

EPSON

DS-900WN DS-800WN

Administraatori juhend

Teie eesmärgiks vajalikud sätted

Võrgusätted

Nõutud sätted skannimiseks

Põhilised turvasätted

Täpsemad turvalisuse sätted

Funktsiooni Epson Open Platform kasutamine

Autoriõigus

Ühtki käesoleva trükise osa ei tohi paljundada, salvestada otsingusüsteemis ega edastada üheski vormis ega viisil elektrooniliselt, mehaaniliselt, fotokopeerimise, salvestamise ega muul teel ilma ettevõtte Seiko Epson Corporation eelneva kirjaliku loata. Selles esitatud teabe kasutamise suhtes ei võeta vastutust patendiõiguste rikkumise eest. Vastutust ei võeta ka esitatud teabe kasutamise põhjustatud kahju eest. Käesolevas dokumendis sisalduv teave on mõeldud kasutamiseks ainult koos selle Epsoni tootega. Epson ei vastuta selle teabe kasutamise eest muude toodete jaoks.

Seiko Epson Corporation ega selle sidusettevõtted ei vastuta selle toote ostja ega kolmanda osapoole ees ostjal või kolmandal osapoolel tootega juhtunud õnnetuse, väärast kasutamisest või kuritarvitamisest või loata tehtud muudatustest või remondist või (v.a USA-s) ettevõtte Seiko Epson Corporation kasutus- ja hooldusjuhiste mittejärgimise tagajärjel tekkinud kahju või kulude eest.

Seiko Epson Corporation ega selle sidusettevõtted ei vastuta kahjude ega probleemide eest, mis tulenevad lisaseadmete või kulumaterjalide kasutamisest, mis ei ole Epsoni originaaltooted või ei ole heaks kiidetud ettevõtte Seiko Epson Corporation poolt.

Seiko Epson Corporation ei vastuta mitte heaks kiidetud liidesekaablite kasutamisest tulenevate elektromagnetiliste häiringute põhjustatud kahju eest.

© 2024 Seiko Epson Corporation

Selle kasutusjuhendi sisu ja toote tehnilisi andmeid võidakse ette teatamata muuta.

Kaubamärgid

- 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.
- Üldmärkus: kõik muud kaubamärgid kuuluvad nende omanikele ja neid on kasutatud ainult tuvastamise eesmärgil.

Sisukord

Autoriõigus

Kaubamärgid

Sissejuhatus

Selle dokumendi sisu.	7
Kasutusjuhendi kasutamine.	7
Märgid ja sümbolid.	7
Käesolevas juhendis kasutatud kirjeldused.	7
Opsüsteemide viited.	7

Märkused administraatori parooli kohta

Märkused administraatori parooli kohta.	10
Algne administraatori parool.	10
Toimingud, mis nõuavad administraatori parooli.	10
Administraatori parooli muutmise.	10
Administraatori parooli lähtestamine.	10

Teie eesmärgiks vajalikud sätted

Teie eesmärgiks vajalikud sätted.	12
---	----

Võrgusätted

Skanneri võrku ühendamine.	15
Enne võrguühenduse tegemist.	15
Juhtpaneelilt võrku ühendamine.	17
Arvuti või seadmete lisamine või asendamine.	21
Ühenduse loomine võrku ühendatud skanneriga.	21
Nutiseadme ja skanneri otse ühendamine (Wi-Fi Direct).	23
Võrguühenduse uuesti seadistamine.	25
Võrguühenduse oleku kontrollimine.	27
Võrguühenduse oleku kontrollimine juhtpaneelilt.	27
Võrgu spetsifikatsioonid.	28
Wi-Fi tehnilised andmed.	28
Etherneti tehnilised nõuded.	30
Võrgufunktsioonid ja protokollid IPv4/IPv6 tugi.	30
Turvaprotokoll.	31
Skanneri jaoks pordi kasutamine.	31
Probleemide lahendamine.	32
Võrguga ei saa ühendust luua.	32

Skanneri seadistamise tarkvara

Skanneritoimingute konfigureerimise rakendus (Web Config).	37
Kuidas kasutada veebibrauseris rakendust Web Config.	37
Epson Device Admin.	38
Konfiguratsioonimall.	39

Nõutud sätted skannimiseks

Meiliserveri registreerimine.	44
Meiliserveri ühenduse kontrollimine.	45
Võrgukausta loomine.	46
Kontaktide kättesaadavaks tegemine.	54
Kontaktide konfiguratsiooni võrdlus.	55
Sihtkoha registreerimine kontaktide hulka utiliidi Web Config abil.	55
Sihtkohtade registreerimine rühmana Web Config kaudu.	57
Kontaktide varundamine ja importimine.	58
Kontaktide eksportimine ja hulgiregistreerimine tööriista abil.	59
Koostöö LDAP-serveri ja kasutajate vahel.	60
Funktsiooni AirPrint seadistamine.	63
Probleemid võrguskannimise ettevalmistamisega.	64
Nõuandeid probleemide lahendamiseks.	64
Utiliiti Web Config ei õnnestu avada.	64

Juhtpaneeli ekraani kohandamine

Registreerimine: Eelsätted.	67
Menüüsuvandid: Eelsätted.	68
Juhtpaneeli avakuva redigeerimine.	69
Avakuva Paigutusi muutmise.	69
Lisa ikoon.	70
Eemalda ikoon.	71
Teisalda ikoon.	72

Põhilised turvasätted

Toote turvalisuse funktsioonide juhend.	74
Administraatori sätted.	74
Seadistage administraatori parool.	74
Funktsiooni Lukustamise sätted kasutamine juhtpaneelil.	76
Juhtpaneelilt administraatorina sisselogimine.	79

Saadaval funktsioonide piiramine (Juurdepääsu haldamine).	80
Kasutajakonto loomine.	80
Suvandi Juurdepääsu haldamine lubamine.	81
Logimine skannerisse, kui lubatud on Juurdepääsu haldamine.	81
Välise liidese keelamine.	82
Programmikinnituse lubamine käivitamisel.	82
Võrgust skannimise keelamine arvutist.	83
WSD-skannimise lubamine ja keelamine.	83
Kaugskanneri jälgimine.	84
Kaugskanneri teabe vaatamine.	84
Meiliteavituste saamine sündmuste toimumisel.	84
Skanneri toiteallika juhtimine rakenduses Web Config.	85
Vaikesätete taastamine.	85
Teenuse Epson Remote Services teave.	86
Probleemide lahendamine.	86
Administraatori parool on ununenud.	86

Täpsemad turvalisuse sätted

Turvalisuse sätted ja ohtude vältimine.	88
Turvalisuse sätted.	89
Juhtimine protokollidega.	89
Juhtimisprotokollid.	89
Protokollid, mida saate lubada või keelata.	89
Protokolli sätteüksused.	90
Digitaalsertifikaadi kasutamine.	92
Digitaalsest sertimisest.	92
CA-signed Certificate seadistamine.	92
Iseallkirjastatud sertifikaadi värskendamine.	96
CA Certificate seadistamine.	96
SSL/TLS-side skanneriga.	97
SSL/TLS põhisätete seadistamine.	97
Skannerile serveri sertifikaadi konfigureerimine.	98
Krüptitud side IPsec/IP-filtreerimisega.	98
Teave rakenduse IPsec/IP Filtering kohta.	98
Vaikepoliitika konfigureerimine.	98
Rühmapoliitika konfigureerimine.	102
IPsec/IP Filtering konfiguratsiooni näited.	108
IPsec/IP-filtrimine sertifikaadi seadistamine.	109
Skanneri ühendamine IEEE802.1X-võrguga.	109
IEEE 802.1X-võrgu konfigureerimine.	109
IEEE 802.1X sertifikaadi seadistamine.	111
Täpsemate turvasätetega seotud probleemide lahendamine.	111
Turvasätete taastamine.	111

Probleemid võrgu turvafunktsioonide kasutamisel.	112
Probleemid digitaalsertifikaadi kasutamisel.	114

Funktsiooni Epson Open Platform kasutamine

Ülevaade: Epson Open Platform.	119
Epson Open Platformi seadistamine.	119
Epson Open Platformi valideerimine.	119

Autentimisseadme paigaldamine

Autentimisseadme ühendamine.	121
Autentimisseadme töötamise kontroll.	121
Autentimiskaardi tuvastuse kinnitamine.	121
Autentimisseadme tõrkeotsing.	121
Autentimiskaarti pole võimalik lugeda.	121

Hooldamine

Skanneri korpuse puhastamine.	124
Skanneri sisemuse puhastamine.	124
Rulli montaažikomplekti vahetamine.	129
Rulli montaažikomplekti koodid.	134
Skannide arvu lähtestamine pärast rullikute vahetamist.	134
Energia säästmine.	135
Skanneri transportimine.	135
Sätete varundamine.	136
Sätete eksportimine.	136
Sätete import.	137
Taasta vaikesätted.	137
Rakenduste ja püsivara värskendamine.	138
Skanneri püsivara värskendamine juhtpaneeli abil.	138
Püsivara värskendamine rakenduses Web Config.	139
Püsivara värskendamine ilma internetiühendusega.	139

Sissejuhatus

Selle dokumendi sisu.	7
Kasutusjuhendi kasutamine.	7

Selle dokumendi sisu

See dokument sisaldab skanneri administraatorite jaoks järgmist teavet.

- Võrgusätted
- Skannifunktsiooni ettevalmistamine
- Turvasätete lubamine ja haldamine
- Igapäevase hoolduse tegemine

Skanneri standardseid kasutusmeetodeid vaadake dokumendist *Kasutusjuhend*.

Kasutusjuhendi kasutamine

Märgid ja sümbolid



Ettevaatust!

Juhised, mida tuleb hoolega jälgida, et vältida kehavigastuse ohtu.



Oluline teave:

Juhised, mida tuleb hoolega jälgida, et hoida ära seadmete kahjustamist.

Märkus.

Täiendav teatmematerjal.

Seotud teave

➔ Lingid seotud osadele.

Käesolevas juhendis kasutatud kirjeldused

- Rakenduste ekraanipildid on platvormilt Windows 10 või macOS High Sierra. Ekraanipiltide sisu on mudelist ja olukorrast olenevalt erinev.
- Käesolevas juhendis kasutatud illustratsioonid on toodud ainult viiteks. Kuigi need võivad tegelikust tootest veidi erineda, on töömeetodid samad.

Opsüsteemide viited

Windows

Selles juhendis olevad terminid „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”, ja „Windows Server 2008” viitavad järgmistele opsüsteemidele. Terminit „Windows” kasutatakse kõikide versioonide puhul.

- Microsoft® Windows® 11 opsüsteem
- Microsoft® Windows® 10 opsüsteem
- Microsoft® Windows® 8.1 opsüsteem
- Microsoft® Windows® 8 opsüsteem
- Microsoft® Windows® 7 opsüsteem
- Microsoft® Windows Server® 2022 opsüsteem
- Microsoft® Windows Server® 2019 opsüsteem
- Microsoft® Windows Server® 2016 opsüsteem
- Microsoft® Windows Server® 2012 R2 opsüsteem
- Microsoft® Windows Server® 2012 opsüsteem
- Microsoft® Windows Server® 2008 R2 opsüsteem
- Microsoft® Windows Server® 2008 opsüsteem

Mac OS

Selles juhendis tähendab „Mac OS” opsüsteemi Mac OS X 10.9 või uuemat ning opsüsteemi macOS 11 või uuemat.

Märkused administraatori parooli kohta

Märkused administraatori parooli kohta.	10
Algne administraatori parool.	10
Toimingud, mis nõuavad administraatori parooli.	10
Administraatori parooli muutmine.	10
Administraatori parooli lähtestamine.	10

Märkused administraatori parooli kohta

Seade võimaldab administraatori parooli määramist, et takistada kolmandate isikute volitamata juurdepääsu seadme sätetele ja võrgusätetele, mis on seadmesse salvestatud, kui seade võrku ühendatakse.

Kui määrate administraatori parooli, peate sätete muutmiseks konfiguratsioonitarkvaras (nt Web Config) sisestama selle parooli.

Algne administraatori parool on skannerile määratud, aga te võite selle oma valitud parooliks muuta.

Algne administraatori parool

Algne administraatori parool erineb olenevalt tootele kinnitatud sildist. Kui tagaküljele on kinnitatud silt „PASSWORD“, sisestage sildil olev 8-kohaline number. Kui silti „PASSWORD“ ei ole, sisestage administraatori paroolina toote tagaküljel oleval sildil toodud seerianumber.

Me soovime algse administraatori parooli vaikesätte ära muuta.

Märkus.

Kasutajanime vaikimisi määratud ei ole.

Toimingud, mis nõuavad administraatori parooli

Kui teil palutakse järgmiste toimingute ajal sisestada administraatori parool, sisestage tootele määratud administraatori parool.

- Rakenduse Web Config täpsematesse sätetesse logimine
- Administraatori poolt lukustatud juhtpaneeli menüü kasutamine
- Seadme sätete muutmine rakenduses
- Seadme püsivara uuendamine
- Administraatori parooli muutmine või lähtestamine

Administraatori parooli muutmine

Saate seda muuta toote juhtpaneelil või rakenduses Web Config.

Parooli muutmisel peab uus parool olema 8 kuni 20 tärki pikk ja sisaldama ainult ühebaadilisi tärke.

Administraatori parooli lähtestamine

Administraatori parooli saate algsätetele lähtestada toote juhtpaneelil või rakenduses Web Config.

Kui olete parooli unustanud ja ei saa seda vaikesätetele lähtestada, tuleb toodet parandada. Võtke ühendust kohaliku edasimüüjaga.

Teie eesmärgiks vajalikud sätted

Teie eesmärgiks vajalikud sätted.	12
---	----

Teie eesmärgiks vajalikud sätted

Oma eesmärgiks vajalike sätete seadistamise kohta lugege allpool.

Skanneri võrku ühendamine

Eesmärk	Nõutud sätted
Tahan skanneri võrku ühendada.	Häälestage skanner võrguskannimiseks. „Skanneri võrku ühendamine“ lk 15
Tahan skanneri uue arvutiga ühendada.	Seadistage skanneri võrgusätted uues arvutis. „Arvuti või seadmete lisamine või asendamine“ lk 21

Skannimise sätted

Eesmärk	Nõutud sätted
Tahan skannitud pilte meilitsi saata. (Scan to Email)	1. Seadistage meiliserver, mida soovite ühendada. „Meiliserveri registreerimine“ lk 44 2. Registreerige adressaadi meiliaadress suvandis Contacts (valikuline). Kui registreerite meiliaadressi, ei ole teil vaja seda iga kord saatmiseks sisestada, saate selle valida kontaktidest. „Kontaktide kättesaadavaks tegemine“ lk 54
Tahan skannitud pildid võrgukausta salvestada. (Scan to Network Folder/FTP)	1. Looge võrku kaust, kuhu tahate pildid salvestada. „Võrgukausta loomine“ lk 46 2. Registreerige kaustatee suvandis Contacts (valikuline). Kui registreerite kaustatee, ei ole teil vaja seda iga kord saatmiseks sisestada, saate selle valida kontaktidest. „Kontaktide kättesaadavaks tegemine“ lk 54
Tahan skannitud pildid pilveteenusesse salvestada. (Scan to Cloud)	Seadistage rakendus Epson Connect. Seadistamise kohta lugege portaali Epson Connect veebisaidilt. Seadistamiseks on vajalik ühendatava veebisalvestusteenuse kasutajakonto. https://www.epsonconnect.com/ http://www.epsonconnect.eu (ainult Euroopa)

Juhtpaneeli ekraani kohandamine

Eesmärk	Nõutud sätted
Tahan muuta skanneri juhtpaneelil kuvatud üksusi.	Seadistage Eelsätted või Muuda avakuva . Saate oma lemmikud skannimissätted registreerida juhtpaneelil ja redigeerida kuvatud üksusi. „Juhtpaneeli ekraani kohandamine“ lk 66

Põhiliste turvafunktsioonide seadistamine

Eesmärk	Nõutud sätted
Tahan takistada skanneri sätete muutmist kõigil peale administraatori.	Määrake skannerile administraatori parool. „Administraatori sätted“ lk 74
Tahan keelata skannerite kasutamise USB-ühenduse kaudu.	Keelake välisliides. „Välise liidese keelamine“ lk 82

Täpsemate turvafunktsioonide seadistamine

Eesmärk	Nõutud sätted
Tahan omada kontrolli kasutatavate protokollide üle.	Lubage või keelake protokollid. „Juhtimine protokollidega“ lk 89
Tahan krüptida sidetee.	1. Seadistage digisert. „Digitaalsertifikaadi kasutamine“ lk 92 2. Seadistage SSL-/TLS-andmeside. „SSL/TLS-side skanneriga“ lk 97
Tahan kasutada krüptitud andmesidet (IPsec). Tahan, et tarkvara saaks kasutada ainult kindlast arvutist (IP-filtrimine).	Seadistuspoliitika liidluse filtrimiseks. „Krüptitud side IPsec/IP-filtreerimisega“ lk 98
Tahan kasutada skannerit IEEE802.1X-võrgus.	Seadistage skannerile IEEE802.1X. „Skanneri ühendamine IEEE802.1X-võrguga“ lk 109

Skanneri sünkroonimine autentimissüsteemiga

Hankige spetsiaalselt veebisaidilt tootevõti ja aktiveerige skanneris Epson Open Platform.

[„Funktsiooni Epson Open Platform kasutamine“ lk 118](#)

Autentimisvõimaluse kasutamine (Epson Print Admin/Epson Print Admin Serverless)

Selle valiku kasutamiseks vajae litsentsivõtit.

Lisateabe saamiseks võtke ühendust oma edasimüüjaga.

Märkus.

Funktsiooni Epson Print Admin Serverless ei saa kasutada, kui süsteem on sünkroonitud platvormiga Epson Open Platform.

Võrgusätted

Skanneri võrku ühendamine.	15
Arvuti või seadmete lisamine või asendamine.	21
Võrguühenduse oleku kontrollimine.	27
Võrgu spetsifikatsioonid.	28
Probleemide lahendamine.	32

Skanneri võrku ühendamine

Selles jaotises on kirjeldatud skanneri võrku ühendamist skanneri juhtpaneeli abil.

Märkus.

Kui teie skanner ja arvuti on samas segmendis, saate ühenduse luua ka installeriga.

Installeri käivitamiseks avage järgmine veebisait ja sisestage seejärel toote nimi. Valige **Häälestus** ja alustage seadistamist.

<https://epson.sn>

Kasutusjuhendit saate vaadata jaotises Veebifilmi juhendid. Avage järgmine URL.

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

Enne võrguühenduse tegemist

Võrguga ühenduse loomiseks kontrollige eelnevalt ühendusmeetodit ja ühenduse seadistamise teavet.

Teabe kogumine ühenduse seadistuse kohta

Pange valmis ühenduse loomiseks vajalik seadistusteave. Kontrollige eelnevalt järgmist teavet.

Jaotis	Üksused	Märkus
Seadme ühendusmeetod	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Otsustage, kuidas skanner võrku ühendada. Juhtmega LAN-i korral ühendage see juhtme abil kommutaatoriga. Wi-Fi-ühenduse korral looge ühendus pääsupunkti võrguga (SSID).
LAN-ühenduse teave	<input type="checkbox"/> IP-aadress <input type="checkbox"/> Alamvõrgumask <input type="checkbox"/> Vaikelüüs	Valige skanneri IP-aadress. Kui määrate IP-aadressi staatiliselt, tuleb sisestada kõik väärtused. Kui määrate IP-aadressi dünaamiliselt DHCP-funktsiooniga, ei ole see teave vajalik, kuna see määratakse automaatselt.
Wi-Fi-ühenduse teave	<input type="checkbox"/> SSID <input type="checkbox"/> Parool	Need on SSID (võrgu nimi) ja parool, mis kuuluvad pääsupunktile, millega skanner ühendatakse. Kui seadistatud on MAC-aadressi filtrimine, registreerige eelnevalt skanneri MAC-aadress, et saaksite skanneri registreerida. Toetatud standardeid vaadake allpool. „Võrgu spetsifikatsioonid“ lk 28
DNS-serveri teave	<input type="checkbox"/> Peamise DNS-i IP-aadress <input type="checkbox"/> Sekundaarse DNS-i IP-aadress	Need on vajalikud DNS-serverite täpsustamise korral. Sekundaarne DNS seadistatakse, kui süsteemil on liigne konfiguratsioon ja olemas on sekundaarne DNS-server. Kui teie organisatsioon on väike ja te ei seadista DNS-serverit, siis määrake selleks ruuteri IP-aadress.

Jaotis	Üksused	Märkus
Puhverserveri teave	<input type="checkbox"/> Puhverserveri nimi	Seadistage see, kui teie võrgukeskkond kasutab juurdepääsuks sisevõrgust internetile puhverserverit ja te kasutate funktsiooni, mis annab skannerile otsejuurdepääsu internetile. Järgmiste funktsioonide jaoks loob skanner internetiga otseühenduse. <input type="checkbox"/> Epson Connecti teenused <input type="checkbox"/> Muude ettevõtete pilveteenused <input type="checkbox"/> Püsivara värskendamine <input type="checkbox"/> Skannitud kujutiste saatmine SharePointi (WebDAV)
Pordinumbri teave	<input type="checkbox"/> Pordinumber avamiseks	Kontrollige skanneri ja arvuti kasutatavat pordinumbrit ja seejärel avage vajaduse korral tulemüüri blokeeritud port. Skanneri kasutatava pordinumbri kohta lugege allpool. „Skanneri jaoks pordi kasutamine“ lk 31

IP-aadressi määramine

IP-aadressi on võimalik määrata alljärgnevate meetoditega.

Staatiline IP-aadress:

Määrake skannerile (host) etteantud IP-aadress käsitsi.

Võrguga ühendamise teave (alamvõrgumask, vaikelüüs, DNS-server jms) tuleb seadistada käsitsi.

Kuna IP-aadress ei muutu isegi siis, kui seade lülitatakse välja, on see kasulik siis, kui soovite hallata seadmeid keskkonnaga, milles te ei saa IP-aadressi muuta, või kui soovite hallata seadmeid IP-aadressi abil. Me soovime määrata seadistused skannerile, serverile jms, mida kasutavad paljud arvutid. Lisaks, kui kasutusel on turvafunktsioonid nagu IPsec/IP-filtrimine, siis määrake fikseeritud IP-aadress, mis ei muutu.

Automaatne määramine DHCP-funktsiooniga (dünaamiline IP-aadress):

Määrake skannerile (host) IP-aadress automaatselt, kasutades DHCP serveri või ruuteri DHCP-funktsiooni.

Võrguga ühendamise teave (alamvõrgumask, vaikelüüs, DNS-server jms) seadistatakse automaatselt ning tänu sellele saate seadme võrguga lihtsasti ühendada.

Seadme või ruuteri väljalülitamise korral või olenevalt DHCP serveri sätetest võib IP-aadress uuesti ühendamise järel muutuda.

Me soovime hallata muid seadmeid peale IP-aadressi ja pidada sidet IP-aadressi järgida suutvate protokollidega.

Märkus.

Kasutades DHCP IP-aadressi säilitamise funktsiooni, saate määrata seadmetele igal ajal sama IP-aadressi.

DNS-server ja puhverserver

DNS-serveril on hostinimi, meiliaadressi domeeninimi jms seoses IP-aadressi teabega.

Andmeside ei ole võimalik, kui teist poolt kirjeldab hostinimi, domeeninimi vms ajal, mil arvuti või skanner teostab IP-sidet.

Küsib DNS-serverilt seda teavet ja saab teise poole IP-aadressi. Seda protsessi kutsutakse nimelahenduseks.

Seega saavad seadmed nagu arvutid ja skannerid suhelda IP-aadressi abil.

Nimelahendus on vajalik selleks, et skanner saaks pidada andmesidet meilifunktsiooni või internetiühenduse funktsiooni abil.

Neid funktsioone kasutades määrake DNS-serveri sätted.

Kui määrate skanneri IP-aadressi DHCP-serveri või ruuteri DHCP-funktsiooniga, määratakse see automaatselt.

Puhverserver asub lüüsis võrgu ja Interneti vahel ning suhtleb arvuti, skanneri ja Internetiga (vastasserver) nende asemel. Vastasserver suhtleb ainult puhverserveriga. Seega ei ole võimalik näha skanneri teavet, nagu IP-aadress ja pordinumber, mis suurendab turvalisust.

Kui loote internetiühenduse puhverserveri kaudu, konfigureerige puhverserver skanneris.

Juhtpaneelilt võrku ühendamine

Ühendage skanner võrku, kasutades skanneri juhtpaneeli.

IP-aadressi määramine

Seadistage põhiüksused, nagu hosti aadress, Alamvõrgumask, Vaikelüüs.

Selles jaotises on selgitatud, kuidas seadistada staatilist IP-aadressi.

1. Lülitage skanner sisse.
2. Valige skanneri juhtpaneeli avakuval **Sätted**.
3. Valige **Võrgusätted > Täpsem > TCP/IP**.
4. Suvandi **Käsitsi** sätteks valige **Hangi IP-aadress**.

Kui määrate IP-aadressi automaatselt, kasutades ruuteri DHCP-funktsiooni, valige **Automaatne**. Sellisel juhul määratakse ka **IP-aadress**, **Alamvõrgumask** ja **Vaikelüüs** sammudes 5 kuni 6 automaatselt, seega jätkake sammust 7.

5. Sisestage IP-aadress.

Valikutega ◀ ja ▶ muutub aktiivseks järgmine või eelmine segment, mis on eraldatud punktiga.

Kontrollige eelmisel kuval näidatud väärtust.

6. Seadistage **Alamvõrgumask** ja **Vaikelüüs**.

Kontrollige eelmisel kuval näidatud väärtust.



Oluline teave:

*Kui suvandite IP-aadress, Alamvõrgumask ja Vaikelüüs kombinatsioon on väär, on **Käivita häälestus** inaktiveeritud ja seadistamist ei saa jätkata. Kontrollige, et kirjes ei oleks vigu.*

7. Sisestage peamise DNS-serveri IP-aadress.

Kontrollige eelmisel kuval näidatud väärtust.

Märkus.

Kui valite IP aadressi määramise säteteks **Automaatne**, siis valiku **Käitsi** või **Automaatne** alt valida DNS-serveri sätteid. Kui DNS-serveri aadressi ei saa automaatselt hankida, valige **Käitsi** ja sisestage DNS-serveri aadress. Seejärel sisestage otse sekundaarse DNS-serveri aadress. Kui teete valiku **Automaatne**, jätkake sammust 9.

8. Sisestage sekundaarse DNS-serveri IP-aadress.
Kontrollige eelmisel kuval näidatud väärtust.
9. Puudutage nuppu **Käivita häälestus**.

Puhverserveri seadistamine


Seadistage puhverserver, kui kehtivad mõlemad järgmistest tingimustest.

- Puhverserver on loodud internetiühenduseks.
- Kui kasutate funktsiooni, millega skanner loob internetiga otseühenduse, (nt teenus Epson Connect või muu ettevõtte pilveteenus).

1. Valige avakuval **Sätteid**.
Kui teete sätteid pärast IP-aadressi määramist, kuvatakse kuva **Täpsem**. Minge sammule 3.
2. Valige **Võrgusätted > Täpsem**.
3. Valige **Puhverserver**.
4. Suvandi **Kasuta** sätteks valige **Puhverserveri sätteid**.
5. Sisestage puhverserveri aadress IPv4- või FQDN-vormingus.
Kontrollige eelmisel kuval näidatud väärtust.
6. Sisestage puhverserveri pordinumber.
Kontrollige eelmisel kuval näidatud väärtust.
7. Puudutage nuppu **Käivita häälestus**.

Ühendamine Ethernetiga

Ühendage skanner LAN-kaabli abil võrku ja kontrollige seejärel ühendust.

1. Ühendage skanner ja jaotur (LAN-kommutaator) LAN-kaabli abil.
2. Valige avakuval .
3. Valige **Ruuter**.
4. Kontrollige, kas suvandite Ühendus ja IP-aadress sätteid on õiged.
5. Puudutage nuppu **Sule**.

Ühendamine raadiovõrku (Wi-Fi)

Skannerit saab raadiovõrku (Wi-Fi) ühendada mitmel moel. Valige ühendusmeetod, mis vastab kasutatavale keskkonnale ja tingimustele.

Kui teile on teada ruuteri teave, nagu SSID ja parool, saate sätteid määrata käsitsi.

Kui ruuter toetab ainult WPS-i, saate sätteid määrata surunupuga seadistamise abil.

Pärast skanneri võrku ühendamist looge skanneriga ühendus seadmest, mida soovite kasutada (arvuti, nutiseade, tahvelarvuti jne).

Märge Wi-Fi 5 GHz ühenduse kasutamisel

Sellel toode kasutab Wi-Fi Directiga (lihtne AP) ühenduse loomisel tavaliselt kanalit W52 (36ch). Kuna juhtmeta LAN-i (Wi-Fi) ühenduse jaoks valitakse kanal automaatselt, võib kasutatav kanal erineda, kui seda kasutatakse Wi-Fi Directi ühendusega samal ajal. Kui kanalid on erinevad, võib andmeside skanneriga aeglane olla. Kui see kasutamist ei sega, looge SSID-ga ühendus 2,4 GHz sagedusega. 2,4 GHz sagedusala puhul on kasutatavad kanalid samad.

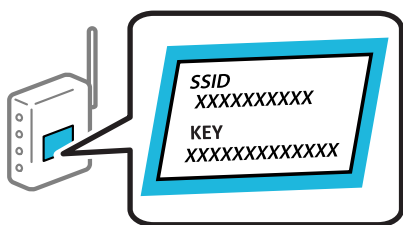
Kui seadistate juhtmeta LAN-i sagedusele 5 GHz, soovitame Wi-Fi Directi keelata.


Wi-Fi sätete määramine, sisestades SSID ja parooli

Te saate seadistada Wi-Fi-võrgu, sisestades ühenduse loomiseks vajalikud andmed käsitsi skanneri juhtpaneelilt. Käsitsi seadistamiseks vajate pääsupunkti SSID-d ja parooli.

Märkus.

Kui kasutate juhtmevaba pääsupunkti nende vaikesätetega, leiate SSID ja parooli andmesildilt. Kui te SSID-d ja parooli ei tea, võtke ühendust juhtmevaba pääsupunkti seadistanud isikuga või vaadake pääsupunktiga kaasnenud dokumentatsioonist.



1. Puudutage avakuval suvandit .
2. Valige **Ruuter**.
3. Puudutage nuppu **Käivita häälestus**.

Kui võrguühendus on juba seadistatud, kuvatakse ühenduse üksikasjad. Puudutage valikut **Lülitage ümber Wi-Fi-ühendusele**, või **Muuda sätteid**, et muuta sätteid.

4. Valige **Wi-Fi häälestusviisard**.
5. Järgige SSID valimiseks ekraanil kuvatud juhtnööre, sisestage juhtmeta ruuteri parool ja käivitage seadistus. Skanneri võrguühenduse oleku kontrollimiseks pärast seadistamist vaadake allpool olevat seotud teabe linki.

Märkus.

- Kui te SSID-d ei tea, kontrollige, kas see on kirjutatud juhtmevaba pääsupunkti andmesildile. Kui kasutate juhtmevaba pääsupunkti vaikesätetega, kasutage andmesildile kirjutatud SSID-d. Kui te infot ei leia, tutvuge juhtmevaba pääsupunktiga kaasneva dokumentatsiooniga.
- Parool on tõstutundlik.
- Kui te parooli ei tea, kontrollige, kas see on kirjutatud juhtmevaba pääsupunkti andmesildile. Sildil võib parool olla „Network Key“, „Wireless Password“ vms. Kui kasutate juhtmevaba pääsupunkti vaikesätetega, kasutage andmesildile kirjutatud parooli.
- Kui te ei näe SSID-d, millega soovite ühendust luua, kasutage Wi-Fi seadistamiseks arvutist või nutiseadmest (nutitelefon, tahvelarvuti) tarkvara või rakendust. Lisateabe saamiseks sisestage veebisaidi avamiseks brauserisse „<https://epson.sn>“, sisestage oma toote nimi ja avage **Häälestus**.

Seotud teave

➔ „Võrguühenduse oleku kontrollimine“ lk 27

Wi-Fi seadistuste tegemine ühe nupuvajutusega (WPS)


Saate Wi-Fi-võrgu automaatselt seadistada raadiovõrgu ruuteri nuppu vajutades. Saate teha häälestuse selliselt, kui on täidetud alljärgnevad tingimused.

- Raadiovõrgu ruuter ühildub WPS-iga (Wi-Fi Protected Setup).
- Hetkel toimiv Wi-Fi ühendus on loodud juhtmevaba nupule vajutamisega.

Märkus.

Kui te ei leia nuppu või kasutate häälestamiseks tarkvara, lugege ruuteriga kaasnenud dokumentatsiooni.



1. Puudutage avakuval suvandit .
2. Valige **Ruuter**.
3. Puudutage nuppu **Käivita häälestus**.

Kui võrguühendus on juba seadistatud, kuvatakse ühenduse üksikasjad. Puudutage valikut **Lülitage ümber Wi-Fi-ühendusele**, või **Muuda sätteid**, et muuta sätteid.

4. Valige **Surunupu häälestus (WPS)**.
5. Järgige ekraanil olevaid juhtnööre.

Skanneri võrguühenduse oleku kontrollimiseks pärast seadistamist vaadake allpool olevat seotud teabe linki.

Märkus.

Kui ühenduse loomine ei õnnestu, lähtestage raadiovõrgu pääsupunkt, viige see skannerile lähemale ja proovige uuesti.

Seotud teave

➔ „Võrguühenduse oleku kontrollimine“ lk 27

Wi-Fi-sätete tegemine PIN-koodi häälestusega (WPS)

PIN-koodi kasutades saate raadiovõrgu pääsupunktiga ühenduse luua automaatselt. Saate seda meetodit häälestamiseks kasutada, kui ruuteril on olemas WPS (Wi-Fi Protected Setup). Kasutage arvutit, et sisestada PIN-kood ruuterisse.

1. Puudutage avakuval suvandit .

2. Valige **Ruuter**.

3. Puudutage nuppu **Käivita häälestus**.

Kui võrguühendus on juba seadistatud, kuvatakse ühenduse üksikasjad. Puudutage valikut **Lülitage ümber Wi-Fi-ühendusele**, või **Muuda sätteid**, et muuta sätteid.

4. Valige **Muud > PIN-koodi häälestus (WPS)**

5. Järgige ekraanil olevaid juhtnööre.

Skanneri võrguühenduse oleku kontrollimiseks pärast seadistamist vaadake allpool olevat seotud teabe linki.

Märkus.

Lugege üksikasju PIN-koodi sisestamise kohta ruuteriga kaasnenud dokumentatsioonist.

Seotud teave

➔ „Võrguühenduse oleku kontrollimine” lk 27

Arvuti või seadmete lisamine või asendamine

Ühenduse loomine võrku ühendatud skanneriga

Kui skanner on juba võrku ühendatud, saate arvuti või nutiseadme skanneriga ühendada üle võrgu.

Võrguskanneri kasutamine teisest arvutist

Soovitame skanneri arvutiga ühendamiseks kasutada installerit.

Installeri käivitamiseks avage järgmine veebisait ja sisestage seejärel toote nimi. Valige **Häälestus** ja alustage seadistamist.

