



**DS-900WN DS-800WN**

# **Administrators rokasgrāmata**

**Jūsu nolūkiem nepieciešamie  
iestatījumi**

**Tīkla iestatījumi**

**Nepieciešamie skenēšanas iestatījumi**

**Pamata drošības iestatījumi**

**Tīkla drošības iestatījumi**

**Funkcijas Epson Open Platform  
lietošana**

# Autortiesības

Nevienu šīs publikācijas daļu bez iepriekšējas Seiko Epson Corporation rakstveida atļaujas nedrīkst reproducēt, uzglabāt izgūšanas sistēmā vai jebkādā formā vai izmantojot jebkādus līdzekļus — elektroniskus, mehāniskus, fotokopēšanas, ierakstīšanas vai citus — nodot citiem. Mēs neuzņemamies nekāda veida atbildību par patentu pārkāpumiem, kas saistīti ar šajā dokumentā esošo informāciju. Mēs arī neuzņemamies nekāda veida atbildību par zaudējumiem, kas var rasties, izmantojot šajā dokumentā sniegto informāciju. Šeit sniegtā informācija paredzēta tikai lietošanai ar šo Epson ierīci. Epson neuzņemas atbildību par šīs informācijas izmantošanu saistībā ar citām ierīcēm.

Seiko Epson Corporation un tās filiāles neuzņemas atbildību par šī produkta bojājumiem, zaudējumiem vai izmaksām, kas pircējam vai trešajām personām radušās negadījuma dēļ, šo produktu nepareizi lietojot, ļaunprātīgi to izmantojot vai veicot tajā neapstiprinātas izmaiņas, to remontējot vai pārveidojot, vai (izņemot ASV) nerīkojoties saskaņā ar Seiko Epson Corporation lietošanas un apkopes instrukciju.

Seiko Epson Corporation un tā filiāles neatbild par jebkādu kaitējumu vai problēmām, kas radušās jebkuru papildpiederumu vai patērējamo produktu lietošanas dēļ, kas nav Seiko Epson Corporation Oriģinālie Epson vai Epson Apstiprinātie produkti.

Seiko Epson Corporation neatbild par jebkādu kaitējumu, kas radies elektromagnētisko traucējumu ietekmē, izmantojot tos saskarnes kabeļus, kurus Seiko Epson Corporation nav apzīmējusi kā Epson Apstiprinātos produktus.

© 2024 Seiko Epson Corporation

Šīs rokasgrāmatas saturs un šī produkta specifikācijas var tikt mainītas bez iepriekšēja paziņojuma.

# Preču zīmes

- Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- Chrome, Chromebook and Android are trademarks of Google LLC.
- Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Vispārējs paziņojums: visas citas preču zīmes ir to atbilstošo īpašnieku īpašums un ir izmantotas tikai identifikācijas nolūkos.

# Satura rādītājs

## Autortiesības

## Preču zīmes

## Ievads

Šī dokumenta saturs. . . . .	7
Šīs pamācības izmantošana. . . . .	7
Zīmes un simboli. . . . .	7
Šajā rokasgrāmatā lietotie apraksti. . . . .	7
Operētājsistēmu atsauces. . . . .	7

## Piezīmes par administratora paroli

Piezīmes par administratora paroli. . . . .	10
Sākotnējā administratora parole. . . . .	10
Darbības, kurām nepieciešama administratora parole. . . . .	10
Administratora paroles maiņa. . . . .	10
Administratora paroles atiestatīšana. . . . .	10

## Jūsu nolūkiem nepieciešamie iestatījumi

Jūsu nolūkiem nepieciešamie iestatījumi. . . . .	12
--	----

## Tikla iestatījumi

Skenera savienošana ar tīklu. . . . .	15
Pirms tīkla savienojuma izveides. . . . .	15
Savienošana ar tīklu, izmantojot vadības paneli. . . . .	17
Datora vai ierīču pievienošana vai nomaiņa. . . . .	21
Savienojuma izveide ar skeneri, kas ir bijis savienots ar tīklu. . . . .	21
Tieši savienojiet viedierīci un skeneri (Wi-Fi Direct). . . . .	23
Tīkla savienojuma atiestatīšana. . . . .	25
Tīkla savienojuma statusa pārbaude. . . . .	27
Tīkla savienojuma statusa pārbaude, izmantojot vadības paneli. . . . .	27
Tīkla specifikācijas. . . . .	28
Wi-Fi specifikācijas. . . . .	28
Ethernet tehniskie dati. . . . .	30
Tīkla funkcijas un IPv4/IPv6 atbalsts. . . . .	30
Drošības protokols. . . . .	31
Porta izmantošana skenerim. . . . .	31
Problēmu risināšana. . . . .	32

Nevar izveidot savienojumu ar tīklu. . . . .	32
--	----

## Programmatūra skenera iestatīšanai

Lietojumprogramma skenera darbību konfigurēšanai (Web Config). . . . .	37
Web Config palaišana tīmekļa pārlūkprogrammā. . . . .	37
Epson Device Admin. . . . .	38
Konfigurācijas veidne. . . . .	39

## Nepieciešamie skenēšanas iestatījumi

E-pasta servera reģistrēšana. . . . .	44
E-pasta servera savienojuma pārbaude. . . . .	45
Tikla mapes izveide. . . . .	46
Kontaktpersonu pieejamības sniegšana. . . . .	54
Kontaktu konfigurācijas salīdzinājums. . . . .	55
Mērķa reģistrēšana kontaktpersonu sadaļā, izmantojot Web Config. . . . .	55
Mērķa kā grupas reģistrēšana, izmantojot Web Config. . . . .	57
Kontaktpersonu dublēšana un importēšana. . . . .	58
Liela kontaktpersonu apjoma eksportēšana un reģistrācija, izmantojot rīku. . . . .	59
LDAP servera un lietotāju mijiedarbība. . . . .	60
Funkcijas AirPrint iestatīšana. . . . .	63
Problēmas sagatavot tīkla skenēšanu. . . . .	64
Problēmu risināšanas padomi. . . . .	64
Nevar piekļūt Web Config. . . . .	64

## Vadības paneļa displeja pielāgošana

Priekšiestat. reģistrēšana. . . . .	68
Izvēlnes opcijas Priekšiestat. . . . .	69
Vadības paneļa sākuma ekrāna rediģēšana. . . . .	70
Mainīt Izkārttojums sākuma ekrānā. . . . .	70
Pievienot ikonu. . . . .	71
Noņemt ikonu. . . . .	72
Pārvietot ikonu. . . . .	73

## Pamata drošības iestatījumi

Produkta drošības funkciju. Ievads. . . . .	75
Administratora iestatījumi. . . . .	75
Administratora paroles konfigurēšana. . . . .	75

Bloķēšanas iestatījums izmantošana vadības panelim. . . . .	77
Pieteikšanās kā administratoram, izmantojot vadības paneli. . . . .	80
Pieejamo funkciju ierobežošana (Piekļuves vadība). . . . .	81
Lietotāja konta izveide. . . . .	81
Opcijas Piekļuves vadība iespējošana. . . . .	82
Pieteikšanās skenerī, kurā ir iespējota Piekļuves vadība. . . . .	82
Ārējās saskarnes atspējošana. . . . .	83
Programmas verificācijas iespējošana palaišanas laikā. . . . .	83
Tīkla skenēšanas atspējošana datorā. . . . .	84
WSD skenēšanas iespējošana vai atspējošana. . . . .	84
Attāla skenera kontrole. . . . .	85
Attāla skenera informācijas pārbaudīšana. . . . .	85
E-pasta ziņojumu saņemšana notikumu gadījumā. . . . .	85
Web Config izmantošana skenera barošanas avota kontrolei. . . . .	86
Noklusējuma iestatījumu atjaunošana. . . . .	86
Epson Remote Services informācija. . . . .	87
Problēmu risināšana. . . . .	87
Aizmirsta administratora parole. . . . .	87
<b>Tīkla drošības iestatījumi</b>	
Drošības iestatījumi un bīstamības novēršana. . . . .	89
Drošības funkciju iestatījumi. . . . .	90
Vadība, izmantojot protokolus. . . . .	90
Protokolu vadība. . . . .	90
Protokoli, kurus var iespējot vai atspējot. . . . .	90
Protokolu iestatīšanas vienumi. . . . .	91
Ciparsertifikāta lietošana. . . . .	93
Par ciparsertifikātiem. . . . .	93
CA-signed Certificate konfigurēšana. . . . .	93
Pašparakstīta sertifikāta atjaunināšana. . . . .	97
CA Certificate konfigurēšana. . . . .	97
SSL/TLS sakari ar skeneri. . . . .	98
Pamata SSL/TLS iestatījumu konfigurēšana. . . . .	98
Skenera servera sertifikāta konfigurēšana. . . . .	99
Šifrētie sakari, izmantojot IPsec/IP filtrēšanu. . . . .	99
Par IPsec/IP Filtering. . . . .	99
Noklusējuma politikas konfigurēšana. . . . .	99
Grupas politikas konfigurēšana. . . . .	103
IPsec/IP Filtering konfigurāciju piemēri. . . . .	109
IPsec/IP filtrēšanas sertifikāta konfigurēšana. . . . .	110
Skenera pievienošana IEEE802.1X tīklam. . . . .	110

IEEE 802.1X tīkla konfigurēšana. . . . .	110
IEEE 802.1X sertifikāta konfigurēšana. . . . .	112
Drošības papildu iestatījumu problēmu risināšana	112
Drošības iestatījumu atjaunošana. . . . .	112
Tīkla drošības funkciju lietošanas problēmas. . . . .	113
Ciparsertifikāta lietošanas problēmas. . . . .	115

## **Funkcijas Epson Open Platform lietošana**

Pārskats par Epson Open Platform. . . . .	120
Epson Open Platform konfigurēšana. . . . .	120
Epson Open Platform validēšana. . . . .	120

## **Autentifikācijas ierīces uzstādīšana**

Autentifikācijas ierīces pievienošana. . . . .	122
Autentifikācijas ierīces darbības pārbaude. . . . .	122
Autentifikācijas kartes atpazīšanas apstiprināšana.	122
Autentifikācijas ierīces problēmu novēršana. . . . .	123
Nevar nolasīt autentifikācijas karti. . . . .	123

## **Apkope**

Skenera korpusa tīrīšana. . . . .	125
Skenera iekšpuses tīrīšana. . . . .	125
Veltnišu bloka nomaiņa. . . . .	130
Veltnišu bloka kodi. . . . .	135
Ieskenēto lapu skaita atiestate pēc rullīšu nomaiņas. . . . .	135
Enerģijas taupīšana. . . . .	136
Skenera transportēšana. . . . .	136
Iestatījumu dublēšana. . . . .	137
Iestatījumu eksportēšana. . . . .	137
Iestatījumu importēšana. . . . .	138
Atjaunot noklusējuma iestatījumus. . . . .	138
Programmu un aparātprogrammatūras atjaunināšana. . . . .	139
Skenera aparātprogrammatūras atjaunināšana, izmantojot vadības paneli. . . . .	139
Aparātprogrammatūras atjaunināšana, izmantojot programmu Web Config. . . . .	140
Aparātprogrammatūras atjaunināšana, neizveidojot savienojumu ar internetu. . . . .	140

---



# levads

Šī dokumenta saturs. . . . . 7

Šīs pamācības izmantošana. . . . . 7

## Šī dokumenta saturs

Šis dokuments skenera administratoriem sniedz turpmāk minēto informāciju.

- Tikla iestatījumi
- Skenēšanas funkciju sagatavošana
- Drošības iestatījumu iespējošana un pārvaldība
- Ikdienas apkopes veikšana

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

---

## 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 ekrānuņēmumi 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.

## Operētājsistēmu atsauces

### Windows

Šajā rokasgrāmatā tādi termini kā „Windows 11”, „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Server 2022”, „Windows Server 2019”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012”, „Windows Server 2008 R2” un „Windows Server 2008” attiecas uz turpmāk norādītajām operētājsistēmām. Turklāt termins „Windows” tiek lietots kā atsauce uz visām šo operētājsistēmu versijām.

- Operētājsistēma Microsoft® Windows® 11
- Operētājsistēma Microsoft® Windows® 10
- Operētājsistēma Microsoft® Windows® 8.1
- Operētājsistēma Microsoft® Windows® 8
- Operētājsistēma Microsoft® Windows® 7
- Operētājsistēma Microsoft® Windows Server® 2022
- 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
- Operētājsistēma Microsoft® Windows Server® 2008

### **Mac OS**

Šajā rokasgrāmatā termins „Mac OS” tiek lietots, lai apzīmētu Mac OS X 10.9 vai jaunāku versiju un macOS 11 vai jaunāku versiju.



---

# Piezīmes par administratora paroli

Piezīmes par administratora paroli. . . . .	10
Sākotnējā administratora parole. . . . .	10
Darbības, kurām nepieciešama administratora parole. . . . .	10
Administratora paroles maiņa. . . . .	10
Administratora paroles atiestatīšana. . . . .	10

---

## Piezīmes par administratora paroli

Šī ierīce ļauj iestatīt administratora paroli, lai novērstu, ka nepilnvarotas trešās personas piekļūst vai maina ierīces iestatījumus vai tīkla iestatījumus, kas ir saglabāti ierīcē, kad tā ir savienota ar tīklu.

Ja iestatāt administratora paroli, parole ir jāievada, kad maināt iestatījumus tādā konfigurācijas programmatūrā kā Web Config.

Skenerim ir iestatīta sākotnējā parole, bet jūs varat to mainīt uz jebkādu paroli.

---

## Sākotnējā administratora parole

Sākotnējā administratora parole mainās atkarībā no produktam piestiprinātās etiķetes. Ja produkta aizmugurē ir piestiprināta etiķete „PASSWORD”, ievadiet etiķetē redzamo 8 ciparu numuru. Ja etiķete „PASSWORD” nav piestiprināta, kā administratora paroli ievadiet sērijas numuru, kas redzams produkta aizmugurē piestiprinātajā etiķetē.

Mēs iesakām mainīt sākotnējo administratora paroli no noklusējuma iestatījuma.

***Piezīme:***

*Nav iestatīts noklusējuma lietotājvārds.*

---

## Darbības, kurām nepieciešama administratora parole

Ja jums tiek pieprasīts ievadīt administratora paroli, veicot tālāk norādītās darbības, ievadiet produktam iestatīto administratora paroli.

- Kad pierakstāties Web Config papildu iestatījumos
- Kad izmantojat vadības paneļa izvēlni, kuru ir bloķējis administrators
- Kad maināt ierīces iestatījumus programmā
- Kad atjaunināt ierīces aparātprogrammatūru
- Kad maināt vai atiestatāt administratora paroli

---

## Administratora paroles maiņa

To var mainīt, izmantojot produkta vadības paneli vai programmā Web Config.

Mainot paroli, jaunajai parolei jābūt 8 līdz 20 rakstzīmes garai un tajā var iekļaut tikai viena bita burtciparu rakstzīmes un simbolus.

---

## Administratora paroles atiestatīšana

Varat atiestatīt administratora paroli uz sākotnējo iestatījumu, izmantojot produkta vadības paneli vai programmā Web Config.

Ja aizmirsāt paroli un nevar to atiestatīt uz noklusējuma iestatījumiem, produktam ir nepieciešams remonts. Sazinieties ar vietējo izplatītāju.

---

# **Jūsu nolūkiem nepieciešamie iestatījumi**

Jūsu nolūkiem nepieciešamie iestatījumi. . . . .	.12
--	-----

## 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. <a href="#">"Skenera savienošana ar tīklu" 15. lpp.</a>
Vēlos pievienot skeneri jaunam datoram.	Iestatiet skenera tīkla iestatījumus jaunajā datorā. <a href="#">"Datora vai ierīču pievienošana vai nomaiņa" 21. lpp.</a>

### Skenēšanas iestatījumi

Nolūks	Nepieciešamie iestatījumi
Vēlos sūtīt skenētos attēlus uz e-pastu. (Scan to Email)	1. Iestatiet e-pasta serveri, ko vēlaties saistīt. <a href="#">"E-pasta servera reģistrēšana" 44. lpp.</a> 2. Reģistrējiet saņēmēja e-pasta adresi <b>Contacts</b> (izvēles). Reģistrējot e-pasta adresi, jums tā nebūs jāievada katru reizi, kad vēlēsities kaut ko nosūtīt. Varēsit to izvēlēties no Kontaktiem. <a href="#">"Kontaktpersonu pieejamības sniegšana" 54. lpp.</a>
Vēlos saglabāt skenētos attēlus tīkla mapē. (Scan to Network Folder/FTP)	1. Izveidojiet tīkla mapi, kurā vēlaties saglabāt attēlus. <a href="#">"Tīkla mapes izveide" 46. lpp.</a> 2. Reģistrējiet ceļu uz mapi <b>Contacts</b> (izvēles). Reģistrējot mapes ceļu, jums tas nebūs jāievada katru reizi, kad vēlēsities kaut ko nosūtīt. Varēsit to izvēlēties no Kontaktiem. <a href="#">"Kontaktpersonu pieejamības sniegšana" 54. lpp.</a>
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. <a href="https://www.epsonconnect.com/">https://www.epsonconnect.com/</a> <a href="http://www.epsonconnect.eu">http://www.epsonconnect.eu</a> (tikai Eiropā)

### Vadības paneļa displeja pielāgošana

Nolūks	Nepieciešamie iestatījumi
Vēlos mainīt skenera vadības paneli attēlotos vienumus.	Iestatiet <b>Priekšiestat.</b> vai <b>Sāku lapas rediģēšana</b> . Vadības paneli varat reģistrēt savus iecienītākos skenēšanas iestatījumus un rediģēt attēlotos vienumus. <a href="#">"Vadības paneļa displeja pielāgošana" 67. lpp.</a>

## Pamata drošības funkciju iestatīšana

Nolūks	Nepieciešamie iestatījumi
Vēlos novērst, ka skenera iestatījumus maina kāds cits nevis administrators.	Iestatiet skenera administratora paroli. <a href="#">"Administratora iestatījumi" 75. lpp.</a>
Vēlos atspējot skeneru izmantošanu ar USB savienojumiem.	Atspējojiet ārējo saskarni. <a href="#">"Ārējās saskarnes atspējošana" 83. lpp.</a>

## Papildu drošības funkciju iestatīšana

Nolūks	Nepieciešamie iestatījumi
Vēlos kontrolēt kādus protokolus izmantot.	Iespējojiet vai atspējojiet protokolus. <a href="#">"Vadība, izmantojot protokolus" 90. lpp.</a>
Vēlos šifrēt sakaru ceļu.	1. Iestatiet savu digitālo sertifikātu. <a href="#">"Ciparsertifikāta lietošana" 93. lpp.</a> 2. Iestatiet SSL/TLS sakarus. <a href="#">"SSL/TLS sakari ar skeneri" 98. lpp.</a>
Vēlos izmantot šifrētus sakarus (IPsec). Vēlos izmantot programmatūru tikai no konkrēta datora (IP filtrēšana).	Iestatiet trafika filtrēšanas politikas. <a href="#">"Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 99. lpp.</a>
Vēlos izmantot skeneri IEEE802.1X tīklā.	Iestatiet IEEE802.1X skeneri. <a href="#">"Skenera pievienošana IEEE802.1X tīklam" 110. lpp.</a>

## Skenera sinhronizēšana, izmantojot autentifikācijas sistēmu

Iegūstiet produkta atslēgu no specializētās tīmekļa vietnes un aktivizējiet savā skenerī Epson Open Platform.

["Funkcijas Epson Open Platform lietošana" 119. lpp.](#)

## Autentifikācijas opcijas izmantošana (Epson Print Admin/Epson Print Admin Serverless)

Lai izmantotu opciju, ir nepieciešama licences atslēga.

Lai iegūtu vairāk informācijas, sazinieties ar izplatītāju.

