EPSON
EXCEED YOUR VISION

Administratora rokasgrāmata

NPD5668-00 LV

Satura rādītājs

Pielikums

Papildu drošības iestatījumi uzņēmumiem

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 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.
- ❏ 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

Zīmes un simboli

> ***Brīdinājums:***
> *Norādījumi, kas rūpīgi jāievēro, lai nepieļautu traumas.*

> ***Svarīga informācija:***
> *Norādījumi, kas jāievēro, lai nepieļautu aprīkojuma bojājumus.*

Piezīme:
Norādījumi, kuros ietverti noderīgi padomi un skenera darbības ierobežojumi.

Saistītā informācija

➡ Noklikšķinot uz šīs ikonas, tiks parādīta saistītā informācija.

Šajā rokasgrāmatā izmantotie apraksti

❏ Skenera draivera ekrānuzņēmumi un Epson Scan 2 (skenera draiveris) ekrāni ir no operētājsistēmas Windows 10 vai OS X El Capitan. Ekrānos redzamais saturs var atšķirties atkarībā no modeļa un situācijas.

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

❏ Daži no izvēlnes vienumiem LCD ekrānā ir atkarīgi no modeļa un iestatījumiem.

Operētājsistēmu atsauces

Windows

Šajā rokasgrāmatā ar terminiem „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” un „Windows Server 2003” ir apzīmētas attiecīgās operētājsistēmas. Turklāt termins „Windows” tiek lietots kā atsauce uz visām šīs operētājsistēmas versijām.

❏ Operētājsistēma Microsoft® Windows® 10

❏ Operētājsistēma Microsoft® Windows® 8.1

❏ Operētājsistēma Microsoft® Windows® 8

❏ Operētājsistēma Microsoft® Windows® 7

❏ Operētājsistēma Microsoft® Windows Vista®

❏ Operētājsistēma Microsoft® Windows® XP

❏ Operētājsistēma Microsoft® Windows® XP Professional x64 Edition

Par šo rokasgrāmatu

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

Mac OS

Šajā rokasgrāmatā termins „Mac OS" tiek lietots kā atsauce uz macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x un Mac OS X v10.6.8.

Ievads

Rokasgrāmatas daļas

Šī rokasgrāmata ir paredzēta ierīces administratoram, kurš atbild par printera vai skenera pievienošanu tīklam, un tā satur informāciju par to, kā izvēlēties funkciju iestatījumus.

Informāciju par funkciju lietošanu skatiet *Lietotāja rokasgrāmata*.

Sagatavošana

Aprakstīti administratora darba uzdevumi, ierīču iestatīšana un pārvaldības programmatūra.

Savienojums

Paskaidro, kā pievienot ierīci tīklam vai tālruņa līnijai. Satur arī tīkla vides skaidrojumus, piemēram, porta izmantošanu ierīcei, informāciju par DNS un starpniekserveri.

Funkciju iestatījumi

Apraksta katras ierīces darbības iestatījumus.

Pamata drošības iestatījumi

Paskaidro funkcijām, piemēram, drukāšanai, skenēšanai un faksu pārraidei, pieejamos iestatījumus.

Lietošanas un pārvaldības iestatījumi

Paskaidro darbības, ko veic, sākot lietot ierīces, piemēram, informācijas pārbaudi un apkopi.

Problēmu risinājumi

Paskaidro iestatījumu inicializāciju un tīkla darbības problēmu risināšanu.

Papildu drošības iestatījumi uzņēmumiem

Izskaidro iestatīšanas paņēmienu, ko var izmantot, lai uzlabotu ierīces drošību, piemēram, CA sertifikātu, SSL/TLS sakaru un IPsec/IP filtrēšanas izmantošanu.

Atsevišķos modeļos dažas šajā nodaļā aprakstītās funkcijas netiek atbalstītas.

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 maršrutētāju, starpniekserveri, DNS serveri un pasta serveri, kontrolējot interneta vai lokālā tīkla sakarus.

Lietotājs

Persona, kas lieto ierīces, piemēram, printerus vai skenerus.

Web Config (ierīces tīmekļa lapa)

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

Rīks

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

Pašpiegādes skenēšana

Vispārējs termins, ar kuru apzīmē skenēšanu, izmantojot ierīces vadības paneli.

ASCII (Amerikas informācijas apmaiņas standartkods)

Viens no rakstzīmju standartkodiem. Iekļautas 128 rakstzīmes, tostarp alfabēta burti (a–z, A–Z), arābu cipari (0–9), simboli, tukšumzīmes un kontroles rakstzīmes. Šajā pamācībā ar „ASCII" ir domāts zemāk norādītais skaitlis 0x20–0x7E (heksadecimāls), kas 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	{	|	}	~	

* Atstarpes rakstzīme.

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 paskaidrota administratora loma un sagatavošanās darbības pirms iestatījumu izvēles.

Skenera iestatījumu un pārvaldības plūsma

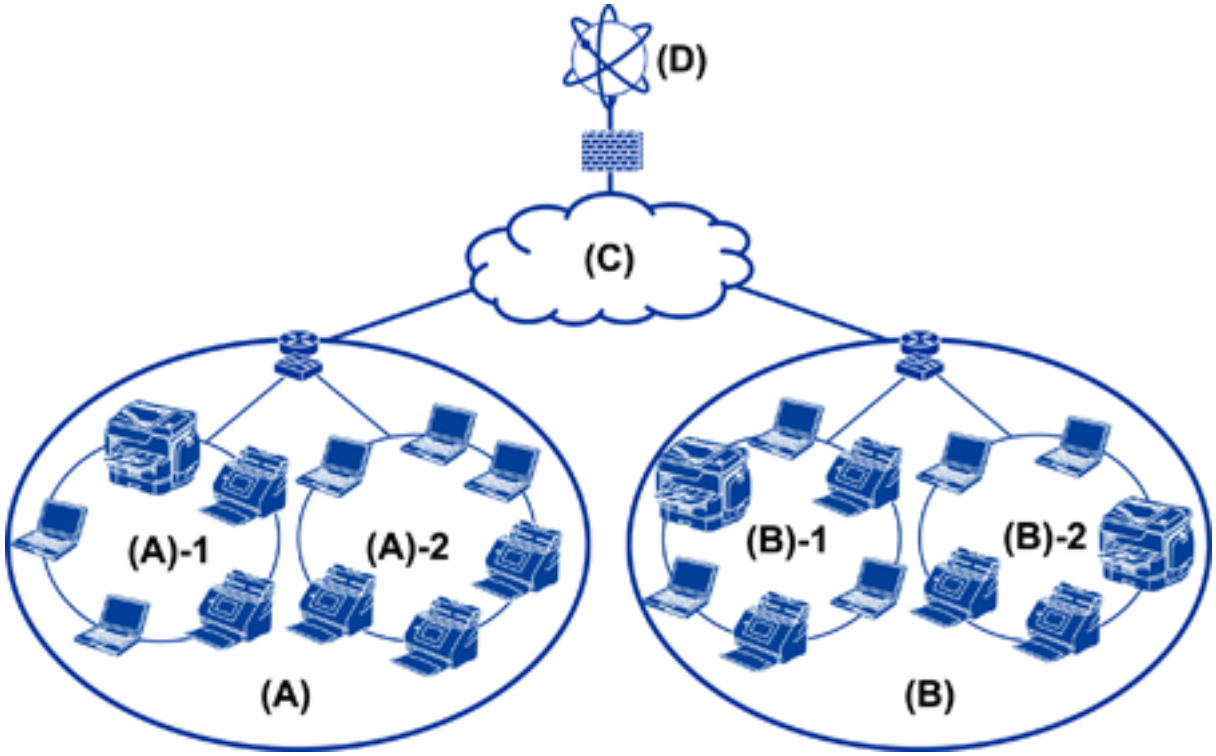
Administrators veic skenera vai skenera tīkla savienojuma iestatīšanu, sākotnējo iestatīšanu un apkopi, lai skeneris būtu pieejams lietotājiem.

1. Sagatavošana
   - ❏ Savienojuma iestatījumu informācijas apkopošana
   - ❏ Lēmums par savienojuma metodi
2. Savienojuma izveide
   - ❏ Tīkla savienojums, izmantojot skenera vadības paneli
3. Funkciju iestatīšana
   - ❏ Skenera draivera iestatījumi
   - ❏ Citi papildiestatījumi
4. Drošības iestatījumi
   - ❏ Administratora iestatījumi
   - ❏ SSL/TLS
   - ❏ Protokolu vadība
   - ❏ Papildu drošības iestatījumi (pēc izvēles)
5. Lietošana un pārvaldība
   - ❏ Ierīces statusa pārbaude
   - ❏ Rīcība ārkārtas situācijās
   - ❏ Ierīces iestatījumu dublēšana

Saistītā informācija

➡ "Sagatavošana" 10. lpp.
➡ "Savienojums" 15. lpp.
➡ "Funkciju iestatījumi" 22. lpp.
➡ "Pamata drošības iestatījumi" 32. lpp.
➡ "Lietošanas un pārvaldības iestatījumi" 40. lpp.

Tīkla vides piemērs



(A): 1. birojs

❏ (A) – 1: 1. lokālais tīkls

❏ (A) – 2: 2. lokālais tīkls

(B): 2. birojs

❏ (B) – 1: 1. lokālais tīkls

❏ (B) – 2: 2. lokālais tīkls

(C): teritoriālais tīkls

(D): internets

SkeneSSkenera savienojuma iestatījuma piemērs

Pastāv divas pamata savienojuma iespējas atkarībā no skenera lietošanas veida. Ar tām abām skeneri pieslēdz tīklam ar datoru, izmantojot centrmezglu.

❏ Servera/klienta savienojums (skeneris izmanto Windows serveri, darbu pārvaldība)

❏ Vienādranga savienojums (tiešs savienojums ar klienta datoru)

Saistītā informācija

➡ "Servera/klienta savienojums" 12. lpp.

➡ "Vienādranga savienojums" 12. lpp.

Servera/klienta savienojums

Centralizējiet skenera un darbu pārvaldību, izmantojot serverī instalētu programmu Document Capture Pro Server. Šī iespēja ir visnoderīgākā liela skaita zināma formāta dokumentu skenēšanai ar vairākiem skeneriem.

Saistītā informācija

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

Vienādranga savienojums

Izmantojiet atsevišķu skeneri ar klienta datorā instalētu skenera draiveri, piemēram, Epson Scan 2. Document Capture Pro (Document Capture) instalēšana klienta datorā ļaus veikt darbus skenera individuālā klienta datoros.

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	Vienumi	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. Konfigurēt, ja tiek piešķirta automātiski, izmantojot DHCP funkciju, un kad DNS serveri nevar piešķirt automātiski.
Starpniekservera informācija	❏ Starpniekservera nosaukums ❏ Porta numurs	Konfigurēt, interneta savienojumam izmantojot starpniekserveri, un kad tiek izmantots pakalpojums Epson Connect vai aparātprogrammatūras automātiskās atjaunināšanas funkcija.

Skenera specifikācija

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

Porta numuru izmantošana

Informāciju par skenera izmantoto portu numuriem skatiet „Pielikumā”.

Saistītā informācija

➡ "Porta izmantošana skenerim" 60. lpp.

IP adreses piešķiršanas veids

IP adresi skenerim var piešķirt divos veidos.

Statiska IP adrese:

Piešķiriet skenerim iepriekš noteiktu, unikālu IP adresi.

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

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

Automātiska piešķiršana, izmantojot DHCP funkciju:

Pareizā IP adrese tiek piešķirta automātiski pēc tam, kad tiek izveidoti sakari starp skeneri 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.

DNS serveris un starpniekserveris

Ja izmantojat interneta savienojuma pakalpojumu, konfigurējiet DNS serveri. Ja to nekonfigurēsiet, piekļuvei būs jānorāda IP adrese, jo var neizdoties nosaukumu atpazīšana.

Starpniekserveris atrodas vārtejā starp tīklu un internetu, un tas sazinās ar datoru, skeneri un internetu (pretējo serveri) šo ierīču vietā. Pretējais serveris sazinās tikai ar starpniekserveri. Tādēļ nevar nolasīt tādu skenera informāciju kā IP adrese un porta numurs, un nepieciešama uzlabota drošība.

Izmantojot filtrēšanas funkciju, var aizliegt piekļuvi noteiktam URL, jo starpniekserveris spēj pārbaudīt sakaru saturu.

Tīkla savienojuma iestatīšanas metode

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

Izmantojot vadības paneli:

Konfigurējiet iestatījumus katrā skenerī, izmantojot tā vadības paneli. Pēc skenera savienojuma iestatījumu konfigurēšanas izveidojiet savienojumu ar tīklu.

Izmantojot instalētāju:

Ja tiek izmantots instalētājs, skenera tīkla iestatījumi un klientdators tiek iestatīti automātiski. Iestatīšanu veic, izpildot instalētāja norādes, un to var veikt arī bez padziļinātām zināšanām par tīklu.

Sagatavošana

Rīka izmantošana:

Izmantojiet rīku administratora datorā. Varat atrast un iestatīt skeneri vai izveidot SYLK failu un vienlaikus norādīt iestatījumus vairākiem skeneriem. Iestatījumus var izvēlēties daudziem skeneriem, taču lai to varētu izdarīt, tiem jābūt fiziski savienotiem, izmantojot Ethernet vadu. Tāpēc, veicot iestatīšanu, ieteicams izveidot Ethernet savienojumu.

Saistītā informācija

➡ "Savienojuma izveide ar tīklu, izmantojot vadības paneli" 15. lpp.

➡ "Savienojums ar tīklu, izmantojot instalētāju" 19. lpp.

➡ "IP adreses piešķiršana, izmantojot EpsonNet Config" 56. lpp.

Savienojums

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

Savienojums ar tīklu

Savienojuma izveide ar tīklu, izmantojot vadības paneli

Savienojiet skeneri ar tīklu, izmantojot skenera vadības paneli.

Plašāku informāciju par skenera vadības paneli skatiet *Lietotāja rokasgrāmata*.

IP adreses piešķiršana

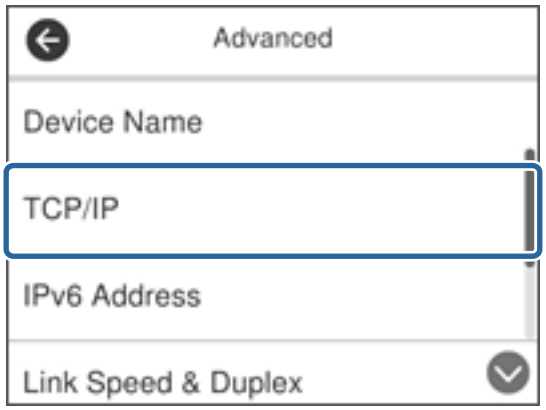
Izvēlieties pamata iestatījumus, piemēram, IP adrese, Apakštīkla maska un Noklusējuma vārteja.

1. Ieslēdziet skeneri.
2. Skenera vadības panelī pārvelciet ekrānu pa kreisi un pēc tam pieskarieties **Iestatījumi**.

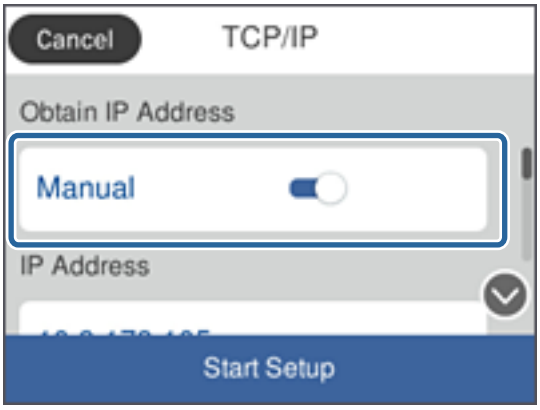
3. Pieskarieties **Tīkla iestatījumi** > **Mainīt iestatījumus**.

   Ja vienums nav redzams, pārvelciet ekrānu uz augšu, lai to parādītu.

4. Pieskarieties **TCP/IP**.

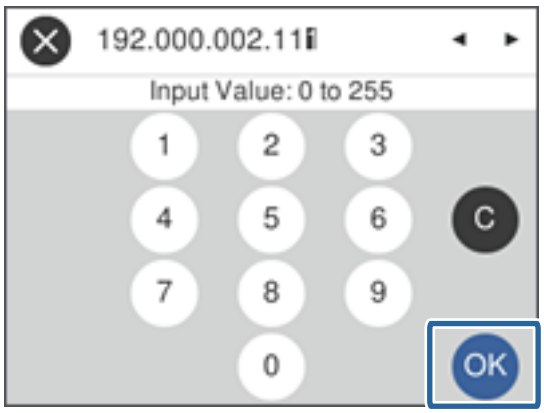


5. Iestatījumam **Iegūt IP adresi** atlasiet **Manuāli**.



Piezīme:
*Ja IP adrese iestatīta automātiski, izmantojot maršrutētāja DHCP funkciju, atlasiet **Auto**. Šādā gadījumā 6.–7. darbībā norādāmie iestatījumi **IP adrese**, **Apakštīkla maska** un **Noklusējuma vārteja** arī tiek izvēlēti automātiski, tādēļ pārejiet uz 8. darbību.*

6. Pieskarieties laukam **IP adrese**, ievadiet IP adresi, izmantojot ekrānā parādīto tastatūru, un pēc tam pieskarieties **Labi**.



Apstipriniet iepriekšējā ekrānā parādīto vērtību.

7. Iestatiet vienumu **Apakštīkla maska** un **Noklusējuma vārteja**.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

   Piezīme:
   Ja iestatījumu IP adrese, Apakštīkla maska un Noklusējuma vārteja kombinācija nav pareiza, ***Sākt iestatīšanu*** *nav aktīvs, un iestatīšanu nevar turpināt. Pārbaudiet, vai ievadītajos datos nav kļūdu.*

8. Pieskarieties laukam **Primārais DNS** sadaļā **DNS serveris**, ievadiet primārā DNS servera IP adresi, izmantojot ekrānā parādīto tastatūru, un pēc tam pieskarieties **Labi**.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

   Piezīme:
   IP adreses piešķiršanas iestatījumos atlasot vienumu ***Auto****, iespējams DNS servera iestatījumiem atlasīt režīmu* ***Manuāli*** *vai* ***Auto****. Ja DNS servera adresi nevar iegūt automātiski, atlasiet vienumu* ***Manuāli*** *un ievadiet DNS servera adresi. Pēc tam ievadiet sekundārā DNS servera adresi. Ja ir atlasīts vienums* ***Auto****, pārejiet uz 10. darbību.*

9. Pieskarieties laukam **Sekundārais DNS**, ievadiet sekundārā DNS servera IP adresi, izmantojot ekrānā parādīto tastatūru, un pēc tam pieskarieties **Labi**.

   Apstipriniet iepriekšējā ekrānā parādīto vērtību.

10. Pieskarieties **Sākt iestatīšanu**.

11. Apstiprinājuma ekrānā pieskarieties **Aizvērt**.

    Ja nepieskaras **Aizvērt**, ekrāns pēc noteikta laika automātiski tiek aizvērts.

Ethernet savienojums

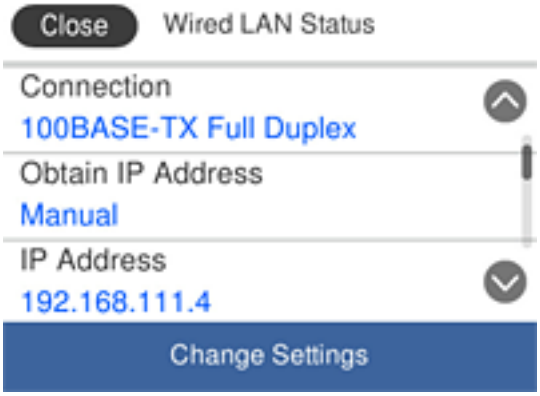
Savienojiet skeneri ar tīklu, izmantojot Ethernet vadu, un pēc tam pārbaudiet savienojumu.

1. Savienojiet skeneri ar centrmezglu (L2 komutatoru), izmantojot Ethernet vadu.

   Ikona sākuma ekrānā mainās uz  .

2. Sākuma ekrānā pieskarieties  .

3. Pavelciet ekrānu uz augšu, pārbaudiet savienojuma stāvokli un pārliecinieties, ka IP adrese ir pareiza.



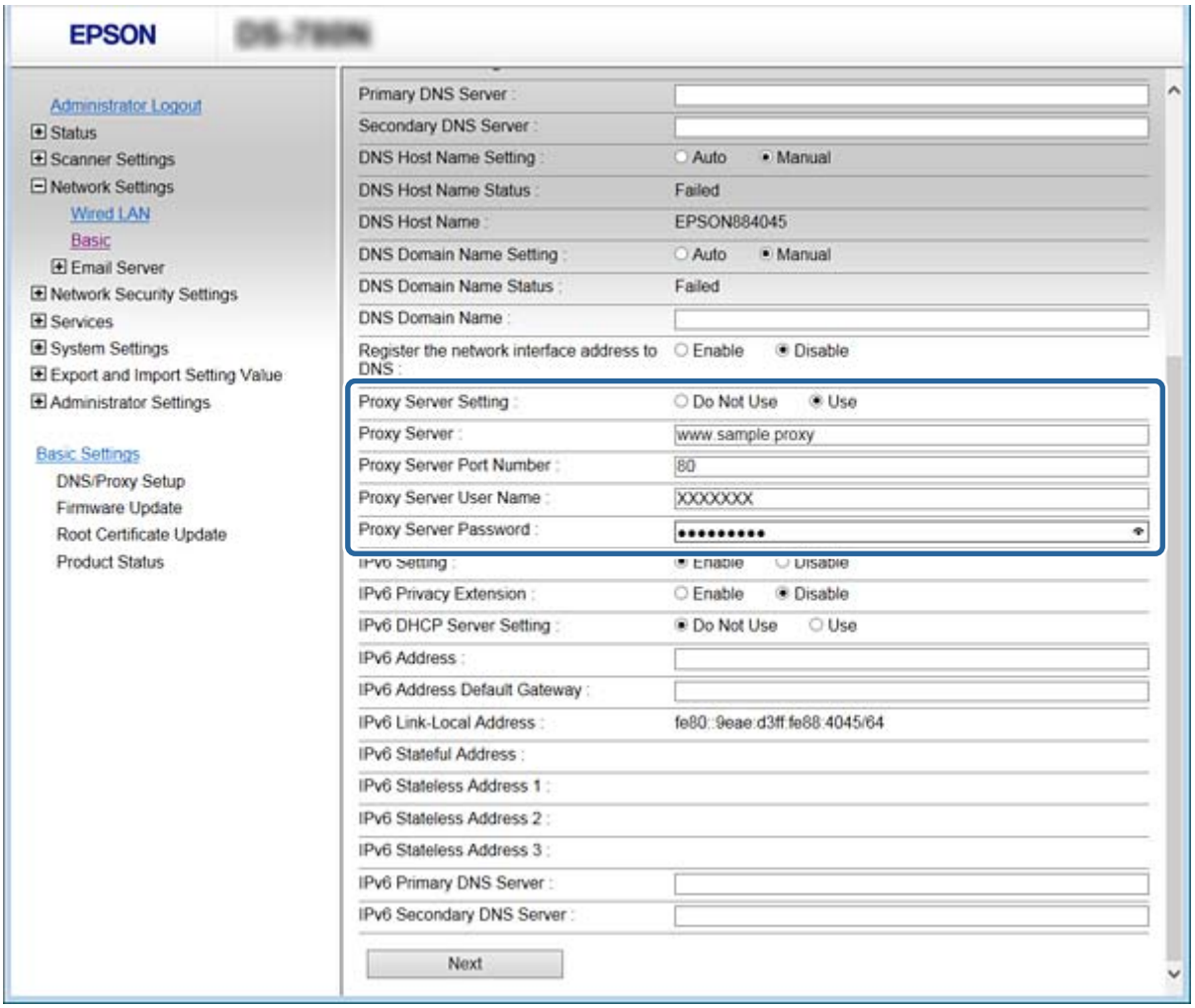
Starpniekservera iestatīšana

Starpniekserveri nevar iestatīt panelī. Konfigurējiet to, izmantojot Web Config.

