

# Järjestelmänvalvojan opas

## Sisältö

### Tekijänoikeus

### Tavaramerkit

### Tietoja tästä käyttöoppaasta

Merkit ja symbolit. . . . .	6
Tässä käyttöoppaassa käytetyt kuvaukset. . . . .	6
Käyttöjärjestelmien viitteet. . . . .	6

### Johdanto

Käyttöopasosa. . . . .	8
Oppaassa käytetyt termit ja käsitteet. . . . .	8

### Valmistelu

Skannerien asetusten ja hallinnan prosessikaavio. . .	10
Verkkoympäristöesimerkki. . . . .	11
Esimerkkejä skannerin liittamisestä verkkoon. . .	11
Valmistelut ennen verkkoon kytkemistä. . . . .	12
Yhteyksien määrittämistä varten tarvittavien tietojen kerääminen. . . . .	12
Skannerin ominaisuudet. . . . .	12
Porttinumeron käyttäminen. . . . .	13
IP-osoitteen asettaminen. . . . .	13
DNS-palvelin ja välityspalvelin. . . . .	13
Verkkoyhteyden määrittäminen. . . . .	13

### Verkkoon liittäminen

Laitteen liittäminen verkkoon. . . . .	15
Verkkoyhteyden ottaminen käyttöön ohjauspaneelista. . . . .	15
Laitteen liittäminen verkkoon asennusohjelman avulla. . . . .	19

### Toimintojen asetukset

Ohjelmistoasetukset. . . . .	22
Web Config (laitteen verkkohallintasivu). . . . .	22
Skannaustoimintojen käyttäminen. . . . .	24
Skannaus tietokoneelta. . . . .	24
Skannaaminen ohjauspaneelista. . . . .	26
Järjestelmäasetusten määrittäminen. . . . .	28
Järjestelmän asetusten määrittäminen ohjauspaneelista. . . . .	28

Järjestelmän asetusten määrittäminen Web Config -hallintasivun kautta. . . . .	30
--	----

### Tietoturvan perusasetukset

Yleistietoja tietoturvan perusasetuksista. . . . .	32
Järjestelmänvalvojan salasanan määrittäminen. . . . .	33
Järjestelmänvalvojan salasanan määrittäminen ohjauspaneelista. . . . .	33
Järjestelmänvalvojan salasanan määrittäminen Web Config -toiminnolla. . . . .	33
Järjestelmänvalvojan salasananalla lukittavat asetukset. . . . .	34
Ohjausprotokollat. . . . .	35
Protokollat, jotka voidaan määrittää käyttöön tai pois käytöstä. . . . .	36
Protokolla-asetukset. . . . .	37

### Käyttö- ja hallinta-asetukset

Laitteen tietojen tarkistaminen. . . . .	40
Laitteiden hallinta (Epson Device Admin). . . . .	40
Tapahtumista ilmoittavien sähköpostien vastaanotto. . . . .	41
Tietoja sähköposti-ilmoituksista. . . . .	41
Sähköposti-ilmoitusten määrittäminen. . . . .	41
Postipalvelimen määrittäminen. . . . .	42
Postipalvelimen yhteyden tarkistaminen. . . . .	44
Laitteohjelmiston päivittäminen. . . . .	46
Laitteohjelmiston päivittäminen Web Config -hallintasivun kautta. . . . .	46
Laitteohjelmiston päivittäminen Epson Firmware Updater -ohjelman avulla. . . . .	46
Asetusten varmuuskopiointi. . . . .	47
Asetusten vieminen. . . . .	47
Asetusten tuominen. . . . .	47

### Ongelmien ratkaisu

Vinkkejä ongelmanratkaisuun. . . . .	49
Palvelimen tai verkkoon liitetyn laitteen lokin tarkastaminen. . . . .	49
Verkkoasetusten alustaminen. . . . .	49
Verkkoasetusten palauttaminen ohjauspaneelista. . . . .	49
Laitteiden ja tietokoneen välisen tiedonsiirron tarkastaminen. . . . .	49

Yhteyden tarkistaminen Ping-komennolla — Windows. . . . .	49
Yhteyden tarkistus Ping-komennolla — Mac OS. . . . .	51
Verkko-ohjelmiston käyttöön liittyviä ongelmia. . . . .	52
Web Config -hallintasivun käyttäminen ei onnistu. . . . .	52
Mallin nimeä ja/tai IP-osoitetta ei näy EpsonNet Config -ohjelmistossa. . . . .	53

## Liite

Yleistietoja verkko-ohjelmistosta. . . . .	55
Epson Device Admin. . . . .	55
EpsonNet Config. . . . .	55
EpsonNet SetupManager. . . . .	56
IP-osoitteen määrittäminen EpsonNet Config - sovelluksen avulla. . . . .	56
IP-osoitteen määrittäminen eräasetusten avulla. . . . .	56
IP-osoitteen määrittäminen kullekin verkon laitteelle. . . . .	59
Skannerin käyttämät porttinumerot. . . . .	60

## Suojauksen lisäasetukset (yrityskäyttäjät)

Laiteasetukset ja riskien hallinta. . . . .	62
Suojaustoimintojen asetukset. . . . .	63
SSL/TLS-suojattu tiedonsiirto ja skannerin käyttö. . . . .	63
Tietoja digitaalisesta varmennuksesta. . . . .	63
CA:n allekirjoittaman varmenteen hankinta ja tuonti. . . . .	64
CA:n allekirjoittaman varmenteen poisto. . . . .	67
Itse allekirjoitetun varmenteen päivitys. . . . .	68
Määritä CA Certificate. . . . .	69
Tiedonsiirron salaus IPsec-suojauksen ja IP- osoitteiden suodatuksen avulla. . . . .	71
Tietoja IPsec/IP Filtering -sovelluksesta. . . . .	71
Default Policy -määrittäminen. . . . .	72
Group Policy -määrittäminen. . . . .	75
IPsec/IP Filtering -konfigurointiesimerkit. . . . .	81
IPsec/IP Filtering -sertifikaatin määrittäminen. . . . .	82
SNMPv3-protokollan käyttö. . . . .	83
Tietoja SNMPv3-protokollasta. . . . .	83
SNMPv3-määrittäminen. . . . .	83
Skannerin kytkentä IEEE802.1X-verkkoon. . . . .	85
IEEE802.1X-verkon määrittäminen. . . . .	85
IEEE802.1X-sertifikaatin määrittäminen. . . . .	86
Tietosuojaan liittyvien ongelmien ratkaiseminen. . . . .	87
Suojausasetusten palautus. . . . .	87

Ongelmia verkon suojaustoimintojen käytössä. . . . .	88
Ongelmia digitaalisen varmenteen käytössä. . . . .	90

# Tekijänoikeus

Mitään tämän julkaisun osaa ei saa toisintaa, tallentaa tietojenhakujärjestelmään tai siirtää missään muodossa tai millään tavoin, elektronisesti, mekaanisesti, valokopioimalla, nauhoittamalla tai muuten ilman Seiko Epson Corporationin etukäteen antamaa kirjallista suostumusta. Julkaisija ei vastaa julkaisun sisältämien tietojen käytöstä. Julkaisija ei myöskään vastaa julkaisun sisältämien tietojen käytön seurauksista. Tässä oppaassa annettuja tietoja on tarkoitus käyttää vain tämän Epson-laitteen yhteydessä. Epson ei vastaa vahingoista, jotka aiheutuvat näiden tietojen soveltamisesta muihin tulostimiin.

Seiko Epson Corporation tai sen tytäryhtiöt eivät ole vastuussa tämän tuotteen hankkijalle tai kolmansille osapuolille mahdollisesti aiheutuvista vahingoista, menetyksistä, kustannuksista tai kuluista, jotka aiheutuvat onnettomuudesta, tämän tuotteen väärinkäytöstä tai siihen tehdystä luvattomista muunnoksista, korjauksista tai muutoksista tai (Yhdysvaltoja lukuun ottamatta) siitä, että Seiko Epson Corporationin antamia käyttö- ja huolto-ohjeita ei noudateta tarkoin.

Seiko Epson Corporation ja sen tytäryhtiöt eivät ole vastuussa vahingoista tai vaikeuksista, jotka aiheutuvat muiden lisävarusteiden tai tarvikkeiden kuin Seiko Epson Corporationin ilmoittamien alkuperäisten Epson-tuotteiden tai Epson-hyväksynnän saaneiden tuotteiden käytöstä.

Seiko Epson Corporation ei vastaa sähkömagneettisista häiriöistä johtuvista vahingoista, mikäli niihin on synnä muiden kuin Seiko Epson Corporationin Epson-hyväksynnän saaneiden liitântäkaapeleiden käyttö.

©Seiko Epson Corporation 2016.

Tämän oppaan sisältö ja tämän tuotteen tekniset tiedot saattavat muuttua ilman erillistä ilmoitusta.

# Tavaramerkit

- ❑ EPSON® on rekisteröity tavaramerkki, ja EPSON EXCEED YOUR VISION tai EXCEED YOUR VISION on Seiko Epson Corporationin tavaramerkki.
- ❑ 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.
- ❑ Yleinen ilmoitus: Muut julkaisussa käytetyt tuotenimet on mainittu vain tunnistamistarkoituksessa, ja ne saattavat olla vastaavien omistajiensa tavaramerkkejä. Epson ei vaadi itselleen mitään oikeuksia näihin tuotenimiin.

# Tietoja tästä käyttöoppaasta

---

## Merkit ja symbolit



**Vaara:**

Ohjeet, joita on noudatettava huolellisesti henkilövahinkojen välttämiseksi.



**Tärkeää:**

Ohjeet, jotka on huomioitava laitteistovahinkojen välttämiseksi.

**Huomautus:**

Ohjeet, jotka sisältävät hyödyllisiä vinkkejä ja skanneritoimintojen rajoituksia.

### Liittyvät tiedot

➔ Tätä kuvaketta napsauttamalla pääset liittyviin tietoihin.

---

## Tässä käyttöoppaassa käytetyt kuvaukset

- Skanneriohjaimen ja Epson Scan 2 -sovelluksen (skanneriohjain) näyttökuvat ovat Windows 10- ja OS X El Capitan -käyttöjärjestelmistä. Näytöllä näkyvät tiedot vaihtelevat laitemallin ja käyttötilanteen mukaan.
- Käyttöoppaassa käytetyt kuvat ovat vain esimerkkejä. Vaikka mallien välillä voi olla pieniä eroja, toimintaperiaatteet ovat samat.
- Jotkin LCD-näytön valikon osista vaihtelevat mallista ja asetuksista riippuen.

---

## Käyttöjärjestelmien viitteet

### Windows

Tässä käyttöoppaassa käytetyt termit, kuten "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", viittaavat seuraaviin käyttöjärjestelmiin. Tämän lisäksi "Windows" tarkoittaa kaikkia sen versioita.

- Microsoft® Windows® 10-käyttöjärjestelmä
- Microsoft® Windows® 8.1-käyttöjärjestelmä
- Microsoft® Windows® 8-käyttöjärjestelmä
- Microsoft® Windows® 7-käyttöjärjestelmä
- Microsoft® Windows Vista®-käyttöjärjestelmä
- Microsoft® Windows® XP-käyttöjärjestelmä
- Microsoft® Windows® XP Professional x64 Edition-käyttöjärjestelmä

## Tietoja tästä käyttöoppaasta

- Microsoft® Windows Server® 2016-käyttöjärjestelmä
- Microsoft® Windows Server® 2012 R2-käyttöjärjestelmä
- Microsoft® Windows Server® 2012-käyttöjärjestelmä
- Microsoft® Windows Server® 2008 R2-käyttöjärjestelmä
- Microsoft® Windows Server® 2008-käyttöjärjestelmä
- Microsoft® Windows Server® 2003 R2-käyttöjärjestelmä
- Microsoft® Windows Server® 2003-käyttöjärjestelmä

### **Mac OS**

Tässä käyttöoppassa "Mac OS" tarkoittaa versioita 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.

# Johdanto

---

## Käyttöopasosa

Tämä käyttöopas on tarkoitettu laitteiden ylläpitäjille, jotka ovat vastuussa tulostinten tai skannereiden liittamisestä verkkoon. Opas sisältää tietoja laitteiden asetuksista ja ominaisuuksista.

Lisätietoja eri toimintojen käyttämisestä on *Käyttöopas* -oppaassa.

### Valmistelu

Tässä kohdassa kuvataan järjestelmänvalvojan tehtävät, laitteiden asetusten määrittäminen ja laitteiden hallinnassa käytettävät ohjelmistot.

### Verkkoon liittäminen

Tässä kohdassa kerrotaan, miten laite liitetään lähiverkkoon tai kytketään puhelinlinjaan. Se sisältää myös tietoja verkkoympäristöstä, kuten laitteiden porttimäärityksistä sekä DNS- ja välityspalvelimen käyttämisestä.

### Toimintojen asetukset

Esittelee laitteen eri toimintoihin liittyvät asetukset.

### Tietoturvan perusasetukset

Esittelee eri toimintoihin, kuten tulostamiseen, skannaamiseen ja faksien lähettämiseen ja vastaanottamiseen liittyvät asetukset.

### Käyttö- ja hallinta-asetukset

Kertoo miten laitetta käytetään käyttöönoton jälkeen, miten laitetietoja tarkastellaan ja miten laitetta huolletaan.

### Ongelmien ratkaisu

Kertoo, miten asetukset nollataan ja miten verkkoyhteysongelmia selvitetään.

### Suojauksen lisäasetukset (yrityskäyttäjät)

Esittelee suojauksen lisäasetukset, kuten CA-varmenteisiin, SSL/TLS-suojattuun tiedonsiirtoon sekä IPsec-suojaukseen ja IP-osoitteiden suodatukseen liittyvät asetukset.

Laitemallista riippuen kaikki tässä luvussa kuvatut toiminnot eivät ehkä ole tuettuja.

---

## Oppaassa käytetyt termit ja käsitteet

Tässä käyttöoppaassa käytetään seuraavia termejä ja käsitteitä.

### Järjestelmänvalvoja

Henkilö, joka vastaa laitteen tai verkon asetuksista ja hallinnasta työpaikalla tai organisaatioissa. Pienissä organisaatioissa järjestelmänvalvoja voi vastata sekä laitteiden että verkon ylläpidosta. Suurissa organisaatioissa



## Johdanto

Järjestelmänvalvojat voivat vastata esimerkiksi yksikön tai osaston verkosta tai laitteista ja verkonvalvojat vastaavat organisaatiotason ylittävän tietoliikenteen, kuten Internet-yhteyksien, hallinnasta.

### Verkonvalvoja

Henkilö, joka vastaa verkossa tapahtuvan tietoliikenteen hallinnasta. Verkonvalvoja määrittää reitittimet, välityspalvelimet, DNS-palvelimet ja sähköpostipalvelimet sisäverkon liikennettä ja Internet-yhteyksiä varten.

### Käyttäjä

Henkilö, joka käyttää laitteita, kuten tulostimia ja skannereita.

### Web Config (laitteen oma hallintasivu verkossa)

Laitteeseen integroitu web-palvelin. Laitteen hallintasivun nimi on Web Config. Sivun avulla voit tarkistaa laitteen tilan ja muuttaa asetuksia verkkoselaimella.

### Työkalu

Yleisnimitys laitteiden hallinnassa käytettäville ohjelmistoille, joita ovat esimerkiksi Epson Device Admin, EpsonNet Config ja EpsonNet SetupManager.

### Push-skannaus

Yleistermi skannaamiselle laitteen ohjauspaneelia käyttäen.

### ASCII (American Standard Code for Information Interchange)

Yleisesti käytetty merkkijärjestelmä. Johon kuuluu 128 merkkiä, kuten aakkoset (a–z, A–Z), arabialaiset numerot (0–9), symbolit, välimerkit ja ohjausmerkit. Tässä oppaassa ASCII ymmärretään merkkeinä 0x20–0x7E (heksanumero, lueteltu alla) ilman ohjausmerkkejä.

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	{		}	~	

\* Väliilyöntimerkki.

### Unicode (UTF-8)

Kansainvälinen merkkijärjestelmä, joka kattaa kaikkien suurten kielten merkkijärjestelmät. Tässä käyttöoppaassa UTF-8 tarkoittaa UTF-8-muotoon koodattuja merkkejä.

# Valmistelu

Tässä luvussa kuvataan järjestelmänvalvojan tehtävät ja ennen asetusten määrittämistä tarvittavat valmistelut.

---

## Skannerien asetusten ja hallinnan prosessikaavio

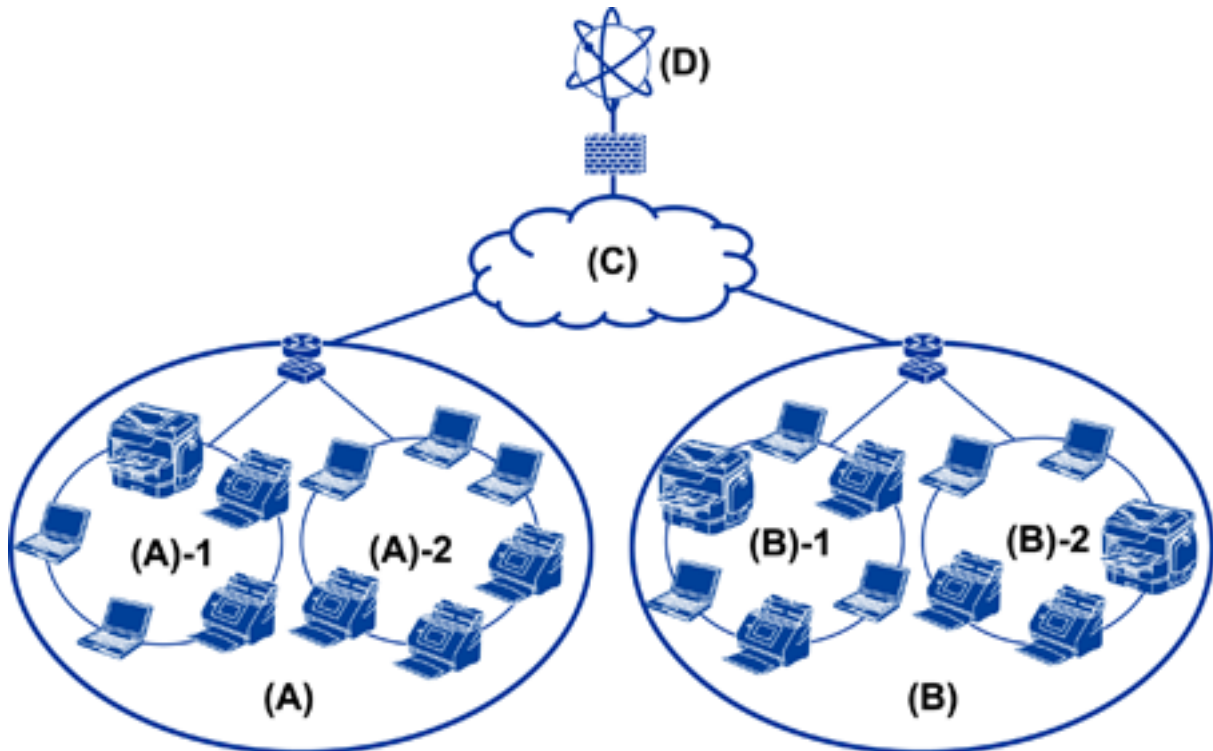
Järjestelmänvalvoja määrittää verkon yhteysasetukset, määrittää skannerin asetukset ja ylläpidon ja määrittää laitteet käyttäjien käyttöön.

1. Valmistelu
  - Yhteysmäärittämissä tarvittavien tietojen kerääminen
  - Käytettävän yhteystavan valitseminen
2. Yhteyden toteuttaminen
  - Verkkoyhteys skannerin ohjauspaneelistä
3. Toimintojen määrittäminen
  - Skanneriohjaimen asetukset
  - Muut lisäasetukset
4. Suojausasetukset
  - Pääkäyttäjän asetukset
  - SSL/TLS
  - Protokollien hallinta
  - Suojauksen lisäasetukset (valinnainen)
5. Käyttö ja hallinta
  - Laitteen tilan valvonta
  - Laitetapahtumien hallinta
  - Laitteasetusten varmuuskopiointi

### Liittyvät tiedot

- ➔ ["Valmistelu" sivulla 10](#)
- ➔ ["Verkkoon liittäminen" sivulla 15](#)
- ➔ ["Toimintojen asetukset" sivulla 22](#)
- ➔ ["Tietoturvan perusasetukset" sivulla 32](#)
- ➔ ["Käyttö- ja hallinta-asetukset" sivulla 40](#)

## Verkkoympäristöesimerkki



(A): Toimisto 1

(A)-1: LAN 1

(A)-2: LAN 2

(B): Toimisto 2

(B)-1: LAN 1

(B)-2: LAN 2

(C): WAN

(D): Internet

### Esimerkkejä skannerin liittämisestä verkkoon

Skanneri voidaan laitteen käyttötavasta riippuen liittää verkkoon kahdella eri tavalla. Skanneri liitetään molemmissa tavoissa verkkoon tietokoneen kautta.

- Palvelin/asiakasyhteys (Windows-palvelin ja tulostustöiden hallinta)
- Vertaisyhteys (suoratulostus asiakaskoneista)

#### Liittyvät tiedot

- ➔ ”Palvelimen ja työaseman välinen yhteys” sivulla 12
- ➔ ”Vertaisyhteydet” sivulla 12

## Valmistelu

### Palvelimen ja työaseman välinen yhteys

Skannaus ja töiden hallinta voidaan keskittää asentamalla palvelimeen Document Capture Pro Server -ohjelmisto. Tämä ratkaisu soveltuu erityisesti tehtäviin, joissa käytetään useita skannereita ja skannataan suuri määrä asiakirjoja tiettyyn tiedostomuotoon.

#### Liittyvät tiedot

→ ”Oppaassa käytetyt termit ja käsitteet” sivulla 8

### Vertaisyhteydet

Voit käyttää yksittäistä skanneria asiakaskoneeseen asennetun skanneriohjaimen, kuten Epson Scan 2, kautta. Voit suorittaa töitä skannerin yksittäisissä asiakaskoneissa asentamalla asiakaskoneisiin Document Capture Pro (Document Capture) -ohjelmiston.

#### Liittyvät tiedot

→ ”Oppaassa käytetyt termit ja käsitteet” sivulla 8

---

## Valmistelut ennen verkkoon kytkemistä

### Yhteyksien määrittämistä varten tarvittavien tietojen kerääminen

Verkkoyhteyden määrittämistä varten tarvitaan mm. IP-osoite ja yhdyskäytävän osoite. Tarkista, että sinulla on valmiina seuraavat tiedot.

Luokka	Asetus	Huomaus
Laitteen liitântätapa	<input type="checkbox"/> Ethernet	Käytä Ethernet-verkkokaapelina vähintään luokan 5e suojattua kierrettyä parikaapelia (STP).
Lähiverkon asetustiedot	<input type="checkbox"/> IP-osoite <input type="checkbox"/> Aliverkon peite <input type="checkbox"/> Oletusyhdykäytävä	Jos IP-osoite määritetään automaattisesti reitittimen DHCP-toiminnolla, näitä asetuksia ei tarvita.
DNS-palvelimen tiedot	<input type="checkbox"/> Ensisijaisen DNS-palvelimen IP-osoite <input type="checkbox"/> Toissijaisen DNS-palvelimen IP-osoite	Jos IP-osoitteeksi määritetään staattinen IP-osoite, myös DNS-palvelin on määritettävä. DNS-palvelin on määritettävä myös, jos osoitteet määritetään automaattisesti DHCP-palvelun kautta mutta DNS-palvelimen automaattinen määrittäminen ei onnistu.
Välityspalvelimen asetukset	<input type="checkbox"/> Välityspalvelimen nimi <input type="checkbox"/> Porttinumero	Välityspalvelu määritetään, jos Internet-yhteys toimii välityspalvelimen kautta ja jos Epson Connect -palvelu tai laiteohjelmistojen automaattinen päivitys halutaan ottaa käyttöön.

### Skannerin ominaisuudet

Skannerin tekniset tiedot ja liitännät on kuvattu *Käyttöopas* -oppaassa.

## Porttinumeron käyttäminen

Katso lisätiedot skannerin käyttämien porttien numeroista liitteistä.

### Liittyvät tiedot

➔ ”Skannerin käyttämät porttinumerot” sivulla 60

## IP-osoitteen asettaminen

Skannerille voidaan asettaa IP-osoite kahdella eri tavalla.

### Staattinen IP-osoite:

Skannerille määritetään ennalta tiedossa oleva yksilöllinen IP-osoite.

IP-osoite pysyy samana, vaikka skanneri tai reititin sammutettaisiin. Voit hallita laitetta pelkän IP-osoitteen perusteella.

Staattinen IP-osoite on hyvä ratkaisu verkoissa, joissa on useita skannereita, kuten suurissa toimistoissa tai kouluissa.

### IP-osoitteen automaattinen asettaminen DHCP-toiminnolla:

DHCP-toimintoa tukeva reititin asettaa skannerin IP-osoitteen automaattisesti.

Jos IP-osoitteen vaihtaminen laitteelle on hankalaa, varaa IP-osoite etukäteen ja määritä se käyttöön haluttuna ajankohtana.

## DNS-palvelin ja välityspalvelin

Jos käytät Internet-yhteyttä, sinun on määritettävä DNS-palvelin (nimipalvelu). Jos et määritä nimipalvelua, yhteysosoitteina on käytettävä IP-numeroita, koska nimiosoitteiden selvitys ei todennäköisesti toimi.

Välityspalvelin toimii sisäverkon ja Internetin välissä välittäen liikennettä tietokoneilta ja skannereilta Internetiin ja toisinpäin. Sisäverkon ulkopuoliset palvelimet ovat yhteydessä vain välityspalvelimeen. Skannerin tietoja, kuten IP-osoitetta ja porttinumeroa, ei tällöin välitetä ulospäin, minkä ansiosta tietoturva on parempi.

Koska välityspalvelin pystyy tarvittaessa valvomaan sen kautta kulkevan verkkoliikenteen sisältöä, voit tarvittaessa myös estää liikenteen tiettyyn URL-osoitteeseen suodatustoiminnolla.

## Verkkoyhteyden määrittäminen

Jos haluat määrittää skannerin verkkoyhteyksasetukset, kuten IP-osoitteen, aliverkon peitteen ja oletusyhdyskäytävän, toimi seuraavasti.

### Asetusten määrittäminen ohjauspaneelista:

Voit määrittää asetukset jokaiselle skannerille erikseen laitteen ohjauspaneelin kautta. Määritä skannerin verkkoasetukset ennen verkkoyhteyden muodostamista.