### **Piezīme:**

*Epson Print Admin Serverless nevar lietot, ja sistēma ir sinhronizēta ar Epson Open Platform.*

---

# Tīkla iestatījumi

Skenera savienošana ar tīklu. . . . .	15
Datora vai ierīču pievienošana vai nomainīšana. . . . .	21
Tīkla savienojuma statusa pārbaude. . . . .	27
Tīkla specifikācijas. . . . .	28
Problēmu risināšana. . . . .	32

## Skenera savienošana ar tīklu

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

### Piezīme:

*Ja skeneris un dators atrodas vienā segmentā, varat arī izveidot savienojumu, izmantojot instalēšanas programmu.*

*Lai palaistu instalēšanas programmu, atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.*

<https://epson.sn>

Varat skatīt lietošanas norādījumus Video rokasgrām.. Piekļūstiet šādai URL adresei.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

## 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	<input type="checkbox"/> Ethernet <input type="checkbox"/> 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	<input type="checkbox"/> IP adrese <input type="checkbox"/> Apakštīkla maska <input type="checkbox"/> 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	<input type="checkbox"/> SSID <input type="checkbox"/> 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.  <a href="#">"Tīkla specifikācijas" 28. lpp.</a>
DNS servera informācija	<input type="checkbox"/> Primārā DNS servera IP adrese <input type="checkbox"/> 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	<input type="checkbox"/> Starpniekservera nosaukums	<p>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.</p> <p>Lai izmantotu tālāk norādītās funkcijas, skeneris izveido tiešu savienojumu ar internetu.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Epson Connect pakalpojumi</li> <li><input type="checkbox"/> Citu uzņēmumu mākoņpakalpojumi</li> <li><input type="checkbox"/> Aparātprogrammatūras atjaunināšana</li> <li><input type="checkbox"/> Skenēto attēlu sūtīšana, izmantojot SharePoint(WebDAV)</li> </ul>
Porta numura informācija	<input type="checkbox"/> Izlaižamais porta numurs	<p>Pārbaudiet skenera un datora izmantoto porta numuru, pēc tam nepieciešamības gadījumā atveriet portu, ko nobloķējis ugunsmūris.</p> <p>Skatiet tālāk norādīto, lai iegūtu porta numuru, kuru izmanto skeneris.</p> <p><a href="#">"Porta izmantošana skenerim" 31. lpp.</a></p>

## 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 statistikas 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 pāreijiet 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 datus 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 **Tikla 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. Pārlicinieties, 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.)

### ***Ņemiet vērā, kad izmantojat Wi-Fi 5 GHz savienojumu***

Šis printeris parasti izmanto W52 (36ch) kā kanālu, kad savienojas ar Wi-Fi Direct (vienkāršais PP). Tā kā bezvadu LAN (Wi-Fi) savienojuma kanāls tiek izvēlēts automātiski, izmantotais kanāls var atšķirties, ja tas tiek izmantots vienlaikus ar Wi-Fi Direct savienojumu. Ja kanāli atšķiras, datu saziņa ar skeneri var būt lēna. Ja tas netraucē lietošanai, izveidojiet savienojumu ar SSID 2,4 GHz joslā. 2,4 GHz frekvenču joslā izmantotie kanāli sakrīt.

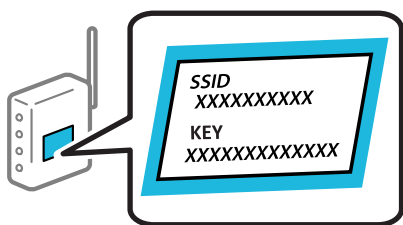
Iestatot bezvadu lokālo tīklu 5 GHz frekvencē, mēs iesakām atspējot Wi-Fi Direct.


### ***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 tā noklusējuma iestatījumiem, SSID un parole ir norādīti uzlīmē. 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. Atlasiet **Maršrutētājs**.
3. Pieskarieties pie **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 reģistrjūtīga.
- 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.
- Ja neredzat SSID, ar kuru vēlaties izveidot savienojumu, izmantojiet programmatūru vai lietotni, lai iestatītu Wi-Fi no sava datora vai viedierīces, piemēram, viedtālruna vai planšetdatora. Lai iegūtu papildinformāciju, pārlūkprogrammā ievadiet „<https://epson.sn>” ievadiet produkta nosaukumu un pārejiet uz **Iestatīšana**.

**Saistītā informācija**

➔ "Tikla savienojuma statusa pārbaude" 27. 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**

➔ "Tikla savienojuma statusa pārbaude" 27. 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" 27. lpp.](#)

---

## Datora vai ierīču pievienošana vai nomaīņa

### 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.

Lai palaistu instalēšanas programmu, atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

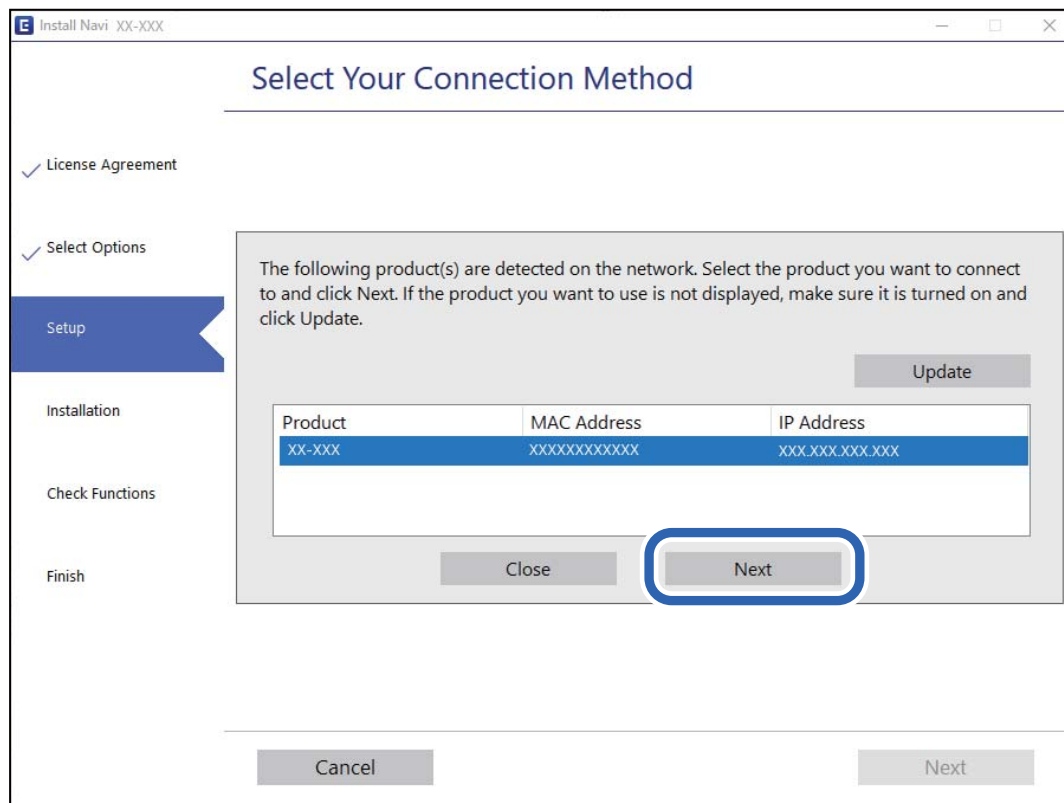
<https://epson.sn>

Varat skatīt lietošanas norādījumus Video rokasgrām.. Piekļūstiet šādai URL adresei.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

## 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.

## Tikla 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" 26. lpp.](#)

### Savienojuma izveide, izmantojot Wi-Fi Direct

Pievienojiet viedierīci tieši pie skenera, neizmantojot bezvadu maršrutētāju.

Lai uzzinātu vairāk, skatiet zemāk sniegto informāciju.

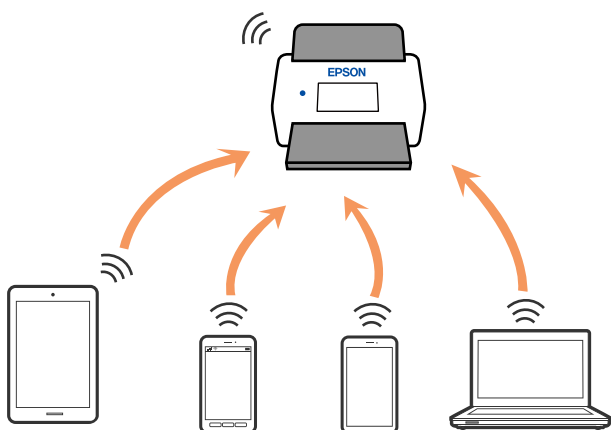
["Tieši savienojiet viedierīci un skeneri \(Wi-Fi Direct\)" 23. lpp.](#)

## 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
- Tikla nosaukuma (SSID) mainīšana
- Paroles mainīšana
- Frekvenču diapazons maiņa  
*Atkarībā no reģiona šis iestatījums, iespējams, netiks parādīts.*
- Wi-Fi Direct (vienkāršā PP) iestatījumu atjaunošana

## Tikla savienojuma atiestatīšana

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

## Nomainot bezvadu maršrutētāju

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

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

### **Iestatījumu veikšana savienojuma izveidei ar datoru**

Skenera savienošanai ar datoru ieteicams izmantot instalētāju.

Lai palaistu instalēšanas programmu, atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

<https://epson.sn>

Varat skatīt lietošanas norādījumus Video rokasgrām.. Piekļūstiet šādai URL adresei.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

### **Savienojuma metodes izvēle**

Izpildiet ekrānā sniegtos norādījumus. Ekrānā **Atlasīt instalēšanas opciju** 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" 32. 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, atveriet šādu tīmekļa vietni un pēc tam ievadiet produkta nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

<https://epson.sn>

Pieklūstiet 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.

Lai palaistu instalēšanas programmu, atveriet turpmāk norādīto tīmekļa vietni un pēc tam ievadiet ierīces nosaukumu. Izvēlieties **Iestatīšana** un sāciet iestatīšanu.

<https://epson.sn>

Varat skatīt lietošanas norādījumus Video rokasgrām.. Pieklūstiet šādai URL adresei.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Izpildiet ekrānā sniegtos norādījumus.

## **Metodes savienojumam ar datoru maiņa**

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

### ***Tikla savienojuma izmaiņšana 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)" 19. lpp.

### ***Tikla savienojuma izmaiņšana no Wi-Fi uz Ethernet***

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

1. Sākuma ekrānā izvēlieties **Iestatījumi**.
2. Atlasiet **Tikla iestatījumi** > **Vadu LAN iestatīšana**.
3. Izpildiet ekrānā sniegtos norādījumus.

### **Savienojuma maiņa no USB uz tīkla savienojumu**

Instalētāja izmantošana un cita savienojuma veida iestatīšana.

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

<https://epson.sn>

### **Savienojuma veida maiņa**

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

Izvēlieties 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.

---

## **Tikla savienojuma statusa pārbaude**

Tikla savienojuma statusu var pārbaudīt turpmāk aprakstītajā veidā.









### **Tikla savienojuma statusa pārbaude, izmantojot vadības paneli**

Tikla savienojuma statusu varat pārbaudīt, apskatot tīkla ikonu vai tīkla informāciju skenera vadības paneli.

### **Tikla savienojuma statusa pārbaude, apskatot tīkla ikonu**

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



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

## 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	<b>A tabula</b>
Īrija, Apvienotā Karaliste, Austrija, Vācija, Lihtenšteina, Šveice, Francija, Beļģija, Luksemburga, Nīderlande, Itālija, Portugāle, Spānija, Dānija, Somija, Norvēģija, Zviedrija, Islande, Horvātija, Kipra, Grieķija, Ziemeļmaķedonija, Serbija, Slovēnija, Malta, Bosnija un Hercegovina, Kosova, Melnkalne, Albānija, Bulgārija, Čehija, Igaunija, Ungārija, Latvija, Lietuva, Polija, Rumānija, Slovākija, Izraēla, Austrālija, Jaunzēlande, Taivāna	<b>B tabula</b>
Turcija	DS-900WN: Sērijas numuri, sākot ar XDA8: <b>A tabula</b> Sērijas numuri, sākot ar XDA7: <b>B tabula</b>
	DS-800WN: Sērijas numuri, sākot ar XDA2: <b>A tabula</b> Sērijas numuri, sākot ar XD9Z: <b>B tabula</b>

#### A tabula

Standarti	IEEE 802.11b/g/n*1
Frekvenču diapazons	2400–2483,5 MHz
Maksimālā raidītā radiofrekvenču signāla jauda	20 dBm (EIRP)
Kanāli	1/2/3/4/5/6/7/8/9/10/11/12/13
Savienojuma režīmi	Infrastruktūra, Wi-Fi Direct (vienkāršais 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* <sup>2</sup> /13* <sup>2</sup>
		5 GHz* <sup>3</sup>	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* <sup>2</sup> /13* <sup>2</sup>
		5 GHz* <sup>3</sup>	W52 (36/40/44/48) W58 (149/153/157/161/165)
Savienojuma režīmi	Infrastruktūra, Wi-Fi Direct (vienkāršais PP)* <sup>4</sup> , * <sup>5</sup>		
Drošības protokoli* <sup>6</sup>	WEP (64/128bit), WPA2-PSK (AES)* <sup>7</sup> , 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)* <sup>1</sup> IEEE802.3u (100BASE-TX)* <sup>1</sup> IEEE802.3ab (1000BASE-T)* <sup>1</sup> IEEE802.3az (energoefektīvs Ethernet)* <sup>2</sup>
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.

## Tikla funkcijas un IPv4/IPv6 atbalsts

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

## 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
	WebDAV serveris	NetBIOS (TCP)	139	
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	
Lietotāju informācijas vākšana (izmantojot kontaktpersonas skenerī)	LDAP serveris	LDAP (TCP)	389	
		LDAP SSL/TLS (TCP)	636	
		LDAP STARTTLS (TCP)	389	

Lietošana	Mērķis (serveris)	Protokols	Porta numurs
Lietotāju autentificēšana, vācot lietotāju informāciju (izmantojot kontaktpersonas skeneri) 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.

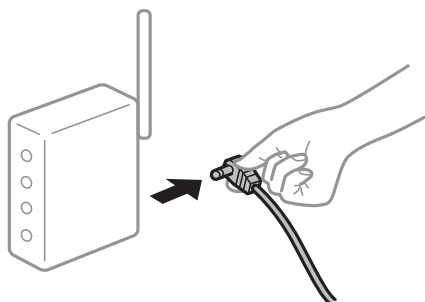
#### ■ Tīkla ierīcēm ir radušās problēmas izveidot Wi-Fi savienojumu.

##### 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 neatbilst jaunajam maršrutētājam.**

**Risinājumi**

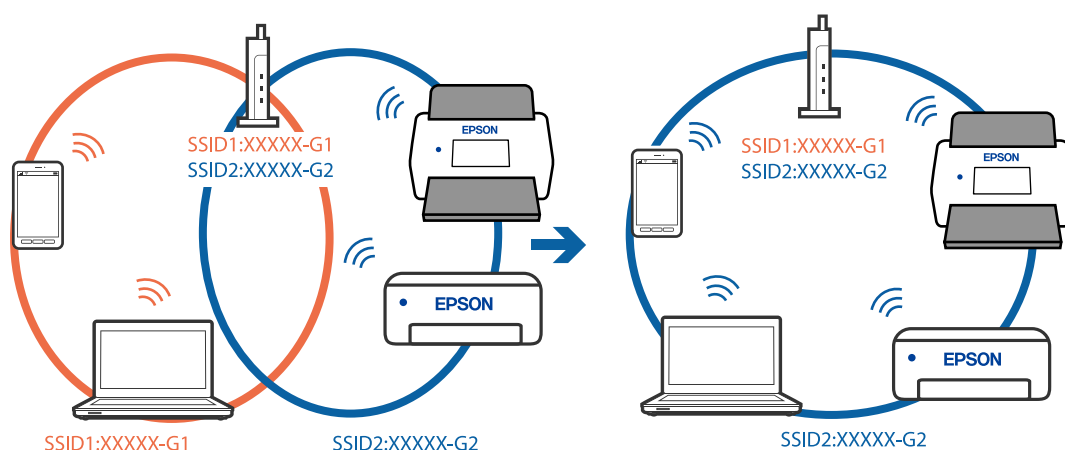
Vēlreiz veiciet savienojuma iestatījumus, lai tie atbilstu jaunajam bezvadu maršrutētājam.

**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 > Tikla 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, tā tad 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.

Sekojiēt 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.  
["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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 atspējot IEEE 802.3az, kā norādīts 2. solī, iespējot 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**

Pārlicinieties, ka skeneris ir ieslēgts.

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

---

# Programmatūra skenera iestatīšanai

Lietojumprogramma skenera darbību konfigurēšanai (Web Config) . . . . .	37
Epson Device Admin. . . . .	38

## Lietojumprogramma skenera darbību konfigurēšanai (Web Config)

Web Config ir programma, kas darbojas tīmekļa pārlūkprogrammās, piemēram, Microsoft Edge un Safari, datorā vai viedierīcē. Var apstiprināt skenera statusu vai mainīt tīkla pakalpojuma un skenera iestatījumus. Lai izmantotu programmu Web Config, savienojiet skeneri un datoru vai ierīci ar vienu tīklu.

Tiek atbalstītas šādas pārlūkprogrammas. Lietojiet jaunāko versiju.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

### **Piezīme:**

Jums var tikt pieprasīts ievadīt administratora paroli, kad izmantojat šo ierīci. Papildinformāciju par administratora paroli skatiet tālāk.

*"Piezīmes par administratora paroli" 10. lpp.*

### **Saistītā informācija**

➔ "Nevar piekļūt Web Config" 64. lpp.

## Web Config palaišana tīmekļa pārlūkprogrammā

Skenerim ir iebūvēta programmatūra Web Config (tīmekļa lapa, kurā var veikt iestatījumus). Lai piekļūtu Web Config, pārlūkprogrammā vienkārši ievadiet tīklam pievienota skenera IP adresi.

1. Pārbaudiet skenera IP adresi.

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

IP adreses piemērs: 192.168.100.201

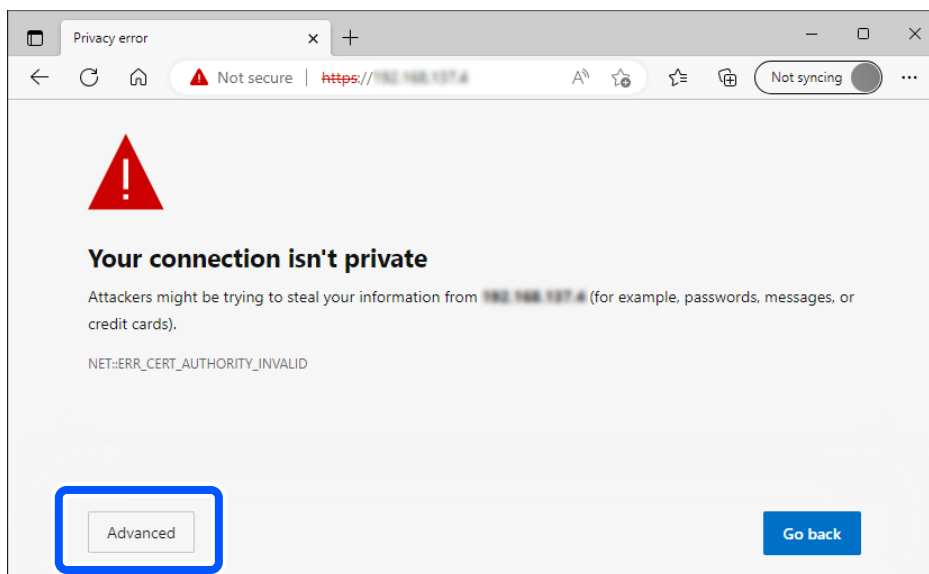
2. Datorā vai viedierīcē palaidiet tīmekļa pārlūkprogrammu un tad ievadiet skenera IP adresi adreses joslā.

Formāts: http://skenera IP adrese/

Piemērs: http://192.168.100.201/

A pārlūkprogrammā tiek parādīts brīdinājuma ekrāns, varat droši ignorēt brīdinājumu un parādīt tīmekļa lapu (Web Config). 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. Atkarībā no jūsu pārlūkprogrammas, lai skatītu tīmekļa lapu, var būt nepieciešams noklikšķināt uz **Advanced Settings**.

Piemērs: Microsoft Edge



**Piezīme:**

Ja brīdinājuma ekrāns netiek parādīts, pārejiet uz nākamo soli.

IPv6 adresēm izmantojiet šādu formātu.

Formāts: `http://[skenera IP adrese]/`

Piemērs: `http://[2001:db8::1000:1]/`

3. Lai mainītu skenera iestatījumus, ir jāpiesakās kā Web Config administratoram.

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

Tālāk sniegtas Web Config sākotnējās vērtības administratora informācijai.

·Lietotājsvārds: nav (tukšs)

·Parole: atkarībā no etiķetes, kas piestiprināta produktam.

Ja produkta aizmugurē ir piestiprināta etiķete „PASSWORD”, ievadiet etiķetē redzamo 8 ciparu numuru. Ja etiķete „PASSWORD” nav piestiprināta, kā administratora paroli ievadiet sērijas numuru, kas redzams produkta aizmugurē piestiprinātajā etiķetē.

**Piezīme:**

Ja ekrāna augšdaļā labajā pusē redzams **Log out**, jūs jau esat pierakstījies kā administrators.

Jūs tiksiet izrakstīti automātiski pēc aptuveni 20 minūtēm bezdarbības.

---

## 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.

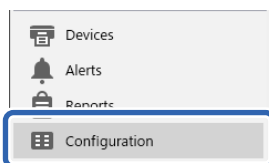
Varat lejupielādēt Epson Device Admin no Epson atbalsta tīmekļa vietnes. Papildinformāciju par to, kā izmantot šo lietojumprogrammu, skatiet Epson Device Admin dokumentācijā vai palīdzības sadaļā.

