EPSON
EXCEED YOUR VISION

Administraatori juhend

NPD5668-00 ET

Sisukord

Sisukord

Lisa

Täpsemad turvasätted ettevõttele

Autoriõigus

Kaubamärgid

- ❏ EPSON® on registreeritud kaubamärk ja EPSON EXCEED YOUR VISION või EXCEED YOUR VISION on ettevõtte Seiko Epson Corporation kaubamärk.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Üldteatis: muid tootenimesid on selles trükises kasutatud ainult tuvastamise eesmärgil ja need võivad olla vastavate omanike kaubamärgid. Epson ütleb lahti kõigist õigustest neilekaubamärkidele.

Teave juhendi kohta

Tähised ja sümbolid

> ***Ettevaatust!***
> *Juhised, mida tuleb kehavigastuste vältimiseks hoolikalt järgida.*

> ***Oluline teave:***
> *Juhised, mida tuleb järgida seadmestiku kahjustuste vältimiseks.*

Märkus.
Juhised, mis sisaldavad kasulikke nõuandeid ning kirjeldavad skanneri kasutamisega seotud piiranguid.

Seotud teave

➡ Selle ikooni klõpsamine viib teid seotud teabe juurde.

Selles juhendis kasutatavad kirjeldused

❏ Skanneridraiveri ja skanneridraiveri Epson Scan 2 ekraanipildid on tehtud opsüsteemis Windows 10 või OS X El Capitan. Ekraanipiltide sisu on mudelist ja olukorrast olenevalt erinev.

❏ Joonised selles juhendis on toodud vaid näiteks. Ehkki sõltuvalt mudelist võivad need olla pisut erinevad, on nende töömeetod sama.

❏ Mõned LCD-ekraani menüükirjed erinevad olenevalt mudelist ja sätetest.

Opsüsteemide viited

Windows

Selles juhendis olevad terminid „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Vista“, „Windows XP“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“, „Windows Server 2008 R2“, „Windows Server 2008“, „Windows Server 2003 R2“, ja „Windows Server 2003“ viitavad järgmistele opsüsteemidele. Terminit „Windows“ kasutatakse kõikide versioonide puhul.

❏ Microsoft® Windows® 10 opsüsteem

❏ Microsoft® Windows® 8.1 opsüsteem

❏ Microsoft® Windows® 8 opsüsteem

❏ Microsoft® Windows® 7 opsüsteem

❏ Microsoft® Windows Vista® opsüsteem

❏ Microsoft® Windows® XP opsüsteem

❏ Microsoft® Windows® XP Professional x64 Edition opsüsteem

Teave juhendi kohta

- ❏ Microsoft® Windows Server® 2016 opsüsteem
- ❏ Microsoft® Windows Server® 2012 R2 opsüsteem
- ❏ Microsoft® Windows Server® 2012 opsüsteem
- ❏ Microsoft® Windows Server® 2008 R2 opsüsteem
- ❏ Microsoft® Windows Server® 2008 opsüsteem
- ❏ Microsoft® Windows Server® 2003 R2 opsüsteem
- ❏ Microsoft® Windows Server® 2003 opsüsteem

Mac OS

Terminit „Mac OS“ kasutatakse versioonide „macOS Sierra“, „OS X El Capitan“, „OS X Yosemite“, „OS X Mavericks“, „OS X Mountain Lion“, „Mac OS X v10.7.x“ ja „Mac OS X v10.6.8“ puhul.

Sissejuhatus

Juhendi osad

See juhend on mõeldud seadme administraatorile, kes vastutab printeri või skanneri võrku ühendamise eest, ja see sisaldab teavet funktsioonide häälestamise kohta.

Funktsioonide kasutamise kohta lugege teavet juhendist *Kasutusjuhend*.

Ettevalmistus

Kirjeldab administraatori ülesandeid, seadmete paigaldamist ja haldustarkvara.

Ühendamine

Kirjeldab, kuidas ühendada seade võrku või telefoniliiniga. Lisaks kirjeldab see võrgukeskkonda, nagu seadme jaoks pordi kasutamist ning teavet DNS- ja puhverserveri kohta.

Funktsioonide sätted

Kirjeldab seadme iga funktsiooni sätteid.

Põhilised turvasätted

Kirjeldab iga funktsiooni sätteid, näiteks printimiseks, skannimiseks ja faksimiseks.

Kasutamise ja haldamise sätted

Kirjeldab toiminguid pärast seadme kasutuselevõttu, nagu teabe kontrollimine ja hooldus.

Probleemide lahendamine

Kirjeldab sätete lähtestamist ja võrgu tõrkeotsingut.

Täpsemad turvasätted ettevõttele

Kirjeldab sätteid seadme turvalisuse tõstmiseks, nagu sertimiskeskuse sertifikaadi kasutamine, SSL/TLS-side ja IPsec/IP-filtreerimine.

Olenevalt mudelist ei ole mõned selle peatüki funktsioonidest toetatud.

Käesolevas juhendis kasutatud mõistete selgitused

Käesolevas juhendis on kasutatud alljärgnevaid mõisteid.

Administraator

Isik, kes vastutab organisatsioonis seadme või võrgu paigaldamise ja häälestamise eest. Väikestes organisatsioonides võib see isik olla vastutav nii seadme kui võrgu haldamise eest. Suurtes organisatsioonides vastutavad administraatorid osakonnas või allüksuses kasutatava võrgu ja seadmete eest ning võrguadministraatorid vastutavad organisatsioonist väljapoole ulatuvate sidesätete eest (näiteks Internett).

Sissejuhatus

Võrguadministraator

Isik, kes vastutab võrguside juhtimise eest. Isik, kes häälestab marsruuteri, puhverserveri, DNS-serveri ja meiliserveri side juhtimiseks läbi Interneti või võrgu.

Kasutaja

Isik, kes kasutab seadmeid, nagu printerid või skannerid.

Web Config (seadme veebileht)

Seadme sisse ehitatud veebiserver. Selle nimi on Web Config. Selles saate brauseriga kontrollida ja muuta seadme olekut.

Tööriist

Üldmõiste tarkvara kohta, millega seadet häälestatakse või hallatakse, näiteks Epson Device Admin, EpsonNet Config, EpsonNet SetupManager jne.

Tõukeskannimine

Üldmõiste seadme juhtpaneelilt skannimise kohta.

ASCII (Ameerika Informatsioonivahetuse Standardkood)

Üks standardsetest tärgikoodidest. Määratletud on 128 tärki, mille hulgas on tähemärgid (a–z, A–Z), araabia numbrid (0–9), sümbolid, tühimärgid ja juhtmärgid. Selles juhendis tähistab „ASCII“ allpool toodud tärke 0x20–0x7E (kuueteistkümnendnumber) ning ei hõlma juhtmärke.

SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* Tühik.

Unicode (UTF-8)

Rahvusvaheline standardkood, mis hõlmad suuremaid keeli üle maailma. Selles juhendis tähistab „UTF-8“ tärkide kodeerimist UTF-8-vormingus.

Ettevalmistus

Selles peatükis on kirjeldatud administraatori rolli ja ettevalmistusi enne sätete määramist.

Skanneri sätete ja haldamise töövoog

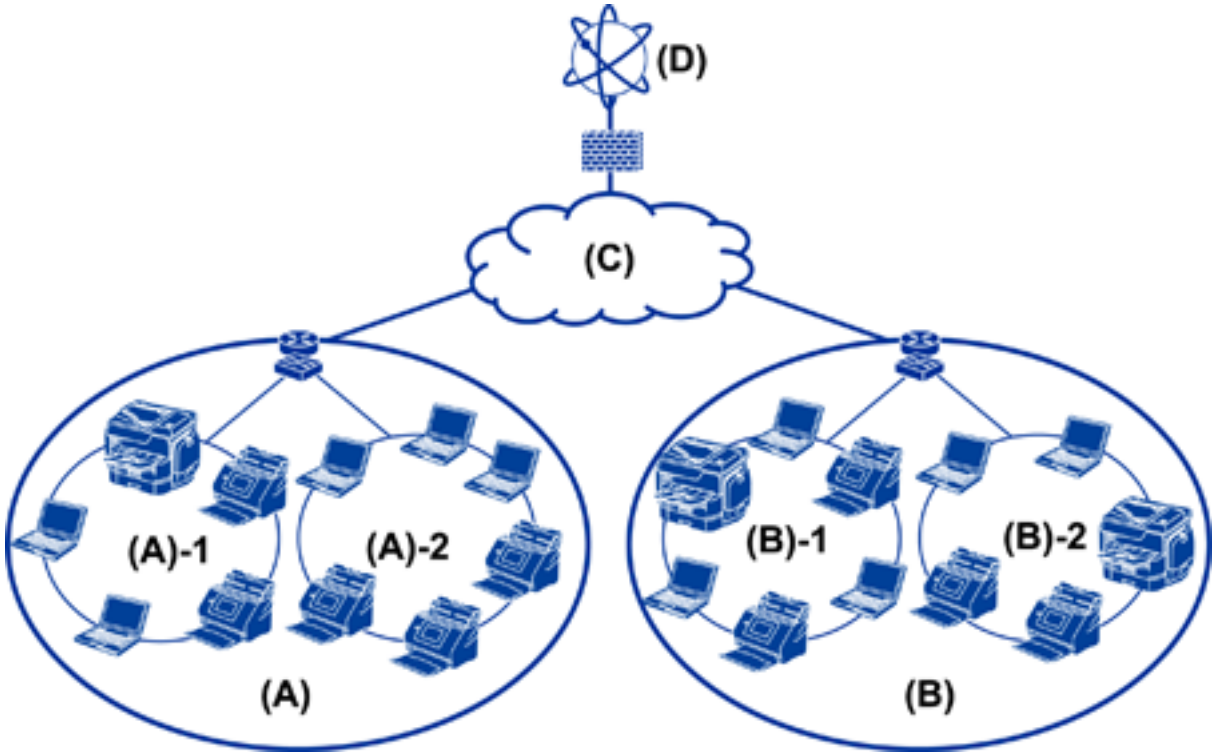
Skanneri võrguühenduse sätted, alghäälestuse ja hoolduse teeb administraator, et need oleksid kasutajatele saadaval.

1. Ettevalmistus
   - ❏ Teabe kogumine ühenduse sätete kohta
   - ❏ Ühendusmeetodi valimine
2. Ühendamine
   - ❏ Võrguühenduse loomine skanneri juhtpaneelilt
3. Funktsioonide häälestamine
   - ❏ Skanneridraiveri sätted
   - ❏ Muud täpsemad sätted
4. Turvasätted
   - ❏ Administraatori sätted
   - ❏ SSL/TLS
   - ❏ Protokolli juhtimine
   - ❏ Täpsemad turvasätted (valikuline)
5. Kasutamine ja haldamine
   - ❏ Seadme oleku kontrollimine
   - ❏ Tegevus sündmuste esinemise korral
   - ❏ Seadme sätete varundamine

Seotud teave

➡ „Ettevalmistus” lk 10
➡ „Ühendamine” lk 15
➡ „Funktsioonide sätted” lk 22
➡ „Põhilised turvasätted” lk 32
➡ „Kasutamise ja haldamise sätted” lk 40

Võrgukeskkonna näidis



(A): kontor 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): kontor 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internett

Skanneri ühendussätte näite tutvustus

Olenevalt skanneri kasutamise meetodist on peamiselt kasutusel kaks ühendustüüpi. Mõlema puhul ühendatakse skanner arvutiga võrku jaoturi vahendusel.

❏ Serveri/kliendi ühendus (skanner kasutab Windowsi serverit, töö haldust)

❏ Võrdõigusühendus (otseühendus klientarvutiga)

Seotud teave

➡ „Serveri/kliendi ühendus” lk 12

➡ „Võrdõigusühendus” lk 12

Serveri/kliendi ühendus

Tsentraliseerige skanneri ja tööde haldus serverisse installitud rakendusega Document Capture Pro Server. See sobib kõige paremini tööks, mille jaoks kasutatakse mitut skannerit ja suurt arvu dokumente kindlas vormingus.

Seotud teave

➡ „Käesolevas juhendis kasutatud mõistete selgitused” lk 8

Võrdõigusühendus

Kasutage eraldiseisvat skannerit klientarvutisse installitud skanneridraiveriga, nagu Epson Scan 2. Document Capture Pro (Document Capture) installimine klientarvutisse võimaldab teil teha töid skanneri eraldiseisvates klientarvutites.

Seotud teave

➡ „Käesolevas juhendis kasutatud mõistete selgitused” lk 8

Võrguühenduse ettevalmistamine

Teabe kogumine ühenduse sätete kohta

Teil peab olema võrguühenduse IP-aadress, lüüsi aadress jne. Kontrollige eelnevalt alljärgnevat.

Jaotus	Üksused	Märkus
Seadme ühendusmeetod	❏ Ethernet	Kasutage Etherneti-ühenduseks 5e või kõrgema kategooria STP-kaablit (varjestatud keerdpaar).
LAN-ühenduse teave	❏ IP-aadress ❏ Alamvõrgumask ❏ Vaikelüüs	Kui määrate IP-aadressi automaatselt marsruuteri DHCP-funktsiooniga, ei ole seda vaja.
DNS-serveri teave	❏ Esmase DNS-i IP-aadress ❏ Sekundaarse DNS-i IP-aadress	Kui kasutate IP-aadressina staatilist IP-aadressi, konfigureerige DNS-server. Konfigureerige, kui määratakse automaatselt DHCP-funktsiooniga ja kui DNS-serverit ei saa automaatselt määrata.
Puhverserveri teave	❏ Puhverserveri nimi ❏ Pordinumber	Konfigureerige, kui Interneti-ühenduseks kasutatakse puhverserverit ja kui kasutatakse teenust Epson Connect või püsivara automaatse värskendamise funktsiooni.

Skanneri spetsifikatsioonid

Skanneri toetatud standardite ja ühendusrežiimide spetsifikatsioone vaadake juhendist *Kasutusjuhend*.

Pordinumbri kasutamine

Skanneri kasutatavat pordinumbrit vaadake jaotisest „Lisa“.

Seotud teave

➡ „Skanneri jaoks pordi kasutamine” lk 60

IP-aadressi määramise meetod

Skannerile IP-aadressi määramiseks on kaks meetodit.

Staatiline IP-aadress:

Skannerile määratakse etteantud unikaalne IP-aadress.

IP-aadressi ei muudeta isegi siis, kui skanner või marsruuter välja lülitatakse, seega saate seadet hallata IP-aadressi järgi.

See meetod sobib võrku, kus hallatakse paljusid skannereid, nagu suure kontori või kooli võrk.

Automaatne määramine DHCP-funktsiooniga:

Õige IP-aadress määratakse automaatselt, kui luuakse ühendus skanneri ja DHCP-funktsiooni toetava marsruuteri vahel.

Kui mingi seadme IP-aadressi vahetamine on ebamugavust tekitav, reserveerige IP-aadress eelnevalt ja seejärel määrake see.

DNS-server ja puhverserver

Kui kasutate Interneti-ühenduse teenust, konfigureerige DNS-server. Kui te seda ei konfigureeri, peate juurdepääsuks määrama IP-aadressi, sest nimelahendus võib nurjuda.

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

Saate keelata juurdepääsu kindlale URL-ile, kasutades filtreerimisfunktsiooni, sest puhverserver saab kontrollida andmeside sisu.

Võrguühenduse häälestusmeetod

Skanneri IP-aadressi, alamvõrgu maski ja vaikelüüsi sätete määramiseks toimige alljärgnevalt.

Juhtpaneeli kasutades

Konfigureerige sätted iga skanneri jaoks skanneri juhtpaneelilt. Pärast skanneri ühendussätete konfigureerimist looge võrguga ühendus.

Installerit kasutades

Kui kasutatakse installerit, häälestatakse skanneri võrk ja klientarvuti automaatselt. Selle häälestusmeetodi kasutamiseks järgige lihtsalt installeris kuvatud juhiseid, isegi kui teil puuduvad põhjalikumad teadmised võrgust.

Ettevalmistus

Tööriista kasutades

Kasutage tööriista administraatori arvutis. Saate skanneri tuvastada ja seejärel häälestada või luua skanneritele pakettsätete määramiseks SYLK-faili. Saate häälestada palju skannereid, kuid need tuleb enne häälestust ühendada füüsiliselt Etherneti-kaabliga. Seetõttu on seda soovitatav kasutada, kui saate häälestuseks luua Etherneti-võrgu.

Seotud teave

- „Juhtpaneelilt võrku ühendamine” lk 15
- „Ühendamine võrku installeri abil” lk 19
- „IP-aadressi määramine rakendusega EpsonNet Config” lk 56

Ühendamine

See peatükk kirjeldab keskkonda või protseduuri skanneri ühendamiseks võrku.

Ühendamine võrku

Juhtpaneelilt võrku ühendamine

Ühendage skanner võrku, kasutades skanneri juhtpaneeli.

Lisateavet skanneri juhtpaneeli kohta lugege juhendist *Kasutusjuhend*.

IP-aadressi määramine

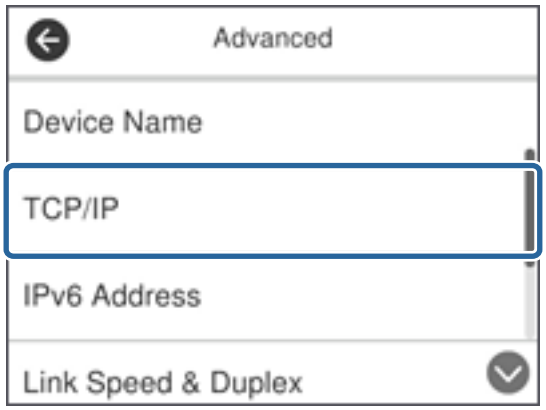
Häälestage põhiüksused, nagu IP-aadress, Alamvõrgumask ja Vaikelüüs.

1. Lülitage skanner sisse.
2. Libistage skanneri juhtpaneelil ekraani vasakule ja seejärel puudutage valikut **Sätted**.

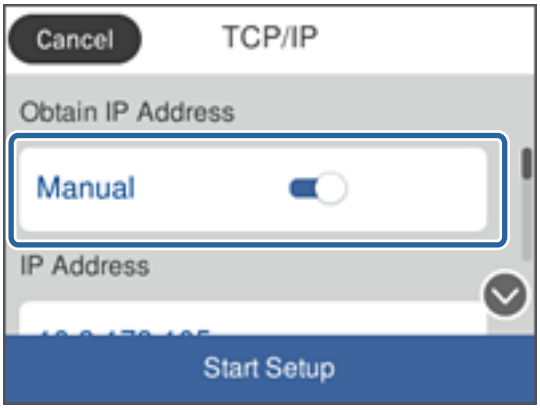
3. Puudutage valikut **Võrgusätted** > **Muuda sätteid**.

   Kui üksust ei kuvata, libistage selle kuvamiseks ekraani ülespoole.

4. Puudutage valikut **TCP/IP**.

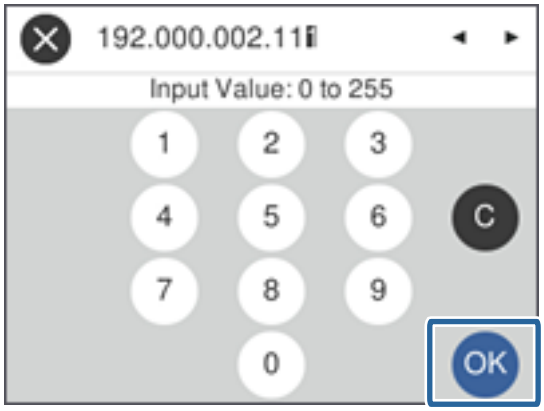


5. Suvandi **Käsitsi** sätteks valige **Hangi IP-aadress**.



Märkus.
*Kui määrate IP-aadressi automaatselt marsruuteri DHCP-funktsiooniga, valige **Automaatne**. Sel juhul määratakse sammudes 6–7 **IP-aadress**, **Alamvõrgumask** ja **Vaikelüüs** samuti automaatselt, seega jätkake sammust 8.*

6. Puudutage välja **IP-aadress**, sisestage ekraanil kuvatud klaviatuuriga IP-aadress ja seejärel puudutage valikut **OK**.



Kontrollige eelmisel ekraanil näidatavat väärtust.

7. Määrake suvandid **Alamvõrgumask** ja **Vaikelüüs**.

   Kontrollige eelmisel ekraanil näidatavat väärtust.

   Märkus.
   *Kui suvandite IP-aadress, Alamvõrgumask ja Vaikelüüs kombinatsioon on vale, jääb **Käivita häälestus** passiivseks ja sätete tegemist ei saa jätkata. Kontrollige, et sisestatud andmetes ei oleks vigu.*

8. Puudutage välja **Primaarne DNS** suvandis **DNS server**, sisestage ekraanil kuvatud klaviatuuriga primaarse DNS-serveri IP-aadress ja seejärel puudutage valikut **Nõus**.

   Kontrollige eelmisel ekraanil näidatavat väärtust.

   Märkus.
   *Kui valite IP-aadressi määramise sätteks **Automaatne**, saate DNS-serveri sätteks määrata **Käsitsi** või **Automaatne**. Kui te ei saa hankida DNS-serveri aadressi automaatselt, valige **Käsitsi** ja sisestage DNS-serveri aadress. Seejärel sisestage sekundaarne DNS-serveri aadress otse. Kui teete valiku **Automaatne**, jätkake sammust 10.*

9. Puudutage välja **Sekundaarne DNS**, sisestage ekraanil kuvatud klaviatuuriga sekundaarse DNS-serveri aadress ja seejärel puudutage valikut **Nõus**.

   Kontrollige eelmisel ekraanil näidatavat väärtust.

10. Puudutage valikut **Käivita häälestus**.

11. Puudutage kinnitusekraanil valikut **Sule**.

    Pärast teatud ajavahemikku sulgub ekraan automaatselt, kui te ei puuduta valikut **Sule**.

Ühendamine Ethernetiga

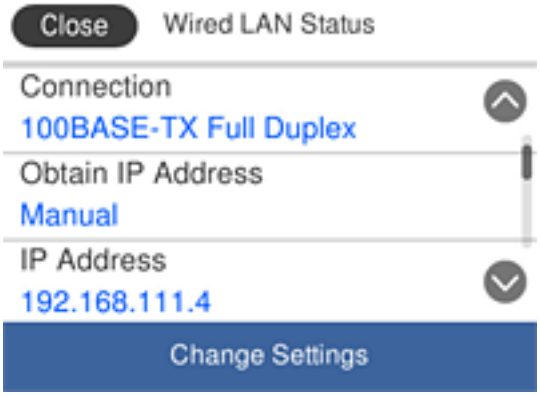
Ühendage Etherneti-kaabliga skanner võrku ja kontrollige ühendust.

1. Ühendage Etherneti-kaabliga skanner ja jaotur (L2-kommutaator).

   Ikoon avakuval muutub ikooniks  .

