EPSON

DS-790WN

Administraatori juhend

Teie eesmärgiks vajalikud sätted

Võrgusätted

Nõutud sätted skannimiseks

Põhilised turvasätted

Täpsemad turvalisuse sätted

Authentication Settings

NPD6726-05 ET

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 kasutamisega 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.

© 2022-2026 Seiko Epson Corporation

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

Kaubamärgid

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION ja nende logod on registreeritud kaubamärgid või Seiko Epsoni kaubamärgid.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa ja PaSoRi on ettevõtte Sony Corporation registreeritud kaubamärgid.
- ❏ MIFARE on ettevõtte NXP Semiconductor Corporation registreeritud kaubamärk.
- ❏ Üldmärkus: muid tootenimesid on selles dokumendis kasutatud ainult tuvastamise eesmärgil ja need võivad olla vastavatele omanikele kuuluvad kaubamärgid. Epson ütleb lahti kõigist nende kaubamärkide õigustest.

Sisukord

Autoriõigus

Kaubamärgid

Sissejuhatus

Selle dokumendi sisu. 7
Kasutusjuhendi kasutamine. 7
Märgid ja sümbolid. 7
Käesolevas juhendis kasutatud kirjeldused. 7
Operatsioonisüsteemi viited. 8

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

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 spetsifikatsioonid. 28
Etherneti tehnilised nõuded. 30
Võrgufunktsioonid ja IPv4/IPv6. 30
Turvaprotokoll. 30
Skanneri jaoks pordi kasutamine. 30
Probleemide lahendamine. 32
Võrguga ei saa ühendust luua. 32

Skanneri seadistamise tarkvara

Web Config. 36
Utiliidi Web Config kasutamine veebibrauseris. . 36
Utiliidi Web Config käivitamine Windowsis. . . . 37
Epson Device Admin. 37
Konfiguratsioonimall. 37

Nõutud sätted skannimiseks

Meiliserveri registreerimine. 42
Suvandi SMTP AUTH lubamine teenuses Exchange Online. 43
Meiliserveri autentimismeetodi OAuth2.0 seadistamine. 43
Meiliserveri ühenduse kontrollimine. 45
Jagatud võrgukausta sätted. 47
Jagatud kausta loomine. 47
Kontaktide kättesaadavaks tegemine. 63
Kontaktide konfiguratsiooni võrdlus. 64
Sihtkoha registreerimine kontaktide hulka utiliidi Web Config abil. 64
Sihtkohtade registreerimine rühmana Web Config kaudu. 66
Kontaktide varundamine ja importimine. 67
Kontaktide eksportimine ja hulgiregistreerimine tööriista abil. 68
Koostöö LDAP-serveri ja kasutajate vahel. 69
Funktsiooni Document Capture Pro Server kasutamine. 72
Serverirežiimi määramine. 73
Funktsiooni AirPrint seadistamine. 73
Probleemid võrguskannimise ettevalmistamisega. . . 73
Nõuandeid probleemide lahendamiseks. 73
Utiliiti Web Config ei õnnestu avada. 74
Teenusega Microsoft Exchange Online ei saa skannitud kujutisi meilile saata. 75

Juhtpaneeli ekraani kohandamine

Registreerimine: Eelsätted. 79
Menüüsuvandid: Eelsätted. 80
Juhtpaneeli avakuva redigeerimine. 81
Avakuva Paigutusi muutmine. 81
Lisa ikoon. 82
Eemalda ikoon. 83
Teisalda ikoon. 84

Põhilised turvasätted

Toote turvalisuse funktsioonide juhend. 87
Administraatori sätted. 87
Seadistage administraatori parool. 87
Funktsiooni Lukustamise sätted kasutamine juhtpaneelil. 89
Juhtpaneelilt administraatorina sisselogimine. . . 92
Välise liidese keelamine. 93
Kaugskanneri jälgimine. 94
Kaugskanneri teabe vaatamine. 94
Meiliteavituste saamine sündmuste toimumisel. . 94
Probleemide lahendamine. 95
Administraatori parool on ununenud. 95

Täpsemad turvalisuse sätted

Turvalisuse sätted ja ohtude vältimine. 97
Turvalisuse sätted. 98
Juhtimine protokollidega. 98
Juhtimisprotokollid. 98
Protokollid, mida saate lubada või keelata. 98
Protokolli sätteüksused. 99
Digitaalsertifikaadi kasutamine. 101
Digitaalsest sertimisest. 101
CA-signed Certificate seadistamine. 101
Iseallkirjastatud sertifikaadi värskendamine. . . . 105
CA Certificate seadistamine. 105
SSL/TLS-side skanneriga. 106
SSL/TLS põhisätete seadistamine. 106
Skannerile serveri sertifikaadi konfigureerimine 107
Krüptitud side IPsec/IP-filtreerimisega. 107
Teave rakenduse IPsec/IP Filtering kohta. 107
Vaikepoliitika konfigureerimine. 107
Rühmapoliitika konfigureerimine. 111
IPsec/IP Filtering konfiguratsiooni näited. 117
IPsec/IP-filtrimine sertifikaadi seadistamine. . . 118
Skanneri ühendamine IEEE802.1X-võrguga. 118
IEEE 802.1X-võrgu konfigureerimine. 118
IEEE 802.1X sertifikaadi seadistamine. 120
Täpsemate turvasätetega seotud probleemide lahendamine. 120
Turvasätete taastamine. 120
Probleemid võrgu turvafunktsioonide kasutamisel. 120
Probleemid digitaalsertifikaadi kasutamisel. . . . 122

Authentication Settings

Authentication Settings: info. 128
Authentication Settings: saadaval funktsioonid. 128
Authentication Method: info. 129
Seadistamise tarkvara. 131
Skanneri püsivara värskendamine. 131
Autentimisseadme ühendamine ja konfigureerimine. 131
Ühilduvate kaardilugejate loend. 131
Autentimisseadme ühendamine. 134
Autentimisseadme sätted. 135
Teabe registreerimine ja seadistamine. 136
Seadistamine. 136
Autentimise lubamine. 137
Authentication Settings. 137
User Settings: registreerimine. 139
Sünkroonimine üksusega LDAP Server. 145
Meiliserveri seadistamine. 148
Funktsiooni Scan to My Folder seadistamine. . . 149
Customize One-touch Functions. 151
Aruanded Job History rakenduses Epson Device Admin. 152
Üksused, mille saab aruandesse lisada. 152
Juhtpaneelilt administraatorina sisselogimine. . . . 152
Funktsiooni Authentication Settings keelamine. . . 152
Funktsiooni Authentication Settings teabe kustutamine (Taasta vaikesätted). 153
Probleemide lahendamine. 153
Autentimiskaardi lugemine ei õnnestu. 153

Hooldamine

Skanneri korpuse puhastamine. 155
Skanneri sisemuse puhastamine. 155
Rulli montaažikomplekti vahetamine. 160
Rulli montaažikomplekti koodid. 165
Skannide arvu lähtestamine. 165
Energia säästmine. 165
Skanneri transportimine. 166
Sätete varundamine. 167
Sätete eksportimine. 167
Sätete import. 168
Taasta vaikesätted. 168
Rakenduste ja püsivara värskendamine. 168
Skanneri püsivara värskendamine juhtpaneeli abil. 169
Püsivara värskendamine rakenduses Web Config. 170
Püsivara värskendamine ilma internetiühenduseta. 170

Sissejuhatus

Selle dokumendi sisu. 7

Kasutusjuhendi kasutamine. 7

Selle dokumendi sisu

See dokument sisaldab skanneri administraatorite jaoks järgmist teavet.

❏ Võrgusätted

❏ Skannimisfunktsiooni ettevalmistamine

❏ Turvasätete lubamine ja haldamine

❏ Funktsiooni Authentication Settings lubamine ja haldamine

❏ Igapäevase hoolduse tegemine

Skanneri standardseid kasutusmeetodeid vaadake dokumendist *Kasutusjuhend*.

Märkus.
See dokument kirjeldab funktsiooni Authentication Settings kasutamist iseseisvaks autentimiseks ilma autentimisserverita. Lisaks selles juhendis kirjeldatud funktsioonile Authentication Settings saate luua autentimissüsteemi ka autentimisserveri abil. Süsteemi loomiseks kasutage rakendust Document Capture Pro Server Authentication Edition (lühendatud nimega Document Capture Pro Server AE).

Lisateabe saamiseks võtke ühendust kohaliku Epsoni esindusega.

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.

Operatsioonisüsteemi viited

Windows

Selles juhendis viitavad terminid „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Server 2019“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“ ja „Windows Server 2008 R2“ järgmistele operatsioonisüsteemidele. Lisaks kasutatakse terminit „Windows“ kõigi versioonide kohta ja terminit „Windows Server“ operatsioonisüsteemide „Windows Server 2019“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“ ja „Windows Server 2008 R2“ kohta.

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

Mac OS

Käesolevas juhendis viitab „Mac OS“ operatsioonisüsteemidele macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan ja OS X Yosemite.

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 soovitame 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 ühebaidilisi tärke.

Administraatori parooli lähtestamine

Administraatori parooli saate algsättele 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 42 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 63
Tahan skannitud pildid võrgukausta salvestada. (Scan to Network Folder/FTP)	1. Looge võrku kaust, kuhu tahate pildid salvestada. „Jagatud võrgukausta sätted" lk 47 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 63
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 kuva kohandamine

Eesmärk	Nõutud sätted
Tahan muuta skanneri juhtpaneelil kuvatud üksusi.	Seadistage **Eelsätted** või **Muuda avakuva**. Saate oma lemmik skannimissätted registreerida juhtpaneelil ja redigeerida kuvatud üksusi. „Juhtpaneeli ekraani kohandamine" lk 78

Põhiliste turvafunktsioonide seadistamine

Eesmärk	Nõutud sätted
Tahan takistada skanneri sätete muutmist kõigil peale administraatori.	Määrake skannerile administraatori parool. „Administraatori sätted" lk 87
Tahan keelata skannerite kasutamise USB-ühenduse kaudu.	Keelake välisliides. „Välise liidese keelamine" lk 93

Täpsemate turvafunktsioonide seadistamine

Eesmärk	Nõutud sätted
Tahan omada kontrolli kasutatavate protokollide üle.	Lubage või keelake protokollid. „Juhtimine protokollidega" lk 98
Tahan krüptida sidetee.	1. Seadistage digisert. „Digitaalsertifikaadi kasutamine" lk 101 2. Seadistage SSL-/TLS-andmeside. „SSL/TLS-side skanneriga" lk 106
Tahan kasutada krüptitud andmesidet (IPsec). Tahan, et tarkvara saaks kasutada ainult kindlast arvutist (IP-filtrimine).	Seadistuspoliitikad liikluse filtrimiseks. „Krüptitud side IPsec/IP-filtreerimisega" lk 107
Tahan kasutada skannerit IEEE802.1X-võrgus.	Seadistage skannerile IEEE802.1X. „Skanneri ühendamine IEEE802.1X-võrguga" lk 118

Skanneriga autenditavate funktsioonide määramine

Eesmärk	Nõutud sätted
Tahan lubada funktsiooni Authentication Settings.	Vt järgmist, et saada lisateavet funktsioonide Authentication Settings ja Authentication Method kohta. „Authentication Settings: info" lk 128 „Authentication Method: info" lk 129

Serveri autentimissüsteemi kasutamine

Rakendusega Document Capture Pro Server Authentication Edition (lühidalt Document Capture Pro Server AE) saate luua autentimissüsteemi, mis kasutab autentimiseks serverit.

Lisateabe saamiseks võtke ühendust kohaliku Epsoni esindusega.

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 skanner ja arvuti on samas võrgusegmendis, võite ühendamiseks kasutada ka installerit.

❏ *Seadistamine veebisaidilt*

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

http://epson.sn

❏ *Seadistamine tarkvaraketta abil (ainult mudelid, millega on kaasas tarkvaraketas, ja kasutajad, kellel on operatsioonisüsteemiga Windows arvuti, millel on kettadraiv).*

Sisestage tarkvaraketas arvutisse ja järgige ekraanil olevaid juhtnööre.

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	❏ Ethernet ❏ 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	❏ IP-aadress ❏ Alamvõrgumask ❏ 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	❏ SSID ❏ 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	❏ Peamise DNS-i IP-aadress ❏ 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	❏ 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. ❏ Epson Connecti teenused ❏ Muude ettevõtete pilveteenused ❏ Püsivara värskendamine ❏ Skannitud kujutiste saatmine SharePointi (WebDAV)
Pordinumbri teave	❏ Pordinumber avamiseks	Kontrollige skanneri ja arvuti kasutatavat pordinumbrit ja seejärel avage vajaduse korral tulemüüriga blokeeritud port. Skanneri kasutatava pordinumbri kohta lugege allpool. „Skanneri jaoks pordi kasutamine" lk 30

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 soovitame 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 soovitame 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 **Käsitsi** või **Automaatne** alt valida DNS-serveri sätted. Kui DNS-serveri aadressi ei saa automaatselt hankida, valige **Käsitsi** 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 **Sätted**.

   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 sätted**.

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 sätted 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 sätted määrata käsitsi.

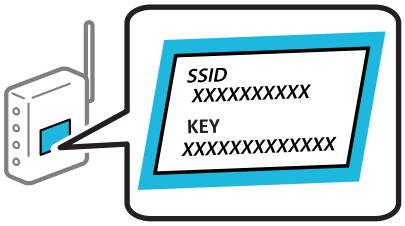
Kui ruuter toetab ainult WPS-i, saate sätted määrata surunupuga seadistamise abil.

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

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 selle vaikesätetega, on SSID ja parool andmesildil. 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 **Lülituge ümber Wi-Fi-ühendusele.** või **Muuda sätteid**, et muuta sätteid.
4. Valige **Wi-Fi häälestusviisard**.
5. Järgige SSID valimiseks ekraanil kuvatud juhiseid, 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. Andmesildil võib parool olla kirjutatud väljale „Network Key“, „Wireless Password“ vms. Kui kasutate juhtmevaba pääsupunkti vaikesätetega, kasutage andmesildile kirjutatud parooli.*

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 **Lülituge 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 **Lülituge 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. Installerit saab käivitada ühega järgmistest meetoditest.

❏ Seadistamine veebisaidilt

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

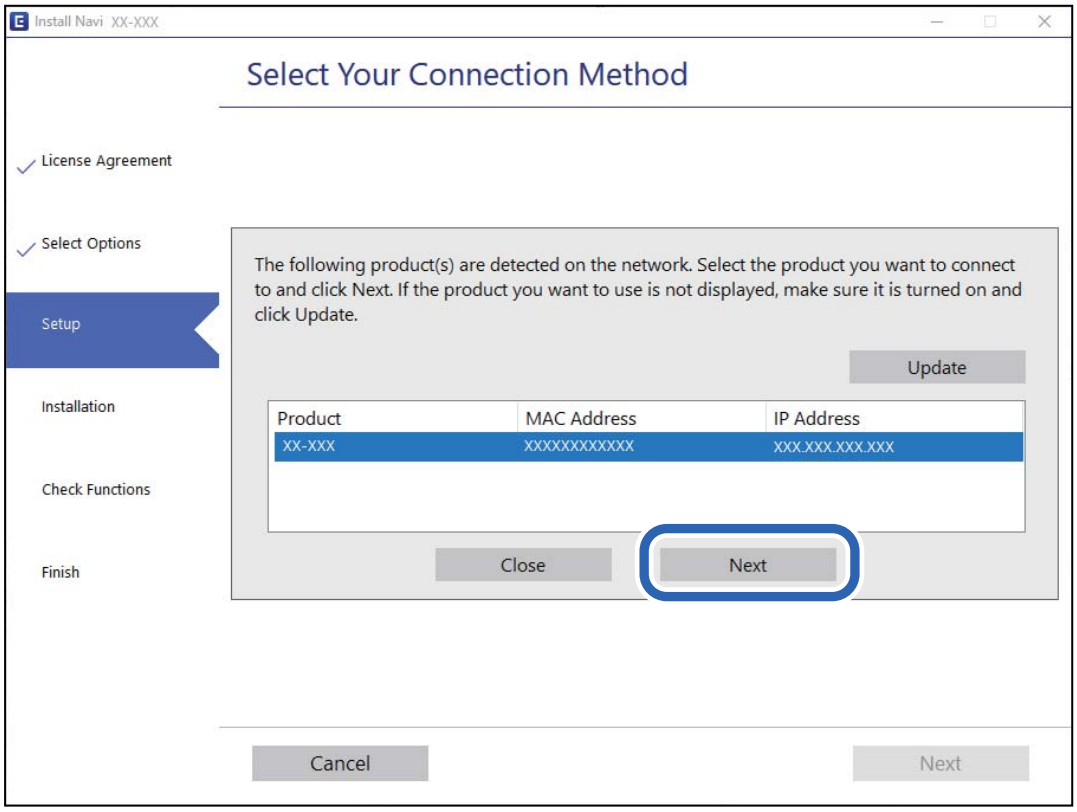
http://epson.sn

❏ Seadistamine tarkvaraketta abil (ainult mudelid, millega on kaasas tarkvaraketas, ja Windows arvutid, millel on kettadraiv).

Sisestage tarkvaraketas arvutisse ja järgige ekraanil olevaid juhtnööre.

Skanneri valimine

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



Järgige ekraanil olevaid 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.

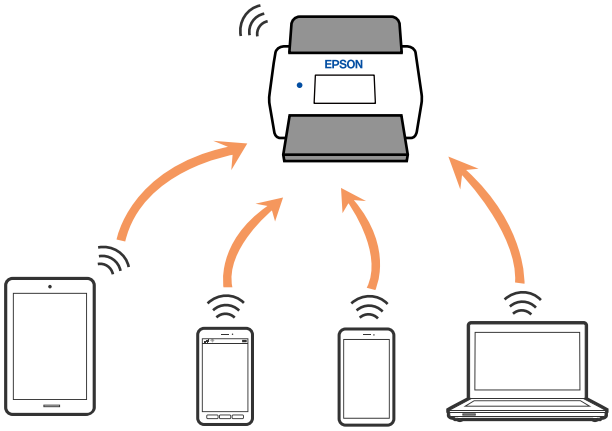
„Nutiseadme ja skanneri otse ühendamine (Wi-Fi Direct)” lk 23

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-Fit 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-Figa, 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 muutmine

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-tärkide 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-tärkide 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 muutmine 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.
Alljärgnevate 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. Installerit saab käivitada ühega järgmistest meetoditest.

- ❏ Seadistamine veebisaidilt

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

  http://epson.sn
- ❏ Seadistamine tarkvaraketta abil (ainult mudelid, millega on kaasas tarkvaraketas, ja Windows arvutid, millel on kettadraiv).

  Sisestage tarkvaraketas arvutisse ja järgige ekraanil olevaid juhtnööre.

Ühendusviisi valimine

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

Järgige häälestuse lõpetamiseks ekraanil olevaid 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 toote nimi. Valige **Häälestus** ja alustage seadistamist.

http://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 saab käivitada järgmise meetodi abil.

❏ Seadistamine veebisaidilt

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

http://epson.sn

❏ Seadistamine tarkvaraketta abil (ainult mudelid, millega on kaasas tarkvaraketas, ja Windows arvutid, millel on kettadraiv).

Sisestage tarkvaraketas arvutisse ja järgige ekraanil olevaid juhtnööre.

Järgige ekraanil olevaid 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.

❏ Seadistamine veebisaidilt

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

http://epson.sn

❏ Seadistamine tarkvaraketta abil (ainult mudelid, millega on kaasas tarkvaraketas, ja Windows arvutid, millel on kettadraiv).

Sisestage tarkvaraketas arvutisse ja järgige ekraanil olevaid juhtnööre.

Ühendusmeetodi muutmise valimine

Järgige ekraanil olevaid juhtnööre. Valige kuval **Valige oma toiming** 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 olevaid 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.

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

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 spetsifikatsioonid

Järgmisest tabelist leiate Wi-Fi tehnilised andmed.

Riigid või piirkonnad, v.a. need, mis on kirjas all	Tabel A

Austraalia Uus-Meremaa Taiwan Lõuna-Korea	Tabel B

Tabel A

Standardid	IEEE 802.11b/g/n*1
Sagedusvahemik	2,4 GHz
Maksimaalne edastatav raadiosageduslik võimsus	2400–2483,5 MHz: 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 poolduplekse, 100 Mbps täisdupleksne, 100 Mbps poolduplekse
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 IPv4/IPv6

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

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
		NetBIOS (TCP)	139
	WebDAV-server	Protokoll HTTP (TCP)	80
		Protokoll HTTPS (TCP)	443
Meilimine (kui skannerist kasutatakse meilile skannimise funktsiooni)	SMTP-server	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP- enne SMTP-ühendust (kui skannerist kasutatakse meilile skannimise funktsiooni)	POP-server	POP3 (TCP)	110
Teenuse Epson Connect kasutamisel	Epson Connecti server	HTTPS	443
		XMPP	5222
Kasutajateabe kogumine (kasutatakse skanneri kontakte)	LDAP-server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
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 tõukeskannimist rakendusest	Klientarvuti	Võrgu avastamine tõukeskannimisega	2968

Kui saatja (klient) on klientarvuti

Kasutus	Siht (server)	Protokoll	Pordinumber
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

Kasutus	Siht (server)	Protokoll	Pordinumber
WSD-skanneri otsimine	Skanner	WS-Discovery (UDP)	3702
Skanniandmete edastamine rakendusest	Skanner	Võrguskannimine (TCP)	1865
Tööteabe kogumine, kui kasutate tõukeskannimist rakendusest	Skanner	Võrgu tõukeskannimine	2968
Web Config	Skanner	HTTP (TCP)	80
		HTTPS (TCP)	443

Probleemide lahendamine

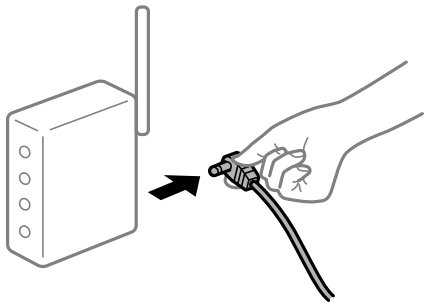
Võrguga ei saa ühendust luua

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

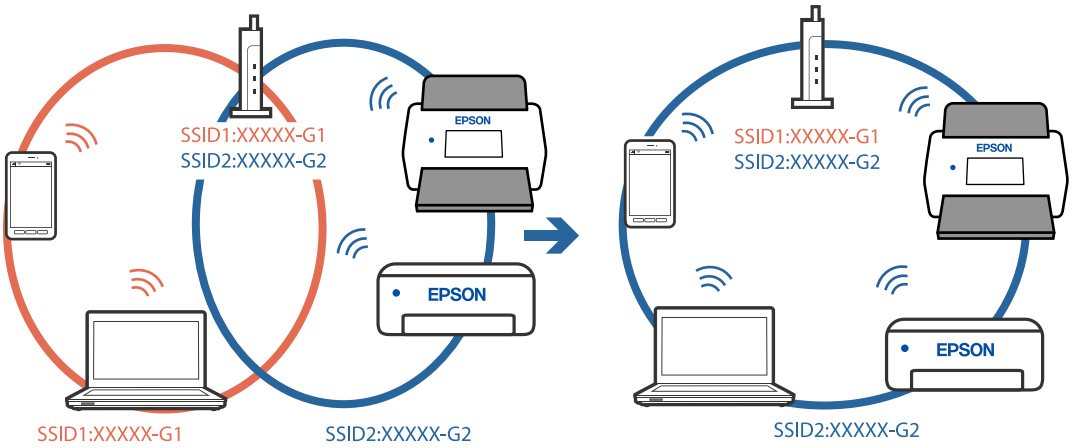
Tehke ühenduse seaded uuesti, et need vastaksid uuele juhtmeta ruuterile.

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-aadrss 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.

   „Utiliidi Web Config kasutamine veebibrauseris” lk 36
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

Web Config. 36

Epson Device Admin. 37

Web Config

Web Config on rakendus, mis töötab arvuti veebibrauserites, nagu Microsoft Edge ja Safari. Saate kontrollida skanneri olekut või muuta võrguteenuseid ja skanneri sätteid. Kuna skanneritega tehakse toiminguid otse võrgus, sobib see korraga ühe skanneri häälestamiseks. Ühendage rakenduse Web Config kasutamiseks oma arvuti skanneriga 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 74

Utiliidi Web Config kasutamine veebibrauseris

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.

2. Avage arvutis või nutiseadmes veebibrauser ja sisestage sellesse skanneri IP-aadress.

   Vorming:

   IPv4: http://skanneri IP-aadress/

   IPv6: http://[skanneri IP-aadress]/

   Näide:

   IPv4: http://192.168.100.201/

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

   Märkus.
   Kuna skanner kasutab HTTPS-aadressile pöördumiseks iseallkirjastatud sertifikaati, kuvatakse rakenduse Web Config käivitamisel brauseris hoiatus. See ei viita probleemile ja seda võib ohutult ignoreerida.

3. Skanneri sätete muutmiseks logige sisse kui administraator.

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

   Märkus.
   - *Allpool on toodud rakenduse Web Config administraatori teabe algväärtused.*

     ·Kasutajanimi: puudub (tühi)

     ·Parool: oleneb toote tagaküljele 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 ekraanil on üleval paremal kuvatud **Log out**, olete juba administraatorina sisse logitud.*
   - *Teid logitakse automaatselt välja, kui ligikaudu 20 minutit pole tehtud ühtegi toimingut.*

Utiliidi Web Config käivitamine Windowsis

Kui ühendate arvuti skanneriga, kasutades WSD-d, järgige allpool toodud samme utiliidi Web Config käivitamiseks.

1. Avage arvutis skannerite loend.
   - ❏ Windows 10

     Klõpsake nuppu Start ja valige **Windowsi süsteem** > **Juhtpaneel** > **Kuva seadmed ja printerid** jaotisest **Riistvara ja heli**.
   - ❏ Windows 8.1/Windows 8

     Valige **Riistvara ja heli** (või **Riistvara**) alt **Töölaud** > **Sätted** > **Juhtpaneel** > **Kuva seadmed ja printerid**.
   - ❏ Windows 7

     Klõpsake nuppu Start ja valige **Riistvara ja heli** alt **Juhtpaneel** > **Kuva seadmed ja printerid**.
2. Tehke skanneril paremklõps ja valige **Atribuudid**.
3. Valige vahekaart **Veebiteenus** ja klõpsake URL-i.

   Kuna skanner kasutab HTTPS-aadressile pöördumiseks iseallkirjastatud sertifikaati, kuvatakse rakenduse Web Config käivitamisel brauseris hoiatus. See ei viita probleemile ja seda võib ohutult ignoreerida.

   Märkus.
   - ❏ *Allpool on toodud rakenduse Web Config administraatori teabe algväärtused.*

     ·Kasutajanimi: puudub (tühi)

     ·Parool: oleneb toote tagaküljele 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 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.