## Valmistelu

### Asetusten määrittäminen asetusohjelmalla:

Asennusohjelmaa käytettäessä skannerin verkkoasetukset ja työaseman asetukset määritetään automaattisesti. Asetukset voidaan määrittää asennusohjelman ohjeiden mukaisesti myös ilman syvällistä verkkotuntemusta.

### Työkaluohjelman avulla:

Voit käyttää järjestelmänvalvojan tietokoneeseen asennettua työkaluohjelmaa. Voit etsiä skannerin ja määrittää laitteen asetukset, tai voit luoda SYLK-tiedoston ja määrittää useiden skannereiden asetukset erätoimintona. Voit määrittää asetukset useisiin skannereihin, mutta laitteiden on oltava liitettynä tietokoneeseen Ethernet-kaapelilla ennen asetusten määrittämistä. Asennusta varten suositellaan tämän vuoksi rakennettavaksi Ethernet-verkko.

### Liittyvät tiedot

- ➔ [”Verkkoyhteyden ottaminen käyttöön ohjauspaneelistä”](#) sivulla 15
- ➔ [”Laitteen liittäminen verkkoon asennusohjelman avulla”](#) sivulla 19
- ➔ [”IP-osoitteen määrittäminen EpsonNet Config -sovelluksen avulla”](#) sivulla 56

# Verkkoon liittäminen

Tässä luvussa kuvataan skannerin liittäminen verkkoon.

---

## Laitteen liittäminen verkkoon

### Verkkoyhteyden ottaminen käyttöön ohjauspaneelist

Voit liittää skannerin verkkoon skannerin ohjauspaneelin kautta.

Lisätietoja skannerin ohjauspaneelist on *Käyttöopas* -oppaassa.

### IP-osoitteen määrittäminen

Määritä perustiedot, kuten IP-osoite, Aliverk. peite ja Olet.yhd.käyt..

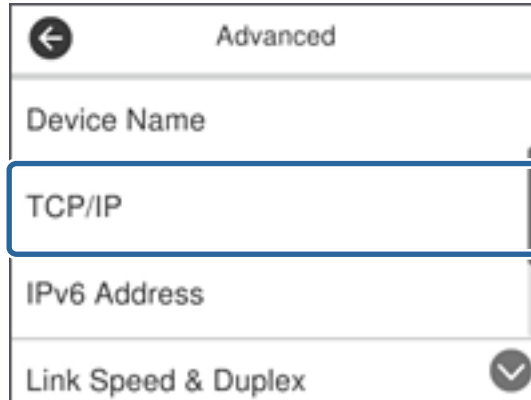
1. Käynnistä skanneri.
2. Pyyhkäise skannerin ohjauspaneelissa vasemmalle ja valitse sitten **Asetukset**.



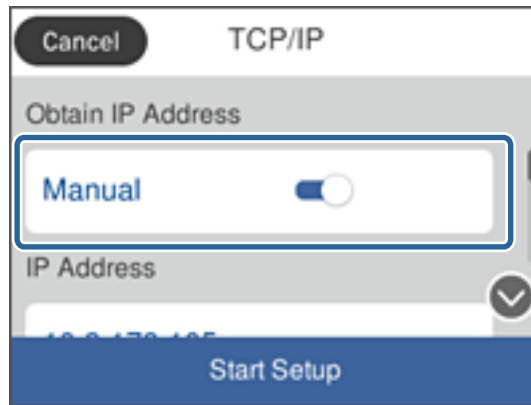
3. Valitse **Verkkoasetukset** > **Muuta asetuksia**.  
Jos valinta ei ole näkyvässä, pyyhkäise ruutua ylöspäin.

## Verkkoon liittäminen

4. Valitse **TCP/IP**.



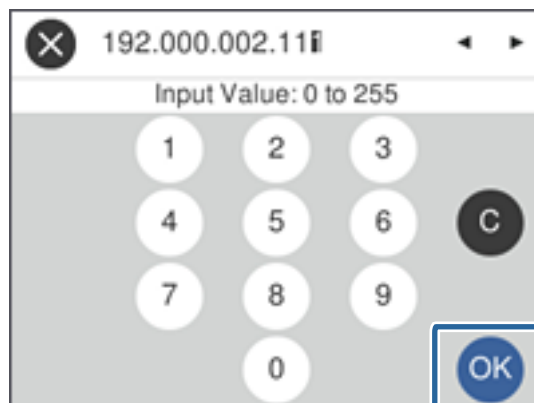
5. Valitse **Hae IP-osoite** -kohdassa **Man..**



**Huomautus:**

Jos haluat määrittää IP-osoitteen automaattisesti reitittimen DHCP-toiminnon avulla, valitse **Automaattinen**. Tällöin kohdat 6–7 eli **IP-osoite**, **Aliverk. peite** ja **Olet.yhd.käyt.** asetetaan automaattisesti. Siirry kohtaan 8.

6. Valitse **IP-osoite** -kenttä, kirjoita IP-osoite käyttäen näytössä näkyvää näppäimistöä ja valitse **OK**.



Vahvista edellisessä näytössä näkyvä arvo.

7. Aseta **Aliverk. peite** ja **Olet.yhd.käyt.**

Vahvista edellisessä näytössä näkyvä arvo.



## Verkkoon liittäminen

### **Huomautus:**

Jos asetusten (IP-osoite, Aliverk. peite ja Olet.yhd.käyt.) yhdistelmä on virheellinen, **Käynnistä asetus** -valinta ei ole aktiivinen eikä toimintoa voi jatkaa. Varmista, ettei tiedoissa ole virheitä.

8. Valitse **DNS-palvelin** -kohdassa **Ensisijainen DNS** -kenttä, kirjoita ensisijaisen DNS-palvelimen IP-osoite näytössä näkyvällä näppäimistöllä ja valitse sitten **OK**.

Vahvista edellisessä näytössä näkyvä arvo.

### **Huomautus:**

Jos valitset IP-osoitteen määrittäväksi **Automaattinen**, voit valita DNS-palvelimen asetusten määrittäväksi **Man.** tai **Automaattinen**. Jos DNS-palvelimen osoitteen hakeminen automaattisesti ei ole mahdollista, valitse **Man.** ja kirjoita DNS-palvelimen osoite. Kirjoita sitten toissijaisen DNS-palvelimen osoite. Jos valitset asetukseksi **Automaattinen**, siirry kohtaan 10.

9. Valitse **Toissijainen DNS** -kenttä, kirjoita toissijaisen DNS-palvelimen osoite näytössä näkyvällä näppäimistöllä ja valitse sitten **OK**.

Vahvista edellisessä näytössä näkyvä arvo.

10. Valitse **Käynnistä asetus**.


11. Valitse vahvistusnäytössä **Sulje**.


Jos et valitse **Sulje**, näyttö sammuu automaattisesti tietyn ajan kuluttua.

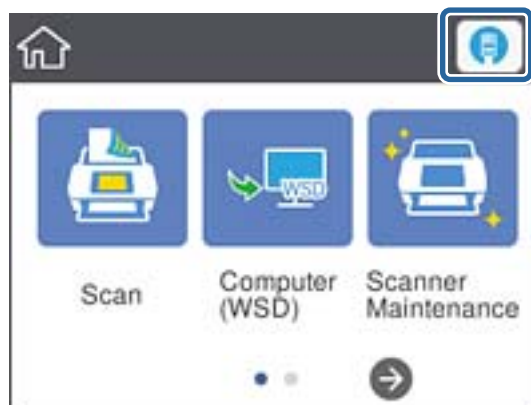
## Laitteen liittäminen Ethernet-lähiverkkoon

Liitä skanneri lähiverkkoon Ethernet-kaapelilla ja tarkista että yhteys toimii.

1. Kytke skanneri keskittimeen (L2-kytkin) Ethernet-kaapelilla.

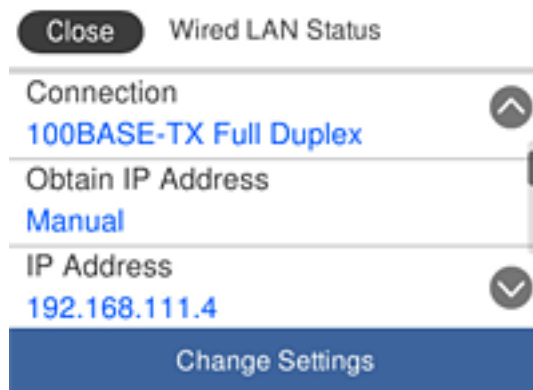
Aloituspäätön kuvake muuttuu muotoon  .

2. Valitse aloitusnäytössä  .



## Verkkoon liittäminen

3. Pyyhkäise näyttöä ylöspäin ja tarkista, että yhteyden tila ja IP-osoite ovat oikein.



## Välityspalvelinasetusten määrittäminen

Välityspalvelinta ei voi määrittää ohjauspaneelin kautta. Asetukset määritetään Web Config -hallintatoiminnolla.

1. Avaa Web Config ja valitse **Network Settings > Basic**.
2. Valitse **Proxy Server Setting** -kohdasta **Use**.
3. Kirjoita välityspalvelimen osoite IPv4- tai FQDN-muodossa **Välityspalvelin** -kohtaan ja kirjoita sitten portin numero **Proxy Server Port Number** -kohtaan.

Jos välityspalvelin edellyttää todennusta, kirjoita välityspalvelimeen kirjaututtaessa käytettävä käyttäjätunnus ja salasana.

## Verkkoon liittäminen

4. Napsauta **Next**-painiketta.

The screenshot shows the Epson Web Config interface for a printer. The left sidebar contains navigation options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Wired LAN', 'Basic', 'Email Server', 'Network Security Settings', 'Services', 'System Settings', 'Export and Import Setting Value', and 'Administrator Settings'. Under 'Basic Settings', 'DNS/Proxy Setup' is selected. The main content area shows various network settings. The 'Proxy Server Setting' section is highlighted with a blue box and includes the following fields: 'Proxy Server Setting' (radio buttons for 'Do Not Use' and 'Use', with 'Use' selected), 'Proxy Server' (text field with 'www.sample.proxy'), 'Proxy Server Port Number' (text field with '80'), 'Proxy Server User Name' (text field with 'XXXXXXXX'), and 'Proxy Server Password' (password field with masked characters). Below this section are settings for IPv6, including 'IPv6 Setting' (radio buttons for 'Enable' and 'Disable', with 'Disable' selected), 'IPv6 Privacy Extension' (radio buttons for 'Enable' and 'Disable', with 'Disable' selected), 'IPv6 DHCP Server Setting' (radio buttons for 'Do Not Use' and 'Use', with 'Do Not Use' selected), and several IPv6 address and DNS server fields. A 'Next' button is located at the bottom of the settings area.

5. Vahvista asetukset ja valitse sitten **Asetukset**.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Laitteen liittäminen verkkoon asennusohjelman avulla

Suosittu tapa on liittää skanneri tietokoneeseen asennusohjelman avulla. Voit suorittaa asennusohjelman jollakin seuraavista tavoista.

- Asennusohjelman lataaminen verkkosivustosta

Siirry seuraavaan verkkosivustoon ja kirjoita tuotteen nimi. Siirry kohtaan **Asetus** ja aloita asennus.

<http://epson.sn>

- Asentaminen ohjelmistolevyllä (vain laitemallit, joiden mukana toimitetaan ohjelmistolevy, ja vain käyttäjät, joiden tietokoneessa on levyasema)

Aseta ohjelmistolevy tietokoneeseen ja noudata näytössä näkyviä ohjeita.

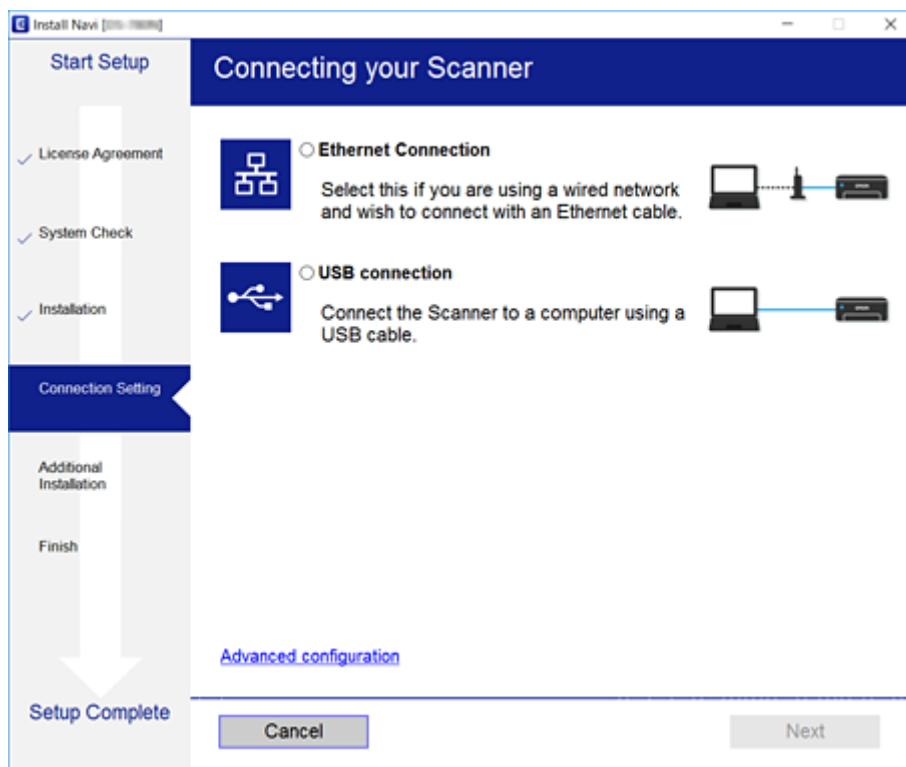
## Verkkoon liittäminen

### Liitännätavan valitseminen

Noudata näytössä näkyviä ohjeita, kunnes seuraava näyttö tulee näkyviin, ja valitse sitten liitännätapa, jolla skanneri liitetään tietokoneeseen.

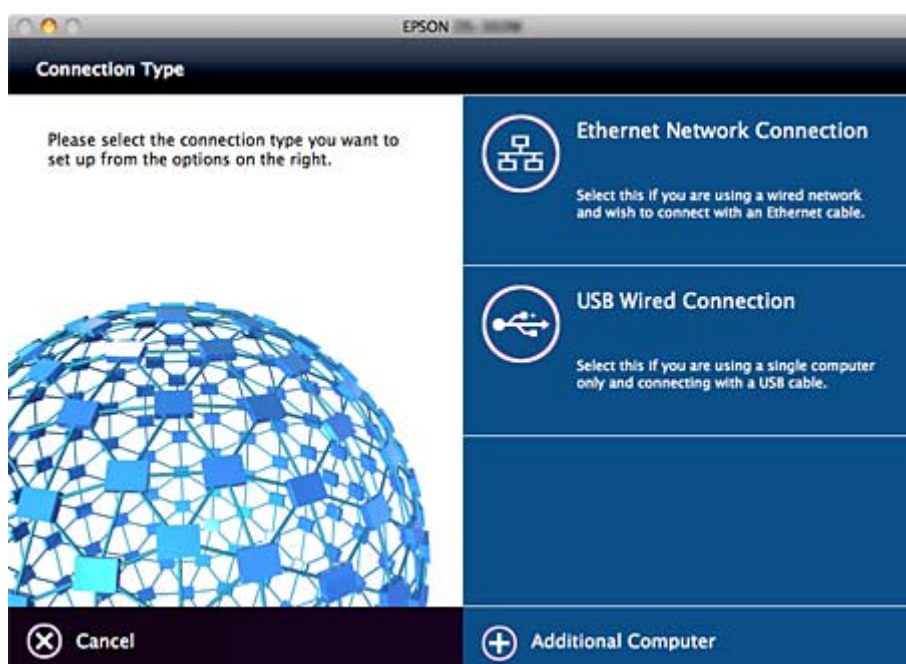
#### Windows

Valitse liitännätapa ja valitse sitten **Seuraava**.



#### Mac OS

Valitse liitännätapa.



## **Verkkoon liittäminen**

Noudata näytössä näkyviä ohjeita. Tietokone asentaa tarvittavat ohjelmistot.

# Toimintojen asetukset

Tässä luvussa kuvataan laitteen toimintojen käyttöönottoa varten tarvittavat asetukset.

---

## Ohjelmistoasetukset

Tässä ohjeaiheessa kuvataan asetusten määrittäminen järjestelmänvalvojan tietokoneelta käsin käyttäen Web Config -hallintasivua.

### Web Config (laitteen verkkohallintasivu)

#### Tietoja Web Config -sovelluksesta

Web Config on selainpohjainen sovellus skannerin asetusten määrittämiseen.

Jotta Web Config -ohjelmistoa voi käyttää, skannerille on ensin määritettävä IP-osoite.

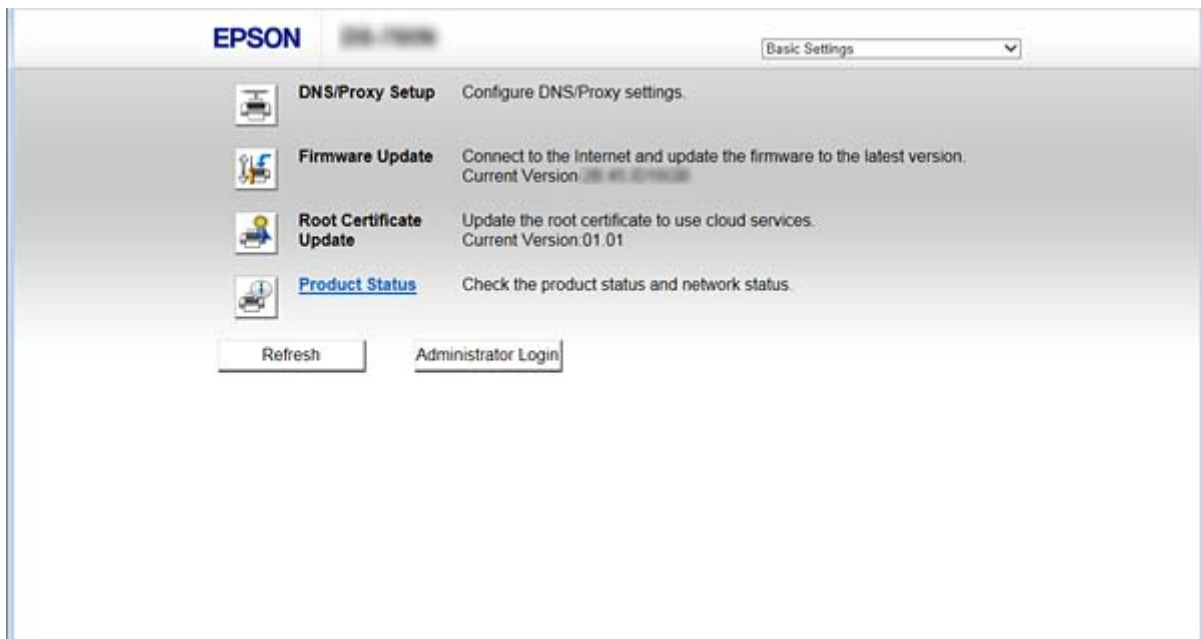
**Huomautus:**

Voit lukita asetukset määrittämällä järjestelmänvalvojan salasanan skannerille.

Alla on kuvattu kaksi asetussivua.

**Basic Settings**

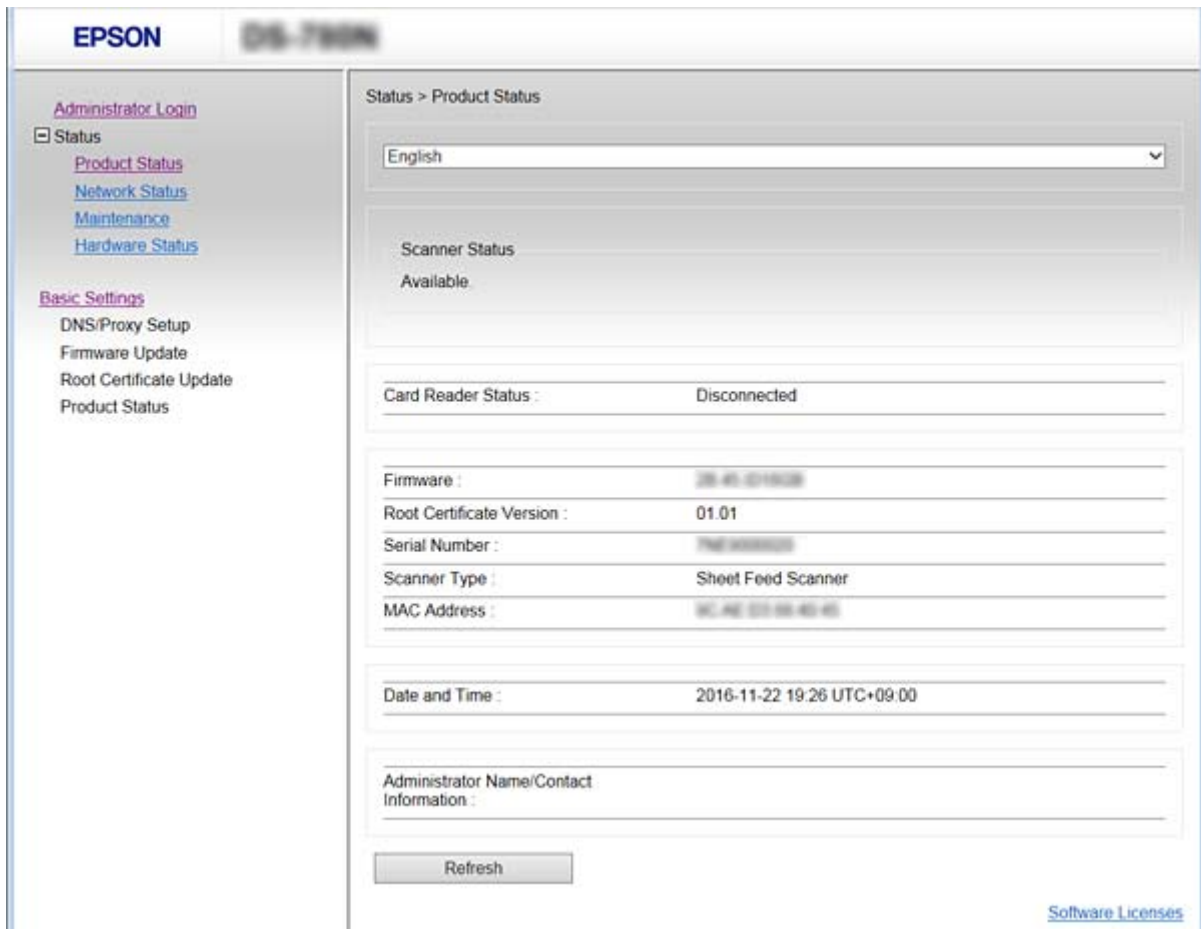
Voit määrittää skannerin perusasetukset.



## Toimintojen asetukset

### ❑ Advanced Settings

Voit määrittää skannerin lisäasetukset. Tämä sivu on tarkoitettu pääasiassa järjestelmänvalvojalle.



## Web Config -ohjelmiston käyttö

Kirjoita skannerin IP-osoite verkkoselaimeen. JavaScript on oltava käytössä. Kun käytät Web Config -ohjelmistoa HTTPS:n kautta, selaimessasi näytetään varoitusviesti, koska käytössä on skanneriin tallennettu itse allekirjoitettu varmenne.

### ❑ Käyttö HTTPS:n kautta

IPv4: <https://<skannerin IP-osoite>> (ilman merkkejä: < >)

IPv6: [https://\[skannerin IP-osoite\]/](https://[skannerin IP-osoite]/) (ilman merkkejä: [ ])

### ❑ Käyttö HTTP:n kautta

IPv4: <http://<skannerin IP-osoite>> (ilman merkkejä: < >)

IPv6: [http://\[skannerin IP-osoite\]/](http://[skannerin IP-osoite]/) (ilman merkkejä: [ ])

## Toimintojen asetukset

### **Huomautus:**

**Esimerkit**

IPv4:

<https://192.0.2.111/>

<http://192.0.2.111/>

IPv6:

[https://\[2001:db8::1000:1\]/](https://[2001:db8::1000:1]/)

[http://\[2001:db8::1000:1\]/](http://[2001:db8::1000:1]/)

- Jos skannerin nimi on rekisteröity DNS-palvelimella, voit käyttää skannerin IP-osoitteen sijasta sen nimeä.

### **Liittyvät tiedot**

- ➔ [”SSL/TLS-suojattu tiedonsiirto ja skannerin käyttö” sivulla 63](#)
- ➔ [”Tietoja digitaalisesta varmennuksesta” sivulla 63](#)

---

## Skannaustoimintojen käyttäminen

Asenna seuraavat ohjelmistot ja määritä asetukset skannerin käyttötavan mukaan.

**Skannaaminen tietokoneesta**

- Varmista Web Config -hallintasivulta, että verkkoskannauspalvelu on käytössä (tehdasmääritetty).
- Epson Scan 2 -sovelluksen asentaminen tietokoneeseen ja IP-osoitteen määrittäminen
- Jos skannauksessa halutaan käyttää esimääritettyjä töitä, asenna Document Capture Pro (Document Capture) ja määritä työn asetukset.

**Skannaaminen ohjauspaneelista**

- Jos käytössä on Document Capture Pro tai Document Capture Pro Server:  
Asenna Document Capture Pro tai Document Capture Pro Server  
DCP-asetus (palvelin- tai asiakastila).
- Jos WSD-protokolla on käytössä:  
Tarkista Web Config -hallintanäytöstä että WSD-asetukset (tehdasmääritetty) ovat oikein  
Laitekohtaiset lisäasetukset (Windows-tietokoneet).

## Skannaus tietokoneelta

Asenna ohjelmisto ja tarkista, että verkkoskannauspalvelu on käytössä, jos haluat mahdollistaa verkkoskannauksen.

### **Liittyvät tiedot**

- ➔ [”Asennettavat ohjelmistot” sivulla 25](#)
- ➔ [”Verkkoskannauksen ottaminen käyttöön” sivulla 25](#)



## Toimintojen asetukset

### Asennettavat ohjelmistot

#### Epson Scan 2

Tämä on skannerin laiteohjain. Jos käytät laitetta tietokoneella, asenna ohjain jokaiseen tietokoneeseen, josta laitetta käytetään. Jos Document Capture Pro tai Document Capture on asennettuna, voit käyttää laitteen painikkeisiin määritettyjä toimintoja.

Jos EpsonNet SetupManager on asennettuna, tulostinohjaimet voidaan jaella yhteen pakattuina paketteina.