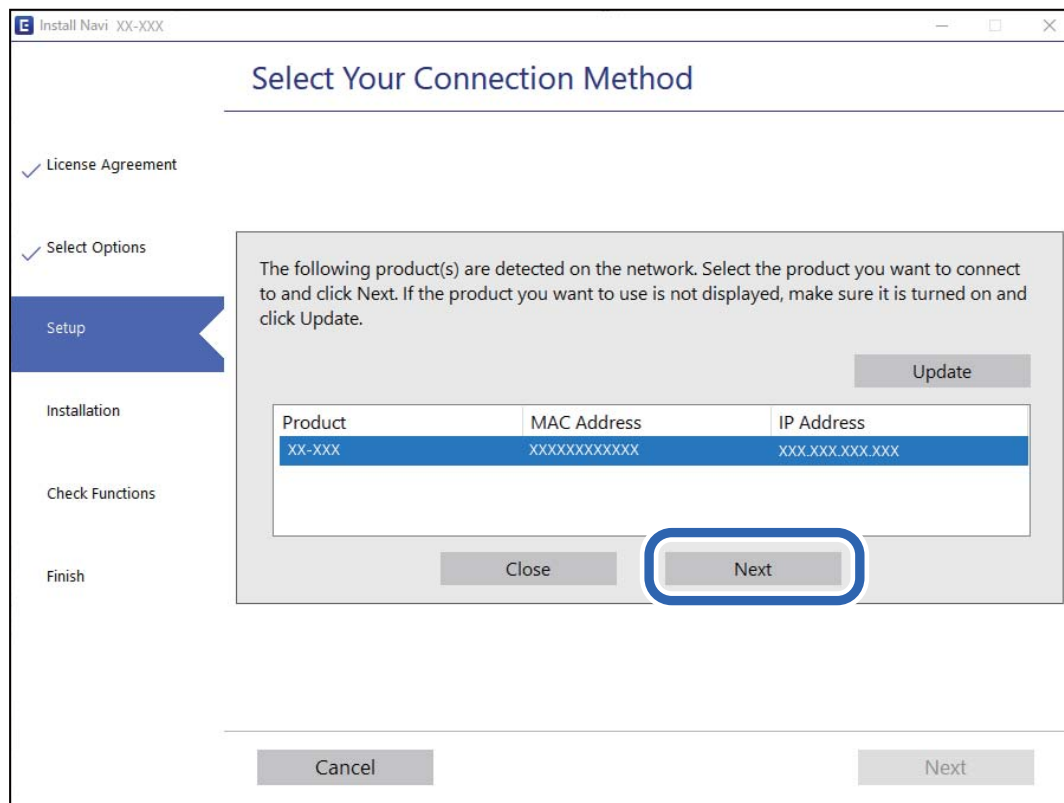
<https://epson.sn>

Kasutusjuhendit saate vaadata jaotises Veebifilmi juhendid. Avage järgmine URL.

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

Skanneri valimine

Järgige ekraanil kuvatud juhiseid, kuni kuvatakse järgmine aken, valige skanneri nimi, millega soovite ühendust luua, ja seejärel klõpsake nuppu **Edasi**.



Järgige ekraanil kuvatud juhtnööre.

Võrguskanneri kasutamine nutiseadmest

Saate nutiseadme skanneriga ühendada, kasutades ühte alljärgnevatest meetoditest.

Ühendamine raadiovõrgu ruuteri abil

Ühendage nutiseade skanneriga samasse Wi-Fi-võrku (SSID).

Lisateabe saamiseks lugege alljärgnevat infot.

[„Nutiseadmega ühendamise sätete tegemine” lk 26](#)

Ühendamine Wi-Fi Direct abil

Ühendage nutiseade skanneriga otse raadiovõrgu ruuterit kasutamata.

Lisateabe saamiseks lugege alljärgnevat infot.

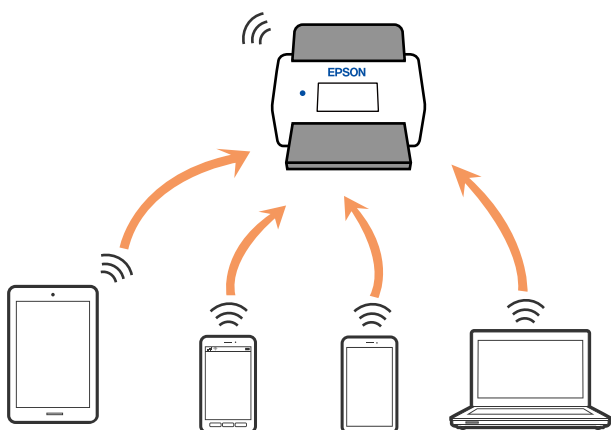
[„Nutiseadme ja skanneri otse ühendamine \(Wi-Fi Direct\)” lk 23](#)

Nutiseadme ja skanneri otse ühendamine (Wi-Fi Direct)

Wi-Fi Direct (lihtne AP) võimaldab ühendada nutiseadme otse skanneriga (kasutamata raadiovõrgu marsruuterit) ja skannida nutiseadmest.

Wi-Fi Direct info


Kasutage seda ühendusviisi, kui te ei kasuta Wi-Fi kodus või kontoris, või kui soovite skanneri ja arvuti/nutiseadme otse ühendada. Selles režiimis toimib skanner raadiovõrgu marsruuterina ja kasutaja saab seadmeid skanneriga ühendada ilma standardset raadiovõrgu marsruuterit kasutamata. Skanneriga otse ühendatud seadmed ei saa aga üksteisega skanneri vahendusel suhelda.



Skanner võib olla samaaegselt ühendatud Wi-Fi või Etherneti ja Wi-Fi Directiga (lihtne AP). Kui loote võrguühenduse režiimis Wi-Fi Direct (lihtne AP) ja samal ajal on skanner ühendatud Wi-Fi-ga, siis Wi-Fi-ühendus katkestatakse ajutiselt.

Ühendamine nutiseadmega režiimis Wi-Fi Direct

See meetod võimaldab ühendada skanneri otse nutiseadmega raadiovõrgu marsruuterit kasutamata.

1. Valige avakuval .
2. Valige **Wi-Fi Direct**.
3. Valige **Käivita häälestus**.
4. Käivitage nutiseadmes Epson Smart Panel.
5. Järgige skanneri ühendamiseks rakenduses Epson Smart Panel kuvatud juhtnööre.
Kui nutiseade on skanneriga ühendatud, minge järgmise toimingu juurde.
6. Valige skanneri juhtpaneelil **Valmis**.

Wi-Fi Direct (lihtne AP) ühenduse katkestamine

Ühendust Wi-Fi Direct (lihtne AP) saab inaktiveerida kahel meetodil; saate keelata kõik ühendused skanneri juhtpaneelilt või keelata iga ühenduse eraldi arvutist või nutiseadmest.

Kui soovite kõik ühendused keelata, valige  > **Wi-Fi Direct** > **Käivita häälestus** > **Muuda** > **Keela funktsioon Wi-Fi Direct**.

Oluline teave:


Kui Wi-Fi Directi (lihtne AP) ühendus on keelatud, katkestatakse ühendus kõigi arvutite ja nutiseadmetega, mis on skanneriga ühendatud Wi-Fi Directi (lihtne AP) ühenduse abil.

Märkus.

Kui soovite katkestada ühenduse konkreetse seadmega, katkestage ühenduse skanneri asemel seadmest. Ühenduse Wi-Fi Direct (lihtne AP) katkestamiseks seadmest kasutage ühte järgmistest meetoditest.

- Lahutage Wi-Fi-ühendus skanneri võrgu nimega (SSID).
- Looge ühendus muu võrgu nimega (SSID).

Wi-Fi Direct (lihtne AP) sätete nagu SSID muutmise

Kui ühendus Wi-Fi Direct (lihtne AP) on lubatud, valige sätete muutmiseks  > **Wi-Fi Direct** > **Käivita häälestus** > **Muuda** ja järgige siis kuvatud menüü-üksuste juhtnööre.

Muuda võrgu nime

Muutke ühenduse Wi-Fi Direct (lihtne AP) võrgunime (SSID), mis on vabalt valitav nimi, mida kasutatakse skanneri ühendamiseks. Saate määrata võrgunime (SSID) ASCII-tärgide abil, mis on kuvatud juhtpaneeli tarkvaraklaviatuuril. Te saate sisestada kuni 22 tähemärki.

Pärast võrgunime (SSID) muutmist katkestatakse kõikide ühendatud seadmete ühendused. Kasutage seadmete uuesti ühendamiseks uut võrgunime (SSID).

Muuda parooli

Muutke ühenduse Wi-Fi Direct (lihtne AP) parooli, mis on vabalt valitav nimi, mida kasutatakse skanneri ühendamiseks. Saate määrata parooli ASCII-tärgide abil, mis on kuvatud juhtpaneeli tarkvaraklaviatuuril. Te saate sisestada 8 kuni 22 tähemärki.

Pärast parooli muutmist katkestatakse kõikide ühendatud seadmete ühendused. Kasutage seadmete uuesti ühendamiseks uut parooli.

Muuda sagedusvahemikku

Ühenduse Wi-Fi Direct sagedusvahemiku muutmise skanneriga ühendamiseks. Valikuteks on 2,4 GHz ja 5 GHz.

Pärast sagedusvahemiku muutmist katkestatakse kõikide ühendatud seadmete ühendused. Ühendage seade uuesti. 5 GHz valimisel ei ole võimalik uuesti ühendada seadmeid, mis ei toeta 5 GHz sagedusala.

Olenevalt piirkonnast ei pruugita seda sätet kuvada.

Keela funktsioon Wi-Fi Direct

Skanneri ühenduse Wi-Fi Direct (lihtne AP) sätete väljalülitamine. Selle väljalülitamise korral katkestatakse kõigi funktsiooniga Wi-Fi Direct (lihtne AP) ühendatud seadmete ühendus skanneriga.

Taasta vaikesätted

Taastab kõik ühenduse Wi-Fi Direct (lihtne AP) vaikesätted.

Nutiseadme skannerisse salvestatud ühenduse Wi-Fi Direct (lihtne AP) teave kustutatakse.

Märkus.

Alljärgnevat sätete muutmiseks avage menüü *Web Config* > **Network** > **Wi-Fi Direct**.

- Wi-Fi Direct (lihtne AP) funktsiooni sisse või välja lülitamine*
- Võrgunime (SSID) muutmine*
- Parooli muutmine*
- Sisendsageduse muutmine*
Olenevalt piirkonnast ei pruugita seda sätet kuvada.
- Ühenduse Wi-Fi Direct (lihtne AP) sätete taastamine*

Võrguühenduse uuesti seadistamine

Selles jaotises selgitatakse, kuidas juhtmeta ruuteri või arvuti vahetamisel võrguühenduse seadeid ja ühendusmeetodit muuta.

Juhtmeta ruuteri asendamisel

Kui asendate raadiovõrgu ruuteri, määrake sätted ühenduse loomiseks arvuti või nutiseadme ja skanneri vahel.

Need sätted tuleb määrata, kui vahetate sideteenuse pakkujat jne.

Arvutiga ühendamise sätete tegemine

Soovitame skanneri arvutiga ühendamiseks kasutada installerit.

Installeri käivitamiseks avage järgmine veebisait ja sisestage seejärel toote nimi. Valige **Häälestus** ja alustage seadistamist.

<https://epson.sn>

Kasutusjuhendit saate vaadata jaotises Veebifilmi juhendid. Avage järgmine URL.

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

Ühendusmeetodi valimine

Järgige ekraanil kuvatud juhtnööre. Valige kuval **Valige installimine** suvand **Häälesta Printer ühendus uuesti (uue marsruuteri jaoks, üleminekul USB-lt võrguühendusele jne)** ja klõpsake seejärel nuppu **Edasi**.

Järgige häälestuse lõpetamiseks ekraanil kuvatud juhtnööre.

Kui te ei saa ühendust, püüdke lahendus leida allpool kirjeldatu abil.

„Võrguga ei saa ühendust luua” lk 32

Nutiseadmega ühendamise sätete tegemine

Te saate skannerit kasutada nutiseadmest, kui ühendate skanneri nutiseadmega samasse Wi-Fi võrku (SSID). Skanneri kasutamiseks nutiseadmest avage järgmine veebisait ja sisestage seejärel toote nimi. Valige **Häälestus** ja alustage seadistamist.

<https://epson.sn>

Minge veebisaidile nutiseadmest, mida soovite skanneriga ühendada.

Arvuti vahetamisel

Arvuti vahetamise korral määrake arvuti ja skanneri ühenduse sätted.

Arvutiga ühendamise sätete tegemine

Soovitame skanneri arvutiga ühendamiseks kasutada installerit.

Installeri käivitamiseks avage järgmine veebisait ja sisestage seejärel toote nimi. Valige **Häälestus** ja alustage seadistamist.

<https://epson.sn>

Kasutusjuhendit saate vaadata jaotises Veebifilmi juhendid. Avage järgmine URL.

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

Järgige ekraanil kuvatud juhtnööre.

Arvutiga ühendamismeetodi muutmine

Selles jaotises on kirjeldatud, kuidas muuta ühendamismeetodit, kui arvuti ja skanner on ühendatud.

Võrguühenduse muutmine võrguühendusest Wi-Fi ühenduseks

Muutke võrguühendus Wi-Fi ühenduseks skanneri juhtpaneeli abil. Ühendusviisi muutmise meetod on põhimõtteliselt samasugune, kui Wi-Fi ühenduse seaded.

Seotud teave

➔ „Ühendamine raadiovõrku (Wi-Fi)” lk 19

Võrguühenduse muutmine Wi-Fi ühendusest võrguühenduseks

Võrguühenduse muutmiseks Wi-Fi ühendusest võrguühenduseks järgige allpooltoodud samme.

1. Valige avakuval **Sätted**.
2. Valige **Võrgusätted** > **Kaabel-LAN-i häälestus**.
3. Järgige ekraanil olevaid juhtnööre.

USB ühenduse muutmine võrguühenduseks

Installeri ja uue seadistuse kasutamine erinevas ühendusmeetodis.

Avage järgmine veebisait ja sisestage seejärel toote nimi. Valige **Häälestus** ja alustage seadistamist.

<https://epson.sn>

Ühendusmeetodi muutmise valimine

Järgige igas aknas kuvatud juhtnööre. Valige kuval **Valige installimine** suvand **Häälesta Printer ühendus uuesti (uue marsruuteri jaoks, üleminekul USB-lt võrguühendusele jne)** ja klõpsake seejärel nuppu **Edasi**.

Valige võrguühendus, mida soovite kasutada — **Ühenda raadiovõrgu (Wi-Fi) kaudu** või **Ühenda arvutivõrgu (Ethernet) abil** — ja klõpsake seejärel nuppu **Edasi**.

Järgige häälestuse lõpetamiseks ekraanil kuvatud juhtnööre.

Võrguühenduse oleku kontrollimine

Saate kontrollida võrguühenduse olekut allpool toodud viisil.

Võrguühenduse oleku kontrollimine juhtpaneelilt

Saate võrguühenduse olekut kontrollida, kasutades skanneri juhtpaneelil olevat võrguikooni või võrguteavet.

Võrguühenduse oleku kontrollimine võrguikooni abil

Saate kontrollida võrguühenduse olekut ja raadiolaine tugevust skanneri avakuval oleva võrguikooni abil.



	<p>Kuvab võrguühenduse oleku.</p> <p>Sätete vaatamiseks ja muutmiseks valige ikoon. See on otsetee järgmisesse menüüsse.</p> <p>Sätted > Võrgusätted > Wi-Fi häälestus</p>
	<p>Skanner ei ole ühendatud raadiovõrku (Wi-Fi).</p>
	<p>Skanner otsid SSID-d, seadistamata IP-aadress või probleem raadiovõrguga (Wi-Fi).</p>
	<p>Skanner on ühendatud raadiovõrku (Wi-Fi).</p> <p>Pulkade arv näitab ühenduse signaalitugevust. Mida rohkem pulki, seda tugevam on ühendus.</p>
	<p>Skanner ei ole ühendatud raadiovõrku (Wi-Fi) režiimis Wi-Fi Direct (lihtne AP).</p>
	<p>Skanner on ühendatud raadiovõrku (Wi-Fi) režiimis Wi-Fi Direct (lihtne AP).</p>
	<p>Skanner ole ühendatud juhtmega võrku (Ethernet) või see on seadistamata.</p>
	<p>Skanner on ühendatud juhtmega võrku (Ethernet).</p>

Üksikasjaliku võrguteabe kuvamine juhtpaneel

Kui skanner on ühendatud võrku, saate kuvada ka muud võrguga seotud teavet, valides võrgumenüüsid, mida soovite vaadata.

1. Valige avakuval **Sätted**.
2. Valige **Võrgusätted > Võrgu olek**.
3. Teabe vaatamiseks valige menüüd, mida soovite vaadata.
 - Juhtmega LAN-i / Wi-Fi olek
Kuvab võrguteabe (seadme nimi, ühendus, signaalitugevus jne) Etherneti- või Wi-Fi-ühenduse kohta.
 - Wi-Fi Directi olek
Kuvab, kas Wi-Fi Direct on lubatud või keelatud, ning SSID-parooli jmt režiimi Wi-Fi Direct ühenduste kohta.
 - Meiliserveri olek
Kuvab meiliserveri võrguteavet.

Võrgu spetsifikatsioonid

Wi-Fi tehnilised andmed

Järgmisest tabelist leiate Wi-Fi tehnilised andmed.

Riigid või regioonid, v.a allpool toodud	Tabel A
--	----------------

<p>Iirimaa, Ühendkuningriik, Austria, Saksamaa, Liechtenstein, Šveits, Prantsusmaa, Belgia, Luksemburg, Madalmaad, Itaalia, Portugal, Hispaania, Taani, Soome, Norra, Rootsi, Island, Horvaatia, Küpros, Kreeka, Põhja-Makedoonia, Serbia, Sloveenia, Malta, Bosnia ja Hertsegoviina, Kosovo, Montenegro, Albaania, Bulgaaria, Tšehhima, Eesti, Ungari, Läti, Leedu, Poola, Rumeenia, Slovakkia, Iisrael, Austraalia, Uus-Meremaa, Taiwan</p>	<p>Tabel B</p>
<p>Türgi</p>	<p>DS-900WN. Seerianumbrid algusega XDA8: Tabel A Seerianumbrid algusega XDA7: Tabel B</p>
	<p>DS-800WN. Seerianumbrid algusega XDA2: Tabel A Seerianumbrid algusega XD9Z: Tabel B</p>

Tabel A

Standardid	IEEE 802.11b/g/n*1
Sagedusvahemik	2400–2483,5 MHz
Maksimaalne raadiosageduslik võimsus	20 dBm (EIRP)
Kanalid	1/2/3/4/5/6/7/8/9/10/11/12/13
Ühendusrežiimid	Infrastruktuur, Wi-Fi Direct (lihtne AP)*2*3
Turvaprotokollid*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Saadaval ainult HT20 korral.

*2 Ei toetata IEEE 802.11b korral.

*3 Infrastruktuuri ja Wi-Fi Direct režiime või Ethernet võrguühendust saab kasutada samaaegselt.

*4 Wi-Fi Direct toetab ainult režiimi WPA2-PSK (AES).

*5 Vastab WPA2 standarditele ja toetab režiimi WPA/WPA2 Personal.

Tabel B

Standardid	IEEE 802.11a/b/g/n*1/ac
Sagedusvahemikud	IEEE 802.11b/g/n: 2.4 GHz, IEEE 802.11a/n/ac: 5 GHz

Kanalid	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48) W58 (149/153/157/161/165)
Ühendusrežiimid	Infrastruktuur, Wi-Fi Direct (lihtne AP)* ⁴ , * ⁵		
Turvaprotokollid* ⁶	WEP (64/128bit), WPA2-PSK (AES)* ⁷ , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Saadaval ainult HT20 korral.

*2 Pole Taiwanis saadaval.

*3 Nende kanalite saadavus ja toote kasutamine õues nende kanalite kaudu erineb asukohati. Lisateabe saamiseks vt <http://support.epson.net/wifi5ghz/>

*4 Ei toetata IEEE 802.11b korral.

*5 Infrastruktuuri ja Wi-Fi Direct režiime või Ethernet võrguühendust saab kasutada samaaegselt.

*6 Wi-Fi Direct toetab ainult režiimi WPA2-PSK (AES).

*7 Vastab WPA2 standarditele ja toetab režiimi WPA/WPA2 Personal.

Etherneti tehnilised nõuded

Standardid	IEEE802.3i (10BASE-T)* ¹ IEEE802.3u (100BASE-TX)* ¹ IEEE802.3ab (1000BASE-T)* ¹ IEEE802.3az (Energiasäästlik Ethernet)* ²
Kommunikatsioonirežiim	Automaatne, 10 Mbps täisdupleksne, 10 Mbps pooldupleksne, 100 Mbps täisdupleksne, 100 Mbps pooldupleksne
Ühenduspesa	RJ-45

*1 Kasutage 5e või kõrgema kategooria STP- (Shielded twisted pair) kaablit, et vältida raadiohäirete ohtu.

*2 Ühendatud seade peab vastama IEEE802.3az standarditele.

Võrgufunktsioonid ja protokollid IPv4/IPv6 tugi

Funktsioonid	Toetatud
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Turvaprotokoll

IEEE802.1X*	
IPsek/IP-filtreerimine	
SSL/TLS	HTTPS server/klient
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Te peate kasutama ühendusseadet, mis on vastavuses IEEE802.1X-ga.

Skanneri jaoks pordi kasutamine

Skanner kasutab alljärgnevat porti. Need pordid tuleks võrguadministraatori poolt vajadusepõhiselt vabastada.

Kui saatja (klient) on skanner

Kasutus	Siht (server)	Protokoll	Pordinumber
Faili saatmine (kui skannerist kasutatakse skannimist võrgukausta)	FTP/FTPS-server	FTP/FTPS (TCP)	20
			21
	Failiserver	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
	WebDAV-server	NetBIOS (TCP)	139
Protokoll HTTP (TCP)		80	
Meilimine (kui skannerist kasutatakse meilile skannimise funktsiooni)	SMTP-server	Protokoll HTTPS (TCP)	443
		SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
SMTP STARTTLS (TCP)		587	
	POP-server	POP3 (TCP)	110
	Teenuse Epson Connect kasutamisel	Epson Connecti server	HTTPS
XMPP			5222
Kasutajateabe kogumine (kasutatakse skanneri kontakte)	LDAP-server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389

Kasutus	Siht (server)	Protokoll	Pordinumbe r
Kasutaja autentimine, kui kogutakse kasutajateavet (kasutatakse skanneri kontakte) Kasutaja autentimine, kui kasutatakse skannimist võrgukausta (SMB)	KDC-server	Kerberos	88
WSD-juhtimine	Klientarvuti	WSD (TCP)	5357
Otsige arvutit, kui kasutate töökeskannimist rakendusest	Klientarvuti	Võrgu avastamine töökeskannimisega	2968

Kui saatja (klient) on klientarvuti

Kasutus	Siht (server)	Protokoll	Pordinumbe r
Skanneri tuvastamine rakenduses nagu EpsonNet Config ja skanneridraiveris.	Skanner	ENPC (UDP)	3289
MIB teabe kogumine ja häälestamine rakenduses nagu EpsonNet Config ja skanneridraiveris.	Skanner	SNMP (UDP)	161
WSD-skanneri otsimine	Skanner	WS-Discovery (UDP)	3702
Skanniandmete edastamine rakendusest	Skanner	Võrguskannimine (TCP)	1865
Tööteabe kogumine, kui kasutate töökeskannimist rakendusest	Skanner	Võrgu töökeskannimine	2968
Web Config	Skanner	HTTP (TCP)	80
		HTTPS (TCP)	443

Probleemide lahendamine

Võrguga ei saa ühendust luua

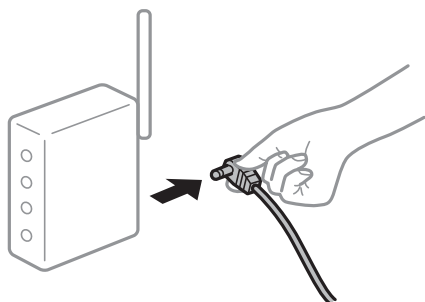
Probleemide põhjused võivad olla alljärgnevad.

■ Wi-Fi-ühenduse võrguseadmetega on midagi valesti.

Lahendused

Lülitage välja seadmed, mida soovite võrguga ühendada. Oodake ligikaudu 10 sekundit ja seejärel lülitage seadmed järgmises järjekorras sisse: raadiovõrgu ruuter, arvuti või nutiseade ja seejärel skanner. Viige

skanner ja arvuti või nutiseade raadiovõrgu ruuterile lähemale, et parandada raadiosidet, ning proovige seejärel uuesti võrgusätted määrata.



Seadmed ei saa juhtmeta ruuterilt signaale vastu võtta, sest need on üksteisest liiga kaugel.

Lahendused

Pärast arvuti või nutiseadme ja skanneri juhtmeta ruuterile lähemale viimist lülitage juhtmeta ruuter välja ja seejärel uuesti sisse.

Juhtmeta ruuteri vahetamisel ei vasta seaded uuele ruuterile.

Lahendused

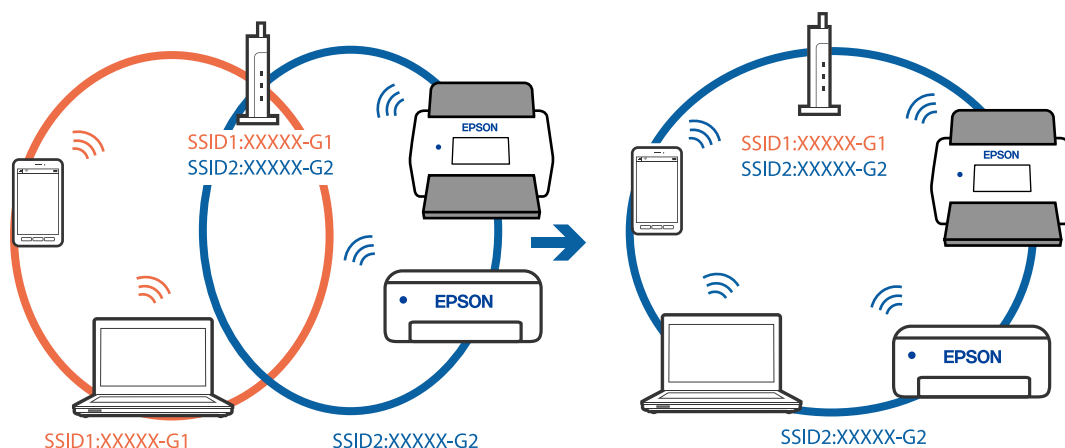
Tehke ühenduse seaded uuesti, et need vastaksid uuele juhtmeta ruuterile.

Arvutil või nutiseadmel ja nendega ühendatud arvutil on erinevad SSID-d.

Lahendused

Kui kasutate samaaegselt mitut juhtmeta ruuterit või kui juhtmeta ruuteril on mitu SSID-d ja seadmed on ühendatud erinevate SSID-dega, ei saa te juhtmeta ruuteriga ühendust luua.

Ühendage arvuti või nutiseade sama SSID külge, mille külge on ühendatud skanner.



Juhtmeta ruuteri privaatsuseraldaja on aktiivne.

Lahendused

Enamik raadiovõrgu ruutereid on privaatsuseraldaja funktsiooniga, mis blokeerib sidet ühendatud seadmete vahel. Kui te ei saa luua ühendust skanneri ja arvuti või nutiseadme vahel, ehkki need on ühendatud samasse võrku, inaktiveerige ruuteri privaatsuseraldaja. Lugege üksikasju juhtmevaba ruuteriga kaasnenud juhendist.

■ IP-aadress ei ole korrektselt määratud.

Lahendused

Kui skannerile määratud IP-aadress on 169.254.XXX.XXX ja alamvõrgumask 255.255.0.0, ei pruugita IP-aadressi õigesti määrata.

Valige skanneri juhtpaneelil **Sätted > Võrgusätted > Täpsem > TCP/IP** ja kontrollige siis skannerile määratud IP-aadressi ja alamvõrgumaski.

Lähtestage raadiovõrgu ruuter või lähtestage skanneri võrgusätted.

■ Probleem printeri võrgusätetega.

Lahendused

Proovige arvutist pääseda mis tahes veebisaidile veendumaks, et arvuti võrgusätted on õiged. Kui te ei pääse ühelegi veebisaidile, on probleem arvutis.

Kontrollige arvuti võrguühendust. Lugege üksikasju arvutiga kaasnenud dokumentatsioonist.

■ Skanneri Ethernetiga ühendamiseks on kasutatud seadmeid, mis toetavad standardit IEEE 802.3az (energiatõhus Ethernet).

Lahendused

Kui ühendate skanneri Ethernetiga, kasutades seadmeid, mis toetavad standardit IEEE 802.3az (energiatõhus Ethernet), võivad olenevalt kasutatavast jaoturist või ruuterist esineda järgmised probleemid.

- Ühendus muutub ebastabiilseks, ühendus skanneriga katkeb pidevalt.
- Skanneriga ei õnnestu ühendust luua.
- Side kiirus muutub aeglaseks.

Järgige allpool toodud samme standardi IEEE 802.3az keelamiseks skanneris ja looge seejärel ühendus uuesti.

1. Eemaldage arvuti ja skanneriga ühendatud Etherneti-kaabel.
2. Kui IEEE 802.3az on arvutis lubatud, keelake see.
Lugege üksikasju arvutiga kaasnenud dokumentatsioonist.
3. Ühendage arvuti ja skanner Etherneti-kaabliga otse.
4. Kontrollige skanneri võrgusätteid.
Valige **Sätted > Võrgusätted > Võrgu olek > Juhtmega LAN-i / Wi-Fi olek**.
5. Kontrollige skanneri IP-aadressi.
6. Avage arvutis Web Config.
Käivitage veebibrauser ja sisestage seejärel skanneri IP-aadress.
[„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)
7. Valige vahekaart **Network > Wired LAN**.
8. Suvandi **OFF** sätteks valige **IEEE 802.3az**.

9. Klõpsake nuppu **Next**.
 10. Klõpsake nuppu **OK**.
 11. Eemaldage arvuti ja skanneriga ühendatud Etherneti-kaabel.
 12. Kui keelasite sammus 2 arvutis standardi IEEE 802.3az, lubage see.
 13. Ühendage sammus 1 eemaldatud Etherneti-kaablid arvuti ja skanneriga.
- Kui probleem ei kao, võib probleem olla põhjustatud mõne muu seadme mitte skanneri poolt.

■ **Skanner on välja lülitatud.**

Lahendused

Veenduge, et skanner oleks sisse lülitatud.

Oodake, kuni olekutuli lõpetab vilkumise, mis tähendab, et skanner on töövalmis.

Skanneri seadistamise tarkvara

Skanneritoimingute konfigureerimise rakendus (Web Config)	37
Epson Device Admin.	38

Skanneritoimingute konfigureerimise rakendus (Web Config)

Web Config on rakendus, mis töötab arvuti või nutiseadme veebibrauserites, nagu Microsoft Edge ja Safari. Saate kontrollida skanneri olekut või muuta võrguteenuseid ja skanneri sätteid. Rakenduse Web Config kasutamiseks ühendage skanner ja arvuti või seade samasse võrku.

Toetatud on järgmised brauserid. Kasutage uusimat versiooni.

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

Märkus.

Teilt võidakse seadme kasutamiseks küsida administraatori parooli. Lugege lisateavet administraatori parooli kohta allpool.

[„Märkused administraatori parooli kohta” lk 10](#)

Seotud teave

➔ [„Utiliiti Web Config ei õnnestu avada” lk 64](#)

Kuidas kasutada veebibrauseris rakendust Web Config

Skannerisse on integreeritud tarkvara nimega Web Config (veebileht, mille saate sätteid määrata). Rakenduse Web Config avamiseks sisestage lihtsalt brauserisse võrku ühendatud skanneri IP-aadress.

1. Kontrollige skanneri IP-aadressi.

Valige skanneri juhtpaneelil **Sätted > Võrgusätted > Võrgu olek**. Seejärel valige aktiivne ühendusmeetod (**Juhtmega LAN-i / Wi-Fi olek** või **Wi-Fi Directi olek**), et kontrollida skanneri IP aadressi.

IP-aadressi näide: 192.168.100.201

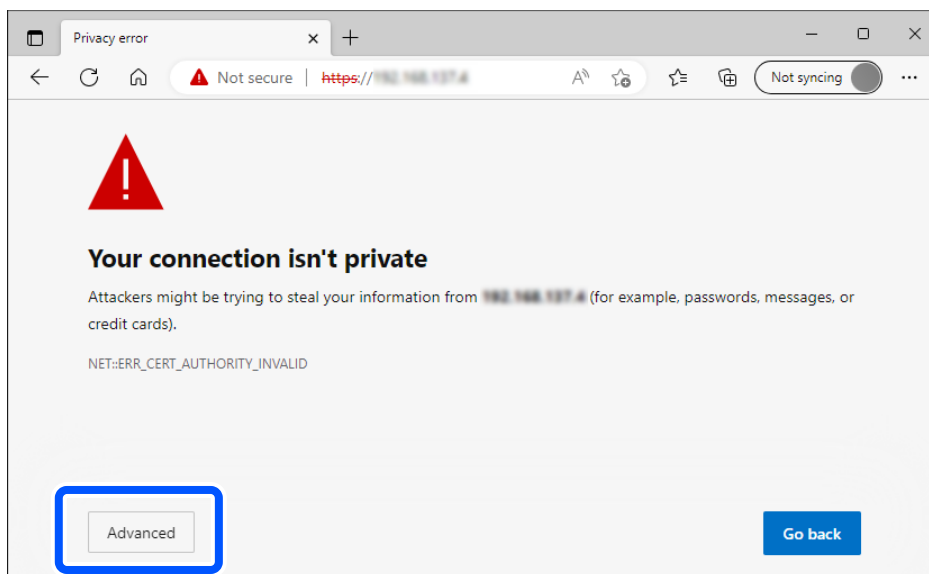
2. Avage arvutis või nutiseadmes brauser ja sisestage aadressiribale skanneri IP-aadress.

Vorming: http://skanneri IP-aadress/

Näide: http://192.168.100.201/

Kui brauseris kuvatakse hoiatus, võite seda ohutult ignoreerida ja avada veebilehe (Web Config). Kuna skanner kasutab HTTPS-aadressile pöördumiseks iseallkirjastatud sertifikaati, kuvatakse rakenduse Web Config käivitamisel brauseris hoiatus. See ei viita probleemile ja seda võib ohutult ignoreerida. Olenevalt brauserist võib veebilehe avamiseks olla vajalik klõpsata nuppu **Täpsemad sätted**.

Näide: Microsoft Edge



Märkus.

Kui hoiatust ei kuvata, minge järgmise punkti juurde.

Kasutage IPv6-aadressi korral järgmist vormingut.

Vorming: `http://[skanneri IP-aadress]/`

Näide: `http://[2001:db8::1000:1]/`

3. Skanneri sätete muutmiseks peate sisse logima rakenduse Web Config administraatorina.

Klõpsake ekraanil üleval paremal nuppu **Log in**. Sisestage **User Name** ja **Current password** ning seejärel klõpsake nuppu **OK**.

Allpool on toodud rakenduse Web Config administraatori teabe algväärtused.

