EPSON
EXCEED YOUR VISION

Administratoriaus vadovas

NPD5668-00 LT

Turinys

Autorių teisės

Prekės ženklai

Apie šią instrukciją

Ženklai ir simboliai. 6
Šiame vadove naudojami aprašymai. 6
Operacinių sistemų nuorodos. 6

Įvadas

Vadovo komponentas. 8
Naudotojo vadove vartojamų terminų aprašai. 8

Pasiruošimas

Skaitytuvo nustatymų ir valdymo srautas. 10
Tinklo aplinkos pavyzdys. 11
Skaitytuvo ryšio nustatymo pavyzdžio pristatymas. 11
Ryšio su tinklu paruošimas. 12
Informacijos apie ryšio nustatymą rinkimas. . . . 12
Skaitytuvo techniniai duomenys. 12
Prievado numerio naudojimas. 13
IP adreso priskyrimo būdai. 13
DNS serveris ir tarpinis serveris. 13
Tinklo ryšio nustatymo būdas. 13

Ryšys

Prijungimas prie tinklo. 15
Prisijungimas prie tinklo valdymo skydelyje. . . . 15
Prisijungimas prie tinklo naudojant diegimo programą. 19

Funkcijos nustatymai

Nustatymo programinė įranga. 22
Web Config (Įrenginiui skirtas tinklalapis). 22
Skenerio funkcijų naudojimas. 24
Nuskaitymas iš kompiuterio. 24
Nuskaitymas naudojant valdymo skydelį. 26
Sistemos nustatymų pasirinkimas. 28
Sistemos nustatymas valdymo skydelyje. 28
Sistemos nustatymas naudojant tinklo konfigūravimo langą. 30

Pagrindiniai saugumo nustatymai

Pagrindinių saugumo funkcijų įvadas. 32
Administratoriaus slaptažodžio konfigūravimas. . . 33
Administratoriaus slaptažodžio konfigūravimas valdymo skydelyje. 33
Administratoriaus slaptažodžio konfigūravimas naudojant Web Config. 33
Administratoriaus slaptažodžiu užrakinamas elementas. 34
Valdymo protokolai. 35
Protokolai, kuriuos galite įjungti arba išjungti. . . 36
Protokolo nustatymo elementai. 37

Operacijų ir valdymo nustatymai

Patvirtinkite įrenginio informaciją. 40
Įrenginių valdymas (Epson Device Admin). 40
Pranešimų el. paštu gavimas įvykus įvykiams. 41
Apie el. laiško pranešimus. 41
El. laiško pranešimo konfigūravimas. 41
Pašto serverio konfigūravimas. 42
Pašto serverio ryšio patikrinimas. 44
Mikroprogramininės įrangos naujinimas. 46
Aparatinės programinės įrangos atnaujinimas naudojant Web Config. 46
Mikroprogramininės įrangos naujinimas naudojant Epson Firmware Updater. 46
Nustatymų atsarginių kopijų kūrimas. 47
Parametrų eksportavimas. 47
Parametrų importavimas. 47

Problemų sprendimas

Problemų sprendimo patarimai. 49
Serverio ir tinklo įrenginio žurnalo patikra. 49
Tinklo nustatymų inicijavimas. 49
Tinklo būsenos atkūrimas per valdymo skydą. . . 49
Komunikacijos tarp įrenginių ir kompiuterių patikrinimas. 49
Ryšio patikrinimas naudojant ryšio patikrinimo komandą — „Windows“. 49
Ryšio patikra naudojant ryšio patikrinimo komandą — „Mac OS“. 51
Tinklo programinės įrangos naudojimo problemos. 52
Nepavyksta pasiekti tinklo konfigūravimo lango. 52

Modelio pavadinimas ir (arba) IP adresas nėra rodomi EpsonNet Config. 53

Priedas

Tinklo programinės įrangos įvadas. 55
Epson Device Admin. 55
„EpsonNet Config“. 55
EpsonNet SetupManager. 56
IP adreso priskyrimas naudojant EpsonNet Config. 56
IP adreso priskyrimas naudojant partijos nustatymus. 56
IP adreso kiekvienam įrenginiui priskyrimas. . . . 59
Skaitytuvo prievado naudojimas. 60

Išplėstiniai saugumo nustatymai verslui

Saugumo nustatymai ir pavojaus prevencija. 62
Saugumo funkcijos nustatymai. 63
SSL / TLS ryšys su skaitytuvu. 63
Apie skaitmeninį sertifikatą. 63
SI pasirašyto sertifikato gavimas ir importavimas. 64
SI pasirašyto sertifikato šalinimas. 67
Naudotojo pasirašyto sertifikato atnaujinimas. . . 68
CA Certificate konfigūravimas. 69
Užkoduota komunikacija naudojant „IPsec“ / IP filtravimą. 71
Apie IPsec/IP Filtering. 71
Default Policy konfigūravimas. 72
Group Policy konfigūravimas. 75
IPsec/IP Filtering konfigūracijos pavyzdžiai. 80
IPsec/IP Filtering sertifikato konfigūravimas. . . . 81
„SNMPv3“ protokolo naudojimas. 82
Apie SNMPv3. 82
SNMPv3 konfigūravimas. 82
Skaitytuvo prijungimas prie IEEE802.1X tinklo. . . . 84
IEEE802.1X tinklo sukonfigūravimas. 84
IEEE802.1X sertifikato konfigūravimas. 86
Papildomos saugos problemų sprendimas. 87
Saugumo nustatymų atkūrimas. 87
Tinklo saugos funkcijų naudojimo problemos. . . 88
Skaitmeninio sertifikato naudojimo problemos. . 89

Autorių teisės

Prekės ženklai

- ❏ „EPSON®“ yra registruotasis prekės ženklas, o EPSON EXCEED YOUR VISION arba EXCEED YOUR VISION yra prekių ženklai, priklausantys bendrovei „Seiko Epson Corporation“.
- ❏ 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.
- ❏ Bendroji pastaba: kiti čia pateikti gaminių pavadinimai yra skirti tik gaminiams atpažinti ir gali būti atitinkamų savininkų prekių ženklai. „Epson“ nepriklauso jokios teisės į šiuos ženklus.

Apie šią instrukciją

Ženklai ir simboliai

> ⚠ ***Perspėjimas:***
>
> *Instrukcijos, kurių būtina kruopščiai laikytis, norint išvengti kūno traumos.*

> ***Svarbu:***
>
> *Instrukcijos, kurių būtina paisyti, norint išvengti įrangos sugadinimo.*

Pastaba:
Instrukcijos, kuriose pateikiama naudingų patarimų ir apribojimų dėl skaitytuvo naudojimo.

Susijusi informacija

➡ Spustelėjus piktogramą, parodoma susijusi informacija.

Šiame vadove naudojami aprašymai

❏ Skaitytuvo tvarkyklės ir „Epson Scan 2“ (skaitytuvo tvarkyklės) ekranų momentinės nuotraukos padarytos naudojant „Windows 10“ arba „OS X El Capitan“. Koks turinys rodomas ekranuose, lemia modelis ir aplinkybės.

❏ Šiame vadove naudojami paveikslėliai yra tik pavyzdžiai. Nors, atsižvelgiant į modelį, gali būti nedidelių skirtumų, tačiau naudojimo būdas nesiskiria.

❏ Kokie meniu punktai yra rodomi skystųjų kristalų ekrane, lemia modelis ir nustatymai.

Operacinių sistemų nuorodos

Windows

Šiame vadove vartojami terminai, pvz., „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“ ir „Windows Server 2003“, reiškia toliau nurodytas operacines sistemas. Be to, „Windows“ naudojama, kai turimos omenyje visos versijos.

❏ „Microsoft® Windows® 10“ operacinė sistema

❏ „Microsoft® Windows® 8.1“ operacinė sistema

❏ „Microsoft® Windows® 8“ operacinė sistema

❏ „Microsoft® Windows® 7“ operacinė sistema

❏ „Microsoft® Windows Vista®“ operacinė sistema

❏ „Microsoft® Windows® XP“ operacinė sistema

- ❏ „Microsoft® Windows® XP Professional x64 Edition“ operacinė sistema
- ❏ „Microsoft® Windows Server® 2016“ operacinė sistema
- ❏ „Microsoft® Windows Server® 2012 R2“ operacinė sistema
- ❏ „Microsoft® Windows Server® 2012“ operacinė sistema
- ❏ „Microsoft® Windows Server® 2008 R2“ operacinė sistema
- ❏ „Microsoft® Windows Server® 2008“ operacinė sistema
- ❏ „Microsoft® Windows Server® 2003 R2“ operacinė sistema
- ❏ „Microsoft® Windows Server® 2003“ operacinė sistema

Mac OS

Šiame vadove terminas „Mac OS“ vartojamas, kai kalbama apie „macOS Sierra“, „OS X El Capitan“, „OS X Yosemite“, „OS X Mavericks“, „OS X Mountain Lion“, „Mac OS X v10.7.x“ ir „Mac OS X v10.6.8“.