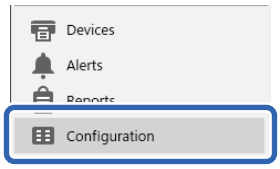
Konfiguratsioonimall

Konfiguratsioonimalli loomine

Looge uus konfiguratsioonimall.

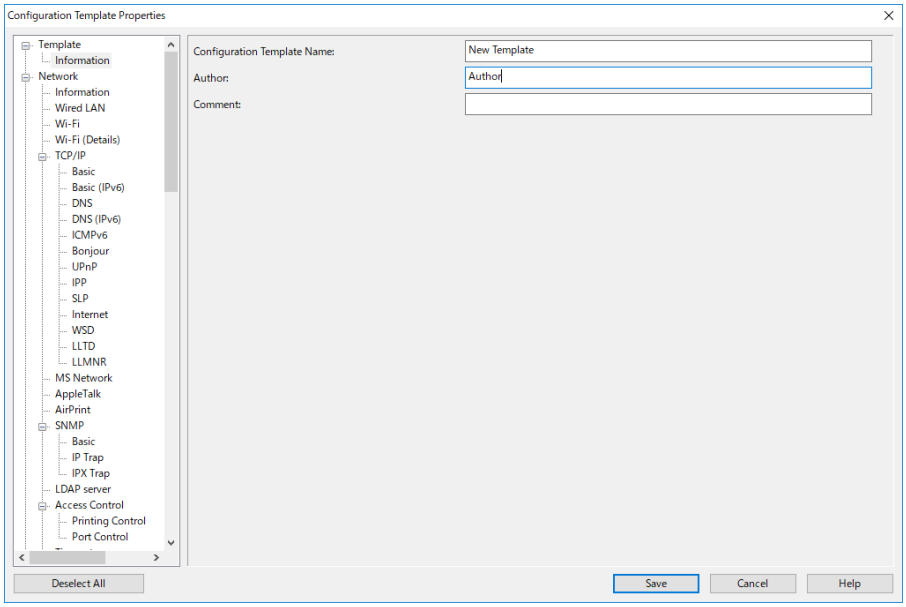
1. Käivitage Epson Device Admin.

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

5. 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 loobumisnuppu 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.

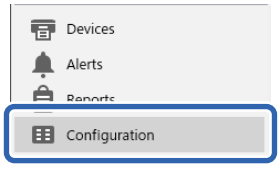
*1. Valige seadmeloendi ribamenüüs: **Options** > **Password manager**.*

*2. Valige **Enable automatic password management** ja klõpsake seejärel nuppu **Password manager**.*

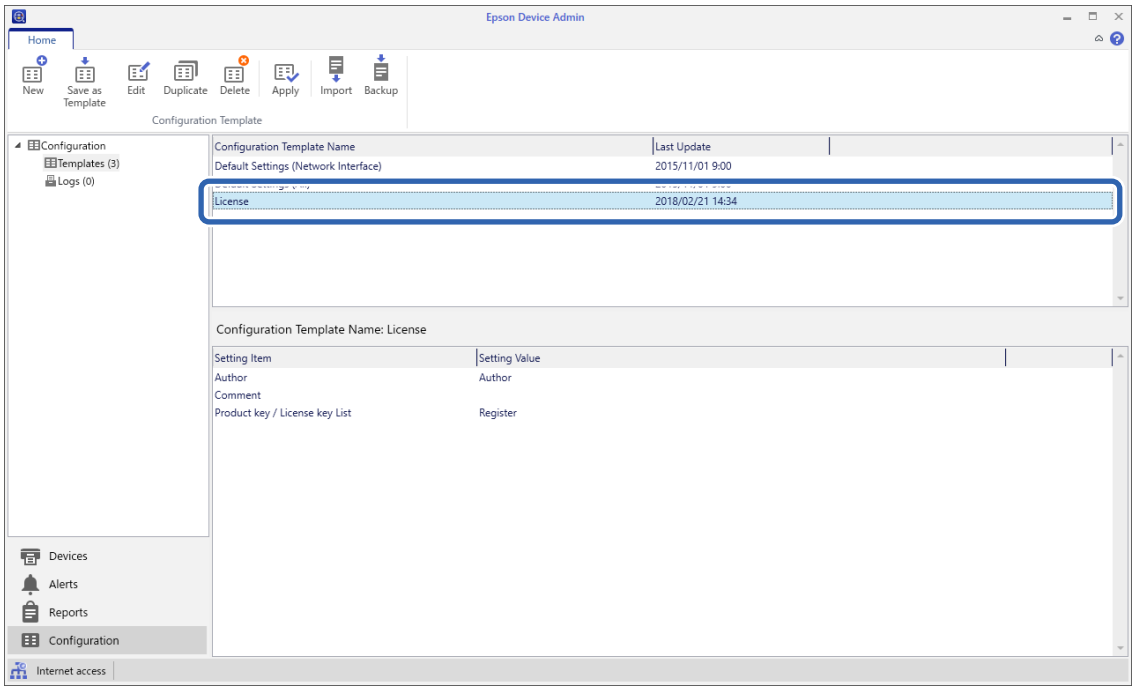
*3. Valige asjakohane skanner ja klõpsake seejärel nuppu **Edit**.*

*4. Seadistage parool ja klõpsake seejärel nuppu **OK**.*

1. Valige külgriba tegumimenüüst **Configuration**.



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



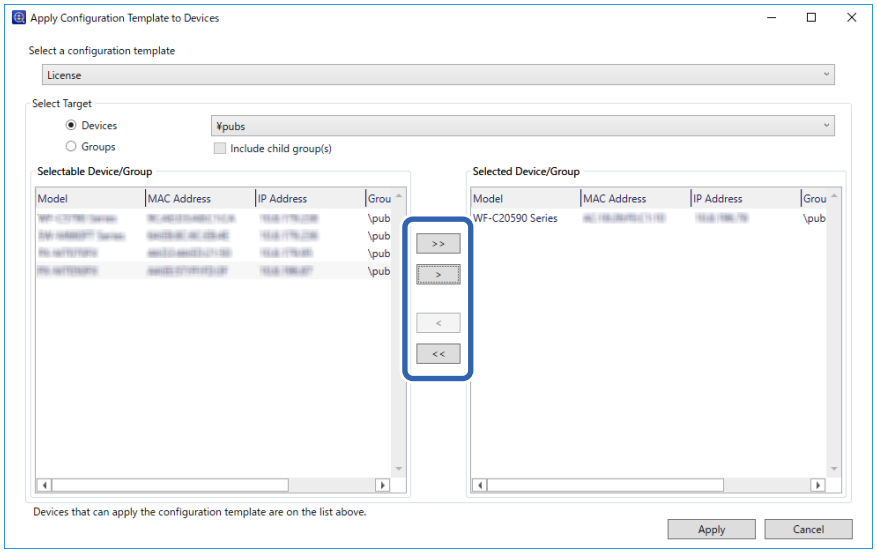
3. Klõpsake ribamenüüs nuppu **Apply**.

   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.*

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



6. Klõpsake nuppu **Apply**.

   Kuvatakse rakendatava konfiguratsioonimalli kinnituskuva.

7. Klõpsake konfiguratsioonimalli rakendamiseks nuppu **OK**.

8. Kui kuvatakse teade, mis ütleb, et protseduur on lõpetatud, klõpsake nuppu **OK**.

9. Klõpsake nuppu **Details** ja lugege läbi kuvatud teave.

   Kui rakendatud üksustel kuvatakse , on rakendamine edukalt lõpetatud.

10. Klõpsake nuppu **Close**.

Nõutud sätted skannimiseks

Meiliserveri registreerimine. 42

Jagatud võrgukausta sätted. 47

Kontaktide kättesaadavaks tegemine. 63

Funktsiooni Document Capture Pro Server kasutamine. 72

Funktsiooni AirPrint seadistamine. 73

Probleemid võrguskannimise ettevalmistamisega. 73

Meiliserveri registreerimine

Enne meiliserveri konfigureerimist kontrollige järgmist.

❏ Skanner on võrku ühendatud

❏ Meiliserveri häälestusteave

Kui kasutate veebipõhist meiliserverit, saate sätteteabe teenusepakkujalt või veebisaidilt.

Registreerimine

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

„Utiliidi Web Config kasutamine veebibrauseris" lk 36

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

Meiliserveri sätteüksused

Üksus	Sätted ja selgitused	
Authentication Method	Juurdepääsuks meiliserverile valige skanneri autentimismeetod. **Kui kasutate teenust Microsoft Exchange Online.** Teenuse Microsoft Exchange Online täiustatud turvameetmete pole varem kasutusel olnud elementaarautentimine enam saadaval ja SMTP-autentimine (SMTP AUTH) on vaikimisi keelatud. Seega tuleb edaspidi meiliteenuse kasutamiseks kasutada autentimismeetodit **OAuth2**. Kui kasutate skanneri meilisaatmise/meiliteavituse funktsiooni, konfigureerige meiliserveri sätted autentimismeetodi **OAuth2** kasutamiseks. Lisaks tuleb lubada SMTP AUTH teenuses Exchange Online. „Suvandi SMTP AUTH lubamine teenuses Exchange Online" lk 43	
	Off	Autentimine on meiliserveriga suhtlemisel keelatud.
	SMTP AUTH	Meiliserver peab toetama SMTP-autentimist.
	POP before SMTP	Kui valite selle üksuse, siis määrake POP3-server.
	OAuth2	Kui valite selle üksuse, siis määrake Email service.
Email service	Kui **OAuth2** on määratud suvandi **Authentication Method** sätteks, valige meiliteenus ripploendist. Klõpsake nuppu **Sign In** ja järgige ekraanil kuvatud juhtnööre sisselogimiseks meiliteenusesse. „Meiliserveri autentimismeetodi OAuth2.0 seadistamine" lk 43 ***Märkus.*** *Isiklikuks kasutuseks valige* ***Outlook.com****.*	
Authenticated Account	Kui **SMTP AUTH** või **POP before SMTP** on määratud suvandi **Authentication Method** sätteks, tuleb sisestada autenditud 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 autenditud parool. Sisestage 0 kuni 70 tärki ASCII-vormingus (0x20–0x7E).	

Üksus	Sätted ja selgitused	
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 kuni 255 tärki: A–Z, a–z, 0–9. - . Võite kasutada vormingut IPv4 või FQDN.	
SMTP Server Port Number	Sisestage arv vahemikus 1 kuni 65535.	
Secure Connection	Määrake meiliserveri turvalise ühenduse meetod.	
	None	Kui **POP before SMTP** määratakse suvandi **Authentication Method** sätteks, määratakse ühendusmeetodiks **None**.
	SSL/TLS	See on saadaval, kui suvandi **Authentication Method** säte on **Off** või **SMTP AUTH**.
	STARTTLS	See on saadaval, kui suvandi **Authentication Method** säte on **Off** või **SMTP AUTH**.
Certificate Validation (ainult Web Config)	Kui see on lubatud, kontrollitakse sertifikaati. Soovitame kasutada sätet **Enable**, kui suvandi **Secure Connection** säte on miski muu kui **None**.	
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. Võite kasutada vormingut IPv4 või FQDN.	
POP3 Server Port Number	Seadistage, kui **POP before SMTP** on määratud suvandi **Authentication Method** sätteks. Sisestage arv vahemikus 1 kuni 65535.	

Suvandi SMTP AUTH lubamine teenuses Exchange Online

Tooted kasutavad meilide saatmiseks protokolli SMTP, seega tuleb teil lubada SMTP AUTH teenuses Exchange Online.

Täpsed juhtnöörid leiate veebisaidilt Microsoft Learn.

Seadistamine

❏ Keelake teenuse **Exchange administreerimiskeskuses turbe vaikesätted** kogu organisatsiooni jaoks ja lubage SMTP AUTH.

❏ Lubage teenuse **Microsoft 365 administreerimiskeskuses** SMTP AUTH toote administraatori postkasti jaoks.

Meiliserveri autentimismeetodi OAuth2.0 seadistamine

Kasutage rakendust Web Config, et konfigureerida meiliserveri autentimismeetod OAuth 2.0.

1. Avage Web Config.

   „Utiliidi Web Config kasutamine veebibrauseris” lk 36

2. Valige vahekaart **Network** > **Email Server** > **Basic**.

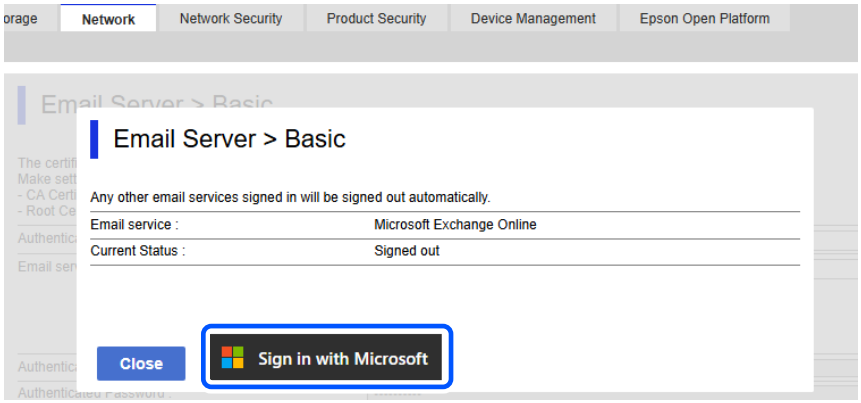
3. Valige **OAuth2** suvandi **Authentication Method** sätteks.

4. Valige **Microsoft Exchange Online** suvandi **Email service** sätteks.

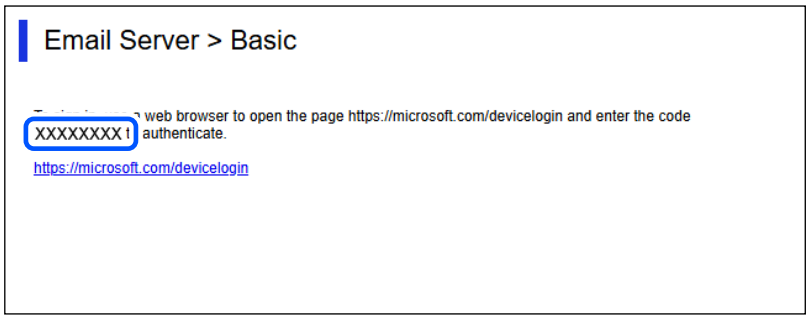
   Märkus.
   *Isiklikuks kasutuseks valige **Outlook.com**.*

5. Logige sisse.

   Klõpsake nuppu **Sign In** ja seejärel klõpsake avanevas aknas **Sign in with Microsoft**.



6. Kopeerige ekraanil kuvatud autentimiskood ja seejärel klõpsake autentimisakna avamiseks kuvatud URLi.



7. Sisestage autentimiskoodi sisestuskuval kopeeritud kood ja klõpsake nuppu **Next**.

8. Sisestage Microsofti sisselogimisaknas oma konto andmed ja klõpsake nuppu **Next**.

   Sisselogimiseks peab kontole olema määratud vähemalt **pilvrakenduse administraatori** roll.

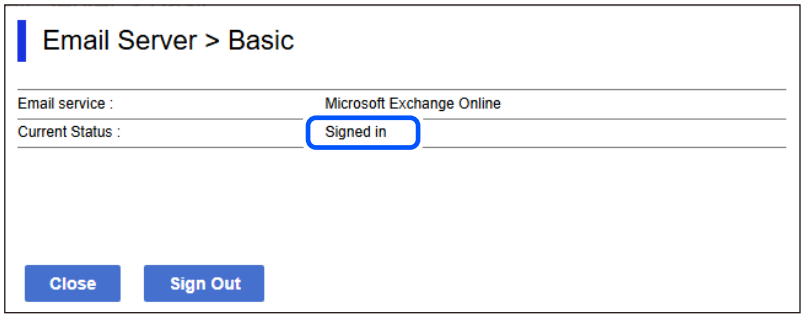
9. Sisestage parool ja klõpsake nuppu **Sign In**.

   Märkus.
   Kui sisselogimine nõuab lisatoiminguid, järgige ekraanil kuvatud juhtnööre.

10. Valige avanevas aknas nõustumine organisatsiooni nimel ja klõpsake nuppu **Nõustu**.

    Kui autentimine on lõpetatud, kuvatakse sisselogimisteade ja te saate brauseriakna sulgeda.

Sisselogimise oleku vaatamiseks valige vahekaart **Network** > **Email Server** > leht **Basic** rakenduses Web Config.



Kui olekunäit on **Signed in**, kuvatakse autentimismeetodi OAuth 2.0 konto andmed.

11. Klõpsake nuppu **OK**, et saata autentimismeetodi OAuth 2.0 sätteteave tootesse.

Meiliserveri ühenduse kontrollimine

Meiliserveri ühenduse kontrollimiseks tehke ühenduse kontroll.

1. Sisestage brauserisse skanneri IP-aadress ja käivitage Web Config.
2. Sisestage administraatori parool, et administraatorina sisse logida.
3. Valige järgmises järjestuses.

   Vahekaart **Network** > **Email Server** > **Connection Test**
4. Valige **Start**.

   Algab meiliserveri ühenduse kontroll. Pärast kontrolli kuvatakse kontrolli aruanne.

   Märkus.
   Ühendust meiliserveriga saab kontrollida ka juhtpaneelilt. Juurdepääs on järgmine.

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

Meiliserveri ühendustesti viited

Teated	Põhjus
Connection test was successful.	See teade kuvatakse, kui ühendus serveriga on loodud.
SMTP server communication error. Check the following. - Network Settings	See teade kuvatakse alljärgnevatel juhtudel ❏ Skanner ei ole ühendatud võrku ❏ SMTP-server on maas ❏ Võrguühendus on side ajal katkenud ❏ Vastu on võetud ebatäielikud andmed

Teated	Põhjus
POP3 server communication error. Check the following. - Network Settings	See teade kuvatakse alljärgnevatel juhtudel ❏ Skanner ei ole ühendatud võrku ❏ POP3-server on maas ❏ Võrguühendus on side ajal katkenud ❏ 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 ❏ DNS-serveriga ühenduse loomine on nurjunud ❏ SMTP-serveri nimelahendus on nurjunud
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	See teade kuvatakse alljärgnevatel juhtudel ❏ DNS-serveriga ühenduse loomine on nurjunud ❏ POP3-serveri nimelahendus on nurjunud
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 kellaaja 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.

Teated	Põhjus
Cannot access the product until processing is complete.	See teade kuvatakse, kui skanner on hõivatud.

Jagatud võrgukausta sätted

Seadistage skannitud kujutise salvestamiseks võrgukaust.

Faili kausta salvestamisel logib skanner sisse kausta loomiseks kasutatud arvuti kasutajana.

Jagatud kausta loomine

Seotud teave

➡ „Enne jagatud kausta loomist” lk 47

➡ „Võrguprofiili kontrollimine” lk 47

➡ „Jagatud kausta loomise koht ja näide turvalisusest” lk 48

➡ „Juurdepääsu lubava rühma või kasutaja lisamine” lk 59

Enne jagatud kausta loomist

Enne jagatud kausta loomist kontrollige alljärgnevat.

❏ Skanner on ühendatud võrku, mille kaudu see pääseb ligi arvutile, kuhu luuakse jagatud kaust.

❏ Arvuti, kuhu luuakse jagatud kaust, nimi ei sisalda mitmebaidist tärki.

Oluline teave:

Kui arvuti nimi sisaldab mitmebaidist tärki, ei pruugi faili salvestamine jagatud kausta õnnestuda.

Sel juhul kasutage arvutit, mille nimi ei sisalda mitmebaidist tärki, või muutke algse arvuti nime.

Arvuti nime muutes kinnitage see eelnevalt administraatoriga üle, sest see võib mõjutada mõningaid sätteid nagu arvuti haldus, juurdepääs ressurssidele jms.

Võrguprofiili kontrollimine

Kontrollige arvutist, kuhu luuakse jagatud kaust, kas kausta jagamine on lubatud.

1. Logige sisse arvutisse, kuhu luuakse jagatud kaust administraatori volituse kasutajakontoga.
2. Valige **Juhtpaneel** > **Võrk ja Internet** > **Võrgu- ja ühiskasutuskeskus**.
3. Klõpsake nuppu **Muuda ühiskasutuse täpsemaid sätteid** ja seejärel klõpsake kuvatud võrguprofiilide hulgast profiili **(praegune profiil)**.

4. Kontrollige, kas suvandi **Failide ja printerite ühiskasutus** alt on valitud **Lülita failide ja printerite ühiskasutus sisse**.

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

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

Jagatud kausta loomise koht ja näide turvalisusest

Turvalisus ja mugavus olenevad jagatud kausta loomise kohast.

Jagatud kausta haldamiseks skanneritest või teistest arvutitest on vajalikud järgmised kausta lugemis- ja muutmisõigused.

❏ Vahekaart **Ühiskasutus** > **Täpsemad ühiskasutuse suvandid** > **Õigused**

See juhib jagatud kausta võrgu juurdepääsu õigust.

❏ Vahekaardi **Turvalisus** juurdepääsu õigus

See juhib jagatud kausta võrgu juurdepääsu ja kohaliku juurdepääsu õigust.

Kui määrate jagatud kausta loomise näitena töölauale loodud jagatud kausta sätteks **Kõik**, saavad sellele ligi pääseda kõik kasutajad, kes pääsevad ligi arvutile.

Kuid ilma volituseta kasutaja ei pääse sellele ligi, sest töölaud (kaust) on kasutaja kausta kontrolli all ning sel juhul kehtivad kasutaja kausta turvasätted ka sellele. Kasutaja, kellel puudub ligipääs vahekaardil **Turvalisus** (antud juhul sisselogitud kasutaja ja administraator), saab seda kausta hallata.

Õige asukoha loomiseks lugege altpoolt.

Selles näites luuakse kaust „scan_folder“.

Seotud teave

➡ „Konfigureerimise näide failiserverite jaoks” lk 48

➡ „Konfigureerimise näide personaalarvuti jaoks” lk 54

Konfigureerimise näide failiserverite jaoks

Selles osas on näite alusel selgitatud jagatud arvutis oleva draiveri juurele jagatud kausta loomist, näiteks failiserver järgmistel tingimustel.

Reguleeritava juurdepääsuga kasutajad, nagu isikud, kellel on jagatud kausta loomiseks arvuti sama domeen, pääsevad jagatud kaustale ligi.

Määrake see konfiguratsioon siis, kui lubate ükskõik millisel kasutajal lugeda arvutis olevat jagatud kausta ja sellesse kirjutada, näiteks failiserveri ja jagatud arvuti puhul.

❏ Jagatud kausta loomise koht: draiveri juur

❏ Kausta rada: C:\scan_folder

❏ Juurdepääsu õigus võrgu kaudu (Jaga õiguseid): kõik

❏ Juurdepääsu õigus failisüsteemis (Turvalisus): autenditud kasutajad

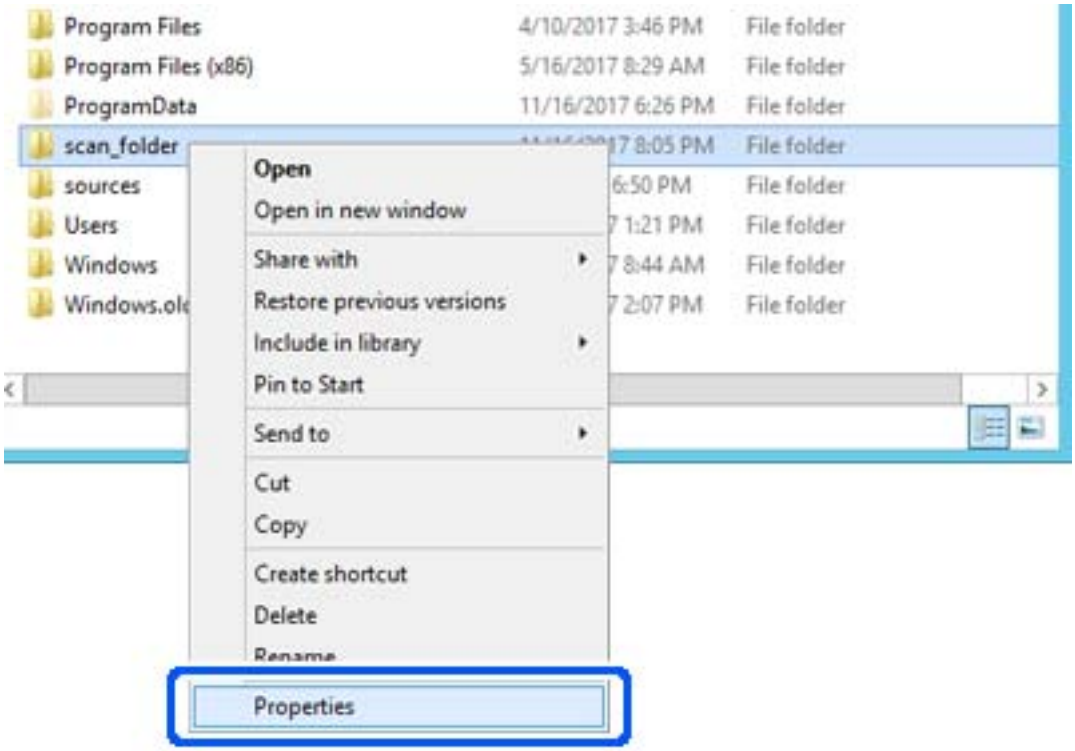
1. Logige sisse arvutisse, kuhu luuakse jagatud kaust administraatori volituse kasutajakontoga.

2. Käivitage Explorer.

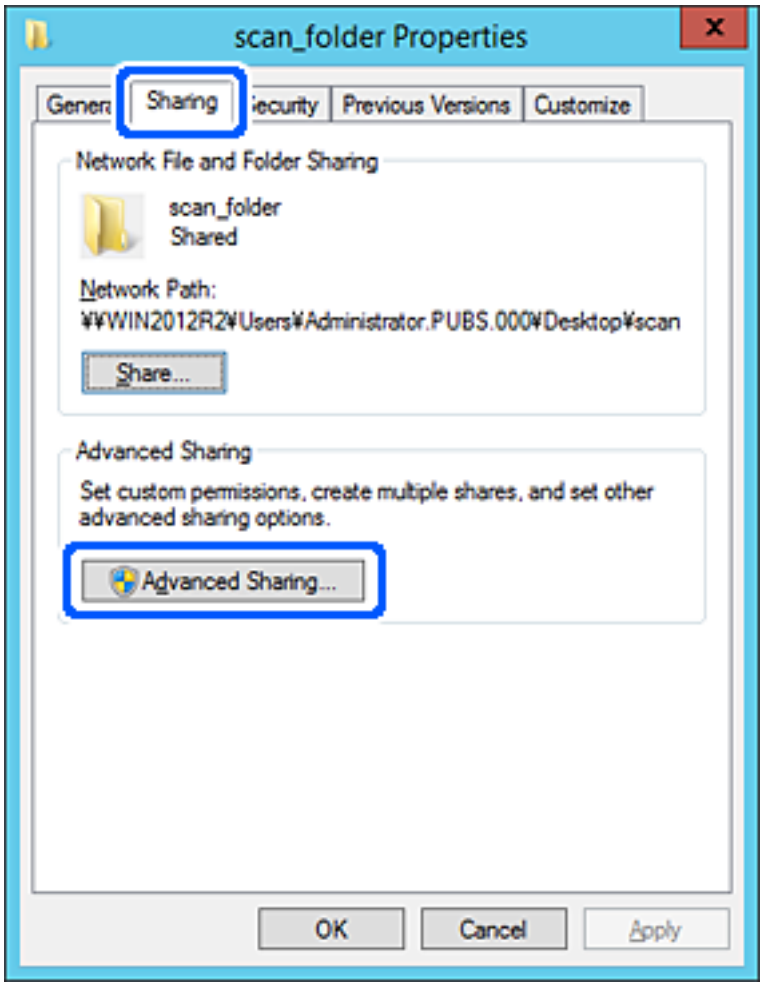
3. Looge kaust draiveri juurele ja pange sellele nimeks „scan_folder“.