1. Atveriet programmu Web Config un atlasiet **Network Settings** > **Basic**.
2. Sadaļā **Proxy Server Setting** atlasiet **Use**.
3. Sadaļā **Starpniekserveris** norādiet starpniekserveri IPv4 adreses vai FQDN formātā un tad sadaļā **Proxy Server Port Number** ievadiet porta numuru.

   Starpniekserveros, kuros nepieciešama autentifikācija, ievadiet starpniekservera autentifikācijas lietotājvārdu un starpniekservera autentifikācijas paroli.

4. Noklikšķiniet uz pogas **Next**.



5. Apstipriniet iestatījumus un tad noklikšķiniet uz **Iestatījumi**.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Savienojums ar tīklu, izmantojot instalētāju

Savienojot skeneri ar datoru, ieteicams izmantot instalētāju. Instalētāju var palaist, izmantojot kādu no turpmāk aprakstītajām metodēm.

❏ Iestatīšana, izmantojot vietni

Atveriet turpmāk norādīto vietni un pēc tam ievadiet produkta nosaukumu. Izvēlieties **Iestatīšana** un pēc tam sāciet iestatīšanu.

http://epson.sn

❏ Iestatīšana, izmantojot programmatūras disku (tikai modeļiem, kuru komplektā iekļauts programmatūras disks, un lietotājiem, kuru datori ir aprīkoti ar diskdziņiem.)

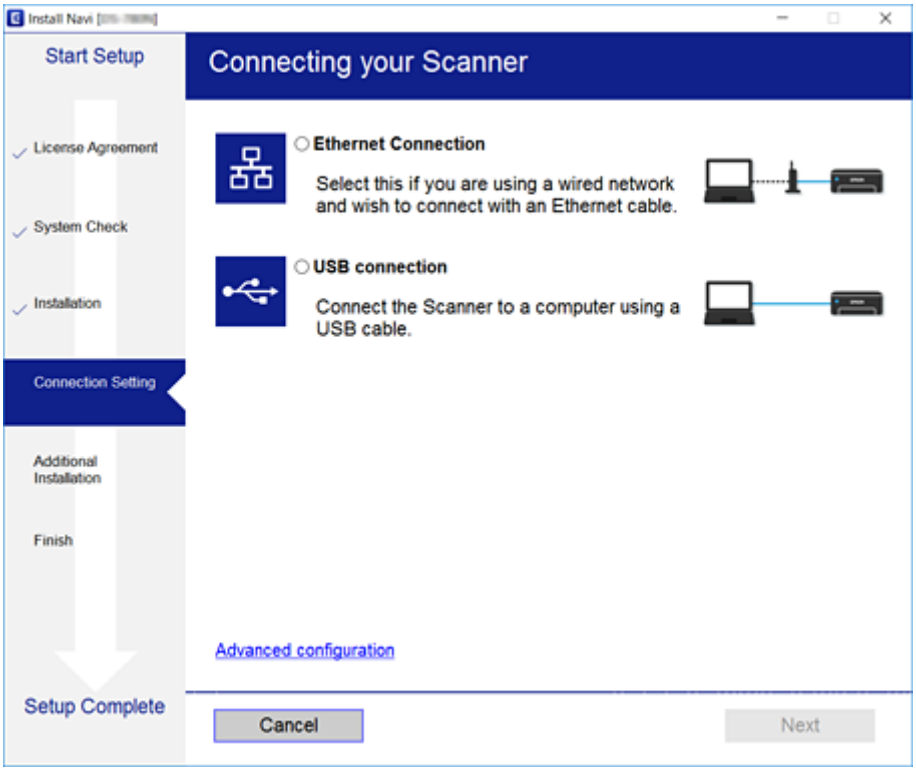
Ievietojiet programmatūras disku datorā un izpildiet ekrānā redzamos norādījumus.

Savienojuma metožu izvēle

Izpildiet ekrānā redzamos norādījumus, līdz parādās attēlā redzamais ekrāns, pēc tam atlasiet metodi, kura tiks izmantota skenera savienojumam ar datoru.

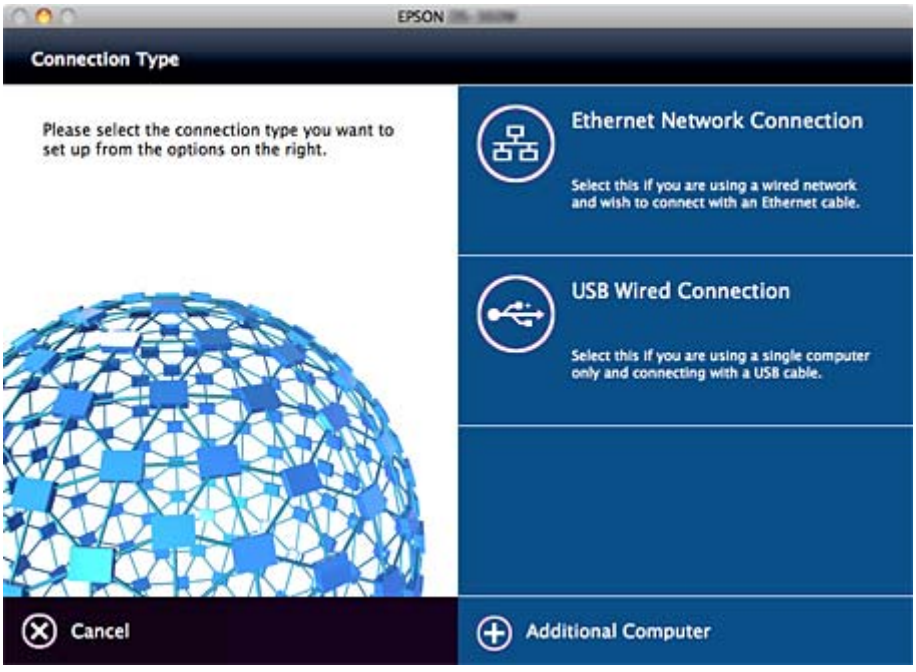
❏ Windows

Atlasiet savienojuma veidu un pēc tam noklikšķiniet uz **Tālāk**.



❏ Mac OS

Atlasiet savienojuma veidu.



Savienojums

Izpildiet ekrānā redzamās instrukcijas. Nepieciešamā programmatūra tiek instalēta.

Funkciju iestatījumi

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

Programmatūra iestatīšanai

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

Web Config (ierīces tīmekļa lapa)

Par Web Config

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

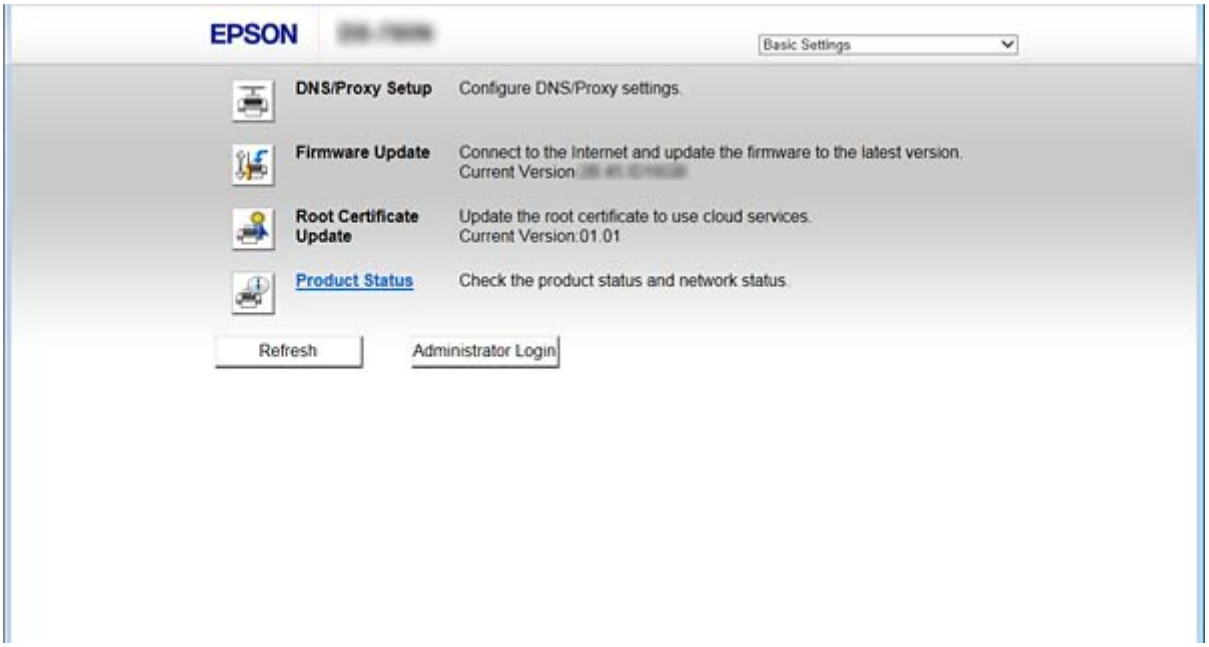
Lai piekļūtu lietojumprogrammai Web Config, skenerim ir jābūt piešķirtai IP adresei.

Piezīme:
Iestatījumus var bloķēt, konfigurējot skenera administratora paroli.

Pieejamas divas turpmāk norādītās iestatījumu lapas.

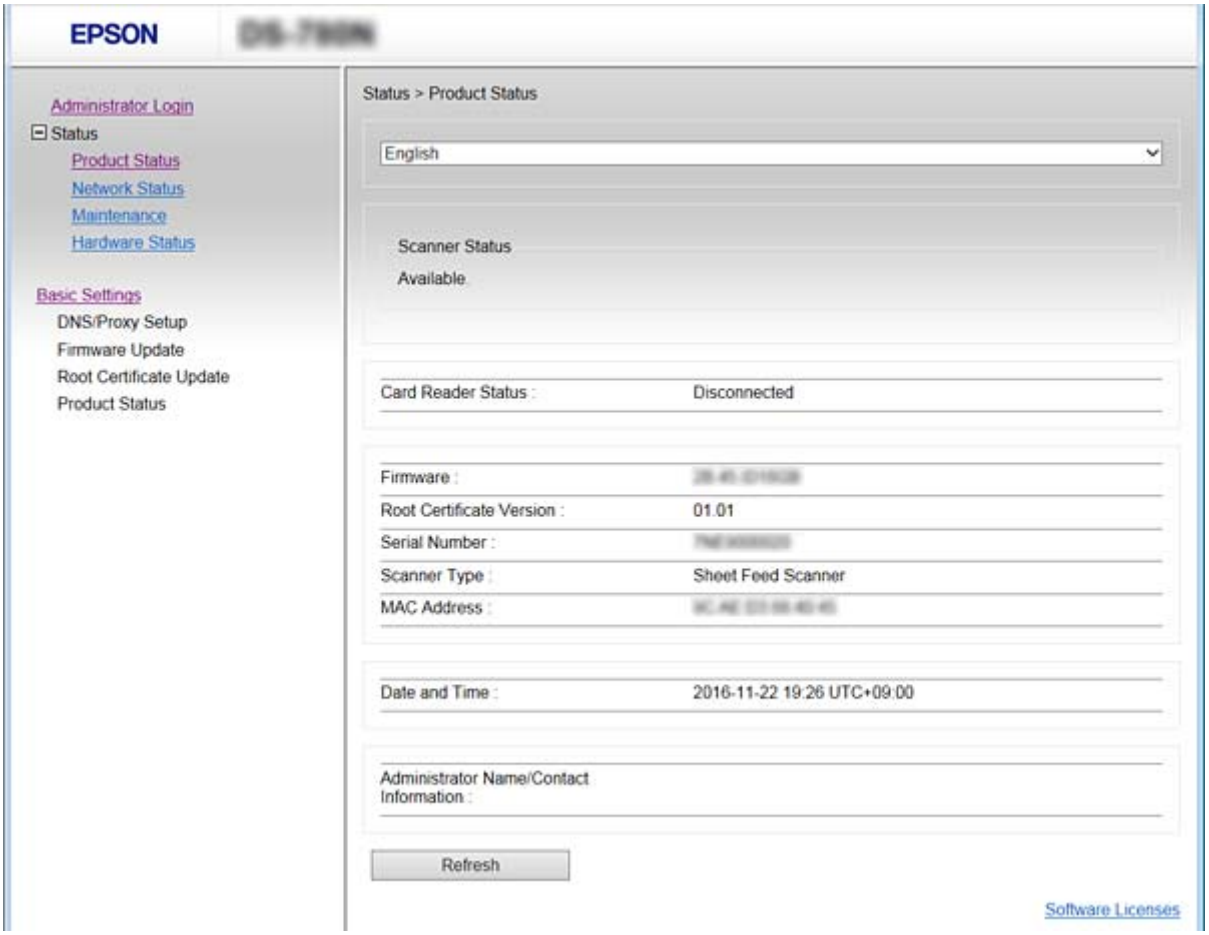
❏ **Basic Settings**

Var konfigurēt skenera pamata iestatījumus.



❏ **Advanced Settings**

Var konfigurēt skenera papildu iestatījumus. Šī lapa paredzēta galvenokārt administratoram.



Piekļuve lietojumprogrammai Web Config

Ievadiet tīmekļa pārlūkprogrammā skenera IP adresi. Jābūt iespējotai opcijai JavaScript. Kad piekļuvei Web Config izmanto HTTPS protokolu, pārlūkprogrammā parādās brīdinājuma ziņojums, jo tiek izmantots pašparakstīts sertifikāts, kas glabājas skenerī.

❏ Piekļuve, izmantojot HTTPS

IPv4: https://<skenera IP adrese> (bez < >)

IPv6: https://[skenera IP adrese]/ (ar [ ])

❏ Piekļuve, izmantojot HTTP

IPv4: http://<skenera IP adrese> (bez < >)

IPv6: http://[skenera 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 skenera nosaukums ir reģistrēts DNS serverī, var izmantot nevis skenera IP adresi, bet gan skenera nosaukumu.*

Saistītā informācija

➡ "SSL/TLS sakari ar skeneri" 63. lpp.

➡ "Par ciparsertifikātiem" 63. lpp.

Skenēšanas funkciju izmantošana

Atkarībā no skenera lietošanas veida instalējiet turpmāk norādīto programmatūru un ar to veiciet iestatījumus.

❏ **Skenēšana no datora**

❏ Apstipriniet tīkla skenēšanas pakalpojuma derīgumu ar Web Config (derīgs, piegādājot no rūpnīcas).

❏ Instalējiet savā datorā Epson Scan 2 un iestatiet IP adresi

❏ Ja veicat skenēšanu, izmantojot darbus, instalējiet Document Capture Pro (Document Capture) un iestatiet darba iestatījumus.

❏ **Skenēšana no vadības paneļa**

❏ Izmantojot Document Capture Pro vai Document Capture Pro Server:

instalējiet Document Capture Pro vai Document Capture Pro Server

DCP iestatījums (servera režīms, klienta režīms).

❏ Izmantojot WSD protokolu:

apstipriniet WSD derīgumu programmā Web Config vai vadības panelī (derīgs, piegādājot no rūpnīcas)

Ierīces papildu iestatījumi (Windows dators).

Skenēšana no datora

Instalējiet programmatūru un pārbaudiet, vai ir iespējots tīkla skenēšanas pakalpojums, lai skenētu no datora, izmantojot tīklu.

Saistītā informācija

➡ "Instalējamā programmatūra" 25. lpp.

➡ "Tīkla skenēšanas iespējošana" 25. lpp.

Instalējamā programmatūra

❏ Epson Scan 2

Šis ir skenera draiveris. Ja izmantojat ierīces funkcijas no datora, instalējiet draiveri katrā klienta datorā. Ja ir instalēta programmatūra Document Capture Pro/Document Capture, varat veikt ierīces pogām piešķirtās darbības.

Ar EpsonNet SetupManager printera draiverus var izplatīt arī apvienotus pakotnēs.

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

Instalējiet klienta datorā. Varat izsaukt un izpildīt darbus, kas reģistrēti datorā, izmantojot tīklā instalētu programmu Document Capture Pro/Document Capture no datora un skenera vadības paneļa.

Varat arī skenēt no datora, izmantojot tīklu. Lai skenētu, nepieciešama programma Epson Scan 2.

Saistītā informācija

➡ "EpsonNet SetupManager" 56. lpp.

Skenera IP adreses iestatīšana programmā Epson Scan 2

Norādiet skenera IP adresi, lai skeneri varētu izmantot tīklā.

1. Sadaļā **Sākt** > **Visas programmas** > **EPSON** > **Epson Scan 2** startējiet **Epson Scan 2 Utility**.

   Ja ir jau reģistrēts cits skeneris, pārejiet uz 2. darbību.

   Ja nav reģistrēts, pārejiet uz 4. darbību.

2. Sadaļā **Skeneris** noklikšķiniet uz ▼.

3. Noklikšķiniet uz **Iestatījumi**.

4. Noklikšķiniet uz **Iespējot rediģēšanu** un tad noklikšķiniet uz **Pievienot**.

5. Sadaļā **Modelis** atlasiet skenera modeļa nosaukumu.

6. Sadaļas **Meklēt tīklu** iespējā **Adrese** atlasiet izmantojamā skenera IP adresi.

   Noklikšķiniet uz  un uz  , lai atjauninātu sarakstu. Ja nevarat atrast skenera IP adresi, atlasiet **Ievadīt adresi** un ievadiet IP adresi.

7. Noklikšķiniet uz **Pievienot**.

8. Noklikšķiniet uz **OK**.

Tīkla skenēšanas iespējošana

Skenējot no klienta datora tīklā, var iestatīt tīkla skenēšanas pakalpojumu. Iespējots noklusējuma iestatījums.

1. Atveriet programmu Web Config un atlasiet **Services** > **Network Scan**.

2. Pārliecinieties, ka **EPSON Scan** iestatījums ir **Enable scanning**.

   Ja tas tā ir, uzdevums ir izpildīts. Aizveriet Web Config.

   Ja pie tā atzīmes nav, atlasiet to un pārejiet uz nākamo darbību.

3. Noklikšķiniet uz **Next**.

4. Noklikšķiniet uz **OK**.

   Tīkla savienojums tiek atjaunots, un pēc tam tiek iespējoti iestatījumi.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Skenēšana, izmantojot vadības paneli

Skenēšana uz mapi un skenēšana uz pastu, izmantojot skenera vadības paneli, kā arī skenēšanas rezultātu pārsūtīšana uz pastu, mapēm utt. tiek veikta, izpildot darbu datorā.

Pārsūtot skenēšanas rezultātus, iestatiet darbu ar programmu Document Capture Pro Server vai Document Capture Pro.

Precīzāku informāciju par iestatījumiem un darba iestatīšanu skatiet programmas Document Capture Pro Server vai Document Capture Pro dokumentācijā vai palīdzības sadaļā.

Saistītā informācija

➡ "Document Capture Pro Server/Document Capture Pro iestatījumi" 26. lpp.

➡ "Serveru un mapju iestatījumi" 27. lpp.

Datorā instalējama programmatūra

❏ **Document Capture Pro Server**

Šī ir programmatūras Document Capture Pro servera versija. Instalējiet to Windows serverī. Serverī var centrāli pārvaldīt vairākas ierīces un darbus. Darbus var vienlaikus veikt no vairākiem skeneriem.

Izmantojot sertificētu programmatūras Document Capture Pro Server versiju, ir iespējams pārvaldīt darbus un skenēšanas vēsturi, kas saistīta ar lietotājiem un grupām.

Lai saņemtu papildinformāciju par Document Capture Pro Server, sazinieties ar vietējo Epson biroju.

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

Tāpat kā skenējot no datora, varēsit izsaukt datorā reģistrētos darbus no vadības paneļa un izpildīt tos. Datora darbus nav iespējams veikt no vairākiem skeneriem.

Document Capture Pro Server/Document Capture Pro iestatījumi

Veiciet iestatījumus skenēšanas funkcijas izmantošanai no skenera vadības paneļa.

1. Atveriet programmu Web Config un atlasiet **Services** > **Document Capture Pro**.

2. Izvēlieties **Darba režīms**.

   ❏ Server Mode:

   atlasiet šo iespēju, lietojot Document Capture Pro Server vai izmantojot Document Capture Pro tikai tiem darbiem, kas tika iestatīti konkrētam datoram.

   ❏ Client Mode:

   iestatiet šo iespēju, ja atlasāt katra klienta datorā tīklā instalētās programmas Document Capture Pro (Document Capture) darba iestatījumu, nenorādot datoru.

3. Iestatiet turpmāk norādītās iespējas saskaņā ar atlasīto režīmu.

   ❏ Server Mode:

   sadaļā **Server Address** norādiet serveri, kurā ir instalēta programma Document Capture Pro Server. Adresē var būt no 2 līdz 252 rakstzīmēm IPv4, IPv6, resursdatora nosaukuma vai FQDN formātā. FQDN formātā var izmantot US-ASCII burtus, skaitļus, alfabētu un domuzīmes (izņemot sākumu un beigas).

   ❏ Client Mode:

   Norādiet **Group Settings**, lai izmantotu skeneru grupu, kas norādīta programmā Document Capture Pro (Document Capture).

4. Noklikšķiniet uz **Iestatījumi**.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Serveru un mapju iestatījumi

Programma Document Capture Pro un Document Capture Pro Server vienu reizi saglabā skenētos datus serverī vai klienta datorā un izmanto pārsūtīšanas funkciju, lai veiktu skenēšanu uz mapi un skenēšanu uz pastu.

Lai pārsūtītu datus no datora, kurā ir instalēta programma Document Capture Pro, Document Capture Pro Server uz datoru vai mākoņpakalpojumu, nepieciešamas pilnvaras un informācija.

Sagatavojiet informāciju par funkciju, kuru izmantosit, ievērojot turpmāk norādīto.

Šo funkciju iestatījumus var veikt programmā Document Capture Pro vai Document Capture Pro Server. Precīzāku informāciju par iestatījumiem skatiet programmas Document Capture Pro Server vai Document Capture Pro dokumentācijā vai palīdzības sadaļā.

Nosaukums	Iestatījumi	Prasība
Skenēt uz tīkla mapi (SMB)	Izveidojiet saglabāšanas mapi un iestatiet tās koplietošanu	Administratīvā lietotāja konts datorā, kurā izveidotas saglabāšanas mapes.
	Mērķis skenēšanai uz tīkla mapi (SMB)	Lietotājvārds un parole, ko izmanto, lai pieteiktos datorā, kur atrodas saglabāšanas mape, un tiesības atjaunināt saglabāšanas mapi.
Skenēt uz tīkla mapi (FTP)	FTP servera pieteikšanās iestatīšana	Pieteikšanās informācija FTP serverim un tiesības atjaunināt saglabāšanas mapi.
Skenēt uz e-pastu	E-pasta servera iestatījumi	E-pasta servera iestatījumu informācija

Nosaukums	Iestatījumi	Prasība
Skenēšana uz Document Capture Pro (izmantojot Document Capture Pro Server)	Iestatījumi, lai pieteiktos mākoņpakalpojumos	Interneta savienojuma vide Konta reģistrēšana mākoņpakalpojumos

WSD skenēšanas izmantošana (tikai sistēmā Windows)

Ja dators izmanto operētājsistēmu Windows Vista vai jaunāku versiju, ir iespējams izmantot WSD skenēšanu.

Ja var lietot WSD protokolu, skenera vadības panelī tiks atvērta izvēlne **Dators (WSD)**.

1. Atveriet programmu Web Config un atlasiet **Services** > **Protocol**.
2. Pārbaudiet, vai sadaļā **WSD Settings** ir atzīmēta iespēja **Enable WSD**.
   Ja tā ir atzīmēta, uzdevums ir pabeigts un programmu Web Config var aizvērt.
   Ja tā nav atzīmēta, atzīmējiet un pārejiet uz nākamo darbību.
3. Noklikšķiniet uz pogas **Next**.
4. Apstipriniet iestatījumus un noklikšķiniet uz **Iestatījumi**.