2. Puudutage avakuval nuppu  .

3. Libistage ekraani ülespoole ja veenduge, kas ühenduse olek ja IP-aadress on õiged.



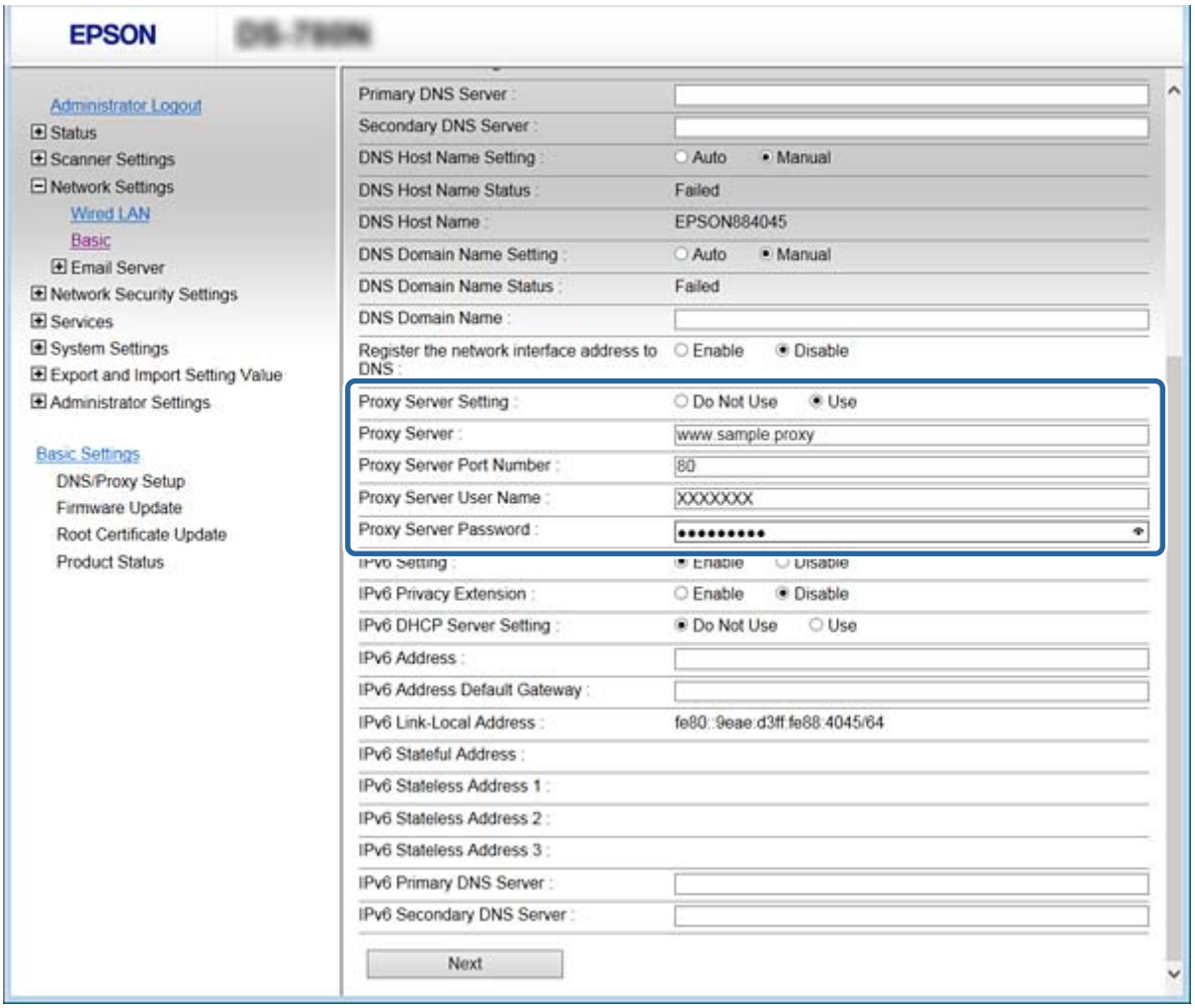
Puhverserveri määramine

Puhverserverit ei saa paneelilt määrata. Konfigureerige see rakenduses Web Config.

1. Avage Web Config ja valige **Network Settings** > **Basic**.
2. Valige säte **Use** suvandis **Proxy Server Setting**.
3. Määrake puhverserver IPv4-aadressi või FQDN-vormingus suvandis **Puhverserver** ja seejärel sisestage pordinumber suvandis **Proxy Server Port Number**.

   Autentimist nõudvate puhverserverite korral tuleb sisestada puhverserveri autentimise kasutajanimi ja parool.

4. Klõpsake nuppu **Next**.



5. Kinnitage sätted ja klõpsake seejärel valikut **Sätted**.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Ühendamine võrku installeri abil

Soovitame skanneri ühendamiseks arvutiga kasutada installerit. Installeri käivitamiseks saate kasutada ühte alljärgnevatest meetoditest.

❏ Häälestamine veebisaidilt

Minge alljärgnevale veebisaidile ja sisestage toote nimi. Valige **Häälestus** ja alustage häälestamist.

http://epson.sn

❏ Häälestamine tarkvaraketta abil (ainult siis, kui mudel on varustatud tarkvarakettaga ja kasutaja arvutil on olemas kettadraiv.)

Sisestage tarkvaraketas arvutisse ja seejärel järgige ekraanil kuvatud juhiseid.

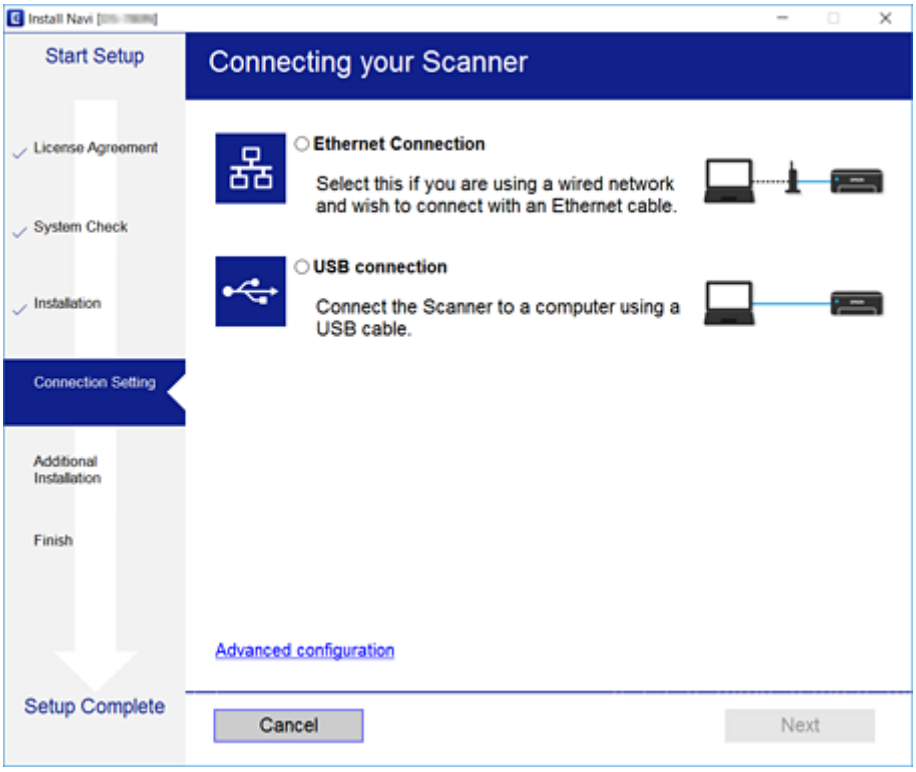
Ühendamine

Ühendusmeetodite valimine

Järgige ekraanil kuvatud juhiseid, kuni kuvatakse alljärgnev ekraan, seejärel valige ühendusmeetod skanneri ühendamiseks arvutiga.

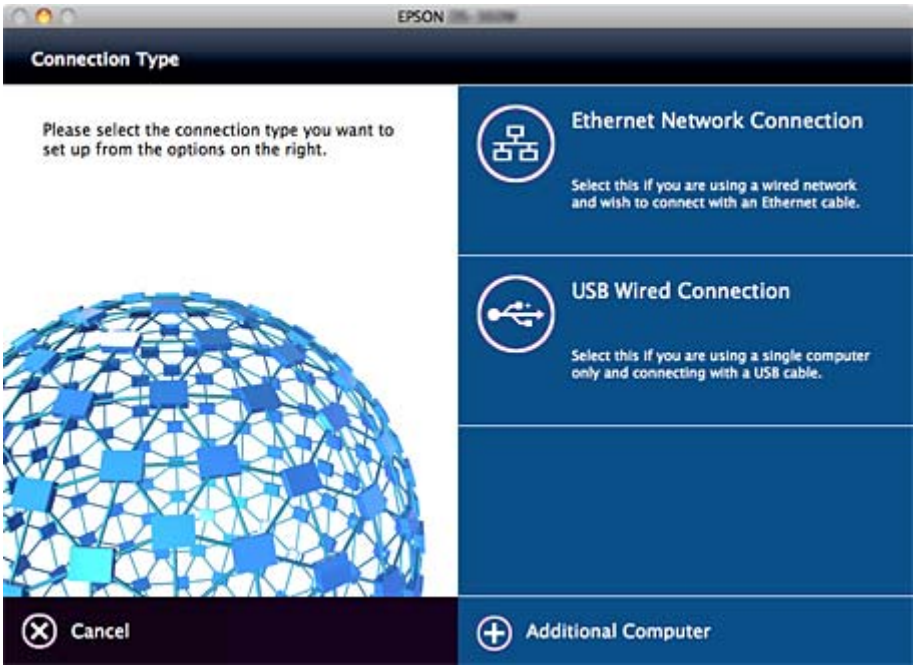
❏ Windows

Valige ühenduse tüüp ja seejärel klõpsake valikut **Edasi**.



❏ Mac OS

Valige ühenduse tüüp.



Ühendamine

Järgige ekraanil kuvatud juhiseid. Vajalik tarkvara on installitud.

Funktsioonide sätted

Selles peatükis on kirjeldatud esmaseid sätteid, mis tuleb teha, et kasutada seadme igat funktsiooni.

Häälestustarkvara

Selles teemas on kirjeldatud protseduuri sätete määramiseks administraatori arvutis tarkvaraga Web Config.

Web Config (seadme veebileht)

Teave rakenduse Web Config kohta

Web Config on skanneri sätete konfigureerimiseks mõeldud brauseripõhine rakendus.

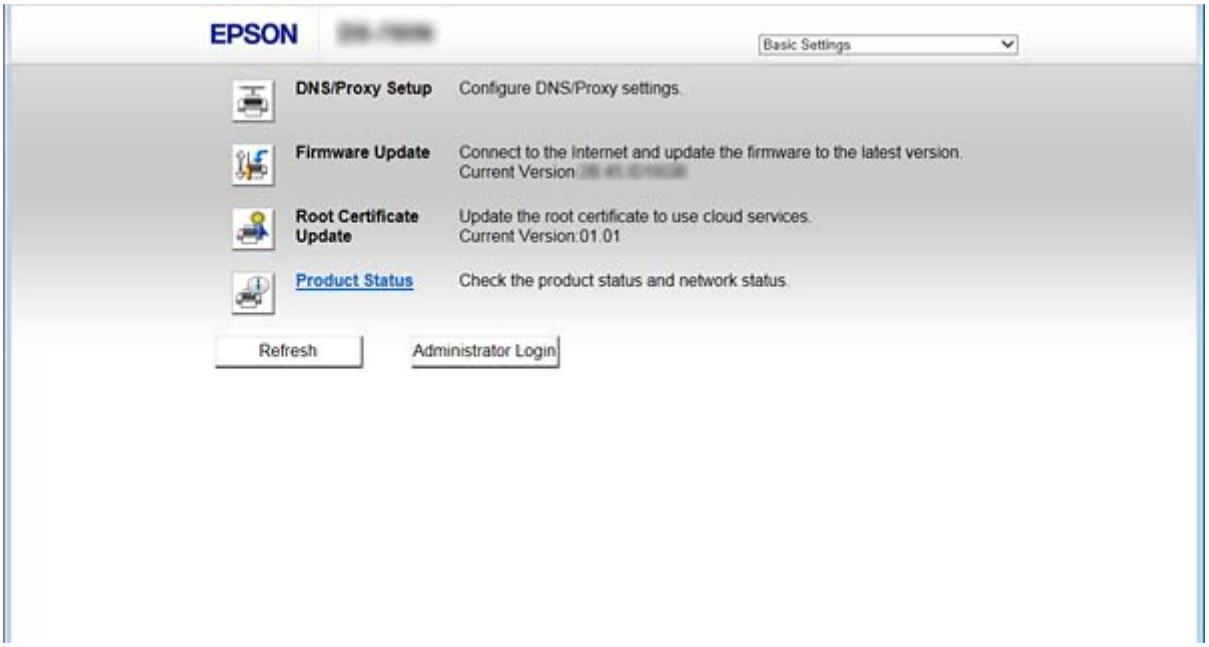
Rakendusele Web Config juurdepääsuks peate esmalt määrama skannerile IP-aadressi.

Märkus.
Te saate sätete lukustamiseks konfigureerida skannerile administraatori parooli.

Sätete seadistamiseks on kaks allpool kirjeldatud lehte.

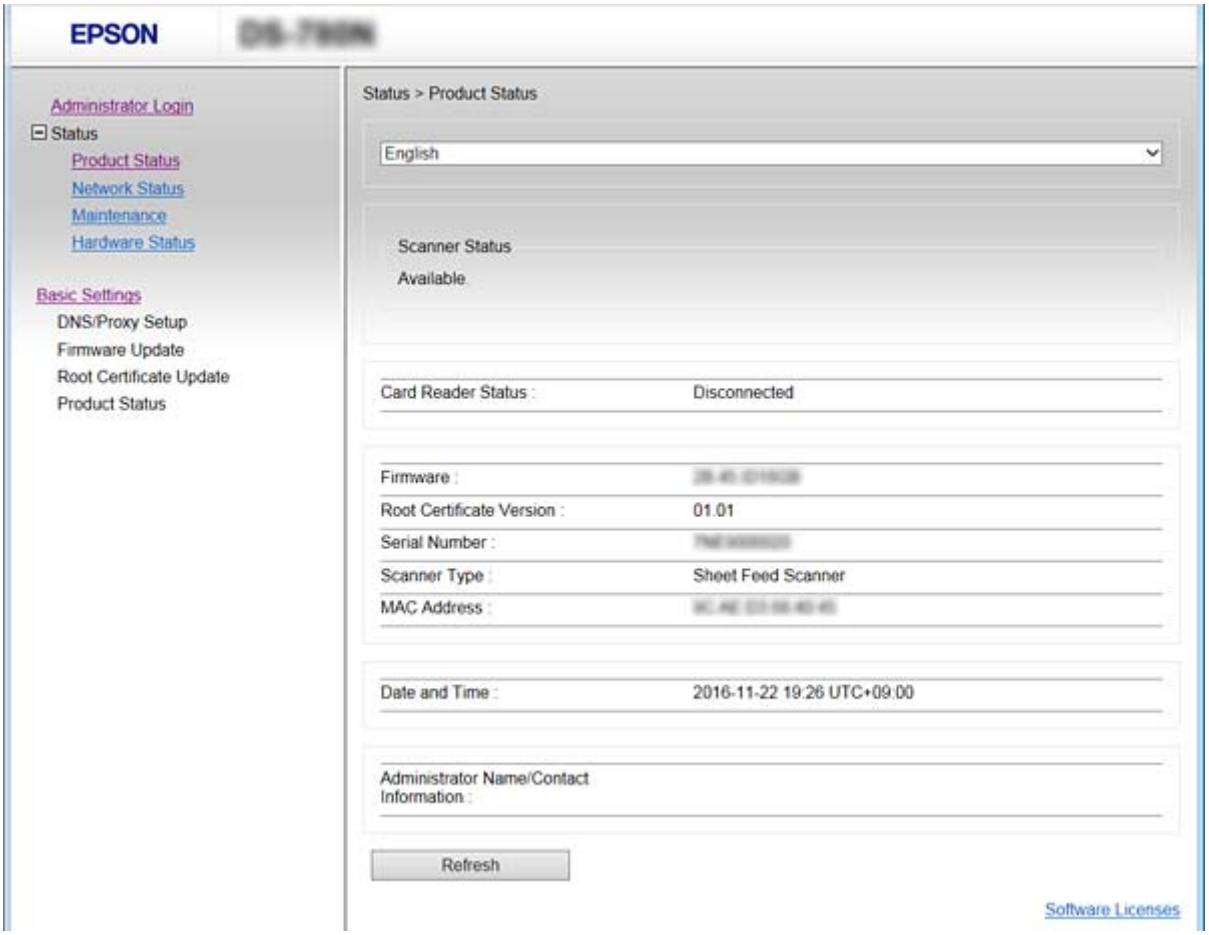
❏ **Basic Settings**

Sellel lehel saate konfigureerida skanneri põhisätteid.



❏ **Advanced Settings**

Sellel lehel saate konfigureerida skanneri täpsemaid sätteid. See leht on mõeldud eeskätt administraatorile.



Juurdepääs rakendusele Web Config

Sisestage veebibrauserisse skanneri IP-aadress. JavaScript peab olema aktiveeritud. Rakenduse Web Config avamisel HTTPS-i kaudu kuvatakse brauseris hoiatusteade, sest kasutatakse skannerisse salvestatud iseallkirjastatud sertifikaati.

❏ Juurdepääs protokolliga HTTPS

IPv4: https://<skanneri IP-aadress> (ilma sümboliteta < ja >)

IPv6: https://[skanneri IP-aadress]/ (koos sümbolitega [ja])

❏ Juurdepääs protokolliga HTTP

IPv4: http://<skanneri IP-aadress> (ilma sümboliteta < ja >)

IPv6: http://[skanneri IP-aadress]/ (koos sümbolitega [ja])

Märkus.

❏ *Näited*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

https://[2001:db8::1000:1]/

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

❏ *Kui skanneri nimi on registreeritud DNS-serveriga, saate skanneri IP-aadressi asemel kasutada skanneri nime.*

Seotud teave

➡ „SSL/TLS-side skanneriga” lk 62

➡ „Teave digitaalsertimise kohta” lk 62

Skannifunktsioonide kasutamine

Olenevalt sellest, kuidas te skannerit kasutate, installige enne kasutamist alljärgnev tarkvara ja määrake selles sätted.

❏ **Skannimine arvutist**

❏ Kinnitage võrguskannimise teenuse kehtivus rakenduses Web Config (kehtiv tehasest saatmisel).

❏ Installige oma arvutisse Epson Scan 2 ja määrake IP-aadress

❏ Tööde kasutamisega skannimise korral installige Document Capture Pro (Document Capture) ja määrake töö sätted.

❏ **Skannimine juhtpaneelilt**

❏ Kui kasutate rakendust Document Capture Pro või Document Capture Pro Server:

Installige Document Capture Pro või Document Capture Pro Server

DCP-säte (serveri režiim, kliendi režiim).

❏ Kui kasutate WSD-protokolli:

Kinnitage WSD kehtivus rakenduses Web Config või juhtpaneelil (kehtiv tehasest saatmisel)

Seadme lisasätted (Windowsi arvuti).

Arvutist skannimine

Installige tarkvara ja kontrollige, et võrguskannimise teenus oleks lubatud, et skannida arvutist võrgu kaudu.

Seotud teave

➡ „Installitav tarkvara” lk 25

➡ „Võrguskannimise aktiveerimine” lk 25

Installitav tarkvara

❏ Epson Scan 2

See on skanneridraiver. Kui kasutate seadet arvutist, installige draiver igasse klientarvutisse. Kui installitud on Document Capture Pro/Document Capture, saate teha toiminguid, mis on omistatud seadme nuppudele.

Rakendusega EpsonNet SetupManager saab printeridraivereid levitada ka koos pakettidena.

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

Installige klientarvutisse. Saate võrgus arvutist ja skanneri juhtpaneelilt välja kutsuda ja käivitada töid, mis on registreeritud arvutis, kuhu on installitud Document Capture Pro/Document Capture arvutis registreeritud töid installed on the network from the computer and scanner's operationpanel.

Saate võrgu kaudu ka arvutist skannida. Skannimiseks on vajalik Epson Scan 2.

Seotud teave

➡ „EpsonNet SetupManager" lk 56

Skanneri IP-aadressi määramine rakenduses Epson Scan 2

Määrake skanneri IP-aadress, et saaksite skannerit võrgus kasutada.

1. Käivitage rakendus **Epson Scan 2 Utility** asukohast **Start** > **Kõik programmid** > **EPSON** > **Epson Scan 2**.

   Kui juba on registreeritud teine skanner, minge sammu 2 juurde.

   Kui ei ole registreeritud, minge sammu 4 juurde.

2. Klõpsake ikooni ▼ suvandis **Skanner**.
3. Klõpsake nuppu **Seaded**.
4. Klõpsake valikut **Luba redigeerimine** ja seejärel **Lisa**.
5. Valige skanneri mudeli nimi suvandis **Mudel**.
6. Valige kasutatav skanneri IP-aadress suvandis **Aadress** kirjes **Võrguotsing**.

   Klõpsake ikooni  ja seejärel  , et loend uuendada. Kui te ei leia skanneri IP-aadressi, valige **Sisestage aadress** ja sisestage IP-aadress.

7. Klõpsake nuppu **Lisa**.
8. Klõpsake nuppu **OK**.

Võrguskannimise aktiveerimine

Saate kasutada võrguskannimise teenust, kui skannite üle võrgu klientarvutist. Vaikimisi on see aktiveeritud.

1. Avage rakendus Web Config ja valige **Services** > **Network Scan**.

2. Veenduge, et **Enable scanning** oleks valitud suvandis **EPSON Scan**.

   Kui see on valitud, on ülesanne täidetud. Sulgege Web Config.

   Kui see on valimata, valige see ja minge järgmise sammu juurde.

3. Klõpsake nuppu **Next**.

4. Klõpsake nuppu **OK**.

   Võrguga luuakse uuesti ühendus ja sätted aktiveeritakse.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Juhtpaneelilt skannimine

Skanneri juhtpaneelilt kausta skannimise funktsiooni ja meilile skannimise funktsiooni ning skannimistulemuste saatmist meilile, kaustadesse jne saab kasutada, käivitades töö arvutist.

Skannimistulemuste edastamise korral häälestage töö rakendusega Document Capture Pro Server või Document Capture Pro.

Üksikasju sätete ja töö häälestamise kohta vaadake rakenduse Document Capture Pro Server või Document Capture Pro dokumentatsioonist või spikrist.

Seotud teave

➡ „Rakenduse Document Capture Pro Server/Document Capture Pro sätted” lk 26

➡ „Serverite ja kaustade sätted” lk 27

Arvutisse installitav tarkvara

❏ **Document Capture Pro Server**

See on rakenduse Document Capture Pro serveri versioon. Installige see Windowsi serverisse. Serveriga saab tsentraalselt hallata mitmeid seadmeid ja töid. Töid saab käivitada samaaegselt mitmest skannerist.

Rakenduse Document Capture Pro Server sertifitseeritud versiooni kasutades saate hallata töid ja skannimisajalugu, mis on seotud kasutajate ja rühmadega.

Üksikasju rakenduse Document Capture Pro Server kohta küsige kohalikust Epsoni kontorist.

❏ **Document Capture Pro (Windows)/Document Capture (Mac OS)**

Nagu ka arvutist skannides, saate juhtpaneelilt välja kutsuda ja käivitada töid, mis on arvutis registreeritud. Ei ole võimalik käivitada arvuti töid samaaegselt mitmest skannerist.

Rakenduse Document Capture Pro Server/Document Capture Pro sätted

Määrake sätted skannimisfunktsiooni kasutamiseks skanneri juhtpaneelilt.

1. Avage Web Config ja valige **Services** > **Document Capture Pro**.

2. Valige **Töörežiim**.

   ❏ Server Mode:

   Valige see, kui kasutate rakendust Document Capture Pro Server või Document Capture Pro ainult kindla arvuti jaoks seadistatud tööde jaoks.

   ❏ Client Mode:

   Valige see, kui valite töö sätte rakenduse Document Capture Pro (Document Capture) jaoks, mis on installitud igasse klientarvutisse arvutit määratlemata.