·Kasutajanimi: puudub (tühi)

·Parool: oleneb tootele kinnitatud sildist.

Kui tagaküljele on kinnitatud silt „PASSWORD“, sisestage sildil olev 8-kohaline number. Kui silti „PASSWORD“ ei ole, sisestage administraatori paroolina toote tagaküljel oleval sildil toodud seerianumber.

Märkus.

Kui ekraanil on üleval paremal kuvatud **Log out**, olete juba administraatorina sisse logitud.

Teid logitakse automaatselt välja, kui ligikaudu 20 minutit pole tehtud ühtegi toimingut.

Epson Device Admin

Epson Device Admin on mitmefunktsiooniline rakendus, millega saate hallata võrguseadmeid.

Saate kasutada konfiguratsioonimalle, et rakendada samu sätteid mitmele skannerile võrgus, mis muudab selle sobivaks mitme skanneri installimiseks ja haldamiseks.

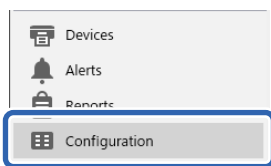
Rakenduse Epson Device Admin saate alla laadida Epsoni toe veebisaidilt. Üksikasju rakenduse kasutamise kohta vaadake rakenduse Epson Device Admin dokumentatsioonist või spikrist.

Konfiguratsioonimall

Konfiguratsioonimalli loomine

Looge uus konfiguratsioonimall.

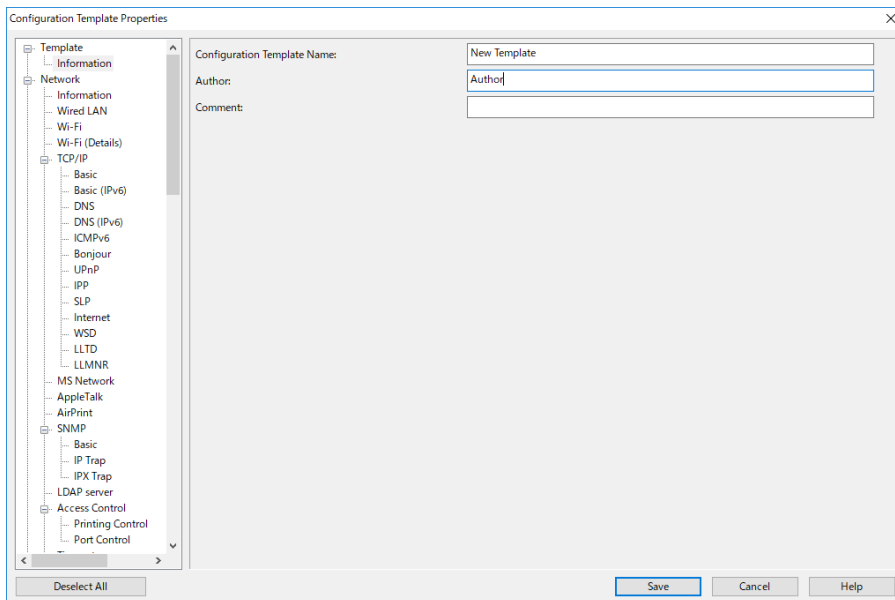
1. Käivitage Epson Device Admin.
2. Valige külgriba tegumimenüüst **Configuration**.



3. Valige ribamenüüst **New**.



4. Seadistage kõik kirjed.



Kirje	Selgitus
Configuration Template Name	Konfiguratsioonimalli nimi. Sisestage kuni 1024 tähemärki koodis Unicode (UTF-8).
Author	Teave malli looja kohta. Sisestage kuni 1024 tähemärki koodis Unicode (UTF-8).

Kirje	Selgitus
Comment	Sisestage lisateave. Sisestage kuni 1024 tähemärki koodis Unicode (UTF-8).

- Valige seadistatavad kirjed vasakult.

Märkus.

Erinevatele kuvadele minemiseks valige vasakult menüükirjeid. Seadistatud väärtus salvestatakse, kui te kuva muudate, aga seda ei salvestata, kui te kuval loobumispuppu vajutate. Kui olete seadistamise lõpetanud, klõpsake nuppu **Save**.

Konfiguratsioonimalli rakendamine

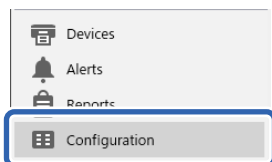
Rakendage salvestatud konfiguratsioonimall skanneris. Rakendatakse mallis valitud sätted. Kui sihtskanneril asjakohane funktsioon puudub, siis seda ei rakendata.

Märkus.

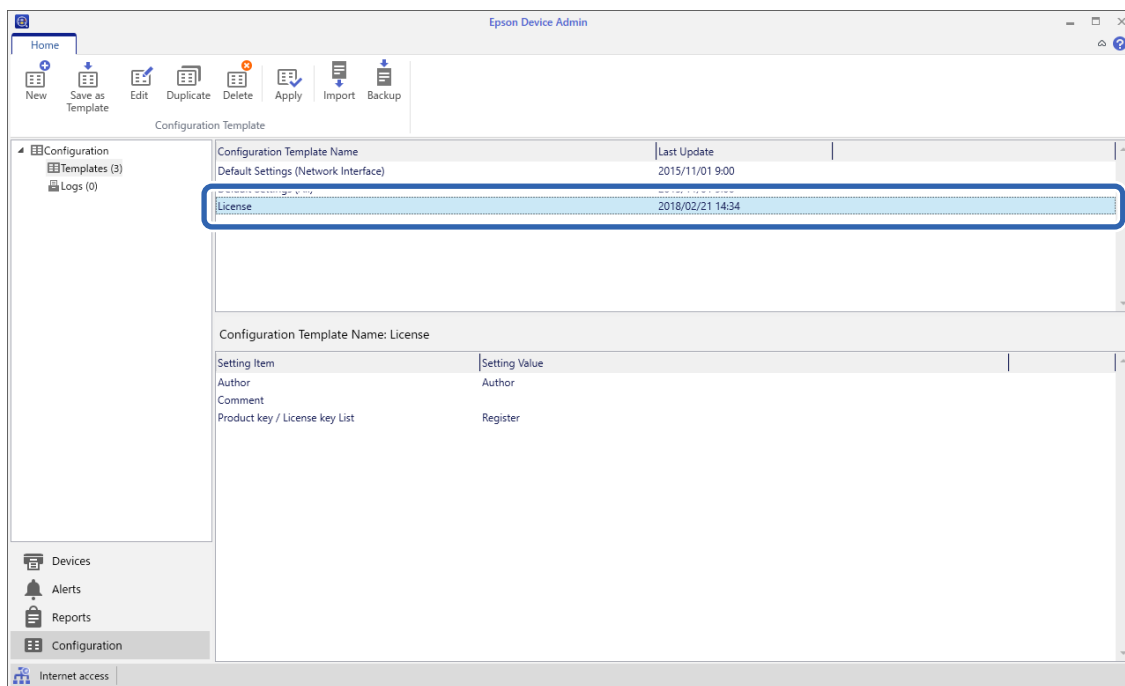
Kui skannerile on määratud administraatori parool, konfigureerige see eelnevalt.

- Valige seadmeloendi ribamenüüs: **Options > Password manager**.
- Valige **Enable automatic password management** ja klõpsake seejärel nuppu **Password manager**.
- Valige asjakohane skanner ja klõpsake seejärel nuppu **Edit**.
- Seadistage parool ja klõpsake seejärel nuppu **OK**.

- Valige külgriba tegumimenüüst **Configuration**.

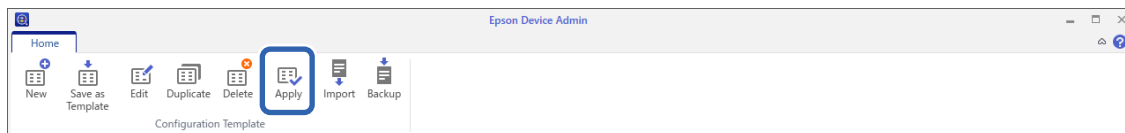


2. Valige rakendatav konfiguratsioonimall asukohast **Configuration Template Name**.



3. Klõpsake ribamenüüs nupp **Apply**.

Kuvatakse seadme valimise kuva.

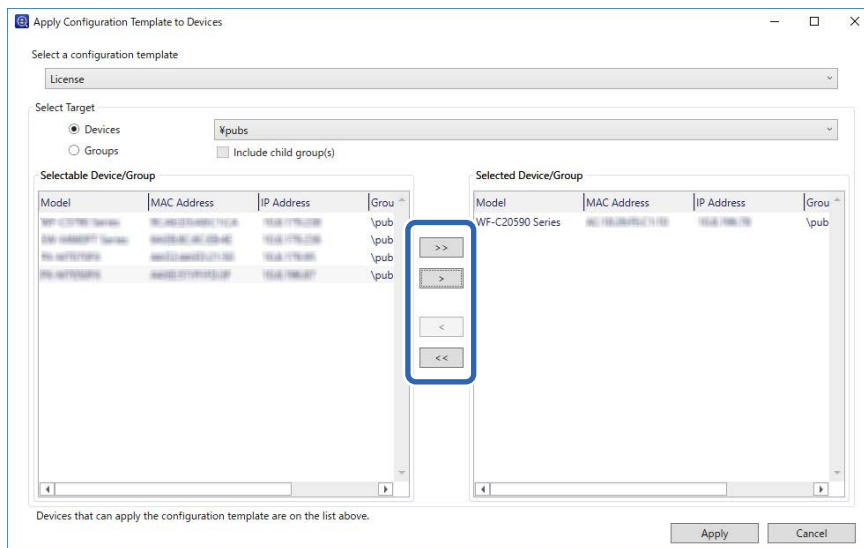


4. Valige konfiguratsioonimall, mida soovite rakendada.

Märkus.

- Kui teete valiku **Devices** ja valite rippmenüüst seadmeid sisaldavaid rühmi, kuvatakse iga seade.
- Rühmad kuvatakse, kui teete valiku **Groups**. Valige **Include child group(s)**, et valida valitud rühmast automaatselt alamrühmi.

- Teisaldage skanner või rühmad, millele soovite malli rakendada, asukohta **Selected Device/Group**.



- Klõpsake nuppu **Apply**.
Kuvatakse rakendatava konfiguratsioonimalli kinnitusküsimus.
- Klõpsake konfiguratsioonimalli rakendamiseks nuppu **OK**.
- Kui kuvatakse teade, mis ütleb, et protseduur on lõpetatud, klõpsake nuppu **OK**.
- Klõpsake nuppu **Details** ja lugege läbi kuvatut teave.
Kui rakendatud üksustel kuvatakse , on rakendamine edukalt lõpetatud.
- Klõpsake nuppu **Close**.

Nõutud sätted skannimiseks

Meiliserveri registreerimine.	44
Võrgukausta loomine.	46
Kontaktide kättesaadavaks tegemine.	54
Funktsiooni AirPrint seadistamine.	63
Probleemid võrguskannimise ettevalmistamisega.	64

Meiliserveri registreerimine

Enne meiliserveri konfigureerimist kontrollige järgmist.

Skanner on võrku ühendatud

Meiliserveri häälestusteave

Kui kasutate veebipõhist meiliserverit, uurige sätteid pakkujalt või veebisaidilt.

Registreerimine

Avage Web Config, vahekaart **Network** > **Email Server** > **Basic**.

„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Seadistamine on võimalik ka skanneri juhtpaneelilt. Valige **Sätted** > **Võrgusätted** > **Täpsem** > **Meiliserver** > **Serverisätted**.

Meiliserveri sätteüksused

Kirje	Sätted ja selgitused	
Authentication Method	Määrake skannerile autentimismeetod, mida kasutatakse meiliserverile juurdepääsul.	
	Off	Autentimine on side ajal meiliserveriga inaktiveeritud.
	SMTP AUTH	Meiliserver peab toetama SMTP-autentimist.
	POP before SMTP	Kui valite selle üksuse, siis määrake POP3-server.
Authenticated Account	Kui SMTP AUTH või POP before SMTP on määratud suvandi Authentication Method sätteks, tuleb sisestada autentitud konto nimi. Sisestage 0 kuni 255 tärki ASCII-vormingus (0x20–0x7E).	
Authenticated Password	Kui SMTP AUTH või POP before SMTP on määratud suvandi Authentication Method sätteks, tuleb sisestada autentitud parool. Sisestage 0 kuni 20 tärki ASCII-vormingus (0x20–0x7E).	
Sender's Email Address	Määrake meiliaadress, mida kasutatakse skannerist meilimiseks. Ehkki saate kasutada juba kasutusel olevat meiliaadressi, soovitame luua ja seadistada eraldi meiliaadressi, et skannerist saadetud meile oleks võimalik eristada. Sisestage 0 kuni 255 tärki ASCII-vormingus (0x20–0x7E) v.a : () < > [] ; ¥. Punkt „.” ei saa olla esimene tärk.	
SMTP Server Address	Sisestage 0–255 tähemärki (A–Z a–z 0–9 . -). Te võite kasutada vormingut IPv4 või FQDN.	
SMTP Server Port Number	Sisestage number vahemikus 1 kuni 65535.	
Secure Connection	Määrake e-posti serveri turvalise ühenduse viis.	
	None	Kui valite POP before SMTP viisiks Authentication Method , siis on ühendusviis seadistatud kui None .
	SSL/TLS	See on saadaval, kui Authentication Method on seadistatud olekusse Off või SMTP AUTH .
	STARTTLS	See on saadaval, kui Authentication Method on seadistatud olekusse Off või SMTP AUTH .
Certificate Validation (ainult Web Config)	Kui see on aktiveeritud, on sert kontrollitud. Soovitame kasutada sätet Enable , kui suvandi Secure Connection säte on miski muu kui None .	

Kirje	Sätted ja selgitused
POP3 Server Address	Kui POP before SMTP on määratud suvandi Authentication Method sätteks, tuleb sisestada POP3-serveri aadress. Saate sisestada 0 kuni 255 tärki, kasutades tärke A–Z, a–z, 0–9. Te võite kasutada vormingut IPv4 või FQDN.
POP3 Server Port Number	Seadistage, kui POP before SMTP on määratud suvandi Authentication Method sätteks. Sisestage number vahemikus 1 kuni 65535.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)

Meiliserveri ühenduse kontrollimine

1. Valige ühenduse kontrollimise menüü.

Seadistamine rakenduses Web Config.

Valige vahekaart **Network > Email Server > Connection Test > Start.**

Seadistamine juhtpaneelilt.

Valige **Sätted > Võrgusätted > Täpsem > Meiliserver > Ühenduse kontrollimine.**

Algab meiliserveri ühenduse kontroll.

2. Vaadake kontrolli tulemusi.

Ühenduse kontroll õnnestus, kui kuvatakse teade **Connection test was successful.**

Kui kuvatakse tõrge, järgige tõrke eemaldamiseks teates olevaid juhtnööre.

[„Meiliserveri ühenduse testimisviited” lk 45](#)

Meiliserveri ühenduse testimisviited

Teade	Põhjus
SMTP server communication error. Check the following. - Network Settings	See teade kuvatakse alljärgnevatel juhtudel <ul style="list-style-type: none"> <input type="checkbox"/> Skanner ei ole ühendatud võrku <input type="checkbox"/> SMTP-server on maas <input type="checkbox"/> Võrguühendus on side ajal katkenud <input type="checkbox"/> Vastu on võetud ebatäielikud andmed
POP3 server communication error. Check the following. - Network Settings	See teade kuvatakse alljärgnevatel juhtudel <ul style="list-style-type: none"> <input type="checkbox"/> Skanner ei ole ühendatud võrku <input type="checkbox"/> POP3-server on maas <input type="checkbox"/> Võrguühendus on side ajal katkenud <input type="checkbox"/> Vastu on võetud ebatäielikud andmed
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	See teade kuvatakse alljärgnevatel juhtudel <ul style="list-style-type: none"> <input type="checkbox"/> DNS-serveriga ühenduse loomine on nurjunud <input type="checkbox"/> SMTP-serveri nimelahendus on nurjunud

Teade	Põhjus
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	See teade kuvatakse alljärgnevatel juhtudel <input type="checkbox"/> DNS-serveriga ühenduse loomine on nurjunud <input type="checkbox"/> POP3-serveri nimelahendus nurjus
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	See teade kuvatakse, kui SMTP-serveri autentimine on nurjunud.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	See teade kuvatakse, kui POP3-serveri autentimine on nurjunud.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	See teade kuvatakse, kui püüate sidet pidada toetamata protokolle kasutades.
Connection to SMTP server failed. Change Secure Connection to None.	See teade kuvatakse, kui serveri ja kliendi vahel esineb SMTP lahknevus või kui server ei toeta turvalist SMTP-ühendust (SSL-ühendus).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	See teade kuvatakse, kui serveri ja kliendi vahel esineb SMTP lahknevus või kui server taotleb SSL/TLS-ühenduse kasutamist turvalise SMTP-ühenduse jaoks.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	See teade kuvatakse, kui serveri ja kliendi vahel esineb SMTP lahknevus või kui server taotleb STARTTLS-ühenduse kasutamist turvalise SMTP-ühenduse jaoks.
The connection is untrusted. Check the following. - Date and Time	See teade kuvatakse, kui skanneri kuupäeva ja kellaaaja säte on vale või sertifikaat on aegunud.
The connection is untrusted. Check the following. - CA Certificate	See teade kuvatakse, kui skanneril puudub serverile vastav juursert või kui CA Certificate on importimata.
The connection is not secured.	See teade kuvatakse, kui hangitud sertifikaat on kahjustatud.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	See teade kuvatakse, kui serveri ja kliendi vahel esineb autentimismeetodi lahknevus. Server toetab autentimislaiendit SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	See teade kuvatakse, kui serveri ja kliendi vahel esineb autentimismeetodi lahknevus. Server ei toeta autentimislaiendit SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	See teade kuvatakse, kui määratud saatja meiliaadress on vale.
Cannot access the product until processing is complete.	See teade kuvatakse, kui skanner on hõivatud.

Võrgukausta loomine

Looge arvutis võrgukaust. Arvuti peab olema ühendatud skanneriga samasse võrku.

Võrgukausta määramise meetod erineb olenevalt keskkonnast. See on näide võrgukausta loomisest lauaarvuti töölaua ja järgmises keskkonnas.

- Operatsioonisüsteem: Windows 10
- Ühiskausta loomise koht: töölaua
- Kausta tee: C:\Users\xxxx\Desktop\scan_folder (looge töölauale võrgukaust nimega „scan_folder“)

1. Logige arvutiülesõiduga kasutajakontoga arvutisse, kuhu tahate luua võrgukausta.

Märkus.

Kui te ei tea, millisel kasutajakontol on arvutiülesõiduga õigused, küsige seda oma arvutiadministraatorilt.

2. Veenduge, et seadme nimes (arvuti nimi) ei oleks kahebaidiseid tärke. Klõpsake Windowsis nuppu Start ja valige seejärel  **Sätted > Süsteem > Teave.**

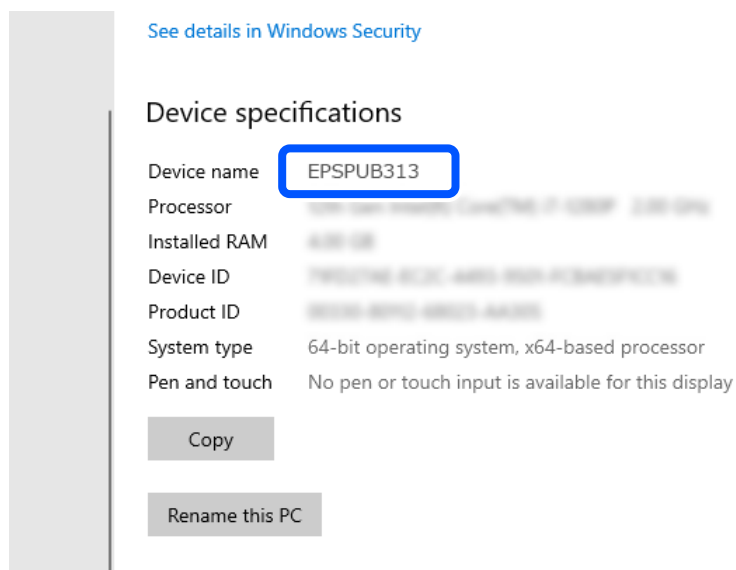
Märkus.

Kui seadme nimes on kahebaidiseid tärke, võib faili salvestamine nurjuda.

3. Veenduge, et asukohas **Seadme tehnilised andmed > Seadme nimi** kuvatud string ei sisaldaks kahebaidiseid tärke.

Kui seadme nimi sisaldab ainult ühebaidiseid tärke, ei tohiks probleeme esineda. Sulgege aken.

Näide: EPSPUB313



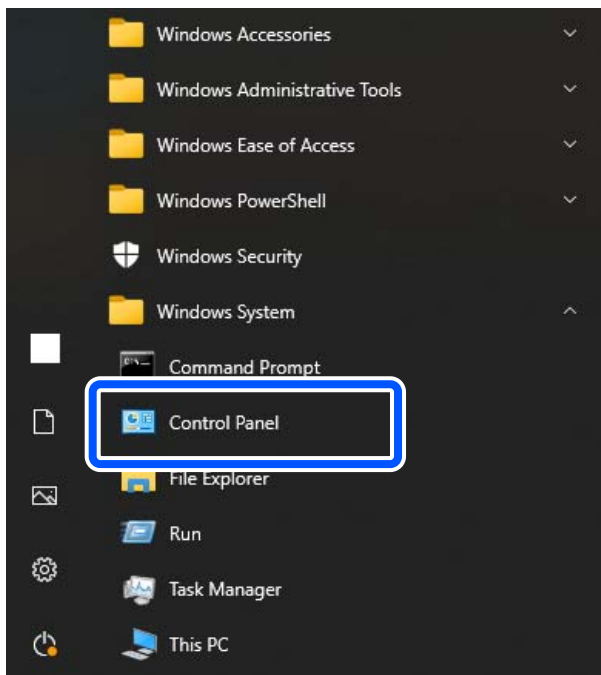
Oluline teave:

Kui seadme nimi sisaldab kahebaidiseid tärke, kasutage arvutit, mis ei kasuta kahebaidiseid tärke või nimetage seade ümber.

Kui peate seadme nime muutma, teavitage sellest eelnevalt oma arvutiadministraatorit, kuna see võib mõjutada arvuti haldamist ja juurdepääsu ressurssidele.

Seejärel vaadake üle oma arvuti sätted.

4. Klõpsake Windowsis nuppu Start ja valige seejärel **Windowsi süsteem > Juhtpaneel**.



5. Klõpsake juhtpaneelil nuppu **Võrk ja Internet > Võrgu- ja ühiskasutuskeskus > Muuda ühiskasutuse täpsemaid sätteid**.

Kuvatakse võrguprofil.

6. Veenduge, et **Lülita failide ja printerite ühiskasutus sisse** oleks võrguprofilile (valitud profiil) asukohas **Failide ja printerite ühiskasutus** valitud.

Kui see on juba valitud, klõpsake nuppu **Loobu** ja sulgege aken.

Kui muudate sätteid, klõpsake **Salvesta muudatused** ja sulgege aken.

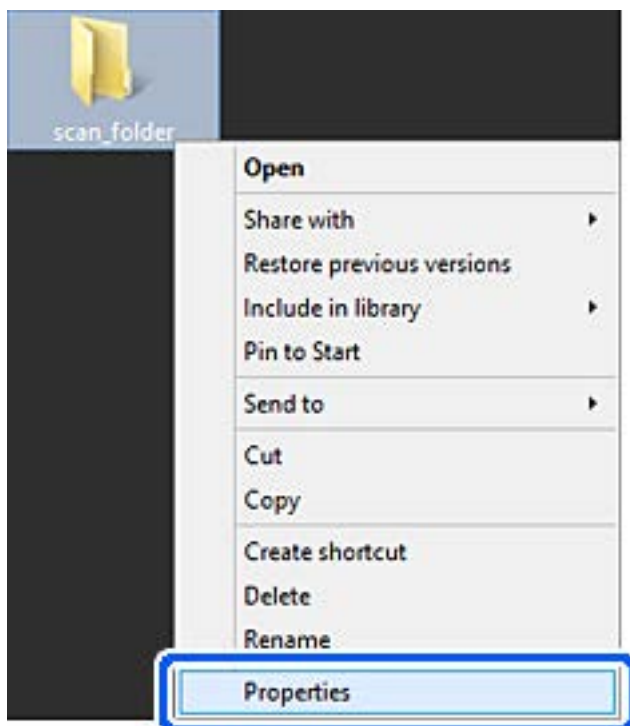
Seejärel looge võrgukaust.

7. Looge töölaual kaust ja andke sellele nimi.

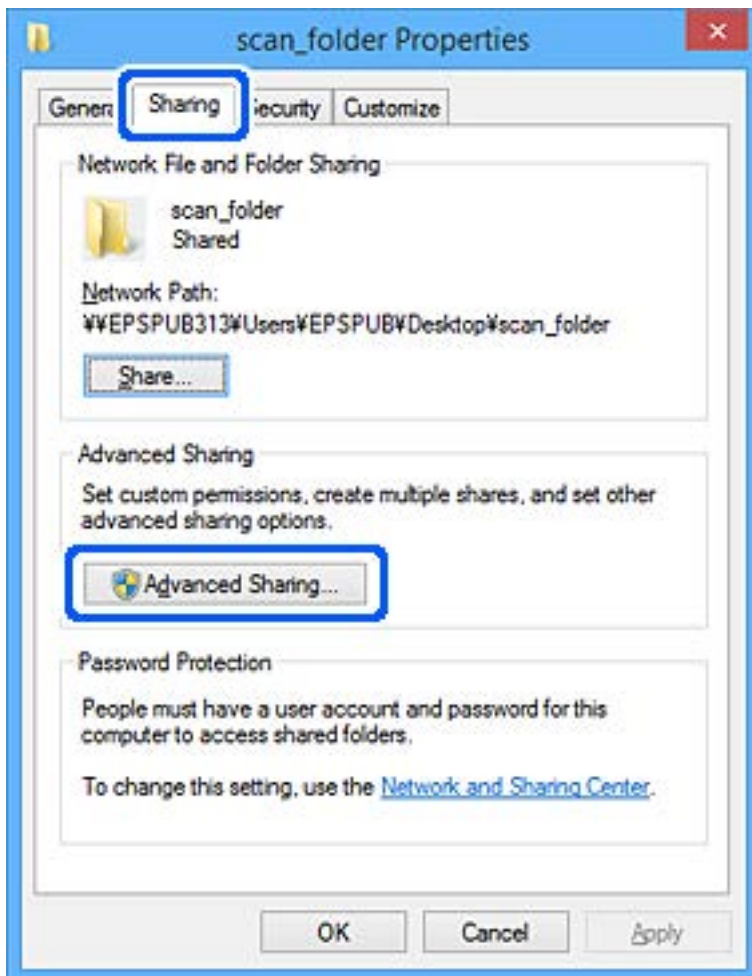
Valige kaustanimeks 1 kuni 12 tärgist koosnev nimi. Kui nimi on pikem kui 12 tärki, ei pruugi olenevalt keskkonnast juurdepääs sellele võimalik olla.

Näide: scan_folder

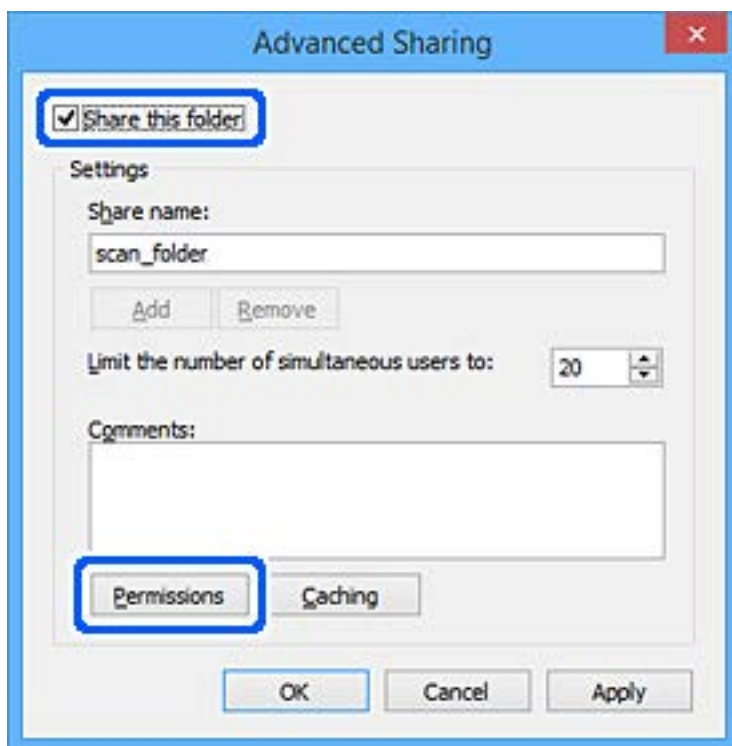
8. Paremklopsake kausta ja seejärel valige **Atribuudid**.



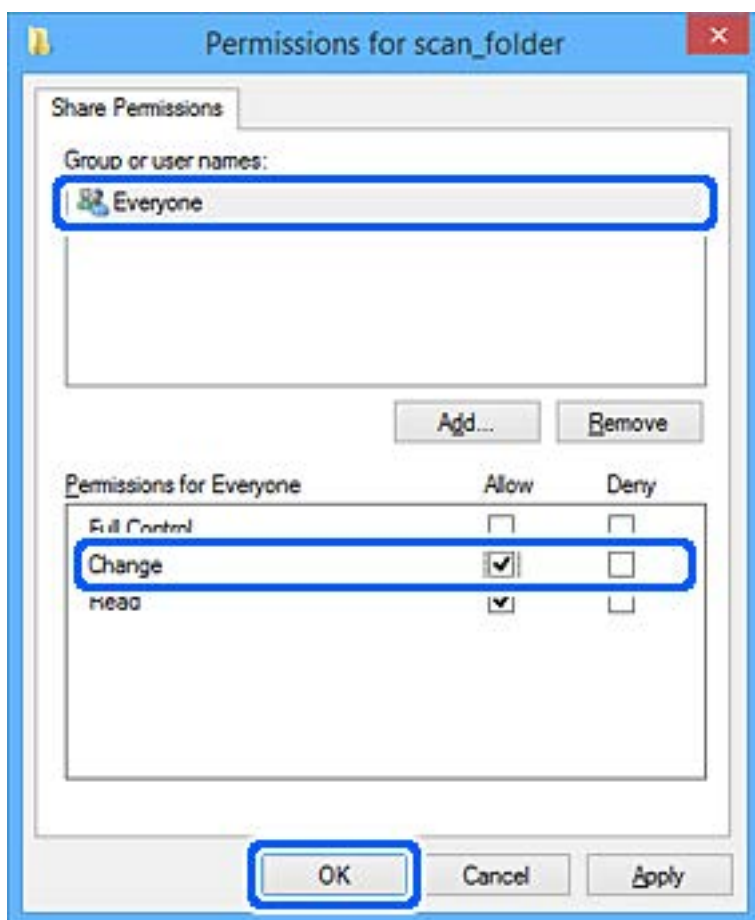
9. Klõpsake vahekaardil **Ühiskasutus** valikut **Täpsemad ühiskasutuse suvandid**.



10. Valige Anna see kaust ühiskasutusse ja seejärel klõpsake nuppu **Õigused**.



11. Valige **Rühma-** või **kasutajanimed** alt rühm **Kõik**, valige **Luba** suvandis **Muuda** ja seejärel klõpsake nuppu **OK**.

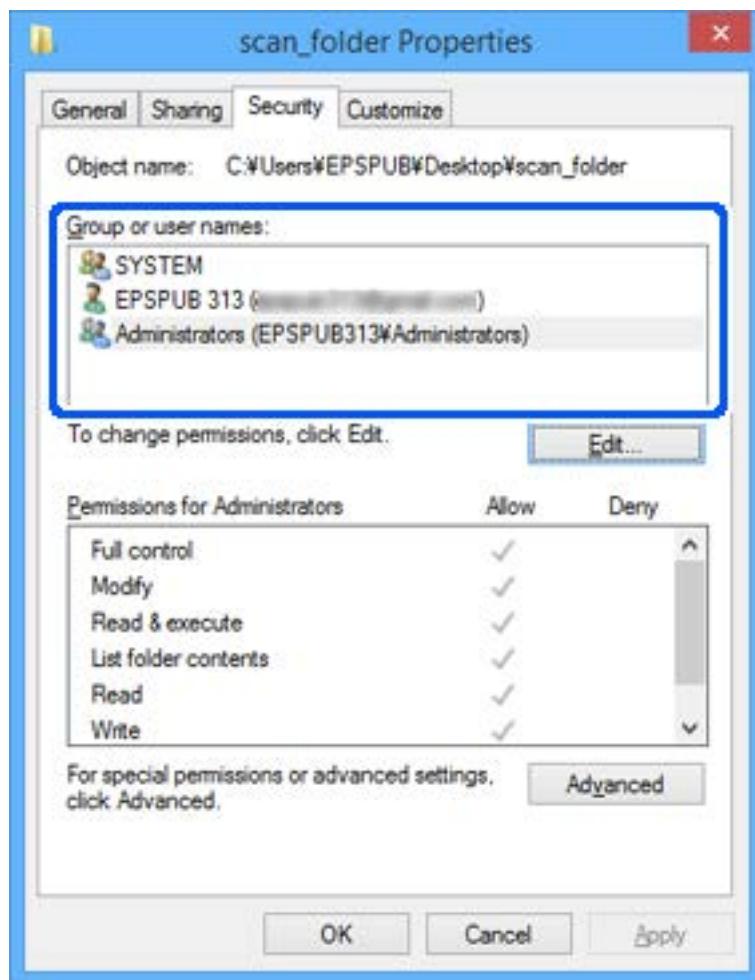


12. Klõpsake nuppu **OK**, et aken sulgeda ja naasta atribuutide aknasse.

Märkus.

Millised rühmad ja kasutajad võrgukaustale juurdepääsu omavad saate kontrollida vahekaardil **Turve > Rühma- või kasutajanimed**.