Įvadas

Vadovo komponentas

Šis vadovas skirtas vadovo administratoriui, kuris atsakingas už spausdintuvo arba skaitytuvo prijungimą prie tinklo, ir jame yra informacija apie nustatymų pasirinkimą, norint naudoti funkcijas.

Funkcijų naudojimo informacijos ieškokite *Vartotojo vadovas*.

Pasiruošimas

Paaiškina administratoriaus užduotis, kaip nustatyti įrenginius ir valdyti programinę įrangą.

Ryšys

Paaiškina, kaip prijungti įrenginį prie tinklo arba telefono linijos. Taip pat paaiškina tinklo aplinką, pvz., prievado naudojimą įrenginiui prijungti, DNS ir tarpinio serverio informaciją.

Funkcijos nustatymai

Paaiškina kiekvienos įrenginio funkcijos nustatymus.

Pagrindiniai saugumo nustatymai

Paaiškina kiekvienos funkcijos, pvz. spausdinimo, nuskaitymo ir faksogramos siuntimo, nustatymus.

Operacijų ir valdymo nustatymai

Paaiškina operacijas pradėjus naudoti įrenginius, pvz. informacijos patikrinimą ir priežiūrą.

Problemų sprendimas

Paaiškina nustatymų inicijavimą ir tinklo trikčių šalinimą.

Išplėstiniai saugumo nustatymai verslui

Paaiškina nustatymų metodą, skirtą įrenginio saugumui pagerinti, pvz., CA sertifikato, SSL / TLS ryšio ir „IPsec“ / IP filtravimo funkcijos naudojimą.

Priklausomai nuo modelio, kai kurios šio skyriaus funkcijos gali būti nepalaikomos.

Naudotojo vadove vartojamų terminų aprašai

Šiame naudotojo vadove vartojami toliau nurodyti terminai.

Administratorius

Asmuo, atsakingas už įrenginio arba tinklo diegimą biure arba organizacijoje. Mažose organizacijose šis asmuo gali būti atsakingas ir už įrenginio, ir už tinklo administravimą. Didelėse organizacijose administratoriai įgalioti valdyti skyriaus arba padalinio grupės įrenginio tinklą arba įrenginius, o tinklo administratoriai atsakingi už ryšio už organizacijos ribų, pvz. interneto, nustatymus.

Tinklo administratorius

Asmuo, atsakingas už tinklo ryšio valdymą. Asmuo, nustatantis maršrutizatorių, tarpinį serverį, DNS serverį ir pašto serverį, valdydamas interneto arba tinklo ryšį.

Naudotojas

Asmuo, naudojantis įrenginius, pvz. spausdintuvus arba skaitytuvus.

Web Config (įrenginio žiniatinklio puslapis)

Įrenginyje integruotas žiniatinklio serveris. Jis vadinamas Web Config. Jame galite patikrinti ir pakeisti įrenginio būseną, naudodami naršyklę.

Įrankis

Bendrinis programinės įrangos, skirtos įrenginio sąrankai arba valdymui, pvz. Epson Device Admin, EpsonNet Config, EpsonNet SetupManager ir t. t., pavadinimas.

Nuskaitymas paspaudus mygtuką

Bendrinis nuskaitymo iš įrenginio valdymo skydelio terminas.

ASCII (Amerikos standartinis kodas duomenų mainams)

Vienas iš simbolių kodų standartų. Apibrėžti 128 simboliai, įskaitant abėcėlę (a–z, A–Z), arabiškus skaičius (0–9), simbolius, tuščius simbolius ir kontrolinius simbolius. Kai šiame vadove aprašomas ASCII, jis reiškia toliau pateiktus 0x20–0x7E (šešioliktainius skaičius), tačiau kontroliniai simboliai į jį neįtraukiami.

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	{	|	}	~	

* Tarpo simbolis.

„Unicode“ (UTF-8)

Tarptautinis standartinis kodas, apimantis daugumą pasaulio kalbų. Kai šiame vadove aprašomas „UTF-8“, jis nurodo simbolių kodavimą UTF-8 formatu.

Pasiruošimas

Šiame skyriuje paaiškinamas administratoriaus vaidmuo ir pasiruošimas prieš nustatymų pasirinkimą.

Skaitytuvo nustatymų ir valdymo srautas

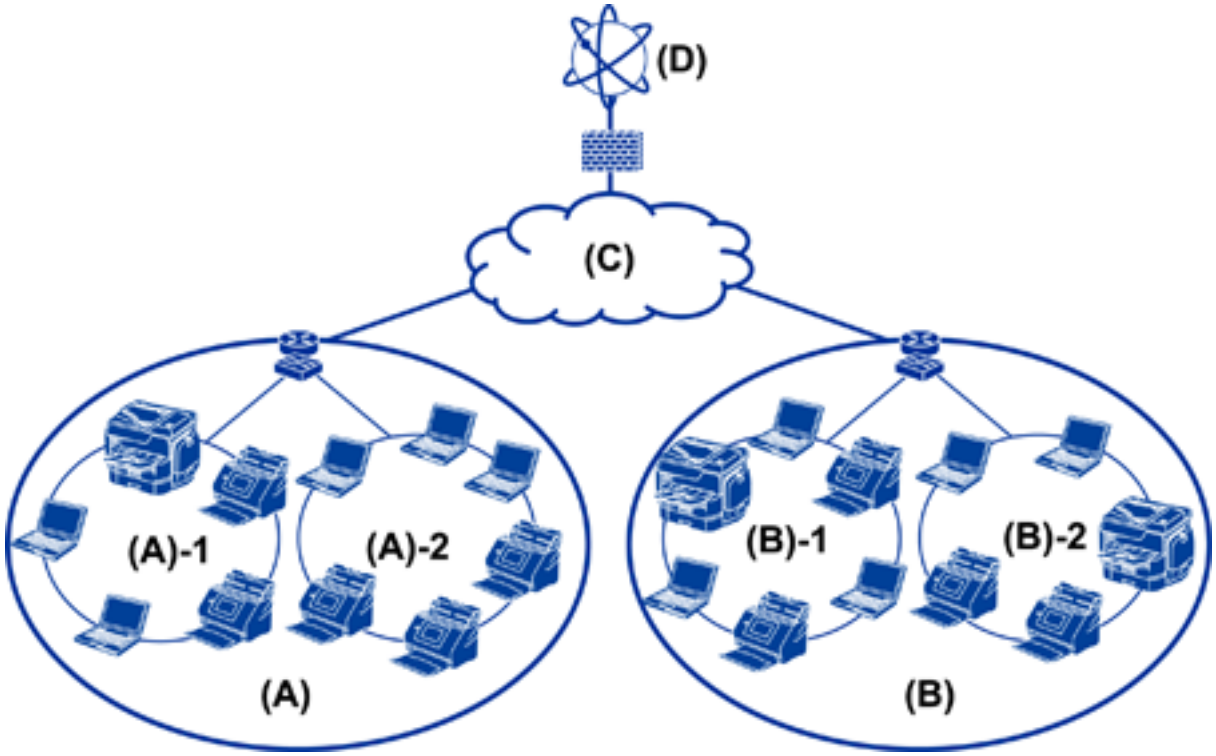
Administratorius nustato tinklo ryšio nustatymus, atlieka skaitytuvo pradinę sąranką ir priežiūros darbus, kad skaitytuvas būtų prieinamas vartotojams.

1. Paruošimas
   - ❏ Ryšio nustatymo informacijos rinkimas
   - ❏ Sprendimas dėl ryšio būdo
2. Prijungimas
   - ❏ Tinklo ryšys, nustatomas skaitytuvo valdymo skydelyje
3. Funkcijų nustatymas
   - ❏ Skaitytuvo tvarkyklės nustatymai
   - ❏ Kiti išplėstiniai nustatymai
4. Saugumo nustatymai
   - ❏ Administratoriaus nustatymai
   - ❏ SSL / TLS
   - ❏ Protokolo valdymas
   - ❏ Išplėstiniai saugumo nustatymai (pasirinktinai)
5. Naudojimas ir valdymas
   - ❏ Įrenginio būsenos tikrinimas
   - ❏ Vykstančių įvykių valdymas
   - ❏ Įrenginio nustatymų atsarginė kopija

Susijusi informacija

➡ „Pasiruošimas” puslapyje 10
➡ „Ryšys” puslapyje 15
➡ „Funkcijos nustatymai” puslapyje 22
➡ „Pagrindiniai saugumo nustatymai” puslapyje 32
➡ „Operacijų ir valdymo nustatymai” puslapyje 40

Tinklo aplinkos pavyzdys



(A): 1 biuras

❏ (A) – 1: 1 LAN

❏ (A) – 2: 2 LAN

(B): 2 biuras

❏ (B) – 1: 1 LAN

❏ (B) – 2: 2 LAN

(C): WAN

(D): internetas

Skaitytuvo ryšio nustatymo pavyzdžio pristatymas

Yra du pagrindiniai ryšio tipai, priklausantys nuo to, kaip naudojamas skaitytuvas. Naudojant abu tipus, skaitytuvas prijungiamas prie tinklo per koncentratorių, naudojant kompiuterį.