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

Ohjelma asennetaan asiakaskoneeseen. Voit hakea ja suorittaa laitteeseen Document Capture Pro- tai Document Capture -sovelluksella tietokoneella tallennettuja töitä skannerin ohjauspaneelistä.

Voit myös skannata tietokoneella verkon kautta. Skannaaminen edellyttää Epson Scan 2 -ohjelmistoa.

### Liittyvät tiedot

➔ ”EpsonNet SetupManager” sivulla 56

### Määritä skannerin IP-osoite Epson Scan 2 -sovellukseen


Määritä skannerille IP-osoite, jotta skanneria voidaan käyttää verkossa.

1. Käynnistä **Epson Scan 2 Utility** valitsemalla **Start > Kaikki ohjelmat > EPSON > Epson Scan 2**.

Jos jokin toinen skanneri on jo tallennettuna, siirry kohtaan 2.

Jos mitään laitetta ei ole tallennettu, siirry kohtaan 4.

2. Valitse **Skanneri**-kohdassa ▼.
3. Valitse **Asetukset**.
4. Valitse **Ota muokkaus käyttöön** ja valitse sitten **Lisää**.
5. Valitse skannerin mallinimi **Malli**-kohdassa.
6. Valitse skannerin IP-osoite kohdassa **Hae verkkoa > Osoite**.

Valitse  ja päivitä luettelo valitsemalla . Jos skannerin IP-osoitetta ei löydy, valitse **Syötä osoite** ja kirjoita IP-osoite.

7. Valitse **Lisää**.
8. Valitse **OK**.

### Verkkoskannauksen ottaminen käyttöön

Verkkoskannauksen avulla voit skannata verkkoon kytketyn skannerin kautta. Verkkoskannaus on oletusarvoisesti käytössä.

1. Avaa Web Config -hallintasivu ja valitse **Services > Network Scan**.

## Toimintojen asetukset

2. Varmista, että **Enable scanning** on valittuna **EPSON Scan** -kohdassa.  
Jos asetus on valittuna, tämä vaihe on valmis. Sulje hallintasivu.  
Jos asetuksen valinta on poistettu, valitse asetus ja siirry seuraavaan vaiheeseen.
3. Valitse **Next**.
4. Valitse **OK**.  
Verkkoyhteys muodostetaan uudelleen ja asetukset tulevat voimaan.

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Skannaaminen ohjauspaneelistä

Skannaamista kansioon ja skannaamista sähköpostiin käytetään skannerin ohjauspaneelistä. Skannatut tiedostot voidaan siirtää sähköpostiin, kansioihin ja muihin kohteisiin suorittamalla haluttu tehtävä tietokoneen kautta.

Voit siirtää skannatut tiedostot määrittämällä työn Document Capture Pro Server- tai Document Capture Pro -sovelluksessa.

Lisätietoja töiden määrittämisestä on Document Capture Pro Server- ja Document Capture Pro -sovellusten ohjeissa.

### Liittyvät tiedot

➔ ”Document Capture Pro Server- ja Document Capture Pro -asetukset” sivulla 26

➔ ”Palvelinten ja kansioden asetukset” sivulla 27

## Tietokoneeseen asennettavat ohjelmistot

### Document Capture Pro Server

Tämä on Document Capture Pro -ohjelmiston palvelinversio. Ohjelma asennetaan Windows-palvelimeen. Palvelimen kautta voidaan hallita keskitetysti useita laitteita ja töitä. Töitä voidaan suorittaa samanaikaisesti useista skannereista.

Käyttämällä Document Capture Pro Server -ohjelmiston varmennettua versiota voit hallita myös käyttäjien ja ryhmien työ- ja skannaushistoriaa.

Voit pyytää lisätietoja Document Capture Pro Server -ohjelmistosta lähimmältä Epson-edustajalta.

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

Voit suorittaa skannaustöitä samalla tavalla kuin tietokoneella valitsemalla ja suorittamalla tietokoneella tallennetun työn ohjauspaneelistä. Tietokoneella tallennettuja töitä ei voi suorittaa samanaikaisesti useista skannereista.

## Document Capture Pro Server- ja Document Capture Pro -asetukset

Määritä skannaustoiminnon asetukset skannerin ohjauspaneelistä.

1. Avaa Web Config ja valitse **Services > Document Capture Pro**.

## Toimintojen asetukset

### 2. Valitse **Toimintatila**.

Server Mode:

Valitse tämä, jos käytössä on Document Capture Pro Server tai jos Document Capture Pro on käytössä vain määrättyyn tietokoneeseen määritetyissä töissä.

Client Mode:

Valitse tämä, jos työasetukseksi on valittu Document Capture Pro (Document Capture) -sovelluksen asennus verkon asiakaskoneisiin mutta tietokonetta ei ole määritetty.

### 3. Määritä seuraavat asetukset valittuna olevan tilan mukaisesti.

Server Mode:

Määritä **Server Address** -kohdassa sen palvelimen osoite, johon Document Capture Pro Server on asennettu. Arvon pituus on 2–252 merkkiä, ja se annetaan IPv4-, IPv6- tai FQDN-muodossa tai isäntänimenä. FQDN-muodossa voidaan käyttää US-ASCII-kirjaimia, numeroja, aakkosmerkkejä ja tavuviivaa (paitsi alussa ja/tai lopussa).

Client Mode:

Määritä **Group Settings**, jos haluat käyttää Document Capture Pro (Document Capture) -sovelluksessa määritettyä skanneriryhmää.

### 4. Valitse **Asetukset**.

## Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Palvelinten ja kansioden asetukset

Document Capture Pro ja Document Capture Pro Server tallentavat skannatut tiedostot palvelimeen tai asiakaskoneeseen ja siirtävät tiedoston kansioon tai sähköpostiin siirtotoiminnolla.

Käyttäjällä on oltava riittävät käyttöoikeudet ja määrittäykset tiedostojen siirtämiseen tietokoneesta, johon Document Capture Pro tai Document Capture Pro Server on asennettuna, kohdekoneeseen tai pilvipalveluun.

Määritä käytettävän toiminnon asetukset seuraavasti.

Voit määrittää toimintojen asetukset Document Capture Pro- tai Document Capture Pro Server -sovelluksessa. Lisätietoja asetuksista on Document Capture Pro Server- ja Document Capture Pro -sovellusten ohjeissa.

Nimi	Asetus	Edellytys
Skannaus verkkokansioon (SMB)	Tallennuskansion luominen ja jakaminen	Järjestelmänvalvojan tunnus tietokoneeseen, johon tallennuskansio luodaan.
	Verkkoskannauskansio (SMB)	Käyttäjätunnus ja salasana tietokoneeseen, jossa tallennuskansio on, sekä oikeus kansion sisällön päivittämiseen.
Skannaus verkkokansioon (FTP)	FTP-palvelimen kirjautumistiedot	Kirjautumistiedot FTP-palvelimeen ja oikeus kansion sisällön päivittämiseen.
Skannaus sähköpostiin	Sähköpostipalvelimen asetukset	Sähköpostipalvelimen asetustiedot

## Toimintojen asetukset

Nimi	Asetus	Edellytys
Skannaus Document Capture Pro -sovellukseen (jos Document Capture Pro Server on käytössä)	Pilvipalvelujen kirjausasetusten määrittäminen	Internet-ympäristö Pilvipalvelujen käyttäjätunnusten määrittäminen

### Skannaus WSD-toiminnolla (vain Windows)

Jos tietokoneessa on Windows Vista tai uudempi, voit skannata WSD-toiminnolla.

WSD-protokollan ollessa käytössä **Tietokone (WSD)** -valikko näkyy skannerin ohjauspaneelissa.

1. Avaa Web Config ja valitse **Services > Protocol**.
2. Varmista, että **Enable WSD** on valittuna **WSD Settings** -kohdassa.  
Jos valinta on valittuna, asetukset ovat valmiit ja voit sulkea Web Config -toiminnon.  
Jos valinta ei ole valittuna, valitse se ja siirry seuraavaan kohtaan.
3. Napsauta **Next**-painiketta.
4. Vahvista asetukset ja valitse sitten **Asetukset**.



---

## Järjestelmäasetusten määrittäminen

### Järjestelmän asetusten määrittäminen ohjauspaneelista

#### Näytön kirkkauden asettaminen

Voit asettaa näytön kirkkauden.

1. Valitse aloitusnäytössä **Asetukset**.
2. Valitse **Yleiset asetukset > LCD-kirkkaus**.
3. Säädä kirkkautta valitsemalla  tai .  
Voit valita kirkkauden väliltä 1–9.
4. Valitse **OK**.

#### Merkkiäänten valinta

Voit valita ohjauspaneelin näppäinään ja laitteen virhemerkkiään.

1. Valitse aloitusnäytössä **Asetukset**.

## Toimintojen asetukset

2. Valitse **Yleiset asetukset > Ääni**.
3. Määritä halutut asetukset.
  - Näppäinääni  
Valitse ohjauspaneelin näppäinäänen voimakkuus.
  - Virhemerkkiääni  
Valitse virhemerkkiäänen voimakkuus.
4. Valitse **OK**.

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Alkuperäiskappaleen kaksoissyötön tunnistus

Määrittää skannattavan alkuperäiskappaleen kaksoissyötön tunnistuksen. Skannaus keskeytetään, jos laite havaitsee kaksoissyötön.

Jos haluat skannata alkuperäiskappaleita, jotka laite tunnistaa kaksoissyötöksi, kuten kirjekuoria tai papereita, joissa on tarroja, poista toiminto käytöstä.

### **Huomautus:**

*Asetus voidaan määrittää myös Web Config -hallintasivulla ja Epson Scan 2 -sovelluksessa.*

1. Valitse aloitusnäytössä **Asetukset**.
2. Valitse **Ulkoiset Hakuasetukset > Ultraäänitunnistus 2x-nopeudella**.
3. Voit ottaa toiminnon käyttöön ja poistaa sen käytöstä valitsemalla **Ultraäänitunnistus 2x-nopeudella**.
4. Valitse **Sulje**.

## Hidastilan valinta

Paperitukosten estämiseksi voit asettaa laitteen skannaamaan hitaasti esimerkiksi ohuita sivuja skannattaessa.

1. Valitse aloitusnäytössä **Asetukset**.
2. Valitse **Ulkoiset Hakuasetukset > Hidas**.
3. Voit ottaa toiminnon käyttöön ja poistaa sen käytöstä valitsemalla **Hidas**.
4. Valitse **Sulje**.

## Järjestelmän asetusten määrittäminen Web Config -hallintasivun kautta

### Virransäästöasetukset laitteen ollessa käyttämättä

Voit määrittää virransäästöasetuksen, jota käytetään, kun skanneri on käyttämättä. Määritä sopiva aika käyttöympäristön mukaan.

**Huomautus:**

*Voit määrittää virransäästöasetukset myös skannerin ohjauspaneelistä.*

1. Avaa Web Config ja valitse **System Settings > Power Saving**.
2. Määritä **Sleep Timer** -kohtaan aika, jonka jälkeen laite siirtyy virransäästötilaan, mikäli laitetta ei käytetä. Voit määrittää ajan minuutin tarkkuudella. Enimmäisaika on 240 minuuttia.
3. **Power Off Timer** -asetuksen avulla voit määrittää laitteelle sammumisajan.
4. Valitse **OK**.

#### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

### Ohjauspaneelin asetukset

Skannerin ohjauspaneelin asetusten määrittäminen. Voit määrittää asetukset seuraavasti.

1. Avaa Web Config ja valitse **System Settings > Control Panel**.
2. Määritä halutut asetukset.
  - Language  
Valitse ohjauspaneelin näyttökieli.
  - Panel Lock  
Jos **ON** on valittuna, järjestelmänvalvojan toiminnot on avattava järjestelmänvalvojan salasanalla ennen asetusten määrittämistä. Jos järjestelmänvalvojan salasanaa ei ole asetettu, ohjauspaneelia ei lukita.
  - Operation Timeout  
Jos **ON** on valittuna, järjestelmä kirjaa järjestelmänvalvojana kirjautuneen käyttäjän automaattisesti ulos ja palaa aloitusnäyttöön, mikäli ohjauspaneeli on käyttämättä määrätyn ajan.  
Voit määrittää uloskirjausajan väliltä 10 sekuntia – 240 minuuttia.
3. Valitse **OK**.

#### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Toimintojen asetukset

### Ulkoisten liitännöiden käytön rajoittaminen

Voit estää tietokoneen USB-liitännän käytön. Valitse asetus, jos haluat estää skannauksen muualta kuin verkosta.

1. Avaa Web Config ja valitse **System Settings > External Interface**.
2. Valitse **Enable** tai **Disable**.  
Ota rajoitus käyttöön valitsemalla **Disable**.
3. Valitse **OK**.

### Laitteen päivämäärän ja kellonajan synkronointi palvelimen kanssa

Voit välttää useimmat kellonaikaan liittyvät ongelmat käyttämällä CA-varmennetta.

1. Avaa Web Config -toiminto ja valitse **System Settings > Date and Time > Time Server**.
2. Valitse **Use Time Server** -kohdassa **Use**.
3. Kirjoita kellonaikapalvelimen osoite **Time Server Address** -kohtaan.  
Voit käyttää IPv4-, IPv6- tai FQDN-muotoa. Enimmäispituus on 252 merkkiä. Jos et halua määrittää asetusta, jätä se tyhjäksi.
4. Syötä **Update Interval (min)**.  
Voit määrittää synkronointivälin minuutin tarkkuudella. Enimmäispituus on 10 800 minuuttia.
5. Valitse **OK**.

**Huomautus:**

*Time Server Status* -kohdan avulla voit tarkistaa, että yhteys kellonaikapalvelimeen toimii.

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

# Tietoturvan perusasetukset

Tässä luvussa kuvataan tietoturvaan liittyvät perusasetukset, jotka eivät edellytä erityistä käyttöympäristöä.

## Yleistietoja tietoturvan perusasetuksista

Tässä kohdassa esitellään Epson-laitteiden suojausasetukset.

Ominaisuuden nimi	Ominaisuuden tyyppi	Mitä asetetaan	Mitä estetään
Järjestelmänvalvojan salasana	Voit lukita järjestelmäasetukset, kuten verkkoyhteyksiä ja USB-liitäntöjä koskevat asetukset. Tällöin vain järjestelmänvalvoja voi muuttaa asetuksia.	Järjestelmänvalvoja määrittää laitteelle salasanan.  Asetuksia voidaan määrittää ja päivittää Web Config -hallintasivulla, ohjauspaneelista, Epson Device Admin -toiminnolla ja EpsonNet Config -toiminnolla.	Estää laitteeseen tallennettujen tietojen, kuten tunnusten, salasanojen, verkkoasetusten ja yhteystietojen, luvattoman lukemisen ja muuttamisen. Estää lisäksi useita tietoturvariskejä, kuten verkkoympäristöä ja tietoturvakäytäntöjä koskevien tietojen vuotamisen.
SSL/TLS-tiedonsiirto	Tiedonsiirto salataan SSL/TLS-suojauksella, kun laitteen palveluja käytetään Internet-yhteyden välityksellä, esimerkiksi toimintoja verkkoselaimella käytettäessä tai laiteohjelmistoa päivitettäessä.	Hanki varmennemyöntäjän allekirjoittama varmenne ja lataa se skanneriin.	Laitetunnuksen vahvistaminen CA-varmenteella estää laitteeksi tekeytymisen verkossa ja laitteen luvattoman käytön. Tietoliikenteen salaaminen SSL/TLS-salauksella estää tulostettavien tietojen ja laiteasetusten vuotamisen.
Hallintaprotokollat	Hallintaprotokollia käytetään laitteiden ja tietokoneiden välisessä tiedonsiirrossa sekä toimintojen määrittämisessä käyttöön ja pois käytöstä.	Protokolla tai palvelu, jonka avulla toimintoja hallitaan yksitellen.	Vähentää toimintojen vahingossa tapahtuvan käytön aiheuttamia tietoturvariskejä tarpeettomien toimintojen poistamisen kautta.

### Liittyvät tiedot

- ➔ ”Tietoja Web Config -sovelluksesta” sivulla 22
- ➔ ”EpsonNet Config” sivulla 55
- ➔ ”Epson Device Admin” sivulla 55
- ➔ ”Järjestelmänvalvojan salasanan määrittäminen” sivulla 33
- ➔ ”Ohjausprotokollat” sivulla 35



---

## Järjestelmänvalvojan salasanan määrittäminen

Jos järjestelmänvalvojan salasana on määritetty, vain järjestelmänvalvoja voi muuttaa järjestelmänvalvojan määritettäviä asetuksia. Voit asettaa järjestelmänvalvojan salasanan ja muuttaa sitä Web Config -toiminnolla, skannerin ohjauspaneelin kautta tai ohjelmallisesti (Epson Device Admin tai EpsonNet Config). Voit lukea lisätietoja ohjelmista kunkin sovelluksen käyttöohjeesta.

### Liittyvät tiedot

- ➔ ”Järjestelmänvalvojan salasanan määrittäminen ohjauspaneelistä” sivulla 33
- ➔ ”Järjestelmänvalvojan salasanan määrittäminen Web Config -toiminnolla” sivulla 33
- ➔ ”EpsonNet Config” sivulla 55
- ➔ ”Epson Device Admin” sivulla 55

## Järjestelmänvalvojan salasanan määrittäminen ohjauspaneelistä

Voit määrittää järjestelmänvalvojan salasanan skannerin ohjauspaneelistä.

1. Valitse aloitusnäytössä **Asetukset**.
2. Valitse **Järjestelmän hallinta > Järjestelmänvalv. asetukset**.  
Jos valittava kohde ei ole näkyvässä, pyyhkäise ruutua ylöspäin.
3. Valitse **Järj.valvojan salasana > Rekisteröi**.
4. Kirjoita uusi salasana ja valitse **OK**.
5. Kirjoita salasana uudestaan ja valitse **OK**.
6. Valitse vahvistusnäytössä **OK**.  
Järjestelmänvalvojan asetusnäyttö tulee näkyviin.
7. Valitse **Lukkoasetus** ja valitse vahvistusnäytössä **OK**.  
Lukkoasetus -asetukseksi on valittu **Pääl.**. Valikon lukittuja kohteita voi käyttää vain kirjoittamalla pääkäyttäjän salasanan.

### Huomautus:

- Jos valitset **Asetukset > Yleiset asetukset > Toiminnan aikakatkaisu** -asetuksen arvoksi **Pääl.**, skanneri kirjaa käyttäjän ulos, jos ohjauspaneeli on käyttämättä tietyn ajan.
- Voit vaihtaa järjestelmänvalvojan salasanan tai poistaa sen valitsemalla **Järj.valvojan salasana** -näytössä **Muuttaa** tai **Nollaa** ja kirjoittamalla järjestelmänvalvojan salasanan.

## Järjestelmänvalvojan salasanan määrittäminen Web Config -toiminnolla

Voit määrittää järjestelmänvalvojan salasanan Web Config -toiminnolla.

1. Avaa Web Config ja valitse **Administrator Settings > Change Administrator Authentication Information**.

## Tietoturvan perusasetukset

2. Kirjoita salasana kohtaan **New Password** ja **Confirm New Password**. Tarvittaessa kirjoita käyttäjätunnus.  
Jos haluat vaihtaa salasanan uuteen, anna nykyinen salasana.

3. Valitse **OK**.

**Huomautus:**

- Jos haluat asettaa tai muuttaa valikon lukittuja kohtia, valitse **Administrator Login** ja kirjoita järjestelmänvalvojan salasana.
- Jos haluat poistaa järjestelmänvalvojan salasanan, valitse **Administrator Settings > Delete Administrator Authentication Information** ja kirjoita järjestelmänvalvojan salasana.

**Liittyvät tiedot**

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Järjestelmänvalvojan salasanalla lukittavat asetukset

Järjestelmänvalvoja voi muuttaa laitteen kaikkien toimintojen asetuksia.

Jos määrität laitteeseen järjestelmänvalvojan salasanan, voit lukita laitteen siten, ettei laitehallintaan liittyviä asetuksia voi muuttaa.

Seuraavat asetukset ovat järjestelmänvalvojan hallittavia asetuksia.

Asetus	Kuvaus
Skannausasetukset	Kaksoissyötön tunnistuksen ja hidastilan määrittäminen.
Kaapelilähiverkon (Ethernet) asetukset	Laitteiden nimien ja IP-osoitteiden hallinta, DNS-palvelimen ja välityspalvelimen asetukset ja verkkoyhteyksiin liittyvien asetusten muuttaminen.

## Tietoturvan perusasetukset

Asetus	Kuvaus
Verkkopalveluasetukset	Verkkoprotokolliin liittyvät asetukset sekä verkkoskannaukseen ja Document Capture Pro -sovelluksen palveluihin liittyvät asetukset.
Sähköpostipalvelimen asetukset	Laitteiden käyttämän sähköpostipalvelimen asetukset.
Suojausasetukset	Verkon suojausasetukset, kuten SSL/TLS-suojattu tiedonsiirto, IPsec-suojaus ja IP-osoitteiden suodatus sekä IEEE802.1X-suojaus.
Päävarmenteen päivittäminen	Document Capture Pro Server -todennuksessa ja laiteohjelmistoa Web Config -hallintasivun kautta päivitettäessä vaadittavan päävarmenteen päivitys.
Laiteohjelmiston päivitys	Laitteiden laiteohjelmistojen versiotietojen tarkastelu ja ohjelmistojen päivitys.
Kellonaika ja ajastin	Lepotilaansiirtymisaika, automaattinen virran katkaisu, päivämäärä ja kellonaika, sulku aika ja muut ajastetut toiminnot.
Oletusarvojen palautus	Skannerin asetusten palautus tehdasasetuksiin.
Järjestelmänvalvojan asetus	Järjestelmänvalvojan lukituksen ja salasanan määrittäminen.
Laitevarmennusasetus	Todennuslaitteen tunnus. Määritetään käyttöön, jos skanneria käytetään todennuslaitteita tukevassa ympäristössä.

## Ohjausprotokollat

Voit skannata käyttämällä erilaisia toimintatapoja ja protokollia. Voit esimerkiksi käyttää verkkoskannausta vapaavalintaisesta määrästä verkkoon liitettyjä tietokoneita. Voit myös rajoittaa skannausten tiettyihin protokollisiin ja kohteisiin. Voit vähentää tahattomia turvallisuusvaaroja rajoittamalla hakua määrättyistä kohteista tai ohjaamalla käytettävissä olevia toimintoja.

Määrittää protokolla-asetukset.

1. Avaa Web Config ja valitse **Services > Protocol**.
2. Määritä kaikki kohteet.
3. Valitse **Next**.
4. Valitse **OK**.

Asetukset on otettu käyttöön skannerissa.

### Liittyvät tiedot

- ➔ ["Web Config -ohjelmiston käyttö" sivulla 23](#)
- ➔ ["Protokollat, jotka voidaan määrittää käyttöön tai pois käytöstä" sivulla 36](#)
- ➔ ["Protokolla-asetukset" sivulla 37](#)

## Tietoturvan perusasetukset

## Protokollat, jotka voidaan määrittää käyttöön tai pois käytöstä

Protokolla	Kuvaus
Bonjour Settings	Voit määrittää, käytätkö Bonjour-protokollaa. Bonjour-protokollaa käytetään laitteiden hakemiseen, skannaamiseen ja muihin toimintoihin.
SLP Settings	Voit ottaa SLP-toiminnon käyttöön tai pois käytöstä. SLP-toimintoa käytetään Epson Scan 2 -sovelluksessa ja EpsonNet Config. -toiminnon verkkohaussa.
WSD Settings	Voit ottaa WSD-toiminnon käyttöön tai poistaa sen käytöstä. Jos toiminto on käytössä, voit lisätä WSD-laitteita ja skannata WSD-portista.
LLTD Settings	Voit ottaa LLTD-toiminnon käyttöön tai pois käytöstä. Jos tämä toiminto on käytössä, laite näkyy Windows-verkkokartassa.
LLMNR Settings	Voit ottaa LLMNR-toiminnon käyttöön tai pois käytöstä. Jos tämä toiminto on käytössä, voit käyttää nimenselvitystä ilman NetBIOS-ominaisuutta, vaikka et voisi käyttää DNS:ää.
SNMPv1/v2c Settings	Voit määrittää, otetaanko SNMPv1/v2c-tila käyttöön. Tätä käytetään laitteiden asettamiseen, valvontaan jne.
SNMPv3 Settings	Voit määrittää, otetaanko SNMPv3-tila käyttöön. Tätä käytetään salattujen laitteiden asettamiseen, valvontaan jne.

## Liittyvät tiedot

- ➔ ”Ohjausprotokollat” sivulla 35
- ➔ ”Protokolla-asetukset” sivulla 37

## Protokolla-asetukset

The screenshot shows the 'Services > Protocol' configuration page in the EPSON network utility. The left sidebar contains navigation links such as 'Administrator Logout', 'Status', 'Product Status', 'Network Status', 'Panel Snapshot', 'Maintenance', 'Hardware Status', 'Scanner Settings', 'Network Settings', 'Network Security Settings', 'Services', 'System Settings', 'Export and Import Setting Value', 'Administrator Settings', and 'Basic Settings' (including DNS/Proxy Setup, Firmware Update, Root Certificate Update, and Product Status).

The main content area is titled 'Services > Protocol' and includes a note: 'Note: If you need to change the Device Name used on each protocol and the Bonjour Name, change the Device Name in the Network Settings. If you need to change the Location used on each protocol, change it in the Network Settings.'

The configuration sections are as follows:

- Bonjour Settings:**
  - Use Bonjour
  - Bonjour Name: EPSON884045.local
  - Bonjour Service Name: EPSON
  - Location: (empty)
- SLP Settings:**
  - Enable SLP
- WSD Settings:**
  - Enable WSD
  - Scanning Timeout (sec): 300
  - Device Name: EPSON
  - Location: (empty)
- LLTD Settings:**
  - Enable LLTD
  - Device Name: EPSON
- LLMNR Settings:**
  - Enable LLMNR
- SNMPv1/v2c Settings:**
  - Enable SNMPv1/v2c
  - Access Authority: Read/Write
  - Community Name (Read Only): public
  - Community Name (Read/Write): (empty)
- SNMPv3 Settings:**
  - Enable SNMPv3
  - User Name: admin
  - Authentication Settings:**
    - Algorithm: MD5
    - Password: (empty)
    - Confirm Password: (empty)
  - Encryption Settings:**
    - Algorithm: DES
    - Password: (empty)
    - Confirm Password: (empty)
- Context Name: EPSON

A 'Next' button is located at the bottom of the configuration area.

