atdalot tos ar komatiem. Pirmais elements tiek saglabāts pie kopējā nosaukuma, bet citi elementi tiek saglabāti sertifikāta tēmas aizstājvārda laukā. Piemērs: Skenera IP adrese: 192.0.2.123, skenera nosaukums: EPSONA1B2C3 Common Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organization/ Organizational Unit/ Locality/ State/Province	Ir iespējams ievadīt no 0 līdz 64 ASCII formāta rakstzīmēm (0x20–0x7E). Atšķiramos nosaukumus var atdalīt ar komatiem.
Country	Ievadiet valsts divciparu kodu atbilstīgi standarta ISO-3166 noteikumiem.
Sender's Email Address	Sūtītāja e-pasta adresi varat ievadīt pasta servera iestatījumos. Ievadiet to pašu e-pasta adresi kā **Sender's Email Address** cilnē **Network** > **Email Server** > **Basic**.

CA parakstīta sertifikāta importēšana

Importējiet iegūto CA-signed Certificate skenerī.

Svarīga informācija:

- ❏ *Pārliecinieties, vai skenera datums un laiks ir iestatīts pareizi. Sertifikāts, iespējams, nav derīgs.*
- ❏ *Ja sertifikāts ir iegūts, izmantojot lietojumprogrammā Web Config izveidotu CSR, sertifikātu var importēt vienu reizi.*

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security**. Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.

2. Noklikšķiniet uz **Import**

   Tiek atvērta sertifikāta importēšanas lapa.

3. Ievadiet vērtību katram vienumam. Pārbaudot sertifikāta ceļu tīmekļa pārlūkprogrammai, kas piekļūst skenerim, iestatiet **CA Certificate 1** un **CA Certificate 2**.

   Atkarībā no CSR izveides vietas un sertifikāta faila formāta nepieciešamie iestatījumi var atšķirties. Ievadiet nepieciešamās vienumu vērtības, ievērojot turpmāk sniegtos norādījumus.

   - ❏ PEM/DER formāta sertifikāts, kas iegūts, izmantojot Web Config
     - ❏ **Private Key**: Nekonfigurējiet, jo skenerī ir privāta atslēga.
     - ❏ **Password**: nekonfigurējiet.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: Izvēles
   - ❏ PEM/DER formāta sertifikāts, kas iegūts no datora
     - ❏ **Private Key**: Jāiestata.
     - ❏ **Password**: nekonfigurējiet.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: Izvēles

❏ PKCS#12 formāta sertifikāts, kas iegūts no datora

❏ **Private Key**: nekonfigurējiet.

❏ **Password**: Izvēles

❏ **CA Certificate 1/CA Certificate 2**: Nekonfigurējiet.

4. Noklikšķiniet uz **OK**.

Tiek parādīts ziņojums par pabeigšanu.

Piezīme:
*Lai pārbaudītu sertifikāta informāciju, noklikšķiniet uz **Confirm**.*

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

CA parakstīta sertifikāta importēšanas iestatījumu vienumi

Vienumi	Iestatījumi un skaidrojums
Server Certificate vai Client Certificate	Atlasiet sertifikāta formātu. SSL/TLS savienojumam tiek rādīts Server Certificate. IPsec/IP Filtering vai IEEE 802.1X tiek rādīts Client Certificate.
Private Key	Ja iegūstat PEM/DER formāta sertifikātu, izmantojot CSR, kas izveidots datorā, norādiet privāto atslēgas failu, kurš atbilst sertifikātam.
Password	Ja faila formāts ir **Certificate with Private Key (PKCS#12)**, ievadiet paroli, kas šifrē privāto paroli, kas tika iestatīta, iegūstot sertifikātu.
CA Certificate 1	Ja sertifikāta formāts ir **Certificate (PEM/DER)**, importējiet sertificēšanas iestādes, kas izdod CA-signed Certificate, ko izmanto kā servera sertifikātu, sertifikātu. Ja nepieciešams, norādiet failu.
CA Certificate 2	Ja sertifikāta formāts ir **Certificate (PEM/DER)**, importējiet sertificēšanas iestādes, kas izdod CA Certificate 1, sertifikātu. Ja nepieciešams, norādiet failu.

CA parakstīta sertifikāta dzēšana

Importētu sertifikātu var dzēst, kad beidzies tā derīguma termiņš vai kad šifrēts savienojums vairs nav nepieciešams.

Svarīga informācija:
Ja sertifikāts ir iegūts, izmantojot lietojumprogrammā Web Config izveidotu CSR, dzēstu sertifikātu nevar importēt vēlreiz.Šādā gadījumā izveidojiet CSR un iegūstiet sertifikātu vēlreiz.

1. Atveriet programmu „Web Config” un tad atlasiet cilni **Network Security**.Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.

2. Noklikšķiniet uz **Delete**.

3. Apstipriniet, ka vēlaties dzēst sertifikātu, kas parādīts ziņojumā.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Pašparakstīta sertifikāta atjaunināšana

Tā kā Self-signed Certificate izsniedz skeneris, to var atjaunināt, kad beidzas tā derīguma termiņš vai ja aprakstītais saturs izmainās.

1. Piekļūstiet Web Config un atlasiet **Network Security** tab > **SSL/TLS** > **Certificate**.
2. Noklikšķiniet uz **Update**.
3. Ievadiet **Common Name**.

   Varat ievadīt līdz 5 IPv4 adresēm, IPv6 adresēm, resursdatora nosaukumiem, FQDN, kuru garums ir no 1 līdz 128 rakstzīmēm un kas ir atdalīti ar komatiem. Pirmais parametrs tiek saglabāts kopējā nosaukumā un pārējie tiek saglabāti sertifikāta temata aizstājvārda laukā.

   Piemērs:

   Skenera IP adrese: 192.0.2.123, skenera nosaukums: EPSONA1B2C3

   Kopējais nosaukums: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Norādiet sertifikāta derīguma termiņu.
5. Noklikšķiniet uz **Next**.

   Tiek parādīts apstiprinājuma ziņojums.
6. Noklikšķiniet uz **OK**.

   Skeneris ir atjaunināts.

Piezīme:
*Sertifikāta informāciju varat pārbaudīt, dodoties uz cilni **Network Security** > **SSL/TLS** > **Certificate** > **Self-signed Certificate** un noklikšķinot **Confirm**.*

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

CA Certificate konfigurēšana

Iestatot CA Certificate, varat validēt CA sertifikāta ceļu serverim, kuram piekļūst skeneris. Tā var novērst uzdošanos par citu personu.

CA Certificate var iegūt no sertificēšanas iestādes, kas izsniegusi CA-signed Certificate.

CA Certificate importēšana

Importējiet CA Certificate skenerī.

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security** > **CA Certificate**.
2. Noklikšķiniet uz **Import**.
3. Norādiet CA Certificate, kuru vēlaties importēt.
4. Noklikšķiniet uz **OK**.

Kad importēšana ir pabeigta, notiek atgriešanās ekrānā **CA Certificate** un tiek parādīts CA Certificate.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

CA Certificate dzēšana

Importēto CA Certificate var dzēst.

1. Piekļūstiet Web Config un tad atlasiet cilni **Network Security** > **CA Certificate**.
2. Noklikšķiniet uz **Delete** blakus tam CA Certificate, kuru vēlaties dzēst.
3. Apstipriniet, ka vēlaties dzēst ziņojumā parādīto sertifikātu.
4. Noklikšķiniet uz **Reboot Network** un pēc tam pārbaudiet, vai dzēstai CA sertifikāts nav redzams atjauninātajā ekrānā.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

SSL/TLS sakari ar skeneri

Ja servera sertifikāts ir iestatīts, izmantojot SSL/TLS (drošligzdu slāņa/transporta slāņa drošības) sakarus ar skeneri, sakaru ceļu starp datoriem var šifrēt. Veiciet šo procedūru, ja vēlaties novērst attālu un neatļautu piekļuvi.

Pamata SSL/TLS iestatījumu konfigurēšana

Ja skeneris atbalsta HTTPS servera funkciju, varat izmantot SSL/TLS saziņu, lai saziņu šifrētu. Skeneri varat konfigurēt un pārvaldīt, izmantojot Web Config, un tajā pašā laikā nodrošinot drošību.

Konfigurējiet šifrēšanas pakāpi un novirzīšanas funkciju.

1. Piekļūstiet Web Config un tad atlasiet cilni **Network Security** > **SSL/TLS** > **Basic**.

2. Atlasiet katram vienumam vērtību.
   - ❏ Encryption Strength
     Atlasiet šifrēšanas pakāpes līmeni.
   - ❏ Redirect HTTP to HTTPS
     Piekļūstot HTTP, novirziet uz HTTPS.
3. Noklikšķiniet uz **Next**.
   Tiek parādīts apstiprinājuma ziņojums.
4. Noklikšķiniet uz **OK**.
   Skeneris ir atjaunināts.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Skenera servera sertifikāta konfigurēšana

1. Atveriet programmu Web Config un atlasiet cilni **Network Security** > **SSL/TLS** > **Certificate**.
2. Norādiet izmantojamo sertifikātu sadaļā **Server Certificate**.
   - ❏ Self-signed Certificate
     Skeneris ģenerē pašparakstītu sertifikātu. Atlasiet šo iespēju, ja nav pieejams CA parakstīts sertifikāts.
   - ❏ CA-signed Certificate
     Varat norādīt šo opciju, ja iepriekš ir iegūts un importēts CA parakstīts sertifikāts.
3. Noklikšķiniet uz **Next**.
   Tiek parādīts apstiprinājuma ziņojums.
4. Noklikšķiniet uz **OK**.
   Skeneris tiek atjaunināts.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.
➡ "CA-signed Certificate konfigurēšana" 98. lpp.
➡ "CA Certificate konfigurēšana" 102. lpp.

Šifrētie sakari, izmantojot IPsec/IP filtrēšanu

Par IPsec/IP Filtering

Jūs varat filtrēt datplūsmu pēc IP adresēm, pakalpojumiem un porta, izmantojot IPsec/IP filtrēšanas funkciju. Kombinējot filtrēšanas metodes, var konfigurēt skeneri tā, lai tas pieņemtu vai bloķētu noteiktus klientus un noteiktus datus. Turklāt, izmantojot IPsec, var uzlabot drošības pakāpi.

Piezīme:
Datori ar operētājsistēmu Windows Vista vai jaunāku Windows versiju vai Windows Server 2008 atbalsta IPsec.

Noklusējuma politikas konfigurēšana

Lai filtrētu trafiku, konfigurējiet noklusējuma politiku. Noklusējuma politika attiecas uz visiem lietotājiem vai grupām, kas veido savienojumu ar skeneri. Lai precīzāk noteiktu lietotāju grupu un atsevišķu lietotāju tiesības, konfigurējiet grupu politikas.

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Ievadiet vērtību katram vienumam.
3. Noklikšķiniet uz **Next**.

   Tiek parādīts apstiprinājuma ziņojums.
4. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Sadaļas Default Policy vienumu iestatīšana

Default Policy

Posms	Iestatījumi un skaidrojums
IPsec/IP Filtering	Var iespējot vai atspējot IPsec/IP filtrēšanas funkciju.

❏ **Access Control**

Konfigurējiet IP pakešu trafika kontroles metodi.

Posms	Iestatījumi un skaidrojums
Permit Access	Atlasiet šo opciju, lai atļautu konfigurēto IP pakešu tranzītu.
Refuse Access	Atlasiet šo opciju, lai noraidītu konfigurēto IP pakešu tranzītu.
IPsec	Atlasiet šo opciju, lai atļautu konfigurēto IPsec pakešu tranzītu.

❏ **IKE Version**

Atlasiet **IKEv1** vai **IKEv2** kā iestatījumu sadaļā **IKE Version**. Atlasiet kādu no tām atbilstoši ierīcei, ar kuru ir savienots skeneris.

❏ IKEv1

Izvēloties **IKEv1** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.

Posms	Iestatījumi un skaidrojums
Authentication Method	Lai atlasītu **Certificate**, ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.

❏ IKEv2

Izvēloties **IKEv2** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.

Posms		Iestatījumi un skaidrojums
Local	Authentication Method	Lai atlasītu **Certificate**, ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
	ID Type	Ja atlasāt **Pre-Shared Key** sadaļā **Authentication Method**, atlasiet skenera ID tipu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.

Posms		Iestatījumi un skaidrojums
Remote	Authentication Method	Lai atlasītu **Certificate**, ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
	ID Type	Ja atlasāt **Pre-Shared Key** sadaļā **Authentication Method**, atlasiet ID tipu ierīcei, kuru vēlaties autentificēt.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.

❏ Encapsulation

Atlasot **IPsec** kā **Access Control** iestatījumu, jākonfigurē iekapsulēšanas režīms.

Posms	Iestatījumi un skaidrojums
Transport Mode	Atlasiet šo opciju, ja izmantojat skeneri tikai vienā lokālajā tīklā. 4. slāņa un jaunākas IP paketes tiek šifrētas.
Tunnel Mode	Atlasiet šo opciju, ja izmantojat skeneri tīklā ar interneta izmantošanas iespēju, piemēram, IPsec-VPN tīklā. Tiek šifrētas IP pakešu galvenes un dati. **Remote Gateway(Tunnel Mode)**: Ja vienuma **Encapsulation** iestatījums ir **Tunnel Mode**, ievadiet vārtejas adresi, kuras garums ir no 1 līdz 39 rakstzīmēm.

❏ Security Protocol

Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām.

Posms	Iestatījumi un skaidrojums
ESP	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti un šifrētu datus.
AH	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti. Pat tad, ja datu šifrēšana ir aizliegta, IPsec var izmantot.

❏ **Algorithm Settings**

Ieteicams izvēlēties **Any** attiecībā uz visiem iestatījumiem vai atlasīt katram iestatījumam vienumu, kas ir atšķirīgs no **Any**. Ja atlasāt **Any** dažiem iestatījumiem, bet citiem iestatījumiem izvēlaties vienumu, kas ir atšķirīgs no **Any**, ierīce, iespējams, nevarēs nodrošināt sakarus, un tas būs atkarīgs no otras ierīces, kuru vēlēsieties autentificēt.

Posms		Iestatījumi un skaidrojums
IKE	Encryption	Atlasiet IKE šifrēšanas algoritmu. Vienumi ir atkarīgi no IKE versijas.
	Authentication	Atlasiet IKE autentificēšanas algoritmu.
	Key Exchange	Atlasiet IKE atslēgu apmaiņas algoritmu. Vienumi ir atkarīgi no IKE versijas.
ESP	Encryption	Atlasiet ESP šifrēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
	Authentication	Atlasiet ESP autentificēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
AH	Authentication	Atlasiet AH šifrēšanas algoritmu. Tas ir pieejams, kad **AH** ir izvēlēts kā **Security Protocol** iestatījums.

Grupas politikas konfigurēšana

Grupas politika ir viena vai vairākas kārtulas, kas piemērotas lietotāju grupai vai lietotājam. Skeneris kontrolē IP paketes, kas atbilst konfigurētajām politikām. IP paketes tiek autentificētas 1.–10. grupas politikas secībā, pēc tam tiek piemērota noklusējuma politika.

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Noklikšķiniet uz konfigurējamās numurētās cilnes.
3. Ievadiet vērtību katram vienumam.
4. Noklikšķiniet uz **Next**.

   Tiek parādīts apstiprinājuma ziņojums.
5. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Sadaļas Group Policy vienumu iestatīšana

Posms	Iestatījumi un skaidrojums
Enable this Group Policy	Var iespējot vai atspējot grupas politiku.

Access Control

Konfigurējiet IP pakešu trafika kontroles metodi.

Posms	Iestatījumi un skaidrojums
Permit Access	Atlasiet šo opciju, lai atļautu konfigurēto IP pakešu tranzītu.
Refuse Access	Atlasiet šo opciju, lai noraidītu konfigurēto IP pakešu tranzītu.
IPsec	Atlasiet šo opciju, lai atļautu konfigurēto IPsec pakešu tranzītu.

Local Address (Scanner)

Izvēlieties IPv4 vai IPv6 adresi, kas atbilst jūsu tīkla videi. Ja IP adrese netiek piešķirta automātiski, varat izvēlēties **Use auto-obtained IPv4 address**.

Piezīme:
Ja IPv6 adreses tiek piešķirtas automātiski, savienojums var nebūt pieejams. Konfigurējiet statisko IPv6 adresi.

Remote Address(Host)

Lai kontrolētu piekļuvi, ievadiet ierīces IP adresi. IP adresei jābūt 43 rakstzīmes garai vai īsākai. Ja IP adrese netiek ievadīta, tiek kontrolētas visas adreses.

Piezīme:
Ja IP adreses tiek piešķirtas automātiski (piemēram, adreses piešķir DHCP), savienojums var nebūt pieejams. Konfigurējiet statisko IP adresi.

Method of Choosing Port

Atlasiet portu norādīšanas metodi.

❏ Service Name

Atlasot **Service Name** kā **Method of Choosing Port** iestatījumu, jāizvēlas kāda no opcijām.

❏ Transport Protocol

Atlasot **Port Number** kā **Method of Choosing Port** iestatījumu, jākonfigurē iekapsulēšanas režīms.

Posms	Iestatījumi un skaidrojums
Any Protocol	Atlasiet, lai kontrolētu visu veidu protokolus.
TCP	Atlasiet, lai kontrolētu uniraides datus.
UDP	Atlasiet, lai kontrolētu apraides un multiraides datus.
ICMPv4	Atlasiet, lai kontrolētu ehotestēšanas komandu.

❏ Local Port

Atlasot **Port Number** kā **Method of Choosing Port** iestatījumu, un **TCP** vai **UDP** — kā **Transport Protocol** iestatījumu, ievadiet portu numurus, lai kontrolētu pakešu saņemšanu, atdalot tos ar komatiem. Var ievadīt līdz 10 portu numuriem.

Piemērs: 20,80,119,5220

Ja porta numurs nav ievadīts, tiek kontrolēti visi porti.

❏ Remote Port

Atlasot **Port Number** kā **Method of Choosing Port** iestatījumu, un **TCP** vai **UDP** — kā **Transport Protocol** iestatījumu, ievadiet portu numurus, lai kontrolētu pakešu sūtīšanu, atdalot tos ar komatiem. Var ievadīt līdz 10 portu numuriem.

Piemērs: 25,80,143,5220

Ja porta numurs nav ievadīts, tiek kontrolēti visi porti.

IKE Version

Atlasiet **IKEv1** vai **IKEv2** kā iestatījumu sadaļā **IKE Version**. Atlasiet kādu no tām atbilstoši ierīcei, ar kuru ir savienots skeneris.

❏ IKEv1

Izvēloties **IKEv1** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.

Posms	Iestatījumi un skaidrojums
Authentication Method	Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.

❏ IKEv2

Izvēloties **IKEv2** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.