Sistēmas iestatījumu izvēle

Sistēmas iestatījumu veikšana, izmantojot vadības paneli

EkrEkrāna spilgtuma iestatīšana

Iestatiet LCD ekrāna spilgtumu.

1. Sākuma ekrānā pieskarieties **Iestatījumi**.
2. Pieskarieties **Bieži izmantotie iestatījumi** > **LCD spilgtums**.
3. Pieskarieties  vai  , lai regulētu spilgtumu.
   Spilgtuma līmeni var iestatīt diapazonā no 1 līdz 9.
4. Pieskarieties **Labi**.

SkaņSkaņas iestatīšana

Iestatiet paneļa darbības skaņu un kļūdas ziņojumu skaņu.

1. Sākuma ekrānā pieskarieties **Iestatījumi**.

2. Pieskarieties **Bieži izmantotie iestatījumi** > **Skaņa**.
3. Ja nepieciešams, iestatiet turpmāk norādītos vienumus.
   - ❏ Darbības skaņu
     Iestatiet vadības paneļa darbības skaņas skaļuma līmeni.
   - ❏ Kļūdu ziņojumu skaņu
     Iestatiet kļūdu ziņojumu skaņas skaļuma līmeni.
4. Pieskarieties **Labi**.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

OriOriģināla divkāršās pievades noteikšana

Norādiet funkciju, kas jāizmanto, lai noteiktu divkāršu skenējamā dokumenta pievadi un apturētu skenēšanu vairākkārtējas pievades gadījumā.

Lai skenētu oriģinālus, ko paredzēts pievadīt vairākkārt, piemēram, aploksnes vai papīru ar uzlīmēm, iestatiet šo funkciju izslēgšanas stāvoklī.

Piezīme:
Šo funkciju var iestatīt arī programmā Web Config vai Epson Scan 2.

1. Sākuma ekrānā pieskarieties **Iestatījumi**.
2. Pieskarieties **Ārējie skenēšanas iestatījumi** > **Dubultas ievades not. ar ultrask.**.
3. Pieskarieties **Dubultas ievades not. ar ultrask.**, lai to ieslēgtu vai izslēgtu.
4. Pieskarieties **Aizvērt**.

LēnaMaza ātruma režīma iestatīšana

Iestatiet, lai skenētu mazā ātrumā un izvairītos no papīra iestrēgšanas, skenējot plānus dokumentus, piemēram, veidlapas.

1. Sākuma ekrānā pieskarieties **Iestatījumi**.
2. Pieskarieties **Ārējie skenēšanas iestatījumi** > **Lēni**.
3. Pieskarieties **Lēni**, lai to ieslēgtu vai izslēgtu.
4. Pieskarieties **Aizvērt**.

SistSistēmas iestatījumu veikšana, izmantojot Web Config

Iestatījumi enerģijas taupīšanai dīkstāves laikā

Izvēlieties enerģijas taupīšanas iestatījumus laikam, kad skeneris nedarbojas. Iestatiet laiku atkarībā no lietošanas vides.

Piezīme:
Enerģijas taupīšanas iestatījumus var veikt arī skenera vadības panelī.

1. Atveriet programmu Web Config un atlasiet **System Settings** > **Power Saving**.
2. Ievadiet iestatījuma **Sleep Timer** vērtību — dīkstāves laiku, kuram paejot, notiek pārslēgšanās uz enerģijas taupīšanas režīmu.

   Pa minūtei var iestatīt laika periodu līdz 240 minūtēm.
3. Atlasiet **Power Off Timer** izslēgšanas laiku.
4. Noklikšķiniet uz **OK**.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Vadības paneļa iestatīšana

Iestatījumi skenera vadības panelim. Var veikt turpmāk norādītos iestatījumus.

1. Atveriet programmu Web Config un atlasiet **System Settings** > **Control Panel**.
2. Ja nepieciešams, iestatiet turpmāk norādītos vienumus.
   - ❏ Language

     Atlasiet vadības paneļa valodu.
   - ❏ Panel Lock

     Ja atlasīts iestatījums **ON**, ikreiz, kad veiksiet darbības, kurām nepieciešamas administratora tiesības, tiks pieprasīta administratora parole. Ja administratora parole nav iestatīta, paneļa bloķēšana ir atspējota.
   - ❏ Operation Timeout

     Ja atlasīts iestatījums **ON**, lietotājam piesakoties kā administratoram, notiek automātiska lietotāja izrakstīšana no sistēmas un parādīts sākotnējais ekrāns, ja noteiktu laiku netiek veiktas nekādas darbības.

     Ar sekundes precizitāti var iestatīt laika periodu no 10 sekundēm līdz 240 minūtēm.
3. Noklikšķiniet uz **OK**.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Ārējo saskarņu ierobežojumu iestatīšana

Varat ierobežot USB savienojuma izveidi no datora. Iestatiet to, lai skenēšanu varētu veikt tikai tīklā.

1. Atveriet programmu Web Config un atlasiet **System Settings** > **External Interface**.
2. Atlasiet **Enable** vai **Disable**.

   Lai iestatītu ierobežojumu, atlasiet **Disable**.
3. Pieskarieties **OK**.

Datuma un laika sinhronizēšana ar laika serveri

Ja izmantojat CA sertifikātu, varat novērst ar laiku saistītas problēmas.

1. Atveriet programmu Web Config un atlasiet **System Settings** > **Date and Time** > **Time Server**.
2. Iestatījumam **Use Time Server** atlasiet **Use**.
3. Ievadiet laukā **Time Server Address** laika servera adresi.

   Var izmantot IPv4, IPv6 vai FQDN formātu. Ievadiet līdz 252 rakstzīmēm. Ja nenorādāt šo iestatījumu, atstājiet lauku tukšu.
4. Atveriet **Update Interval (min)**.

   Pa minūtei var iestatīt laika periodu līdz 10 800 minūtēm.
5. Noklikšķiniet uz **OK**.

   Piezīme:
   *Savienojuma ar laika serveri statusu var pārbaudīt laukā **Time Server Status**.*

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Pamata drošības iestatījumi

Šajā nodaļā ir paskaidroti pamata drošības iestatījumi, kuriem nav nepieciešama īpaša vide.

Pamata drošības funkciju apraksts

Šeit ir aprakstītas Epson ierīču pamata drošības funkcijas.

Funkcijas nosaukums	Funkcijas veids	Kas jāiestata	Kas tiek novērsts
Administratora paroles iestatīšana	Bloķējiet ar sistēmu saistītus iestatījumus, piemēram, tīkla un USB savienojuma iestatījumus, lai tos varētu mainīt tikai administrators.	Administrators iestata ierīces paroli. Konfigurācijai vai atjaunināšanai var piekļūt, izmantojot Web Config, vadības paneli, Epson Device Admin un EpsonNet Config.	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.
SSL/TLS sakaru sistēma	Ja piekļūstat Epson serverim internetā no ierīces, piemēram, veicot saziņu ar datoru pārlūkprogrammā vai aparātprogrammatūras atjaunināšanu, saziņas saturu šifrē ar SSL/TLS sakaru sistēmu.	Iegūstiet sertificēšanas iestādes parakstītu sertifikātu un tad importējiet to skenerī.	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.
Pārvalda protokolus	Pārvalda protokolus, ko izmanto saziņā starp ierīcēm un datoriem, iespējo un atspējo funkcijas.	Protokols vai pakalpojums, kuru izmanto atsevišķu funkciju atļaušanai vai aizliegšanai.	Netīšu drošības risku mazināšana, aizliedzot lietotājiem nevajadzīgu funkciju izmantošanu.

Saistītā informācija

➡ "Par Web Config" 22. lpp.
➡ "EpsonNet Config" 55. lpp.
➡ "Epson Device Admin" 55. lpp.
➡ "Administratora paroles konfigurēšana" 32. lpp.
➡ "Protokolu vadība" 35. lpp.

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, skenera vadības paneli vai

programmatūru (Epson Device Admin vai EpsonNet Config). Norādījumus programmatūras lietošanai skatiet attiecīgās programmatūras dokumentācijā.

Saistītā informācija

➡ "Administratora paroles konfigurēšana, izmantojot vadības paneli" 33. lpp.

➡ "Administratora paroles konfigurēšana, izmantojot Web Config" 33. lpp.

➡ "EpsonNet Config" 55. lpp.

➡ "Epson Device Admin" 55. lpp.

Administratora paroles konfigurēšana, izmantojot vadības paneli

Administratora paroli var iestatīt, izmantojot skenera vadības paneli.

1. Sākuma ekrānā pieskarieties **Iestatījumi**.
2. Pieskarieties **Sistēmas administrēšana** > **Administratora iestatījumi**.

   Ja vienums nav redzams, pārvelciet ekrānu uz augšu, lai parādītu vienumu.
3. Pieskarieties **Admin. parole** > **Reģistrēties**.
4. Ievadiet jauno paroli un pēc tam pieskarieties **Labi**.
5. Vēlreiz ievadiet paroli un pēc tam pieskarieties **Labi**.
6. Apstiprinājuma ekrānā pieskarieties **Labi**.

   Tiek parādīts administratora iestatījumu ekrāns.
7. Pieskarieties **Bloķēšanas iestatījums** un pēc tam apstiprinājuma ekrānā pieskarieties **Labi**.

   Iestatījums Bloķēšanas iestatījums tiek mainīts uz **Iesl**, un ikreiz, kad tiks lietots bloķētais izvēlnes vienums, tiks pieprasīta administratora parole.

Piezīme:

❏ *Ja vienuma **Iestatījumi** > **Bieži izmantotie iestatījumi** > **Darbības noildze** iestatījums ir **Iesl**, skeneris automātiski veiks atteikšanos, ja noteiktu laiku nav izmantots vadības panelis.*

❏ *Administratora paroli var mainīt vai dzēst, atlasot **Mainīt** vai **Atiestatīt** ekrānā **Admin. parole** un ievadot administratora paroli.*

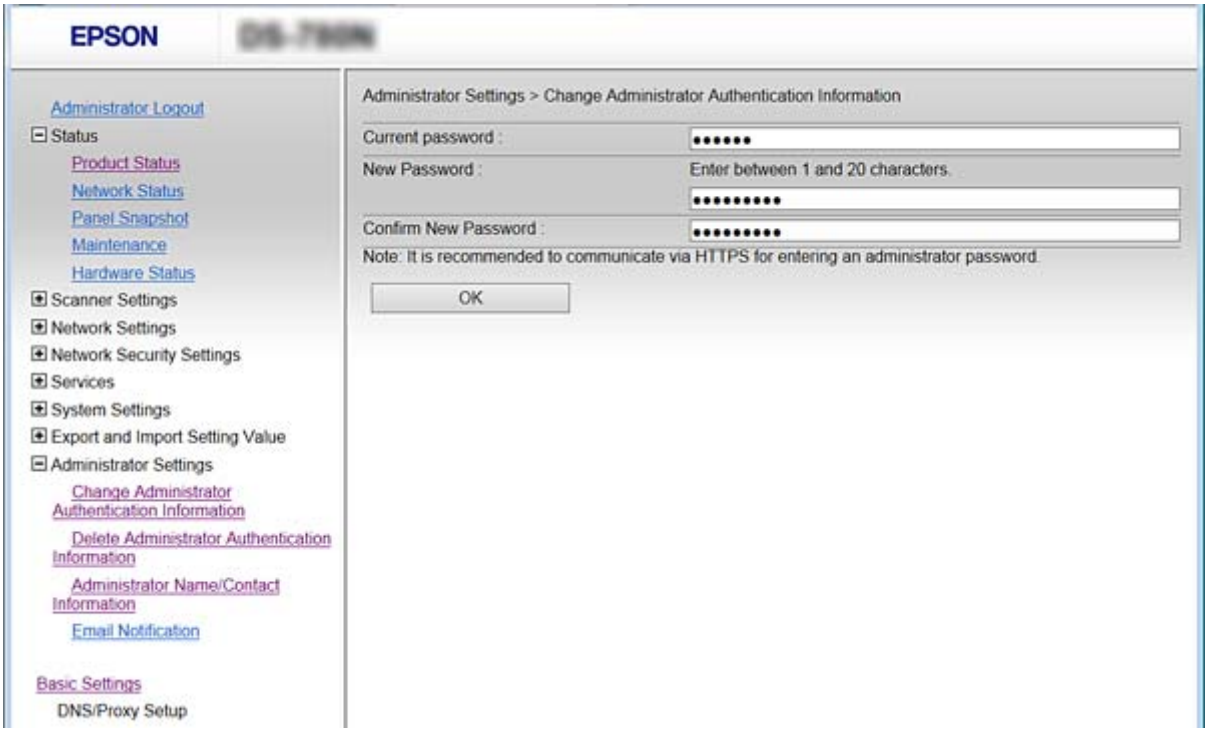
Administratora paroles konfigurēšana, izmantojot Web Config

Administratora paroli var iestatīt, izmantojot programmu Web Config.

1. Atveriet programmu Web Config un atlasiet **Administrator Settings** > **Change Administrator Authentication Information**.

2. Ievadiet paroli laukos **New Password** un **Confirm New Password**. Ja nepieciešams, ievadiet lietotājvārdu.

   Ja vēlaties mainīt paroli, ievadiet pašreizējo paroli.



3. Izvēlieties **OK**.

   Piezīme:

   ❏ *Lai iestatītu vai mainītu bloķētos izvēļņu vienumus, noklikšķiniet uz **Administrator Login** un pēc tam ievadiet administratora paroli.*

   ❏ *Lai dzēstu administratora paroli, noklikšķiniet uz **Administrator Settings** > **Delete Administrator Authentication Information** un pēc tam ievadiet administratora paroli.*

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Vienumi, ko bloķē, izmantojot administratora paroli

Administratoriem ir visu ierīces funkciju iestatīšanas un mainīšanas privilēģijas.

Arī, ja ierīcē iestatāt administratora paroli, varat bloķēt ierīci, lai nebūtu iespējams mainīt vienumus, kas saistīti ar ierīces pārvaldību.

Turpmāk aprakstīti vienumi, kurus var kontrolēt administrators.

Vienums	Apraksts
Skenera iestatījumi	Divkāršas pievades noteikšanas un maza ātruma režīma iestatīšana.
Ethernet savienojuma iestatījumi	Ierīču nosaukumu un IP adrešu maiņa, DNS servera vai starpniekservera iestatījumi un ar tīkla savienojumiem saistītu iestatījumu maiņa.

Pamata drošības iestatījumi

Vienums	Apraksts
Lietotāja pakalpojumu iestatījumi	Sakaru protokolu vadības, skenēšanas tīklā un Document Capture Pro pakalpojumu iestatīšana.
E-pasta servera iestatījumi	E-pasta servera, ar kuru ierīces veido tiešos sakarus, iestatījumi.
Drošības iestatījumi	Tīkla drošības iestatījumi, piemēram, SSL/TLS sakari, IPsec/IP filtrēšana un IEEE802.1X.
Saknes sertifikāta atjaunināšana	Atjaunojiet saknes sertifikātu, kas nepieciešams Document Capture Pro Server autentifikācijai un Web Config aparātprogrammatūras atjaunināšanai.
Aparātprogrammatūras atjaunināšana	Pārbaudīt un atjaunināt ierīču aparātprogrammatūru.
Laiks, taimera iestatījumi	Laiks līdz pārejai miega režīmā, automātiskā izslēgšanās, datums/laiks, dīkstāves taimeris, citi ar taimeriem saistīti iestatījumi.
Atjaunot noklusējuma iestatījumus	Skenera rūpnīcas iestatījumu atiestates iestatīšana.
Administratora iestatījumi	Administratora bloķēšanas vai paroles iestatījumi.
Sertificēto ierīču iestatījumi	Autentificēšanas ierīču ID iestatījumi. Iestatīt, izmantojot skeneri autentificēšanas sistēmā, kas atbalsta autentificēšanas ierīces.

Protokolu vadība

Skenēšanai var izmantot dažādus ceļus un protokolus. Tīkla skenēšanas funkciju var izmantot arī no nenoteikta skaita tīklam pieslēgtiem datoriem. Piemēram, skenēšana atļauta, izmantojot tikai norādītos ceļus un protokolus. Netīšus drošības riskus var samazināt, ierobežojot skenēšanu no noteiktiem ceļiem vai kontrolējot pieejamās funkcijas.

Konfigurējiet protokola iestatījumus.

1. Atveriet programmu Web Config un atlasiet **Services** > **Protocol**.
2. Konfigurējiet katru vienumu.
3. Noklikšķiniet uz **Next**.
4. Noklikšķiniet uz **OK**.

   Skenerim tiek piemēroti iestatījumi.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "Protokoli, kurus var iespējot vai atspējot" 36. lpp.
➡ "Protokolu iestatīšanas vienumi" 37. lpp.

Protokoli, kurus var iespējot vai atspējot

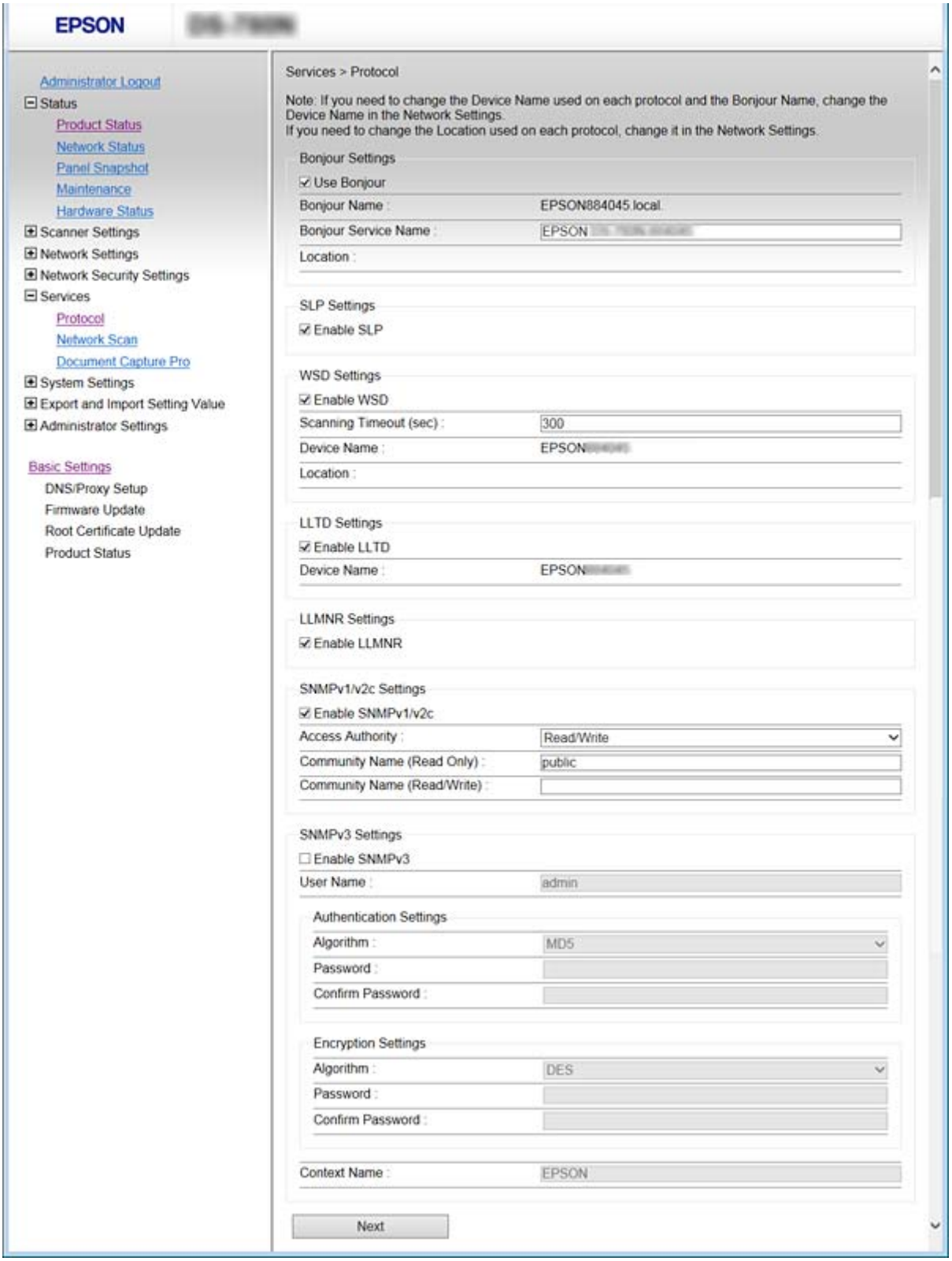
Protokols	Apraksts
Bonjour Settings	Var norādīt, vai lietot Bonjour. Bonjour lieto, lai meklētu ierīces, skenētu un veiktu citas darbības.
SLP Settings	Varat iespējot vai atspējot SLP funkciju. SLP lieto programmā Epson Scan 2 un tīkla meklēšanai programmā EpsonNet Config.
WSD Settings	Varat iespējot vai atspējot WSD funkciju. Iespējojot šo funkciju, var pievienot WSD ierīces vai skenēt no WSD porta.
LLTD Settings	Var iespējot vai atspējot LLTD funkciju. Iespējojot šo funkciju, tas tiek parādīts Windows tīkla kartē.
LLMNR Settings	Var iespējot vai atspējot LLMNR funkciju. Iespējojot šo funkciju, var lietot nosaukumu atpazīšanu bez NetBIOS pat tad, ja nevar lietot DNS.
SNMPv1/v2c Settings	Var norādīt, vai iespējot SNMPv1/v2c. To izmanto ierīču iestatīšanai, pārraudzībai u.t.t.
SNMPv3 Settings	Var norādīt, vai iespējot SNMPv3. To izmanto šifrētu ierīču iestatīšanai, pārraudzībai utt.

Saistītā informācija

➡ "Protokolu vadība" 35. lpp.

➡ "Protokolu iestatīšanas vienumi" 37. lpp.

Protokolu iestatīšanas vienumi



Vienumi	Vērtības iestatīšana un apraksts
Bonjour Settings	

Pamata drošības iestatījumi

Vienumi	Vērtības iestatīšana un apraksts
Use Bonjour	Atlasiet šo iespēju, lai meklētu vai lietotu ierīces, izmantojot Bonjour.
Bonjour Name	Tiek parādīts Bonjour nosaukums.
Bonjour Service Name	Varat apskatīt un iestatīt Bonjour nosaukumu.
Location	Tiek parādīts Bonjour vietas nosaukums.
SLP Settings	
Enable SLP	Atlasiet šo iespēju, lai iespējotu SLP funkciju. Tā tiek izmantota, lai sameklētu tīklu programmā Epson Scan 2 un EpsonNet Config.
WSD Settings	
Enable WSD	Atlasiet šo iespēju, lai iespējotu ierīču pievienošanu, izmantojot WSD, drukātu un skenētu no WSD porta.
Scanning Timeout (sec)	Ievadiet sakaru taimauta vērtību WSD skenēšanai no 3 līdz 3600 sekundēm.
Device Name	Tiek parādīts WSD ierīces nosaukums.
Location	Tiek parādīts WSD vietas nosaukums.
LLTD Settings	
Enable LLTD	Atlasiet šo iespēju, lai iespējotu LLTD. Skeneris tiek parādīts Windows tīkla mapē.
Device Name	Tiek parādīts LLTD ierīces nosaukums.
LLMNR Settings	
Enable LLMNR	Atlasiet šo iespēju, lai iespējotu LLMNR. Var lietot nosaukumu atpazīšanu bez NetBIOS pat tad, ja nevar lietot DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Atlasiet, lai iespējotu SNMPv1/v2c. Tiek parādīti tikai tie skeneri, kuri atbalsta SNMPv3.
Access Authority	Iestatiet piekļuves pilnvaras, kad ir iespējots SNMPv1/v2c. Atlasiet **Read Only** vai **Read/Write**.
Community Name (Read Only)	Ievadiet no 0 līdz 32 ASCII (0x20–0x7E) rakstzīmēm.
Community Name (Read/Write)	Ievadiet no 0 līdz 32 ASCII (0x20–0x7E) rakstzīmēm.
SNMPv3 Settings	
Enable SNMPv3	Atzīmējot izvēles rūtiņu, tiek iespējots SNMPv3.
User Name	Ievadiet no 1 līdz 32 vienbaita rakstzīmēm.
Authentication Settings	
Algorithm	Atlasiet SNMPv3 autentificēšanas algoritmu.