❏ Serverio / kliento ryšys (skaitytuvas, kuriame naudojamas „Windows“ serveris, užduočių valdymas)

❏ Lygiaverčių mazgų ryšys (tiesioginis kliento kompiuterio ryšys)

Susijusi informacija

➡ „Serverio / kliento ryšys” puslapyje 12

➡ „Lygiaverčių mazgų ryšys” puslapyje 12

Serverio / kliento ryšys

Centralizuokite skaitytuvo ir užduočių valdymą naudodami Document Capture Pro Server, įdiegtą serveryje. Ši funkcija labiausiai tinka atliekant darbus, per kuriuos naudojami keli skaitytuvai dideliam skaičiui tam tikro formato dokumentų nuskaityti.

Susijusi informacija

➡ „Naudotojo vadove vartojamų terminų aprašai” puslapyje 8

Lygiaverčių mazgų ryšys

Naudokite atskirą skaitytuvą su skaitytuvo tvarkykle, pvz., Epson Scan 2, įdiegta kliento kompiuteryje. Įdiegę Document Capture Pro (Document Capture) kliento kompiuteryje, galite vykdyti užduotis skaitytuvo atskiruose klientų kompiuteriuose.

Susijusi informacija

➡ „Naudotojo vadove vartojamų terminų aprašai” puslapyje 8

Ryšio su tinklu paruošimas

Informacijos apie ryšio nustatymą rinkimas

Tinklo ryšiui reikia turėti IP adresą, tinklų sietuvo adresą ir t. t. Iš anksto patikrinkite toliau pateiktus elementus.

Padaliniai	Elementai	Pastaba
Įrenginio ryšio būdas	❑ Eternetas	Eterneto ryšiui naudokite 5e arba aukštesnės kategorijos STP (ekranuotą vytos poros) kabelį.
LAN ryšio informacija	❑ IP adresas ❑ Potinklio šablonas ❑ Numatytasis tinklų sietuvas	Tai nebūtina, jei automatiškai nustatėte IP adresą, naudodami tinklų sietuvo DHCP funkciją.
DNS serverio informacija	❑ Pirminio DNS IP adresas ❑ Antrinio DNS IP adresas	Jei naudojate statinį IP adresą, sukonfigūruokite DNS serverį. Sukonfigūruokite, kai priskiriate automatiškai, naudodami DHCP funkciją ir kaip DNS serverio negalima priskirti automatiškai.
Tarpinio serverio informacija	❑ Tarpinio serverio pavadinimas ❑ Prievado numeris	Sukonfigūruokite, kada naudoti tarpinį serverį interneto ryšiui užmegzti ir kada naudoti Epson Connect paslaugą arba programinės aparatinės įrangos automatinio atnaujinimo funkciją.

Skaitytuvo techniniai duomenys

Specifikacijų, ar skaitytuvas palaiko standartinį arba ryšio režimą, ieškokite *Vartotojo vadovas*.

Prievado numerio naudojimas

Skaitytuvo naudojamą prievado numerį žr. „Priede“.

Susijusi informacija

➡ „Skaitytuvo prievado naudojimas” puslapyje 60

IP adreso priskyrimo būdai

Yra du IP adreso priskyrimo skeneriui būdai.

Statinis IP adresas:

Skeneriui priskirkite iš anksto nustatytą unikalų IP adresą.

IP adresas nepakeičiamas net išjungiant skenerį arba maršrutizatorių, todėl įrenginį galima valdyti naudojant IP adresą.

Šį būda galima naudoti tinkle, kai vienu metu valdoma daug skenerių, pvz., biure arba mokykloje.

Automatinis priskyrimas naudojant DHCP funkciją:

Teisingas IP adresas automatiškai priskiriamas užsimezgus ryšiui tarp skenerio ir maršrutizatoriaus, kurie palaiko DHCP funkciją.

Jei pakeisti konkretaus įrenginio IP adresą nepatogu, IP adresą išsaugokite iš anksto ir vėliau jį priskirkite.

DNS serveris ir tarpinis serveris

Jei naudojate interneto ryšio paslaugą, sukonfigūruokite DNS serverį. Jei jo nesukonfigūruosite, reikės nurodyti IP adresą prieigai, nes gali nepavykti išversti vardo.

Tarpinis serveris yra ties tinklų sietuvu tarp tinklo ir interneto ir komunikuoja su kompiuteriu, skaitytuvu ir internetu (kitu serveriu) kiekvieno iš jų vardu. Kitas serveris komunikuoja tik su tarpiniu serveriu. Todėl negalima nuskaityti skaitytuvo informacijos, pvz. IP adreso ir prievado numerio, todėl saugumas padidinamas.

Galite uždrausti prieigą prie konkretaus URL, naudodami filtravimo funkciją, kadangi tarpinis serveris gali patikrinti komunikavimo turinį.

Tinklo ryšio nustatymo būdas

Skaitytuvo IP adreso, potinklio šablono ir numatytojo tinklų sietuvo ryšio nustatymus atlikite kaip aprašyta toliau.

Naudojant valdymo skydelį:

Sukonfigūruokite nustatymus, naudodami kiekvieno skaitytuvo valdymo skydelį. Sukonfigūravę skaitytuvo ryšio nustatymus prisijunkite prie tinklo.

Naudojant diegimo programą:

Naudojant diegimo programą skaitytuvo tinklas ir kliento kompiuteris nustatomi automatiškai. Nustatyti galima vykdant diegimo programos instrukcijas, net jei neturite išsamių žinių apie tinklą.

Pasiruošimas

Naudojant įrankį:

Naudokite įrankį administratoriaus kompiuteryje. Galite atrasti skaitytuvą ir tada jį nustatyti arba sukurti SYLK failą, norint skaitytuvams pasirinkti partijos nustatymus. Galite nustatyti daug skaitytuvų, tačiau prieš nustatymą jie turi būti fiziškai prijungti eterneto kabeliu. Todėl tai rekomenduojama, jei nustatymui galite sujungti eternetą.

Susijusi informacija

- „Prisijungimas prie tinklo valdymo skydelyje” puslapyje 15
- „Prisijungimas prie tinklo naudojant diegimo programą” puslapyje 19
- „IP adreso priskyrimas naudojant EpsonNet Config” puslapyje 56

Ryšys

Šiame skyriuje paaiškinama skaitytuvo prijungimo prie tinklo aplinka arba procedūra.

Prijungimas prie tinklo

Prisijungimas prie tinklo valdymo skydelyje

Prijunkite skaitytuvą prie tinklo, naudodamiesi skaitytuvo valdymo skydeliu.

Skaitytuvo valdymo skydelyje žr. *Vartotojo vadovas*, jei reikia išsamios informacijos.

IP adreso priskyrimas

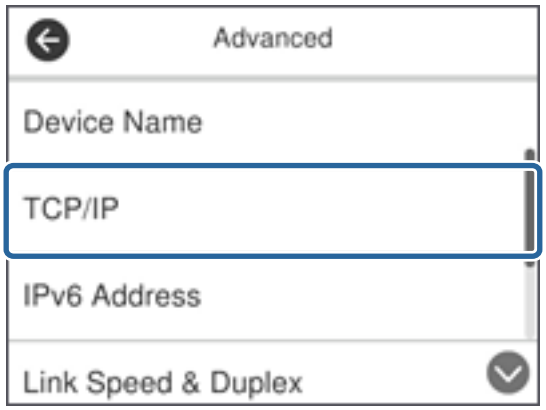
Nustatykite pagrindinius elementus, pvz., IP adresas,Potinklio šablonas ir Numatytasis tinklų sietuvas.

1. Įjunkite skaitytuvą.
2. Skaitytuvo valdymo skydelyje braukite ekraną į kairę, tada palieskite **Nuostatos**.

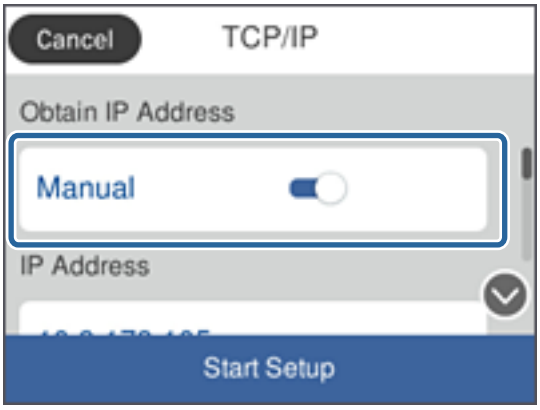
3. Palieskite **Tinklo nuostatos** > **Keisti nuostatas**.