Asetus	Asetusarvo ja kuvaus
Bonjour Settings	

## Tietoturvan perusasetukset

Asetus	Asetusarvo ja kuvaus
Use Bonjour	Valitse tämä, jos haluat etsiä tai käyttää laitteita Bonjour-protokollalla.
Bonjour Name	Näyttää Bonjour-nimen.
Bonjour Service Name	Voit tuoda Bonjour-palvelunimen näkyviin ja asettaa nimen.
Location	Näyttää Bonjour-sijaintinimen.
SLP Settings	
Enable SLP	Valitse tämä, jos haluat ottaa käyttöön SLP-toiminnon. Toimintoa käytetään laitteiden verkkohakuun Epson Scan 2- ja EpsonNet Config -sovelluksissa.
WSD Settings	
Enable WSD	Valitse tämä, jos haluat ottaa käyttöön laitteiden lisäämisen WSD-toiminnolla tai skannauksen WSD-portista.
Scanning Timeout (sec)	Syötä tiedonsiirron aikakatkaisu-arvo WSD-skannaukselle väliltä 3–3600 sekuntia.
Device Name	Näyttää WSD-laitenimen.
Location	Näyttää WSD-sijaintinimen.
LLTD Settings	
Enable LLTD	Valitse tämä, jos haluat ottaa käyttöön LLTD-toiminnon. Skanneri näkyy Windows-verkkokartassa.
Device Name	Näyttää LLTD-laitenimen.
LLMNR Settings	
Enable LLMNR	Valitse tämä, jos haluat ottaa käyttöön LLMNR-toiminnon. Voit käyttää nimenselvitystä ilman NetBIOS-toimintoa, vaikka et voisi käyttää DNS:ää.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Valitse tämä, jos haluat ottaa käyttöön SNMPv1/v2c-toiminnon. Vain skannerit, jotka tukevat SNMPv3-protokollaa, näkyvät näytössä.
Access Authority	Aseta käyttöoikeus, jos SNMPv1/v2c on otettu käyttöön. Valitse <b>Read Only</b> tai <b>Read/Write</b> .
Community Name (Read Only)	Syötä 0–32 ASCII (0x20–0x7E) -merkkiä.
Community Name (Read/Write)	Syötä 0–32 ASCII (0x20–0x7E) -merkkiä.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 on käytössä, kun ruutu on valittuna.
User Name	Syötä 1–32 merkkiä käyttämällä yksitavuisia merkkejä.
Authentication Settings	
Algorithm	Valitse SNMPv3-todennuksessa käytettävä algoritmi.

## Tietoturvan perusasetukset

Asetus	Asetusarvo ja kuvaus
Password	Valitse SNMPv3-todennuksessa käytettävä salasana. Syötä 8–32 merkkiä ASCII-muodossa (0x20–0x7E). Jos et halua määrittää asetusta, jätä se tyhjäksi.
Confirm Password	Anna salasana, jonka määritit vahvistusta varten.
Encryption Settings	
Algorithm	Valitse SNMPv3.-salauksessa käytettävä algoritmi.
Password	Valitse SNMPv3-salauksessa käytettävä salasana. Syötä 8–32 merkkiä ASCII-muodossa (0x20–0x7E). Jos et halua määrittää asetusta, jätä se tyhjäksi.
Confirm Password	Anna salasana, jonka määritit vahvistusta varten.
Context Name	Enimmäispituus on 32 merkkiä. Käytettävä merkistö on Unicode (UTF-8). Jos et halua määrittää asetusta, jätä se tyhjäksi. Merkkien enimmäismäärä vaihtelee kielen mukaan.

## Liittyvät tiedot

➔ ”Ohjausprotokollat” sivulla 35

➔ ”Protokollat, jotka voidaan määrittää käyttöön tai pois käytöstä” sivulla 36

# Käyttö- ja hallinta-asetukset

Tässä luvussa kuvataan laitteiden päivittäiseen käyttöön ja hallintaan liittyvät asiat.

---

## Laitteen tietojen tarkistaminen

Voit tarkistaa käytössä olevan laitteen tiedot valitsemalla Web Config -toiminnossa **Status**.

Product Status

Näet tällöin laitteen kieliasetuksen, tilan, laitenumeron, MAC-osoitteen ja muita tietoja.

Network Status

Voit myös esimerkiksi tarkistaa verkkoyhteyden tilan sekä IP-osoitteen ja DNS-palvelimen osoitteen.

Panel Snapshot

Voit myös tarkastella näyttökuvaa laitteen ohjauspaneelista.

Maintenance

Näet aloituspäivämäärän, skannaustiedot ja muita tietoja.

Hardware Status

Näet skannerin tilatiedon.

### Liittyvät tiedot

➔ [”Web Config -ohjelmiston käyttö” sivulla 23](#)

---

## Laitteiden hallinta (Epson Device Admin)

Voit hallita ja käyttää useita laitteita Epson Device Admin -toiminnon avulla. Epson Device Admin mahdollistaa myös eri verkoissa olevien laitteiden hallinnan. Tärkeimmät hallintatoiminnot kuvataan seuraavassa.

Lisätietoja toiminnoista ja ohjelmiston käytöstä on ohjelmistojen käyttöoppaissa sekä Epson Device Admin -toiminnon ohjeessa.

Laitteiden etsintä

Voit etsiä verkossa olevat laitteet ja tallentaa tiedot luetteloksi. Jos Epson-laitteita, kuten tulostimia ja skannereita, on kytketty samaan verkon segmenttiin järjestelmänvalvojan tietokoneen kanssa, laitteet voidaan löytää verkosta vaikka niille ei olisi määritetty IP-osoitetta.

Voit myös etsiä laitteita, jotka on liitetty verkkoon kytkettyihin tietokoneisiin USB-kaapelilla. Tietokoneissa on tällöin oltava asennettuna Epson Device USB Agent -ohjelma.

Laiteasetusten määrittäminen

Voit luoda asetussmallin käytettävistä asetuksista, kuten verkkoliitännästä ja paperikoosta, ja jakaa asetukset muihin laitteisiin asetussmallin avulla. Voit myös määrittää IP-osoitteen laitteeseen, jolle ei ole määritetty IP-osoitetta.



## Käyttö- ja hallinta-asetukset

### Laitteiden valvonta

Voit hakea verkkoon kytkettyjen laitteiden tilatiedot ja muita tietoja haluttuina aikoina. Voit myös valvoa laitteita, jotka on kytketty verkkoon liitettyihin tietokoneisiin USB-kaapelilla, sekä valvoa muiden valmistajien laitteita, jotka on rekisteröity laiteluetteloon. USB-liitännän kautta kytkettyjen laitteiden valvonta edellyttää Epson Device USB Agent -ohjelmiston asentamista.

### Hälytysten hallinta

Voit seurata laitteiden tilatietoihin ja tarvikemääriin liittyviä hälytyksiä. Järjestelmä lähettää järjestelmänvalvojalle automaattisesti sähköposti-ilmoituksia määrättyjen ehtojen täytyessä.

### Raporttien hallinta

Voit määrittää järjestelmän keräämiin laitetietoihin ja tarvikemääriin perustuvia raportteja. Voit tallentaa raportit ja lähettää ne sähköpostitse.

### Liittyvät tiedot

➔ ["Epson Device Admin" sivulla 55](#)

---

## Tapahtumista ilmoittavien sähköpostien vastaanotto

### Tietoja sähköposti-ilmoituksista

Tämän ominaisuuden avulla voit vastaanottaa sähköposti-ilmoituksia tiettyjen tapahtumien yhteydessä. Voit rekisteröidä korkeintaan viisi sähköpostiosoitetta ja valita, mistä tapahtumista haluat saada ilmoituksia.

Toiminnon käyttäminen edellyttää myös, että sähköpostipalvelin on määritetty.

### Liittyvät tiedot

➔ ["Postipalvelimen määrittäminen" sivulla 42](#)

### Sähköposti-ilmoitusten määrittäminen

Ominaisuuden käyttö vaatii postipalvelimen määrittämisen.

1. Käytä Web Config -toimintoa ja valitse **Administrator Settings > Email Notification**.
2. Anna sähköpostiosoite, johon haluat saada sähköposti-ilmoituksia.
3. Valitse sähköposti-ilmoitusten kieli.

## Käyttö- ja hallinta-asetukset

4. Valitse niiden ilmoitusten ruudut, joita haluat vastaanottaa.

Administrator Settings > Email Notification

Set up the Email Server to enable the email notification.

Email Address Settings

Email in selected language will be sent to each address.

1 :	admin@aaa.com	English
2 :	aaa@aaa.com	English
3 :		English
4 :		English
5 :		English

Notification Settings

Email will be sent when product status is as checked.

	1	2	3	4	5
Administrator password changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scanner error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Restore Default Settings

5. Napsauta OK.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”Postipalvelimen määrittäminen” sivulla 42

## Postipalvelimen määrittäminen

Tarkista seuraava ennen määrittämistä.

- Skanneri on liitetty verkkoon.
- Tietokoneen sähköpostipalvelintiedot.

1. Käytä Web Config -toimintoa ja valitse **Network Settings > Email Server > Basic**.
2. Syötä arvo kullekin kohteelle.
3. Valitse **OK**.

Valitsemasi asetukset tulevat näyttöön.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”Postipalvelimen asetukset” sivulla 43

## Käyttö- ja hallinta-asetukset

### Postipalvelimen asetukset

The screenshot shows the Epson printer's web interface for configuring the Email Server. The left sidebar contains a navigation menu with options like Status, Contacts, User Default Settings, Access Control Settings, Printer Settings, Network Settings, Wi-Fi, Wired LAN, Basic, Email Server, LDAP Server, Network Security Settings, Services, System Settings, Export and Import Setting Value, Administrator Settings, Basic Settings, Epson Connect Services, and Google Cloud Print Services. The main area is titled 'Network Settings > Email Server > Basic'. It contains a warning about certificates, a dropdown for 'Authentication Method' (set to SMTP AUTH), text boxes for 'Authenticated Account', 'Authenticated Password', 'Sender's Email Address', 'SMTP Server Address', and 'SMTP Server Port Number' (set to 25). There is a 'Secure Connection' dropdown (set to None) and radio buttons for 'Certificate Validation' (Enable is selected). Below this is a warning message and text boxes for 'POP3 Server Address' and 'POP3 Server Port Number'. An 'OK' button is at the bottom.

Kohdat	Asetukset ja selitys
Authentication Method	Määritä todennusmenetelmä skannerin postipalvelimen käyttöä varten.
	Off Todennus ei ole käytettävissä postipalvelimen kanssa kommunikoitaessa.
	SMTP AUTH Vaatii, että postipalvelin tukee SMTP-todennusta.
	POP before SMTP Määritä POP3-palvelin, kun valitaan tämä menetelmä.
Authenticated Account	Jos valitset <b>SMTP AUTH:n</b> tai <b>POP before SMTP:n Authentication Method</b> -menetelmäksi, syötä varmennettu tilinimi, jossa on 0–255 ASCII-merkkiä (0x20–0x7E).
Authenticated Password	Jos valitset kohteen <b>SMTP AUTH</b> tai <b>POP before SMTP</b> kohdasta <b>Authentication Method</b> , anna todennettu salasana, jonka pituus on 0–20 merkkiä: A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Sender's Email Address	Syötä lähettäjän sähköpostiosoite. Syötä 0–255 merkkiä ASCII-muodossa (0x20–0x7E) paitsi : ( ) < > [ ] ; ¥. Piste "." ei voi olla ensimmäinen merkki.
SMTP Server Address	Syötä 0–255 merkkiä käyttämällä merkkejä A–Z, a–z, 0–9 . - . Voit käyttää IPv4- tai FQDN-muotoa.
SMTP Server Port Number	Syötä numero väliltä 1–65535.

## Käyttö- ja hallinta-asetukset

Kohdat	Asetukset ja selitys	
Secure Connection	Määritä sähköpostipalvelimelle suojattu yhteysmenetelmä.	
	None	Jos valitset <b>POP before SMTP</b> kohdassa <b>Authentication Method</b> , yhteysmenetelmäksi valitaan <b>None</b> .
	SSL/TLS	Tämä ominaisuus on käytössä, kun <b>Authentication Method</b> on asetettu tilaan <b>Off</b> tai <b>SMTP AUTH</b> .
	STARTTLS	Tämä ominaisuus on käytössä, kun <b>Authentication Method</b> on asetettu tilaan <b>Off</b> tai <b>SMTP AUTH</b> .
Certificate Validation	Sertifikaatti on vahvistettu, kun tämä ominaisuus on otettu käyttöön. On suositeltavaa asettaa tämä tilaan <b>Enable</b> .	
POP3 Server Address	Jos valitset kohteen <b>POP before SMTP</b> kohdasta <b>Authentication Method</b> , anna POP3-palvelimen osoite, jonka pituus on 0–255 merkkiä: A–Z a–z 0–9 . - . Voit käyttää IPv4- tai FQDN-muotoa.	
POP3 Server Port Number	Jos valitset kohteen <b>POP before SMTP</b> kohdasta <b>Authentication Method</b> , anna numero väliltä 1–65 535.	

### Liittyvät tiedot

➔ ”Postipalvelimen määrittäminen” sivulla 42

## Postipalvelimen yhteyden tarkistus

- Käytä Web Config -toimintoa ja valitse **Network Settings > Email Server > Connection Test**.
- Valitse **Start**.  
Sähköpostipalvelimen yhteystesti käynnistyy. Testin jälkeen näytetään tarkistusraportti.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”Postipalvelimen yhteystestin viitteet” sivulla 44

## Postipalvelimen yhteystestin viitteet

Viestit	Selitys
Connection test was successful.	Tämä viesti tulee esiin, kun yhteys palvelimeen toimii.
SMTP server communication error. Check the following. - Network Settings	Tämä viesti tulee näkyviin, kun <ul style="list-style-type: none"> <li><input type="checkbox"/> Skanneria ei ole liitetty verkkoon</li> <li><input type="checkbox"/> SMTP-palvelin on kaatunut</li> <li><input type="checkbox"/> Verkkoyhteys on katkennut tiedonsiirron aikana</li> <li><input type="checkbox"/> Vastaanotettu epätäydellisiä tietoja</li> </ul>

### Käyttö- ja hallinta-asetukset

Viestit	Selitys
POP3 server communication error. Check the following. - Network Settings	Tämä viesti tulee näkyviin, kun <ul style="list-style-type: none"> <li><input type="checkbox"/> Skanneria ei ole liitetty verkkoon</li> <li><input type="checkbox"/> POP3-palvelin on kaatunut</li> <li><input type="checkbox"/> Verkkoyhteys on katkennut tiedonsiirron aikana</li> <li><input type="checkbox"/> Vastaanotettu epätäydellisiä tietoja</li> </ul>
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Tämä viesti tulee näkyviin, kun <ul style="list-style-type: none"> <li><input type="checkbox"/> Liittäminen DNS-palvelimeen epäonnistui</li> <li><input type="checkbox"/> SMTP-palvelimen nimenselvitys epäonnistui</li> </ul>
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Tämä viesti tulee näkyviin, kun <ul style="list-style-type: none"> <li><input type="checkbox"/> Liittäminen DNS-palvelimeen epäonnistui</li> <li><input type="checkbox"/> POP3-palvelimen nimenselvitys epäonnistui</li> </ul>
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Tämä viesti tulee näkyviin, kun SMTP-palvelimen varmennus epäonnistuu.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Tämä viesti tulee näkyviin, kun POP3-palvelimen varmennus epäonnistuu.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Tämä viesti tulee näkyviin, kun yrität tiedonsiirtoa protokollalla, jota ei tueta.
Connection to SMTP server failed. Change Secure Connection to None.	Tämä viesti tulee näkyviin, kun ilmenee SMTP:n vastaamattomuus palvelimen ja asiakkaan välillä, tai kun palvelin ei tue suojattua SMTP-yhteyttä (SSL-yhteys).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Tämä viesti tulee näkyviin, kun ilmenee SMTP:n vastaamattomuus palvelimen ja asiakkaan välillä, tai kun palvelin vaatii SSL/TLS-yhteyden käyttöä suojatulla SMTP-yhteydellä.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Tämä viesti tulee näkyviin, kun ilmenee SMTP:n vastaamattomuus palvelimen ja asiakkaan välillä, tai kun palvelin vaatii STARTTLS-yhteyden käyttöä suojatulla SMTP-yhteydellä.
The connection is untrusted. Check the following. - Date and Time	Tämä viesti tulee näkyviin, kun skannerin päivämäärä- ja aika-asetus on väärä tai sertifikaatti on vanhentunut.
The connection is untrusted. Check the following. - CA Certificate	Tämä viesti tulee näkyviin, kun skannerilla ei ole palvelinta vastaavaa juurisertifikaattia tai CA Certificate -sertifikaattia ei ole tuotu.
The connection is not secured.	Tämä viesti tulee näkyviin, kun haettu sertifikaatti on vahingoittunut.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Tämä viesti tulee näkyviin, kun ilmenee varmennusmenetelmän vastaamattomuus palvelimen ja asiakkaan välillä. Palvelin tukee SMTP AUTH -varmennusta.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Tämä viesti tulee näkyviin, kun ilmenee varmennusmenetelmän vastaamattomuus palvelimen ja asiakkaan välillä. Palvelin ei tue SMTP AUTH -varmennusta.

## Käyttö- ja hallinta-asetukset

Viestit	Selitys
Sender's Email Address is incorrect. Change to the email address for your email service.	Tämä viesti tulee näkyviin, kun määritetyn lähettäjän sähköpostiosoite on väärä.
Cannot access the product until processing is complete.	Tämä viesti tulee esiin, kun skanneri on varattu.

### Liittyvät tiedot

➔ ”Postipalvelimen yhteyden tarkistus” sivulla 44

## Laiteohjelmiston päivittäminen

### Laiteohjelmiston päivittäminen Web Config -hallintasivun kautta

Päivittää laiteohjelmiston Web Config -toiminnon avulla. Laitteen on oltava kytkettynä Internetiin.

1. Avaa Web Config ja valitse **Basic Settings > Firmware Update**.

2. Valitse **Start**.

Laiteohjelmiston tarkistus alkaa, ja uuden laiteohjelmiston tiedot tulevat näkyviin, jos päivitys on saatavana.

3. Valitse **Start** ja noudata näytössä näkyviä ohjeita.

#### **Huomautus:**

Voit päivittää laiteohjelmiston myös *Epson Device Admin* -toiminnolla. Voit tarkistaa laiteohjelmiston tiedot laiteluettelosta. Toiminto on hyödyllinen erityisesti silloin, jos haluat päivittää useiden laitteiden laiteohjelmiston kerralla. Lisätietoja on *Epson Device Admin* -toiminnon oppaassa ja ohjetoiminnossa.

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

➔ ”Epson Device Admin” sivulla 55

### Laiteohjelmiston päivittäminen Epson Firmware Updater -ohjelman avulla

Voit ladata laiteohjelmiston Epsonin verkkosivustosta tietokoneeseen, liittää laitteen tietokoneeseen USB-kaapelilla ja päivittää laiteohjelmiston tietokoneen kautta. Jos et voi päivittää laiteohjelmistoa verkon kautta, kokeile tätä keinoa.

1. Lataa laiteohjelmisto Epsonin verkkosivustosta.

2. Kytke laiteohjelmiston sisältävä tietokone ja laite toisiinsa USB-kaapelilla.

3. Kaksoisnapsauta lataamaasi .exe-tiedostoa.

Epson Firmware Updater käynnistyy.

4. Noudata näytössä näkyviä ohjeita.

---

## Asetusten varmuuskopiointi

Voit kopioida asetukset toisiin skannereihin viemällä ne tiedostoon Web Config -hallintasivun avulla.

### Asetusten vieminen

Vie kaikki skanneriasetukset.

1. Käytä Web Config -toimintoa ja valitse sitten **Export and Import Setting Value > Export**.
2. Valitse vietävät asetukset.  
Valitse asetukset, jotka haluat viedä. Jos valitset pääluokan, myös alaluokat valitaan. Kuitenkin alaluokkia, jotka aiheuttavat virheitä kopioitumalla samassa verkossa (kuten IP-osoitteen jne.), ei voi kopioida.
3. Syötä salasana salataksesi viedyn tiedoston.  
Tarvitset salasanan tuodaksesi tiedoston. Jätä tämä tyhjäksi, jollet halua salata tiedostoa.
4. Napsauta **Export**.



**Tärkeää:**

*Jos haluat viedä skannerin verkkoasetukset, kuten skannerin nimen ja IP-osoitteen, valitse **Enable to select the individual settings of device** ja valitse lisää kohteita. Käytä ainoastaan valittuja arvoja vaihdettavassa skannerissa.*

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

### Asetusten tuominen

Tuo viety Web Config -tiedosto skanneriin.



**Tärkeää:**

*Tuotaessa arvoja, jotka sisältävä yksilöiviä tietoja, kuten skannerin nimen tai IP-osoitteen, varmista, ettei samaa IP-osoitetta ole samassa verkossa. Jos IP-osoitteet menevät päällekkäin, skanneri ei heijasta arvoa.*

1. Käytä Web Config -toimintoa ja valitse sitten **Export and Import Setting Value > Import**.
2. Valitse viety tiedosto ja syötä sitten salattu salasana.
3. Napsauta **Next**.
4. Valitse tuotavat asetukset ja napsauta sitten **Next**.
5. Napsauta **OK**.

## Käyttö- ja hallinta-asetukset

Asetukset on otettu käyttöön skannerissa.

### Liittyvät tiedot

➔ [”Web Config -ohjelmiston käyttö” sivulla 23](#)



# Ongelmien ratkaisu

---

## Vinkkejä ongelmanratkaisuun

Voit lukea lisätietoja seuraavasta oppaasta.

Käyttöopas

Sisältää ohjeita skannerin käyttöön, huoltoon ja vianmääritykseen.

---

## Palvelimen tai verkkoon liitetyn laitteen lokin tarkastaminen

Jos verkkoyhteydessä on ongelmia, syy voidaan joissakin tapauksissa selvittää tarkistamalla sähköpostipalvelimen, LDAP-palvelimen tai muun laitteen lokitiedot. Voit myös tarkistaa laitteen tilan verkkoon kytketyn laitteen järjestelmälokista tai käyttämällä esimerkiksi reitittimen laitekomentoja.

---

## Verkkoasetusten alustaminen

### Verkkoasetusten palauttaminen ohjauspaneelistä

Voit palauttaa kaikki verkkoasetukset oletusasetuksiin.

1. Valitse aloitusnäytössä **Asetukset**.
2. Valitse **Järjestelmän hallinta > Palauta oletusasetukset > Verkkoasetukset**.
3. Tarkista viesti ja valitse sitten **Kyllä**.
4. Kun valmis-viesti tulee näkyviin, valitse **Sulje**.

Jos et valitse **Sulje**, näyttö sammuu automaattisesti tietyn ajan kuluttua.

---

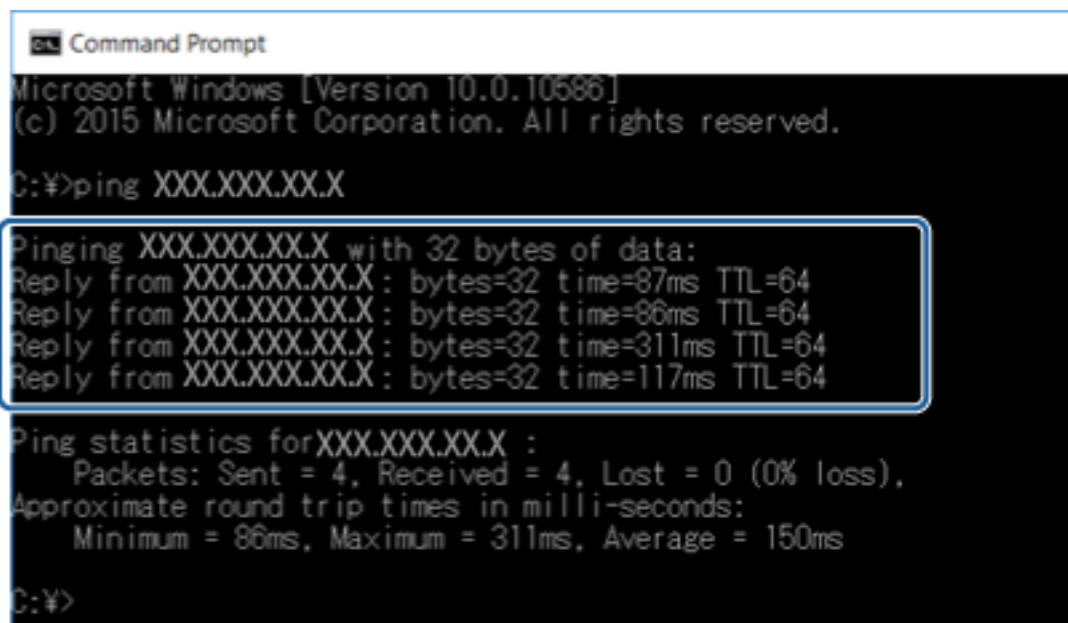
## Laitteiden ja tietokoneen välisen tiedonsiirron tarkastaminen

### Yhteyden tarkistaminen Ping-komennolla — Windows

Voit varmistaa Ping-komennon avulla, että tietokone on liitetty skanneriin. Tarkista yhteys Ping-komennon avulla alla olevien ohjeiden mukaisesti.

## Ongelmien ratkaisu

1. Tarkista skannerin IP-osoite yhteydelle, jonka haluat tarkistaa.  
Voit tarkistaa tämän Epson Scan 2 -sovelluksen avulla.
2. Näytä tietokoneen komentokehotenäyttö.
  - Windows 10  
Napsauta käynnistyspainiketta hiiren kakkospainikkeella tai pidä se painettuna ja valitse sitten **Komentokehote**.
  - Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012  
Näytä sovellusnäyttö ja valitse sitten **Komentokehote**.
  - Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 tai vanhempi  
Napsauta käynnistyspainiketta, valitse **Kaikki ohjelmat** tai **Ohjelmat > Apuohjelmat > Komentokehote**.
3. Syötä ”ping xxx.xxx.xxx.xxx” ja paina sitten Enter-näppäintä.  
Syötä skannerin IP-osoite kohteelle xxx.xxx.xxx.xxx.
4. Tarkista tietoliikenneyhteyden tila.  
Jos skanneri ja tietokone kommunikoivat, esiin tulee seuraava viesti.