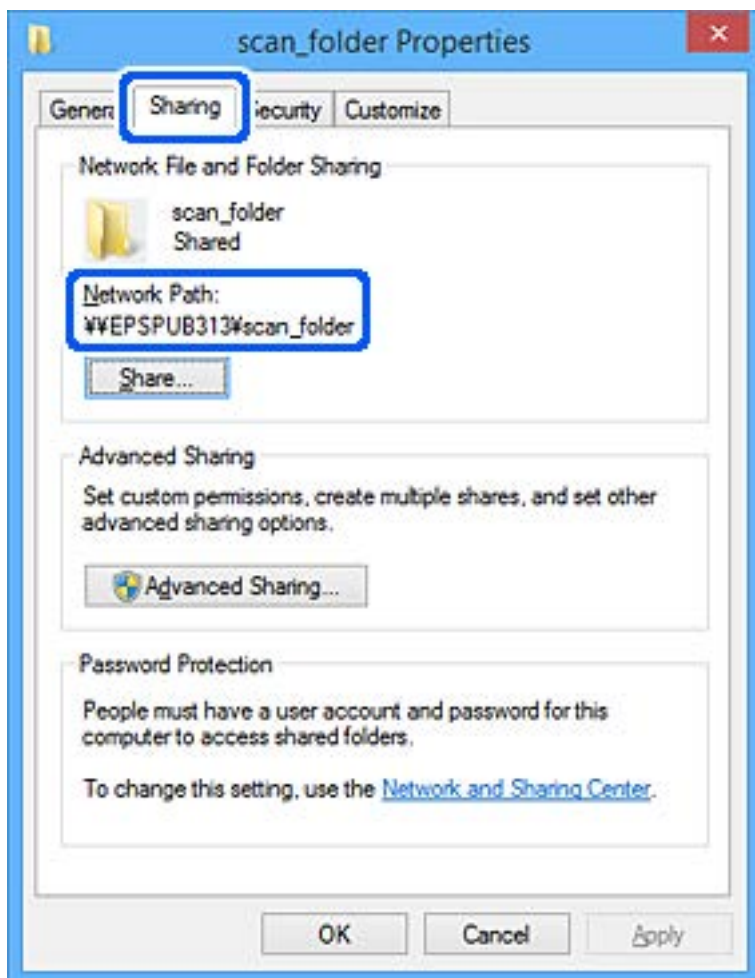
Näide: kui võrgukaustale omavad juurdepääsu nii arvutisse logitud kasutaja kui ka arvutiülemad



13. Valige vahekaart **Ühiskasutus**.

Kuvatakse võrgukausta võrgutee. Seda kasutatakse teie skanneri kontaktidesse registreerimisel. Kirjutage see üles.

Näide: \\EPSPUB313\scan_folder



14. Klõpsake akna sulgemiseks nuppu **Sule** või **OK**.

Sellega on võrgukausta loomine lõpetatud.

Kontaktide kättesaadavaks tegemine

Sihtkohtade registreerimine skanneri kontaktidesse võimaldab skannides mugavalt sihtkoha sisestada.

Kontaktiloendisse saab registreerida järgmisi kontaktitüüpe. Kokku saate registreerida kuni 300 kannet.

Märkus.

Lisaks saate sihtkoha sisestamiseks kasutada ka LDAP-serverit (LDAP-otsingut).

E-post	E-posti sihtkoht. Enne peate seadistama meiliserveri sätteid.
Võrgukaust	Skanniandmete sihtkoht. Võrgukaust tuleb eelnevalt ettevalmistada.

Seotud teave

➔ „Koostöö LDAP-serveri ja kasutajate vahel” lk 60

Kontaktide konfiguratsiooni võrdlus

Skanneri kontaktide configureerimiseks on kolm tööriista: Web Config, Epson Device Admin ja skanneri juhtpaneel. Kolme tööriista erinevused on loetletud allpool toodud tabelis.

Funktsioonid	Web Config*	Epson Device Admin	Skanneri juhtpaneel
Sihtkoha registreerimine	✓	✓	✓
Sihtkoha redigeerimine	✓	✓	✓
Grupi lisamine	✓	✓	✓
Grupi redigeerimine	✓	✓	✓
Sihtkoha või gruppide kustutamine	✓	✓	✓
Kõigi sihtkohtade kustutamine	✓	✓	–
Faili importimine	✓	✓	–
Faili eksportimine	✓	✓	–

* Seadistamiseks logige sisse administraatorina.

Sihtkoha registreerimine kontaktide hulka utiliidi Web Config abil

Märkus.

Saate kontakte registreerida ka skanneri juhtpaneelilt.

1. Avage Web Config ja valige vahekaart **Scan > Contacts**.
2. Valige number, mida soovite registreerida, ja seejärel klõpsake valikut **Edit**.
3. Sisestage **Name** ja **Index Word**.
4. Valige sihtkoha tüüp suvandi **Type** sätteks.

Märkus.

Te ei saa suvandi **Type** sätet pärast registreerimise lõpetamist muuta. Kui tahate muuta tüüpi, kustutage sihtkoht ja seejärel registreerige see uuesti.

5. Sisestage igale üksusele väärtus ja seejärel klõpsake valikut **Apply**.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Sihtkoha sätteüksused

Üksused	Sätted ja selgitused
Üldsätted	
Name	Sisestage kontaktides kuvatav nimi pikkusega kuni 30 tärki vormingus Unicode (UTF-16). Kui te seda ei täpsusta, jätke see tühjaks.
Index Word	Sisestage 30 või vähemast vormingus Unicode (UTF-16) tärgist koosnev nimi, et otsida kontakte skanneri juhtpaneelilt. Kui te seda ei täpsusta, jätke see tühjaks.
Type	Valige registreeritava aadressi tüüp.
Assign to Frequent Use	Valige, kas määrata registreeritud aadress sageli kasutatavaks aadressiks. Kui see määratakse sageli kasutatavaks aadressiks, kuvatakse seda skannimise ülemisel ekraanil ning te saate täpsustada sihtkoha kontakte kuvamata.
Email	
Email Address	Sisestage kombinatsioon pikkusega 1–255 tärki, kasutades täärke „A–Z“, „a–z“ ja „0–9“ ja ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Network Folder (SMB)	
Save to	\\„Kaustatee“ Sisestage asukoht, kus sihtkaust asub, pikkusega 1–253 tärki vormingus Unicode (UTF-16), jättes välja tärgid „\“. Sisestage võrgutee, mis on kuvatud kausta atribuutide aknas. Lisateavet võrgutee seadistamise kohta vt allpool. „Võrgukausta loomine“ lk 46
User Name	Sisestage võrgukaustale juurdepääsuks kasutajanimi pikkusega kuni 30 tärki vormingus Unicode (UTF-16). Vältige aga juhtmärkide kasutamist (0x00–0x1F, 0x7F).
Password	Sisestage võrgukausta avamiseks parool pikkusega 0 kuni 20 tärki vormingus Unicode (UTF-16). Vältige aga juhtmärkide kasutamist (0x00–0x1F, 0x7F).
FTP	
Secure Connection	Olenevalt failiedastusprotokollist, mida FTP-server toetab, valige kas FTP või FTPS. Skanneri turvameetmetega side lubamiseks valige FTPS .
Save to	Sisestage serveri nimi pikkusega 1 kuni 253 tärki vormingus Unicode (UTF-16), jättes välja eesliited „ftp://“ ja „ftps://“.
User Name	Sisestage FTP-serverile juurdepääsuks kasutajanimi pikkusega kuni 30 tärki vormingus Unicode (UTF-16). Vältige aga juhtmärkide kasutamist (0x00–0x1f, 0x7F). Kui server lubab anonüümset ühendamist, sisestage kasutajanimiks näiteks Anonymous või FTP. Kui te seda ei täpsusta, jätke see tühjaks.
Password	Sisestage parool FTP serverisse pääsemiseks pikkusega 0 kuni 20 tärki vormingus Unicode (UTF-16). Vältige aga juhtmärkide kasutamist (0x00–0x1F, 0x7F). Kui te seda ei täpsusta, jätke see tühjaks.
Connection Mode	Valige menüüst ühendusrežiim. Kui skanneri ja FTP-serveri vahel on tulemüür, valige Passive Mode .
Port Number	Sisestage FTP-serveri pordinumber vahemikus 1–65535.

Üksused	Sätted ja selgitused
Certificate Validation	FTP-serveri sertifikaat kinnitatakse, kui see on lubatud. See on saadaval, kui FTPS on valitud suvandi Secure Connection sätteks. Seadistamiseks tuleb skannerisse importida CA Certificate.
SharePoint(WebDAV)*	
Secure Connection	Olenevalt failiedastusprotokollist, mida server toetab, valige kas HTTP või HTTPS. Skanneri turvameetmetega side lubamiseks valige HTTPS .
Save to	Sisestage serveri nimi pikkusega 1 kuni 253 tärgi vormingus Unicode (UTF-16), jättes välja eesliited „http://“ ja „https://“.
User Name	Sisestage serverile juurdepääsuks kasutajanimi pikkusega kuni 30 tärgi vormingus Unicode (UTF-16). Vältige aga juhtmärkide kasutamist (0x00–0x1F, 0x7F). Kui te seda ei täpsusta, jätke see tühjaks.
Password	Sisestage parool serverisse pääsemiseks pikkusega 0 kuni 20 tärgi vormingus Unicode (UTF-16). Vältige aga juhtmärkide kasutamist (0x00–0x1F, 0x7F). Kui te seda ei täpsusta, jätke see tühjaks.
Certificate Validation	Serveri sertifikaat valideeritakse, kui see on lubatud. See on saadaval, kui HTTPS on valitud suvandi Secure Connection sätteks. Seadistamiseks tuleb skannerisse importida CA Certificate.
Proxy Server	Valige, kas puhverserverit kasutatakse või mitte.

* SharePoint Online pole toetatud, kui skannite skanneri juhtpaneelilt võrgukausta.

Kui tahate skannitud kujutise salvestada rakenduses SharePoint Online, kasutage rakendust Document Capture Pro, kui olete installinud rakenduse SharePoint Online Connector. Lugege lisateavet rakenduse Document Capture Pro juhendist.

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

Sihtkohtade registreerimine rühmana Web Config kaudu

Kui sihtkoha tüübiks on määratud **Email**, siis saate registreerida sihtkohti rühmana.

1. Avage Web Config ja valige vahekaart **Scan > Contacts**.
2. Valige number, mida soovite registreerida, ja seejärel klõpsake valikut **Edit**.
3. Valige rühm suvandist **Type**.
4. Klõpsake valikut **Select** suvandi **Contact(s) for Group** jaoks.
Kuvatakse saadaval sihtkohad.
5. Valige sihtkoht, mida soovite registreerida rühma, ja seejärel klõpsake valikut **Select**.
6. Sisestage **Name** ja **Index Word**.
7. Valige, kas registreeritud rühm määratakse sageli kasutatavaks rühmaks.

Märkus.

Sihtkohti saab registreerida mitmesse rühma.

8. Klõpsake nuppu **Apply**.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Kontaktide varundamine ja importimine

Kontakte saate varundada ja importida rakendusega Web Config või muude tööriistadega.

Rakendusega Web Config kontaktide varundamiseks saate eksportida skanneri sätteid, mis sisaldavad kontakte. Eksportitud faili ei ole võimalik redigeerida, sest see eksportitakse kahendfailina.

Kui impordite skannerisse skanneri sätteid, kirjutatakse kontaktid üle.

Rakenduse Epson Device Admin puhul saab kontakte eksportida ainult seadme atribuutide aknast. Lisaks, kui te ei ekspordite turvalisusega seotud üksuseid, saate redigeerida eksportitud kontakte ja neid importida, sest seda saab salvestada SYLK-failina või CSV-failina.

Kontaktide importimine Web Config kaudu

Kui teil on skanner, mis võimaldab kontakte varundada ja on selle skanneriga ühilduv, saate kontakte lihtsalt varufaili importides registreerida.

Märkus.

Skanneri kontaktide varundamise kohta lugege skanneriga kaasas olevast kasutusjuhendist.

Tehke kontaktide importimiseks skannerisse järgmised toimingud.

1. Avage Web Config, valige vahekaart **Device Management** > **Export and Import Setting Value** > **Import**.
2. Valige suvandis **File** loodud varufail, sisestage parool ning klõpsake nuppu **Next**.
3. Valige märkeruut **Contacts** ning seejärel klõpsake **Next**.

Kontaktide varundamine Web Config kaudu

Kontaktide andmed võivad skanneri rikke tõttu kaotsi minna. Soovitame teil andmed värskendamise korral varundada. Epson ei vastuta mingisuguste andmete kadumise, andmete ja/või sätete varundamise ega taastamise eest isegi garantiiajal.

Kasutades rakendust Web Config saate skannerisse salvestatud kontaktandmed arvutis varundada.

1. Avage Web Config ja seejärel valige vahekaart **Device Management** > **Export and Import Setting Value** > **Export**.
2. Valige märkeruut **Contacts** kategooriast **Scan**.
3. Eksportitud faili krüptimiseks sisestage parool.
Faili importimiseks on vajalik parool. Kui te ei taha faili krüptida, jätke see tühjaks.
4. Klõpsake nuppu **Export**.

Kontaktide eksportimine ja hulgiregistreerimine tööriista abil

Kui kasutate tööriista Epson Device Admin, saate varundada üksnes kontakte ja redigeerida eksporditud faile ning neid seejärel kõiki korraga registreerida.

See on kasulik juhul, kui soovite varundada ainult kontakte või vahetate skannerit ja soovite kontaktid vanast skannerist uude üle kanda.

Kontaktide eksportimine

Salvestage kontaktide teave failile.

Te saate redigeerida SYLK- või CSV-vormingus salvestatud faile arvutustabeli rakenduse või tekstiredaktoriga. Te saate registreerida kõik korraga pärast teabe kustutamist või lisamist.

Turvaüksuseid sisaldavat teavet, näiteks parool ja isikuandmed, saab salvestada binaarformaadis parooliga. Faili ei ole võimalik redigeerida. Seda saab kasutada teabe, sealhulgas turvaüksuste, varufailina.

1. Käivitage Epson Device Admin.
2. Valige külgriba tegumimenüüst **Devices**.
3. Valige seadmete loendist seade, mida soovite konfigurereerida.
4. Klõpsake nuppu **Device Configuration** ribamenüü vahekaardil **Home**.
Kui administraatori parool on määratud, sisestage see ja klõpsake suvandil **OK**.
5. Klõpsake nuppu **Common > Contacts**.
6. Valige eksportimise vorming suvandis **Export > Export items**.

All Items

Eksportige krüptitud kahendfail. Valige, millal te soovite lisada turvaüksuseid nagu parool ja isikuandmed. Faili ei ole võimalik redigeerida. Seda valides peate määrama parooli. Klõpsake suvandil **Configuration** ja määrake 8–63 tähemärgi pikkune parool standardkoodis ASCII. Seda parooli vajatakse kahendfaili importimiseks.

Items except Security Information

Eksportige SYLK- või CSV-vormingus failid. Valige, millal te soovite redigeerida eksporditud faili teavet.

7. Klõpsake nuppu **Export**.
8. Määrake koht, kuhu fail salvestatakse, valige faili tüüp ja seejärel klõpsake suvandil **Save**.
Kuvatakse lõpetamise teadet.
9. Klõpsake nuppu **OK**.
Kontrollige, kas fail salvestati määratud kohta.

Kontaktide importimine

Importige faililt kontaktide teave.

Saate importida SYLK- või CSV-vormingus salvestatud faile või turvaüksuseid sisaldavat varundatud kahendfaili.

1. Käivitage Epson Device Admin.
2. Valige külgriba tegumimenüüst **Devices**.
3. Valige seadmete loendist seade, mida soovite konfigurēerida.
4. Klõpsake nuppu **Device Configuration** ribamenüü vahekaardil **Home**.
Kui administraatori parool on määratud, sisestage see ja klõpsake suvandil **OK**.
5. Klõpsake nuppu **Common > Contacts**.
6. Klõpsake nuppu **Browse** suvandis **Import**.
7. Valige importimiseks fail ja klõpsake suvandil **Open**.
Kui valite kahendfaili, sisestage faili eksportimise ajal määratud parool suvandis **Password**.
8. Klõpsake nuppu **Import**.
Kuvatakse kinnitusekraan.
9. Klõpsake nuppu **OK**.
Kuvatakse valideerimistulemus.
 - Edit the information read
Klõpsake, kui soovite seda teavet eraldi redigeerida.
 - Read more file
Klõpsake, kui soovite importida mitut faili.
10. Klõpsake suvandil **Import** ja seejärel klõpsake importimise lõpetamise ekraanil suvandil **OK**.
Naaske seadme atribuutide ekraanile.
11. Klõpsake nuppu **Transmit**.
12. Klõpsake kinnitusteatel **OK**.
Sätted saadetakse skannerisse.
13. Klõpsake saatmise lõpetamise kuval nuppu **OK**.
Skanneri teave värskendatakse.
Avage kontaktid kas rakendusest Web Config või skanneri juhtpaneelilt ja seejärel kontrollige, kas kontakt on värkendatud.

Koostöö LDAP-serveri ja kasutajate vahel

LDAP-serveriga koostööd tehes saate kasutada LDAP-serverisse registreeritud aadressiteavet meiliadressaadina.

LDAP-serveri konfigureerimine

LDAP-serveri teabe kasutamiseks registreerige see skanneris.

1. Avage Web Config ja valige vahekaart **Network > LDAP Server > Basic**.
2. Sisestage iga üksuse jaoks väärtus.
3. Valige **OK**.
Kuvatakse teie valitud sätted.

LDAP-serveri sätteüksused

Üksused	Sätted ja selgitused
Use LDAP Server	Valige Use või Do Not Use .
LDAP Server Address	Sisestage LDAP-serveri aadress. Sisestage 1–255 tärki vormingus IPv4, IPv6 või FQDN. Vormingu FQDN korral võite kasutada tärke vormingus ASCII (0x20–0x7E) ning tärki „-“, välja arvatud aadressi alguses ja lõpus.
LDAP server Port Number	Sisestage LDAP-serveri pordinumber vahemikus 1–65535.
Secure Connection	Valige skanneri autentimismeetod, kui skanner LDAP-serveriga suhtleb.
Certificate Validation	Kui see on lubatud, valideeritakse LDAP-serveri sertifikaat. Soovitame teha sätte Enable . Seadistamiseks peab CA Certificate olema skannerisse imporditud.
Search Timeout (sec)	Määrake aeg otsingu tegemiseks vahemikus 5–300, misjärel esineb ajalõpp.
Authentication Method	Valige üks meetoditest. Kui teete valiku Kerberos Authentication , valige Kerberos Settings > et määrata Kerberose sätted. Kerberos Authentication'i teostamiseks on vajalik järgmine keskkond. <input type="checkbox"/> Skanner ja DNS-server saavad omavahel suhelda. <input type="checkbox"/> Skanneri, KDC-serveri ja autentimiseks vajaliku serveri (LDAP-server, SMTP-server, failiserver) ajad on sünkronitunud. <input type="checkbox"/> Kui teenindusserver on määratud IP-aadressiks, on teenindusserveri FQDN registreeritud DNS-serveri pöördotsingu tsooni.
Kerberos Realm to be Used	Kui teete valiku Kerberos Authentication suvandis Authentication Method , valige Kerberose vald, mida soovite kasutada.
Administrator DN / User Name	Sisestage LDAP-serveri kasutajanimi pikkusega kuni 128 tärki vormingus Unicode (UTF-8). Te ei saa kasutada tärke 0x00–0x1F ja 0x7F. Seda sätet ei kasutata, kui Anonymous Authentication on valitud suvandi Authentication Method sätteks. Kui te seda ei täpsusta, jätke see tühjaks.
Password	Sisestage LDAP-serveris autentimiseks parool pikkusega kuni 128 tärki vormingus Unicode (UTF-8). Te ei saa kasutada tärke 0x00–0x1F ja 0x7F. Seda sätet ei kasutata, kui Anonymous Authentication on valitud suvandi Authentication Method sätteks. Kui te seda ei täpsusta, jätke see tühjaks.

Kerberose sätted

Kui **Kerberos Authentication** on valitud suvandi **Authentication Method** sätteks valikus **LDAP Server > Basic**, määrake alljärgnevat Kerberose sätted vahekaardil **Network > Kerberos Settings**. Kerberose säteteks saate registreerida kuni 10 sätet.

Üksused	Sätted ja selgitused
Realm (Domain)	Sisestage Kerberose autentimise vald pikkusega kuni 255 tärki vormingus ASCII (0x20–0x7E). Kui te seda ei registreeri, jätke see tühjaks.
KDC Address	Sisestage Kerberose autentimisserveri aadress. Sisestage kuni 255 tärki vormingus IPv4, IPv6 või FQDN. Kui te seda ei registreeri, jätke see tühjaks.
Port Number (Kerberos)	Sisestage Kerberose serveri pordinumber vahemikus 1–65535.

LDAP-serveri otsingusätete konfigureerimine

Kui häälestate otsingusätteid, saate kasutada LDAP-serverisse registreeritud meiliaadressi.

1. Avage Web Config ja valige vahekaart **Network > LDAP Server > Search Settings**.
2. Sisestage iga üksuse jaoks väärtus.
3. Sättetulemuse kuvamiseks klõpsake nuppu **OK**.
Kuvatakse teie valitud sätted.

LDAP-serveri otsingu sätteüksused

Üksused	Sätted ja selgitused
Search Base (Distinguished Name)	Kui tahate otsida arbitraarseid domeeni, täpsustage LDAP-serveri domeeni nimi. Sisestage 0–128 tärki vormingus Unicode (UTF-8). Kui te ei otsi arbitraarseid atribuuti, jätke see tühjaks. Näide kohaliku serveri kaustast: dc=server,dc=local
Number of search entries	Täpsustage otsingukirjete arv vahemikus 5–500. Määratud otsingukirjete arv salvestatakse ja seda kuvatakse ajutiselt. Isegi kui otsingukirjete arv on määratud arvust suurem ja kuvatakse tõrketeade, saab otsingu lõpuni viia.
User name Attribute	Täpsustage atribuudi nimi, mida kuvatakse kasutajanimede otsimise korral. Sisestage 1–255 tärki vormingus Unicode (UTF-8). Esimene tärk peab olema „a–z“ või „A–Z“. Näide: cn, uid
User name Display Attribute	Täpsustage atribuudi nimi, mida kuvatakse kasutajanimena. Sisestage 0–255 tärki vormingus Unicode (UTF-8). Esimene tärk peab olema „a–z“ või „A–Z“. Näide: cn, sn
Email Address Attribute	Täpsustage atribuudi nimi, mida kuvatakse meiliaadresside otsimise korral. Sisestage kombinatsioon pikkusega 1–255 tärki, kasutades tärke „A–Z“, „a–z“, „0–9“ ja „-“. Esimene tärk peab olema „a–z“ või „A–Z“. Näide: mail
Arbitrary Attribute 1 - Arbitrary Attribute 4	Võite täpsustada muid arbitraarseid atribuute, mida otsida. Sisestage 0–255 tärki vormingus Unicode (UTF-8). Esimene tärk peab olema „a–z“ või „A–Z“. Kui te ei soovi arbitraarseid atribuute otsida, jätke see tühjaks. Näide: o, ou

LDAP-serveri ühenduse kontrollimine

Teostab LDAP-serveriga ühendamise testi, kasutades suvandites **LDAP Server > Search Settings** määratud parameetrit.

1. Avage Web Config ja valige vahekaart **Network > LDAP Server > Connection Test**.
2. Valige **Start**.

Käivitatakse ühenduse test. Pärast testi kuvatakse kontrolli aruanne.

LDAP-serveri ühenduse testi viited

Teated	Selgitus
Connection test was successful.	See teade kuvatakse, kui ühendus serveriga on loodud.
Connection test failed. Check the settings.	See teade kuvatakse alljärgnevatel põhjustel: <input type="checkbox"/> LDAP-serveri aadress või pordinumber on vale. <input type="checkbox"/> Esinenud on ajalõpp. <input type="checkbox"/> Do Not Use on valitud suvandi Use LDAP Server sätteks. <input type="checkbox"/> Kui Kerberos Authentication on valitud suvandi Authentication Method sätteks, on sellised sätted nagu Realm (Domain) , KDC Address ja Port Number (Kerberos) valed.
Connection test failed. Check the date and time on your product or server.	See teade kuvatakse, kui ühenduse loomine nurjub tulenevalt skanneri ja LDAP-serveri ajasätete lahknevusest.
Authentication failed. Check the settings.	See teade kuvatakse alljärgnevatel põhjustel: <input type="checkbox"/> User Name ja/või Password on vale. <input type="checkbox"/> Kui Kerberos Authentication on valitud suvandi Authentication Method sätteks, ei saa kellaega/kuupäeva konfigureerida.
Cannot access the product until processing is complete.	See teade kuvatakse, kui skanner on hõivatud.

Funktsiooni AirPrint seadistamine

Avage Web Config, valige vahekaart **Network** ja seejärel valige **AirPrint Setup**.

Üksused	Selgitus
Bonjour Service Name	Sisestage Bonjour'i teenusenimi, kasutades kuni 41 tärki koodis ASCII (0x20 kuni 0x7E).
Bonjour Location	Sisestage skanneri asukoha kirjeldus, kasutades kuni 127 baiti teksti koodis Unicode (UTF-8).
Wide-Area Bonjour	Määrake, kas Wide-Area Bonjour on kasutusel või mitte. Kui te seda kasutate, tuleb skanner registreerida DNS-serveris, et skannerit segmendis otsida.

Üksused	Selgitus
Enable AirPrint	Lubab teenused Bonjour ja AirPrint (skanniteenus). See nupp on saadaval ainult siis, kui AirPrint on keelatud. Märkus. <i>Kui AirPrint on keelatud, keelatakse ka Mopria skannimine Chromebookist, Windowsist ja rakendusest Mopria Scan.</i>

Probleemid võrguskannimise ettevalmistamisega

Nõuandeid probleemide lahendamiseks

Veateate kontrollimine

Törke ilmumise korral kontrollige esmalt, kas skanneri juhtpaneelil või draiverikuval on teateid. Kui olete määranud sündmuste ilmumise korral teavitusemeili saamise, saate selle oleku kiiresti teada.

Andmeside oleku kontrollimine

Kontrollige serveri- või klientarvuti andmeside olekut, kasutades käsklust nagu ping ja ipconfig.

Ühendustest

Skanneri ja meiliserveri vahelise ühenduse kontrollimiseks tehke skanneris ühendustest. Lisaks kontrollige klientarvuti ja serveri vahelist ühendust, et kontrollida andmeside olekut.

Sätete käivitamine

Kui sätted ja andmeside olek ühtegi probleemi ei näita, võib probleemide lahendamiseks piisata skanneri võrgusätete inaktiveerimisest või lähtestamisest ja nende uuesti häälestamisest.

Utiliiti Web Config ei õnnestu avada

IP-aadressi ei ole skannerile määratud.

Lahendused

Kehtiv IP-aadress võib olla skannerile määramata. Konfigureerige IP-aadress skanneri juhtpaneelilt. Te saate kehtivaid sätteid kontrollida skanneri juhtpaneelilt.

Veebibrauser ei toeta SSL/TLS-i krüptimistugevust.

Lahendused

SSL/TLS-il on Encryption Strength. Saate utiliidi Web Config avada, kasutades veebibrauserit, mis toetab allpool toodud hulgikrüptimisi. Kontrollige, kas kasutate toetatud brauserit.

80 bitti: AES256/AES128/3DES

112 bitti: AES256/AES128/3DES

128 bitti: AES256/AES128

192 bitti: AES256

256 bitti: AES256

CA-signed Certificate on aegunud.

Lahendused

Kui esineb probleeme sertifikaadi aegumisega, kuvatakse SSL/TLS-ühenduse (https) loomisel utiliidiga Web Config teade „Sertifikaat on aegunud”. Kui teade kuvatakse enne sertifikaadi aegumiskuupäeva, kontrollige, kas skanneri kuupäev on õigesti konfigureeritud.

Sertifikaadi ja skanneri pärisnimi ei ühti.

Lahendused

Kui sertifikaadi pärisnimi ja skanner ei ühti, kuvatakse SSL/TLS-ühenduse (https) loomisel utiliidiga Web Config teade „Turvasertifikaadi nimi ei ühti...”. See juhtub, kuna järgmised IP-aadressid ei ühti.

- Skanneri IP-aadress, mis sisestati pärisnime väljale, et luua Self-signed Certificate või CSR
- Utiliidi Web Config käivitamisel veebibrauserisse sisestatud IP-aadress

Sertifikaadi Self-signed Certificate jaoks tuleb sertifikaati värskendada.

Sertifikaadi CA-signed Certificate jaoks võtke skannerile sertifikaat uuesti.

Veebibrauseris on seadistamata kohaliku aadressi puhverserver.

Lahendused

Kui skanner on seadistatud kasutama puhverserverit, konfigureerige veebibrauser nii, et see ei looks puhverserveri kaudu ühendust kohaliku aadressiga.

- Windows:

Valige **Juhtpaneel > Võrk ja Internet > Interneti-suvandid > Ühendused > Kohtvõrgu sätted > Puhverserver** ja seejärel konfigureerige kohtvõrgu puhverserveri mittekasutamine (kohalikud aadressid).

- Mac OS:

Valige **Süsteemieelistused (või Süsteemi sätted) > Võrk > Täpsem > Puhvrid** ja seejärel registreerige kohalik aadress suvandis **Ära kasuta puhvisätteid nende hostide ja domeenide jaoks**.

Näide:

192.168.1.*: Kohalik aadress 192.168.1.XXX, alamvõrgumask 255.255.255.0

192,168.*.*:Kohalik aadress 192.168.XXX.XXX, alamvõrgumask 255.255.0.0

DHCP on arvuti sätetes keelatud.

Lahendused

Kui DHCP IP-aadressi automaatseks hankimiseks on arvutis keelatud, ei saa rakendust Web Config avada. Lubage DHCP.

Näide operatsioonisüsteemis Windows 10.

Avage juhtpaneel ja klõpsake seejärel nuppu **Võrk ja Internet > Võrgu- ja ühiskasutuskeskus > Muuda adapteri sätteid**. Avage kasutatava ühenduse atribuutide aken ja seejärel **Internet Protocoli versiooni 4 (TCP/IPv4)** või **Internet Protocoli versiooni 6 (TCP/IPv6)** atribuudid. Veenduge, et kuvatud aknas oleks valitud **Hangi IP-aadress automaatselt**.


Juhtpaneeli ekraani kohandamine

Registreerimine: Eelsätted.	67
Juhtpaneeli avakuva redigeerimine.	69

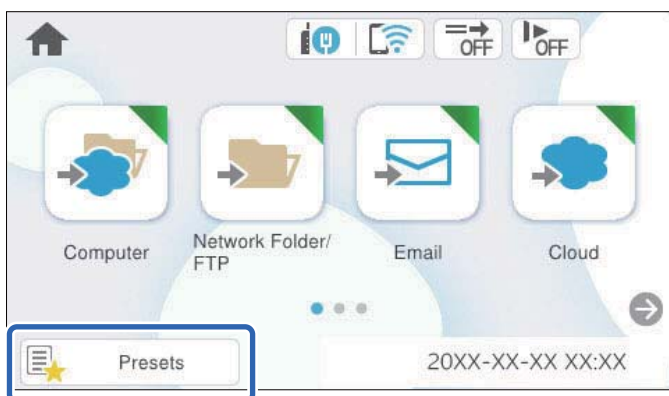
Registreerimine: Eelsätted

Sageli kasutatavad skannimissätted on võimalik salvestada loendisse **Eelsätted**. Registreerida saab kuni 48 eelsätet.

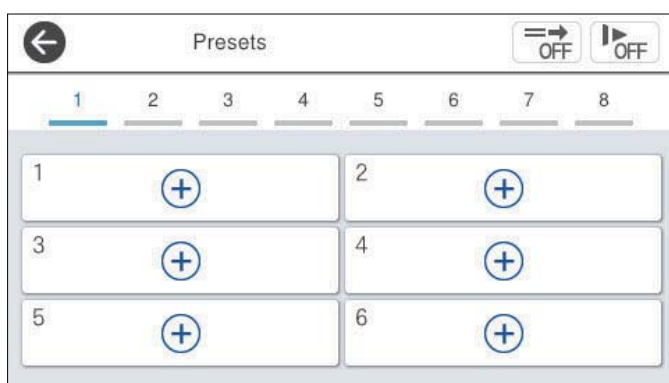
Märkus.

- Kehtivate sätete registreerimiseks valige skannimise käivitamise kuval .
- Samuti on loendisse **Presets** registreerimine võimalik rakenduses *Web Config*.
Valige vahekaart **Scan** > **Presets**.
- Kui valite registreerimisel sätte **Skanni arvutisse**, saate registreerida rakenduses *Document Capture Pro* loodud töö suvandis **Presets**. See on saadaval ainult võrgu kaudu ühendatud arvutites. Registreerige eelnevalt töö rakenduses *Document Capture Pro*.
- Kui autentimisfunktsioon on aktiveeritud, on suvandis **Presets** registreerimine saadaval ainult administraatorile.

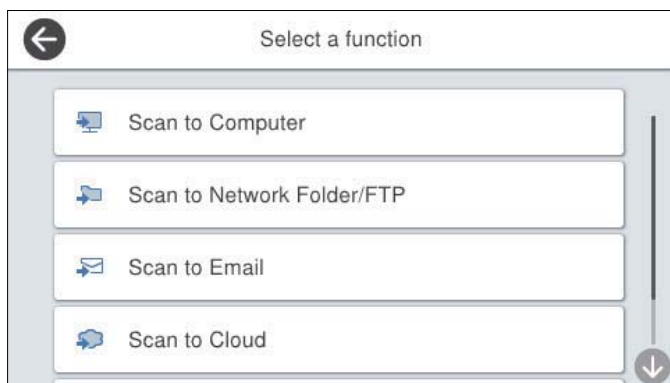
1. Valige skanneri juhtpaneeli avakuval **Eelsätted**.




2. Valige .



3. Valige menüü, mida soovite eelsätte registreerimiseks kasutada.



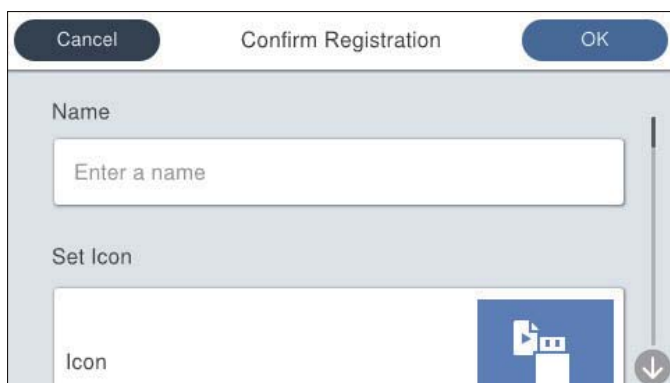
4. Seadistage kõik üksused ja seejärel valige .

Märkus.

Kui teete valiku **Skanni arvutisse**, valige arvuti, kuhu on installitud Document Capture Pro, ja valige siis registreeritud töö. See on saadaval ainult võrgu kaudu ühendatud arvutites.


5. Määrake eelsätte sätted.

- Nimi:** määrake nimi.
- Ikooni seadmine:** valige kuvatava ikooni pilt ja värv.
- Kiirsaatmise sätted:** käivitab eelsätte valimise korral kohe skannimise, ilma et oleks vaja kinnitada.
- Sisukord:** kontrollige skannimissätteid.



6. Valige OK.

Menüüsuvandid: Eelsätted

Eelsätte sätteid saate muuta, tehes eelsättes valiku  .

Nime muutmise:

muudab eelsätte nime.

Ikooni muutmise:

muudab eelsätte ikooni pilti ja värvi.

Kiirsaatmise sätted:

käivitab eelsätte valimise korral kohe skannimise, ilma et oleks vaja kinnitada.

Muuda asendit:

muudab eelsätete kuvajärjekorda.

Kustuta:

kustutab eelsätte.

Ikooni lisamine Avalehele või sellelt eemaldamine:

lisab eelsätte ikooni avakuvale või kustutab selle avakuvalt.

Kinnitage Üksikasjad:

eelsätte sätete vaatamiseks. Eelsätte laadimiseks valige **Kasuta seda sätet**.

Juhtpaneeli avakuva redigeerimine

Avakuva kohandamiseks valige skanneri juhtpaneelil **Sätted** > **Muuda avakuva**.

