EPSON
EXCEED YOUR VISION

Tīkla vednis

NPD5771-00 LV

Satura rādītājs

Pielikums

Autortiesības

Preču zīmes

- EPSON® ir reģistrēta preču zīme, un EPSON EXCEED YOUR VISION vai EXCEED YOUR VISION ir Seiko Epson Corporation preču zīme.
- Epson Scan 2 programmatūra ir daļēji balstīta uz Independent JPEG Group.
- Google Cloud Print™, Chrome™, Chrome OS™ un Android™ ir Google Inc. reģistrētas preču zīmes.
- Microsoft®, Windows®, Windows Server® un Windows Vista® ir reģistrētas Microsoft Corporation preču zīmes.
- IBM ir reģistrēta International Business Machines Corporation preču zīme.
- Vispārīga norāde. Citi šeit izmantotie produktu nosaukumi ir paredzēti tikai identificēšanai, un tie var būt to attiecīgo īpašnieku preču zīmes. Epson nepretendē uz jebkādām šo preču zīmju tiesībām.

Par šo rokasgrāmatu

Apzīmējumi un simboli

> ***Uzmanību!***
> *Norādījumi, kas ir rūpīgi jāievēro, lai izvairītos no traumām.*

> ***Svarīgi!***
> *Norādījumi, kas ir jāievēro, lai izvairītos no aprīkojuma bojājumiem.*

> ***Piezīme.***
> *Norādījumi, kas ietver noderīgus padomus par printera darbību un darbības ierobežojumiem.*

Saistītā informācija

➡ Noklikšķinot uz šīs ikonas, tiks parādīta saistītā informācija.

Šajā rokasgrāmatā izmantotie apraksti

Šajā rokasgrāmatā izmantotie printera attēli ir tikai piemēri. Lai gan var būt nelielas atšķirības atkarībā no modeļa, darbības metode ir tāda pati.

Operētājsistēmu atsauces

Windows

Šajā rokasgrāmatā tādi termini kā „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Vista”, „Windows XP”, „Windows Server 2012 R2”, „Windows Server 2012”, „Windows Server 2008 R2”, „Windows Server 2008”, „Windows Server 2003 R2” un „Windows Server 2003” attiecas uz turpmāk norādītajām operētājsistēmām. Turklāt termins „Windows” tiek lietots kā atsauce uz visām šīs operētājsistēmas versijām.

- ❏ Microsoft® Operētājsistēma Windows® 10
- ❏ Microsoft® Operētājsistēma Windows® 8.1
- ❏ Microsoft® Operētājsistēma Windows® 8
- ❏ Microsoft® Operētājsistēma Windows® 7
- ❏ Microsoft® Operētājsistēma Windows Vista®
- ❏ Microsoft® Operētājsistēma Windows® XP
- ❏ Microsoft® Operētājsistēma Windows® XP Professional x64 Edition
- ❏ Microsoft® Operētājsistēma Windows Server® 2012 R2

Par šo rokasgrāmatu

- ❏ Microsoft® Operētājsistēma Windows Server® 2012
- ❏ Microsoft® Operētājsistēma Windows Server® 2008 R2
- ❏ Microsoft® Operētājsistēma Windows Server® 2008
- ❏ Microsoft® Operētājsistēma Windows Server® 2003 R2
- ❏ Microsoft® Operētājsistēma Windows Server® 2003

Ievads

Rokasgrāmatas daļas

Šajā rokasgrāmatā ir paskaidrota printera pievienošana tīklam, un tajā iekļauta informācija par to, kā izvēlēties funkciju iestatījumus.

Informāciju par funkciju lietošanu skatiet *Lietotāja rokasgrāmata*.

Sagatavošana
Aprakstīta ierīču iestatīšana un pārvaldības programmatūra.

Savienojums
Paskaidro, kā pievienot printeri tīklam.

Funkciju iestatījumi
Paskaidro drukāšanas iestatījumus.

Drošības iestatījumi
Paskaidro drošības iestatījumus, piemēram, administratora paroles iestatījumus un protokolu vadību.

Problēmu risinājumi
Paskaidro iestatījumu inicializāciju un tīkla darbības problēmu risināšanu.

Šajā pamācībā izmantoto terminu definīcijas

Šajā pamācībā izmantoti turpmāk aprakstītie termini.

Administrators
Par ierīces vai biroja/organizācijas tīkla uzstādīšanu un iestatīšana atbildīgā persona. Mazās organizācijās šāda persona var būt atbildīga gan par ierīces, gan par tīkla administrēšanu. Lielās organizācijās administratori atbild par nodaļas grupas vienības tīklu vai ierīcēm, un tīkla administratori atbild par iestatījumiem, kas attiecas uz sakariem ārpus organizācijas robežām, piemēram, interneta sakariem.

Tīkla administrators
Persona, kas atbild par tīkla sakaru kontroli. Persona, kas iestata maršurtētāju, starpniekserveri, DNS serveri un pasta serveri, kontrolējot interneta vai lokālā tīkla sakarus.

Lietotājs
Persona, kas lieto ierīces, piemēram, printerus.

Servera/klienta savienojums (printera koplietošana, izmantojot Windows serveri)
Šāda savienojuma gadījumā printeris ir savienots ar Windows serveri tīklā vai izmantojot USB vadu, un serverī iestatīto drukas rindu var koplietot. Printera un datora savstarpējos sakarus nodrošina serveris, un printeri vada serverī.

Vienādranga savienojums (tiešā drukāšana)
Šāda savienojuma gadījumā printeris un dators ir savienoti ar tīklu, izmantojot centrmezglu vai piekļuves punktu, un drukas uzdevumu var izpildīt tieši no datora.

Web Config (ierīces tīmekļa lapa)
Ierīcē iebūvētais tīmekļa serveris. Tā nosaukums ir Web Config. Izmantojot pārlūkprogrammu, tajā var pārbaudīt un mainīt ierīces statusu.

Drukas rinda
Operētājsistēmas Windows sadaļā **Device and Printer (Ierīces un printeri)** redzamās portu ikonas, piemēram, printerim. Pat vienai ierīcei tiek izveidotas divas vai lielāks ikonu skaits, ja ierīce ir pievienota tīklam, izmantojot divus vai lielāku portu skaitu, piemēram, standarta TCP/IP.

Rīks
Vispārējs termins, ar kuru apzīmē programmatūru ierīces iestatīšanai vai pārvaldībai, piemēram, Epson Device Admin, EpsonNet Config, EpsonNet SetupManager utt.

ASCII (Amerikas informācijas apmaiņas standartkods)
Viens no rakstzīmju standartkodiem. Izšķir 128 rakstzīmes, tostarp alfabēta burtus (a–ž, A–Ž), arābu ciparus (0–9), simbolus, tukšumzīmes un kontroles rakstzīmes. Šajā rokasgrāmata ar "ASCII" ir domāts zemāk norādītais skaitlis 0x20–0x7E (heksadecimāls), kurš neietver kontroles rakstzīmes.

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	{	|	}	~	

* Tukšumzīme.

Unikods (UTF-8)
Starptautisks standartkods, kas ietver lielāko pasaules valodu rakstzīmes. Šajā pamācībā ar "UTF-8" ir apzīmētas kodējuma rakstzīmes UTF-8 formātā.

Sagatavošana

Šajā nodaļā ir paskaidrots, kas nepieciešams, lai sagatavotos darbībām pirms iestatījumu veikšanas.

Printera iestatījumu plūsma

Jūs veicat tīkla savienojuma iestatīšanu un sākotnējo iestatīšanu, lai printeris būtu pieejams lietotājiem.

1 Sagatavošana

- ❏ Savienojuma iestatījumu informācijas apkopošana
- ❏ Lēmums par savienojuma metodi

2 Savienojuma izveide

- ❏ Tīkla savienojuma izveide, izmantojot EpsonNet Config

3 Drukāšanas iestatīšana

- ❏ Printera draivera iestatījumi

4 Drošības iestatījumi

- ❏ Administratora iestatījumi
- ❏ SSL/TLS
- ❏ Protokolu vadība
- ❏ IPsec/IP filtering (IPsec/IP filtrēšana)

Saistītā informācija

➡ "Savienojums" 14. lpp.
➡ "Funkciju iestatījumi" 20. lpp.
➡ "Drošības iestatījumi" 28. lpp.

Ievads par printera savienojumu

Printera tīkla savienojumam ir pieejamas divas tālāk norādītās metodes.

- ❏ Servera/klienta savienojums (printera koplietošana, izmantojot Windows serveri)
- ❏ Vienādranga savienojums (tiešā drukāšana)

Saistītā informācija

➡ "Servera/klienta savienojuma iestatījumi" 11. lpp.
➡ "Vienādranga savienojuma iestatījumi" 11. lpp.

Servera/klienta savienojuma iestatījumi

Savienojuma metode:

Savienojiet printeri ar tīklu, izmantojot centrmezglu (L2 slēdzis). Printeri var savienot ar serveri arī, izmantojot USB vadu.

Printera draiveris:

Atkarībā no klientdatoru operētajsistēmām printera draiveris jāinstalē Windows serverī. Piekļūstot Windows serverim un izveidojiet savienojumu ar printeri, printera draiveris tiek instalēts klientdatorā, un to var izmantot.

Funkcijas:

- ❏ Printera un printera draivera centralizēta pārvaldība.
- ❏ Atkarība no servera specifikācijām līdz drukas uzdevuma sākšanai var paiet noteikts laiks, jo visi drukas uzdevumi tiek izpildīti ar drukas servera starpniecību.
- ❏ Kad Windows serveris ir izslēgts, drukāt nav iespējams.

Saistītā informācija

➡ "Šajā pamācībā izmantoto terminu definīcijas" 8. lpp.

Vienādranga savienojuma iestatījumi

Savienojuma metode:

Savienojiet printeri ar tīklu, izmantojot centrmezglu (L2 slēdzis).

Printera draiveris:

Instalējiet printera draiveri katrā klientdatorā. To var iegūt pakotnes veidā, izmantojot EpsonNet SetupManager, vai automātiski, izmantojot Windows servera grupas politiku.

Funkcijas:

- ❏ Drukas uzdevums tiek sākts nekavējoties, jo tas tiek nosūtīts uz printeri tiešā veidā.
- ❏ Drukāšana ir iespējama, kamēr printeris ir ieslēgts.

Saistītā informācija

➡ "Šajā pamācībā izmantoto terminu definīcijas" 8. lpp.

Sagatavošanās savienojuma izveidei ar tīklu

Informācijas apkopošana savienojuma iestatīšanai

Lai izveidotu tīkla savienojumu, nepieciešama IP adrese, vārtejas adrese utt. Iepriekš pārbaudiet turpmāk norādītos datus.

Sadaļas	Vienības	Piezīme
Ierīces savienojuma metode	❏ Ethernet	Ethernet savienojumam izmantojiet 5e vai augstākas kategorijas STP (ekranētu vītā pāra) kabeli.
Lokālā tīkla savienojuma informācija	❏ IP adrese ❏ Apakštīkla maska ❏ Noklusējuma vārteja	Nav nepieciešams, ja IP adrese iestatīta automātiski, izmantojot maršrutētāja DHCP funkciju.
DNS servera informācija	❏ Primārā DNS servera IP adrese ❏ Sekundārā DNS servera IP adrese	Ja izmantojat statisku IP adresi, konfigurējiet DNS serveri. Konfigurējiet, ja IP adreses tiek piešķirtas automātiski, izmantojot DHCP funkciju, un kad DNS serveri nevar piešķirt automātiski.

Printera specifikācija

Specifikācijas, kuras printeris atbalsta standarta vai savienojuma režīmā, skatiet *Lietotāja rokasgrāmata*.

IP adreses piešķiršanas veids

IP adresi printerim var piešķirt divos veidos.

Statiska IP adrese:

Piešķiriet printerim iepriekš noteiktu, unikālu IP adresi.

IP adrese nemainās pat pēc printera ieslēgšanas vai maršrutētāja izslēgšanas, tādējādi ierīci iespējams pārvaldīt, izmantojot IP adresi.

Šis veids ir piemērots tīkliem, kur tiek izmantots liels printeru skaits, piemēram, lielā birojā vai skolā.

Automātiska piešķiršana, izmantojot DHCP funkciju:

Pareizā IP adrese tiek piešķirta automātiski pēc tam, kad tiek izveidoti sakari starp printeri un maršrutētāju, kurš atbalsta DHCP funkciju.

Ja nav noteiktas ierīces IP adreses maiņa rada neērtības, rezervējiet IP adresi jau iepriekš un pēc tam to piešķiriet.

Piezīme.
Drukas rindas portam atlasiet protokolu, kurš var automātiski noteikt IP adresi, piemēram, EpsonNet Print Port.

Tīkla savienojuma iestatīšanas metode

Lai norādītu tādus savienojuma iestatījumus, kā printera IP adrese, apakštīkla maska un noklusējuma vārteja, veiciet turpmāk aprakstīto procedūru.

EpsonNet Config izmantošana:

Izmantojiet EpsonNet Config administratora datorā. Iestatījumus var izvēlēties daudziem printeriem, taču lai to varētu izdarīt, tiem jābūt fiziski savienotiem, izmantojot Ethernet vadu. Zemu drošības risku var saglabāt, ja iestatīšanai iespējams izveidot Ethernet savienojumu, iestatāt printera tīkla iestatījumus un pēc tam savienojat printeri ar parasto tīklu.

Izmantojot instalētāju:

Ja tiek izmantots instalētājs, printera tīkla iestatījumi un klientdators tiek iestatīti automātiski. Iestatīšanu veic, izpildot instalētāja norādes, un to var veikt arī bez padziļinātām zināšanām par tīklu. Šī metode ir ieteicama, iestatot printeri un dažus klientdatorus un izmantojot servera/klienta savienojumu (printera koplietošana, izmantojot Windows serveri).

Saistītā informācija

➡ "IP adreses piešķiršana, izmantojot EpsonNet Config" 14. lpp.
➡ "Savienojums ar tīklu, izmantojot instalētāju" 18. lpp.

Instalēšana EpsonNet Config

Lejupielādējiet EpsonNet Config no Epson atbalsta vietnes un pēc tam instalējiet to, izpildot ekrānā redzamos norādījumus.

Palaišana EpsonNet Config

Atlasiet **All Programs (Visas programmas)** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Piezīme.
Ja tiek parādīts ugunsmūra brīdinājums, atļaujiet EpsonNet Config piekļuvi.

Savienojums

Šajā nodaļā ir aprakstīta nepieciešamā vide un procedūra, kas jāveic, lai savienotu printeri ar tīklu.

Savienojums ar tīklu

Savienojums ar lokālo tīklu

Savienojiet printeri ar tīklu, izmantojot Ethernet savienojumu.

Saistītā informācija

➡ "Savienojums ar tīklu, izmantojot instalētāju" 18. lpp.

IP adreses piešķiršana, izmantojot EpsonNet Config

Piešķiriet printerim IP adresi, izmantojot EpsonNet Config.

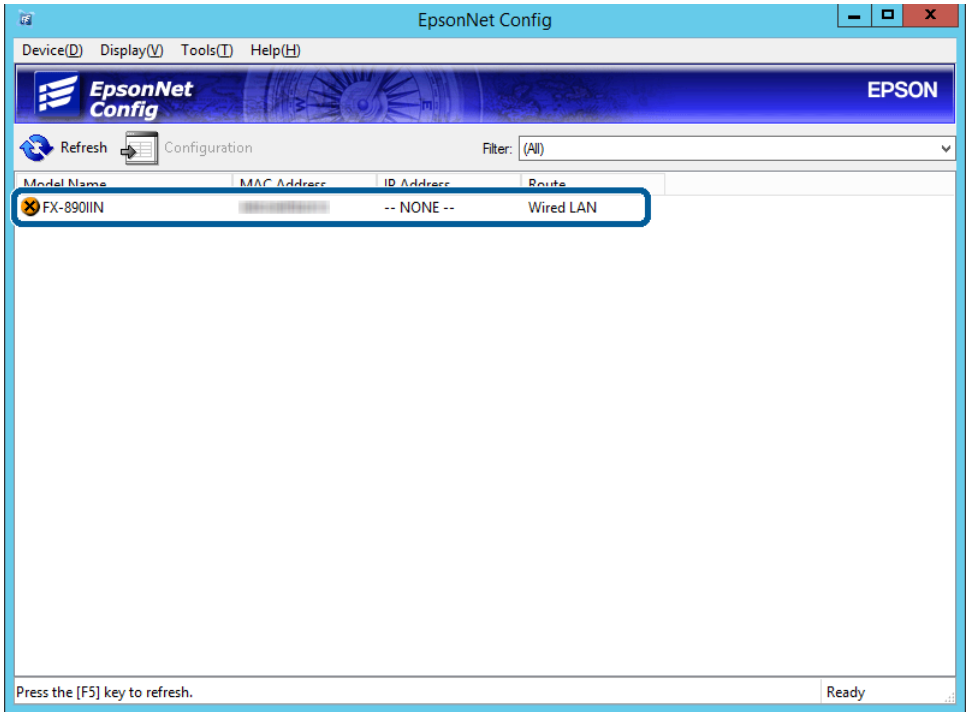
1. Ieslēdziet printeri.
2. Pievienojiet printeri tīklam, izmantojot Ethernet vadu.
3. Startējiet EpsonNet Config.

   Tiek parādīts tīkla printeru saraksts. Var paiet zināms laiks, pirms tie tiks parādīti.
4. Veiciet dubultklikšķi uz printera, kuram vēlaties piešķirt adresi.

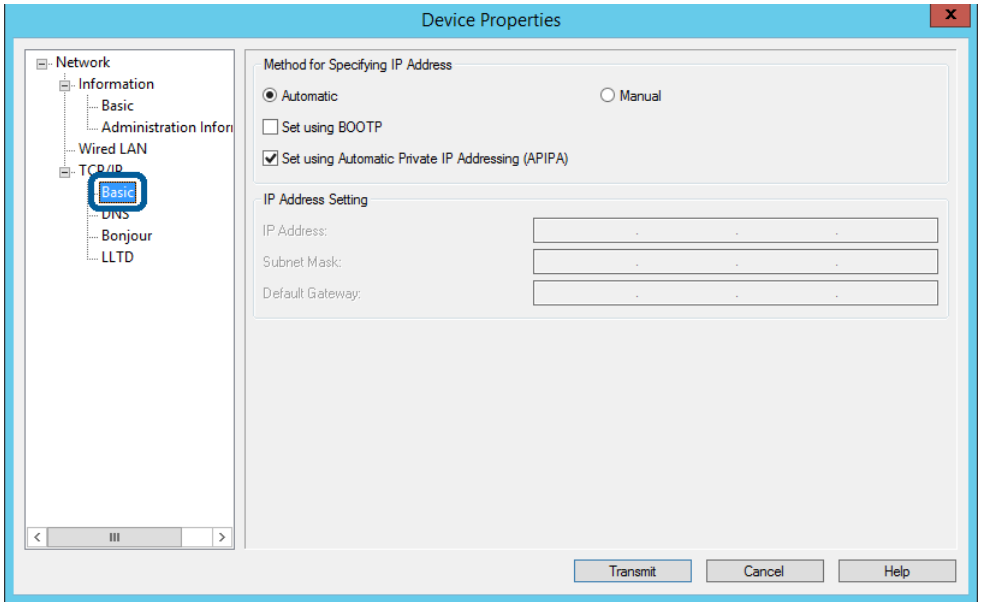
   Ja pievienojat printeri tīklam ar pieejamo DHCP funkciju, IP adrese tiek piešķirta, izmantojot DHCP funkciju, un pēc tam tiek parādīta.