3. Määrake alljärgnev vastavalt valitud režiimile.

   ❏ Server Mode:

   Määrake suvandis **Server Address** server, kuhu on installitud Document Capture Pro Server. See võib olla 2–252 tärki IPv4-, IPv6-, hostinime või FQDN-vormingus. FQDN-vormingus saab kasutada, US-ASCII tähti, numbreid, tähemärke ja sidekriipse (välja arvatud ees ja lõpus).

   ❏ Client Mode:

   Määrake **Group Settings**, et kasutada skanneri rühma, mis on valitud rakenduses Document Capture Pro (Document Capture).

4. Klõpsake nuppu **Sätted**.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Serverite ja kaustade sätted

Document Capture Pro ja Document Capture Pro Server salvestavad skannitud andmed serverisse või klientarvutisse ühe korra ja kasutavad edastamisfunktsiooni, et käivitada kausta skannimise funktsiooni ja meilile skannimise funktsiooni.

Teil peavad olema volitused ja teave, et edastada andmeid arvutist, kuhu on installitud Document Capture Pro, Document Capture Pro Server, arvutisse või pilveteenusesse.

Valmistage kasutatava funktsiooni teave ette, lähtudes alljärgnevast.

Nende funktsioonide sätteid saate määrata rakenduses Document Capture Pro või Document Capture Pro Server. Üksikasju sätete kohta vaadake rakenduse Document Capture Pro Server või Document Capture Pro dokumentatsioonist või spikrist.

Nimi	Sätted	Nõue
Skannimine võrgukausta (SMB)	Looge ja häälestage salvestuskausta ühiskasutusse andmine	Administratiivne kasutajakonto arvutisse, mis loob salvestuskaustu.
	Võrgukausta skannimise (SMB) sihtkoht	Kasutajanimi ja parool sisselogimiseks arvutisse, kus on salvestuskaust ja õigus salvestuskausta värskendamiseks.
Skannimine võrgukausta (FTP)	FTP-serverisse sisselogimise häälestamine	FTP-serveri sisselogimisteave ja õigus salvestuskausta värskendamiseks.
Skannimine meili	Meiliserveri häälestus	Meiliserveri häälestusteave

Funktsioonide sätted

Nimi	Sätted	Nõue
Skannimine rakendusse Document Capture Pro (kui kasutatakse rakendust Document Capture Pro Server)	Pilveteenustesse logimise teave	Interneti-ühenduse keskkond Pilveteenuste konto registreerimine

WSD-skannimise kasutamine (ainult Windows)

Kui arvuti kasutab opsüsteemi Windows Vista või uuemat, saate kasutada WSD-skannimist.

Kui kasutada saab WSD-protokolli, kuvatakse skanneri juhtpaneelil menüü **Arvuti (WSD)**.

1. Avage Web Config ja valige **Services** > **Protocol**.
2. Veenduge, et **Enable WSD** oleks suvandis **WSD Settings** märgitud.
   Kui see on märgitud, on ülesanne täidetud ja võite rakenduse Web Config sulgeda.
   Kui see on märkimata, märkige see ja minge järgmise sammu juurde.
3. Klõpsake nuppu **Next**.
4. Kinnitage sätted ja klõpsake valikut **Sätted**.

Süsteemi sätete määramine

Süsteemi sätete määramine juhtpaneelilt

Ekraani ereduse määramine

Määrake LCD-ekraani eredus.

1. Puudutage avakuval valikut **Sätted**.
2. Puudutage valikut **Tavasätted** > **LCD heledus**.
3. Puudutage ikooni  või  , et reguleerida eredust.
   Saate reguleerida vahemikus 1–9.
4. Puudutage valikut **Nõus**.

Heli määramine

Valige paneeli kasutamise heli ja tõrke heli.

1. Puudutage avakuval valikut **Sätted**.
2. Puudutage valikut **Tavasätted** > **Heli**.

3. Määrake vastavalt vajadusele alljärgnevad sätted.
   - ❏ Kasutamise heli
     Määrake helitugevus juhtpaneeli kasutamisel.
   - ❏ Tõrke heli
     Määrake tõrke heli helitugevus.
4. Puudutage valikut **Nõus**.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Originaali topeltsöötmise tuvastamine

Määrake funktsioon, millega tuvastada skannitava dokumendi topeltsöötmine ja skannimise peatamine, kui toimub mitmekordne söötmine.

Mitmekordset söötmist nõudvate originaalide skannimiseks (näiteks ümbrikud, kleebistega paberid) lülitage need välja.

Märkus.
Seda saab määrata ka rakenduses Web Config või Epson Scan 2.

1. Puudutage avakuval valikut **Sätted**.
2. Puudutage valikut **Välised skannimise sätted** > **Kahe lehe söötmise ultraheliandur**.
3. Puudutage valikut **Kahe lehe söötmise ultraheliandur**, et see sisse või välja lülitada.
4. Puudutage valikut **Sule**.

Madala kiiruse režiimi määramine

Valige skannimiseks madala kiirusega, et õhukeste dokumentide (näiteks sedelid) skannimise korral ei esineks paberiummistusi.

1. Puudutage avakuval valikut **Sätted**.
2. Puudutage valikut **Välised skannimise sätted** > **Aeglane**.
3. Puudutage valikut **Aeglane**, et see sisse või välja lülitada.
4. Puudutage valikut **Sule**.

Süsteemi sätete määramine rakendusega Web Config

Energiasäästu sätted jõudeoleku ajal

Määrake skanneri jõudeoleku ajaks energiasäästu säte. Määrake aeg vastavalt kasutuskeskkonnale.

Märkus.
Saate energiasäästu sätteid määrata ka skanneri juhtpaneelilt.

1. Avage Web Config ja valige **System Settings** > **Power Saving**.
2. Sisestage aeg suvandis **Sleep Timer**, et lülitada sisse energiasäästurežiim, kui esineb jõudeolekut.

   Saate minuti pealt valida kuni 240 minutit.
3. Valige väljalülitusaeg suvandis **Power Off Timer**.
4. Klõpsake nuppu **OK**.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Juhtpaneeli sätted

Skanneri juhtpaneeli häälestamine. Sätted saate määrata, nagu on kirjeldatud allpool.

1. Avage Web Config ja valige **System Settings** > **Control Panel**.
2. Häälestage vastavalt vajadusele alljärgnevad sätted.
   - ❏ Language

     Valige juhtpaneelil kuvatav keel.
   - ❏ Panel Lock

     Kui teete valiku **ON**, küsitakse administraatori parooli, kui teete toiminguid, mis nõuavad administraatori volitusi. Kui administraatori parool on määramata, on paneeli lukk inaktiveeritud.
   - ❏ Operation Timeout

     Kui teete valiku **ON** ja logite sisse administraatorina, logitakse teid automaatselt välja ja viiakse algekraanile, kui teatud aja jooksul ei tehta ühtegi toimingut.

     Saate sekundi pealt valida 10 sekundit kuni 240 minutit.
3. Klõpsake nuppu **OK**.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Välisliidese piirangu määramine

Saate USB-ühenduse kasutamist arvutist piirata. Seadistage see, et piirata skannimine mujalt peale võrgu.

1. Avage Web Config ja valige **System Settings** > **External Interface**.
2. Valige **Enable** või **Disable**.

   Piiramiseks valige **Disable**.
3. Puudutage valikut **OK**.

Kuupäeva ja kellaaja sünkroonimine ajaserveriga

Sertimiskeskuse sertifikaadi kasutamine hoiab ära probleemid ajaga.

1. Avage Web Config ja valige **System Settings** > **Date and Time** > **Time Server**.
2. Suvandi **Use** sätteks valige **Use Time Server**.
3. Sisestage väljale **Time Server Address** ajaserveri aadress.

   Te võite kasutada vormingut IPv4, IPv6 või FQDN. Sisestage 252 tärki või vähem. Kui te seda ei kasuta, jätke see tühjaks.
4. Sisestage nimi väljale **Update Interval (min)**.

   Saate minuti pealt valida kuni 10 800 minutit.
5. Klõpsake nuppu **OK**.

   Märkus.
   *Ühenduse olekut ajaserveriga näitab **Time Server Status**.*

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Põhilised turvasätted

Selles peatükis on kirjeldatud põhilisi turvasätteid, mis ei nõua erilist keskkonda.

Põhiliste turvafunktsioonide tutvustus

Tutvustame teile Epsoni seadmete põhilisi turvafunktsioone.

Funktsiooni nimi	Funktsiooni tüüp	Sätted	Mida ennetatakse
Administraatori parooli määramine	Lukustage süsteemiga seotud sätted, nagu võrgu- ja USB-ühenduse sätted, et neid ei saaks muuta keegi peale administraatori.	Administraator määrab seadmele parooli. Konfigureerimine ja värskendamine on võimalikud kõikjal rakendusega Web Config, juhtpaneelilt, rakendusega Epson Device Admin ja rakendusega EpsonNet Config.	Takistab seadmesse salvestatud teabe (näiteks ID, parool, võrgusätted, kontaktid) ebaseaduslikku lugemist. Lisaks vähendab paljusid turvariske, nagu võrgukeskkonna või turvapoliitika teabe lekkimine.
SSL/TLS-side	Kui kasutate Epsoni serverit Internetis seadmest, näiteks arvutiga ühenduse loomisel läbi veebibrauseri või püsivara uuendamisel, kasutatakse side krüptimiseks SSL/TLS-sidet.	Hankige sertimiskeskuse allkirjastatud sertifikaat ja importige see skannerisse.	Seadme identifitseerimine sertimiskeskuse allkirjastatud sertifikaadiga hoiab ära teeskluse ja volitamata juurdepääsu. Lisaks on SSL/TLS-andmeside sisu kaitstud ja see takistab printimisandmete ja häälestusteabe lekkimist.
Protokollide juhtimine	Juhib protokolle, mida kasutatakse sideks seadmete ja arvutite vahel ning aktiveerib ja inaktiveerib funktsioone.	Funktsioonide eraldi keelamine või lubamine neile kohalduva protokolli või teenusega.	Tahtmatust kasutusest tulenevate turvariskide vähendamine, takistades kasutajatel ebavajalike funktsioonide kasutamist.

Seotud teave

➡ „Teave rakenduse Web Config kohta” lk 22
➡ „EpsonNet Config” lk 55
➡ „Epson Device Admin” lk 55
➡ „Administraatori parooli konfigureerimine” lk 32
➡ „Juhtimisprotokollid” lk 35

Administraatori parooli konfigureerimine

Kui te määrate administraatori parooli, ei saa muud kasutajad peale administraatori süsteemihalduse sätteid muuta. Administraatori parooli saab määrata ja muuta rakenduses Web Config, skanneri juhtpaneelilt või tarkvaras (Epson Device Admin või EpsonNet Config). Kui kasutate tarkvara, lugege vastava tarkvara dokumentatsiooni.

Seotud teave

➡ „Administraatori parooli konfigureerimine juhtpaneelilt” lk 33
➡ „Administraatori parooli konfigureerimine rakenduses Web Config” lk 33
➡ „EpsonNet Config” lk 55
➡ „Epson Device Admin” lk 55

Administraatori parooli konfigureerimine juhtpaneelilt

Saate määrata administraatori parooli skanneri juhtpaneelilt.

1. Puudutage avakuval valikut **Sätted**.
2. Puudutage valikut **Süsteemi administreerimine** > **Administraatori sätted**.

   Kui üksust ei kuvata, libistage selle kuvamiseks ekraani ülespoole.
3. Puudutage valikut **Administraatori parool** > **Registreeri**.
4. Sisestage uus parool ja seejärel puudutage valikut **Nõus**.
5. Sisestage parool uuesti ja seejärel puudutage valikut **Nõus**.
6. Puudutage kinnitusekraanil valikut **Nõus**.

   Kuvatakse administraatori sätete ekraan.
7. Puudutage valikut **Lukustamise sätted** ja seejärel puudutage kinnitusekraanil valikut **Nõus**.

   Suvandi Lukustamise sätted sätteks määratakse **Sees** ja lukustatud menüükirje kasutamiseks nõutakse administraatori parooli.

Märkus.

❏ *Kui määrate suvandi **Sätted** > **Tavasätted** > **Toimingu ajalõpp** sätteks **Sees**, logib skanner teid välja, kui juhtpaneelil ei tehta teatud aja jooksul ühtegi toimingut.*

❏ *Saate administraatori parooli muuta või kustutada, kui teete valiku **Muuda** või **Lähtesta** ekraanil **Administraatori parool** ja sisestate administraatori parooli.*

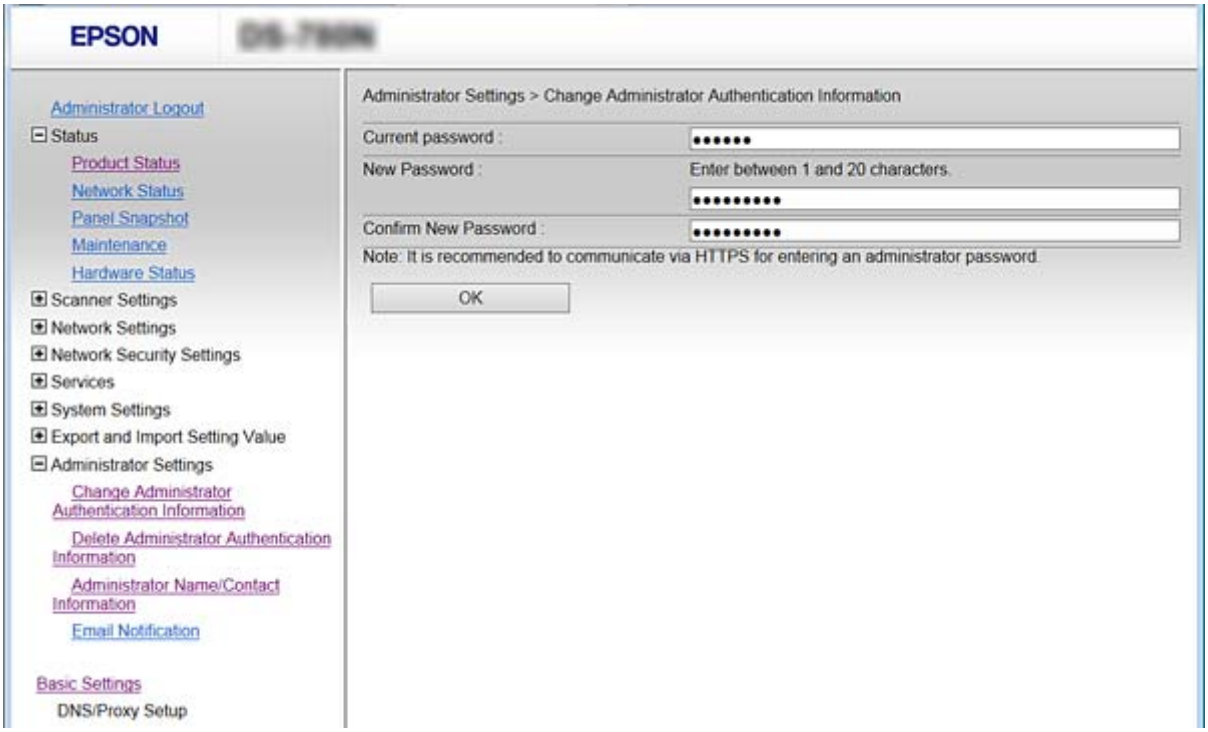
Administraatori parooli konfigureerimine rakenduses Web Config

Administraatori parooli saate määrata rakenduses Web Config.

1. Avage Web Config ja valige **Administrator Settings** > **Change Administrator Authentication Information**.

2. Sisestage parool väljadele **New Password** ja **Confirm New Password**. Vajaduse korral sisestage kasutajanimi.

   Kui soovite parooli uue vastu vahetada, sisestage kehtiv parool.



3. Valige **OK**.

   Märkus.

   ❏ *Lukustatud menüükirjete määramiseks või muutmiseks klõpsake valikut **Administrator Login** ja seejärel sisestage administraatori parool.*

   ❏ *Administraatori parooli kustutamiseks klõpsake valikut **Administrator Settings** > **Delete Administrator Authentication Information** ja seejärel sisestage administraatori parool.*

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Administraatori parooliga lukustatavad üksused

Administraatoritel on õigused seadmete kõigi funktsioonide muutmiseks ja sätete määramiseks.

Lisaks, kui te määrate seadmes administraatori parooli, saate selle lukustada, et seadme haldusega seotud üksusi ei saaks muuta.

Allpool on toodud üksused, mida saab kontrollida administraator.

Üksus	Kirjeldus
Skanneri sätted	Topeltsöötmise tuvastuse ja madala kiiruse režiimi määramine.
Etherneti-ühenduse sätted	Muutke seadmete nimesid, IP-aadressi, häälestage DNS-serverit ja puhverserverit, muutke võrguühendusega seotud sätteid.

Üksus	Kirjeldus
Kasutaja teenuste sätted	Häälestamine sideprotokollide, võrguskannimise ja Document Capture Pro teenuste juhtimiseks.
Meiliserveri sätted	Meiliserveri, millega seadmed otse suhtlevad, häälestamine.
Turvasätted	Võrgu turvasätted, nagu SSL/TLS-side, IPsec/IP-filtreerimine ja IEEE802.1X.
Juurserdi värskendamine	Rakenduse Document Capture Pro Server jaoks vajalike juursertide autentimine ja püsivara uuendamine rakendusest Web Config.
Püsivara värskendamine	Kontrollige ja värskendage seadmete püsivara.
Aja ja taimeri sätted	Unerežiimi minemise aeg, automaatne väljalülitus, kuupäev/kellaaeg, jõudeolekutaimer, muud taimeriga seotud sätted.
Vaikesätete taastamine	Säte skanneri tehasesätete taastamiseks.
Administraatori sätted	Administraatori luku või administraatori parooli määramine.
Sertifitseeritud seadme säte	Autentimisseadme ID säte. Aktiveerige see, kui kasutate skannerit autentimissüsteemis, mis toetab autentimisseadmeid.

Juhtimisprotokollid

Te saate skannimiseks kasutada mimeid radasid ja protokolle. Saate võrguskannimist kasutada ka määramata arvust võrguarvutitest. Näiteks on lubatud skannimine, kasutades ainult kindlaks määratud radasid ja protokolle. Saate langetada kasutamisel ilmnevaid turvariske, kui piirate skannimist teatud radade kaudu või kui vaatate üle saadavalolevad funktsioonid.

Häälestage protokolli sätted.

1. Avage Web Config ja valige **Services** > **Protocol**.
2. Määrake kõik sätted.
3. Klõpsake nuppu **Next**.
4. Klõpsake nuppu **OK**.

   Sätted rakenduvad skannerile.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Aktiveeritavad ja deaktiveeritavad protokollid” lk 35

➡ „Protokolli sätete määramine” lk 37

Aktiveeritavad ja deaktiveeritavad protokollid

Protokoll	Kirjeldus
Bonjour Settings	Saate määrata, kas kasutada Bonjour. Rakendust Bonjour kasutatakse seadmete otsimiseks, skannimiseks jne.

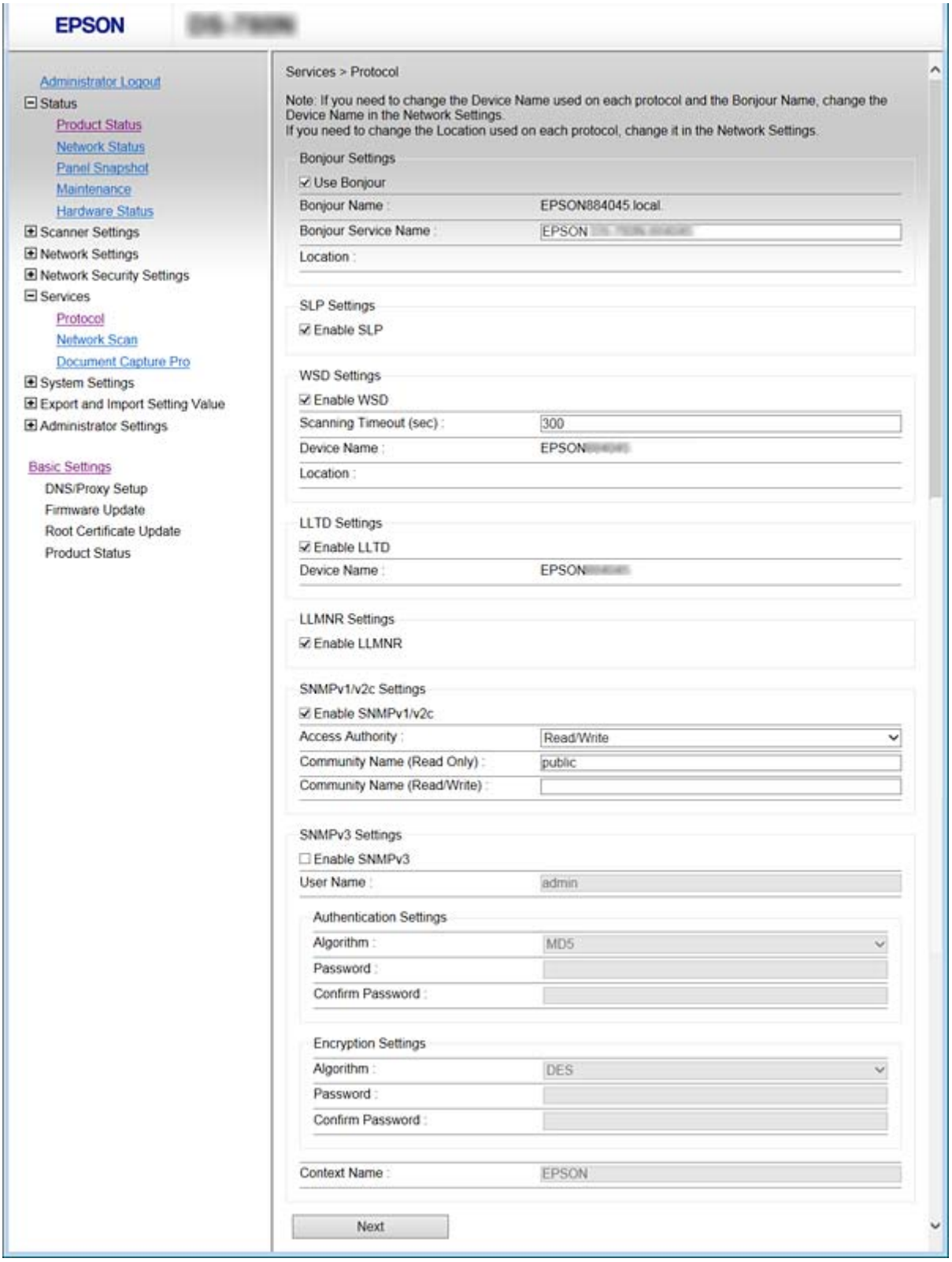
Protokoll	Kirjeldus
SLP Settings	Saate funktsiooni SLP aktiveerida või inaktiveerida. Funktsiooni SLP kasutatakse rakenduses Epson Scan 2 ja võrgu otsimiseks rakenduses EpsonNet Config.
WSD Settings	Saate funktsiooni WSD aktiveerida või inaktiveerida. Kui see on aktiveeritud, saate lisada WSD-seadmeid või skannida WSD-pordi kaudu.
LLTD Settings	Saate funktsiooni LLTD aktiveerida või deaktiveerida. Kui see funktsioon on aktiveeritud, kuvatakse see võrgukaardil Windows.
LLMNR Settings	Saate funktsiooni LLMNR aktiveerida või deaktiveerida. Kui see funktsioon on aktiveeritud, saate kasutada nimelahendust ilma protokolli NetBIOS rakendamata, isegi kui te ei saa kasutada DNS serverit.
SNMPv1/v2c Settings	Saate määrata, kas aktiveerida protokoll SNMPv1/v2c või mitte. Seda kasutatakse seadmete alghäälestamiseks, jälgimiseks jne.
SNMPv3 Settings	Saate määrata, kas aktiveerida protokoll SNMPv3 või mitte. Seda kasutatakse krüptitud seadmete häälestamiseks, jälgimiseks jne.