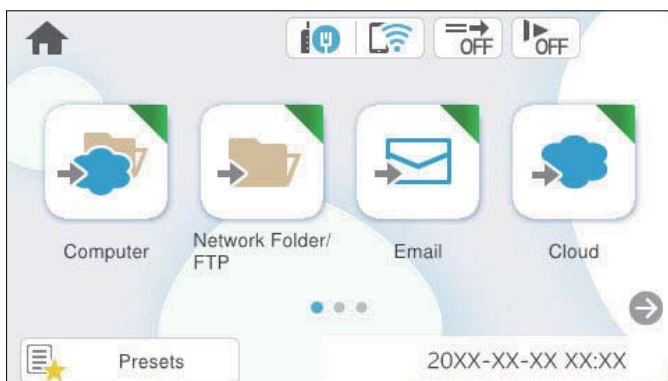
- Paigutus: muudab menüüikoonide kuvameetodit.
[„Avakuva Paigutusi muutmine” lk 69](#)
- Lisa ikoon: lisab ikooni teie tehtud suvandi **Eelsätted** sätete jaoks või taastab ikoonid, mis on kuvalt eemaldatud.
[„Lisa ikoon” lk 70](#)
- Eemalda ikoon: eemaldab ikooni avakuvalt.
[„Eemalda ikoon” lk 71](#)
- Teisalda ikoon: muudab ikoonide kuvajärjekorda.
[„Teisalda ikoon” lk 72](#)
- Taasta vaikimisi ikoonid: taastab avakuva kuvasätete vaikesätteid.

Avakuva Paigutusi muutmine

1. Valige skanneri juhtpaneelil **Sätted** > **Muuda avakuva** > **Paigutus**.


2. Valige **Rida** või **Maatriks**.

Rida:



Maatriks:



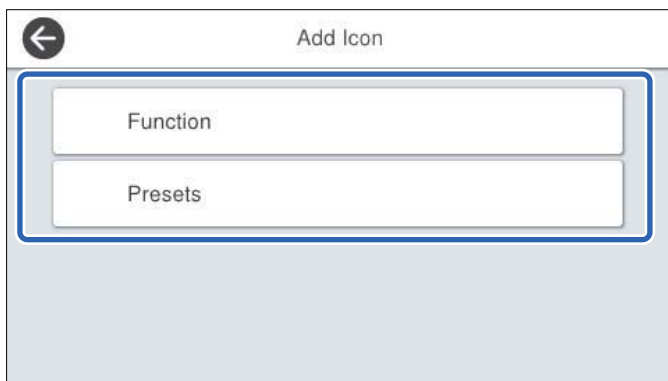
3. Naasmiseks ja avakuva ülevaatamiseks valige .

Lisa ikoon

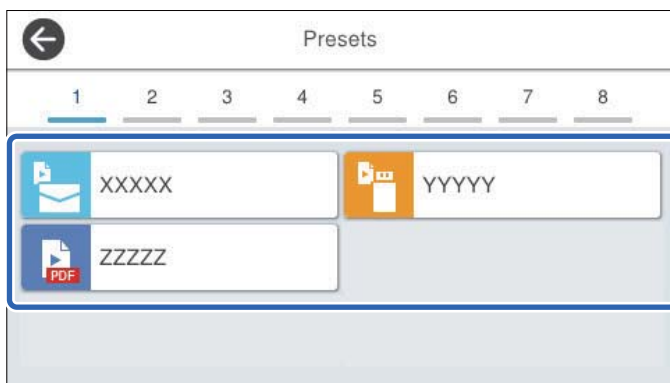
1. Valige skanneri juhtpaneelil **Sätted** > **Muuda avakuva** > **Lisa ikoon**.

2. Valige **Funktsioon** või **Eelsätted**.

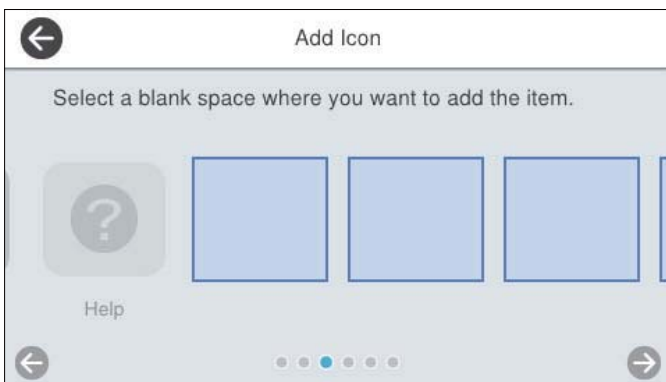
- Funktsioon: kuvab avakuval näidatud vaikefunktsioonid.
- Eelsätted: kuvab registreeritud eelsätted.




3. Valige üksus, mille soovite lisada avakuvale.



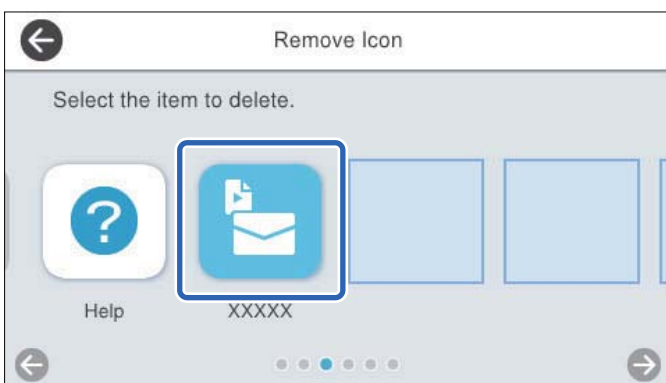
4. Valige tühi koht, kuhu soovite üksuse lisada.
Kui soovite lisada mitu ikooni, korrake toiminguid 3 kuni 4.



5. Naasmiseks ja avakuva ülevaatomiseks valige .


Eemalda ikoon

1. Valige skanneri juhtpaneelil **Sätted** > **Muuda avakuva** > **Eemalda ikoon**.
2. Valige ikoon, mida soovite eemaldada.



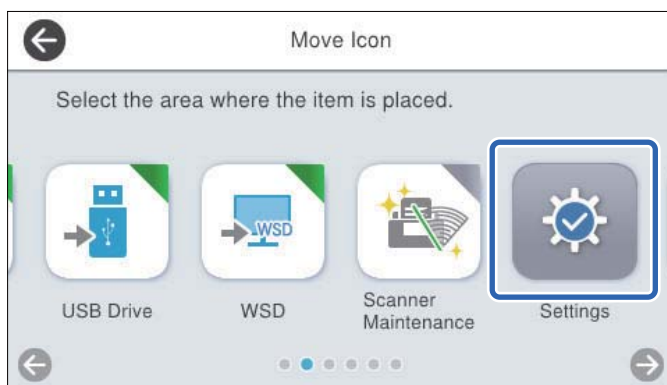
3. Lõpetamiseks valige **Jah**.

Kui soovite eemaldada mitu ikooni, korrake toiminguid 2 kuni 3.

4. Naasmiseks ja avakuva ülevaatamiseks valige .

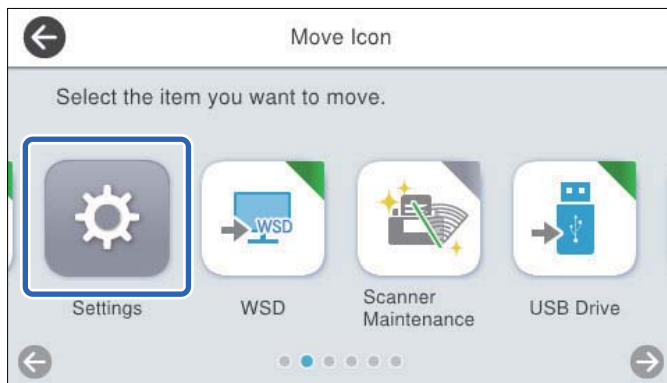
Teisalda ikoon


1. Valige skanneri juhtpaneelil **Sätted** > **Muuda avakuva** > **Teisalda ikoon**.
2. Valige ikoon, mida soovite teisaldada.



3. Valige sihtraam.

Kui sihtraamis on juba teine ikoon, asendatakse see.



4. Naasmiseks ja avakuva ülevaatamiseks valige .

Põhilised turvasätted

Toote turvalisuse funktsioonide juhend.	74
Administraatori sätted.	74
Saadaval funktsioonide piiramine (Juurdepääsu haldamine).	80
Välise liidese keelamine.	82
Programmikinnituse lubamine käivitamisel.	82
Võrgust skannimise keelamine arvutist.	83
WSD-skannimise lubamine ja keelamine.	83
Kaugskanneri jälgimine.	84
Vaikesätete taastamine.	85
Teenuse Epson Remote Services teave.	86
Probleemide lahendamine.	86

Toote turvalisuse funktsioonide juhend

Selles jaotises tutvustatakse Epsoni seadmete turvalisuse funktsioone.

Funktsiooni nimi	Funktsiooni tüüp	Mida seadistada	Mida vältida
Seadistage administraatori parool	Lukustab süsteemi sätteid, näiteks ühenduse seadistuse võrgule või USB-le.	Seadme parooli määrab administraator. Määramine ja muutmine on võimalik rakenduses Web Config või skanneri juhtpaneelil.	Takistab seadmes hoitavate andmete, näiteks ID, parooli, võrgusätete jne õigusvastast lugemist ja muutmist. Lisaks vähendab see erinevaid turvariske nagu näiteks andmete lekkimine võrgukeskkonna või turvalisuse poliitika kohta.
Access Control Settings	Seadme kasutamiseks tuleb seadmesse sisse logida varem registreeritud kasutajakontoga.	Registreerige ükskõik milline kasutajakonto. Saate registreerida kuni 10 kasutajakontot.	Kasutajate piiramine hoiab ära seadme volitamata kasutamise.
Välisliidese seadistus	Kontrollib seadmega ühendamise liidest.	Lubage või keelake arvuti USB-ühendus.	Arvuti USB-ühendus: takistab seadme lubamatut kasutamist, keelates võrguta skannimise.

Seotud teave

- ➔ „Seadistage administraatori parool” lk 74
- ➔ „Välise liidese keelamine” lk 82

Administraatori sätted

Seadistage administraatori parool

Administraatori parooli määrates saate takistada süsteemihalduse sätete muutmist kasutajate poolt. Ostu ajal on määratud vaikeväärtused. Muutke neid vajaduse järgi.

Märkus.

Allpool on toodud rakenduse administraatori teabe vaikeväärtused.

- Kasutajanimi (kasutatakse ainult rakenduses Web Config): puudub (tühi)
- Parool: oleneb tootele kinnitatud sildist.

Kui tagaküljele on kinnitatud silt „PASSWORD“, sisestage sildil olev 8-kohaline number. Kui silti „PASSWORD“ ei ole, sisestage administraatori paroolina toote tagaküljel oleval sildil toodud seerianumber.

Administraatori parooli saate muuta kas rakenduses Web Config, skanneri juhtpaneelil või rakenduses Epson Device Admin. Kui kasutate rakendust Epson Device Admin lugege rakenduse Epson Device Admin juhendit või spikrit.

Administraatori parooli muutmise rakenduses Web Config

Muutke administraatori parooli rakenduses Web Config.

1. Avage Web Config ja valige vahekaart **Product Security > Change Administrator Password**.
2. Sisestage vajalik teave väljadele **Current password**, **User Name**, **New Password** ja **Confirm New Password**.

Uus parool peab olema 8 kuni 20 tärki pikk ja sisaldama ainult ühebaidiseid tärke.

Märkus.

Allpool on toodud rakenduse administraatori teabe vaikeväärtused.

Kasutajanimi: puudub (tühi)

Parool: oleneb tootele kinnitatud sildist.

Kui tagaküljele on kinnitatud silt „PASSWORD“, sisestage sildil olev 8-kohaline number. Kui silti „PASSWORD“ ei ole, sisestage administraatori paroolina toote tagaküljel oleval sildil toodud seerianumber.



Oluline teave:

Jätke määratud administraatori parool kindlasti meelde. Kui te parooli unustate, ei saa te seda lähtestada ja peate abi paluma teeninduspersonalilt.

3. Valige **OK**.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config“ lk 37](#)

Administraatori parooli muutmise skanneri juhtpaneelilt

Administraatori parooli saab muuta skanneri juhtpaneelil.

1. Valige skanneri juhtpaneelil **Sätted**.
2. Valige **Süsteemi administreerimine > Administraatori sätted**.
3. Valige **Administraatori parool > Muuda**.
4. Sisestage kehtiv parool.

Märkus.

Ostu ajal määratud algne administraatori parool (vaikesäte) erineb olenevalt tootele kinnitatud sildist. Kui tagaküljele on kinnitatud silt „PASSWORD“, sisestage sildil olev 8-kohaline number. Kui silti „PASSWORD“ ei ole, sisestage administraatori paroolina toote tagaküljel oleval sildil toodud seerianumber.

5. Sisestage uus parool.

Uus parool peab olema 8 kuni 20 tärki pikk ja sisaldama ainult ühebaidiseid tärke.



Oluline teave:

Jätke määratud administraatori parool kindlasti meelde. Kui te parooli unustate, ei saa te seda lähtestada ja peate abi paluma teeninduspersonalilt.


6. Sisestage uus parool kinnitamiseks uuesti.


Kuvatakse lõpetamise teade.

Funktsiooni Lukustamise sätted kasutamine juhtpaneelil

Te võite juhtpaneeli lukustamiseks kasutada funktsiooni Lukustamise sätted, et kasutajad ei saaks muuta süsteemi sätteid.

Funktsiooni Lukustamise sätted seadistamine juhtpaneelil

1. Kui soovite funktsiooni **Lukustamise sätted** pärast selle lubamist tühistada, puudutage avakuval üleval paremas nurgas ikooni , et administraatorina sisse logida.

 pole kuvatud, kui **Lukustamise sätted** on keelatud. Kui soovite selle sätte lubada, minge järgmise sammu juurde.

2. Valige **Sätted**.

3. Valige **Süsteemi administreerimine** > **Administraatori sätted**.

4. Valige **Sees** või **Välj.** suvandi **Lukustamise sätted** sätteks.

Funktsiooni Lukustamise sätted seadistamine rakenduses Web Config

1. Valige vahekaart **Device Management** > **Control Panel**.

2. Valige suvandi **ON** sätteks **OFF** või **Panel Lock**.

3. Klõpsake nuppu **OK**.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)

Funktsiooni Lukustamise sätted üksused menüüs Sätted

See on loend üksustest, mis juhtpaneeli menüüs **Sätted** funktsiooniga Lukustamise sätted lukustatakse.


✓: lukustatakse.

-: ei lukustata.

Menüü Sätted	Lukustamise sätted
Põhisätted	-

Menüü Sätted		Lukustamise sätted
	LCD heledus	-
	Heli	-
	Unetaimer	✓
	Väljalülitustaimer	✓
	Võrgutoide	✓
	Kuupäeva/kellaaja sätted	✓
	Keel/Language	✓/-*
	Klaviatuur (See funktsioon ei pruugi olenevalt teie asukohast saadaaval olla.)	-
	Toimingu aegumine	✓
	Avuti ühendamine USB kaudu	✓
Skanneri sätted		-
	Aeglane	-
	Topeltsöödu seiskamisaeg	✓
	DFDS-funktsioon	-
	Paberi kaitse	✓
	Klaasi määrdumise tuvastus	✓
	Kahe lehe söötmise ultraheliandur	✓
	Automaatse söötmissrežiimi ajalõpp	✓
	Kinnitage adressaat	✓
Muuda avakuva		✓
	Paigutus	✓
	Lisa ikoon	✓
	Eemalda ikoon	✓
	Teisalda ikoon	✓
	Taasta vaikimisi ikoonid	✓
Kasutaja sätted		✓
	Võrgukaust/FTP	✓
	Meil	✓
	Pilv	✓
	USB-draiv	✓


Menüü Sätted		Lukustamise sätted
Võrgusätted		✓
	Wi-Fi häälestus	✓
	Kaabel-LAN-i häälestus	✓
	Võrgu olek	✓
	Täpsem	✓
Veebiteenuse sätted		✓
	Epson Connect teenused	✓
Document Capture Pro		-
	Muuda sätteid	✓
Kontaktide haldur		-
	Registreeri/Kustuta	✓/!*
	Sagedased	-
	Kuva suvandid	-
	Otsingusuvandid	-
Süsteemi administreerimine		✓
	Kontaktide haldur	✓
	Administraatori sätted	✓
	Piirangud	✓
	Juurdepääsu haldamine	✓
	Paroolide krüptimine	✓
	Kliendiuring	✓
	WSD sätted	✓
	Taasta vaikesätted	✓
	Püsivara värskendamine	✓
Seadme info		-



Menüü Sätted		Lukustamise sätted
	Seerianumber	-
	Praegune versioon	-
	Skannimiste koguarv	-
	1-poolsete skannimiste arv	-
	2-poolsete skannimiste arv	-
	Kandja Lehe skannimiste arv	-
	Skannitud eksemplaride arv pärast rulliku vahetamist	-
	Skannitud eksemplare pärast tavalist puhastamist	-
	Autentimisseadme olek	-
	Teave rakenduse Epson Open Platform kohta	-
	 (Lähtesta skannimiste arv)	✓
Skanneri hooldus		-
	Rulliku puhastamine	-
	Rulliku asendamine	-
	Lähtesta skannimiste arv	✓
	Kuidas vahetada	-
	Tavaline puhastamine	-
	Lähtesta skannimiste arv	✓
	Kuidas puhastada?	-
	Klaasi puhastamine	-
Rulli vahetamise märguande säte		✓
	Loenduri märguanne	✓
Regulaarse puhastuse märguande sätted		✓
	Hoaitusmärguande sätted	✓
	Loenduri märguanne	✓

* Saate määrata, kas muudatuste tegemine menüüs **Süsteemi administreerimine > Piirangud** on lubatud.

Juhtpaneelilt administraatorina sisselogimine

Kui **Lukustamise sätted** on lubatud, saate skanneri juhtpaneelilt sisselogimiseks kasutada ükskõik millist järgmistest meetoditest.

1. Puudutage ekraanil üleval paremas nurgas ikooni .
2. Kui avaneb kuva **Valige kasutaja**, valige **Administraator**.
3. Sisestage sisselogimiseks parool.
Kuvatakse sisselogimise teade ja seejärel kuvatakse juhtpaneelil avakuva.

Väljalogimiseks puudutage nuppu  ekraani ülemises paremas nurgas või vajutage nuppu .

Saadaval funktsioonide piiramine (Juurdepääsu haldamine)

Skanneris kasutajakontosid registreerides saab kasutajaid piirata.

Kui Juurdepääsu haldamine on lubatud, peab kasutaja skannifunktsioonide kasutamiseks sisestama skanneri juhtpaneelil parooli ja sisse logima. Sisselogimiseta ei saa skannida.

Arvutist skannimiseks tuleb registreerida Kasutajanimi ja Parool skanneridraiveris (Epson Scan 2). Lugege lisateavet sätete kohta rakenduse Epson Scan 2 spikrist või toote dokumendist *Kasutusjuhend*.

Kasutajakonto loomine

Saate luua konto funktsiooniga Juurdepääsu haldamine.

1. Avage Web Config, seejärel valige vahekaart **Product Security** > **Access Control Settings** > **User Settings**.
2. Klõpsake nuppu **Add** numbri jaoks, mida registreerida soovite.



Oluline teave:

Kui kasutate skannerit Epsoni või muu ettevõtte autentimissüsteemiga, registreerige User Name suvandis Access Control Settings kohal number 2 kuni 10.

Rakendustarkvara, näiteks autentimissüsteem, kasutab kohta number 1, seega ei kuvata kasutajanime skanneri juhtpaneelil.

3. Seadistage kõik üksused.
 - User Name.
Sisestage kasutajanimede loendis kuvatud nimi, mis on 1 kuni 14 tärki pikk.
 - Password.
Sisestage parool pikkusega 0 kuni 20 tärki ASCII-vormingus (0x20–0x7E). Parooli lähtestamisel jätke see tühjaks.
 - Select the check box to enable or disable each function.
Kui soovite lubada skannimise funktsioonid, valige **Scan**.
4. Klõpsake nuppu **Apply**.

Kasutajakonto redigeerimine

Funktsiooniga Juurdepääsu haldamine registreeritud kontot saab redigeerida.

1. Avage Web Config, seejärel valige vahekaart **Product Security** > **Access Control Settings** > **User Settings**.
2. Klõpsake redigeeritava numbri jaoks nuppu **Edit**.
3. Muutke iga üksust.
4. Klõpsake nuppu **Apply**.

Kasutajakonto kustutamine

Funktsiooniga Juurdepääsu haldamine registreeritud konto saab kustutada.

1. Avage Web Config, seejärel valige vahekaart **Product Security** > **Access Control Settings** > **User Settings**.
2. Klõpsake kustutatava numbri jaoks nuppu **Edit**.
3. Klõpsake nuppu **Delete**.



Oluline teave:

Kui klõpsate käsku **Delete**, kustutatakse kasutajakonto kinnitussõnumit kuvamata. Olge konto kustutamisel ettevaatlik.

Suvandi Juurdepääsu haldamine lubamine

Funktsiooni Juurdepääsu haldamine lubamise korral saab printerit kasutada ainult registreeritud kasutaja.


Märkus.

Kui **Access Control Settings** on lubatud, peate kasutajat tema konto teabest teavitama.

1. Avage Web Config, seejärel valige vahekaart **Product Security** > **Access Control Settings** > **Basic**.
2. Valige **Enables Access Control**.
Kui lubate funktsiooni **Access Control Settings** ja skannite autentimisteabeta arvutist, valige **Allow printing and scanning without authentication information from a computer**.
3. Klõpsake nuppu **OK**.



Logimine skannerisse, kui lubatud on Juurdepääsu haldamine

Kui **Juurdepääsu haldamine** on lubatud, saate skanneri juhtpaneelilt sisselogimiseks kasutada ükskõik millist järgmistest meetoditest.

1. Puudutage ekraanil üleval paremas nurgas ikooni .
2. Valige kasutaja, kui avatud on kuva **Valige kasutaja**.

3. Sisestage sisselogimiseks parool.

Kuvatakse sisselogimise teade ja seejärel kuvatakse juhtpaneelil avakuva.

Väljalogimiseks puudutage nuppu  ekraani ülemises paremas nurgas või vajutage nuppu .

Välise liidese keelamine

Saate keelata liidese, mida kasutatakse seadme ühendamiseks skanneriga. Määrake keelavad sätted, et skannimine oleks lubatud vaid võrgu kaudu.

Märkus.

Piiravad sätted saate määrata ka skanneri juhtpaneelilt.

Avuti ühendamine USB kaudu: **Sätted** > **Põhisätted** > **Avuti ühendamine USB kaudu**

1. Avage Web Config ja valige vahekaart **Product Security** > **External Interface**.

2. Valige **Disable** funktsioonidele, mida soovite määrata.

Valige **Enable**, kui soovite kontrollimise katkestada.

Avuti ühendamine USB kaudu

Teil on võimalik USB-ühenduse kasutust arvuti kaudu piirata. Kui soovite seda piirata, vajutage nuppu **Disable**.

3. Klõpsake nuppu **OK**.

4. Kontrollige, kas keelatud porti ei ole võimalik kasutada.

Avuti ühendamine USB kaudu

Kui draiver on arvutisse installitud

Ühendage skanner USB-kaabli abil arvutiga ning kontrollige, et skanner ei skanniks.

Kui draiverit pole arvutisse installitud

Windows:

Avage seadmehaldur ja jätke see tööle. Ühendage skanner USB-kaabli abil arvutiga ja veenduge, et seadmehalduri kuvasisu ei muutuks.

Mac OS:

Ühendage skanner USB-kaabli abil arvutiga ning kontrollige, et skannerit ei saaks lisada jaotisest **Printerid & Skannerid**.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)

Programmikinnituse lubamine käivitamisel

Kui lubate programmi kinnitamise funktsiooni, kontrollib skanner käivitamisel, kas volitamata kolmandad isikud on programmi rikkunud. Kui tuvastatakse probleeme, ei lähe skanner tööle.

Märkus.

Selle funktsiooni lubamine pikendab skanneri käivitamise aega.

1. Avage Web Config ja valige seejärel vahekaart **Product Security** > **Program Verification on Start Up**.

Märkus.

Seadistamine on võimalik ka skanneri juhtpaneelilt.

Sätted > **Süsteemi administreerimine** > **Programmikontroll käivitamise ajal**

2. Valige **ON**, et funktsioon **Program Verification on Start Up** lubada.
3. Klõpsake nuppu **OK**.

Võrgust skannimise keelamine arvutist

Arvutist saab rakenduses Web Config võrgust skannimise keelamiseks rakenduses Epson Scan 2 määrata järgmised sätted.

1. Avage Web Config ja valige seejärel vahekaart **Scan** > **Network Scan**.
2. Tühjendage rakenduses **Epson Scan 2** märkeruut **Enable scanning**.
3. Klõpsake nuppu **Next**.
Avaneb sätte kinnituskuva.
4. Klõpsake nuppu **OK**.

WSD-skannimise lubamine ja keelamine

Märkus.

Seadistamine on võimalik ka skanneri juhtpaneelilt. Valige **Sätted** > **Süsteemi administreerimine** > **WSD sätted**.

Saate funktsiooni WSD lubada või keelata.

Kui te ei taha, et arvuti konfigureeriks skanneri WSD-skanniseadmena, keelake WSD sätted.

1. Avage Web Config ja valige seejärel vahekaart **Network Security** > **Protocol**.
2. Eemaldage suvandis **WSD Settings** valik märkeruudust **Enable WSD**.
3. Klõpsake nuppu **Next**.
Avaneb sätte kinnituskuva.
4. Klõpsake nuppu **OK**.

Märkus.

Kui teie arvuti konfigureerib endiselt skannerit WSD-skanniseadmena, valige vahekaart **Scan** > **Network Scan** ja eemaldage valik märkeruudust **Enable scanning** jaotises **AirPrint**.

Kui AirPrint on keelatud, keelatakse ka Mopria skannimine Chromebookist, Windowsist ja rakendusest Mopria Scan.

Kaugskanneri jälgimine

Kaugskanneri teabe vaatamine

Töötava skanneri kohta saate suvandist **Status** rakenduses Web Config vaadata alljärgnevat teavet.

- Product Status
Vaadake olekut, pilveteenust, tootenumbrit, MAC-aadressi jne.
- Network Status
Vaadake võrguühenduse olekut, IP-aadressi, DNS-serverit jne.
- Usage Status
Vaadake esimest skannimise kuupäeva, skannimiste arvu jne.
- Hardware Status
Vaadake skanneri iga funktsiooni olekut.
- Panel Snapshot
Kuvab skanneri juhtpaneeli kuva hetktõmmise.

Meiliteavituste saamine sündmuste toimumisel

Teave meiliteatiste kohta

See on teavitusfunktsioon, mis saadab määratud aadressile meili, kui ilmnevad sündmused nagu skannimise peatumine ja skanneri tõrge.

Saate registreerida kuni viis sihtkohta ja määrata iga sihtkoha jaoks teavitamise sätte.

Selle funktsiooni kasutamiseks peate enne teavituste määramist üles seadma meiliserveri.

Seotud teave

➔ [„Meiliserveri registreerimine” lk 44](#)

Meiliteadete konfigureerimine

Seadistage meiliteated Web Config kaudu.

1. Avage Web Config ja valige vahekaart **Device Management > Email Notification**.
2. Määrake meiliteate teema.
Valige teemareal kuvatav sisu kahe rippmenüü abil.
 - Valitud sisu kuvatakse **Subject** kõrval.
 - Vasakule ja paremale ei saa valida sama sisu.
 - Kui **Location** tähemärkide maht on üle 32 baidi, siis jäetakse mahtu ületavad tähemärgid välja.

3. Sisestage meiliteate saatmise e-posti aadress.

Kasutage A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @ ja sisestage 1 kuni 255 tähemärki.

4. Valige meiliteadete keel.

5. Märgistage märkeruudud sündmuste juures mille puhul soovite meiliteateid.

Notification Settings arv on seotud **Email Address Settings** sihtkoha arvuga.

Näide:

Kui soovite administraatori parooli muutmise korral saata teatist meiliaadressile, mis on seotud numbri 1 alla suvandis **Email Address Settings**, valige tulba **1** märkeruut real **Administrator password changed**.

6. Klõpsake nuppu **OK**.

Meiliteavituse töö kontrollimiseks põhjustage asjakohane sündmus.

Näide. Administraatori parool on muudetud.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)

Meiliteadete üksused

Üksused	Sätted ja selgitused
Administrator password changed	Teade, kui muudetakse administraatori parooli.
Scanner error	Teade skanneri tõrgete korral.
Wi-Fi rike	Teade juhtmevaba LAN-liidese tõrke korral.

Skanneri toiteallika juhtimine rakenduses Web Config

Kui teie arvuti on skannerist eemal, saate rakendusega Web Config ikkagi skannerit välja lülitada ja taaskäivitada.

1. Avage Web Config ja valige seejärel vahekaart **Device Management** > **Power**.
2. Valige **Power Off** või **Reboot**.
3. Klõpsake nuppu **Execute**.

Vaikesätete taastamine

Saate valida skanneris salvestatud võrgusätted või muud sätted ja taastada nende vaikeväärtused.

1. Avage Web Config ja valige seejärel vahekaart **Device Management** > **Restore Default Settings**.

Märkus.

Seadistamine on võimalik ka skanneri juhtpaneelilt.

Sätted > **Süsteemi administreerimine** > **Taasta vaikesätted**

2. Valige üksused, mida soovite taastada.
3. Klõpsake nuppu **Execute**.
Järgige lõpetamiseks ekraanil kuvatud juhtnööre.

Teenuse Epson Remote Services teave

Epson Remote Services on teenus, mis kogub regulaarselt interneti kaudu printeri kohta teavet. Seda võib kasutada prognoosimaks, millal on tarvis kulutarvikuid või kuluvaid osi vahetada või täita, või tõrgete ja probleemide lahendamiseks.

Lisateabe saamiseks teenuse Epson Remote Services kohta võtke ühendust oma edasimüüjaga.

Probleemide lahendamine

Administraatori parool on ununenud

Vajate hooldustöötajate abi. Võtke ühendust kohaliku edasimüüjaga.

Märkus.

Allpool on toodud rakenduse Web Config administraatori algväärtused.

Kasutajanimi: puudub (tühi)

Parool: oleneb tootele kinnitatud sildist.

Kui tagaküljele on kinnitatud silt „PASSWORD“, sisestage sildil olev 8-kohaline number.

Kui silti „PASSWORD“ ei ole, sisestage administraatori paroolina toote tagaküljel oleval sildil toodud seerianumber.

Kui te administraatori parooli taastate, lähtestatakse see ostuaegsele algväärtusele.

Täpsemad turvalisuse sätted

Turvalisuse sätted ja ohtude vältimine.	88
Juhtimine protokollidega.	89
Digitaalsertifikaadi kasutamine.	92
SSL/TLS-side skanneriga.	97
Krüptitud side IPsec/IP-filtreerimisega.	98
Skanneri ühendamine IEEE802.1X-võrguga.	109
Täpsemate turvasätetega seotud probleemide lahendamine.	111

Turvalisuse sätted ja ohtude vältimine

Kui skanner on ühendatud võrku, omate sellele juurdepääsu kaugasukohast. Lisaks saavad paljud inimesed skannerit jagada, mis muudab töö tegemise tõhusamaks ja mugavamaks. Samas suureneb õigusvastase juurdepääsu, ebaseadusliku kasutamise ja andmete rikkumise oht. Kui kasutate skannerit keskkonnas, kus teil on juurdepääs Internetti, on risk veelgi suurem.

Välise juurdepääsu eest kaitsmata skannerite puhul saab Interneti kaudu lugeda skannerisse salvestatud skannitööde logisid.

Selle ohu vältimiseks on Epsoni skanneritel erinevad turvatehnoloogiad.

Häälestage skanner vastavalt keskkonnatingimustele, mis on loodud kliendi keskkonna teabele tuginedes.

Nimi	Funktsiooni tüüp	Mida seadistada	Mida vältida
Protokolli kontrollimine	Kontrollib protokolle ja teenuseid skanneri ja arvutite vahelise suhtluse puhul ja lülitab funktsioone sisse või välja.	Funktsioonile kohaldatav protokoll või teenus on eraldi lubatud või keelatud.	Väärkasutusest põhjustatud turvariskide vähendamine läbi kasutajate jaoks ebaoluliste funktsioonide välistamise.
SSL/TLS side	Andmeside on SSL/TLS-sidet kasutades krüptitud, kui Epsoni serverit kasutatakse Internetis skannerist näiteks arvutiga suhtlemiseks läbi veebibrauseri, teenuse Epson Connect kasutamiseks ja püsivara värskendamiseks.	Hankige sertimiskeskuse allkirjastatud sertifikaat ja importige see skannerisse.	Skanneri identifitseerimine sertimiskeskuse allkirjastatud sertifikaadiga hoiab ära isiku matkimise ja volitamata juurdepääsu. Lisaks on SSL/TLS-ühenduse sisu kaitstud, mis takistab skannitavate andmete ja skannisätete lekkimist.
IPsec/IP-filtrimine	Saate määrata teatud kliendi või teatud tüüpi andmete keelamise ja katkestamise. IPsec kaitseb andmeid IP-pakettide üksuste kaupa (krüptimine ja autentimine), mistõttu on ka kaitsmata protokolliga side turvaline.	Looge üldpoliitika ja individuaalne poliitika, et määrata skannerile juurdepääsu omav klient või andmete tüüp.	Kaitske skannerisse liikuvaid sideandmeid volitamata juurdepääsu, muutmise ja ümbersuunamise eest.
IEEE 802.1X	Lubab võrguga ühenduda ainult autentitud kasutajatel. Võimaldab skannerit kasutada ainult selleks luba omaval kasutajal.	RADIUS-serveri (autentimisserver) autentimise seadistus.	Kaitseb skannerit volitamata juurdepääsu ja kasutamise eest.

Seotud teave

- ➔ „Juhtimine protokollidega” lk 89
- ➔ „SSL/TLS-side skanneriga” lk 97
- ➔ „Krüptitud side IPsec/IP-filtreerimisega” lk 98
- ➔ „Skanneri ühendamine IEEE802.1X-võrguga” lk 109

Turvalisuse sätted

IPsec/IP-filtrimise või IEEE 802.1X määramisel on soovitatav avada Web Config seadistuse edastamiseks SSL/TLS ühendusega, et vähendada turvariske nagu näiteks rikkumine või andmete vahelt kogumine.

Veenduge, et olete enne IPsec/IP-filtrimise või IEEE 802.1X seadistamist määranud administraatori parooli.

Juhtimine protokollidega

Te saate skannimiseks kasutada mimeid teid ja protokolle. Saate võrguskannimist kasutada ka määramata arvust võrguarvutitest.

Saate vähendada soovimatuid turvariske, piirates skannimist kindlatest asukohtadest või piirates saadaval funktsioone.

Juhtimisprotokollid

Konfigureerige protokollide sätted, mida skanner toetab.