   Jei elementas nerodomas, brūkštelėkite per ekraną aukštyn, kad jis būtų parodytas.

4. Palieskite „**TCP/IP**“.

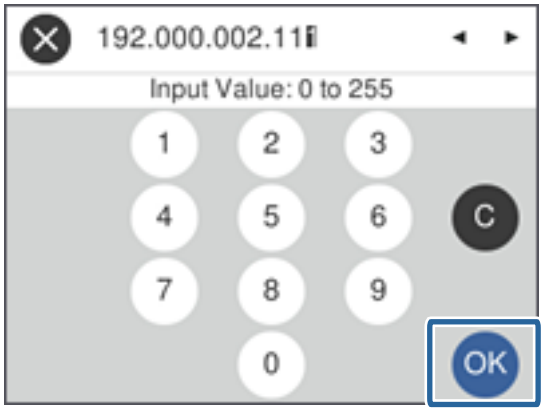


5. Pasirinkite **Rankinis**, kai naudojate **Gauti IP adresą**.



Pastaba:
*Nustatant IP adresą automatiškai, naudojant tinklų sietuvo DHCP funkciją, pasirinkite **Automatiškai**. Šiuo atveju **IP adresas**, **Potinklio šablonas** ir **Numatytasis tinklų sietuvas** taip pat nustatomi automatiškai 6–7 žingsniuose, todėl pereikite prie 8 žingsnio.*

6. Palieskite laukelį **IP adresas**, įveskite IP adresą ekrane rodoma klaviatūra, tada palieskite **GERAI**.



Patvirtinkite ankstesniame ekrane rodytą reikšmę.

7. Nustatykite **Potinklio šablonas** ir **Numatytasis tinklų sietuvas**.

   Patvirtinkite ankstesniame ekrane rodytą reikšmę.

   Pastaba:
   Jei IP adresas, Potinklio šablonas ir Numatytasis tinklų sietuvas derinys neteisingas, ***Pradėti sąranką*** *bus neaktyvus ir su nustatymais nebus galima tęsti. Patvirtinkite, kad įvedant nepadaryta klaidų.*

8. Palieskite laukelį **Pirminis DNS**, skirtą **DNS serveris**, įveskite pirminio DNS serverio IP adresą ekrane rodoma klaviatūra, tada palieskite **Gerai**.

   Patvirtinkite ankstesniame ekrane rodytą reikšmę.

   Pastaba:
   IP adreso priskyrimo nustatymams pasirinkus ***Automatiškai****, galite pasirinkti DNS serverio nustatymus iš* ***Rankinis*** *arba* ***Automatiškai****. Jei negalite automatiškai gauti DNS serverio adreso, pasirinkite* ***Rankinis*** *ir įveskite DNS serverio adresą. Tada tiesiogiai įveskite antrinio DNS serverio adresą. Jei pasirinkote* ***Automatiškai****, pereikite prie 10 žingsnio.*

9. Palieskite laukelį **Antrinis DNS**, įveskite antrinio DNS serverio IP adresą ekrane rodoma klaviatūra, tada palieskite **Gerai**.

   Patvirtinkite ankstesniame ekrane rodytą reikšmę.

10. Palieskite „**Pradėti sąranką**“.

11. Patvirtinimo ekrane palieskite **Uždaryti**.

    Ekranas automatiškai užsidarys po tam tikro laiko tarpo, jei nepaliesite **Uždaryti**.

Prijungimas prie eterneto

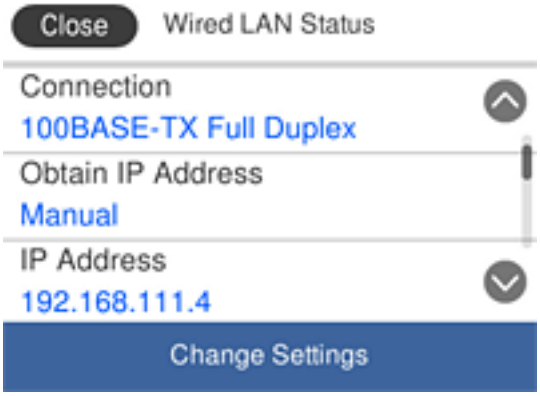
Prijunkite skaitytuvą prie tinklo eterneto laidu ir patikrinkite ryšį.

1. Sujunkite skaitytuvą ir koncentratorių (L2 perjungiklį) eterneto laidu.

   Pradžios ekrane rodoma piktograma pasikeičia į  .

2. Pradžios ekrane palieskite  .

3. Brūkštelėkite per ekraną aukštyn ir įsitikinkite, kad ryšio būsena ir IP adresas tinkami.



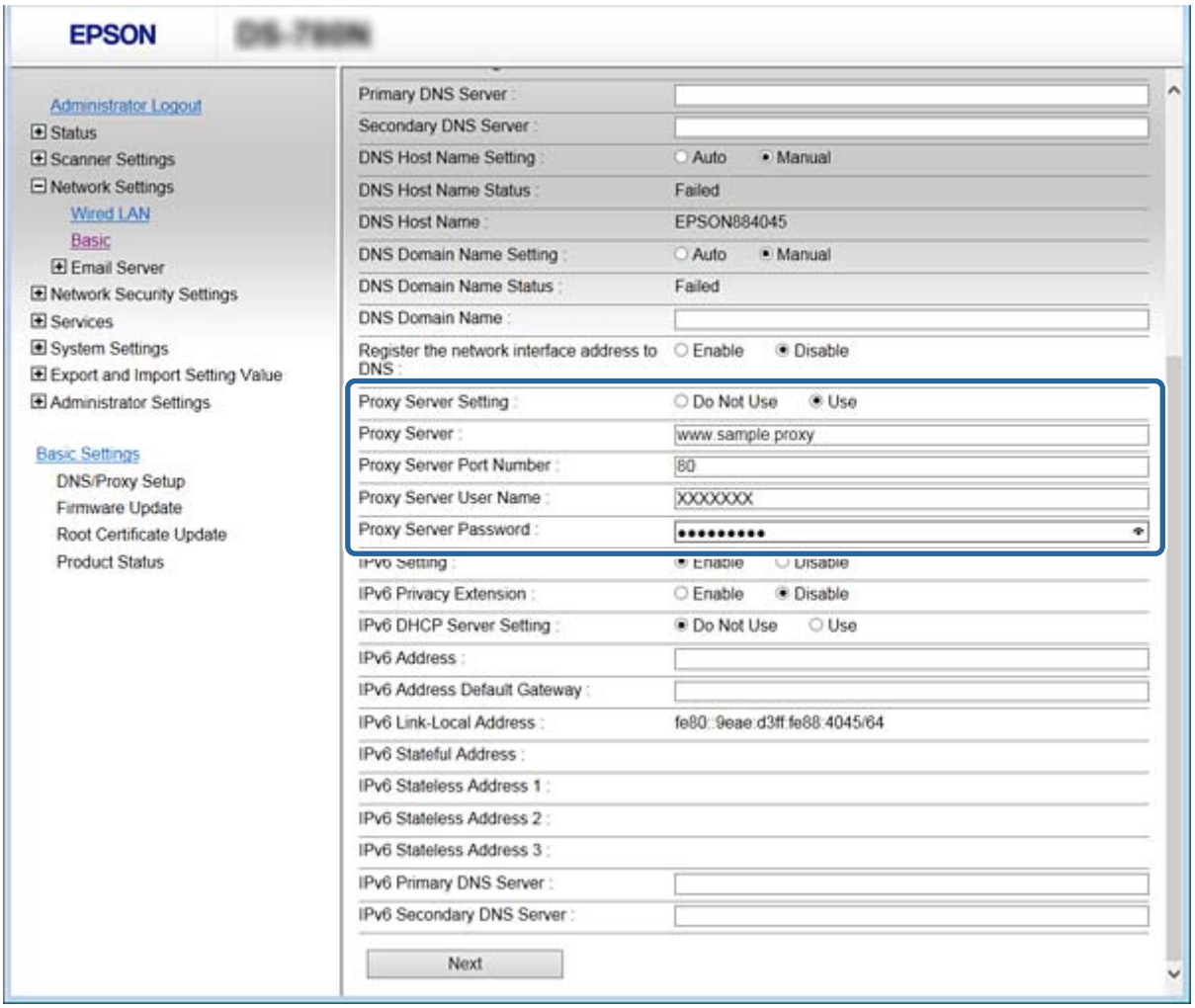
Tarpinio serverio nustatymas

Skydelyje negalima nustatyti tarpinio serverio. Sukonfigūruokite naudodami Web Config.

1. Atverkite Web Config ir pasirinkite **Network Settings** > **Basic**.
2. Pasirinkite **Use** dalyje **Proxy Server Setting**.
3. Dalyje **Tarpinis serveris** nurodykite tarpinį serverį IPv4 adreso arba FQDN formatu ir įveskite prievado numerį dalyje **Proxy Server Port Number**.