   Piezīme.
   - ❏ *Ja ir pievienoti vairāki vienāda modeļa printeri, varat identificēt printeri, izmantojot MAC adresi.*
   - ❏ *Pēc tam, kad printerī ir izveidots tīkla savienojums, varat mainīt IP adreses piešķiršanas metodi.*

Savienojums

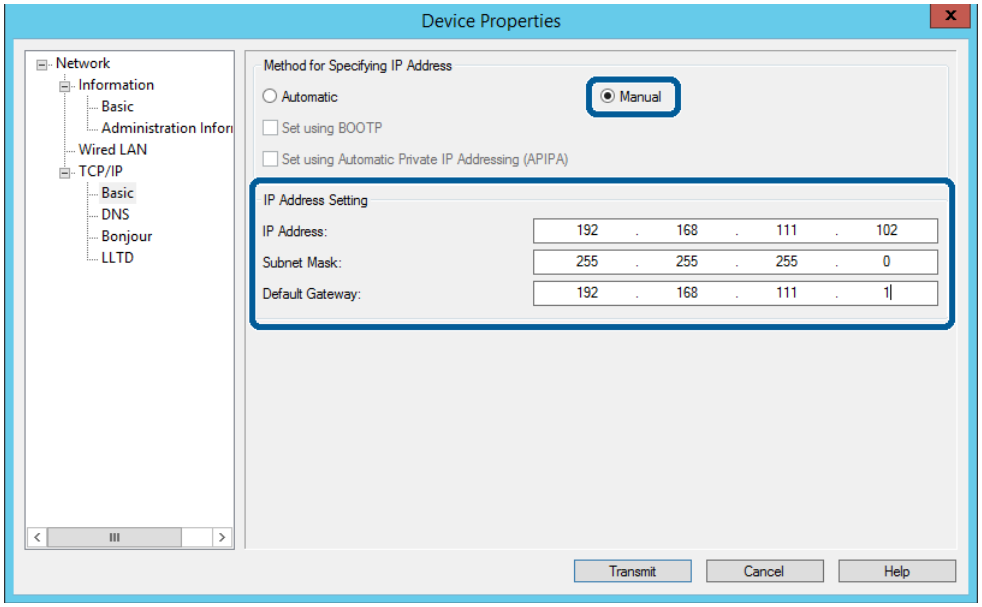


5 Atlasiet **Network (Tīkls)** > **TCP/IP** > **Basic (Pamata)**.



Savienojums

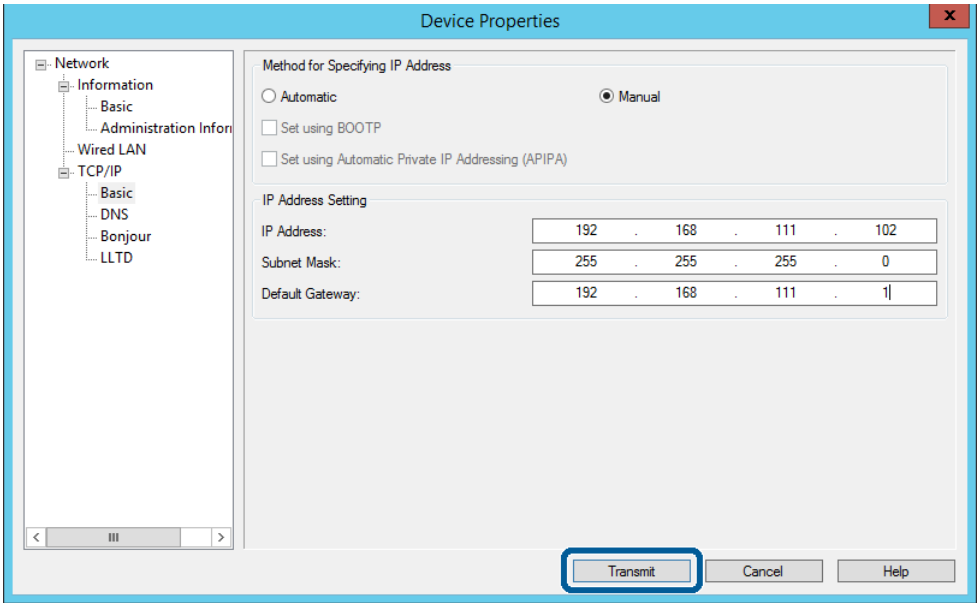
6 Ievadiet adreses laukos **IP Address (IP adrese)**, **Subnet Mask (Apakštīkla maska)** un **Default Gateway (Noklusējuma vārteja)**.



Piezīme.

- ❏ *Pievienojot printeri drošam tīklam, ievadiet statisku adresi.*
- ❏ *Izvēlnes **TCP/IP** ekrānā **DNS** var atlasīt DNS iestatījumus.*

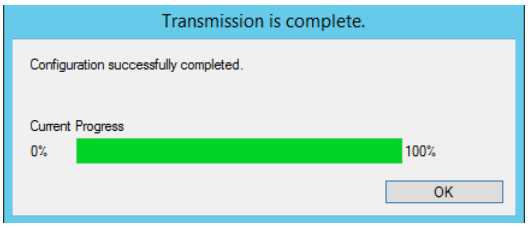
7 Noklikšķiniet uz **Transmit (Pārraidīt)**.



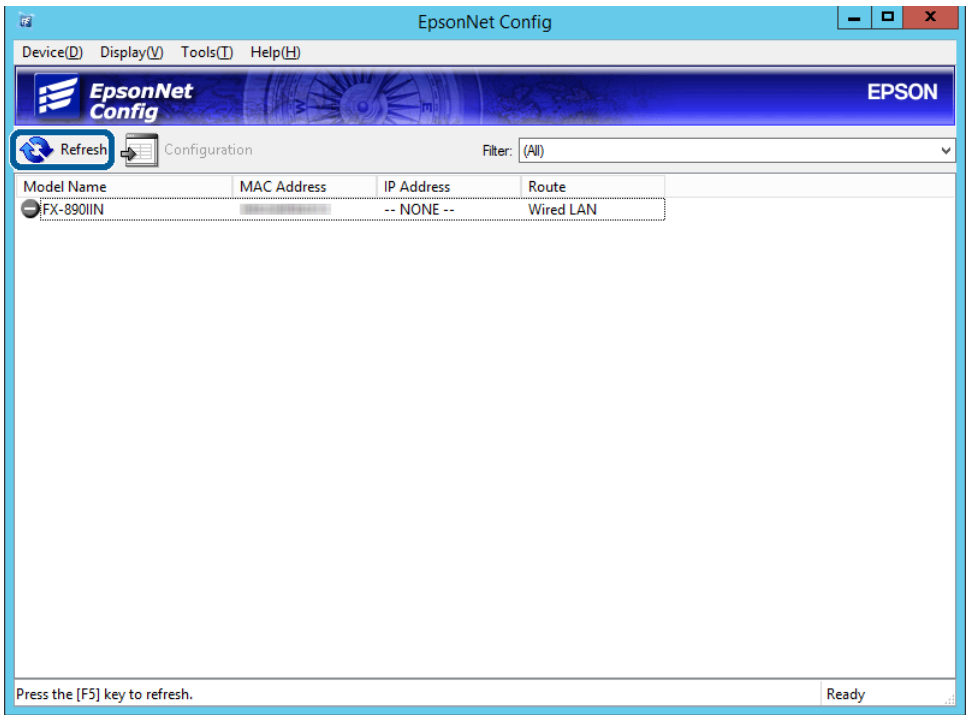
8 Apstiprinājuma ekrānā noklikšķiniet uz **OK (Labi)**.

Savienojums

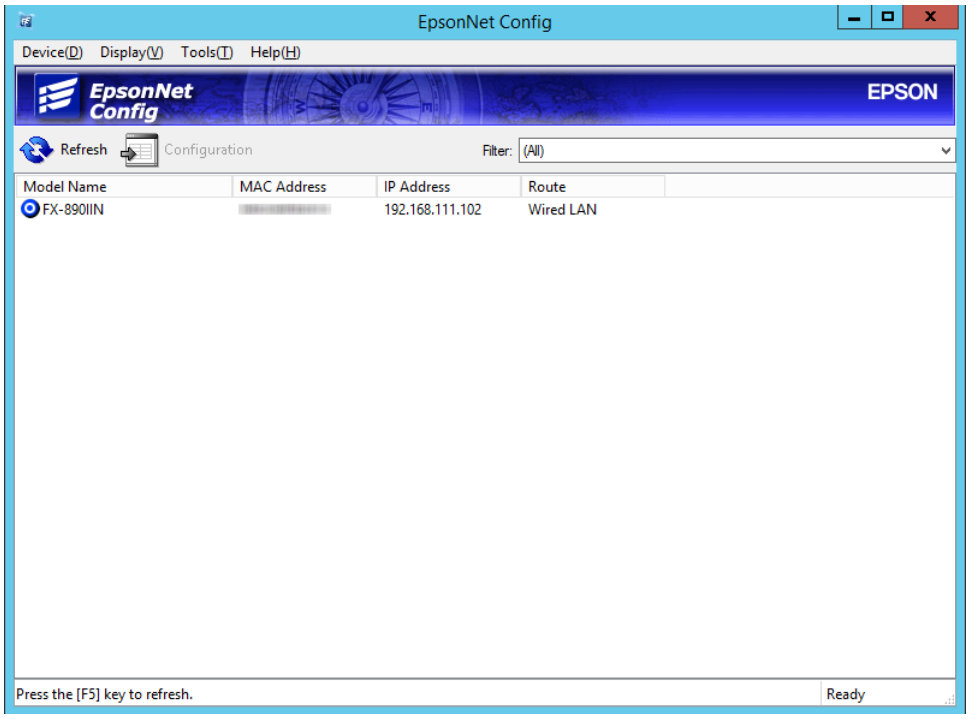
9 Noklikšķiniet uz **OK (Labi)**.



10 Noklikšķiniet uz **Refresh (Atsvaidzināt)**.



Pārbaudiet, vai ir piešķirta IP adrese.

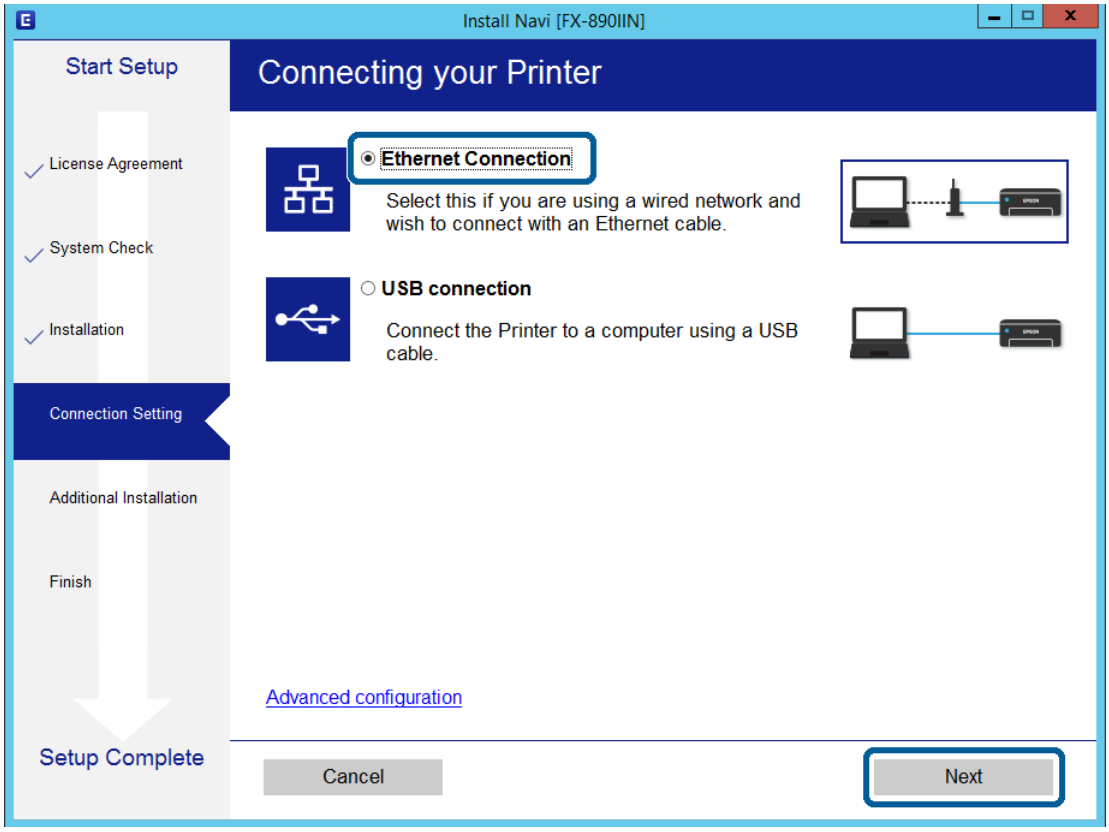


Savienojums ar tīklu, izmantojot instalētāju

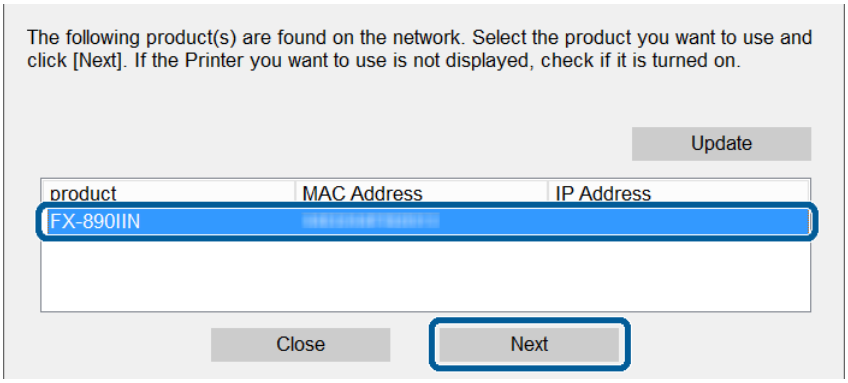
Savienojot printeri ar datoru, ieteicams izmantot instalētāju.

1 Ievietojiet programmatūras disku datorā un izpildiet ekrānā redzamos norādījumus.

2 Izpildiet ekrānā sniegtos norādījumus, līdz parādās attēlā redzamais ekrāns, atlasiet **Ethernet Connection (Ethernet savienojums)**, un pēc tam noklikšķiniet uz **Next (Tālāk)**.



Ja pievienojat printeri tīklam ar Ethernet kabeli, parādās attēlā redzamais ekrāns. Atlasiet printeri un pēc tam noklikšķiniet uz **Next (Tālāk)**.



3 Izpildiet ekrānā redzamās instrukcijas.

Funkciju iestatījumi

Šajā nodaļā ir paskaidroti pirmie iestatījumi, kas jāizvēlas, lai izmantotu katru no ierīces funkcijām.

Šajā sadaļā ir paskaidrota iestatīšana, ko veic administratora datorā, izmantojot programmu Web Config.

Web Config (Ierīces tīmekļa lapa)

Apraksts Web Config

Web Config ir pārlūkprogrammai paredzēta lietojumprogramma, ko izmanto printera iestatījumu konfigurēšanai.

Lai piekļūtu programmai Web Config, printerim ir jābūt piešķirtai IP adresei.

Piezīme.
Iestatījumus var bloķēt, konfigurējot printera administratora paroli.

Piekļuve Web Config

Lai piekļūtu programmai Web Config, ir pieejamas divas metodes. Pārlūkprogrammā jābūt iespējotai valodai JavaScript.

IP adreses ievadīšana

Startējiet EpsonNet Config un pēc tam divreiz noklikšķiniet uz sarakstā redzamā printera.

Ievadiet pārlūkprogrammā printera IP adresi. Kad piekļuvei Web Config izmanto HTTPS protokolu, pārlūkprogrammā parādās brīdinājuma ziņojums, jo tiek izmantots pašparakstīts sertifikāts, kas glabājas printerī.

❏ Piekļuve, izmantojot HTTPS
IPv4: https://<printera IP adrese> (bez < >)
IPv6: https://[printera IP adrese]/ (ar [ ])

❏ Piekļuve, izmantojot HTTP
IPv4: http://<printera IP adrese> (bez < >)
IPv6: http://[printera IP adrese]/ (ar [ ])

Piezīme.

❏ *Piemēri*
IPv4:
https://192.0.2.111/
http://192.0.2.111/
IPv6:
https://[2001:db8::1000:1]/
http://[2001:db8::1000:1]/

❏ *Ja printera nosaukums ir reģistrēts DNS serverī, var izmantot nevis printera IP adresi, bet gan printera nosaukumu.*

❏ *Piekļūstot Web Config ar HTTP protokolu, netiek rādītas visas izvēlnes. Lai skatītu visas izvēlnes, atveriet Web Config, izmantojot HTTPS protokolu.*

Saistītā informācija

➡ "SSL/TLS sakari ar printeri" 34. lpp.
➡ "Par ciparsertifikātiem" 35. lpp.

Drukāšanas funkciju izmantošana

Iespējojiet, lai izmantotu printera drukāšanas funkciju.

Prasības drukāšanai tīklā

Lai varētu drukāt tīklā, jāievēro turpmāk minētās prasības. Šos iestatījumus var konfigurēt, izmantojot printera draiveri un operētājsistēmas funkcijas.

❏ Printera draivera instalēšana

❏ Drukas rindas izveide datorā

❏ Porta iestatīšana tīklam

Printera draivera iestatīšana, izmantojot servera/klienta savienojumu

Veiciet iestatījumus, lai iespējotu printerī drukāšanu no datora, kas iepriekš iestatīts kā drukas serveris, un koplietojiet printeri. Instalējiet drukas serverī printera draiveri gan serverim, gan klientam. Ja tiek izmantots instalētājs, tīkla iestatīšana printerī vai datorā, draivera instalēšana un drukas rindas izveide notiek automātiski.

Standarta TCP/IP portu iestatīšana — Windows

Iestatiet standarta TCP/IP portu drukas serverī un izveidojiet drukas rindu drukāšanai tīklā.

1 Atveriet ierīču un printeru ekrānu.

❏ Operētājsistēma Windows 10/Windows Server 2016
Noklikšķiniet ar peles labo pogu uz pogas Start (Sākt) un turiet to nospiestu, pēc tam atlasiet **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** > **Devices and Printers (Ierīces un printeri)**.