1. Avage Web Config ja seejärel valige vahekaart **Network Security** tab > **Protocol**.
2. Määrake kõik sätted.
3. Klõpsake nuppu **Next**.
4. Klõpsake nuppu **OK**.
Sätted rakendatakse skanneris.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)

Protokollid, mida saate lubada või keelata

Protokoll	Kirjeldus
Bonjour Settings	Saate täpsustada, kas Bonjour kasutada. Protokollid Bonjour kasutatakse seadmete otsimiseks, skannimiseks jne.
SLP Settings	Saate SLP-funktsiooni lubada või keelata. SLP on mõeldud tõukeskannimiseks ja võrguotsinguks rakendusestEpsonNet Config.
WSD Settings	Saate WSD-funktsiooni lubada või keelata. Kui see on lubatud, saate lisada WSD-seadmeid ja skannida WSD-pordist.
LLTD Settings	Saate LLTD-funktsiooni lubada või keelata. Kui see on lubatud, kuvatakse see Windowsi võrgukaardil.
LLMNR Settings	Saate LLMNR-funktsiooni lubada või keelata. Kui see on lubatud, saate nime lahendamist ilma protokollita NetBIOS kasutada ka siis, kui DNS-i kasutamine ei ole võimalik.

Protokoll	Kirjeldus
SNMPv1/v2c Settings	Saate täpsustada, kas SNMPv1/v2c on lubatud. Seda kasutatakse seadmete seadistamiseks, jälgimiseks ja muuks.
SNMPv3 Settings	Saate täpsustada, kas SNMPv3 on lubatud. Seda kasutatakse krüptitud seadmete seadistamiseks, jälgimiseks jne.

Protokollide sätted

Bonjour Settings

Üksused	Seadistuse väärtus ja kirjeldus
Use Bonjour	Valige see, et otsida või kasutada teenuseid läbi Bonjour.
Bonjour Name	Kuvab Bonjour nime.
Bonjour Service Name	Kuvab Bonjour teenuse nime.
Location	Kuvab Bonjour asukoha nime.
Wide-Area Bonjour	Valige, kas kasutada teenust Wide-Area Bonjour.

SLP Settings

Üksused	Seadistuse väärtus ja kirjeldus
Enable SLP	Valige SLP funktsiooni aktiveerimiseks. Seda kasutatakse võrguotsinguks rakenduses EpsonNet Config.

WSD Settings

Üksused	Seadistuse väärtus ja kirjeldus
Enable WSD	Valige, et lubada seadmete lisamine funktsiooniga WSD ja skannimine WSD-pordist.
Scanning Timeout (sec)	Sisestage WSD skannimise side ajalõpu väärtus vahemikus 3 kuni 3600 sekundit.
Device Name	Kuvab WSD-seadme nime.
Location	Kuvab WSD asukoha nime.

LLTD Settings

Üksused	Seadistuse väärtus ja kirjeldus
Enable LLTD	Valige, et lubada LLTD. Skanner kuvatakse Windowsi võrgukaardil.
Device Name	Kuvab LLTD-seadme nime.

LLMNR Settings

Üksused	Seadistuse väärtus ja kirjeldus
Enable LLMNR	Valige, et lubada LLMNR. Nime lahendamist saate ilma Net-BIOSita kasutada ka siis, kui DNS ei ole võimalik.

SNMPv1/v2c Settings

Üksused	Seadistuse väärtus ja kirjeldus
Enable SNMPv1/v2c	Valige SNMPv1/v2c lubamiseks.
Access Authority	Seadistage juurdepääsuõigused SNMPv1/v2c lubamisel. Valige Read Only või Read/Write .
Community Name (Read Only)	Sisestage 0 kuni 32 ASCII (0x20–0x7E) tähemärki.
Community Name (Read/Write)	Sisestage 0 kuni 32 ASCII (0x20–0x7E) tähemärki.

SNMPv3 Settings

Üksused	Seadistuse väärtus ja kirjeldus
Enable SNMPv3	SNMPv3 on lubatud, kui märkeruut on täidetud.
User Name	Sisestage 1 kuni 32 tähemärki, kasutades ainult 1-baidiseid tähte.
Authentication Settings	
Algorithm	Valige SNMPv3 autentimise algoritm.
Password	Sisestage SNMPv3 autentimise parool. Sisestage 8 kuni 32 ASCII (0x20–0x7E) tähemärki. Kui te seda ei täpsusta, jätkke see tühjaks.
Confirm Password	Sisestage kinnitamiseks valitud parool.
Encryption Settings	
Algorithm	Valige SNMPv3 krüptimise algoritm.
Password	Sisestage SNMPv3 krüptimise parool. Sisestage 8 kuni 32 ASCII (0x20–0x7E) tähemärki. Kui te seda ei täpsusta, jätkke see tühjaks.
Confirm Password	Sisestage kinnitamiseks valitud parool.
Context Name	Sisestage kuni 32 tähti vormingus Unicode (UTF-8). Kui te seda ei täpsusta, jätkke see tühjaks. Sisestatavate tähemärkide arv võib sõltuvalt keelest erineda.

Digitaalsertifikaadi kasutamine

Digitaalsest sertimisest

CA-signed Certificate

See on sertimiskeskuse (SK) poolt allkirjastatud sertifikaat. Seda on võimalik sertimiskeskusest taotleda. See sertifikaat kinnitab skanneri olemasolu ja seda kasutatakse SSL-/TLS-side jaoks, et tagada andmeside turvalisus. SSL-/TLS-side puhul kasutatakse seda serveri sertifikaadina.

Kui see on määratud IPsec/IP-filtreerimise või IEEE 802.1X andmeside jaoks, siis kasutatakse seda kliendisertifikaadina.

SK-sertifikaat

See kuulub CA-signed Certificate'ide alla ja seda nimetatakse ka SK-sertifikaadiks. Veebibrauser kasutab seda skanneri sertifikaadi asukohta kontrollimiseks, et pääseda ligi teise poole serverile või utiliidile Web Config.

SK-sertifikaadi puhul tuleb määrata, millal lubada skannerist juurdepääsu serveri sertifikaadile. Skanneri puhul tuleb määrata CA-signed Certificate'i asukoht SSL-/TLS-side jaoks.

Skanneri SK-sertifikaadi saate SK-sertifikaate väljastavast sertimiskeskusest.

Samuti saate teise poole serveri valideerimiseks kasutatava SK-sertifikaadi hankida teise serveri CA-signed Certificate'i väljastanud sertimiskeskusest.

Self-signed Certificate

Selle sertifikaadi allkirjastab ja väljastab skanner ise. Seda nimetatakse ka juursertifikaadiks. Kuna sertifikaadi väljastaja serdib iseennast, ei ole see usaldusväärne ning ei ole võimalik välistada pettust.

Kasutage seda turvasätete tegemisel ja lihtsa SSL-/TLS-side jaoks ilma CA-signed Certificate'ita.

Kui kasutate seda sertifikaati SSL-/TLS-side jaoks, võib veebibrauser kuvada turvahoiatuse, sest sertifikaat ei ole veebibrauseris registreeritud. Te saate sertifikaati Self-signed Certificate kasutada üksnes SSL-/TLS-andmesideks.

Seotud teave

- ➔ [„CA-signed Certificate seadistamine” lk 92](#)
- ➔ [„Iseallkirjastatud sertifikaadi värskendamine” lk 96](#)
- ➔ [„CA Certificate seadistamine” lk 96](#)

CA-signed Certificate seadistamine

Sertimiskeskuse allkirjastatud sertifikaadi hankimine

Looge sertimiskeskuse allkirjastatud sertifikaadi hankimiseks sertifikaadi allkirjastamistaotlus (CSR — Certificate Signing Request) ja edastage see sertimiskeskusele. Te saate sertifikaadi allkirjastamistaotluse luua rakendust Web Config ja arvutit kasutades.

Järgige rakenduse Web Config abil sertifikaadi allkirjastamistaotluse loomisel ja sertimiskeskuse allkirjastatud sertifikaadi hankimisel alljärgnevaid suuniseid. Kui loote sertifikaadi allkirjastamistaotluse rakenduse Web Config abil, on sertifikaat PEM/DER-vormingus.

1. Avage Web Config ja seejärel valige vahekaart **Network Security**. Seejärel valige **SSL/TLS > Certificate** või **IPsec/IP Filtering > Client Certificate** või **IEEE802.1X > Client Certificate**.

Olenemata sellest, mille te valite, saate te hankida sama sertifikaadi ja kasutada seda ühiselt.

2. Klõpsake nuppu **Generate** valiku **CSR** all.

Avaneb sertifikaadi allkirjastamisaotluse loomisleht.

3. Sisestage iga üksuse jaoks väärtus.

Märkus.

Kasutatav võtme pikkus ja lühendid varieeruvad sertimiskeskuste lõikes. Looge konkreetse sertimiskeskuse reeglitele vastav taotlus.

4. Klõpsake nuppu **OK**.

Kuvatakse lõpetamise teade.

5. Valige vahekaart **Network Security**. Seejärel valige **SSL/TLS > Certificate** või **IPsec/IP Filtering > Client Certificate** või **IEEE802.1X > Client Certificate**.

6. Klõpsake sertifikaadi allkirjastamisaotluse arvutisse allalaadimiseks ühte taotluse **CSR** allalaadimisnuppudest, lähtudes konkreetse sertimiskeskuse määratud vormingust.



Oluline teave:

Ärge CSR-faili enam genereerige. Kui seda teete, ei ole teil enam võimalik CA-signed Certificate importida ja väljastada.

7. Saatke CSR sertimiskeskusele ja teile väljastatakse CA-signed Certificate.

Järgige saatmismeetodi ja vormi valimisel konkreetse sertimiskeskuse reegleid.

8. Salvestage sertimiskeskuse poolt välja antud CA-signed Certificate skanneriga ühendatud arvutisse.

Sertimiskeskuse CA-signed Certificate on lõppenud, kui olete sertifikaadi sihtkohta salvestanud.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

CSR sätteüksused

Üksused	Sätted ja selgitused
Key Length	Valige CSR võtme pikkus.
Common Name	Saate sisestada 1 kuni 128 tähemärki. Kui tegemist on IP-aadressiga, siis peab see olema staatiline IP-aadress. Saate sisestada 1 kuni 5 komaga eraldatud IPv4 aadressi, IPv6 aadressi, hostinime, FQDN-i. Esimene element salvestatakse üldise nimena ja ülejäänud sertifikaadi teema aliaste väljale. Näide: Skanneri IP-aadress: 192.0.2.123, skanneri nimi: EPSONA1B2C3 Common Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

Üksused	Sätted ja selgitused
Organization/ Organizational Unit/ Locality/ State/Province	Saate sisestada 0 kuni 64 ASCII (0x20–0x7E) tähemärki. Eraldi nimed saate eraldada komadega.
Country	Sisestage ISO-3166 kohane kahekohaline riigikood.
Sender's Email Address	Meiliserveri seadistuse jaoks saate sisestada saatja e-posti aadressi. Sisestage sama e-posti aadress mille sisestasite väljale Sender's Email Address vahekaardil Network > Email Server > Basic .

CA-allkirjastatud sertifikaadi importimine

Importige hangitud CA-signed Certificate skannerisse.



Oluline teave:

- Veenduge, et skanneri kuupäev ja kellaeg oleks õigesti seadistatud. Sertifikaat võib olla kehtetu.
- Kui saate sertifikaadi CSR võtme abil, mis on loodud utiliidi Web Config kaudu, on sertifikaati võimalik importida üks kord.

1. Avage Web Config ja seejärel valige vahekaart **Network Security**. Seejärel valige **SSL/TLS > Certificate** või **IPsec/IP Filtering > Client Certificate** või **IEEE802.1X > Client Certificate**.

2. Klõpsake nuppu **Import**

Avatakse sertifikaadi importimise leht.

3. Sisestage iga üksuse jaoks väärtus. Määrake **CA Certificate 1** ja **CA Certificate 2**, kui kinnitate sertifikaadi teed veebibrauseris, millel on juurdepääs skannerile.

Vajalikud sätted võivad erineda olenevalt loodava CSR-võtme asukohast ja sertifikaadi failiformaadist. Sisestage nõutud üksuste väärtused, nagu allpool viidatud.

- PEM/DER-formaadis Web Config utiliidist saadud sertifikaat
 - Private Key**: ärge konfigureerige, sest skanner sisaldab privaatvõtit.
 - Password**: jätke konfigureerimata.
 - CA Certificate 1/CA Certificate 2**: valikuline
- PEM/DER-formaadis arvutist saadud sertifikaat
 - Private Key**: vajalik on seadistamine.
 - Password**: jätke konfigureerimata.
 - CA Certificate 1/CA Certificate 2**: valikuline
- PKCS#12 -formaadis arvutist saadud sertifikaat
 - Private Key**: jätke konfigureerimata.
 - Password**: valikuline
 - CA Certificate 1/CA Certificate 2**: jätke konfigureerimata.

4. Klõpsake nuppu **OK**.

Kuvatakse lõpetamise teade.

Märkus.

Sertifikaadi teabe kontrollimiseks klõpsake **Confirm**.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

CA-allkirjastatud sertifikaadi importimise sätted

Üksused	Sätted ja selgitused
Server Certificate või Client Certificate	Valige sertifikaadi vorming. SSL/TLS ühenduse puhul kuvatakse Server Certificate. IPsec/IP-filtrimise või IEEE 802.1X puhul kuvatakse Client Certificate.
Private Key	Kui hangite PEM/DER vormingus sertifikaadi arvutis loodid CSR-i kasutades, siis määrake sertifikaadile vastav privaatne võtmefail.
Password	Kui failivorming on Certificate with Private Key (PKCS#12) , siis sisestage privaatse võtmefaili jaoks sertifikaadi hankimisel määratud parool.
CA Certificate 1	Kui sertifikaadi vorming on Certificate (PEM/DER) , siis importige sertifikaat sertifitseerimisasutuselt mis väljastas serveri sertifikaadina kasutatava CA-signed Certificate'i. Vajadusel määrake fail.
CA Certificate 2	Kui sertifikaadi vorming on Certificate (PEM/DER) , siis importige sertifikaat sertifitseerimisasutuse CA Certificate 1. Vajadusel määrake fail.

Sertimiskeskuse allkirjastatud sertifikaadi kustutamine

Te saate imporditud sertifikaadi kustutada, kui sertifikaat on aegunud või kui krüptitud ühendus ei ole enam vajalik.



Oluline teave:

Kui hangite sertifikaadi rakendusest Web Config loodud sertifikaadi allkirjastamisaotlust kasutades, ei saa te kustutatud sertifikaati uuesti importida. Sellisel juhul looge sertifikaadi allkirjastamisaotlus ja hankige sertifikaat uuesti.

1. Avage rakendus Web Config ja seejärel valige vahekaart **Network Security**. Seejärel valige **SSL/TLS > Certificate** või **IPsec/IP Filtering > Client Certificate** või **IEEE802.1X > Client Certificate**.
2. Klõpsake nuppu **Delete**.
3. Kinnitage, et soovite kuvatava serdi kustutada.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Iseallkirjastatud sertifikaadi värskendamine

Kuna Self-signed Certificate väljastab skanner, saate seda värskendada, kui see on aegunud või kui kirjeldatud sisu muutub.

1. Avage Web Config ja valige vahekaart **Network Security** tab > **SSL/TLS** > **Certificate**.
2. Klõpsake nuppu **Update**.
3. Sisestage nimi väljale **Common Name**.

Te saate sisestada kuni 5 IPv4 aadressi, IPv6 aadressi, hostinime, FQDN-formaate pikkusega 1 kuni 128 tärki, eraldades need komadega. Esimene parameeter salvestatakse ühisnime juurde ning teised salvestatakse sertifikaadi subjekti aliase välja juurde.

Näide:

Skanneri IP-aadress: 192.0.2.123, Skanneri nimi: EPSONA1B2C3

Ühisnimi: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Määrake sertifikaadi kehtivusperiood.
5. Klõpsake nuppu **Next**.
6. Klõpsake nuppu **OK**.

Kuvatakse kinnitusteade.

Skannerit värskendatakse.

Märkus.

Sertifikaadi teavet saate kontrollida, kui lähete **Network Security** vahekaardile > **SSL/TLS** > **Certificate** > **Self-signed Certificate** ja klõpsate **Confirm**.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)

CA Certificate seadistamine

Sertifikaadi CA Certificate määramisel saate valideerida CA-sertifikaadi tee skanneri kasutatavas serveris. See aitab vältida isiku matkimist.

CA Certificate on saadaval CA-signed Certificate väljastuskoha sertifitseerimisasutuselt.

CA Certificate import

Importige CA Certificate skannerisse.

1. Avage Web Config ja seejärel valige vahekaart **Network Security** > **CA Certificate**.
2. Klõpsake nuppu **Import**.
3. Määrake imporditav CA Certificate.
4. Klõpsake nuppu **OK**.

Pärast importi liigute tagasi kuvale **CA Certificate** kus on näha imporditud CA Certificate.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

CA Certificate kustutamine

Imporditud CA Certificate on kustutatav.

1. Avage Web Config ja valige vahekaart **Network Security** > **CA Certificate**.
2. Klõpsake **Delete** kustutatava CA Certificate kõrval.
3. Kinnitage kuvatava sõnumi juures, et soovite sertifikaadi kustutada.
4. Klõpsake **Reboot Network** ja kontrollige, et kustutatud CE Certificate on uuendatud kuvalt kadunud.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

SSL/TLS-side skanneriga

Kui serveri sertifikaat on määratud kasutama skanneriga suhtlemiseks SSL/TLS-sidet (turvasoklite kiht/transpordikihi turve), saate sidetee arvutite vahel krüptida. Tehke seda, kui soovite takistada kaug- ja volitamata juurdepääsu.

SSL/TLS põhisätete seadistamine

Kui skanneril on HTTPS serveri funktsioon, saate kasutada side krüptimiseks SSL/TLS sidet. Skannerit saate seadistada ja hallata turvaliselt Web Config kaudu.

Seadistage krüptimise tugevus ja ümbersuunamise funktsioon.

1. Avage Web Config ja valige vahekaart **Network Security** > **SSL/TLS** > **Basic**.
2. Valige iga üksuse jaoks väärtus.
 - Encryption Strength
Valige krüptimise taseme tugevus.
 - Redirect HTTP to HTTPS
Suunake HTTP juurdepääs ümber HTTPS peale.
3. Klõpsake nuppu **Next**.
Kuvatakse kinnitussõnum.
4. Klõpsake nuppu **OK**.
Skanner on värskendatud.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Skannerile serveri sertifikaadi konfigureerimine

1. Avage Web Config ja valige vahekaart **Network Security** > **SSL/TLS** > **Certificate**.
2. Määrake kasutatav sertifikaat menüüst **Server Certificate**.
 - Self-signed Certificate
Skanner on loonud iseallkirjastatud sertifikaadi. Kui te ei hangi CA-allkirjastatud sertifikaati, siis valige see.
 - CA-signed Certificate
Kui olete hankinud ja juba importinud CA-allkirjastatud sertifikaadi, siis saate valida selle.
3. Klõpsake nuppu **Next**.
Kuvatakse kinnitussõnum.
4. Klõpsake nuppu **OK**.
Skanner värskendatakse.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

➔ „CA-signed Certificate seadistamine” lk 92

➔ „CA Certificate seadistamine” lk 96

Krüptitud side IPsec/IP-filtreerimisega

Teave rakenduse IPsec/IP Filtering kohta

Te saate filtreerida liiklust IP-aadresside, teenuste ja portide alusel IPsec/IP-filtreerimise funktsiooniga. Te saate filtreerimise kombineerimisega konfigureerida skannerit lubama või blokeerima teatud kliente ja määratud andmeid. Lisaks saate IPsec-filtreerimise abil tõsta turvataset.

Märkus.

Arvutid, millel on operatsioonisüsteem Windows Vista või uuem või Windows Server 2008 või uuem, toetavad standardit IPsec.

Vaikepoliitika konfigureerimine

Konfigureerige liikluse filtreerimiseks vaikepoliitika. Vaikepoliitika kehtib kõigile kasutajatele või gruppidele, kes skanneriga ühendust loovad. Konfigureerige kasutajate või kasutajagruppide optimaalsemaks reguleerimiseks rühmapoliitikat.

1. Avage Web Config ja seejärel valige vahekaart **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Sisestage iga üksuse jaoks väärtus.

3. Klõpsake nuppu **Next**.
Kuvatakse kinnitusteade.
4. Klõpsake nuppu **OK**.
Skannerit värskendatakse.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Suvandi Default Policy sättekirjed

Default Policy

Üksused	Sätted ja selgitused
IPsec/IP Filtering	Te saate IPsec-/IP-filtreerimise aktiveerida või inaktiveerida.

Access Control

Konfigureerige IP-pakettide liikluse reguleerimismeetod.

Üksused	Sätted ja selgitused
Permit Access	Valige see suvand, et lubada konfigureeritud IP-pakettide läbipääs.
Refuse Access	Valige see suvand, et keelata konfigureeritud IP-pakettide läbipääs.
IPsec	Valige see suvand, et lubada konfigureeritud IPsec-pakettide läbipääs.

IKE Version

Valige suvandi **IKEv1** sätteks **IKEv2** või **IKE Version**. Valige neist üks vastavalt seadmele, millega skanner on ühendatud.

IKEv1

Kui **IKEv1** on valitud suvandi **IKE Version** sätteks, kuvatakse alljärgnevad üksused.

Üksused	Sätted ja selgitused
Authentication Method	Suvandi Certificate valimiseks peate kõigepealt hankima ja importima sertimiskeskuse allkirjastatud sertifikaadi.
Pre-Shared Key	Kui valite sätte Pre-Shared Key suvandi Authentication Method sätteks, sisestage eelnevalt ühiskasutatud võti, mis koosneb 1–127 tähemärgist.
Confirm Pre-Shared Key	Sisestage kinnitamiseks konfigureeritud võti.

IKEv2

Kui **IKEv2** on valitud suvandi **IKE Version** sätteks, kuvatakse alljärgnevad üksused.

Üksused	Sätted ja selgitused	
Local	Authentication Method	Suvandi Certificate valimiseks peate kõigepealt hankima ja importima sertimiskeskuse allkirjastatud sertifikaadi.
	ID Type	Kui valite Pre-Shared Key suvandi Authentication Method sätteks, valige skanneri ID tüüp.
	ID	Sisestage skanneri ID, mis vastab ID-tüübile. Esimese tärgina ei saa kasutada tärke „@“, „#“ ja „=“. Distinguished Name: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „=“. IP Address: sisestage IPv4- või IPv6-vormingus. FQDN: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“ ja punkt (.). Email Address: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „@“. Key ID: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) tärki.
	Pre-Shared Key	Kui valite sätte Pre-Shared Key suvandi Authentication Method sätteks, sisestage eelnevalt ühiskasutatud võti, mis koosneb 1–127 tähemärgist.
	Confirm Pre-Shared Key	Sisestage kinnitamiseks konfigureeritud võti.

Üksused		Sätted ja selgitused
Remote	Authentication Method	Suvandi Certificate valimiseks peate kõigepealt hankima ja importima sertimiskeskuse allkirjastatud sertifikaadi.
	ID Type	Kui Pre-Shared Key valitakse suvandi Authentication Method sätteks, valige ID tüüp seadmele, mida soovite autentida.
	ID	Sisestage skanneri ID, mis vastab ID-tüübile. Esimese tärgina ei saa kasutada tärke „@“, „#“ ja „=“. Distinguished Name: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki. Nende hulgas peab olema „=“. IP Address: sisestage IPv4- või IPv6-vormingus. FQDN: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“ ja punkt (.). Email Address: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki. Nende hulgas peab olema „@“. Key ID: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki.
	Pre-Shared Key	Kui valite sätte Pre-Shared Key suvandi Authentication Method sätteks, sisestage eelnevalt ühiskasutatud võti, mis koosneb 1–127 tähemärgist.
	Confirm Pre-Shared Key	Sisestage kinnitamiseks konfigureeritud võti.

Encapsulation

Kui valite sätte **IPsec** suvandi **Access Control** sätteks, peate konfigureerima kapseldusrežiimi.

Üksused	Sätted ja selgitused
Transport Mode	Kui kasutate skannerit ainult ühes kohtvõrgus, valige see suvand. 4. kihi või edasiste kihtide IP-paketid krüptitakse.
Tunnel Mode	Kui kasutate skannerit Interneti-valmidusega võrgus (nagu IPsec-VPN), valige see suvand. IP-pakettide päis ja andmed krüptitakse. Remote Gateway(Tunnel Mode): kui valite sätte Tunnel Mode suvandi Encapsulation sätteks, sisestage lüüsi aadress, mis koosneb 1–39 tärgist.

Security Protocol

Kui valite sätte **IPsec** suvandis **Access Control**, valige suvand.

Üksused	Sätted ja selgitused
ESP	Valige see suvand, et tagada autentimise ja andmete terviklus ning andmete krüptimine.
AH	Valige see suvand, et tagada autentimise ja andmete terviklus. Te saate IPsec kasutada ka siis, kui andmete krüptimine on keelatud.

❑ Algorithm Settings

Soovitame valida kõikide suvandite sätteks **Any** või valida iga suvandi sätteks midagi muud kui **Any**. Kui osade suvandite sätteks **Any** ja teiste suvandite sätteks midagi muud kui **Any**, ei pruugi olenevalt seadmest, mida soovite autentida, side seadmega võimalik olla.

Üksused		Sätted ja selgitused
IKE	Encryption	Valige IKE krüptimisalgoritm. Üksused, mis erinevad olenevalt IKE versioonist.
	Authentication	Valige IKE autentimisalgoritm.
	Key Exchange	Valige IKE võtmevahetusalgoritm. Üksused, mis erinevad olenevalt IKE versioonist.
ESP	Encryption	Valige ESP krüptimisalgoritm. See on võimalik, kui ESP on valitud suvandi Security Protocol sätteks.
	Authentication	Valige ESP autentimisalgoritm. See on võimalik, kui ESP on valitud suvandi Security Protocol sätteks.
AH	Authentication	Valige AH krüptimisalgoritm. See on võimalik, kui Security Protocol on valitud suvandi AH sätteks.

Rühmapoliitika konfigureerimine

Rühmapoliitika tähistab kasutajale või kasutajagrupile kehtestatud ühte või mitut reeglit. Skanner kontrollib IP-pakette, mis ühtivad konfigureeritud poliitikaga. IP-pakette autentitakse rühmapoliitika järjestuses 1 kuni 10, ning kui ükski rühmapoliitika säte ei ühti, rakendatakse seejärel vaikepoliitikat.

1. Avage Web Config ja seejärel valige vahekaart **Network Security > IPsec/IP Filtering > Basic**.
2. Klõpsake nummerdatud vahekaarti, mida soovite konfigureerida.
3. Sisestage iga üksuse jaoks väärtus.
4. Klõpsake nuppu **Next**.
Kuvatakse kinnitusteade.
5. Klõpsake nuppu **OK**.
Skannerit värskendatakse.

Suvandi Group Policy sättekirjed

Üksused	Sätted ja selgitused
Enable this Group Policy	Te saate rühmapoliitikat aktiveerida või blokeerida.

Access Control

Konfigureerige IP-pakettide liikluse reguleerimismeetod.

Üksused	Sätted ja selgitused
Permit Access	Valige see suvand, et lubada konfigureeritud IP-pakettide läbipääs.
Refuse Access	Valige see suvand, et keelata konfigureeritud IP-pakettide läbipääs.
IPsec	Valige see suvand, et lubada konfigureeritud IPsec-pakettide läbipääs.

Local Address (Scanner)

Valige IPv4-aadress või IPv6-aadress, mis vastab teie võrgukeskkonnale. Kui IP-aadress määratakse automaatselt, võite teha valiku **Use auto-obtained IPv4 address**.

Märkus.

Kui IPv6-aadress määratakse automaatselt, ei pruugi ühendus kasutatav olla. Konfigureerige staatiline IPv6-aadress.

Remote Address(Host)

Sisestage juurdepääsu reguleerimiseks seadme IP-aadress. IP-aadress peab olema pikkusega 43 tärki või lühem. Kui jätate IP-aadressi sisestamata, reguleeritakse kõiki aadresse.

Märkus.

Kui IP-aadress määratakse automaatselt (näiteks DHCP poolt), ei pruugi ühendus kasutatav olla. Konfigureerige staatiline IP-aadress.

Method of Choosing Port

Valige portide määramise meetod.

Service Name

Kui valite sätte **Service Name** suvandis **Method of Choosing Port**, valige suvand.

Transport Protocol

Kui valite sätte **Port Number** suvandi **Method of Choosing Port** sätteks, peate konfigureerima kapseldusrežiimi.

Üksused	Sätted ja selgitused
Any Protocol	Valige see säte, et reguleerida kõiki protokollide tüüpe.
TCP	Valige see säte, et reguleerida ainusaate andmeid.
UDP	Valige see säte, et reguleerida levi- ja multisaate andmeid.
ICMPv4	Valige see säte, et reguleerida pingimiskäsku.

Local Port

Kui valite sätte **Port Number** suvandi **Method of Choosing Port** sätteks ja **TCP** või **UDP** suvandi **Transport Protocol** sätteks, sisestage pordinumbrid pakettide vastuvõtmise reguleerimiseks, eraldades need komadega. Te saate maksimaalselt sisestada 10 pordinumbrit.

Näide: 20,80,119,5220

Kui jätate pordinumbri sisestamata, reguleeritakse kõiki porte.

Remote Port

Kui valite sätte **Port Number** suvandi **Method of Choosing Port** sätteks ja **TCP** või **UDP** suvandi **Transport Protocol** sätteks, sisestage pordinumbrid pakettide saatmise reguleerimiseks, eraldades need komadega. Te saate maksimaalselt sisestada 10 pordinumbrit.

Näide: 25,80,143,5220

Kui jätate pordinumbri sisestamata, reguleeritakse kõiki porte.

IKE Version

Valige suvandi **IKEv1** sätteks **IKEv2** või **IKE Version**. Valige neist üks vastavalt seadmele, millega skanner on ühendatud.

IKEv1

Kui **IKEv1** on valitud suvandi **IKE Version** sätteks, kuvatakse alljärgnevad üksused.

Üksused	Sätted ja selgitused
Authentication Method	Kui valite sätte IPsec suvandis Access Control , valige suvand. Kasutatav sertifikaat ühtib vaikepoliitikaga.
Pre-Shared Key	Kui valite sätte Pre-Shared Key suvandi Authentication Method sätteks, sisestage eelnevalt ühiskasutatud võti, mis koosneb 1–127 tähemärgist.
Confirm Pre-Shared Key	Sisestage kinnitamiseks konfigureeritud võti.

☐ IKEv2

Kui **IKEv2** on valitud suvandi **IKE Version** sätteks, kuvatakse alljärgnevad üksused.

Üksused		Sätted ja selgitused
Local	Authentication Method	Kui valite sätte IPsec suvandis Access Control , valige suvand. Kasutata sertifikaat ühtib vaikepoliitikaga.
	ID Type	Kui valite Pre-Shared Key suvandi Authentication Method sätteks, valige skanneri ID tüüp.
	ID	Sisestage skanneri ID, mis vastab ID-tüübile. Esimese tärgina ei saa kasutada tärke „@“, „#“ ja „=“. Distinguished Name: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki. Nende hulgas peab olema „=“. IP Address: sisestage IPv4- või IPv6-vormingus. FQDN: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“ ja punkt (.). Email Address: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki. Nende hulgas peab olema „@“. Key ID: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki.
	Pre-Shared Key	Kui valite sätte Pre-Shared Key suvandi Authentication Method sätteks, sisestage eelnevalt ühiskasutatud võti, mis koosneb 1–127 tähemärgist.
	Confirm Pre-Shared Key	Sisestage kinnitamiseks konfigureeritud võti.
	Remote	Authentication Method
Remote	ID Type	Kui Pre-Shared Key valitakse suvandi Authentication Method sätteks, valige ID tüüp seadmele, mida soovite autentida.
	ID	Sisestage skanneri ID, mis vastab ID-tüübile. Esimese tärgina ei saa kasutada tärke „@“, „#“ ja „=“. Distinguished Name: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki. Nende hulgas peab olema „=“. IP Address: sisestage IPv4- või IPv6-vormingus. FQDN: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“ ja punkt (.). Email Address: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki. Nende hulgas peab olema „@“. Key ID: sisestage 1–255 1-baidist ASCII-vormingus (0x20–0x7E) täarki.
	Pre-Shared Key	Kui valite sätte Pre-Shared Key suvandi Authentication Method sätteks, sisestage eelnevalt ühiskasutatud võti, mis koosneb 1–127 tähemärgist.
	Confirm Pre-Shared Key	Sisestage kinnitamiseks konfigureeritud võti.

Encapsulation

Kui valite sätte **IPsec** suvandi **Access Control** sätteks, peate konfigureerima kapseldusrežiimi.

Üksused	Sätted ja selgitused
Transport Mode	Kui kasutate skannerit ainult ühes kohtvõrgus, valige see suvand. 4. kihi või edasiste kihtide IP-paketid krüptitakse.
Tunnel Mode	Kui kasutate skannerit Interneti-valmidusega võrgus (nagu IPsec-VPN), valige see suvand. IP-pakettide päis ja andmed krüptitakse. Remote Gateway(Tunnel Mode): kui valite sätte Tunnel Mode suvandi Encapsulation sätteks, sisestage lüüsi aadress, mis koosneb 1–39 tärgist.

Security Protocol

Kui valite sätte **IPsec** suvandis **Access Control**, valige suvand.

Üksused	Sätted ja selgitused
ESP	Valige see suvand, et tagada autentimise ja andmete terviklus ning andmete krüptimine.
AH	Valige see suvand, et tagada autentimise ja andmete terviklus. Te saate IPsec kasutada ka siis, kui andmete krüptimine on keelatud.

Algorithm Settings

Soovitame valida kõikide suvandite sätteks **Any** või valida iga suvandi sätteks midagi muud kui **Any**. Kui osade suvandite sätteks **Any** ja teiste suvandite sätteks midagi muud kui **Any**, ei pruugi olenevalt seadmest, mida soovite autentida, side seadmega võimalik olla.

Üksused	Sätted ja selgitused	
IKE	Encryption	Valige IKE krüptimisalgoritm. Üksused, mis erinevad olenevalt IKE versioonist.
	Authentication	Valige IKE autentimisalgoritm.
	Key Exchange	Valige IKE võtmevahetusalgoritm. Üksused, mis erinevad olenevalt IKE versioonist.
ESP	Encryption	Valige ESP krüptimisalgoritm. See on võimalik, kui ESP on valitud suvandi Security Protocol sätteks.
	Authentication	Valige ESP autentimisalgoritm. See on võimalik, kui ESP on valitud suvandi Security Protocol sätteks.
AH	Authentication	Valige AH krüptimisalgoritm. See on võimalik, kui AH on valitud suvandi Security Protocol sätteks.

Suvandite Local Address (Scanner) ja Remote Address(Host) kombinatsioon funktsioonis Group Policy

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

Suvandi Remote Address(Host) säte	IPv4* ¹	✓	–	✓
	IPv6* ^{1, *2}	–	✓	✓
	Tühi	✓	✓	✓

*1 Kui **IPsec** on valitud suvandi **Access Control** sätteks, ei saa te eesliite pikkust määrata.

*2 Kui **IPsec** on valitud suvandi **Access Control** säteks, saate te valida link-kohaliku aadressi (fe80::), aga rühmapoliitika inaktiveeritakse.

*3 Välja arvatud link-kohalikud IPv6-aadressid.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Rühma poliitika teenuse nimetuse referentsid

Märkus.

Teenudes mida kasutada ei saa kuvatakse aga neid ei saa valida.