   Jei naudojate tarpinius serverius, kuriuos reikia autentifikuoti, įveskite tarpinio serverio autentifikavimo vartotojo vardą ir tarpinio serverio autentifikavimo slaptažodį.

4. Spustelėkite mygtuką **Next**.



5. Patvirtinkite nustatymus ir spustelėkite **Nuostatos**.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Prisijungimas prie tinklo naudojant diegimo programą

Skaitytuvo prijungimui prie kompiuterio rekomenduojame naudoti diegimo programą. Vienu iš toliau nurodytų metodų galite paleisti diegimo programą.

❏ Nustatymas svetainėje

Eikite į toliau nurodytą tinklalapį ir įveskite produkto pavadinimą. Eikite į **Sąranka**, tada pradėkite nustatymą.

http://epson.sn

❏ Nustatymas naudojant programinės įrangos diską (tik modeliams, parduodamiems su programinės įrangos disku ir kompiuteriams su diskų įrenginiu.)

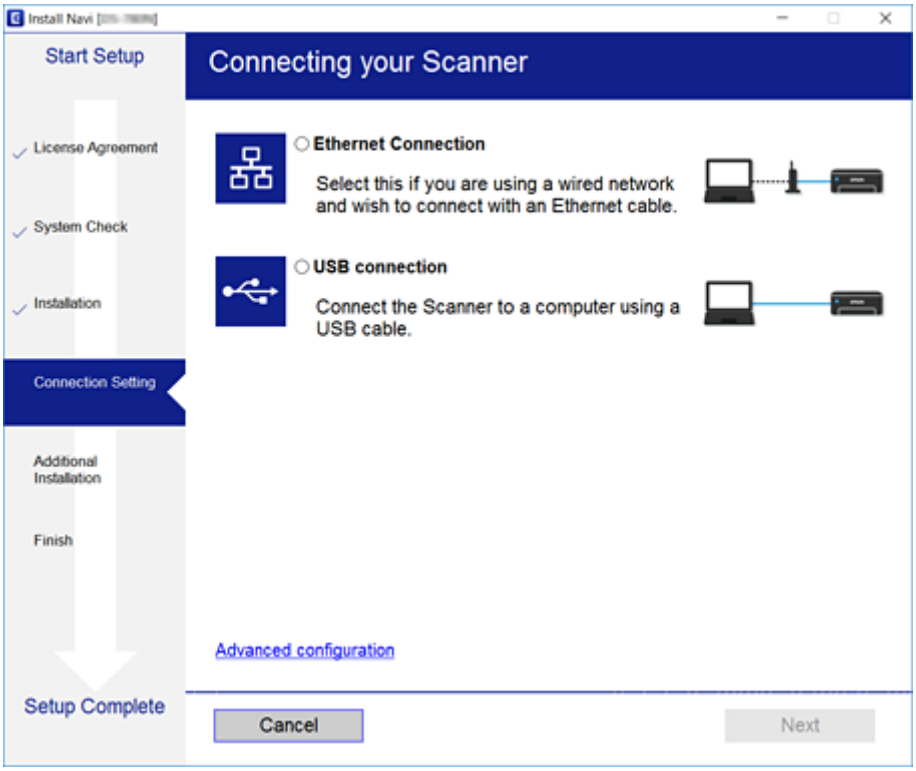
Įdėkite programinės įrangos kompaktinį diską į kompiuterį ir sekite ekrane esančiomis instrukcijomis.

Ryšio būdų pasirinkimas

Vykdykite ekrane rodomas instrukcijas kol pasirodys toliau pateiktas ekranas, tada pasirinkite skaitytuvo ryšio su kompiuteriu būdą.

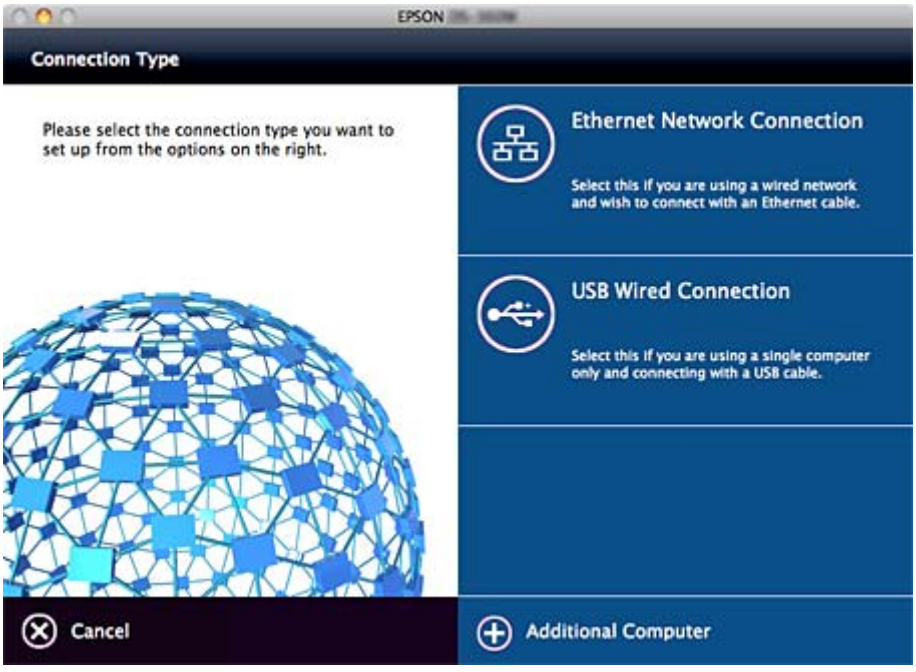
❏ Windows

Pasirinkite ryšio tipą ir spustelėkite **Toliau**.



❏ Mac OS

Pasirinkite ryšio tipą.



Ryšys

Vadovaukitės ekrane rodomomis instrukcijomis. Įdiegiama reikalinga programinė įranga.

Funkcijos nustatymai

Šiame skyriuje paaiškinami pirmieji nustatymai, kuriuos reikia pasirinkti, norint naudoti kiekvieną įrenginio funkciją.

Nustatymo programinė įranga

Šioje temoje paaiškinama procedūra, kaip atlikti adminsitartoriaus kompiuterio nustatymus naudojant Web Config.

Web Config (Įrenginiui skirtas tinklalapis)

Apie Web Config

Web Config yra naršyklės pagrindu veikianti programa, skirta skaitytuvo nuostatoms konfigūruoti.

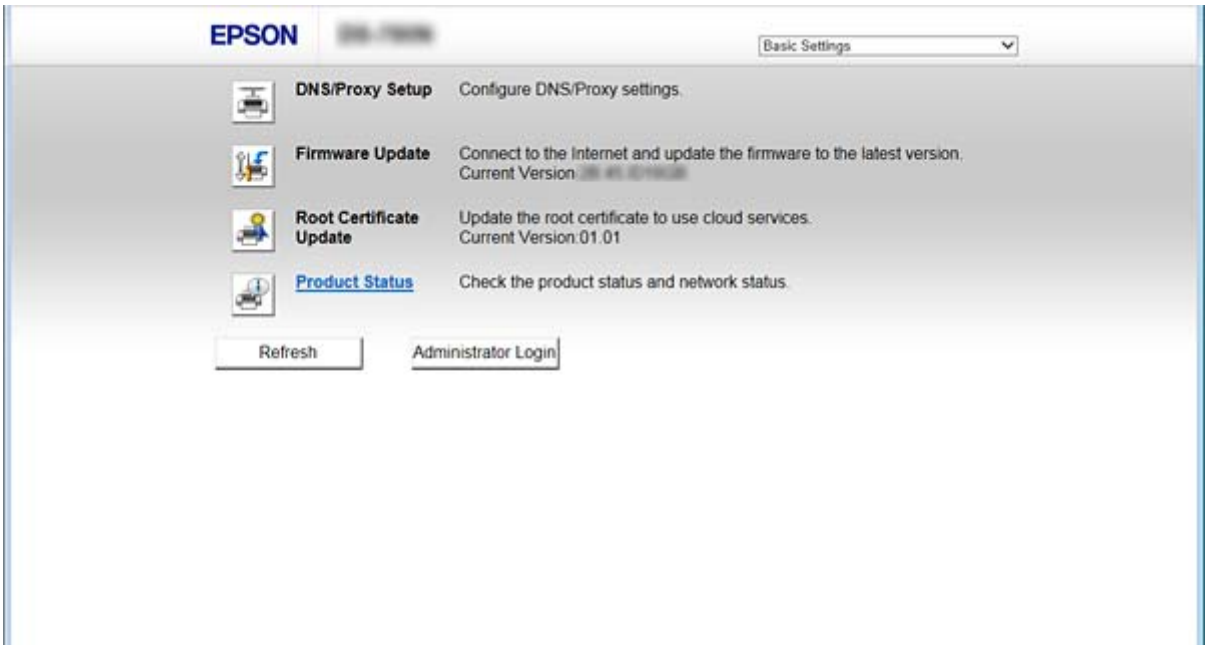
Norėdami pasiekti Web Config, pirmiausia turite skaitytuvui priskirti IP adresą.