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

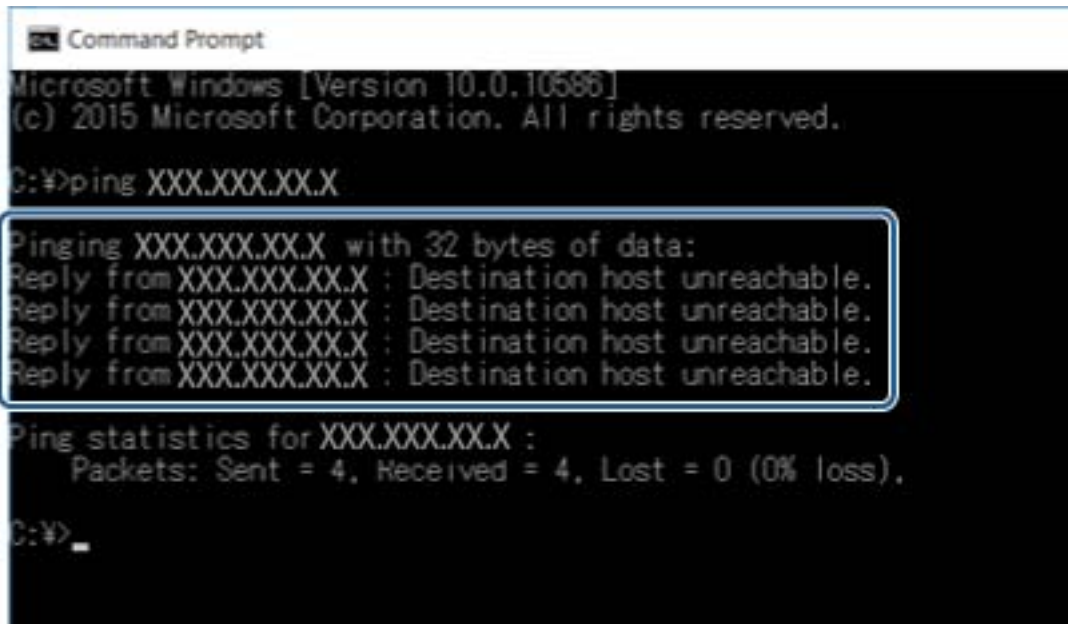
Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : bytes=32 time=87ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=86ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=311ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=117ms TTL=64

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 86ms, Maximum = 311ms, Average = 150ms

C:\>
```

## Ongelmien ratkaisu

Jos skanneri ja tietokone eivät kommunikoi, esiin tulee seuraava viesti.



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.

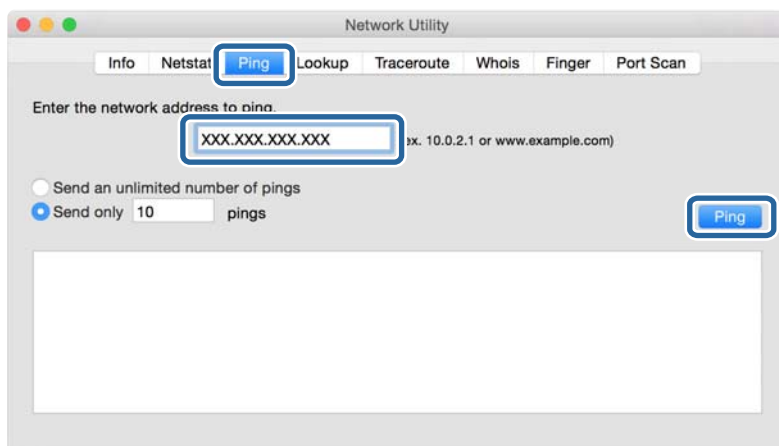
Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>_
```

## Yhteyden tarkistus Ping-komennolla — Mac OS

Voit varmistaa Ping-komennon avulla, että tietokone on liitetty skanneriin. Tarkista yhteys Ping-komennon avulla alla olevien ohjeiden mukaisesti.

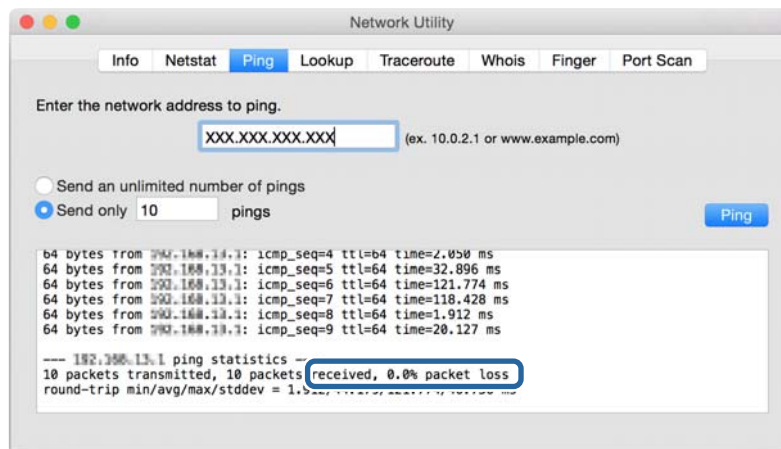
1. Tarkista skannerin IP-osoite yhteydelle, jonka haluat tarkistaa.  
Voit tarkistaa tämän Epson Scan 2 -sovelluksen avulla.
2. Suorita Network Utility.  
Syötä "Network Utility" kohdassa **Spotlight**.
3. Osoita **Ping**-välilehteä, anna IP-osoite, jonka tarkastit vaiheessa 1 ja osoita sitten **Ping**.



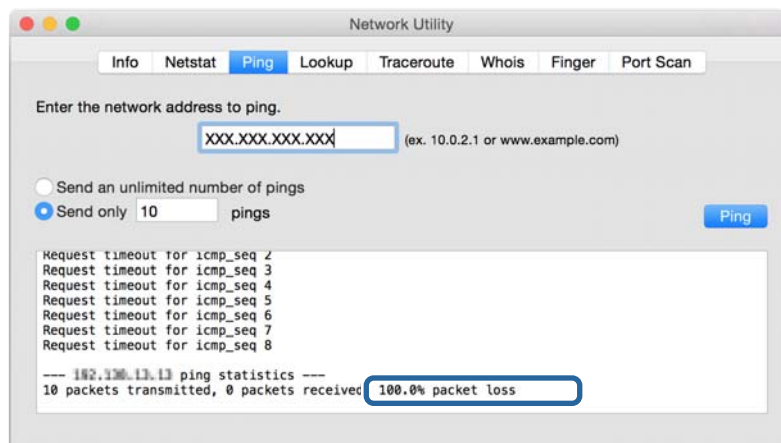
## Ongelmien ratkaisu

### 4. Tarkista tietoliikenneyhteyden tila.

Jos skanneri ja tietokone kommunikoivat, esiin tulee seuraava viesti.



Jos skanneri ja tietokone eivät kommunikoivat, esiin tulee seuraava viesti.



## Verkko-ohjelmiston käyttöön liittyviä ongelmia

### Web Config -hallintasivun käyttäminen ei onnistu

#### Onko skannerin IP-osoite määritetty oikein?

Määritä IP-osoite Epson Device Admin- tai EpsonNet Config -ohjelmiston avulla.

#### Tukeeko selaimesi kohteen Encryption Strength/SSL/TLS joukkosalausta?

Kohteen Encryption Strength/SSL/TLS joukkosalaukset toimivat seuraavasti. Web Config -ohjelmistoa voidaan käyttää vain selaimessa, joka tukee seuraavia joukkosalauksia. Tarkista selaimen salaustuki.

- 80-bittinen: AES256/AES128/3DES
- 112-bittinen: AES256/AES128/3DES
- 128-bittinen: AES256/AES128

## Ongelmien ratkaisu

- 192-bittinen: AES256
- 256-bittinen: AES256

### Viesti "Vanhentunut" tulee esiin, kun käytetään Web Config -ohjelmistoa SSL-yhteydellä (https).

Jos varmenne on vanhentunut, hanki varmenne uudelleen. Jos viesti tulee näkyviin ennen varmenteen eräpäivää, varmista, että skannerin päivämääräasetus on oikein.

### Viesti "Suojausvarmenteen nimi ei täsmää..." tulee esiin, kun käytetään Web Config -ohjelmistoa SSL-yhteydellä (https).

Skannerin IP-osoite, joka annetaan **Common Name** -kohteelle itse allekirjoitetun varmenteen tai CSR:n luontiin, ei täsmää selaimen annetun osoitteen kanssa. Hanki tai tuo varmenne uudelleen tai muuta skannerin nimeä.

### Skanneria käytetään välityspalvelimen kautta.

Jos käytät skanneria välityspalvelimen kautta, selaimen välityspalvelinasetukset on määritettävä.

- Windows:

Valitse **Ohjauspaneeli > Verkko ja Internet > Internet-asetukset > Yhteydet > Lähiverkon asetukset > Välityspalvelin**, ja tee sitten määrittäminen, että välityspalvelinta ei käytetä paikallisille osoitteille.

- Mac OS:

Valitse **Järjestelmäasetukset > Verkko > Lisäasetukset > Välipalvelimet**, ja rekisteröi sitten paikallinen osoite kohteelle **Ohita näiden palvelimien ja toimialueiden välipalvelinasetukset**.

Esimerkki:

192.168.1.\*: paikallinen osoite 192.168.1.XXX, aliverkon peite 255.255.255.0

192.168.\*.\*: paikallinen osoite 192.168.XXX.XXX, aliverkon peite 255.255.0.0

### Liittyvät tiedot

- ➔ ["Web Config -ohjelmiston käyttö" sivulla 23](#)
- ➔ ["IP-osoitteen määrittäminen" sivulla 15](#)
- ➔ ["IP-osoitteen määrittäminen EpsonNet Config -sovelluksen avulla" sivulla 56](#)

## Mallin nimeä ja/tai IP-osoitetta ei näy EpsonNet Config -ohjelmistossa

### Valitsitko Estä, Peruuta tai Sammuta, kun näkyvässä oli Windows-suojausnäyttö tai palomuurin näyttö?

Jos valitsit **Torju, Peruuta** tai **Sammuta**, IP-osoite tai mallin nimi ei näy EpsonNet Config- tai EpsonNet Setup -ohjelmistossa.

Kun haluat korjata tämän, rekisteröi EpsonNet Config poikkeukseksi Windows-palomuurissa ja kaupallisessa suojausohjelmistossa. Jos käytät viruksentorjunta- tai suojausohjelmistoa, sulje se ja yritä sitten käyttää EpsonNet Config -ohjelmistoa.

### Onko yhteysvirheen aikakatkaistu asetettu liian lyhyeksi?

Suorita EpsonNet Config ja valitse **Tools > Options > Timeout**, ja pidennä sitten aikaa **Communication Error** -asetukselle. Huomaa, että jos näin tehdään, EpsonNet Config voi toimia hitaammin.

## Ongelmien ratkaisu

### Liittyvät tiedot

- ➔ [”EpsonNet Config -ohjelmiston käynnistäminen — Windows” sivulla 56](#)
- ➔ [”EpsonNet Config -ohjelmiston käynnistäminen — Mac OS” sivulla 56](#)

# Liite

## Yleistietoja verkko-ohjelmistosta

Seuraavassa kuvataan laitteiden asetusten määrittämisessä ja hallinnassa käytettävä ohjelmisto.

### Epson Device Admin

Epson Device Admin on sovellus, jonka avulla voit asentaa laitteita verkkoon, määrittää laitteiden asetukset ja hallita niitä. Sovelluksen avulla voit kerätä laitteista tarkat tilatiedot ja tiedot tarvikemääristä, lähettää ilmoituksia laitteiden käyttäjille ja luoda raportteja laitteiden käytöstä. Voit luoda asetusmallipohjan ja jakaa asetukset useisiin laitteisiin sen avulla. Epson Device Admin on ladattavissa Epson-tukisivustolta. Katso lisätietoja Epson Device Admin -sovelluksen oppaasta tai ohjeesta.

### Epson Device Admin -sovelluksen käyttäminen (vain Windows)

Valitse **All Programs > EPSON > Epson Device Admin > Epson Device Admin**.

**Huomautus:**

*Jos näyttöön tulee palomuurin hälytys, salli käyttö Epson Device Admin -sovellukselle.*

### EpsonNet Config

EpsonNet Config -ohjelmiston avulla järjestelmänvalvoja voi määrittää skannerin verkkoasetukset, kuten IP-osoitteen ja yhteystavan. Lisäksi Windows tukee ohjelmiston eräasetustoimintoa. Katso lisätietoja EpsonNet Config -sovelluksen oppaasta tai ohjeesta.



## EpsonNet Config -ohjelmiston käynnistäminen — Windows

Valitse **Kaikki ohjelmat** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

### **Huomautus:**

*Jos näyttöön tulee palomuurin hälytys, salli käyttö EpsonNet Config -sovellukselle.*

## EpsonNet Config -ohjelmiston käynnistäminen — Mac OS

Valitse **Siirry** > **Sovellukset** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

## EpsonNet SetupManager

EpsonNet SetupManager -ohjelmistolla voidaan luoda käteviä asennuspaketteja skanneriasennuksiin, kuten skanneriohjaimen asennukseen ja asetusten määrittämiseen ja Document Capture Pro -ohjelmiston asennukseen. Ohjelmiston avulla järjestelmänvalvoja voi luoda yksilöllisiä ohjelmapaketteja, jotka voidaan jakaa työryhmille.

Lisätietoa saat alueelliselta Epson-verkkosivustolta.

---

## IP-osoitteen määrittäminen EpsonNet Config -sovelluksen avulla

Voit määrittää skannerille IP-osoitteen EpsonNet Config -sovelluksella. EpsonNet Config mahdollistaa IP-osoitteen määrittämisen skannerille, jolle ei ole vielä määritetty osoitetta. Laite kytketään tällöin verkkoon Ethernet-kaapelilla.

## IP-osoitteen määrittäminen eräasetusten avulla

### Eräasetustiedoston luominen

Voit luoda IP-osoitteiden määrittämistä varten SYLK-tiedoston käyttämällä avaimina laitteiden MAC-osoitteita ja mallinimiä.

1. Avaa taulukkolaskentasovellus, kuten Microsoft Excel, tai tekstieditori.
2. Kirjoita ensimmäiselle riville asetusten nimiksi "Info\_MACAddress", "Info\_ModelName" ja "TCPIP\_IPAddress".

Kirjoita asetusarvot seuraaville riveille. Pieni ja iso kirjainkoko sekä merkin yksi- tai kaksibittisyys ovat merkitseviä; asetusta ei tunnisteta, jos yksikin merkki poikkeaa oikeasta muodosta.

Kirjoita asetuksen nimi tarkalleen seuraavalla tavalla. Muussa tapauksessa EpsonNet Config ei tunnista asetuksia.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress



## Liite

3. Kirjoita kullekin verkkoliitännälle laiteosoite (MAC-osoite), mallinimi ja IP-osoite.

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. Kirjoita tiedostolle nimi ja tallenna se SYLK-tiedostona (\*.slk).

## Eräasetusten määrittäminen kokoonpanotiedoston avulla

Voit määrittää IP-osoitteet kokoonpanotiedostoon (SYLK-tiedosto) yksi osoite kerrallaan. Luo kokoonpanotiedosto ennen osoitteiden määrittämistä.

1. Kytke kaikki laitteet verkkoon Ethernet-kaapelilla.
2. Käynnistä skanneri.
3. Käynnistä EpsonNet Config.

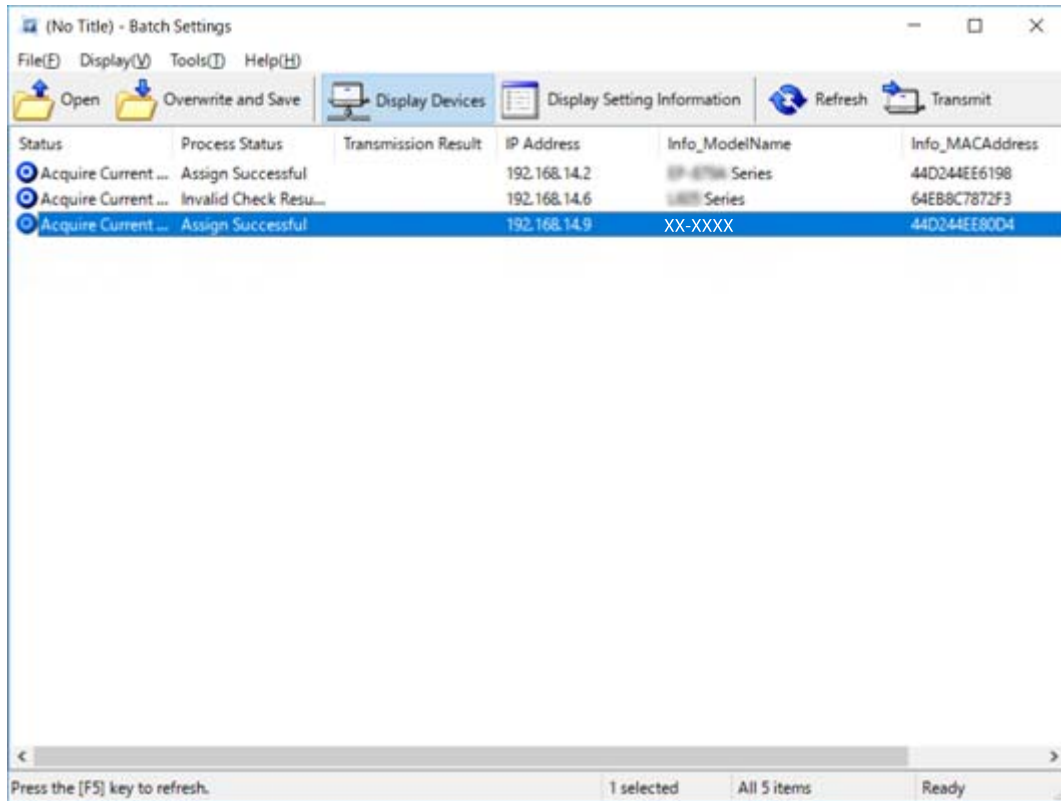
Luettelo verkkoon kytketyistä skannereista tulee näkyviin. Laitteiden tuleminen näkyviin voi kestää jonkin aikaa.

4. Valitse **Tools > Batch Settings**.
5. Valitse **Open**.
6. Valitse tiedostonvalintänäytössä halutut asetukset sisältävä SYLK-tiedosto (\*.slk) ja valitse sitten **Open**.

**Liite**

- Valitse laitteet, joille haluat määrittää asetukset erätyönä (**Status**-sarakeessa arvo **Unassigned**, **Process Status**-sarakkeen arvo **Assign Successful**).

Jos haluat valita useita laitteita, paina Ctrl- tai Shift-näppäintä tai vedä hiirellä.



- Valitse **Transmit**.
- Kun salasananäyttö tulee näkyviin, kirjoita salasana ja valitse **OK**.

Lähetä asetukset.

**Huomautus:**



Tietojen lähettäminen verkkoliitännän kautta on meneillään, kunnes edistymismittari ilmoittaa toiminnon olevan valmis. Älä sammuta laitetta tai langattoman verkon sovitinta äläkä lähetä dataa laitteeseen tietojen lähetyksen ollessa meneillään.






- Valitse **Transmitting Settings** -näytössä **OK**.



## Liite

## 11. Tarkista valitun laitteen tila.

Jos laitteen kohdalla näkyy  tai , tarkista asetustiedoston sisältö ja varmista, että laite on käynnistynyt uudelleen normaalisti.

Kuvake	Status	Process Status	Selitys
	Setup Complete	Setup Successful	Asennus valmistui normaalisti.
	Setup Complete	Rebooting	Kun tiedot on lähetetty, asetukset on otettava käyttöön käynnistämällä kukin laite uudelleen. Yhteyden muodostuminen tarkistetaan laitteen uudelleenkäynnistämisen jälkeen.
	Setup Complete	Reboot Failed	Laitteen toiminnan tarkistaminen asetusten lähettämisen jälkeen ei onnistu. Tarkista, että laite on kytketty päälle ja että se on käynnistynyt uudelleen normaalisti.
	Setup Complete	Searching	Asetustiedostossa määritetyn laitteen haku.*
	Setup Complete	Search Failed	Aiemmin määritettyjen laitteiden tarkistaminen ei onnistu. Tarkista, että laite on kytketty päälle ja että se on käynnistynyt uudelleen normaalisti.*

\* Vain jos asetustiedot ovat näkyvissä.

**Liittyvät tiedot**

- ➔ [”EpsonNet Config -ohjelmiston käynnistäminen — Windows” sivulla 56](#)
- ➔ [”EpsonNet Config -ohjelmiston käynnistäminen — Mac OS” sivulla 56](#)

**IP-osoitteen määrittäminen kullekin verkon laitteelle**

Määritä IP-osoite skannerille EpsonNet Config -sovelluksella.

1. Käynnistä skanneri.

2. Kytke skanneri verkkoon Ethernet-kaapelilla.

3. Käynnistä EpsonNet Config.

Luettelo verkkoon kytketyistä skannereista tulee näkyviin. Laitteiden tuleminen näkyviin voi kestää jonkin aikaa.

4. Kaksoisnapsauta skanneria, jolle haluat määrittää IP-osoitteen.

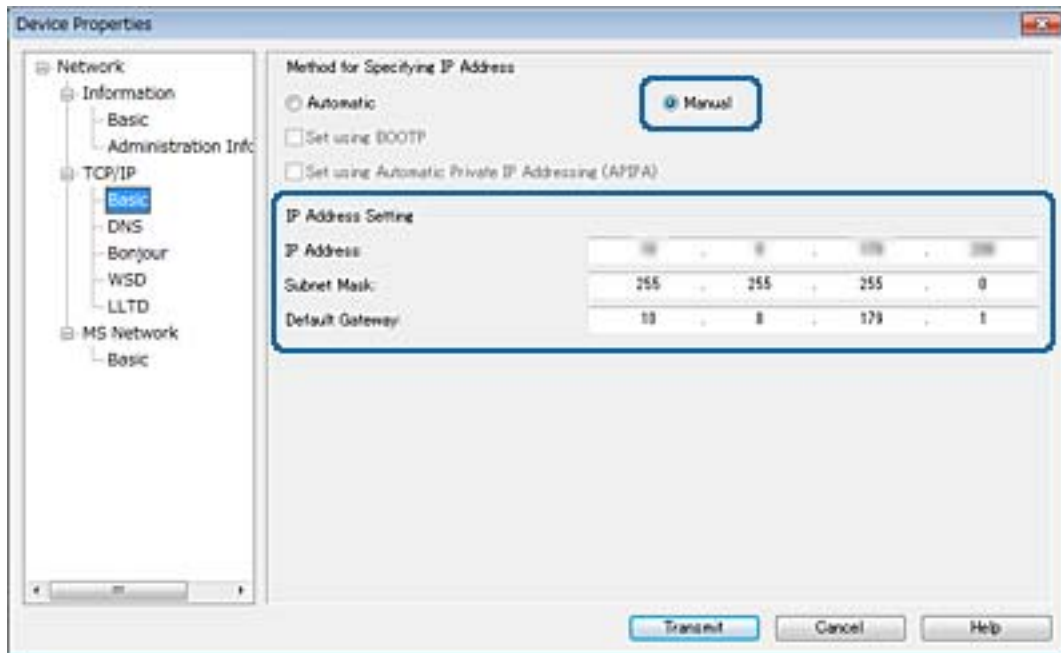
**Huomautus:**

*Jos verkkoon on kytketty useita saman laitetyyppin skannereita, voit erottaa tulostimet toisistaan laiteosoitteen (MAC-osoite) perusteella.*

5. Valitse **Network > TCP/IP > Basic**.

## Liite

6. Kirjoita osoitteet **IP Address**, **Subnet Mask**- ja **Default Gateway** -kohtiin.

**Huomautus:**

Jos skanneri liitetään suojattuun verkkoon, kirjoita staattinen IP-osoite.

7. Valitse **Transmit**.

Tietojen siirron vahvistusnäyttö tulee näkyviin.

8. Valitse **OK**.

Vahvistus tiedonsiirron onnistumisesta tulee näkyviin.

**Huomautus:**

Tiedot siirretään laitteeseen ja asetusten määrittämisen onnistumisen vahvistava viesti tulee näkyviin. Älä sammuta laitetta äläkä lähetä palveluun dataa.

9. Valitse **OK**.

**Liittyvät tiedot**

- ➔ ”EpsonNet Config -ohjelmiston käynnistäminen — Windows” sivulla 56
- ➔ ”EpsonNet Config -ohjelmiston käynnistäminen — Mac OS” sivulla 56

---

## Skannerin käyttämät porttinumerot

Skanneri käyttää seuraavia portteja. Liikenne seuraaviin portteihin on suositeltavaa sallia (verkonvalvojan harkinnan ja käyttötarpeen mukaan).

## Liite

Lähtettäjä (työasema)	Käyttötarkoitus	Kohde (palvelin)	Protokolla	Porttinumero
Skanneri	Sähköpostin lähettäminen (sähköposti-ilmoitus)	SMTP-palvelin	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP ennen SMTP-yhteyttä (sähköposti-ilmoitus)	POP-palvelin	POP3 (TCP)	110
	WSD-hallinta	Työasema	WSD (TCP)	5357
	Tietokoneen haku, kun push-skannaus suoritetaan kohteesta Document Capture Pro	Työasema	Push-skannauksen haku verkossa	2968
Työtietojen haku, kun push-skannaus suoritetaan kohteesta Document Capture Pro	Työasema	Push-skannaus verkossa	2968	
Työasema	Skannerin haku sovelluksesta, kuten EpsonNet Config -ohjelmasta tai skanneriohjaimesta.	Skanneri	ENPC (UDP)	3289
	MIB-tietojen haku ja määrittäminen sovelluksesta, kuten EpsonNet Config -ohjelmasta tai skanneriohjaimesta.	Skanneri	SNMP (UDP)	161
	WSD-skannerihaku	Skanneri	WS-Discovery (UDP)	3702
	Document Capture Pro - skannaustietojen edelleenlähetys	Skanneri	Skannaus verkkoon (TCP)	1865

# Suojauksen lisäasetukset (yrityskäyttäjät)

Tässä luvussa kuvataan suojauksen lisäasetukset.

## Laiteasetukset ja riskien hallinta

Jos laite on kytketty verkkoon, sitä voidaan käyttää etäsjainneista. Tämän lisäksi laite voidaan jakaa useiden käyttäjien käytettäväksi, mikä tehostaa toimintaa ja helpottaa käyttöä. Laitteiden verkkoon jakamiseen kuitenkin liittyy luvattomaan käyttöön ja tietojen peukalointiin liittyviä riskejä. Jos laite on kytketty verkkoon, josta on yhteys Internetiin, riskit ovat vielä suuremmat.

Jotta näiltä riskeiltä vältyttäisiin, Epsonin laitteissa on käytössä erilaisia suojaustekniikoita.