   Sisestage kausta nimi 1–12 tähemärgiga. Kui ületate kausta nime tähemärkide piiri, ei pruugi te saada sellele tavapärast juurdepääsu erilaadse keskkonna tõttu.

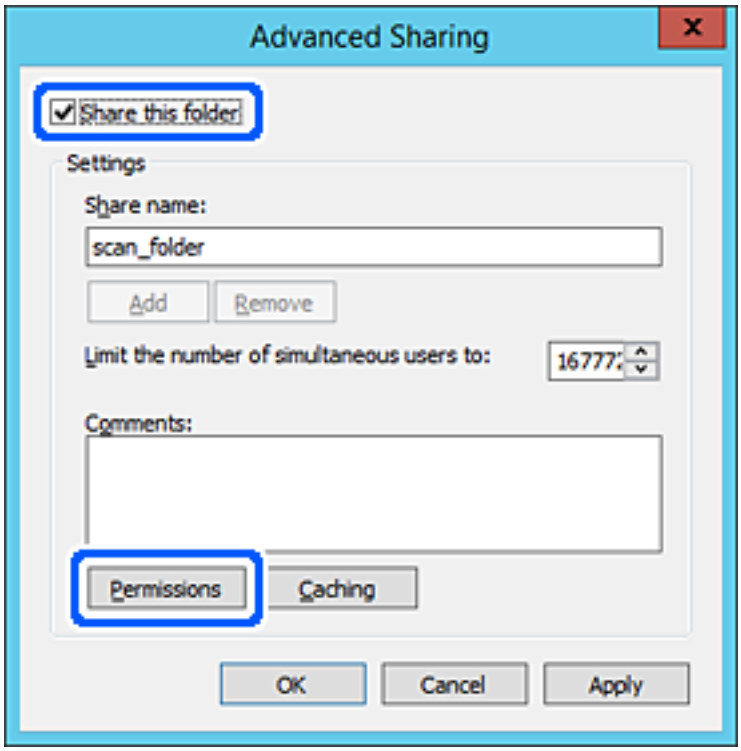
4. Paremklõpsake kaustal ja seejärel valige **Atribuudid**.



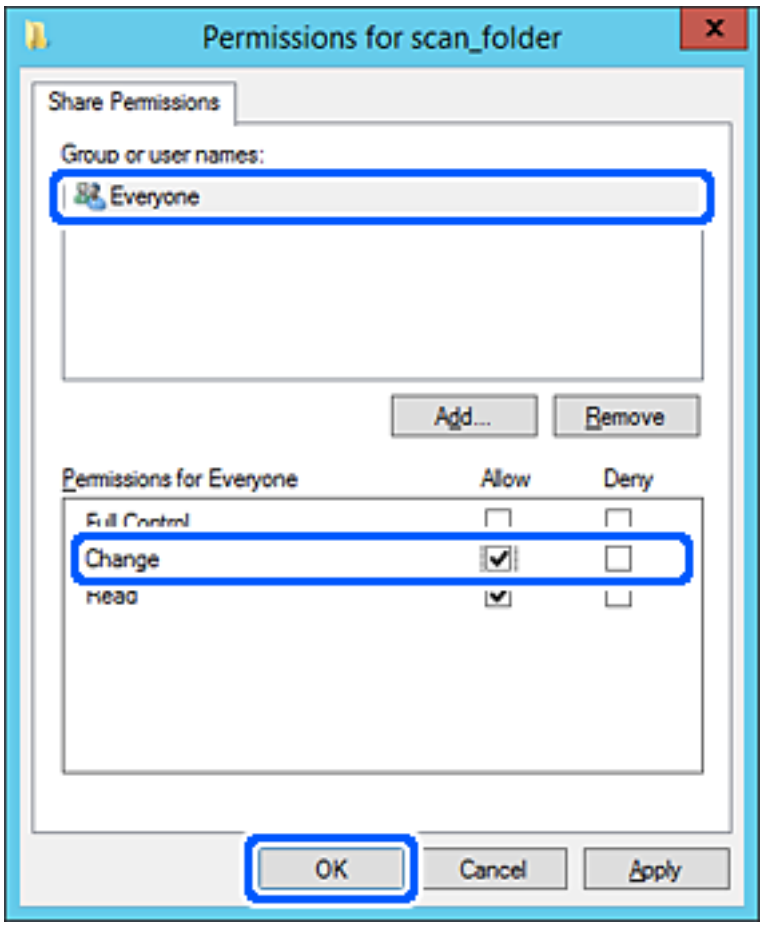
5. Klõpsake vahekaardil **Ühiskasutus** valikut **Täpsemad ühiskasutuse suvandid**.



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

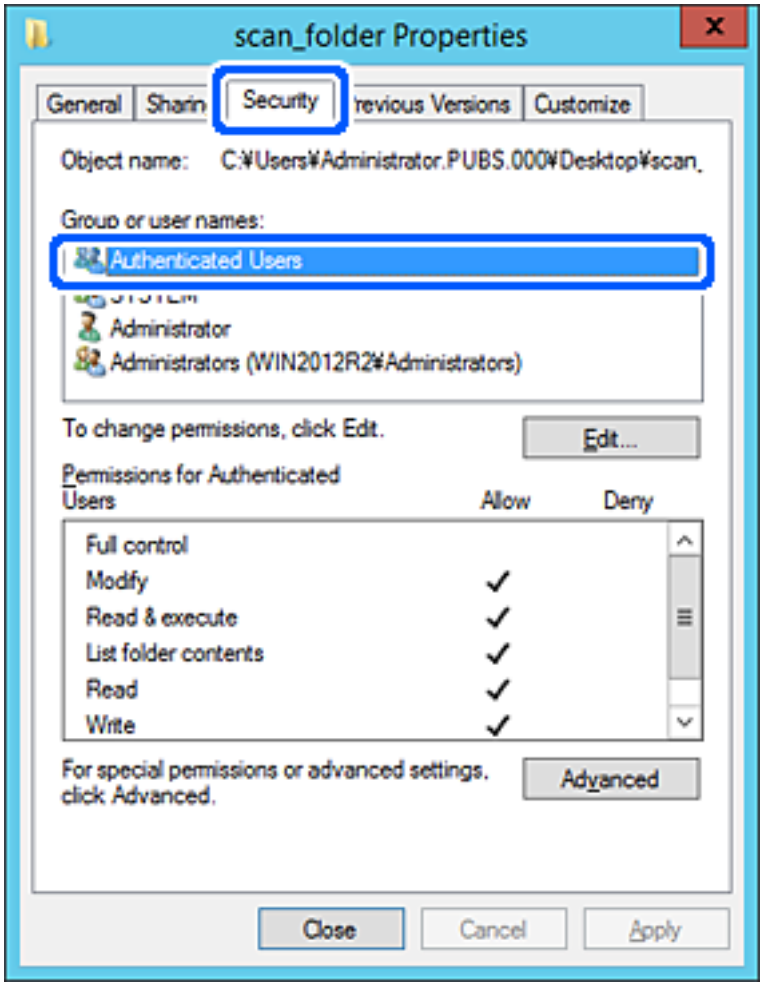


7. Valige **Rühma- või kasutajanimed** alt rühm **Kõik**, valige **Rakendamine** alt **Luba** ja seejärel klõpsake **OK**.



8. Klõpsake nuppu **OK**.

9. Valige vahekaart **Turvalisus** ja seejärel valige **Rühma- või kasutajanimed** alt **Autenditud kasutajad**.

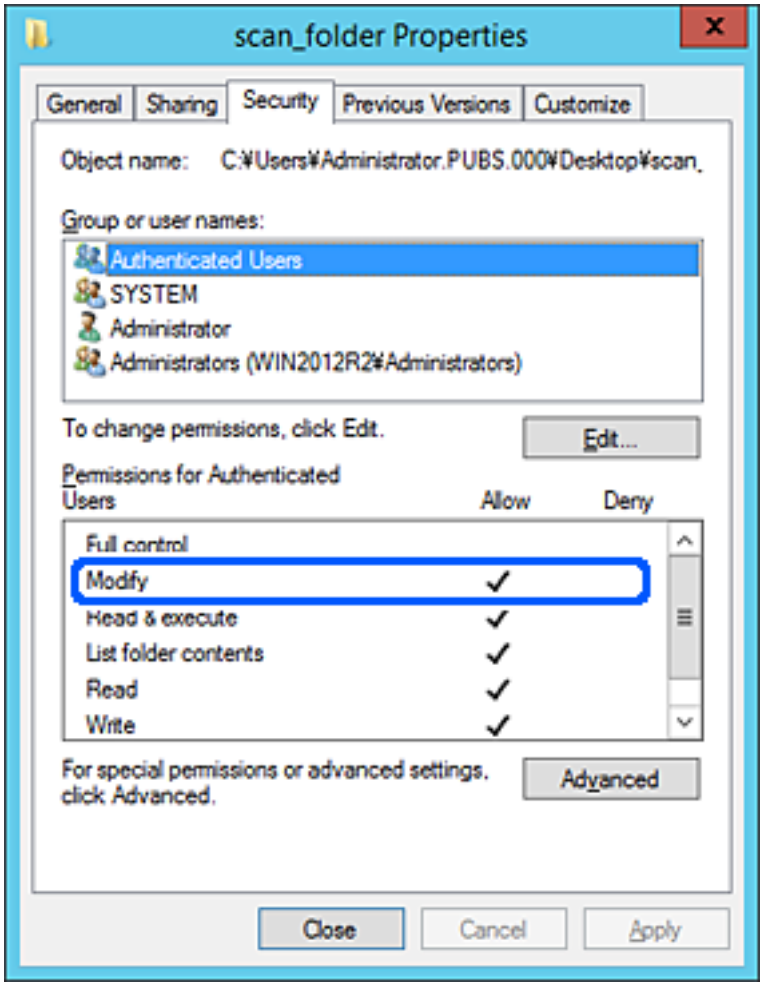


„Autenditud kasutajad“ on erirühm, mis hõlmab kõiki kasutajaid, kes saavad domeeni või arvutisse sisse logida. Seda rühma kuvatakse ainult siis, kui kaust luuakse vahetult juurkausta alla.

Kui seda ei kuvata, klõpsake selle lisamiseks nuppu **Redigeerimine**. Rohkem teavet leiate seotud teabe jaotisest.

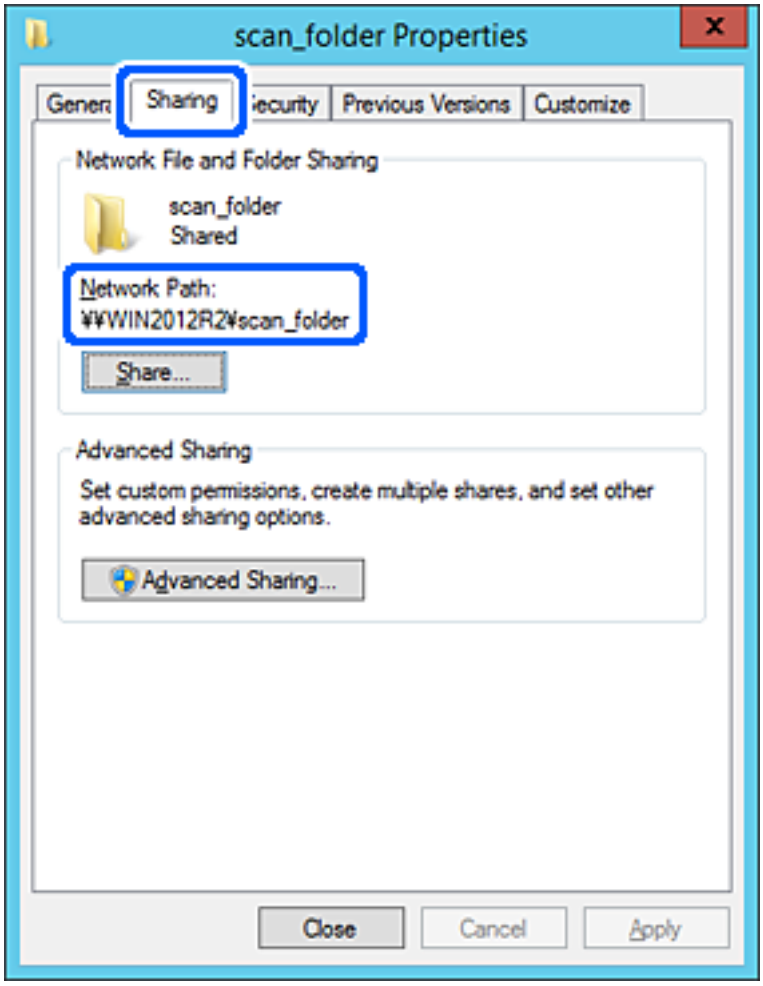
10. Kontrollige, kas **Autenditud kasutajate õigused** all jaotises **Muutmine** on valitud **Rakendamine**.

    Kui see ei ole valitud, valige **Autenditud kasutajad**, klõpsake **Redigeerimine**, valige **Autenditud kasutajate õigused** alt jaotisest **Muutmine** suvand **Rakendamine** ja seejärel klõpsake **OK**.



11. Valige vahekaart **Ühiskasutus**.

    Kuvatakse jagatud kausta võrguteed. Seda kasutatakse skanneri kontaktide registreerimisel. Kirjutage see üles.



12. Ekraani sulgemiseks klõpsake nuppu **OK** või **Sule**.

    Kontrollige, kas faili saab sama domeeni arvutites olevas jagatud kaustas kirjutada või lugeda.

Seotud teave

➡ „Juurdepääsu lubava rühma või kasutaja lisamine” lk 59

➡ „Sihtkoha registreerimine kontaktide hulka utiliidi Web Config abil” lk 64

Konfigureerimise näide personaalarvuti jaoks

Selles osas on näite alusel selgitatud jagatud kausta loomist praegu arvutisse sisse logiva kasutaja töölauale.

Kasutaja, kes logib sisse arvutisse ja kellel on administraatori õigused, saab juurdepääsu töölaua kataloogile ja dokumentide kataloogile, mis asuvad kasutaja kaustades.

Määrake see konfiguratsioon siis, kui te EI luba teisel kasutajal personaalarvutis olevat jagatud kausta lugeda ega kirjutada.

❏ Jagatud kausta loomise koht: töölaud

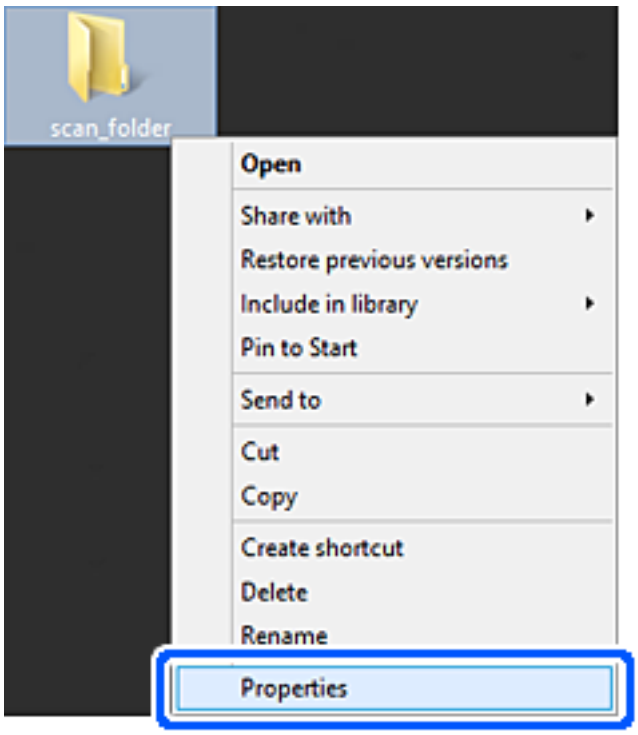
❏ Kausta rada: C:\Users\xxxx\Desktop\scan_folder

❏ Juurdepääsu õigus võrgu kaudu (Jaga õiguseid): kõik

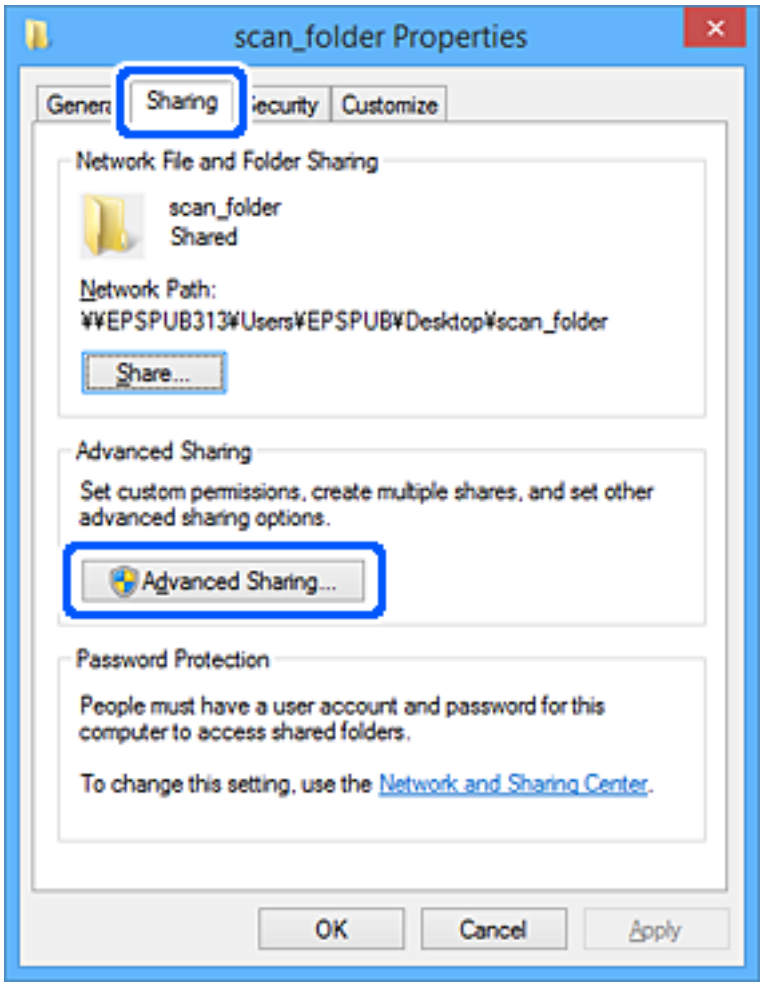
❏ Juurdepääsu õigus failisüsteemis (Turvalisus): ärge lisage või lisage kasutaja-/rühmanimesid, et lubada juurdepääsu

1. Logige sisse arvutisse, kuhu luuakse jagatud kaust administraatori volituse kasutajakontoga.
2. Käivitage Explorer.
3. Looge kaust töölauale ja pange sellele nimeks „scan_folder“.

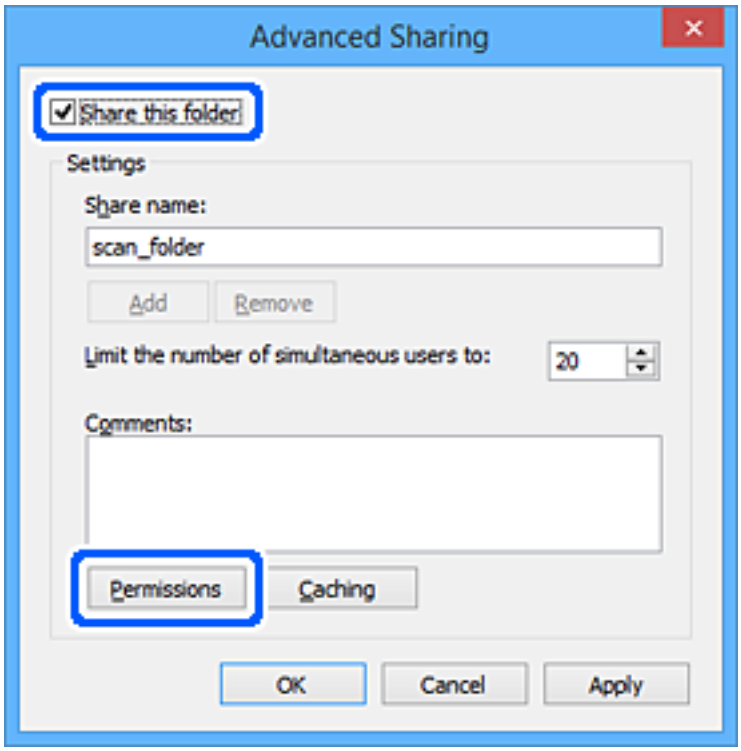
   Sisestage kausta nimi 1–12 tähemärgiga. Kui ületate kausta nime tähemärkide piiri, ei pruugi te saada sellele tavapärast juurdepääsu erilaadse keskkonna tõttu.
4. Paremklõpsake kaustal ja seejärel valige **Atribuudid**.



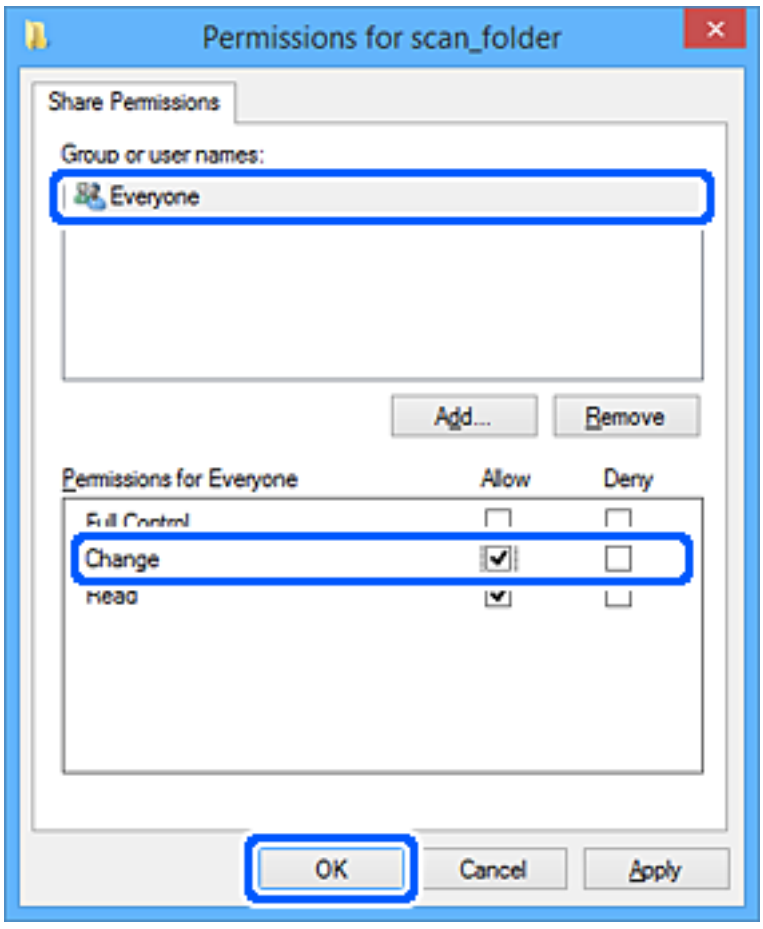
5. Klõpsake vahekaardil **Ühiskasutus** valikut **Täpsemad ühiskasutuse suvandid**.



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



7. Valige **Rühma- või kasutajanimed** alt rühm **Kõik**, valige **Rakendamine** alt **Luba** ja seejärel klõpsake **OK**.

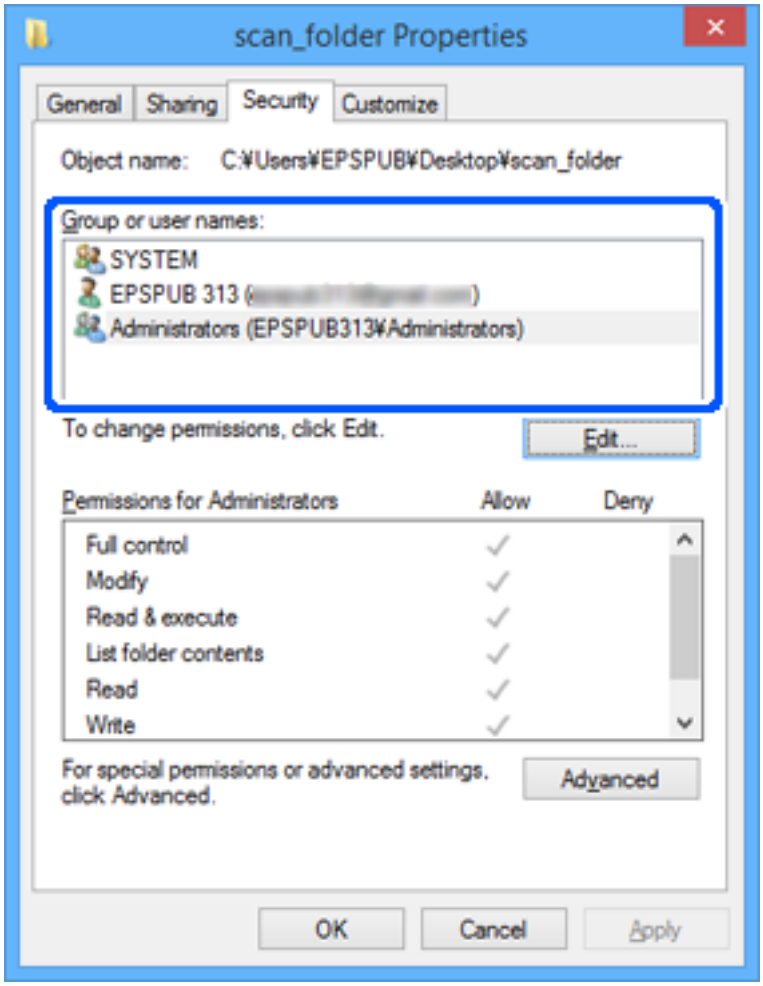


8. Klõpsake nuppu **OK**.
9. Valige vahekaart **Turvalisus**.
10. Valige grupp või kasutaja valikust **Grupi- või kasutajanimed**.