Posms		Iestatījumi un skaidrojums
Local	Authentication Method	Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
	ID Type	Ja atlasāt **Pre-Shared Key** sadaļā **Authentication Method**, atlasiet skenera ID tipu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.
Remote	Authentication Method	Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
	ID Type	Ja atlasāt **Pre-Shared Key** sadaļā **Authentication Method**, atlasiet ID tipu ierīcei, kuru vēlaties autentificēt.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 255 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.

Encapsulation

Atlasot **IPsec** kā **Access Control** iestatījumu, jākonfigurē iekapsulēšanas režīms.

Posms	Iestatījumi un skaidrojums
Transport Mode	Atlasiet šo opciju, ja izmantojat skeneri tikai vienā lokālajā tīklā. 4. slāņa un jaunākas IP paketes tiek šifrētas.
Tunnel Mode	Atlasiet šo opciju, ja izmantojat skeneri tīklā ar interneta izmantošanas iespēju, piemēram, IPsec-VPN tīklā. Tiek šifrētas IP pakešu galvenes un dati. **Remote Gateway(Tunnel Mode)**: Ja vienuma **Encapsulation** iestatījums ir **Tunnel Mode**, ievadiet vārtejas adresi, kuras garums ir no 1 līdz 39 rakstzīmēm.

Security Protocol

Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām.

Posms	Iestatījumi un skaidrojums
ESP	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti un šifrētu datus.
AH	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti. Pat tad, ja datu šifrēšana ir aizliegta, IPsec var izmantot.

Algorithm Settings

Ieteicams izvēlēties **Any** attiecībā uz visiem iestatījumiem vai atlasīt katram iestatījumam vienumu, kas ir atšķirīgs no **Any**. Ja atlasāt **Any** dažiem iestatījumiem, bet citiem iestatījumiem izvēlaties vienumu, kas ir atšķirīgs no **Any**, ierīce, iespējams, nevarēs nodrošināt sakarus, un tas būs atkarīgs no otras ierīces, kuru vēlēsieties autentificēt.

Posms		Iestatījumi un skaidrojums
IKE	Encryption	Atlasiet IKE šifrēšanas algoritmu. Vienumi ir atkarīgi no IKE versijas.
	Authentication	Atlasiet IKE autentificēšanas algoritmu.
	Key Exchange	Atlasiet IKE atslēgu apmaiņas algoritmu. Vienumi ir atkarīgi no IKE versijas.
ESP	Encryption	Atlasiet ESP šifrēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
	Authentication	Atlasiet ESP autentificēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
AH	Authentication	Atlasiet AH šifrēšanas algoritmu. Tas ir pieejams, kad **AH** ir izvēlēts kā **Security Protocol** iestatījums.

Local Address (Scanner) un Remote Address(Host) kombinācija, Group Policy

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

Remote Address(Host) iestatīšana	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Tukšs	✓	✓	✓

*1 Ja izvēlas **IPsec** kā **Access Control** iestatījumu, nevar norādīt prefiksa garumu.

*2 Ja izvēlas **IPsec** kā **Access Control** iestatījumu, var izvēlēties saiti-lokālo adresi (fe80::), taču grupas politika tiks atspējota.

*3 Izņemot IPv6 saites lokālās adreses.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Norādes uz pakalpojuma nosaukumiem grupas politikā

Piezīme:
Nepieejamie pakalpojumi ir redzami, taču tos nevar atlasīt.

Pakalpojuma nosaukums	Protokola veids	Lokālā porta numurs	Attālā porta numurs	Kontrolētās funkcijas
Any	–	–	–	Visi pakalpojumi
ENPC	UDP	3289	Jebkurš ports	Skenera meklēšana, izmantojot tādas programmas kā Epson Device Admin un skenera draiverus
SNMP	UDP	161	Jebkurš ports	MIB iegūšana un konfigurēšana, izmantojot tādas programmas kā Epson Device Admin, un Epson skenera draiveri
WSD	TCP	Jebkurš ports	5357	WSD vadība
WS-Discovery	UDP	3702	Jebkurš ports	Meklē WSD skenerus
Network Scan	TCP	1865	Jebkurš ports	Skenēto datu pārsūtīšana no Document Capture Pro
Network Push Scan	TCP	Jebkurš ports	2968	Pašpiegādes skenēšanas uzdevumu informācijas ieguve programmā Document Capture Pro
Network Push Scan Discovery	UDP	2968	Jebkurš ports	Datora meklēšana no skenera
FTP Data (Remote)	TCP	Jebkurš ports	20	FTP klients (skenēto datu pārsūtīšana) Tomēr šādi var kontrolēt FTP serveri tikai tad, ja tajā izmantotais attālā porta numurs ir 20.
FTP Control (Remote)	TCP	Jebkurš ports	21	FTP klients (pārsūtīto skenēto datu vadība)
CIFS (Remote)	TCP	Jebkurš ports	445	CIFS klients (skenēto datu pārsūtīšana uz mapi)

Pakalpojuma nosaukums	Protokola veids	Lokālā porta numurs	Attālā porta numurs	Kontrolētās funkcijas
NetBIOS Name Service (Remote)	UDP	Jebkurš ports	137	CIFS klients (skenēto datu pārsūtīšana uz mapi)
NetBIOS Datagram Service (Remote)	UDP	Jebkurš ports	138	
NetBIOS Session Service (Remote)	TCP	Jebkurš ports	139	
HTTP (Local)	TCP	80	Jebkurš ports	HTTP(S) serveris (Web Config un WSD datu pārsūtīšana)
HTTPS (Local)	TCP	443	Jebkurš ports	
HTTP (Remote)	TCP	Jebkurš ports	80	HTTP(S) klients (aparātprogrammatūras un saknes sertifikāta atjaunināšana)
HTTPS (Remote)	TCP	Jebkurš ports	443	

IPsec/IP Filtering konfigurāciju piemēri

Tikai IPsec pakešu saņemšana

Piemērā skaidrota tikai noklusējuma politikas konfigurēšana.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: ievadiet līdz 127 rakstzīmēm.

Group Policy: nekonfigurējiet.

Skenējuma datu un skenera iestatījumu saņemšana

Šajā piemērā tiek atļauta skenējumu datu un skenera konfigurācijas pārraide no norādītajiem pakalpojumiem.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: atzīmējiet izvēles rūtiņu.

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

❏ **Remote Address(Host)**: klienta IP adrese

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

❏ **Service Name**: atzīmējiet izvēles rūtiņas **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)** un **Network Scan**.

Piekļuves piešķiršana tikai norādītajai IP adresei

Šajā piemērā redzams, kā atļaut piekļuvi skenerim no norādītas IP adreses.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: atzīmējiet izvēles rūtiņu.

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

❏ **Remote Address(Host)**: administratora klienta IP adrese

Piezīme:
Neatkarīgi no politikas konfigurācijas klients varēs piekļūt skenerim un konfigurēt to.

IPsec/IP filtrēšanas sertifikāta konfigurēšana

Konfigurējiet klienta IPsec/IP filtrēšanas sertifikātu. To iestatot, sertifikātu var izmantot kā IPsec/IP filtrēšanas autentifikācijas metodi. Ja vēlaties konfigurēt sertificēšanas iestādi, dodieties uz **CA Certificate**.

1. Piekļūstiet Web Config un tad atlasiet cilni **Network Security** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importējiet sertifikātu **Client Certificate**.

   Ja jau esat importējis sertifikātu, ko izdevusi sertificēšanas iestāde, varat izveidot sertifikāta kopiju un izmantot to IPsec/IP filtrēšanai. Lai izveidotu kopiju, atlasiet sertifikātu sadaļā **Copy From** un noklikšķiniet uz **Copy**.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

➡ "CA-signed Certificate konfigurēšana" 98. lpp.

➡ "CA Certificate konfigurēšana" 102. lpp.

Skenera pievienošana IEEE802.1X tīklam

IEEE 802.1X tīkla konfigurēšana

Iestatot skenerim IEEE 802.1X, jūs to varat izmantot tīklā, kas savienots ar RADIUS serveri, lokālā tīkla komutatoru ar autentifikācijas funkciju vai piekļuves punktu.

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security** > **IEEE802.1X** > **Basic**.

2. Ievadiet vērtību katram vienumam.

   Ja vēlaties izmantot skeneri Wi-Fi tīklā, noklikšķiniet uz **Wi-Fi Setup** un atlasiet vai ievadiet SSID.

   Piezīme:
   Ethernet un Wi-Fi tīklam iespējams izmantot kopīgus iestatījumus.

3. Noklikšķiniet uz **Next**.

   Tiek parādīts apstiprinājuma ziņojums.

4. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

IEEE 802.1X tīkla vienumu iestatīšana

Posms	Iestatījumi un skaidrojums	
IEEE802.1X (Wired LAN)	Varat iespējot vai atspējot lapas iestatījumus (**IEEE802.1X** > **Basic**) IEEE802.1X tīklam (vadu LAN).	
IEEE802.1X (Wi-Fi)	Tiek parādīts IEEE802.1X tīkla savienojuma statuss (Wi-Fi).	
Connection Method	Tiek parādīta pašreizējā tīkla savienojuma metode.	
EAP Type	Atlasiet skenera un RADIUS servera autentifikācijas metodes opciju.	
	EAP-TLS	Ir jāiegūst un jāimportē sertifikāts ar CA parakstu.
	PEAP-TLS	
	PEAP/MSCHAPv2	Ir jākonfigurē parole.
	EAP-TTLS	
User ID	Konfigurējiet ID, kas jāizmanto RADIUS servera autentifikācijai. Ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.	
Password	Konfigurējiet paroli, lai autentificētu skeneri. Ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Ja izmantojat Windows serveri kā RADIUS serveri, var ievadīt līdz 127 rakstzīmēm.	
Confirm Password	Lai apstiprinātu, ievadiet konfigurēto paroli.	
Server ID	Servera ID var konfigurēt noteikta RADIUS servera autentificēšanai. Autentificētājs pārbauda, vai servera sertifikāta, ko sūta RADIUS serveris, laukā subject/subjectAltName ir ietverts servera ID. Ievadiet 0 līdz 128 viena bita ASCII (0x20–0x7E) rakstzīmes.	
Certificate Validation	Var iestatīt sertifikāta validāciju neatkarīgi no autentifikācijas metodes. Importējiet sertifikātu laukā **CA Certificate**.	
Anonymous Name	Opcijas **PEAP-TLS** vietā atlasot **PEAP/MSCHAPv2** vai **EAP Type**, var konfigurēt anonīmu nosaukumu, kas „PEAP" autentifikācijas 1. posmā jāizmanto lietotāja ID vietā. Ievadiet 0 līdz 128 viena bita ASCII (0x20–0x7E) rakstzīmes.	

Posms	Iestatījumi un skaidrojums	
Encryption Strength	Var atlasīt vienu no turpmāk norādītajām iespējām.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

IEEE 802.1X sertifikāta konfigurēšana

Konfigurējiet klienta IEEE802.1X sertifikātu. Kad tas ir iestatīts, varat izmantot **EAP-TLS** un **PEAP-TLS** kā IEEE 802.1X autentifikācijas metodi. Ja vēlaties konfigurēt sertificēšanas iestādes sertifikātu, dodieties uz **CA Certificate**.

1. Piekļūstiet Web Config un tad atlasiet cilni **Network Security** > **IEEE802.1X** > **Client Certificate**.
2. Ievadiet sertifikātu **Client Certificate**.

   Ja jau esat importējis sertifikātu, ko izdevusi sertificēšanas iestāde, varat izveidot sertifikāta kopiju un izmantot to IEEE802.1X. Lai izveidotu kopiju, atlasiet sertifikātu sadaļā **Copy From** un noklikšķiniet uz **Copy**.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Drošības papildu iestatījumu problēmu risināšana

Drošības iestatījumu atjaunošana

Izveidojot augstas drošības vidi, piemēram, izmantojot IPsec/IP filtrēšanu, pastāv iespēja, ka nevarēs sazināties ar ierīcēm nepareizu iestatījumu vai ierīces vai servera darbības traucējumu dēļ. Šādā gadījumā atjaunojiet drošības iestatījumus, lai vēlreiz iestatītu ierīci vai nodrošinātu īslaicīgu lietošanu.

Drošības funkcijas atspējošana, izmantojot Web Config

Jūs varat atspējot IPsec/IP Filtering, izmantojot Web Config.

1. Atveriet programmu Web Config un atlasiet cilni **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Atspējojiet **IPsec/IP Filtering**.

Tīkla drošības funkciju lietošanas problēmas

Aizmirsta iepriekš koplietota atslēga

Atkārtoti konfigurējiet iepriekš koplietotu atslēgu.

Lai mainītu atslēgu, atveriet programmu Web Config un atlasiet cilni **Network Security** > **IPsec/IP Filtering** > **Basic** > **Default Policy** vai **Group Policy**.

Mainot iepriekš koplietotu atslēgu, konfigurējiet datoriem paredzētu iepriekš koplietotu atslēgu.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.
➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 105. lpp.

Nevar izveidot sakarus, izmantojot IPsec

Norādiet algoritmu, ko skeneris vai dators neatbalsta.

Skeneris atbalsta turpmāk norādītos algoritmus. Pārbaudiet datora iestatījumus.

Drošības metodes	Algoritmi
IKE šifrēšanas algoritms	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE autentificēšanas algoritms	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE atslēgu apmaiņas algoritms	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 šifrēšanas algoritms	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP autentificēšanas algoritms	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH autentificēšanas algoritms	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* pieejams tikai protokolam IKEv2

Saistītā informācija

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 105. lpp.

Pēkšņi nevar izveidot sakarus

Skenera IP adrese ir mainīta vai to nevar izmantot.

Kad sadaļā Group Policy lokālajai adresei reģistrētā IP adrese ir mainīta vai to nevar izmantot, nevar izveidot IPsec sakarus. Atspējojiet IPsec, izmantojot skenera vadības paneli.

Ja nav atjaunināts DHCP, veicat atsāknēšanu vai arī nav atjaunināta vai iegūta IPv6 adrese, skenera programmā Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) reģistrētā IP adrese, iespējams, netiks atrasta.

Izmantojiet statisku IP adresi.

Datora IP adrese ir mainīta vai to nevar izmantot.

Kad sadaļā Group Policy attālajai adresei reģistrētā IP adrese ir mainīta vai to nevar izmantot, nevar izveidot IPsec sakarus.

Atspējojiet IPsec, izmantojot skenera vadības paneli.

Ja nav atjaunināts DHCP, veicat atsāknēšanu vai arī nav atjaunināta vai iegūta IPv6 adrese, skenera programmā Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) reģistrētā IP adrese, iespējams, netiks atrasta.

Izmantojiet statisku IP adresi.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 105. lpp.

Nevar izveidot savienojumu pēc IPsec/IP filtrēšanas konfigurācijas

IPsec/IP filtrēšanas iestatījumi ir nepareizi.

Skenera vadības panelī atspējojiet IPsec/IP filtrēšanu. Pievienojiet printeri datoram un vēlreiz veiciet IPsec/IP filtrēšanas iestatījumus.

Saistītā informācija

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 105. lpp.

Pēc IEEE 802.1X konfigurēšanas neizdodas piekļūt skenerim

IEEE 802.1X iestatījumi ir nepareizi.

Skenera vadības panelī atspējojiet IEEE 802.1X un Wi-Fi. Pievienojiet skeneri datoram un tad vēlreiz konfigurējiet IEEE 802.1X.

Pievienojiet skeneri datoram un tad vēlreiz konfigurējiet IEEE 802.1X.

Saistītā informācija

➡ "IEEE 802.1X tīkla konfigurēšana" 115. lpp.

Ciparsertifikāta lietošanas problēmas

Nevar importēt CA-signed Certificate

CA-signed Certificate un CSR informācija atšķiras.

Ja informācija CA-signed Certificate un CSR atšķiras, CSR nevar importēt. Pārbaudiet turpmāk norādīto:

❏ Vai mēģināt importēt sertifikātu ierīcē, kurā nav tāda pati informācija?
Pārbaudiet CSR informāciju un pēc tam importējiet sertifikātu ierīcē, kurā ir tāda pati informācija.

❏ Vai pēc CSR nosūtīšanas sertificēšanas iestādei skenerī saglabātais CSR tika pārrakstīts?
Vēlreiz iegūstiet CA parakstītu sertifikātu, izmantojot CSR.

CA-signed Certificate lielums pārsniedz 5 KB.

Nevar importēt CA-signed Certificate, kura lielums pārsniedz 5 KB.

Sertifikāta importēšanas parole nav pareiza.

Ievadiet pareizu paroli. Ja parole aizmirsta, sertifikātu nevar importēt. Atkārtoti iegūstiet CA-signed Certificate.

Saistītā informācija

➡ "CA parakstīta sertifikāta importēšana" 100. lpp.

Nevar atjaunināt pašparakstītu sertifikātu

Common Name nav ievadīts.

Jābūt ievadītai vērtībai laukā **Common Name**.

Laukā Common Name ievadītas neatbalstītas rakstzīmes.

Ievadiet 1–128 rakstzīmes IPv4 IPv6 resursdatora nosaukuma vai FQDN formātā ASCII kodējumā (0x20–0x7E).

Kopējā nosaukumā ir izmantots komats vai atstarpe.

Ja ievadīts komats, lauka **Common Name** vērtība šajā punktā tiek sadalīta. Ja pirms vai pēc komata ievadīta atstarpe, notiek kļūda.

Saistītā informācija

➡ "Pašparakstīta sertifikāta atjaunināšana" 102. lpp.

Nevar izveidot CSR

Common Name nav ievadīts.

Jābūt ievadītai vērtībai laukā **Common Name**.

Laukos Common Name, Organization, Organizational Unit, Locality un State/Province ievadītas neatbalstītas rakstzīmes.

Ievadiet rakstzīmes IPv4, IPv6 resursdatora nosaukuma vai FQDN formātā, ASCII kodējumā (0x20–0x7E).

Laukā Common Name ir izmantots komats vai atstarpe.

Ja ievadīts komats, lauka **Common Name** vērtība šajā punktā tiek sadalīta. Ja pirms vai pēc komata ievadīta atstarpe, notiek kļūda.

Saistītā informācija

➡ "CA parakstīta sertifikāta iegūšana" 98. lpp.

Tiek parādīts ar ciparsertifikāta lietošanu saistīts brīdinājums

Ziņojumi	Cēlonis/risinājums
Enter a Server Certificate.	**Cēlonis:** Nav atlasīts importējamais fails. **Risinājums:** Atlasiet failu un noklikšķiniet uz **Import**.
CA Certificate 1 is not entered.	**Cēlonis:** Nav ievadīts 1. CA sertifikāts; ievadīts tikai 2. CA sertifikāts. **Risinājums:** Vispirms importējiet 1. CA sertifikātu.
Invalid value below.	**Cēlonis:** Faila ceļā un/vai parolē ietvertas neatbalstītas rakstzīmes. **Risinājums:** Pārliecinieties, vai vienuma rakstzīmes ir ievadītas pareizi.
Invalid date and time.	**Cēlonis:** Nav iestatīts skenera datums un laiks. **Risinājums:** Iestatiet datumu un laiku, izmantojot Web Config vai EpsonNet Config.
Invalid password.	**Cēlonis:** Iestatītā CA sertifikāta parole nesakrīt ar ievadīto paroli. **Risinājums:** Ievadiet pareizu paroli.