Pamata drošības iestatījumi

Vienumi	Vērtības iestatīšana un apraksts
Password	Atlasiet SNMPv3 autentificēšanas paroli. Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E). Ja nenorādāt šo iestatījumu, atstājiet lauku tukšu.
Confirm Password	Lai apstiprinātu, ievadiet konfigurēto paroli.
Encryption Settings	
Algorithm	Atlasiet SNMPv3. šifrēšanas algoritmu.
Password	Atlasiet SNMPv3 šifrēšanas paroli. Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20–0x7E). Ja nenorādāt šo iestatījumu, atstājiet lauku tukšu.
Confirm Password	Lai apstiprinātu, ievadiet konfigurēto paroli.
Context Name	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" 35. lpp.
➡ "Protokoli, kurus var iespējot vai atspējot" 36. lpp.

Lietošanas un pārvaldības iestatījumi

Šajā nodaļā ir paskaidroti vienumi, kuri ir saistīti ar ierīces ikdienas lietošanu un pārvaldību.

Ierīces informācijas pārbaude

Sadaļā **Status**, izmantojot programmu Web Config, var pārbaudīt turpmāk norādīto informāciju.

❏ Product Status

Valodu, statusu, izstrādājuma numuru, MAC adresi utt.

❏ Network Status

Tīkla savienojuma statusu, IP adresi, DNS serveri utt.

❏ Panel Snapshot

Atvērt ekrāna attēla momentuzņēmumu, kas redzams ierīces vadības panelī.

❏ Maintenance

Pārbaudīt sākuma datumu, skenēšanas informāciju utt.

❏ Hardware Status

Pārbaudīt skenera statusu.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Ierīču pārvaldība (Epson Device Admin)

Izmantojot programmu Epson Device Admin, var pārvaldīt un vadīt daudz ierīču. Programma Epson Device Admin nodrošina iespēju pārvaldīt ierīces, kas atrodas citā tīklā. Turpmāk aprakstītas galvenās pārvaldības funkcijas.

Plašāku informāciju par funkcijām un programmatūras lietošanu skatiet programmas Epson Device Admin dokumentācijā vai palīdzībā.

❏ Ierīču atrašana

Varat tīklā atrast ierīces un reģistrēt tās sarakstā. Ja tam pašam tīkla segmentam, kur atrodas administratora dators, ir pievienotas Epson ierīces, piemēram, printeri un skeneri, tās var atrast pat tad, ja tām nav piešķirtas IP adreses.

Atrast var arī ierīces, kuras ir pievienotas tīkla datoriem ar USB vadu. Datorā jāinstalē programma Epson Device USB Agent.

❏ Ierīču iestatīšana

Pastāv iespēja sagatavot veidni ar tādiem iestatījumu vienumiem, kā tīkla saskarne un papīra avots, un izmantot to citām ierīcēm kā koplietojamus iestatījumus. Kad ierīci, kurai nav piešķirta IP adrese, pievieno tīklam, tai var piešķirt IP adresi.

❏ Ierīču pārraudzība

Pastāv iespēja regulāri skatīt tīkla ierīču statusu un detalizētu informāciju par tām. Var pārraudzīt arī ierīces, kuras ir pievienotas tīkla datoriem ar USB vadu, kā arī citu uzņēmumu ierīces, kuras ir reģistrētas ierīču sarakstā. Lai varētu pārraudzīt ar USB vadu pievienotās ierīces, jāinstalē programma Epson Device USB Agent.

❏ Brīdinājumu pārvaldība

Var pārraudzīt brīdinājumus par ierīču un patērējamo materiālu statusu. Pamatojoties uz iestatītajiem nosacījumiem, sistēma automātiski sūta administratoram e-pasta paziņojumus.

❏ Pārskatu pārvaldība

Sistēmai uzkrājot datus par ierīces lietojumu un patērējamajiem materiāliem, var regulāri veidot pārskatus. Šos izveidotos pārskatus pēc tam var saglabāt un nosūtīt, izmantojot e-pastu.

Saistītā informācija

➡ "Epson Device Admin" 55. lpp.

E-pasta ziņojumu saņemšana notikumu gadījumā

Par e-pasta paziņojumiem

Šo līdzekli var izmantot, lai noteiktās situācijās saņemtu e-pastā brīdinājumus. Iespējams reģistrēt līdz 5 e-pasta adresēm un izvēlēties, par kādiem notikumiem saņemt paziņojumus.

Lai izmantotu šo funkciju, jākonfigurē pasta serveris.

Saistītā informācija

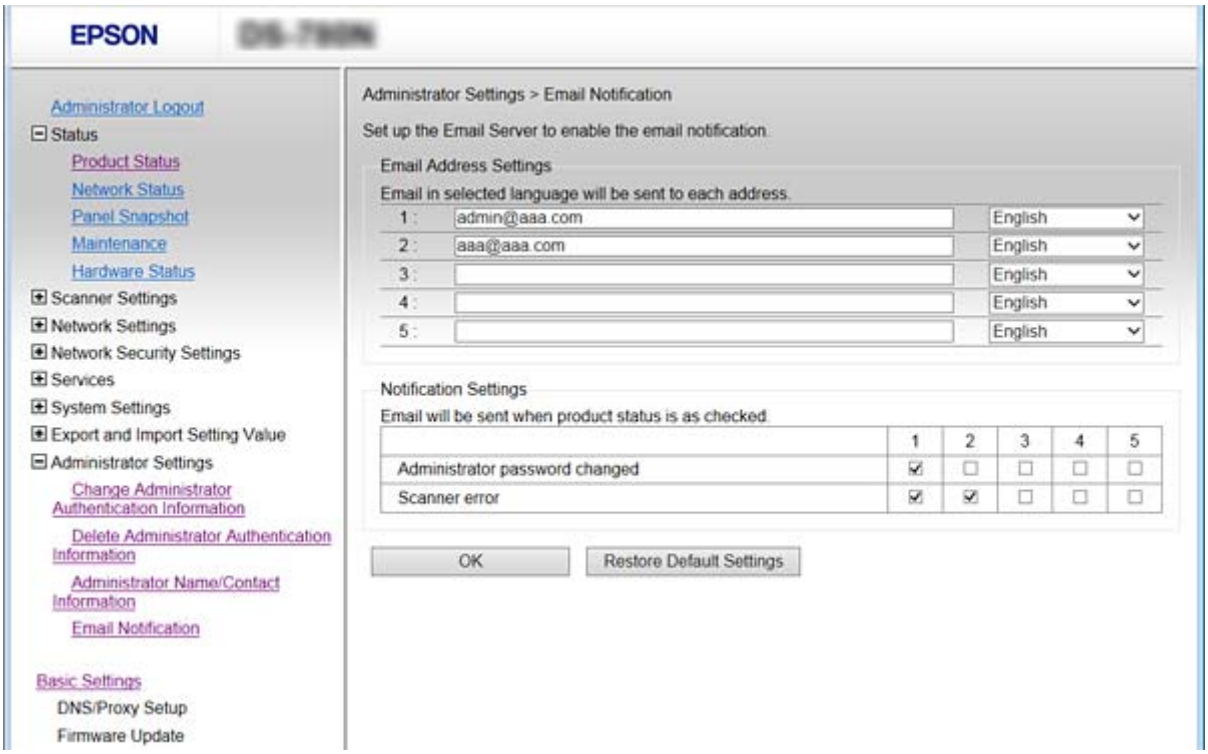
➡ "Pasta servera konfigurēšana" 42. lpp.

E-pasta paziņojumu konfigurēšana

Lai izmantotu šo funkciju, jākonfigurē pasta serveris.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Administrator Settings** > **Email Notification**.
2. Ievadiet e-pasta adresi, kurā vēlaties saņemt e-pasta paziņojumus.
3. Izvēlieties e-pasta paziņojumu valodu.

4. Atzīmējiet izvēles rūtiņas pie paziņojumiem, kurus vēlaties saņemt.



5. Noklikšķiniet uz **OK**.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

➡ "Pasta servera konfigurēšana" 42. lpp.

Pasta servera konfigurēšana

Pirms konfigurēšanas pārbaudiet turpmāk norādīto.

❏ Skeneris ir pieslēgts tīklam.

❏ Datora e-pasta servera informācija.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Settings** > **Email Server** > **Basic**.
2. Ievadiet katra vienuma vērtību.
3. Atlasiet **OK**.

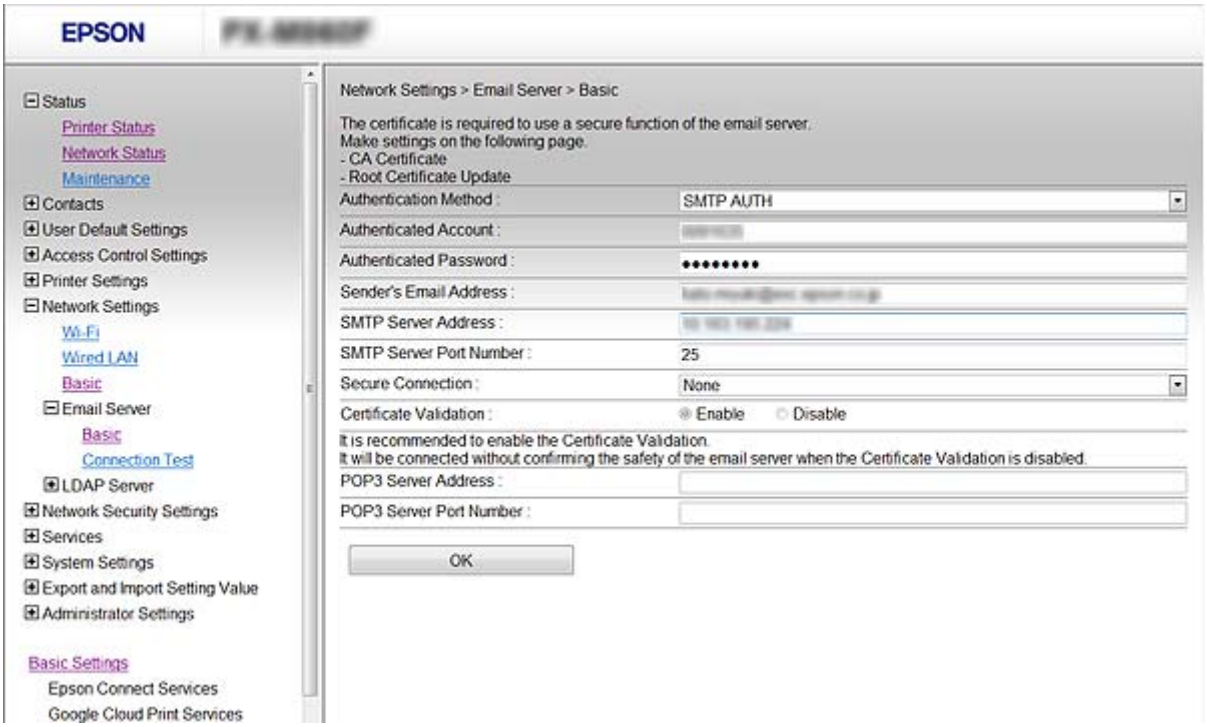
   Tiek parādīti atlasītie iestatījumi.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

➡ "Pasta servera vienumu iestatīšana" 43. lpp.

Pasta servera vienumu iestatīšana



Vienumi	Iestatījumi un skaidrojumi	
Authentication Method	Norādiet autentifikācijas metodi, kuru skeneris izmantos piekļuvei e-pasta serverim.	
	Off	Sazinoties ar pasta serveri, autentifikācija ir atspējota.
	SMTP AUTH	Nepieciešams, lai pasta serveris atbalstītu SMTP autentifikāciju.
	POP before SMTP	Atlasot šo metodi, konfigurējiet POP3 serveri.
Authenticated Account	Atlasot **SMTP AUTH** vai **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet autentifikācijas konta nosaukumu, kas sastāv no 0 līdz 255 ASCII rakstzīmēm (0x20–0x7E).	
Authenticated Password	Atlasot **SMTP AUTH** vai **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet autentifikācijas paroli, kas sastāv no 0 līdz 20 rakstzīmēm (A–Z a–z 0–9) ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Ievadiet sūtītāja e-pasta adresi. Ievadiet no 0 līdz 255 ASCII rakstzīmēm (0x20–0x7E), izņemot šīs : ( ) < > [ ] ; ¥. Pirmā rakstzīme nedrīkst būt punkts (.).	
SMTP Server Address	Ievadiet no 0 līdz 255 rakstzīmēm (A–Z a–z 0–9). - . Var izmantot IPv4 vai FQDN formātu.	
SMTP Server Port Number	Ievadiet skaitli no 1 līdz 65 535.	

Vienumi	Iestatījumi un skaidrojumi	
Secure Connection	Norādiet e-pasta servera drošā savienojuma metodi.	
	None	Atlasot **POP before SMTP** kā **Authentication Method** iestatījumu, savienojuma metode tiek iestatīta kā **None**.
	SSL/TLS	Tas ir pieejams, kad **Authentication Method** ir iestatīta kā **Off** vai „**SMTP AUTH**".
	STARTTLS	Tas ir pieejams, kad **Authentication Method** ir iestatīta kā **Off** vai „**SMTP AUTH**".
Certificate Validation	Iespējojot šo funkciju, sertifikāts tiek validēts. Ieteicams to iestatīt kā **Enable**.	
POP3 Server Address	Atlasot **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet POP3 servera adresi, kas sastāv no 0 līdz 255 rakstzīmēm (A–Z a–z 0–9). - . Var izmantot IPv4 vai FQDN formātu.	
POP3 Server Port Number	Atlasot **POP before SMTP** kā **Authentication Method** iestatījumu, ievadiet skaitli no 1 līdz 65535.	

Saistītā informācija

➡ "Pasta servera konfigurēšana" 42. lpp.

Pasta servera savienojuma pārbaude

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Settings** > **Email Server** > **Connection Test**.
2. Atlasiet **Start**.

   Tiek sākts pasta servera savienojuma tests. Pēc testēšanas tiek parādīta pārbaudes atskaite.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "Pasta servera savienojuma testēšanas atsauces" 44. lpp.

Pasta servera savienojuma testēšanas atsauces

Ziņojumi	Skaidrojums
Connection test was successful.	Šis ziņojums tiek parādīts, ja savienojums ar serveri ir veiksmīgs.
SMTP server communication error. Check the following. - Network Settings	Šis ziņojums tiek parādīts turpmāk norādītajos gadījumos ❏ Skeneris nav pieslēgts tīklam ❏ SMTP serveris nedarbojas ❏ Tīkla savienojums atvienojies sazināšanās laikā ❏ Saņemti nepilnīgi dati

Lietošanas un pārvaldības iestatījumi

Ziņojumi	Skaidrojums
POP3 server communication error. Check the following. - Network Settings	Šis ziņojums tiek parādīts turpmāk norādītajos gadījumos ❏ Skeneris nav pieslēgts tīklam ❏ POP3 serveris nedarbojas ❏ Tīkla savienojums atvienojies sazināšanās laikā ❏ Saņemti nepilnīgi dati
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Šis ziņojums tiek parādīts turpmāk norādītajos gadījumos ❏ Savienošanās ar DNS serveri neizdevās ❏ SMTP servera nosaukuma atpazīšana neizdevās
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Šis ziņojums tiek parādīts turpmāk norādītajos gadījumos ❏ Savienošanās ar DNS serveri neizdevās ❏ POP3 servera nosaukuma atpazīšana neizdevās
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Šis ziņojums tiek parādīts, ja SMTP servera autentifikācija neizdevās.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Šis ziņojums tiek parādīts, ja POP3 servera autentifikācija neizdevās.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Šis ziņojums tiek parādīts, ja mēģiniet izveidot sakarus ar neatbalstītiem protokoliem.
Connection to SMTP server failed. Change Secure Connection to None.	Šis ziņojums tiek parādīts, ja ir radusies servera un klienta SMTP neatbilstība vai ja serveris neatbalsta SMTP drošu savienojumu (SSL savienojums).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Šis ziņojums tiek parādīts, ja ir radusies servera un klienta SMTP neatbilstība vai ja serveris pieprasa lietot SSL/TLS savienojumu, lai izveidotu SMTP drošu savienojumu.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Šis ziņojums tiek parādīts, ja ir radusies servera un klienta SMTP neatbilstība vai ja serveris pieprasa lietot STARTTLS savienojumu, lai izveidotu SMTP drošu savienojumu.
The connection is untrusted. Check the following. - Date and Time	Šis ziņojums tiek parādīts, ja skenera datuma un laika iestatījumi nav pareizi vai ja sertifikātam ir beidzies derīguma termiņš.
The connection is untrusted. Check the following. - CA Certificate	Šis ziņojums tiek parādīts, ja skenerim nav serverim atbilstoša saknes sertifikāta vai ja CA Certificate nav importēts.
The connection is not secured.	Šis ziņojums tiek parādīts, ja iegūtais sertifikāts ir bojāts.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Šis ziņojums tiek parādīts, ja ir radusies servera un klienta autentifikācijas metodes neatbilstība. Serveris atbalsta SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Šis ziņojums tiek parādīts, ja ir radusies servera un klienta autentifikācijas metodes neatbilstība. Serveris neatbalsta SMTP AUTH.

Ziņojumi	Skaidrojums
Sender's Email Address is incorrect. Change to the email address for your email service.	Šis ziņojums tiek parādīts, ja norādītā sūtītāja e-pasta adrese nav pareiza.
Cannot access the product until processing is complete.	Šis ziņojums tiek parādīts, ja skeneris ir aizņemts.

Saistītā informācija

➡ "Pasta servera savienojuma pārbaude" 44. lpp.

Aparātprogrammatūras atjaunināšana

Aparātprogrammatūras atjaunināšana, izmantojot programmu Web Config

Atjaunina aparātprogrammatūru, izmantojot programmu Web Config. Ierīcei jābūt savienotai ar internetu.

1. Atveriet programmu Web Config un atlasiet **Basic Settings** > **Firmware Update**.
2. Noklikšķiniet uz **Start**.

   Tiek sākta aparātprogrammatūras pārbaude, un, ja pastāv atjaunināta aparātprogrammatūra, tiek parādīta informācija par aparātprogrammatūru.
3. Noklikšķiniet uz **Start** un izpildiet ekrānā sniegtos norādījumus.

Piezīme:
Aparātprogrammatūru var atjaunināt arī, izmantojot Epson Device Admin. Ierīču sarakstā var vizuāli pārbaudīt aparātprogrammatūras informāciju. Šī iespēja noderīga, ja nepieciešams atjaunināt aparātprogrammatūru vairākās ierīcēs. Plašāku informāciju skatiet Epson Device Admin pamācībā vai palīdzībā.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "Epson Device Admin" 55. lpp.

Aparātprogrammatūras atjaunināšana, izmantojot programmu Epson Firmware Updater

Ierīces aparātprogrammatūru var lejupielādēt datorā no Epson tīmekļa vietnes, un pēc tam, lai atjauninātu aparātprogrammatūru, ierīci var savienot ar datoru, izmantojot USB vadu. Ja nevar veikt atjaunināšanu tīklā, izmēģiniet šo metodi.

1. Atveriet Epson tīmekļa vietni un lejupielādējiet aparātprogrammatūru.
2. Izmantojot USB vadu, savienojiet ar ierīci datoru, kurā atrodas lejupielādētā aparātprogrammatūra.

3. Veiciet dubultklikšķi uz lejupielādētā .exe faila.

   Tiek palaista programma Epson Firmware Updater.

4. Izpildiet ekrānā redzamās instrukcijas.

Iestatījumulestatījumu dublēšana

Eksportējot iestatījumu vienumus programmā Web Config, tos var kopēt uz citiem skeneriem.

Iestatījumu eksportēšana

Eksportējiet katru skenera iestatījumu.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Export and Import Setting Value** > **Export**.

2. Atlasiet iestatījumus, kurus vēlaties eksportēt.

   Atlasiet iestatījumus, kurus vēlaties eksportēt. Atlasot galveno kategoriju, tiek atlasītas arī apakškategorijas. Tomēr nevar izvēlēties tās apakškategorijas, kuras rada kļūdas, dubultojot tās tajā pašā tīklā (piemēram, IP adreses u.t.t.).

3. Lai šifrētu eksportēto failu, ievadiet paroli.

   Nepieciešama parole, lai importētu failu. Atstājiet tukšu, ja nevēlaties šifrēt failu.

4. Noklikšķiniet uz **Export**.

   Svarīga informācija:

   *Ja vēlaties eksportēt skenera tīkla iestatījumus, piemēram, skenera nosaukumu un IP adresi, atlasiet **Enable to select the individual settings of device** un norādiet arī citus vienumus. Izmantojiet tikai nomaiņas skenera atlasītās vērtības.*

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Iestatījumu importēšana

Importējiet eksportēto Web Config failu skenerī.

Svarīga informācija:

Importējot vērtības ar individuālu informāciju, piemēram, skenera nosaukumu vai IP adresi, pārliecinieties, vai tajā pašā tīklā neeksistē tāda pati IP adrese. Ja IP adrese pārklājas, skeneris neatspoguļo vērtību.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Export and Import Setting Value** > **Import**.

2. Atlasiet eksportēto failu un pēc tam ievadiet šifrēto paroli.

3. Noklikšķiniet uz **Next**.

4. Atlasiet importējamos iestatījumus un noklikšķiniet uz **Next**.
5. Noklikšķiniet uz **OK**.

Skenerim tiek piemēroti iestatījumi.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Problēmu risināšana

Problēmu risināšanas padomi

Papildinformāciju var atrast turpmāk norādītajā rokasgrāmatā.

❏ Lietotāja rokasgrāmata

Sniedz norādījumus par skenera lietošanu, apkopi un problēmu novēršanu.

Servera un tīkla ierīces žurnāla pārbaude

Ja rodas tīkla savienojuma kļūda, var būt iespējams noteikt iemeslu, apstiprinot pasta servera, LDAP servera u. c. žurnālu, veicot statusa pārbaudi ar sistēmas aprīkojuma žurnālu un komandu, piemēram, maršrutētāju, tīkla žurnālu.

Tīkla iestatījumu inicializēšana

Tīkla iestatījumu atjaunošana, izmantojot vadības paneli

Tīkla iestatījumiem var atjaunot noklusējuma vērtības.

1. Sākuma ekrānā pieskarieties **Iestatījumi**.
2. Pieskarieties **Sistēmas administrēšana** > **Atjaunot noklusējuma iestatījumus** > **Tīkla iestatījumi**.
3. Apskatiet ziņojumu un pēc tam pieskarieties **Jā**.
4. Kad tiek parādīts ziņojums par pabeigšanu, pieskarieties **Aizvērt**.

   Ja nepieskaras **Aizvērt**, ekrāns pēc noteikta laika automātiski tiek aizvērts.

Ierīču un datoru savstarpējo sakaru pārbaude

Savienojuma pārbaude, izmantojot ehotestēšanas komandu — Windows

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

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

   To var pārbaudīt, izmantojot Epson Scan 2.

2. Atveriet datora komandu uzvednes ekrānu.

   ❏ Windows 10

   Ar peles labo pogu noklikšķiniet uz palaides pogas vai nospiediet un turiet to, pēc tam izvēlieties **Komandu uzvedne**.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Atveriet lietojumprogrammas ekrānu, pēc tam izvēlieties **Komandu uzvedne**.