    Siin kuvatav rühm või kasutaja saavad juurdepääsu jagatud kaustale.

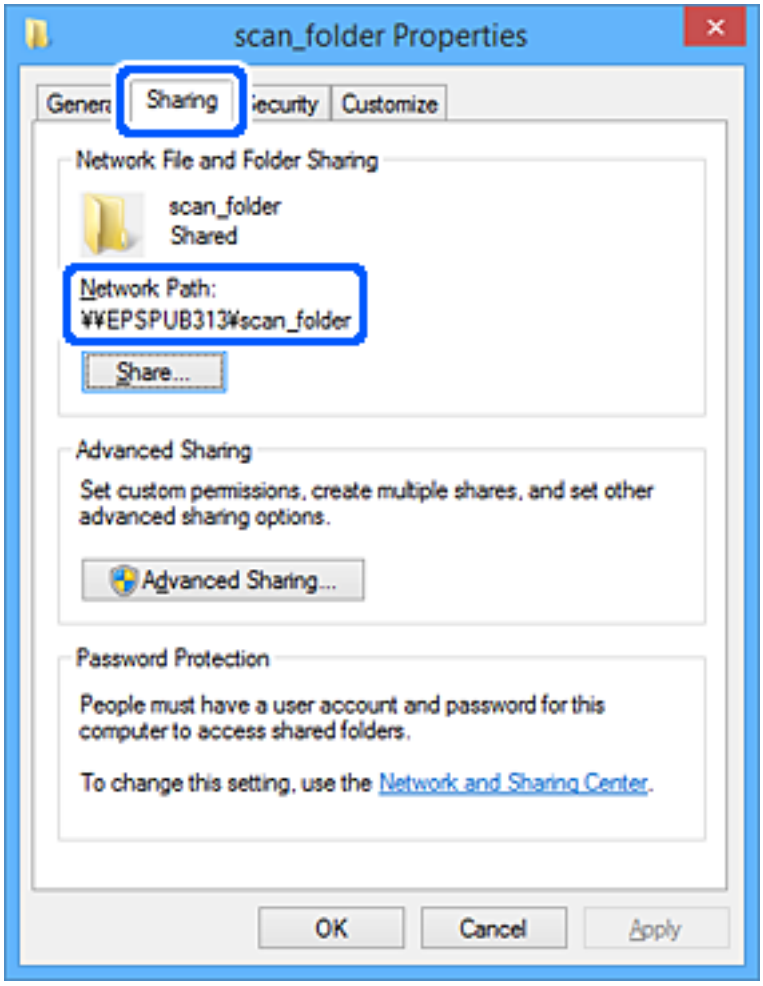
    Sel juhul saavad kasutajad ja administraatorid, kes sellesse arvutisse sisse logivad, jagatud kausta kasutada.

    Vajaduse korral lisage juurdepääsu õigus. Selle lisamiseks klõpsake nuppu **Redigeerimine**. Rohkem teavet leiate seotud teabe jaotisest.



11. Valige vahekaart **Ühiskasutus**.

    Kuvatakse jagatud kausta võrguteed. Seda kasutatakse skanneri kontaktide registreerimisel. Kirjutage see üles.



12. Ekraani sulgemiseks klõpsake nuppu **OK** või **Sule**.

    Kontrollige, kas faili saab juurdepääsu õigusega kasutajate või rühmade arvutites olevas jagatud kaustas kirjutada või lugeda.

Seotud teave

➡ „Juurdepääsu lubava rühma või kasutaja lisamine” lk 59

➡ „Sihtkoha registreerimine kontaktide hulka utiliidi Web Config abil” lk 64

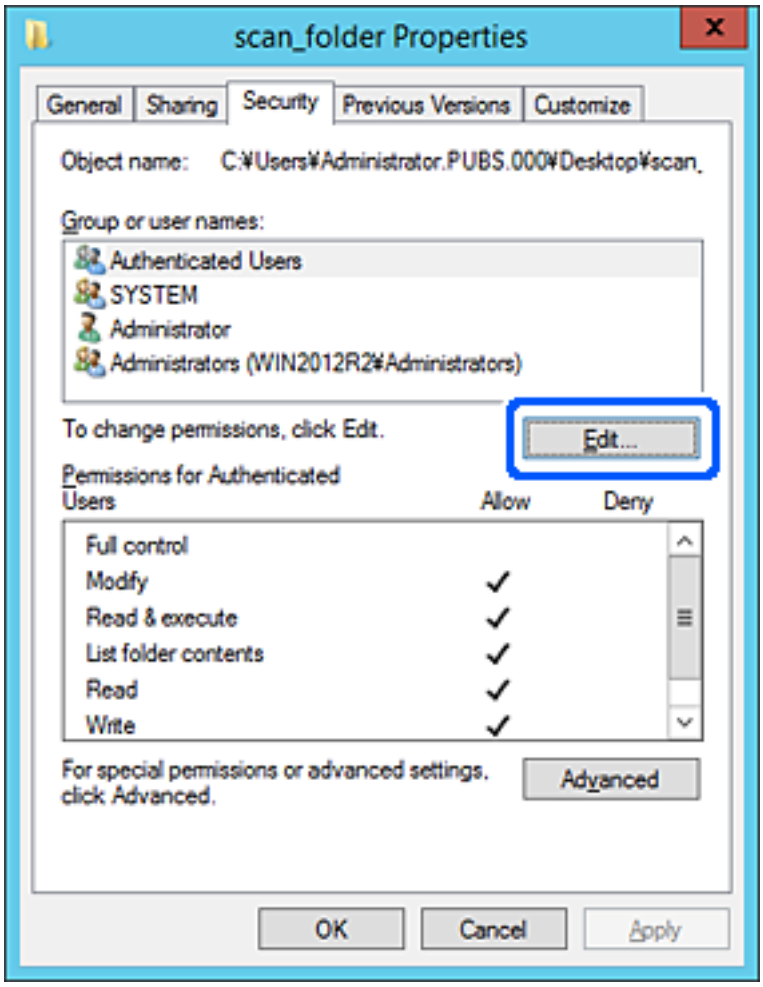
Juurdepääsu lubava rühma või kasutaja lisamine

Te saate lisada rühma või kasutaja, mis lubab juurdepääsu.

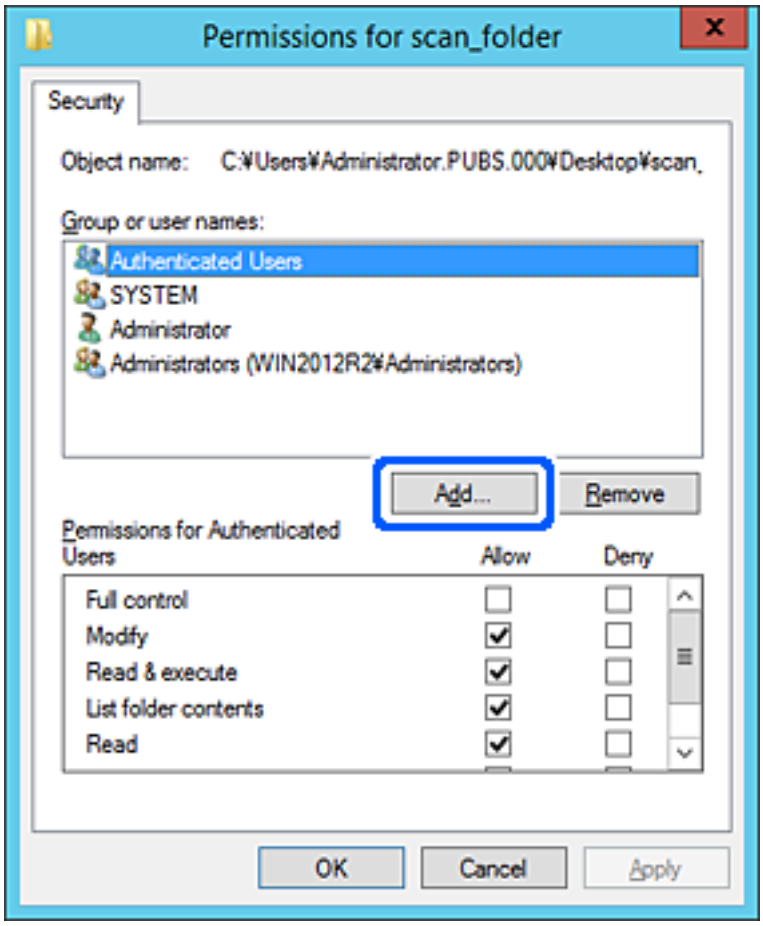
1. Paremklõpsake kaustal ja valige **Atribuudid**.

2. Valige vahekaart **Turvalisus**.

3. Klõpsake nuppu **Redigeeri**.



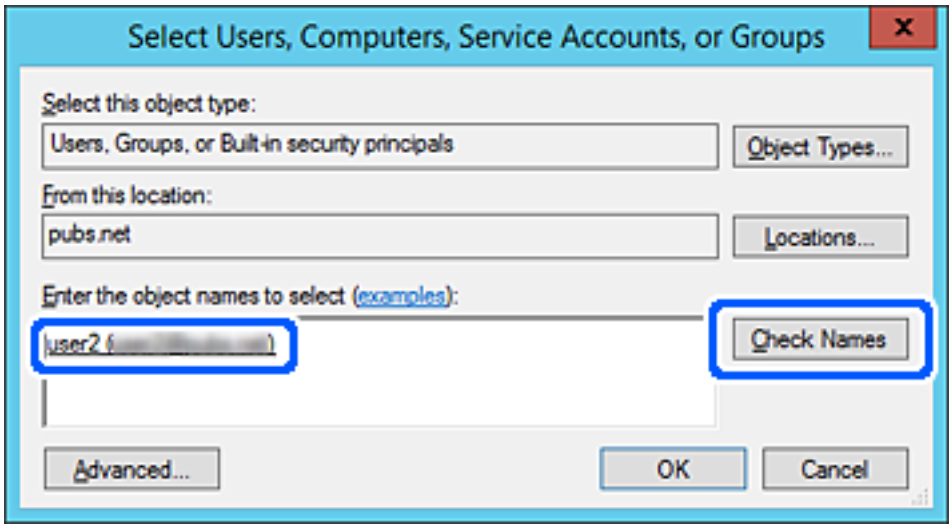
4. Klõpsake jaotise **Rühma- või kasutajanimed** all nuppu **Lisa**.



5. Sisestage juurdepääsu lubava rühma- või kasutajanimi ja seejärel klõpsake suvandil **Kontrolli nimesid**.
   Vastav nimi kriipsutatakse alla.

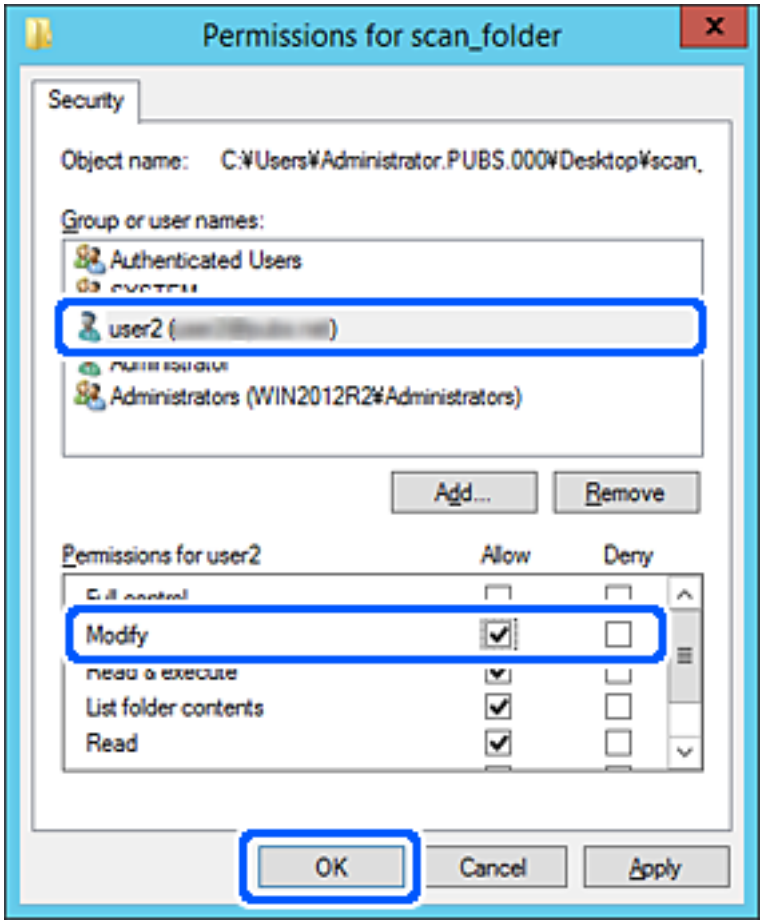
Märkus.
Kui te ei tea rühma või kasutaja täisnime, sisestage osa nimest ja seejärel klõpsake suvandil ***Kontrolli nimesid****. Kuvatakse loetelu rühma- või kasutajanimedest, mis osaliselt ühtivad osalise nimega, ja te saate loetelust valida täisnime.*

Kui ühtib ainult üks nimi, kuvatakse allakriipsutatud täisnime väljal ***Sisestage valitava objekti nimi****.*



6. Klõpsake **OK**.

7. Valige õiguste ekraanilt kasutajanimi, mis on sisestatud väljale **Rühma- või kasutajanimed**, valige juurdepääsu luba suvandi **Muutmine** alt ja seejärel klõpsake nuppu **OK**.



8. Ekraani sulgemiseks klõpsake nuppu **OK** või **Sule**.

   Kontrollige, kas faili saab juurdepääsu õigusega kasutajate või rühmade arvutites olevas jagatud kaustas kirjutada või lugeda.

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 sätted.
Võrgukaust	Skanniandmete sihtkoht. Võrgukaust tuleb eelnevalt ettevalmistada.

Seotud teave

➡ „Koostöö LDAP-serveri ja kasutajate vahel” lk 69

Kontaktide konfiguratsiooni võrdlus

Skanneri kontaktide konfigureerimiseks 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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 tärke „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. „Konfigureerimise näide personaalarvuti jaoks“ lk 54
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 kasutajanimeks 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 tärki vormingus Unicode (UTF -16), jättes välja eesliited „http://“ ja „https://“.
User Name	Sisestage serverile juurdepääsuks kasutajanimi pikkusega kuni 30 tärki 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 tärki 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

Kontaktide varundamine ja importimine

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

Rakendusega Web Config kontaktide varundamiseks saate eksportida skanneri sätted, mis sisaldavad kontakte. Eksporditud faili ei ole võimalik redigeerida, sest see eksporditakse kahendfailina.

Kui impordite skannerisse skanneri sätted, kirjutatakse kontaktid üle.

Rakenduse Epson Device Admin puhul saab kontakte eksportida ainult seadme atribuutide aknast. Lisaks, kui te ei ekspordi turvalisusega seotud üksuseid, saate redigeerida eksporditud 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 skannerissse 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. Eksporditud 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 konfigureerida.
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 konfigureerida.
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. ❏ Skanner ja DNS-server saavad omavahel suhelda. ❏ Skanneri, KDC-serveri ja autentimiseks vajaliku serveri (LDAP-server, SMTP-server, failiserver) ajad on sünkroonitud. ❏ 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 otsingusätted, 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 arbitraarset domeeni, täpsustage LDAP-serveri domeeni nimi. Sisestage 0–128 tärki vormingus Unicode (UTF-8). Kui te ei otsi arbitraarset 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: ❏ LDAP-serveri aadress või pordinumber on vale. ❏ Esinenud on ajalõpp. ❏ **Do Not Use** on valitud suvandi **Use LDAP Server** sätteks. ❏ 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: ❏ **User Name** ja/või **Password** on vale. ❏ Kui **Kerberos Authentication** on valitud suvandi **Authentication Method** sätteks, ei saa kellaaega/kuupäeva konfigureerida.
Cannot access the product until processing is complete.	See teade kuvatakse, kui skanner on hõivatud.

Funktsiooni Document Capture Pro Server kasutamine

Kasutades rakendust Document Capture Pro Server saate hallata skanneri juhtpaneelilt tehtud skannimise tulemuse sortimismeetodit, salvestusvormingut, ja edastamise sihtkohta. Saate skanneri juhtpaneelilt välja kutsuda ja käivitada varasemalt serveris registreeritud töid.

Installige see serverarvutisse.

Lisateavet tarkvara Document Capture Pro Server kohta küsige kohalikust Epsoni kontorist.

Serverirežiimi määramine

Rakenduse Document Capture Pro Server kasutamiseks häälestage see alljärgnevalt.

1. Avage Web Config ja valige vahekaart **Scan** > **Document Capture Pro**.
2. Suvandi **Server Mode** sätteks valige **Mode**.
3. Sisestage serveri aadress, kuhu on installitud Document Capture Pro Server, väljale **Server Address**.

   Sisestage 2 kuni 255 tähemärki IPv4-, IPv6-, hostinime või FQDN-vormingus. FQDN-vormingus saate kasutada tärke ASCII-vormingus (0x20–0x7E) ja sümbolit „-“, aga mitte aadressi alguses ja lõpus.
4. Klõpsake nuppu **OK**.

   Võrguga luuakse uuesti ühendus ja sätted aktiveeritakse.

Funktsiooni AirPrint seadistamine

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

Üksused	Selgitus
Bonjour Service Name	Sisestage Bonjouri 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.
Enable AirPrint	Bonjour ja AirPrint (skannimisteenus) on lubatud.

Probleemid võrguskannimise ettevalmistamisega

Nõuandeid probleemide lahendamiseks

❏ Veateate kontrollimine

Tõrke ilmnemise korral kontrollige esmalt, kas skanneri juhtpaneelil või draiverikuval on teateid. Kui olete määranud sündmuste ilmnemise korral teavitusmeili 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 **Süsteemi eelistused** > **Võrk** > **Täpsem** > **Puhvrid** ja seejärel registreerige kohalik aadress suvandis **Ära kasuta puhvrisätteid 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**.

Teenusega Microsoft Exchange Online ei saa skannitud kujutisi meilile saata

Ei saa sisse logida või kasutajad ei saa sisse logida

Teie Entra ID võib olla blokeeritud tingimusliku juurdepääsupoliitika tõttu.

Lahendus.

Vaadake oma Entra ID tingimuslikke juurdepääsupoliitikaid.

Täpsed juhtnöörid leiate veebisaidilt Microsoft Learn.

Ei saa meili saata

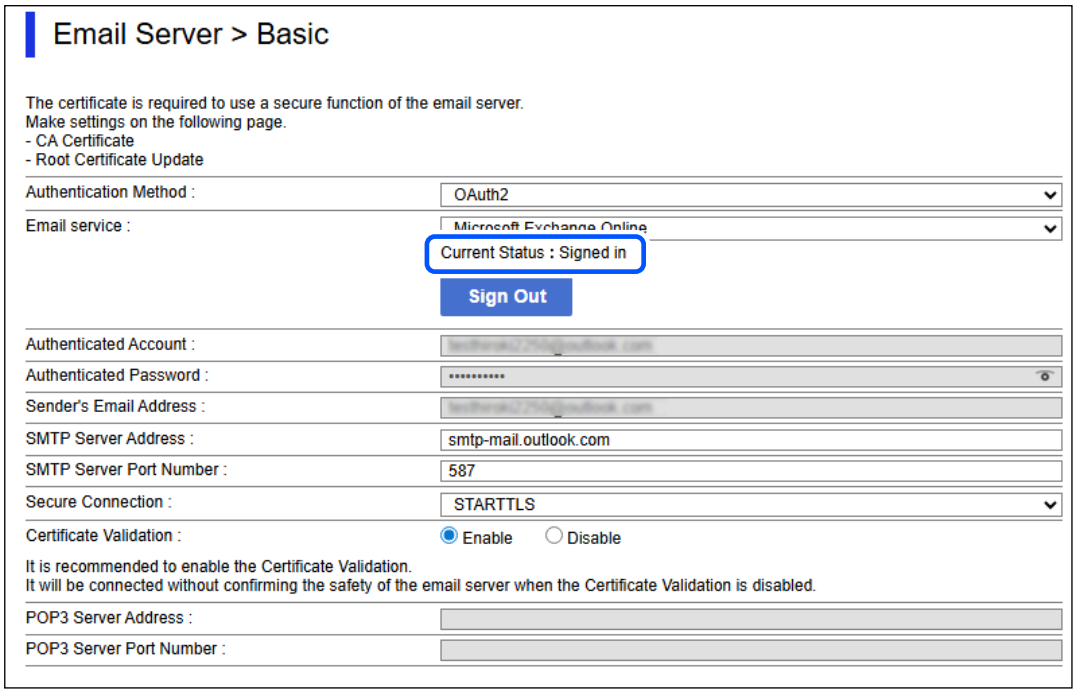
Olek.

Kuvatakse teade: „Selle funktsiooni kasutamiseks peate meiliteenusesse sisse logima. Võtke ühendust administraatoriga.“.

Lahendus.

Vaadake kehtivat olekut rakendusest Web Config.

Valige vahekaart **Network** > **Email Server** > **Basic**



Kui **Current Status** on **Signed in**, võib sisselogimisteave olla jäänud skannerisse salvestamata. Klõpsake nuppu **OK**, et saata sätteteave skannerisse.

Kui **Current Status** puudub ja kuvatud on nupp **Sign In**, siis logige sisse.

„Meiliserveri autentimismeetodi OAuth2.0 seadistamine” lk 43

Olek.

Pilveteenus või meiliteenus on ühendamata või on ühendus aegunud.

Lahendus.

Looge ühendus pilveteenuse või meiliteenusega.

Olek.

Peate pilveteenusesse uuesti sisse logima.

Lahendus.

Logige sisse pilveteenusesse.

Kuvatakse aegumisteade

Sisselogimisest on ilma meilisaatmise funktsiooni kasutamiseta on möödunud teatav aeg.

Kui autentimismeetodit OAuth 2.0 kasutavat skannerit pole kaua aega kasutatud või ei ole kasutatud meilisaatmise funktsiooni, muutuvad juurdepääsuluba ja värskendusluba kehtetuks.

Lahendus.

Administraator peab sisselogimise uuesti tegema.

„Meiliserveri autentimismeetodi OAuth2.0 seadistamine” lk 43

Juhtpaneeli ekraani kohandamine

Registreerimine: Eelsätted. 79

Juhtpaneeli avakuva redigeerimine. 81

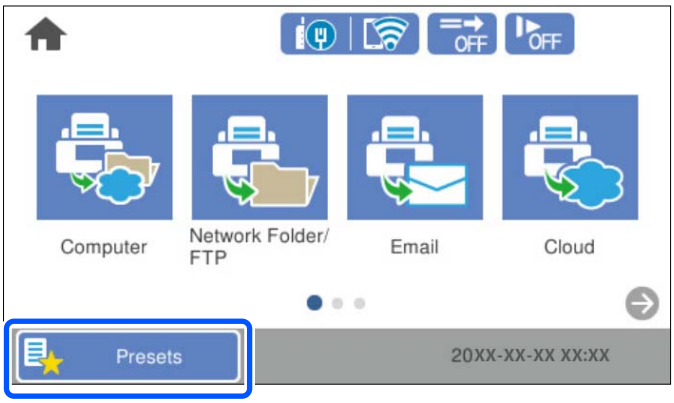
Registreerimine: Eelsätted

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

Märkus.

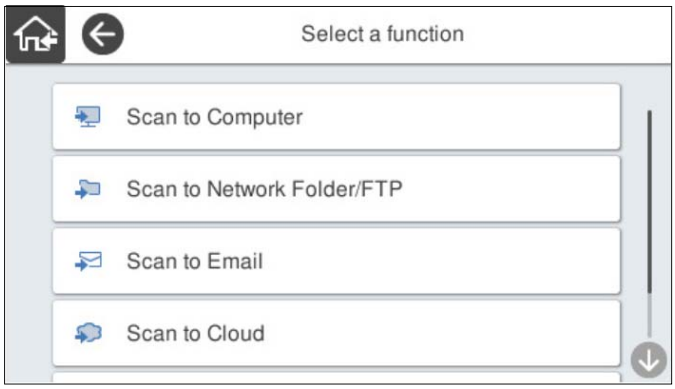
- *Kehtivate sätete registreerimiseks valige skannimise käivitamise kuval* ☆.
- *Samuti on loendisse **Presets** registreerimine võimalik rakenduses Web Config.*
  *Valige vahekaart **Scan** > **Presets**.*
- *Kui valite registreerimisel sätte **Skanni arvutisse**, saate registreerida rakenduses Document 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.

     Kui kasutate rakendust Document Capture Pro Server, on skanneri eelsätetes valitud **Kiirsaatmise sätted** tarkvarast prioriteetsem, isegi kui seate tarkvara enne skannimist töö sisu kinnitama.
   - ❏ **Sisukord**: kontrollige skannimissätteid.

6. Valige **OK**.

Menüüsuvandid: Eelsätted

Eelsätte sätteid saate muuta, tehes eelsättes valiku ›.

Nime muutmine:

muudab eelsätte nime.

Ikooni muutmine:

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 81
- Lisa ikoon: lisab ikooni teie tehtud suvandi **Eelsätted** sätete jaoks või taastab ikoonid, mis on kuvalt eemaldatud.
  „Lisa ikoon” lk 82
- Eemalda ikoon: eemaldab ikooni avakuvalt.
  „Eemalda ikoon” lk 83
- Teisalda ikoon: muudab ikoonide kuvajärjekorda.
  „Teisalda ikoon” lk 84
- Taasta vaikimisi ikoonid: taastab avakuva kuvasätete vaikesätted.
- Taustapilt: muutke avakuval taustpildi värvi.

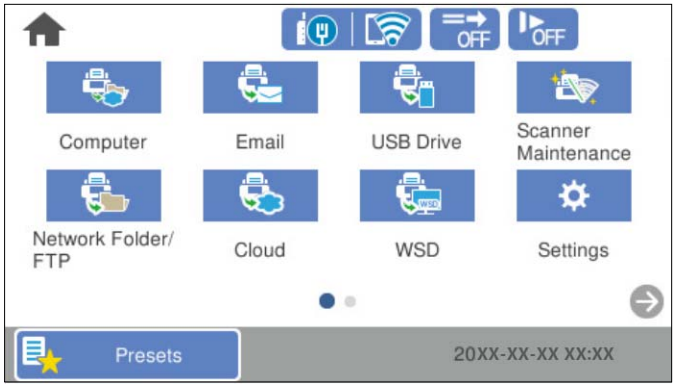
Avakuva Paigutusi muutmine

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

2. Valige **Rida** või **Maatriks**.

   Rida:

   Maatriks:



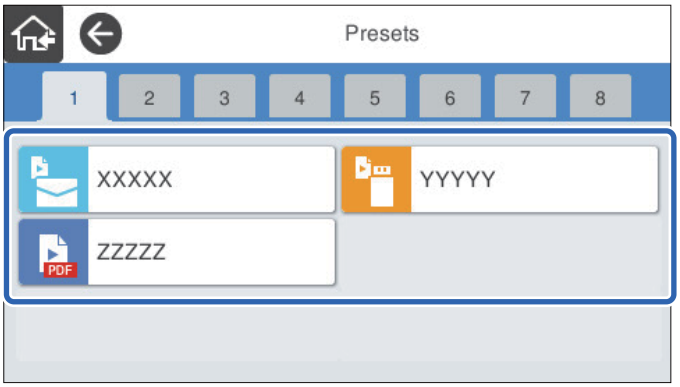
3. Naasmiseks ja avakuva ülevaatamiseks valige .