Järjestelmänvalvoja määrittää tarvittavat suojausasetukset käyttöympäristön mukaan.

Nimi	Ominaisuuden tyyppi	Mitä asetetaan	Mitä estetään
SSL/TLS-tiedonsiirto	Tietokoneen ja laitteen välinen tiedonsiirto voidaan suojata SSL/TLS-salauksella. Selainkäytön tietoliikenteen sisältö on suojattu.	Laitteeseen voidaan lisäksi määrittää varmennemyöntäjän allekirjoittama varmenne.	Estää asetustietojen ja tulostustöiden sisällön vuotamisen skannerin ja tietokoneen välisessä tietoliikenteessä. Tulostimen ja Internetin palvelinten välinen liikenne voidaan suojata myös esimerkiksi päivittämällä laiteohjelmisto.
IPsec-suojaus ja IP-osoitteiden suodatus	Näiden ominaisuuksien avulla voit estää tietyistä osoitteista peräisin olevat yhteydet tai yhteydet, joiden tietosisältö on määrätynlainen. Koska IPsec suojaa datan IP-pakettitasolla (salauksella ja todennus), IPsec-ympäristössä voidaan käyttää suojaamattomia skannausprotokollia turvallisesti.	Sallitut yhteydet voidaan määrittää peruskäytännön ja yksittäiskäytäntöjen avulla.	Estää luvattoman käytön sekä laitteeseen lähetettävien tietojen peukaloinnin ja luvattoman tallentamisen.
SNMPv3	Useita suojausominaisuuksia, kuten verkkoon kytkettyjen laitteiden valvonta, SNMP-tietojen eheyden valvonta, salaus ja käyttäjien todennus.	Ota SNMPv3 käyttöön ja määritä todennus- ja salausmenetelmät.	Suojaa ja varmistaa asetusmuutosten oikeellisuuden ja tilatiedot.
IEEE802.1X	Rajoittaa yhteydet käyttäjiin, jotka ovat todentaneet itsensä kaapelilähiverkkoon. Vain sallitut käyttäjät voivat käyttää laitetta.	Todennus RADIUS-palvelimen (todennuspalvelin) kautta.	Suojaa laitteen luvattomalta käytöltä.

## Suojauksen lisäasetukset (yrityskäyttäjät)

Nimi	Ominaisuuden tyyppi	Mitä asetetaan	Mitä estetään
Tunnuskortti	Laitetta voidaan käyttää erillisen tunnuskorttipohjaisen todennuksen avulla. Voit rajoittaa lokitietojen saannin yksittäiseen käyttäjään ja laitteeseen sekä rajata käytettävissä olevien laitteiden ja ominaisuuksien määrän yksilö- ja ryhmätasolla.	Liitä todennuslaite tulostimeen tai skanneriin ja määritä käyttäjän tiedot todennusjärjestelmään.	Estää laitteen luvattoman käytön ja huijaukset.

### Liittyvät tiedot

- ➔ ”SSL/TLS-suojattu tiedonsiirto ja skannerin käyttö” sivulla 63
- ➔ ”Tiedonsiirron salaus IPsec-suojauksen ja IP-osoitteiden suodatuksen avulla” sivulla 71
- ➔ ”SNMPv3-protokollan käyttö” sivulla 83
- ➔ ”Skannerin kytkentä IEEE802.1X-verkkoon” sivulla 85

## Suojaustoimintojen asetukset

Jos IPsec-suojaus, IP-osoitteiden suodatus tai IEEE802.1X-suojaus on käytössä, Web Config -hallintänyttöä käytettäessä on suositeltavaa käyttää suojattua SSL/TLS-yhteyttä, jotta salakuuntelun tai tietojen väärentämisen riski olisi pienempi.

## SSL/TLS-suojattu tiedonsiirto ja skannerin käyttö

Jos palvelimen varmenne on määritetty käyttämään SSL/TLS-suojausta (Secure Sockets Layer/Transport Layer Security) skannerin tietoliikenteen suojaamiseen, tietokoneiden välinen tiedonsiirto voidaan salata. Ota toiminto käyttöön, jos haluat estää luvattoman etäkäytön.

## Tietoja digitaalisesta varmennuksesta

- CA:n allekirjoittama varmenne

CA:n (Certificate Authority) allekirjoittama varmenne on saatava varmennusviranomaiselta. Voit varmistaa turvallisen tiedonsiirron käyttämällä CA:n allekirjoittamaa varmennetta. Voit käyttää CA:n allekirjoittamaa varmennetta kullekin suojaustoiminnolle.

- CA-varmenne

CA-varmenne osoittaa, että kolmas osapuoli on varmentanut palvelimen identiteetin. Tämä on tärkeä osa web-of-trust-tyylin suojausta. CA-varmenne palvelimen todennukseen on saatava varmenteita myöntävältä CA:lta.

- Itse allekirjoitettu varmenne

Skanneri myöntää ja allekirjoittaa itse allekirjoitetun varmenteen. Tämä varmenne on epäluotettava eikä se voi estää huijauksia. Jos käytät tätä varmennetta SSL/TLS-varmenteena, selaimessa voi näkyä suojausvaroitus. Voit käyttää tätä varmennetta vain SSL/TLS-tiedonsiirtoon.

## Suojauksen lisäasetukset (yrityskäyttäjät)

### Liittyvät tiedot

- ➔ ”CA:n allekirjoittaman varmenteen hankinta ja tuonti” sivulla 64
- ➔ ”CA:n allekirjoittaman varmenteen poisto” sivulla 67
- ➔ ”Itse allekirjoitetun varmenteen päivitys” sivulla 68

## CA:n allekirjoittaman varmenteen hankinta ja tuonti

### CA:n allekirjoittaman varmenteen hankinta

Kun haluat CA:n allekirjoittaman varmenteen, luo varmenteen allekirjoituspyyntö (CSR) ja lähetä se varmenneviranomaiselle. Voit luoda CSR:n Web Config -ohjelmiston ja tietokoneen avulla.

Luo CSR ja hanki CA:n allekirjoittama varmenne käyttämällä Web Config -ohjelmistoa. Kun CSR luodaan käyttämällä Web Config -ohjelmistoa, varmenne on PEM/DER-muodossa.

1. Käytä Web Config -toimintoa ja valitse sitten **Network Security Settings**. Valitse seuraavaksi **SSL/TLS > Certificate** tai **IPsec/IP Filtering > Client Certificate** tai **IEEE802.1X > Client Certificate**.
2. Napsauta **Generate** kohdasta **CSR**.  
CSR:n luontisivu avautuu.
3. Syötä arvo kullekin kohteelle.  
**Huomautus:**  
*Käytettävissä oleva avaimen pituus ja lyhenteet vaihtelevat varmenneviranomaisen mukaan. Luo pyyntö kunkin varmenneviranomaisen sääntöjen mukaisesti.*
4. Napsauta **OK**.  
Esiin tulee suoritusviesti.
5. Valitse **Network Security Settings**. Valitse seuraavaksi **SSL/TLS > Certificate**, tai **IPsec/IP Filtering > Client Certificate** tai **IEEE802.1X > Client Certificate**.
6. Napsauta jotakin latauspainikkeista kohdassa **CSR** kunkin varmenneviranomaisen määräämän muodon mukaisesti ja lataa CSR tietokoneeseen.

**Tärkeää:**

Älä luo CSR:ää uudelleen. Jos teet niin, et ehkä voi tuoda myönnettyä CA-signed Certificate -sertifikaattia.

7. Lähetä CSR sertifikaatin myöntäjälle ja hae CA-signed Certificate.  
Noudata kunkin varmenneviranomaisen sääntöjä lähetyksen menetelmän ja -muodon suhteen.
8. Tallenna CA-signed Certificate skanneriin liitettyyn tietokoneeseen.  
CA-signed Certificate:n hakeminen on valmis, kun tallennat sertifikaatin kohdekansioon.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”CSR-asetuskohteet” sivulla 65



## Suojauksen lisäasetukset (yrityskäyttäjät)

➔ ”CA:n allekirjoittaman varmenteen tuonti” sivulla 66

### CSR-asetuskohteet

The screenshot shows the 'Certificate' configuration page in the EPSON Network Security Settings. The left sidebar contains a navigation menu with categories like Status, Scanner Settings, Network Settings, Network Security Settings (expanded), Services, System Settings, and Administrator Settings. Under Network Security Settings, 'SSL/TLS' is expanded to show 'Basic' and 'Certificate' options. The main content area is titled 'Network Security Settings > SSL/TLS > Certificate' and contains the following fields:

- Key Length: 2048
- Common Name: 10.152.12.225
- Organization: (empty)
- Organizational Unit: (empty)
- Locality: (empty)
- State/Province: (empty)
- Country: (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form.

Asetus	Asetusarvot ja kuvaus
Key Length	Valitse CSR:n avaimen pituus.
Common Name	Syötä 1–128 merkkiä. Jos tämä on IP-osoite, sen tulee olla staattinen IP-osoite. Esimerkki: Web Config -hallintasivun URL-osoite: https://10.152.12.225 Yleinen nimi: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Voit syöttää 0–64 merkkiä ASCII-muodossa (0x20–0x7E). Voit erottaa nimetyt nimet pilkuilla.
Country	Syötä maakoodi kaksinumeroisena lukuna ISO-3166-standardissa määritetyllä tavalla.

### Liittyvät tiedot

➔ ”CA:n allekirjoittaman varmenteen hankinta” sivulla 64

## CA:n allekirjoittaman varmenteen tuonti



**Tärkeää:**

- Varmista, että skannerin päivämäärä ja kellonaika on asetettu oikein.
- Jos saat CSR-pyyntöä käyttämällä varmenteen, joka on luotu Web Config -ohjelmistosta, voit tuoda varmenteen yhden kerran.

1. Käytä Web Config -toimintoa ja valitse sitten **Network Security Settings**. Valitse seuraavaksi **SSL/TLS > Certificate**, tai **IPsec/IP Filtering > Client Certificate** tai **IEEE802.1X > Client Certificate**.

2. Napsauta **Import**.

Varmenteen tuontisivu avautuu.

3. Syötä arvo kullekin kohteelle.

Vaaditut asetukset vaihtelevat CSR:n luontipaikan ja varmenteen tiedostomuodon mukaan. Syötä arvot vaadituille kohteille seuraavan mukaisesti.

- PEM/DER-muodon varmenne, joka on saatu Web Config -tiedostosta
  - Private Key:** Älä määritä, koska skanneri sisältää yksityisen avaimen.
  - Password:** Älä määritä.
  - CA Certificate 1/CA Certificate 2:** Valinnainen
- PEM/DER-muodon varmenne, joka on saatu tietokoneesta
  - Private Key:** Tulee asettaa.
  - Password:** Älä määritä.
  - CA Certificate 1/CA Certificate 2:** Valinnainen
- PKCS#12-muodon varmenne, joka on saatu tietokoneesta
  - Private Key:** Älä määritä.
  - Password:** Valinnainen
  - CA Certificate 1/CA Certificate 2:** Älä määritä.

4. Napsauta **OK**.

Esiin tulee suoritusviesti.

**Huomautus:**

Tarkista varmenteen tiedot napsauttamalla **Confirm**.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”CA:n allekirjoittaman varmenteen tuonnin asetukset” sivulla 67

## Suojauksen lisäasetukset (yrityskäyttäjät)

### CA:n allekirjoittaman varmenteen tuonnin asetuskohdeet

The screenshot shows the 'Certificate' configuration page in the Epson network security settings. The left sidebar contains a navigation menu with options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Network Security Settings', 'SSL/TLS', 'IPsec/IP Filtering', 'IEEE802.1X', 'Services', 'System Settings', 'Export and Import Setting Value', 'Administrator Settings', and 'Basic Settings'. The main content area is titled 'Network Security Settings > SSL/TLS > Certificate'. It includes fields for 'Server Certificate' (set to 'Certificate (PEM/DER)'), 'Private Key', 'Password', 'CA Certificate 1', and 'CA Certificate 2', each with a 'Browse...' button. A note at the bottom states: 'Note: It is recommended to communicate via HTTPS for importing a certificate.' There are 'OK' and 'Back' buttons at the bottom.

Kohdat	Asetukset ja selitys
Server Certificate tai Client Certificate	Valitse varmenteen muoto.
Private Key	Jos saat PEM/DER-muotoisen varmenteen käyttämällä CSR-pyyntöä, joka on luotu tietokoneesta, määritä yksityinen avaintiedosto, joka vastaa varmennetta.
Password	Salaa yksityinen avain antamalla salasana.
CA Certificate 1	Jos varmenteen muoto on <b>Certificate (PEM/DER)</b> , tuo varmenne varmenneviranomaiselta, joka myöntää palvelinvarmenteita. Määritä tiedosto tarvittaessa.
CA Certificate 2	Jos varmenteen muoto on <b>Certificate (PEM/DER)</b> , tuo varmenne varmenneviranomaiselta, joka myöntää <b>CA Certificate 1</b> -varmenteita. Määritä tiedosto tarvittaessa.

#### Liittyvät tiedot

➔ ”CA:n allekirjoittaman varmenteen tuonti” sivulla 66

### CA:n allekirjoittaman varmenteen poisto

Voit poistaa tuodun varmenteen, jos varmenne on vanhentunut tai jos salattu yhteys ei ole enää tarpeen.

## Suojauksen lisäasetukset (yrityskäyttäjät)



**Tärkeää:**

*Jos olet saanut varmenteen Web Config -hallintasivun CSR-pyyntöllä, et voi tuoda poistettua varmennetta uudelleen. Luo tässä tapauksessa uusi CSR-pyyntö ja hanki uusi varmenne.*

1. Avaa Web Config -toiminto ja valitse **Network Security Settings**. Valitse sitten **SSL/TLS > Certificate** tai **IPsec/IP Filtering > Client Certificate** tai **IEEE802.1X > Client Certificate**.
2. Valitse **Delete**.
3. Vahvista varmenteen poisto näkyviin tulevassa viestissä.

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Itse allekirjoitetun varmenteen päivitys

Jos skanneri tukee HTTPS-palvelinominaisuutta, voit päivittää itse allekirjoitetun varmenteen. Kun Web Config -ohjelmistoon siirrytään käyttämällä itse allekirjoitettua varmennetta, esiin tulee varoitusviesti.

Käytä itse allekirjoitettua varmennetta väliaikaisesti, kunnes saat ja tuot CA:n allekirjoittaman varmenteen.

1. Avaa Web Config -toiminto ja valitse **Network Security Settings > SSL/TLS > Certificate**.
2. Valitse **Update**.
3. Syötä **Common Name**.

Syötä skannerille IP-osoite tai tunniste, kuten FQDN-nimi. Syötä 1–128 merkkiä.

**Huomautus:**

*Voit erottaa nimetyt nimet (CN) pilkuilla.*

## Suojauksen lisäasetukset (yrityskäyttäjät)

- Määritä varmenteen voimassaoloaika.

The screenshot shows the Epson Web Config interface. On the left is a navigation menu with options like 'Administrator Logout', 'Status', 'Product Status', 'Network Status', 'Panel Snapshot', 'Maintenance', 'Hardware Status', 'Scanner Settings', 'Network Settings', 'Network Security Settings', 'SSL/TLS', 'Basic', 'Certificate', 'IPsec/IP Filtering', 'IEEE802.1X', 'CA Certificate', 'Services', 'System Settings', 'Export and Import Setting Value', and 'Administrator Settings'. The main content area is titled 'Network Security Settings > SSL/TLS > Certificate'. It contains the following fields:

Key Length :	2048
Common Name :	SEIKO EPSON CORP.
Organization :	SEIKO EPSON CORP.
Valid Date (UTC) :	2016-11-24 02:49:09 UTC
Certificate Validity (year) :	10

At the bottom of the form are two buttons: 'Next' and 'Back'.

- Valitse **Next**.

Esiin tulee vahvistusviesti.

- Valitse **OK**.

Skanneri on päivitetty.

**Huomautus:**

Tarkista varmenteen tiedot napsauttamalla **Confirm**.

**Liittyvät tiedot**

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Määritä CA Certificate

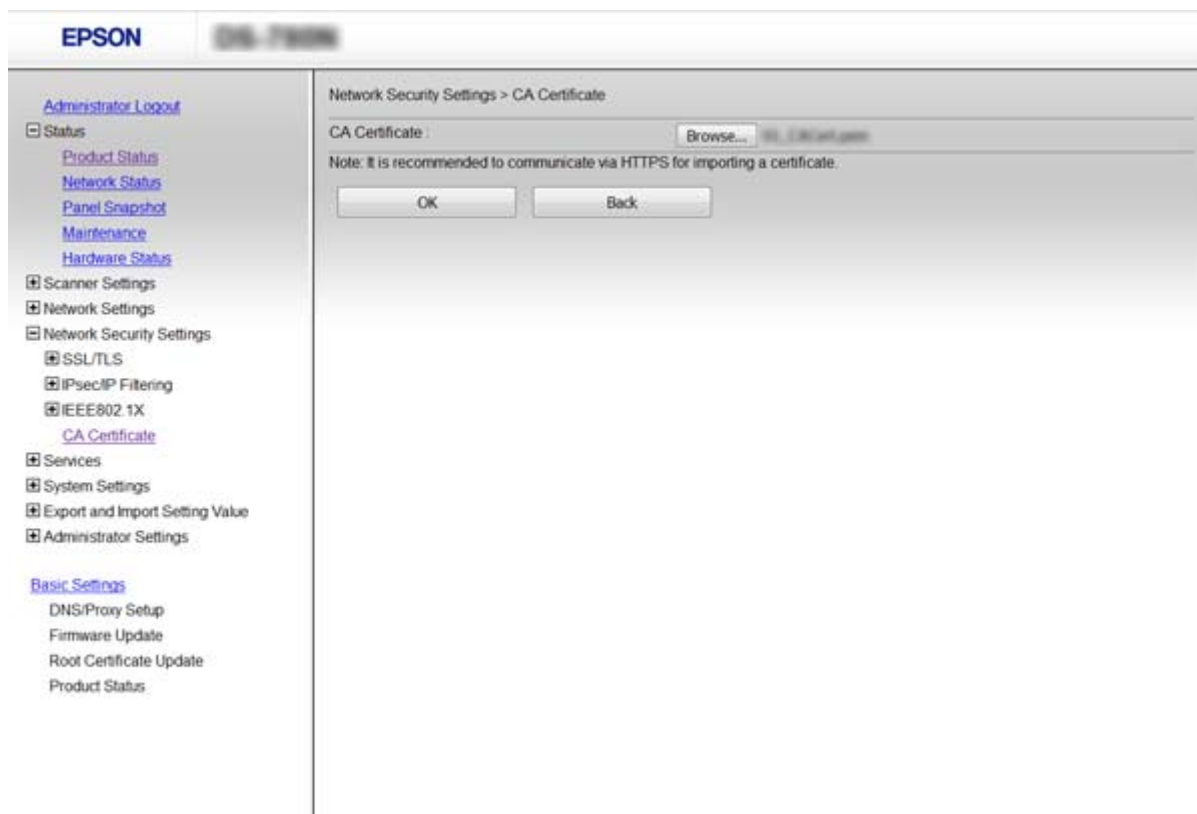
Voit tuoda, näyttää, poistaa CA Certificate -sertifikaatin.

### CA Certificate -sertifikaatin tuominen

- Käytä Web Config -toimintoa ja valitse sitten **Network Security Settings > CA Certificate**.
- Napsauta **Import**.

## Suojauksen lisäasetukset (yrityskäyttäjät)

- Määritä tuotava CA Certificate.



- Napsauta **OK**.

Kun tuonti on valmis, sinut palautetaan **CA Certificate** -näyttöön ja tuotu CA Certificate näkyy näytössä.

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

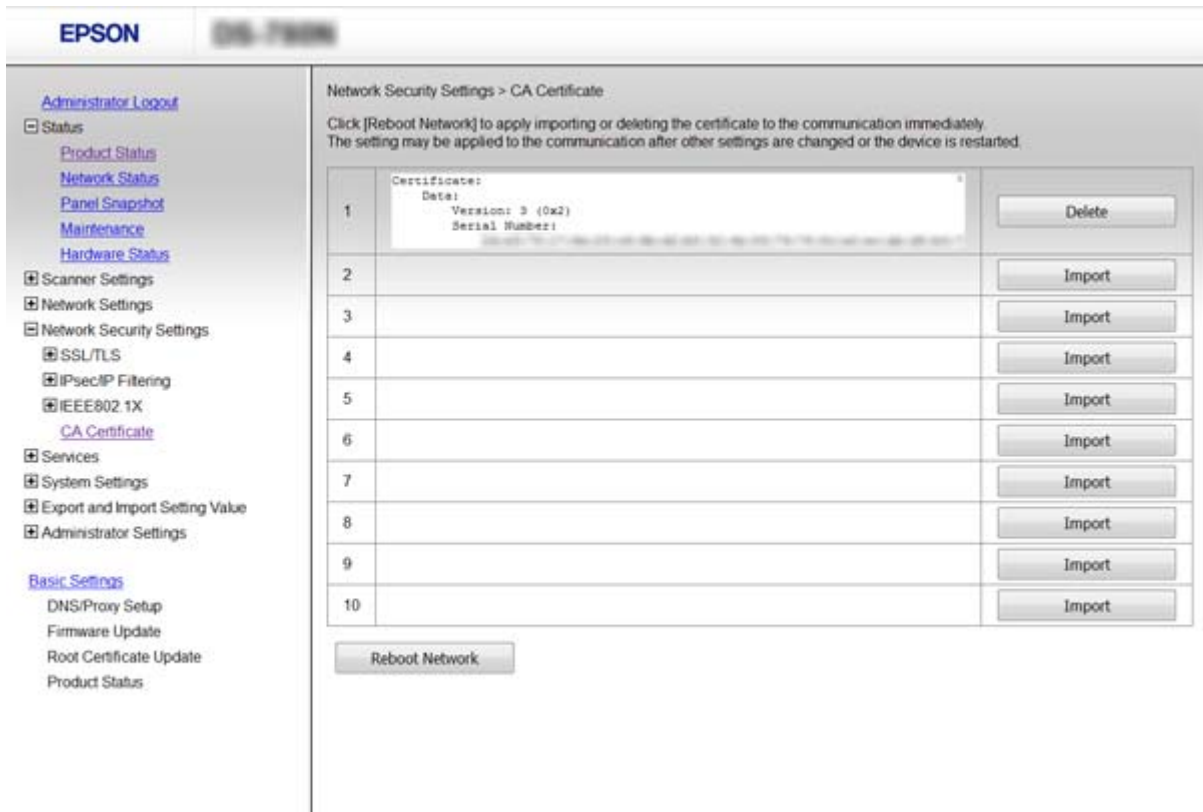
## CA Certificate -sertifikaatin poistaminen

Voit poistaa tuodun CA Certificate -sertifikaatin.

- Käytä Web Config -toimintoa ja valitse sitten **Network Security Settings > CA Certificate**.

## Suojauksen lisäasetukset (yrityskäyttäjät)

- Napsauta **Delete** CA Certificate poistettavan sertifikaatin vieressä.



- Vahvista näkyviin tulevassa viestissä, että haluat poistaa sertifikaatin.

### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

## Tiedonsiirron salaus IPsec-suojauksen ja IP-osoitteiden suodatuksen avulla

### Tietoja IPsec/IP Filtering -sovelluksesta

Jos skanneri tukee IPsec/IP-suodatustoimintoa, voit suodattaa liikennettä IP-osoitteiden, palvelujen ja porttien perusteella. Suodatuksen yhdistämisellä voit määrittää skannerin hyväksymään tai estämään tietyt asiakkaat ja määrättyt tiedot. Voit lisäksi parantaa suojaustasoa käyttämällä IPsec-protokollaa.

Kun haluat suodattaa liikennettä, määritä oletuskäytäntö. Oletuskäytäntö on voimassa jokaiselle käyttäjälle tai ryhmälle, joka kytkeytyy skanneriin. Jos haluat tarkempaa käyttäjien ja ryhmien hallintaa, määritä ryhmäkäytännöt. Ryhmäkäytäntö on yksi tai useampia sääntöjä, joita sovelletaan käyttäjään tai käyttäjäryhmään. Skanneri hallitsee IP-paketteja, jotka vastaavat määritettyjä käytäntöjä. IP-paketit todennetaan järjestyksessä: ryhmäkäytäntö 1–10 ja sitten oletuskäytäntö.

#### **Huomautus:**

Tietokoneet, joissa on Windows Vista tai uudempi tai Windows Server 2008 tai uudempi, tukevat IPsec:ia.

## Suojauksen lisäasetukset (yrityskäyttäjät)

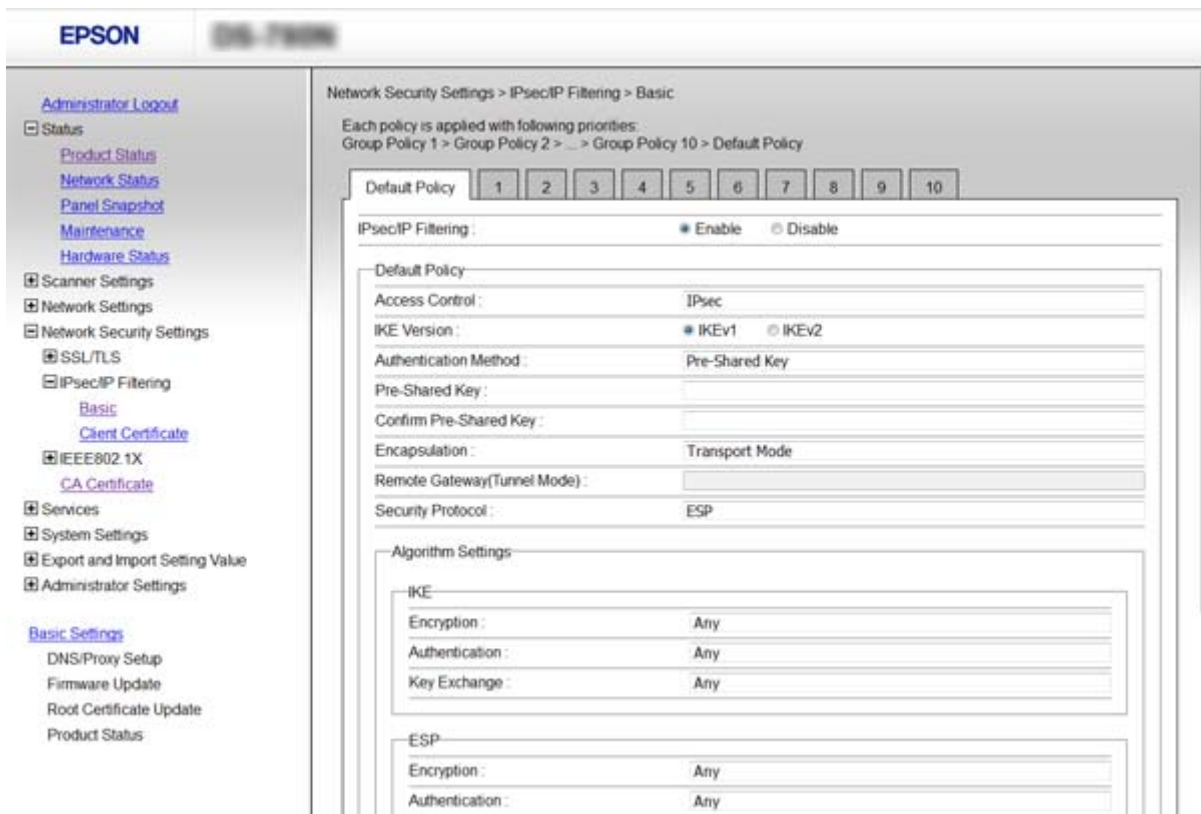
### Default Policy -määrittäminen

1. Käytä Web Config -toimintoa ja valitse **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Syötä arvo kullekin kohteelle.
3. Napsauta **Next**.  
Esiin tulee vahvistusviesti.
4. Napsauta **OK**.  
Skanneri on päivitetty.

#### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”Asetukset: Default Policy” sivulla 72

### Asetukset: Default Policy



Asetus	Asetusarvot ja kuvaus
IPsec/IP Filtering	Voit määrittää IPsec-suojauksen ja IP-osoitteiden suodatuksen käyttöön tai poistaa toiminnon käytöstä.



## Suojauksen lisäasetukset (yrityskäyttäjät)

Asetus	Asetusarvot ja kuvaus	
Access Control	Määritä hallintamenetelmä IP-pakettiliikenteelle.	
	Permit Access	Sallit määritettyjen IP-pakettien kulun valitsemalla tämän.
	Refuse Access	Estät määritettyjen IP-pakettien kulun valitsemalla tämän.
	IPsec	Sallit määritettyjen IPsec-pakettien kulun valitsemalla tämän.
IKE Version	Valitse IKE-versioksi IKEv1 tai IKEv2. Valitse jokin seuraavista sen mukaan, mihin laitteeseen skanneri on kytketty.	
IKEv1	Seuraavat kohteet näkyvät, kun <b>IKE Version</b> -arvoksi on valittu <b>IKEv1</b> .	
	Authentication Method	Jos valitset <b>Certificate</b> , CA:n allekirjoittama varmenne on hankittava etukäteen.
	Pre-Shared Key	Jos valitset <b>Authentication Method</b> -kohdassa <b>Pre-Shared Key</b> , anna esijaettu avain, jonka pituus on 1–127 merkkiä.
	Confirm Pre-Shared Key	Vahvista määritetty avain.
IKEv2	Seuraavat kohteet näkyvät, kun <b>IKE Version</b> -arvoksi on valittu <b>IKEv2</b> .	
Local	Authentication Method	Jos valitset <b>Certificate</b> , CA:n allekirjoittama varmenne on hankittava etukäteen.
	ID Type	Valitse skannerin tunnuksen tyyppi.
	ID	Kirjoita skannerin tunnus. Tunnuksen täytyy vastata tunnuksen tyyppiä. Ensimmäinen merkki ei saa olla @, # tai =. <b>Distinguished Name:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin = täytyy sisältyä merkkijonoon. <b>IP Address:</b> kirjoita IPv4- tai IPv6-muodossa oleva IP-osoite. <b>FQDN:</b> syötä 1–255 merkin yhdistelmä käyttämällä merkkejä A–Z, a–z, 0–9, - ja piste. <b>Email Address:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin @ täytyy sisältyä merkkijonoon. <b>Key ID:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E).
	Pre-Shared Key	Jos valitset <b>Authentication Method</b> -kohdassa <b>Pre-Shared Key</b> , anna esijaettu avain, jonka pituus on 1–127 merkkiä.
	Confirm Pre-Shared Key	Vahvista määritetty avain.

## Suojauksen lisäasetukset (yrityskäyttäjät)

Asetus	Asetusarvot ja kuvaus	
Remote	Authentication Method	Jos valitset <b>Certificate</b> , CA:n allekirjoittama varmenne on hankittava etukäteen.
	ID Type	Valitse todennettavan laitteen tunnustyyppi.
	ID	Kirjoita skannerin tunnus. Tunnuksen täytyy vastata tunnuksen tyyppiä. Ensimmäinen merkki ei saa olla @, # tai =. <b>Distinguished Name:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin = täytyy sisältyä merkkijonoon. <b>IP Address:</b> kirjoita IPv4- tai IPv6-muodossa oleva IP-osoite. <b>FQDN:</b> syötä 1–255 merkin yhdistelmä käyttämällä merkkejä A–Z, a–z, 0–9, - ja piste. <b>Email Address:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin @ täytyy sisältyä merkkijonoon. <b>Key ID:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E).
	Pre-Shared Key	Jos valitset <b>Authentication Method</b> -kohdassa <b>Pre-Shared Key</b> , anna esijaettu avain, jonka pituus on 1–127 merkkiä.
	Confirm Pre-Shared Key	Vahvista määritetty avain.
Encapsulation	Jos valitset <b>Access Control</b> -kohdassa <b>IPsec</b> , myös kapselointitila on määritettävä.	
	Transport Mode	Jos skanneria käytetään vain yhdessä lähiverkossa, valitse tämä. IP-paketit kerroksessa 4 ja sitä ylempänä salataan.
	Tunnel Mode	Valitse tämä vaihtoehto, jos käytät skanneria Internet-yhteensopivassa verkossa, kuten IPsec-VPN. IP-pakettien otsikko ja data salataan.
Remote Gateway(Tunnel Mode)	Jos valitset <b>Encapsulation</b> -kohdassa <b>Tunnel Mode</b> , anna yhdyskäytävän osoite, jonka pituus on 1–39 merkkiä.	
Security Protocol	Jos valitset <b>Access Control</b> -kohdassa <b>IPsec</b> , valitse asetus.	
	ESP	Varmistat todennuksen ja datan eheyden ja salaat datan valitsemalla tämän.
	AH	Varmistat todennuksen ja datan eheyden valitsemalla tämän. Voit käyttää IPsec-protokollaa, vaikka datan salausta olisi kiellettyä.
Algorithm Settings		
IKE	Encryption	Valitse IKE-salausalgoritmi. Valittavana olevat kohteet määräytyvät käytössä olevan IKE-version mukaan.
	Authentication	Valitse IKE-todennusalgoritmi.
	Key Exchange	Valitse IKE-avainvaihtoalgoritmi. Valittavana olevat kohteet määräytyvät käytössä olevan IKE-version mukaan.

## Suojauksen lisäasetukset (yrityskäyttäjät)

Asetus	Asetusarvot ja kuvaus	
ESP	Encryption	Valitse ESP-salausalgoritmi. Tämä valinta on käytettävissä, jos <b>ESP</b> on valittuna <b>Security Protocol</b> -kohdassa.
	Authentication	Valitse ESP-todennusalgoritmi. Tämä valinta on käytettävissä, jos <b>ESP</b> on valittuna <b>Security Protocol</b> -kohdassa.
AH	Authentication	Valitse AH-salausalgoritmi. Tämä valinta on käytettävissä, jos <b>AH</b> on valittuna <b>Security Protocol</b> -kohdassa.

### Liittyvät tiedot

➔ ”Default Policy -määrittäminen” sivulla 72

## Group Policy -määrittäminen

- Käytä Web Config -toimintoa ja valitse **Network Security Settings > IPsec/IP Filtering > Basic**.
- Napsauta sitä numeroitua välilehteä, jonka haluat määrittää.
- Syötä arvo kullekin kohteelle.
- Napsauta **Next**.  
Esiin tulee vahvistusviesti.
- Napsauta **OK**.  
Skanneri on päivitetty.

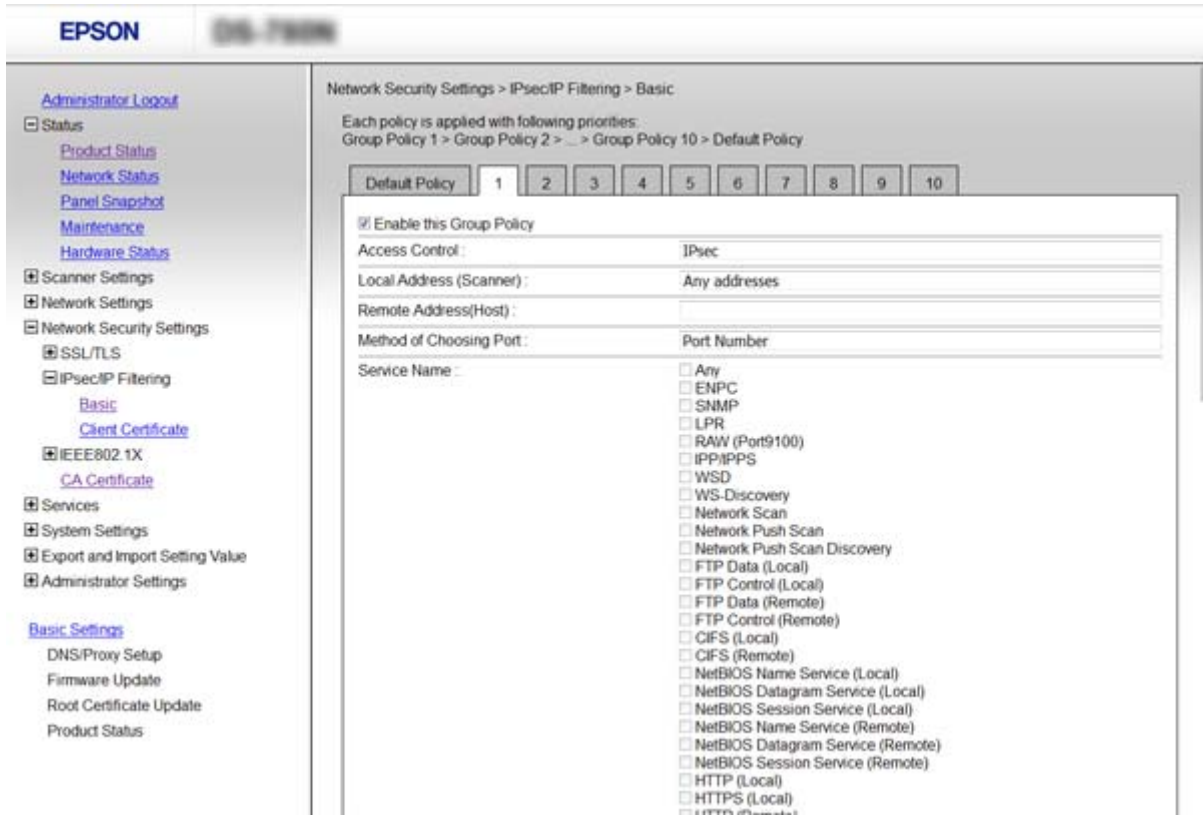
### Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

➔ ”Asetukset: Group Policy” sivulla 76

Suojauksen lisäasetukset (yrityskäyttäjät)

Asetukset: Group Policy



Asetus	Asetusarvot ja kuvaus	
Enable this Group Policy	Voit ottaa ryhmäkäytännön käyttöön tai poistaa sen käytöstä.	
Access Control	Määritä hallintamenetelmä IP-paketti liikenteelle.	
	Permit Access	Sallit määritettyjen IP-pakettien kulun valitsemalla tämän.
	Refuse Access	Estät määritettyjen IP-pakettien kulun valitsemalla tämän.
	IPsec	Sallit määritettyjen IPsec-pakettien kulun valitsemalla tämän.
Local Address (Scanner)	Valitse IPv4- tai IPv6-osoite, joka vastaa verkkoympäristöäsi. Jos IP-osoite määritetään automaattisesti, voit valita <b>Use auto-obtained IPv4 address</b> .	
Remote Address(Host)	Anna laitteen IP-osoite käytön hallintaa varten. IP-osoitteen enimmäispituus on 43 merkkiä. Jos et anna IP-osoitetta, kaikkia osoitteita hallitaan.  <b>Huomautus:</b> <i>Jos IP-osoite määritetään automaattisesti (esim. DHCP:n määrittämänä), yhteys ei ehkä ole käytettävissä. Määritä staattinen IP-osoite.</i>	
Method of Choosing Port	Valitse porttien määritysmenetelmä.	
Service Name	Jos valitset <b>Method of Choosing Port</b> -kohdassa <b>Service Name</b> , valitse vaihtoehto.	

## Suojauksen lisäasetukset (yrityskäyttäjät)

Asetus	Asetusarvot ja kuvaus	
Transport Protocol	Jos valitset <b>Method of Choosing Port</b> -kohdassa <b>Port Number</b> , myös kapselointitila on määritettävä.	
	Any Protocol	Valvo kaikkia protokollatyyppejä valitsemalla tämä.
	TCP	Valvo yksittäislähetysten dataa valitsemalla tämä.
	UDP	Valvo yleislähetysten ja monilähetysten dataa valitsemalla tämä.
	ICMPv4	Valvo ping-komentoa valitsemalla tämä.
Local Port	Jos valitset <b>Method of Choosing Port</b> -kohdassa <b>Port Number</b> ja <b>Transport Protocol</b> -kohdassa <b>TCP</b> tai <b>UDP</b> , anna porttien numerot vastaanotettavien pakettien valvontaa varten ja erota numerot toisistaan pilkuilla. Voit syöttää enintään 10 portin numeroa. Esimerkki: 20,80,119,5220 Jos et anna portin numeroa, kaikkia portteja hallitaan.	
Remote Port	Jos valitset <b>Method of Choosing Port</b> -kohdassa <b>Port Number</b> ja <b>Transport Protocol</b> -kohdassa <b>TCP</b> tai <b>UDP</b> , anna porttien numerot lähetettävien pakettien valvontaa varten ja erota numerot toisistaan pilkuilla. Voit syöttää enintään 10 portin numeroa. Esimerkki: 25,80,143,5220 Jos et anna portin numeroa, kaikkia portteja hallitaan.	
IKE Version	Valitse IKE-versioksi IKEv1 tai IKEv2. Valitse jokin seuraavista sen mukaan, mihin laitteeseen skanneri on kytketty.	
IKEv1	Seuraavat kohteet näkyvät, kun <b>IKE Version</b> -arvoksi on valittu <b>IKEv1</b> .	
	Authentication Method	Jos valitset <b>Access Control</b> -kohdassa <b>IPsec</b> , valitse vaihtoehto. Varmenteen käyttäminen on yleinen valinta oletuskäytäntöä käytettäessä.
	Pre-Shared Key	Jos valitset <b>Authentication Method</b> -kohdassa <b>Pre-Shared Key</b> , anna esijaettu avain, jonka pituus on 1–127 merkkiä.
	Confirm Pre-Shared Key	Vahvista määritetty avain.
IKEv2	Seuraavat kohteet näkyvät, kun <b>IKE Version</b> -arvoksi on valittu <b>IKEv2</b> .	

## Suojauksen lisäasetukset (yrityskäyttäjät)

Asetus	Asetusarvot ja kuvaus	
Local	Authentication Method	Jos valitset <b>Access Control</b> -kohdassa <b>IPsec</b> , valitse vaihtoehto. Varmenteen käyttäminen on yleinen valinta oletuskäytäntöä käytettäessä.
	ID Type	Valitse skannerin tunnuksen tyyppi.
	ID	<p>Kirjoita skannerin tunnus. Tunnuksen täytyy vastata tunnuksen tyyppiä.</p> <p>Ensimmäinen merkki ei saa olla @, # tai =.</p> <p><b>Distinguished Name:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin = täytyy sisältyä merkkijonoon.</p> <p><b>IP Address:</b> kirjoita IPv4- tai IPv6-muodossa oleva IP-osoite.</p> <p><b>FQDN:</b> syötä 1–255 merkin yhdistelmä käyttämällä merkkejä A–Z, a–z, 0–9, - ja piste.</p> <p><b>Email Address:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin @ täytyy sisältyä merkkijonoon.</p> <p><b>Key ID:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E).</p>
	Pre-Shared Key	Jos valitset <b>Authentication Method</b> -kohdassa <b>Pre-Shared Key</b> , anna esijaettu avain, jonka pituus on 1–127 merkkiä.
	Confirm Pre-Shared Key	Vahvista määritetty avain.
Remote	Authentication Method	Jos valitset <b>Access Control</b> -kohdassa <b>IPsec</b> , valitse vaihtoehto. Varmenteen käyttäminen on yleinen valinta oletuskäytäntöä käytettäessä.
	ID Type	Valitse todennettavan laitteen tunnustyyppi.
	ID	<p>Kirjoita skannerin tunnus. Tunnuksen täytyy vastata tunnuksen tyyppiä.</p> <p>Ensimmäinen merkki ei saa olla @, # tai =.</p> <p><b>Distinguished Name:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin = täytyy sisältyä merkkijonoon.</p> <p><b>IP Address:</b> kirjoita IPv4- tai IPv6-muodossa oleva IP-osoite.</p> <p><b>FQDN:</b> syötä 1–255 merkin yhdistelmä käyttämällä merkkejä A–Z, a–z, 0–9, - ja piste.</p> <p><b>Email Address:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E). Merkin @ täytyy sisältyä merkkijonoon.</p> <p><b>Key ID:</b> kirjoita 1–128 yksitavuista ASCII-merkkiä (0x20–0x7E).</p>
	Pre-Shared Key	Jos valitset <b>Authentication Method</b> -kohdassa <b>Pre-Shared Key</b> , anna esijaettu avain, jonka pituus on 1–127 merkkiä.
	Confirm Pre-Shared Key	Vahvista määritetty avain.

## Suojauksen lisäasetukset (yrityskäyttäjät)

Asetus	Asetusarvot ja kuvaus	
Encapsulation	Jos valitset <b>Access Control</b> -kohdassa <b>IPsec</b> , myös kapselointitila on määritettävä.	
	Transport Mode	Jos skanneria käytetään vain yhdessä lähiverkossa, valitse tämä. IP-paketit kerroksessa 4 ja sitä ylempänä salataan.
	Tunnel Mode	Valitse tämä vaihtoehto, jos käytät skanneria Internet-yhteensopivassa verkossa, kuten IPsec-VPN. IP-pakettien otsikko ja data salataan.
Remote Gateway(Tunnel Mode)	Jos valitset <b>Encapsulation</b> -kohdassa <b>Tunnel Mode</b> , anna yhdyskäytävän osoite, jonka pituus on 1–39 merkkiä.	
Security Protocol	Jos valitset <b>Access Control</b> -kohdassa <b>IPsec</b> , valitse vaihtoehto.	
	ESP	Varmistat todennuksen ja datan eheyden ja salaat datan valitsemalla tämän.
	AH	Varmistat todennuksen ja datan eheyden valitsemalla tämän. Voit käyttää IPsec-protokollaa, vaikka datan salaus olisi kiellettyä.
Algorithm Settings		
IKE	Encryption	Valitse IKE-salausalgoritmi. Valittavana olevat kohteet määräytyvät käytössä olevan IKE-version mukaan.
	Authentication	Valitse IKE-todennusalgoritmi.
	Key Exchange	Valitse IKE-avainvaihtoalgoritmi. Valittavana olevat kohteet määräytyvät käytössä olevan IKE-version mukaan.
ESP	Encryption	Valitse ESP-salausalgoritmi. Tämä valinta on käytettävissä, jos <b>ESP</b> on valittuna <b>Security Protocol</b> -kohdassa.
	Authentication	Valitse ESP-todennusalgoritmi. Tämä valinta on käytettävissä, jos <b>ESP</b> on valittuna <b>Security Protocol</b> -kohdassa.
AH	Authentication	Valitse AH-todennusalgoritmi. Tämä valinta on käytettävissä, jos <b>AH</b> on valittuna <b>Security Protocol</b> -kohdassa.

## Liittyvät tiedot

- ➔ ”Group Policy -määrittys” sivulla 75
- ➔ ”Kohteiden Local Address (Scanner) ja Remote Address(Host) yhdistelmä kohdassa Group Policy” sivulla 80
- ➔ ”Palvelun nimeä koskevat viittaukset ryhmäkäytännöissä” sivulla 80

## Suojauksen lisäasetukset (yrityskäyttäjät)

## Kohteiden Local Address (Scanner) ja Remote Address(Host) yhdistelmä kohdassa Group Policy

		Local Address (Scanner) -asetus		
		IPv4	IPv6* <sup>2</sup>	Any addresses* <sup>3</sup>
Remote Address(Host) -asetus	IPv4* <sup>1</sup>	✓	–	✓
	IPv6* <sup>1</sup> , * <sup>2</sup>	–	✓	✓
	Tyhjä	✓	✓	✓

\*1 Jos **IPsec** on valittuna kohdassa **Access Control**, esiasetettua pituutta ei voida määrittää.

\*2 Jos **IPsec** on valittuna kohdassa **Access Control**, voit valita linkin paikallisen osoitteen (fe80::), mutta ryhmäkäytäntö poistuu käytöstä.

\*3 IPv6-linkkien paikallisia osoitteita lukuun ottamatta.

## Palvelun nimeä koskevat viittaukset ryhmäkäytännöissä

**Huomautus:**

*Ei-käytettävissä olevat palvelut näytetään, mutta niitä ei voi valita.*

Palvelun nimi	Protokollatyyppi	Paikallisen portin numero	Etäportin numero	Ohjatut ominaisuudet
Any	–	–	–	Kaikki palvelut
ENPC	UDP	3289	Mikä tahansa portti	Skannerin haku sovelluksista, kuten EpsonNet Config ja skanneriohjain
SNMP	UDP	161	Mikä tahansa portti	MIB:n hakeminen ja määrittys sovelluksista, kuten EpsonNet Config ja Epson-skanneriohjain
WSD	TCP	Mikä tahansa portti	5357	WSD-ohjaus
WS-Discovery	UDP	3702	Mikä tahansa portti	Skannerin haku kohteesta WSD
Network Scan	TCP	1865	Mikä tahansa portti	Skannaustietojen edelleenlähetys kohteesta Document Capture Pro
Network Push Scan Discovery	UDP	2968	Mikä tahansa portti	Tietokoneen etsiminen skannerista.
Network Push Scan	TCP	Mikä tahansa portti	2968	Push-skannaustyön tietojen hakeminen Document Capture Pro- tai Document Capture -sovelluksesta
HTTP (Local)	TCP	80	Mikä tahansa portti	HTTP(S)-palvelin (Web Config- ja WSD-tietojen edelleenlähetys)
HTTPS (Local)	TCP	443	Mikä tahansa portti	



## Suojauksen lisäasetukset (yrityskäyttäjät)

Palvelun nimi	Protokollatyyppi	Paikallisen portin numero	Etäportin numero	Ohjatut ominaisuudet
HTTP (Remote)	TCP	Mikä tahansa portti	80	HTTP(S)-asiakasohjelma (laiteohjelmistopäivityksen ja päävarmenepäivityksen välinen tiedonsiirto)
HTTPS (Remote)	TCP	Mikä tahansa portti	443	

## IPsec/IP Filtering -konfigurointiesimerkit

### Vain IPsec-pakettien vastaanotto

Tämä esimerkki on vain oletuskäytännön määrittystä varten.

#### Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: IPsec
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: Syötä enintään 127 merkkiä.

#### Group Policy:

Älä määritä.

### Skannauksen hyväksyminen Epson Scan 2 -ohjelmasta ja skannerin asetukset

Tässä esimerkissä skannaustietoja ja skanneriasetuksia koskeva tietoliikenne sallitaan tietyistä laitteista.

#### Default Policy:

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

#### Group Policy:

- Enable this Group Policy: Valitse ruutu.
- Access Control: Permit Access
- Remote Address(Host): Asiakkaan IP-osoite
- Method of Choosing Port: Service Name
- Service Name: Valitse ruutu kohdassa ENPC, SNMP, Network Scan, HTTP (Local) ja HTTPS (Local).

### Käytön sallinta vain määrittystä IP-osoitteesta

Tässä esimerkissä skannerin käyttö sallitaan määrätylle IP-osoitteelle.

#### Default Policy:

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

#### Group Policy:

- Enable this Group Policy: Valitse ruutu.
- Access Control: Permit Access

## Suojauksen lisäasetukset (yrityskäyttäjät)

**Remote Address(Host):** Järjestelmänvalvojan asiakkaan IP-osoite

**Huomautus:**

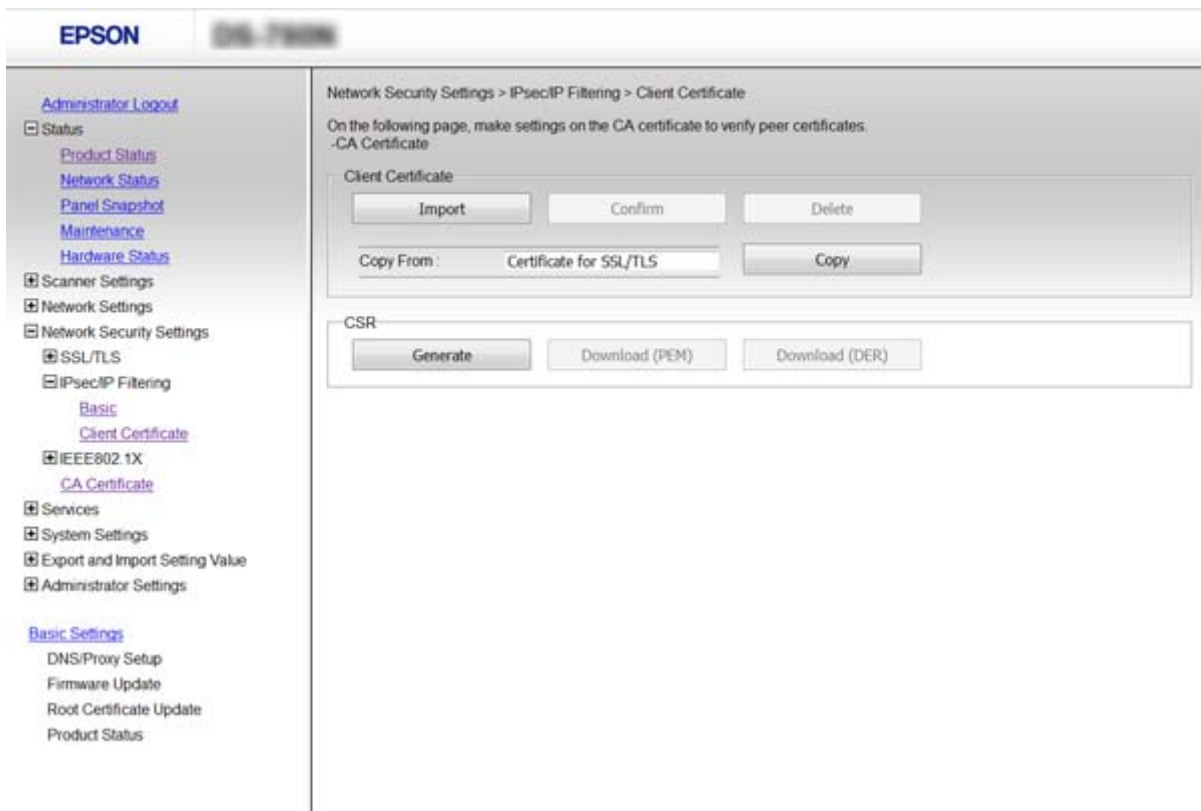
Asiakas voi käyttää skanneria ja määrittää sen riippumatta käytännön määrittämisestä.