   ❏ Operētājsistēmā Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 vai vecākās operētājsistēmās

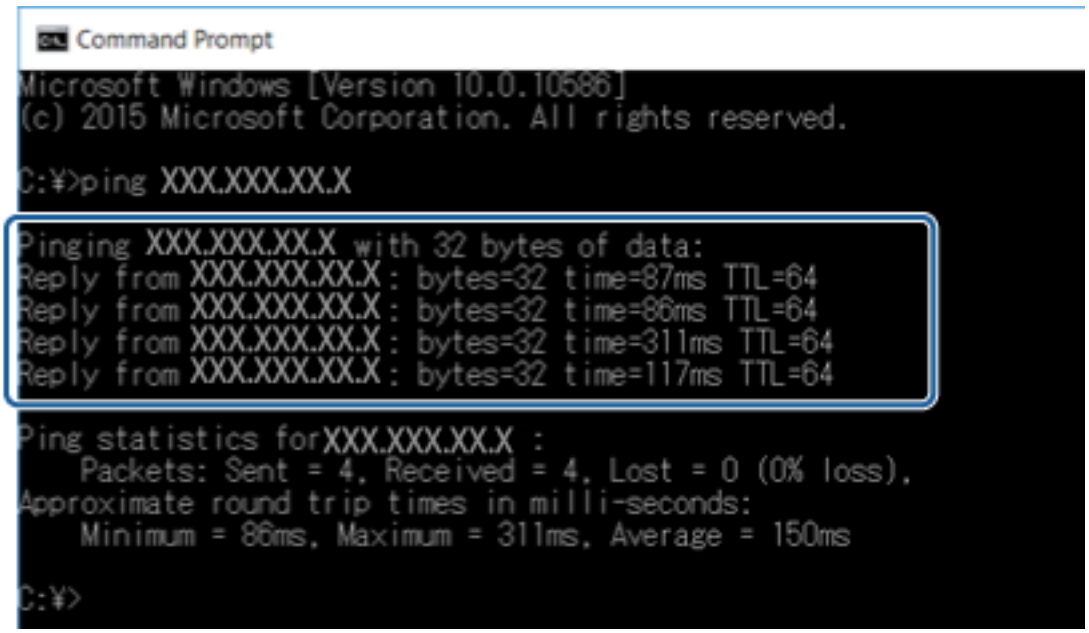
   Noklikšķiniet uz pogas Sākt, izvēlieties **Visas programmas** vai **Programmas** > **Piederumi** > **Komandu uzvedne**.

3. Uzrakstiet „ping xxx.xxx.xxx.xxx”, pēc tam nospiediet taustiņu Enter.

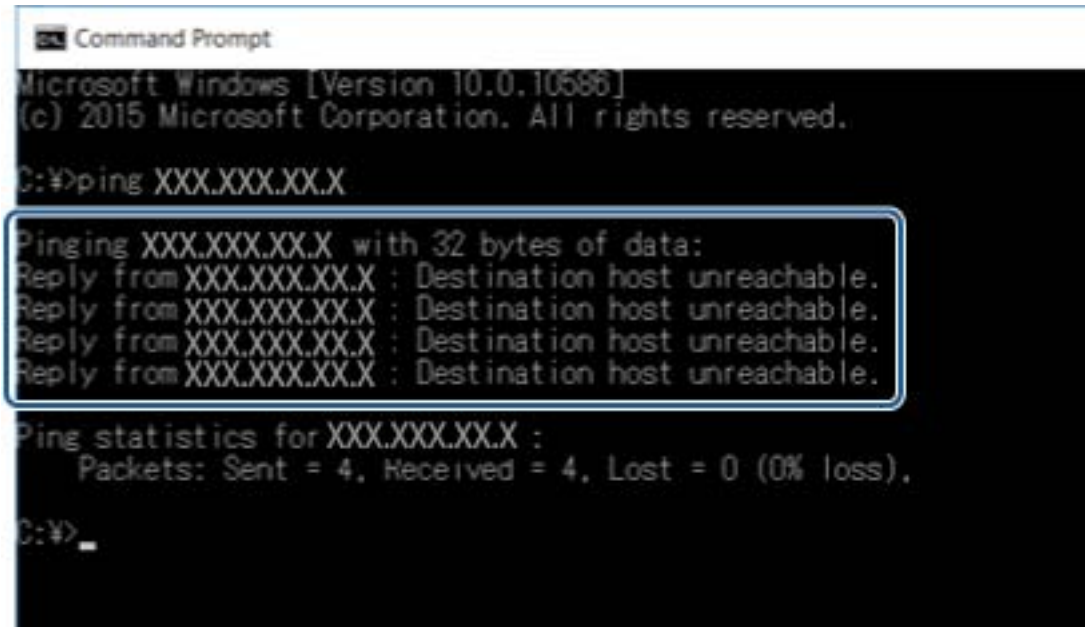
   Ievadiet skenera IP adresi xxx.xxx.xxx.xxx.

4. Pārbaudiet sakaru statusu.

   Ja skenerim ir sakari ar datoru, tiek parādīts nākamajā attēlā redzamais ziņojums.



Ja skenerim nav sakaru ar datoru, tiek parādīts nākamajā attēlā redzamais ziņojums.



Savienojuma pārbaude, izmantojot ehotestēšanas komandu — Mac OS

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

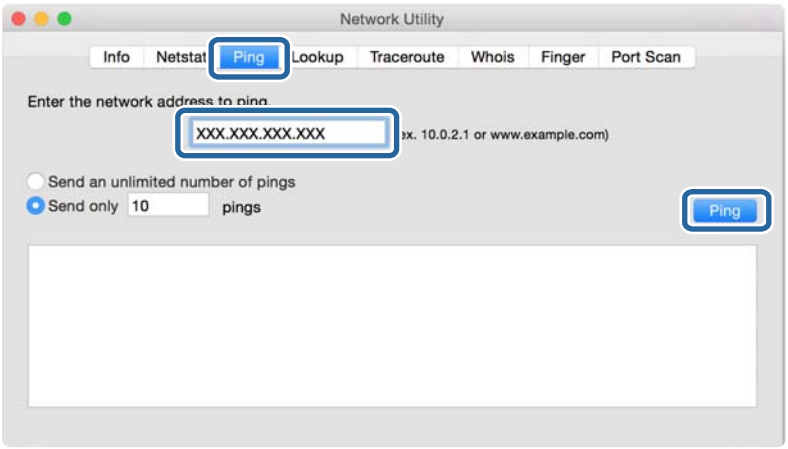
1. Savienojumam, kuru vēlaties pārbaudīt, pārbaudiet skenera IP adresi.

   To var pārbaudīt, izmantojot Epson Scan 2.

2. Palaidiet programmu Tīkla utilīta.

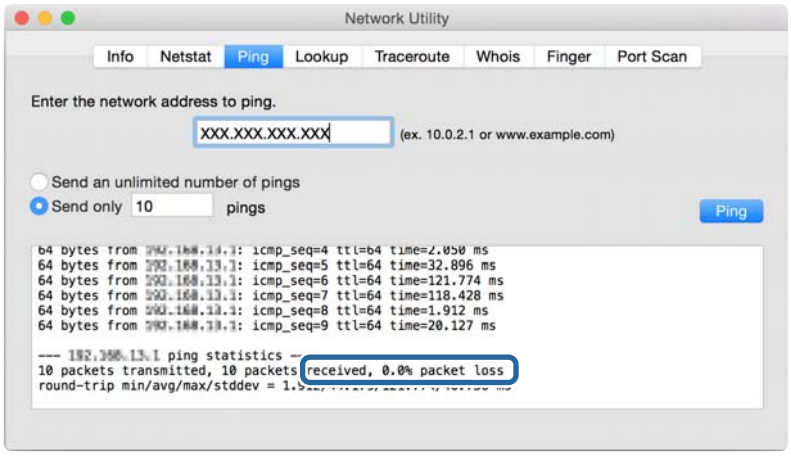
   Spotlight uzrakstiet „Tīkla utilīta”.

3. Noklikšķiniet uz cilnes **Ping**, ievadiet IP adresi, kuru pārbaudījāt, veicot 1. darbību, pēc tam noklikšķiniet uz **Ping**.

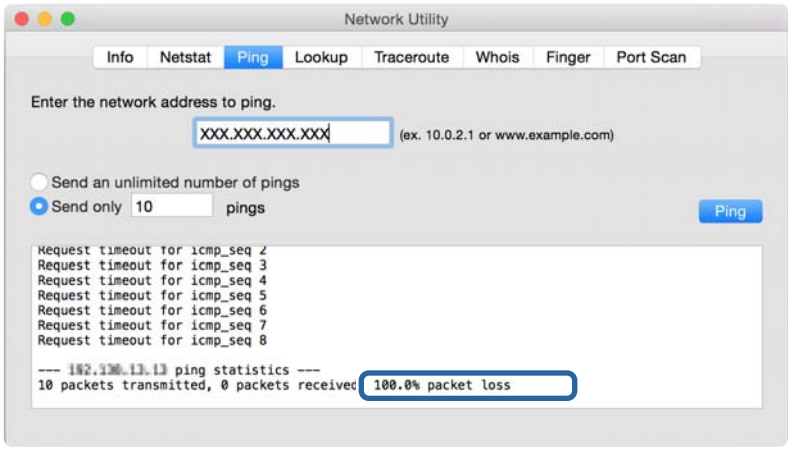


4. Pārbaudiet sakaru statusu.

   Ja skenerim ir sakari ar datoru, tiek parādīts nākamajā attēlā redzamais ziņojums.



   Ja skenerim nav sakaru ar datoru, tiek parādīts nākamajā attēlā redzamais ziņojums.



Tīkla programmatūras lietošanas problēmas

Nevar atvērt tīmekļa konfigurācijas sadaļu

Vai skenera IP adrese ir pareizi konfigurēta?

Konfigurējiet IP adresi, izmantojot Epson Device Admin vai EpsonNet Config.

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 turpmāk. Web Config var piekļūt tikai tādā pārlūkprogrammā, kas atbalsta turpmāk 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, pirms tā derīgums beidzies, pārbaudiet, vai skenera datums ir konfigurēts pareizi.

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

Skenera IP adrese, kas ievadīta laukā **Common Name**, lai izveidotu pašparakstītu sertifikātu vai CSR, neatbilst pārlūkprogrammā ievadītajai adresei. Iegūstiet un importējiet sertifikātu vēlreiz vai mainiet skenera nosaukumu.

Piekļuve skenerim notiek, izmantojot starpniekserveri.

Ja savienojumā ar skeneri izmantojat starpniekserveri, jākonfigurē pārlūkprogrammas starpniekservera iestatījumi.

❏ Windows:

Atlasiet **Vadības panelis** > **Tīkls un internets** > **Interneta opcijas** > **Savienojumi** > **LAN iestatījumi** > **Starpniekserveris** un pēc tam konfigurējiet, lai vietējās adreses neizmantotu starpniekserveri.

❏ Mac OS:

Atlasiet **Sistēmas preferences** > **Tīkls** > **Papildu** > **Starpniekserveri**, un pēc tam reģistrējiet lokālo adresi sadaļā **Apiet starpniekservera iestatījumus šiem resursdatoriem un domēniem**.

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 lietojumprogrammai Web Config" 23. lpp.

➡ "IP adreses piešķiršana" 15. lpp.

➡ "IP adreses piešķiršana, izmantojot EpsonNet Config" 56. lpp.

Lietotnē „EpsonNet Config" netiek parādīts modeļa nosaukums un/vai IP adrese

Vai atlasījāt iespēju Bloķēt, Atcelt vai Beidzēšana mirklī, kad tika attēlots Windows drošības ekrāns vai ugunsmūra ekrāns?

Ja atlasīta iespēja **Bloķēt**, **Atcelt** vai **Beidzēšana**, 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** > **Options** > **Timeout**, un pēc tam pagariniet laika posmu opcijas **Communication Error** iestatījumā. Ievērojiet: rīkojoties šādi, „EpsonNet Config” darbība var palēnināties.

Saistītā informācija

➡ "EpsonNet Config palaišana — sistēmā Windows" 56. lpp.

➡ "EpsonNet Config palaišana — sistēmā Mac OS" 56. 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. Lietojumprogrammu Epson Device Admin var lejupielādēt no Epson atbalsta vietnes. Papildinformāciju skatiet Epson Device Admin dokumentācijā vai palīdzībā.

Programmas Epson Device Admin palaišana (tikai operētājsistēmā Windows)

Atlasiet **Visas programmas** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Piezīme:
Ja tiek parādīts ugunsmūra brīdinājums, piešķiriet piekļuvi programmai Epson Device Admin.

EpsonNet Config

Izmantojot EpsonNet Config, administrators var konfigurēt skenera tīkla iestatījumus, piemēram, piešķirt IP adreses un mainīt savienojuma veidu. Windows atbalsta pakešuzdevumu iestatīšanas funkciju. Papildinformāciju skatiet EpsonNet Config dokumentācijā vai palīdzībā.

EpsonNet Config palaišana — sistēmā Windows

Atlasiet **Visas programmas** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Piezīme:
Ja tiek parādīts ugunsmūra brīdinājums, piešķiriet piekļuvi programmai EpsonNet Config.

EpsonNet Config palaišana — sistēmā Mac OS

Izvēlēties **Aiziet!** > **Lietojumprogrammas** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager ir programmatūra, kuru izmantojot, var izveidot pakotni skenera instalēšanas vienkāršošanai, piemēram, skenera draivera instalēšanai un konfigurēšanai un Document Capture Pro instalēšanai. Izmantojot šo programmatūru, administrators var izveidot unikālas programmatūras pakotnes un izplatīt tās grupās.

Papildinformāciju skatiet reģionālajā Epson tīmekļa vietnē.

IP adreses piešķiršana, izmantojot EpsonNet Config

Skenerim var piešķirt IP adresi, izmantojot programmu EpsonNet Config. Programma EpsonNet Config ļauj piešķirt IP adresi skenerim, kuram tā nav piešķirta pēc savienojuma izveides, izmantojot Ethernet vadu.

IP adrešu piešķiršana, izmantojot pakešiestatījumus

Pakešveida iestatījumu faila izveide

Izmantojot kā atslēgas MAC adresi un modeļa nosaukumu, var izveidot jaunu SYLK failu, lai iestatītu IP adresi.

1. Atveriet izklājlapu lietojumprogrammu (piemēram, Microsoft Excel) vai teksta redaktoru.

2. Pirmajā rindā kā iestatījumu vienumu nosaukumus ievadiet „Info_MACAddress”, „Info_ModelName” un „TCPIP_IPAddress”.

   Ievadiet iestatījumu vienumus sekojošajām teksta virknēm. Tiek izšķirti lielie/mazie burti un dubultbaitu/vienbaita rakstzīmes, tādēļ, ja kaut viena rakstzīmes atšķiras, vienums netiek atpazīts.

   Ievadiet iestatījuma vienumu, kā aprakstīts turpmāk; pretējā gadījumā programma EpsonNet Config nespēs atpazīt iestatījumu vienumus.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Ievadiet katrai tīkla saskarnei MAC adresi, modeļa nosaukumu un IP adresi.

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. Ievadiet nosaukumu un saglabājiet kā SYLK failu (*.slk).

Iestatījumu izvēle vienlaikus vairākām ierīcēm, izmantojot konfigurācijas failu

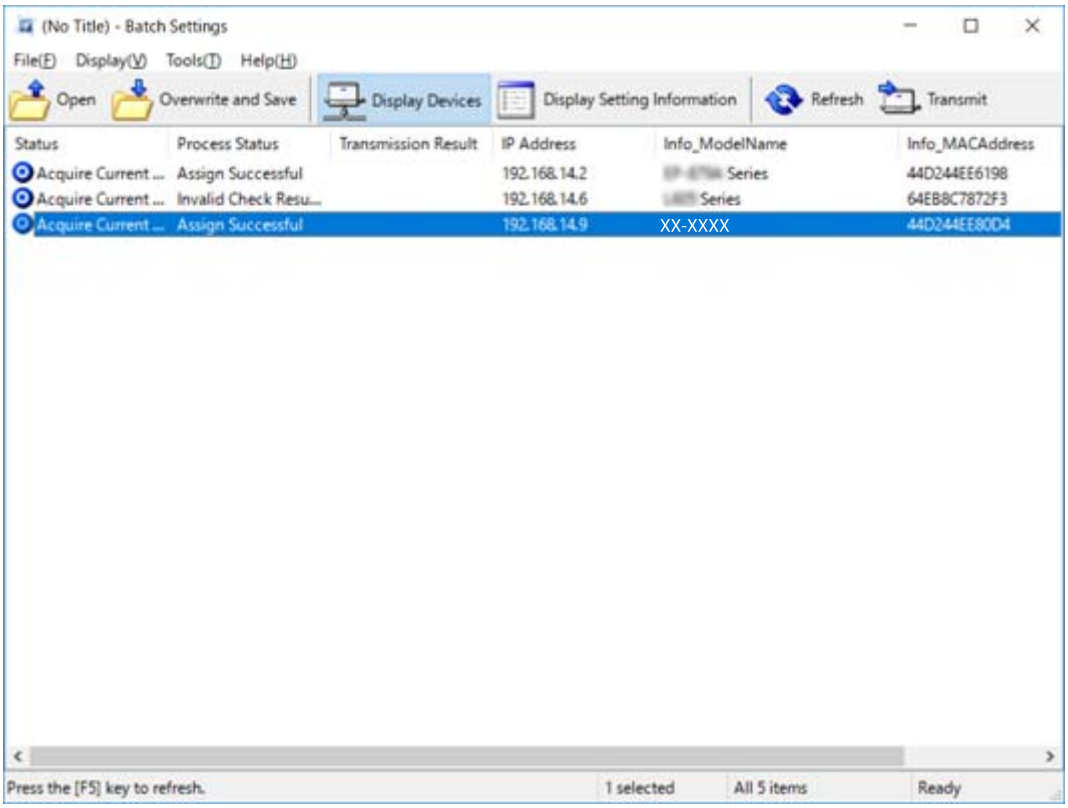
Piešķiriet IP adreses konfigurācijas failā (SYLK file) vienlaikus. Pirms adrešu piešķiršanas jāizveido konfigurācijas fails.

1. Pievienojiet visas ierīces tīklam, izmantojot Ethernet vadus.
2. Ieslēdziet skeneri.
3. Palaidiet programmu EpsonNet Config.

   Tiek parādīts tīkla skeneru saraksts. Var paiet zināms laiks, pirms tie tiks parādīti.
4. Noklikšķiniet uz **Tools** > **Batch Settings**.
5. Noklikšķiniet uz **Open**.
6. Faila izvēles ekrānā atlasiet SYLK failu (*.slk), kurš satur iestatījumus, un pēc tam noklikšķiniet uz **Open**.

7. Atlasiet ierīces, kurām vēlaties vienlaikus norādīt iestatījumus, kolonnā **Status** izvēloties iestatījumu **Unassigned**, un kolonnā **Process Status** — iestatījumu **Assign Successful**.

   Lai vienlaikus atlasītu vairākus vienumus, nospiediet Ctrl vai Shift, vai arī klikšķiniet un velciet ar peli.



8. Noklikšķiniet uz **Transmit**.

9. Kad tiek parādīts paroles ievades ekrāns, ievadiet paroli un noklikšķiniet uz **OK**.

   Pārraidiet iestatījumus.

   Piezīme:
   Informācija tiek pārraidīta uz tīkla saskarni, līdz norises josla norāda, ka darbība pabeigta. Neizslēdziet ierīci vai bezvadu adapteru un nesūtiet uz ierīci datus.

10. Ekrānā **Transmitting Settings** noklikšķiniet uz **OK**.

11. Pārbaudiet iestatītās ierīces statusu.

    Ierīcēm, kurām tiek rādīts statuss  vai  : pārbaudiet iestatījumu faila saturu vai pārliecinieties, ka ierīce ir pareizi atsāknēta.

Ikona	Status	Process Status	Skaidrojums
	Setup Complete	Setup Successful	Iestatīšana pabeigta veiksmīgi.
	Setup Complete	Rebooting	Lai iespējotu iestatījumus, pēc informācijas pārsūtīšanas jāatsāknē katra ierīce. Pēc atsāknēšanas tiek veikta pārbaude, lai noteiktu, vai ar ierīci var izveidot savienojumu.
	Setup Complete	Reboot Failed	Pēc iestatījumu pārraides neizdodas pārbaudīt ierīci. Pārbaudiet, vai ierīce ir ieslēgta un vai tā ir veiksmīgi atsāknēta.
	Setup Complete	Searching	Notiek iestatījumu failā norādītās ierīces meklēšana.*
	Setup Complete	Search Failed	Nevar pārbaudīt jau iestatītās ierīces. Pārbaudiet, vai ierīce ir ieslēgta un vai tā ir veiksmīgi atsāknēta.*

    * Tikai, ja redzama iestatījumu informācija.

Saistītā informācija

➡ "EpsonNet Config palaišana — sistēmā Windows" 56. lpp.
➡ "EpsonNet Config palaišana — sistēmā Mac OS" 56. lpp.

IP adreses piešķiršana katrai ierīcei

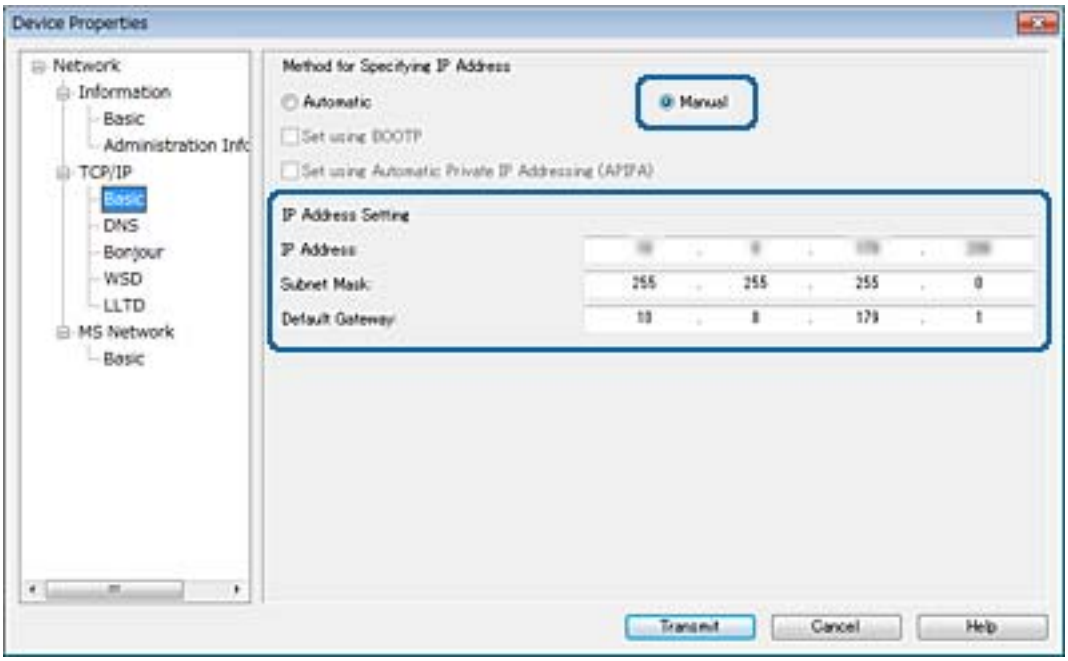
Piešķiriet skenerim IP adresi, lietojot EpsonNet Config.

1. Ieslēdziet skeneri.
2. Pievienojiet skeneri tīklam, izmantojot Ethernet vadu.
3. Palaidiet programmu EpsonNet Config.

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

   Piezīme:
   Ja ir pievienoti vairāki vienāda modeļa skeneri, varat identificēt skeneri, izmantojot MAC adresi.
5. Atlasiet **Network** > **TCP/IP** > **Basic**.

6. Ievadiet adreses laukos **IP Address**, **Subnet Mask** un **Default Gateway**.



Piezīme:
Pievienojot skeneri drošam tīklam, ievadiet statisku adresi.