Lisa ikoon

1. Valige skanneri juhtpaneelil **Sätted** > **Muuda avakuva** > **Lisa ikoon**.
2. Valige **Funktsioon** või **Eelsätted**.
   - ❏ Funktsioon: kuvab avakuval näidatud vaikefunktsioonid.

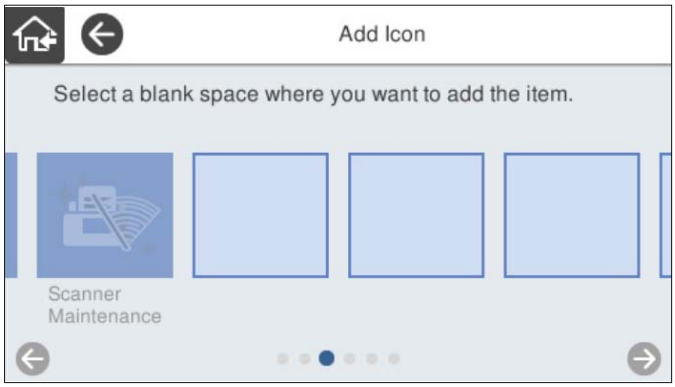
❏ Eelsätted: kuvab registreeritud eelsätted.

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.

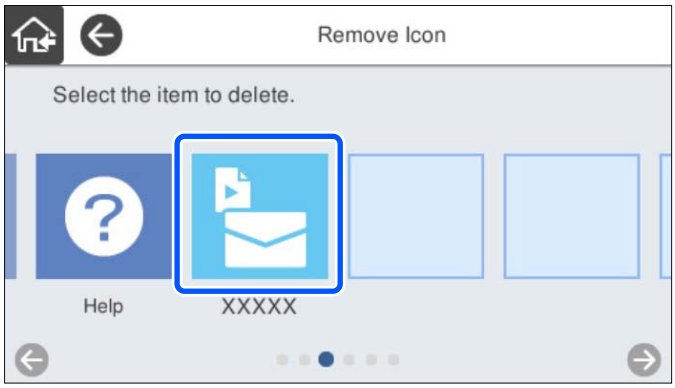


5. Naasmiseks ja avakuva ülevaatamiseks valige .

Eemalda ikoon

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

2. Valige ikoon, mida soovite eemaldada.



3. Lõpetamiseks valige **Jah**.

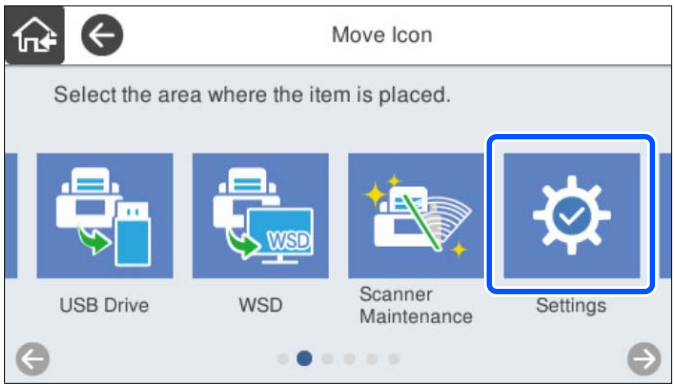
   Kui soovite eemaldada mitu ikooni, korrake toiminguid 2 kuni 3.

4. Naasmiseks ja avakuva ülevaatamiseks valige .

Teisalda ikoon

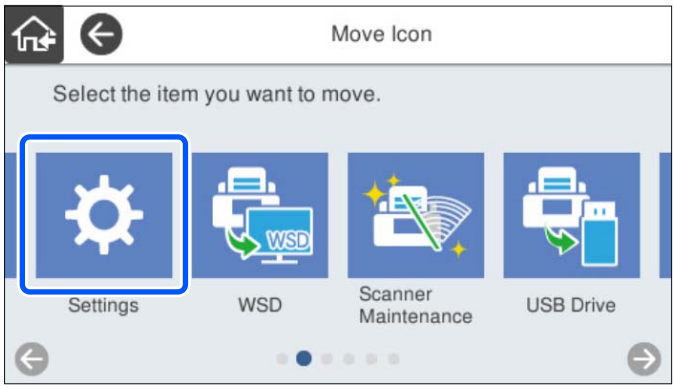
1. Valige skanneri juhtpaneelil **Sätted** > **Muuda avakuva** > **Teisalda ikoon**.

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. 87

Administraatori sätted. 87

Välise liidese keelamine. 93

Kaugskanneri jälgimine. 94

Probleemide lahendamine. 95

Toote turvalisuse funktsioonide juhend

Selles jaotises tutvustatakse Epsoni seadmete turvalisuse funktsioone.

Funktsiooni nimi	Funktsiooni tüüp	Mida seadistada	Mida vältida
Administraatori parooli seadistamine	Lukustab süsteemi sätted, näiteks võrguühenduse seadistuse või USB.	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.
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 87

➡ „Välise liidese keelamine” lk 93

Administraatori sätted

Seadistage administraatori parool

Administraatori parooli määrates saate takistada süsteemi halduse 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 toote tagaküljele 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. Rakenduse Epson Device Admin kasutamise korral lugege rakenduse Epson Device Admin juhendit või spikrit.

Administraatori parooli muutmine 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 ühebaidilisi tärke.

   Märkus.
   Allpool on toodud rakenduse administraatori teabe vaikeväärtused.

   ❏ *Kasutajanimi: puudub (tühi)*

   ❏ *Parool: oleneb toote tagaküljele 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

Administraatori parooli muutmine juhtpaneelil

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 toote tagaküljele 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 ühebaidilisi 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.

Märkus.
Kui lubate skanneris funktsiooni Authentication Settings, lubatakse ka juhtpaneeli funktsioon Lukustamise sätted. Kui Authentication Settings on lubatud, ei saa juhtpaneeli lukust avada.

Isegi kui te funktsiooni Authentication Settings keelate, jääb Lukustamise sätted lubatuks. Kui soovite selle keelata, saate asjakohased sätted teha juhtpaneelil või rakenduses Web Config.

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

Funktsiooni Lukustamise sätted üksused menüüs Sätted

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

✓: lukustatakse.

- : ei lukustata.

Menüü Sätted	Lukustamise sätted
Põhisätted	-

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

Menüü Sätted		**Lukustamise sätted**
	Võrgukaust/FTP	✓
	Meil	✓
	Pilv	✓
	USB-draiv	✓
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	✓
	Paroolide krüptimine	✓
	Kliendiuuring	✓
	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		-
	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

Skanneri juhtpaneelilt administraatorina sisselogimiseks saate kasutada ükskõik millist järgmistest meetoditest.

1. Puudutage ekraanil üleval paremas nurgas ikooni .
   - ❏ Kui Authentication Settings on lubatud, on ikoon kuval **Tere tulemast!** (autentimise ootekuva).
   - ❏ Kui Authentication Settings on keelatud, on ikoon avakuval.

2. Kui kuvatakse kinnituskuva, puudutage nuppu **Jah**.
3. Sisestage administraatori parool.

   Kuvatakse sisselogimise teade ja seejärel kuvatakse juhtpaneelil avakuva.

Väljalogimiseks puudutage avakuval üleval paremas nurgas ikooni .

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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 42

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.

   ❏ Valutud 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 seatud 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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.

Probleemide lahendamine

Administraatori parool on ununenud

Vajate teeninduspersonali abi. Võtke ühendust kohaliku edasimüüjaga.

Märkus.
Allpool on toodud rakenduse Web Config administraatori algväärtused.

- ❏ *Kasutajanimi: puudub (tühi)*
- ❏ *Parool: oleneb toote tagaküljele 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. 97

Juhtimine protokollidega. 98

Digitaalsertifikaadi kasutamine. 101

SSL/TLS-side skanneriga. 106

Krüptitud side IPsec/IP-filtreerimisega. 107

Skanneri ühendamine IEEE802.1X-võrguga. 118

Täpsemate turvasätetega seotud probleemide lahendamine. 120

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 autenditud 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 98
- „SSL/TLS-side skanneriga” lk 106
- „Krüptitud side IPsec/IP-filtreerimisega” lk 107
- „Skanneri ühendamine IEEE802.1X-võrguga” lk 118

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 protokolli 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

Protokollid, mida saate lubada või keelata

Protokoll	Kirjeldus
Bonjour Settings	Saate täpsustada, kas Bonjouri kasutada. Protokolli 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.

Protokolli sätteüksused

Bonjour Settings

Üksused	Seadistuse väärtus ja kirjeldus
Use Bonjour	Valige see, et otsida või kasutada teenuseid läbi Bonjouri.
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 NetBIOSita 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 tärke.
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, jätke 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, jätke see tühjaks.
	Confirm Password	Sisestage kinnitamiseks valitud parool.
Context Name		Sisestage kuni 32 tärki vormingus Unicode (UTF-8). Kui te seda ei täpsusta, jätke 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 sertimiskekusest 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 asukoha 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 101

➡ „Iseallkirjastatud sertifikaadi värskendamine" lk 105

➡ „CA Certificate seadistamine" lk 105

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 allkirjastamistaotluse 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 allkirjastamistaotluse 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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 kellaaeg 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 sertifkaadi 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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 allkirjastamistaotlust kasutades, ei saa te kustutatud sertifikaati uuesti importida.Sellisel juhul looge sertifikaadi allkirjastamistaotlus 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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**.

   Kuvatakse kinnitusteade.
6. Klõpsake nuppu **OK**.

   Skannerit värskendatakse.

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

Seotud teave

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36
➡ „CA-signed Certificate seadistamine” lk 101
➡ „CA Certificate seadistamine” lk 105

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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) 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.

❏ 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**

Soovitatame 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 autenditakse 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. Kasutatav 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) 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.
Remote	Authentication Method	Kui valite sätte **IPsec** suvandis **Access Control**, valige suvand. Kasutatav sertifikaat ühtib vaikepoliitikaga.
	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) 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.

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

Soovitatame 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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 tõukeskannimiseks 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 kasutavat 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36
➡ „CA-signed Certificate seadistamine” lk 101
➡ „CA Certificate seadistamine” lk 105

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

IEEE 802.1X-võrgu sättekirjed

Üksused	Sätted ja selgitused	
IEEE802.1X (Wired LAN)	Saate lehe sätteid aktiveerida või inaktiveerida (**IEEE802.1X** > **Basic**) võrgule IEEE802.1X (juhtmega LAN).	
IEEE802.1X (Wi-Fi)	Kuvatakse ühenduse olek vastavalt standardile IEEE802.1X (Wi-Fi).	
Connection Method	Kuvatakse käesoleva võrgu ühendusmeetod.	
EAP Type	Valige autentimismeetod skanneri ja RADIUS-serveri vahel.	
	EAP-TLS	Peate hankima ja importima sertimiskeskuse allkirjastatud sertifikaadi.
	PEAP-TLS	
	PEAP/MSCHAPv2	Peate konfigureerima parooli.
	EAP-TTLS	
User ID	Konfigureerige ID, mida kasutatakse RADIUS-serveri autentimiseks. Sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki.	
Password	Konfigureerige parool skanneri autentimiseks. Sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Kui kasutate Windowsi serverit, nagu server RADIUS, saate sisestada kuni 127 tärki.	
Confirm Password	Sisestage kinnitamiseks valitud parool.	
Server ID	Saate konfigureerida serveri ID autentimiseks RADIUS-serveris. Autentimisrakendus kontrollib, kas serveri ID sisaldub serveri väljal subject/subjectAltName ja kas sert on saadetud RADIUS-serverist või mitte. Sisestage 0–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki.	
Certificate Validation	Saate määrata serdi kinnitamise vaatamata autentimisviisile. Importige sertifikaat suvandist **CA Certificate**.	
Anonymous Name	Kui valite sätte **PEAP-TLS** või **PEAP/MSCHAPv2** suvandis **EAP Type**, saate PEAP-autentimise esimeses etapis konfigureerida kasutaja ID asemel anonüümse nime. Sisestage 0–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki.	
Encryption Strength	Valikud on alljärgnevad.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

➡ „Krüptitud side IPsec/IP-filtreerimisega” lk 107

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 107

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36
➡ „Krüptitud side IPsec/IP-filtreerimisega” lk 107

Ei saa ühendust pärast IPsec/IP filtreerimise häälestamist

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 107

Pärast standardi IEEE 802.1X konfigureerimist puudub juurdepääs skannerile

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.

Ühendage skanner ja arvuti ja seejärel konfigureerige IEEE 802.1X uuesti.

Seotud teave

➡ „IEEE 802.1X-võrgu konfigureerimine” lk 118

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 103

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 105

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 101

Kuvatakse digitaalsertifikaadiga seotud hoiatus

Teated	Põhjus/tegevusmeede
Enter a Server Certificate.	**Põhjus:** Te ei ole importimiseks faili valinud. **Tegevusmeede:** Valige fail ja klõpsake nuppu **Import**.
CA Certificate 1 is not entered.	**Põhjus:** Sertimiskeskuse sertifikaat 1 ei ole sisestatud ning sisestatud on üksnes sertimiskeskuse sertifikaat 2. **Tegevusmeede:** Importige esimesena sertimiskeskuse sertifikaat 1.
Invalid value below.	**Põhjus:** Faili tee ja/või parool sisaldab toetamata tähemärke. **Tegevusmeede:** Kontrollige, kas tähemärgid on väljale õigesti sisestatud.
Invalid date and time.	**Põhjus:** Skanneri kuupäev ja kellaaeg on seadistamata. **Tegevusmeede:** Seadistage kuupäev ja kellaaeg, kasutades rakendust Web Config või EpsonNet Config.
Invalid password.	**Põhjus:** Sertimiskeskuse sertifikaadile määratud parool ja sisestatud parool ei ühti. **Tegevusmeede:** Sisestage õige parool.
Invalid file.	**Põhjus:** Imporditava sertifikaadi fail ei ole X509-vormingus. **Tegevusmeede:** Kontrollige, kas olete valinud õige sertifikaadi, mille on saatnud usaldusväärne sertimiskeskus.
	Põhjus: Imporditud fail on liiga suur. Maksimaalne lubatud faili maht on 5 KB. **Tegevusmeede:** Kui valisite õige faili, võib sertifikaat olla rikutud või võltsitud.
	Põhjus: Sertifikaadis sisalduv ahel on lubamatu. **Tegevusmeede:** Külastage sertifikaadi kohta lisateabe saamiseks sertimiskeskuse veebisaiti.

Teated	Põhjus/tegevusmeede
Cannot use the Server Certificates that include more than three CA certificates.	**Põhjus:** PKCS#12-vormingus sertifikaadi fail sisaldab rohkem kui kolme sertimiskeskuse sertifikaati. **Tegevusmeede:** Importige kõik sertifikaadid, konvertides PKCS#12-vormingu PEM-vormingusse, või importige PKCS#12-vormingus sertifikaadi fail, mis sisaldab kuni kahte sertimiskeskuse sertifikaati.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Põhjus:** Sertifikaat on aegunud. **Tegevusmeede:** ❏ Kui sertifikaat on aegunud, hankige ja importige uus sertifikaat. ❏ Kui sertifikaat ei ole aegunud, kontrollige, kas skanneri kuupäev ja kellaaeg on õigesti seadistatud.
Private key is required.	**Põhjus:** Sertifikaadiga ei ole seotud ühtegi privaatvõtit. **Tegevusmeede:** ❏ Kui sertifikaat on PEM/DER-vormingus ja see on hangitud arvutist saadetud sertifikaadi allkirjastamistaotlusega, määratlege privaatvõtme fail. ❏ Kui sertifikaat on PKCS#12-vormingus ja see on hangitud arvutist saadetud sertifikaadi allkirjastamistaotlusega, looge privaatvõtit sisaldav fail.
	Põhjus: Olete uuesti importinud PEM/DER-vormingus sertifikaadi, mis on hangitud rakendusest Web Config saadetud sertifikaadi allkirjastamistaotlusega. **Tegevusmeede:** Kui sertifikaat on PEM/DER-vormingus ja see on hangitud rakendusest Web Config saadetud sertifikaadi allkirjastamistaotlusega, saate sertifikaati importida vaid ühe korra.
Setup failed.	**Põhjus:** Konfigureerimise lõpetamine ei ole võimalik skanneri ja arvuti vahelise sideühenduse nurjumise tõttu või ei ole faili lugemine teatud vigadest tingitult võimalik. **Tegevusmeede:** Kontrollige määratud faili ja sideühendust ning importige fail seejärel uuesti.

Seotud teave

➡ „Digitaalsest sertimisest” lk 101

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 allkirjastamistaotlust kasutades, ei saa te kustutatud sertifikaati uuesti importida. Looge sertifikaadi allkirjastamistaotlus ja hankige uus sertifikaat.

Seotud teave

➡ „CA-allkirjastatud sertifikaadi importimine” lk 103

➡ „Sertimiskeskuse allkirjastatud sertifikaadi kustutamine” lk 104

Authentication Settings

Authentication Settings: info. 128

Authentication Method: info. 129

Seadistamise tarkvara. 131

Skanneri püsivara värskendamine. 131

Autentimisseadme ühendamine ja konfigureerimine. 131

Teabe registreerimine ja seadistamine. 136

Aruanded Job History rakenduses Epson Device Admin. 152

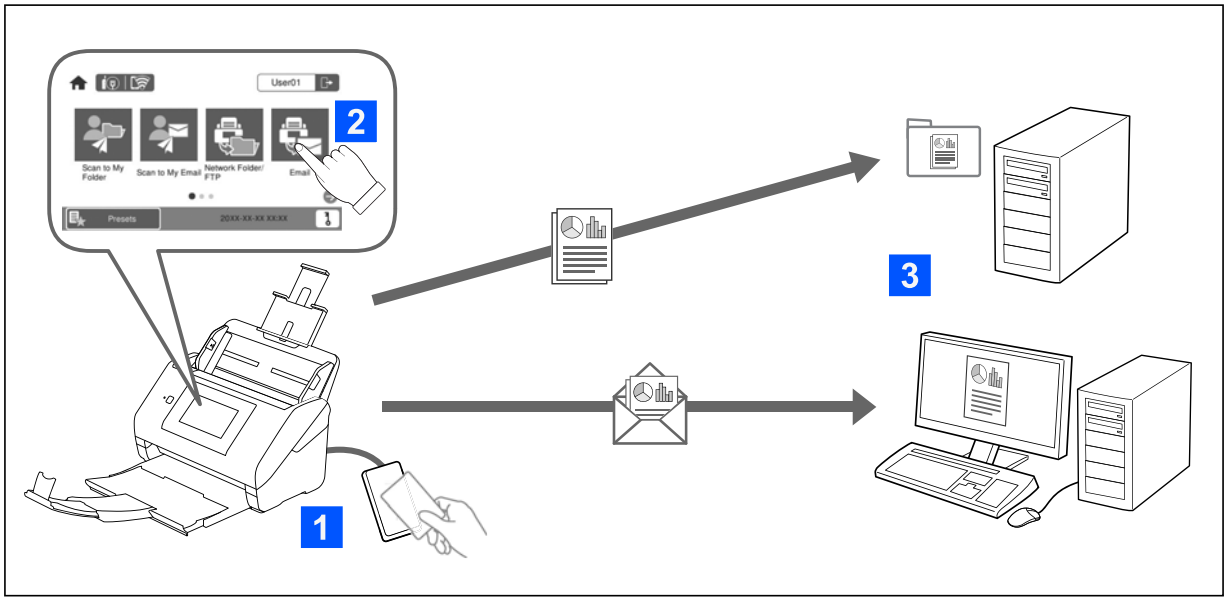
Juhtpaneelilt administraatorina sisselogimine. 152

Funktsiooni Authentication Settings keelamine. 152

Funktsiooni Authentication Settings teabe kustutamine (Taasta vaikesätted). 153

Probleemide lahendamine. 153

Authentication Settings: info



Kui Authentication Settings on lubatud, on skannimise käivitamiseks vaja kasutaja autentida. Saate seadistada skannimismeetodid, mida iga kasutaja kasutada saab, et hoida ära tahtmatud toimingud.

Saate määrata skannimise sihtkohaks autenditud kasutaja meiliaadressi (Scan to My Email) või salvestada iga kasutaja andmed isiklikku kausta (Scan to My Folder). Samuti saate määrata muud skannimismeetodid.

Märkus.

❏ *Kui Authentication Settings on lubatud, ei saa te skannida arvutist ega nutiseadmest.*

❏ *Lisaks selles juhendis kirjeldatud funktsioonile Authentication Settings saate luua autentimissüsteemi ka autentimisserveri abil. Süsteemi loomiseks kasutage rakendust Document Capture Pro Server Authentication Edition (lühendatud nimega Document Capture Pro Server AE). Lisateabe saamiseks võtke ühendust kohaliku Epsoni esindusega.*

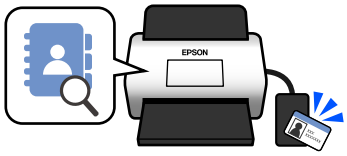
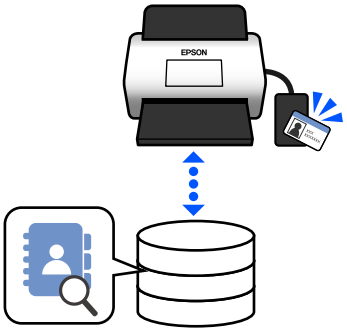
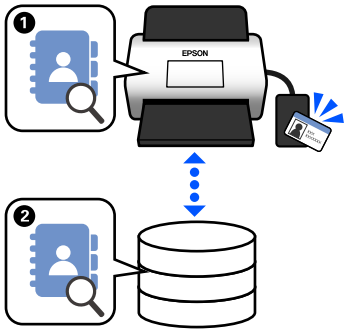
Authentication Settings: saadaval funktsioonid

Skannimisfunktsioon juhtpaneelil	Authentication Settings	
	Kui on lubatud	Kui on keelatud
Skanni Minu kausta Salvestab pildid autenditud kasutajale määratud kausta.	✓	-
Skanni minu e-posti Saadab pildid autenditud kasutaja meiliaadressile.	✓	-
Skanni võrgukausta/FTP-sse Salvestab pildid võrgukausta.	✓	✓

Skannimisfunktsioon juhtpaneelil	Authentication Settings	
	Kui on lubatud	Kui on keelatud
Skanni arvutisse Salvestab pildid ühendatud arvutisse, kasutades programmis Document Capture Pro (Windows) / Document Capture (Mac OS) loodud töid. * Kui Authentication Settings on lubatud, saate kasutada ainult loendis **Eelsätted** registreeritud töid.	✓*	✓
Skanni meili Saadab pildid teie valitud meiliaadressile.	✓	✓
Skannimine pilve Saadab pildid teie valitud pilveteenusesse.	✓	✓
Skanni USB-draivile Salvestab pildid skanneriga ühendatud USB-draivile. See on saadaval vaid siis, kui skanneriga ei ole ühendatud autentimisseadet.	✓	✓
Skanni WSD-le Salvestab pildid WSD-funktsiooni abil ühendatud arvutisse.	-	✓
Eelsätted Registreerida saab kuni 48 skannimisfunktsiooni eelsätet. Kuni viis üksust Eelsätted on võimalik eraldada kasutajatele, kes on registreeritud suvandis Local DB. Eraldatud üksused Eelsätted on saadaval ainult sellele kasutajale. Üksusi Eelsätted, mida pole ühelegi kasutajale eraldatud, saavad kasutada kõik kasutajad.	✓	✓

Authentication Method: info

See skanner võimaldab autentimist järgmiste meetoditega, ilma et oleks vaja luua autentimisserverit.

	Local DB	LDAP	Local DB and LDAP
Kasutajateabe asukoht	**Skanneri mälu** See autentimismeetod kontrollib skanneris registreeritud kasutajateavet ja võrdleb seda skannimisfunktsiooni kasutava kasutajaga.	**LDAP-server*** See autentimismeetod kontrollib skanneriga sünkroonitud LDAP-serveri kasutajateavet. Kuna skanneri vahemällu saab ajutiselt salvestada kuni 300 kasutajateabe kirjet, saab LDAP-serveri mittetöötamise korral autentimiseks kasutada vahemälu. * Server, mis pakub kataloogiteenust, mis saab suhelda LDAP-ga.	**Skanneri mälu ja LDAP-server** Kontrollige esmalt skanneris registreeritud kasutajateavet (❶) ja kui vastet pole, võrrelge kasutajateavet LDAP-serveris (❷).
			
Registreeritud kasutajate arv	50 (skanneri mälu)	Piiramatu (LDAP-server)	50 (skanneri mälu) Piiramatu (LDAP-server)
Skanneri vahemälu	-	300	Max 300 (50 vahemälukohta on jagatud üksusega User Settings andmebaasis Local DB)
Sisselogimismeetodid	Saate kasutada ükskõik millist järgmistest meetoditest. ❏ Hoidke üleval autentimiskaarti või sisestage **User ID** ja **Password** ❏ Hoidke üleval autentimiskaarti või sisestage **ID Number** ❏ Sisestage **User ID** ja **Password** ❏ Sisestage **User ID** ❏ Sisestage **ID Number**		
Funktsiooni „Skannimine asukohta“ piirangud	Määrake igale kasutajale individuaalselt	Samad sätted kõigile LDAP kasutajatele	Local DB kasutajad: määrake individuaalselt LDAP kasutajad: samad sätted kõigile kasutajatele
Üksuste Eelsätted eraldamine kasutajatele	Kuni 5 kasutaja kohta	- (Ei saa määrata individuaalselt)	Local DB kasutajad: kuni 5 kasutaja kohta LDAP kasutajad: -

Seadistamise tarkvara

Seadistage rakendusega Web Config või Epson Device Admin.

❏ Kui kasutate rakendust Web Config, peate skanneri seadistamiseks kasutama veebibrauserit.

„Web Config” lk 36

❏ Kui kasutate rakendust Epson Device Admin, saate korraga seadistada mitu skannerit, kasutades konfiguratsioonimalli.

„Epson Device Admin” lk 37

Skanneri püsivara värskendamine

Enne funktsiooni Authentication Settings lubamist värskendage skanneri püsivara uusimale versioonile. Ühendage esmalt skanner internetti.