Ziņojumi	Cēlonis/risinājums
Invalid file.	**Cēlonis:** Netiek importēts X509 formāta sertifikāta fails. **Risinājums:** Pārliecinieties, vai atlasāt pareizo sertifikāta failu, kas saņemts no uzticamas sertificēšanas iestādes.
	Cēlonis: Importētais fails ir pārāk liels. Maksimālais lielums ir 5 KB. **Risinājums:** Ja atlasīts pareizais fails, iespējams, sertifikāts ir bojāts vai safabricēts.
	Cēlonis: Nederīga sertifikātā iekļautā ķēde. **Risinājums:** Papildinformāciju par sertifikātu skatiet sertificēšanas iestādes tīmekļa vietnē.
Cannot use the Server Certificates that include more than three CA certificates.	**Cēlonis:** PKCS#12 formāta sertifikāta failā ietverti vairāk nekā 3 CA sertifikāti. **Risinājums:** Importējiet katru sertifikātu, konvertējot no PKCS#12 formāta PEM formātā, vai importējiet PKCS#12 formāta sertifikāta failu, kurā ietverti ne vairāk kā 2 CA sertifikāti.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Cēlonis:** Beidzies sertifikāta derīguma termiņš. **Risinājums:** ❏ Ja beidzies sertifikāta derīguma termiņš, iegūstiet un importējiet jaunu sertifikātu. ❏ Ja sertifikāta derīguma termiņš nav beidzies, pārliecinieties, vai skenera datums un laiks ir iestatīts pareizi.
Private key is required.	**Cēlonis:** Nav ar sertifikātu pārī savienotas privātas atslēgas. **Risinājums:** ❏ Ja sertifikāts ir PEM/DER formātā un ir iegūts no CSR, izmantojot datoru, norādiet privāto atslēgas failu. ❏ Ja sertifikāts ir PKCS#12 formātā un ir iegūts no CSR, izmantojot datoru, izveidojiet failu, kas satur privāto atslēgu.
	Cēlonis: Izmantojot Web Config, no CSR iegūts PEM/DER sertifikāts ir importēts atkārtoti. **Risinājums:** Ja sertifikāts ir PEM/DER formātā un ir iegūts no CSR, izmantojot Web Config, to var importēt tikai vienu reizi.

Ziņojumi	Cēlonis/risinājums
Setup failed.	**Cēlonis:** Nevar pabeigt konfigurēšanu, jo nav izveidoti skenera un datora sakari, vai failu nevar nolasīt kļūdu dēļ. **Risinājums:** Pēc norādītā faila un sakaru pārbaudes importējiet failu vēlreiz.

Saistītā informācija

➡ "Par ciparsertifikātiem" 98. lpp.

CA parakstīta sertifikāta nejauša dzēšana

CA parakstītam sertifikātam nav dublējuma faila.

Ja ir pieejams dublējuma fails, importējiet sertifikātu vēlreiz.

Ja sertifikāts ir iegūts, izmantojot lietojumprogrammā Web Config izveidotu CSR, dzēstu sertifikātu nevar importēt vēlreiz. Izveidojiet CSR un iegūstiet jaunu sertifikātu.

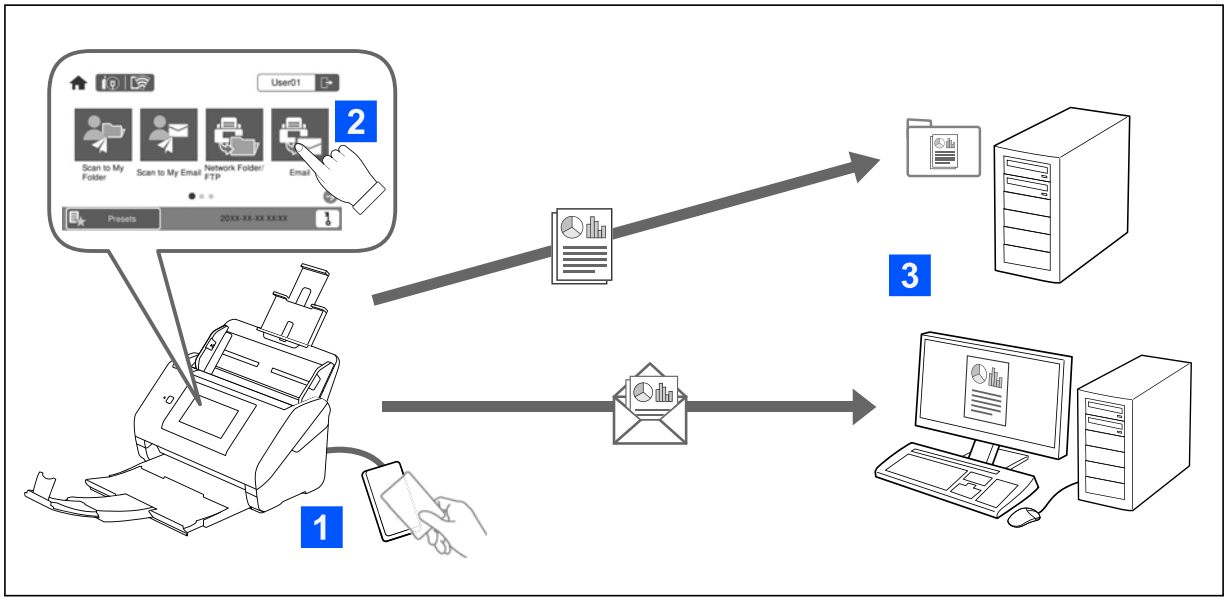
Saistītā informācija

➡ "CA parakstīta sertifikāta importēšana" 100. lpp.

➡ "CA parakstīta sertifikāta dzēšana" 101. lpp.

Authentication Settings

Par Authentication Settings



Kad Authentication Settings ir iespējoti, lai sāktu skenēšanu nepieciešama lietotāja autentifikācija. Jūs varat iestatīt katram lietotājam paredzētas skenēšanas metodes, un novērst nejaušas darbības.

Jūs varat norādīt autentificēto lietotāju e-pasta adresi kā skenēšanas galamērķi (Scan to My Email) vai saglabāt katra lietotāja datus personiskā mapē (Scan to My Folder). Var norādīt arī citas skenēšanas metodes.

Piezīme:

❏ *Jūs nevarat skenēt no datora vai viedierīces, ja Authentication Settings ir iespējoti.*

❏ *Papildus šajā rokasgrāmatā izskaidrotajiem Authentication Settings, jūs varat izveidot autentifikācijas sistēmu, izmantojot autentifikācijas serveri. Lai izveidotu sistēmu, izmantojiet Document Capture Pro Server Authentication Edition (saīsinātais nosaukums ir Document Capture Pro Server AE). Lai iegūtu plašāku informāciju, sazinieties ar vietējo Epson biroju.*

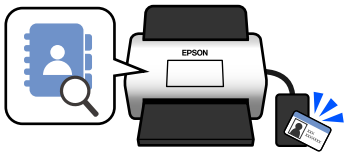
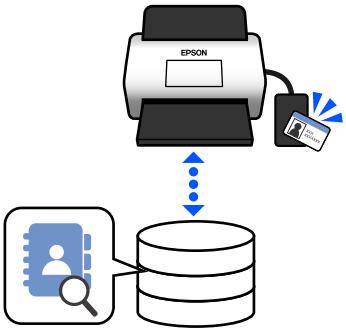
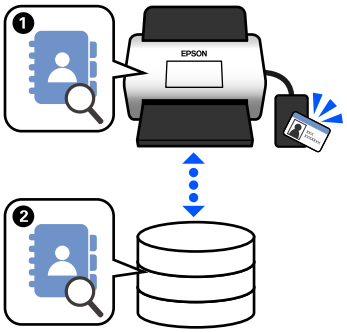
Pieejamās funkcijas attiecībā uz Authentication Settings

Skenēšanas funkcijas vadības panelī	Authentication Settings	
	Kad iespējots	Kad atspējots
Skenēt uz manu mapi Saglabā attēlus mapē, kas piešķirta autentificētam lietotājam.	✓	-
Skenēt uz e-pastu Sūta attēlus uz autentificētā lietotāja e-pasta adresi.	✓	-
Skenēt tīkla mapē/FTP Saglabā attēlus tīkla mapē.	✓	✓

Skenēšanas funkcijas vadības panelī	Authentication Settings	
	Kad iespējots	Kad atspējots
Skenēt uz datoru Saglabā attēlus pievienotajā datorā, izmantojot Document Capture Pro (Windows)/Document Capture (Mac OS) izveidotos uzdevumus. * Kad Authentication Settings ir iespējoti, jūs varat izmantot tikai **Priekšiestat.** reģistrētos darbus.	✓*	✓
Skenēt uz e-pastu Sūta attēlus uz iestatīto e-pasta adresi.	✓	✓
Skenēt uz mākoni Sūta attēlus uz iestatīto mākoņpakalpojumu.	✓	✓
Skenēt uz USB disku Saglabā attēlus USB diskā, kas pievienots skenerim. Tas pieejams tikai, ja skenerim nav pieslēgta neviena autentifikācijas ierīce.	✓	✓
Skenēt uz WSD Saglabā attēlus pievienotā datorā, izmantojot WSD funkciju.	-	✓
Priekšiestat. Ir iespējams reģistrēt līdz 48 priekšiestatītas skenēšanas funkcijas. Varat piešķirt līdz pieciem Priekšiestat. Local DB reģistrētiem lietotājiem. Piešķirtie Priekšiestat. pieejami tikai konkrētam lietotājam. Priekšiestat., kas nav piešķirti nevienam lietotājam, var izmantot visi lietotāji.	✓	✓

Par Authentication Method

Šis skeneris var nodrošināt autentifikāciju, izmantojot turpmākās metodes, bez autentifikācijas servera izveides.

	Local DB	LDAP	Local DB and LDAP
Lietotāja informācijas atrašanās vieta	**Skenera atmiņa** Šī autentifikācijas metode pārbauda skenerī reģistrēto lietotāja informāciju un salīdzina to ar lietotāju, kurš izmanto skenēšanas funkciju.	**LDAP serveris*** Šī autentifikācijas metode pārbauda ar skeneri sinhronizētā LDAP serverī esošo lietotāja informāciju. Tā kā skenera kešatmiņā īslaicīgi var saglabāties līdz 300 vienumiem lietotāja informācijas no LDAP servera, ja LDAP serveris nedarbojas autentifikācijai var izmantot kešatmiņu. * Serveris, kas nodrošina ar LDAP komunicējošu direktorija pakalpojumu.	**Skenera atmiņa un LDAP serveris** Vispirms pārbaudiet skenerī reģistrēto lietotāja informāciju (❶) un, ja nav atbilstošas informācijas, pārbaudiet lietotāja informāciju LDAP serverī (❷).
			
Reģistrēto lietotāju skaits	50 (skenera atmiņā)	Neierobežots (LDAP serverī)	50 (skenera atmiņā) Neierobežots (LDAP serverī)
Skenera kešatmiņa	-	300	Maks. 300 (50 kešatmiņas vietas tiek koplietotas ar User Settings Local DB)
Pieteikšanās metodes	Varat izmantot vienu no turpmāk norādītajām metodēm. ❏ Pielieciet autentifikācijas karti vai ievadiet **User ID** un **Password** ❏ Pielieciet autentifikācijas karti vai ievadiet **ID Number** ❏ Ievadiet **User ID** un **Password** ❏ Ievadiet **User ID** ❏ Ievadiet **ID Number**		
Ierobežojumi „Skenēt uz" funkcijai	Iestatiet individuāli katram lietotājam	Vienādi iestatījumi visiem LDAP lietotājiem	Local DB lietotāji: iestatīt individuāli LDAP lietotāji: vienādi iestatījumi visiem lietotājiem
Priekšiestat. piešķiršana lietotājiem	Ne vairāk kā 5 katram lietotājam	- (Nevar iestatīt individuāli)	Local DB lietotāji: ne vairāk kā 5 katram lietotājam LDAP lietotāji: -

Programmatūra iestatīšanai

Iestatiet, izmantojot Web Config vai Epson Device Admin.

❏ Izmantojot Web Config, varat iestatīt skeneri, izmantojot tikai tīmekļa pārlūkprogrammu.
"Web Config" 35. lpp.

❏ Izmantojot Epson Device Admin, varat iestatīt vairākus skenerus vienlaicīgi, izmantojot konfigurācijas veidni.
"Epson Device Admin" 36. lpp.

Skenera aparātprogrammatūras atjaunināšana

Pirms iespējot Authentication Settings, atjauniniet skenera aparātpogrammatūru uz jaunāko versiju. Jau sākumā izveidojiet interneta savienojumu ar skeneri.

Svarīga informācija:
Atjaunināšanas laikā neizslēdziet datoru vai skeneri.

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Device Management** > **Firmware Update** un pēc tam ņemiet vērā ekrānā redzamās instrukcijas aparātprogrammatūras atjaunināšanai.

Iestatīšana, izmantojot Epson Device Admin:

Ierīces saraksta ekrānā atlasiet **Home** > **Firmware** > **Update** un pēc tam ņemiet vērā ekrānā redzamās instrukcijas aparātprogrammatūras atjaunināšanai.

Piezīme:
Ja jau ir instalēta jaunākā aparātprogrammatūra, atjaunināšana nav jāveic.

Autentifikācijas ierīču tabulaAAaAAutentifikācijas ierīces pievienošana un konfigurācija

Ja vēlaties pievienot un izmantot autentifikācijas ierīci, piemēram, IC karšu lasītāju, jums vispirms jākonfigurē ierīce. Tas nav nepieciešams, ja neizmantojat autentifikācijas ierīci.

Saistītā informācija

➡ "Autentifikācijas ierīces pievienošana" 131. lpp.

➡ "Autentifikācijas ierīces iestatījumi" 132. lpp.

Saderīgu karšu lasītāju saraksts

Saraksts negarantē tajā esošo karšu lasītāju darbību.

Jā: atbalstīts (ID informāciju var nolasīt, izmantojot standarta karšu lasītāja iestatījumus).

Nē: nav saderīgs

Ražotājs	Modelis	Modeļa numurs	Autentifikācijas karte							Režīms
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Jā	Jā*1	Jā*1	Jā*1	Nē	Nē	Nē	Tastatūra
RF IDEAS	pcProx	RDR-7081BKU	Jā*1	Nē	Jā	Jā	Nē	Nē	Nē	Tastatūra
RF IDEAS	pcProx	RDR-7581AKU	Jā	Nē	Jā*1	Jā*1	Nē	Nē	Nē	Tastatūra
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Nē	Nē	Jā	Jā	Nē	Nē	Nē	Tastatūra
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Jā	Nē	Jā	Jā	Jā	Jā	Jā	Tastatūra
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Jā	Jā	Jā	Jā	Jā	Jā	Jā	Tastatūra
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Jā	Jā	Jā	Jā	Jā	Jā	Jā	Tastatūra
ELATEC	TWN4 Slim	T4QC-FC3B7	Jā	Jā	Jā	Jā	Jā	Jā	Jā	Tastatūra
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Jā	Jā	Jā	Jā	Jā	Nē	Jā	Tastatūra*1
ACS	ACR122U	ACR122U	Nē	Nē	Jā*2	Jā*2	Jā	Nē	Jā*2	PC/SC

Ražotājs	Modelis	Modeļa numurs	Autentifikācijas karte							Režīms
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ACS	ACR1252	ACR1252	Nē	Nē	Jā*2	Jā*2	Jā	Jā	Jā*2	PC/SC
Sony	PaSoRi	RC-S330/S	Nē	Nē	Jā*2	Jā*2	Jā*2	Jā*2	Jā*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Nē	Nē	Jā*2	Jā*2	Jā*2	Jā*2	Jā*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Jā	Jā	Jā	Jā	Jā	Jā	Jā	Tastatūra
DMZ	Leitor RFID Multi-125	DMZ087	Nē	Jā	Nē	Nē	Nē	Nē	Nē	Tastatūra
DMZ	Leitor RFID Mifare	DMZ088	Nē	Nē	Jā	Jā	Nē	Nē	Nē	Tastatūra
DMZ	Biometric & RFID Reader	DMZ073	Nē	Jā	Nē	Nē	Nē	Nē	Nē	Tastatūra
inepro	SCR708	SCR708	Jā*1	Jā*1	Jā*1	Jā*1	Jā*1	Jā*1	Jā*1	Tastatūra
Y Soft	YU030888 001	MU0388	Jā	Jā	Jā	Jā	Jā	Jā	Jā	Tastatūra
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Nē	Nē	Jā	Jā	Nē	Nē	Jā	Tastatūra
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Nē	Nē	Jā	Jā	Nē	Nē	Jā	Tastatūra

Ražotājs	Modelis	Modeļa numurs	Autentifikācijas karte							Režīms
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
NT-ware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Jā	Jā	Jā	Jā	Jā	Jā	Jā	Tastatūra
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Jā*1	Jā*1	Jā*1	Jā*1	Nē	Nē	Nē	Tastatūra
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Jā	Jā	Jā	Jā	Jā	Jā	Nē	Tastatūra

*1 Jums nepieciešams mainīt karšu lasītāja iestatījumus, izmantojot ar īpašumtiesībām aizsargātu programmatūru, ko nodrošina karšu lasītāja ražotājs.

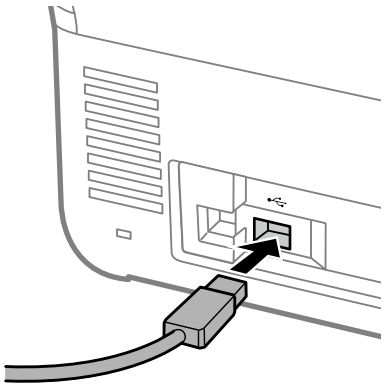
*2 Ja jums nepieciešams izmantot konkrētus kartes vietas datus nevis kartes standarta ID kā autentifikācijas ID, konfigurējot produkta iestatījumus, lūdzu, sazinieties ar Epson partneri vai vietējo pārstāvi, lai iegūtu papildinformāciju par to, kā iestatīt produktu.

Autentifikācijas ierīces pievienošana

Svarīga informācija:

Pievienojot autentifikācijas ierīci vairākiem skeneriem, izmantojiet produktu ar identisku modeļa numuru.

Savienojiet karšu lasītāja USB kabeli ar ārējās saskarnes USB portu uz skenera.



Autentifikācijas ierīces darbības pārbaude

Savienojuma statusu un autentifikācijas ierīces autentifikācijas kartes atpazīšanu varat pārbaudīt no skenera vadības paneļa.

Informācija būs redzama, ja atlasīsit **Iestatījumi** > **Ierīces informācija** > **Autentifikācijas ierīces statuss**.

Autentifikācijas ierīces iestatījumi

Iestatiet no autentifikācijas kartes saņemtās autentifikācijas informācijas lasīšanas formātu.