❏ Operētājsistēma Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Desktop (Darbvirsma) > **Settings (Iestatījumi)** > **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** vai **Hardware (Aparatūra)** > **Devices and Printers (Ierīces un printeri)**.

❏ Operētājsistēma Windows 7/Windows Server 2008 R2
Noklikšķiniet uz Start (Sākt) > **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** (vai **Hardware (Aparatūra)**) > **Devices and Printers (Ierīces un printeri)**.

❏ Operētājsistēma Windows Vista/Windows Server 2008
Noklikšķiniet uz Start (Sākt) > **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** > **Printers (Printeri)**.

❏ Operētājsistēma Windows XP/Windows Server 2003 R2/Windows Server 2003
Noklikšķiniet uz Start (Sākt) > **Control Panel (Vadības panelis)** > **Printers and Other Hardware (Printeri un cita aparatūra)** > **Printers and Faxes (Printeri un faksi)**.

2 Pievienojiet printeri.

❏ Operētājsistēma Windows 10/Windows 8.1/Windows 8/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012
Noklikšķiniet uz **Add printer (Pievienot printeri)**, pēc tam izvēlieties **The printer that I want isn't listed (Sarakstā nav printera, ko vēlos lietot)**.

❏ Operētājsistēma Windows 7/Windows Server 2008 R2
Noklikšķiniet uz **Add printer (Pievienot printeri)**.

❏ Operētājsistēma Windows Vista/Windows Server 2008
Noklikšķiniet uz **Install Printer (Instalēt printeri)**.

❏ Operētājsistēma Windows XP/Windows Server 2003 R2/Windows Server 2003
Noklikšķiniet uz **Install Printer (Instalēt printeri)** un pēc tam uz **Next (Tālāk)**.

3 Pievienojiet lokālo printeri.

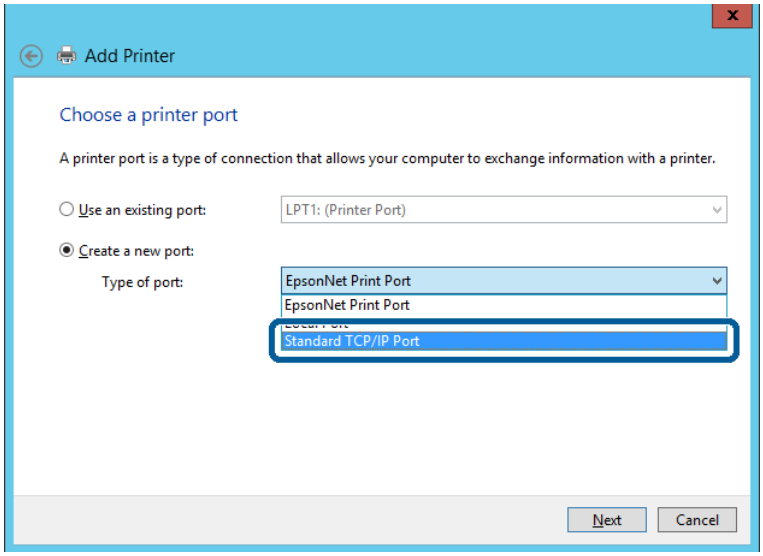
❏ Operētājsistēma Windows 10/Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Atlasiet **Add a local printer or network printer with manual settings (Pievienot lokālu vai tīkla printeri, izmantojot manuālus iestatījumus)**, pēc tam noklikšķiniet uz **Next (Tālāk)**.

❏ Operētājsistēma Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008
Noklikšķiniet uz **Add a local printer (Pievienot lokālo printeri)**.

❏ Operētājsistēma Windows XP/Windows Server 2003 R2/Windows Server 2003
Atlasiet **Local printer attached to this computer (Šim datoram pievienots lokāls printeris)**, pēc tam noklikšķiniet uz **Next (Tālāk)**.

4 Atlasiet **Create a new port (Izveidot jaunu portu)**, atlasiet **Standard TCP/IP Port (Standarta TCP/IP ports)** kā porta veidu un pēc tam noklikšķiniet uz **Next (Tālāk)**.

Operētājsistēmā Windows XP/Windows Server 2003 R2/Windows Server 2003 noklikšķiniet uz **Next (Tālāk)**, kad tiek parādīts ekrāns **Add Standard TCP/IP Printer Port Wizard (Pievienot standarta TCP/IP printera porta vedni)**.

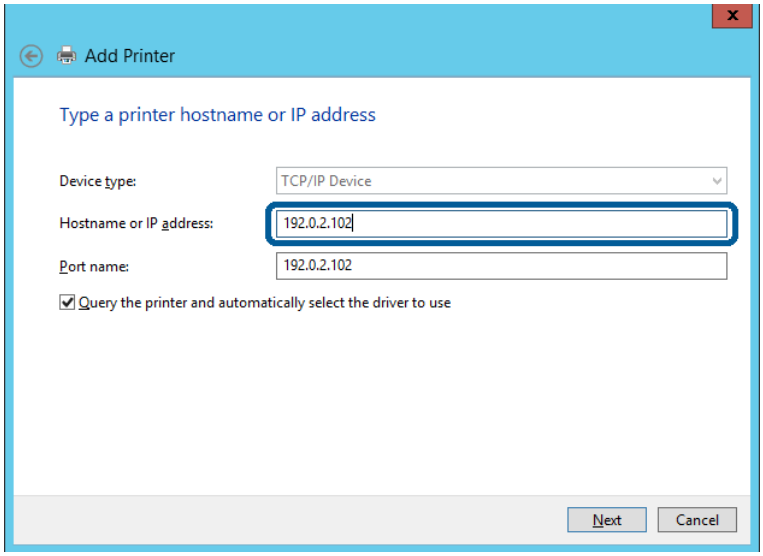


5 Ievadiet printera IP adresi vai nosaukumu laukā **Host Name or IP Address (Resursdatora nosaukums vai IP adrese)** vai **Printer Name or IP Address (Printera nosaukums vai IP adrese)**, pēc tam noklikšķiniet uz **Next (Tālāk)**.

Nemainiet vērtību **Port name (Porta nosaukums)**.

Noklikšķiniet uz **Continue (Turpināt)**, kad parādās ekrāns **User Account Control (Lietotāja konta kontrole)**.

Operētājsistēmā Windows XP/Windows Server 2003 R2/Windows Server 2003 noklikšķiniet uz **Done (Gatavs)**, kad tiek parādīts ekrāns **Standard TCP/IP Printer Port (Standarta TCP/IP printera ports)**.



> ***Piezīme.***
> *Ja norādāt printera nosaukumu tīklā, kur ir pieejama nosaukumu atpazīšana, IP adrese tiek izsekota pat tad, ja DHCP ir mainījis printera IP adresi. Printera nosaukumu var uzzināt tīkla statusa ekrānā, izmantojot printera vadības paneli, vai tīkla statusa lapā.*

6 Iestatiet printera draiveri.

- ❏ Ja printera draiveris jau ir instalēts:
  Atlasiet **Manufacturer (Ražotājs)** un **Printers (Printeri)**. Noklikšķiniet uz **Next (Tālāk)**.

- ❏ Ja printera draiveris nav instalēts:
  Noklikšķiniet uz **Have Disc (Lietot disku)** un pēc tam ievietojiet printera komplektā iekļauto programmatūras disku. Noklikšķiniet uz **Browse (Pārlūkot)** un pēc tam atlasiet diskā mapi, kurā atrodas printera draiveris. Noteikti atlasiet pareizo mapi. Mapes atrašanās vieta ir atkarīga no operētājsistēmas.
  Windows 32 bitu versijā: WINX86
  Windows 64 bitu versijā: WINX64

7 Izpildiet ekrānā redzamās instrukcijas.

Operētājsistēmas Windows XP/Windows Server 2003 R2/Windows Server 2003 iestatīšana ir pabeigta. Operētājsistēmai Windows Vista/ Windows Server 2008 un jaunākām Windows versijām pārbaudiet porta konfigurāciju.

Izmantojot printeri servera/klienta savienojumā (printera koplietošana, izmantojot Windows serveri), pēc šīs procedūras izvēlieties koplietošanas iestatījumus.

Saistītā informācija
➡ "Printera koplietošana" 25. lpp.

Porta konfigurācijas pārbaude — Windows

Pārbaudiet, vai drukas rindai iestatīts pareizais ports.

1 Atveriet ierīču un printeru ekrānu.

- ❏ Operētājsistēma Windows 10/Windows Server 2016
  Noklikšķiniet ar peles labo pogu uz pogas Start (Sākt) un turiet to nospiestu, pēc tam atlasiet **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** > **Devices and Printers (Ierīces un printeri)**.

- ❏ Operētājsistēma Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
  Desktop (Darbvirsma) > **Settings (Iestatījumi)** > **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** vai **Hardware (Aparatūra)** > **Devices and Printers (Ierīces un printeri)**.

- ❏ Operētājsistēma Windows 7/Windows Server 2008 R2
  Noklikšķiniet uz Start (Sākt) > **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** (vai **Hardware (Aparatūra)**) > **Devices and Printers (Ierīces un printeri)**.

- ❏ Operētājsistēma Windows Vista/Windows Server 2008
  Noklikšķiniet uz Start (Sākt) > **Control Panel (Vadības panelis)** > **Hardware and Sound (Aparatūra un skaņa)** > **Printers (Printeri)**.

2 Atveriet printera rekvizītu ekrānu.

❏ Operētājsistēma Windows 10/Windows 8.1/Windows 8/Windows 7/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012/ Windows Server 2008 R2
Ar peles labo pogu noklikšķiniet uz printera ikonas, pēc tam noklikšķiniet uz **Printer properties (Printera rekvizīti)**.

❏ Windows Vista
Noklikšķiniet ar peles labo pogu uz printera ikonas, pēc tam atlasiet **Run as administrator (Palaist kā administratoram)** > **Properties (Rekvizīti)**.

❏ Windows Server 2008
Noklikšķiniet ar peles labo pogu uz printera ikonas, pēc tam noklikšķiniet uz **Properties (Rekvizīti)**.

3 Noklikšķiniet uz cilnes **Ports (Porti)**, atlasiet **Standard TCP/IP Port (Standarta TCP/IP ports)**, pēc tam noklikšķiniet uz **Configure Port (Konfigurēt portu)**.

4 Pārbaudiet porta konfigurāciju.

❏ RAW
Pārbaudiet, vai sadaļā **Protocol (Protokols)** ir atlasīta opcija **Raw**, pēc tam noklikšķiniet uz **OK (Labi)**.

❏ LPR
Pārbaudiet, vai sadaļā **Protocol (Protokols)** ir atlasīta opcija **LPR**. Ievadiet "PASSTHRU" sadaļas **LPR Settings (LPR iestatījumi)** laukā **Queue name (Rindas nosaukums)**. Atlasiet **LPR Byte Counting Enabled (LPR baitu skaitīšana iespējota)**, pēc tam noklikšķiniet uz **OK (Labi)**.

Printera koplietošana

Izmantojot printeri servera/klienta savienojumā (printera koplietošana, izmantojot Windows serveri), iestatiet printera koplietošanu drukas serverī.

1 Drukas serverī atlasiet **Control Panel (Vadības panelis)** > **View devices and printers (Skatīt ierīces un printerus)**.

2 Ar peles labo pogu noklikšķiniet uz tā printera ikonas (drukas rindā), kuru vēlaties koplietot, un pēc tam izvēlieties **Printer Properties (Printera rekvizīti)** > cilni **Sharing (Koplietošana)**.

3 Atlasiet **Share this printer (Koplietot šo printeri)** un pēc tam ievadiet **Share name (Koplietojuma nosaukums)**.

Izmantojot Windows Server 2012, noklikšķiniet uz **Change Sharing Options (Mainīt koplietošanas opcijas)** un pēc tam konfigurējiet iestatījumus.

Papildu draiveru instalēšana

Ja atšķiras servera un klientdatoru Windows versijas, ieteicams drukas serverī instalēt papildu draiverus.

1 Drukas serverī atlasiet **Control Panel (Vadības panelis)** > **View devices and printers (Skatīt ierīces un printerus)**.

2 Noklikšķiniet ar peles labo pogu uz tā printera ikonas, kuru vēlaties koplietot ar klientiem, un pēc tam noklikšķiniet uz **Printer Properties (Printera rekvizīti)** > cilnes **Sharing (Koplietošana)**.

3 Noklikšķiniet uz **Additional Drivers (Papildu draiveri)**.

Izmantojot Windows Server 2012, noklikšķiniet uz **Change Sharing Options (Mainīt koplietošanas opcijas)** un pēc tam konfigurējiet iestatījumus.

4 Atlasiet klientu Windows versijas un pēc tam noklikšķiniet uz **OK (Labi)**.

5 Atlasiet printera draivera informācijas failu (*.inf) un instalējiet draiveri.

Saistītā informācija

➡ "Koplietota printera izmantošana" 26. lpp.

Koplietota printera izmantošana

Administratoram jāinformē klienti par drukas serverim piešķirto datora nosaukumu un par tā pievienošanu klientu datoriem. Ja papildu draiveris(-i) vēl nav konfigurēti, informējiet klientus par to, kā jālieto sadaļa **Devices and Printers (Ierīces un printeri)**, lai pievienotu koplietotu printeri.

Ja drukas serverī jau ir konfigurēts papildu draiveris(-i), veiciet turpmāk norādītās darbības.

1 Atlasiet drukas serverim piešķirto nosaukumu sadaļā **Windows Explorer**.

2 Veiciet dubultklikšķi uz printera, kuru vēlaties izmantot.

Saistītā informācija

➡ "Printera koplietošana" 25. lpp.
➡ "Papildu draiveru instalēšana" 25. lpp.

Printera draivera iestatījumi vienādranga savienojumam

Lai izveidotu vienādranga (tiešās drukāšanas) savienojumu, katrā klientdatorā jābūt instalētam printera draiveri.

Saistītā informācija

➡ "Printera draivera iestatīšana" 26. lpp.

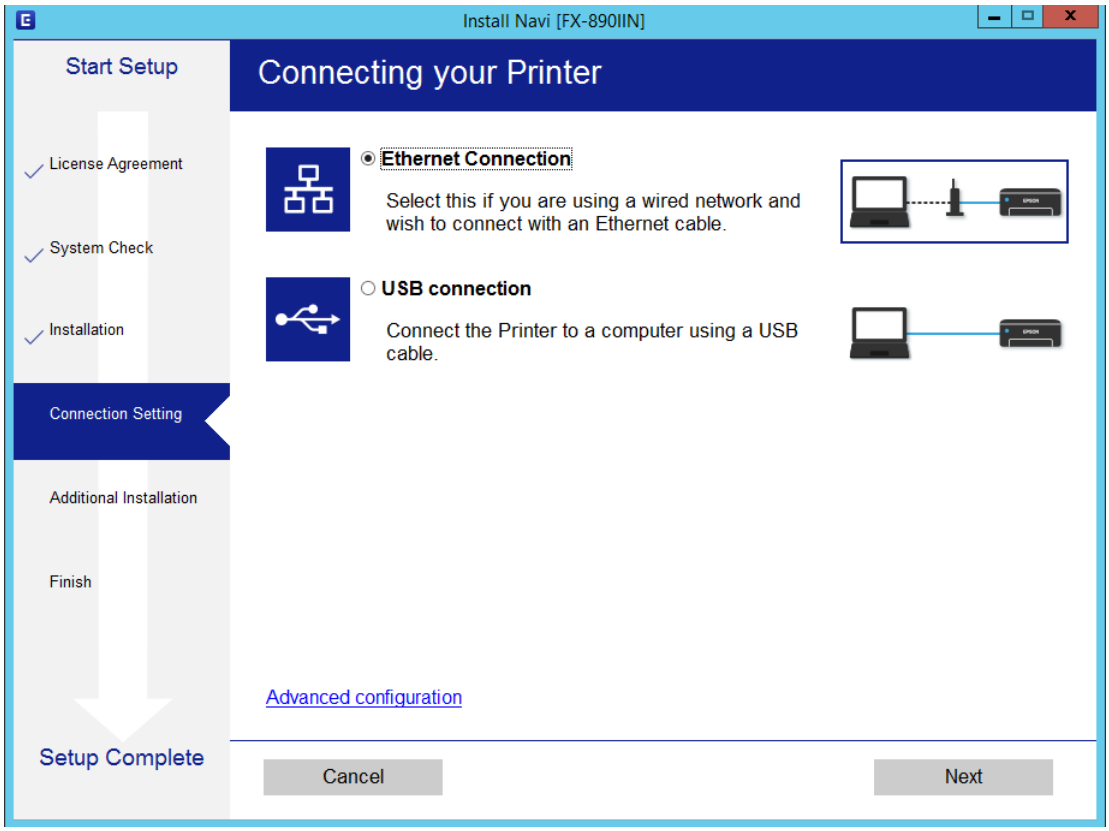
Printera draivera iestatīšana

Mazām organizācijām ieteicams printera draiveri instalēt katrā klientdatorā.

> ***Piezīme.***
> *Ja printeris tiek izmantots daudzos klientdatoros, EpsonNet SetupManager izmantošana un draivera nodrošināšana pakotnes veidā var ievērojami samazināt instalēšanas laiku.*

1 Palaidiet instalētāju.

2 Izvēlieties printerim savienojuma metodi, pēc tam noklikšķiniet uz **Next (Tālāk)**.



Piezīme.
*Ja tiek parādīts ekrāns **Select Software Installation (Atlasiet opciju „Programmatūras instalēšana”)**, atlasiet **Change or re-set the connection method (Nomainiet vai atiestatiet savienojuma metodi)** un pēc tam noklikšķiniet uz **Next (Tālāk)**.*

3 Izpildiet ekrānā redzamās instrukcijas.

Saistītā informācija

➡ "EpsonNet SetupManager" 61. lpp.

Drošības iestatījumi

Šajā nodaļā ir paskaidroti drošības iestatījumi.

Drošības iestatījumi un bīstamības novēršana

Ja ierīce ir pievienota tīklam, varat tai piekļūt attālināti. Turklāt ierīci var koplietot vairāki cilvēki, kas palīdz uzlabot darba efektivitāti un padara to ērtāku. Tomēr pieaug dažādi riski, piemēram, neatļauta piekļuve, lietošana un manipulācijas ar datiem.

Lai novērstu šo risku, Epson printeri ir aprīkoti ar dažādām drošības tehnoloģijām. Veiciet ierīcē nepieciešamos iestatījumus atbilstoši klienta informācijas vides apstākļiem.