Seotud teave

➡ „Juhtimisprotokollid” lk 35

➡ „Protokolli sätete määramine” lk 37

Protokolli sätete määramine



Üksused	Sätteväärtus ja kirjeldus
Bonjour Settings	

Põhilised turvasätted

Üksused	Sätteväärtus ja kirjeldus
Use Bonjour	Valige see, et otsida või kasutada seadmeid läbi rakenduse Bonjour.
Bonjour Name	Kuvab rakenduse Bonjour nime.
Bonjour Service Name	Saate kuvada ja määrata rakenduse Bonjour teenuse nime.
Location	Kuvab rakenduse Bonjour asukohta.
SLP Settings	
Enable SLP	Valige see SLP funktsiooni aktiveerimiseks. Seda kasutatakse rakendustes Epson Scan 2 ja EpsonNet Config võrgu avastamiseks.
WSD Settings	
Enable WSD	Valige see, et lubada seadmete lisamine WSD-ga ning printida ja skannida WSD-pordi kaudu.
Scanning Timeout (sec)	Sisestage WSD kaudu skannimise ooteaeg vahemikus 3 kuni 3600 sekundit.
Device Name	Kuvab rakenduse WSD seadme nime.
Location	Kuvab rakenduse WSD asukohta.
LLTD Settings	
Enable LLTD	Valige see LLTD funktsiooni aktiveerimiseks. Skanner kuvatakse Windows võrgukaardil.
Device Name	Kuvab rakenduse LLTD seadme nime.
LLMNR Settings	
Enable LLMNR	Valige see LLMNR funktsiooni aktiveerimiseks. Saate kasutada nimelahendust ilma protokolli NetBIOS rakendamata, isegi kui te ei saa kasutada DNS serverit.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Valige, et aktiveerida SNMPv1/v2c. Kuvatakse ainult need skannerid, mis toetavad SNMPv3 sidet.
Access Authority	Määrake juurdepääsu volitused, kui SNMPv1/v2c on aktiveeritud. Valige **Read Only** või **Read/Write**.
Community Name (Read Only)	Sisestage 0 kuni 32 ASCII (0x20 kuni 0x7E) vormingus tähemärki.
Community Name (Read/Write)	Sisestage 0 kuni 32 ASCII (0x20 kuni 0x7E) vormingus tähemärki.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 on aktiveeritud, kui märkeruut on valitud.
User Name	Sisestage 1 kuni 32 tärki, kasutades 1-baidiseid tärke.
Authentication Settings	

Põhilised turvasätted

Üksused	Sätteväärtus ja kirjeldus
Algorithm	Valige protokolli SNMPv3 autentimisalgoritm.
Password	Sisestage parool protokolli SNMPv3 autentimiseks. Sisestage 8–32 tärki ASCII-vormingus (0x20–0x7E). Kui te seda ei kasuta, jätke see tühjaks.
Confirm Password	Sisestage kinnitamiseks konfigureeritud parool.
Encryption Settings	
Algorithm	Valige protokolli SNMPv3. krüptimisalgoritm.
Password	Sisestage parool protokolli SNMPv3 krüptimiseks. Sisestage 8–32 tärki ASCII-vormingus (0x20–0x7E). Kui te seda ei kasuta, jätke see tühjaks.
Confirm Password	Sisestage kinnitamiseks konfigureeritud parool.
Context Name	Sisestage 32 tärki või vähem Unicode-vormingus (UTF-8). Kui te seda ei kasuta, jätke see tühjaks. Sisestatavate tärkide arv erineb keelest olenevalt.

Seotud teave

➡ „Juhtimisprotokollid” lk 35

➡ „Aktiveeritavad ja deaktiveeritavad protokollid” lk 35

Kasutamise ja haldamise sätted

Selles peatükis on kirjeldatud üksusi, mis on seotud seadme igapäevaste toimingute ja haldamisega.

Seadme teabe kontrollimine

Suvandist **Status** saate rakendusega Web Config vaadata töötava seadme kohta alljärgnevat teavet.

❏ Product Status

Vaadake keelt, olekut, tootenumbrit, MAC-aadressi jne.

❏ Network Status

Vaadake võrguühenduse olekut, IP-aadressi, DNS-serverit jne.

❏ Panel Snapshot

Kuvab seadme juhtpaneeli ekraanipildi hetktõmmise.

❏ Maintenance

Vaadake alguskuupäeva, skannimisteavet jne.

❏ Hardware Status

Vaadake skanneri olekut.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Seadmete haldamine (Epson Device Admin)

Rakendusega Epson Device Admin saate hallata ja kasutada paljusid seadmeid. Epson Device Admin laseb teil hallata erinevas võrgus asuvaid seadmeid. Alljärgnev võtab kokku peamised haldusfunktsioonid.

Lisateavet funktsioonide ja tarkvara kasutamise kohta lugege rakenduse Epson Device Admin dokumentatsioonist või spikrist.

❏ Seadmete tuvastamine

Saate tuvastada võrgus olevaid seadmeid ja neid seejärel loendis registreerida. Kui Epsoni seadmed, nagu printerid ja skannerid, on ühendatud administraatori arvutiga samasse võrgusegmenti, saate neid tuvastada isegi siis, kui neile ei ole määratud IP-aadressi.

Lisaks saate tuvastada seadmeid, mis on USB-kaabliga ühendatud võrgus olevate arvutitega. Peate arvutisse installima rakenduse Epson Device USB Agent.

❏ Seadmete häälestamine

Saate luua malli, mis sisaldab sätteüksusi (näiteks võrguliides ja paberiallikas), ja rakendada seda muudele seadmetele ühiskasutatavate sätetena. Kui seade on ühendatud võrku ja sellele ei ole IP-aadressi määratud, saate sellele määrata IP-aadressi.

❏ Seadmete jälgimine

Saate regulaarselt vaadata võrgus olevate seadmete olekut ja üksikasjalikku teavet. Samuti saate jälgida seadmeid, mis on USB-kaabliga ühendatud võrgus olevate arvutitega, ja teiste ettevõtete seadmeid, mis on registreeritud seadmete loendis. USB-kaabliga ühendatud seadmete jälgimiseks peate installima rakenduse Epson Device USB Agent.

❏ Hoiatuste haldamine

Saate jälgida hoiatusi seadmete ja tarvikute oleku kohta. Süsteem saadab administraatorile automaatselt meiliteatisi, lähtudes määratud tingimustest.

❏ Aruannete haldamine

Saate luua regulaarseid aruandeid, kui süsteem kogub andmeid seadmete ja tarvikute kasutamise kohta. Seejärel saate loodud aruanded salvestada ja neid meilitsi saata.

Seotud teave

➡ „Epson Device Admin” lk 55

Meiliteavituste saamine sündmuste toimumisel

Teave meiliteatiste kohta

Saate seda funktsiooni kasutada teatiste vastuvõtmiseks meiliaadressile, kui midagi juhtub. Saate registreerida kuni 5 meiliaadressi ja teha valida, millistest sündmustest teid teavitatakse.

Selle funktsiooni kasutamiseks tuleb konfigureerida meiliserver.

Seotud teave

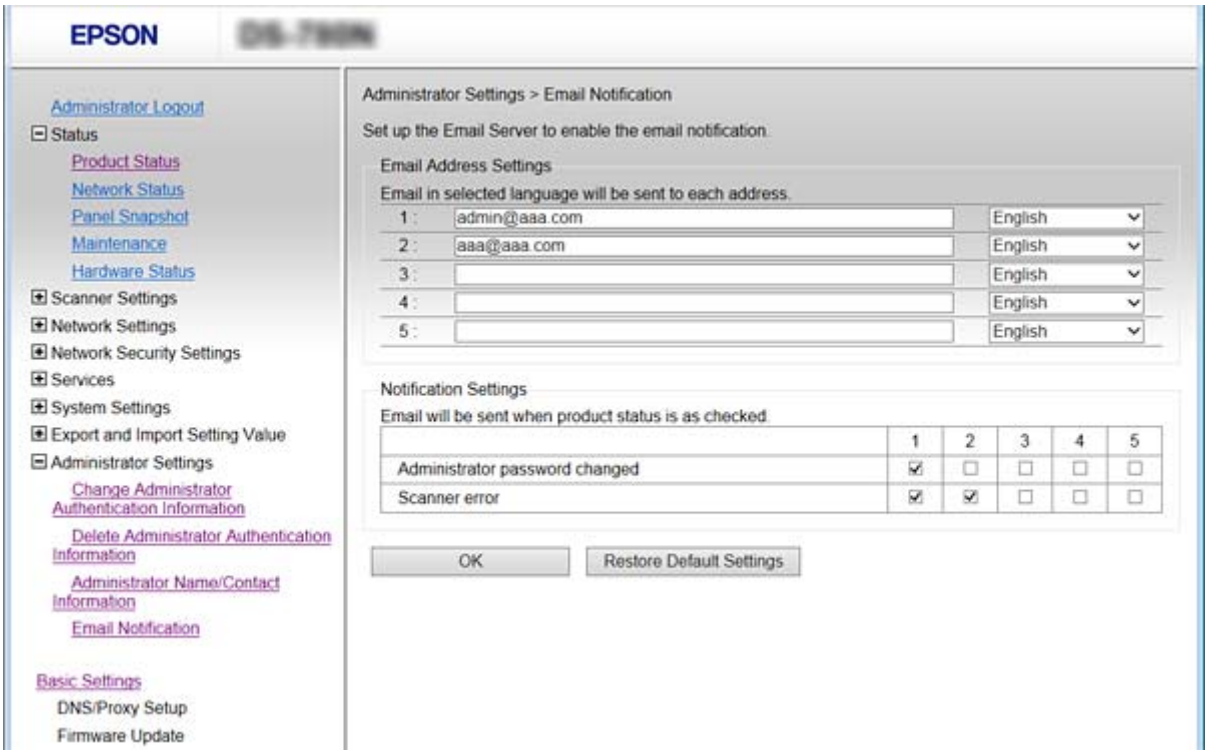
➡ „Meiliserveri konfigureerimine” lk 42

Meiliteatiste konfigureerimine

Funktsiooni kasutamiseks peate konfigureerima meiliserveri.

1. Avage Web Config ja valige **Administrator Settings** > **Email Notification**.
2. Sisestage meiliaadressid, millele soovite saada meiliteatisi.
3. Valige meiliteatiste keel.

4. Märgistage nende meiliteatiste kastid, mida soovite saada.



5. Klõpsake nuppu **OK**.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Meiliserveri konfigureerimine” lk 42

Meiliserveri konfigureerimine

Enne häälestamist kontrollige järgmist.

❏ Skanner on ühendatud võrku.

❏ Vaadake üle e-posti serveri sätted.

1. Avage Web Config ja valige **Network Settings** > **Email Server** > **Basic**.
2. Sisestage kõigile kirjetele väärtus.
3. Valige suvand **OK**.

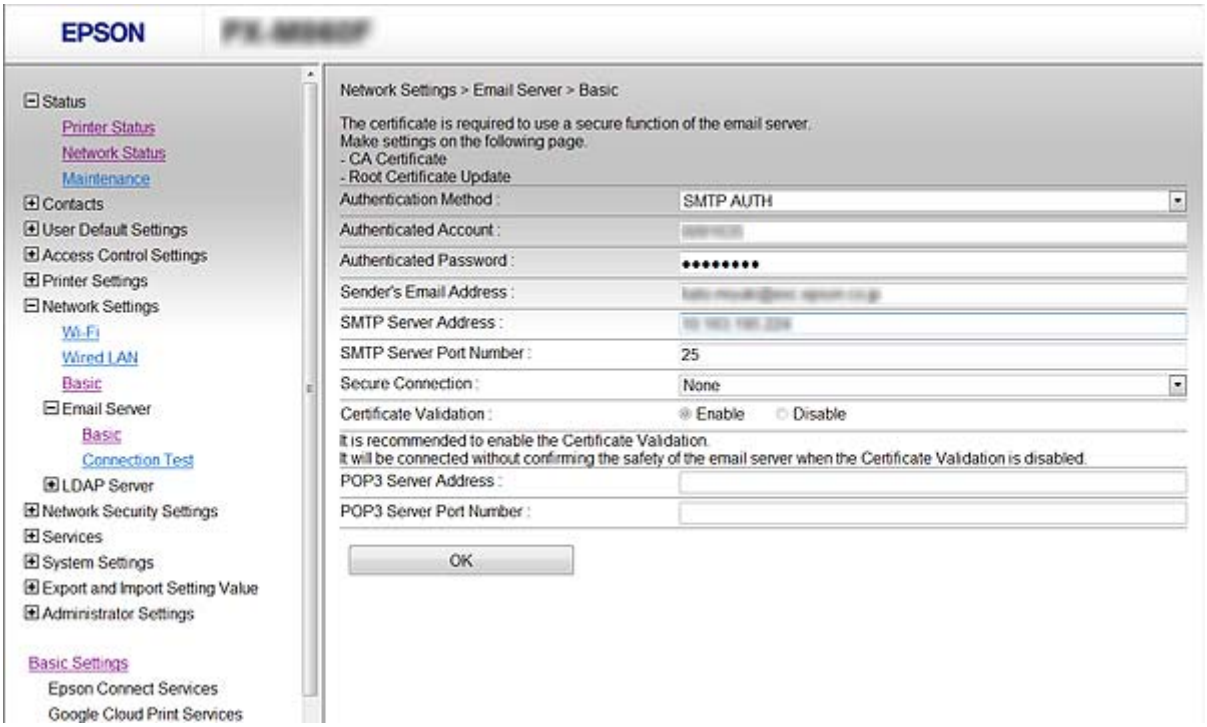
   Kuvatakse valitud sätted.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Meiliserveri sättekirjed” lk 43

Meiliserveri sättekirjed



Kirjed	Sätted ja selgitus	
Authentication Method	Määrake skannerile autentimismeetod, mida kasutatakse meiliserverile juurdepääsul.	
	Off	Autentimine on side ajal meiliserveriga inaktiveeritud.
	SMTP AUTH	Nõuab, et meiliserver toetaks SMTP-autentimist.
	POP before SMTP	Kui valite selle meetodi, konfigureerige POP3-server.
Authenticated Account	Kui te valite **SMTP AUTH** või **POP before SMTP** autentimisviisiks **Authentication Method**, sisestage autentimiskonto nimi, mille pikkus on vahemikus 0 kuni 255 tähemärki ASCII (0x20–0x7E) vormingus.	
Authenticated Password	Kui valite sätte **SMTP AUTH** või **POP before SMTP** suvandi **Authentication Method** sätteks, sisestage autentimisparool pikkusega 0–20 tähemärki (A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @).	
Sender's Email Address	Sisestage saatja meiliaadress. Sisestage 0–255 tähemärki standardkoodis ASCII (0x20–0x7E), kuid ärge kasutage sümboleid : ( ) < > [ ] ; ¥. Punkt „.” ei tohi olla esimeseks tähemärgiks.	
SMTP Server Address	Sisestage 0–255 tähemärki (A–Z a–z 0–9 . -). Te võite kasutada vormingut IPv4 või FQDN.	
SMTP Server Port Number	Sisestage number vahemikus 1 kuni 65535.	

Kirjed	Sätted ja selgitus	
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 aktiveeritud, on sert kontrollitud. Soovitame selle sätteks määrata **Enable**.	
POP3 Server Address	Kui valite sätte **POP before SMTP** suvandi **Authentication Method** sätteks, sisestage POP3-serveri aadress pikkusega 0–255 tähemärki (A–Z a–z 0–9 . -). Te võite kasutada vormingut IPv4 või FQDN.	
POP3 Server Port Number	Kui valite sätte **POP before SMTP** suvandi **Authentication Method** sätteks, sisestage arv 1–65535.	

Seotud teave

➡ „Meiliserveri konfigureerimine” lk 42

Meiliserveri ühenduse kontrollimine

1. Avage Web Config ja valige **Network Settings** > **Email Server** > **Connection Test**.
2. Valige suvand **Start**.

   Algab e-posti serveri ühenduse test. Pärast testimist kuvatakse kontrollaruanne.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23
➡ „Meiliserveri ühenduse testimisviited” lk 44

Meiliserveri ühenduse testimisviited

Teated	Selgitus
Connection test was successful.	See teade kuvatakse siis, kui ühendus serveriga toimib ja vastab nõuetele.
SMTP server communication error. Check the following. - Network Settings	Ekraanil kuvatakse teade alljärgnevas olukorras ❏ Skanner ei ole võrku ühendatud ❏ SMTP-server ei tööta ❏ Võrguühendus katkes sidepidamise ajal ❏ Vastuvõetud andmed on puudulikud

Kasutamise ja haldamise sätted

Teated	Selgitus
POP3 server communication error. Check the following. - Network Settings	Ekraanil kuvatakse teade alljärgnevas olukorras ❏ Skanner ei ole võrku ühendatud ❏ POP3-server ei tööta ❏ Võrguühendus katkes sidepidamise ajal ❏ Vastuvõetud andmed on puudulikud
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Ekraanil kuvatakse teade alljärgnevas olukorras ❏ Ühendamine DNS-serveriga ebaõnnestus ❏ Nimelahendus SMTP-serveris ebaõnnestus
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Ekraanil kuvatakse teade alljärgnevas olukorras ❏ Ühendamine DNS-serveriga ebaõnnestus ❏ Nimelahendus POP3-serveris ebaõnnestus
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	See teade kuvatakse siis, kui SMTP-serveri autentimine ebaõnnestus.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	See teade kuvatakse siis, kui POP3-serveri autentimine ebaõnnestus.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	See teade kuvatakse siis, kui soovite saada ühendust mittetoetatud protokolle kasutades.
Connection to SMTP server failed. Change Secure Connection to None.	See teade kuvatakse, kui SMTP-serveris ilmneb serveri ja kliendi andmete lahknevus või kui server ei toeta SMTP turvalist ühendust (SSL-ühendus).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	See teade kuvatakse, kui SMTP-serveris ilmneb serveri ja kliendi andmete lahknevus või kui server nõuab SSL/TLS-ühenduse kasutamist SMTP turvalise ühenduse jaoks.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	See teade kuvatakse, kui SMTP-serveris ilmneb serveri ja kliendi andmete lahknevus või kui server nõuab STARTTLS-ühenduse kasutamist SMTP turvalise ühenduse jaoks.
The connection is untrusted. Check the following. - Date and Time	See teade kuvatakse siis, kui skanneri kuupäeva ja kellaaja sätted on valed või sertifikaat on aegunud.
The connection is untrusted. Check the following. - CA Certificate	See teade kuvatakse siis, kui skanneril puudub serverile vastav juursert või kui sert CA Certificate on importimata.
The connection is not secured.	See teade kuvatakse siis, kui saadud sert on vigastatud.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	See teade kuvatakse, kui serveri ja kliendi autentimisviisid ei ole vastavuses. Server toetab autentimisviisi SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	See teade kuvatakse, kui serveri ja kliendi autentimisviisid ei ole vastavuses. Server ei toeta autentimisviisi SMTP AUTH.

Teated	Selgitus
Sender's Email Address is incorrect. Change to the email address for your email service.	See teade kuvatakse siis, kui määratud saatja e-posti aadress on vale.
Cannot access the product until processing is complete.	See teade kuvatakse siis, kui skanner on hõivatud.

Seotud teave

➡ „Meiliserveri ühenduse kontrollimine” lk 44

Püsivara värskendamine

Püsivara värskendamine rakendusega Web Config

Värskendab püsivara rakendusega Web Config. Seade peab olema ühendatud Internetti.

1. Avage Web Config ja valige **Basic Settings** > **Firmware Update**.
2. Klõpsake nuppu **Start**.

   Algab püsivara kontrollimine ja kui olemas on värskendatud püsivara, kuvatakse püsivara teave.
3. Klõpsake valikut **Start** ja järgige ekraanil kuvatud juhiseid.

Märkus.
Püsivara võite värskendada ka rakendusega Epson Device Admin. Püsivara teavet saate visuaalselt kontrollida seadmete loendist. See on kasulik, kui soovite värskendada mitme seadme püsivara. Lisateavet vaadake rakenduse Epson Device Admin juhendist või spikrist.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23
➡ „Epson Device Admin” lk 55

Püsivara värskendamine rakendusega Epson Firmware Updater

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.

1. Avage Epsoni veebisait ja laadige alla püsivara.
2. Ühendage allalaaditud püsivara sisaldav arvuti USB-kaabli abil seadmega.
3. Topeltklõpsake allalaaditud faili laiendiga .exe.

   Epson Firmware Updater käivitub.
4. Järgige ekraanil kuvatud juhiseid.

Sätete varundamine

Kui ekspordite sätteüksused rakendusest Web Config, saate üksused kopeerida teistesse skanneritesse.

Sätete eksportimine

Eksportige skanneri iga säte.

1. Avage Web Config ja valige seejärel **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 teil vaja parooli. Kui soovite faili krüptida, jätke see väli tühjaks.
4. Klõpsake nuppu **Export**.

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

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Sätete importimine

Importige eksporditud rakenduse Web Config fail printerisse.

> ***Oluline teave:***
>
> *Kui impordite väärtusi, mis sisaldavad üksikteavet, nagu skanneri nimi ja IP aadress, veenduge, et samas võrgus poleks sama IP aadressi. Kui IP-aadress kattub, siis skanner seda väärtust vastu ei võta.*

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

Sätted rakenduvad skannerile.

Kasutamise ja haldamise sätted

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Probleemide lahendamine

Soovitused probleemide lahendamiseks

Lisateavet saate alljärgnevast juhendist.

❏ Kasutusjuhend

Sisaldab juhiseid skanneri kasutamise, hoolduse ja probleemide lahendamise kohta.

Serveri ja võrguseadme logi kontrollimine

Kui võrguühendusega on probleeme, võib olla võimalik nende põhjustaja tuvastamine meiliserveri, LDAP-serveri vms logist, kontrollides olekut süsteemi seadmete (nagu marsruuter) logide ja käskude võrgulogi.

Võrgusätete lähtestamine

Võrgusätete taastamine printeri juhtpaneelilt

Saate taastada kõikide võrgusätete vaikeväärtused.

1. Puudutage avakuval valikut **Sätted**.
2. Puudutage valikut **Süsteemi administreerimine** > **Taasta vaikesätted** > **Võrgusätted**.
3. Lugege teadet ja seejärel puudutage valikut **Jah**.
4. Kui kuvatakse lõpetamise teade, puudutage valikut **Sule**.

   Pärast teatud ajavahemikku sulgub ekraan automaatselt, kui te ei puuduta valikut **Sule**.