Jūs varat iestatīt turpmāko autentifikācijas ierīces lasīšanas metodi.

❏ Lasīt konkrētu autentifikācijas kartes vietu, piemēram, darbinieka numuru vai personas kodu.

❏ Izmantot autentifikācijas kartes informācijas, izņemot UID (autentifikācijas kartes informāciju, piemēram, sērijas numuru).

Varat izmantot rīku, lai ģenerētu darbības parametrus. Papildinformāciju jautājiet savam izplatītājam.

Piezīme:
Atšķirīgu ražotāju autentifikācijas karšu izmantošana:

Izmantojot UID kartes informāciju (kartes ID informāciju, piemēram, sērijas numuru), jūs varat izmantot dažādu veidu autentifikācijas kartes. Šo iespēju nevar izmantot, ja izmantojat citu kartes informāciju.

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Device Management** > **Card Reader**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Administrator Settings** > **Authentication Settings** > **Card Reader**.

Vienums	Skaidrojums
Vendor ID	Iestatiet autentifikācijas ierīces piegādātāja ID, kas ierobežo izmantošanu, no 0000 līdz FFFF, izmantojot 4 burtciparu rakstzīmes. Ja nevēlaties ierobežot, ievadiet 0000.
Product ID	Iestatiet autentifikācijas ierīces produkta ID, kas ierobežo izmantošanu, no 0000 līdz FFFF, izmantojot 4 burtciparu rakstzīmes. Ja nevēlaties ierobežot, ievadiet 0000.
Operational parameter	Iestatiet autentifikācijas ierīces darbības parametru robežās no 0 līdz 8192 rakstzīmēm. A~Z, a~z, 0~9, +, /, =,atstarpe, un rindiņas padeve ir pieejami.
Card Reader	Atlasiet autentifikācijas ierīces pārvēršanas formātu. Jūs varat pārbaudīt formāta informāciju. Skatiet vienuma aprakstā sniegto saiti.
Authentication Card ID save format	Atlasiet ID kartes autentifikācijas informācijas pārvēršanas formātu. Jūs varat pārbaudīt formāta informāciju. Skatiet vienuma aprakstā sniegto saiti.
Set card ID range	Iespējojiet lasīšanas pozīcijas specifikācijas.
Text Start Position	Norādiet teksta sākuma pozīciju, lai nolasītu ID informāciju. Varat norādīt no 1 līdz 4096.
Number of Characters	Norādiet rakstzīmju skaitu, kas nolasāms no ID informācijas sākuma pozīcijas. Varat norādīt no 1 līdz 4096.

Reģistrēšanas un iestatīšanas informācija

Iestatīšana

Veiciet nepieciešamos iestatījumus atkarībā no izmantotās Authentication Method un skenēšanas metodes.

Svarīga informācija:

Pirms sākt iestatīšanu, pārbaudiet, vai skenera laika iestatījums ir pareizs.

Ja laika iestatījums ir nepareizs, būs redzams kļūdas ziņojumus „Licences derīguma termiņš ir beidzies", kas var būt iemesls kāpēc neizdodas skenera iestatīšana. Turklāt, lai izmantotu tādas drošības funkcijas kā SSL/TLS sakari vai IPsec, laika iestatījumam jābūt pareizam. Laiku var iestatīt kā norādīts turpmāk.

❏ *Cilnē Web Config:* ***Device Management*** > ***Date and Time*** > ***Date and Time****.*

❏ *Skenera vadības panelī:* ***Iestatījumi*** > ***Pamatiestatījumi*** > ***Datuma/laika iestatījumi****.*

Iestatījumi	Local DB	LDAP	Local DB and LDAP
Autentifikācijas iespējošana Pirms veikt autentifikācijas iestatījumus, jāiespējo autentifikācija. "Autentifikācijas iespējošana" 134. lpp.	✓	✓	✓
Authentication Settings Authentication Method iestatīšana un, kā autentificēt lietotāju. "Authentication Settings" 134. lpp.	✓	✓	✓
User Settings reģistrēšana Reģistrējiet iestatījumus katram lietotājam. Varat reģistrēt vairākus lietotājus, izmantojot CSV failu. "User Settings reģistrēšana" 135. lpp.	✓	–	✓
Sinhronizēšana ar LDAP Server Veiciet LDAP servera sinhronizācijas iestatījumus. "Sinhronizēšana ar LDAP Server" 142. lpp.	–	✓	✓
Email Server iestatīšana Veiciet e-pasta servera iestatījumus. Iestatiet tos, izmantojot funkcijas, kas pieprasa e-pasta servera iestatījumus, piemēram, Scan to My Email. "E-pasta servera iestatīšana" 145. lpp.	✓	✓	✓
Scan to My Folder iestatīšana Iestatiet mērķa mapes. Iestatiet, kad izmantojat funkciju Scan to My Folder. "Scan to My Folder iestatīšana" 146. lpp.	✓	✓	✓

Iestatījumi	Local DB	LDAP	Local DB and LDAP
Customize One-touch Functions Iestatiet, kad mainīt skenera vadības panelī attēlotos vienumus. Varat vadības panelī attēlot tikai nepieciešamās ikonas, vai mainīt ikonu izkārtojumu. "Customize One-touch Functions" 148. lpp.	✓	✓	✓

Autentifikācijas iespējošana

Pirms veikt autentifikācijas iestatījumus, jāiespējo autentifikācija.

Iestatīšana, izmantojot Web Config:

Atlasiet **Ieslēgts (ierīce/LDAP serveris)** cilnē **Product Security** > **Basic** > **Authentication**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Ieslēgts (ierīce/LDAP serveris)** no **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Piezīme:
Ja skenerī iespējosiet Authentication Settings, vadības panelim arī tiks iespējots Bloķēšanas iestatījums. Vadības paneli nevar atbloķēt, kad Authentication Settings ir iespējoti.

Pat, ja atspējosit Authentication Settings, Bloķēšanas iestatījums paliek iespējoti. Ja vēlaties tos atspējot, šos iestatījumus varat veikt no vadības paneļa vai Web Config.

Saistītā informācija

➡ "Bloķēšanas iestatījums iestatīšana, izmantojot vadības paneli" 86. lpp.
➡ "Bloķēšanas iestatījums iestatīšana, izmantojot Web Config" 86. lpp.

Authentication Settings

Authentication Method iestatīšana un, kā autentificēt lietotāju.

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Product Security** > **Authentication Settings**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Administrator Settings** > **Authentication Settings** > **Authentication Settings**.

Vienums	Skaidrojums
Authentication Method	Atlasiet Authentication Method. ❏ Local DB Autentifikācija, izmantojot skenerī reģistrētos User Settings. Ir nepieciešams skenerī reģistrēt lietotāju. ❏ LDAP Autentificēt, izmantojot ar skeneri sinhronizētā LDAP serverī esošo lietotāja informāciju. Vispirms jākonfigurē LDAP servera iestatījumi. ❏ Local DB and LDAP Autentificēt, izmantojot skenerī reģistrēto vai ar skeneri sinhronizētā LDAP serverī esošo lietotāja informāciju. Jums jāreģistrē lietotājs skenerī un jāiestata LDAP serveris.
How to Authenticate User	Atlasiet, kā autentificēt lietotāju. ❏ Card or User ID and Password Lietotāju autentifikācijai izmantot autentifikācijas karti. Autentifikācija varat izmantot arī lietotāja ID un paroli. ❏ User ID and Password Lietotāju autentifikācijai izmantot lietotāja ID un paroli. Izvēloties šo funkciju, nevarēsiet autentifikācijai izmantot autentifikācijas karti. ❏ User ID Lietotāju autentifikācijai, izmantot tikai lietotāja ID. Nav nepieciešams iestatīt paroli. ❏ Card or ID Number Lietotāju autentifikācijai izmantot autentifikācijas karti. Varat izmantot arī ID Number. ❏ ID Number Lietotāju autentifikācijai, izmantot tikai ID numuru.
Allow users to register authentication cards	Iespējojiet to, ja atļaujat lietotājiem reģistrēt autentifikācijas karti sistēmā. Atlasot **LDAP** kā **Authentication Method**, jūs nevarat to iestatīt. Papildinformācija par to, kā lietotāji var reģistrēt savas autentifikācijas kartes, skatiet *Lietotāja rokasgrāmata* sadaļā „Autentifikācijas kartes reģistrēšana".
The Minimum Digit Number of ID Number	Atlasiet minimālo ID numura ciparu skaitu.
Caching for LDAP authenticated users	Autentifikācijai izmantojot LDAP serveri, varat iestatīt vai izmantot vai neizmantot kešatmiņu lietotāja informācijai.
Use user information in SMTP authentication	Autentifikācijai izmantojot lietotāja ID un paroli, varat iestatīt vai izmantot vai neizmantot lietotāja informāciju SMTP autentifikācijai. Sistēma izmanto pēdējā pieteikušā lietotāja ID un paroli.
Restrictions for LDAP authenticated users	Izmantojot LDAP, varat iestatīt lietotājam pieejamās funkcijas.

User Settings reģistrēšana

Reģistrējiet lietotāja autentifikācijai paredzētos User Settings. Varat reģistrēties izmantojot vienu no turpmāk norādītajām metodēm.

❏ Reģistrēt User Settings vienu pēc otra (Web Config)

❏ Reģistrēt vairākus User Settings kā pakotni, izmantojot CSV failu (Web Config)

❏ Reģistrēt User Settings vairākos skeneros kā pakotni, izmantojot konfigurācijas veidni (Epson Device Admin)

Saistītā informācija

➡ "User Settings individuāla (Web Config) reģistrēšana" 136. lpp.

➡ "Vairāku User Settings reģistrēšana, izmantojot CSV failu (Web Config)" 137. lpp.

➡ "Reģistrēt User Settings vairākos skeneros kā pakotni (Epson Device Admin)" 140. lpp.

User Settings individuāla (Web Config) reģistrēšana

Atveriet Web Config un atlasiet cilni **Product Security** > **User Settings** > **Add**, pēc tam ievadiet User Settings.

Vienums	Skaidrojums
User ID	Ievadiet lietotāja ID, ko vēlaties autentificēt, izmantojot 1 līdz 83 baitus, kas izsakāmi Unicode (UTF-8) formātā. Tā kā lietotāja ID nav reģistrjutīgs, jūs varat pieteikties, izmantojot gan lielos, gan mazos burtus.
User name Display	Ievadiet skenera vadības panelī redzamo lietotāja nosaukumu, izmantojot līdz 32 rakstzīmēm, kas izsakāmas Unicode (UTF-16) formātā. Varat atstāt šo lauku tukšu.
Password	Lai autentificētos ievadiet vēlamo paroli, izmantojot līdz 32 rakstzīmēm ASCII formātā. Parole ir reģistrjutīga. Atstājiet šo lauku tukšu, ja atlasījāt **User ID How to Authenticate User**.
Authentication Card ID	Ievadiet autentifikācijas kartes ID, izmantojot līdz 116 rakstzīmēm ASCII formātā. Varat atstāt šo lauku tukšu. Kad atļauts **Allow users to register authentication cards Authentication Settings**, atspoguļoti tiek reģistrēto lietotāju rezultāti.
ID Number	Šis vienums redzams, kad **Card or ID Number** vai **ID Number** ir atlasīts **Authentication Settings** > **How to Authenticate User**. Ievadiet numuru, kas ir robežās starp iestatīto numuru **Authentication Settings** > **The Minimum Digit Number of ID Number** un līdz 8 cipariem.
Auto Generate	Šis vienums redzams, kad **Card or ID Number** vai **ID Number** ir atlasīts **Authentication Settings** > **How to Authenticate User**. Noklikšķiniet, lai automātiski ģenerētu ID numuru ar vienādiem cipariem, kurus atlasījāt **The Minimum Digit Number of ID Number**.
Department	Ievadiet nodaļas nosaukumu un citu informāciju, kas identificē lietotāju, izmantojot līdz 40 rakstzīmēm Unicode (UTF-16) formātā. Varat atstāt šo lauku tukšu.
Email Address	Ievadiet lietotāja e-pasta adresi, izmantojot līdz 200 rakstzīmēm ASCII formātā. Tiek izmantots kā mērķis, izvēloties **Scan to My Email**. Varat atstāt šo lauku tukšu.
Scan to My Folder	Iestatiet saglabāšanas vietas individuāli, atlasot **Individual Scan to My Folder** > **Setting Type**. Skatiet turpmāk minēto papildinformāciju par iestatījuma vienumiem. "Scan to My Folder iestatīšana" 146. lpp.

Vienums	Skaidrojums
Restrictions	Katra lietotāja funkcijas var ierobežot. Atlasiet funkciju, kuru atļaujat izmantot.
Presets	Varat veikt līdz pieciem sākotnējiem iestatījumiem, kas pieejami tikai konkrētam skenerī reģistrētam lietotājam, izmantojot Presets. ❏ Presets, kas piešķirti lietotājam, var izmantot tikai šis lietotājs. Presets, kas nav piešķirti nevienam lietotājam, var izmantot visi lietotāji. ❏ Ja lietotājam pieejams tikai viens Presets, pēc autentifikācijas tas automātiski tiek ielādēts. Ja pieejami vairāki Presets pēc autentifikācijas tiks attēlots Presets saraksts. ❏ Nevarat izveidot vai attēlot Presets, kas izmanto sadaļā **Restrictions** ierobežotās funkcijas.

Vairāku User Settings reģistrēšana, izmantojot CSV failu (Web Config)

Ievadiet katra lietotāja iestatījumus CSV failā un reģistrējiet tos kā pakotni.

CSV faila izveidošana

Izveidojiet CSV failu, lai importētu User Settings.

Piezīme:
Ja iepriekš izveidojat vienu vai vairākus User Settings un pēc tam eksportējat formatētu failu (CSV failu), varat izmantot reģistrēto iestatījumu kā atsauci iestatījuma vienumu ievadīšanai.

1. Atveriet programmu Web Config un atlasiet cilni **Product Security** > **User Settings**.
2. Noklikšķiniet uz **Export**.
3. Atlasiet faila formātu **File Format**.

   Atlasiet to, skatot informāciju turpmāk.

Vienums	Skaidrojums
CSV UTF-16 (Tab delimited)	Atlasiet, ja rediģēsit failu, izmantojot Microsoft Excel. Katru parametru iekļauj „[ ]" (iekavas). Ievadiet parametrus „[ ]". Ja atjaunināt failu, iesakām faila pārrakstīšanu. Ja saglabājat failu no jauna, atlasiet Unicode tekstu (*.txt) kā faila formātu.
CSV UTF-8 (Comma delimited)	Atlasiet, ja rediģēsit failu, izmantojot teksta redaktoru vai macro, neizmantojot Microsoft Excel.
CSV UTF-8 (Semicolon delimited)	

4. Noklikšķiniet uz **Export**.

5. Rediģējiet un saglabājiet CSV failu izklājlapu lietojumprogrammā, piemēram, Microsoft Excel vai teksta redaktorā.

> ***Svarīga informācija:***
> *Rediģējot failu, nemainiet kodējumu vai virsraksta informāciju.*

CSV faila vienumu iestatīšana

Vienums	Iestatījumi un skaidrojums
UserID	Lai autentificētos ievadiet lietotāja ID no 1 līdz 83 baitiem Unicode formātā.
UserName	Ievadiet skenera vadības panelī redzamo lietotāja nosaukumu, izmantojot līdz 32 rakstzīmēm Unicode formātā. Varat atstāt šo lauku tukšu.
Password	Lai autentificētos ievadiet paroli, izmantojot līdz 32 rakstzīmēm ASCII formātā. Importējot, šī tiek iestatīta kā parole nevis **EncPassword**. Atstājiet šo lauku tukšu, ja atlasījāt **User ID How to Authenticate User**. Eksportējot, šis lauks vienmēr ir tukšs.
AuthenticationCardID	Iestatiet autentifikācijas kartes lasīšanas rezultātu. Kad atļauts **Allow users to register authentication cards Authentication Settings**, atspoguļoti tiek reģistrēto lietotāju rezultāti. Ievadiet līdz 116 rakstzīmēm ASCII formātā. Varat atstāt šo lauku tukšu.
IDNumber	Šis vienums redzams, kad **Card or ID Number** vai **ID Number** ir atlasīts **Authentication Settings** > **How to Authenticate User**. Ievadiet numuru, kas ir robežās starp iestatīto numuru **Authentication Settings** > **The Minimum Digit Number of ID Number** un līdz 8 cipariem. ID numuru nevar dublēt. Ja to dublē, saņemsit brīdinājuma kļūdu, importējot failu. Atstājot lauku tukšu, numurs tiek piešķirts automātiski.
Department	Ievadiet nodaļas nosaukuma pieņēmumu, lai atšķirtu lietotājus. Ievadiet līdz 40 rakstzīmēm Unicode formātā. Varat atstāt šo lauku tukšu.
MailAddress	Iestatiet lietotāju e-pasta adresi. Tiek izmantots kā mērķis, izvēloties **Scan to My Email**. Varat izmantot A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Ievadiet līdz 200 rakstzīmēm vai mazāk. Pirmā rakstzīme nedrīkst būt „,” (komats). Varat atstāt šo lauku tukšu.
FolderProtocol	Iestatiet funkcijas Scan to My Folder veidu. Tīkla mape/FTP (SMB): 0, FTP: 1
FolderPath	Iestatiet funkcijas Scan to My Folder saglabāšanas mērķi.
FolderUserName	Iestatiet funkcijas Scan to My Folder lietotājvārdu.
FolderPassword	Iestatiet mērķa mapes autentifikācijas paroli funkcijai Scan to My Folder, izmantojot ne vairāk kā 32 rakstzīmes ASCII formātā. Importējot, šī tiek iestatīta kā parole nevis **EncPassword**. Eksportējot, šis lauks vienmēr ir tukšs.
FtpPassive	Iestatiet FTP servera savienojuma režīmu, kad **FTP** ir atlasīts kā **Type** Scan to My Folder funkcijai. Aktīvs režīms: 0, Pasīvs režīms: 1

Vienums	Iestatījumi un skaidrojums
FtpPort	Iestatiet porta numuru skenēto datu nosūtīšanai uz FTP serveri no 0 līdz 65535, kad **FTP** ir atlasīts kā **Type** Scan to My Folder funkcijai.
ScanToMemory	Iestatiet ierobežojumus Scan to USB Drive. Nav atļauts: 0, Atļauts: 1
ScanToMail	Iestatiet ierobežojumus Scan to Email. Varat iestatīt **Skenēt uz e-pastu** tikai, ja iespējots **Scan to Email**. Nav atļauts: 0, Atļauts: 1
ScanToFolder	Iestatiet ierobežojumus Scan to Network Folder/FTP. Varat iestatīt **Skenēt uz manu mapi** tikai, ja iespējots **Scan to Network Folder/FTP**. Nav atļauts: 0, Atļauts: 1
ScanToCloud	Iestatiet ierobežojumus Scan to Cloud. Nav atļauts: 0, Atļauts: 1
ScanToComputer	Iestatiet ierobežojumus Skenēt uz datoru. Nav atļauts: 0, Atļauts: 1
PresetIndex	Iestatiet Presets, ko vēlaties asociēt ar lietotāju. Varat iestatīt līdz pat pieciem Presets reģistrācijas numuriem, atdalot tos ar komatiem.
EncPassword	Eksportējot lietotāja iestatījumus, iestatītais parametrs **Password** ir šifrēts, un pēc tam BASE64 vērtību kodē un izvada. Importējot ar jaunu paroli **Password**, šī vērtība tiek ignorēta. Ja lauks **Password** ir tukšs, izmantota tiek šī vērtība un parole ir tāda pati kā pirms eksportēšanas.
EncFolderPassword	Eksportējot iestatītais parametrs **FolderPassword** ir šifrēts, un pēc tam BASE64 vērtību kodē un izvada. Importējot ar jaunu paroli **FolderPassword**, šī vērtība tiek ignorēta. Ja lauks **FolderPassword** ir tukšs, izmantota tiek šī vērtība un parole ir tāda pati kā pirms eksportēšanas.