Funkcijas nosaukums	Funkcijas veids	Kas jāiestata	Kas tiek novērsts
Administratora paroles iestatīšana	Bloķē sistēmas iestatījumus, piemēram, tīkla savienojuma vai USB iestatījumus.	Administrators iestata ierīces paroli. Konfigurācijai vai atjaunināšanai var piekļūt, izmantojot Web Config un Epson Device Admin.	Novērš neatļautu ierīcē saglabātās informācijas, piemēram, ID, paroles, tīkla iestatījumu un kontaktpersonu, skatīšanu un mainīšanu. Turklāt samazina dažādu drošības risku, piemēram, tīkla vides vai drošības politikas informācijas noplūdes iespējamību.
Protokoli un pakalpojumu vadība	Kontrolē protokolus un pakalpojumus, ko izmanto sakariem starp ierīcēm un datoriem, iespējo un atspējo funkcijas, piemēram, drukāšanu.	Protokols vai pakalpojums, kuru izmanto atsevišķu funkciju atļaušanai vai aizliegšanai.	Netīšu drošības risku mazināšana, aizliedzot lietotājiem nevajadzīgu funkciju izmantošanu.
SSL/TLC sakari	Datora un printera savstarpējo sakaru ceļš tiek šifrēts, izmantojot SSL/TLS protokolus. Sakaru saturu aizsargā printera iestatījumi un — drukājot pārlūkprogrammā — IPPS protokola iestatījumi.	Iegūstiet sertificēšanas iestādes parakstītu sertifikātu un importējiet to printerī.	Ierīču identifikācija, izmantojot sertificēšanas iestāžu parakstītus sertifikātus, novērš uzdošanos par citu personu un neatļautu piekļuvi. Turklāt tiek aizsargāts SSL/TLS sakaru saturs un novērsta drukājamā satura un iestatījumu informācijas noplūde.
IPsec/IP filtrēšana	Varat iestatījumos atļaut no noteikta klienta saņemtu vai noteikta veida datu atdalīšanu. Tā kā IPsec aizsargā datus atsevišķām IP pakešu vienībām (šifrēšana un autentificēšana), varat droši veidot sakarus, izmantojot nedrošu drukas protokolu un skenēšanas protokolu.	Izveidojiet pamata politiku un individuālas politikas, lai iestatītu klientu vai datu veidu, kas var piekļūt ierīcei.	Nodrošiniet aizsardzību pret nesankcionētu piekļuvi, manipulācijām ar datiem, kas tiek pārsūtīti uz ierīci, un to pārtveršanu.

Funkcijas nosaukums	Funkcijas veids	Kas jāiestata	Kas tiek novērsts
SNMPv3	Pievienotas tādas funkcijas kā pievienoto ierīču pārraudzība tīklā, datu integritāte SNMP protokolā vadībai, šifrēšanai, lietotāju autentificēšanai utt.	Iespējojiet SNMPv3 un pēc tam iestatiet autentificēšanas un šifrēšanas metodi.	Mainiet iestatījumus tīklā, nodrošiniet stāvokļa novērošanas konfidencialitāti.

Saistītā informācija

➡ "Administratora paroles konfigurēšana" 29. lpp.
➡ "Protokolu un pakalpojumu vadība" 30. lpp.
➡ "SSL/TLS sakari ar printeri" 34. lpp.

Drošības funkciju iestatījumi

Ja ir iestatīta IPsec/IP filtering (IPsec/IP filtrēšana), Web Config ieteicams piekļūt, izmantojot SSL/TLS, lai pārraidītu iestatījumu informāciju, nepieļaujot tādus drošības riskus kā manipulācijas ar datiem vai to pārtveršanu.

Administratora paroles konfigurēšana

Kad tiek iestatīta administratora parole, lietotāji, kuri nav administratori, nevar mainīt sistēmas administrēšanas iestatījumus. Administratora paroli var iestatīt un mainīt, izmantojot Web Config.

Saistītā informācija

➡ "Administratora paroles konfigurēšana, izmantojot Web Config" 29. lpp.

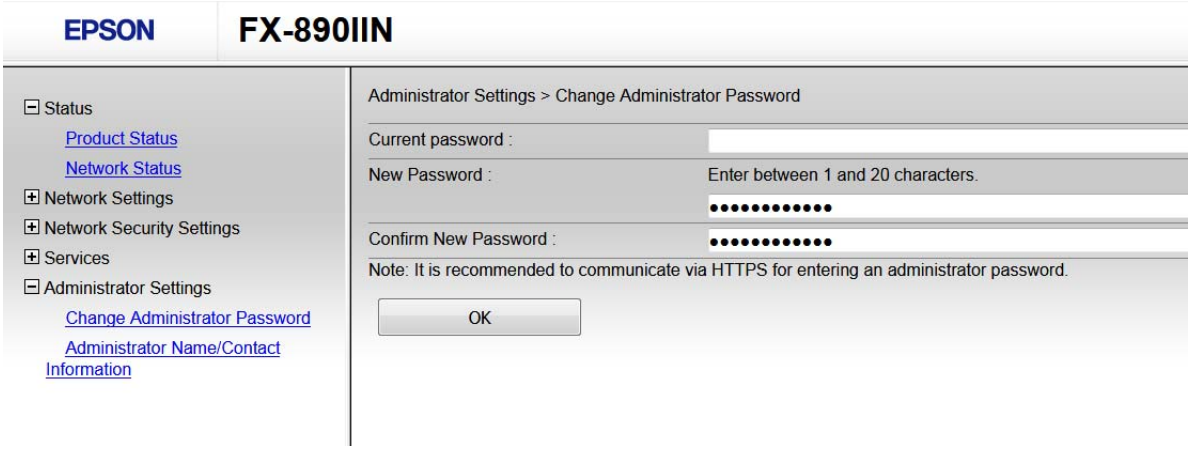
Administratora paroles konfigurēšana, izmantojot Web Config

Administratora paroli var iestatīt, izmantojot Web Config.

1. Atveriet Web Config un atlasiet **Administrator Settings (Administratora iestatījumi)** > **Change Administrator Password (Mainīt administratora paroli)**.

2 Ievadiet paroli laukos **New Password (Jauna parole)** un **Confirm New Password (Apstiprināt jauno paroli)**.

Ja vēlaties mainīt paroli, ievadiet pašreizējo paroli.



3 Atlasiet **OK (Labi)**.

Piezīme.

- ❏ *Lai iestatītu vai mainītu bloķētos izvēlņu vienumus, noklikšķiniet uz **Administrator Login (Administratora pieteikšanās)** un pēc tam ievadiet administratora paroli.*
- ❏ *Lai dzēstu administratora paroli, noklikšķiniet uz **Administrator Settings (Administratora iestatījumi)** > **Delete Administrator Authentication Information (Dzēst administratora autentifikācijas informāciju)** un pēc tam ievadiet administratora paroli.*

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.

Protokolu un pakalpojumu vadība

Drukāšanai var izmantot dažādus ceļus un protokolus. Netīšus drošības riskus var samazināt, ierobežojot drukāšanu no īpašiem ceļiem vai kontrolējot pieejamās funkcijas.

Protokolu vadība

Konfigurējiet protokola iestatījumus.

1 Atveriet Web Config un atlasiet **Services (Pakalpojumi)** > **Protocol (Protokols)**.

2 Konfigurējiet katru vienumu.

3 Noklikšķiniet uz **Next (Tālāk)**.

4 Noklikšķiniet uz **OK (Labi)**.

Printerim tiek piemēroti iestatījumi.

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.
➡ "Protokoli, kurus var iespējot vai atspējot" 31. lpp.
➡ "Protokolu iestatīšanas vienumi" 32. lpp.

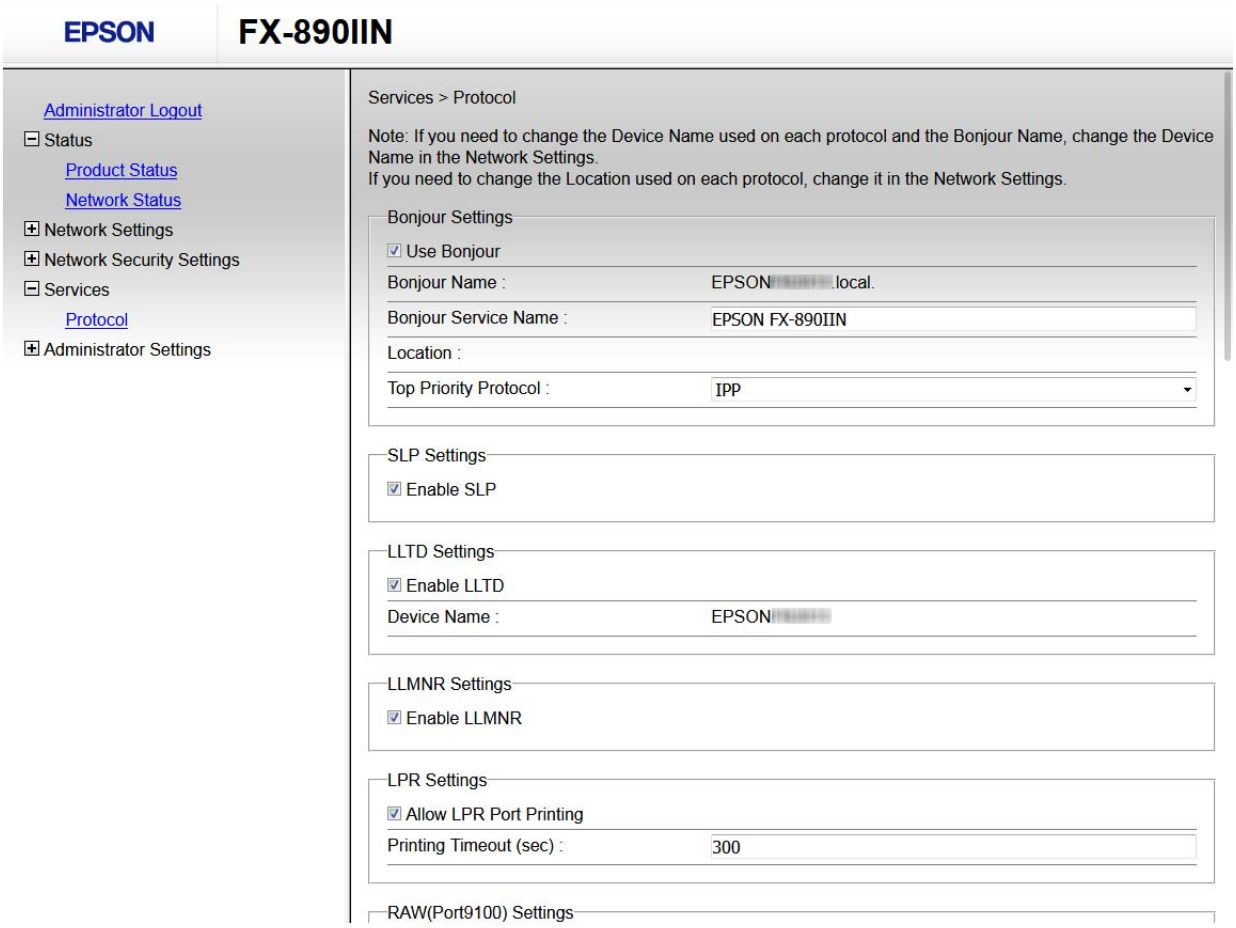
Protokoli, kurus var iespējot vai atspējot

Protokols	Apraksts
Bonjour settings (Bonjour iestatījumi)	Var norādīt, vai lietot Bonjour. Bonjour lieto, lai meklētu ierīces, drukātu (AirPrint) utt.
SLP Settings (SLP iestatījumi)	Var iespējot vai atspējot SLP funkciju. SLP funkciju lieto, lai meklētu tīklu programmā EpsonNet Config.
LLTD Settings (LLTD iestatījumi)	Var iespējot vai atspējot LLTD funkciju. Iespējojot šo funkciju, tas tiek parādīts Windows tīkla kartē.
LLMNR Settings (LLMNR iestatījumi)	Var iespējot vai atspējot LLMNR funkciju. Iespējojot šo funkciju, var lietot nosaukumu atpazīšanu bez NetBIOS pat tad, ja nevar lietot DNS.
LPR Settings (LPR iestatījumi)	Var norādīt, vai atļaut LPR drukāšanu. Iespējojot šo funkciju, var drukāt no LPR porta.
RAW(Port9100) Settings (RAW(Port9100) iestatījumi)	Var norādīt, vai atļaut drukāšanu no RAW porta (ports 9100). Iespējojot šo funkciju, var drukāt no RAW porta (ports 9100).
RAW(Custom Port) Settings (RAW (pielāgota porta) iestatījumi)	Var norādīt, vai atļaut drukāšanu no RAW porta (pielāgota porta). Iespējojot šo funkciju, var drukāt no RAW porta (pielāgota porta).
IPP Settings (IPP iestatījumi)	Var norādīt, vai atļaut drukāšanu no IPP. Iespējojot šo funkciju, var drukāt, izmantojot internetu (tostarp AirPrint).
FTP Settings (FTP iestatījumi)	Var norādīt, vai atļaut FTP drukāšanu. Iespējojot šo funkciju, var drukāt no FTP servera.
SNMPv1/v2c Settings (SNMPv1/v2c iestatījumi)	Var norādīt, vai iespējot SNMPv1/v2c. To izmanto ierīču iestatīšanai, pārraudzībai u.t.t.
SNMPv3 Settings (SNMPv3 iestatījumi)	Var norādīt, vai iespējot SNMPv3. To izmanto šifrētu ierīču iestatīšanai, pārraudzībai utt.

Saistītā informācija

➡ "Protokolu vadība" 30. lpp.
➡ "Protokolu iestatīšanas vienumi" 32. lpp.

Protokolu iestatīšanas vienumi



Vienības	Vērtības iestatīšana un apraksts
Bonjour settings (Bonjour iestatījumi)	
Use Bonjour (Lietot Bonjour)	Atlasiet šo iespēju, lai meklētu vai lietotu ierīces, izmantojot Bonjour. Nevar izmantot AirPrint, ja tas ir nodzēsts.
Bonjour Name (Bonjour nosaukums)	Tiek parādīts Bonjour nosaukums.
Bonjour Service Name (Bonjour pakalpojuma nosaukums)	Tiek parādīts Bonjour pakalpojuma nosaukums.
Location (Atrašanās vieta)	Tiek parādīts Bonjour atrašanās vietas nosaukums.
Top Priority Protocol (Augstākās prioritātes protokols)	Atlasiet augstākās prioritātes protokolu drukāšanai, izmantojot Bonjour.
SLP Settings (SLP iestatījumi)	
Enable SLP (Iespējot SLP)	Atlasiet šo iespēju, lai iespējotu SLP funkciju. To izmanto, lai meklētu tīklu programmā EpsonNet Config.
LLTD Settings (LLTD iestatījumi)	
Enable LLTD (Iespējot LLTD)	Atlasiet šo iespēju, lai iespējotu LLTD funkciju. Printeris tiek parādīts Windows tīkla mapē.
Device Name (Ierīces nosaukums)	Tiek parādīts LLTD ierīces nosaukums.

Drošības iestatījumi

Vienības	Vērtības iestatīšana un apraksts
LLMNR Settings (LLMNR iestatījumi)	
Enable LLMNR (Iespējot LLMNR)	Atlasiet šo iespēju, lai iespējotu LLMNR funkciju. Var lietot nosaukumu atpazīšanu bez NetBIOS pat tad, ja nevar lietot DNS.
LPR Settings (LPR iestatījumi)	
Allow LPR Port Printing (Atļaut drukāšanu no LPR porta)	Atlasiet, lai atļautu drukāšanu no LPR porta.
Printing Timeout (sec) (Drukāšanas taimauts (sek.))	Ievadiet taimauta vērtību LPR drukāšanai no 0 līdz 3600 sekundēm. Ja nevēlaties taimautu, ievadiet 0.
RAW(Port9100) Settings (RAW(Port9100) iestatījumi)	
Allow RAW(Port9100) Printing (Atļaut drukāšanu no RAW (ports 9100))	Atlasiet, lai atļautu drukāšanu no RAW porta (ports 9100).
Printing Timeout (sec) (Drukāšanas taimauts (sek.))	Ievadiet taimauta vērtību RAW porta (ports 9100) drukāšanai no 0 līdz 3600 sekundēm. Ja nevēlaties taimautu, ievadiet 0.
RAW(Custom Port) Settings (RAW (pielāgota porta) iestatījumi)	
Allow RAW(Custom Port) Printing (Atļaut drukāšanu no RAW (pielāgota porta))	Atlasiet, lai atļautu drukāšanu no RAW porta (pielāgots ports).
Port Number (Porta numurs)	Ievadiet porta numuru RAW (pielāgota porta) drukāšanai no 1024 līdz 65535, izņemot 9100, 1865 un 2968.
Printing Timeout (sec) (Drukāšanas taimauts (sek.))	Ievadiet taimauta vērtību RAW porta (pielāgota porta) drukāšanai no 0 līdz 3600 sekundēm. Ja nevēlaties taimautu, ievadiet 0.
IPP Settings (IPP iestatījumi)	
Enable IPP (Iespējot IPP)	Atlasiet, lai iespējotu IPP savienojumu. Tiek parādīti tikai tie printeri, kuri atbalsta IPP. Nevar izmantot AirPrint, ja tas ir atspējots.
Allow Non-secure Communication (Atļaut nedrošus sakarus)	Atlasiet, lai atļautu printerim izveidot sakarus bez jebkādiem drošības pasākumiem (IPP).
Communication Timeout (sec) (Sakaru taimauts (sek.))	Ievadiet taimauta vērtību IPP drukāšanai no 0 līdz 3600 sekundēm.
URL (Network (Tīkls))	Tiek parādīti IPP URL (http un https), kad printeris ir savienots ar vadu LAN. URL ir printera IP adreses, porta numura un IPP printera nosaukuma apvienotā vērtība.
Printer Name (Printera nosaukums)	Tiek parādīts IPP printera nosaukums.
Location (Atrašanās vieta)	Tiek parādīta IPP atrašanās vieta.
FTP Settings (FTP iestatījumi)	
Enable FTP Server (Iespējot FTP serveri)	Atlasiet, lai iespējotu FTP drukāšanu. Tiek parādīti tikai tie printeri, kuri atbalsta FTP drukāšanu.
Communication Timeout (sec) (Sakaru taimauts (sek.))	Ievadiet taimauta vērtību FTP sakariem no 0 līdz 3600 sekundēm. Ja nevēlaties taimautu, ievadiet 0.
SNMPv1/v2c Settings (SNMPv1/v2c iestatījumi)	

Drošības iestatījumi

Vienības	Vērtības iestatīšana un apraksts
Enable SNMPv1/v2c (Iespējot SNMPv1/v2c)	Atlasiet, lai iespējotu SNMPv1/v2c. Tiek parādīti tikai tie printeri, kuri atbalsta SNMPv3.
Access Authority (Piekļuves pilnvaras)	Iestatiet piekļuves pilnvaras, kad ir iespējots SNMPv1/v2c. Atlasiet **Read Only (Tikai lasīšanai)** vai **Read/Write (Lasīt/rakstīt)**.
Community Name (Read Only) (Kopienas nosaukums (tikai lasīšanai))	Ievadiet no 0 līdz 32 ASCII (0x20–0x7E) rakstzīmēm.
Community Name (Read/Write) (Kopienas nosaukums (lasīt/rakstīt))	Ievadiet no 0 līdz 32 ASCII (0x20–0x7E) rakstzīmēm.
SNMPv3 Settings (SNMPv3 iestatījumi)	
Enable SNMPv3 (Iespējot SNMPv3)	Atzīmējot izvēles rūtiņu, tiek iespējots SNMPv3.
User Name (Lietotājvārds)	Ievadiet no 1 līdz 32 vienbaita rakstzīmēm.
Authentication Settings (Autentifikācijas iestatījumi)	
Algorithm (Algoritms)	Atlasiet SNMPv3 autentificēšanas algoritmu.
Password (Parole)	Atlasiet SNMPv3 autentificēšanas paroli. Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E). Ja nenorādāt šo iestatījumu, atstājiet lauku tukšu.
Confirm Password (Apstiprināt paroli)	Lai apstiprinātu, ievadiet konfigurēto paroli.
Encryption Settings (Šifrēšanas iestatījumi)	
Algorithm (Algoritms)	Atlasiet SNMPv3 šifrēšanas algoritmu.
Password (Parole)	Atlasiet SNMPv3 šifrēšanas paroli. Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E). Ja nenorādāt šo iestatījumu, atstājiet lauku tukšu.
Confirm Password (Apstiprināt paroli)	Lai apstiprinātu, ievadiet konfigurēto paroli.
Context Name (Konteksta nosaukums)	Ievadiet 32 unikoda (UTF-8) rakstzīmes vai mazāku rakstzīmju skaitu. Ja nenorādāt šo iestatījumu, atstājiet lauku tukšu. Rakstzīmju skaits, ko var ievadīt, ir atkarīgs no valodas.