Side kontrollimine seadmete ja arvutite vahel

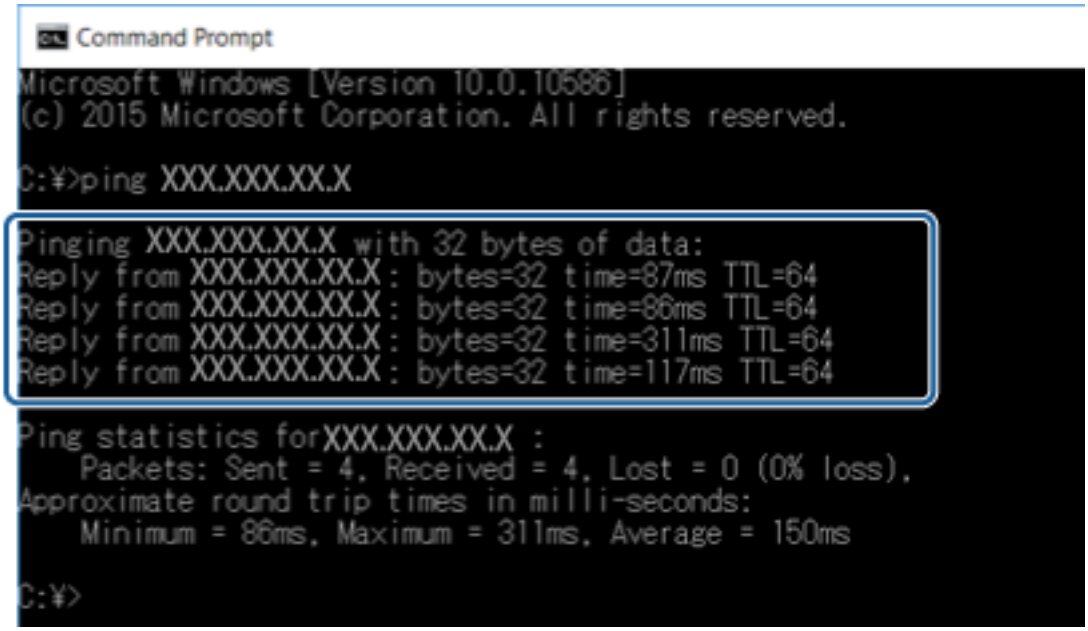
Ühenduse kontrollimine pingimiskäsu abil — Windows

Saate kasutada pingimiskäsku, et teha kindlaks, kas arvuti on skanneriga ühendatud. Järgige alltoodud samme, et kontrollida ühendust pingimiskäsuga.

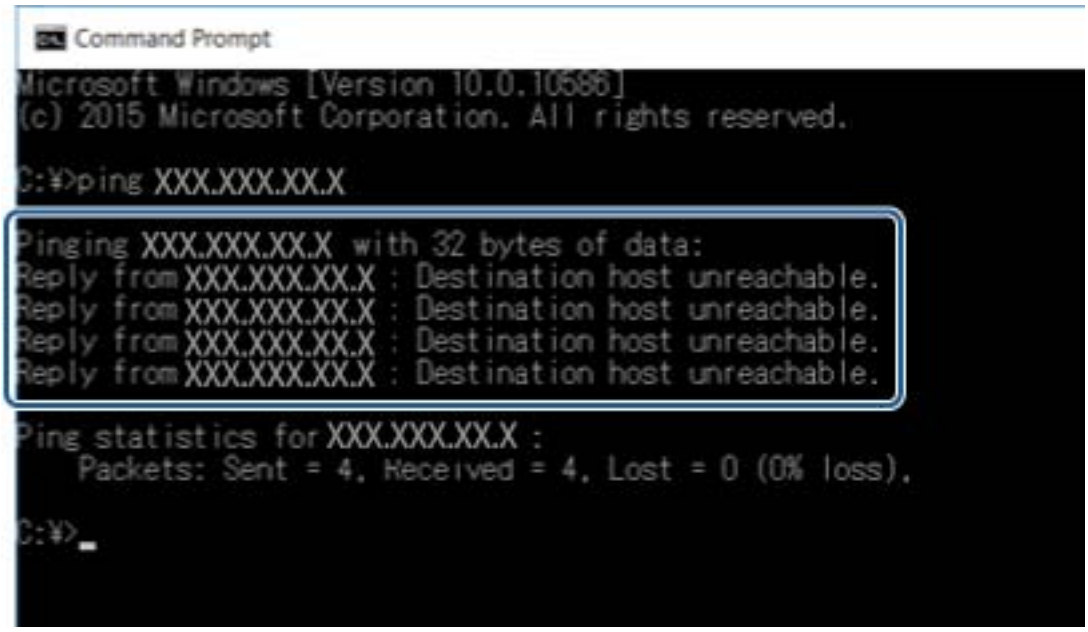
1. Vaadake järele kontrollitava ühenduse skanneri IP-aadress.

   Saate seda kontrollida rakendusega Epson Scan 2.

2. Kuvage arvuti käsuviiba aken.
   - ❏ Windows 10
     Paremklõpsake või vajutage ja hoidke all nuppu Start ning valige seejärel **Käsuviip**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Kuvage rakenduse aken ja valige seejärel **Käsuviip**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 või varasem
     Klõpsake nuppu Start, valige **Kõik programmid** või **Programmid** > **Tarvikud** > **Käsuviip**.
3. Sisestage „ping xxx.xxx.xxx.xxx“ ja vajutage seejärel sisestusklahvi.
   xxx.xxx.xxx.xxx asemel sisestage skanneri IP-aadress.
4. Kontrollige sideühendust.
   Kui skanner ja arvuti suhtlevad, kuvatakse alljärgnev teade.



Kui skanner ja arvuti ei suhtle, kuvatakse alljärgnev teade.



Ühenduse kontrollimine pingimiskäsu abil — Mac OS

Saate kasutada pingimiskäsku, et teha kindlaks, kas arvuti on skanneriga ühendatud. Järgige alltoodud samme, et kontrollida ühendust pingimiskäsuga.

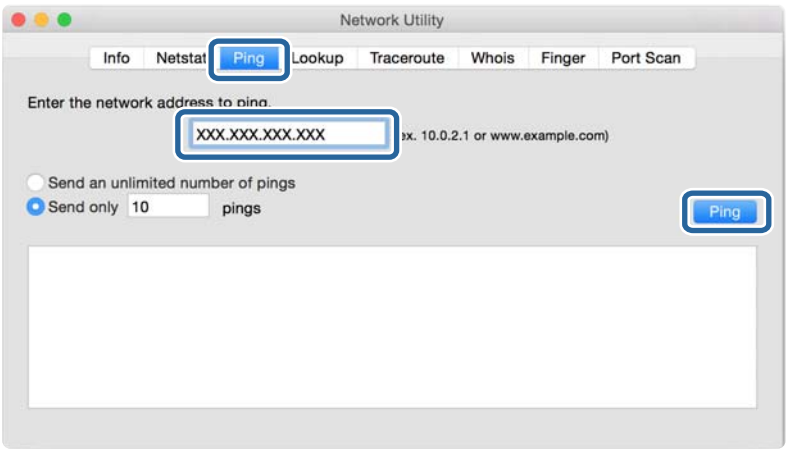
1. Vaadake järele kontrollitava ühenduse skanneri IP-aadress.

   Saate seda kontrollida rakendusega Epson Scan 2.

2. Käivitage võrguutiliit.

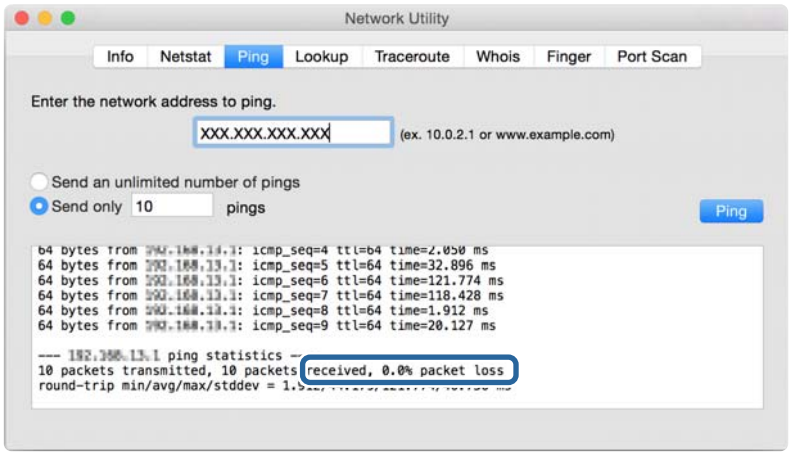
   Sisestage valikust **Spotlight** „Võrguutiliit“.

3. Klõpsake vahekaarti **Ping**, sisestage IP-aadress, mida kontrollisite sammus 1, seejärel klõpsake **Ping**.

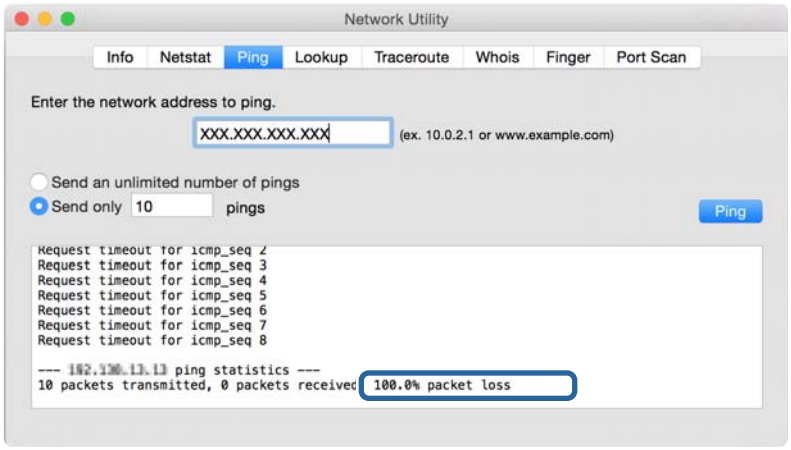


4. Kontrollige sideühendust.

   Kui skanner ja arvuti suhtlevad, kuvatakse alljärgnev teade.



   Kui skanner ja arvuti ei suhtle, kuvatakse alljärgnev teade.



Probleemid võrgu tarkvara kasutamisel

Puudub juurdepääs rakendusele Web Config

Kas skanneri IP-aadress on õigesti konfigureeritud?

Konfigureerige IP-aadress rakendusega Epson Device Admin või EpsonNet Config.

Kas teie brauser toetab hulgikrüptimist suvandiga Encryption Strength protokollile SSL/TLS?

Hulgikrüptimine suvandiga Encryption Strength protokollile SSL/TLS toimib alljärgnevalt. Web Config on avatav vaid brauseriga, mis toetab alljärgnevaid hulgikrüptimisstandardeid. Kontrollige brauseri krüptimistuge.

- ❏ 80 bitti: AES256/AES128/3DES
- ❏ 112 bitti: AES256/AES128/3DES
- ❏ 128 bitti: AES256/AES128

❏ 192 bitti: AES256

❏ 256 bitti: AES256

Teade „Aegunud“ kuvatakse rakendusele Web Config juurdepääsuks SSL-andmeside (https) kasutamisel.

Kui sertifikaat on aegunud, hankige sertifikaat uuesti. Kui teade kuvatakse enne sertifikaadi aegumiskuupäeva, kontrollige, kas skanneri kuupäev on õigesti konfigureeritud.

Teade „Turvasertifikaadi nimi ei ühti…“ kuvatakse rakendusele Web Config juurdepääsuks SSL-andmeside (https) kasutamisel.

Iseallkirjastatud sertifikaadi või sertifikaadi allkirjastamistaotluse loomisel väljale **Common Name** sisestatud skanneri IP-aadress ei ühti brauserisse sisestatud aadressiga. Hankige ja importige sertifikaat uuesti või muutke skanneri nime.

Skannerile juurdepääsuks kasutatakse puhverserverit.

Kui kasutate koos skanneriga puhverserverit, peate konfigureerima brauseri puhvrisätted.

❏ Windows:

Valige **Juhtpaneel** > **Võrk ja Internet** > **Interneti-suvandid** > **Ühendused** > **Kohtvõrgu sätted** > **Puhverserver**, ning valige seejärel selline konfiguratsioon, mis ei kasuta kohalike aadresside jaoks puhverserverit.

❏ Mac OS:

Valige **System Preferences** > **Network** > **Advanced** > **Proxies** ning registreerige seejärel kohalikud aadressid suvandisse **Bypass proxy settings for these Hosts & Domains**.

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

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „IP-aadressi määramine” lk 15

➡ „IP-aadressi määramine rakendusega EpsonNet Config” lk 56

Mudeli nimi ja/või IP-aadress ei ole tarkvararakenduses EpsonNet Config kuvatud

Kas valisite Blokeeri, Loobu või Lülita välja, kui kuvati Windows-i turvaekraan või tulemüüri ekraan?

Kui valite **Blokeeri**, **Loobu** või **Lülita välja**, ei kuvata IP-aadressi ja mudeli nime tarkvararakendustes EpsonNet Config ja EpsonNet Setup.

Registreerige selle korrigeerimiseks tarkvararakendus EpsonNet Config erandina, kasutades operatsioonisüsteemi Windows tulemüüri ja kaubanduses saadavalolevat turbetarkvara. Kui kasutate viirustõrjeprogrammi või turberakendust, sulgege see ning proovige seejärel kasutada tarkvara EpsonNet Config.

Kas sideühenduse vea ajalõpu säte on liiga lühike?

Käivitage EpsonNet Config ja valige **Tools** > **Options** > **Timeout** ning suurendage seejärel suvandi **Communication Error** sätte ajalist kestust. Pöörake tähelepanu sellele, et ajalõpu sätte pikendamisel võib EpsonNet Config aeglasemalt töötada.

Seotud teave

➡ „Rakenduse EpsonNet Config kasutamine — Windows” lk 56

➡ „Rakenduse EpsonNet Config kasutamine — Mac OS” lk 56

Lisa

Võrgutarkvara tutvustus

Alljärgnev kirjeldab tarkvara, mis konfigureerib ja haldab seadmeid.

Epson Device Admin

Epson Device Admin on rakendus, mis lubab installida seadmeid võrgus ja seejärel seadmeid konfigureerida ja hallata. Saate hankida seadmete üksikasjalikku teavet, nagu olek ja tarvikud, saata teatisi hoiatuste kohta ja luua aruandeid seadme kasutuse kohta. Lisaks saate luua malli, mis sisaldab sätteüksusi, ja rakendada seda muudele seadmetele ühiskasutatavate sätetena. Saate rakenduse Epson Device Admin alla laadida ettevõtte Epson kasutajatoe veebisaidilt. Lisateabe saamiseks vaadake rakenduse Epson Device Admin dokumentatsiooni või spikrit.

Rakenduse Epson Device Admin käivitamine (ainult Windows)

Valige **Kõik programmid** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Märkus.
Kui kuvatakse tulemüüri hoiatus, lubage juurdepääs rakendusele Epson Device Admin.

EpsonNet Config

EpsonNet Config võimaldab administraatoril konfigureerida skanneri võrgusätteid, näiteks määrata IP-aadressi ja muuta ühendusrežiimi. Pakettseadistuse funktsiooni toetab Windows. Lisateabe saamiseks vaadake rakenduse EpsonNet Config dokumentatsiooni või spikrit.

Rakenduse EpsonNet Config kasutamine — Windows

Valige **Kõik programmid** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Märkus.
Kui kuvatakse tulemüüri hoiatus, lubage juurdepääs rakendusele EpsonNet Config.

Rakenduse EpsonNet Config kasutamine — Mac OS

Valige **Mine** > **Rakendused** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager on tarkvararakendus, mis võimaldab luua paketi skanneri hõlpsaks installimiseks, näiteks skanneri draiveri installimiseks ja konfigureerimiseks ning rakenduse Document Capture Pro installimiseks. See tarkvara lubab administraatoril luua unikaalseid tarkvarapakette ja neid gruppidele jagada.

Külastage lisateabe saamiseks ettevõtte Epson piirkondlikku veebisaiti.

IP-aadressi määramine rakendusega EpsonNet Config

Saate määrata skannerile IP-aadressi rakendusega EpsonNet Config. EpsonNet Config võimaldab pärast Ethernet-kaabliga ühendamist määrata skannerile IP-aadressi, kui sellele ei ole veel IP-aadressi määratud.

IP-aadressi määramine pakettsätetega

Pakettsätete faili loomine

Kui kasutate võtmetena MAC-aadressi ja mudeli nime, saate luua IP-aadressi määramiseks uue SYLK-faili.

1. Avage arvutustabeli rakendus (näiteks Microsoft Excel) või tekstiredaktor.

2. Sisestage esimesele reale sätteüksuste nimedeks „Info_MACAddress“, „Info_ModelName“ ja „TCPIP_IPAddress“.

   Sisestage alljärgnevate tekstistringide sätteüksused. Suurtähtede/väiketähtede ja kahebaidiste/ühebaidiste märkide eristamiseks ei tuvastata üksust, kui erinev on ainult üks tärk.

   Sisestage allpool kirjeldatud viisil sätteüksuse nimi, muidu ei tunne EpsonNet Config sätteüksusi ära.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Sisestage iga võrguliidese jaoks MAC-aadress, mudeli nimi ja IP-aadress.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102

0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Sisestage nimi ja salvestage kui SYLK-fail (*.slk).

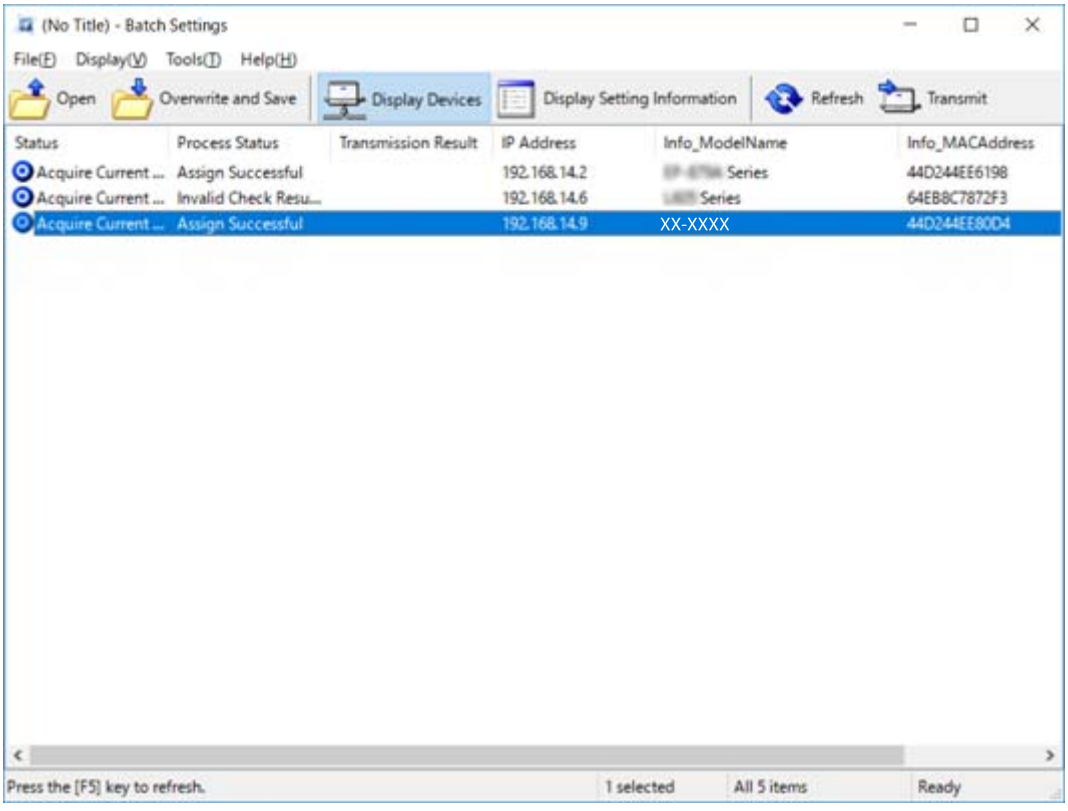
Pakettsätete kasutamine konfiguratsioonifaili abil

Määrake konfiguratsioonifailis (SYLK-fail) ükshaaval IP-aadressid. Enne määramist peate looma konfiguratsioonifaili.

1. Ühendage kõik seadmed Etherneti-kaablite abil võrku.
2. Lülitage skanner sisse.
3. Käivitage EpsonNet Config.

   Kuvatakse loend võrgus olevatest skanneritest. Nende kuvamiseks võib kuluda pisut aega.
4. Klõpsake valikut **Tools** > **Batch Settings**.
5. Klõpsake nuppu **Open**.
6. Valige faili valimise ekraanil sätteid sisaldav SYLK-fail (*.slk) ja seejärel klõpsake valikut **Open**.
7. Valige seadmed, millele soovite määrata pakettsätteid, veeru **Status** sättega **Unassigned** ja veeru **Process Status** sättega **Assign Successful**.

   Kui teete mitu valikut, vajutage juhtklahvi (Ctrl) või tõstuklahvi (Shift) ja klõpsake või lohistage hiirega.



8. Klõpsake nuppu **Transmit**.

9. Kui kuvatakse parooli sisestamise ekraan, sisestage parool ja klõpsake valikut **OK**.

   Edastage sätted.

   Märkus.
   Teavet saadetakse võrguliidesesse seni, kuni edenemisnäidik jõuab lõppu. Ärge lülitage seadet ega raadiovõrguadapterit välja ja ärge saatke seadmesse mingeid andmeid.

10. Klõpsake ekraanil **Transmitting Settings** valikut **OK**.

11. Kontrollige häälestatud seadme olekut.

    Seadmete korral, millel on kuvatud  või  , kontrollige sättefaili sisu ja seda, kas seade on normaalselt taaskäivitunud.

Ikoon	Status	Process Status	Selgitus
	Setup Complete	Setup Successful	Häälestus normaalselt lõpuni viidud.
	Setup Complete	Rebooting	Kui teave on saadetud, tuleb iga seade sätete aktiveerimiseks taaskäivitada. Pärast taaskäivitamist kontrollitakse, kas seadmega saab luua ühenduse.
	Setup Complete	Reboot Failed	Pärast sätete saatmist ei õnnestu saada kinnitust. Kontrollige, kas seade on sisse lülitatud ja normaalselt taaskäivitatud.
	Setup Complete	Searching	Sättefailis viidatud seadme otsimine.*
	Setup Complete	Search Failed	Kontrollida ei saa seadmeid, mis on juba häälestatud. Kontrollige, kas seade on sisse lülitatud ja normaalselt taaskäivitatud.*

* Ainult siis, kui kuvatud on sätteteave.

Seotud teave

➡ „Rakenduse EpsonNet Config kasutamine — Windows” lk 56
➡ „Rakenduse EpsonNet Config kasutamine — Mac OS” lk 56

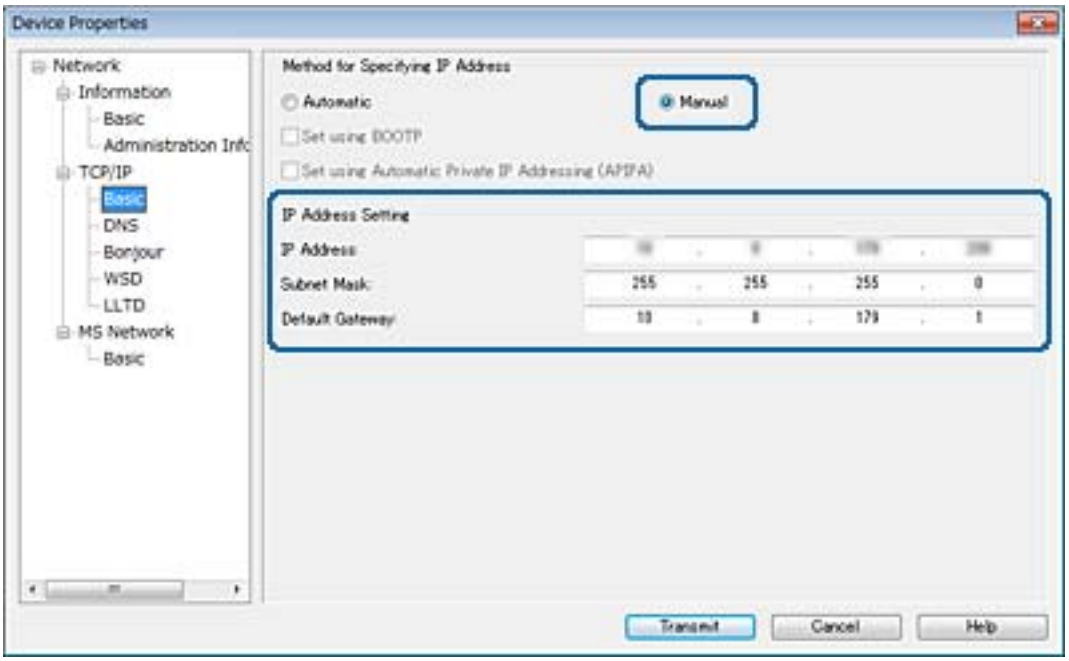
IP-aadressi määramine igale seadmele

Määrake skannerile IP-aadress rakendusega EpsonNet Config.