Teenuse nimi	Protokolli tüüp	Kohaliku pordi number	Kaugpordi number	Kontrollitavad funktsioonid
Any	–	–	–	Kõik teenused
ENPC	UDP	3289	Kõik pordid	Skanneri otsimine rakendustest nagu näiteks Epson Device Admin ja skanneridraiver
SNMP	UDP	161	Kõik pordid	MIB hankimine ja konfigureerimine rakendustest nagu Epson Device Admin ja Epsoni skanneridraiver
WSD	TCP	Kõik pordid	5357	WSD kontrollimine
WS-Discovery	UDP	3702	Kõik pordid	WSD-skannerite otsimine
Network Scan	TCP	1865	Kõik pordid	Skannitud andmete edastamine rakendusest Document Capture Pro
Network Push Scan	TCP	Kõik pordid	2968	Tööteabe hankimine töökeskannimiseks rakendusest Document Capture Pro
Network Push Scan Discovery	UDP	2968	Kõik pordid	Arvuti otsimine skannerist
FTP Data (Remote)	TCP	Kõik pordid	20	FTP-klient (skannitud andmete edastamine) Saab kontrollida ainult kaugporti 20 kasutatavat FTP serverit.
FTP Control (Remote)	TCP	Kõik pordid	21	FTP-klient (edastatud skannitud andmete kontrollimine)
CIFS (Remote)	TCP	Kõik pordid	445	CIFS-klient (skannitud andmete edastamine kausta)

Teenuse nimi	Protokolli tüüp	Kohaliku pordi number	Kaugpordi number	Kontrollitavad funktsioonid
NetBIOS Name Service (Remote)	UDP	Kõik pordid	137	CIFS-klient (skannitud andmete edastamine kausta)
NetBIOS Datagram Service (Remote)	UDP	Kõik pordid	138	
NetBIOS Session Service (Remote)	TCP	Kõik pordid	139	
HTTP (Local)	TCP	80	Kõik pordid	HTTP(S) server (Web Config ja WSD andmete edastamine)
HTTPS (Local)	TCP	443	Kõik pordid	
HTTP (Remote)	TCP	Kõik pordid	80	HTTP(S)-klient (püsivara ja juurserdi värskendamine)
HTTPS (Remote)	TCP	Kõik pordid	443	

IPsec/IP Filtering konfiguratsiooni näited

Ainult IPsec pakettide vastuvõtmine

See näide on ainult vaikimisi poliitika konfigureerimiseks.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: IPsec
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: sisestage kuni 127 tähemärki.

Group Policy: jätke konfigureerimata.

Skannimise andmete ja skanneri sätete vastuvõtmine

See näide võimaldab määratud seadmetest skannimise andmete ja skanneri sätete vastuvõtmist.

Default Policy:

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

Group Policy:

- Enable this Group Policy: märgistage ruut.
- Access Control: Permit Access
- Remote Address(Host): kliendi IP-aadress
- Method of Choosing Port: Service Name
- Service Name: märgistage ruudud ENPC, SNMP, HTTP (Local), HTTPS (Local) ja Network Scan juures.

Juurdepääsu lubamine ainult määratud IP-aadressilt

See näide lubab skannerile juurdepääsu ainult määratud IP-aadressilt.

Default Policy:

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

Group Policy:

- Enable this Group Policy: märgistage ruut.
- Access Control: Permit Access
- Remote Address(Host): administraatori kliendi IP-aadress

Märkus.

Kliendil on skannerile juurdepääs ja konfigureerimise võimalus sõltumata poliitika konfiguratsioonist.

IPsec/IP-filtrimine sertifikaadi seadistamine

Seadistage IPsec/IP-filtrimise kliendi sertifikaat. Pärast seadistamist saate sertifikaati kasutada IPsec/IP-filtrimise autentimise meetodina. Sertifitseerimisasutuse seadistamiseks avage **CA Certificate**.

1. Avage Web Config ning valige sakk **Network Security > IPsec/IP Filtering > Client Certificate**.
2. Importige sertifikaat menüüst **Client Certificate**.

Kui olete sertifitseerimisasutuse väljastatud sertifikaadi juba importinud, siis saate selle kopeerida kasutamiseks ka IPsec/IP-filtrimise puhul. Kopeerimiseks valige sertifikaat menüüst **Copy From** ja klõpsake **Copy**.

Seotud teave

- ➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37
- ➔ „CA-signed Certificate seadistamine” lk 92
- ➔ „CA Certificate seadistamine” lk 96

Skanneri ühendamine IEEE802.1X-võrguga

IEEE 802.1X-võrgu konfigureerimine

Kui määrate skannerile IEEE 802.1X, saate seda kasutada RADIUS-serveriga ühendatud võrgus, autentimisfunktsiooniga kohtvõrgu kommutaatoriga või pääsupunktiga.

1. Avage Web Config ja seejärel valige vahekaart **Network Security > IEEE802.1X > Basic**.
2. Sisestage iga üksuse jaoks väärtus.

Kui soovite kasutada skannerit Wi-Fi-võrgus, klõpsake nuppu **Wi-Fi Setup** ja valige või sisestage SSID.

Märkus.

Etherneti- ja Wi-Fi-sätted võivad olla samad.

3. Klõpsake nuppu **Next**.
Kuvatakse kinnitusteade.
4. Klõpsake nuppu **OK**.
Skannerit värskendatakse.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Võrgu IEEE 802.1X säteteüksused

Üksused	Sätted ja selgitused	
IEEE802.1X (Wired LAN)	Saate lehel sätteid lubada ja keelata (IEEE802.1X > Basic) võrgu IEEE802.1X jaoks (traadiga LAN).	
IEEE802.1X (Wi-Fi)	Kuvatakse IEEE802.1X-i (Wi-Fi) ühenduse olek.	
Connection Method	Kuvatakse praeguse võrgu ühendusmeetod.	
EAP Type	Valige skanneri ja RADIUS-serveri vahelise autentimise meetodi suvand.	
	EAP-TLS	Peate omandama ja importima CA-allkirjastatud sertifikaadi.
	PEAP-TLS	
	PEAP/MSCHAPv2	Peate seadistama parooli.
	EAP-TTLS	
User ID	Seadistage ID, mida RADIUS-serveri autentimiseks kasutada. Sisestage 1–128 ühebaidist ASCII (0x20–0x7E) tähti.	
Password	Seadistage skanneri autentimiseks parool. Sisestage 1–128 ühebaidist ASCII (0x20–0x7E) tähti. Kui kasutate Windowsi serverit RADIUS-serverina, saate sisestada kuni 127 tähti.	
Confirm Password	Sisestage kinnitamiseks määratud parool.	
Server ID	Saate seadistada serveri ID, mida määratud RADIUS-serveriga autentida. Autentikaator kinnitab, kas serveri ID sisaldub RADIUS-serverist saadatud serveri sertifikaadi väljal „subject/subjectAltName“ või mitte. Sisestage 0–128 ühebaidist ASCII (0x20–0x7E) tähti.	
Certificate Validation (traadiga LAN)	Kui soovite kasutada funktsiooni Certificate Validation võrgus IEEE802.1X (Wired LAN) , valige Enable . Kui lubate selle, lugege läbi asjassepuutuv teave ja importige CA Certificate . Arvestage, et Certificate Validation on võrgus IEEE802.1X (Wi-Fi) alati lubatud. Importige kindlasti CA Certificate.	
Anonymous Name	Kui PEAP-TLS või PEAP/MSCHAPv2 on valitud suvandi EAP Type sätteks, saate PEAP-autentimise 1. faasi jaoks konfigureerida kasutaja ID asemel anonüümse nime. Sisestage 0–128 ühebaidist ASCII (0x20–0x7E) tähti.	

Üksused	Sätted ja selgitused	
Encryption Strength	Saate valida ühe alljärgnevatest.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Seotud teave

➔ „CA Certificate seadistamine” lk 96

IEEE 802.1X sertifikaadi seadistamine

IEEE802.1X kliendi sertifikaadi seadistamine. Pärast seadistamist saate IEEE 802.1X autentimise meetodiks valida EAP-TLS ja PEAP-TLS. Sertifitseerimisasutuse sertifikaadi seadistamiseks avage **CA Certificate**.

1. Avage Web Config ning valige sakk **Network Security > IEEE802.1X > Client Certificate**.
2. Sisestage sertifikaat valikuga **Client Certificate**.

Kui olete sertifitseerimisasutuse väljastatud sertifikaadi juba importinud, siis saate selle kopeerida kasutamiseks ka IEEE802.1X puhul. Kopeerimiseks valige sertifikaat menüüst **Copy From** ja klõpsake **Copy**.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Täpsemate turvasätetega seotud probleemide lahendamine

Turvasätete taastamine

Kui loote kõrge turvalisustasemega keskkonna, nagu IPsec/IP-filtrimine, ei pruugi seadmetega suhtlemine valede sätete või seadme või serveri probleemide tõttu olla võimalik. Sel juhul taastage turvasätted, et määrata seadme sätted uuesti või võimaldada ajutist kasutamist.

Turvafunktsiooni keelamine rakenduses Web Config

IPsec/IP Filtering on võimalik välja lülitada rakenduses Web Config.

1. Avage Web Config ja valige vahekaart **Network Security > IPsec/IP Filtering > Basic**.
2. Keelake **IPsec/IP Filtering**.

Probleemid võrgu turvafunktsioonide kasutamisel

Ühiskasutatud võtme unustamine

Rekonfigureerige ühiskasutatud võti.

Võtme muutmiseks avage Web Config ja valige vahekaart **Network Security > IPsec/IP Filtering > Basic > Default Policy** või **Group Policy**.

Kui te ühiskasutatud võtit muudate, konfigureerige ühiskasutatud võti arvutite jaoks.

Seotud teave

- ➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37
- ➔ „Krüptitud side IPsec/IP-filtreerimisega” lk 98

IPsec-sideühenduse kasutamine ei ole võimalik

Tehke kindlaks algoritm, mida skanner või arvuti ei toeta.

Skanner toetab alljärgnevaid algoritme. Kontrollige arvuti sätteid.

Turbemeetodid	Algoritmid
IKE krüptimisalgoritm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE autentimisalgoritm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE võtmevahetusalgoritm	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 krüptimisalgoritm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP autentimisalgoritm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH autentimisalgoritm	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Saadaval ainult IKEv2 jaoks

Seotud teave

- ➔ „Krüptitud side IPsec/IP-filtreerimisega” lk 98

Sideühendus ei ole ootamatult kasutatav

Skanneri IP-aadressi on muudetud või seda ei ole võimalik kasutada.

Kui suvandis Group Policy olevale kohalikule aadressile registreeritud IP-aadressi on muudetud või kui seda ei ole võimalik kasutada, ei saa IPsec andmesidet teostada. Inaktiveerige skanneri juhtpaneelilt IPsec.

Kui DHCP on aegunud või taaskäivitamisel või IPv6-aadress on aegunud või hankimata, ei pruugita skanneri rakenduses Web Config (vahekaart **Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) registreeritud IP-aadressi leida.

Kasutage staatilist IP-aadressi.

Arvuti IP-aadressi on muudetud või seda ei ole võimalik kasutada.

Kui suvandis Group Policy olevale eemalasuvale aadressile registreeritud IP-aadressi on muudetud või kui seda ei ole võimalik kasutada, ei saa IPsec andmesidet teostada.

Inaktiveerige skanneri juhtpaneelilt IPsec.

Kui DHCP on aegunud või taaskäivitamisel või IPv6-aadress on aegunud või hankimata, ei pruugita skanneri rakenduses Web Config (vahekaart **Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) registreeritud IP-aadressi leida.

Kasutage staatilist IP-aadressi.

Seotud teave

- ➔ [„Kuidas kasutada veebibrauseris rakendust Web Config” lk 37](#)
- ➔ [„Krüptitud side IPsec/IP-filtreerimisega” lk 98](#)

Ei saa ühendust pärast IPsec/IP filtreerimise häällestamist

IPsec/IP filtreerimise sätted on valed.

Inaktiveerige IPsec/IP-filtreerimine skanneri juhtpaneelilt. Ühendage skanner ja arvuti ning määrake IPsec/IP-filtreerimise sätted uuesti.

Seotud teave

- ➔ [„Krüptitud side IPsec/IP-filtreerimisega” lk 98](#)

Pärast standardi IEEE 802.1X konfigureerimist puudub seadmele juurdepääs

Standardi IEEE 802.1X-i sätted on valed.

Inaktiveerige IEEE 802.1X ja Wi-Fi skanneri juhtpaneelilt. Ühendage skanner ja arvuti ja seejärel konfigureerige IEEE 802.1X uuesti.

Seotud teave

- ➔ [„IEEE 802.1X-võrgu konfigureerimine” lk 109](#)

Probleemid digitaalsertifikaadi kasutamisel

Sertifikaadi CA-signed Certificate importimine ei õnnestu

Sertifikaat CA-signed Certificate ja sertifikaadi allkirjastamistaotlusel olev teave ei ühti.

Kui sertifikaadi CA-signed Certificate ja sertifikaadi allkirjastamistaotlusel ei ole ühesugune informatsioon, ei ole sertifikaadi allkirjastamistaotluse importimine võimalik. Kontrollige alljärgnevat:

- Kas püüate importida sertifikaati seadmesse, millel ei ole sama informatsiooni?
Kontrollige sertifikaadi allkirjastamistaotlusel sisalduvat teavet ning importige seejärel sertifikaat seadmesse, millel on sama informatsioon.
- Kas kirjutasite skannerisse salvestatud sertifikaadi allkirjastamistaotluse pärast sertifikaadi allkirjastamistaotluse sertimiskeskusele saatmist üle?
Hankige sertimiskeskuse allkirjastatud sertifikaat uuesti, kasutades sertifikaadi allkirjastamistaotlust.

CA-signed Certificate on üle 5 KB.

Te ei saa importida sertifikaati CA-signed Certificate, mis on suurem kui 5 KB.

Sertifikaadi importimiseks kasutatav parool on vale.

Sisestage õige parool. Kui unustasite parooli, ei ole sertifikaadi importimine võimalik. Hankige sertifikaat CA-signed Certificate uuesti.

Seotud teave

➔ [„CA-allkirjastatud sertifikaadi importimine” lk 94](#)

Iseallkirjastatud sertifikaadi värskendamine ei ole võimalik

Common Name väljale ei ole midagi sisestatud.

Common Name peab olema sisestatud.

Common Name väljale on sisestatud tähemärke, mida ei toetata.

Sisestage 1 kuni 128 tähemärki, mis vastavad Interneti-protokollile IPv4, IPv6 või hostinimele, või on FQDN-vormingus, kasutades standardkoodi ASCII (0x20–0x7E).

Ühisnimes on kasutatud koma või tühikut.

Kui sisestatud on koma, jagatakse Common Name koma sisestuskohas. Kui enne või pärast koma on sisestatud ainult tühik, ei vasta ühisnimi nõuetele.

Seotud teave

➔ [„Iseallkirjastatud sertifikaadi värskendamine” lk 96](#)

Sertifikaadi allkirjastamistaotluse loomine ei ole võimalik

Common Name väljale ei ole midagi sisestatud.

Common Name peab olema sisestatud.

Väljadele Common Name, Organization, Organizational Unit, Locality ja State/Province on sisestatud tähemärke, mida ei toetata.

Sisestage tähemärgid, mis vastavad Interneti-protokollile IPv4, IPv6 või hostinimele, või on FQDN-vormingus, kasutades standardkoodi ASCII (0x20–0x7E).

Common Name sisaldab koma või tühikut.

Kui sisestatud on koma, jagatakse **Common Name** koma sisestuskohas. Kui enne või pärast koma on sisestatud ainult tühik, ei vasta ühisnimi nõuetele.

Seotud teave

➔ „Sertimiskeskuse allkirjastatud sertifikaadi hankimine” lk 92

Kuvatakse digitaalsertifikaadiga seotud hoiatus

Teated	Põhjus/tegevusmeede
Enter a Server Certificate.	<p>Põhjus:</p> <p>Te ei ole importimiseks faili valinud.</p> <p>Tegevusmeede:</p> <p>Valige fail ja klõpsake nuppu Import.</p>
CA Certificate 1 is not entered.	<p>Põhjus:</p> <p>Sertimiskeskuse sertifikaat 1 ei ole sisestatud ning sisestatud on üksnes sertimiskeskuse sertifikaat 2.</p> <p>Tegevusmeede:</p> <p>Importige esimesena sertimiskeskuse sertifikaat 1.</p>
Invalid value below.	<p>Põhjus:</p> <p>Faili tee ja/või parool sisaldab toetamata tähemärke.</p> <p>Tegevusmeede:</p> <p>Kontrollige, kas tähemärgid on väljale õigesti sisestatud.</p>
Invalid date and time.	<p>Põhjus:</p> <p>Skanneri kuupäev ja kellaeg on seadistamata.</p> <p>Tegevusmeede:</p> <p>Seadistage kuupäev ja kellaeg, kasutades rakendust Web Config või EpsonNet Config.</p>

Teated	Põhjus/tegevusmeede
Invalid password.	<p>Põhjus: Sertimiskeskuse sertifikaadile määratud parool ja sisestatud parool ei ühti.</p> <p>Tegevusmeede: Sisestage õige parool.</p>
Invalid file.	<p>Põhjus: Imporditava sertifikaadi fail ei ole X509-vormingus.</p> <p>Tegevusmeede: Kontrollige, kas olete valinud õige sertifikaadi, mille on saatnud usaldusväärne sertimiskeskus.</p>
	<p>Põhjus: Imporditud fail on liiga suur. Maksimaalne lubatud faili maht on 5 KB.</p> <p>Tegevusmeede: Kui valisite õige faili, võib sertifikaat olla rikutud või võltsitud.</p>
	<p>Põhjus: Sertifikaadis sisalduv ahel on lubamatu.</p> <p>Tegevusmeede: Külastage sertifikaadi kohta lisateabe saamiseks sertimiskeskuse veebisaiti.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p>Põhjus: PKCS#12-vormingus sertifikaadi fail sisaldab rohkem kui kolme sertimiskeskuse sertifikaati.</p> <p>Tegevusmeede: Importige kõik sertifikaadid, konvertides PKCS#12-vormingu PEM-vormingusse, või importige PKCS#12-vormingus sertifikaadi fail, mis sisaldab kuni kahte sertimiskeskuse sertifikaati.</p>
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p>Põhjus: Sertifikaat on aegunud.</p> <p>Tegevusmeede:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Kui sertifikaat on aegunud, hankige ja importige uus sertifikaat. <input type="checkbox"/> Kui sertifikaat ei ole aegunud, kontrollige, kas skanneri kuupäev ja kellaaeg on õigesti seadistatud.

Teated	Põhjus/tegevusmeede
Private key is required.	<p>Põhjus:</p> <p>Sertifikaadiga ei ole seotud ühtegi privaatvõtit.</p> <p>Tegevusmeede:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Kui sertifikaat on PEM/DER-vormingus ja see on hangitud arvutist saadetud sertifikaadi allkirjastamisaotlusega, määratlege privaatvõtme fail. <input type="checkbox"/> Kui sertifikaat on PKCS#12-vormingus ja see on hangitud arvutist saadetud sertifikaadi allkirjastamisaotlusega, looge privaatvõtit sisaldav fail.
	<p>Põhjus:</p> <p>Olete uuesti importinud PEM/DER-vormingus sertifikaadi, mis on hangitud rakendusest Web Config saadetud sertifikaadi allkirjastamisaotlusega.</p> <p>Tegevusmeede:</p> <p>Kui sertifikaat on PEM/DER-vormingus ja see on hangitud rakendusest Web Config saadetud sertifikaadi allkirjastamisaotlusega, saate sertifikaati importida vaid ühe korra.</p>
Setup failed.	<p>Põhjus:</p> <p>Konfigureerimise lõpetamine ei ole võimalik skanneri ja arvuti vahelise sideühenduse nurjumise tõttu või ei ole faili lugemine teatud vigadest tingitud võimalik.</p> <p>Tegevusmeede:</p> <p>Kontrollige määratud faili ja sideühendust ning importige fail seejärel uuesti.</p>

Seotud teave

➔ [„Digitaalsest sertimisest” lk 92](#)

Sertimiskeskuse allkirjastatud sertifikaadi kogemata kustutamine

Sertimiskeskuse allkirjastatud sertifikaadi varufaili ei ole.

Kui teil on varufail, importige sertifikaat uuesti.

Kui hangite sertifikaadi rakendusest Web Config loodud sertifikaadi allkirjastamisaotlust kasutades, ei saa te kustutatud sertifikaati uuesti importida. Looge sertifikaadi allkirjastamisaotlus ja hankige uus sertifikaat.

Seotud teave

➔ [„CA-allkirjastatud sertifikaadi importimine” lk 94](#)

➔ [„Sertimiskeskuse allkirjastatud sertifikaadi kustutamine” lk 95](#)

Funktsiooni Epson Open Platform kasutamine

Ülevaade: Epson Open Platform.119

Epson Open Platformi seadistamine.119

Epson Open Platformi valideerimine. 119

Ülevaade: Epson Open Platform

Epson Open Platform on platvorm, mis võimaldab selle skanneriga kasutada autentimissüsteeme.

Seda saab kasutada rakendusega Epson Print Admin (Epsoni autentimissüsteem) või kolmanda poole autentimissüsteemiga. Saate hankida logisid seadme ja kasutaja järgi, konfigureerida kasutajatele ja rühmadele kasutamiseks saadaval seadmeid, seada piiranguid funktsioonidele jne.

Kui ühendate autentimisseadme, saate lisaks kasutajaid autentida ID-kaardiga.

Epson Open Platformi seadistamine

Võimaldage Epson Open Platform, et saaksite seadet autentimissüsteemi kaudu kasutada.

1. Hankige spetsiaalselt veebisaidilt tootevõti.
Vaadake lisateavet platvormi Epson Open Platform juhendist (nt tootevõtme hankimise kohta).
2. Avage Web Config ja valige seejärel vahekaart **Epson Open Platform > Product Key or License Key**.
3. Vaadake üle ja seadistage kõik üksused.
 - Serial Number
Kuvatakse seadme seerianumber.
 - Epson Open Platform Version
Valige Epson Open Platformi versioon. Vastav versioon varieerub olenevalt autentimissüsteemist.
 - Product Key or License Key
Sisestage hangitud tootevõti.
4. Klõpsake nuppu **Next**.
Avaneb sätte kinnituskuva.
5. Klõpsake nuppu **OK**.
Sätted rakendatakse skanneris.

Märkus.

Funktsiooni Epson Print Admin Serverless ei saa kasutada, kui süsteem on sünkroonitud platvormiga Epson Open Platform.

Epson Open Platformi valideerimine

Saate platvormi Epson Open Platform kehtivust kontrollida, kasutades ühte alljärgnevatest meetoditest.

- Web Config
Tootevõti on vahekaardil **Epson Open Platform > Product Key or License Key > Product Key or License Key** sisestatud ja vasakpoolses menüüpuus kuvatakse vahekaart **Epson Open Platform > Authentication System**.
- Skanneri juhtpaneel
Veenduge, et toote võti oleks kuvatud jaotises **Sätted > Seadme info > Teave rakenduse Epson Open Platform kohta**.

Autentimisseadme paigaldamine

Autentimisseadme ühendamine.	121
Autentimisseadme töötamise kontroll.	121
Autentimiskaardi tuvastuse kinnitamine.	121
Autentimisseadme tõrkeotsing.	121

Autentimisseadme ühendamine

Märkus.

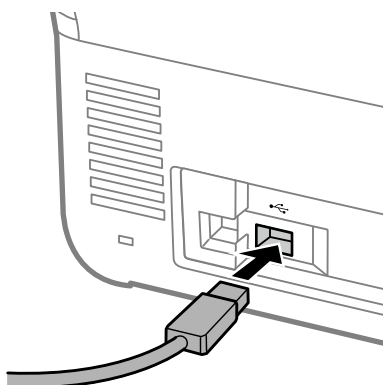
Autentimisseadet kasutatakse koos autentimissüsteemiga.



Oluline teave:

Kui ühendate autentimisseadme mitme skanneriga, kasutage sama mudelikoodiga toodet.

Ühendage kaardilugeja USB-kaabel skanneri välisliidese USB-porti.



Autentimisseadme töötamise kontroll

Saate kontrollida autentimisseadme ühenduse olekut ja autentimiskaardi tuvastust skanneri juhtpaneelilt.

Asjakohane teave kuvatakse, kui teete valiku **Sätted > Seadme info > Autentimisseadme olek**.

Autentimiskaardi tuvastuse kinnitamine

Saate autentimiskaartide tuvastamist kontrollida funktsiooni Web Config kasutades.

1. Avage Web Config ja valige seejärel vahekaart **Device Management > Card Reader**.
2. Hoidke autentimiskaarti autentimisseadme kohal.
3. Klõpsake nuppu **Check**.
Kuvatakse tulemus.

Autentimisseadme tõrkeotsing

Autentimiskaarti pole võimalik lugeda

Kontrollige järgmist.

- Kontrollige, kas autentimisseade on skanneriga õigesti ühendatud.
Ühendage autentimisseade skanneri tagaküljel olevasse välisliidese USB-porti.
- Kontrollige, et autentimisseade ja autentimiskaart oleksid sertifitseeritud.
Toetatud autentimisseadmete ja -kaartide kohta teabe saamiseks võtke ühendust oma edasimüüjaga.

Hooldamine

Skanneri korpuse puhastamine.	124
Skanneri sisemuse puhastamine.	124
Rulli montaažikomplekti vahetamine.	129
Skannide arvu lähtestamine pärast rullikute vahetamist.	134
Energia säästmine.	135
Skanneri transportimine.	135
Sätete varundamine.	136
Taasta vaikesätted.	137
Rakenduste ja püsivara värskendamine.	138


Skanneri korpuse puhastamine

Pühkige korpusel olevad plekid ära kuiva lapiga või lapiga, mida on niisutatud pehme pesuaine ja veega.



Oluline teave:

- Ärge kasutage skanneri puhastamiseks kunagi alkoholi, lahustit ega söövitavat lahust. Selle tagajärjeks võib olla deformeerumine või värvimuutus.
- Ärge laske veel toote sisse tungida. See võib tekitada tõrke.
- Ärge kunagi avage skanneri korpust.

1. Skanneri väljalülitamiseks vajutage nuppu .
2. Võtke vahelduvvooluadapter skanneri küljest lahti.
3. Puhastage väliskorpust lahja puhastusaine ja veega niisutatud lapiga.

Märkus.

Pühkige puutekraani pehme kuiva lapiga.

Skanneri sisemuse puhastamine

Skanneri pikema kasutamise järel võivad rullile või skanneri sees olevale klaasist osale kogunenud paberi ja ruumi tolm põhjustada probleeme paberi söötmisega või skannitud pildi kvaliteediga. Puhastage skanneri sisemust iga 5,000 skaneeringu järel.


Uusimat skannitud dokumentide arvu saate vaadata juhtpaneelil või rakenduses Epson Scan 2 Utility.

Kui pind on määrdunud ja plekk on raskesti eemaldatav, kasutage puhastamiseks Epsoni originaalset puhastuskomplekti. Plekkide eemaldamiseks kandke puhastuslapile väike kogus puhastusvahendit.

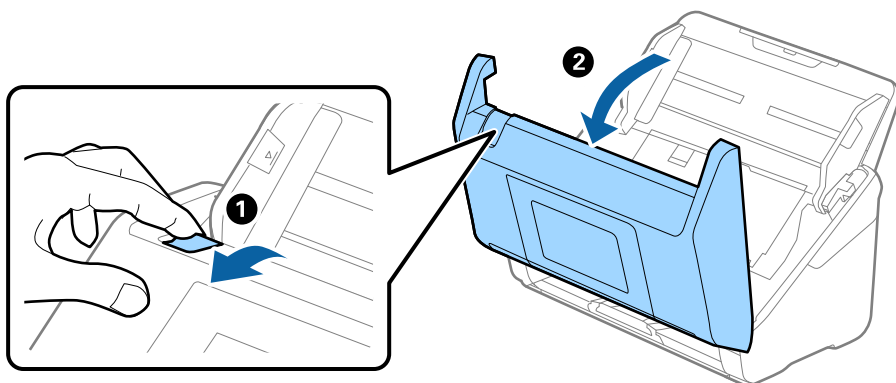


Oluline teave:

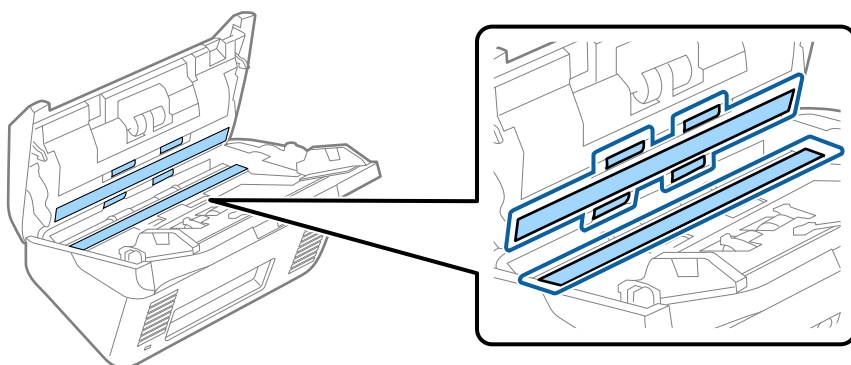
- Ärge kasutage skanneri puhastamiseks kunagi alkoholi, lahustit ega söövitavat lahust. Selle tagajärjeks võib olla deformeerumine või värvimuutus.
- Ärge pihustage skannerile vedelikku ega õlitusainet. Seadmete või elektriskeemide kahjustused võivad põhjustada tööhäireid.
- Ärge kunagi avage skanneri korpust.

1. Skanneri väljalülitamiseks vajutage nuppu .
2. Võtke vahelduvvooluadapter skanneri küljest lahti.

3. Tõmmake hooba ja avage skanneri kaas.



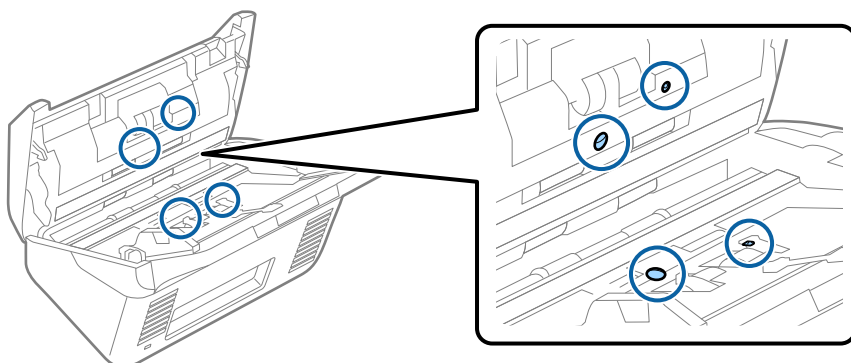
4. Pühkige ära plekid skanneri sees oleva plastrullil (4 kohta) ja skanneri kaane all oleva klaaspinnal. Pühkige pehme kiuvaba lapiga, mida on niisutatud väikese koguse spetsiaalse puhastusvahendi või veega.



Oluline teave:

- Ärge suruge liiga tugevasti klaaspinda.
- Ärge kasutage harja ega kõva tööriista. Klaasil olevad kriimud võivad skannimise kvaliteeti mõjutada.
- Ärge pihustage puhastusainet otse klaaspinnale.

5. Pühkige vatitupsuga ära anduritel olevad plekid.

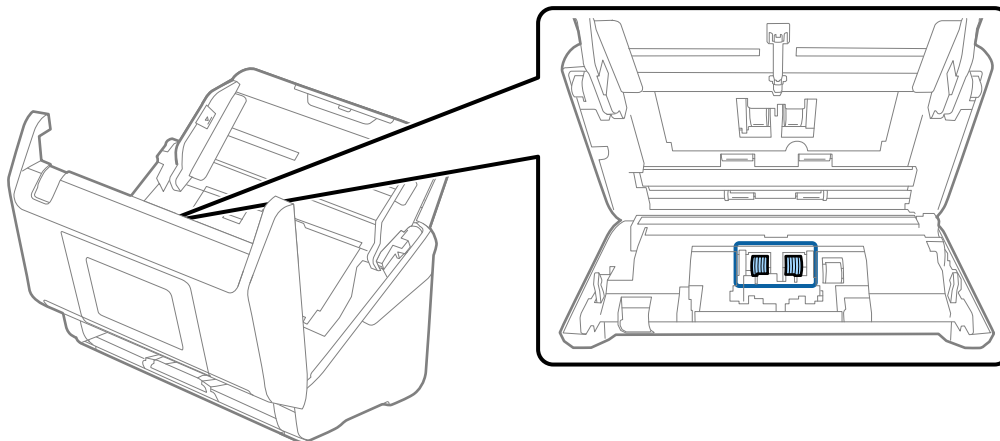


! *Oluline teave:*

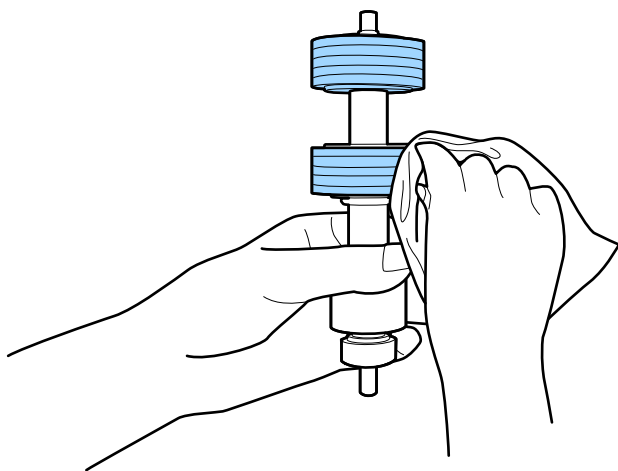
Ärge kandke vatitupsule vedelikku, näiteks puhastusainet.

6. Avage kaas ja eemaldage eraldusrull.

Vt lisateavet jaotisest „Rulliku montaažikomplekti vahetamine“.



7. Pühkige puhtaks eraldusrull. Pühkige pehme kiuvaba lapiga, mida on niisutatud väikese koguse spetsiaalse puhastusvahendi või veega.