Saistītā informācija

➡ "Protokolu vadība" 30. lpp.
➡ "Protokoli, kurus var iespējot vai atspējot" 31. lpp.

SSL/TLS sakari ar printeri

Ja servera sertifikāts ir iestatīts, izmantojot SSL/TLS (drošligzdu slāņa/transporta slāņa drošības) sakarus ar printeri, sakaru ceļu starp datoriem var šifrēt. Veiciet šo procedūru, ja vēlaties novērst attālu un neatļautu piekļuvi.

Par ciparsertifikātiem

❏ CA parakstīts sertifikāts
Sertificēšanas iestādē jāiegūst CA (Certificate Authority — Sertificēšanas iestāde) parakstīts sertifikāts. Izmantojot CA parakstītu sertifikātu, var garantēt drošus sakarus. CA parakstītu sertifikātu var izmantot katrai drošības funkcijai.

❏ CA sertifikāts
CA sertifikāts liecina, ka servera identitāti ir pārbaudījusi trešā puse. Šis sertifikāts ir galvenā droša tīmekļa veida drošības sistēmas sastāvdaļa. Sertificēšanas iestādē jāiegūst servera autentifikācijas CA sertifikāts.

❏ Pašparakstīts sertifikāts
Pašparakstīts sertifikāts ir sertifikāts, kuru izsniedz un paraksta pats printeris. Šis sertifikāts ir neuzticams un nenovērš izlikšanos. Ja izmantojat šo sertifikātu SSL/TLS sertifikātam, pārlūkprogrammā var tikt parādīts drošības brīdinājums. Šo sertifikātu var izmantot tikai SSL/TLS sakariem.

Saistītā informācija

➡ "CA parakstīta sertifikāta iegūšana un importēšana" 35. lpp.
➡ "CA parakstīta sertifikāta dzēšana" 38. lpp.
➡ "Pašparakstīta sertifikāta atjaunināšana" 39. lpp.

CA parakstīta sertifikāta iegūšana un importēšana

CA parakstīta sertifikāta iegūšana

Lai iegūtu CA parakstītu sertifikātu, izveidojiet sertifikāta parakstīšanas pieprasījumu (CSR — Certificate Signing Request) un iesniedziet to sertificēšanas iestādē. CSR var izveidot, izmantojot programmu Web Config un datoru.

Lai izveidotu CSR un iegūtu CA parakstītu sertifikātu, izmantojot Web Config, veiciet tālāk norādītās darbības. CSR izveidei izmantojot Web Config, sertifikāta formāts ir PEM/DER.

1 Atveriet programmu Web Config un pēc tam atlasiet **Network Security Settings (Tīkla drošības iestatījumi)**. Tālāk atlasiet **SSL/TLS** > **Certificate (Sertifikāts)**.

2 Sadaļā **CSR** noklikšķiniet uz **Generate (Ģenerēt)**.

Tiek atvērta CSR izveides lapa.

3 Ievadiet katra vienuma vērtību.

> ***Piezīme.***
> *Pieejamais atslēgas garums un saīsinājumi atšķiras atkarībā no sertifikācijas iestādes. Izveidojiet pieprasījumu atbilstīgi katras sertificēšanas iestādes noteikumiem.*

4 Noklikšķiniet uz **OK (Labi)**.

Tiek parādīts ziņojums par pabeigšanu.

5 Atlasiet **Network Security Settings (Tīkla drošības iestatījumi)**. Tālāk atlasiet **SSL/TLS** > **Certificate (Sertifikāts)**.

6 Lai lejupielādētu CSR datorā, noklikšķiniet uz sertificēšanas iestādes attiecīgā formāta **CSR** sertifikāta lejupielādes pogas.

> ***Svarīgi!***
> *Neģenerējiet CSR no jauna. Ja tā izdarāt, iespējams, nevarēs importēt izsniegtu CA parakstītu sertifikātu.*

7 Nosūtiet CSR sertificēšanas iestādei un iegūstiet CA parakstītu sertifikātu.

Ievērojiet katras sertificēšanas iestādes nosūtīšanas un formas noteikumus.

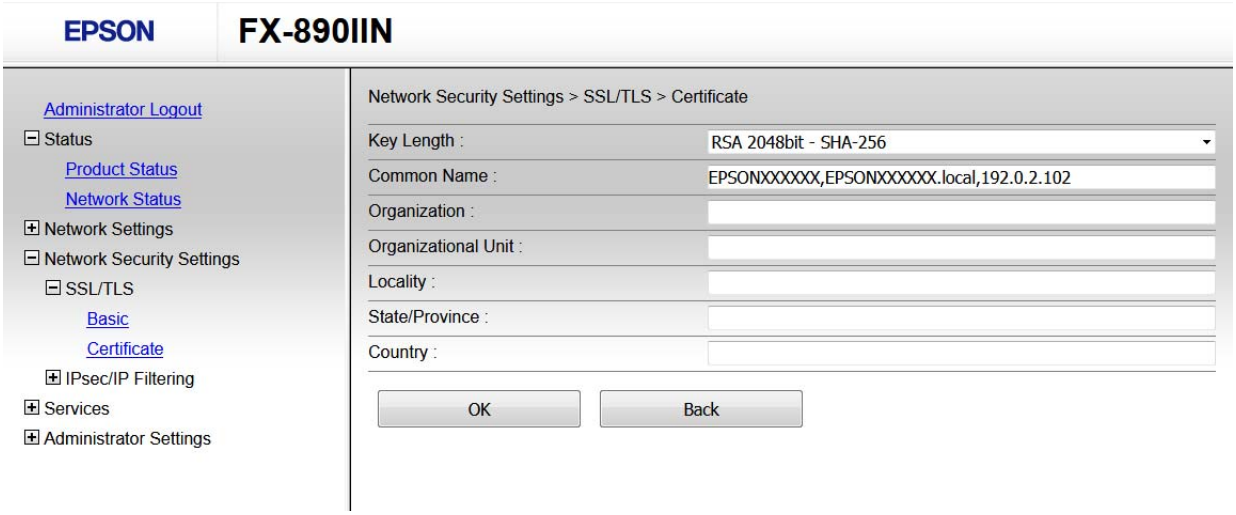
8 Saglabājiet izsniegto, CA parakstīto sertifikātu datorā, kas pievienots printerim.

Kad sertifikāts tiek saglabāts galamērķī, CA parakstīta sertifikāta iegūšana ir pabeigta.

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.
➡ "CSR vienumu iestatīšana" 36. lpp.
➡ "CA parakstīta sertifikāta importēšana" 37. lpp.

CSR vienumu iestatīšana



Vienības	Iestatījumi un skaidrojumi
Key Length (Atslēgas garums)	Atlasiet CSR atslēgas garumu.
Common Name (Kopējais nosaukums)	Var ievadīt no 1 līdz 128 rakstzīmēm. Ja tā ir IP adrese, tai jābūt statiskai IP adresi. Piemērs: Web Config piekļuves vietrādis URL: https://10.152.12.225 Kopējais nosaukums: 10.152.12.225
Organization (Organizācija)/ Organizational Unit (Organizācijas vienība)/ Locality (Vieta)/ State/Province (Novads/ pagasts)	Ievadiet no 0 līdz 64 ASCII rakstzīmēm (0x20 - 0x7E). Atšķiramos nosaukumus var atdalīt, izmantojot komatus.
Country (Valsts)	Ievadiet valsts divciparu kodu atbilstīgi standarta ISO-3166 noteikumiem.

Saistītā informācija

➡ "CA parakstīta sertifikāta iegūšana" 35. lpp.

CA parakstīta sertifikāta importēšana

Svarīgi!

❏ *Pārliecinieties, vai printera datums un laiks ir iestatīts pareizi.*

❏ *Ja sertifikāts ir iegūts, izmantojot programmā Web Config izveidotu CSR, sertifikātu var importēt vienu reizi.*

1 Atveriet programmu Web Config un pēc tam atlasiet **Network Security Settings (Tīkla drošības iestatījumi)**. Tālāk atlasiet **SSL/TLS** > **Certificate (Sertifikāts)**.

2 Noklikšķiniet uz **Import (Importēt)**.

Tiek atvērta sertifikāta importēšanas lapa.

3 Ievadiet katra vienuma vērtību.

Atkarībā no CSR izveides vietas un sertifikāta faila formāta nepieciešamie iestatījumi var atšķirties. Ievadiet nepieciešamās vienumu vērtības, ievērojot turpmāk sniegtos norādījumus.

❏ PEM/DER formāta sertifikāts, kas iegūts no Web Config
- **Private Key (Privātā atslēga)**: nekonfigurējiet, jo printerī ir privāta atslēga.
- **Password (Parole)**: nekonfigurējiet.
- **CA Certificate 1 (1. CA sertifikāts)**/**CA Certificate 2 (2. CA sertifikāts)**: pēc izvēles

❏ PEM/DER formāta sertifikāts, kas iegūts no datora
- **Private Key (Privātā atslēga)**: jāiestata.
- **Password (Parole)**: nekonfigurējiet.
- **CA Certificate 1 (1. CA sertifikāts)**/**CA Certificate 2 (2. CA sertifikāts)**: pēc izvēles

❏ PKCS#12 formāta sertifikāts, kas iegūts no datora
- **Private Key (Privātā atslēga)**: nekonfigurējiet.
- **Password (Parole)**: pēc izvēles
- **CA Certificate 1 (1. CA sertifikāts)**/**CA Certificate 2 (2. CA sertifikāts)**: nekonfigurējiet.

4 Noklikšķiniet uz **OK (Labi)**.

Tiek parādīts ziņojums par pabeigšanu.

Piezīme.

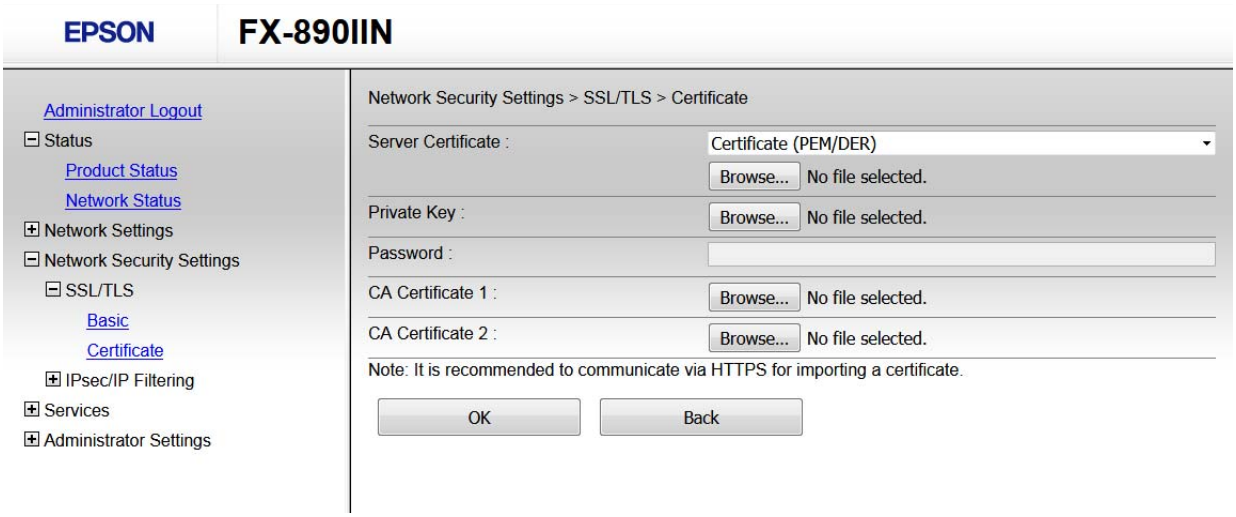
Lai pārbaudītu sertifikāta informāciju, noklikšķiniet uz ***Confirm (Apstiprināt)****.*

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.

➡ "CA parakstīta sertifikāta importēšanas vienumu iestatīšana" 38. lpp.

CA parakstīta sertifikāta importēšanas vienumu iestatīšana



Vienības	Iestatījumi un skaidrojumi
Server Certificate (Servera sertifikāts) vai Client Certificate (Klienta sertifikāts)	Atlasiet sertifikāta formātu.
Private Key (Privātā atslēga)	Ja PEM/DER formāta sertifikāts ir iegūts, izmantojot datorā izveidotu CSR, norādiet sertifikātam atbilstīgu privāto atslēgas failu.
Password (Parole)	Lai šifrētu privāto atslēgu, ievadiet paroli.
CA Certificate 1 (1. CA sertifikāts)	Ja sertifikāta formāts ir **Certificate (PEM/DER) (Sertifikāts (PEM/DER))**, importējiet sertificēšanas iestādes izsniegto sertifikātu. Ja nepieciešams, norādiet failu.
CA Certificate 2 (2. CA sertifikāts)	Ja sertifikāta formāts ir **Certificate (PEM/DER)**, importējiet sertificēšanas iestādes izsniegto sertifikātu **CA Certificate 1 (1. CA sertifikāts)**. Ja nepieciešams, norādiet failu.

Saistītā informācija

➡ "CA parakstīta sertifikāta importēšana" 37. lpp.

CA parakstīta sertifikāta dzēšana

Importētu sertifikātu var dzēst, kad beidzies tā derīguma termiņš vai kad šifrēts savienojums vairs nav nepieciešams.

> ***Svarīgi!***
> *Ja sertifikāts ir iegūts, izmantojot programmā Web Config izveidotu CSR, dzēstu sertifikātu nevar importēt vēlreiz. Šādā gadījumā izveidojiet CSR un iegūstiet sertifikātu vēlreiz.*

1. Atveriet programmu Web Config un pēc tam atlasiet **Network Security Settings (Tīkla drošības iestatījumi)**. Tālāk atlasiet **SSL/TLS** > **Certificate (Sertifikāts)**.
2. Noklikšķiniet uz **Delete (Dzēst)**.
3. Apstipriniet, ka vēlaties dzēst sertifikātu, kas parādīts ziņojumā.

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.

Pašparakstīta sertifikāta atjaunināšana

Ja printeris atbalsta servera funkciju HTTPS, var atjaunināt pašparakstītu sertifikātu. Piekļūstot programmai Web Config ar pašparakstītu sertifikātu, tiek parādīts brīdinājuma ziņojums.

Izmantojiet pašparakstītu sertifikātu īslaicīgi, līdz iegūstat un saņemat CA parakstītu sertifikātu.

1. Atveriet programmu Web Config un atlasiet **Network Security Settings (Tīkla drošības iestatījumi)** > **SSL/TLS** > **Certificate (Sertifikāts)**.

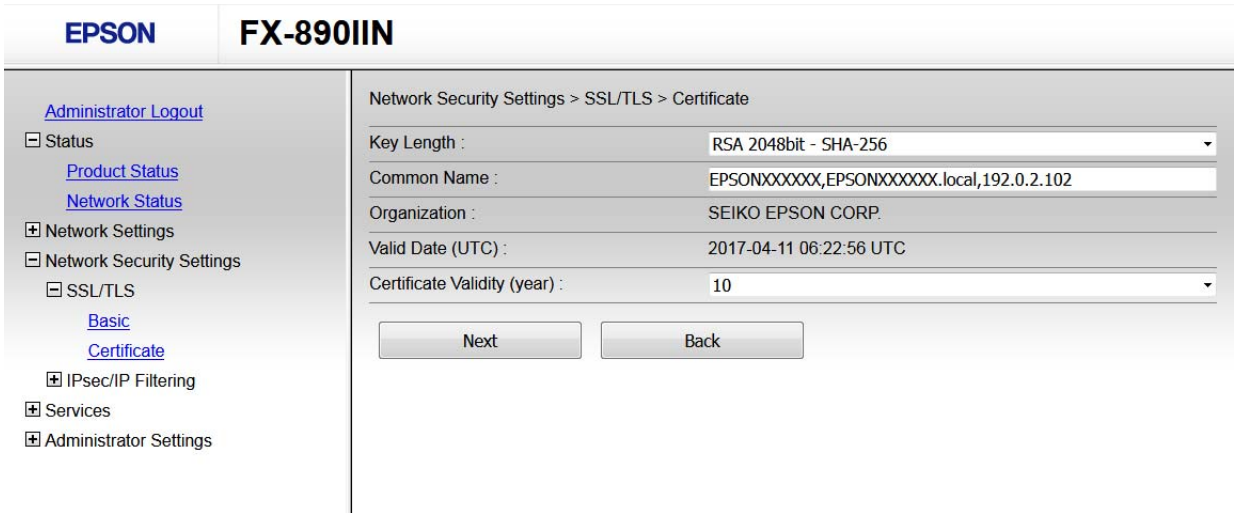
2. Noklikšķiniet uz **Update (Atjaunināt)**.

3. Atveriet **Common Name (Kopējais nosaukums)**.

   Ievadiet IP adresi vai identifikatoru, piemēram, printera FQDN nosaukumu. Var ievadīt no 1 līdz 128 rakstzīmēm.

   > ***Piezīme.***
   > *Atšķiramos nosaukumus (CN) var atdalīt, izmantojot komatus.*

4. Norādiet sertifikāta derīguma termiņu.



5. Noklikšķiniet uz **Next (Tālāk)**.

   Tiek parādīts apstiprinājuma ziņojums.

6. Noklikšķiniet uz **OK (Labi)**.

   Printeris tiek atjaunināts.

Piezīme.
Lai pārbaudītu sertifikāta informāciju, noklikšķiniet uz Confirm (Apstiprināt).

Saistītā informācija
➡ "Piekļuve Web Config" 20. lpp.