7. Noklikšķiniet uz **Transmit**.

   Tiks atvērts ekrāns, kas apstiprina informācijas pārraidīšanu.

8. Noklikšķiniet uz **OK**.

   Tiks parādīts pārraidīšanas pabeigšanas ekrāns.

   Piezīme:
   Informācija tiek pārraidīta uz ierīci, tad parādās ziņojums „Konfigurācija pabeigta veiksmīgi". Neizslēdziet ierīci un nesūtiet uz ierīci datus.

9. Noklikšķiniet uz **OK**.

Saistītā informācija

➡ "EpsonNet Config palaišana — sistēmā Windows" 56. lpp.
➡ "EpsonNet Config palaišana — sistēmā Mac OS" 56. lpp.

Porta izmantošana skenerim

Skeneris izmanto turpmāk norādītos portus. Tīkla administratoram jānodrošina piekļuve šiem portiem pēc nepieciešamības.

Pielikums

Sūtītājs (klients)	Pielietojums	Mērķis (serveris)	Protokols	Porta numurs
Skeneris	E-pasta ziņojumu sūtīšana (e-pasta paziņojums)	SMTP serveris	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP pirms SMTP savienojuma (e-pasta paziņojums)	POP serveris	POP3 (TCP)	110
	WSD vadība	Klienta dators	WSD (TCP)	5357
	Datora meklēšana, veicot pašpiegādes skenēšanu programmā Document Capture Pro	Klienta dators	Network Push Scan Discovery	2968
	Uzdevumu informācijas ieguve, veicot pašpiegādes skenēšanu programmā Document Capture Pro	Klienta dators	Network Push Scan	2968
Klienta dators	Atrodiet skeneri, izmantojot programmu, piemēram, EpsonNet Config un skenera draiveri.	Skeneris	ENPC (UDP)	3289
	Apkopojiet un iestatiet MIB informāciju, izmantojot programmu, piemēram, EpsonNet Config un skenera draiveri.	Skeneris	SNMP (UDP)	161
	WSD skenera meklēšana	Skeneris	WS-Discovery (UDP)	3702
	Skenēšanas datu pārsūtīšana no Document Capture Pro	Skeneris	Network Scan (TCP)	1865

Papildu drošības iestatījumi uzņēmumiem

Šajā nodaļā ir aprakstītas papildu drošības funkcijas.

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. Ja izmantojat ierīci vidē ar piekļuvi internetam, risks ir pat vēl lielāks.

Lai novērstu šo risku, Epson ierīces ir aprīkotas ar dažādām drošības tehnoloģijām.

Veiciet ierīcē nepieciešamos iestatījumus atbilstoši klienta informācijas vides apstākļiem.

Nosaukums	Funkcijas veids	Kas jāiestata	Kas tiek novērsts
SSL/TLS sakari	Datora un ierīces savstarpējo sakaru ceļš tiek šifrēts, izmantojot SSL/TLS protokolus. Saturs, veicot saziņu pārlūkprogrammā, tiek aizsargāts.	Iestatiet ierīcē sertificēšanas iestādes parakstītu CA (Certificate Authority) sertifikātu.	Novērsiet iestatījumu informācijas un no datora uz skeneri pārsūtīto drukājamo datu satura noplūdi. Piekļuvi Epson serverim internetā no ierīces var aizsargāt arī, izmantojot aparātprogrammatūras atjauninājumus utt.
IPsec/IP filtrēšana	Varat iestatījumos atļaut no noteikta klienta saņemtu vai noteikta veida datu atdalīšanu. Tā kā IPsec aizsargā datus pa IP pakešu vienībām (šifrēšana un autentificēšana), varat droši veidot sakarus, izmantojot nedrošu 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.
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.
IEEE802.1X	Savienojums atļauts tikai lietotājam, kas ir veicis Ethernet autentifikāciju. Atļauj tikai pilnvarotiem lietotājiem izmantot ierīci.	Autentificēšanas iestatījumi RADIUS serverī (autentificēšanas serverī).	Aizsardzība pret nesankcionētu piekļuvi un ierīces izmantošanu.

Papildu drošības iestatījumi uzņēmumiem

Nosaukums	Funkcijas veids	Kas jāiestata	Kas tiek novērsts
Lasīt ID kartes datus	Varat izmantot ierīci, turot ID karti virs pievienotas autentificētas ierīces. Var ierobežot žurnālu iegūšanu katram lietotājam un ierīcei, kā arī ierīču izmantošanu un katram lietotājam un grupai pieejamās funkcijas.	Savienojiet autentificēšanas ierīci ar ierīci un pēc tam iestatiet autentificēšanas sistēmā lietotāja informāciju.	Nepieļaujiet nesankcionētu lietošanu un ierīces datu viltošanu.

Saistītā informācija

➡ "SSL/TLS sakari ar skeneri" 63. lpp.

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 71. lpp.

➡ "„SNMPv3" protokola izmantošana" 82. lpp.

➡ "Skenera pievienošana IEEE802.1X tīklam" 84. lpp.

Drošības funkciju iestatījumi

Ja ir iestatīta IPsec/IP filtrēšana vai IEEE802.1X, programmai Web Config ieteicams piekļūt, izmantojot SSL/TLS, lai pārraidītu iestatījumu informāciju, nepieļaujot tādus drošības riskus kā manipulācijas ar datiem vai to pārtveršana.

SSL/TLS sakari ar skeneri

Ja servera sertifikāts ir iestatīts, izmantojot SSL/TLS (drošligzdu slāņa/transporta slāņa drošības) sakarus ar skeneri, 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 skeneris. 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" 64. lpp.

➡ "CA parakstīta sertifikāta dzēšana" 67. lpp.

➡ "Pašparakstīta sertifikāta atjaunināšana" 68. 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 lietojumprogrammu Web Config un datoru.

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

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings**. Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.

2. Sadaļā **Generate** noklikšķiniet uz **CSR**.

   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**.

   Tiek parādīts ziņojums par pabeigšanu.

5. Atlasiet **Network Security Settings**. Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.

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

   > ***Svarīga informācija:***
   > *Neģenerējiet CSR no jauna. Ja tā izdarāt, iespējams, nevarēs importēt izsniegtu CA-signed Certificate.*

7. Nosūtiet CSR sertificēšanas iestādei un iegūstiet CA-signed Certificate.

   Ievērojiet katras sertificēšanas iestādes nosūtīšanas un formas noteikumus.

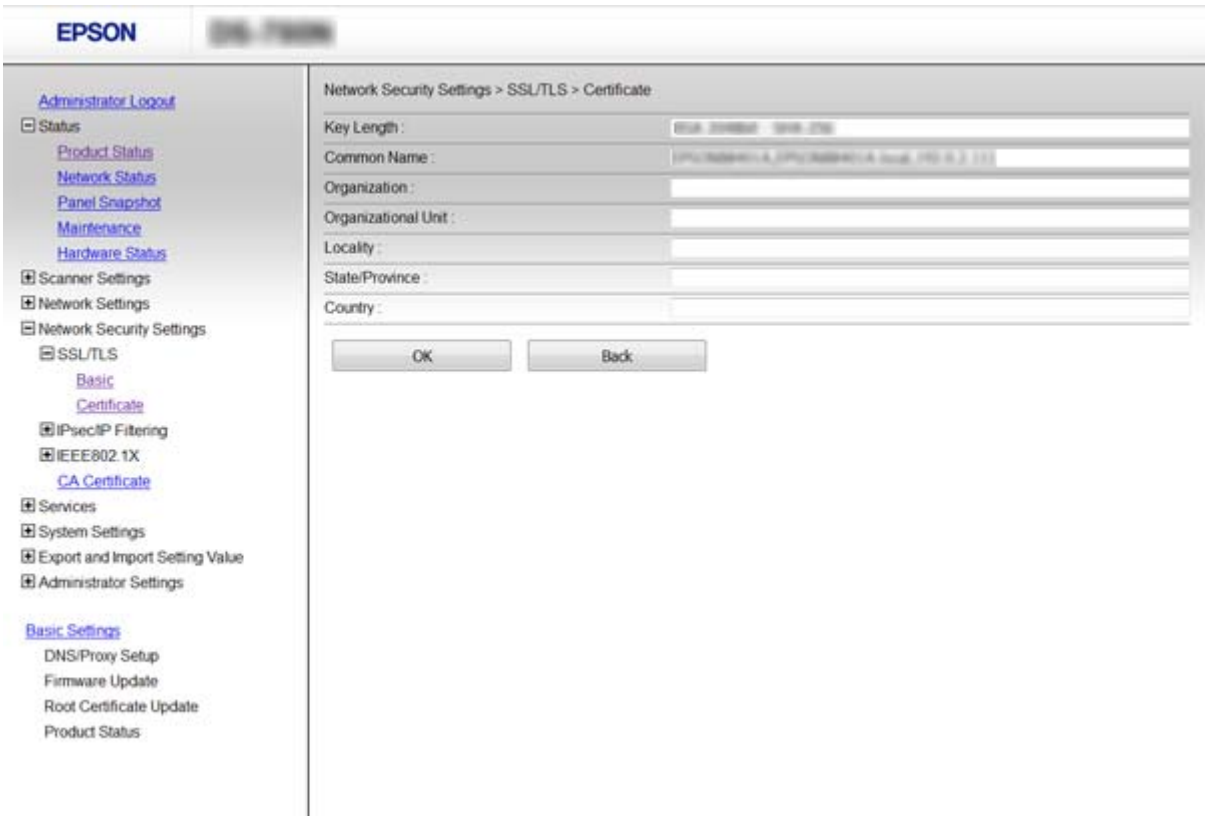
8. Saglabājiet izsniegto CA-signed Certificate datorā, kas pievienots skenerim.

   Kad sertifikāts tiek saglabāts galamērķī, CA-signed Certificate iegūšana ir pabeigta.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "CSR vienumu iestatīšana" 65. lpp.
➡ "CA parakstīta sertifikāta importēšana" 65. lpp.

CSR vienumu iestatīšana



Vienumi	Iestatījumi un skaidrojumi
Key Length	Atlasiet CSR atslēgas garumu.
Common Name	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 Parastais nosaukums: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Ir iespējams ievadīt no 0 līdz 64 ASCII formāta rakstzīmēm (0x20–0x7E). Atšķiramos nosaukumus var atdalīt ar komatiem.
Country	Ievadiet valsts divciparu kodu atbilstīgi standarta ISO-3166 noteikumiem.

Saistītā informācija

➡ "CA parakstīta sertifikāta iegūšana" 64. lpp.

CA parakstīta sertifikāta importēšana

Svarīga informācija:

- *Pārliecinieties, vai skenera datums un laiks ir iestatīts pareizi.*
- *Ja sertifikāts ir iegūts, izmantojot lietojumprogrammā Web Config izveidotu CSR, sertifikātu var importēt vienu reizi.*

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings**. Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.

2. Noklikšķiniet uz **Import**.

   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, izmantojot Web Config
     - ❏ **Private Key**: nekonfigurējiet, jo skenerī ir privāta atslēga.
     - ❏ **Password**: nekonfigurējiet.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: pēc izvēles
   - ❏ PEM/DER formāta sertifikāts, kas iegūts no datora
     - ❏ **Private Key**: jāiestata.
     - ❏ **Password**: nekonfigurējiet.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: pēc izvēles
   - ❏ PKCS#12 formāta sertifikāts, kas iegūts no datora
     - ❏ **Private Key**: nekonfigurējiet.
     - ❏ **Password**: pēc izvēles
     - ❏ **CA Certificate 1**/**CA Certificate 2**: nekonfigurējiet.

4. Noklikšķiniet uz **OK**.

   Tiek parādīts ziņojums par pabeigšanu.

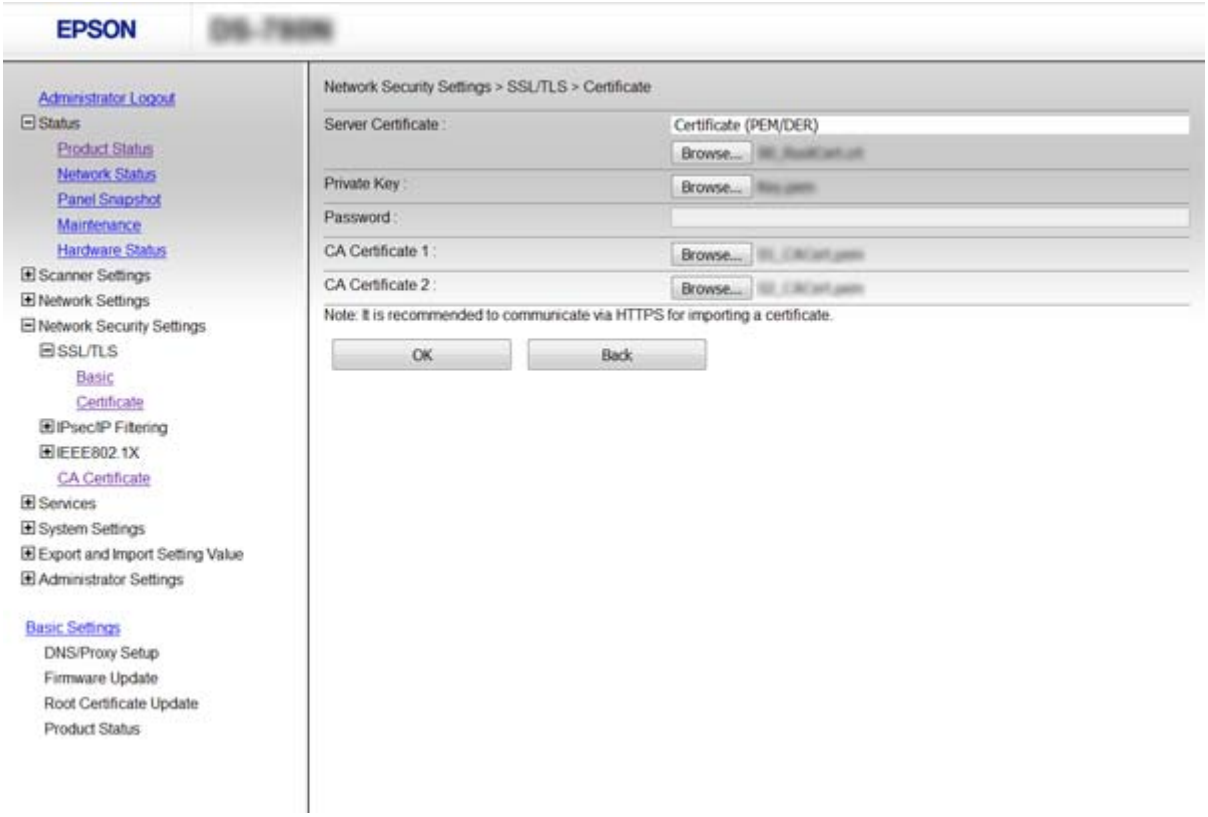
Piezīme:
Lai pārbaudītu sertifikāta informāciju, noklikšķiniet uz ***Confirm****.*

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

➡ "CA parakstīta sertifikāta importēšanas vienumu iestatīšana" 67. lpp.

CA parakstīta sertifikāta importēšanas vienumu iestatīšana



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

Saistītā informācija

➡ "CA parakstīta sertifikāta importēšana" 65. lpp.

CA parakstīta sertifikāta dzēšana

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

> ***Svarīga informācija:***
>
> *Ja sertifikāts ir iegūts, izmantojot lietojumprogrammā Web Config izveidotu CSR, dzēstu sertifikātu nevar importēt vēlreiz. Šādā gadījumā izveidojiet CSR un iegūstiet sertifikātu vēlreiz.*

1. Atveriet programmu Web Config un atlasiet **Network Security Settings**. Pēc tam atlasiet **SSL/TLS** > **Certificate** vai **IPsec/IP Filtering** > **Client Certificate** vai **IEEE802.1X** > **Client Certificate**.
2. Noklikšķiniet uz **Delete**.
3. Apstipriniet, ka vēlaties dzēst sertifikātu, kas parādīts ziņojumā.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Pašparakstīta sertifikāta atjaunināšana

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

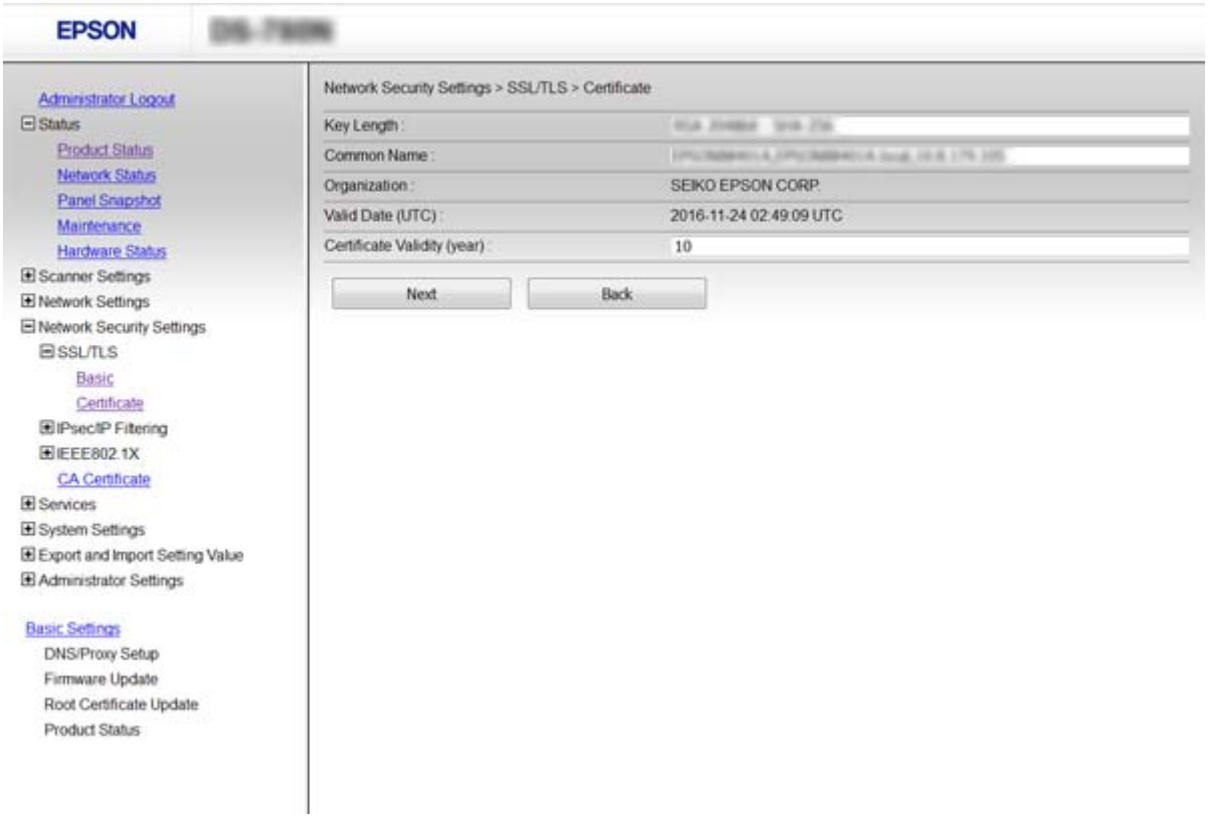
Izmantojiet pašparakstītu sertifikātu īslaicīgi, līdz iegūstat un saņemat CA parakstītu sertifikātu.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Noklikšķiniet uz **Update**.
3. Atveriet **Common Name**.

   Ievadiet IP adresi vai identifikatoru, piemēram, skenera 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**.

   Tiek parādīts apstiprinājuma ziņojums.

6. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Piezīme:
Lai pārbaudītu sertifikāta informāciju, noklikšķiniet uz ***Confirm****.*

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Konfigurējiet CA Certificate

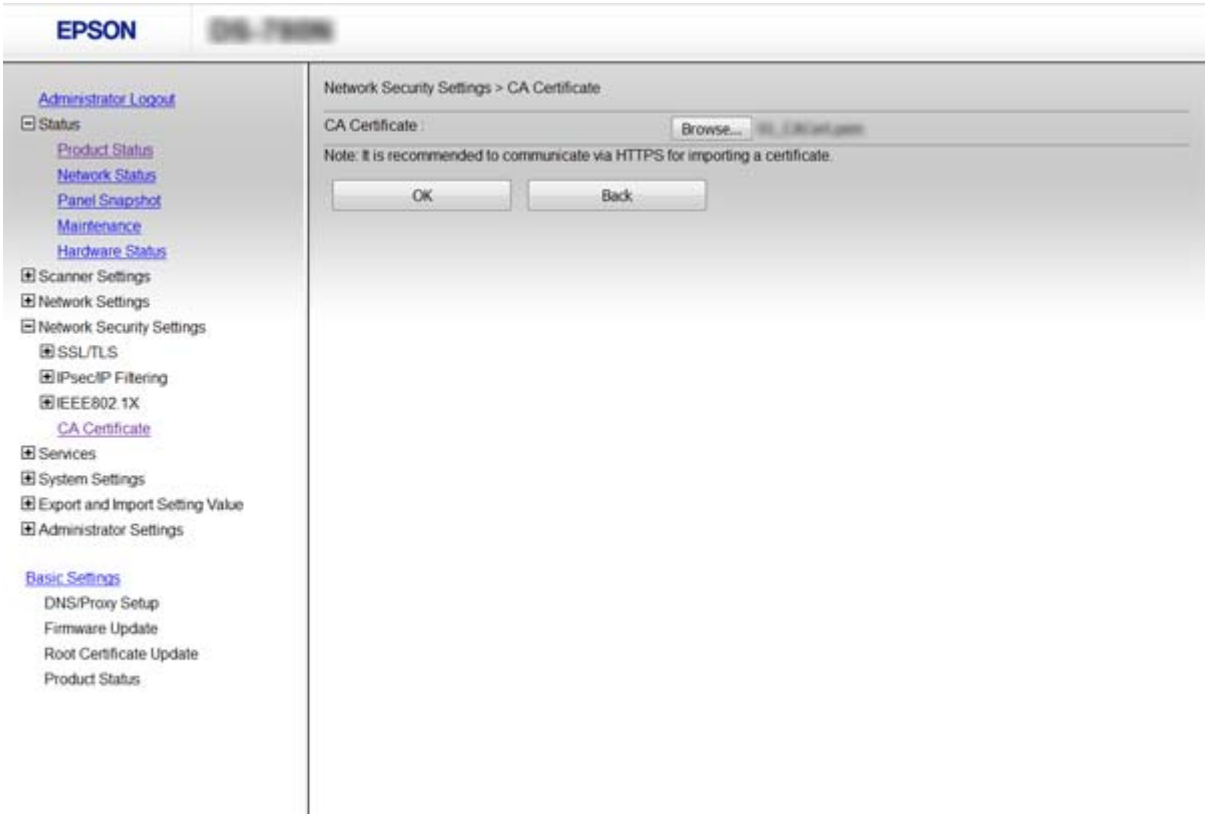
CA Certificate var tikt importēts, parādīts vai dzēsts.

CA Certificate importēšana

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **CA Certificate**.

2. Noklikšķiniet uz **Import**.

3. Norādiet CA Certificate, kuru vēlaties importēt.



4. Noklikšķiniet uz **OK**.

Kad importēšana ir pabeigta, notiek atgriešanās ekrānā **CA Certificate** un tiek parādīts CA Certificate.