Oluline teave:

Ärge lülitage arvutit või skannerit värskendamise ajal välja.

Seadistamine rakenduses Web Config.

Valige vahekaart **Device Management** > **Firmware Update** ja järgige seejärel püsivara värskendamiseks ekraanil kuvatud juhtnööre.

Seadistamine rakenduses Epson Device Admin.

Valige seadmeloendi kuval **Home** > **Firmware** > **Update** ja järgige seejärel püsivara värskendamiseks ekraanil kuvatud juhtnööre.

Märkus.

Kui uusim püsivara on juba installitud, pole värskendada vaja.

Autentimisseadme ühendamine ja konfigureerimine

Kui soovite ühendada autentimisseadme (nt IC-kaardilugeja) ja seda kasutada, peate seadme esmalt konfigureerima. See pole vajalik, kui te ei kasuta autentimisseadet.

Seotud teave

➡ „Autentimisseadme ühendamine” lk 134

➡ „Autentimisseadme sätted” lk 135

Ühilduvate kaardilugejate loend

Loendis olevate kaaridlugejate töö ei ole tagatud.

Jah: toetatud (ID-teavet saab lugeda standardsete kaardilugeja sätetega)

Ei: pole ühilduv

Valmistaja	Mudel	Mudelikood	Autentimiskaart							Režiim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Jah	Jah*1	Jah*1	Jah*1	Ei	Ei	Ei	Klaviatuur
RF IDEAS	pcProx	RDR-7081BKU	Jah*1	Ei	Jah	Jah	Ei	Ei	Ei	Klaviatuur
RF IDEAS	pcProx	RDR-7581AKU	Jah	Ei	Jah*1	Jah*1	Ei	Ei	Ei	Klaviatuur
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Ei	Ei	Jah	Jah	Ei	Ei	Ei	Klaviatuur
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Jah	Ei	Jah	Jah	Jah	Jah	Jah	Klaviatuur
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Jah	Jah	Jah	Jah	Jah	Jah	Jah	Klaviatuur
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Jah	Jah	Jah	Jah	Jah	Jah	Jah	Klaviatuur
ELATEC	TWN4 Slim	T4QC-FC3B7	Jah	Jah	Jah	Jah	Jah	Jah	Jah	Klaviatuur
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Jah	Jah	Jah	Jah	Jah	Ei	Jah	Klaviatuur*1
ACS	ACR122U	ACR122U	Ei	Ei	Jah*2	Jah*2	Jah	Ei	Jah*2	PC/SC

Valmistaja	Mudel	Mudelikood	Autentimiskaart							Režiim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ACS	ACR1252	ACR1252	Ei	Ei	Jah*2	Jah*2	Jah	Jah	Jah*2	PC/SC
Sony	PaSoRi	RC-S330/S	Ei	Ei	Jah*2	Jah*2	Jah*2	Jah*2	Jah*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Ei	Ei	Jah*2	Jah*2	Jah*2	Jah*2	Jah*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Jah	Jah	Jah	Jah	Jah	Jah	Jah	Klaviatuur
DMZ	Leitor RFID Multi-125	DMZ087	Ei	Jah	Ei	Ei	Ei	Ei	Ei	Klaviatuur
DMZ	Leitor RFID Mifare	DMZ088	Ei	Ei	Jah	Jah	Ei	Ei	Ei	Klaviatuur
DMZ	Biometric & RFID Reader	DMZ073	Ei	Jah	Ei	Ei	Ei	Ei	Ei	Klaviatuur
inepro	SCR708	SCR708	Jah*1	Jah*1	Jah*1	Jah*1	Jah*1	Jah*1	Jah*1	Klaviatuur
Y Soft	YU030888 001	MU0388	Jah	Jah	Jah	Jah	Jah	Jah	Jah	Klaviatuur
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Ei	Ei	Jah	Jah	Ei	Ei	Jah	Klaviatuur
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Ei	Ei	Jah	Jah	Ei	Ei	Jah	Klaviatuur

Valmistaja	Mudel	Mudelikood	Autentimiskaart							Režiim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
NT-ware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Jah	Jah	Jah	Jah	Jah	Jah	Jah	Klaviatuur
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Jah*1	Jah*1	Jah*1	Jah*1	Ei	Ei	Ei	Klaviatuur
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Jah	Jah	Jah	Jah	Jah	Jah	Ei	Klaviatuur

*1 Peate muutma kaardilugeja sätteid, kasutades kaardilugeja valmistaja tarkvara.

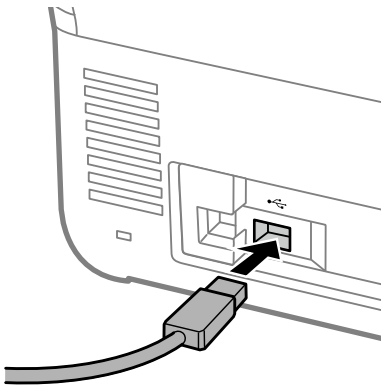
*2 Kui teil on autentimiseks vaja kasutada kaardil olevaid andmeid kindlast kohast, mis ei ole standardne tuvastusteabe koht, ning peate selleks muutma toote sätteid, võtke ühendust Epsoni partneri või kohaliku esindajaga, et saada lisateavet toote seadistamise kohta.

Autentimisseadme ühendamine

Oluline teave:

Kui ühendate autentimisseadme mitme skanneriga, kasutage sama mudelikoodiga toodet.

Ühendage kaaridlugeja 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**.

Autentimisseadme sätted

Määrake autentimiskaardilt saadud autentimisteabe lugemisvorming.

Autentimisseadmele saate määrata järgmise lugemismeetodi.

❏ Autentimiskaardi kindla koha lugemine, nagu töötaja number või personaalne ID.

❏ Autentimiskaardi teabe kasutamine, välja arvatud UID (autentimiskaardi teave, nagu seerianumber).
Tööparameetrire loomiseks saate kasutada tööriista. Küsige üksikasju edasimüüjalt.

Märkus.
Erinevate tootjate autentimiskaartide kasutamine.

Kui kasutate UID-kaarditeavet (kaardi ID-teave, nagu seerianumber), saate kasutada segamini erinevat tüüpi autentimiskaarte. Segamine ei ole võimalik, kui kasutatakse muud kaarditeavet.

Seadistamine rakenduses Web Config.

Valige vahekaart **Device Management** > **Card Reader**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallis **Administrator Settings** > **Authentication Settings** > **Card Reader**.

Kirje	Selgitus
Vendor ID	Määrake autentimisseadme ettevõtja ID, mis piirab kasutamise vahemikku 0000 kuni FFFF, kasutades 4 tärki. Kui te piirangut seada ei soovi, valige 0000.
Product ID	Määrake autentimisseadme toote ID, mis piirab kasutamise vahemikku 0000 kuni FFFF, kasutades 4 tärki. Kui te piirangut seada ei soovi, valige 0000.
Operational parameter	Määrake autentimisseadme tööparameeter vahemikus 0 kuni 8192 tärki. Saadaval on A–Z, a–z, 0–9, +, /, =, tühik ja reavahe.
Card Reader	Valige autentimisseadme teisendusvorming. Saate vormingu üksikasjad üle vaadata. Kasutage linki kirje kirjelduses.
Authentication Card ID save format	Valige ID-kaardi autentimisteabe teisendusvorming. Saate vormingu üksikasjad üle vaadata. Kasutage linki kirje kirjelduses.
Set card ID range	Lubage lugemiskoha määrang.
Text Start Position	Määrake teksti algpunkt ID-teabe lugemiseks. Määratav on vahemik 1 kuni 4096.
Number of Characters	Määrake tärkide arv, mis loetakse ID-teabe algpunktist. Määratav on vahemik 1 kuni 4096.

Teabe registreerimine ja seadistamine

Seadistamine

Tehke lähtuvalt funktsioonist Authentication Method ja kasutatavast skannimismeetodist vajalikud sätted.

Oluline teave:

Enne kui alustate seadistamist, kontrollige skanneri kellaaja sätet.

Kui kellaaja säte on vale, kuvatakse teade „License is expired“ (Litsents on aegunud), mis võib kaasa tuua skanneri seadistamise nurjumise. Õige kellaaja säte on vajalik ka selleks, et kasutada turvafunktsioone nagu SSL/TLS või IPsec. Kellaaega saate seadistada järgmiselt.

- ❏ *Web Config: vahekaart **Device Management** > **Date and Time** > **Date and Time**.*
- ❏ *Skanneri juhtpaneel: **Sätted** > **Põhisätted** > **Kuupäeva/kellaaja sätted**.*

Sätted	Local DB	LDAP	Local DB and LDAP
Autentimise lubamine Enne autentimissätete tegemist peate autentimise lubama. „Autentimise lubamine“ lk 137	✓	✓	✓
Authentication Settings Funktsiooni Authentication Method seadistamine ja kasutaja autentimine. „Authentication Settings“ lk 137	✓	✓	✓
User Settings: registreerimine Registreerige iga kasutaja sätted. Kasutajateabe saab ka kogumina registreerida, kasutades CSV-faili. „User Settings: registreerimine“ lk 139	✓	–	✓
Sünkroonimine üksusega LDAP Server Määrake LDAP-serveri sünkroonimissätted. „Sünkroonimine üksusega LDAP Server“ lk 145	–	✓	✓
Üksuse Email Server seadistamine Määrake meiliserveri sätted. Seadistage see, kui kasutate funktsioone, milleks on vajalikud meiliserveri sätted, nagu Scan to My Email. „Meiliserveri seadistamine“ lk 148	✓	✓	✓
Funktsiooni Scan to My Folder seadistamine Määrake sihtkaustad. Seadistage see, kui kasutate funktsiooni Scan to My Folder. „Funktsiooni Scan to My Folder seadistamine“ lk 149	✓	✓	✓

Sätted	Local DB	LDAP	Local DB and LDAP
Customize One-touch Functions Seadistage see, kui muudate üksusi, mida kuvatakse skanneri juhtpaneelil. Skanneri juhtpaneelil võib kuvada ainult vajalikud ikoonid, samuti saab muuta ikoonide järjekorda. „Customize One-touch Functions" lk 151	✓	✓	✓

Autentimise lubamine

Enne autentimissätete tegemist peate autentimise lubama.

Seadistamine rakenduses Web Config.

Valige **Sees (seade/LDAP-server)** vahekaardilt **Product Security** > **Basic** > **Authentication**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallil **Sees (seade/LDAP-server)** asukohast **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Märkus.
Kui lubate skanneris funktsiooni Authentication Settings, lubatakse ka juhtpaneeli funktsioon Lukustamise sätted. Kui Authentication Settings on lubatud, ei saa juhtpaneeli lukust avada.

Isegi kui te funktsiooni Authentication Settings keelate, jääb Lukustamise sätted lubatuks. Kui soovite selle keelata, saate asjakohased sätted teha juhtpaneelil või rakenduses Web Config.

Seotud teave

➡ „Funktsiooni Lukustamise sätted seadistamine juhtpaneelil" lk 89

➡ „Funktsiooni Lukustamise sätted seadistamine rakenduses Web Config" lk 89

Authentication Settings

Funktsiooni Authentication Method seadistamine ja kasutaja autentimine.

Seadistamine rakenduses Web Config.

Valige vahekaart **Product Security** > **Authentication Settings**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallis **Administrator Settings** > **Authentication Settings** > **Authentication Settings**.

Kirje	Selgitus
Authentication Method	Valige Authentication Method. ❏ Local DB Autentimine skanneris registreeritud sätete User Settings abil. Kasutaja tuleb skanneris registreerida. ❏ LDAP Kasutage autentimiseks skanneriga sünkroonitud LDAP-serveri kasutajateavet. Selleks peate esmalt konfigureerima LDAP-serveri sätted. ❏ Local DB and LDAP Kasutage autentimiseks skanneris registreeritud või skanneriga sünkroonitud LDAP-serveri kasutajateavet. Selleks peate registreerima kasutaja skanneris ja seadistama LDAP-serveri.
How to Authenticate User	Valige kasutaja autentimisviis. ❏ Card or User ID and Password Kasutage kasutajate autentimiseks autentimiskaarti. Samuti võite autentimiseks kasutada kasutaja ID-d ja parooli. ❏ User ID and Password Kasutage kasutajate autentimiseks kasutaja ID-d ja parooli. Kui valite selle funktsiooni, ei saa te kasutada autentimiseks autentimiskaarti. ❏ User ID Kasutage kasutajate autentimiseks ainult kasutaja ID-d. Parooli ei ole vaja määrata. ❏ Card or ID Number Kasutage kasutajate autentimiseks autentimiskaarti. Samuti võite kasutada üksust ID Number. ❏ ID Number Kasutage kasutajate autentimiseks ainult ID-numbrit.
Allow users to register authentication cards	Lubage see, kui lubate kasutajatel registreerida süsteemis autentimiskaardi. Kui **LDAP** on valitud suvandi **Authentication Method** sätteks, ei saa seda valida. Lugege lisateavet võimaluste kohta, kuidas kasutajad saavad oma autentimiskaardi registreerida, jaotisest „Autentimiskaardi registreerimine“ dokumendis *Kasutusjuhend*.
The Minimum Digit Number of ID Number	Valige minimaalne kohtade arv ID-numbris.
Minimum Number of Bytes for User ID (UTF-8)	Valige User ID miinimumbaidid. Toetatud ainult Euroopas, Lähis-Idas ja Aafrikas.
Caching for LDAP authenticated users	Kui kasutate autentimist LDAP-serveriga, saate määrata, kas salvestada kasutajateave vahemällu.
Use user information in SMTP authentication	Kui kasutate autentimiseks kasutaja ID-d ja parooli, saate määrata, kas kasutada kasutajateavet SMTP-autentimiseks. Süsteem kasutab viimati sisse logitud kasutaja ID-d ja parooli.
Restrictions for LDAP authenticated users	Kui kasutate LDAP-d, saate määrata kasutajale saadaval funktsioonid.

User Settings: registreerimine

Registreerige üksused User Settings, mida kasutatakse kasutaja autentimiseks. Saate registreerimiseks kasutada ükskõik millist järgmistest meetoditest.

❏ Üksuste User Settings registreerimine ükshaaval (Web Config)

❏ Mitme üksuse User Settings registreerimine kogumina CSV-faili kasutades (Web Config)

❏ Üksuste User Settings registreerimine mitmesse skannerisse kogumina, kasutades konfiguratsioonimalli (Epson Device Admin)

Seotud teave

➡ „Üksuste User Settings registreerimine individuaalselt (Web Config)” lk 139

➡ „Mitme üksuse User Settings registreerimine CSV-faili abil (Web Config)” lk 140

➡ „Üksuste User Settings registreerimine mitmesse skannerisse kogumina (Epson Device Admin)” lk 143

Üksuste User Settings registreerimine individuaalselt (Web Config)

Avage Web Config, valige vahekaart **Product Security** > **User Settings** > **Add** ja sisestage seejärel üksused User Settings.

Kirje	Selgitus
User ID	Sisestage kasutaja ID, mida tahate kasutada autentimiseks, kasutades 1 kuni 83 baiti koodis Unicode (UTF-8). Kuna kasutaja ID pole tõstutundlik, võite sisselogimisel kasutada nii väike- kui ka suurtähti.
User name Display	Sisestage skanneri juhtpaneelil kuvatav kasutajanimi pikkusega kuni 32 tärki koodis Unicode (UTF-16). Selle võite tühjaks jätta.
Password	Sisestage parool, mida tahate kasutada autentimiseks, kasutades kuni 32 tärki koodis ASCII. Parool on tõstutundlik. Kui **User ID** on valitud suvandi **How to Authenticate User** sätteks, jätke see tühjaks.
Authentication Card ID	Sisestage autentimiskaardi ID, kasutades kuni 116 tärki koodis ASCII. Selle võite tühjaks jätta. Kui lubate sätte **Allow users to register authentication cards** suvandis **Authentication Settings**, näidatakse kasutajate registreeritud tulemust.
ID Number	See üksus kuvatakse, kui **Card or ID Number** või **ID Number** on valitud suvandis **Authentication Settings** > **How to Authenticate User**. Sisestage number, mille pikkus jääb suvandis **Authentication Settings** > **The Minimum Digit Number of ID Number** valitud sätte sisse ning pole pikem kui 8 kohta.
Auto Generate	See üksus kuvatakse, kui **Card or ID Number** või **ID Number** on valitud suvandis **Authentication Settings** > **How to Authenticate User**. Klõpsake, et luua automaatselt ID-number, milles on sama palju kohti, nagu määrasite suvandis **The Minimum Digit Number of ID Number**.

Kirje	Selgitus
Department	Sisestage osakonna nimi ja muu kasutajat tuvastav teave, kasutades kuni 40 tärki koodis Unicode (UTF-16). Selle võite tühjaks jätta.
Email Address	Sisestage kasutaja meiliaadress, kasutades kuni 200 tärki koodis ASCII. Seda kasutatakse funktsiooni **Scan to My Email** sihtkohana. Selle võite tühjaks jätta.
Scan to My Folder	Kui **Individual** on valitud suvandis **Scan to My Folder** > **Setting Type**, seadistage salvestamise sihtkohad individuaalselt. Vt järgmist, et saada lisateavet sätteüksuste kohta. „Funktsiooni Scan to My Folder seadistamine" lk 149
Restrictions	Funktsioone saab iga kasutaja jaoks piirata. Valige funktsioon, mida lubate kasutada.
Presets	Saate seadistada kuni viis eelsätet, mis on saadaval skanneris registreeritud üksusest Presets ainult valitud kasutajale. ❏ Üksusi Presets, mis on määratud kasutajale, saab kasutada ainult see kasutaja. Üksusi Presets, mida pole ühelegi kasutajale eraldatud, saavad kasutada kõik kasutajad. ❏ Kui kasutajale on saadaval ainult üks Presets, laaditakse see pärast autentimist automaatselt. Kui saadaval on mitu üksust Presets, kuvatakse pärast autentimist üksuste Presets loend. ❏ Te ei saa luua ega kuvada üksusi Presets, mis kasutavad funktsioone, mis on suvandis **Restrictions** keelatud.

Mitme üksuse User Settings registreerimine CSV-faili abil (Web Config)

Sisestage iga kasutaja seaded CSV-faili ja registreerige need kogumina.

CSV-faili loomine

Looge CSV-fail üksuste User Settings importimiseks.

Märkus.
Kui registreerite eelnevalt ühe või mitu üksust User Settings ja ekspordite seejärel vormindatud faili (CSV-fail), saate kasutada registreeritud sätet viitena sätteüksuste sisestamiseks.

1. Avage Web Config ja valige vahekaart **Product Security** > **User Settings**.
2. Klõpsake nuppu **Export**.
3. Valige suvandis **File Format** failivorming.

   Tehke valik allpool toodud teabe abil.

Kirje	Selgitus
CSV UTF-16 (Tab delimited)	Valige, kui kasutate faili redigeerimiseks rakendust Microsoft Excel. Iga parameeter on ümbritsetud nurksulgudega „[ ]". Sisestage parameetrid nurksulgudesse „[ ]". Kui te faili uuendate, soovitame selle üle kirjutada. Kui te salvestate uut faili, valige failivorminguks Unicode-tekst (*.txt).
CSV UTF-8 (Comma delimited)	Valige, kui kasutate faili redigeerimiseks tekstiredaktorit või makrot ilma rakenduseta Microsoft Excel.
CSV UTF-8 (Semicolon delimited)	

4. Klõpsake nuppu **Export**.

5. Redigeerige CSV-faili ja salvestage see arvutustabeli rakenduses, nagu Microsoft Excel, või salvestage see tekstiredaktoris.

> ***Oluline teave:***
> *Ärge muutke faili redigeerides kodeerimis- ega päiseteavet.*

CSV-faili sätteüksused

Kirje	Sätted ja selgitused
UserID	Sisestage autentimiseks kasutaja ID vahemikus 1 kuni 83 baiti koodis Unicode.
UserName	Sisestage skanneri juhtpaneelil kuvatav kasutajanimi pikkusega kuni 32 tärki koodis Unicode. Selle võite tühjaks jätta.
Password	Sisestage autentimiseks kasutatav parool pikkusega kuni 32 tärki koodis ASCII. Importimise korral seatakse see parooliks üksuse **EncPassword** asemel. Kui **User ID** on valitud suvandi **How to Authenticate User** sätteks, jätke see tühjaks. Eksportimise korral on see alati tühi.
AuthenticationCardID	Seadistage kaardi autentimise lugemise tulemus. Kui lubate sätte **Allow users to register authentication cards** suvandis **Authentication Settings**, näidatakse kasutajate registreeritud tulemust. Sisestage kuni 116 tärki koodis ASCII. Selle võite tühjaks jätta.
IDNumber	See üksus kuvatakse, kui **Card or ID Number** või **ID Number** on valitud suvandis **Authentication Settings** > **How to Authenticate User**. Sisestage number, mille pikkus jääb suvandis **Authentication Settings** > **The Minimum Digit Number of ID Number** valitud sätte sisse ning pole pikem kui 8 kohta. ID-number ei saa olla korduv. Kui seda korratakse, kuvatakse faili importimisel tõrge. Kui see tühjaks jäetakse, määratakse sellele automaatselt number.
Department	Sisestage omal valikul osakonna nimi, et kasutajate vahel vahet teha. Sisestage kuni 40 tärki koodis Unicode. Selle võite tühjaks jätta.

Kirje	Sätted ja selgitused
MailAddress	Seadistage kasutajate jaoks meiliaadress. Seda kasutatakse funktsiooni **Scan to My Email** sihtkohana. Võite kasutada tärke A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Sisestage kuni 200 tärki. Esimese tärgina ei saa kasutada koma (,). Selle võite tühjaks jätta.
FolderProtocol	Määrake funktsiooni Scan to My Folder tüüp. Võrgukaust / FTP (SMB): 0, FTP: 1
FolderPath	Määrake funktsioonile Scan to My Folder sihtkoht salvestamiseks.
FolderUserName	Määrake funktsioonile Scan to My Folder kasutajanimi.
FolderPassword	Määrake parool sihtkausta autentimiseks funktsioonile Scan to My Folder, sisestage kuni 32 tärki koodis ASCII. Importimise korral seatakse see parooliks üksuse **EncPassword** asemel. Eksportimise korral on see alati tühi.
FtpPassive	Seadistage FTP-serveri ühendusrežiim, kui **FTP** on valitud suvandi **Type** sätteks funktsioonile Scan to My Folder. Aktiivrežiim: 0, passiivrežiim: 1
FtpPort	Määrake pordinumber vahemikus 0 kuni 65535 skannitud andmete saatmiseks FTP-serverisse, kui **FTP** on valitud suvandi **Type** sätteks funktsioonile Scan to My Folder.
ScanToMemory	Seadke piirangud funktsioonile Scan to USB Drive. Pole lubatud: 0, lubatud: 1
ScanToMail	Seadke piirangud funktsioonile Scan to Email. Sätte **Skanni minu e-posti** saab valida ainult siis, kui **Scan to Email** on lubatud. Pole lubatud: 0, lubatud: 1
ScanToFolder	Seadke piirangud funktsioonile Scan to Network Folder/FTP. Sätte **Skanni Minu kausta** saab valida ainult siis, kui **Scan to Network Folder/FTP** on lubatud. Pole lubatud: 0, lubatud: 1
ScanToCloud	Seadke piirangud funktsioonile Scan to Cloud. Pole lubatud: 0, lubatud: 1
ScanToComputer	Seadke piirangud funktsioonile Skanni arvutisse. Pole lubatud: 0, lubatud: 1
PresetIndex	Seadistage üksused Presets, mida soovite kasutajaga seostada. Saate seadistada kuni viis üksuse Presets komaga eraldatud registreerimisnumbrit.
EncPassword	Kasutajasätete eksportimise korral krüptitakse suvandi **Password** parameeter, seejärel kodeeritakse väärtus BASE64 abil ja väljastatakse. Kui imporditakse uue parooliga suvandis **Password**, siis seda väärtust eiratakse. Kui **Password** on tühjaks jäetud, kasutatakse seda väärtust ja parool jääb samaks, mis see oli enne eksportimist.

Kirje	Sätted ja selgitused
EncFolderPassword	Eksportimise korral krüptitakse suvandi **FolderPassword** parameeter, seejärel kodeeritakse väärtus BASE64 abil ja väljastatakse. Kui imporditakse uue parooliga suvandis **FolderPassword**, siis seda väärtust eiratakse. Kui **FolderPassword** on tühjaks jäetud, kasutatakse seda väärtust ja parool jääb samaks, mis see oli enne eksportimist.

CSV-faili importimine

1. Avage Web Config ja valige vahekaart **Product Security** > **User Settings**.
2. Klõpsake nuppu **Import**.
3. Valige fail, mida soovite importida.
4. Klõpsake nuppu **Import**.
5. Lugege kuvatud teave läbi ja klõpsake nuppu **OK**.

Üksuste User Settings registreerimine mitmesse skannerisse kogumina (Epson Device Admin)

Saate registreerida üksused User Settings, mida kasutatakse Local DB-s kogumina, kasutades LDAP-serverit või CSV-/ENE-faili.

Märkus.
*ENE-fail on Epsonilt saadud kahendfail, mis krüptib ja salvestab teabe üksuse **Contacts** jaoks isikliku teabena ja üksustena User Settings. Selle saab eksportida Epson Device Administ ning võimalik on määrata parool. See on kasulik, kui soovite importida üksused User Settings varundfailist.*

Importimine CSV-/ENE-failist

1. Valige konfiguratsioonimallis **Administrator Settings** > **Authentication Settings** > **User Settings**.
2. Klõpsake nuppu **Import**.
3. Valige **CSV or ENE File** suvandis **Import Source**.
4. Klõpsake nuppu **Browse**.
   Kuvatakse faili valimise kuva.
5. Valige fail, mida soovite importida, et see avada.
6. Valige importimismeetod.
   - ❏ Overwrite and Add: kui sama kasutaja ID on juba olemas, siis kirjutab selle üle, kui seda ei ole olemas, lisab uue ID.
   - ❏ Replace All: asendab kõik kasutajasätetega, mida soovite importida.

7. Klõpsake nuppu **Import**.

   Kuvatakse sätte kinnituskuva.

8. Klõpsake nuppu **OK**.

   Kuvatakse valideerimistulemus.

   Märkus.
   - ❏ *Kui imporditavate kasutajasätete arv on suurem kui lubatud, kuvatakse teade, mis käsib teil osa kasutajasätteid kustutada. Kustutage enne importimist üleliigsed kasutajasätted.*
   - ❏ *Valige kasutajasätted, mida soovite enne importimist kustutada, ja klõpsake seejärel nuppu **Delete**.*

9. Klõpsake nuppu **Import**.

   Kasutajasätted imporditakse konfiguratsioonimalli.

Importimine LDAP-serverist

1. Valige konfiguratsioonimallis **Administrator Settings** > **Authentication Settings** > **User Settings**.
2. Klõpsake nuppu **Import**.
3. Valige **LDAP** suvandis **Import Source**.
4. Klõpsake nuppu **Settings**.