Šifrētie sakari, izmantojot IPsec/IP filtrēšanu

Par IPsec/IP Filtering (IPsec/IP filtrēšanu)

Ja printeris atbalsta IPsec/IP filtrēšanu, var filtrēt trafiku, izmantojot IP adreses, pakalpojumus un portu. Kombinējot filtrēšanas metodes, var konfigurēt printeri tā, lai tas pieņemtu vai bloķētu noteiktus klientus un noteiktus datus. Turklāt, izmantojot IPsec, var uzlabot drošības pakāpi.

Lai filtrētu trafiku, konfigurējiet noklusējuma politiku. Noklusējuma politika attiecas uz visiem lietotājiem vai grupām, kas veido savienojumu ar printeri. Lai precīzāk noteiktu lietotāju grupu un atsevišķu lietotāju tiesības, konfigurējiet grupu politikas. Grupas politika ir viena vai vairākas kārtulas, kas piemērotas lietotāju grupai vai lietotājam. Printeris kontrolē IP paketes, kas atbilst konfigurētajām politikām. IP paketes tiek autentificētas 1.–10. grupas politikas secībā, pēc tam tiek piemērota noklusējuma politika.

Piezīme.
Datori ar operētājsistēmu Windows Vista vai jaunāku Windows versiju vai Windows Server 2008 atbalsta IPsec.

Noklusējuma politikas konfigurēšana

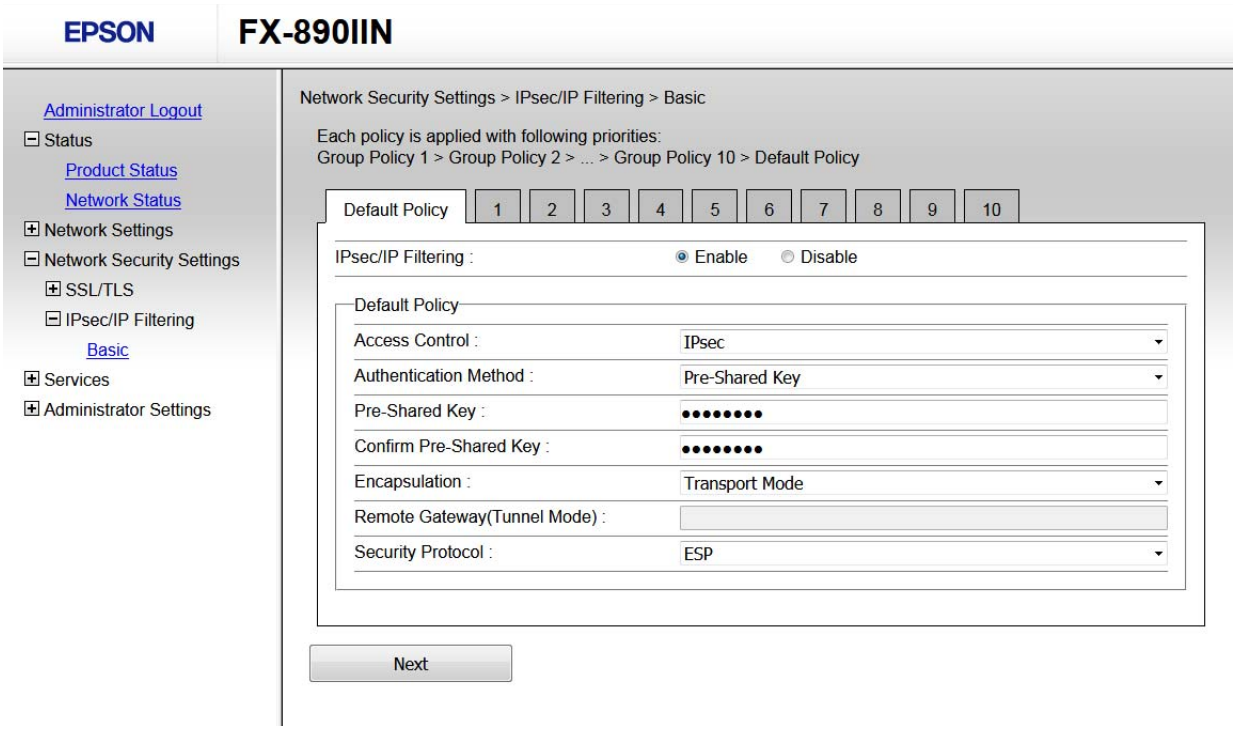
1. Atveriet programmu Web Config un atlasiet **Network Security Settings (Tīkla drošības iestatījumi)** > **IPsec/IP Filtering (IPsec/IP filtrēšana)** > **Basic (Pamata)**.
2. Ievadiet katra vienuma vērtību.
3. Noklikšķiniet uz **Next (Tālāk)**.

   Tiek parādīts apstiprinājuma ziņojums.
4. Noklikšķiniet uz **OK (Labi)**.

   Printeris tiek atjaunināts.

Saistītā informācija
➡ "Piekļuve Web Config" 20. lpp.
➡ "Noklusējuma politikas vienumu iestatīšana" 41. lpp.

Noklusējuma politikas vienumu iestatīšana



Vienības	Iestatījumi un skaidrojumi	
IPsec/IP Filtering (IPsec/IP filtrēšana)	Var iespējot vai atspējot IPsec/IP filtrēšanas funkciju.	
Access Control (Piekļuves vadība)	Konfigurējiet IP pakešu trafika kontroles metodi.	
	Permit Access (Atļaut piekļuvi)	Atlasiet šo opciju, lai atļautu konfigurēto IP pakešu tranzītu.
	Refuse Access (Noraidīt piekļuvi)	Atlasiet šo opciju, lai noraidītu konfigurēto IP pakešu tranzītu.
	IPsec	Atlasiet šo opciju, lai atļautu konfigurēto IPsec pakešu tranzītu.
Authentication Method (Autentifikācijas metode)	Parāda saderīgās autentifikācijas metodes.	
Pre-Shared Key (Iepriekš koplietota atslēga)	Ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.	
Confirm Pre-Shared Key (Apstiprināt iepriekš koplietotu atslēgu)	Lai apstiprinātu, ievadiet konfigurēto atslēgu.	
Encapsulation (Iekapsulēšana)	Atlasot **IPsec** kā **Access Control (Piekļuves vadība)** iestatījumu, jākonfigurē iekapsulēšanas režīms.	
	Transport Mode (Transporta režīms)	Atlasiet šo opciju, ja izmantojat printeri tikai vienā lokālajā tīklā (LAN). 4. slāņa un jaunākas IP paketes tiek šifrētas.
	Tunnel Mode (Tuneļa režīms)	Atlasiet šo opciju, ja izmantojat printeri tīklā ar interneta izmantošanas iespēju, piemēram, IPsec-VPN tīklā. Tiek šifrētas IP pakešu galvenes un dati.

Drošības iestatījumi

Vienības	Iestatījumi un skaidrojumi	
Remote Gateway(Tunnel Mode) (Attālā vārteja (tuneļa režīms))	Atlasot **Tunnel Mode (Tuneļa režīms)** kā **Encapsulation (Iekapsulēšana)** iestatījumu, ievadiet vārtejas adresi, kuras garums ir no 1 līdz 39 rakstzīmēm.	
Security Protocol (Drošības protokols)	Atlasot **IPsec** kā **Access Control (Piekļuves vadība)** iestatījumu, jāizvēlas kāda no opcijām.	
	ESP	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti un šifrētu datus.
	AH	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti. Pat tad, ja datu šifrēšana ir aizliegta, IPsec var izmantot.

Saistītā informācija

➡ "Noklusējuma politikas konfigurēšana" 40. lpp.

Grupas politikas konfigurēšana

1. Atveriet printera programmuWeb Config un atlasiet **Network Security Settings (Tīkla drošības iestatījumi)** > **IPsec/IP Filtering (IPsec/IP filtrēšana)** > **Basic (Pamata)**.
2. Noklikšķiniet uz konfigurējamās numurētās cilnes.
3. Ievadiet katra vienuma vērtību.
4. Noklikšķiniet uz **Next (Tālāk)**.

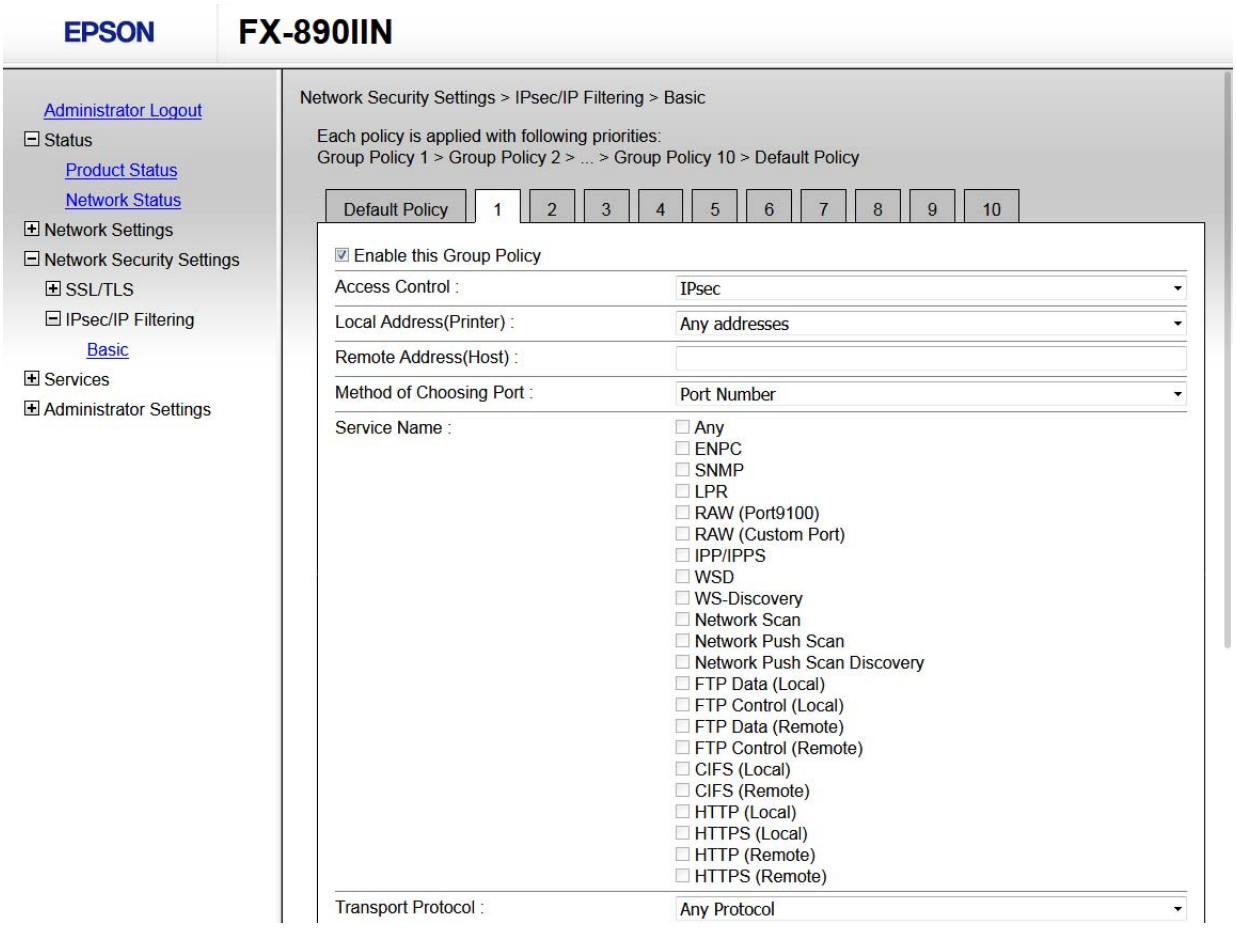
   Tiek parādīts apstiprinājuma ziņojums.
5. Noklikšķiniet uz **OK (Labi)**.

   Printeris tiek atjaunināts.

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.
➡ "Grupas politikas vienumu iestatīšana" 43. lpp.

Grupas politikas vienumu iestatīšana



Vienības	Iestatījumi un skaidrojumi	
Enable this Group Policy (Iespējot šīs grupas politiku)	Var iespējot vai atspējot grupas politiku.	
Access Control (Piekļuves vadība)	Konfigurējiet IP pakešu trafika kontroles metodi.	
	Permit Access (Atļaut piekļuvi)	Atlasiet šo opciju, lai atļautu konfigurēto IP pakešu tranzītu.
	Refuse Access (Noraidīt piekļuvi)	Atlasiet šo opciju, lai noraidītu konfigurēto IP pakešu tranzītu.
	IPsec	Atlasiet šo opciju, lai atļautu konfigurēto IPsec pakešu tranzītu.
Local Address(Printer) (Lokālā adrese (printeris))	Izvēlieties IPv4 vai IPv6 adresi, kas atbilst jūsu tīkla videi. Ja IP adrese tiek piešķirta automātiski, var atlasīt **Use auto-obtained IPv4 address (Lietot automātiski iegūtu IPv4 adresi)**.	
Remote Address(Host) (Attālā adrese (resursdators))	Lai kontrolētu piekļuvi, ievadiet ierīces IP adresi. IP adrese var būt līdz 43 rakstzīmēm gara. Ja IP adrese netiek ievadīta, tiek kontrolētas visas adreses. Piezīme. Ja IP adreses tiek piešķirtas automātiski (piemēram, adreses piešķir DHCP), savienojums var nebūt pieejams. Konfigurējiet statisko IP adresi.	

Drošības iestatījumi

Vienības	Iestatījumi un skaidrojumi	
Method of Choosing Port (Porta izvēles metode)	Atlasiet portu norādīšanas metodi.	
Service Name (Pakalpojuma nosaukums)	Atlasot **Service Name (Pakalpojuma nosaukums)** kā **Method of Choosing Port (Portu izvēles metode)** iestatījumu, jāizvēlas kāda no opcijām.	
Transport Protocol (Transporta protokols)	Atlasot **Port Number (Porta numurs)** kā **Method of Choosing Port (Portu izvēles metode)** iestatījumu, jākonfigurē iekapsulēšanas režīms.	
	Any Protocol (Jebkurš protokols)	Atlasiet, lai kontrolētu visu veidu protokolus.
	TCP	Atlasiet, lai kontrolētu uniraides datus.
	UDP	Atlasiet, lai kontrolētu apraides un multiraides datus.
	ICMPv4	Atlasiet, lai kontrolētu ehotestēšanas komandu.
Local Port (Lokālais ports)	Atlasot **Port Number (Porta numurs)** kā **Method of Choosing Port (Portu izvēles metode)** iestatījumu, un **TCP** vai **UDP** - kā **Transport Protocol (Transporta protokols)** iestatījumu, ievadiet portu numurus, lai kontrolētu pakešu saņemšanu, atdalot tos ar komatiem. Var ievadīt līdz 10 portu numuriem. Piemērs: 20,80,119,5220 Ja porta numurs nav ievadīts, tiek kontrolēti visi porti.	
Remote Port (Attālais ports)	Atlasot **Port Number (Porta numurs)** kā **Method of Choosing Port (Portu izvēles metode)** iestatījumu, un **TCP** vai **UDP** - kā **Transport Protocol (Transporta protokols)** iestatījumu, ievadiet portu numurus, lai kontrolētu pakešu sūtīšanu, atdalot tos ar komatiem. Var ievadīt līdz 10 portu numuriem. Piemērs: 25,80,143,5220 Ja porta numurs nav ievadīts, tiek kontrolēti visi porti.	
Authentication Method (Autentifikācijas metode)	Atlasot **IPsec** kā **Access Control (Piekļuves vadība)** iestatījumu, jāizvēlas kāda no opcijām.	
Pre-Shared Key (Iepriekš koplietota atslēga)	Ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.	
Confirm Pre-Shared Key (Apstiprināt iepriekš koplietotu atslēgu)	Lai apstiprinātu, ievadiet konfigurēto atslēgu.	
Encapsulation (Iekapsulēšana)	Atlasot **IPsec** kā **Access Control (Piekļuves vadība)** iestatījumu, jākonfigurē iekapsulēšanas režīms.	
	Transport Mode (Transporta režīms)	Atlasiet šo opciju, ja izmantojat printeri tikai vienā lokālajā tīklā (LAN). 4. slāņa un jaunākas IP paketes tiek šifrētas.
	Tunnel Mode (Tuneļa režīms)	Atlasiet šo opciju, ja izmantojat printeri tīklā ar interneta izmantošanas iespēju, piemēram, IPsec-VPN tīklā. Tiek šifrētas IP pakešu galvenes un dati.
Remote Gateway(Tunnel Mode) (Attālā vārteja (tuneļa režīms))	Atlasot **Tunnel Mode (Tuneļa režīms)** kā **Encapsulation (Iekapsulēšana)** iestatījumu, ievadiet vārtejas adresi, kuras garums ir no 1 līdz 39 rakstzīmēm.	

Drošības iestatījumi

Vienības	Iestatījumi un skaidrojumi	
Security Protocol (Drošības protokols)	Atlasot **IPsec** kā **Access Control (Piekļuves vadība)** iestatījumu, jāizvēlas kāda no opcijām.	
	ESP	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti un šifrētu datus.
	AH	Atlasiet šo opciju, lai nodrošinātu autentifikācijas un datu integritāti. Pat tad, ja datu šifrēšana ir aizliegta, IPsec var izmantot.

Saistītā informācija

➡ "Grupas politikas konfigurēšana" 42. lpp.
➡ "Local Address(Printer) (Lokālās adreses) (printera) un Remote Address(Host) (Attālās adreses (resursdatora)) kombinācija grupas politikā" 45. lpp.
➡ "Norādes uz pakalpojuma nosaukumiem grupas politikā" 45. lpp.

Local Address(Printer) (Lokālās adreses) (printera) un Remote Address(Host) (Attālās adreses (resursdatora)) kombinācija grupas politikā

		Lokālās adreses (printera) iestatīšana		
		IPv4	**IPv6*2**	**Jebkuras adreses*3**
Attālās adreses (resursdatora) iestatīšana	IPv4*1	✓	-	✓
	IPv6*1*2	-	✓	✓
	Tukšs	✓	✓	✓

*1: ja izvēlas **IPsec** kā **Access Control (Piekļuves vadība)** iestatījumu, nevar norādīt prefiksa garumu.

*2: ja izvēlas **IPsec** kā **Access Control (Piekļuves vadība)** iestatījumu, var izvēlēties saiti-lokālo adresi (fe80::), taču grupas politika tiks atspējota.

*3: izņemot IPv6 saites lokālās adreses.

Norādes uz pakalpojuma nosaukumiem grupas politikā

Piezīme.
Nepieejamie pakalpojumi ir redzami, taču tos nevar atlasīt.