## Konfigurācijas veidne

### Konfigurācijas veidnes izveidošana

No jauna izveidojiet konfigurācijas veidni.

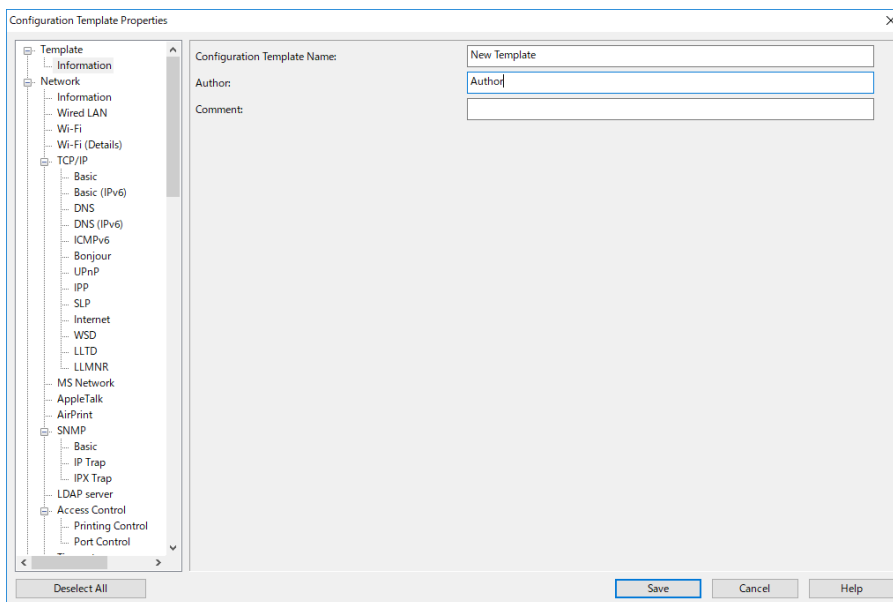
1. Palaidiet Epson Device Admin.
2. Sānu joslas uzdevumu izvēlnē atlasiet **Configuration**.



3. Lentēs 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).

Vienums	Skaidrojums
Comment	<p>levadiet pieņemtu informāciju.</p> <p>levadiet līdz 1024 rakstzīmēm Unicode formātā (UTF-8).</p>

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

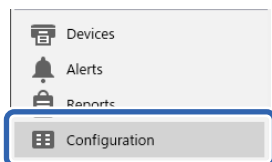
Lietojiet saglabāto konfigurācijas veidni skenerim. Tiek lietoti veidnē atlasītie vienumi. Jā mērķa skenerim nav piemērotas funkcijas, tā netiek lietota.

**Piezīme:**

Ja skenerim iestatīta administratora parole, konfigurējiet paroli pirms tam.

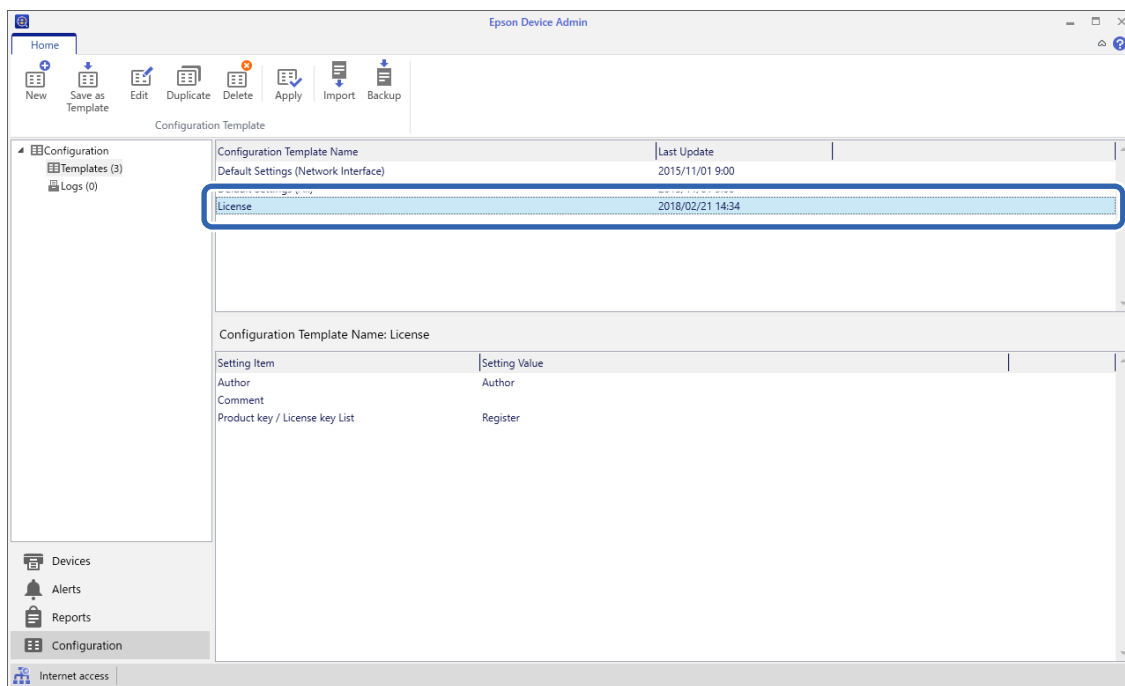
1. Ierīces saraksta ekrāna lentes izvēlnē atlasiet **Options > Password manager**.
2. Izvēlieties **Enable automatic password management** un pēc tam noklikšķiniet uz **Password manager**.
3. Atlasiet atbilstošo skeneri un pēc tam noklikšķiniet uz **Edit**.
4. Iestatiet paroli un noklikšķiniet uz **OK**.

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





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



3. Lentēs izvēlnē noklikšķiniet uz **Apply**.

Tiek parādīts ierīces atlasē ekrāns.

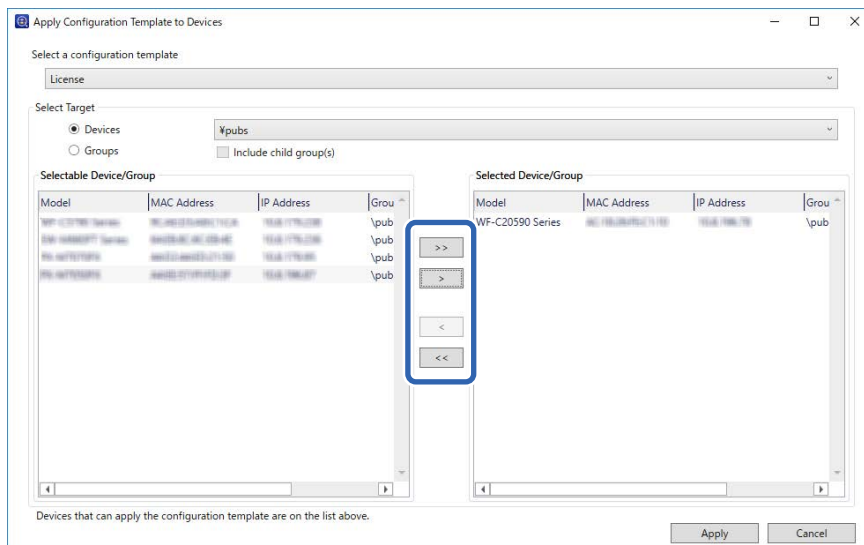


4. Atlasiet konfigurācijas veidni, ko vēlaties lietot.

**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.

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



- Noklikšķiniet uz **Apply**.  
Tiek parādīts apstiprinājuma ekrāns lietotajai konfigurācijas veidnei.
- Noklikšķiniet uz **OK**, lai lietotu konfigurācijas veidni.
- Kad tiek parādīts ziņojums ar informāciju par to, ka procedūra ir pabeigta, noklikšķiniet uz **OK**.
- Noklikšķiniet uz **Details** un pārbaudiet informāciju.  
Kad lietotajiem vienumiem tiek parādīts , piemērošana ir veiksmīgi pabeigta.
- Noklikšķiniet uz **Close**.

# Nepieciešamie skenēšanas iestatījumi

E-pasta servera reģistrēšana. . . . .	44
Tikla mapes izveide. . . . .	46
Kontaktpersonu pieejamības sniegšana. . . . .	54
Funkcijas AirPrint iestatīšana. . . . .	63
Problēmas sagatavot tīkla skenēšanu. . . . .	64

## E-pasta servera reģistrēšana

Pirms e-pasta servera konfigurēšanas pārbaudiet turpmāko.

Skeneris ir savienots ar tīklu

E-pasta servera iestatījumu informācija

Ja izmantojat interneta e-pasta serveri, pārbaudiet pakalpojumu sniedzēja vai vietnes iestatījumu informāciju.

### Reģistrēšana

Pieklūstiet Web Config, atlasiet cilni **Network > Email Server > Basic**.

["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

Iestatījumus var veikt arī skenera vadības panelī. Atlasiet **Iestatījumi > Tīkla iestatījumi > Papildu > E-pasta serveris > Servera iestatījumi**.

### E-pasta servera iestatījumu vienumi

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 izvēlaties <b>SMTP AUTH</b> vai <b>POP before SMTP</b> kā <b>Authentication Method</b> , ievadiet autentificētā konta nosaukumu. Ievadiet no 0 līdz 255 rakstzīmēm ASCII (0x20–0x7E).	
Authenticated Password	Ja izvēlaties <b>SMTP AUTH</b> vai <b>POP before SMTP</b> kā <b>Authentication Method</b> , ievadiet autentificēto paroli. Ievadiet no 0 līdz 20 ASCII rakstzīmēm (0x20–0x7E).	
Sender's Email Address	Iestatiet e-pasta adresi, kas tiks izmantota, lai nosūtītu e-pastus no skenera. Lai gan varat izmantot esošo e-pasta adresi, iesakām iegādāties un iestatīt īpašu e-pasta adresi, lai to varētu atšķirt no e-pastiem, kas tiek sūtīti no skenera.  Ievadiet no 0 līdz 255 rakstzīmēm ASCII (0x20–0x7E), izņemot : ( ) < > [ ] ; ¥. Pirmā rakstzīme nedrīkst būt punkts (.).	
SMTP Server Address	Ievadiet no 0 līdz 255 rakstzīmēm, izmantojot A–Z a–z 0–9 . - . Var izmantot IPv4 vai FQDN formātu.	
SMTP Server Port Number	Ievadiet skaitli no 1 līdz 65 535.	
Secure Connection	Norādiet e-pasta servera drošā savienojuma metodi.	
	None	Atlasot <b>POP before SMTP</b> kā <b>Authentication Method</b> iestatījumu, savienojuma metode tiek iestatīta kā <b>None</b> .
	SSL/TLS	Tas ir pieejams, kad <b>Authentication Method</b> ir iestatīta kā <b>Off</b> vai „ <b>SMTP AUTH</b> ”.
	STARTTLS	Tas ir pieejams, kad <b>Authentication Method</b> ir iestatīta kā <b>Off</b> vai „ <b>SMTP AUTH</b> ”.
Certificate Validation (tikai operētājsistēmā Web Config)	Iespējot šo funkciju, sertifikāts tiek validēts. Mēs iesakām iestatīt šo opciju uz <b>Enable</b> , ja <b>Secure Connection</b> ir iestatīts uz jebkuru citu opciju, izņemot <b>None</b> .	

Vienums	Iestatījumi un skaidrojums
POP3 Server Address	Ja atlasāt <b>POP before SMTP</b> kā <b>Authentication Method</b> , ievadiet POP3 servera adresi. Varat ievadīt no 0 līdz 255 rakstzīmēm, izmantojot A–Z a-z 0–9. Var izmantot IPv4 vai FQDN formātu.
POP3 Server Port Number	Iestatīts, ja izvēlaties <b>POP before SMTP Authentication Method</b> . Ievadiet skaitli no 1 līdz 65 535.

### Saistītā informācija

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

## E-pasta servera savienojuma pārbaude

1. Atlasiet savienojuma testa izvēlni.

**Iestatot no Web Config:**

Atlasiet cilni **Network > Email Server > Connection Test > Start**.

**Iestatot no vadības paneļa:**

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

Tiek sākts pasta servera savienojuma tests.

2. Pārbaudiet testa rezultātus.

Tests ir veiksmīgs, ja tiek parādīts ziņojums **Connection test was successful**.

Ja tiek parādīta kļūda, izpildiet ziņojumā sniegtos norādījumus, lai kļūdu dzēstu.

["Pasta servera savienojuma testēšanas atsaucis" 45. lpp.](#)

## Pasta servera savienojuma testēšanas atsaucis

Ziņojums	Cēlonis
SMTP server communication error. Check the following. - Network Settings	Šis ziņojums tiek parādīts, ja <ul style="list-style-type: none"> <li><input type="checkbox"/> Skeneris nav savienots ar tīklu</li> <li><input type="checkbox"/> Ir notikusi servera SMTP atteice</li> <li><input type="checkbox"/> Sakaru laikā tiek pārtraukts tīkla savienojums</li> <li><input type="checkbox"/> Saņemti nepilnīgi dati</li> </ul>
POP3 server communication error. Check the following. - Network Settings	Šis ziņojums tiek parādīts, ja <ul style="list-style-type: none"> <li><input type="checkbox"/> Skeneris nav savienots ar tīklu</li> <li><input type="checkbox"/> Ir notikusi servera POP3 atteice</li> <li><input type="checkbox"/> Sakaru laikā tiek pārtraukts tīkla savienojums</li> <li><input type="checkbox"/> Saņemti nepilnīgi dati</li> </ul>
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Šis ziņojums tiek parādīts, ja <ul style="list-style-type: none"> <li><input type="checkbox"/> Neizdodas savienojums ar DNS serveri</li> <li><input type="checkbox"/> Neizdodas atpazīt SMTP servera nosaukumu</li> </ul>

Ziņojums	Cēlonis
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Šis ziņojums tiek parādīts, ja <input type="checkbox"/> Neizdodas savienojums ar DNS serveri <input type="checkbox"/> 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 ir radusies servera un klienta SMTP neatbilstība vai ja serveris neatbalsta SMTP drošu 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 izmantot SMTP drošajam savienojumam 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.
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.

## Tikla mapes izveide

Izveidojiet tikla mapi datorā. Datoram jābūt pieslēgtam tam pašam tīklam, kurā ir skeneris.


Tīkla mapes iestatīšanas metode atšķiras atkarībā no vides. Šis ir tīkla mapes izveides piemērs datora darbvirsnā ar šādu vidi.

- Operētājsistēma: Windows 10
- Koplietotās mapes izveides vieta: darbvirsma
- Mapes ceļš: C:\Users\xxxx\Desktop\scan\_folder (izveidojiet tīkla mapi ar nosaukumu „scan\_folder” uz darbvirsmas)

1. Piesakieties datorā, kurā vēlaties izveidot tīkla mapi, izmantojot lietotāja kontu ar administratora tiesībām.

**Piezīme:**

*Ja nezināt, kuram lietotāja kontam ir administratora tiesības, sazinieties ar datora administratoru.*

2. Pārliecinieties, ka ierīces nosaukums (datora nosaukums) nesatur divbaitu rakstzīmes. Noklikšķiniet uz pogas Windows Sākums un pēc tam atlasiet  **Iestatījumi > Sistēma > Par.**

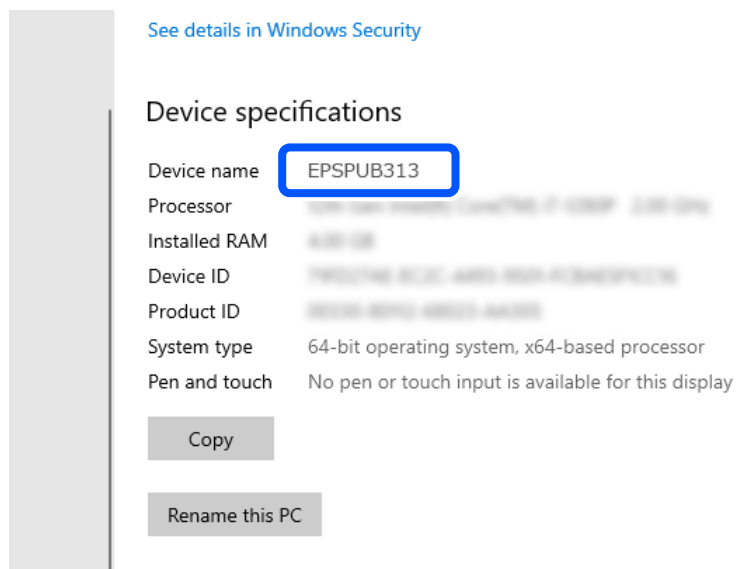
**Piezīme:**

*Ja ierīces nosaukumā ir divbaitu rakstzīmes, faila saglabāšana var neizdoties.*

3. Pārbaudiet, vai virknē, kas parādīta sadaļā **Ierīces specifikācijas > Ierīces nosaukums**, nav divbaitu rakstzīmju.

Ja ierīces nosaukumā ir tikai viena baita rakstzīmes, nevajadzētu rasties problēmām. Aizveriet ekrānu.

Piemērs: EPSPUB313



See details in Windows Security

### Device specifications

Device name	EPSPUB313
Processor	
Installed RAM	
Device ID	
Product ID	
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Copy

Rename this PC



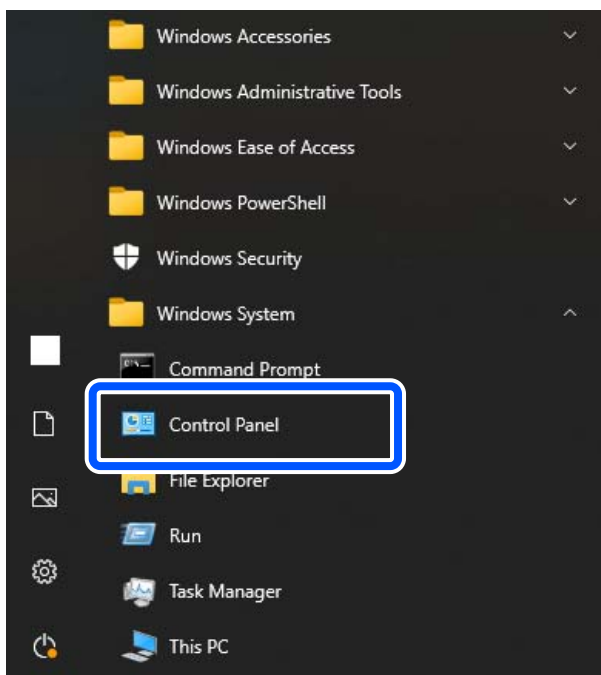
**Svarīga informācija:**

*Ja ierīces nosaukumā ir divbaitu rakstzīmes, izmantojiet datoru, kurā netiek izmantotas divbaitu rakstzīmes, vai pārdēvējiet ierīci.*

*Ja nepieciešams mainīt ierīces nosaukumu, iepriekš sazinieties ar datora administratoru, jo tas var ietekmēt datora pārvaldību un piekļuvi resursiem.*

Pēc tam pārbaudiet datora iestatījumus.

4. Noklikšķiniet uz pogas Windows Sākums un tad atlasiet **Windows sistēma > Vadības panelis**.



5. Vadības paneli noklikšķiniet uz **Tikls un internets > Tikls un koplietošanas centrs > Mainīt uzlabotos koplietošanas iestatījumus**.

Tiek parādīts tikla profils.

6. Pārlicinieties, ka ir atlasīta opcija **Ieslēgt failu un printeru koplietošanu** sadaļā **Failu un printeru koplietošana** tikla profilam (pašreizējais profils).

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

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

Pēc tam izveidojiet tikla mapi.

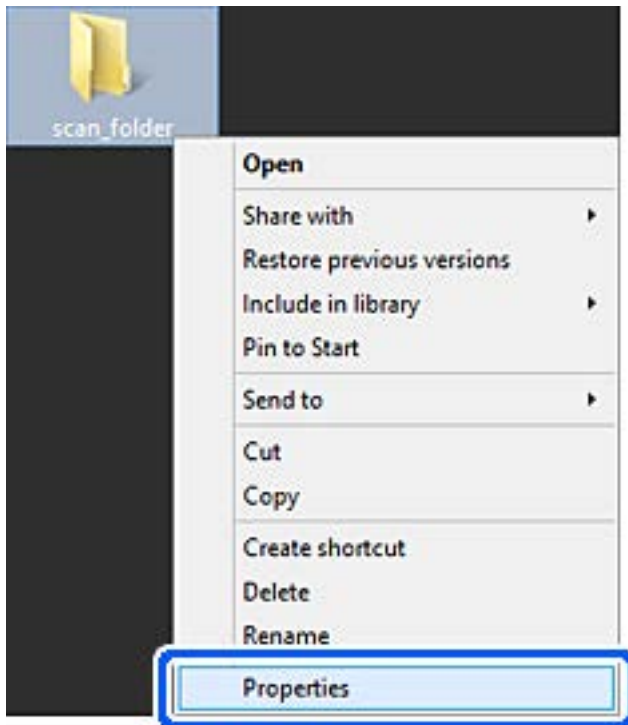
7. Izveidojiet un nosauciet mapi darbvirsnā.