1. Lülitage skanner sisse.
2. Ühendage skanner Etherneti-kaabli abil võrku.
3. Käivitage EpsonNet Config.

   Kuvatakse loend võrgus olevatest skanneritest. Nende kuvamiseks võib kuluda pisut aega.
4. Topeltklõpsake skanneri nime, millele soovite määrata IP-aadressi.

   Märkus.
   Kui olete ühendanud mitu sama mudeli skannerit, saate neid eristada MAC-aadressi abil.
5. Valige **Network** > **TCP/IP** > **Basic**.
6. Sisestage aadressid väljadele **IP Address**, **Subnet Mask** ja **Default Gateway**.



   Märkus.
   Sisestage staatiline aadress, kui ühendate skanneri turvalisse võrku.
7. Klõpsake nuppu **Transmit**.

   Kuvatakse teabe ülekannet kinnitav ekraan.
8. Klõpsake nuppu **OK**.

   Kuvatakse ülekande lõpuleviimise ekraan.

   Märkus.
   Teave edastatakse seadmesse ja seejärel kuvatakse teade konfiguratsiooni eduka lõpuleviimise kohta. Ärge lülitage seadet välja ja ärge saatke seadmesse mingeid andmeid.
9. Klõpsake nuppu **OK**.

Seotud teave

➡ „Rakenduse EpsonNet Config kasutamine — Windows” lk 56

➡ „Rakenduse EpsonNet Config kasutamine — Mac OS” lk 56

Skanneri jaoks pordi kasutamine

Skanner kasutab alljärgnevat porti. Need pordid peavad vastavalt vajadusele olema lubatud võrguadministraatorile kasutamiseks.

Saatja (klient)	Kasutamine	Sihtkoht (server)	Protokoll	Pordinumber
Skanner	Meili saatmine (meiliteatis)	SMTP-server	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP enne SMTP-ühendust (meiliteatis)	POP-server	POP3 (TCP)	110
	WSD juhtimine	Klientarvuti	WSD (TCP)	5357
	Arvuti otsimine tõukeskannimisel rakenduses Document Capture Pro	Klientarvuti	Network Push Scan Discovery	2968
	Töö teabe kogumine tõukeskannimisel rakenduses Document Capture Pro	Klientarvuti	Network Push Scan	2968
Klientarvuti	Skanneri tuvastamine rakenduses nagu EpsonNet Config ja skanneridraiveris.	Skanner	ENPC (UDP)	3289
	MIB teabe kogumine ja häälestamine rakenduses nagu EpsonNet Config ja skanneridraiveris.	Skanner	SNMP (UDP)	161
	WSD-skanneri otsimine	Skanner	WS-Discovery (UDP)	3702
	Skannitud andmete edastamine rakenduses Document Capture Pro	Skanner	Network Scan (TCP)	1865

Täpsemad turvasätted ettevõttele

Selles peatükis kirjeldame täpsemaid turvafunktsioone.

Turvasätted ja ohu ennetamine

Kui seade on ühendatud võrku, omate sellele juurdepääsu kaugasukohast. Lisaks saavad inimesed anda seadme ühiskasutusse, mis muudab töö tegemise tõhusamaks ja mugavamaks. Samas aga kasvab ebaseadusliku juurdepääsu, ebaseadusliku kasutuse ja andmete muutmise oht. Kui kasutate seadet keskkonnas, kus teil on juurdepääs Internetti, on risk veelgi suurem.

Selle ohu vältimiseks on Epsoni seadmetel erinevad turvatehnoloogiad.

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

Nimi	Funktsiooni tüüp	Sätted	Mida ennetatakse
SSL/TLS-side	Arvuti ja seadme sidetee krüptitakse, kasutades SSL/TLS-sidet. Brauseri vahendusel peetava side sisu on kaitstud.	Määrake seadmele serveri jaoks sertimiskeskuse allkirjastatud CA-sertifikaat.	Ennetage sätteteabe ja arvutist skannerisse edastatavate andmete lekkimist. Juurdepääsu seadmest Epsoni serverile Internetis saab kaitsta ka püsivara värskendusega jne.
IPsec/IP-filtreerimine	Saate lubada kindlalt kliendilt pärinevate või teatavat tüüpi andmete äralõikamist. Kuna IPsec kaitseb andmeid IP-pakettüksustena (krüptimine ja autentimine), saate ohutult kasutada andmesideks turvamata skannimisprotokolli.	Looge üldpoliitika ja individuaalne poliitika, et määrata seadmele juurdepääsu omav klient või andmete tüüp.	Kaitske seadmesse liikuvaid sideandmeid volitamata juurdepääsu, muutmise ja ümbersuunamise eest.
SNMPv3	Lisatud on funktsioonid, nagu võrku ühendatud seadmete jälgimine, SNMP-protokolli läbivate andmete tervikluse kontrollimine, krüptimine, kasutaja autentimine jne.	Aktiveerige SNMPv3 ja seejärel määrake autentimis- ja krüptimismeetod.	Tagab sätete muutmise võrgu kaudu, konfidentsiaalsuse oleku jälgimisel.
IEEE802.1X	Lubab Ethernetiga ühenduse luua ainult autenditud kasutajatel. Võimaldab seadet kasutada ainult selleks luba omaval kasutajal.	RADIUS-serveri (autentimisserver) autentimissäte.	Kaitseb seadet volitamata juurdepääsu ja kasutamise eest.
Lugemise ID-kaart	Saate seadet kasutada, hoides ühendatud autentimisseadme kohal ID-kaarti. Saate iga kasutaja ja seadme jaoks piirata logide hankimist ning piirata seadmete ja funktsioonide kasutatavust igale kasutajale ja rühmale.	Ühendage autentimisseade seadme külge ja määrake autentimissüsteemis kasutaja teave.	Takistage seadme volitamata kasutamist ja tüssamist.

Seotud teave

➡ „SSL/TLS-side skanneriga” lk 62
➡ „Krüptitud side IPsec/IP-filtreerimisega” lk 70
➡ „SNMPv3 protokolli kasutamine” lk 81
➡ „Skanneri ühendamine IEEE802.1X-võrguga” lk 83

Turvafunktsioonide sätted

IPsec/IP-filtreerimise või IEEE802.1X-i kasutamise korral on soovitatav avada rakendus Web Config sätteteabe edastamiseks SSL/TLS-iga, et vähendada turvariske, nagu muutmine ja ümbersuunamine.

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.

Teave digitaalsertimise kohta

❏ Sertimiskeskuse allkirjastatud sertifikaat

Sertimiskeskuselt (CA — Certificate Authority) tuleb hankida sertimiskeskuse allkirjastatud sertifikaat. Te saate sertimiskeskuse allkirjastatud sertifikaadi kasutamisega tagada sideühenduse turvalisuse. Te saate sertimiskeskuse allkirjastatud sertifikaati kasutada kõigi turvafunktsioonide jaoks.

❏ Sertimiskeskuse sertifikaat

Sertimiskeskuse sertifikaat viitab sellele, et serveri identiteeti on kontrollinud kolmas osapool. See on usaldusevõrgu (WOT — Web of Trust) tüüpi turbe põhikomponent. Te peate serveri autentimiseks hankima sertimiskeskuse sertifikaadi vastavat sertifikaati väljastavalt sertimiskeskuselt.

❏ Iseallkirjastatud sertifikaat

Iseallkirjastatud sertifikaat on sertifikaat, mille skanner ise väljastab ja allkirjastab. See sertifikaat ei ole usaldusväärne ning ei saa takistada protokollipetet ja võltsimist (spuufimist). Kui kasutate SSL-/TLS-sertifikaadiks seda sertifikaati, võib brauser kuvada turvahoiatuse. Te saate seda sertifikaati kasutada üksnes SSL-/TLS-andmesideks.

Seotud teave

➡ „Sertimiskeskuse allkirjastatud sertifikaadi hankimine ja importimine” lk 63
➡ „Sertimiskeskuse allkirjastatud sertifikaadi kustutamine” lk 66
➡ „Iseallkirjastatud sertifikaadi värskendamine” lk 67

Sertimiskeskuse allkirjastatud sertifikaadi hankimine ja importimine

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 valige seejärel **Network Security Settings**. Seejärel valige **SSL/TLS** > **Certificate** või **IPsec/IP Filtering** > **Client Certificate** või **IEEE802.1X** > **Client Certificate**.

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

   Avaneb sertifikaadi allkirjastamistaotluse loomisleht.

3. Sisestage kõigile kirjetele 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 suvand **Network Security Settings**. 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.

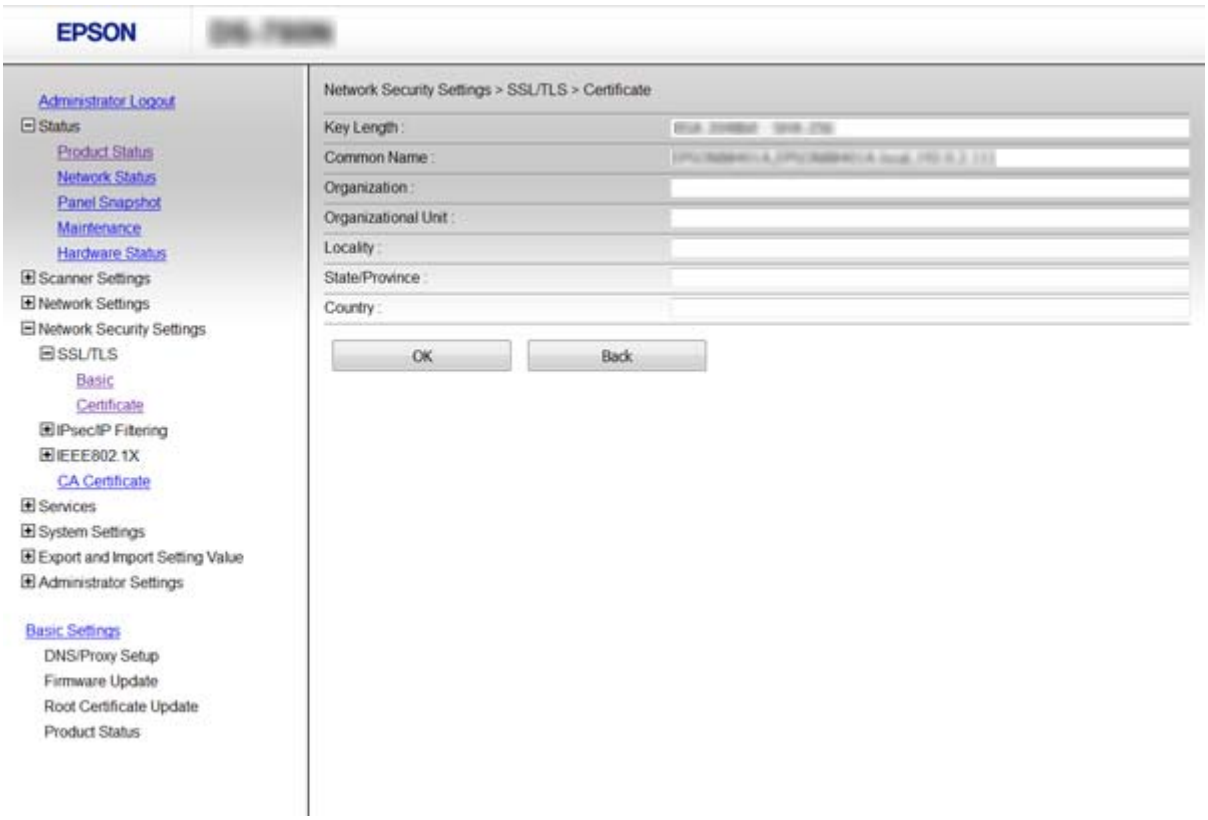
Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Sertifikaadi allkirjastamistaotluse seadistuselemendid” lk 64

➡ „Sertimiskeskuse allkirjastatud sertifikaadi importimine” lk 65

Sertifikaadi allkirjastamistaotluse seadistuselemendid



Üksused	Sätted ja selgitus
Key Length	Valige sertifikaadi allkirjastamistaotluse võtme pikkus.
Common Name	Saate sisestada 1–128 tähemärki. Kui kasutate IP-aadressi, peab selleks olema staatiline IP-aadress. Näide: URL rakendusse Web Config juurdepääsuks: https://10.152.12.225 Ühisnimi: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Saate sisestada 0–64 tärki ASCII-vormingus (0x20–0x7E). Te saate eraldusnimesid eraldada komadega.
Country	Sisestage standardis ISO-3166 määratud kahekohaline riigi kood.

Seotud teave

➡ „Sertimiskeskuse allkirjastatud sertifikaadi hankimine” lk 63

Sertimiskeskuse allkirjastatud sertifikaadi importimine

Oluline teave:

- ❏ *Veenduge, et skanneri kuupäev ja kellaaeg oleks õigesti seadistatud.*
- ❏ *Kui hangite sertifikaadi rakenduses Web Config loodud sertifikaadi allkirjastamistaotlust kasutades, saate korraga importida ühe sertifikaadi.*

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

2. Klõpsake nuppu **Import**.

   Avaneb sertifikaadi importimisleht.

3. Sisestage kõigile kirjetele väärtus.

   Nõutavad sätted võivad varieeruda olenevalt sertifikaadi allkirjastamistaotluse loomise kohast ning sertifikaadi failivormingust. Sisestage nõutavatele kirjetele väärtused, lähtudes alljärgnevast.

   - ❏ PEM/DER-vormingus sertifikaat, mis on hangitud rakendusest Web Config
     - ❏ **Private Key**: ärge konfigureerige, sest skanner sisaldab privaatvõtit.
     - ❏ **Password**: ärge konfigureerige.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: valikuline
   - ❏ PEM/DER-vormingus sertifikaat, mis on hangitud arvutist
     - ❏ **Private Key**: vajalik on seadistamine.
     - ❏ **Password**: ärge konfigureerige.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: valikuline
   - ❏ PKCS#12-vormingus sertifikaat, mis on hangitud arvutist
     - ❏ **Private Key**: ärge konfigureerige.
     - ❏ **Password**: valikuline
     - ❏ **CA Certificate 1**/**CA Certificate 2**: ärge konfigureerige.

4. Klõpsake nuppu **OK**.

   Kuvatakse lõpetamise teade.

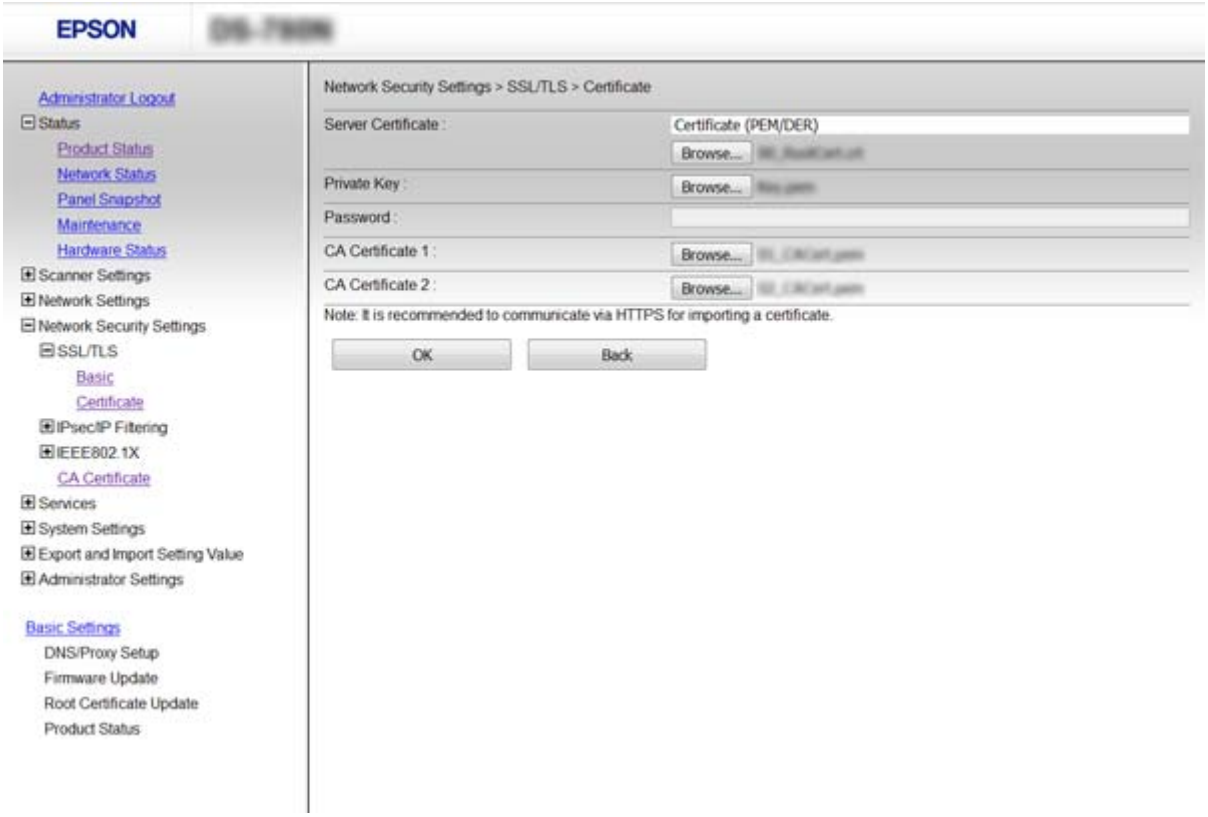
Märkus.
Klõpsake nuppu ***Confirm****, et kontrollida sertifikaadi teavet.*

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Sertimiskeskuse allkirjastatud sertifikaadi importimise seadistuselemendid” lk 66

Sertimiskeskuse allkirjastatud sertifikaadi importimise seadistuselemendid



Elemendid	Sätted ja selgitused
Server Certificate või Client Certificate	Valige sertifikaadi vorming.
Private Key	Kui hangite PEM/DER-vormingus sertifikaadi arvutist loodud sertifikaadi allkirjastamistaotluse abil, määrake privaatvõtme fail, mis vastab sertifikaadile.
Password	Sisestage privaatvõtme krüptimiseks parool.
CA Certificate 1	Kui teie sertifikaadi vorminguks on **Certificate (PEM/DER)**, importige serveri sertifikaati väljastava sertimiskeskuse sertifikaat. Määrake vajaduse korral fail kindlaks.
CA Certificate 2	Kui teie sertifikaadi vorminguks on **Certificate (PEM/DER)**, importige sertifikaati **CA Certificate 1** väljastava sertimiskeskuse sertifikaat. Määrake vajaduse korral fail kindlaks.

Seotud teave

➡ „Sertimiskeskuse allkirjastatud sertifikaadi importimine” lk 65

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 Web Config, ja seejärel valige **Network Security Settings**. 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

➡ „Juurdepääs rakendusele Web Config” lk 23

Iseallkirjastatud sertifikaadi värskendamine

Kui skanner toetab HTTPS-serveri funktsiooni, saate iseallkirjastatud sertifikaati värskendada. Kui loote iseallkirjastatud sertifikaadi abil juurdepääsu rakendusele Web Config, kuvatakse hoiatusteade.

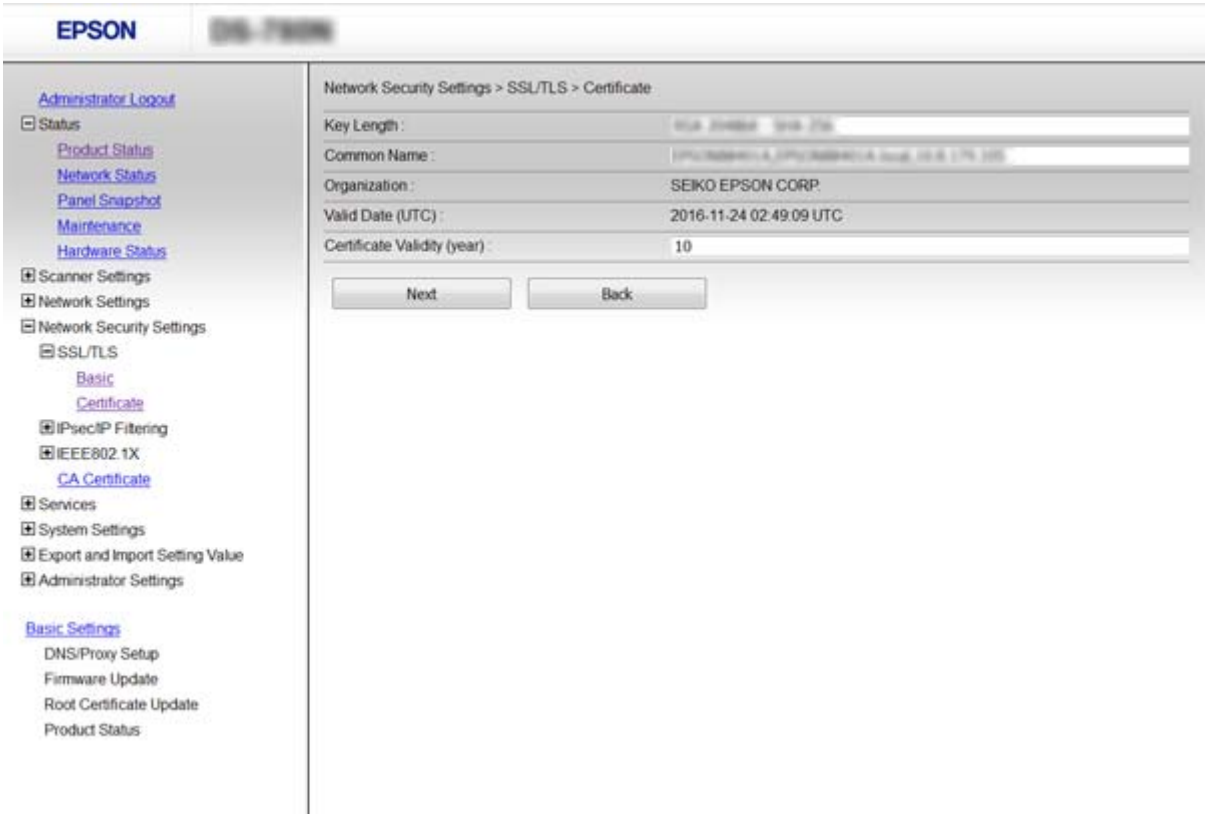
Kasutage iseallkirjastatud sertifikaati ajutiselt sertimiskeskuse allkirjastatud sertifikaadi hankimise ja importimiseni.

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

   Sisestage IP-aadress või identifikaator (näiteks skanneri täielik domeeninimi (FQDN)). Saate sisestada 1–128 tähemärki.

   Märkus.
   Te saate eraldusnime (CN) komadega eraldada.

4. Määrake sertifikaadi kehtivusperiood.



5. Klõpsake nuppu **Next**.

   Kuvatakse kinnitusteade.