Pakalpojuma nosaukums	Protokola veids	Lokālā porta numurs	Attālā porta numurs	Kontrolētās funkcijas
Jebkurš	-	-	-	Visi pakalpojumi
ENPC	UDP	3289	Jebkurš ports	Printera meklēšana, izmantojot tādas programmas kā Epson-Net Config, printera vai skenera draiverus

Drošības iestatījumi

Pakalpojuma nosaukums	Protokola veids	Lokālā porta numurs	Attālā porta numurs	Kontrolētās funkcijas
SNMP	UDP	161	Jebkurš ports	MIB iegūšana un konfigurēšana, izmantojot tādas programmas kā EpsonNet Config, Epson printera draiveris vai Epson skenera draiveris
LPR	TCP	515	Jebkurš ports	LPR datu pārsūtīšana
RAW (Port9100) (RAW (ports 9100))	TCP	9100	Jebkurš ports	RAW datu pārsūtīšana
RAW(Custom Port) (RAW (pielāgots ports))	TCP	2501 (noklusējuma)	Jebkurš ports	RAW datu pārsūtīšana
IPP/IPPS	TCP	631	Jebkurš ports	AirPrint datu pārsūtīšana (IPP/IPPS druka)
WSD	TCP	Jebkurš ports	5357	WSD vadība
WS-Discovery	UDP	3702	Jebkurš ports	Printera meklēšana no WSD
Network Scan (Tīkla skenēšana)	TCP	1865	Jebkurš ports	Skenēšanas datu pārsūtīšana no Document Capture Pro
Network Push Scan (Tīkla pašpiegādes skenēšana)	TCP	Jebkurš ports	2968	Pašpiegādes skenēšanas uzdevumu informācijas ieguve programmā Document Capture Pro
Network Push Scan Discovery	UDP	2968	Jebkurš ports	Datora meklēšana, veicot pašpiegādes skenēšanu programmā Document Capture Pro
FTP Data (Local) (FTP dati (lokāli))	TCP	20	Jebkurš ports	FTP serveris (FTP drukas datu pārsūtīšana)
FTP control (Local) (FTP vadība (lokāli))	TCP	21	Jebkurš ports	FTP serveris (FTP drukas vadība)
FTP Data (Local) (FTP dati (attāli))	TCP	Jebkurš ports	20	FTP klients (skenēšanas datu un saņemto faksu datu pārsūtīšana) Tomēr šādi var kontrolēt FTP serveri tikai tad, ja tajā izmantotais attālā porta numurs ir 20.

Drošības iestatījumi

Pakalpojuma nosaukums	Protokola veids	Lokālā porta numurs	Attālā porta numurs	Kontrolētās funkcijas
FTP Control (Remote) (FTP vadība (attāli))	TCP	Jebkurš ports	21	FTP klients (skenēšanas datu un saņemto faksu datu pārsūtīšanas vadība)
CIFS (Local) (CIFS (lokāli))	TCP	445	Jebkurš ports	CIFS serveris (tīkla mapes koplietošana)
CIFS (Remote) (CIFS (attāli))	TCP	Jebkurš ports	445	CIFS klients (skenēšanas datu un saņemto faksu datu pārsūtīšana uz mapi)
HTTP (Local) (HTTP (lokāli))	TCP	80	Jebkurš ports	HTTP(S) serveris (Web Config un WSD datu pārsūtīšana)
HTTPS (Local) (HTTPS (lokāli))	TCP	443	Jebkurš ports	
HTTP (Remote) (HTTP (attāli))	TCP	Jebkurš ports	80	HTTP(S) klients (savstarpējie sakari Epson Connect vai Google Cloud Print, aparātprogrammatūras un saknes sertifikāta atjaunināšanai)
HTTPS (Remote) (HTTPS (attāli))	TCP	Jebkurš ports	443	

IPsec/IP Filtering (Psec/IP filtrēšanas) konfigurāciju piemēri

Tikai IPsec pakešu saņemšana
Piemērā skaidrota tikai noklusējuma politikas konfigurēšana.

Default Policy (Noklusējuma politika):

❏ **IPsec/IP Filtering (IPsec/IP filtrēšana)**: **Enable (iespējot)**

❏ **Access Control (Piekļuves vadība)**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key (Iepriekš koplietota atslēga)**

❏ **Pre-Shared Key (Iepriekš koplietota atslēga)**: ievadiet līdz 127 rakstzīmēm.

Group Policy (Grupas politika):
nekonfigurējiet.

Drukas datu un printera iestatījumu saņemšana
Šajā piemērā tiek atļauta drukas datu un printera konfigurācijas pārraide no norādītajiem pakalpojumiem.

Default Policy (Noklusējuma politika):

❏ **IPsec/IP Filtering (IPsec/IP filtrēšana)**: **Enable (iespējot)**

❏ **Access Control (Piekļuves vadība)**: **Refuse Access (Noraidīt piekļuvi)**

Group Policy (Grupas politika):

❏ **Enable this Group Policy (Iespējot šīs grupas politiku)**: atzīmējiet izvēles rūtiņu.

❏ **Access Control (Piekļuves vadība)**: **Permit Access (Atļaut piekļuvi)**

❏ **Remote Address(Host) (Attālā adrese (resursdators))**: klienta IP adrese

❏ **Method of Choosing Port (Porta izvēles metode)**: **Service Name (Pakalpojuma nosaukums)**

❏ **Service Name (Pakalpojuma nosaukums)**: atzīmējiet izvēles rūtiņas **ENPC**, **SNMP**, **HTTP (Local) (HTTP (lokāli))**, **HTTPS (Local) (HTTPS (lokāli))** un **RAW (Port9100)**.

Piekļuves piešķiršana tikai norādītajai IP adresei
Šajā piemērā redzams, kā atļaut piekļuvi printerim no norādītas IP adreses.

Default Policy (Noklusējuma politika):

❏ **IPsec/IP Filtering (IPsec/IP filtrēšana)**: **Enable (iespējot)**

❏ **Access Control (Piekļuves vadība)**: **Refuse Access (Noraidīt piekļuvi)**

Group Policy (Grupas politika):

❏ **Enable this Group Policy (Iespējot šīs grupas politiku)**: atzīmējiet izvēles rūtiņu.

❏ **Access Control (Piekļuves vadība)**: **Permit Access (Atļaut piekļuvi)**

❏ **Remote Address(Host) (Attālās adreses (Resursdatora))**: administratora klienta IP adrese

Piezīme.
Neatkarīgi no politikas konfigurācijas klients varēs piekļūt printerim un konfigurēt to.

Protokola SNMPv3 izmantošana

Par SNMPv3

SNMP ir pārraudzības un vadības protokols ar tīklu savienoto ierīču informācijas vākšanai. SNMPv3 ir uzlabota pārvaldības drošības funkcijas versija.

Izmantojot SNMPv3, SNMP sakaru (pakešu) stāvokļa pārraudzības un iestatījumu izmaiņas var autentificēt un šifrēt, lai aizsargātu SNMP sakarus (paketes) pret apdraudējumiem tīklā, piemēram, pārtveršanu, uzdošanos par citu personu un manipulācijām ar datiem.

SNMPv3 konfigurēšana

Ja printeris atbalsta protokolu SNMPv3, iespējams uzraudzīt un pārvaldīt piekļuvi printerim.

1 Atveriet Web Config un atlasiet **Services (Pakalpojumi)** > **Protocol (Protokols)**.

2 Ievadiet katra **SNMPv3 Settings (SNMPv3 iestatījumi)** vienuma vērtību.

3 Noklikšķiniet uz **Next (Tālāk)**.

Tiek parādīts apstiprinājuma ziņojums.

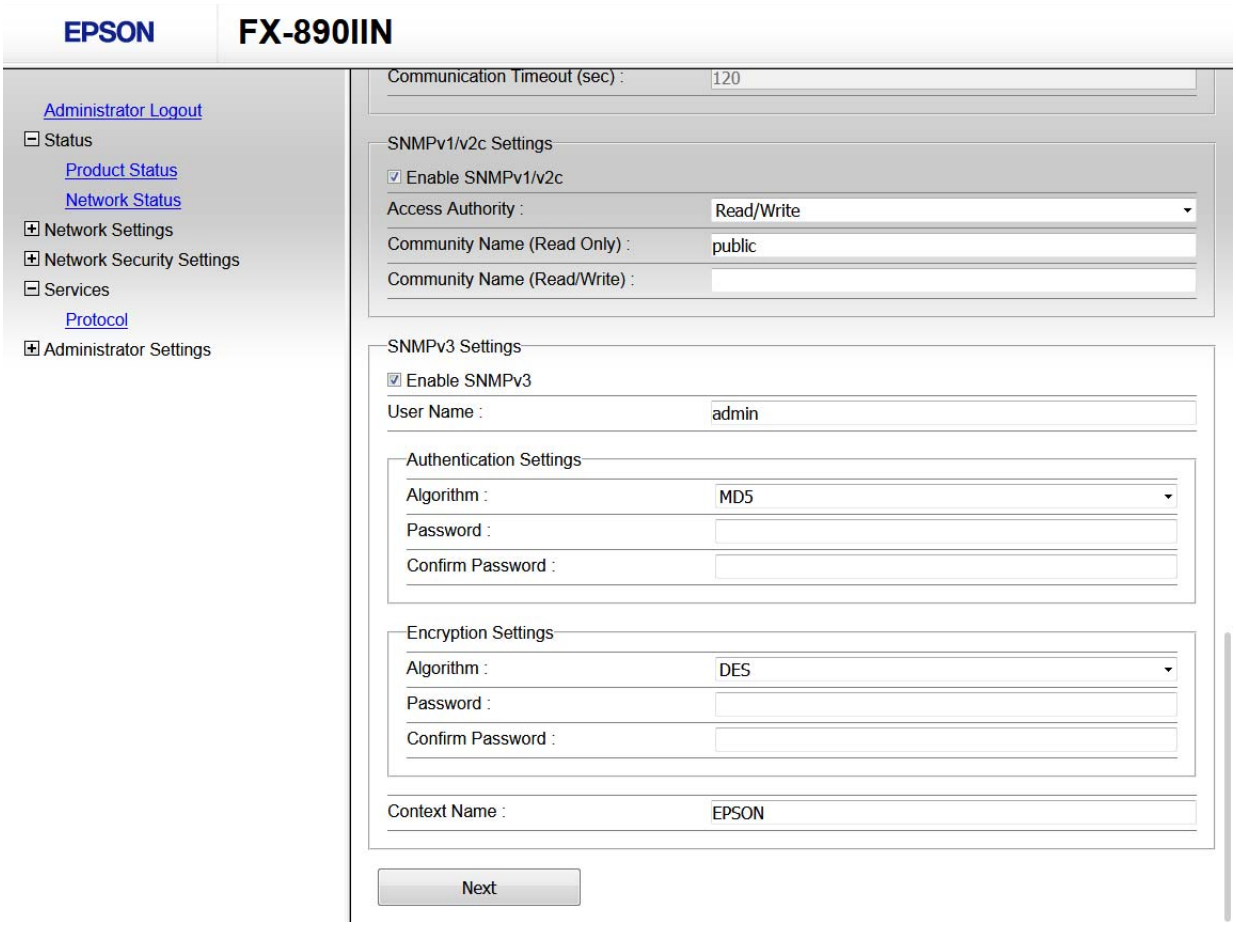
4 Noklikšķiniet uz **OK (Labi)**.

Printeris tiek atjaunināts.

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.
➡ "SNMPv3 vienumu iestatīšana" 49. lpp.

SNMPv3 vienumu iestatīšana



Vienības	Iestatījumi un skaidrojumi
Enable SNMPv3 (Iespējot SNMPv3)	Atzīmējot izvēles rūtiņu, tiek iespējots SNMPv3.
User Name (Lietotājvārds)	Ievadiet no 1 līdz 32 vienbaita rakstzīmēm.
Authentication Settings (Autentifikācijas iestatījumi)	
Algorithm (Algoritms)	Atlasiet autentificēšanas algoritmu.

Drošības iestatījumi

Vienības	Iestatījumi un skaidrojumi
Password (Parole)	Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E).
Confirm Password (Apstiprināt paroli)	Lai apstiprinātu, ievadiet konfigurēto paroli.
Encryption Settings (Šifrēšanas iestatījumi)	
Algorithm (Algoritms)	Atlasiet šifrēšanas algoritmu.
Password (Parole)	Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E).
Confirm Password (Apstiprināt paroli)	Lai apstiprinātu, ievadiet konfigurēto paroli.
Context Name (Konteksta nosaukums)	Ievadiet no 1 līdz 32 vienbaita rakstzīmēm.

Saistītā informācija

➡ "SNMPv3 konfigurēšana" 48. lpp.

Problēmu risinājumi

Servera un tīkla ierīces žurnāla pārbaude

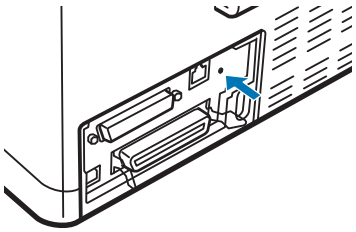
Ja radušās tīkla savienojuma problēmas, varat identificēto to cēloni, pārbaudot pasta servera vai LDAP servera žurnālu, vai statusu, izmantojot tīkla ierīces, piemēram, maršrutētāja, sistēmas žurnālu vai komandas.

Tīkla statusa lapas drukāšana

Varat izdrukāt un pārbaudīt detalizētu tīkla informāciju.

1. Ievietojiet papīru.
2. Aptuveni trīs sekundes turiet nospiestu statusa lapas pogu.

   Tiek izdrukātas tīkla statusa lapas.



Tīkla iestatījumu inicializēšana

Tīkla iestatījumu atjaunošana, izmantojot printeri

Tīkla iestatījumiem var atjaunot noklusējuma vērtības.

1. Izslēdziet printeri.
2. Ieslēdzot printeri, turiet nospiestu statusa lapas pogu.

Tīkla iestatījumu atjaunošana, izmantojot EpsonNet Config

Tīkla iestatījumiem var atjaunot noklusējuma vērtības, izmantojot EpsonNet Config.

1. Startējiet EpsonNet Config.

2 Atlasiet printeri, kuram vēlaties atjaunot tīkla iestatījumus.

3 Noklikšķiniet ar peles labo pogu uz printera nosaukuma un pēc tam atlasiet **Default Settings (Noklusējuma iestatījumi)** > **Network Interface (Tīkla saskarne)**.

4 Apstiprinājuma ekrānā noklikšķiniet uz **OK (Labi)**.

5 Noklikšķiniet uz **OK (Labi)**.

Ierīču un datoru savstarpējo sakaru pārbaude

Savienojuma pārbaude, izmantojot ehotestēšanas komandu

Lai pārbaudītu, vai datoram ir savienojums ar printeri, var izmantot ehotestēšanas komandu. Veiciet turpmāk aprakstīto procedūru, lai pārbaudītu savienojumu, izmantojot ehotestēšanas komandu.

1 Savienojumam, kuru vēlaties pārbaudīt, pārbaudiet printera IP adresi.

To var pārbaudīt tīkla statusa lapas kolonnā **IP Address (IP adrese)**.

2 Atveriet datora komandu uzvednes ekrānu.

- ❏ Operētājsistēma Windows 10
  Noklikšķiniet ar peles labo pogu uz pogas Start (Sākt) vai nospiediet un turiet to, pēc tam atlasiet **Command Prompt (Komandu uzvedne)**.
- ❏ Operētājsistēma Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
  Atveriet lietojumprogrammas ekrānu, pēc tam izvēlieties **Command Prompt (Komandu uzvedne)**.
- ❏ Operētājsistēma Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 vai vecākas versijas
  Noklikšķiniet uz pogas Start (Sākt), atlasiet **All Programs (Visas programmas)** vai **Programs (Programmas)** > **Accessories (Piederumi)** > **Command Prompt (Komandu uzvedne)**.

3 Ievadiet komandrindā tālāk norādīto un pēc tam nospiediet Enter (Ievadīt).

ehotestēšana 192.0.2.111 (ja IP adrese datoram, kuru vēlaties pārbaudīt, ir 192.0.2.111)

4 Ja tiek parādīts tālāk norādītais, apstiprinājums ir pabeigts. Aizveriet **Command Prompt (Komandu uzvedne)**.

192.0.2.111 ehotestēšanas statistika:
Paketes: nosūtīts = 4, saņemts = 4, zaudēts = 0 (0% zudums),
Cikla laiks: (ms):
minimums = 0 ms, maksimums = 0 ms, vidēji = 0 ms

Tīkla programmatūras lietošanas problēmas

Nevar piekļūt Web Config

Vai printera IP adrese ir pareizi konfigurēta?

Konfigurējiet IP adresi, izmantojot EpsonNet Config vai printera vadības paneli. Pašreizējo iestatījumu informāciju var pārbaudīt tīkla statusa lapā vai printera vadības panelī.

Vai jūsu pārlūkprogramma atbalsta liela datu apjoma šifrēšanu Encryption Strength, izmantojot SSL/TLS protokolu?

Liela datu apjoma šifrēšanas Encryption Strength iespējas SSL/TLS protokolam norādītas tālāk. Web Config var piekļūt tikai tādā pārlūkprogrammā, kas atbalsta tālāk norādītās liela datu apjoma šifrēšanas iespējas. Pārbaudiet, vai pārlūkprogramma atbalsta šifrēšanu.

- ❏ 80 bitu: AES256/AES128/3DES
- ❏ 112 bitu: AES256/AES128/3DES
- ❏ 128 bitu: AES256/AES128
- ❏ 192 bitu: AES256
- ❏ 256 bitu: AES256

Piekļūstot lietojumprogrammai Web Config ar SSL sakariem (https), tiek parādīts paziņojums „Beidzies derīguma termiņš”.

Ja beidzies sertifikāta derīguma termiņš, iegūstiet sertifikātu vēlreiz. Ja ziņojums tiek parādīts, bet tā derīguma termiņš vēl nav beidzies, pārliecinieties, vai ir pareizi konfigurēts printera datums.

Piekļūstot lietojumprogrammai Web Config ar SSL sakariem (https), tiek parādīts paziņojums „Neatbilstošs drošības sertifikāta nosaukums···”.

Printera IP adrese, kas ievadīta laukā Common Name (Kopējais nosaukums), izveidojot pašparakstītu sertifikātu vai CSR, neatbilst pārlūkprogrammā ievadītajai adresei. Iegūstiet un importējiet sertifikātu vēlreiz vai mainiet printera nosaukumu.

Piekļuve printerim notiek, izmantojot starpniekserveri.

Ja darbā ar printeri izmanto starpniekserveri, ir jākonfigurē pārlūkprogrammas starpniekservera iestatījumi.

Atlasiet **Control Panel (Vadības panelis)** > **Network and Internet (Tīkls un internets)** > **Internet Options (Interneta opcijas)** > **Connections (Savienojumi)** > **LAN settings (LAN iestatījumi)** > **Proxy server (Starpniekserveris)** un pēc tam konfigurējiet, lai vietējās adreses neizmantotu starpniekserveri.

Piemērs:
192.168.1.*: lokālā adrese 192.168.1.XXX, apakštīkla maska 255.255.255.0
192.168.*.*: lokālā adrese 192.168.XXX.XXX, apakštīkla maska 255.255.0.0

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.
➡ "IP adreses piešķiršana, izmantojot EpsonNet Config" 14. lpp.