CSV faila importēšana

1. Atveriet programmu Web Config un atlasiet cilni **Product Security** > **User Settings**.
2. Noklikšķiniet uz **Import**.
3. Atlasiet failu, kuru vēlaties importēt.
4. Noklikšķiniet uz **Import**.
5. Pēc redzamās informācijas pārbaudes, noklikšķiniet uz **OK**.

Reģistrēt User Settings vairākos skeneros kā pakotni (Epson Device Admin)

Jūs varat reģistrēt User Settings, kas tiek lietoti, Local DB kā pakotni, izmantojot LDAP serveri vai CSV/ENE failu.

Piezīme:
*ENE fails ir Epson nodrošināts binārais fails, kas šifrē un saglabā informāciju **Contacts**, piemēram, persondatus un User Settings. To var eksportēt no Epson Device Admin un jūs varat iestatīt paroli. Tas ir noderīgi, ja vēlaties importēt User Settings no dublējuma faila.*

Importēšana no CSV/ENE faila

1. Konfigurācijas veidnē atlasiet **Administrator Settings** > **Authentication Settings** > **User Settings**.
2. Noklikšķiniet uz **Import**.
3. Sadaļā **Import Source** atlasiet **CSV or ENE File**.
4. Noklikšķiniet uz **Browse**.

   Tiek parādīts faila atlases ekrāns.
5. Atlasiet failu, kuru vēlaties importēt, lai to atvērtu.
6. Atlasiet importēšanas metodi.
   - ❏ Overwrite and Add: pārraksta, ja eksistē tāds pats lietotāja ID; pievieno jaunu ID, ja neeksistē.
   - ❏ Replace All: aizvieto visu ar lietotāja iestatījumiem, ko importējat.
7. Noklikšķiniet uz **Import**.

   Tiek parādīts iestatījumu apstiprinājuma ekrāns.
8. Noklikšķiniet uz **OK**.

   Tiek parādīts validācijas rezultāts.

   Piezīme:
   - ❏ *Ja importējamo lietotāja iestatījumu skaits pārsniedz skaitu, ko var importēt, būs redzams ziņojums, kas aicinās dzēst dažus lietotāja iestatījumus. Dzēsiet jebkādus liekos lietotāja iestatījumus pirms importēšanas.*
   - ❏ *Atlasiet lietotāja iestatījumus, ko vēlaties dzēst pirms importēšanas, un noklikšķiniet uz **Delete**.*
9. Noklikšķiniet uz **Import**.

   Konfigurācijas veidnē tiek importēti lietotāja iestatījumi.

Importēšana no LDAP servera

1. Konfigurācijas veidnē atlasiet **Administrator Settings** > **Authentication Settings** > **User Settings**.
2. Noklikšķiniet uz **Import**.
3. Sadaļā **Import Source** atlasiet **LDAP**.

4. Noklikšķiniet uz **Settings**.

   Tiek parādīti **LDAP Server** iestatījumi.

   Piezīme:
   Šis LDAP servera iestatījums ir lietotāja iestatījumu importēšanai no LDAP servera. Importētie (kopētie) lietotāja iestatījumi tiek izmantoti, lai autentificētu lietotājus, izmantojot skeneri.

   *Taču, atlasot **LDAP** vai **Local DB and LDAP** kā autentifikācijas metodi, lietotāji tiek autentificēti, sazinoties ar LDAP serveri.*

5. Iestatiet katru vienumu.

   Importējot lietotāja iestatījumus no LDAP servera, varat arī konfigurēt turpmākos iestatījumus papildus LDAP iestatījumiem.

   Papildinformāciju skatiet sadaļā „Saistītā informācija”.

Vienums			Skaidrojums
LDAP Server Settings	LDAP Server Type		Ļauj atlasīt LDAP servera veidu.
Search Settings	Search Filter		Varat iestatīt tekstu, ko izmantot LDAP meklēšanas filtram. Atlasiet **Custom**, lai rediģētu meklēšanas tekstu.
	Options	Type	Varat iestatīt saglabāšanas vietas veidu **Scan To My Folder**.
		Connection Mode	Kad **Type** ir iestatīts uz **FTP**, varat iestatīt FTP savienojuma režīmu.
		Port Number	Kad **Type** ir iestatīts uz **FTP**, varat iestatīt porta numuru, ko vēlaties izmantot.

6. Pēc nepieciešamības veiciet savienojuma testēšanu, noklikšķinot uz **Connection Test**.

   Iegūst un attēlot 10 lietotāja iestatījumus no LDAP servera.

7. Noklikšķiniet uz **OK**.

8. Atlasiet importēšanas metodi.

   ❏ Overwrite and Add: pārraksta, ja eksistē tāds pats lietotāja ID; pievieno jaunu ID, ja neeksistē.

   ❏ Replace All: aizvieto visu ar lietotāja iestatījumiem, ko importējat.

9. Noklikšķiniet uz **Import**.

   Tiek parādīts iestatījumu apstiprinājuma ekrāns.

10. Noklikšķiniet uz **OK**.

    Tiek parādīts validācijas rezultāts.

11. Noklikšķiniet uz **Import**.

    Konfigurācijas veidnē tiek importēti lietotāja iestatījumi.

Saistītā informācija

➡ "LDAP servera konfigurēšana" 142. lpp.

➡ "LDAP servera meklēšanas iestatījumu konfigurēšana" 143. lpp.

Sinhronizēšana ar LDAP Server

Izveidojiet LDAP Server iestatījumus skenerim.

Pēc nepieciešamības izveidojiet iestatījumus gan primārajam serverim, gan sekundārajam.

Piezīme:
LDAP Server *iestatījumi tiek koplietoti ar* ***Contacts****.*

PPPPieejami pakalpojumi

Šādi direktorija pakalpojumi tiek atbalstīti.

Pakalpojuma nosaukums	Versija
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

LDAP servera konfigurēšana

Lai izmantotu LDAP serveri, jākonfigurē LDAP serveris.

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Network** > **LDAP Server** > **Basic (Primary Server)** vai **Basic (Secondary Server)**.

Atlasot **Kerberos Authentication** kā **Authentication Method**, atlasiet **Network** > **Kerberos Settings**, lai veiktu Kerberos iestatījumus.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Network** > **LDAP server** > **Server Settings (Primary Server)** vai **Server Settings (Secondary Server)**.

Atlasot **Kerberos Authentication** kā **Authentication Method**, atlasiet **Network — Security** > **Kerberos Settings**, ai veiktu Kerberos iestatījumus.

Vienums	Iestatījumi un skaidrojums
Use LDAP Server	Atlasiet **Use** vai **Do Not Use**.
LDAP Server Address	Ievadiet LDAP servera adresi. Ievadiet 1–255 rakstzīmes IPv4, IPv6 vai FQDN formātā. FQDN formātā var izmantot burtciparu rakstzīmes ASCII (0x20–0x7E) formātā un defises, izņemot adreses sākumu un beigas.
LDAP server Port Number (Port number)	Ievadiet LDAP servera porta numuru — skaitli no 1 līdz 65535.
Secure Connection	Norādiet autentifikācijas metodi, kuru skeneris izmantos piekļuvei LDAP serverim.
Certificate Validation	LDAP servera sertifikāts tiek apstiprināts, kad tas ir iespējots. Iesakām šo iestatīt uz **Enable**. Lai veiktu iestatīšanu, **CA Certificate** jāimportē skenerī.

Vienums	Iestatījumi un skaidrojums
Search Timeout (sec)	Iestatiet meklēšanas laiku, pirms iestājas noildze: diapazonā no 5 līdz 300 sekundēm.
Authentication Method	Atlasiet autentifikācijas paņēmienu. Ja atlasījāt **Kerberos Authentication**, iestatiet Kerberos vispirms. Lai veiktu Kerberos Authentication, nepieciešama tālāk norādītā vide. ❏ Skeneris un DNS serveris var veikt saziņu. ❏ Skenera, KDC servera un autentifikācijai nepieciešamā servera (LDAP servera, SMTP servera, failu servera) laiks tiek sinhronizēts. ❏ Kad pakalpojumu serveris tiek piešķirts kā IP adrese, pakalpojumu servera FQDN tiek reģistrēts DNS servera reversās uzmeklēšanas apgabalā.
Kerberos Realm to be Used	Atlasot **Authentication Method** iespēju **Kerberos Authentication**, izvēlieties izmantojamo Kerberos nozarojumu.
Administrator DN / User Name	Ievadiet lietotājvārdu LDAP serverim, ne garāku par 128 unikoda (UTF-8) rakstzīmēm. Nevar izmantot kontroles rakstzīmes, piemēram, 0x00–0x1F un 0x7F. Šis iestatījums netiek izmantots, ja ir atlasīta **Anonymous Authentication** iespēja **Authentication Method**. Ja nevēlaties to norādīt, atstājiet šo lauku tukšu.
Password	Ievadiet paroli autentifikācijai LDAP serverī, ne garāku par 128 unikoda (UTF-8) rakstzīmēm. Nevar izmantot kontroles rakstzīmes, piemēram, 0x00–0x1F un 0x7F. Šis iestatījums netiek izmantots, ja ir atlasīta **Anonymous Authentication** iespēja **Authentication Method**. Ja nevēlaties to norādīt, atstājiet šo lauku tukšu.

Kerberos iestatījumi

Ja atlasāt **Kerberos Authentication** kā iestatījumu **Authentication Method**, jums jāiestata Kerberos iestatījumi. Ir iespējams reģistrēt līdz 10 Kerberos iestatījumiem.

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Network** > **Kerberos Settings**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Network** > **Security** > **Kerberos Settings**.

Vienums	Iestatījumi un skaidrojums
Realm (Domain)	Ievadiet Kerberos autentifikācijas apgabalu, ne vairāk kā 255 rakstzīmes ASCII formātā (0x20–0x7E). Ja nevēlaties to reģistrēt, atstājiet šo lauku tukšu.
KDC Address	Ievadiet Kerberos autentifikācijas servera adresi. Ievadiet ne vairāk kā 255 rakstzīmes IPv4, IPv6 vai FQDN formātā. Ja nevēlaties to reģistrēt, atstājiet šo lauku tukšu.
Port Number (Kerberos)	Ievadiet Kerberos servera porta numuru diapazonā no 1 līdz 65535.

LDAP servera meklēšanas iestatījumu konfigurēšana

Iestata meklēšanas atribūtus lietotāja iestatījumiem.

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Network** > **LDAP Server** > **Search Settings (Authentication)**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)**.

Vienums	Iestatījumi un skaidrojums
Search Base (Distinguished Name)	Norādiet sākuma stāvokli, meklējot lietotāja informāciju no LDAP servera. Ievadiet 0–128 unikoda rakstzīmes (UTF-8). Ja nevēlaties meklēt brīvi noteiktu atribūtu, atstājiet šo lauku tukšu. Lokālā servera direktorija piemērs: dc=server,dc=local
User ID Attribute	Norādiet atribūta nosaukumu, kas jāparāda, meklējot ID numuru. Ievadiet no 1 līdz 255 rakstzīmēm ASCII formātā. Pirmajai rakstzīmei jābūt a–z vai A–Z. Piemērs: cn, uid
User name Display Attribute	Norādiet atribūta nosaukumu, kas jāparāda kā lietotājvārds. Ievadiet no 0 līdz 255 rakstzīmēm ASCII formātā. Pirmajai rakstzīmei jābūt a–z vai A–Z. Varat atstāt šo lauku tukšu. Piemērs: cn, name
Authentication Card ID Attribute	Norādiet atribūta nosaukumu, kas jāparāda kā autentifikācijas kartes ID. Ievadiet no 0 līdz 255 rakstzīmēm ASCII formātā. Pirmajai rakstzīmei jābūt a–z vai A–Z. Varat atstāt šo lauku tukšu. Piemērs: cn, sn
ID Number Attribute	Norādiet atribūta nosaukumu, kas jāparāda, meklējot ID numuru. Ievadiet no 1 līdz 255 rakstzīmēm ASCII formātā. Pirmajai rakstzīmei jābūt a–z vai A–Z. Piemērs: cn, id
Department Attribute	Norādiet atribūta nosaukumu, kas jāparāda kā nodaļas nosaukums. Ievadiet no 0 līdz 255 rakstzīmēm ASCII formātā. Pirmajai rakstzīmei jābūt a–z vai A–Z. Varat atstāt šo lauku tukšu. Piemērs: ou, ou-cl
Email Address Attribute	Norādiet atribūta nosaukumu, kas jāparāda, meklējot e-pasta adreses. Ievadiet no 1 līdz 255 rakstzīmēm ASCII formātā. Pirmajai rakstzīmei jābūt a–z vai A–Z. Piemērs: mail
Save To Attribute	Norādiet atribūta nosaukumu, kas norāda uz Scan To My Folder atrašanās vietu. Ievadiet no 0 līdz 255 rakstzīmēm ASCII formātā. Piemērs: homeDirectory

LDAP servera savienojuma pārbaude

Veic LDAP servera savienojuma pārbaudi, izmantojot parametru, kas iestatīts sadaļā **LDAP Server** > **Search Settings**.

1. Atveriet programmu Web Config un atlasiet cilni **Network** > **LDAP Server** > **Connection Test**.
2. Izvēlieties **Start**.

   Tiek sākta savienojuma pārbaude. Pēc pārbaudes tiks parādīta pārbaudes atskaite.

LDAP servera savienojuma testēšanas atsauces

Ziņojumi	Skaidrojums
Connection test was successful.	Šis ziņojums tiek parādīts tad, ja savienojuma izveide ar serveri ir veiksmīga.
Connection test failed. Check the settings.	Šis ziņojums tiek parādīts tālāk norādīto iemeslu dēļ: ❏ Nepareiza LDAP servera adrese vai porta numurs. ❏ Ir iestājusies noildze. ❏ Iespēja **Do Not Use** ir atlasīta kā **Use LDAP Server**. ❏ Ja iespēja **Kerberos Authentication** ir atlasīta kā **Authentication Method**, iestatījums **Realm (Domain)**, **KDC Address** un **Port Number (Kerberos)** nav pareizs.
Connection test failed. Check the date and time on your product or server.	Šis ziņojums tiek parādīts, ja savienojuma izveide nav izdevusies, jo nesakrīt skenera un LDAP servera laika iestatījumi.
Authentication failed. Check the settings.	Šis ziņojums tiek parādīts tālāk norādīto iemeslu dēļ: ❏ Laukā **User Name** un/vai **Password** nav ievadīta pareiza informācija. ❏ Ja iespēja **Kerberos Authentication** ir atlasīta kā **Authentication Method**, laiks un datums var netikt konfigurēts.
Cannot access the product until processing is complete.	Šis ziņojums tiek parādīts, ja skeneris ir aizņemts.

E-pasta servera iestatīšana

Kad izmantojat **Scan to My Email**, iestatiet e-pasta serveri.

Piezīme:
*Varat iestatīt **Scan to My Email** tikai, ja iespējots **Scan to Email**.*

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Network** > **Email Server** > **Basic**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Common** > **Email Server** > **Mail Server Settings**.

Vienums	Iestatījumi un skaidrojums	
Authentication Method	Norādiet autentifikācijas metodi, kuru skeneris izmantos piekļuvei e-pasta serverim.	
	Off	Sazinoties ar pasta serveri, autentifikācija ir atspējota.
	SMTP AUTH	E-pasta serverim jāatbalsta SMTP autentifikācija.
	POP before SMTP	Atlasot šo vienumu, iestatiet POP3 serveri.
Authenticated Account	Ja atlasiet **SMTP AUTH** vai **POP before SMTP** kā **Authentication Method**, ievadiet autentificētā konta nosaukumu. Ievadiet no 0 līdz 255 rakstzīmēm ASCII formātā (0x20–0x7E).	
Authenticated Password	Ja atlasiet **SMTP AUTH** vai **POP before SMTP** kā **Authentication Method**, ievadiet autentificēto paroli. Ievadiet no 0 līdz 20 rakstzīmēm ASCII formātā (0x20–0x7E).	

Vienums	Iestatījumi un skaidrojums	
Sender's Email Address	Ievadiet sūtītāja e-pasta adresi. Ievadiet no 0 līdz 255 ASCII rakstzīmēm (0x20–0x7E), izņemot šīs : ( ) < > [ ] ; ¥. Pirmā rakstzīme nedrīkst būt punkts (.).	
SMTP Server Address	Ievadiet no 0 līdz 255 rakstzīmēm A–Z a–z 0–9 . -. Var izmantot IPv4 vai FQDN formātu.	
SMTP Server Port Number	Ievadiet skaitli no 1 līdz 65535.	
Secure Connection	Norādiet e-pasta servera drošā savienojuma metodi.	
	None	Atlasot **POP before SMTP** kā **Authentication Method** iestatījumu, savienojuma metode tiek iestatīta kā **None**.
	SSL/TLS	Tas ir pieejams, kad **Authentication Method** ir iestatīta kā **Off** vai „**SMTP AUTH**".
	STARTTLS	Tas ir pieejams, kad **Authentication Method** ir iestatīta kā **Off** vai „**SMTP AUTH**".
Certificate Validation	Iespējojot šo funkciju, sertifikāts tiek autentificēts. Iesakām šo iestatīt uz **Enable**.	
POP3 Server Address	Ja atlasiet **POP before SMTP** kā **Authentication Method**, ievadiet POP3 servera adresi. Ievadiet no 0 līdz 255 rakstzīmēm A–Z a–z 0–9. Var izmantot IPv4 vai FQDN formātu.	
POP3 Server Port Number	Ja atlasiet **POP before SMTP** kā **Authentication Method**, norādiet porta numuru. Ievadiet skaitli no 1 līdz 65535.	

Scan to My Folder iestatīšana

Saglabā skenētos attēlus mapē, kas piešķirta katram lietotājam. Jūs varat iestatīt tālāk norādītās mapes.