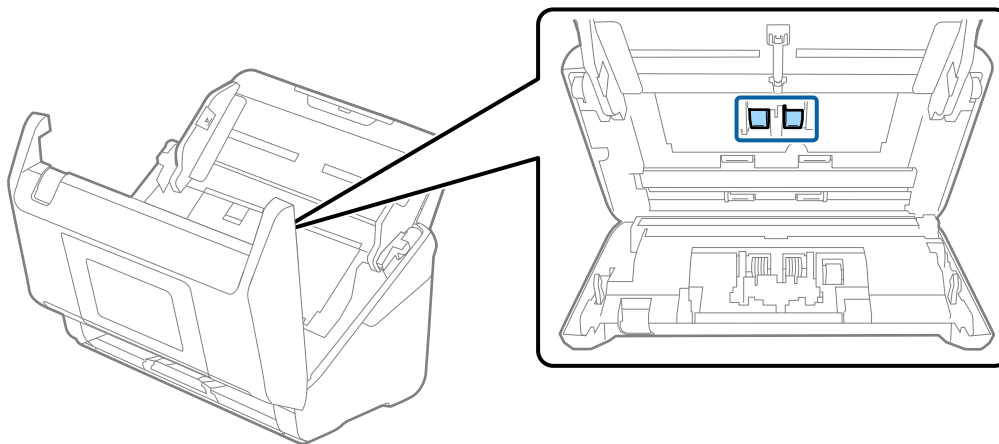


! *Oluline teave:*

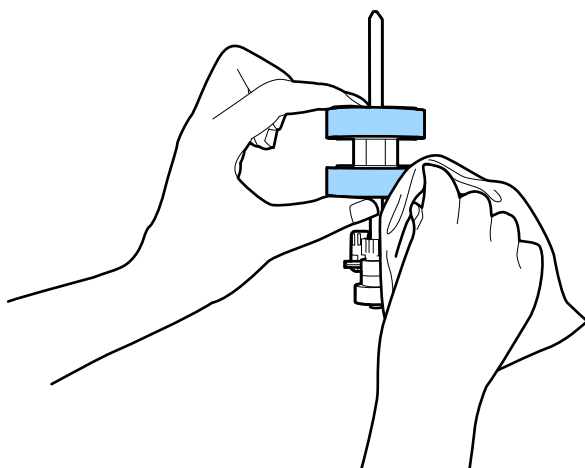
Kasutage rulliku puhastamiseks Epsoni originaalset puhastuskomplekti või pehmet niisket lappi. Kuiva lapi kasutamine võib rulli pealispinda kahjustada.

8. Avage kaas ja eemaldage korjerull.

Vt lisateavet jaotisest „Rulliku montaažikomplekti vahetamine“.



9. Pühkige puhtaks vastuvõturull. Pühkige pehme kiuvaba lapiga, mida on niisutatud väikese koguse spetsiaalse puhastusvahendi või veega.

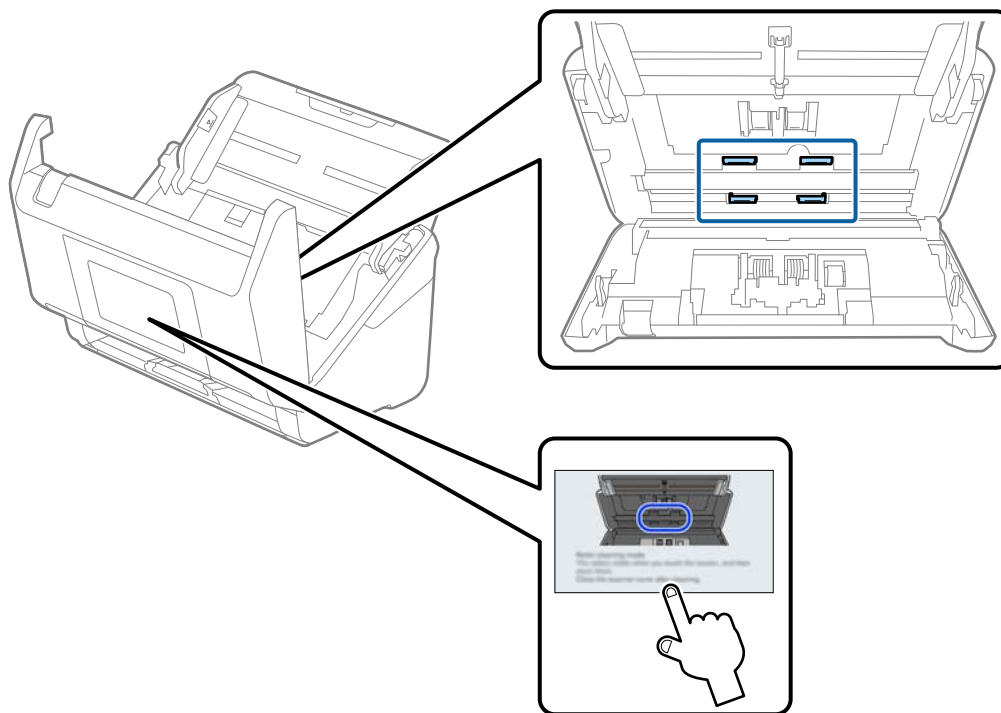


Oluline teave:

Kasutage rulliku puhastamiseks Epsoni originaalset puhastuskomplekti või pehmet niisket lappi. Kuiva lapi kasutamine võib rulli pealispinda kahjustada.

10. Sulgege skanneri kaas.
11. Ühendage vahelduvvooluadapter vooluvõrku ja lülitage skanner sisse.
12. Valige avaekraanilt **Skanneri hooldus**.
13. Valige **Skanneri hooldus** ekraanilt **Rulliku puhastamine**.
14. Tõmmake hooba, et avada skanneri kaas.
Skanner läheb rullide puhastusrežiimi.

15. Pöörake rulle aeglaselt, vajutades mis tahes kohale LCD-ekraanil. Pühkige Epsoni originaalse puhastuskomplekti või pehme niiske lapiga rullide pinda. Korrake seda, kuni rullid saavad puhtaks.



⚠ Ettevaatust!

Olge ettevaatlik, et teie käed või juuksed ei jääks rulli käitamisel mehhanismi vahele. See võib põhjustada vigastuse.

16. Sulgege skanneri kaas.

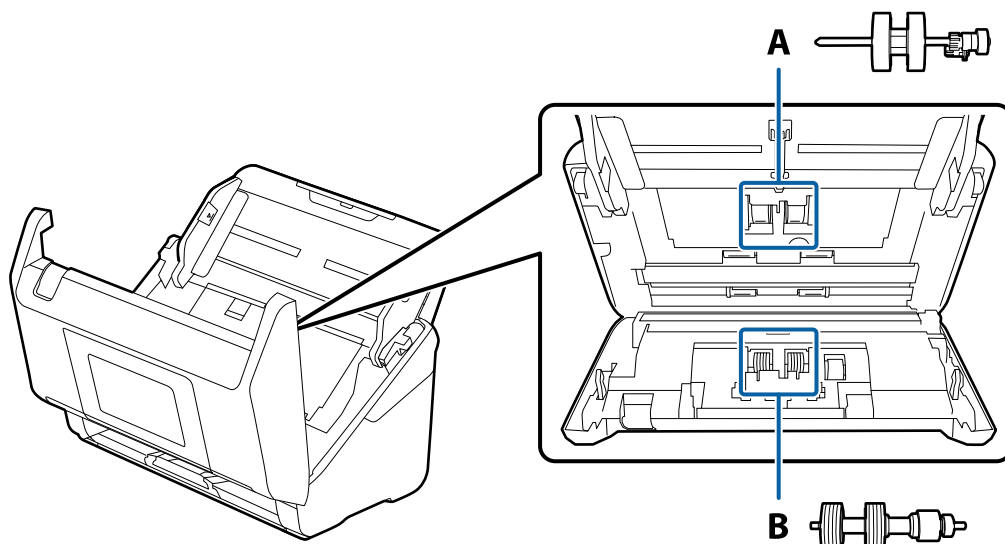
Skanner läheb rullide puhastusrežiimist välja.

Seotud teave


➔ „Rulli montaažikomplekti vahetamine” lk 129

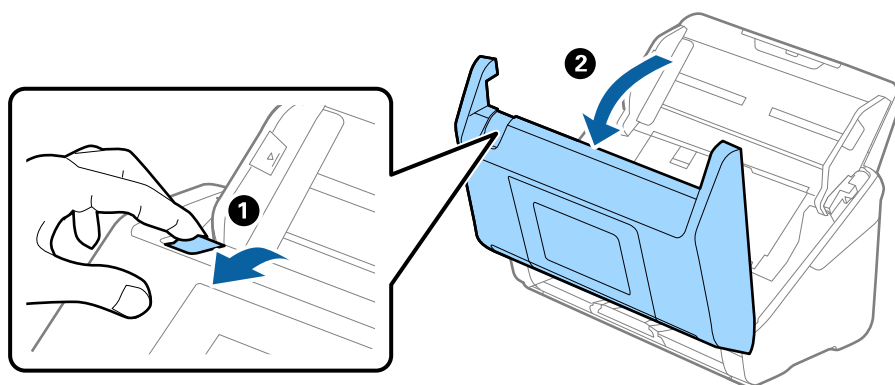
Rulli montaažikomplekti vahetamine

Rulli montaažikomplekt (vastuvõturull ja eraldusrull) on vaja vahetada siis, kui skannide arv ületab rullide kasutustsükli. Kui juhtpaneelil või arvuti ekraanil kuvatakse vahetamise teadet, siis järgige all väljatoodud samme selle vahetamiseks.

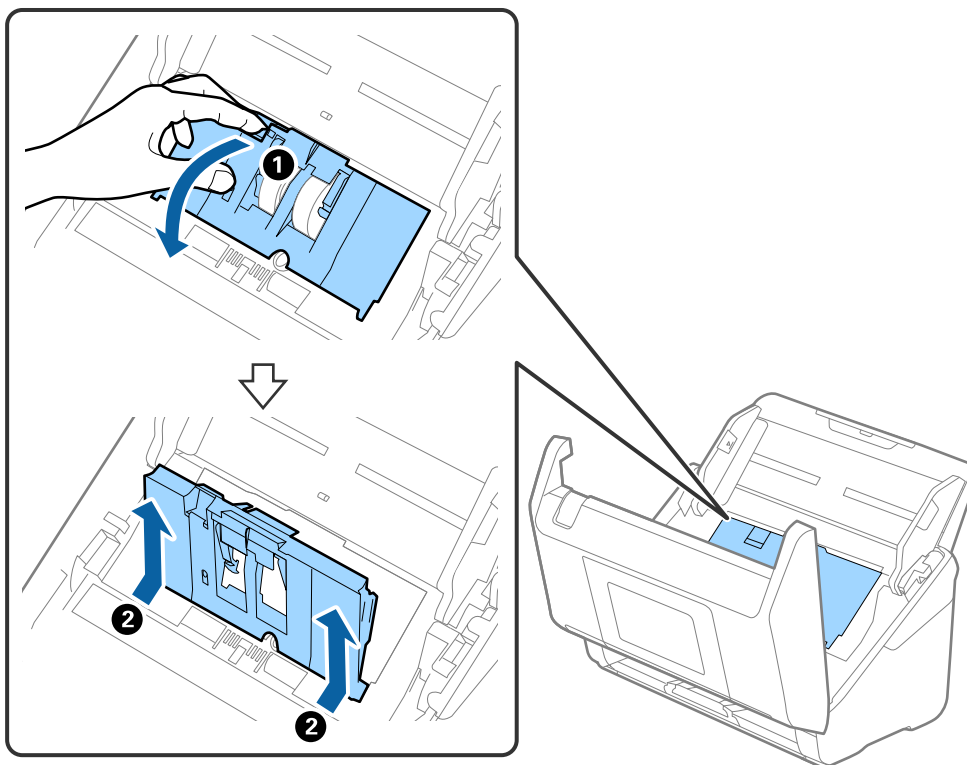


A: vastuvõturull, B: eraldusrull

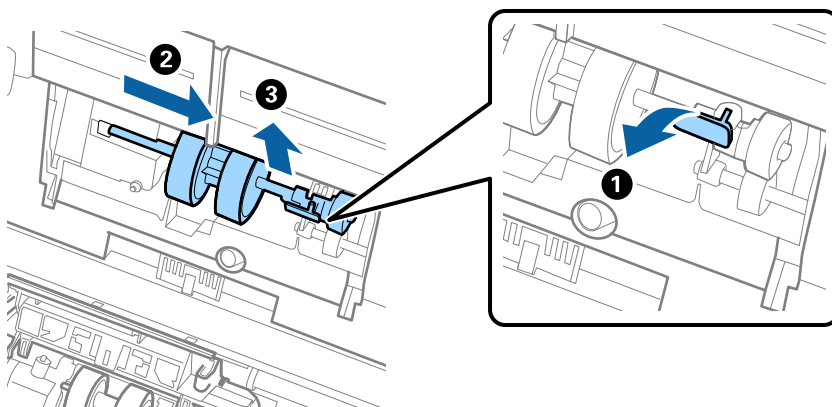
1. Skanneri väljalülitamiseks vajutage nuppu .
2. Võtke vahelduvvooluadapter skanneri küljest lahti.
3. Tõmmake hooba ja avage skanneri kaas.



4. Avage vastuvõturulli kaas, seejärel lükake see välja.



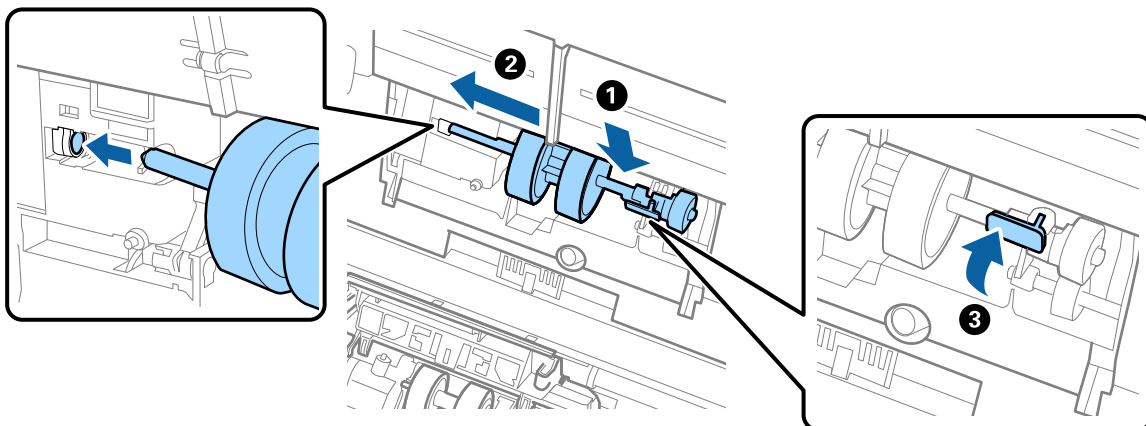
5. Tõmmake rulli telje kinnitusrakis alla, seejärel lükake paigaldatud vastuvõturullid välja.



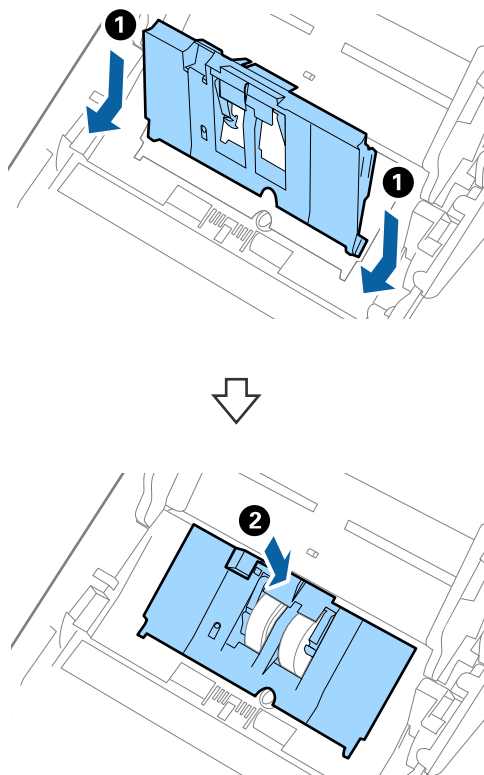
Oluline teave:

Ärge tõmmake vastuvõturulli jõuga välja. See võib skanneri sisemust vigastada.

6. Kinnitusrakist all hoides lükake uus vastuvõturull vasemale ja sisestage see skanneris olevasse auku. Kinnitusrakise lukustamiseks suruge seda.

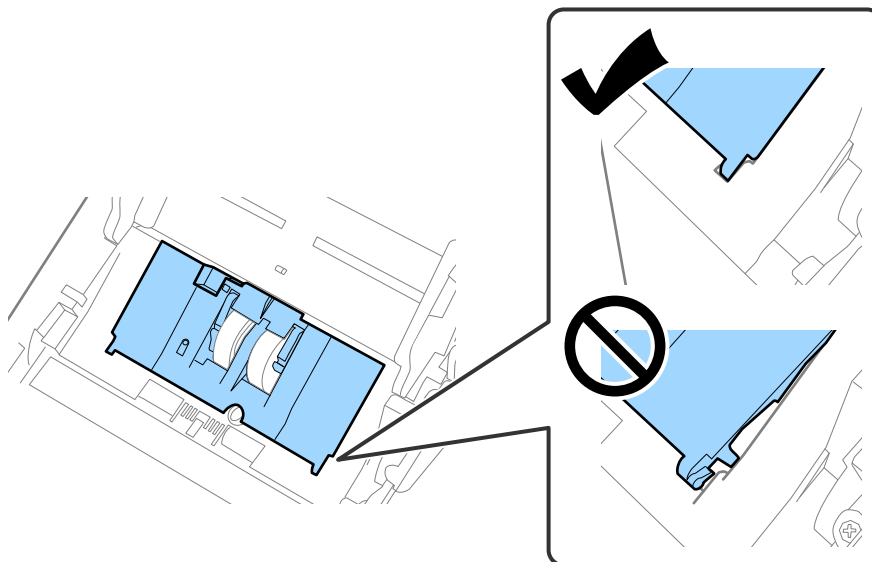


7. Pange vastuvõturulli kaane serv soone sisse ja lükake seda. Sulgege kaas kindlalt.

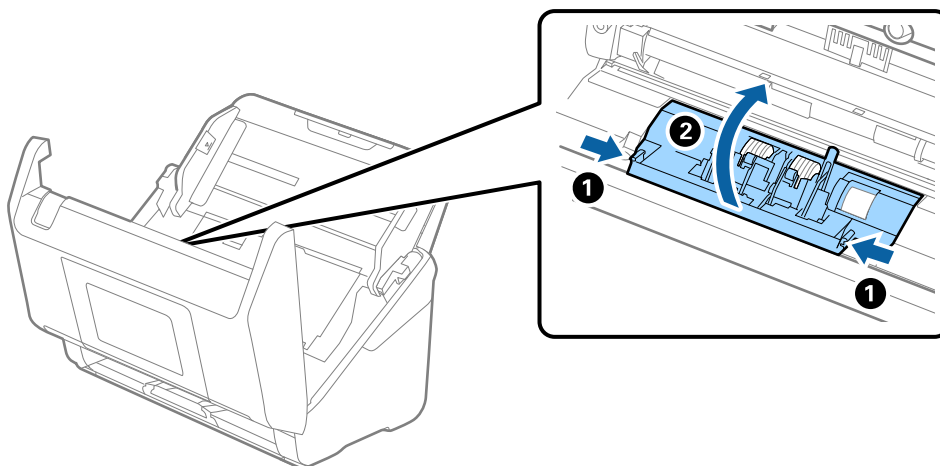


! Oluline teave:

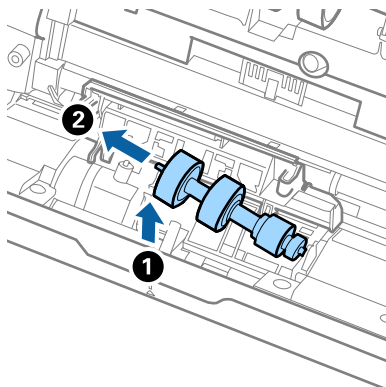
- ❑ Veenduge, et vastuvõturulli kaas on õigesti suletud.
- ❑ Kui kaant on raske sulgeda, kontrollige, kas kogumisrullikud on õigesti paigaldatud.
- ❑ Ärge paigaldage kaant, kui see on üles tõstetud.



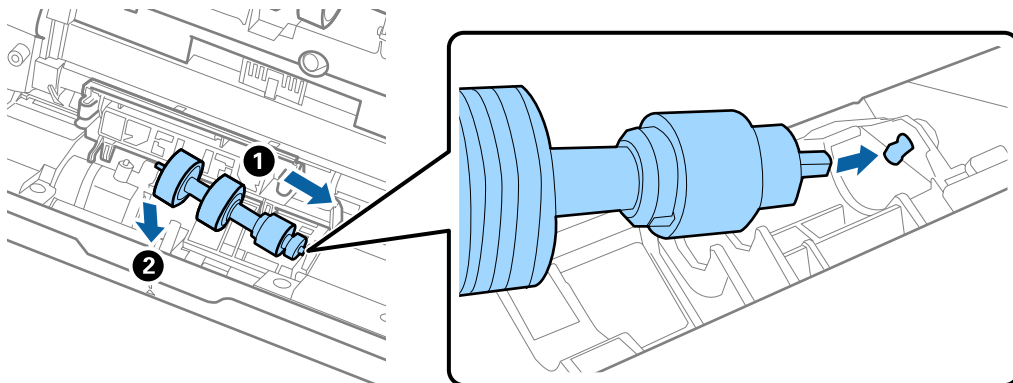
8. Kaane avamiseks suruge eraldusrulli mõlemal otsal olevaid konkse.



9. Tõstke eraldusrulli vasem pool üles, seejärel lükake ja eemaldage paigaldatud eraldusrullid.



10. Sisestage uue eraldusrulli telg paremal pool asuvasse auku, seejärel laske rull alla.



11. Sulgege eraldusrulli kate.



Oluline teave:

Kui kaant on raske sulgeda, veenduge, kas eraldusrullid on õigesti paigaldatud.

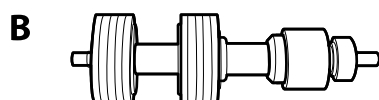
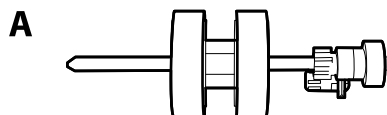
12. Sulgege skanneri kaas.
13. Ühendage vahelduvvooluadapter vooluvõrku ja lülitage skanner sisse.
14. Lähtestage skannide arv juhtpaneelilt.

Märkus.

Vabanege vastuvõturullist ja eraldusrullist kooskõlas kohalike eeskirjadega. Ärge demonteerige neid.

Rulli montaažikomplekti koodid

Osad (vastuvõturrull ja eraldusrull) tuleb vahetada, kui skaneerimiste arv ületab teenindusarvu. Uusimat skaneeritud dokumentide arvu saate vaadata juhtpaneelil või rakenduses Epson Scan 2 Utility.



A: vastuvõturrull, B: eraldusrull

Osa nimi	Koodid	Kasutustsükkel
Rulliku montaažikomplekt 2	B12B819711 B12B819721 (ainult India)	200,000*

* See arv saadi järjestikkusel skaneerimisel Epsoni katseoriginaalpaberitega ja see on vahetustsükli juhiseks. Vahetustsükkel võib olenevalt paberi tüübist erineda. Näiteks rohkelt paberitolmu tekitav paber või karedapinnaline paber võib kasutustsükli lühendada.

Skannide arvu lähtestamine pärast rullikute vahetamist

Pärast rullikoostu vahetamist lähtestage skannide arv juhtpaneelil või rakenduses Epson Scan 2 Utility.

Selles jaotises on kirjeldatud, kuidas lähtestada juhtpaneelilt.

1. Puudutage avakuval nuppu **Skanneri hooldus**.
2. Puudutage nuppu **Rulliku asendamine**.
3. Puudutage nuppu **Lähtesta skannimiste arv**.
4. Valige **Skannitud eksemplaride arv pärast rulliku vahetamist** ja seejärel puudutage valikut **Jah**.

Märkus.

Lähtestamiseks rakendusest Epson Scan 2 Utility käivitage Epson Scan 2 Utility, klõpsake vahekaarti **Loendur** ja seejärel klõpsake nuppu **Lähtesta** jaotises **Rulliku koostekomplekt**.

Seotud teave

➔ „Rulli montaažikomplekti vahetamine” lk 129

Energia säästmine

Energia säästmiseks kasutage unerežiimi või automaatset väljalülitamist, kui skanner ei tee ühtegi toimingut. Saate määrata aja, mille järel skanner läheb puhkerežiimi ja lülitub automaatselt välja. Tõstmine mõjutab toote energiatõhusust. Arvestage muudatuste tegemisel keskkonnaga.


1. Valige avakuval **Sätted**.
2. Valige **Põhisätted**.
3. Valige **Unetaimer** või **Välja lülit. säte** ja määrake seejärel sätted.

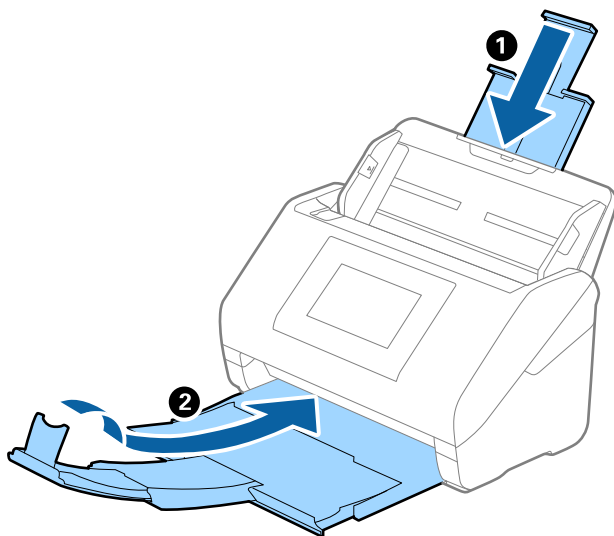
Märkus.

Saadaval funktsioonid võivad olenevalt ostukohast erineda.

Skanneri transportimine

Kui te peate skanneri teise kohta transportima või remonti viima, siis järgige skanneri pakkimiseks alltoodud samme.

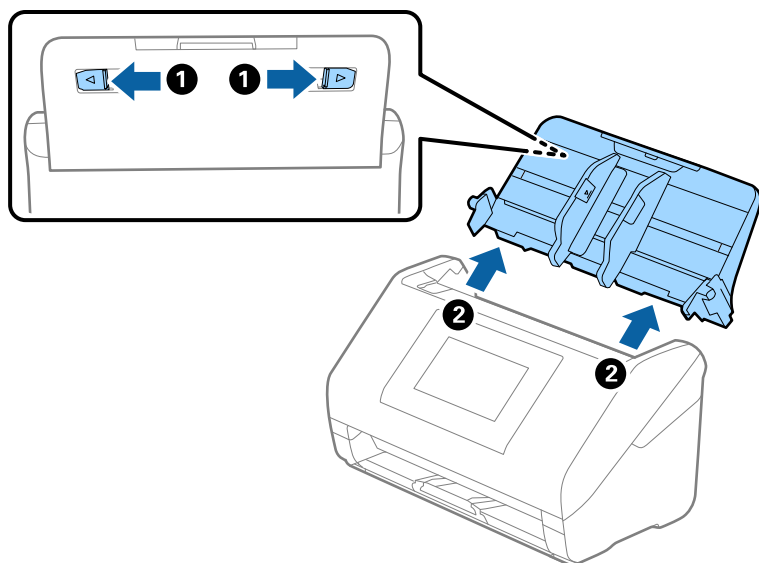
1. Skanneri väljalülitamiseks vajutage nuppu .
2. Ühendage vahelduvvooluadapter elektrivõrgust välja.
3. Eemaldage kaablid ja seadmed.
Eemaldage valikuline või komplekti kuuluv Paper Alignment Plate, kui see on paigaldatud.
4. Sulgege sisestussalve pikendus ja väljastussalv.



Oluline teave:

Sulgege kindlasti väljastussalv turvaliselt, vastasel juhul võib see transportimise ajal viga saada.

5. Eemaldage sisestussalv.



6. Kinnitage skanneriga kaasa tulnud pakkematerjal, seejärel pakkige skanner uuesti originaalkarpi või muusse vastupidavasse karpi.

Sätete varundamine

Te saate eksportida rakenduses Web Config määratud sätteväärtuse failile. Selle abil saate varundada kontakte ja sätteväärtuseid ning skannerit välja vahetada jms.

Eksportitud faili ei ole võimalik redigeerida, sest seda eksportitakse kahendfailina.

Sätete eksportimine

Eksportige skanneri jaoks sätteid.

1. Avage Web Config ja seejärel valige vahekaart **Device Management > Export and Import Setting Value > Export**.

2. Valige sätteid, mida te soovite eksportida.

Valige sätteid, mida soovite eksportida. Kui valite algkategoriat, tuleb valida ka alamkatekoodid. Kuid valida ei saa neid alamkatekoodid, mis põhjustavad dubleerimistõrkeid sama võrgu piires (näiteks IP-aadress jne).

3. Eksportitud faili krüptimiseks sisestage parool.

Faili importimiseks on vajalik parool. Kui te ei taha faili krüptida, jätke see tühjaks.

4. Klõpsake nuppu **Export**.



Oluline teave:

Kui soovite eksportida skanneri võrgusätteid, nagu seadme nimi ja IPv6-aadress, valige **Enable to select the individual settings of device** ja valige rohkem sätteid. Kasutage valitud väärtusi ainult asendusskannerile.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Sätete import

Importige rakendusest Web Config eksporditud fail skannerisse.



Oluline teave:

Individuaalset teavet, nagu näiteks skanneri nimi või IP-aadress, sisaldavate väärtuste importimisel veenduge, et võrgus juba ei ole sama IP-aadressil.

1. Avage Web Config ning valige sakk **Device Management > Export and Import Setting Value > Import**.
2. Valige eksporditud fail ja sisestage seejärel krüptitud parool.
3. Klõpsake nuppu **Next**.
4. Valige imporditavad sätted ja klõpsake **Next**.
5. Klõpsake nuppu **OK**.

Sätted rakendatakse skanneris.

Seotud teave

➔ „Kuidas kasutada veebibrauseris rakendust Web Config” lk 37

Taasta vaikesätted

Valige juhtpaneelil **Sätted > Süsteemi administreerimine > Taasta vaikesätted** ja seejärel valige üksused, mille vaikesätted soovite taastada.

- Võrgusätted: taastage võrguga seotud sätete algolek.
- Kõik peale Võrgusätete: taastage kõigi sätete algolek peale võrguga seotud sätete.
- Kõik sätted: taastage kõigi sätete algolek.



Oluline teave:

Valikuga **Kõik sätted** kustutatakse kõik skanneris registreeritud sätteandmed, kaasa arvatud kontaktid. Kustutatud sätteid ei saa taastada.

Märkus.

Sätteid saate muuta ka rakenduses Web Config.

Vahekaart **Device Management > Restore Default Settings**

Rakenduste ja püsivara värskendamine

Võib-olla saate rakendusi ja püsivara värskendades teatud probleeme lahendada ning funktsioone parandada või lisada. Kasutage kindlasti rakenduste ja püsivara uusimat versiooni.



Oluline teave:

- Ärge lülitage arvutit või skannerit värskendamise ajal välja.

Märkus.

Kui skanner on interneti-ühendusega, saate püsivara värskendada rakenduses Web Config. Valige vahekaart **Device Management** > **Firmware Update**, kontrollige kuvateadet ja klõpsake nuppu **Start**.

1. Veenduge, et skanner ja arvuti oleksid ühendatud ning et arvuti oleks ühendatud internetiga.
2. Käivitage rakendus EPSON Software Updater ja värskendage rakendusi või püsivara.

Märkus.

Operatsioonisüsteemi Windows Server tugi puudub.

- Windows 11

Vajutage nuppu Start ja valige seejärel **Kõik rakendused** > **Epson Software** > **EPSON Software Updater**.

- Windows 10

Klõpsake nuppu Start ja valige seejärel **Epson Software** > **EPSON Software Updater**.

- Windows 8.1 / Windows 8

Sisestage rakenduse nimi otsingu tuumnuppu ja valige seejärel kuvatud ikoon.

- Windows 7

Klõpsake nuppu Start ja valige seejärel **Kõik programmid** või **Programmid** > **Epson Software** > **EPSON Software Updater**.

- Mac OS

Valige **Finder** > **Go** > **Applications** > **Epson Software** > **EPSON Software Updater**.

Märkus.

Kui te ei leia värskendatavat rakendust rakenduste loendist, ei saa te seda EPSON Software Updater iga värskendada. Kontrollige rakenduste viimaste versioonide saadavalolekut oma kohalikul Epsoni veebisaidil.

<http://www.epson.com>

Skanneri püsivara värskendamine juhtpaneeli abil

Kui skanner on interneti ühendatud, saate juhtpaneeli abil skanneri püsivara värskendada. Samuti saate seada skanneri regulaarselt püsivara värskenduse olemasolu kontrollima ja selle leidmise korral teid teavitama.

1. Valige avakuval **Sätted**.
2. Valige **Süsteemi administreerimine** > **Püsivara värskendamine** > **Värskenda**.

Märkus.

Valige **Teatis** > **Sees**, et seada skanner regulaarselt kontrollima, kas püsivarale on olemas värskendus.

3. Lugege ekraanil kuvatud teadet ja alustage värskenduste otsimist.

4. Kui LCD-ekraanil kuvatakse teade, mis kinnitab, et püsivara värskendus on saadaval, järgige värskenduse käivitamiseks ekraanil kuvatud juhtnööre.



Oluline teave:

- Ärge lülitage skannerit välja ega lahutage seda vooluvõrgust enne, kui värskendamine on lõppenud, vastasel korral võib skanneri töös esineda tõrkeid.
- Kui püsivara värskendamist ei viida lõpule või see nurjub, ei käivitu skanner tavapärasel viisil ja skanneri järgmisel sisselülitamisel kuvatakse LCD-ekraanil teade „Recovery Mode“. Selles olukorras peate püsivara arvuti abil uuesti värskendada. Ühendage skanner USB-kaabli abil arvutiga. Kui skanneris on kuvatud „Recovery Mode“, ei saa te püsivara võrguühenduse kaudu värskendada. Avage arvutis Epsoni kohalik veebisait ja laadige seejärel alla skanneri uusim püsivara. Edasiseks tegevuseks leiate juhtnöörid veebisaidilt.

Püsivara värskendamine rakenduses Web Config

Kui skanner on interneti-ühendusega, saate püsivara värskendada rakenduses Web Config.

1. Avage Web Config ja valige vahekaart **Device Management > Firmware Update**.
2. Klõpsake **Start** ja seejärel järgige ekraanil kuvatud juhiseid.

Algab püsivara kontroll ja värskendatud püsivara olemasolu korral kuvatakse püsivara teave.

Märkus.

Püsivara saate värskendada ka utiliidiga *Epson Device Admin*. Püsivara teavet saate visuaalselt kontrollida seadmete loendist. See on kasulik mitme seadme püsivara värskendamiseks. Lisateavet leiate utiliidi *Epson Device Admin* juhendist või spikrist.

Seotud teave

➔ [„Kuidas kasutada veebibrauseris rakendust Web Config“ lk 37](#)

Püsivara värskendamine ilma internetiühendusega

Seadme püsivara saate arvutisse laadida Epsoni veebisaidilt, seejärel ühendage püsivara värskendamiseks USB-kaabli abil seade arvutiga. If you cannot update over the network, try this method.

Märkus.

Enne värskendamist veenduge, et skanneridraiver *Epson Scan 2* oleks arvutisse installitud. Kui *Epson Scan 2* on installimata, installige see.

1. Vaadake uusimaid saadaval püsivara värskendusi Epsoni veebisaidilt.
<http://www.epson.com>
 - Kui seal püsivara teie skannerile, laadige see alla ja jätkake siis järgmisest punktist.
 - Kui veebisaidil pole püsivara kohta teavet, kasutate te juba uusimat püsivara.
2. Ühendage allalaaditud püsivara sisaldav arvuti USB-kaabli abil skanneriga.
3. Topeltklõpsake allalaaditud faili laiendiga *.exe*.
Epson Firmware Updater käivitub.

4. Järgige ekraanil kuvatud juhtnööre.