   Kuvatakse üksuse **LDAP Server** sätted.

   Märkus.
   LDAP-serveri säte on ette nähtud kasutajasätete importimiseks LDAP-serverist. Imporditud (kopeeritud) kasutajasätteid kasutatakse kasutajate autentimiseks skannerit kasutades.

   *Samas, kui valite autentimismeetodi sätteks **LDAP** või **Local DB and LDAP**, autenditakse kasutajad LDAP-serveriga suheldes.*

5. Seadistage kõik kirjed.

   Kui impordite kasutajasätteid LDAP-serverist, saate lisaks LDAP sätetele konfigureerida ka järgmised sätted.

   Muude kirjete kohta lugege seotud teabest.

Kirje			Selgitus
LDAP Server Settings	LDAP Server Type		Võimaldab valida LDAP-serveri tüübi.
Search Settings	Search Filter		Saate määrata teksti, mida kasutatakse LDAP otsingufiltris. Otsinguteksti redigeerimiseks valige **Custom**.
	Options	Type	Saate valida funktsioonile **Scan To My Folder** salvestamise sihtkoha tüübi.
		Connection Mode	Kui suvandi **Type** säte on **FTP**, saate määrata FTP-ühendusrežiimi.
		Port Number	Kui suvandi **Type** säte on **FTP**, saate määrata pordinumbri, mida tahate kasutada.

6. Kontrollige vajaduse korral ühendust, klõpsates nuppu **Connection Test**.

   Hangib ja kuvab LDAP-serverist 10 kasutajasätet.

7. Klõpsake nuppu **OK**.
8. Valige importimismeetod.
   - ❏ Overwrite and Add: kui sama kasutaja ID on juba olemas, siis kirjutab selle üle, kui seda ei ole olemas, lisab uue ID.
   - ❏ Replace All: asendab kõik kasutajasätetega, mida soovite importida.
9. Klõpsake nuppu **Import**.

   Kuvatakse sätte kinnituskuva.
10. Klõpsake nuppu **OK**.

    Kuvatakse valideerimistulemus.
11. Klõpsake nuppu **Import**.

    Kasutajasätted imporditakse konfiguratsioonimalli.

Seotud teave

➡ „LDAP-serveri konfigureerimine” lk 145
➡ „LDAP-serveri otsingusätete konfigureerimine” lk 147

Sünkroonimine üksusega LDAP Server

Seadistage skanneri jaoks üksuse LDAP Server sätted.

Seadistage vastavalt vajadusele nii esmase kui ka sekundaarse serveri sätted.

Märkus.
*Üksuse **LDAP Server** sätteid jagatakse üksusega **Contacts**.*

Saadaval teenused

Toetatud on järgmised kataloogiteenused.

Teenuse nimi	Versioon
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

LDAP-serveri konfigureerimine

LDAP-serveri kasutamiseks tuleb LDAP-server esmalt konfigureerida.

Seadistamine rakenduses Web Config.

Valige vahekaart **Network** > **LDAP Server** > **Basic (Primary Server)** või **Basic (Secondary Server)**.

Kui **Kerberos Authentication** määratakse suvandi **Authentication Method** sätteks, valige Kerberose seadistamiseks **Network** > **Kerberos Settings**.

Seadistamine rakenduses Epson Device Admin.

Valige **Network** > **LDAP server** > **Server Settings (Primary Server)** või **Server Settings (Secondary Server)** konfiguratsioonimallilt.

Kui **Kerberos Authentication** määratakse suvandi **Authentication Method** sätteks, valige Kerberose seadistamiseks **Network — Security** > **Kerberos Settings**.

Kirje	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 sidekriipse, välja arvatud aadressi alguses ja lõpus.
LDAP server Port Number (Port number)	Sisestage LDAP-serveri pordinumber vahemikus 1–65535.
Secure Connection	Määrake skanneri autentimismeetod juurdepääsuks LDAP-serverile. Valiku **None** korral on side krüptimata. Soovitame kasutada muud sätet kui **None**.
Certificate Validation	LDAP-serveri sertifikaat autenditakse, kui see on lubatud. Soovitame kasutada sätet **Enable**. Seadistamiseks peab **CA Certificate** olema skannerisse imporditud.
Search Timeout (sec)	Määrake aeg otsingu tegemiseks vahemikus 5–300 sekundit, misjärel esineb ajalõpp.
Authentication Method	Valige autentimismeetod. Valiku **Simple Authentication** korral soovitame määrata suvandi **Secure Connection** sätteks midagi muud kui **None**. Valiku **Kerberos Authentication** korral määrake eelnevalt Kerberose sätted. Funktsiooni Kerberos Authentication kasutamiseks on vajalik järgmine keskkond. ❏ Skanner ja DNS-server saavad omavahel suhelda. ❏ Skanneri, KDC-serveri ja autentimiseks vajaliku serveri (LDAP-server, SMTP-server, failiserver) ajad on sünkroonitud. ❏ Kui teenuse server on määratud IP-aadressiks, on teenuse serveri FQDN registreeritud DNS-serveri pöördotsingu tsooni.
Kerberos Realm to be Used	Kui **Kerberos Authentication** määratakse suvandi **Authentication Method** sätteks, 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 juhttärke, nagu 0x00–0x1F ja 0x7F. Seda sätet ei kasutata, kui **Anonymous Authentication** on valitud suvandi **Authentication Method** sätteks. Kui te ei taha seda täpsustada, jätke see tühjaks.
Password	Sisestage LDAP-serveris autentimiseks parool pikkusega kuni 128 tärki vormingus Unicode (UTF-8). Te ei saa kasutada juhttärke, nagu 0x00–0x1F ja 0x7F. Seda sätet ei kasutata, kui **Anonymous Authentication** on valitud suvandi **Authentication Method** sätteks. Kui te ei taha seda täpsustada, jätke see tühjaks.

Kerberose sätted

Kui **Kerberos Authentication** on valitud suvandi **Authentication Method** sätteks, peate seadistama Kerberose sätted. Saate registreerida kuni 10 Kerberose sätet.

Seadistamine rakenduses Web Config.

Valige vahekaart **Network** > **Kerberos Settings**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallis **Network** > **Security** > **Kerberos Settings**.

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

LDAP-serveri otsingusätete konfigureerimine

Määrab kasutajasätete otsinguatribuudid.

Seadistamine rakenduses Web Config.

Valige vahekaart **Network** > **LDAP Server** > **Search Settings (Authentication)**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallis **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)**.

Kirje	Sätted ja selgitused
Search Base (Distinguished Name)	Määrake algpunkt kasutajateabe otsimiseks LDAP-serverist. Sisestage 0 kuni 128 tärki koodis Unicode (UTF-8). Kui te ei otsi arbitraarset atribuuti, jätke see tühjaks. Näide kohaliku serveri kaustast: dc=server,dc=local
User ID Attribute	Määrake atribuudi nimi, mis kuvatakse ID-numbri otsimisel. Sisestage 1 kuni 255 tärki koodis ASCII. Esimene tärk peab olema „a–z“ või „A–Z“. Näide: cn, uid
User name Display Attribute	Täpsustage atribuudi nimi, mida kuvatakse kasutajanimena. Sisestage 0 kuni 255 tärki koodis ASCII. Esimene tärk peab olema „a–z“ või „A–Z“. Selle võite tühjaks jätta. Näide: cn, name
Authentication Card ID Attribute	Määrake atribuudi nimi, mis kuvatakse autentimiskaardi ID-na. Sisestage 0 kuni 255 tärki koodis ASCII. Esimene tärk peab olema „a–z“ või „A–Z“. Selle võite tühjaks jätta. Näide: cn, sn
ID Number Attribute	Määrake atribuudi nimi, mis kuvatakse ID-numbri otsimisel. Sisestage 1 kuni 255 tärki koodis ASCII. Esimene tärk peab olema „a–z“ või „A–Z“. Näide: cn, id
Department Attribute	Määrake atribuudi nimi, mis kuvatakse osakonna nimena. Sisestage 0 kuni 255 tärki koodis ASCII. Esimene tärk peab olema „a–z“ või „A–Z“. Selle võite tühjaks jätta. Näide: ou, ou-cl

Kirje	Sätted ja selgitused
Email Address Attribute	Täpsustage atribuudi nimi, mida kuvatakse meiliaadresside otsimise korral. Sisestage 1 kuni 255 tärki koodis ASCII. Esimene tärk peab olema „a–z“ või „A–Z“. Näide: mail
Save To Attribute	Määrake atribuudi nimi, mis osutab funktsiooni Scan To My Folder sihtkohale. Sisestage 0 kuni 255 tärki koodis ASCII. Näide: homeDirectory

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: ❏ LDAP-serveri aadress või pordinumber on vale. ❏ Esinenud on ajalõpp. ❏ **Do Not Use** on valitud suvandi **Use LDAP Server** sätteks. ❏ 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: ❏ **User Name** ja/või **Password** on vale. ❏ Kui **Kerberos Authentication** on valitud suvandi **Authentication Method** sätteks, ei saa kellaaega/kuupäeva konfigureerida.
Cannot access the product until processing is complete.	See teade kuvatakse, kui skanner on hõivatud.

Meiliserveri seadistamine

Kui kasutate funktsiooni **Scan to My Email**, seadistage meiliserver.

Märkus.
*Sätte **Scan to My Email** saab valida ainult siis, kui **Scan to Email** on lubatud.*

Seadistamine rakenduses Web Config.

Valige vahekaart **Network** > **Email Server** > **Basic**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallis **Common** > **Email Server** > **Mail Server Settings**.

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 valitud suvandi **Authentication Method** sätteks, sisestage autenditud konto nimi. Sisestage 0 kuni 255 tärki koodis ASCII (0x20 kuni 0x7E).	
Authenticated Password	Kui **SMTP AUTH** või **POP before SMTP** on valitud suvandi **Authentication Method** sätteks, sisestage autenditud parool. Sisestage 0 kuni 20 tärki koodis ASCII (0x20 kuni 0x7E).	
Sender's Email Address	Sisestage saatja meiliaadress. Sisestage 0 kuni 255 tärki koodis ASCII (0x20 kuni 0x7E), kuid ärge kasutage sümboleid : ( ) < > [ ] ; ¥. Punkt „." ei tohi olla esimene tärk.	
SMTP Server Address	Sisestage 0 kuni 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	Kui see on lubatud, siis sert autenditakse. Soovitame valida selleks sätteks **Enable**.	
POP3 Server Address	Kui **POP before SMTP** on valitud suvandi **Authentication Method** sätteks, sisestage POP3-serveri aadress. Võite sisestada 0 kuni 255 tärki, kasutades tärke A–Z, a–z, 0–9. Te võite kasutada vormingut IPv4 või FQDN.	
POP3 Server Port Number	Kui **POP before SMTP** on valitud suvandi **Authentication Method** sätteks, määrake pordinumber. Sisestage number vahemikus 1 kuni 65535.	

Funktsiooni Scan to My Folder seadistamine

Salvestab skannitud pildid igale kasutajale määratud kausta. Sihtkaustu saab määrata järgmiselt.

Märkus.
*Sätte **Scan To My Folder** saab valida ainult siis, kui **Scan to Network Folder/FTP** on lubatud.*

Salvestamise asukoha säte	Authentication Method	Kaustatee sätte asukoht
Määrake üks võrgukaust kogu funktsioonile Authentication Settings, et luua määratud kausta alla automaatselt isiklik, mille nimi on kasutaja ID.	❏ Local DB ❏ LDAP ❏ Local DB and LDAP	Skanner (suvandi Scan to My Folder säte)
Määrake igale kasutajale eraldi võrgukaust.	Local DB	Skanner (User Settings)
	LDAP	LDAP atribuudid
	Local DB and LDAP	Skanner (User Settings) või LDAP atribuudid

Seadistamine rakenduses Web Config.

Valige vahekaart **Product Security** > **Scan to Network Folder/FTP**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallis **Administrator Settings** > **Authentication Settings** > **Scan to Network Folder/FTP** > **Scan to My Folder**.

Kirje		Selgitus
Save To Setting	Setting Type	❏ **Shared**: Loob automaatselt kasutaja ID nimega kausta suvandis **Save to** määratud kaustatee või URL-i alla ning salvestab skannitud pildid sellesse kausta. ❏ **Individual**: Määrake skannitud piltide salvestamise sihtkoht igale kasutajale eraldi. Local DB kasutajad saab seadistada kasutajasätetes. LDAP kasutajad kasutavad LDAP-serveri otsinguatribuutidest saadud salvestuskohta.
	Type	Valige sideprotokoll lähtuvalt skannimise sihtkohast. Võrgukaust: **Network Folder (SMB)** FTP-server: **FTP**
	Save to	Määrake sihtkoha tee või URL. Sisestage kuni 160 tärki koodis Unicode (UTF-16).
	Connection Mode	Seadistage, kui **FTP** on suvandi **Type** säte. Valige ühendusrežiim FTP-serveri jaoks.
	Port Number	Seadistage, kui **FTP** on suvandi **Type** säte. Sisestage pordinumber vahemikus 0 kuni 65535 skannitud andmete FTP-serverisse saatmiseks.

Kirje		Selgitus
Authentication Settings	Setting Type	Seadistage, kui **Individual** on suvandi **Setting Type** säte suvandis **Save To Setting**. Määrake kaustale juurdepääsuks User Name ja Password. ❏ **Shared**: Kasutage kõigi kasutajate jaoks samu suvandite **User Name** ja **Password** sätteid. ❏ **Individual**: Local DB kasutajate jaoks määrake **User Name** ja **Password** individuaalselt menüüs **Kasutaja sätted**. LDAP kasutajaid ei saa individuaalselt konfigureerida. Selles üksusega määratud **User Name** ja **Password** on kasutusel ühiselt.
	User Name	Sisestage kasutajanimi juurdepääsuks skannitud andmete sihtkaustale. Sisestage kuni 30 tärki koodis Unicode (UTF-16). Seadistage see, kui kasutate **Shared**- või LDAP-serverit.
	Password	Sisestage parool, mis vastab sättele **User Name**. Sisestage kuni 20 tärki koodis Unicode (UTF-16). Seadistage see, kui kasutate **Shared**- või LDAP-serverit.

Funktsiooni Scan to Network Folder/FTP sihtkoha muutmise keelamine

Kirje	Selgitus
Prohibit manual entry of destination	Kui see on lubatud, ei saa kasutaja vaikimisi sihtkohta muuta.

Customize One-touch Functions

Saate kuvada vaid vajalikud ikoonid, redigeerides juhtpaneeli avakuva ikoonipaigutust.

Seadistamine rakenduses Web Config.

Valige vahekaart **Product Security** > **Customize One-touch Functions**.

Seadistamine rakenduses Epson Device Admin.

Valige konfiguratsioonimallis **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions**.

Märkus.
Järgmistel juhtudel ei kuvata määratud funktsioonide ikoone avakuval.

❏ *Kui valite funktsioonid, mis pole lubatud suvandi **Restrictions** tõttu.*

❏ *Kui sisselogitud kasutaja meiliaadress on registreerimata. (Scan to My Email)*

❏ *Kui sihtkaust on määramata. (Scan to My Folder)*

Kirje	Selgitus
Maximum functions per screen	Valige juhtpaneelil kuvatud ikoonide paigutus. Pilt muutub olenevalt valitud paigutusest.

Kirje	Selgitus
Screen(s)	Valige lehekülgede arv.
Number	Valige iga nummerdatud asukoha jaoks funktsioonid, mida soovite kuvada.

Aruanded Job History rakenduses Epson Device Admin

Te saate luua aruande Job History iga rühma ja iga kasutaja jaoks, kasutades rakendust Epson Device Admin. Saate skannerisse salvestada kuni 3000 kasutusajaloo eksemplari. Saate aruande luua, määrates perioodi või seadistades regulaarse graafiku.

Job History väljastamiseks aruandena valige seadmeloendi kuval ribamenüüst **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices**.

Lisateavet kasutaja aruande loomise kohta lugege rakenduse Epson Device Admin dokumentatsioonist.

Üksused, mille saab aruandesse lisada

Kasutaja aruandesse saab lisada järgmised üksused.

Date / Job ID / Operation / User ID / Department / Result / Result details / Scan: Destination type / Scan: Destination / Scan: Paper Size / Scan: 2-Sided / Scan: Color / Scan: Pages / Devices: Model / Devices: IP Address / Devices: Serial Number / Devices: Department / Devices: Location / Devices: Remark / Devices: Note

Juhtpaneelilt administraatorina sisselogimine

Skanneri juhtpaneelilt administraatorina sisselogimiseks saate kasutada ükskõik millist järgmistest meetoditest.

1. Puudutage ekraanil üleval paremas nurgas ikooni .
   - ❏ Kui Authentication Settings on lubatud, on ikoon kuval **Tere tulemast!** (autentimise ootekuva).
   - ❏ Kui Authentication Settings on keelatud, on ikoon avakuval.
2. Kui kuvatakse kinnituskuva, puudutage nuppu **Jah**.
3. Sisestage administraatori parool.

   Kuvatakse sisselogimise teade ja seejärel kuvatakse juhtpaneelil avakuva.

Väljalogimiseks puudutage avakuval üleval paremas nurgas ikooni .

Funktsiooni Authentication Settings keelamine

Authentication Settings on võimalik välja lülitada rakenduses Web Config.

Märkus.
Skanneris registreeritud üksused User Settings jäävad salvestatuks ka siis, kui Authentication Settings keelatakse. Te saate need eemaldada, taastades skanneri vaikesätted.

1. Avage Web Config.
2. Valige vahekaart **Product Security** > **Basic** > **Authentication**.
3. Valige **OFF**.
4. Klõpsake nuppu **Next**.
5. Klõpsake nuppu **OK**.

Märkus.
Isegi kui te funktsiooni Authentication Settings keelate, jääb Lukustamise sätted lubatuks. Kui soovite selle keelata, saate asjakohased sätted teha juhtpaneelil või rakenduses Web Config.

Seotud teave

➡ „Funktsiooni Lukustamise sätted seadistamine juhtpaneelil” lk 89
➡ „Funktsiooni Lukustamise sätted seadistamine rakenduses Web Config” lk 89

Funktsiooni Authentication Settings teabe kustutamine (Taasta vaikesätted)

Funktsiooni Authentication Settings kogu teabe kustutamiseks (Card Reader, Authentication Method, User Settings jne) lähtestage kõik skanneri sätted tehasesätetele.

Valige juhtpaneelil **Sätted** > **Süsteemi administreerimine** > **Taasta vaikesätted** > **Kõik sätted**.

> ***Oluline teave:***
> *Kustutatakse ka kõik kontaktid ja muud võrgusätted. Kustutatud sätteid ei saa taastada.*

Probleemide lahendamine

Autentimiskaardi lugemine ei õnnestu

Kontrollige järgmist.

❏ Kontrollige, kas autentimisseade on skanneriga õigesti ühendatud.
Ühendage autentimisseade skanneri tagaküljel olevasse välisliidese USB-porti.

❏ Kontrollige, kas autentimisseade ja autentimiskaart on toetatud.

Hooldamine

Skanneri korpuse puhastamine. 155

Skanneri sisemuse puhastamine. 155

Rulli montaažikomplekti vahetamine. 160

Skannide arvu lähtestamine. 165

Energia säästmine. 165

Skanneri transportimine. 166

Sätete varundamine. 167

Taasta vaikesätted. 168

Rakenduste ja püsivara värskendamine. 168

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 puuteekraani 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.

Värskeimat skannide arvu saate vaadata juhtpaneelilt või rakendusest Epson Scan 2 Utility.

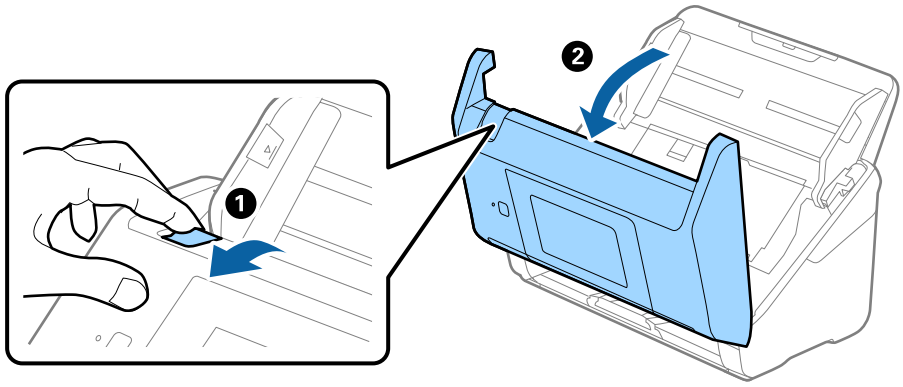
Kui pind on määrdunud ja plekk on raskesti eemaldatav, kasutage puhastamiseks Epsoni originaalset puhastuskomplekti. Plekkide eemaldamiseks kandke puhastuslapile väike kogus puhastusvahendit.

Oluline teave:

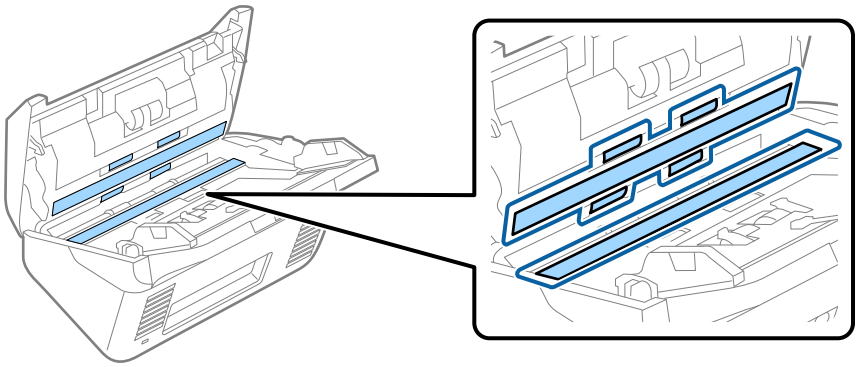
- ❏ *Ärge kasutage skanneri puhastamiseks kunagi alkoholi, lahustit ega söövitavat lahust. Selle tagajärjeks võib olla deformeerumine või värvimuutus.*
- ❏ *Ärge pihustage skannerile vedelikku ega õlitusainet. Seadmete või elektriskeemide kahjustused võivad põhjustada tööhäireid.*
- ❏ *Ärge kunagi avage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

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

3. Tõmmake hooba ja avage skanneri kaas.



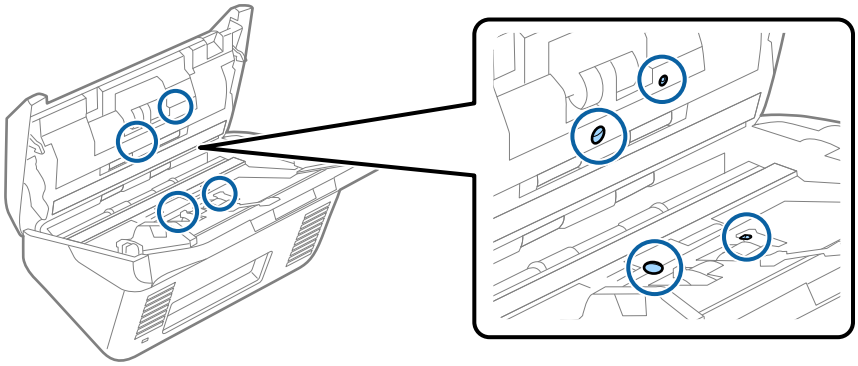
4. Pühkige skanneri sees plastikust rullil ja põhjas asuval klaaspinnal olevad plekid, kasutades pehmet lappi või Epsoni originaalset puhastuskomplekti.



Oluline teave:

- ❏ *Ärge suruge liiga tugevasti klaaspinnale.*
- ❏ *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.

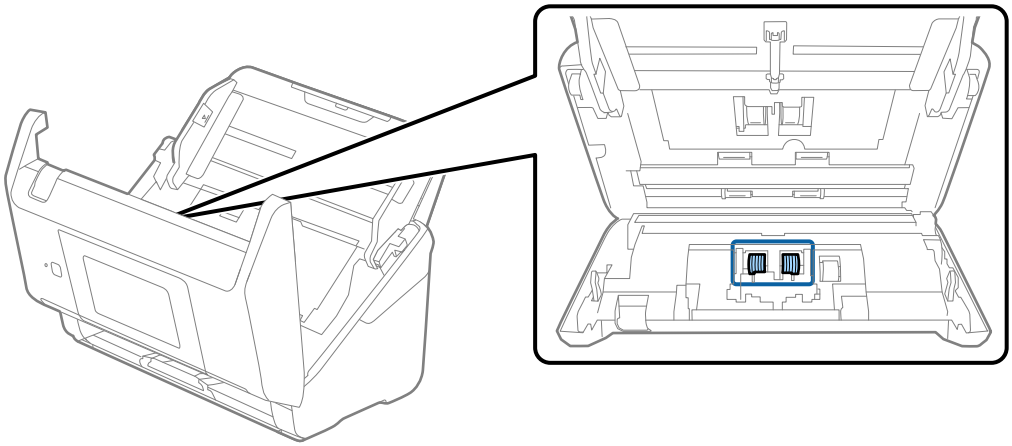


Oluline teave:

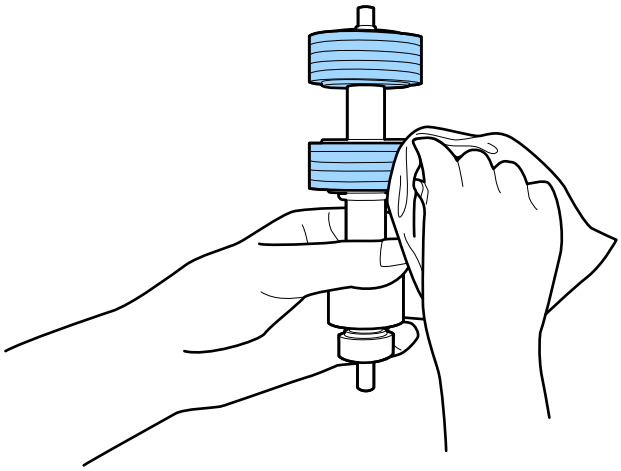
Ärge kandke vatitupsule vedelikku, näiteks puhastusainet.

6. Avage kaas ja eemaldage eraldusrull.

   Vt lisateavet jaotisest „Rulli montaažikomplekti vahetamine“.