Piezīme:
*Varat iestatīt **Scan To My Folder** tikai, ja iespējots **Scan to Network Folder/FTP**.*

Saglabāt šeit iestatījums	Authentication Method	Iestatīt mapes ceļa atrašanās vietu
Norādiet vienu tīkla mapi visiem Authentication Settings, lai automātiski zem turpmāk minētās mapes izveidotu personiskas mapes, izmantojot lietotāja ID nosaukumu.	❏ Local DB ❏ LDAP ❏ Local DB and LDAP	Skenera (Scan to My Folder iestatījums)
Piešķiriet dažādas tīkla mapes atsevišķi katram lietotājam.	Local DB	Skeneris (User Settings)
	LDAP	LDAP atribūti
	Local DB and LDAP	Skeneris (User Settings) vai LDAP atribūti

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Product Security** > **Scan to Network Folder/FTP**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Administrator Settings** > **Authentication Settings** > **Scan to Network Folder/FTP** > **Scan to My Folder**.

Vienums		Skaidrojums
Save To Setting	Setting Type	❏ **Shared**: Automātiski izveidot mapi pēc lietotāja ID zem mapes ceļa vai vietrāža URL, kas norādīts **Save to**, un saglabā skenētos attēlus šajā mapē. ❏ **Individual**: Iestatiet skenēto rezultātu saglabāšanas vietu katram lietotājam. Lietotāja iestatījumos var iestatīt Local DB lietotājus. LDAP lietotāji izmanto no LDAP servera meklēšanas atribūtiem iegūtu krātuves atrašanās vietu.
	Type	Atlasiet pārraides protokolu atbilstoši skenēšanas izvades mērķim. Tīkla mapei: **Network Folder (SMB)** FTP serverim: **FTP**
	Save to	Norādiet izvades ceļu vai URL. Ievadiet līdz 160 rakstzīmēm Unicode (UTF-16).
	Connection Mode	Iestatiet, ja atlasāt **FTP Type**. Atlasiet savienojuma režīmu ar FTP serveri.
	Port Number	Iestatiet, ja atlasāt **FTP Type**. Ievadiet porta numuru, lai sūtīt skenētos datus uz FTP serveri, izmantojot 0 līdz 65535.
Authentication Settings	Setting Type	Iestatiet, ja atlasāt **Individual** kā **Setting Type Save To Setting**. Iestatiet User Name un Password, lai piekļūtu mapei. ❏ **Shared**: Izmantojiet kopēju **User Name** un **Password** visiem lietotājiem. ❏ **Individual**: Local DB lietotājiem, iestatiet **User Name** un **Password** individuāli **Lietotāja iestatījumi**. LDAP lietotājus nevar konfigurēt individuāli. **User Name** un **Password**, kas iestatīti izmantojot šo vienumu, tiek izmantoti kā pakotne.
	User Name	Ievadiet lietotāja nosaukumu, lai piekļūtu skenēšanas izvades mērķa mapei. Ievadiet līdz 30 rakstzīmēm Unicode (UTF-16). Iestatiet šo, ja izmantojat **Shared** vai LDAP serveri.
	Password	Ievadiet **User Name** atbilstošo paroli. Ievadiet līdz 20 rakstzīmēm Unicode (UTF-16). Iestatiet šo, ja izmantojat **Shared** vai LDAP serveri.

Aizliegt mainīt Scan to Network Folder/FTP mērķa mapi

Vienums	Skaidrojums
Prohibit manual entry of destination	Kad iespējots, lietotājs nevar mainīt noklusējuma mērķa mapi.

Customize One-touch Functions

Varat attēlot tikai nepieciešamās ikonas, rediģējot vadības paneļa sākuma ekrānā redzamo ikonu izkārtojumu.

Iestatīšana, izmantojot Web Config:

Atlasiet cilni **Product Security** > **Customize One-touch Functions**.

Iestatīšana, izmantojot Epson Device Admin:

Konfigurācijas veidnē atlasiet **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions**.

Piezīme:
Turpmāk minētajos gadījumos, sākuma ekrānā nav redzamas konkrētu funkciju ikonas.

❏ *Kad atlasāt funkcijas, kas nav atļautas **Restrictions** dēļ.*

❏ *Kad nav reģistrēta e-pasta adrese lietotājam, kurš pieteicies. (Scan to My Email)*

❏ *Kad nav iestatīta mērķa mape. (Scan to My Folder)*

Vienums	Skaidrojums
Maximum functions per screen	Atlasiet vadības panelī redzamo ikonu izkārtojumu. Attēli mainās atbilstoši izvēlētajam izkārtojumam.
Screen(s)	Atlasiet lapu skaitu.
Number	Atlasiet funkcijas, ko vēlaties redzēt katrai numurētajai pozīcijai.

Job History atskaites, izmantojot Epson Device Admin

Jūs varat izveidot Job History atskaiti katrai grupai un katram lietotājam, izmantojot Epson Device Admin. Skenerī jūs varat saglabāt līdz pat 3000 lietošanas gadījumu. Jūs varat izveidot atskaiti, norādot laika posmu vai iestatot regulāru grafiku.

Lai iegūtu Job History kā atskaiti, Ierīču saraksta ekrāna lentes izvēlnē atlasiet **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices**.

Papildinformācijai par to, kā izveidot lietotāja atskaiti, skatiet Epson Device Admin dokumentāciju.

Vienumi, kurus var iekļaut ziņojumā

Lietotāja ziņojumā varat iekļaut turpmāk minētos vienumus.

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

Pieteikšanās kā administratoram, izmantojot vadības paneli

Varat izmantot turpmāk norādītās metodes, lai pieteiktos kā administrators, izmantojot skenera vadības paneli.

1. Ekrāna augšējā labajā pusē pieskarieties pie  .
   - ❏ Kad iespējoti Authentication Settings ekrānā **Laipni lūdzam!** ir redzama ikona (autentifikācijas gaidstāves ekrāns).
   - ❏ Kad atspējoti Authentication Settings, sākuma ekrānā redzama ikona.
2. Pieskarieties **Jā**, kad redzams apstiprinājuma ekrāns.
3. Ievadiet administratora paroli.

   Parādās paziņojums, ka pieteikšanās ir pabeigta, un pēc tam vadības panelī redzams sākuma ekrāns.

Lai atteiktos, ekrāna augšējā labajā pusē pieskarieties pie  .

Authentication Settings atspējošana

Jūs varat atspējot Authentication Settings, izmantojot Web Config.

Piezīme:
Skenerī reģistrētie User Settings tiks saglabāti pat tad, ja Authentication Settings ir atspējoti. Tos varat noņemt, atjaunojot skenera noklusējuma iestatījumus.

1. Atveriet Web Config.
2. Atlasiet cilni **Product Security** > **Basic** > **Authentication**.
3. Atlasiet **OFF**.
4. Noklikšķiniet uz **Next**.
5. Noklikšķiniet uz **OK**.

Piezīme:
Pat, ja atspējosit Authentication Settings, Bloķēšanas iestatījums paliek iespējoti. Ja vēlaties tos atspējot, šos iestatījumus varat veikt no vadības paneļa vai Web Config.

Saistītā informācija

➡ "Bloķēšanas iestatījums iestatīšana, izmantojot vadības paneli" 86. lpp.
➡ "Bloķēšanas iestatījums iestatīšana, izmantojot Web Config" 86. lpp.

Authentication Settings informācijas dzēšana (Atjaunot noklusējuma iestatījumus)

Lai dzēstu visu Authentication Settings informāciju (Card Reader, Authentication Method, User Settings, un tā tālāk), atjaunojiet visus skenera iestatījumus uz noklusējuma iestatījumiem, kas bija aktīvi pirkuma brīdī.

Atlasiet **Iestatījumi** > **Sistēmas administrēšana** > **Atjaunot noklusējuma iestatījumus** > **Visi iestatījumi** vadības panelī.

Svarīga informācija:

Tīks dzēsti arī visi kontakti un citi tīkla iestatījumi. Dzēstos iestatījumus nevar atjaunot.

Problēmu risināšana

Nevar Nevar nolasīt autentifikācijas karti

Pārbaudiet turpmāk norādītos punktus.

❏ Pārbaudiet vai autentifikācijas ierīce ir pareizi pievienota skenerim.

Pievienojiet autentifikācijas ierīci ārējās saskarnes USB portam skenera aizmugurē.

❏ Pārbaudiet, ka autentifikācijas ierīce un karte ir atbalstītas.

Apkope

Skenera korpusa tīrīšana

Ja uz ārējā korpusa ir traipi, noslaukiet tos ar sausu drāniņu vai ar drāniņu, kas samitrināta vieglā mazgāšanas līdzeklī un ūdenī.

Svarīga informācija:

- ❏ *Skenera tīrīšanai nedrīkst lietot spirtu, atšķaidītāju vai korozīvu šķīdinātāju. Tas var izraisīt deformēšanos vai krāsas maiņu.*
- ❏ *Neļaujiet ūdenim iekļūt ierīcē. Tas var izraisīt ierīces darbības traucējumus.*
- ❏ *Nekad neatveriet skenera korpusu.*

1. Nospiediet pogu ⏻, lai izslēgtu skeneri.
2. Atvienojiet maiņstrāvas adapteri no skenera.
3. Korpusa ārpusi tīriet ar drāniņu, kas samitrināta maiga mazgāšanas līdzekļa un ūdens šķīdumā.

   Piezīme:
   Noslaukiet skārienekrānu ar mīkstu, sausu drāniņu.

Skenera iekšpuses tīrīšana

Kad skeneris kādu laiku ir lietots, papīrs un istabas putekļi uz rullīša vai stikla detaļas skenera iekšpusē var izraisīt papīra padeves vai ieskenētā attēla kvalitātes problēmas. Tīriet skenera iekšpusi ik pēc 5,000 skenēšanas reizēm.

Ieskenēto lapu skaitu var apskatīt vadības panelī vai programmā Epson Scan 2 Utility.

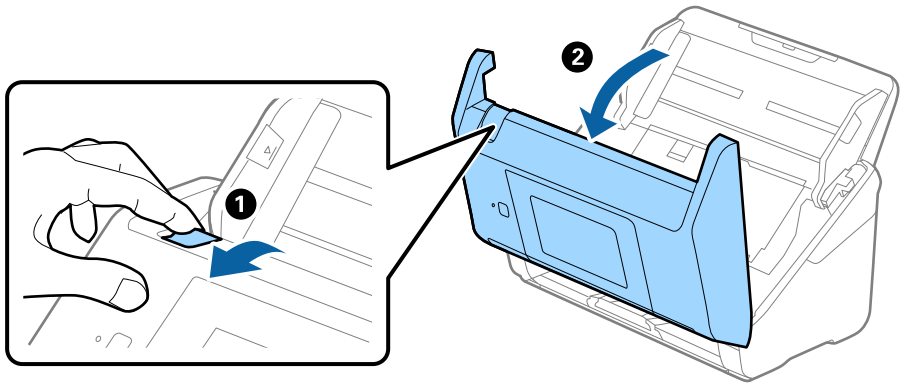
Ja virsma ir notraipīta ar grūti notīrāmu materiālu, izmantojiet autentisku Epson tīrīšanas komplektu, lai notīrītu traipus. Traipu tīrīšanai izmantojiet tīrīšanas drāniņu, kas samitrināta ar nelielu tīrīšanas līdzekļa daudzumu.

Svarīga informācija:

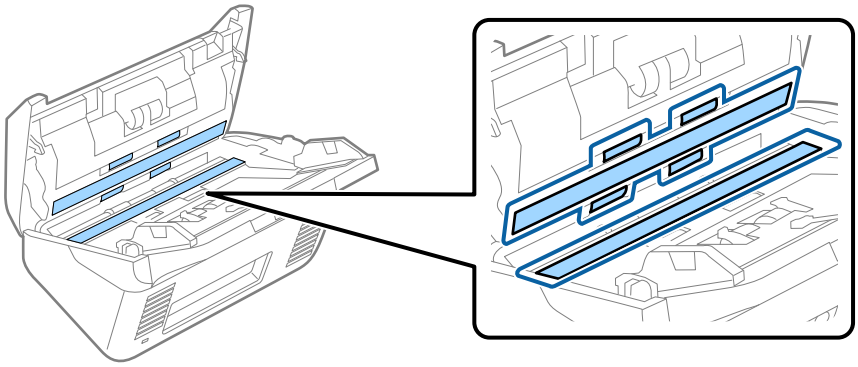
- ❏ *Skenera tīrīšanai nedrīkst lietot spirtu, atšķaidītāju vai korozīvu šķīdinātāju. Tas var izraisīt deformēšanos vai krāsas maiņu.*
- ❏ *Nekādā gadījumā neizsmidziniet uz skenera nekādus šķidrumus vai smērvielas. Aparatūras vai shēmu bojājumi var izraisīt kļūdainu ierīces darbību.*
- ❏ *Nekad neatveriet skenera korpusu.*

1. Nospiediet pogu ⏻, lai izslēgtu skeneri.
2. Atvienojiet maiņstrāvas adapteri no skenera.

3. Pavelciet sviru un atveriet skenera vāku.



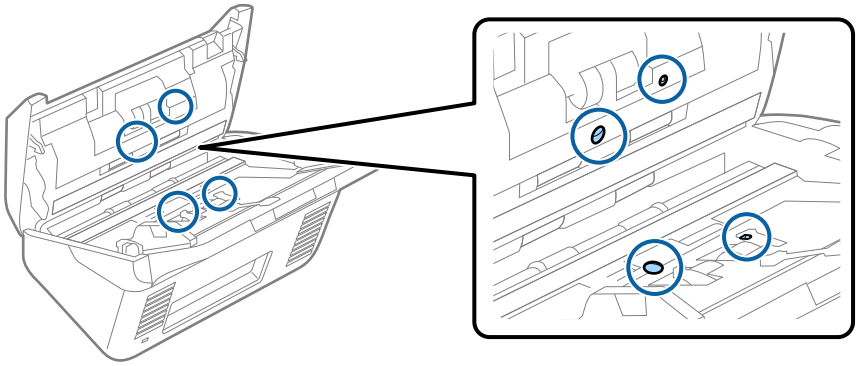
4. Ja uz plastmasas veltnīša un stikla virsmas skenera vāka iekšpusē, apakšdaļā ir traipi, noslaukiet tos ar mīkstu drāniņu vai notīriet, izmantojot autentisku Epson tīrīšanas komplektu.



Svarīga informācija:

- ❏ *Neizdariet pārāk lielu spiedienu uz stikla virsmas.*
- ❏ *Nelietojiet birsti vai cietus darbarīkus. Švīkas uz stikla virsmas var ietekmēt skenēšanas kvalitāti.*
- ❏ *Nesmidziniet tīrīšanas līdzekli tieši uz stikla virsmas.*

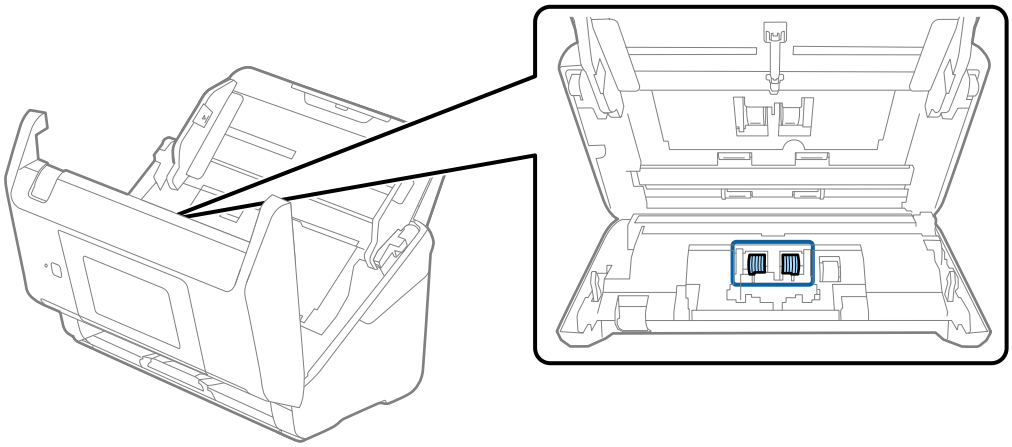
5. Ja uz sensoriem ir traipi, noslaukiet tos ar vates kociņu.



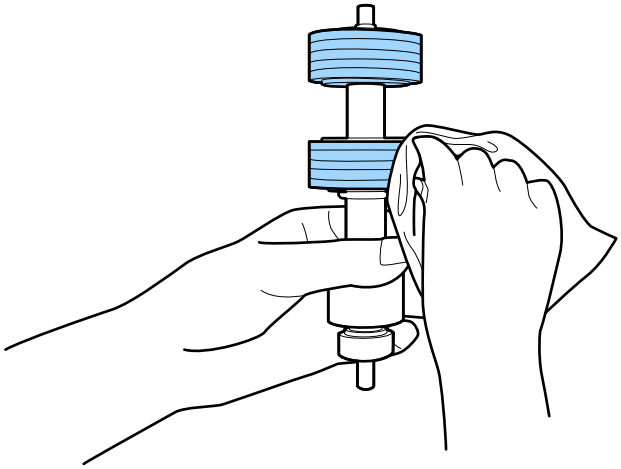
> ***Svarīga informācija:***
> *Nesamitriniet vates kociņu šķidrumā, piemēram, tīrīšanas līdzeklī.*

6. Atveriet vāku un izņemiet atdalīšanas veltnīti.

   Plašāku informāciju skatiet sadaļā „Veltnīšu bloka nomaiņa”.



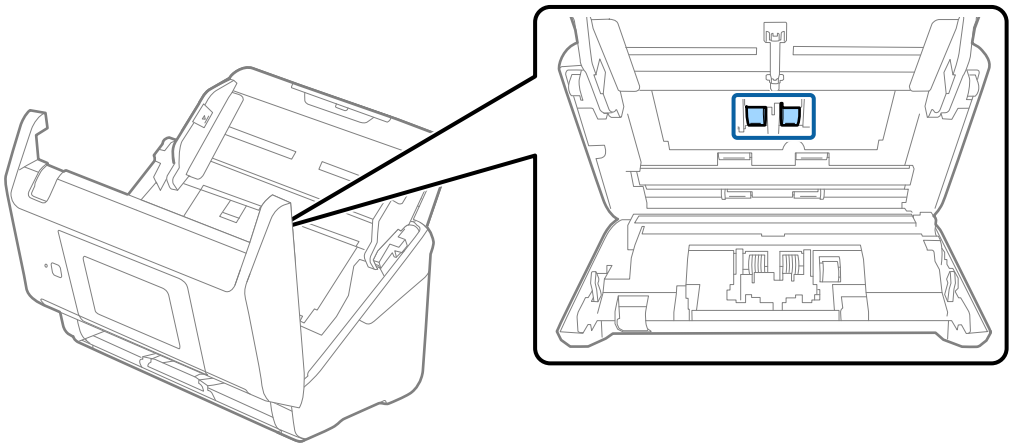
7. Ja uz atdalīšanas veltnīša ir putekļi vai netīrumi, notīriet tos, izmantojot autentisku Epson tīrīšanas komplektu vai mīkstu, samitrinātu drāniņu.