Saistītā informācija

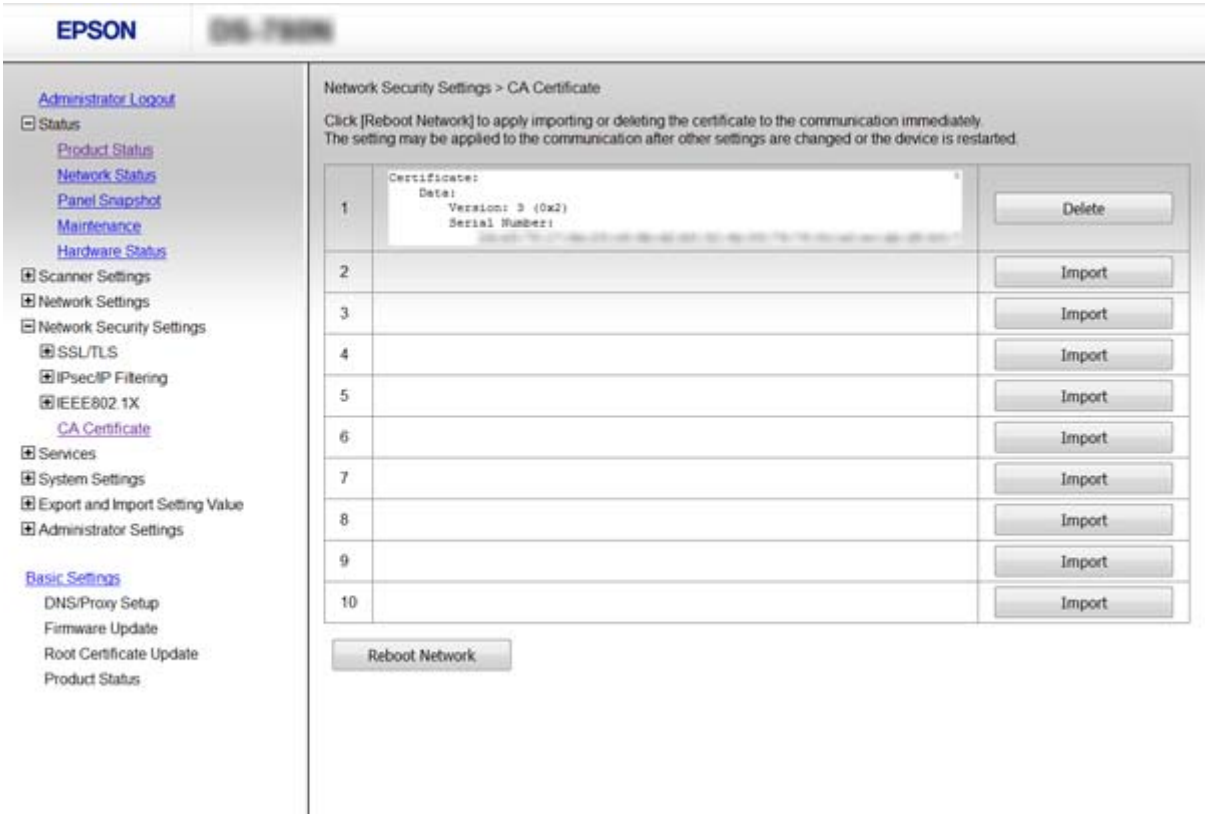
➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

CA Certificate dzēšana

Importēto CA Certificate var dzēst.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **CA Certificate**.

2. Noklikšķiniet uz **Delete** blakus CA Certificate, kuru vēlaties dzēst.



3. Apstipriniet, ka vēlaties dzēst sertifikātu, kas parādīts ziņojumā.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Šifrētie sakari, izmantojot IPsec/IP filtrēšanu

Par IPsec/IP Filtering

Ja skeneris atbalsta IPsec/IP filtrēšanu, var filtrēt trafiku, izmantojot IP adreses, pakalpojumus un portu. Kombinējot filtrēšanas metodes, var konfigurēt skeneri 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 skeneri. 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. Skeneris 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.

Default Policy konfigurēšana

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Ievadiet katra vienuma vērtību.
3. Noklikšķiniet uz **Next**.

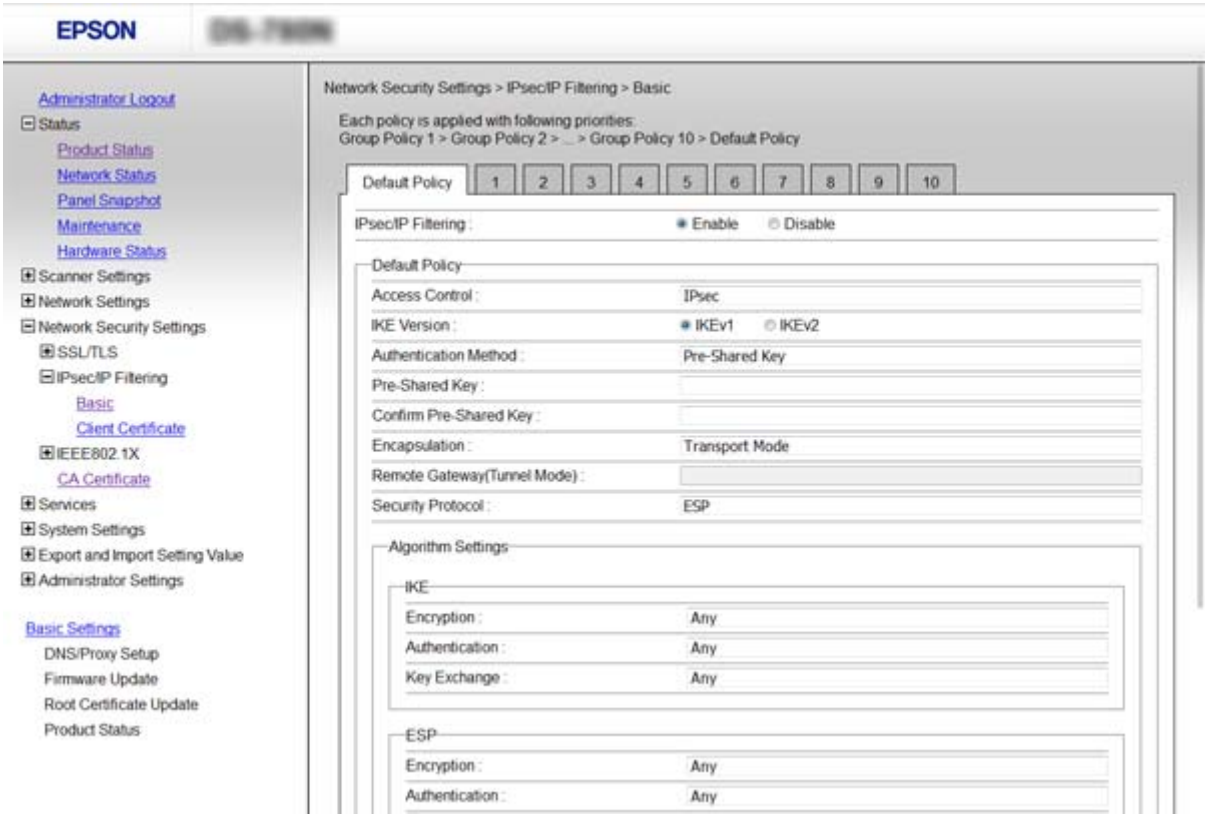
   Tiek parādīts apstiprinājuma ziņojums.
4. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "Sadaļas Default Policy vienumu iestatīšana" 72. lpp.

Sadaļas Default Policy vienumu iestatīšana



Vienumi	Iestatījumi un skaidrojumi
IPsec/IP Filtering	Var iespējot vai atspējot IPsec/IP filtrēšanas funkciju.

Papildu drošības iestatījumi uzņēmumiem

Vienumi	Iestatījumi un skaidrojumi	
Access Control	Konfigurējiet IP pakešu trafika kontroles metodi.	
	Permit Access	Atlasiet šo opciju, lai atļautu konfigurēto IP pakešu tranzītu.
	Refuse Access	Atlasiet šo opciju, lai noraidītu konfigurēto IP pakešu tranzītu.
	IPsec	Atlasiet šo opciju, lai atļautu konfigurēto IPsec pakešu tranzītu.
IKE Version	Atlasiet kā protokola IKE versiju IKEv1 vai IKEv2. Atlasiet kādu no tām atbilstoši ierīcei, ar kuru ir savienots skeneris.	
IKEv1	Izvēloties **IKEv1** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.	
	Authentication Method	Lai atlasītu **Certificate**, ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.
IKEv2	Izvēloties **IKEv2** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.	
Local	Authentication Method	Lai atlasītu **Certificate**, ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
	ID Type	Atlasiet skenera ID veidu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.

Papildu drošības iestatījumi uzņēmumiem

Vienumi	Iestatījumi un skaidrojumi	
Remote	Authentication Method	Lai atlasītu **Certificate**, ir jābūt iepriekš iegūtam un importētam CA parakstītam sertifikātam.
	ID Type	Izvēlieties autentificējamās ierīces ID veidu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.
Encapsulation	Atlasot **IPsec** kā **Access Control** iestatījumu, jākonfigurē iekapsulēšanas režīms.	
	Transport Mode	Atlasiet šo opciju, ja izmantojat skeneri tikai vienā lokālajā tīklā (LAN). 4. slāņa un jaunākas IP paketes tiek šifrētas.
	Tunnel Mode	Atlasiet šo opciju, ja izmantojat skeneri tīklā ar interneta izmantošanas iespēju, piemēram, IPsec-VPN tīklā. Tiek šifrētas IP pakešu galvenes un dati.
Remote Gateway(Tunnel Mode)	Ja vienuma **Encapsulation** iestatījums ir **Tunnel Mode**, ievadiet vārtejas adresi, kuras garums ir no 1 līdz 39 rakstzīmēm.	
Security Protocol	**IPsec** kā **Access Control** iestatījums, atlasiet opciju.	
	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.
Algorithm Settings		
IKE	Encryption	Atlasiet IKE šifrēšanas algoritmu. Vienumi ir atkarīgi no IKE versijas.
	Authentication	Atlasiet IKE autentificēšanas algoritmu.
	Key Exchange	Atlasiet IKE atslēgu apmaiņas algoritmu. Vienumi ir atkarīgi no IKE versijas.

Vienumi	Iestatījumi un skaidrojumi	
ESP	Encryption	Atlasiet ESP šifrēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
	Authentication	Atlasiet ESP autentificēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
AH	Authentication	Atlasiet AH šifrēšanas algoritmu. Tas ir pieejams, kad **AH** ir izvēlēts kā **Security Protocol** iestatījums.

Saistītā informācija

➡ "Default Policy konfigurēšana" 72. lpp.

Group Policy konfigurēšana

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Noklikšķiniet uz konfigurējamās numurētās cilnes.
3. Ievadiet katra vienuma vērtību.
4. Noklikšķiniet uz **Next**.

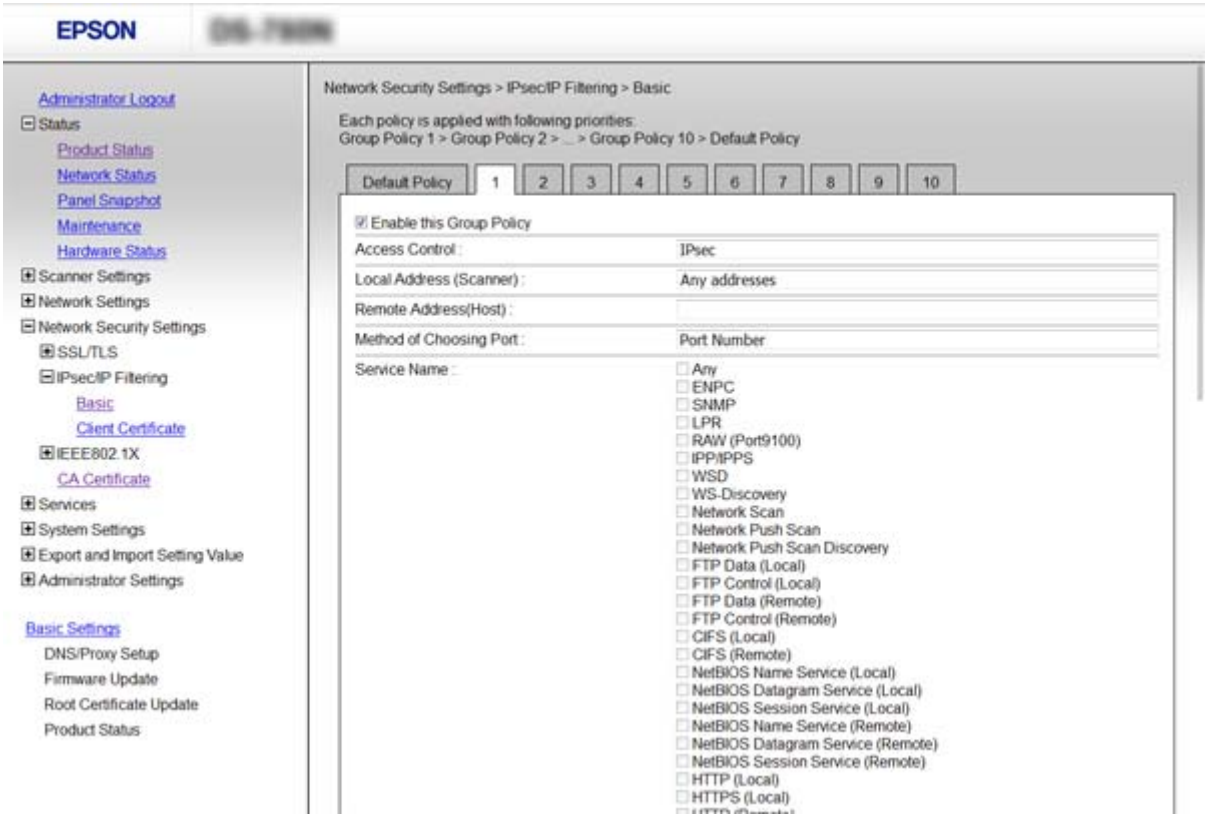
   Tiek parādīts apstiprinājuma ziņojums.
5. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "Sadaļas Group Policy vienumu iestatīšana" 76. lpp.

Sadaļas Group Policy vienumu iestatīšana



Vienumi	Iestatījumi un skaidrojumi	
Enable this Group Policy	Var iespējot vai atspējot grupas politiku.	
Access Control	Konfigurējiet IP pakešu trafika kontroles metodi.	
	Permit Access	Atlasiet šo opciju, lai atļautu konfigurēto IP pakešu tranzītu.
	Refuse Access	Atlasiet šo opciju, lai noraidītu konfigurēto IP pakešu tranzītu.
	IPsec	Atlasiet šo opciju, lai atļautu konfigurēto IPsec pakešu tranzītu.
Local Address (Scanner)	Izvēlieties IPv4 vai IPv6 adresi, kas atbilst jūsu tīkla videi. Ja IP adrese netiek piešķirta automātiski, varat izvēlēties **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Lai kontrolētu piekļuvi, ievadiet ierīces IP adresi. IP adresei jābūt 43 rakstzīmes garai vai īsākai. 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.*	
Method of Choosing Port	Atlasiet portu norādīšanas metodi.	
Service Name	Atlasot **Service Name** kā **Method of Choosing Port** iestatījumu, jāizvēlas kāda no opcijām.	

Papildu drošības iestatījumi uzņēmumiem

Vienumi	Iestatījumi un skaidrojumi	
Transport Protocol	Atlasot **Port Number** kā **Method of Choosing Port** iestatījumu, jākonfigurē iekapsulēšanas režīms.	
	Any Protocol	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	Atlasot **Port Number** kā **Method of Choosing Port** iestatījumu, un **TCP** vai **UDP** — kā **Transport Protocol** 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	Atlasot **Port Number** kā **Method of Choosing Port** iestatījumu, un **TCP** vai **UDP** — kā **Transport Protocol** 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.	
IKE Version	Atlasiet kā protokola IKE versiju IKEv1 vai IKEv2. Atlasiet kādu no tām atbilstoši ierīcei, ar kuru ir savienots skeneris.	
IKEv1	Izvēloties **IKEv1** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.	
	Authentication Method	Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.
IKEv2	Izvēloties **IKEv2** kā **IKE Version** iestatījumu, tiek parādīti turpmāk minētie vienumi.	

Papildu drošības iestatījumi uzņēmumiem

Vienumi	Iestatījumi un skaidrojumi	
Local	Authentication Method	Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
	ID Type	Atlasiet skenera ID veidu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.
Remote	Authentication Method	Atlasot **IPsec** kā **Access Control** iestatījumu, jāizvēlas kāda no opcijām. Izmantotais sertifikāts ir kopīgs ar noklusējuma politikas izmantoto.
	ID Type	Izvēlieties autentificējamās ierīces ID veidu.
	ID	Ievadiet ID veidam atbilstošu skenera ID. Pirmā rakstzīme nedrīkst būt „@", „#" vai „=". **Distinguished Name**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „=". **IP Address**: ievadiet IPv4 vai IPv6 formātu. **FQDN**: ievadiet 1–255 rakstzīmju kombināciju, izmantojot rakstzīmes A–Z, a–z, 0–9, „-" un punktu (.). **Email Address**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Jāiekļauj rakstzīme „@". **Key ID**: ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.
	Pre-Shared Key	Izvēloties vienuma **Authentication Method** iestatījumu **Pre-Shared Key**, ievadiet iepriekš koplietotu atslēgu, kuras garums ir no 1 līdz 127 rakstzīmēm.
	Confirm Pre-Shared Key	Lai apstiprinātu, ievadiet konfigurēto atslēgu.

Papildu drošības iestatījumi uzņēmumiem

Vienumi	Iestatījumi un skaidrojumi	
Encapsulation	Atlasot **IPsec** kā **Access Control** iestatījumu, jākonfigurē iekapsulēšanas režīms.	
	Transport Mode	Atlasiet šo opciju, ja izmantojat skeneri tikai vienā lokālajā tīklā (LAN). 4. slāņa un jaunākas IP paketes tiek šifrētas.
	Tunnel Mode	Atlasiet šo opciju, ja izmantojat skeneri tīklā ar interneta izmantošanas iespēju, piemēram, IPsec-VPN tīklā. Tiek šifrētas IP pakešu galvenes un dati.
Remote Gateway(Tunnel Mode)	Ja vienuma **Encapsulation** iestatījums ir **Tunnel Mode**, ievadiet vārtejas adresi, kuras garums ir no 1 līdz 39 rakstzīmēm.	
Security Protocol	Atlasot **IPsec** kā **Access Control** 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.
Algorithm Settings		
IKE	Encryption	Atlasiet IKE šifrēšanas algoritmu. Vienumi ir atkarīgi no IKE versijas.
	Authentication	Atlasiet IKE autentificēšanas algoritmu.
	Key Exchange	Atlasiet IKE atslēgu apmaiņas algoritmu. Vienumi ir atkarīgi no IKE versijas.
ESP	Encryption	Atlasiet ESP šifrēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
	Authentication	Atlasiet ESP autentificēšanas algoritmu. Tas ir pieejams, kad **ESP** ir izvēlēts kā **Security Protocol** iestatījums.
AH	Authentication	Atlasiet AH autentificēšanas algoritmu. Tas ir pieejams, kad **AH** ir izvēlēts kā **Security Protocol** iestatījums.

Saistītā informācija

➡ "Group Policy konfigurēšana" 75. lpp.

➡ "Local Address (Scanner) un Remote Address(Host) kombinācija, Group Policy" 79. lpp.

➡ "Norādes uz pakalpojuma nosaukumiem grupas politikā" 80. lpp.

Local Address (Scanner) un Remote Address(Host) kombinācija, Group Policy

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

Remote Address(Host) iestatīšana	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Tukšs	✓	✓	✓

*1 Ja izvēlas **IPsec** kā **Access Control** iestatījumu, nevar norādīt prefiksa garumu.

*2 Ja izvēlas **IPsec** kā **Access Control** 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
Any	–	–	–	Visi pakalpojumi
ENPC	UDP	3289	Jebkurš ports	Skenera meklēšana, izmantojot tādas programmas kā EpsonNet Config un skenera draiverus
SNMP	UDP	161	Jebkurš ports	MIB iegūšana un konfigurēšana, izmantojot tādas programmas kā EpsonNet Config, un Epson skenera draiveri
WSD	TCP	Jebkurš ports	5357	WSD vadība
WS-Discovery	UDP	3702	Jebkurš ports	Skenera meklēšana no WSD
Network Scan	TCP	1865	Jebkurš ports	Skenēšanas datu pārsūtīšana no Document Capture Pro
Network Push Scan Discovery	UDP	2968	Jebkurš ports	Datora meklēšana no skenera.
Network Push Scan	TCP	Jebkurš ports	2968	Pašpiegādes skenēšanas darba informācijas ieguve programmā Document Capture Pro vai Document Capture
HTTP (Local)	TCP	80	Jebkurš ports	HTTP(S) serveris (Web Config un WSD datu pārsūtīšana)
HTTPS (Local)	TCP	443	Jebkurš ports	
HTTP (Remote)	TCP	Jebkurš ports	80	HTTP(S) klients (savstarpējie sakari aparātprogrammatūras un saknes sertifikāta atjaunināšanai)
HTTPS (Remote)	TCP	Jebkurš ports	443	

IPsec/IP Filtering konfigurāciju piemēri

Tikai IPsec pakešu saņemšana

Piemērā skaidrota tikai noklusējuma politikas konfigurēšana.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: ievadiet līdz 127 rakstzīmēm.

Group Policy:

nekonfigurējiet.

Skenējuma pieņemšana, izmantojot Epson Scan 2 un skenera iestatījumus

Šajā piemērā tiek atļauta skenējumu datu un skenera konfigurācijas pārraide no norādītajiem pakalpojumiem.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: atzīmējiet izvēles rūtiņu.

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

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

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

❏ **Service Name**: atzīmējiet izvēles rūtiņas **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** un **HTTPS (Local)**.

Piekļuves piešķiršana tikai norādītajai IP adresei

Šajā piemērā redzams, kā atļaut piekļuvi skenerim no norādītas IP adreses.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: atzīmējiet izvēles rūtiņu.

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

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

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

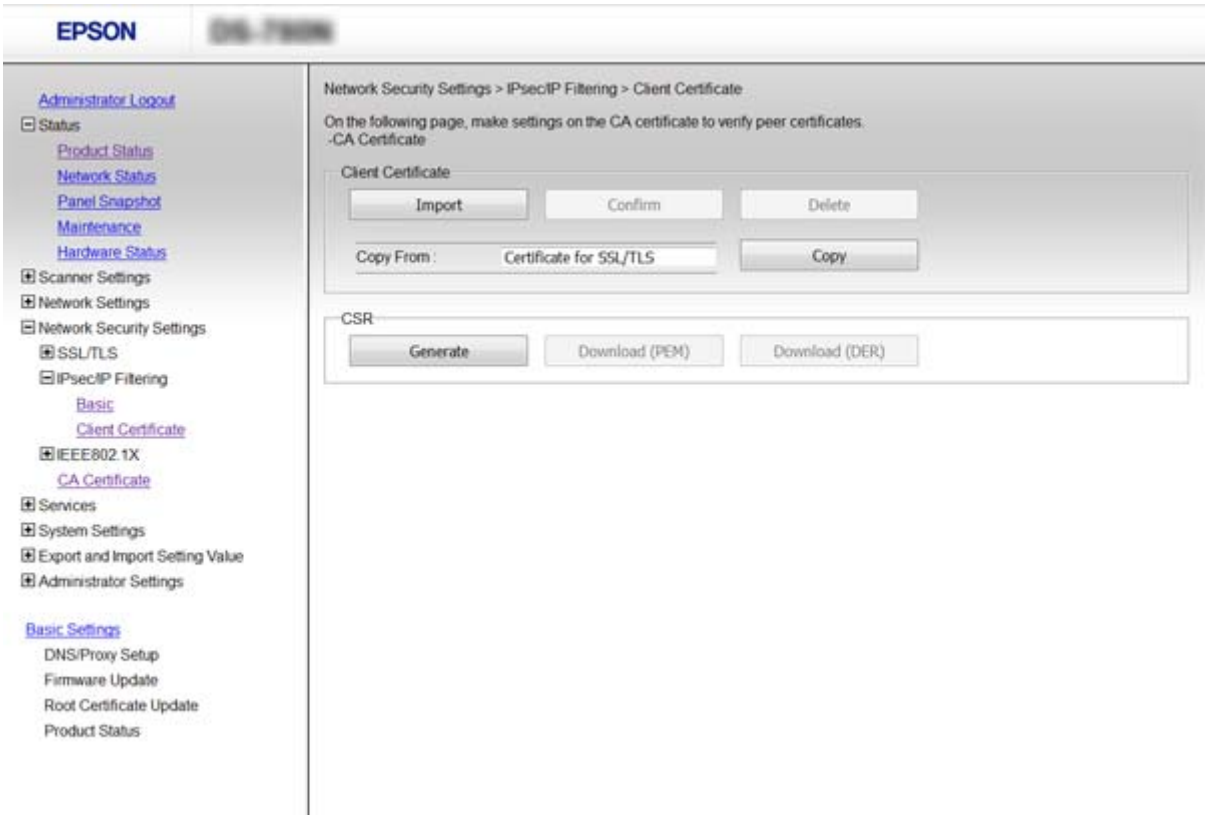
IPsec/IP Filtering tīkla sertifikāta konfigurēšana

Konfigurējiet klienta sertifikātu IPsec/IP filtrēšanai. Ja vēlaties konfigurēt sertificēšanas iestādi, dodieties uz **CA Certificate**.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importējiet sertifikātu laukā **Client Certificate**.