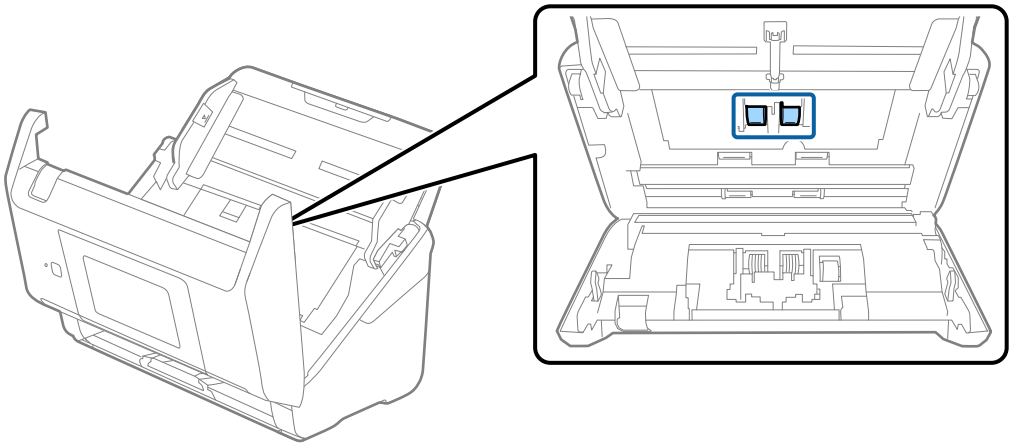
7. Pühkige Epsoni originaalse puhastuskomplekti või pehme niiske lapiga eraldusrullilt tolm ja mustus.



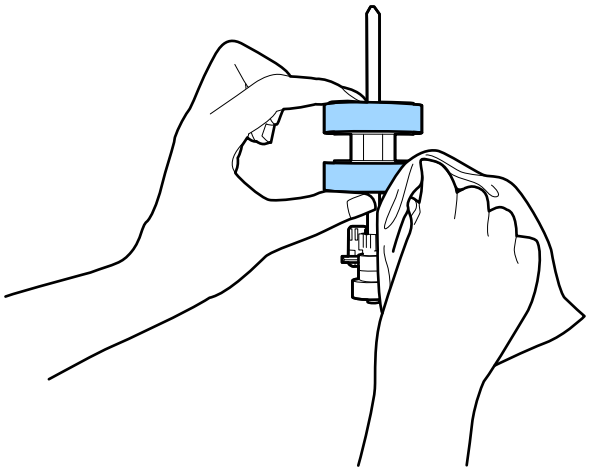
> ***Oluline teave:***
>
> *Kasutage rulli puhastamiseks ainult Epsoni originaalset puhastuskomplekti või pehmet niisket lappi. Kuiva lapi kasutamine võib rulli pealispinda kahjustada.*

8. Avage kaas ja eemaldage korjerull.

   Vt lisateavet jaotisest „Rulli montaažikomplekti vahetamine“.



9. Pühkige Epsoni originaalse puhastuskomplekti või pehme niiske lapiga korjerullilt tolm ja mustus.

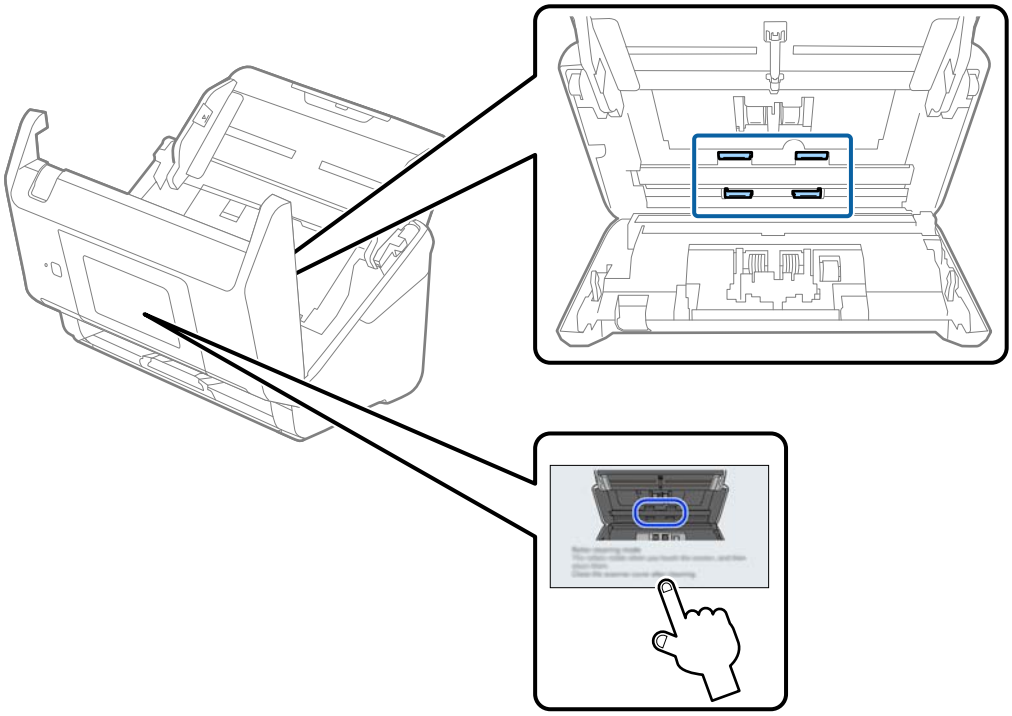


> ***Oluline teave:***
>
> *Kasutage rulli puhastamiseks ainult Epsoni originaalset puhastuskomplekti või pehmet niisket lappi. Kuiva lapi kasutamine võib rulli pealispinda kahjustada.*

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.

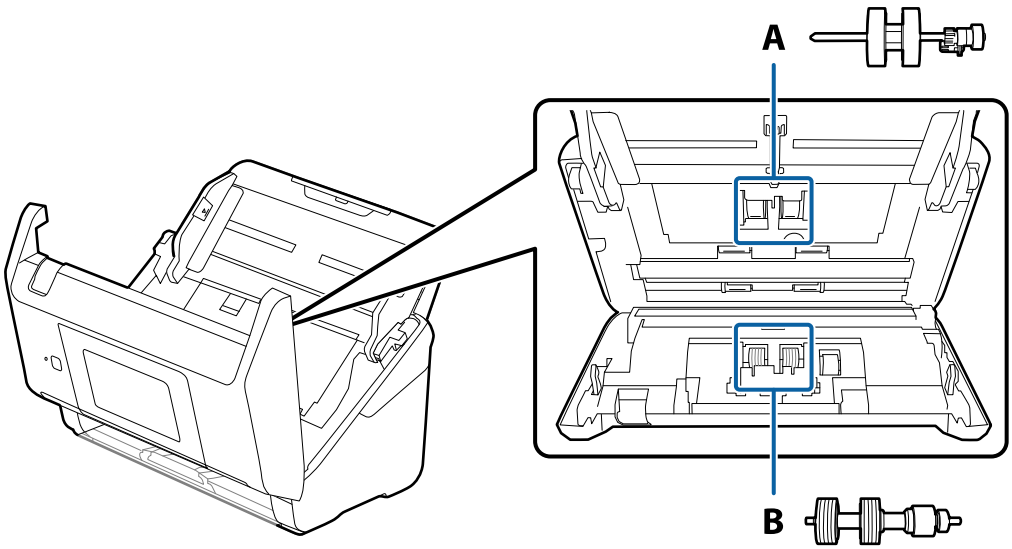
    Skanner läheb rullide puhastusrežiimist välja.

Seotud teave

➡ „Rulli montaažikomplekti vahetamine” lk 160

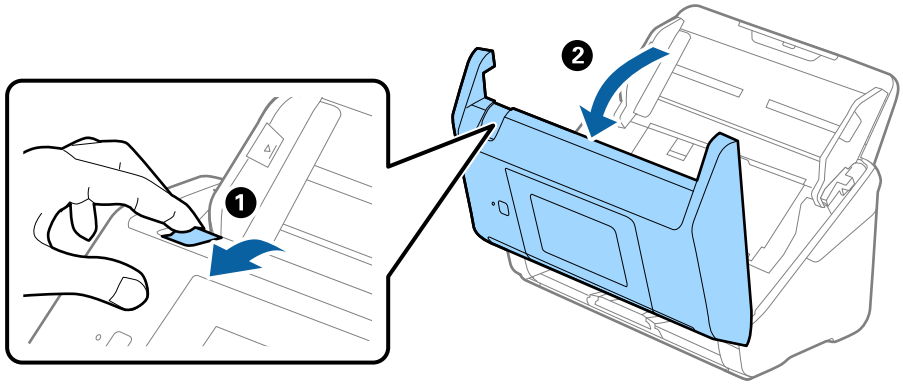
Rulli montaažikomplekti vahetamine

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

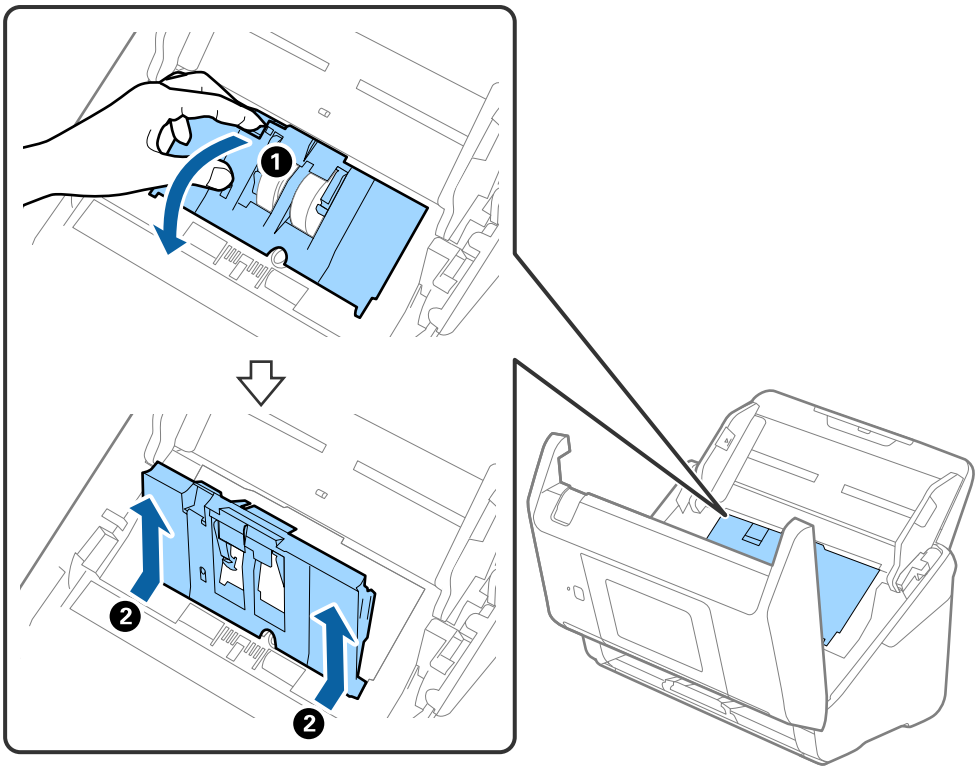


A: vastuvõturull, B: eraldusrull

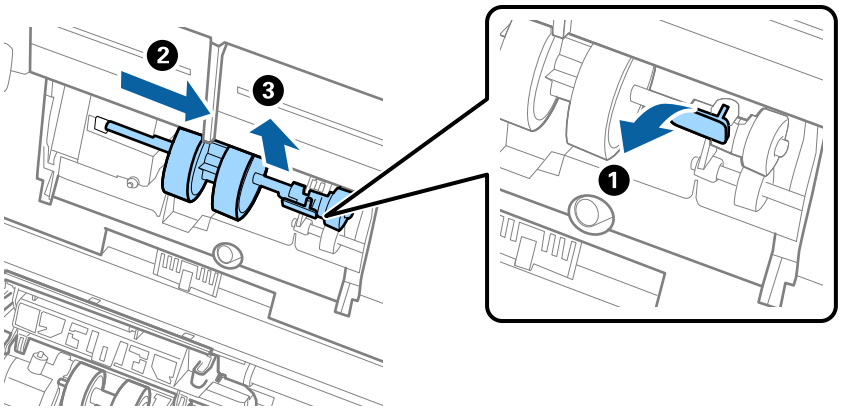
1. Skanneri väljalülitamiseks vajutage nuppu ⏻.
2. Võtke vahelduvvooluadapter skanneri küljest lahti.
3. Tõmmake hooba ja avage skanneri kaas.



4. Avage vastuvõturulli kaas, seejärel lükake see välja.

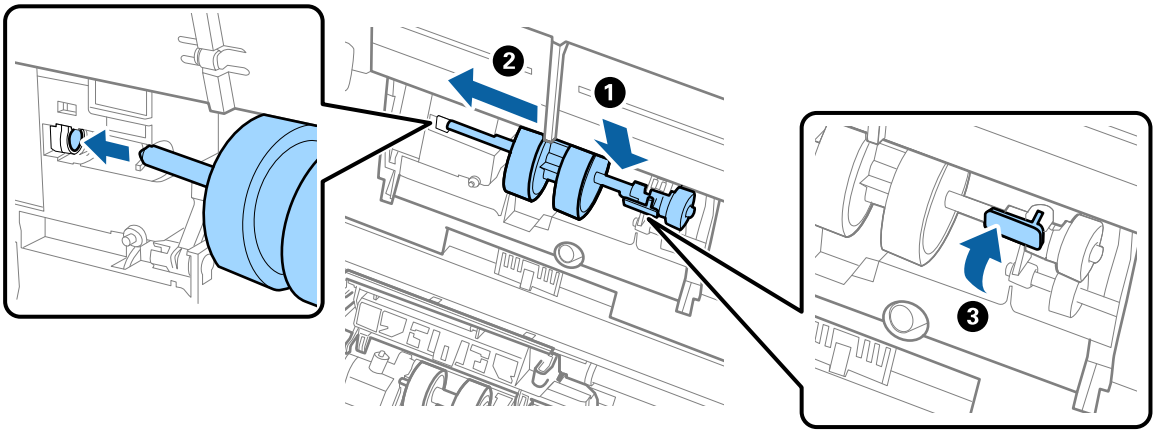


5. Tõmmake rulli telje kinnitusrakis alla, seejärel lükake paigaldatud vastuvõturullid välja.

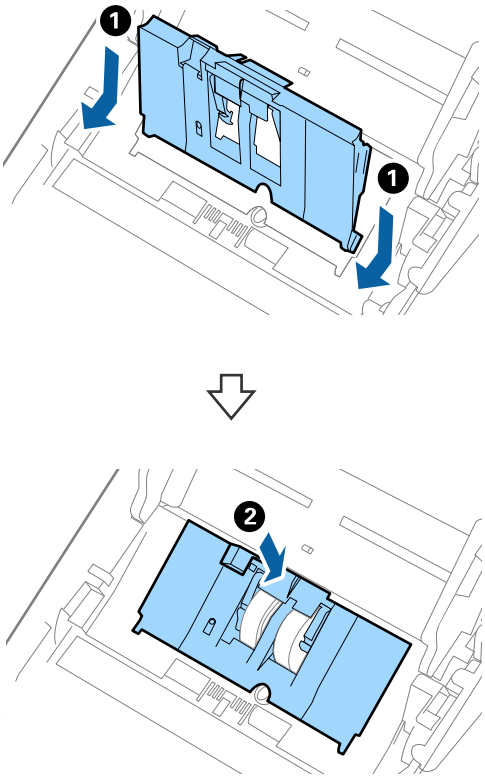


> ***Oluline teave:***
>
> *Ärge tõmmake vastuvõturulli jõuga välja. See võib skanneri sisemust vigastada.*

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

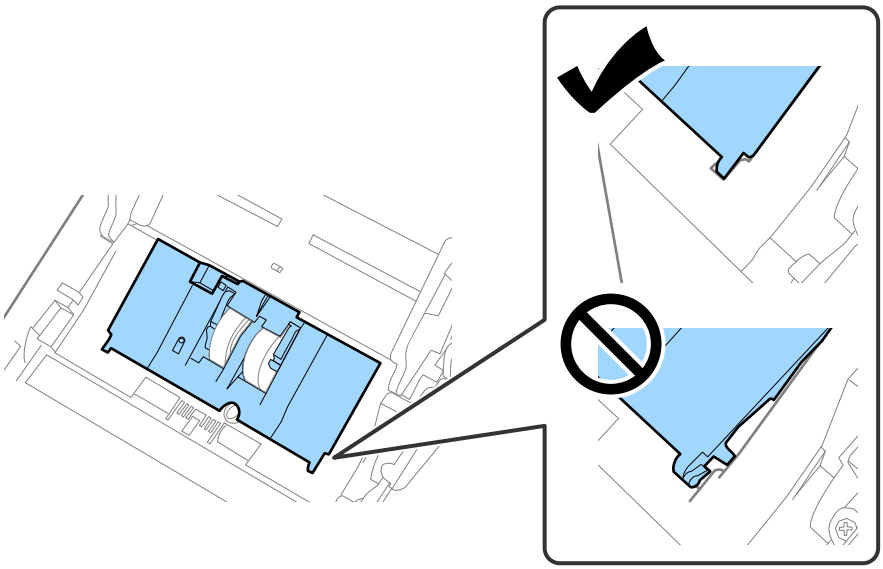


7. Pange vastuvõturulli kaane serv soone sisse ja lükake seda. Sulgege kaas kindlalt.

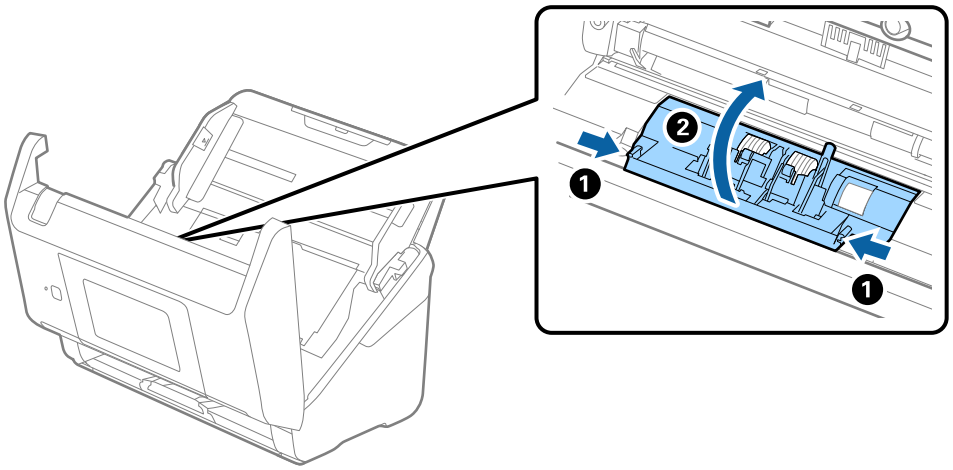


Oluline teave:

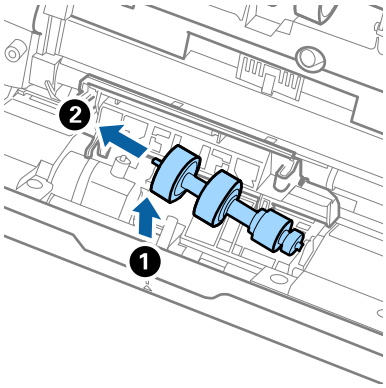
- ❏ *Veenduge, et vastuvõturulli kaas on õigesti suletud.*
- ❏ *Kui kaant on raske sulgeda, kontrollige, kas kogumisrullikud on õigesti paigaldatud.*
- ❏ *Ärge paigaldage kaant, kui see on üles tõstetud.*



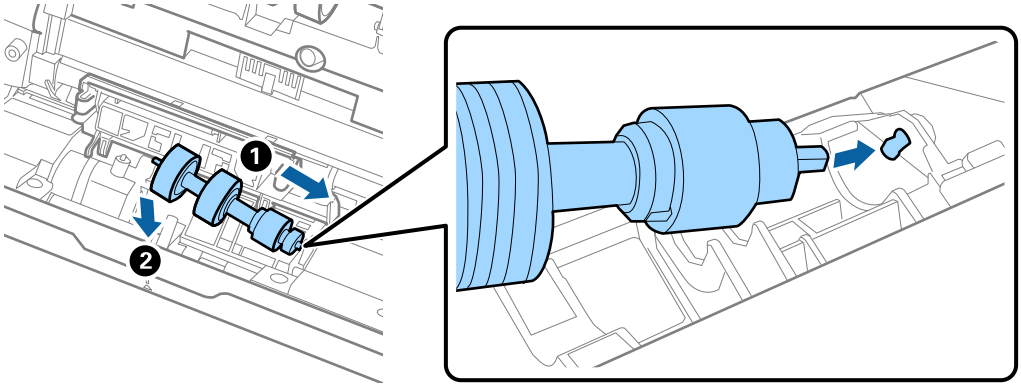
8. Kaane avamiseks suruge eraldusrulli mõlemal otsal olevaid konkse.



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.

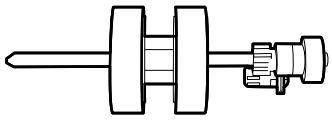
14. Lähtestage skannide arv juhtpaneelilt.

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

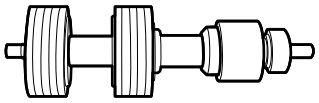
Rulli montaažikomplekti koodid

Osad (vastuvõturull ja eraldusrull) tuleb vahetada, kui skannide arv ületab teenindusarvu. Värskeimat skannide arvu saate vaadata juhtpaneelilt või rakendusest Epson Scan 2 Utility.

A



B



A: vastuvõturull, B: eraldusrull

Osa nimi	Koodid	Kasutustsükkel
Rulli montaažikomplekt	B12B819671 B12B819681 (ainult India)	200,000*

* See arv saadi järjestikusel skannimisel Epsoni originaal-testpaberitega ja see on vahetustsükli suuniseks. Vahetustsükkel võib olenevalt paberi tüübist erineda. Näiteks rohkelt paberitolmu tekitav paber või karedapinnaline paber võib kasutustsüklit lühendada.

Skannide arvu lähtestamine

Skannide arv pärast rullikute montaažikomplekti vahetamist.

1. Valige avakuval **Sätted** > **Seadme info** > **Lähtesta skannimiste arv** > **Skannitud eksemplaride arv pärast rulliku vahetamist**.
2. Puudutage nuppu **Jah**.

Seotud teave

➡ „Rulli montaažikomplekti vahetamine” lk 160

Energia säästmine

Saate energiat säästa, kasutades puhkerežiimi või automaatset välja lülitamist, kui skanner ei tee ühtegi toimingut. Saate määrata aja, mille järel skanner läheb puhkerežiimi ja lülitub automaatselt välja. Tõstmine mõjutab toote energiatõhusust. Püüdke enne muudatuste tegemist arvestada keskkonnaga.

1. Valige avakuval **Sätted**.
2. Valige **Põhisätted**.

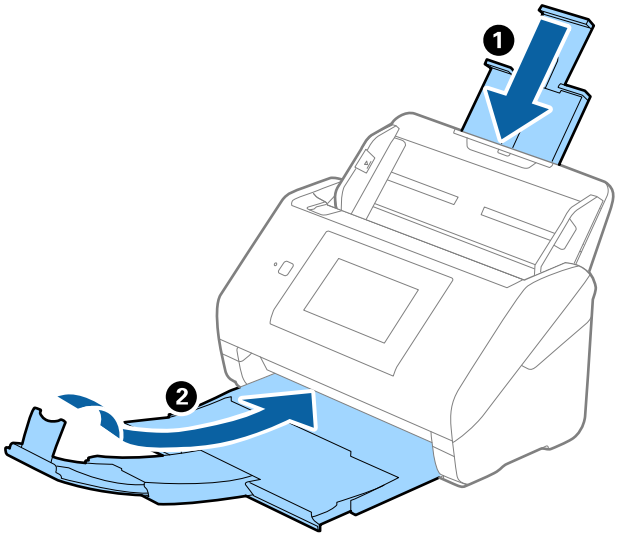
3. Valige suvand **Välja lülit. säte** ja määrake seejärel sätted.

   Märkus.
   Saadaval funktsioonid võivad olenevalt ostukohast erineda.

Skanneri transportimine

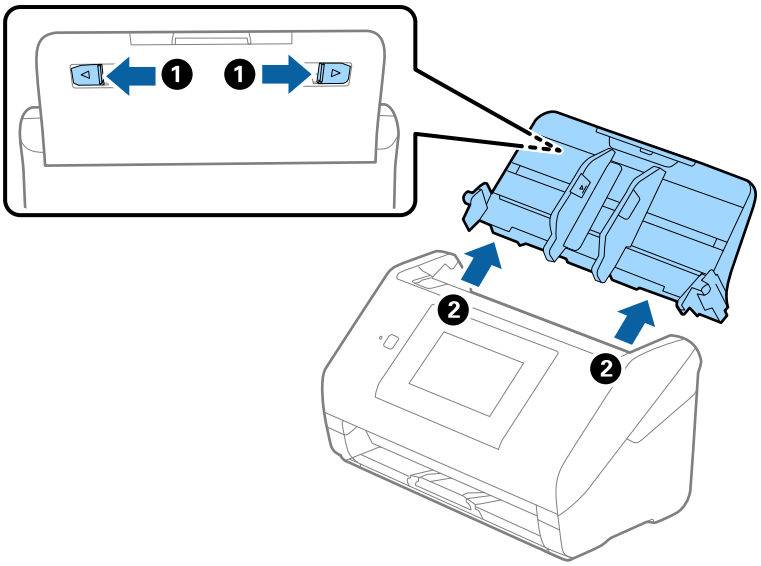
Kui te peate skanneri teise kohta transportima või remonti viima, siis järgige skanneri pakkimiseks alltoodud samme.

1. Skanneri väljalülitamiseks vajutage nuppu ⏻.
2. Ühendage vahelduvvooluadapter elektrivõrgust välja.
3. Eemaldage kaablid ja seadmed.
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.

Eksporditud faili ei ole võimalik redigeerida, sest seda eksporditakse kahendfailina.

Sätete eksportimine

Eksportige skanneri jaoks sätted.

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

2. Valige sätted, mida te soovite eksportida.

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

3. Eksporditud 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

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 tehasesätted.

> ***Oluline teave:***
>
> *Kui teete valiku **Kõik sätted** ja käivitate selle, kustutatakse kõik skanneris registreeritud sätteandmed, kaasa arvatud kontaktid ja kasutaja autentimissätted. Kustutatud sätteid ei saa taastada.*

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 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** > **Mine** > **Rakendused** > **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 internetti 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 värskendama. 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

➡ „Utiliidi Web Config kasutamine veebibrauseris” lk 36

Püsivara värskendamine ilma internetiühenduseta

Seadme püsivara saate arvutisse alla laadida Epsoni veebisaidilt, seejärel ühendage püsivara värskendamiseks USB-kaabli abil seade arvutiga. Kui te ei saa värskendada võrgu kaudu, proovige seda meetodit.

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

1. Kontrollige Epsoni veebisaidilt, kas teie püsivaraversioon on värske.

   http://www.epson.com

   ❏ Kui teie skanneri jaoks on saadaval püsivaravärskendus, laadige see alla ja minge järgmise sammu juurde.

   ❏ Kui veebisaidil ei ole püsivara kohta teavet, siis kasutate juba kõige uuemat 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.