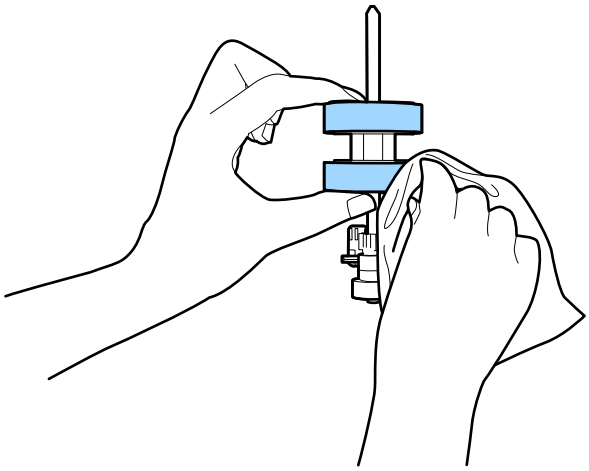
> ***Svarīga informācija:***
> *Veltnīša tīrīšanai izmantojiet tikai autentisku Epson tīrīšanas komplektu vai mīkstu, samitrinātu drāniņu. Izmantojot sausu drāniņu, var sabojāt veltnīša virsmu.*

8. Atveriet vāku un izņemiet uztveršanas veltnīti.

   Plašāku informāciju skatiet sadaļā „Veltnīšu bloka nomaiņa”.



9. Ja uz uztveršanas veltnīša ir putekļi vai netīrumi, notīriet tos, izmantojot autentisku Epson tīrīšanas komplektu vai mīkstu, samitrinātu drāniņu.



> ***Svarīga informācija:***
>
> *Veltnīša tīrīšanai izmantojiet tikai autentisku Epson tīrīšanas komplektu vai mīkstu, samitrinātu drāniņu. Izmantojot sausu drāniņu, var sabojāt veltnīša virsmu.*

10. Aizveriet skenera vāku.

11. Pievienojiet maiņstrāvas adapteri elektrotīklam un ieslēdziet skeneri.

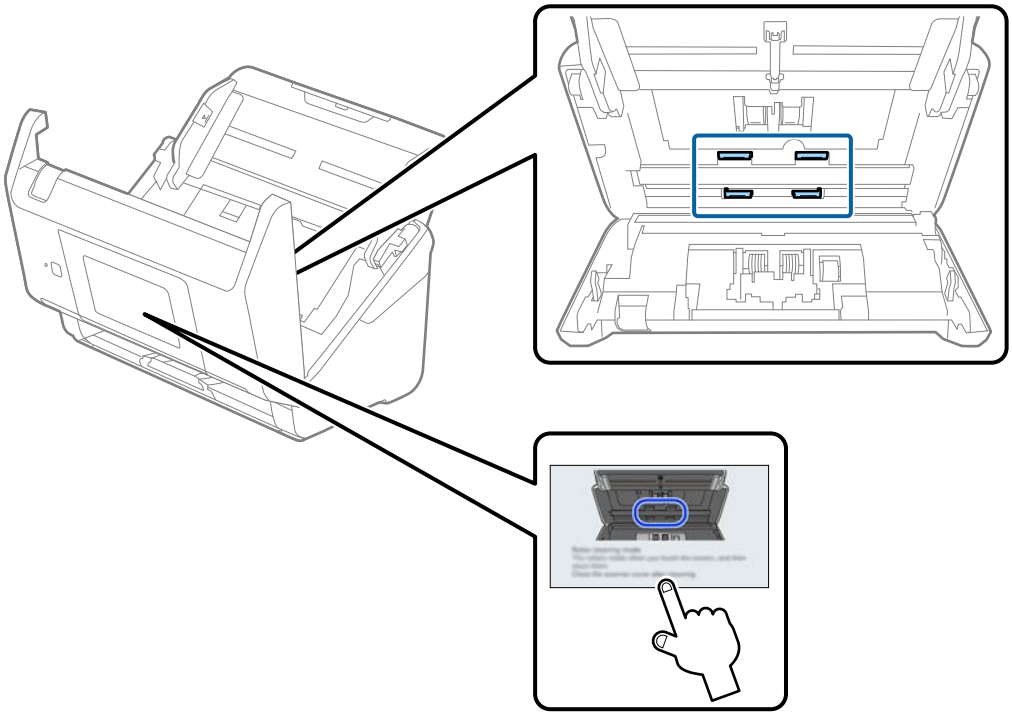
12. Sākuma ekrānā atlasiet **Skenera apkope**.

13. Ekrānā **Skenera apkope** atlasiet **Ruļļu tīrīšana**.

14. Pavelciet sviru, lai atvērtu skenera vāku.

    Skeneris aktivizē veltnīšu tīrīšanas režīmu.

15. Lēnām pagrieziet veltnīšus apakšpusē, pieskaroties jebkurā vietā šķidro kristālu displejā. Noslaukiet veltnīšu virsmu, izmantojot autentisku Epson tīrīšanas komplektu vai mīkstu, ūdenī samitrinātu drāniņu. Atkārtojiet šo darbību, līdz veltniši ir tīri.



> ***Brīdinājums:***
> *Veicot darbības ar rullīti, jāuzmanās, lai mehānismā neiestrēgtu rokas vai mati. Šādi var gūt savainojumus.*

16. Aizveriet skenera vāku.

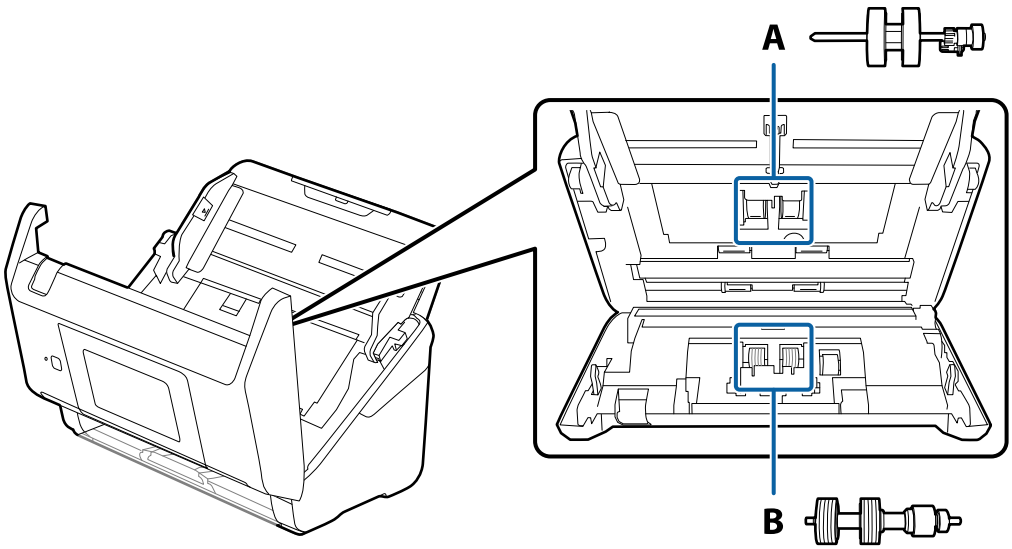
    Skeneris iziet no veltnīšu tīrīšanas režīma.

Saistītā informācija

➡ "Veltnīšu bloka nomaiņa" 157. lpp.

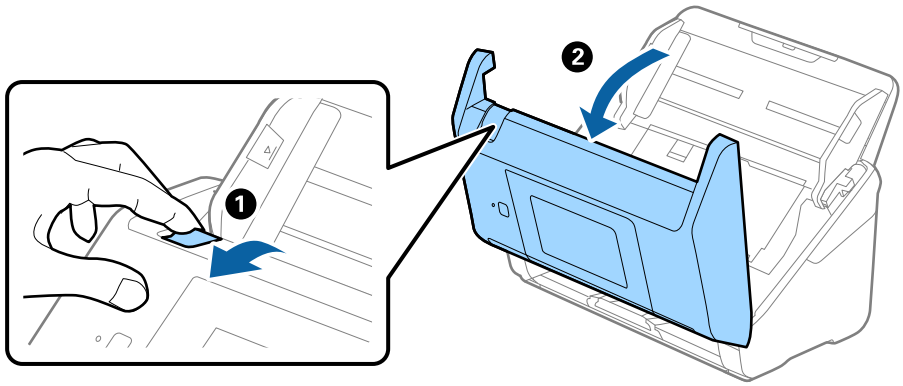
Veltnīšu bloka nomaiņa

Veltnīšu bloks (uztveršanas veltnītis un atdalīšanas veltnītis) jānomaina, kad ieskenēto lapu skaits pārsniedz veltnīšu dzīves ciklu. Kad vadības panelī vai datora ekrānā tiek parādīts ziņojums par nomaiņas nepieciešamību, veiciet turpmāk aprakstīto procedūru, lai to nomainītu.

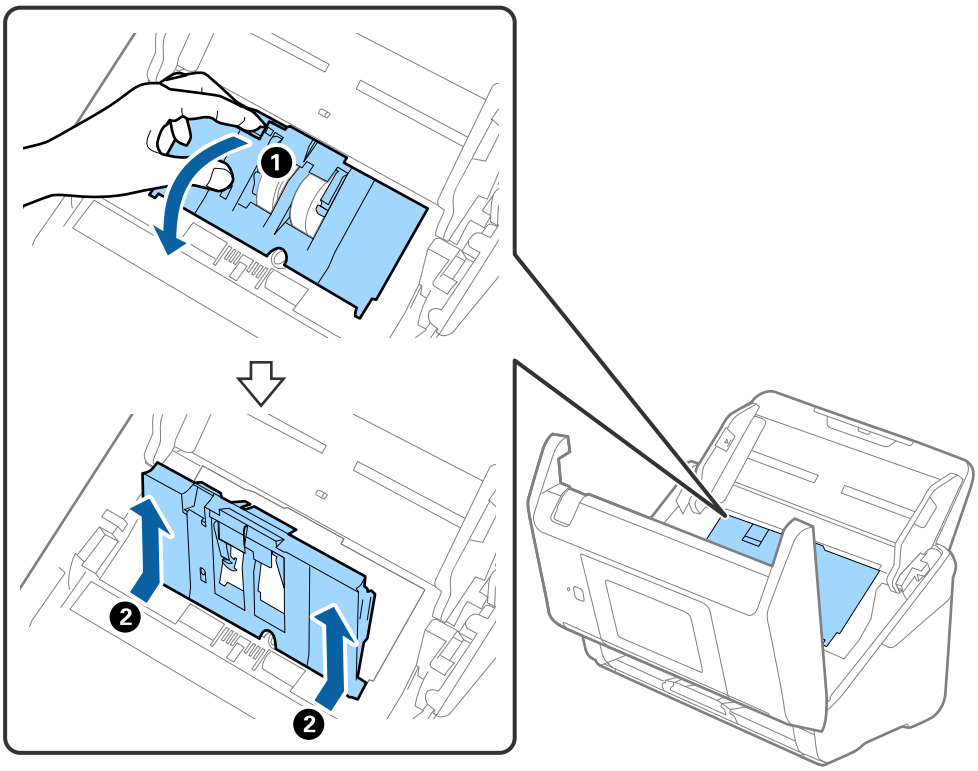


A: uztveršanas veltnītis, B: atdalīšanas veltnītis

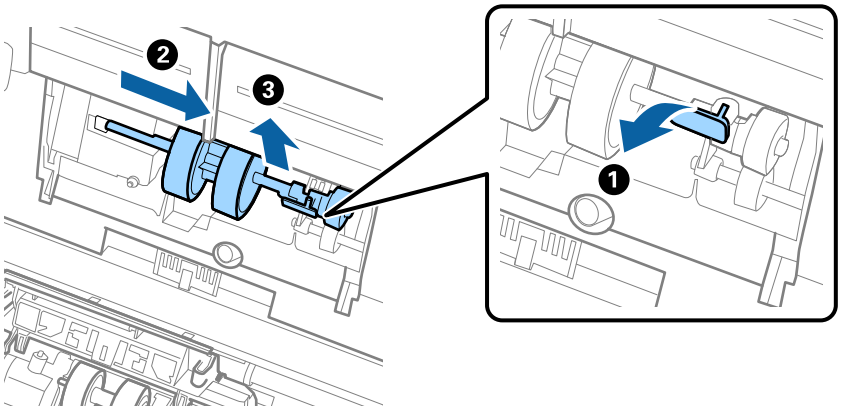
1. Nospiediet pogu ⏻, lai izslēgtu skeneri.
2. Atvienojiet maiņstrāvas adapteri no skenera.
3. Pavelciet sviru un atveriet skenera vāku.



4. Atveriet uztveršanas veltniša vāku, pēc tam izbīdiet un izņemiet to.



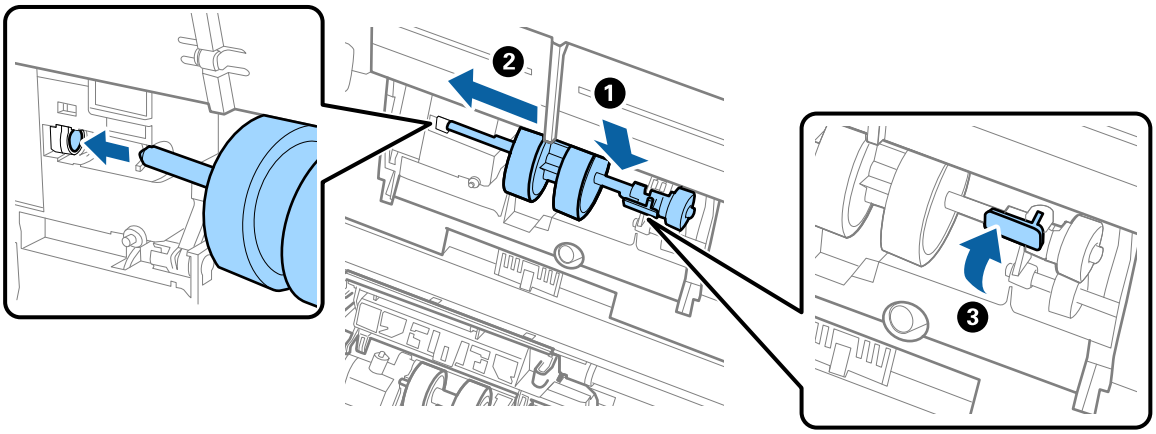
5. Pavelciet uz leju veltnīša ass armatūru, pēc tam izbīdiet un izņemiet uzstādīto uztveršanas veltnīti.



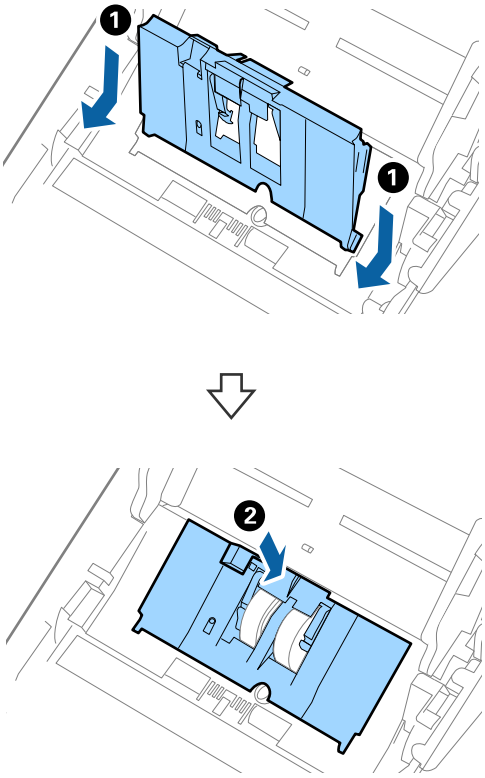
Svarīga informācija:

Velkot uztveršanas veltīti, nepielietojiet pārmērīgi lielu spēku. Tādējādi var sabojāt skenera iekšējās detaļas.

6. Turot armatūru uz leju, virzienā pa kreisi iebīdiet jauno uztveršanas veltnīti un ievietojiet to skenera atverē. Uzspiediet uz armatūras, lai to nofiksētu.

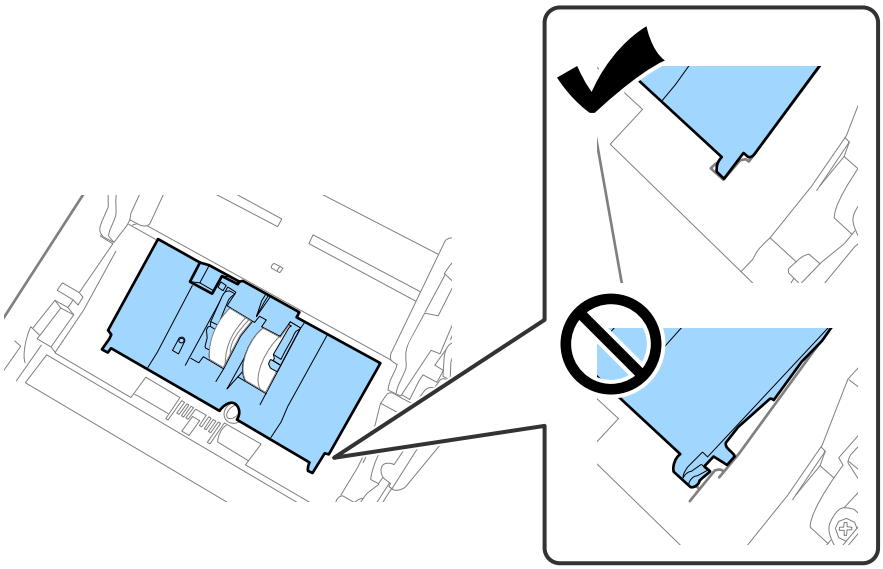


7. Ielieciet uztveršanas veltnīša vāka malu gropē un pabīdiet to. Cieši aizveriet vāku.

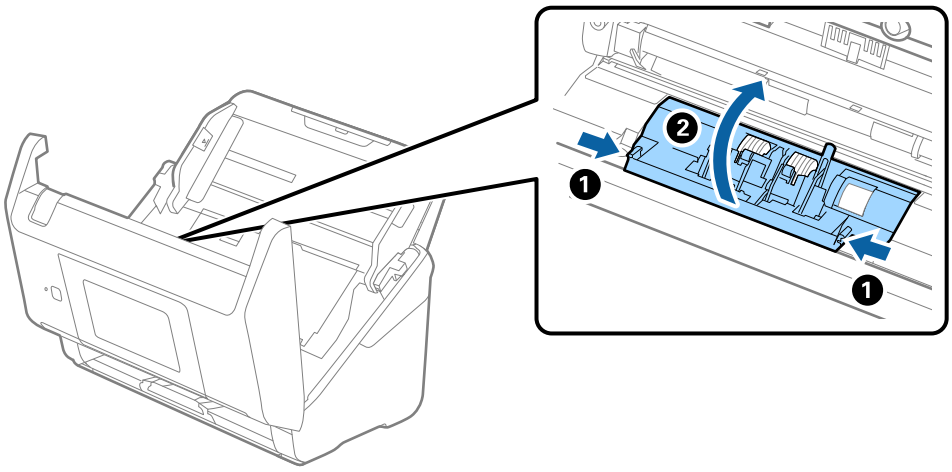


Svarīga informācija:

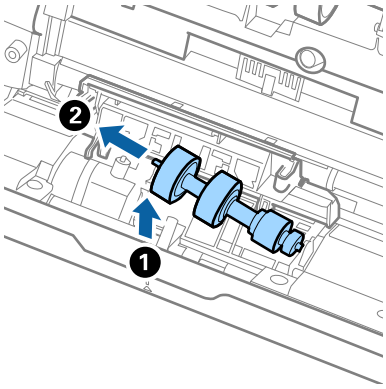
- ❏ *Gādājiet, lai uztveršanas vāks būtu pareizi aizvērts.*
- ❏ *Ja vāku ir grūti aizvērt, pārbaudiet, vai padevējrullīši ir pareizi uzstādīti.*
- ❏ *Neuzstādiet vāku atvērtā stāvoklī.*



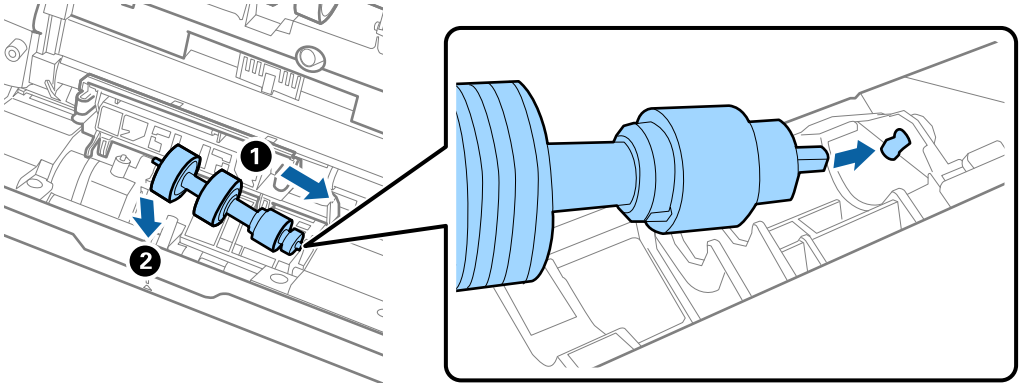
8. Atvirziet āķīšus abos atdalīšanas veltnīša vāka galos, lai atvērtu vāku.