Mapes nosaukumā ievadiet no 1 līdz 12 burtu un ciparu rakstzīmēm. Ja nosaukums pārsniedz 12 rakstzīmes, atkarībā no vides var nebūt iespējams piekļūt mapei.

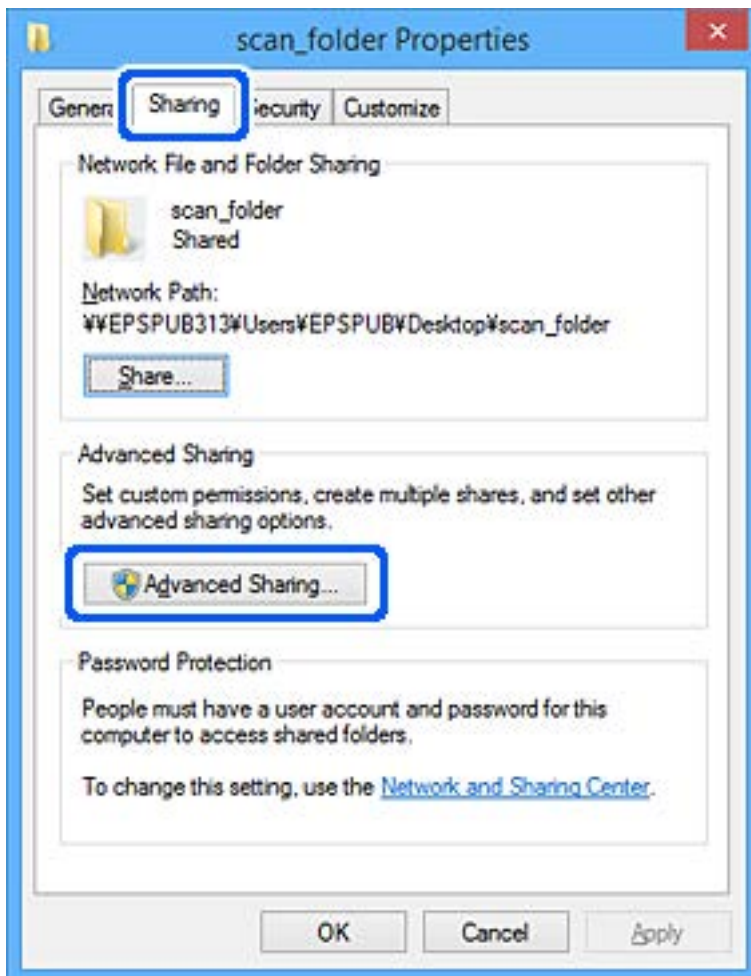
Piemērs: scan\_folder



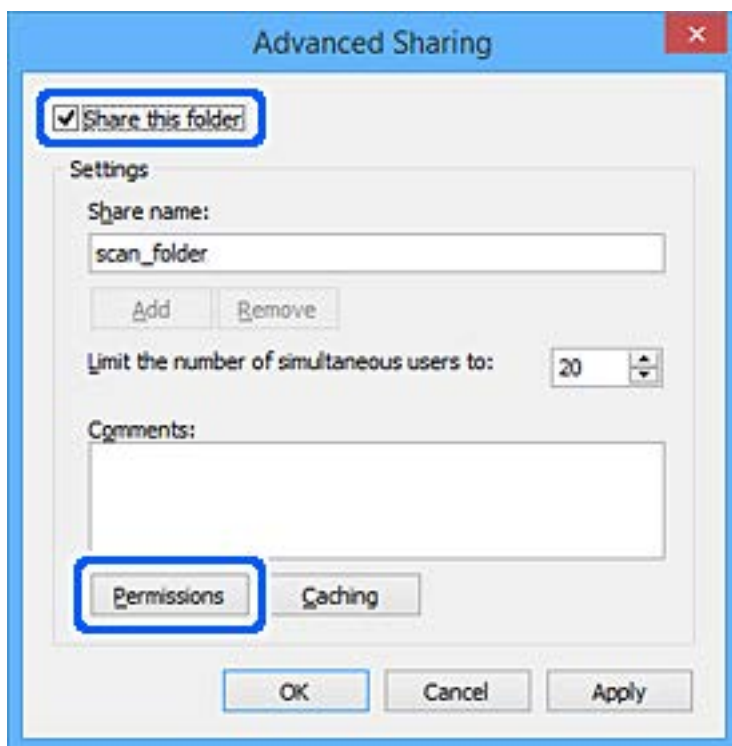
8. Ar peles labo pogu noklikšķiniet uz mapes un tad atlasiet **Rekvizīti**.



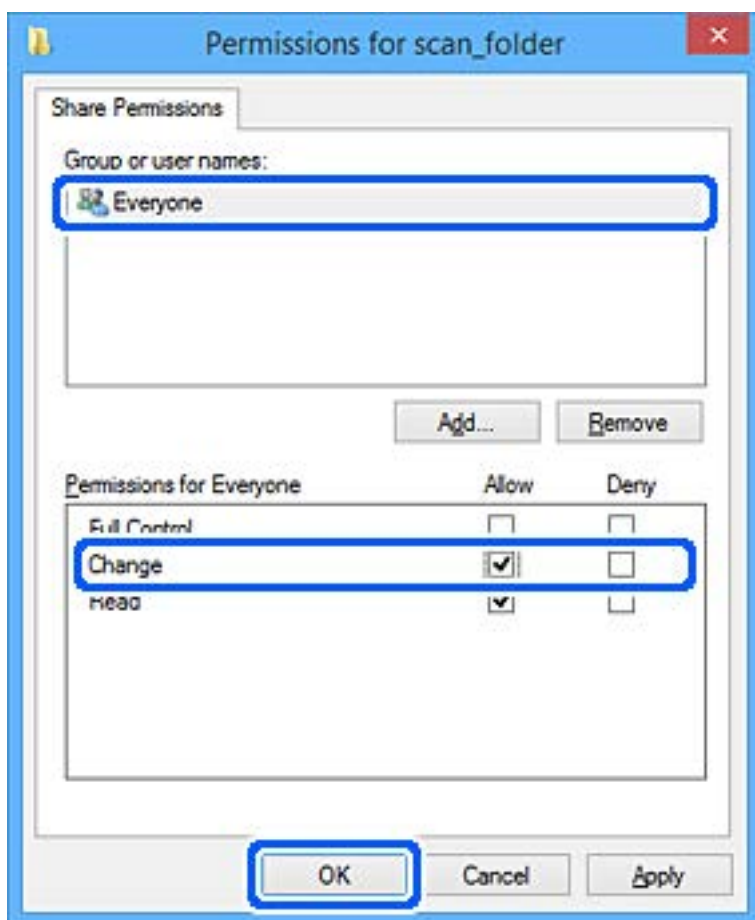
9. Noklikšķiniet uz **Papildu koplietošana** cilnē **Koplietošana**.



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



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

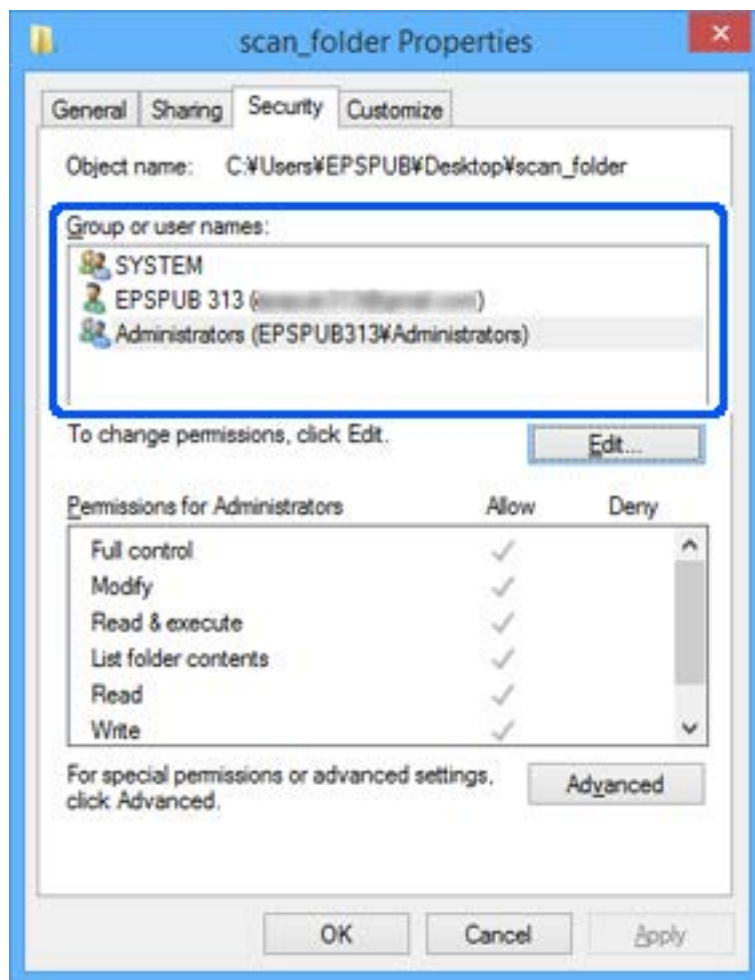


12. Noklikšķiniet uz **Labi**, lai aizvērtu ekrānu un atgrieztos logā Rekvizīti.

**Piezīme:**

Kādām grupām vai lietotājiem ir piekļuve tīkla mapei, varat pārbaudīt cilnē **Drošība** > **Grupu nosaukumi vai lietotājvārdi**.

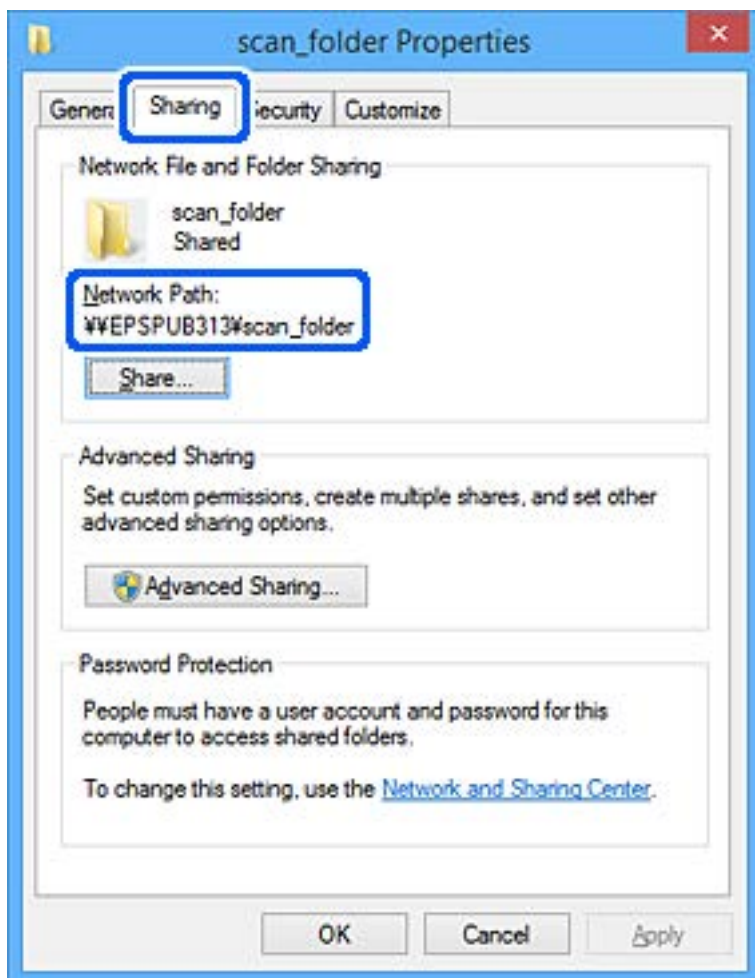
Piemērs: kad datorā pieteicies lietotājs, kā arī administratori var piekļūt tīkla mapei



13. Atlasiet cilni **Koplietošana**.

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

Piemērs: \\EPSPUB313\scan\_folder



14. Noklikšķiniet uz **Aizvērt** vai **Labi**, lai aizvērtu logu.

Tikla mapes izveide ir pabeigta.

---

## 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.
Tikla mape	Skenēšanas datu adresāts. Pirms skenēšanas jā sagatavo tikla mape.

### Saistītā informācija

➔ ["LDAP servera un lietotāju mijiedarbība" 60. lpp.](#)

## Kontaktu konfigurācijas salīdzinājums

Pieejami trīs skenera kontaktpersonu konfigurēšanas riki: 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

## Adresāta iestatīšanas vienumi

Posms	Iestatījumi un skaidrojums
Parastie iestatījumi	
Name	Izmantojot unikoda (UTF-16) 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-16), 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-16) rakstzīmēm, izlaižot daļu „\\”.  Ievadiet tīkla ceļu, kas attēlots mapes rekvizītu ekrānā. Papildinformāciju par tīkla ceļa iestatīšanu skatiet tālāk.  <a href="#">"Tīkla mapes izveide" 46. lpp.</a>
User Name	Lai piekļūtu tīkla mapei, ievadiet lietotājvārdu, ne garāku par 30 unikoda (UTF-16) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F).
Password	Lai piekļūtu tīkla mapei, ievadiet paroli, kas sastāv no 0 līdz 20 unikoda rakstzīmēm (UTF-16). Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F).
FTP	
Secure Connection	Atlasiet FTP vai FTPS atbilstoši faila pārsūtīšanas protokolam, kuru atbalsta FTP serveris. Atlasiet <b>FTPS</b> , lai ļautu skenerim sazināties, izmantojot drošības pasākumus.
Save to	Ievadiet servera nosaukumu, kas sastāv no 1 līdz 253 unikoda rakstzīmēm (UTF-16) un izlaižot „ftp://” vai „ftps://”.
User Name	Lai piekļūtu FTP serverim, ievadiet lietotājvārdu, ne garāku par 30 unikoda (UTF-16) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F). Ja serveris atļauj anonīmus savienojumus, ievadiet lietotājvārdu Anonims un FTP. Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Password	Lai piekļūtu FTP serverim, ievadiet paroli, kas sastāv no 0 līdz 20 unikoda rakstzīmēm (UTF-16). 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 ugunsbūris, atlasiet <b>Passive Mode</b> .
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 <b>FTPS</b> ir izvēlēts kā <b>Secure Connection</b> iestatījums.  Lai veiktu iestatīšanu, CA Certificate jāimportē skenerī.
SharePoint(WebDAV)*	
Secure Connection	Atlasiet HTTP vai HTTPS atbilstoši faila pārsūtīšanas protokolam, kuru atbalsta serveris. Atlasiet <b>HTTPS</b> , lai ļautu skenerim sazināties, izmantojot drošības pasākumus.
Save to	Ievadiet servera nosaukumu, kas sastāv no 1 līdz 253 unikoda rakstzīmēm (UTF-16) un izlaižot „http://” vai „https://”.
User Name	Lai piekļūtu serverim, ievadiet lietotājvārdu, ne garāku par 30 unikoda (UTF-16) rakstzīmēm. Taču neizmantojiet vadības rakstzīmes (0x00–0x1F, 0x7F). Ja nevēlaties to darīt, atstājiet šo lauku tukšu.
Password	Lai piekļūtu serverim, ievadiet paroli, kas sastāv no 0 līdz 20 unikoda rakstzīmēm (UTF-16). 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 <b>HTTPS</b> ir izvēlēts kā <b>Secure Connection</b> iestatījums.  Lai veiktu iestatīšanu, CA Certificate jāimportē skenerī.
Proxy Server	Izvēlieties, vai jāizmanto starpniekservers.

\* SharePoint Online netiek atbalstīts, skenējot uz tīkla mapi no skenera vadības paneļa.

Ja vēlaties saglabāt skenēto attēlu uz SharePoint Online, izmantojiet Document Capture Pro pēc SharePoint Online Connector instalēšanas. Skatiet detalizētu informāciju Document Capture Pro pamācībā.

<https://support.epson.net/dcp/>

## 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. Izvēlieties reģistrējamo numuru un tad noklikšķiniet uz **Edit**.
3. Sadaļā **Type** atlasiet grupu.
4. Noklikšķiniet uz **Select**, lai atvērtu sadaļu **Contact(s) for Group**.  
Tīks 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

➔ ["Web Config palaišana timekļa pārlūkprogrammā" 37. 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. Pieklūstiet 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**.  
Tīks parādīti atlasītie iestatījumi.

### LDAP servera vienumu iestatīšana

Posms	Iestatījumi un skaidrojums
Use LDAP Server	Atlasiet <b>Use</b> vai <b>Do Not Use</b> .
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	Iespējot šo funkciju, tiek validēts LDAP servera sertifikāts. Ieteicams to iestatīt kā <b>Enable</b> . Lai veiktu iestatīšanu, <b>CA Certificate</b> jāimportē skenerī.
Search Timeout (sec)	Iestatiet meklēšanas laiku, pirms iestājas noildze: diapazonā no 5 līdz 300.
Authentication Method	Atlasiet kādu no metodēm. Atlasot <b>Kerberos Authentication</b> , Kerberos iestatījumu veikšanai izvēlieties <b>Kerberos Settings</b> . Lai veiktu Kerberos Authentication, nepieciešama tālāk norādītā vide. <ul style="list-style-type: none"> <li><input type="checkbox"/> Skeneris un DNS serveris var veikt saziņu.</li> <li><input type="checkbox"/> Skenera, KDC servera un autentifikācijai nepieciešamā servera (LDAP servera, SMTP servera, failu servera) laiks tiek sinhronizēts.</li> <li><input type="checkbox"/> Kad pakalpojumu serveris tiek piešķirts kā IP adrese, pakalpojumu servera FQDN tiek reģistrēts DNS servera reversās uzmeklēšanas apgabālā.</li> </ul>
Kerberos Realm to be Used	Atlasot <b>Authentication Method</b> iespēju <b>Kerberos Authentication</b> , 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 <b>Anonymous Authentication</b> iespēja <b>Authentication Method</b> . 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 <b>Anonymous Authentication</b> iespēja <b>Authentication Method</b> . 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 direktoriya 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.
User name Attribute	Norādiet atribūta nosaukumu, kas jāparāda, meklējot lietotājevārdus. 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 lietotājevārds. 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

Posms	Iestatījumi un skaidrojums
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: <ul style="list-style-type: none"> <li><input type="checkbox"/> Nepareiza LDAP servera adrese vai porta numurs.</li> <li><input type="checkbox"/> Ir iestājusies noildze.</li> <li><input type="checkbox"/> Iespēja <b>Do Not Use</b> ir atlasīta kā <b>Use LDAP Server</b>.</li> <li><input type="checkbox"/> Ja iespēja <b>Kerberos Authentication</b> ir atlasīta kā <b>Authentication Method</b>, iestatījums <b>Realm (Domain)</b>, <b>KDC Address</b> un <b>Port Number (Kerberos)</b> nav pareizs.</li> </ul>
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: <ul style="list-style-type: none"> <li><input type="checkbox"/> Laukā <b>User Name</b> un/vai <b>Password</b> nav ievadīta pareiza informācija.</li> <li><input type="checkbox"/> Ja iespēja <b>Kerberos Authentication</b> ir atlasīta kā <b>Authentication Method</b>, laiks un datums var netikt konfigurēti.</li> </ul>
Cannot access the product until processing is complete.	Šis ziņojums tiek parādīts, ja skeneris ir aizņemts.

## Funkcijas AirPrint iestatīšana

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

Vienumi	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 bairi.
Wide-Area Bonjour	Iestatiet neatkarīgi no tā, vai izmantojat pakalpojumu Wide-Area Bonjour. Ja to izmantosit, skeneri jāreģistrē DNS serverī, lai skeneri varētu meklēt segmenta ietvaros.
Enable AirPrint	Enables Bonjour un AirPrint (Skenēšanas pakapojums). Šī poga ir pieejama tikai tad, ja AirPrint ir atspējots.  <i><b>Piezīme:</b></i> <i>Ja AirPrint ir atspējots, tiek atspējota arī Mopria skenēšana no Chromebooks, Windows, un Mopria Scan lietotnes.</i>

## 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, atspējējot 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 izveidotu Self-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 neizmantojot starpniekserveri LAN (lokālām adresēm).