Pastaba:
Skaitytuvui sukonfigūruodami administratoriaus slaptažodį, galite užrakinti nuostatas.

Galimi du nuostatų puslapiai (kaip pateikiama toliau).

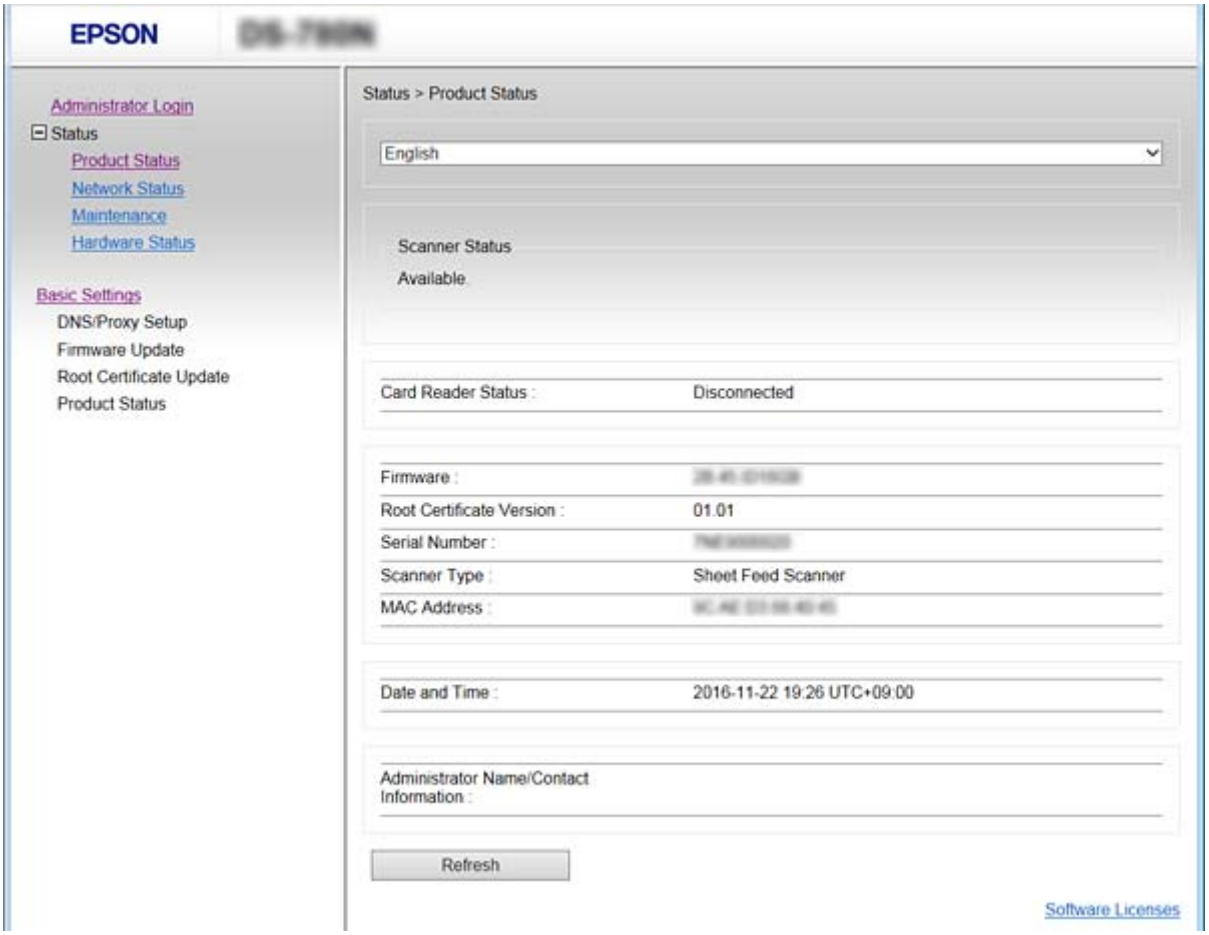
❏ **Basic Settings**

Galite sukonfigūruoti skaitytuvo pagrindines nuostatas.



❏ **Advanced Settings**

Galite sukonfigūruoti skaitytuvo išplėstines nuostatas. Šis puslapis iš esmės skirtas administratoriui.



Prieiga prie Web Config

Į žiniatinklio naršyklę įveskite skaitytuvo IP adresą. Turi būti įgalinta „JavaScript“. Kadangi yra naudojamas naudotojo pasirašytas ir skaitytuve laikomas sertifikatas, prisijungus prie Web Config per HTTPS naršyklėje bus rodomas įspėjamasis pranešimas.

❏ Prieiga per HTTPS

IPv4: https://<skaitytuvo IP adresas> (be < >)

IPv6: https://[skaitytuvo IP adresas]/ (su [ ])

❏ Prieiga per HTTP

IPv4: http://<skaitytuvo IP adresas> (be < >)

IPv6: http://[skaitytuvo IP adresas]/ (su [ ])

Pastaba:

❏ *Pavyzdžiai*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Jei skaitytuvo pavadinimas yra užregistruotas kartu su DNS serveriu, vietoj skaitytuvo IP adreso galite naudoti skaitytuvo pavadinimą.*

Susijusi informacija

➡ „SSL / TLS ryšys su skaitytuvu” puslapyje 63

➡ „Apie skaitmeninį sertifikatą” puslapyje 63

Skenerio funkcijų naudojimas

Atsižvelgdami į tai, kaip naudojate skaitytuvą, įdiekite toliau nurodytą programinę įrangą ir ją naudodami pasirinkite nustatymus.

❏ **Nuskaitymas iš kompiuterio**

❏ Patvirtinkite nuskaitymo per tinklą paslaugos tinkamumą naudodami Web Config (gamykloje nustatyta tinkamai).

❏ Įdiekite Epson Scan 2 savo kompiuteryje ir nustatykite IP adresą

❏ Jei nuskaitote naudodami užduotis, įdiekite Document Capture Pro (Document Capture) ir nustatykite užduočių nustatymus.

❏ **Nuskaitymas iš valdymo skydelio**

❏ Kai naudojamas Document Capture Pro arba Document Capture Pro Server:

Įdiekite Document Capture Pro arba Document Capture Pro Server

DCP nustatymas (serverio režimas, kliento režimas).

❏ Kai naudojamas WSD protokolas:

Patvirtinkite WSD tinkamumą naudodami Web Config arba valdymo skydelį (gamyklos nustatytas tinkamai)

Papildomi įrenginio nustatymai („Windows“ kompiuteris).

Nuskaitymas iš kompiuterio

Įdiekite programinę įrangą ir patikrinkite, ar nuskaitymo per tinklą paslauga įjungta, kad būtų galima nuskaityti iš kompiuterio per tinklą.

Susijusi informacija

➡ „Programinė įranga, kurią reikia įdiegti” puslapyje 25

➡ „Įjungti tinklo nuskaitymą” puslapyje 25

Programinė įranga, kurią reikia įdiegti

❏ Epson Scan 2

Tai skaitytuvo tvarkyklė. Jei prietaisą naudojate iš kompiuterio, tvarkyklę įdiekite kiekvieno kliento kompiuteryje. Jei įdiegtas Document Capture Pro / Document Capture, galite atlikti operacijas, priskirtas prietaiso mygtukams.

Naudojant EpsonNet SetupManager, spausdintuvo tvarkykles galima platinti ir paketais.

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

Įdiekite kliento kompiuteryje. Naudodami kompiuterį ir skaitytuvo valdymo skydelį, galite iškviesti užduotis, užregistruotas kompiuteryje su tinkle įdiegtu Document Capture Pro / Document Capture.

Be to, galite nuskaityti iš kompiuterio per tinklą. Būtina nuskaityti Epson Scan 2.

Susijusi informacija

➡ „EpsonNet SetupManager” puslapyje 56

Nustatykite skaitytuvo IP adresą Epson Scan 2

Nurodykite skaitytuvo IP adresą, kad skaitytuvą būtų galima naudoti tinkle.

1. Paleiskite **Epson Scan 2 Utility** iš **Pradžia** > **Visos programos** > **EPSON** > **Epson Scan 2**.

   Jei jau užregistruotas kitas skaitytuvas, pereikite prie 2 žingsnio.

   Jei neužregistruotas, pereikite prie 4 žingsnio.

2. Spustelėkite ▼ dalyje **Skaitytuvas**.
3. Spustelėkite **Nustatymai**.
4. Spustelėkite **Įjungti redagavimą**, tada spustelėkite **Pridėti**.
5. Dalyje **Modelis** pasirinkite skaitytuvo modelio pavadinimą.
6. Pasirinkite ketinamo naudoti skaitytuvo IP adresą iš **Adresas** dalyje **Ieškoti tinklo**.