## IPsec/IP Filtering-sertifikaatin määrittäminen

Määritä Asiakassertifikaatti IPsec/IP-suodatukselle. Jos haluat määrittää sertifiointivaltuudet, siirry kohtaan **CA Certificate**.

1. Käytä Web Config -toimintoa ja valitse **Network Security Settings > IPsec/IP Filtering > Client Certificate**.
2. Tuo sertifikaatti kohteesta **Client Certificate**.

Jos olet jo tuonut sertifikaatin sen myöntäjältä IEEE802.1X- tai SSL/TLS-yhteydellä, voit kopioida sertifikaatin ja käyttää sitä IPsec/IP-suodatuksessa. Voit kopioida sertifikaatin valitsemalla sen **Copy From** -toiminnolla ja napsauttamalla sitten **Copy**.



### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”CA:n allekirjoittaman varmenteen hankinta ja tuonti” sivulla 64

---

# SNMPv3-protokollan käyttö

## Tietoja SNMPv3-protokollasta

SNMP-protokolla kerää tietoja verkkoon kytketyistä laitteista verkon valvontaa ja hallintaa varten. SNMPv3 on protokollan versio, jossa tietoturvaa ja hallintatoimintoja on kehitetty entistä pidemmälle.

SNMPv3-protokollaa käytettäessä SNMP-tiedonsiirron (pakettien) tilanvalvonta ja asetustoiminnot voidaan todentaa ja salata SNMP-tiedonsiirron suojaamiseksi tietoturvariskeiltä, kuten salakuuntelulta, toiseksi järjestelmäksi tai käyttäjäksi tekeytymiseltä ja tietojen luvattomalta muokkaamiselta.

## SNMPv3-määrittäminen

Jos skanneri tukee SNMPv3-protokollaa, voit valvoa ja hallita skannerin käyttöä.

1. Käytä Web Config -toimintoa ja valitse **Services > Protocol**.
2. Syötä arvo kullekin **SNMPv3 Settings**-kohteelle.
3. Napsauta **Next**.  
Esiin tulee vahvistusviesti.
4. Napsauta **OK**.  
Skanneri on päivitetty.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”SNMPv3-asetuskohteet” sivulla 84

**Suojauksen lisäasetukset (yrityskäyttäjät)**

**SNMPv3-asetuskohteet**

Kohdat	Asetukset ja selitys
Enable SNMPv3	SNMPv3 on käytössä, kun ruutu on valittu.
User Name	Syötä 1–32 merkkiä käyttämällä 1 tavun merkkejä.
Authentication Settings	
Algorithm	Valitse algoritmi todennusta varten.
Password	Syötä 8–32 merkkiä ASCII-muodossa (0x20-0x7E).
Confirm Password	Syötä salasana, jonka määritit vahvistukselle.
Encryption Settings	
Algorithm	Valitse algoritmi salausta varten.
Password	Syötä 8–32 merkkiä ASCII-muodossa (0x20-0x7E).
Confirm Password	Syötä salasana, jonka määritit vahvistukselle.
Context Name	Syötä 1–32 merkkiä käyttämällä 1 tavun merkkejä.

**Liittyvät tiedot**

➔ ”SNMPv3-määrittäminen” sivulla 83

# Skannerin kytkentä IEEE802.1X-verkkoon

## IEEE802.1X-verkon määrittäminen

Jos skanneri tukee IEEE802.1X-protokollaa, voit käyttää skanneria todennetussa verkossa, joka on kytketty RADIUS-palvelimeen, ja keskittimen toimiessa todentajana.

1. Avaa Web Config -toiminto ja valitse **Network Security Settings > IEEE802.1X > Basic**.
2. Syötä arvo kullekin kohteelle.
3. Valitse **Next**.  
Esiin tulee vahvistusviesti.
4. Valitse **OK**.  
Skanneri on päivitetty.

### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”IEEE802.1X-verkon asetuskohdeet” sivulla 85
- ➔ ”Tulostimen tai skannerin käyttö ei onnistu IEEE802.1X-asetusten määrittämisen jälkeen” sivulla 90

## IEEE802.1X-verkon asetuskohdeet

EPSON

Administrator Logout

Status

Product Status

Network Status

Panel Snapshot

Maintenance

Hardware Status

Scanner Settings

Network Settings

Network Security Settings

SSL/TLS

IPsec/IP Filtering

IEEE802.1X

Basic

Client Certificate

CA Certificate

Services

System Settings

Export and Import Setting Value

Administrator Settings

Basic Settings

DNS/Proxy Setup

Firmware Update

Root Certificate Update

Product Status

Network Security Settings > IEEE802.1X > Basic

IEEE802.1X (Wired LAN):  Enable  Disable

EAP Type: EAP-TLS

User ID:

Password:

Confirm Password:

Server ID:

Certificate Validation:  Enable  Disable

Anonymous Name:

Encryption Strength: Middle

Next

## Suojauksen lisäasetukset (yrityskäyttäjät)

Asetus	Asetusarvot ja kuvaus	
IEEE802.1X (Wired LAN)	Voit ottaa sivun asetuksia käyttöön tai poistaa ne käytöstä ( <b>IEEE802.1X &gt; Basic</b> ) kohteelle IEEE802.1X (kiinteä LAN).	
EAP Type	Valitse varmennusmenetelmä skannerin ja RADIUS-palvelimen välillä.	
	EAP-TLS	Sinun on hankittava ja tuotava CA:n allekirjoittama varmenne.
	PEAP-TLS	
	PEAP/MSCHAPv2	Sinun on määritettävä salasana.
User ID	Määritä tunnus RADIUS-palvelimen varmennukselle. Syötä 1–128 yksitavuista ASCII (0x20–0x7E) -merkkiä.	
Password	Todenna skanneri määrittämällä salasana. Syötä 1–128 yksitavuista ASCII (0x20–0x7E) -merkkiä. Jos käytät Windows-palvelinta, kuten RADIUS-palvelin, voit syöttää enintään 127 merkkiä.	
Confirm Password	Anna salasana, jonka määritit vahvistusta varten.	
Server ID	Voit määrittää palvelintunnuksen, jolla varmennetaan määritetty RADIUS-palvelin. Varmentaja tarkistaa sisältykö palvelintunnus siihen palvelinsertifikaatin aihe/subjectAltName-kenttään, joka on lähetetty RADIUS-palvelimelta. Syötä 0–128 yksitavuista ASCII (0x20–0x7E) -merkkiä.	
Certificate Validation	Voit asettaa sertifikaatin vahvistuksen todentamismenetelmästä riippumatta. Tuo sertifikaatti kohteesta <b>CA Certificate</b> .	
Anonymous Name	Jos valitset <b>PEAP-TLS</b> tai <b>PEAP/MSCHAPv2</b> valinnalle <b>Authentication Method</b> , voit määrittää anonyymin nimen käyttäjätunnuksen sijasta PEAP-todennuksen vaiheelle 1. Syötä 0–128 yksitavuista ASCII (0x20–0x7E) -merkkiä.	
Encryption Strength	Voit valita jonkin seuraavista.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

### Liittyvät tiedot

➔ ”IEEE802.1X-verkon määrittäminen” sivulla 85

## IEEE802.1X-sertifikaatin määrittäminen

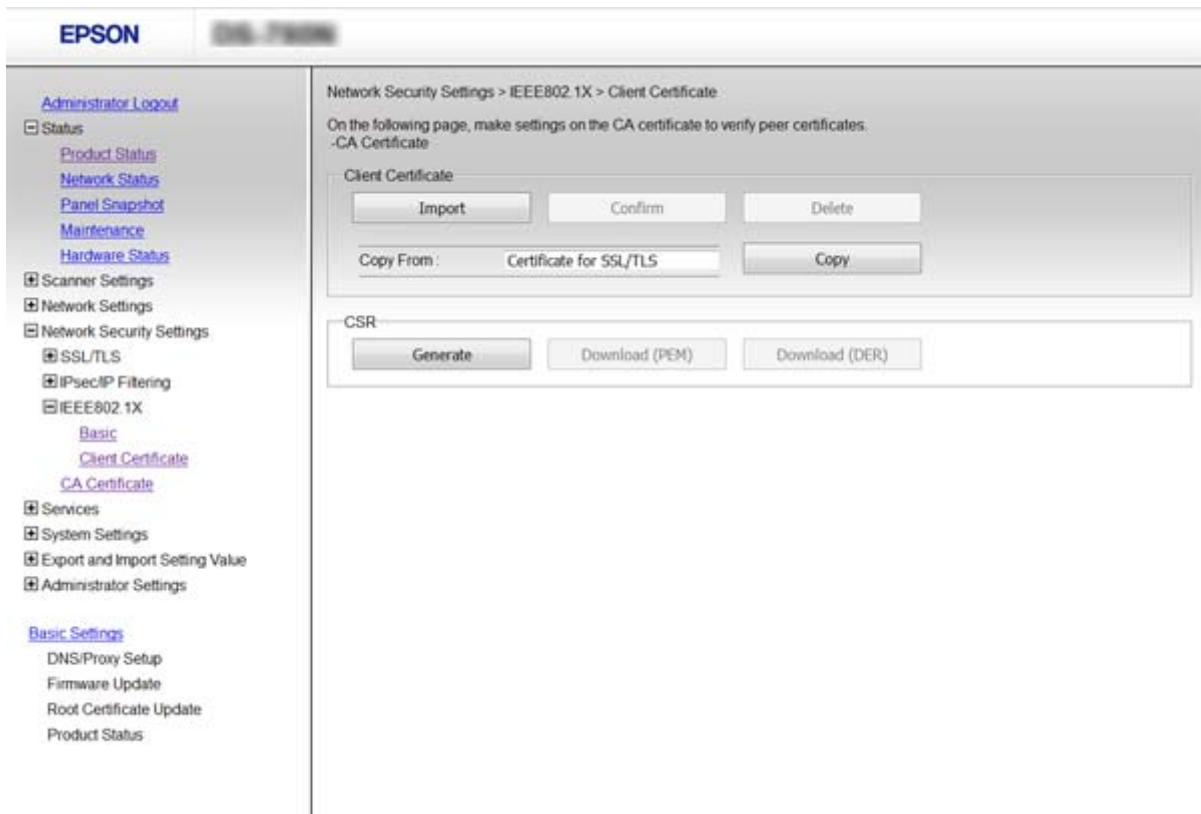
Määritä IEEE802.1X:n asiakassertifikaatti. Jos haluat määrittää sertifiointivaltuuden sertifikaatin, siirry kohtaan **CA Certificate**.

- Käytä Web Config -toimintoa ja valitse **Network Security Settings > IEEE802.1X > Client Certificate**.

## Suojauksen lisäasetukset (yrityskäyttäjät)

### 2. Syötä sertifikaatti kohtaan **Client Certificate**.

Voit kopioida sertifikaatin, jos se on Sertifikaatin myöntäjän julkaisema. Voit kopioida sertifikaatin valitsemalla sen **Copy From** -toiminnolla ja napsauttamalla sitten **Copy**.



### Liittyvät tiedot

- ➔ ”Web Config -ohjelmiston käyttö” sivulla 23
- ➔ ”CA:n allekirjoittaman varmenteen hankinta ja tuonti” sivulla 64

## Tietosuojaan liittyvien ongelmien ratkaiseminen

### Suojausasetusten palautus

Jos käyttöympäristössä käytetään vahvaa suojausta, kuten IPsec-suojausta, IP-osoitteiden suodatusta tai IEEE802.1X-suojausta, voit joutua tilanteeseen, jossa et saa yhteyttä laitteeseen virheellisten asetusten tai muiden laitteessa tai palvelimessa esiintyvien ongelmien vuoksi. Tällöin voit palauttaa suojausasetukset ja määrittää asetukset sitten uudelleen tai käyttää laitetta tilapäisesti ilman suojausasetuksia.

### Suojaustoiminnon poistaminen käytöstä ohjauspaneelin kautta

Voit poistaa IPsec-suojauksen, IP-osoitteiden suodatuksen ja IEEE802.1X-suojauksen käytöstä skannerin ohjauspaneelin kautta.

1. Valitse **Asetukset > Verkkoasetukset**.

## Suojauksen lisäasetukset (yrityskäyttäjät)

2. Valitse **Muuta asetuksia**.
3. Valitse toiminnot, jotka haluat poistaa käytöstä.
  - IPsec/IP-suodatus
  - IEEE802.1X
4. Kun valmis-viesti tulee näkyviin, valitse **Jatka**.

## Suojaustoiminnon palauttaminen Web Config -hallintasivun kautta

Jos käytössä on IEEE802.1X-suojaus, verkon laitteita ei ehkä tunnisteta oikein. Tällöin voit tarvittaessa poistaa toiminnon käytöstä skannerin ohjauspaneelistä.

Jos IPsec-suojaus tai IP-osoitteiden suodatus on käytössä, voit poistaa toiminnot käytöstä, jos voit käyttää laitetta tietokoneen kautta.

### ***IPsec-suojauksen ja IP-osoitteiden suodatuksen poistaminen käytöstä Web Config -hallintasivulla***

1. Avaa Web Config -toiminto ja valitse **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Valitse **Default Policy** -kohdassa **IPsec/IP Filtering** -arvoksi **Disable**.
3. Valitse **Next** ja poista sitten **Enable this Group Policy** -valinta kaikkien ryhmäkäytäntöjen kohdalta.
4. Valitse **OK**.

#### **Liittyvät tiedot**

➔ [”Web Config -ohjelmiston käyttö” sivulla 23](#)

## Ongelmia verkon suojaustoimintojen käytössä

### **Unohtunut esijaettu avain**

#### **Määritä avain uudelleen käyttämällä Web Config -ohjelmistoa.**

Kun haluat muuttaa avaimen, siirry toimintoon Web Config ja valitse **Network Security Settings > IPsec/IP Filtering > Basic > Default Policy** tai **Group Policy**.

Jos esijaettu avain vaihdetaan, uusi esijaettu avain on määritettävä tietokoneisiin.

#### **Liittyvät tiedot**

➔ [”Web Config -ohjelmiston käyttö” sivulla 23](#)



## Suojauksen lisäasetukset (yrityskäyttäjät)

## Tiedonsiirto IPsec-yhteydellä ei toimi

## Käytätkö tietokoneen asetuksille algoritmia, jota ei tueta?

Skanneri tukee seuraavia algoritmeja.

Suojausmenetelmät	Algoritmit
IKE-salausalgoritmi	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-todennusalgoritmi	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE-avaintenvaihtoalgoritmi	DH-ryhmä 1, DH-ryhmä 2, DH-ryhmä 5, DH-ryhmä 14, DH-ryhmä 15, DH-ryhmä 16, DH-ryhmä 17, DH-ryhmä 18, DH-ryhmä 19, DH-ryhmä 20, DH-ryhmä 21, DH-ryhmä 22, DH-ryhmä 23, DH-ryhmä 24, DH-ryhmä 25, DH-ryhmä 26, DH-ryhmä 27*, DH-ryhmä 28*, DH-ryhmä 29*, DH-ryhmä 30*
ESP-salausalgoritmi	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-todennusalgoritmi	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-todennusalgoritmi	SHA-1, SHA-256, SHA-384, SHA-512, MD5

\* Vain IKEv2-versiossa

## Liittyvät tiedot

➔ ”Tiedonsiirron salaus IPsec-suojauksen ja IP-osoitteiden suodatuksen avulla” sivulla 71

## Tiedonsiirto ei yllättäen onnistu

## Onko skannerin IP-osoite väärä tai onko se muuttunut?

Poista IPsec käytöstä skannerin ohjauspaneelist.

Jos DHCP-varaus on vanhentunut tai reititin käynnistetty uudelleen tai jos IPv6-osoite on vanhentunut tai osoitetta ei ole saatu, skannerille Web Config -määrittelyssä rekisteröityä IP-osoitetta (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Local Address (Scanner)**) ei ehkä löydy.

Käytä staattista IP-osoitetta.

## Onko tietokoneen IP-osoite väärä tai onko se muuttunut?

Poista IPsec käytöstä skannerin ohjauspaneelist.

Jos DHCP-varaus on vanhentunut tai reititin käynnistetty uudelleen tai jos IPv6-osoite on vanhentunut tai osoitetta ei ole saatu, skannerille Web Config -määrittelyssä rekisteröityä IP-osoitetta (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Remote Address(Host)**) ei ehkä löydy.

Käytä staattista IP-osoitetta.

## Liittyvät tiedot

➔ ”Web Config -ohjelmiston käyttö” sivulla 23

➔ ”Tiedonsiirron salaus IPsec-suojauksen ja IP-osoitteiden suodatuksen avulla” sivulla 71

## Yhdistäminen ei onnistu IPsec/IP-suodatuksen jälkeen

### Asetettu arvo voi olla väärä.

Ota IPsec/IP-suodatus pois käytöstä skannerin ohjauspaneelistä. Liitä skanneri tietokoneeseen ja määritä IPsec/IP-suodatusasetukset uudelleen.

### Liittyvät tiedot

➔ [”Tiedonsiirron salaus IPsec-suojauksen ja IP-osoitteiden suodatuksen avulla” sivulla 71](#)

## Tulostimen tai skannerin käyttö ei onnistu IEEE802.1X-asetusten määrittämisen jälkeen

### Asetukset saattavat olla väärät.

Poista IEEE802.1X käytöstä skannerin ohjauspaneelistä. Liitä skanneri tietokoneeseen ja määritä IEEE802.1X-asetukset uudelleen.

### Liittyvät tiedot

➔ [”IEEE802.1X-verkon määrittäminen” sivulla 85](#)

## Ongelmia digitaalisen varmenteen käytössä

### CA:n allekirjoittaman varmenteen tuonti ei onnistu

#### Täsmäävätkö CA:n allekirjoittama varmenne ja CSR:n tiedot?

Jos CA:n allekirjoittamassa varmenteessa ja CSR-pyyntössä ei ole samoja tietoja, CSR-pyyntöä ei voi tuoda. Tarkista seuraava:

- Yritätkö tuoda varmennetta laitteeseen, jolla ei ole samoja tietoja?  
Tarkista CSR:n tiedot ja tuo sitten varmenne laitteeseen, jossa on samat tiedot.
- Korvasitko skanneriin tallennetun CSR:n sen jälkeen, kun lähetit CSR:n varmenneviranomaisille?  
Hanki CA:n allekirjoittama varmenne jälleen CSR-pyyntöllä.

#### Onko CA:n allekirjoittaman varmenteen koko suurempi kuin 5 kt?

Et pysty tuomaan CA:n allekirjoittamaa varmennetta, joka on suurempi kuin 5 kt.

#### Onko varmenteen tuonnin salasana oikein?

Jos unohdat salasanan, et voi tuoda varmennetta.

### Liittyvät tiedot

➔ [”CA:n allekirjoittaman varmenteen tuonti” sivulla 66](#)

## Suojauksen lisäasetukset (yrityskäyttäjät)

### Itse allekirjoitetun varmenteen päivitys ei onnistu

#### Onko annettu Common Name?

Common Name on annettava.

#### Onko syötetty tukemattomia merkkejä kohdassa Common Name? Esimerkiksi japania ei tueta.

Syötä 1–128 merkkiä joko IPv4-, IPv6-, isäntänimi- tai FQDN-muodossa ASCII-merkkeinä (0x20-0x7E).

#### Onko Common Name -arvossa pilkkua tai välilyöntiä?

Jos siihen lisätään pilkku, Common Name jaetaan kyseisestä kohdasta. Jos lisätään vain välilyönti pilkkua ennen tai sen jälkeen, tapahtuu virhe.

#### Liittyvät tiedot

➔ [”Itse allekirjoitetun varmenteen päivitys” sivulla 68](#)

### CSR:n luonti ei onnistu

#### Onko annettu Common Name?

Common Name on annettava.

#### Onko syötetty tukemattomia merkkejä kohtiin Common Name, Organization, Organizational Unit, Locality, State/Province? Esimerkiksi japania ei tueta.

Syötä merkit joko IPv4-, IPv6-, isäntänimi- tai FQDN-muodossa ASCII-merkkeinä (0x20-0x7E).

#### Onko Common Name -arvossa pilkkua tai välilyöntiä?

Jos siihen lisätään pilkku, Common Name jaetaan kyseisestä kohdasta. Jos lisätään vain välilyönti pilkkua ennen tai sen jälkeen, tapahtuu virhe.

#### Liittyvät tiedot

➔ [”CA:n allekirjoittaman varmenteen hankinta” sivulla 64](#)

### Esiin tulee varoitus, joka liittyy digitaaliseen varmenteeseen

Viestit	Syy/Mitä tehdä
Enter a Server Certificate.	<p><b>Syy:</b> Et ole valinnut tuotavaa tiedostoa.</p> <p><b>Mitä tehdä:</b> Valitse tiedosto ja napsauta <b>Import</b>.</p>

**Suojauksen lisäasetukset (yrityskäyttäjät)**

Viestit	Syy/Mitä tehdä
CA Certificate 1 is not entered.	<p><b>Syy:</b> CA-varmennetta 1 ei ole annettu ja vain CA-varmenne 2 on annettu.</p> <p><b>Mitä tehdä:</b> Tuo CA-varmenne 1 ensin.</p>
Invalid value below.	<p><b>Syy:</b> Tiedostopolussa ja/tai salasanassa on tukemattomia merkkejä.</p> <p><b>Mitä tehdä:</b> Varmista, että merkit annetaan oikein kohteelle.</p>
Invalid date and time.	<p><b>Syy:</b> Skanneriin ei ole asetettu päivämäärää ja kellonaikaa.</p> <p><b>Mitä tehdä:</b> Aseta päivämäärä ja kellonaika Web Config- tai EpsonNet Config -ohjelmiston avulla.</p>
Invalid password.	<p><b>Syy:</b> CA-varmenteelle asetettu salasana ja annettu salasana eivät täsmää.</p> <p><b>Mitä tehdä:</b> Anna oikea salasana.</p>
Invalid file.	<p><b>Syy:</b> Et tuo varmennetiedostoa X509-muodossa.</p> <p><b>Mitä tehdä:</b> Varmista, että valitset oikean varmenteen, jonka luotettu varmenneviranomaisen on lähettänyt.</p>
	<p><b>Syy:</b> Tuotu tiedosto on liian suuri. Tiedoston maksimikoko on 5 kt.</p> <p><b>Mitä tehdä:</b> Jos valitset oikean tiedoston, varmenne saattaa olla vioittunut tai virheellinen.</p>
	<p><b>Syy:</b> Varmenteeseen sisältyvä ketju on väärä.</p> <p><b>Mitä tehdä:</b> Katso lisätietoja varmenteesta varmenneviranomaisen verkkosivustosta.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p><b>Syy:</b> PKCS#12-muodossa oleva varmennetiedosto sisältää 3 CA-varmennetta.</p> <p><b>Mitä tehdä:</b> Tuo jokainen varmenne aivan kuten muuntaisit sen PKCS#12-muodosta PEM-muotoon, tai tuo PKCS#12-muotoinen varmennetiedosto, joka sisältää enintään 2 CA-varmennetta.</p>

## Suojauksen lisäasetukset (yrityskäyttäjät)

Viestit	Syy/Mitä tehdä
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p><b>Syy:</b> Varmenne on vanhentunut.</p> <p><b>Mitä tehdä:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Jos varmenne on vanhentunut, hanki ja tuo uusi varmenne.</li> <li><input type="checkbox"/> Jos varmenne ei ole vanhentunut, varmista, että skannerin päivämäärä ja kellonaika on asetettu oikein.</li> </ul>
Private key is required.	<p><b>Syy:</b> Varmenteessa ei ole yksityistä avainparia.</p> <p><b>Mitä tehdä:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Jos varmenne on PEM/DER-muodossa ja se saadaan CSR-pyyntöstä tietokoneen avulla, määritä yksityisen avaimen tiedosto.</li> <li><input type="checkbox"/> Jos varmenne on PKCS#12-muodossa ja se saadaan CSR-pyyntöstä tietokoneen avulla, luo tiedosto, joka sisältää yksityisen avaimen.</li> </ul>
	<p><b>Syy:</b> Olet tuonut uudelleen PEM/DER-varmenteen, joka on saatu CSR-pyyntöstä Web Config -ohjelmiston avulla.</p> <p><b>Mitä tehdä:</b> Jos varmenne on PEM/DER-muodossa ja se saadaan CSR-pyyntöstä Web Config -ohjelmiston avulla, voit tuoda sen vain kerran.</p>
Setup failed.	<p><b>Syy:</b> Määrittystä ei voi suorittaa loppuun, koska yhteys skannerin ja tietokoneen välillä epäonnistui tai tiedostoa ei voida lukea joidenkin virheiden vuoksi.</p> <p><b>Mitä tehdä:</b> Sen jälkeen kun olet tarkistanut kyseisen tiedoston ja yhteyden, tuo tiedosto uudelleen.</p>

**Liittyvät tiedot**

➔ ”Tietoja digitaalisesta varmennuksesta” sivulla 63

**CA:n allekirjoittaman varmenteen poisto tahattomasti****Onko varmenteelle olemassa varmuuskopiota?**

Jos varmuuskopio on olemassa, tuo varmenne uudelleen.

Jos saat CSR-pyyntöä käyttämällä varmenteen, joka on luotu Web Config -ohjelmistosta, et voi tuoda poistettua varmennetta uudelleen. Luo CSR ja hanki uusi varmenne.

**Liittyvät tiedot**

➔ ”CA:n allekirjoittaman varmenteen poisto” sivulla 67

➔ ”CA:n allekirjoittaman varmenteen tuonti” sivulla 66