6. Klõpsake nuppu **OK**.

   Skannerit värskendatakse.

Märkus.
*Klõpsake nuppu **Confirm**, et kontrollida sertifikaadi teavet.*

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Serdi CA Certificate seadistamine

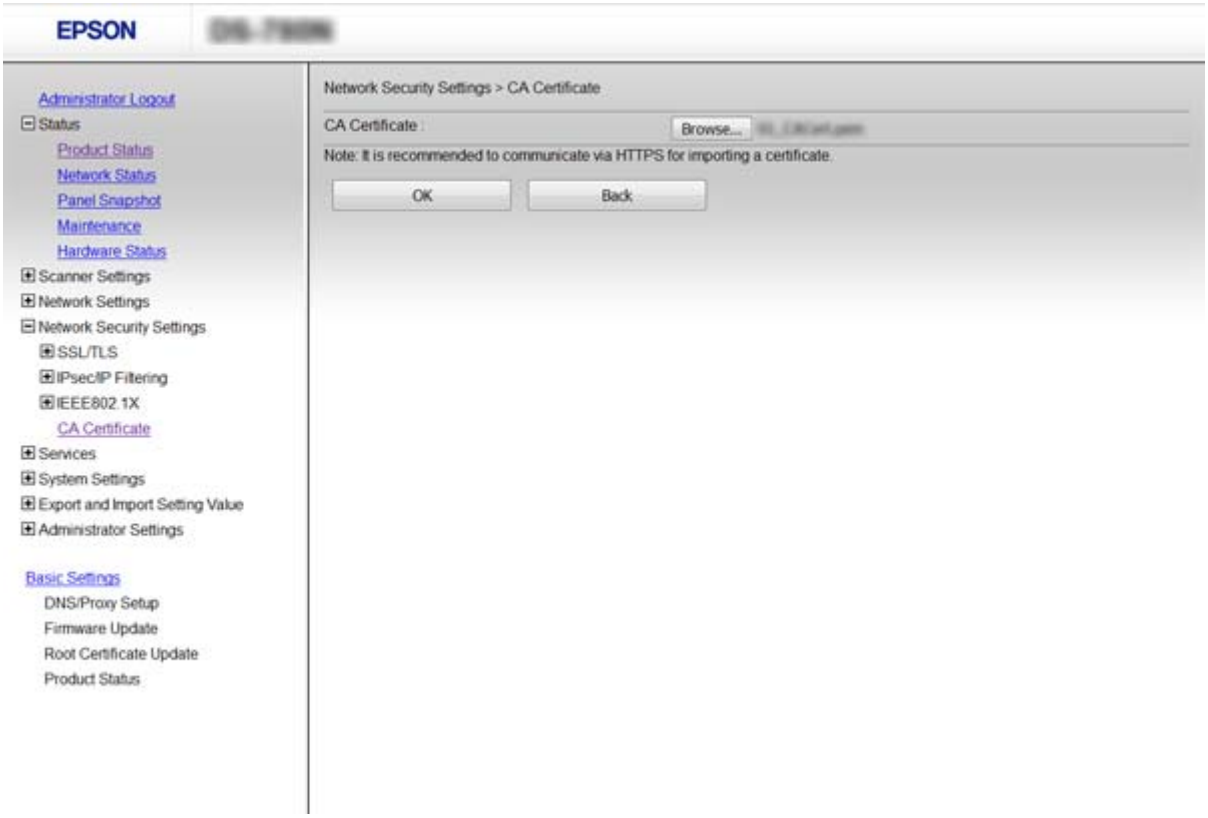
Serti CA Certificate saab importida, kuvada ja kustutada.

Serdi CA Certificate importimine

1. Avage Web Config ja valige seejärel **Network Security Settings** > **CA Certificate**.

2. Klõpsake nuppu **Import**.

3. Määrake CA Certificate, mida soovite importida.



4. Klõpsake nuppu **OK**.

Kui importimine on lõpule viidud, saate naasta serdi **CA Certificate** aknasse, kus näidatakse imporditud CA Certificate.

Seotud teave

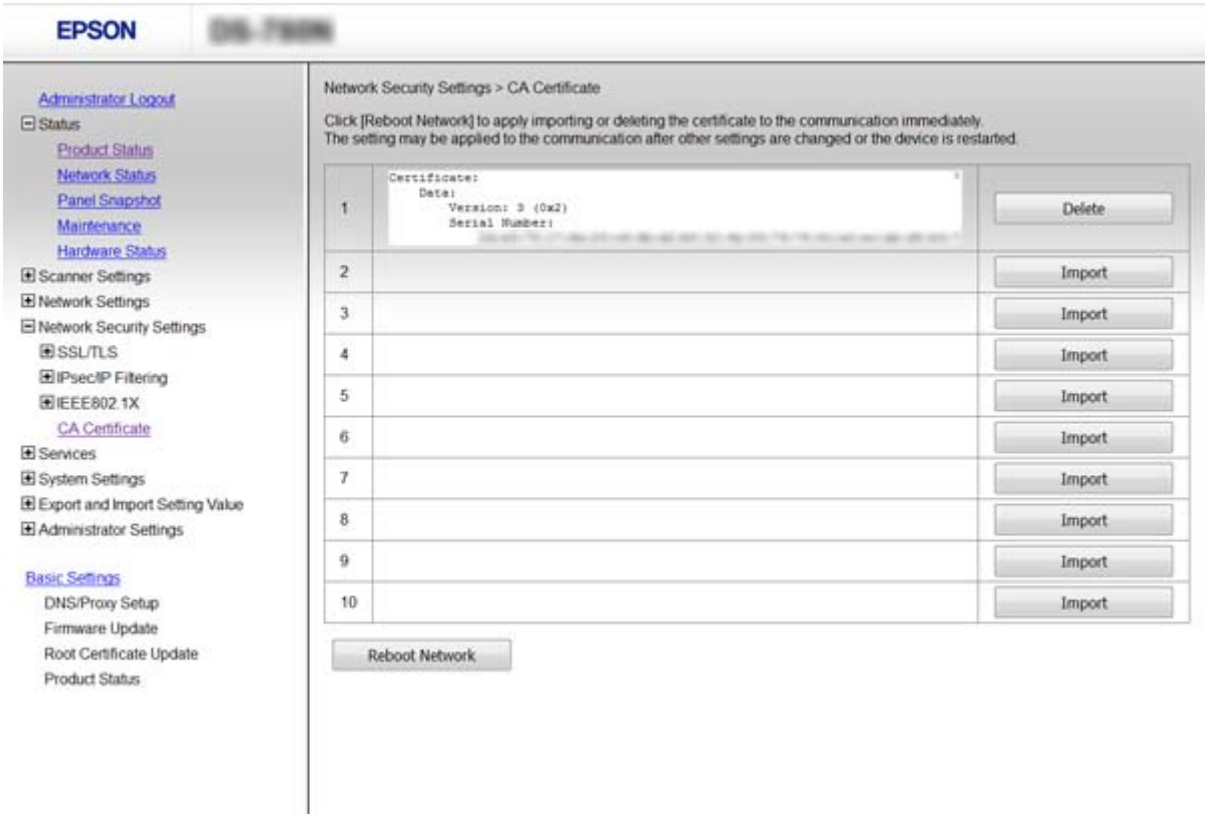
➡ „Juurdepääs rakendusele Web Config” lk 23

Serdi CA Certificate kustutamine

Imporditud serdi CA Certificate saate kustutada.

1. Avage Web Config ja valige seejärel **Network Security Settings** > **CA Certificate**.

2. Klõpsake nuppu **Delete**, mis on kustutatava serdi CA Certificate kõrval.



3. Kinnitage, et soovite kuvatava serdi kustutada.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Krüptitud side IPsec/IP-filtreerimisega

Teave rakenduse IPsec/IP Filtering kohta

Kui skanner toetab IPsec-/IP-filtreerimist, saate filtreerida liiklust IP-aadresside, teenuste ja pordi järgi. Te saate filtreerimise kombineerimisega konfigureerida skannerit lubama või blokeerima teatud kliente ja määratud andmeid. Lisaks saate IPsec-filtreerimise abil tõsta turvataset.

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

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

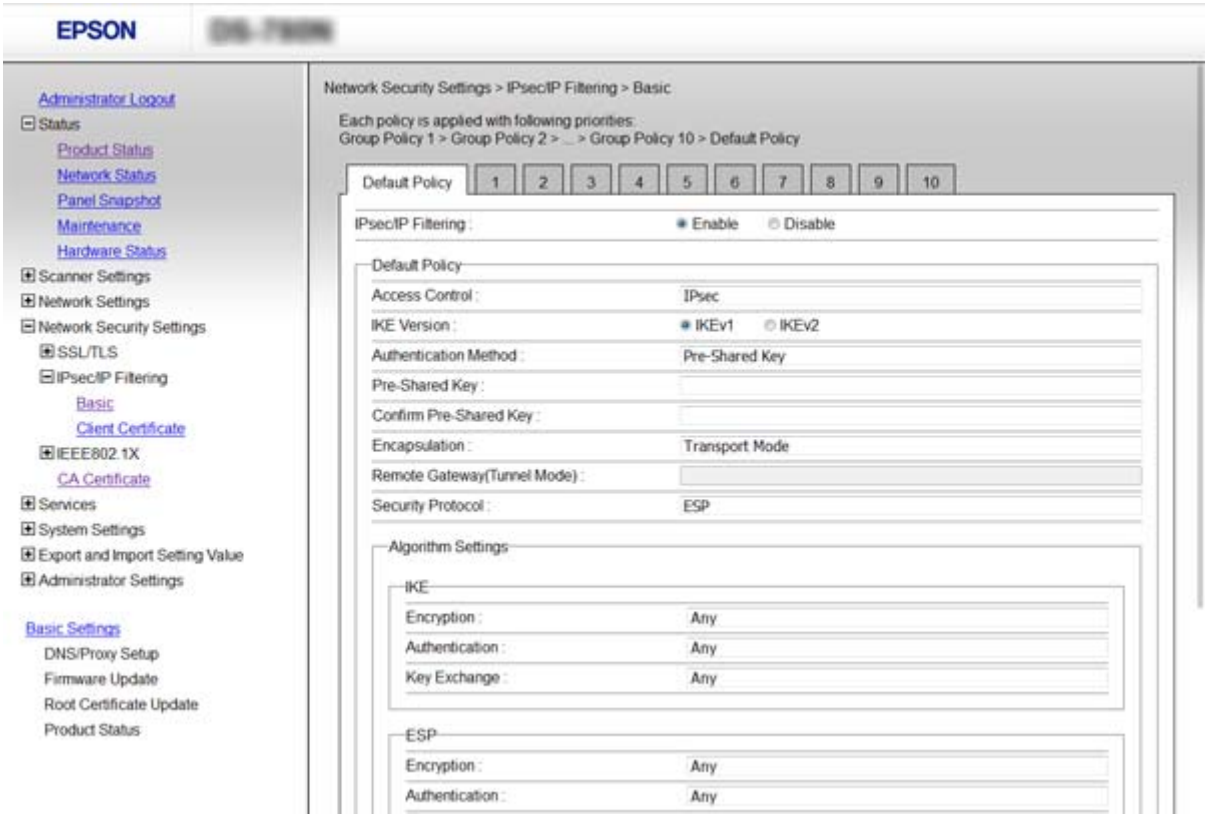
Suvandi Default Policy konfigureerimine

1. Avage Web Config ja valige **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Sisestage kõigile kirjetele väärtus.
3. Klõpsake nuppu **Next**.
   Kuvatakse kinnitusteade.
4. Klõpsake nuppu **OK**.
   Skannerit värskendatakse.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23
➡ „Suvandi Default Policy sättekirjed” lk 71

Suvandi Default Policy sättekirjed



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

Täpsemad turvasätted ettevõttele

Üksused	Sätted ja selgitus	
Access Control	Konfigureerige IP-pakettide liikluse reguleerimismeetod.	
	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 IKE versiooniks IKEv1 või IKEv2. Valige neist üks vastavalt seadmele, millega skanner on ühendatud.	
IKEv1	Kui **IKEv1** on valitud suvandi **IKE Version** sätteks, kuvatakse alljärgnevad üksused.	
	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.	
Local	Authentication Method	Suvandi **Certificate** valimiseks peate kõigepealt hankima ja importima sertimiskeskuse allkirjastatud sertifikaadi.
	ID Type	Valige skanneri ID tüüp.
	ID	Sisestage skanneri ID, mis vastab ID tüübile. Esimese tärgina ei saa kasutada tärke „@“, „#“ ja „=“. **Distinguished Name**: sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „=“. **IP Address**: sisestage vormingus IPv4 või IPv6. **FQDN**: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“, ja punkti (.). **Email Address**: sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „@“. **Key ID**: sisestage 1–128 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.

Täpsemad turvasätted ettevõttele

Üksused	Sätted ja selgitus	
Remote	Authentication Method	Suvandi **Certificate** valimiseks peate kõigepealt hankima ja importima sertimiskeskuse allkirjastatud sertifikaadi.
	ID Type	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 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „=“. **IP Address**: sisestage vormingus IPv4 või IPv6. **FQDN**: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“, ja punkti (.). **Email Address**: sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „@“. **Key ID**: sisestage 1–128 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.	
	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 tähemärgist.	
Security Protocol	**IPsec** suvandi **Access Control** jaoks, valige suvand.	
	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 IP-turvet (IPsec) kasutada ka siis, kui andmete krüptimine on keelatud.
Algorithm Settings		
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.

Üksused	Sätted ja selgitus	
ESP	Encryption	Valige ESP krüptimisalgoritm. See on saadaval, kui **ESP** on valitu suvandi **Security Protocol** sätteks.
	Authentication	Valige ESP autentimisalgoritm. See on saadaval, kui **ESP** on valitu suvandi **Security Protocol** sätteks.
AH	Authentication	Valige AH krüptimisalgoritm. See on saadaval, kui **AH** on valitu suvandi **Security Protocol** sätteks.

Seotud teave

➡ „Suvandi Default Policy konfigureerimine” lk 71

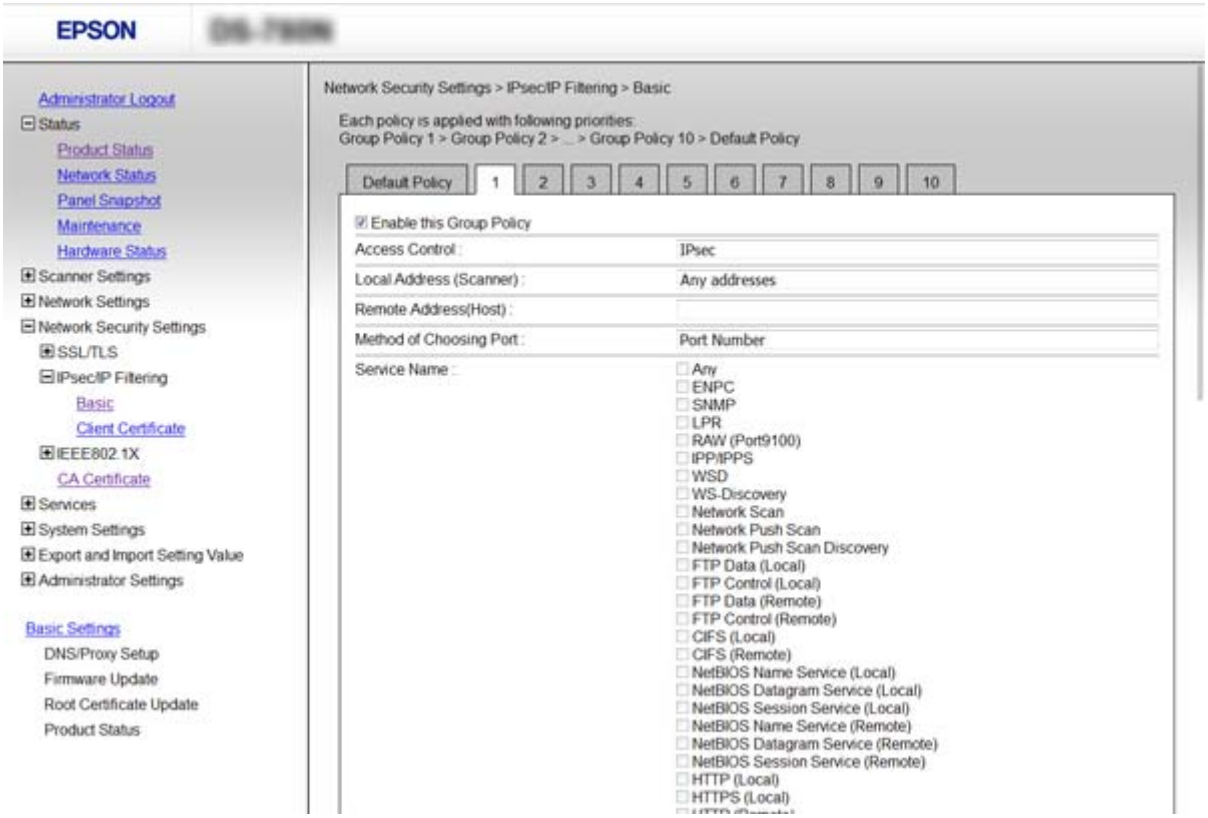
Suvandi Group Policy konfigureerimine

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

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23
➡ „Suvandi Group Policy sättekirjed” lk 75

Suvandi Group Policy sättekirjed



Üksused	Sätted ja selgitus	
Enable this Group Policy	Te saate rühmapoliitikat aktiveerida või blokeerida.	
Access Control	Konfigureerige IP-pakettide liikluse reguleerimismeetod.	
	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**.	
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** suvandile **Method of Choosing Port**, valige suvand.	

Täpsemad turvasätted ettevõttele

Üksused	Sätted ja selgitus	
Transport Protocol	Kui valite sätte **Port Number** suvandi **Method of Choosing Port** sätteks, peate konfigureerima kapseldusrežiimi.	
	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 IKE versiooniks IKEv1 või IKEv2. Valige neist üks vastavalt seadmele, millega skanner on ühendatud.	
IKEv1	Kui **IKEv1** on valitud suvandi **IKE Version** sätteks, kuvatakse alljärgnevad üksused.	
	Authentication Method	Kui valite sätte **IPsec** suvandile **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.	

Täpsemad turvasätted ettevõttele

Üksused	Sätted ja selgitus	
Local	Authentication Method	Kui valite sätte **IPsec** suvandile **Access Control**, valige suvand. Kasutatav sertifikaat ühtib vaikepoliitikaga.
	ID Type	Valige skanneri ID tüüp.
	ID	Sisestage skanneri ID, mis vastab ID tüübile. Esimese tärgina ei saa kasutada tärke „@“, „#“ ja „=“. **Distinguished Name**: sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „=“. **IP Address**: sisestage vormingus IPv4 või IPv6. **FQDN**: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“, ja punkti (.). **Email Address**: sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „@“. **Key ID**: sisestage 1–128 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** suvandile **Access Control**, valige suvand. Kasutatav sertifikaat ühtib vaikepoliitikaga.
	ID Type	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 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „=“. **IP Address**: sisestage vormingus IPv4 või IPv6. **FQDN**: sisestage kombinatsioon 1–255 tärgist, kasutades tärke A–Z, a–z, 0–9, „-“, ja punkti (.). **Email Address**: sisestage 1–128 1-baidist ASCII-vormingus (0x20–0x7E) tärki. Nende hulgas peab olema „@“. **Key ID**: sisestage 1–128 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.	
	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.

Täpsemad turvasätted ettevõttele

Üksused	Sätted ja selgitus	
Remote Gateway(Tunnel Mode)	Kui valite sätte **Tunnel Mode** suvandi **Encapsulation** sätteks, sisestage lüüsi aadress, mis koosneb 1–39 tähemärgist.	
Security Protocol	Kui valite sätte **IPsec** suvandile **Access Control**, valige suvand.	
	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 IP-turvet (IPsec) kasutada ka siis, kui andmete krüptimine on keelatud.
Algorithm Settings		
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 saadaval, kui **ESP** on valitu suvandi **Security Protocol** sätteks.
	Authentication	Valige ESP autentimisalgoritm. See on saadaval, kui **ESP** on valitu suvandi **Security Protocol** sätteks.
AH	Authentication	Valige AH autentimisalgoritm. See on saadaval, kui **AH** on valitu suvandi **Security Protocol** sätteks.

Seotud teave

➡ „Suvandi Group Policy konfigureerimine” lk 74

➡ „Suvandite Local Address (Scanner) ja Remote Address(Host) kombinatsioon funktsioonis Group Policy” lk 78

➡ „Teenuse nime viited rühmapolitikas” lk 79

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.

Teenuse nime viited rühmapolitikas

Märkus.
Mittekasutatavaid teenuseid kuvatakse, aga ei saa valida.

Teenuse nimi	Protokolli tüüp	Kohaliku pordi number	Kaugpordi number	Juhitavad funktsioonid
Any	–	–	–	Kõik teenused
ENPC	UDP	3289	Ükskõik milline port	Skanneri otsimine rakendustest, nagu EpsonNet Config ja skanneridraiver
SNMP	UDP	161	Ükskõik milline port	MIB hankimine ja konfigureerimine rakendustest, nagu EpsonNet Config ja ettevõtte Epson skanneridraiver
WSD	TCP	Ükskõik milline port	5357	WSD juhtimine
WS-Discovery	UDP	3702	Ükskõik milline port	Skanneri otsimine WSD-st
Network Scan	TCP	1865	Ükskõik milline port	Skannitud andmete edastamine tarkvarast Document Capture Pro
Network Push Scan Discovery	UDP	2968	Ükskõik milline port	Arvuti otsimine skannerist.
Network Push Scan	TCP	Ükskõik milline port	2968	Tõukeskannimistöö teabe hankimine tarkvarast Document Capture Pro või Document Capture
HTTP (Local)	TCP	80	Ükskõik milline port	HTTP(S)-server (faili Web Config ja WSD andmete edastamine)
HTTPS (Local)	TCP	443	Ükskõik milline port	
HTTP (Remote)	TCP	Ükskõik milline port	80	HTTP(S)-klient (püsivara värskendamine ja juurserdi värskendamine)
HTTPS (Remote)	TCP	Ükskõik milline port	443	

Funktsiooni IPsec/IP Filtering konfigureerimisnäited

Ainult IPsec-pakettide vastuvõtt

Toodud näide kirjeldab üksnes vaikepoliitika konfigureerimist.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: sisestage kuni 127 tähemärki.

Group Policy:

ärge konfigureerige.

Skannimise kinnitamine rakenduse Epson Scan 2 ja skanneri sätetega

See näide lubab edastada skannimisandmeid ja skanneri konfiguratsiooni kindlatest teenustest.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: märgistage kast linnukesega.

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

❏ **Remote Address(Host)**: kliendi IP-aadress

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

❏ **Service Name**: märgistage kastid **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** ja **HTTPS (Local)**.

Juurdepääsu lubamine üksnes määratud IP-aadressile

Toodud näites on juurdepääs skannerile lubatud vaid määratud IP-aadressile.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: märgistage kast linnukesega.

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

❏ **Remote Address(Host)**: administraatori kliendi IP-aadress

Märkus.
Kliendil on juurdepääs skannerile ja võimalus skannerit konfigureerida poliitika konfiguratsioonist sõltumatult.