- Mac OS:

atlasiet **System Preferences** (vai **System Settings**) > **Network** > **Advanced** > **Proxies**, pēc tam reģistrējiet **Bypass proxy settings for these Hosts & Domains** 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. . . . . 68

Vadības paneļa sākuma ekrāna rediģēšana. . . . . 70

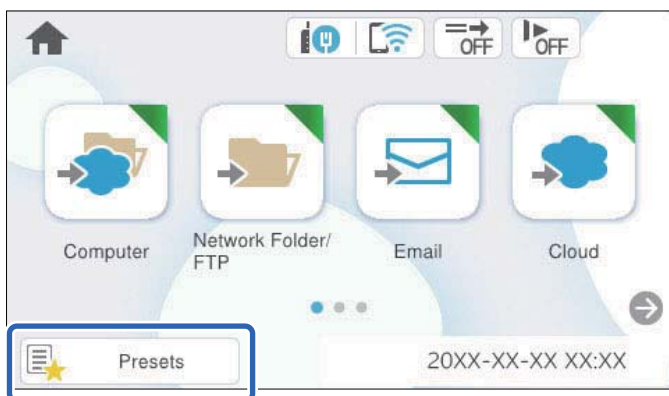
## Priekšiestat. reģistrēšana

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

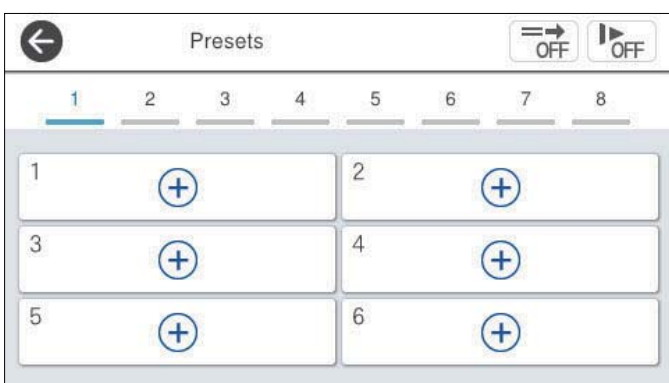
**Piezīme:**

- 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**.

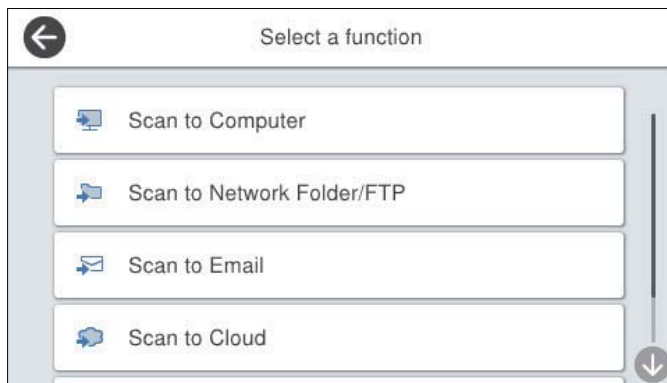
1. Skenera vadības paneļa sākuma ekrānā atlasiet **Priekšiestat.**.




2. Atlasiet .



3. Atlasiet vēlamo izvēlni, lai reģistrētu sākotnējo iestatījumu.



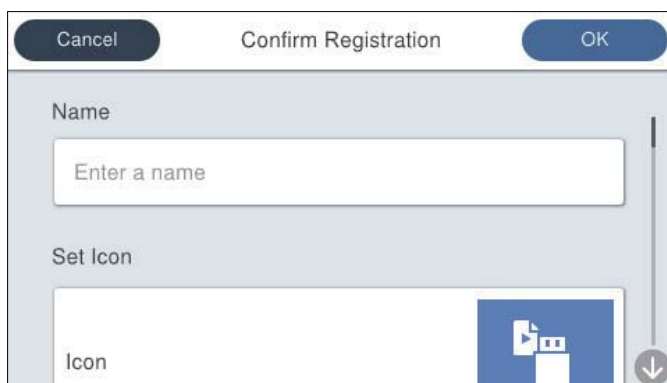
4. Iestatiet katru vienumu un pēc tam atlasiet .

**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.
- 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 paneli atlasot **Iestatījumi > Sākumlapas rediģēšana**.

- Izkārtojums: maina izvēlnes ikonu attēlošanas metodi.  
["Mainīt Izkārtojums sākuma ekrānā" 70. lpp.](#)
- Pievienot ikonu: pievieno ikonas iestatītajiem **Priekšiestat.** vai atgriež ikonas, kuras pirms tām noņēmat no ekrāna.  
["Pievienot ikonu" 71. lpp.](#)
- Noņemt ikonu: noņem ikonu no sākuma ekrāna.  
["Noņemt ikonu" 72. lpp.](#)
- Pārvietot ikonu: maina ikonu attēlošanas kārtību.  
["Pārvietot ikonu" 73. lpp.](#)
- Atjaunot noklus. ikonu attēlojumu: atjauno sākuma ekrāna displeja noklusējuma iestatījumus.

## Mainīt Izkārtojums sākuma ekrānā

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


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

**Līnija:**



**Matrica:**



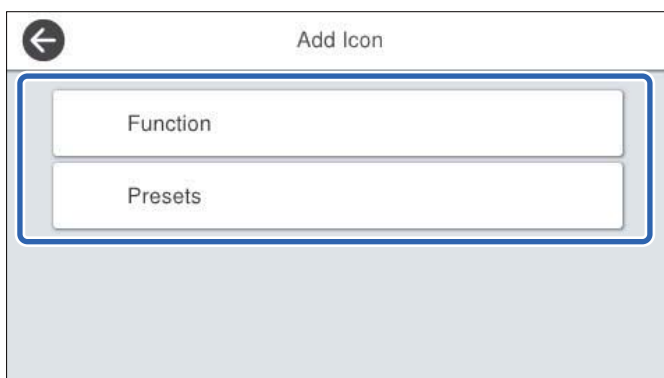
3. Atlasiet , lai atgrieztu un pārbaudītu sākuma ekrānu.

## Pievienot ikonu

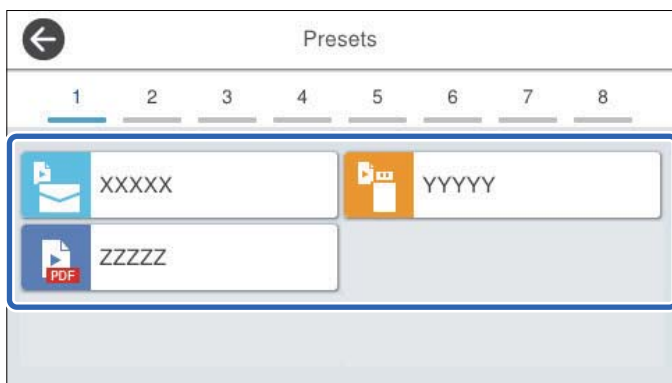
1. Skenera vadības panelī atlasiet **Iestatījumi** > **Sākumlapas rediģēšana** > **Pievienot ikonu**.

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

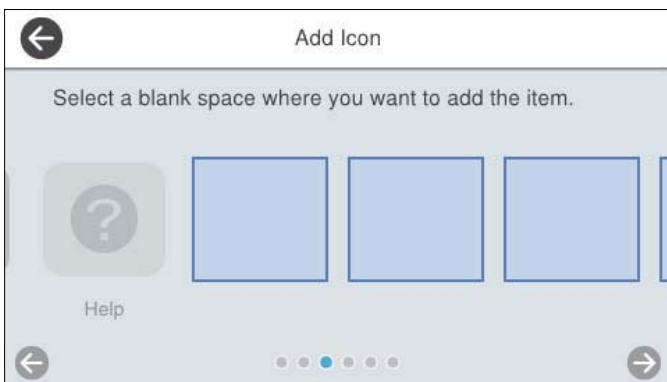
- Funkcija: parāda sākuma ekrāna displeja noklusējuma iestatījumus.
- Priekšiestat.: parāda reģistrētos sākotnējos iestatījumus.




3. Sākuma ekrānā atlasiet vienumu, ko izmantosit.



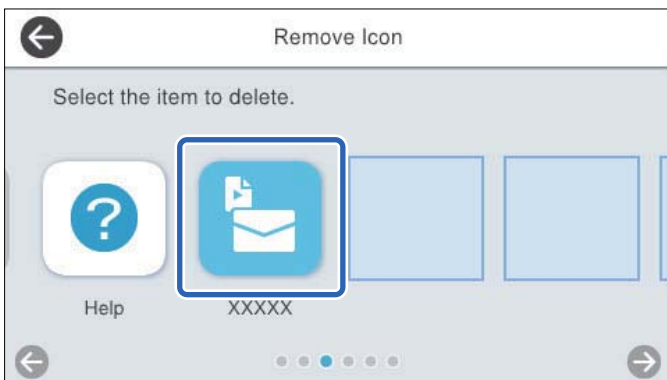
4. Atlasiet tukšo vietu, kurā vēlaties pievienot vienumu.  
Ja vēlaties pievienot vairākas ikonas, atkārtojiet 3. un 4. soli.




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.

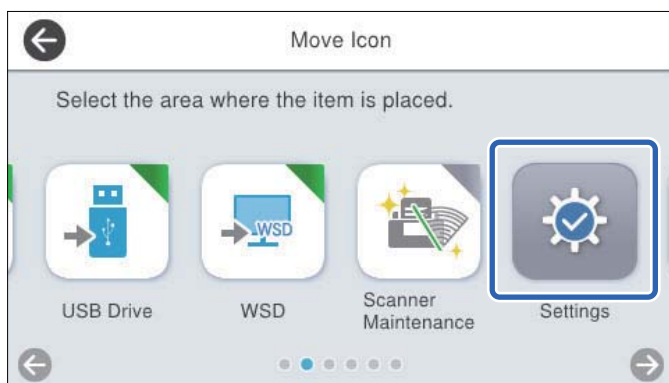




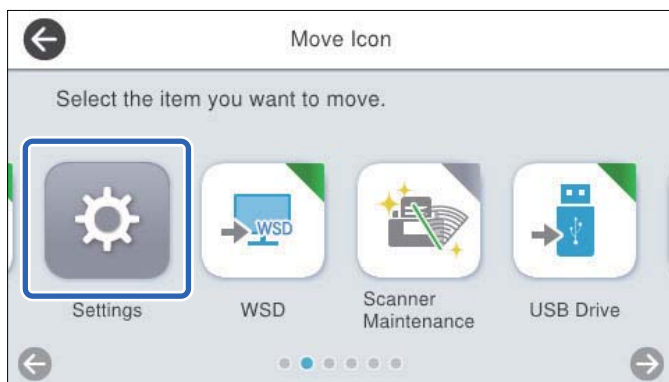
3. Atlasiet **Jā**, lai pabeigtu procedūru.  
Ja vēlaties noņemt vairākas ikonas, atkārtojiet 2 un 3 soli.
4. Atlasiet , lai atgrieztu un pārbaudītu sākuma ekrānu.


## 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

Produkta drošības funkciju. Ievads. . . . .	75
Administratora iestatījumi. . . . .	75
Pieejamo funkciju ierobežošana (Piekļuves vadība). . . . .	81
Ārējās saskarnes atspējošana. . . . .	83
Programmas verifikācijas iespējošana palaišanas laikā. . . . .	83
Tikla skenēšanas atspējošana datorā. . . . .	84
WSD skenēšanas iespējošana vai atspējošana. . . . .	84
Attāla skenera kontrole. . . . .	85
Noklusējuma iestatījumu atjaunošana. . . . .	86
Epson Remote Services informācija. . . . .	87
Problēmu risināšana. . . . .	87

## Produkta drošības funkciju. Ievads

Šajā sadaļā iepazīstinām ar Epson ierīču drošības funkcijām.

Funkcijas nosaukums	Funkcijas veids	Kas jāiestata	Kas jānovērš
Administratora paroles konfigurēšana	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.
Access Control Settings	Ja piesakāties ar iepriekš reģistrētu lietotāja kontu, varat izmantot ierīci.	Reģistrējiet jebkuru lietotāja kontu.  Varat reģistrēt līdz 10 lietotāja kontiem.	Lietotāju ierobežošana novērš nesankcionētu ierīces lietošanu.
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" 75. lpp.](#)
- ➔ ["Ārējās saskarnes atspējošana" 83. lpp.](#)

## Administratora iestatījumi

### Administratora paroles konfigurēšana

Iestatot administratora paroli, jūs varat novērst, ka lietotāji maina sistēmas pārvaldības iestatījumus. Noklusējuma vērtības ir iestatītas iegādes brīdī. Nomainiet tās, ja nepieciešams.

#### Piezīme:

Tālāk ir sniegta administratora informācijas noklusējuma vērtības.

- Lietotājvārds (tiek lietots tikai Web Config): nav (tukšs)
- Parole: atkarībā no etiķetes, kas piestiprināta produktam.

Ja produkta aizmugurē ir piestiprināta etiķete „PASSWORD”, ievadiet etiķetē redzamo 8 ciparu numuru. Ja etiķete „PASSWORD” nav piestiprināta, kā administratora paroli ievadiet sērijas numuru, kas redzams produkta aizmugurē piestiprinātajā etiķetē.

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 programmā Web Config.

1. Atveriet programmu Web Config un atlasiet cilni **Product Security > Change Administrator Password**.
2. Ievadiet nepieciešamo informāciju laukos **Current password**, **User Name**, **New Password** un **Confirm New Password**.

Jaunajai parolei jābūt 8 līdz 20 rakstzīmes garai un tajā var iekļaut tikai viena bita burtciparu rakstzīmes un simbolus.

**Piezīme:**

*Tālāk ir sniegta administratora informācijas noklusējuma vērtības.*

*Lietotājnāvs: nav (tukšs)*

*Parole: atkarībā no etiķetes, kas piestiprināta produktam.*

*Ja produkta aizmugurē ir piestiprināta etiķete „PASSWORD”, ievadiet etiķetē redzamo 8 ciparu numuru. Ja etiķete „PASSWORD” nav piestiprināta, kā administratora paroli ievadiet sērijas numuru, kas redzams produkta aizmugurē piestiprinātajā etiķetē.*



**Svarīga informācija:**

*Neaizmirstiet iestatīto administratora paroli. Ja aizmirstat paroli, to nevarēsiet atiestatīt un būs nepieciešama apkopes personāla palīdzība.*

3. Atlasiet **OK**.

### Saistītā informācija

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

## Administratora paroles maiņa skenera vadības panelī

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:**

*Sākotnējā administratora parole (noklusējums), kas ir iestatīta pirkuma brīdī ir atkarīga no produktam piestiprinātās etiķetes. Ja produkta aizmugurē ir piestiprināta etiķete „PASSWORD”, ievadiet etiķetē redzamo 8 ciparu numuru. Ja etiķete „PASSWORD” nav piestiprināta, kā administratora paroli ievadiet sērijas numuru, kas redzams produkta aizmugurē piestiprinātajā etiķetē.*

5. Ievadiet jauno paroli.

Jaunajai parolei jābūt 8 līdz 20 rakstzīmes garai un tajā var iekļaut tikai viena bita burtciparu rakstzīmes un simbolus.



**Svarīga informācija:**

Neaizmirstiet iestatīto administratora paroli. Ja aizmirstat paroli, to nevarēsiet atiestatīt un būs nepieciešama apkopes personāla palīdzība.


6. Lai apstiprinātu, ievadiet jauno paroli vēlreiz.

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.

### 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 iespētot 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

### Bloķēšanas iestatījums vienumi izvēlnē Iestatījumi

Šis ir to elementu saraksts, kas ir bloķēti vadības paneļa izvēlnē **Iestatījumi**, izmantojot Bloķēšanas iestatījums.

✓: jābloķē.

- : nav bloķējams.

Izvēlne Iestatījumi		Bloķēšanas iestatījums
Pamatiestatījumi		-
	LCD spilgtums	-
	Skaņas	-
	Iemidzināšanas taimeris	✓
	Izslēgšanās taimeris	✓
	Tieša ieslēgšana	✓
	Datuma/laika iestatījumi	✓
	Valoda/Language	✓/-*
	Tastatūra (Šī funkcija var nebūt pieejama atkarībā no reģiona.)	-
	Darbības taimauts	✓
	Datora pievienošana ar USB	✓
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	✓
Lietotāja iestatījumi		✓

Izvēlne Iestatījumi		Bloķēšanas iestatījums
	Tikla mape/FTP	✓
	E-pasts	✓
	Mākonis	✓
	USB disks	✓
Tikla iestatījumi		✓
	Wi-Fi iestatīšana	✓
	Vadu LAN iestatīšana	✓
	Tikla statuss	✓
	Papildu	✓
Tikla 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	✓
	Piekļuves vadība	✓
	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	-
	Nesējloknes skenējumu skaits	-
	Skenējumu skaits pēc apkopes ruļļa nomaiņas	-
	Skenējumu skaits pēc parastās tīrīšanas	-
	Autentifikācijas ierīces statuss	-
	Epson Open Platform informācija	-
	 (Atiestatiet skenējumu skaitu)	✓
Skenera apkope		-
	Ruļļu tīrīšana	-
	Apkopes ruļļa nomaiņa	-
	Atiestatiet skenējumu skaitu	✓
	Nomaiņa	-
	Parasta tīrīšana	-
	Atiestatiet skenējumu skaitu	✓
	Tīrīšana	-
	Stikla tīrīšana	-
Veltnīša 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

Ja **Bloķēšanas iestatījums** ir iespējots, varat izmantot jebkuru no šīm metodēm, lai pieteiktos no skenera vadības paneļa.



1. Ekrāna augšējā labajā pusē pieskarieties pie .
2. Ja tiek parādīts ekrāns **Lietotāja atlase**, atlasiet **Administrators**.
3. Ievadiet paroli, lai pieteiktos.

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

Lai atteiktos, pieskarieties  ekrāna augšdaļai vai nospiediet  pogu.

## Pieejamo funkciju ierobežošana (Piekļuves vadība)

Lietotājus var ierobežot, reģistrējot lietotāju kontus skenerī.

Ja ir iespējota Piekļuves vadība, lietotājs var izmantot skenēšanas funkcijas, ievadot paroli skenera vadības panelī un piesakoties. Nepiesakoties skenēšanu nevar veikt.

Skenēšanu no datora var veikt, reģistrējot savu Lietotājvārds un Parole skenera draiverī (Epson Scan 2). Papildinformāciju par iestatījumu veikšanu skatiet Epson Scan 2 skenēšanas palīdzībā vai izstrādājuma *Lietotāja rokasgrāmata*.

## Lietotāja konta izveide

Varat izveidot Piekļuves vadība kontu.

1. Piekļūstiet Web Config un tad atlasiet **Product Security** cilni > **Access Control Settings** > **User Settings**.
2. Noklikšķiniet uz **Add** skaitam, kuru vēlaties reģistrēt.



### Svarīga informācija:

*Izmantojot skeneri ar Epson vai cita uzņēmuma autentifikācijas sistēmu, reģistrējiet User Name in Access Control Settings slota numurā no 2 līdz 10.*

*Lietojumprogrammatūra, piemēram, autentifikācijas sistēma, izmanto numuru viens, tāpēc lietotāja vārds netiek parādīts skenera vadības panelī.*

3. Iestatiet katru vienumu.
  - User Name:  
Ievadiet lietotājvārdu sarakstā parādāmo vārdu, kas ir no 1 līdz 14 rakstzīmēm garš, izmantojot burtciparu rakstzīmes.
  - Password:  
Ievadiet paroli, kas sastāv no 0 līdz 20 ASCII (0x20–0x7E) rakstzīmēm. Inicializējot paroli, atstājiet to tukšu.
  - Select the check box to enable or disable each function.  
Atlasiet **Scan**, ja vēlaties atļaut skenēšanas funkcijas.
4. Noklikšķiniet uz **Apply**.

## Lietotāja konta rediģēšana

Reģistrēto Piekļuves vadība kontu var rediģēt.

1. Piekļūstiet Web Config un tad atlasiet **Product Security** cilni > **Access Control Settings** > **User Settings**.
2. Noklikšķiniet uz **Edit** numuram, kuru vēlaties rediģēt.
3. Mainiet katru vienumu.
4. Noklikšķiniet uz **Apply**.

## Lietotāja konta dzēšana

Reģistrēto Piekļuves vadība kontu var dzēst.

1. Piekļūstiet Web Config un tad atlasiet **Product Security** cilni > **Access Control Settings** > **User Settings**.
2. Noklikšķiniet uz **Edit** numuram, kuru vēlaties dzēst.
3. Noklikšķiniet uz **Delete**.



**Svarīga informācija:**

Noklikšķinot uz **Delete**, lietotāja konts tiks dzēsts bez apstiprinājuma ziņojuma. Izdzēšot kontu, esiet uzmanīgi.

## Opcijas Piekļuves vadība iespējošana

Kad iespējota Piekļuves vadība, skeneri varēs izmantot tikai reģistrētais lietotājs.

**Piezīme:**

*Ja ir iespējots Access Control Settings, lietotājam ir jāpaziņo konta informācija.*


1. Piekļūstiet Web Config un tad atlasiet **Product Security** cilni > **Access Control Settings** > **Basic**.
2. Atlasiet **Enables Access Control**.