   Spustelėkite  ir  , kad atnaujintumėte sąrašą. Jei nepavyksta rasti skaitytuvo IP adreso, pasirinkite **Įveskite adresą** ir įveskite IP adresą.

7. Spustelėkite **Pridėti**.
8. Spustelėkite **GERAI**.

Įjungti tinklo nuskaitymą

Galite nustatyti tinklo nuskaitymo paslaugą nuskaitydami iš kliento kompiuterio per tinklą. Numatytasis nustatymas yra įjungtas.

1. Atverkite tinklo konfigūravimą ir pasirinkite **Services** > **Network Scan**.

2. Įsitikinkite, kad pasirinkta **EPSON Scan** parinktis **Enable scanning**.

   Jei pasirinkta, užduotis baigta. Uždarykite tinklo konfigūravimo langą.

   Jei ji nepažymėta, pasirinkite ją ir pereikite prie kito žingsnio.

3. Spustelėkite **Next**.

4. Spustelėkite **OK**.

   Tinklas prijungiamas iš naujo, tada nustatymai įjungiami.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Nuskaitymas naudojant valdymo skydelį

Nuskaitymo į aplanką funkcija ir nuskaitymo į paštą funkcija naudojant skaitytuvo valdymo skydelį bei nuskaitymo rezultatų perdavimas į paštą, aplankus ir t. t. vykdomas atliekant užduotį kompiuteryje.

Perduodami nuskaitymo rezultatus, nustatykite užduotį su Document Capture Pro Server arba Document Capture Pro.

Norėdami gauti išsamios informacijos apie nustatymus ir užduoties nustatymą, žr. Document Capture Pro Server arba Document Capture Pro dokumentus arba žinyną.

Susijusi informacija

➡ „Nustatymai Document Capture Pro Server / Document Capture Pro” puslapyje 26

➡ „Serverių ir aplankų nustatymas” puslapyje 27

Kompiuteryje ketinama diegti programinė įranga

❏ **Document Capture Pro Server**

Tai Document Capture Pro serverio versija. Įdiekite ją „Windows“ serveryje. Serveryje galima centralizuotai valdyti kelis įrenginius ir užduotis. Užduotis galima vienu metu atlikti naudojant kelis skaitytuvus.

Naudodami sertifikuotą Document Capture Pro Server versiją, galite valdyti užduotis ir nuskaitymo istoriją, susietą su vartotojais ir grupėmis.

Norėdami gauti išsamios informacijos apie Document Capture Pro Server, kreipkitės į vietinį „Epson“ biurą.

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

Kaip ir nuskaitydami kompiuteriu, valdymo skydelyje galite iškviesti kompiuteryje užregistruotas užduotis ir jas vykdyti. Kompiuterio užduočių negalima vienu metu vykdyti iš kelių skaitytuvų.

Nustatymai Document Capture Pro Server / Document Capture Pro

Skaitytuvo valdymo skydelyje pasirinkite nuskaitymo funkcijos naudojimo nustatymus.

1. Atverkite Web Config ir pasirinkite **Services** > **Document Capture Pro**.

2. Pasirinkite **Darbo režimas**.

   ❏ Server Mode:

   Šią parinktį pasirinkite, kai naudojate Document Capture Pro Server arba kai naudojate Document Capture Pro tik užduotims, nustatytoms vykdyti su konkrečiu kompiuteriu, atlikti.

   ❏ Client Mode:

   Šią parinktį nustatykite, kai pasirenkate Document Capture Pro (Document Capture) užduoties nustatymą, įdiegtą kiekviename prie tinklo prijungtame kompiuteryje, nenurodydami konkretaus kompiuterio.

3. Nustatykite toliau nurodytas parinktis pagal pasirinktą režimą.

   ❏ Server Mode:

   Dalyje **Server Address** nurodykite serverį, kuriame įdiegtas Document Capture Pro Server. Tai gali būti 2–252 simboliai IPv4, IPv6, pagrindinio kompiuterio vardo, FQDN formatu. FQDN formatas: galima naudoti US-ASCII raides, skaičius, abėcėles ir brūkšnelius (išskyrus priekyje ir gale).

   ❏ Client Mode:

   Nurodykite **Group Settings**, kad galėtumėte naudoti skaitytuvų grupę, nurodytą Document Capture Pro (Document Capture).

4. Spustelėkite **Nuostatos**.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Serverių ir aplankų nustatymas

Naudojant Document Capture Pro ir Document Capture Pro Server, nuskaityti duomenys vieną kartą išsaugomi serveryje arba kliento kompiuteryje ir naudojama perdavimo funkcija nuskaitymo į aplanką funkcijai bei nuskaitymo į paštą funkcijai vykdyti.

Reikalingas leidimas ir informacija, kuriuos galėtumėte perduoti iš kompiuterio, kuriame Document Capture Pro, Document Capture Pro Server įdiegiamas į kompiuterį arba debesų paslaugos serverį.

Paruoškite informaciją apie ketinamą naudoti funkciją, vadovaudamiesi toliau pateikta informacija.

Galite pasirinkti šių funkcijų nustatymus naudodami Document Capture Pro arba Document Capture Pro Server. Norėdami gauti išsamios informacijos apie nustatymus, žr. Document Capture Pro Server arba Document Capture Pro dokumentus arba žinyną.

Pavadinimas	Nustatymai	Reikalavimas
Nuskaityti į tinklo aplanką (SMB)	Sukurti ir bendrinti išsaugotą aplanką	Kompiuterio administratoriaus paskyra, iš kurios galima išsaugoti aplankus.
	Paskirtis funkcijai „Scan to Network Folder“ (SMB)	Vartotojo vardas ir slaptažodis prisijungti prie kompiuterio, kuriame saugomi aplankai, ir teisė atnaujinti išsaugotą aplanką.
Nuskaityti į tinklo aplanką (FTP)	FTP serverio prisijungimo sąranka	Prisijungimo prie FTP serverio informacija ir teisė atnaujinti išsaugotą aplanką.
Nuskaityti į el. paštą	El. pašto serverio sąranka	El. pašto serverio sąrankos informacija

Pavadinimas	Nustatymai	Reikalavimas
Nuskaityti į „Document Capture Pro“ (kai naudojama Document Capture Pro Server)	Prisijungimo prie debesų paslaugų sąranka	Interneto prijungimo aplinka Debesų paslaugų paskyros registracija

WSD nuskaitymo funkcijos naudojimas (tik „Windows“)

Jei kompiuteryje naudojama „Windows Vista“ arba naujesnės versijos operacinė sistema, galite naudoti WSD nuskaitymo funkciją.

Kai gali būti naudojamas WSD protokolas, skaitytuvo valdymo skydelyje rodomas meniu **Kompiuteris (WSD)**.

1. Atverkite Web Config ir pasirinkite **Services** > **Protocol**.
2. Patikrinkite, ar parinktis **Enable WSD** pažymėta dalyje **WSD Settings**.

   Jei pažymėta, jūsų užduotis baigta ir galite uždaryti langą Web Config.

   Jei nepažymėta, pažymėkite ir pereikite prie kito žingsnio.
3. Spustelėkite mygtuką **Next**.
4. Patvirtinkite nustatymus ir spustelėkite **Nuostatos**.

Sistemos nustatymų pasirinkimas

Sistemos nustatymas valdymo skydelyje

Ekrano ryškumo nustatymas

Nustatykite LCD ekrano ryškumą.

1. Pradžios ekrane palieskite **Nuostatos**.
2. Palieskite **Bendrosios nuostatos** > **LCD šviesumas**.
3. Palieskite arba , kad sureguliuotumėte ryškumą.

   Galite sureguliuoti nuo 1 iki 9.
4. Palieskite „**Gerai**“.

Garso nustatymas

Nustatykite skydelio valdymo garsą ir klaidos garsą.

1. Pradžios ekrane palieskite **Nuostatos**.

2. Palieskite **Bendrosios nuostatos** > **Garsas**.
3. Jei reikia, nustatykite toliau nurodytus elementus.
   - ❏ Valdymo garsas
     Nustatykite valdymo skydelio valdymo garso garsumą.
   - ❏ Klaidos garsas
     Nustatykite klaidos garso garsumą.
4. Palieskite „**Gerai**“.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Originalo dvigubo tiekimo aptikimas

Nustatykite funkciją, skirtą dvigubam nuskaitomo dokumento tiekimui aptikti ir nuskaitymui sustabdyti, kai tiekiami keli dokumentai.

Norėdami nuskaityti originalus, kurie laikomi keliais tiekiamais dokumentais, pvz., vokus arba popierių su lipdukais, šią funkciją išjunkite.

Pastaba:
Ją taip pat galima nustatyti dalyje Web Config arba Epson Scan 2.