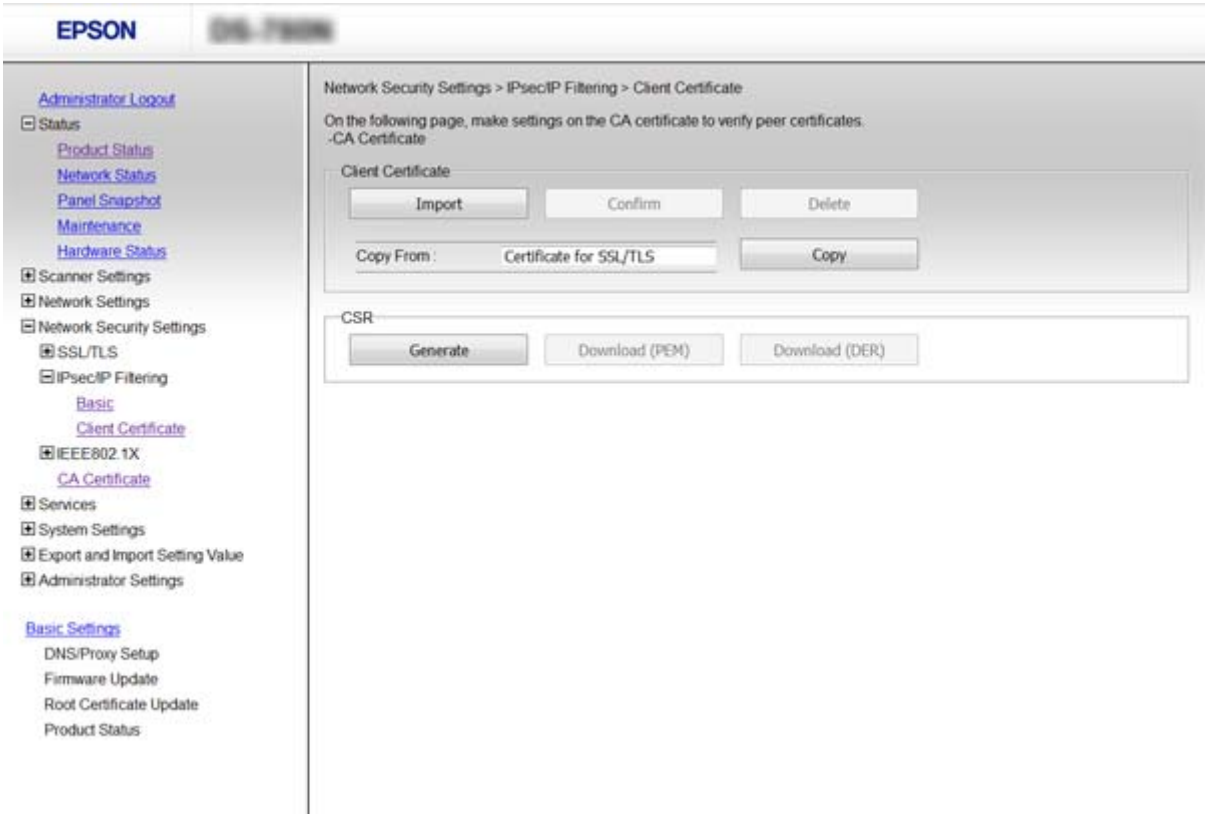
Standardile IPsec/IP Filtering vastava sertifikaadi häälestamine

Häälestage IPsec/IP filtreerimiseks kliendisertifikaat. Kui soovite seadistada sertimiskeskust, valige **CA Certificate**.

1. Avage Web Config ja valige **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importige sertifikaat üksusesse **Client Certificate**.

   Kui olete juba importinud standardile IEEE802.1X või SSL/TLS vastava sertifikaadi sertimiskeskusesse, saate serdi kopeerida ja kasutada seda IPsec/IP filtreerimiseks. Kopeerimiseks valige sert üksuses **Copy From** ja seejärel klõpsake nuppu **Copy**.



Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Sertimiskeskuse allkirjastatud sertifikaadi hankimine ja importimine” lk 63

SNMPv3 protokolli kasutamine

Teave SNMPv3 kohta

SNMP on protokoll, mis teostab jälgimist ja juhtimist teabe kogumiseks võrku ühendatud seadmete kohta. SNMPv3 on haldamise turvafunktsiooni parendatud versioon.

Kui kasutate protokolli SNMPv3, saab SNMP-side (pakett) oleku jälgimist ja sätete muutmist autentida ja krüptida, et kaitsta SNMP-sidet (pakett) võrguriskide eest (näiteks pealtkuulamine, teesklemine, muutmine).

SNMPv3 konfigureerimine

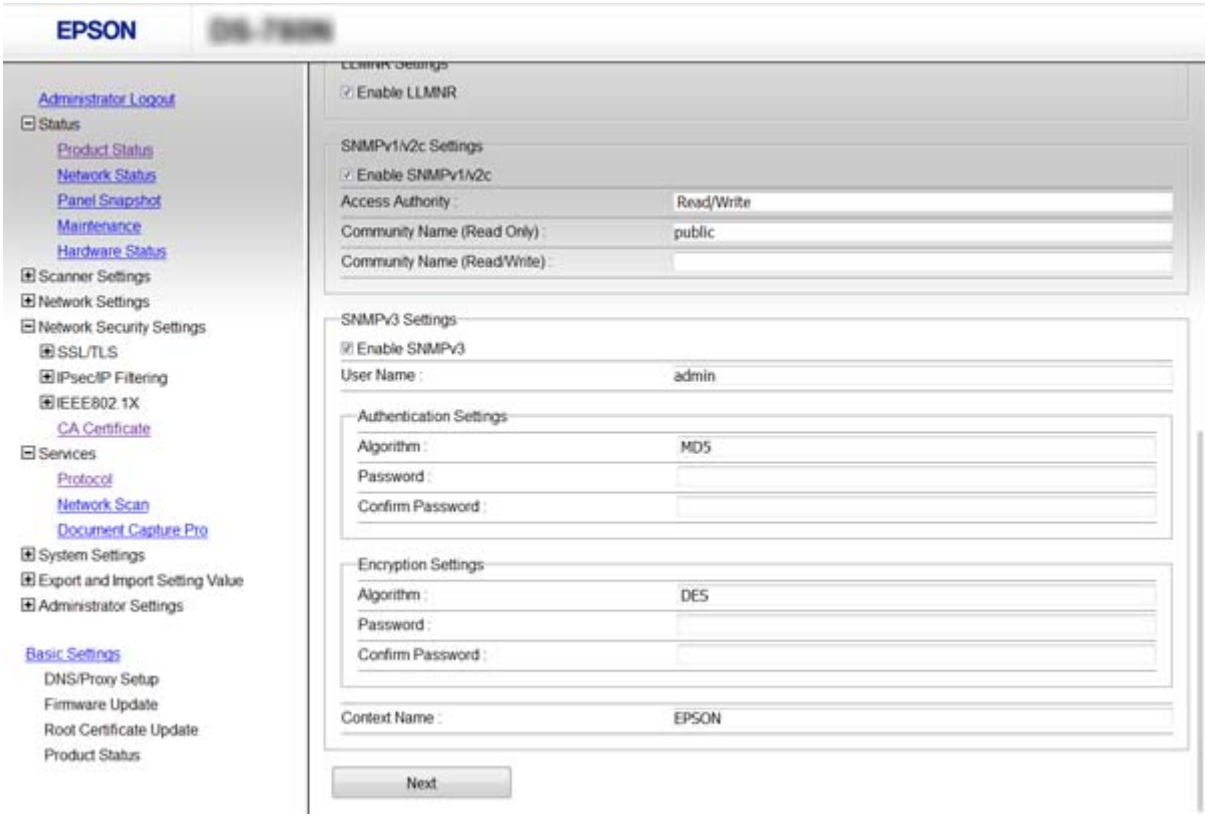
Kui skanner toetab protokolli SNMPv3, saate skannerit jälgida ja kontrollida juurdepääsu skannerile.

1. Avage Web Config ja valige **Services** > **Protocol**.
2. Sisestage suvandi **SNMPv3 Settings** kõigile kirjetele väärtus.
3. Klõpsake nuppu **Next**.
   Kuvatakse kinnitusteade.
4. Klõpsake nuppu **OK**.
   Skannerit värskendatakse.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23
➡ „SNMPv3 seadistuselemendid” lk 82

SNMPv3 seadistuselemendid



Elemendid	Sätted ja selgitused
Enable SNMPv3	SNMPv3 on aktiveeritud, kui märkeruut on märgistatud.
User Name	Sisestage 1 kuni 32 tähemärki, kasutades 1-baidi tähemärke.
Authentication Settings	
Algorithm	Valige autentimiseks algoritm.

Elemendid	Sätted ja selgitused
Password	Sisestage 8 kuni 32 tähemärki koodis ASCII (0x20-0x7E).
Confirm Password	Sisestage kinnitamise jaoks konfigureeritud parool.
Encryption Settings	
Algorithm	Valige krüptimiseks algoritm.
Password	Sisestage 8 kuni 32 tähemärki koodis ASCII (0x20-0x7E).
Confirm Password	Sisestage kinnitamise jaoks konfigureeritud parool.
Context Name	Sisestage 1 kuni 32 tähemärki, kasutades 1-baidi tähemärke.

Seotud teave

➡ „SNMPv3 konfigureerimine” lk 81

Skanneri ühendamine IEEE802.1X-võrguga

IEEE802.1X-võrgu konfigureerimine

Kui skanner toetab IEEE802.1X-võrku, saate skannerit kasutada võrgus, mille autentimiseks kasutatakse ühendust RADIUS-serveriga ja autentikaatoriks on jaotur.

1. Avage Web Config ja valige **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Sisestage kõigile kirjetele väärtus.
3. Klõpsake nuppu **Next**.

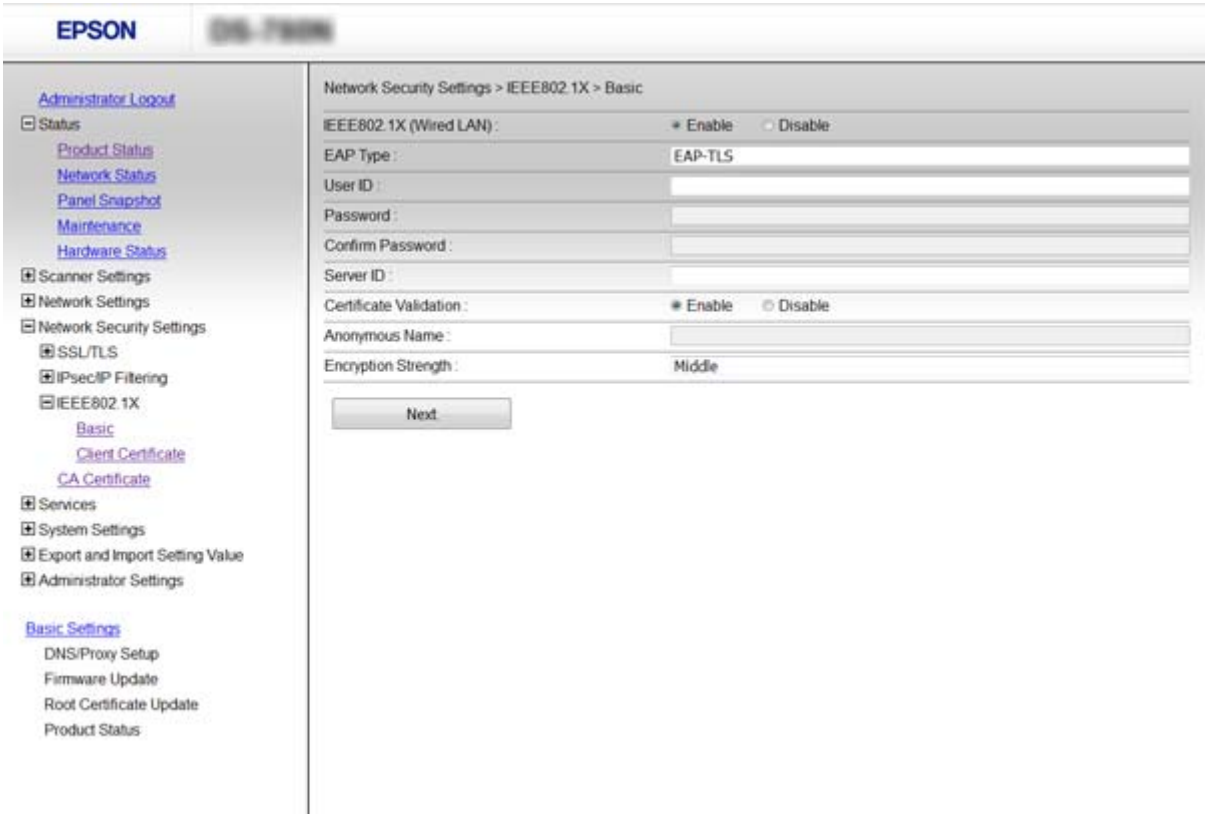
   Kuvatakse kinnitusteade.
4. Klõpsake nuppu **OK**.

   Skannerit värskendatakse.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23
➡ „IEEE802.1X-võrgu sättekirjed” lk 84
➡ „Pärast standardi IEEE802.1X konfigureerimist puudub juurdepääs printerile või skannerile” lk 88

IEEE802.1X-võrgu sättekirjed



Üksused	Sätted ja selgitus	
IEEE802.1X (Wired LAN)	Saate lehe sätteid aktiveerida või inaktiveerida (**IEEE802.1X** > **Basic**) võrgule IEEE802.1X (juhtmega LAN).	
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.
User ID	Konfigureerige ID, mida kasutatakse RADIUS-serveri autentimiseks. Sisestage 1 kuni 128 1-baidist ASCII (0x20 kuni 0x7E) vormingus tähemärki.	
Password	Konfigureerige parool skanneri autentimiseks. Sisestage 1 kuni 128 1-baidist ASCII (0x20 kuni 0x7E) vormingus tähemärki. Kui kasutate Windows serverit, nagu RADIUS, saate sisestada 127 tähemärki.	
Confirm Password	Sisestage kinnitamiseks konfigureeritud parool.	
Server ID	Saate konfigureerida serveri ID autentimiseks määratud RADIUS-serveriga. Autentimisrakendus kontrollib, kas serveri ID sisaldub serveri subject/subjectAltName väljal ja kas sert on saadetud RADIUS serverist või mitte. Sisestage 0 kuni 128 1-baidist ASCII (0x20 kuni 0x7E) vormingus tähemärki.	
Certificate Validation	Saate määrata serdi kinnitamise vaatamata audentimisviisile. Importige sertifikaat üksusesse **CA Certificate**.	

Üksused	Sätted ja selgitus	
Anonymous Name	Kui valite **PEAP-TLS** või **PEAP/MSCHAPv2** suvandi **Authentication Method** sätteks, saate PEAP-autentimise 1. faasi jaoks konfigureerida kasutaja ID asemel anonüümse nime. Sisestage 0 kuni 128 1-baidist ASCII (0x20 kuni 0x7E) vormingus tähemärki.	
Encryption Strength	Valikud on alljärgnevad.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Seotud teave

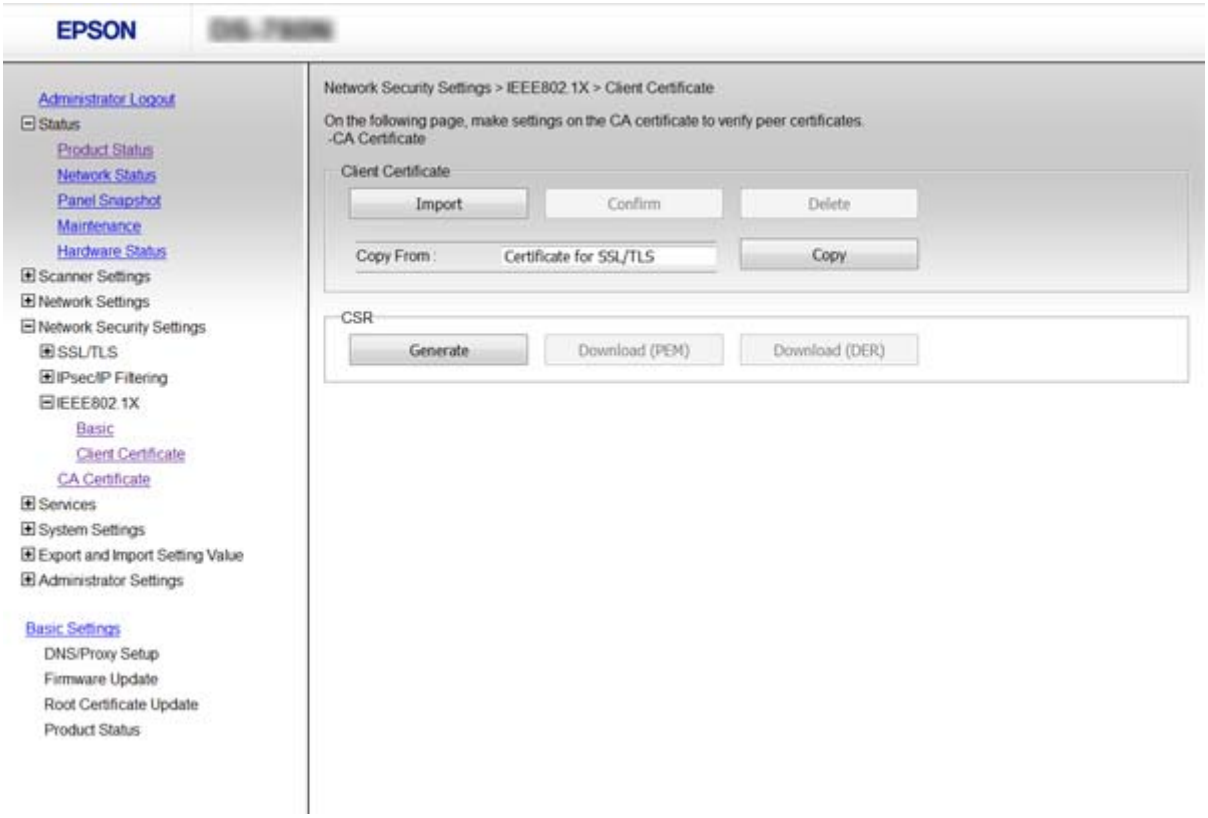
➡ „IEEE802.1X-võrgu konfigureerimine” lk 83

Standardile IEEE802.1X vastava sertifikaadi häälestamine

Häälestage standardile IEEE802.1X vastav kliendisertifikaat. Kui soovite seadistada sertimiskeskuse serti, valige **CA Certificate**.

1. Avage Web Config ja valige **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Sisestage sert üksusesse **Client Certificate**.

   Võite kopeerida serdi, kui see on välja antud sertimiskeskuse poolt. Kopeerimiseks valige sert üksuses **Copy From** ja seejärel klõpsake nuppu **Copy**.



Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Sertimiskeskuse allkirjastatud sertifikaadi hankimine ja importimine” lk 63

Täpsemate turvasätetega seotud probleemide lahendamine

Turvasätete taastamine

Kui loote kõrge turvalisustasemega keskkonna, nagu IPsec/IP-filtreerimine või IEEE802.1X, 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 inaktiveerimine juhtpaneelilt

IPsec/IP-filtreerimise või standardi IEEE802.1X saab inaktiveerida skanneri juhtpaneelilt.

1. Puudutage valikut **Sätted** > **Võrgusätted**.
2. Puudutage valikut **Muuda sätteid**.
3. Puudutage üksusi, mida soovite inaktiveerida.
   - ❏ **IPsec/IP filtreerimine**
   - ❏ **IEEE802.1X**
4. Kui kuvatakse lõpetamise teade, puudutage valikut **Jätka**.

Turvafunktsiooni taastamine rakendusega Web Config

IEEE802.1X puhul ei pruugita seadmeid võrgus tuvastada. Sel juhul inaktiveerige funktsioon skanneri juhtpaneelilt.

IPsec/IP-filtreerimise puhul saate funktsiooni inaktiveerida, kui teil on arvutist seadmele juurdepääs.

IPsec/IP-filtreerimise inaktiveerimine rakendusega Web Config

1. Avage Web Config ja valige **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Valige **Disable** suvandi **IPsec/IP Filtering** sätteks suvandis **Default Policy**.
3. Klõpsake valikut **Next** ja seejärel eemaldage valik **Enable this Group Policy** kõigi rühmapoliitikate jaoks.
4. Klõpsake nuppu **OK**.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

Probleemid võrgu turvafunktsioonide kasutamisel

Ühiskasutatud võtme unustamine

Konfigureerige võti rakenduse Web Config abil uuesti.

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

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

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

IPsec-sideühenduse kasutamine ei ole võimalik

Kas kasutate printeri sätete jaoks toetamata algoritmi?

Skanner toetab alljärgnevaid algoritme.

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 70

Sideühendus ei ole ootamatult kasutatav

Kas skanneri IP-aadress on vale või on seda muudetud?

Blokeerige skanneri juhtpaneeli abil IPsec.

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

Kasutage staatilist IP-aadressi.

Kas arvuti IP-aadress on vale või on seda muudetud?

Blokeerige skanneri juhtpaneeli abil IPsec.

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

Kasutage staatilist IP-aadressi.

Seotud teave

➡ „Juurdepääs rakendusele Web Config” lk 23

➡ „Krüptitud side IPsec/IP-filtreerimisega” lk 70

Ei saa ühendust pärast IPsec/IP filtreerimise häälestamist

Sätteväärtused võivad olla 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 70

Pärast standardi IEEE802.1X konfigureerimist puudub juurdepääs printerile või skannerile

Sätted võivad olla valed.

Inaktiveerige IEEE802.1X skaneri juhtpaneelilt. Ühendage skanner ja arvuti ja seejärel konfigureerige IEEE802.1X uuesti.

Seotud teave

➡ „IEEE802.1X-võrgu konfigureerimine” lk 83

Probleemid digitaalsertifikaadi kasutamisel

Sertimiskeskuse allkirjastatud sertifikaadi importimine ei ole võimalik

Kas sertimiskeskuse allkirjastatud sertifikaadil ja sertifikaadi allkirjastamistaotlusel sisalduv teave ühtivad?

Kui sertimiskeskuse allkirjastatud sertifikaadil 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.

Kas sertimiskeskuse allkirjastatud sertifikaat on suurem kui 5 KB?

Te ei saa importida sertimiskeskuse allkirjastatud sertifikaati, mis on suurem kui 5 KB.

Kas sertifikaadi importimiseks kasutatav parool on õige?

Kui unustasite parooli, ei ole sertifikaadi importimine võimalik.

Seotud teave

➡ „Sertimiskeskuse allkirjastatud sertifikaadi importimine” lk 65

Iseallkirjastatud sertifikaadi värskendamine ei ole võimalik

Kas Common Name on sisestatud?

Common Name peab olema sisestatud.

Kas väljale Common Name on sisestatud toetamata tähemärke? Näiteks jaapani tähemärgid ei ole toetatud.

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

Kas 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

➡ „Iseallkirjastatud sertifikaadi värskendamine” lk 67

Sertifikaadi allkirjastamistaotluse loomine ei ole võimalik

Kas Common Name on sisestatud?

Common Name peab olema sisestatud.

Kas väljale Common Name, Organization, Organizational Unit, Locality, State/Province on sisestatud toetamata tähemärke? Näiteks jaapani tähemärgid ei ole toetatud.

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

Kas 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 63

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.

Täpsemad turvasätted ettevõttele

Teated	Põhjus/tegevusmeede
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.
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.

Teated	Põhjus/tegevusmeede
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

➡ „Teave digitaalsertimise kohta” lk 62

Sertimiskeskuse allkirjastatud sertifikaadi kogemata kustutamine

Kas sertifikaadil on varufail?

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

➡ „Sertimiskeskuse allkirjastatud sertifikaadi kustutamine” lk 66

➡ „Sertimiskeskuse allkirjastatud sertifikaadi importimine” lk 65