Ja iespējojat Access Control Settings un vēlaties drukāt vai skenēt no viedierīcēm, kurās nav autentifikācijas informācijas, atlasiet **Allow printing and scanning without authentication information from a computer**.

3. Noklikšķiniet uz **OK**.


## Pieteikšanās skenerī, kurā ir iespējota Piekļuves vadība

Ja **Piekļuves vadība** ir iespējots, varat izmantot jebkuru no šīm metodēm, lai pieteiktos no skenera vadības paneļa.

1. Ekrāna augšējā labajā pusē pieskarieties pie .
2. Ja tiek parādīts ekrāns **Lietotāja atlase**, atlasiet lietotāju.

3. Ievadiet paroli, lai pieteiktos.

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

Lai atteiktos, pieskarieties  ekrāna augšdaļai vai nospiediet  pogu.

---

## 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 pārliedzinieties, 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 pārliedzinieties, vai ierīču pārvaldnieka displeja saturs paliek nemainīgs.

Mac OS:

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

### **Saistītā informācija**

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

---

## Programmas verifikācijas iespējošana palaišanas laikā

Ja iespējot programmas verifikācijas funkciju, skeneris veic verifikāciju palaišanas laikā, lai pārbaudītu, vai programmā nav iekļautas trešās personas. Ja tiek konstatētas kādas problēmas, skeneris netiek palaists.

### **Piezīme:**

*Iespējot šo funkciju, tiek palielināts skenera startēšanas laiks.*

1. Atveriet programmu Web Config un tad atlasiet cilni **Product Security > Program Verification on Start Up**.

**Piezīme:**

*Iestatījumus var veikt arī skenera vadības panelī.*

**Iestatījumi > Sistēmas administrēšana > Programmas pārbaude uzsākot**

2. Atlasiet **ON**, lai iespējotu **Program Verification on Start Up**.
3. Noklikšķiniet uz **OK**.

---

## Tikla skenēšanas atspējošana datorā

Varat veikt šādus iestatījumus programmā Web Config, lai atspējotu skenēšanu tīklā, izmantojot Epson Scan 2 no datora.

1. Atveriet programmu Web Config un tad atlasiet cilni **Scan > Network Scan**.
2. Sadaļā **Epson Scan 2** notīriet izvēles rūtiņu **Enable scanning**.
3. Noklikšķiniet uz **Next**.  
Tiek parādīts iestatījumu apstiprinājuma ekrāns.
4. Noklikšķiniet uz **OK**.

---

## WSD skenēšanas iespējošana vai atspējošana

**Piezīme:**

*Iestatījumus var veikt arī skenera vadības panelī. Atlasiet **Iestatījumi > Sistēmas administrēšana > WSD iestatījumi**.*

Varat iespējot vai atspējot WSD skenēšanu.

Ja nevēlaties, lai dators konfigurētu skeneri kā WSD skenēšanas ierīci, atspējojiet WSD iestatījumus.

1. Atveriet programmu Web Config un tad atlasiet cilni **Network Security > Protocol**.
2. Sadaļā **WSD Settings** mainiet izvēles rūtiņu **Enable WSD**.
3. Noklikšķiniet uz **Next**.  
Tiek parādīts iestatījumu apstiprinājuma ekrāns.
4. Noklikšķiniet uz **OK**.

**Piezīme:**

*Ja jūsu dators joprojām konfigurē skeneri kā WSD skenēšanas ierīci, atlasiet **Scan cilni > Network Scan**, un pēc tam notīriet **Enable scanning** izvēles rūtiņu **AirPrint**.*

*Ja AirPrint ir atspējots, tiek atspējota arī Mopria skenēšana no Chromebooks, Windows, un Mopria Scan lietotnes.*

## 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 sāka 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

➔ ["E-pasta servera reģistrēšana" 44. 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 bairus, 32 bairus pārsniedošās 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**.

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

Piemērs: ir mainīta administratora parole.

### Saistītā informācija

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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.

## Web Config izmantošana skenera barošanas avota kontrolei

Ja dators ir attālināts no skenera, joprojām varat izmantot Web Config, lai izslēgtu vai restartētu skeneri.

1. Atveriet programmu Web Config un tad atlasiet cilni **Device Management** > **Power**.
2. Atlasiet **Power Off** vai **Reboot**.
3. Noklikšķiniet uz **Execute**.

---

## Noklusējuma iestatījumu atjaunošana

Varat atlasīt tīkla iestatījumus vai citus skeneri saglabātos iestatījumus, lai atjaunotu to noklusējuma iestatījumus.

1. Atveriet programmu Web Config un tad atlasiet cilni **Device Management** > **Restore Default Settings**.

**Piezīme:**

*Iestatījumus var veikt arī skenera vadības panelī.*

**Iestatījumi** > **Sistēmas administrēšana** > **Atjaunot noklusējuma iestatījumus**

2. Atlasiet programmu, kuru vēlaties atjaunot.

3. Noklikšķiniet uz **Execute**.

Visbeidzot, izpildiet ekrānā redzamos norādījumus.

---

## Epson Remote Services informācija

Epson Remote Services ir pakalpojums, kas ar interneta starpniecību periodiski apkopo skenera informāciju. To var izmantot, lai prognozētu, kad patēriņa materiālus un rezerves daļas būs nepieciešams nomainīt vai papildināt un lai ātri atrisinātu kļūdas vai problēmas.

Lai iegūtu vairāk informācijas, sazinieties ar izplatītāju Epson Remote Services.

---

## Problēmu risināšana

### Aizmirsta administratora parole

Nepieciešama apkopes personāla palīdzība. Sazinieties ar vietējo izplatītāju.

**Piezīme:**

*Tālāk sniegta Web Config sākotnējās vērtības administratoram.*

*Lietotājvārds: nav (tukšs)*

*Parole: atkarībā no etiķetes, kas piestiprināta produktam.*

*Ja produkta aizmugurē ir piestiprināta etiķete „PASSWORD”, ievadiet etiķetē redzamo 8 ciparu numuru.*

*Ja etiķete „PASSWORD” nav piestiprināta, kā administratora paroli ievadiet sērijas numuru, kas redzams produkta aizmugurē piestiprinātajā etiķetē.*

*Ja atjaunojat administratora paroli, tā tiek atiestatīta uz sākotnējo vērtību iegādes brīdī.*

# Tīkla drošības iestatījumi

Drošības iestatījumi un bīstamības novēršana. . . . .	89
Vadība, izmantojot protokolus. . . . .	90
Ciparsertifikāta lietošana. . . . .	93
SSL/TLS sakari ar skeneri. . . . .	98
Šifrētie sakari, izmantojot IPsec/IP filtrēšanu. . . . .	99
Skenera pievienošana IEEE802.1X tīklam. . . . .	110
Drošības papildu iestatījumu problēmu risināšana. . . . .	112



## 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 ārpusē, 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.	Netišu 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.	legūstiet sertificēšanas iestādes parakstītu sertifikātu un tad importējiet to skeneri.	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" 90. lpp.](#)
- ➔ ["SSL/TLS sakari ar skeneri" 98. lpp.](#)
- ➔ ["Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 99. lpp.](#)
- ➔ ["Skenera pievienošana IEEE802.1X tīklam" 110. 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. Tikla 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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. Iespējot šo funkciju, var pievienot WSD ierīces un skenēt no WSD porta.
LLTD Settings	Var iespējot vai atspējot LLTD funkciju. Iespējot šo funkciju, tas tiek parādīts Windows tīkla kartē.
LLMNR Settings	Var iespējot vai atspējot LLMNR funkciju. Iespējot 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 <b>Read Only</b> vai <b>Read/Write</b> .
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" 93. lpp.](#)
- ➔ ["Pašparakstīta sertifikāta atjaunināšana" 97. lpp.](#)
- ➔ ["CA Certificate konfigurēšana" 97. 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 sertifikācijas 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 sertifikācijas iestādes attiecīgā formāta **CSR** sertifikāta lejupielādes pogas.



**Svarīga informācija:**

*Nēģenerējiet CSR no jauna. Ja tā izdarāt, iespējams, nevarēs importēt izsniegtu CA-signed Certificate.*

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

Ievērojiet katras sertifikācijas 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**

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

**CSR vienumu iestatīšana**

Posms	Iestatījumi un skaidrojums
Key Length	Atlasiet CSR atslēgas garumu.
Common Name	<p>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.</p> <p>Pirmais elements tiek saglabāts pie kopējā nosaukuma, bet citi elementi tiek saglabāti sertifikāta tēmas aizstājvārda laukā.</p> <p>Piemērs:</p> <p>Skenera IP adrese: 192.0.2.123, skenera nosaukums: EPSONA1B2C3</p> <p>Common Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123</p>

Posms	Iestatījumi un skaidrojums
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 <b>Sender's Email Address</b> cilnē <b>Network &gt; Email Server &gt; Basic</b> .

## CA parakstīta sertifikāta importēšana

Importējiet iegūto CA-signed Certificate skenerī.



### Svarīga informācija:

- Pārliedzieties, 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**

➔ "Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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 <b>Certificate with Private Key (PKCS#12)</b> , ievadiet paroli, kas šifrē privāto paroli, kas tika iestatīta, iegūstot sertifikātu.
CA Certificate 1	Ja sertifikāta formāts ir <b>Certificate (PEM/DER)</b> , 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 <b>Certificate (PEM/DER)</b> , 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**

➔ "Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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. Pieklūstiet 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**

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

## CA Certificate konfigurēšana

Iestatot CA Certificate, varat validēt CA sertifikāta ceļu serverim, kuram pieklūst 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 skeneri.

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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

---

## SSL/TLS sakari ar skeneri

Ja servera sertifikāts ir iestatīts, izmantojot SSL/TLS (drošīgzdu 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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

- ➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)
- ➔ ["CA-signed Certificate konfigurēšana" 93. lpp.](#)
- ➔ ["CA Certificate konfigurēšana" 97. 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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 <b>Certificate</b> , ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
Pre-Shared Key	Izvēloties vienuma <b>Authentication Method</b> iestatījumu <b>Pre-Shared Key</b> , 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 <b>Certificate</b> , ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
	ID Type	Ja atlasāt <b>Pre-Shared Key</b> sadaļā <b>Authentication Method</b> , atlasiet skenera ID tipu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@”, „#” vai „=”. <b>Distinguished Name:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=”. <b>IP Address:</b> ievadiet IPv4 vai IPv6 formātu. <b>FQDN:</b> ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-” un punktu (.). <b>Email Address:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@”. <b>Key ID:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma <b>Authentication Method</b> iestatījumu <b>Pre-Shared Key</b> , 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 <b>Certificate</b> , ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
	ID Type	Ja atlasāt <b>Pre-Shared Key</b> sadaļā <b>Authentication Method</b> , atlasiet ID tipu ierīcei, kuru vēlaties autentificēt.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@”, „#” vai „=”. <b>Distinguished Name:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=”. <b>IP Address:</b> ievadiet IPv4 vai IPv6 formātu. <b>FQDN:</b> ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-” un punktu (.). <b>Email Address:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@”. <b>Key ID:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma <b>Authentication Method</b> iestatījumu <b>Pre-Shared Key</b> , 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. <b>Remote Gateway(Tunnel Mode):</b> Ja vienuma <b>Encapsulation</b> iestatījums ir <b>Tunnel Mode</b> , 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 vēlēties 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 <b>ESP</b> ir izvēlēts kā <b>Security Protocol</b> iestatījums.
	Authentication	Atlasiet ESP autentificēšanas algoritmu. Tas ir pieejams, kad <b>ESP</b> ir izvēlēts kā <b>Security Protocol</b> iestatījums.
AH	Authentication	Atlasiet AH šifrēšanas algoritmu. Tas ir pieejams, kad <b>AH</b> ir izvēlēts kā <b>Security Protocol</b> 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 metodu.

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 īsākam. 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 <b>IPsec</b> kā <b>Access Control</b> iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
Pre-Shared Key	Izvēloties vienuma <b>Authentication Method</b> iestatījumu <b>Pre-Shared Key</b> , 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 <b>IPsec</b> kā <b>Access Control</b> iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
	ID Type	Ja atlasāt <b>Pre-Shared Key</b> sadaļā <b>Authentication Method</b> , atlasiet skenera ID tipu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@”, „#” vai „=”. <b>Distinguished Name:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=”. <b>IP Address:</b> ievadiet IPv4 vai IPv6 formātu. <b>FQDN:</b> ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-” un punktu (.). <b>Email Address:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@”. <b>Key ID:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma <b>Authentication Method</b> iestatījumu <b>Pre-Shared Key</b> , 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 <b>IPsec</b> kā <b>Access Control</b> iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
	ID Type	Ja atlasāt <b>Pre-Shared Key</b> sadaļā <b>Authentication Method</b> , atlasiet ID tipu ierīcei, kuru vēlaties autentificēt.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@”, „#” vai „=”. <b>Distinguished Name:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=”. <b>IP Address:</b> ievadiet IPv4 vai IPv6 formātu. <b>FQDN:</b> ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-” un punktu (.). <b>Email Address:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@”. <b>Key ID:</b> ievadiet no 1 līdz 255 viena bauta ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma <b>Authentication Method</b> iestatījumu <b>Pre-Shared Key</b> , 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.  <b>Remote Gateway(Tunnel Mode):</b> Ja vienuma <b>Encapsulation</b> iestatījums ir <b>Tunnel Mode</b> , 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 vēlēties 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 <b>ESP</b> ir izvēlēts kā <b>Security Protocol</b> iestatījums.
	Authentication	Atlasiet ESP autentificēšanas algoritmu. Tas ir pieejams, kad <b>ESP</b> ir izvēlēts kā <b>Security Protocol</b> iestatījums.
AH	Authentication	Atlasiet AH šifrēšanas algoritmu. Tas ir pieejams, kad <b>AH</b> ir izvēlēts kā <b>Security Protocol</b> iestatījums.

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

	Local Address (Scanner) iestatīšana		
	IPv4	IPv6* <sup>2</sup>	Any addresses* <sup>3</sup>

<b>Remote Address(Host) iestatīšana</b>	IPv4* <sup>1</sup>	✓	–	✓
	IPv6* <sup>1</sup> , * <sup>2</sup>	–	✓	✓
	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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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

- ➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)
- ➔ ["CA-signed Certificate konfigurēšana" 93. lpp.](#)
- ➔ ["CA Certificate konfigurēšana" 97. 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

## IEEE 802.1X tīkla iestatījumu vienumi

Vienumi	Iestatījumi un skaidrojums	
IEEE802.1X (Wired LAN)	Varat iespējot vai atspējot lapas iestatījumus ( <b>IEEE802.1X &gt; Basic</b> ) 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	Nepieciešams iegūt un importēt CA sertifikātu.
	PEAP-TLS	
	PEAP/MSCHAPv2	Nepieciešams konfigurēt paroli.
	EAP-TTLS	
User ID	Konfigurējiet ID, ko izmantot RADIUS servera autentifikācijai. Ievadiet 1 līdz 128 viena bita ASCII (0x20–0x7E) rakstzīmes.	
Password	Konfigurējiet paroli skenera autentifikācijai. Ievadiet 1 līdz 128 viena bita ASCII (0x20–0x7E) rakstzīmes. Ja izmantojat Windows serveri kāRADIUS serveri, ievadīt varat līdz 127 rakstzīmēm.	
Confirm Password	Ievadiet iestatīto paroli, lai apstiprinātu.	
Server ID	Jūs varat konfigurēt servera ID, lai autentificētos ar norādītu RADIUS serveri. Autentificēšana pārbauda, vai RADIUS servera sūtītā servera sertifikāta laukums subject/subjectAltName satur servera ID. Ievadiet 0 līdz 128 viena bita ASCII (0x20–0x7E) rakstzīmes.	
Certificate Validation (vadu LAN)	Ja vēlaties veikt <b>Certificate Validation</b> , izmantojot <b>IEEE802.1X (Wired LAN)</b> , atlasiet <b>Enable</b> . Ja izvēlaties iespējot, skatiet saistīto informāciju un importējiet <b>CA Certificate</b> . Ņemiet vērā, ka Certificate Validation vienmēr ir iespējota IEEE802.1X (Wi-Fi). Noteikti importējiet CA Certificate.	
Anonymous Name	Ja vienumam <b>EAP Type</b> atlasāt <b>PEAP-TLS</b> vai <b>PEAP/MSCHAPv2</b> , PEAP autentifikācijas 1. posmam lietotāja ID vietā varat konfigurēt anonīmu vārdu. Ievadiet 0 līdz 128 viena bita ASCII (0x20–0x7E) rakstzīmes.	

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

#### Saistītā informācija

➔ ["CA Certificate konfigurēšana" 97. lpp.](#)

## 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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

- ➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)
- ➔ ["Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 99. 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" 99. 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**

- ➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)
- ➔ ["Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 99. 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" 99. lpp.](#)

## **Pēc IEEE 802.1X konfigurēšanas neizdodas piekļūt ierīcei**

#### **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.

#### **Saistītā informācija**

- ➔ ["IEEE 802.1X tīkla konfigurēšana" 110. 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" 95. 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" 97. 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" 93. lpp.](#)

## Tiek parādīts ar ciparsertifikāta lietošanu saistīts brīdinājums

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

Ziņojumi	Cēlonis/risinājums
Invalid file.	<p><b>Cēlonis:</b></p> <p>Netiek importēts X509 formāta sertifikāta fails.</p> <p><b>Risinājums:</b></p> <p>Pārlicinieties, vai atlasīt pareizo sertifikāta failu, kas saņemts no uzticamas sertificēšanas iestādes.</p>
	<p><b>Cēlonis:</b></p> <p>Importētais fails ir pārāk liels. Maksimālais lielums ir 5 KB.</p> <p><b>Risinājums:</b></p> <p>Ja atlasīts pareizais fails, iespējams, sertifikāts ir bojāts vai safabrics.</p>
	<p><b>Cēlonis:</b></p> <p>Nederīga sertifikātā iekļautā ķēde.</p> <p><b>Risinājums:</b></p> <p>Papildinformāciju par sertifikātu skatiet sertificēšanas iestādes tīmekļa vietnē.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p><b>Cēlonis:</b></p> <p>PKCS#12 formāta sertifikāta failā ietverti vairāk nekā 3 CA sertifikāti.</p> <p><b>Risinājums:</b></p> <p>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.</p>
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p><b>Cēlonis:</b></p> <p>Beidzies sertifikāta derīguma termiņš.</p> <p><b>Risinājums:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Ja beidzies sertifikāta derīguma termiņš, iegūstiet un importējiet jaunu sertifikātu.</li> <li><input type="checkbox"/> Ja sertifikāta derīguma termiņš nav beidzies, pārlicinieties, vai skenera datums un laiks ir iestatīts pareizi.</li> </ul>
Private key is required.	<p><b>Cēlonis:</b></p> <p>Nav ar sertifikātu pāri savienotas privātas atslēgas.</p> <p><b>Risinājums:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Ja sertifikāts ir PEM/DER formātā un ir iegūts no CSR, izmantojot datoru, norādiet privāto atslēgas failu.</li> <li><input type="checkbox"/> Ja sertifikāts ir PKCS#12 formātā un ir iegūts no CSR, izmantojot datoru, izveidojiet failu, kas satur privāto atslēgu.</li> </ul>
	<p><b>Cēlonis:</b></p> <p>Izmantojot Web Config, no CSR iegūts PEM/DER sertifikāts ir importēts atkārtoti.</p> <p><b>Risinājums:</b></p> <p>Ja sertifikāts ir PEM/DER formātā un ir iegūts no CSR, izmantojot Web Config, to var importēt tikai vienu reizi.</p>

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

#### Saistītā informācija

➔ ["Par ciparsertifikātiem" 93. 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" 95. lpp.](#)

➔ ["CA parakstīta sertifikāta dzēšana" 96. lpp.](#)

---

# Funkcijas Epson Open Platform lietošana

Pārskats par Epson Open Platform. . . . .	120
Epson Open Platform konfigurēšana. . . . .	120
Epson Open Platform validēšana. . . . .	120

## Pārskats par Epson Open Platform

Epson Open Platform ir platforma, kas ļauj izmantot autentifikācijas sistēmas ar šo skeneri.

To var izmantot kopā ar Epson Print Admin (Epson autentifikācijas sistēmu) vai trešās puses nodrošinātu autentifikācijas sistēmu. Varat iegūt žurnālus pēc ierīces un lietotāja, konfigurēt ierīces, kuras lietotāji un grupas var izmantot, iestatīt funkciju ierobežojumus utt.

Ja izveidojat savienojumu ar autentifikācijas ierīci, varat arī veikt lietotāju autentifikāciju, izmantojot ID karti.

---

## Epson Open Platform konfigurēšana

Iespējojiet Epson Open Platform, lai izmantotu ierīci no autentifikācijas sistēmas.