Netiek parādīts modeļa nosaukums un/vai IP adrese lietotnē EpsonNet Config

Vai tad, kad tika parādīts Windows drošības vai ugunsmūra ekrāns, tika atlasīta iespēja Block (Bloķēt), Cancel (Atcelt) vai Shut down (Izslēgt)?

Ja atlasīta iespēja **Block (Bloķēt)**, **Cancel (Atcelt)** vai **Shut down (Izslēgt)**, IP adrese un modeļa nosaukums lietotnē EpsonNet Config vai EpsonNet Setup netiks parādīts.

Lai to novērstu, reģistrējiet EpsonNet Config izņēmumu sarakstā, izmantojot Windows ugunsmūri un tirdzniecībā pieejamo drošības programmatūru. Ja izmanto pretvīrusu vai drošības programmu, aizveriet to un pēc tam mēģiniet lietot EpsonNet Config.

Vai sakaru kļūdas taimauta iestatījums nav pārāk īss?

Palaidiet EpsonNet Config un atlasiet **Tools (Rīki)** > **Options (Opcijas)** > **Timeout (Taimauts)**, un pēc tam pagariniet laika posmu opcijas **Communication Error (Sakaru kļūda)** iestatījumā. Ievērojiet, ka rīkojoties šādi, EpsonNet Config darbība var palēnināties.

Drošības papildu iestatījumu problēmu risināšana

Drošības iestatījumu atjaunošana

Izveidojot augstas drošības vidi, piemēram, izmantojot IPsec/IP Filtering (IPsec/IP filtrēšana), pastāv iespēja, ka nevarēs sazināties ar ierīcēm nepareizu iestatījumu vai ierīces vai servera darbības traucējumu dēļ. Šādā gadījumā atjaunojiet drošības iestatījumus, lai vēlreiz iestatītu ierīci vai nodrošinātu īslaicīgu lietošanu.

Drošības funkcijas atspējošana, izmantojot printeri

Izmantojot printeri, var atspējot IPsec/IP Filtering (IPsec/IP filtrēšana).

1. Pārliecinieties, ka ir ievietots papīrs.
2. Nospiediet pogas **Menu** (**Pitch** un **Tear Off/Bin**), līdz printeris vienreiz signalizē un ieslēdzas **Menu** indikatori (abi **Tear Off/Bin** indikatori).

   Printeris ieslēdzas noklusējuma iestatījumu režīmā un izdrukā ziņojumu ar aicinājumu atlasīt valodu noklusējuma iestatījumu izvēlnei. Valoda, kura ir pasvītrota, norāda pašreizējo iestatījumu.
3. Ja vēlamā valoda nav atlasīta, nospiediet pogu **Item⬇** (Font), līdz izdrukā norādīta vēlamā valoda.
4. Nospiediet pogu **Set** (**Tear Off/Bin**), lai atlasītu vēlamo valodu.

5 Ja vēlaties drukāt pašreizējos iestatījumus, nospiediet pogu **Set**. Ja vēlaties apiet pašreizējo iestatījumu drukāšanu, nospiediet pogu **Item⬇** vai pogu **Item⬆**.

Printeris drukā pirmo izvēlni un izvēlnes pašreizējo vērtību.

6 Nospiediet pogu **Item⬇** vai pogu **Item⬆**, lai atlasītu izvēlnes parametrus no **IPsec/IP Filtering**. Nospiediet pogu **Set**, lai ritinātu starp atlasītā parametra vērtībām, līdz ir atrodama izvēle **Off**.

7 Pēc iestatījumu norādīšanas nospiediet pogas **Menu** (**Pitch** un **Tear Off/Bin**).

Menu indikatori (abi **Tear Off/Bin** indikatori) izslēdzas un printeris iziet no noklusējuma iestatījumu režīma. Veiktie iestatījumi ir saglabāti kā jauna vērtība.

Piezīme.
Ja izslēdzat printeri pirms iziešanas no noklusējuma iestatījumu režīma, visas veiktās izmaiņas tiek atceltas un netiek saglabātas.

Drošības funkcijas atjaunošana, izmantojot Web Config

Funkciju var atspējot, ja var piekļūt ierīcei no datora.

IPsec/IP Filtering (IPsec/IP filtrēšanas) atspējošana, izmantojot Web Config

1 Atveriet programmu Web Config un atlasiet **Network Security Settings (Tīkla drošības iestatījumi)** > **IPsec/IP Filtering (IPsec/IP filtrēšana)** > **Basic (Pamata)**.

2 Atlasiet **Disable (Atspējot)** kā **IPsec/IP Filtering (IPsec/IP filtrēšana)** iestatījumu sadaļā **Default Policy (Noklusējuma politika)**.

3 Noklikšķiniet uz **Next (Tālāk)** un notīriet opciju **Enable this Group Policy (Iespējot šīs grupas politiku)** visām grupu politikām.

4 Noklikšķiniet uz **OK (Labi)**.

Saistītā informācija
➡ "Piekļuve Web Config" 20. lpp.

Tīkla drošības funkciju lietošanas problēmas

Aizmirsta iepriekš koplietota atslēga

Vēlreiz konfigurējiet atslēgu, izmantojot Web Config.

Lai mainītu atslēgu, atveriet programmu Web Config un atlasiet **Network Security Settings (Tīkla drošības iestatījumi)** > **IPsec/IP Filtering (IPsec/IP filtrēšana)** > **Basic (Pamata)** > **Default Policy (Noklusējuma politika)** vai **Group Policy (Grupas politika)**.

Saistītā informācija
➡ "Piekļuve Web Config" 20. lpp.

Nevar izveidot sakarus, izmantojot IPsec

Vai datora iestatījumos netiek izmantots neatbalstīts algoritms?

Printeris atbalsta turpmāk norādītos algoritmus.

Drošības metodes	Algoritmi
Šifrēšanas algoritms	AES-CBC 128,AES-CBC 192,AES-CBC 256,3DES-CBC,DES-CBC
Jaucējkoda algoritms	SHA-1,SHA2-256,SHA2-384,SHA2-512,MD5
Atslēgu apmaiņas algoritms	Diffi e-Hellman Group2,Diffi e-Hellman Group1*,Diffi e-Hellman Group14* Elliptic Curve Diffi e- Hellman P-256*,Elliptic Curve Diffi e-Hellman P-384*

* Pieejamās metodes dažādiem modeļiem atšķiras.

Saistītā informācija

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 40. lpp.

Pēkšņi nevar izveidot sakarus

Vai printera IP adrese ir nederīga vai mainīta?

Atspējojiet IPsec, izmantojot printera vadības paneli.

Ja nav atjaunināts DHCP, atsāknējiet, vai ja nav atjaunināta vai iegūta IPv6 adrese, iespējams, ka programmā Web Config (**Network Security Settings (Tīkla drošības iestatījumi)** > **IPsec/IP Filtering (IPsec/IP filtrēšana)** > **Basic (Pamata)** > **Group Policy (Grupas politika)** > **Local Address(Printer) (Lokālā adrese (Printeris))**) netiks atrasta reģistrētā printera IP adrese. Izmantojiet statisku IP adresi.

Vai datora IP adrese ir nederīga vai mainīta?

Atspējojiet IPsec, izmantojot printera vadības paneli.

Ja nav atjaunināts DHCP, atsāknējiet, vai ja nav atjaunināta vai iegūta IPv6 adrese, iespējams, ka programmā Web Config (**Network Security Settings (Tīkla drošības iestatījumi)** > **IPsec/IP Filtering (IPsec/IP filtrēšana)** > **Basic (Pamata)** > **Group Policy (Grupas politika)** > **Remote Address(Host) (Attālā adrese (resursdators))**) netiks atrasta reģistrētā printera IP adrese. Izmantojiet statisku IP adresi.

Saistītā informācija

➡ "Piekļuve Web Config" 20. lpp.
➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 40. lpp.

Nevar izveidot drošu IPP drukāšanas portu

Vai SSL/TLS sakaru sadaļā ir norādīts pareizs servera sertifikāts?

Ja norādītais sertifikāts ir nepareizs, porta izveide var neizdoties. Pārliecinieties, var izmantojat pareizu sertifikātu.

Vai datorā, kurš piekļūst printerim, ir importēts CA sertifikāts?

Ja datorā nav importēts CA sertifikāts, porta izveide var neizdoties. Pārliecinieties, vai ir importēts CA sertifikāts.

Saistītā informācija
➡ "Piekļuve Web Config" 20. lpp.

Nevar izveidot savienojumu pēc IPsec/IP filtrēšanas konfigurācijas

Iespējams, nav pareiza iestatītā vērtība.

Atspējojiet IPsec/IP filtrēšanu, izmantojot printera vadības paneli. Savienojiet printeri ar datoru un vēlreiz veiciet IPsec/IP filtrēšanas iestatījumus.

Saistītā informācija
➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 40. lpp.

Ciparsertifikāta lietošanas problēmas

Nevar importēt CA parakstītu sertifikātu

Vai CA parakstītais sertifikāts atbilst CSR informācijai?

Ja informācija CA parakstītajā sertifikātā un CSR atšķiras, CSR nevar importēt. Pārbaudiet turpmāk norādīto:

❏ Vai mēģināt importēt sertifikātu ierīcē, kurā nav tāda pati informācija?

Pārbaudiet CSR informāciju un pēc tam importējiet sertifikātu ierīcē, kurā ir tāda pati informācija.

❏ Vai pēc CSR nosūtīšanas sertificēšanas iestādei printerī saglabātais CSR tika pārrakstīts?

Vēlreiz iegūstiet CA parakstītu sertifikātu, izmantojot CSR.

Vai CA parakstītā sertifikāta lielums pārsniedz 5 KB?

Nevar importēt CA parakstītu sertifikātu, kura lielums pārsniedz 5 KB.

Vai sertifikāta importēšanas parole ir pareiza?

Ja parole aizmirsta, sertifikātu nevar importēt.

Saistītā informācija
➡ "CA parakstīta sertifikāta importēšana" 37. lpp.

Nevar atjaunināt pašparakstītu sertifikātu

Vai ir ievadīta vērtība laukā Common Name (Kopējais nosaukums)?

Jābūt ievadītai vērtībai laukā **Common Name (Kopējais nosaukums)**.

Vai laukā Common Name (Kopējais nosaukums) nav izmantotas neatbalstītas rakstzīmes? Netiek atbalstīta, piemēram, japāņu valoda.

Ievadiet 1–128 rakstzīmes IPv4 IPv6 resursdatora nosaukuma vai FQDN formātā ASCII kodējumā (0x20-0x7E).

Vai laukā Common Name (Kopējais nosaukums) ir izmantots komats vai atstarpe?

Ja ievadīts komats, lauka **Common Name (Kopējais nosaukums)** vērtība šajā punktā tiek sadalīta. Ja pirms vai pēc komata ievadīta atstarpe, notiek kļūda.

Saistītā informācija

➡ "Pašparakstīta sertifikāta atjaunināšana" 39. lpp.

Nevar izveidot CSR

Vai ir ievadīta vērtība laukā Common Name (Kopējais nosaukums)?

Jābūt ievadītai vērtībai laukā **Common Name (Kopējais nosaukums)**.

Vai laukā Common Name (Kopējais nosaukums), Organization (Organizācija), Organizational Unit (Organizācijas vienība), Locality (Vieta),State/Province (Novads/pagasts) nav izmantotas neatbalstītas rakstzīmes? Netiek atbalstīta, piemēram, japāņu valoda.

Ievadiet rakstzīmes IPv4, IPv6 resursdatora nosaukuma vai FQDN formātā, ASCII kodējumā (0x20-0x7E).

Vai laukā Common Name (Kopējais nosaukums) ir izmantots komats vai atstarpe?

Ja ievadīts komats, lauka **Common Name (Kopējais nosaukums)** vērtība šajā punktā tiek sadalīta. Ja pirms vai pēc komata ievadīta atstarpe, notiek kļūda.

Saistītā informācija

➡ "CA parakstīta sertifikāta iegūšana" 35. lpp.

Tiek parādīts ar ciparsertifikāta lietošanu saistīts brīdinājums

Ziņojumi	Cēlonis/risinājums
Enter a Server Certificate. (Ievadiet servera sertifikātu.)	**Cēlonis:** Nav atlasīts importējamais fails. **Risinājums:** Atlasiet failu un noklikšķiniet uz Import (Importēt).
CA Certificate 1 is not entered. (1. CA sertifikāts nav ievadīts.)	**Cēlonis:** Nav ievadīts 1. CA sertifikāts; ievadīts tikai 2. CA sertifikāts. **Risinājums:** Vispirms importējiet 1. CA sertifikātu.
Invalid value below (Zemāk ir nederīga vērtība).	**Cēlonis:** Faila ceļā un/vai parolē ietvertas neatbalstītas rakstzīmes. **Risinājums:** Pārliecinieties, vai vienuma rakstzīmes ir ievadītas pareizi.
Invalid date and time (Nederīgs datums un laiks).	**Cēlonis:** Nav iestatīts printera datums un laiks. **Risinājums:** Iestatiet datumu un laiku, izmantojot Web Config vai Epson Device Admin.

Problēmu risinājumi

Ziņojumi	Cēlonis/risinājums
Invalid password (Nederīga parole).	**Cēlonis:** Iestatītā CA sertifikāta parole nesakrīt ar ievadīto paroli. **Risinājums:** Ievadiet pareizu paroli.
Invalid file (Nederīgs fails).	**Cēlonis:** Netiek importēts X509 formāta sertifikāta fails. **Risinājums:** Papildinformāciju par sertifikātu skatiet sertificēšanas iestādes tīmekļa vietnē.
	Cēlonis: Importētais fails ir pārāk liels. Maksimālais lielums ir 5 KB. **Risinājums:** Ja atlasīts pareizais fails, iespējams, sertifikāts ir bojāts vai safabricēts.
	Cēlonis: Nederīga sertifikātā iekļautā ķēde. **Risinājums:** Papildinformāciju par sertifikātu skatiet sertificēšanas iestādes tīmekļa vietnē.
Cannot use the Server Certificates that include more than three CA certificates. (Nevar izmantot servera sertifikātus, kuros ietverti vairāk nekā trīs CA sertifikāti.)	**Cēlonis:** PKCS#12 formāta sertifikāta failā ietverti vairāk nekā 3 CA sertifikāti. **Risinājums:** Importējiet katru sertifikātu, konvertējot no PKCS#12 formāta PEM formātā, vai importējiet PKCS#12 formāta sertifikāta failu, kurā ietverti ne vairāk kā 2 CA sertifikāti.
The certificate has expired. Check if the certificate is valid, or check the date and time on your printer. (Beidzies sertifikāta derīgums. Pārbaudiet sertifikāta derīgumu vai pārbaudiet datumu un laiku uz printera.)	**Cēlonis:** Beidzies sertifikāta derīguma termiņš. **Risinājums:** ❏ Ja beidzies sertifikāta derīguma termiņš, iegūstiet un importējiet jaunu sertifikātu. ❏ Ja sertifikāta derīguma termiņš nav beidzies, pārliecinieties, vai printera datums un laiks ir iestatīts pareizi.
Private key is required. (Nepieciešama privātā atslēga.)	**Cēlonis:** Nav ar sertifikātu pārī savienotas privātas atslēgas. **Risinājums:** ❏ Ja sertifikāts ir PEM/DER formātā un ir iegūts no CSR, izmantojot datoru, norādiet privāto atslēgas failu. ❏ Ja sertifikāts ir PKCS#12 formātā un ir iegūts no CSR, izmantojot datoru, izveidojiet failu, kas satur privāto atslēgu.
	Cēlonis: Izmantojot Web Config, no CSR iegūts PEM/DER sertifikāts ir importēts atkārtoti. **Risinājums:** Ja sertifikāts ir PEM/DER formātā un ir iegūts no CSR, izmantojot Web Config, to var importēt tikai vienu reizi.

Ziņojumi	Cēlonis/risinājums
Setup failed. (Iestatīšana neizdevās.)	**Cēlonis:** Nevar pabeigt konfigurēšanu, jo nav izveidoti printera un datora sakari, vai failu nevar nolasīt kļūdu dēļ. **Risinājums:** Pēc norādītā faila un sakaru pārbaudes importējiet failu vēlreiz.

Saistītā informācija

➡ "Par ciparsertifikātiem" 35. lpp.

CA parakstīta sertifikāta nejauša dzēšana

Vai ir pieejams sertifikāta dublējuma fails?

Ja ir pieejams dublējuma fails, importējiet sertifikātu vēlreiz.

Ja sertifikāts ir iegūts, izmantojot programmā Web Config izveidotu CSR, dzēstu sertifikātu nevar importēt vēlreiz. Izveidojiet CSR un iegūstiet jaunu sertifikātu.

Saistītā informācija

➡ "CA parakstīta sertifikāta dzēšana" 38. lpp.
➡ "CA parakstīta sertifikāta importēšana" 37. lpp.

Pielikums

Tīkla programmatūras apraksts

Turpmāk ir aprakstīta programmatūra, ko izmanto ierīču konfigurēšanai un pārvaldībai.

Epson Device Admin

Epson Device Admin ir lietojumprogramma, ko izmanto, lai tīklā instalētu ierīces un pēc tam tās konfigurētu un pārvaldītu. Varat iegūt detalizētu informāciju par ierīcēm, piemēram, par statusu un patērējamajiem materiāliem, sūtīt brīdinājumu paziņojumus un izveidot ierīces lietošanas pārskatus. Pastāv arī iespēja sagatavot veidni ar iestatījumu vienumiem un izmantot to citām ierīcēm kā koplietojamus iestatījumus. Epson Device Admin pieejams lejupielādei Epson atbalsta tīmekļa vietnē. Papildinformāciju skatiet Epson Device Admin dokumentācijā vai palīdzībā.

Programmas Epson Device Admin palaišana (tikai operētājsistēmā Windows)

Atlasiet **All Programs (Visas programmas)** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Piezīme.
Ja tiek parādīts ugunsmūra brīdinājums, atļaujiet Epson Device Admin piekļuvi.

EpsonNet Print

EpsonNet Print ir programmatūra, kas paredzēta drukāšanai TCP/IP tīklā. Turpmāk sniegta informācija par funkcijām un ierobežojumiem.

- ❏ Printera statuss tiek parādīts spolētāja ekrānā
- ❏ Ja DHCP serveris maina printera IP adresi, printeri joprojām var atrast.
- ❏ Var izmantot printeri, kas atrodas citā tīkla segmentā.
- ❏ Drukāšanai var izmantot vienu no vairākiem protokoliem.
- ❏ IPv6 adrešu izmantošana netiek atbalstīta.

EpsonNet SetupManager

EpsonNet SetupManager ir programmatūra, kuru izmantojot, var izveidot pakotni printera instalēšanas vienkāršošanai, piemēram, printera draivera instalēšanai, EPSON Status Monitor instalēšanai un printera porta izveidei. Izmantojot šo programmatūru, administrators var izveidot unikālas programmatūras pakotnes un izplatīt tās grupās.

Papildinformāciju skatiet reģionālajā Epson tīmekļa vietnē.