9. Paceliet atdalīšanas veltnīša kreiso pusi, pēc tam izbīdiet un izņemiet uzstādītos atdalīšanas veltnīšus.



10. Atverē labajā pusē ievietojiet jauno atdalīšanas veltnīša asi, pēc tam nolaidiet veltnīti.



11. Aizveriet atdalīšanas veltnīša vāku.

> ***Svarīga informācija:***
> *Ja vāku ir grūti aizvērt, pārbaudiet, vai atdalīšanas veltnīši ir pareizi uzstādīti.*

12. Aizveriet skenera vāku.

13. Pievienojiet maiņstrāvas adapteri elektrotīklam un ieslēdziet skeneri.

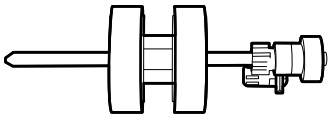
14. Vadības panelī atiestatiet ieskenēto lapu skaitu.

Piezīme:
Utilizējiet uztveršanas veltnīti un atdalīšanas veltnīti, ievērojot pašvaldības likumus un noteikumus. Neizjauciet ierīci.

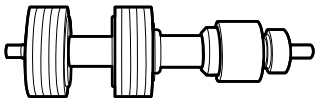
Veltnīšu bloka kodi

Detaļas (uztveršanas veltnītis un atdalīšanas veltnītis) jānomaina, kad ieskenēto lapu skaits pārsniedz apkopes intervāla skaitītāja rādījumu. Ieskenēto lapu skaitu var apskatīt vadības panelī vai programmā vai Epson Scan 2 Utility.

A



B



A: uztveršanas veltnītis, B: atdalīšanas veltnītis

Detaļas nosaukums	Kodi	Dzīves cikls
Veltnīšu bloks	B12B819671 B12B819681 (tikai Indijā)	200,000*

* Šis skaitlis noteikts, secīgi skenējot un izmantojot testēšanas nolūkiem paredzētus Epson oriģinālus, un norāda, kad veicama nomaiņa. Nomaiņas cikls atšķirties atkarībā no izmantotā papīra veida, piemēram, ja izmantots papīrs, kas rada daudz papīra putekļu vai papīrs ar raupju virsmu, kas var samazināt dzīves ciklu.

Ieskenēto lapu skaita atiestate

Atiestata ieskenēto lapu skaitu pēc veltnīšu bloka nomaiņas.

1. Sākuma ekrānā atlasiet **Iestatījumi** > **Ierīces informācija** > **Atiestatiet skenējumu skaitu** > **Skenējumu skaits pēc apkopes ruļļa nomaiņas**.

2. Pieskarieties **Jā**.

Saistītā informācija

➡ "Veltnīšu bloka nomaiņa" 157. lpp.

Enerģijas taupīšana

Laikā, kad skeneris neveic nekādas darbības, var ietaupīt enerģiju, izmantojot miega režīmu vai automātiskās izslēgšanās režīmu. Laika periodu, kuram paejot, skeneris pārslēdzas miega režīmā un automātiski izslēdzas, ir iespējams iestatīt. Vērtības palielināšana ietekmē ierīces energoefektivitāti. Pirms veicat izmaiņas, lūdzu, apsveriet, kā tās ietekmēs apkārtējo vidi.

1. Sākuma ekrānā izvēlieties **Iestatījumi**.

2. Izvēlieties **Pamatiestatījumi**.

3. Atlasiet **Izslēgšanas iest.** un pēc tam veiciet iestatījumus.

   Piezīme:
   Pieejamās funkcijas var atšķirties atkarība no pirkuma vietas.

Skenera transportēšana

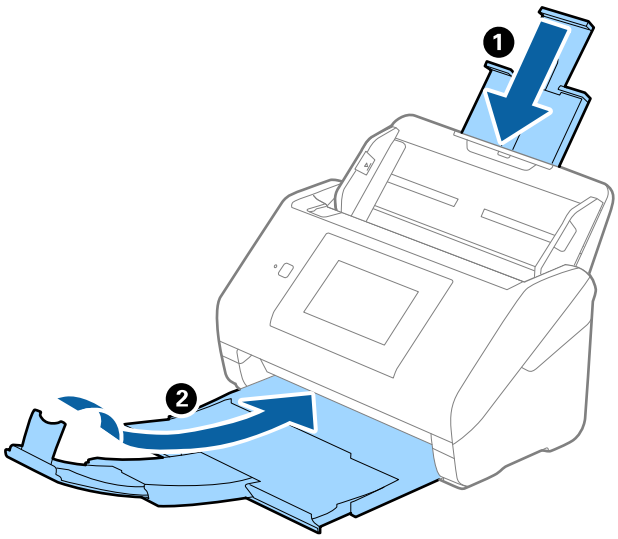
Ja jums jātransportē skeneris, pārceļoties vai nogādājot to uz remonta vietu, izpildiet turpmāk norādītās darbības skenera iepakošanai.

1. Nospiediet pogu ⏻, lai izslēgtu skeneri.

2. Atvienojiet maiņstrāvas adapteri.

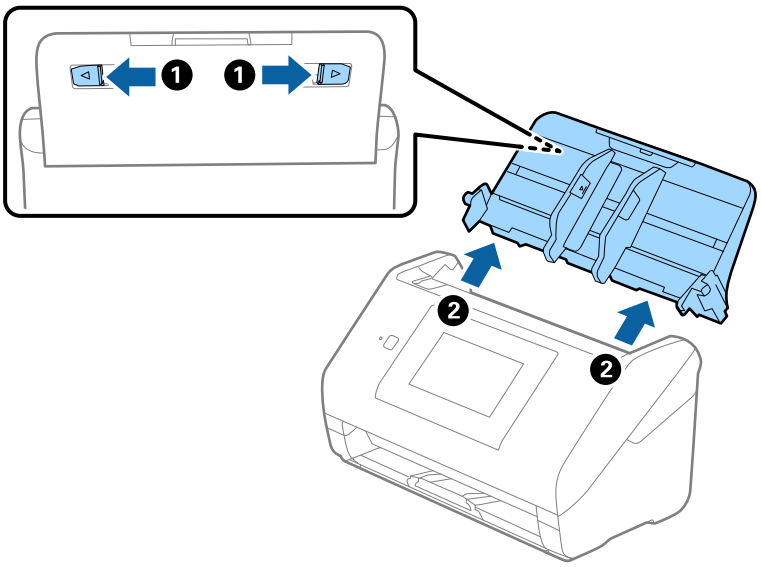
3. Noņemiet kabeļus un ierīces.

4. Aizveriet ievades paplātes pagarinātāju un izvades paplāti.



> ***Svarīga informācija:***
> *Noteikti kārtīgi aizveriet izvades paplāti; pretējā gadījumā tā var tikt bojāta transportēšanas laikā.*

5. Izņemiet ievades paplāti.



6. Pievienojiet skenera komplektācijā ietilpstošos iesaiņojuma materiālus, pēc tam skeneri iesaiņojiet oriģinālajā vai citā izturīgā kastē.

Iestatījumu dublēšana

Iestatījuma vērtību kopu no programmas Web Config varat eksportēt failā. To var izmantot kontaktpersonu dublēšanai, iestatījumu vērtībām, skenera nomaiņai u. c.

Eksportēto failu nevar rediģēt, jo tas ir eksportēts kā binārais fails.

Iestatījumu eksportēšana

Eksportējiet skenera iestatījumu.

1. Atveriet programmu Web Config un tad atlasiet cilni **Device Management** > **Export and Import Setting Value** > **Export**.

2. Atlasiet iestatījumus, kurus vēlaties eksportēt.

   Atlasiet iestatījumus, kurus vēlaties eksportēt. Atlasot galveno kategoriju, tiek atlasītas arī apakškategorijas. Tomēr nevar izvēlēties tās apakškategorijas, kuras rada kļūdas, dubultojot tās tajā pašā tīklā (piemēram, IP adreses u.t.t.).

3. Ievadiet paroli, lai šifrētu eksportēto failu.

   Faila importēšanai nepieciešama parole. Ja nevēlaties šifrēt failu, atstājiet šo lauku tukšu.

4. Noklikšķiniet uz **Export**.

> ***Svarīga informācija:***
> *Ja vēlaties eksportēt skenera tīkla iestatījumus, piemēram, ierīces nosaukumu un IPv6 adresi, atlasiet **Enable to select the individual settings of device** un atlasiet vēl citus vienumus. Izmantojiet tikai nomaiņas skenera atlasītās vērtības.*

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Iestatījumu importēšana

Importējiet eksportēto Web Config failu skenerī.

> ***Svarīga informācija:***
> *Importējot vērtības, kuras ietver atsevišķu informāciju, piemēram, skenera nosaukumu vai IP adresi, pārliecinieties, ka tīklā šāda IP adrese jau nepastāv.*

1. Piekļūstiet Web Config un tad atlasiet **Device Management** cilni > **Export and Import Setting Value** > **Import**.
2. Atlasiet eksportēto failu un tad ievadiet šifrēto paroli.
3. Noklikšķiniet uz **Next**.
4. Atlasiet iestatījumus, kurus vēlaties importēt, un tad noklikšķiniet uz **Next**.
5. Noklikšķiniet uz **OK**.

Šie iestatījumi tiek piemēroti skenerim.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Atjaunot noklusējuma iestatījumus

Vadības panelī, atlasiet **Iestatījumi** > **Sistēmas administrēšana** > **Atjaunot noklusējuma iestatījumus**, un pēc tam vienumus, kurus vēlaties atjaunot uz noklusējumu.

❏ Tīkla iestatījumi: atjaunot sākotnējo tīkla iestatījumu stāvokli.

❏ Viss, izņemot tīkla iestatījumus: atjaunot citu iestatījumu (izņemot ar tīklu saistīto) sākotnējo stāvokli.

❏ Visi iestatījumi: atjaunot visu iestatījumu sākotnējo stāvokli, kāds tas bija ierīces iegādes brīdī.

Svarīga informācija:

*Ja atlasāt un palaižat **Visi iestatījumi**, visi skenerī reģistrētie iestatījumi dati, tostarp kontaktpersonas un lietotāja autentifikācijas iestatījumi, tiks dzēsti. Dzēstos iestatījumus nevar atjaunot.*

Programmu un aparātprogrammatūras atjaunināšana

Iespējams, varēsiet atrisināt noteiktas problēmas un uzlabot vai pievienot funkcijas, atjauninot programmas un aparātprogrammatūru. Pārliecinieties, ka izmantojat programmu un aparātprogrammatūras jaunāko versiju.

Svarīga informācija:

❏ *Atjaunināšanas laikā neizslēdziet datoru vai skeneri.*

Piezīme:
*Ja skeneri var savienot ar internetu, aparātprogrammatūru var atjaunināt, izmantojot programmu Web Config. Atlasiet cilni **Device Management** > **Firmware Update**, pārbaudiet parādīto ziņojumu un pēc tam noklikšķiniet **Start**.*

1. Pārliecinieties, ka skeneris un dators ir savienots un dators savienots ar internetu.

2. Palaidiet EPSON Software Updater un atjauniniet programmas vai aparātprogrammatūru.

   Piezīme:
   Windows Server operētājsistēmas netiek atbalstītas.

   ❏ Windows 10

   Noklikšķiniet uz palaides pogas un atlasiet **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Meklēšanas viedpogā ievadiet lietojumprogrammas nosaukumu un pēc tam izvēlieties attēloto ikonu.

   ❏ Windows 7

   Uzklikšķiniet uz pogas Sākt, izvēlieties **Visas programmas** vai **Programmas** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Atlasiet **Finder** > **Aiziet!** > **Lietojumprogrammas** > **Epson Software** > **EPSON Software Updater**.

Piezīme:
Ja sarakstā nevarat atrast lietojumprogrammu, kuru vēlaties atjaunināt, to nevar atjaunināt, izmantojot EPSON Software Updater. Pārbaudiet programmu jaunāko versiju pieejamību lokālajā Epson tīmekļa vietnē.

http://www.epson.com

Skenera aparātprogrammatūras atjaunināšana, izmantojot vadības paneli

Ja skeneri var savienot ar internetu, skenera aparātprogrammatūru var atjaunināt, izmantojot vadības paneli. Skeneri var iestatīt, lai tas regulāri pārbaudītu aparātprogrammatūras atjauninājumu pieejamību un ziņotu jums, ja tie ir pieejami.

1. Sākuma ekrānā izvēlieties **Iestatījumi**.

2. Atlasiet **Sistēmas administrēšana** > **Aparātprogramatūras atjauninājums** > **Atjaunināt**.

   Piezīme:
   *Atlasiet **Paziņošana** > **Iesl**, lai skeneris regulāri pārbaudītu, vai nav pieejami aparātprogrammatūras atjauninājumi.*

3. Skatiet ekrānā redzamo ziņojumu un sāciet pieejamo atjauninājumu meklēšanu.

4. Ja LCD ekrānā parādās ziņojums, informējot jūs, ka ir pieejams aparātprogrammatūras atjauninājums, izpildiet ekrānā sniegtās instrukcijas, lai sāktu atjaunināšanu.

   Svarīga informācija:
   - ❏ *Neizslēdziet skeneri un neatvienojiet to no strāvas, kamēr nav beigusies atjaunināšana, pretējā gadījumā iespējami skenera darbības traucējumi.*
   - ❏ *Ja aparātprogrammatūras atjaunināšana netiek pabeigta vai tā ir neveiksmīga, skeneris nestartējas, kā paredzēts, un nākamajā tā ieslēgšanas reizē LCD ekrānā redzams uzraksts „Recovery Mode”. Šādā situācijā nepieciešams aparātprogrammatūru jaunināt vēlreiz, izmantojot datoru. Savienojiet skeneri ar datoru, izmantojot USB vadu. Ja skenera displejā redzams uzraksts „Recovery Mode”, aparātprogrammatūru nevar atjaunināt, izmantojot tīkla savienojumu. Datorā atveriet vietējo Epson tīmekļa vietni un lejupielādējiet jaunāko skenera aparātprogrammatūru. Lai uzzinātu, kādas ir turpmākās veicamās darbības, skatiet instrukcijas tīmekļa vietnē.*

Aparātprogrammatūras atjaunināšana, izmantojot programmu Web Config

Ja skeneri var savienot ar internetu, aparātprogrammatūru var atjaunināt, izmantojot programmu Web Config.

1. Atveriet programmu Web Config un atlasiet cilni **Device Management** > **Firmware Update**.

2. Noklikšķiniet **Start** un pēc tam izpildiet ekrānā redzamās instrukcijas.

   Tiek sākta aparātprogrammatūras pārbaude, un, ja pastāv atjaunināta aparātprogrammatūra, tiek parādīta informācija par aparātprogrammatūru.

Piezīme:
Aparātprogrammatūru var atjaunināt, izmantojot arī Epson Device Admin. Ierīču sarakstā var vizuāli pārbaudīt aparātprogrammatūras informāciju. Šī iespēja noder, ja nepieciešams atjaunināt aparātprogrammatūru vairākās ierīcēs. Plašāku informāciju skatiet Epson Device Admin pamācībā vai palīdzībā.

Saistītā informācija

➡ "Tīmekļa konfigurācijas palaišana tīmekļa pārlūkā" 35. lpp.

Aparātprogrammatūras atjaunināšana, neizveidojot savienojumu ar internetu

Ierīces aparātprogrammatūru var lejupielādēt datorā no Epson tīmekļa vietnes, un pēc tam, lai atjauninātu aparātprogrammatūru, ierīci var savienot ar datoru, izmantojot USB vadu. Ja nevar veikt atjaunināšanu tīklā, izmēģiniet šo metodi.

Piezīme:
Pirms atjaunināšanas pārbaudiet, vai skenera draiveris Epson Scan 2 ir instalēts datorā. Ja Epson Scan 2 nav instalēta, instalējiet to.

1. Skatiet Epson tīmekļa vietni, lai iegūtu jaunākos aparātprogrammatūras atjauninājumus.

   http://www.epson.com

   ❏ Ja jūsu skenerim nav aparātprogrammatūras, lejupielādējiet to un pārejiet uz nākamo soli.

   ❏ Ja tīmekļa vietnē nav informācijas par aparātprogrammatūru, jūs jau izmantojat jaunāko aparātprogrammatūru.

2. Izmantojot USB vadu, savienojiet ar skeneri datoru, kurā atrodas lejupielādētā aparātprogrammatūra.

3. Veiciet dubultklikšķi uz lejupielādētā .exe faila.

   Tiek palaista programma Epson Firmware Updater.

4. Izpildiet ekrānā sniegtos norādījumus.