1. Iegūstiet produkta atslēgu no specializētās tīmekļa vietnes.  
Skatiet Epson Open Platform rokasgrāmatu, lai iegūtu informāciju par to, kā iegūt produkta atslēgu.
2. Atveriet programmu Web Config un tad atlasiet cilni **Epson Open Platform > Product Key or License Key**.
3. Pārbaudiet un iestatiet katru vienumu.
  - Serial Number  
Tiek parādīts ierīces sērijas numurs.
  - Epson Open Platform Version  
Izvēlieties versiju no Epson Open Platform. Atbilstošā versija mainās atkarībā no autentifikācijas sistēmas.
  - Product Key or License Key  
Ievadiet iegūto produkta atslēgu.
4. Noklikšķiniet uz **Next**.  
Tiek parādīts iestatījumu apstiprinājuma ekrāns.
5. Noklikšķiniet uz **OK**.  
Šie iestatījumi tiek piemēroti skenerim.

**Piezīme:**

*Epson Print Admin Serverless nevar lietot, ja sistēma ir sinhronizēta ar Epson Open Platform.*

---

## Epson Open Platform validēšana

Epson Open Platform derīgumu var pārbaudīt, izmantojot jebkuru no šādām metodēm.

- Web Config  
Cilnē **Epson Open Platform > Product Key or License Key > Product Key or License Key** un cilnē **Epson Open Platform > Authentication System** tiek parādīta izvēlnes koka kreisajā pusē.
- Skenera vadības panelis  
Pārbaudiet, vai produkta atslēga ir parādīta cilnē **Iestatījumi > Ierīces informācija > Epson Open Platform informācija**.



---

# Autentifikācijas ierīces uzstādīšana

Autentifikācijas ierīces pievienošana. . . . .	122
Autentifikācijas ierīces darbības pārbaude. . . . .	122
Autentifikācijas kartes atpazīšanas apstiprināšana. . . . .	122
Autentifikācijas ierīces problēmu novēršana. . . . .	123

## Autentifikācijas ierīces pievienošana

**Piezīme:**

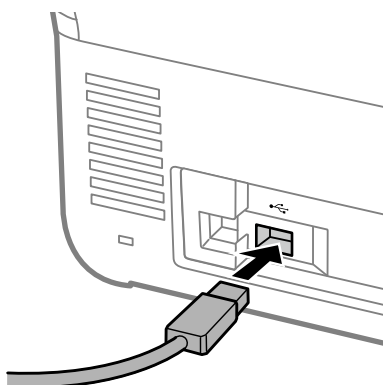
Autentifikācijas ierīci var izmantot, izmantojot autentifikācijas sistēmu.



**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 atlasīsiet **Iestatījumi** > **Ierīces informācija** > **Autentifikācijas ierīces statuss**.

---

## Autentifikācijas kartes atpazīšanas apstiprināšana

Varat pārbaudīt, vai autentifikācijas kartes var atpazīt, izmantojot Web Config.

1. Atveriet programmu Web Config un tad atlasiet cilni **Device Management** > **Card Reader**.
2. Turiet autentifikācijas karti virs autentifikācijas kartes lasītāja.
3. Noklikšķiniet uz **Check**.  
Tiek parādīts rezultāts.

## Autentifikācijas ierīces problēmu novēršana

---

### 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, vai autentifikācijas ierīce un autentifikācijas karte ir sertificētas.  
Lai iegūtu informāciju par atbalstītajām autentifikācijas ierīcēm un kartēm, sazinieties ar izplatītāju.

# Apkope

Skenera korpusa tīrīšana. . . . .	125
Skenera iekšpuses tīrīšana. . . . .	125
Veltnišu bloka nomaiņa. . . . .	130
Ieskenēto lapu skaita atiestate pēc rullīšu nomaiņas. . . . .	135
Enerģijas taupīšana. . . . .	136
Skenera transportēšana. . . . .	136
Iestatījumu dublēšana. . . . .	137
Atjaunot noklusējuma iestatījumus. . . . .	138
Programmu un aparātprogrammatūras atjaunināšana. . . . .	139


## 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 iekšpusēs 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.

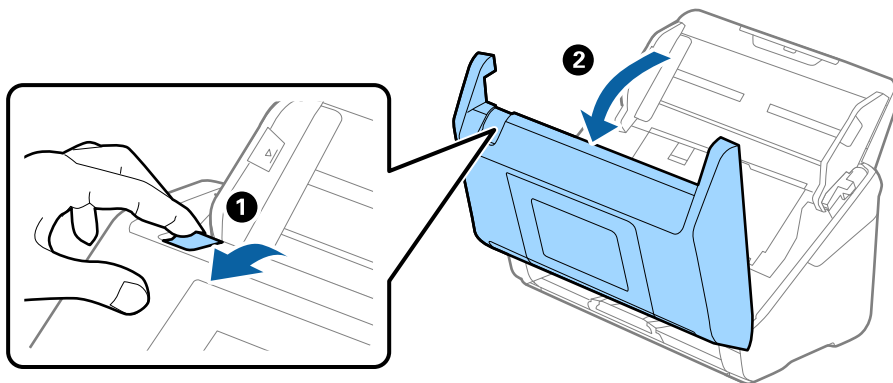


**Svarīga informācija:**

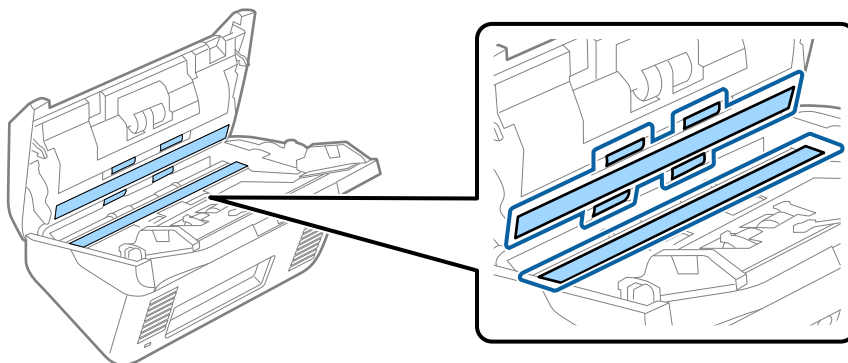
- Skenera tīrīšanai nedrīkst lietot spirtu, atšķaidītāju vai korozīvu šķīdinātāju. Tas var izraisīt deformēšanos vai krāsas maiņu.
- Nekādā gadījumā neizsmidziniet uz skenera nekādus šķidrums vai smērvielas. Aparatūras vai shēmu bojājumi var izraisīt kļūdainu ierīces darbību.
- Nekad neatveriet skenera korpusu.

1. Nospiediet pogu , lai izslēgtu skeneri.
2. Atvienojiet maiņstrāvas adapteri no skenera.

3. Pavelciet sviru un atveriet skenera vāku.



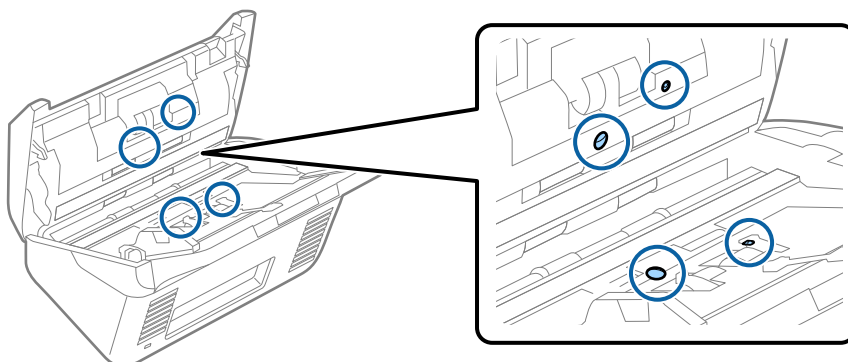
4. Ja uz plastmasas rullīša (4 atrašanās vietas) un stikla virsmas skenera vāka iekšpusē, apakšdaļā ir traipi, noslaukiet tos ar mīkstu drāniņu. Noslaukiet ar mīkstu drāniņu, kas nesatur plūksnas un ir samitrināta ar nelielu daudzumu speciāla tīrīšanas līdzekļa vai ūdens.



**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.



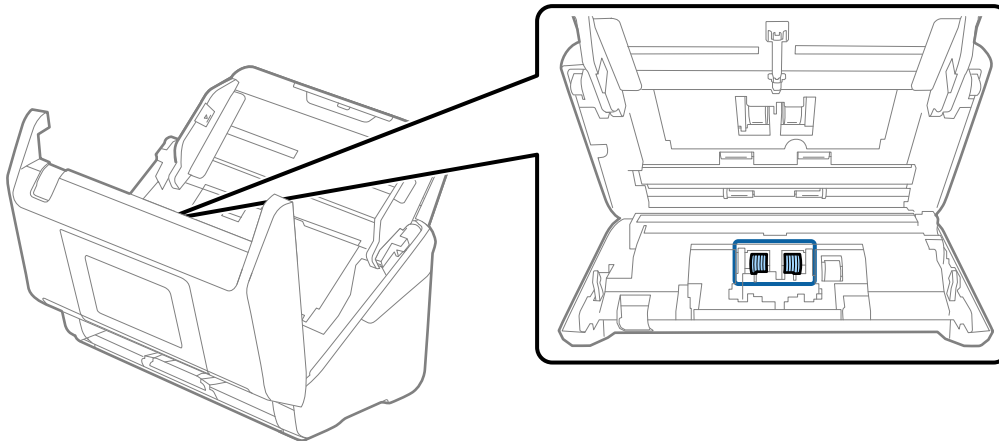


**Svarīga informācija:**

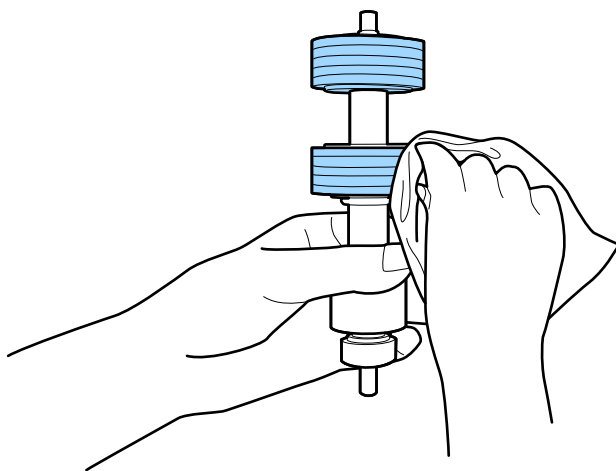
*Nesamitriniet vates kociņu šķidrumā, piemēram, tīrīšanas līdzeklī.*

6. Atveriet vāku un izņemiet atdalīšanas veltnīti.

Plašāku informāciju skatiet sadaļā „Veltņišu bloka nomaiņa”.



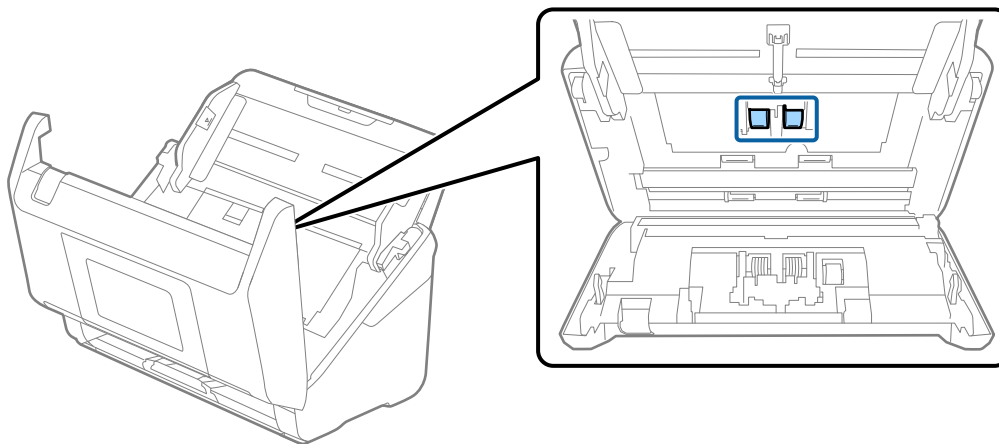
7. Noslaukiet atdalīšanas rullīti. Noslaukiet ar mīkstu drāniņu, kas nesatur plūksnas un ir samitrināta ar nelielu daudzumu speciāla tīrīšanas līdzekļa vai ūdens.



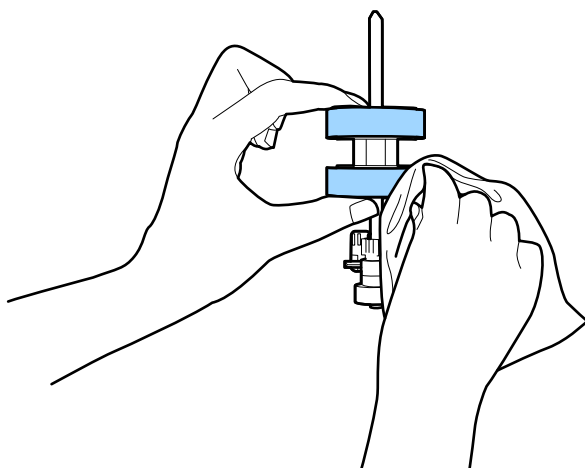
**Svarīga informācija:**

*Veltņiša tīrīšanai izmantojiet tikai autentisku Epson tīrīšanas komplektu vai mīkstu, samitrinātu drāniņu. Izmantojot sausu drāniņu, var sabojāt veltņiša virsmu.*

- Atveriet vāku un izņemiet uztveršanas veltnīti.  
Plašāku informāciju skatiet sadaļā „Veltnīšu bloka nomainīšana”.



- Noslaukiet uztveršanas veltnīti. Noslaukiet ar mīkstu drāniņu, kas nesatur plūksnas un ir samitrināta ar nelielu daudzumu speciāla tīrīšanas līdzekļa vai ūdens.



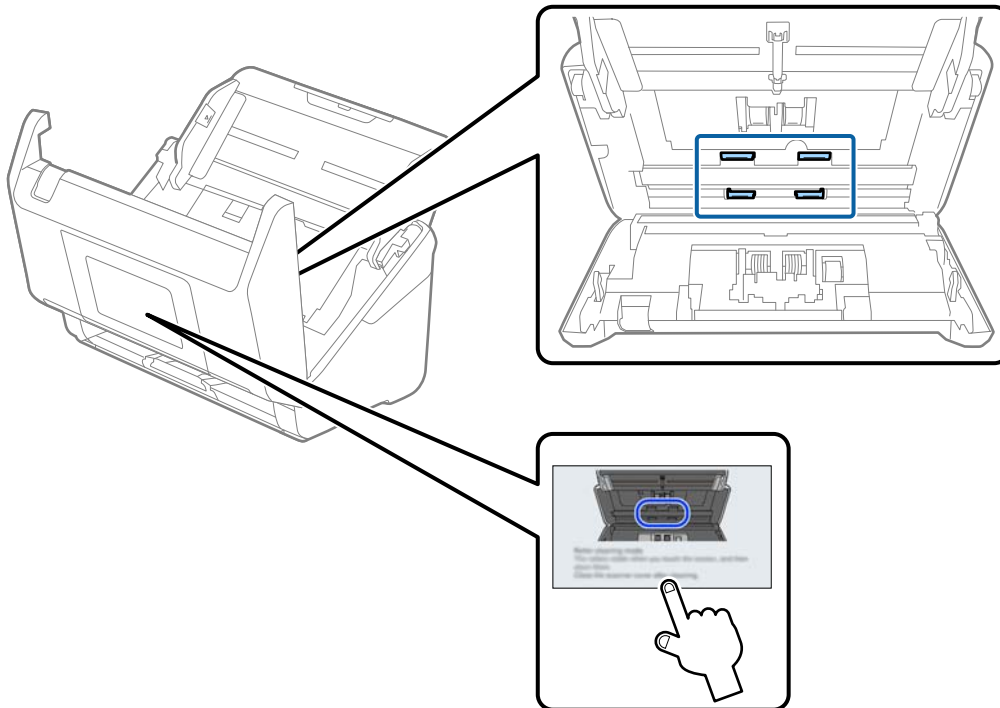
**Svarīga informācija:**

*Veltnīša tīrīšanai izmantojiet tikai autentisku Epson tīrīšanas komplektu vai mīkstu, samitrinātu drāniņu. Izmantojot sausu drāniņu, var sabojāt veltnīša virsmu.*

- Aizveriet skenera vāku.
- Pievienojiet maiņstrāvas adapteri elektrotīklam un ieslēdziet skeneri.
- Sākuma ekrānā atlasiet **Skenera apkope**.
- Ekrānā **Skenera apkope** atlasiet **Rullu tīrīšana**.
- 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 mikstu, ūdenī samitrinātu drāniņu. Atkārtojiet šo darbību, līdz veltnīši ir tīri.



**Brīdinājums:**

*Veicot darbības ar rullīti, jāuzmanās, lai mehānismā neiestrēgtu rokas vai mati. Šādi var gūt savainojumus.*

16. Aizveriet skenera vāku.

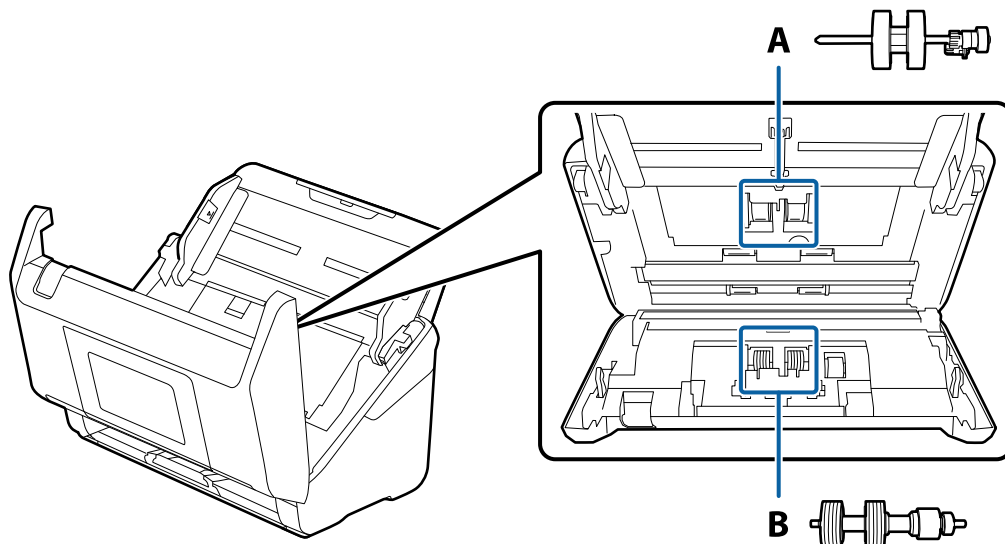
Skeneris iziet no veltnīšu tīrīšanas režīma.

**Saistītā informācija**


➔ "Veltnīšu bloka nomainīšana" 130. lpp.

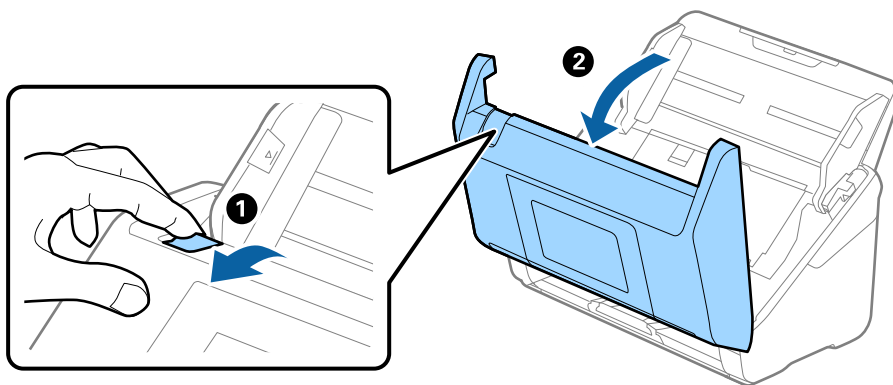
## Veltnišu bloka nomaīņa

Veltnišu bloks (uztveršanas veltnītis un atdalīšanas veltnītis) jānomaina, kad ieskenēto lapu skaits pārsniedz veltnišu dzīves ciklu. Kad vadības panelī vai datora ekrānā tiek parādīts ziņojums par nomaīņas nepieciešamību, veiciet turpmāk aprakstīto procedūru, lai to nomainītu.