   Ja jau esat importējis sertifikātu, ko izdevusi sertificēšanas iestāde IEEE802.1X vai SSL/TLS tīklā, var nokopēt sertifikātu un lietot to IPsec/IP filtrēšanā. Lai kopētu to, atlasiet sertifikātu no **Copy From** un pēc tam noklikšķiniet uz **Copy**.



Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

➡ "CA parakstīta sertifikāta iegūšana un importēšana" 64. lpp.

„SNMPv3" protokola 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 skeneris atbalsta protokolu SNMPv3, iespējams uzraudzīt un pārvaldīt piekļuvi skenerim.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Services** > **Protocol**.
2. Ievadiet katra **SNMPv3 Settings** vienuma vērtību.
3. Noklikšķiniet uz **Next**.

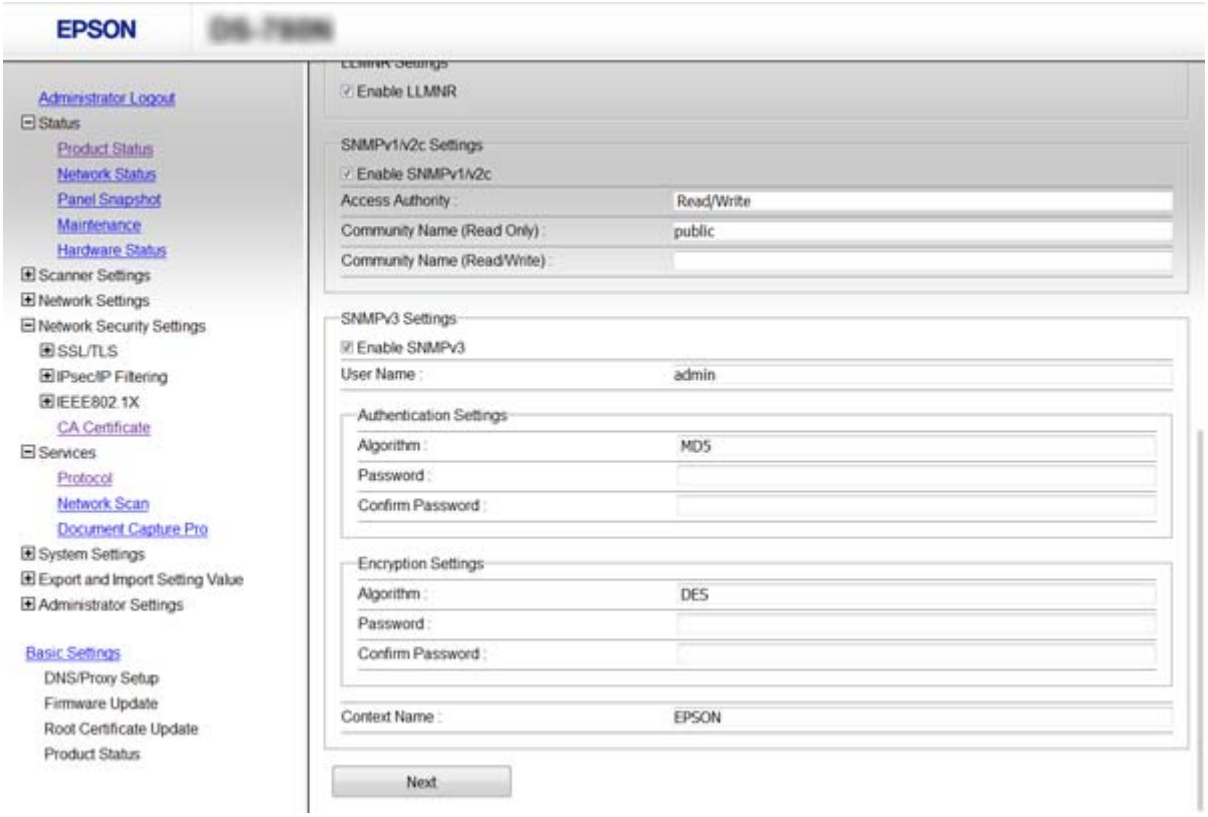
   Tiek parādīts apstiprinājuma ziņojums.
4. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "„SNMPv3” vienumu iestatīšana" 83. lpp.

„SNMPv3” vienumu iestatīšana



Vienumi	Iestatījumi un skaidrojums
Enable SNMPv3	„SNMPv3" ir iespējots, ja izvēles rūtiņa ir iezīmēta.
User Name	Ievadiet no 1 līdz 32 rakstzīmēm, izmantojot 1 bita rakstzīmes.
Authentication Settings	
Algorithm	Atlasiet autentifikācijas algoritmu.
Password	Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20-0x7E).
Confirm Password	Apstiprinājumam ievadiet savu konfigurēto paroli.
Encryption Settings	
Algorithm	Atlasiet šifrēšanas algoritmu.
Password	Ievadiet no 8 līdz 32 ASCII rakstzīmēm (0x20-0x7E).
Confirm Password	Apstiprinājumam ievadiet savu konfigurēto paroli.
Context Name	Ievadiet no 1 līdz 32 rakstzīmēm, izmantojot 1 bita rakstzīmes.

Saistītā informācija

➡ "SNMPv3 konfigurēšana" 83. lpp.

Skenera pievienošana IEEE802.1X tīklam

IEEE802.1X tīkla konfigurēšana

Ja skeneris atbalsta IEEE802.1X, skeneri var izmantot tīklā bez autentifikācijas, kas pievienots „RADIUS" serverim un centrmezglam kā autentificētājs.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Ievadiet katra vienuma vērtību.
3. Noklikšķiniet uz **Next**.

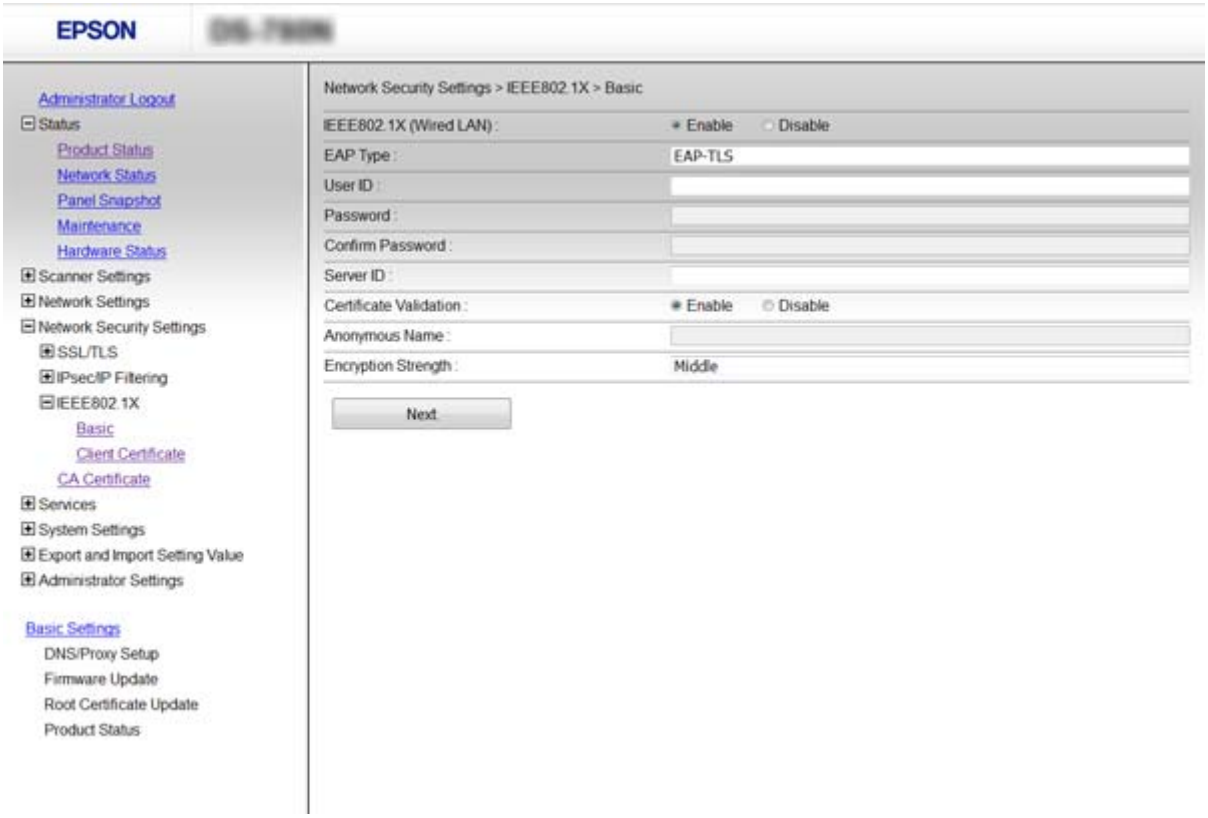
   Tiek parādīts apstiprinājuma ziņojums.
4. Noklikšķiniet uz **OK**.

   Skeneris tiek atjaunināts.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.
➡ "IEEE802.1X tīkla vienumu iestatīšana" 85. lpp.
➡ "Pēc IEEE802.1X konfigurēšanas nevar piekļūt printerim vai skenerim" 89. lpp.

IEEE802.1X tīkla vienumu iestatīšana



Vienumi	Iestatījumi un skaidrojumi	
IEEE802.1X (Wired LAN)	Varat iespējot vai atspējot lapas iestatījumus (**IEEE802.1X** > **Basic**) IEEE802.1X tīklam (vadu LAN).	
EAP Type	Atlasiet skenera un RADIUS servera autentifikācijas metodes opciju.	
	EAP-TLS	Ir jāiegūst un jāimportē sertifikāts ar CA parakstu.
	PEAP-TLS	
	PEAP/MSCHAPv2	Ir jākonfigurē parole.
User ID	Konfigurējiet ID, kas jāizmanto RADIUS servera autentifikācijai. Ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.	
Password	Konfigurējiet paroli, lai autentificētu skeneri. Ievadiet no 1 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm. Ja izmantojat Windows serveri kā RADIUS serveri, var ievadīt līdz 127 rakstzīmēm.	
Confirm Password	Lai apstiprinātu, ievadiet konfigurēto paroli.	
Server ID	Servera ID var konfigurēt noteikta RADIUS servera autentificēšanai. Autentificētājs pārbauda, vai servera sertifikāta, ko sūta RADIUS serveris, laukā subject/subjectAltName ir ietverts servera ID. Ievadiet no 0 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.	
Certificate Validation	Var iestatīt sertifikāta validāciju neatkarīgi no autentifikācijas metodes. Importējiet sertifikātu laukā **CA Certificate**.	

Vienumi	Iestatījumi un skaidrojumi	
Anonymous Name	Opcijas **PEAP-TLS** vietā atlasot **PEAP/MSCHAPv2** vai **Authentication Method**, var konfigurēt anonīmu nosaukumu, kas „PEAP" autentifikācijas 1. posmā jāizmanto lietotāja ID vietā. Ievadiet no 0 līdz 128 viena baita ASCII (0x20–0x7E) rakstzīmēm.	
Encryption Strength	Var atlasīt vienu no turpmāk norādītajām iespējām.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Saistītā informācija

➡ "IEEE802.1X tīkla konfigurēšana" 84. lpp.

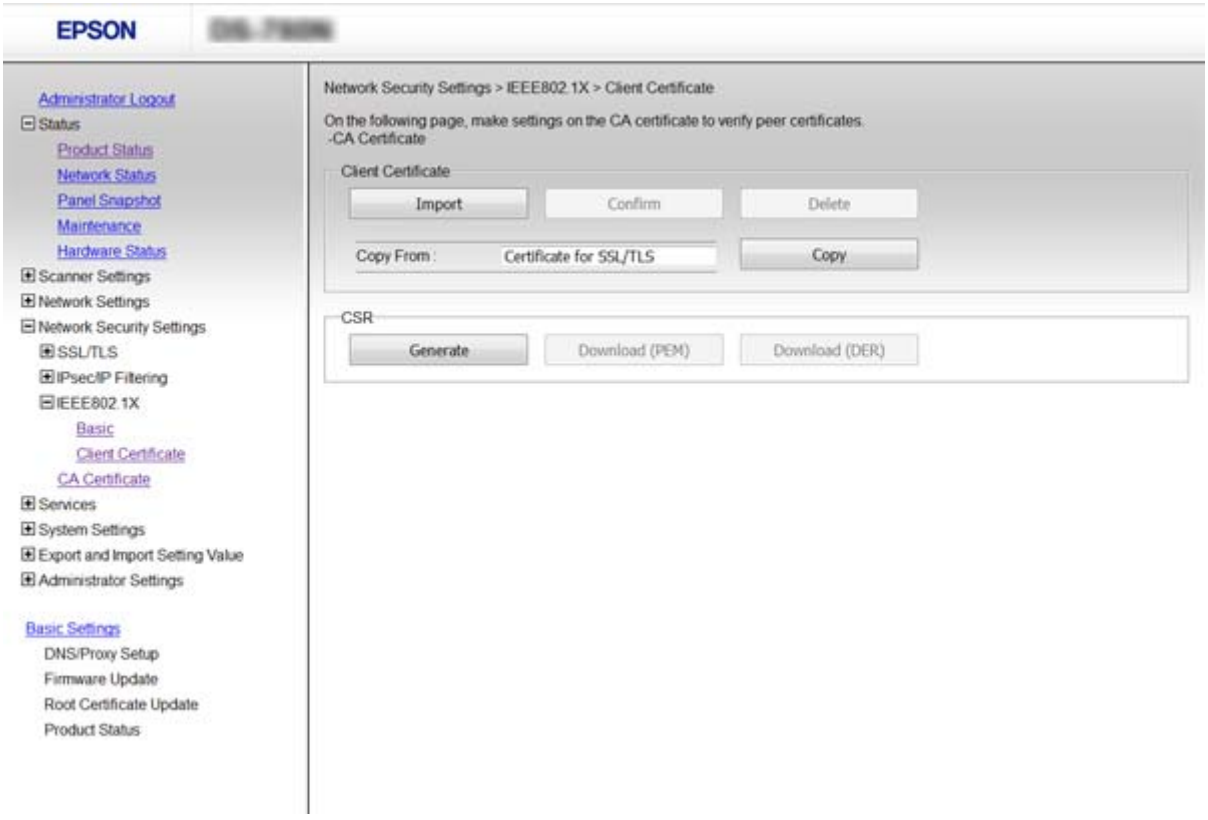
IEEE802.1X tīkla sertifikāta konfigurēšana

Konfigurējiet klienta sertifikātu IEEE802.1X tīklam. Ja vēlaties konfigurēt sertificēšanas iestādes sertifikātu, izvēlieties **CA Certificate**.

1. Atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. Ievadiet sertifikātu laukā **Client Certificate**.

   Ja sertifikātu izdevusi sertificēšanas iestāde, tad sertifikātu var kopēt. Lai kopētu to, atlasiet sertifikātu no **Copy From** un pēc tam noklikšķiniet uz **Copy**.



Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

➡ "CA parakstīta sertifikāta iegūšana un importēšana" 64. lpp.

Drošības papildu iestatījumu problēmu risināšana

Drošības iestatījumu atjaunošana

Izveidojot augstas drošības vidi, piemēram, izmantojot IPsec/IP filtrēšanu vai IEEE802.1X, 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 vadības paneli

Izmantojot skenera vadības paneli, var atspējot IPsec/IP filtrēšanu vai IEEE802.1X.

1. Pieskarieties **Iestatījumi** > **Tīkla iestatījumi**.
2. Pieskarieties **Mainīt iestatījumus**.
3. Pieskarieties vienumiem, kurus vēlaties atspējot.
   - ❏ **IPsec/IP filtrēšana**
   - ❏ **IEEE802.1X**
4. Kad tiek parādīts ziņojums par pabeigšanu, pieskarieties **Turpināt**.

Drošības funkcijas atjaunošana, izmantojot Web Config

IEEE802.1X gadījumā ierīces tīklā var netikt atpazītas. Šādā gadījumā atspējojiet funkciju, izmantojot skenera vadības paneli.

IPsec/IP filtrēšanas gadījumā funkciju var atspējot, ja var piekļūt ierīcei no datora.

IPsec/IP filtrēšanas atspējošana, izmantojot Web Config

1. Atveriet programmu Web Config un atlasiet **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Atlasiet **Disable** kā **IPsec/IP Filtering** iestatījumu sadaļā **Default Policy**.
3. Noklikšķiniet uz **Next** un notīriet opciju **Enable this Group Policy** visām grupu politikām.
4. Noklikšķiniet uz **OK**.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Tīkla drošības funkciju lietošanas problēmas

Aizmirsta iepriekš koplietota atslēga

Vēlreiz konfigurējiet atslēgu, izmantojot Web Config.

Lai mainītu atslēgu, atveriet lietojumprogrammu Web Config un atlasiet **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** vai **Group Policy**.

Mainot iepriekš koplietotu atslēgu, konfigurējiet datoriem paredzētu iepriekš koplietotu atslēgu.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

Nevar izveidot sakarus, izmantojot IPsec

Vai datora iestatījumos netiek izmantots neatbalstīts algoritms?

Skeneris atbalsta turpmāk norādītos algoritmus.

Drošības metodes	Algoritmi
IKE šifrēšanas algoritms	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE autentificēšanas algoritms	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE atslēgu apmaiņas algoritms	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP šifrēšanas algoritms	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP autentificēšanas algoritms	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH autentificēšanas algoritms	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* pieejams tikai protokolam IKEv2

Saistītā informācija

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 71. lpp.

Pēkšņi nevar izveidot sakarus

Vai skenera IP adrese ir nederīga vai tā mainīta?

Atspējojiet IPsec, izmantojot skenera vadības paneli.

Ja nav atjaunināts DHCP, veiciet atsāknēšanu vai arī, ja nav atjaunināta vai iegūta IPv6 adrese, programmā Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) var netikt atrasta reģistrētā skenera IP adrese.

Izmantojiet statisku IP adresi.

Vai datora IP adrese ir nederīga vai tā mainīta?

Atspējojiet IPsec, izmantojot skenera vadības paneli.

Ja nav atjaunināts DHCP, veiciet atsāknēšanu vai arī, ja nav atjaunināta vai iegūta IPv6 adrese, programmā Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) var netikt atrasta reģistrētā skenera IP adrese.

Izmantojiet statisku IP adresi.

Saistītā informācija

➡ "Piekļuve lietojumprogrammai Web Config" 23. lpp.

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 71. lpp.

Nevar izveidot savienojumu pēc IPsec/IP filtrēšanas konfigurācijas

Iespējams, nav pareiza iestatītā vērtība.

Skenera vadības panelī atspējojiet IPsec/IP filtrēšanu. Pievienojiet printeri datoram un vēlreiz veiciet IPsec/IP filtrēšanas iestatījumus.

Saistītā informācija

➡ "Šifrētie sakari, izmantojot IPsec/IP filtrēšanu" 71. lpp.

Pēc IEEE802.1X konfigurēšanas nevar piekļūt printerim vai skenerim

Iespējams, ir nepareizi iestatījumi.

Skenera vadības panelī atspējojiet IEEE802.1X. Pievienojiet skeneri datoram un tad vēlreiz konfigurējiet IEEE802.1X.

Saistītā informācija

➡ "IEEE802.1X tīkla konfigurēšana" 84. 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 skenerī 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" 65. lpp.

Nevar atjaunināt pašparakstītu sertifikātu

Vai ir ievadīta vērtība laukā „Common Name”?

Jābūt ievadītai vērtībai laukā **Common Name**.

Vai laukā „Common Name” 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” ir izmantots komats vai atstarpe?

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

Saistītā informācija

➡ "Pašparakstīta sertifikāta atjaunināšana" 68. lpp.

Nevar izveidot CSR

Vai ir ievadīta vērtība laukā „Common Name”?

Jābūt ievadītai vērtībai laukā **Common Name**.

Vai laukā Common Name, Organization, Organizational Unit, Locality, State/Province ir ievadītas neatbalstītas rakstzīmes? Netiek atbalstīta, piemēram, japāņu valoda.

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

Vai laukā „Common Name” ir izmantots komats vai atstarpe?

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

Saistītā informācija

➡ "CA parakstīta sertifikāta iegūšana" 64. lpp.

Tiek parādīts ar ciparsertifikāta lietošanu saistīts brīdinājums

Ziņojumi	Cēlonis/risinājums
Enter a Server Certificate.	**Cēlonis:** Nav atlasīts importējamais fails. **Risinājums:** Atlasiet failu un noklikšķiniet uz **Import**.
CA Certificate 1 is not entered.	**Cēlonis:** Nav ievadīts 1. CA sertifikāts; ievadīts tikai 2. CA sertifikāts. **Risinājums:** Vispirms importējiet 1. CA sertifikātu.
Invalid value below.	**Cēlonis:** Faila ceļā un/vai parolē ietvertas neatbalstītas rakstzīmes. **Risinājums:** Pārliecinieties, vai vienuma rakstzīmes ir ievadītas pareizi.
Invalid date and time.	**Cēlonis:** Nav iestatīts skenera datums un laiks. **Risinājums:** Iestatiet datumu un laiku, izmantojot Web Config vai EpsonNet Config.
Invalid password.	**Cēlonis:** Iestatītā CA sertifikāta parole nesakrīt ar ievadīto paroli. **Risinājums:** Ievadiet pareizu paroli.
Invalid file.	**Cēlonis:** Netiek importēts X509 formāta sertifikāta fails. **Risinājums:** Pārliecinieties, vai atlasāt pareizo sertifikāta failu, kas saņemts no uzticamas sertificēšanas iestādes.
	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.

Ziņojumi	Cēlonis/risinājums
Cannot use the Server Certificates that include more than three CA certificates.	**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 the product.	**Cēlonis:** Beidzies sertifikāta derīguma termiņš. **Risinājums:** ❏ Ja beidzies sertifikāta derīguma termiņš, iegūstiet un importējiet jaunu sertifikātu. ❏ Ja sertifikāta derīguma termiņš nav beidzies, pārliecinieties, vai skenera datums un laiks ir iestatīts pareizi.
Private key is required.	**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.
Setup failed.	**Cēlonis:** Nevar pabeigt konfigurēšanu, jo nav izveidoti skenera un datora sakari, vai failu nevar nolasīt kļūdu dēļ. **Risinājums:** Pēc norādītā faila un sakaru pārbaudes importējiet failu vēlreiz.

Saistītā informācija

➡ "Par ciparsertifikātiem" 63. 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 lietotnē „Web Config” izveidotu CSR, dzēstu sertifikātu nevar importēt vēlreiz. Izveidojiet CSR un iegūstiet jaunu sertifikātu.

Papildu drošības iestatījumi uzņēmumiem

Saistītā informācija

➡ "CA parakstīta sertifikāta dzēšana" 67. lpp.
➡ "CA parakstīta sertifikāta importēšana" 65. lpp.