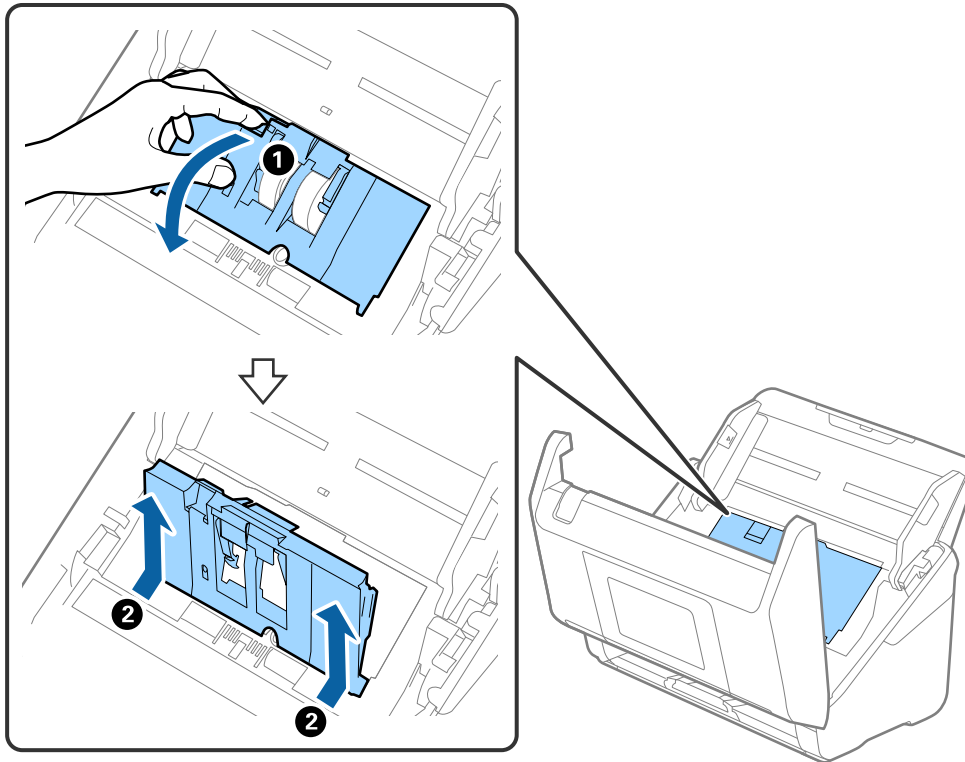


A: uztveršanas veltnītis, B: atdalīšanas veltnītis

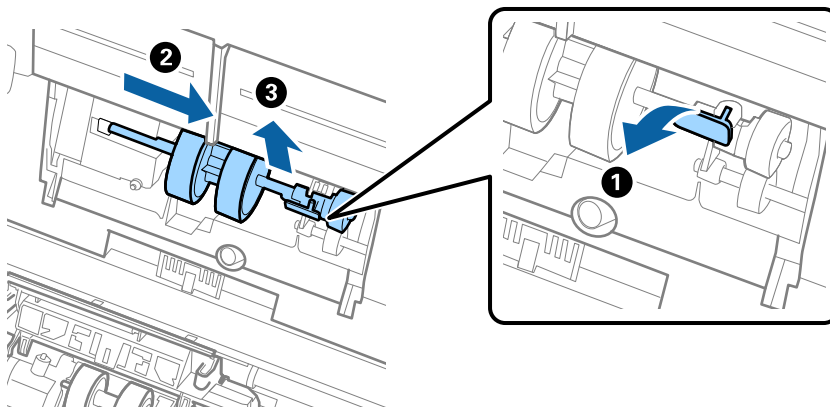
1. Nospiediet pogu , lai izslēgtu skeneri.
2. Atvienojiet maiņstrāvas adapteri no skenera.
3. Pavelciet sviru un atveriet skenera vāku.



4. Atveriet uztveršanas veltņiša vāku, pēc tam izbīdiet un izņemiet to.



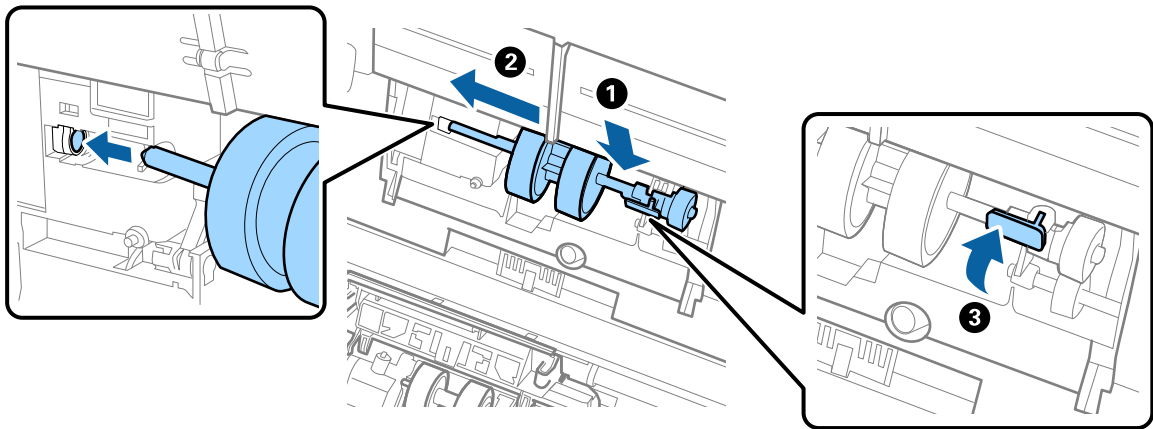
5. Pavelciet uz leju veltņiša ass armatūru, pēc tam izbīdiet un izņemiet uzstādīto uztveršanas veltņīti.



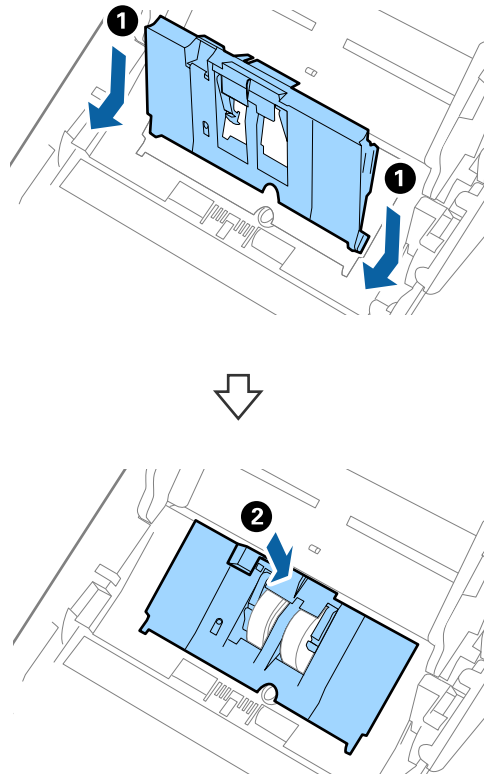
**Svarīga informācija:**

Velkot uztveršanas veltīti, nepielietojiet pārmērīgi lielu spēku. Tādējādi var sabojāt skenera iekšējās detaļas.

6. Turot armatūru uz leju, virzienā pa kreisi iebīdīt jauno uztveršanas veltnīti un ievietojiet to skenera atverē. Uzspiediet uz armatūras, lai to nofiksētu.

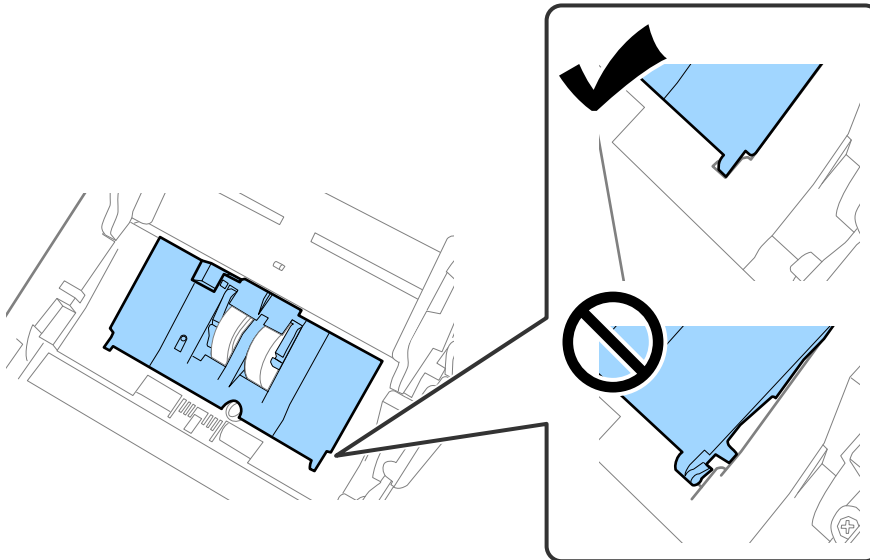


7. Ielieciet uztveršanas veltnīša vāka malu gropē un pabīdiet to. Cieši aizveriet vāku.

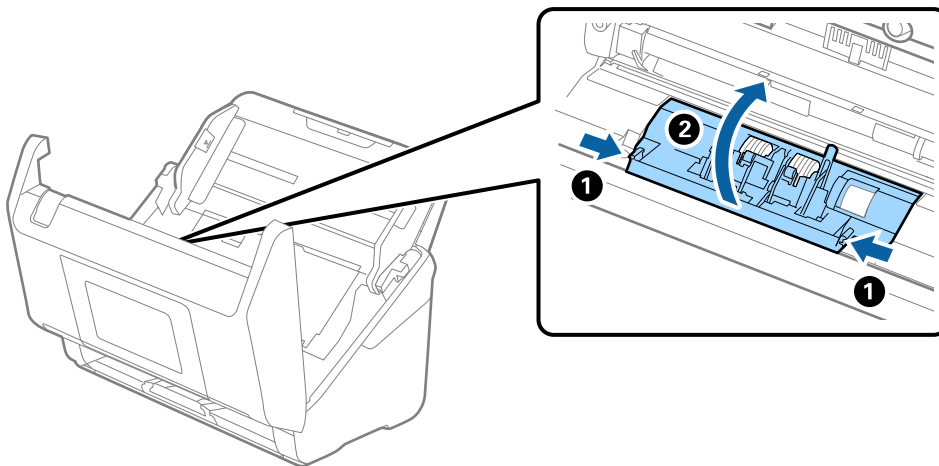


**!** **Svarīga informācija:**

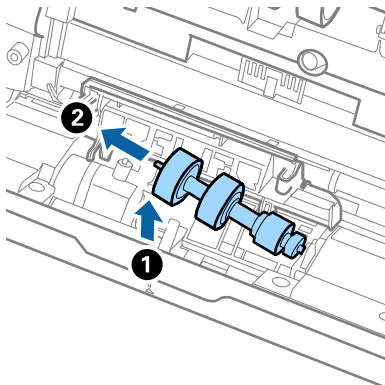
- Gādāriet, lai uztveršanas vāks būtu pareizi aizvērts.
- Ja vāku ir grūti aizvērt, pārbaudiet, vai padevējrullīši ir pareizi uzstādīti.
- Neuzstādiet vāku atvērtā stāvoklī.



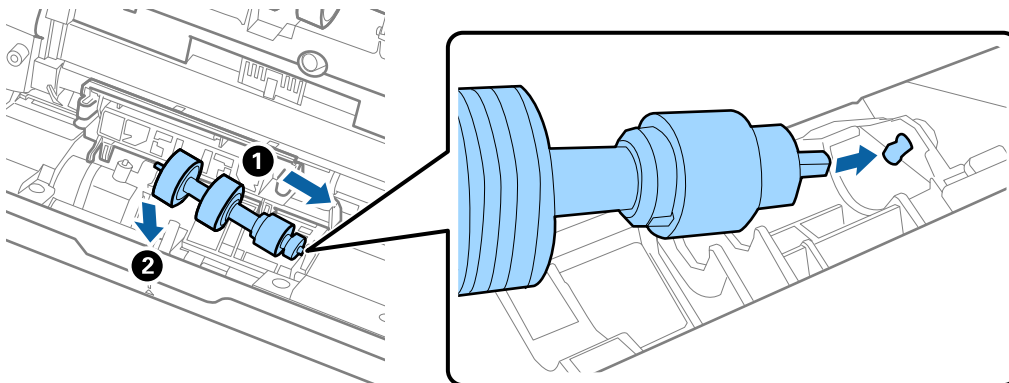
8. Atvirziet āķišus abos atdalīšanas veltņiša vāka galos, lai atvērtu vāku.



9. Paceliet atdalīšanas veltniša kreiso pusi, pēc tam izbīdiet un izņemiet uzstādītos atdalīšanas veltnišus.



10. Atverē labajā pusē ievietojiet jauno atdalīšanas veltniša asi, pēc tam nolaidiet veltnīti.



11. Aizveriet atdalīšanas veltniša vāku.



**Svarīga informācija:**

*Ja vāku ir grūti aizvērt, pārbaudiet, vai atdalīšanas veltniši ir pareizi uzstādīti.*

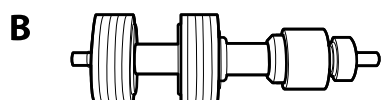
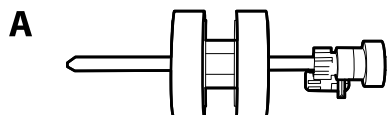
12. Aizveriet skenera vāku.
13. Pievienojiet maiņstrāvas adapteri elektrotīklam un ieslēdziet skeneri.
14. Vadības panelī atiestatiet ieskenēto lapu skaitu.

**Piezīme:**

*Utilizējiet uztveršanas veltnīti un atdalīšanas veltnīti, ievērojot pašvaldības likumus un noteikumus. Neizjauciet ierīci.*

## Veltnīšu bloka kodi

Detalās (uztveršanas veltnītis un atdalīšanas veltnītis) jānomaina, kad ieskenēto lapu skaits pārsniedz apkopes intervāla skaitītāja rādījumu. Ieskenēto lapu skaitu var apskatīt vadības panelī vai programmā Epson Scan 2 Utility.



A: uztveršanas veltnītis, B: atdalīšanas veltnītis

Detalās nosaukums	Kodi	Dzīves cikls
Veltnīšu bloks 2	B12B819711 B12B819721 (tikai Indijā)	200,000*

\* Šis skaitlis noteikts, secīgi skenējot un izmantojot testēšanas nolūkiem paredzētus Epson oriģinālus, un norāda, kad veicama nomaiņa. Nomaiņas cikls var 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 pēc rullīšu nomaiņas

Pēc veltnīšu bloka nomaiņas atiestatiet ieskenēto lapu skaitu, izmantojot vadības paneli vai programmu Epson Scan 2 Utility.

Šajā sadaļā ir izskaidrots, kā atjaunot iestatījumus, izmantojot vadības paneli.

1. Sākuma ekrānā pieskarieties **Skenera apkope**.
2. Pieskarieties pie **Apkopes ruļļa nomaiņa**.
3. Pieskarieties pie **Atiestatiet skenējumu skaitu**.
4. Atlasiet **Skenējumu skaits pēc apkopes ruļļa nomaiņas** un pēc tam pieskarieties **Jā**.

### Piezīme:

Lai atjaunotu iestatījumus no Epson Scan 2 Utility, palaidiet Epson Scan 2 Utility, noklikšķiniet uz cilnes **Skaitītājs** un pēc tam noklikšķiniet uz **Atiestatīt** sadaļā **Rullīša montāžas komplekts**.

### Saistītā informācija

➔ ["Veltnīšu bloka nomaiņa" 130. 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. Lūdzu, izvērtējiet uz apkārtējo vidi radīto ietekmi, pirms veicat jebkādas izmaiņas.


1. Sākuma ekrānā izvēlieties **Iestatījumi**.
2. Atlasiet **Pamatiestatījumi**.
3. Atlasiet **Iemidzināšanas taimeris** vai **Izslēgšanas iest.** un pēc tam veiciet iestatīšanu.

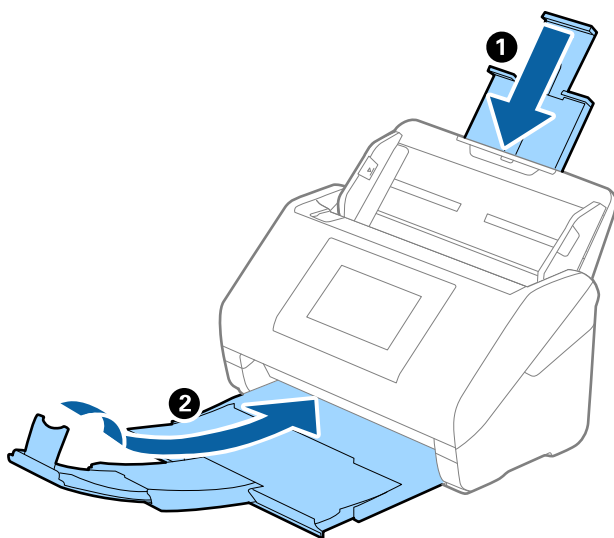
**Piezīme:**

*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 iepakojšanai.

1. Nospiediet pogu , lai izslēgtu skeneri.
2. Atvienojiet maiņstrāvas adapteri.
3. Noņemiet kabeļus un ierīces.  
Noņemiet papildu vai komplektācijā iekļauto Paper Alignment Plate, ja tā ir pievienota.
4. Aizveriet ievades paplātes pagarinātāju un izvades paplāti.

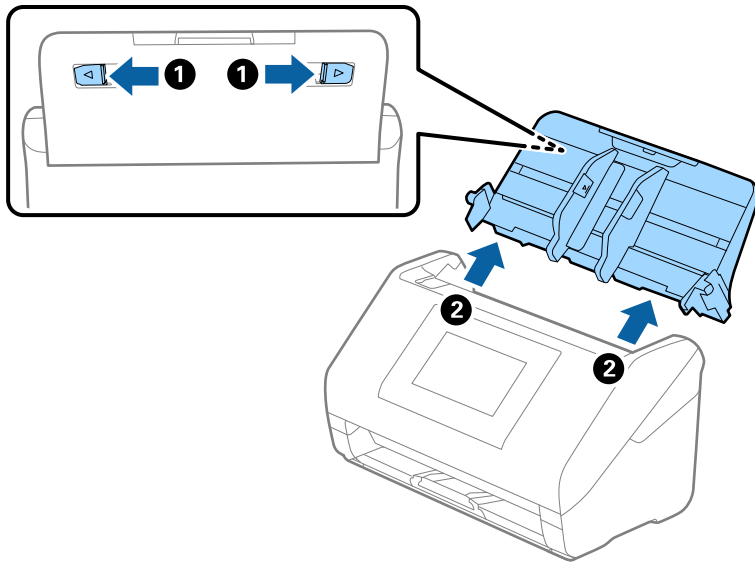


**Svarīga informācija:**

*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, dublējot 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**

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. lpp.](#)

## Iestatījumu importēšana

Importējiet eksportēto Web Config failu skeneri.



**Svarīga informācija:**

*Importējot vērtības, kuras ietver atsevišķu informāciju, piemēram, skenera nosaukumu vai IP adresi, pārliedzinieties, ka tīklā šāda IP adrese jau nepastāv.*

1. Pieklūstiet 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**

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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, tiks dzēsti. Dzēstos iestatījumus nevar atjaunot.*

**Piezīme:**

Iespējams arī mainīt iestatījumus Web Config.

Cilne **Device Management** > **Restore Default Settings**

## Programmu un aparātprogrammatūras atjaunināšana

Iespējams, varēsiet atrisināt noteiktas problēmas un uzlabot vai pievienot funkcijas, atjauninot programmas un aparātprogrammatūru. Pārlicinieties, 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**.

- Pārlicinieties, ka skeneris un dators ir savienots un dators savienots ar internetu.
- Palaidiet EPSON Software Updater un atjauniniet programmas vai aparātprogrammatūru.

**Piezīme:**

Windows Server operētājsistēmas netiek atbalstītas.

- Windows 11

Noklikšķiniet uz pogas **Sākums** un atlasiet **Visas programmas** > **Epson Software** > **EPSON Software Updater**.

- Windows 10

Noklikšķiniet uz pogas **Sākums** 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

Noklikšķiniet uz pogas **Sākums**, 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 > Aparātprogrammatūras 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 nespēj startēt, 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 sākota 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

➔ ["Web Config palaišana tīmekļa pārlūkprogrammā" 37. 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. If you cannot update over the network, try this method.

**Piezīme:**

*Pirms atjaunināšanas pārlicinieties, vai datorā ir instalēts skenera draiveris Epson Scan 2. Ja Epson Scan 2 nav instalēts, instalējiet to.*

1. Pārbaudiet Epson tīmekļa vietni, lai uzzinātu jaunākos programmaparatūras atjauninājumus.  
<http://www.epson.com>
  - Ja ir pieejama skenerim paredzētā programmaparatūra, lejupielādējiet to un pārejiet uz nākamo soli.
  - Ja tīmekļa vietnē nav informācijas par programmaparatūru, jūs jau izmantojat jaunāko programmaparatūru.
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.