1. Pradžios ekrane palieskite **Nuostatos**.
2. Palieskite **Išorinės Nuskaitymo nuostatos** > **Dvigubo tiekimo aptikimas ultragarsu**.
3. Palieskite **Dvigubo tiekimo aptikimas ultragarsu**, kad įjungtumėte arba išjungtumėte.
4. Palieskite „**Uždaryti**“.

Mažo greičio režimo nustatymas

Nustatykite nuskaitymo mažu greičiu režimą, kad neįstrigtų popierius, kai nuskaitomi ploni dokumentai, pvz., kvitai.

1. Pradžios ekrane palieskite **Nuostatos**.
2. Palieskite **Išorinės Nuskaitymo nuostatos** > **Lėtai**.
3. Palieskite **Lėtai**, kad įjungtumėte arba išjungtumėte.
4. Palieskite „**Uždaryti**“.

Sistemos nustatymas naudojant tinklo konfigūravimo langą

Energijos taupymo nustatymai neveiklumo metu

Pasirinkite energijos taupymo nustatymą skaitytuvo neveiklumo laikotarpiu. Nustatykite laiką, priklausomai nuo naudojimo aplinkos.

Pastaba:
Energijos taupymo nustatymą taip pat galite pasirinkti skaitytuvo valdymo skydelyje.

1. Atverkite Web Config ir pasirinkite **System Settings** > **Power Saving**.
2. Įveskite **Sleep Timer** laiką, norėdami perjungti į energijos taupymo režimą neveiklumo metu.

   Galite nustatyti iki 240 minučių vienos minutės tikslumu.
3. Pasirinkite išjungimo laiką **Power Off Timer**.
4. Spustelėkite **OK**.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Valdymo skydelio nustatymas

Skaitytuvo valdymo skydelio sąranka. Ją galite atlikti taip, kaip nurodyta toliau.

1. Atverkite Web Config ir pasirinkite **System Settings** > **Control Panel**.
2. Jei reikia, nustatykite toliau nurodytus elementus.
   - ❏ Language

     Valdymo skydelyje pasirinkite rodomą kalbą.
   - ❏ Panel Lock

     Pasirinkus **ON**, reikia įvesti administratoriaus slaptažodį, kai atliekama operacija, kuriai atlikti reikia administratoriaus įgaliojimų. Jei administratoriaus slaptažodis nenustatytas, išjungiamas skydelio užraktas.
   - ❏ Operation Timeout

     Pasirinkus **ON**, kai registruojatės kaip administratorius, esate automatiškai išregistruojami ir patenkate į pradinį ekraną, jei tam tikrą laiko tarpą nebuvo atlikta jokio veiksmo.

     Galite nustatyti tarp 10 sekundžių ir 240 minučių sekundžių tikslumu.
3. Spustelėkite **OK**.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Išorinės sąsajos apribojimų nustatymas

Kompiuteryje galite apriboti USB ryšį. Nustatykite, kad apribotumėte visas nuskaitymo parinktis, išskyrus nuskaitymo per tinklą.

1. Atverkite Web Config ir pasirinkite **System Settings** > **External Interface**.
2. Pasirinkite **Enable** arba **Disable**.

   Norėdami apriboti, pasirinkite **Disable**.
3. Palieskite „**OK**“.

Datos ir laiko sinchronizavimas su laiko serveriu

Jei naudojate SI sertifikatą, galite išvengti problemų su laiku.

1. Atverkite Web Config ir pasirinkite **System Settings** > **Date and Time** > **Time Server**.
2. Pasirinkite **Use**, kai naudojate **Use Time Server**.
3. Įveskite laiko serverio adresą, skirtą **Time Server Address**.

   Galite naudoti IPv4, IPv6 arba FQDN formatą. Įveskite 252 ženklus arba mažiau. Jei nenorite to nurodyti, palikite tuščią.
4. Įjunkite **Update Interval (min)**.

   Galite nustatyti iki 10 800 minučių tikslumu.
5. Spustelėkite **OK**.

   Pastaba:
   Galite patvirtinti prijungimo būseną, kai laiko serveris nustatytas ***Time Server Status****.*

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Pagrindiniai saugumo nustatymai

Šiame skyriuje paaiškinami pagrindiniai saugumo nustatymai, kuriems nereikalinga speciali aplinka.

Pagrindinių saugumo funkcijų įvadas

Pristatome pagrindines „Epson“ įrenginių saugumo funkcijas.

Funkcijos pavadinimas	Funkcijos tipas	Ką nustatyti	Ko saugotis
Administratoriaus slaptažodžio sąranka	Užrakinkite su sistema susijusius nustatymus, pvz., tinklo ir USB ryšio nustatymus, kad jų niekas, išskyrus administratorių, negalėtų pakeisti.	Administratorius nustato įrenginio slaptažodį. Konfigūracija arba atnaujinimai prieinami bet kur iš Web Config, valdymo skydelio, Epson Device Admin ir EpsonNet Config.	Apsaugo nuo neteisėto įrenginyje saugomos informacijos, pvz. ID, slaptažodžio, tinklo nustatymų ir kontaktų skaitymo ir pakeitimo. Taip pat apsaugo nuo daug kitų saugumo rizikų, pvz. tinklo aplinkos arba saugumo politikos informacijos nutekinimo.
SSL / TLS ryšys	Bandant pasiekti „Epson“ interneto serverį iš įrenginio, pvz., bandant užmegzti ryšį su kompiuteriu per naršyklę arba bandant atnaujinti programinę aparatinę įrangą, ryšio turinys užšifruojamas SSL / TLS ryšiu.	Gaukite CA pasirašytą sertifikatą, tada importuokite jį į skaitytuvą.	Įrenginio identifikacijos aptikrinimas CA pasirašytu sertifikatu apsaugo nuo apsimetinėjimo ir neteisėtos prieigos. Be to, SSL / TLS komunikacijos turinys yra apsaugotas ir neleidžia nutekinti spausdinimo duomenų ir sąrankos informacijos turinio.
Protokolų valdymas	Valdomi protokolai, naudojami ryšiui tarp įrenginių ir kompiuterių užmegzti, bei įjungiamos / išjungiamos funkcijos.	Protokolas arba paslauga, taikoma funkcijoms, leidžiama arba draudžiama atskirai.	Saugumo rizikos dėl neplanuoto panaudojimo sumažinamos neleidžiant naudotojams naudoti nereikalingų funkcijų.

Susijusi informacija

➡ „Apie Web Config” puslapyje 22
➡ „„EpsonNet Config“” puslapyje 55
➡ „Epson Device Admin” puslapyje 55
➡ „Administratoriaus slaptažodžio konfigūravimas” puslapyje 33
➡ „Valdymo protokolai” puslapyje 35

Administratoriaus slaptažodžio konfigūravimas

Kai nustatote administratoriaus slaptažodį, kiti naudotojai, nei administratorius, negalės pakeisti sistemos administravimo nustatymų. Administratoriaus slaptažodį galite nustatyti ir pakeisti naudodami Web Config, skaitytuvo valdymo skydelį, arba programinę įrangą (Epson Device Admin arba EpsonNet Config). Naudodami programinę įrangą, žr. kiekvienos programinės įrangos dokumentaciją.

Susijusi informacija

➡ „Administratoriaus slaptažodžio konfigūravimas valdymo skydelyje” puslapyje 33

➡ „Administratoriaus slaptažodžio konfigūravimas naudojant Web Config” puslapyje 33

➡ „„EpsonNet Config““ puslapyje 55

➡ „Epson Device Admin” puslapyje 55

Administratoriaus slaptažodžio konfigūravimas valdymo skydelyje

Administratoriaus slaptažodį galite nustatyti skaitytuvo valdymo skydelyje.

1. Pradžios ekrane palieskite **Nuostatos**.
2. Palieskite **Sistemos administravimas** > **Administratoriaus nuostatos**.

   Jei elementas nerodomas, braukite ekraną aukštyn, kad elementas būtų parodytas.
3. Palieskite **Administratoriaus slaptažodis** > **Registruoti**.
4. Įveskite naują slaptažodį ir palieskite **Gerai**.
5. Įveskite slaptažodį dar kartą ir palieskite **Gerai**.
6. Patvirtinimo ekrane palieskite **Gerai**.

   Rodomas administratoriaus nustatymų ekranas.
7. Palieskite **Užrakto nuostata**, tada palieskite **Gerai** patvirtinimo ekrane.

   Užrakto nuostata nustatytas ties **Įjung**, o administratoriaus slaptažodis bus reikalingas naudojant užrakintą meniu elementą.

Pastaba:

❏ *Jei nustatote **Nuostatos** > **Bendrosios nuostatos** > **Baigėsi skirtasis operacijos laikas** parinktį **Įjung**, skaitytuvas išregistruoja jus po neveiklumo laikotarpio valdymo skydelyje.*

❏ *Galite pakeisti arba ištrinti administratoriaus slaptažodį, pasirinkdami **Keisti** arba **Atkurti** ekrane **Administratoriaus slaptažodis** ir įvesdami administratoriaus slaptažodį.*

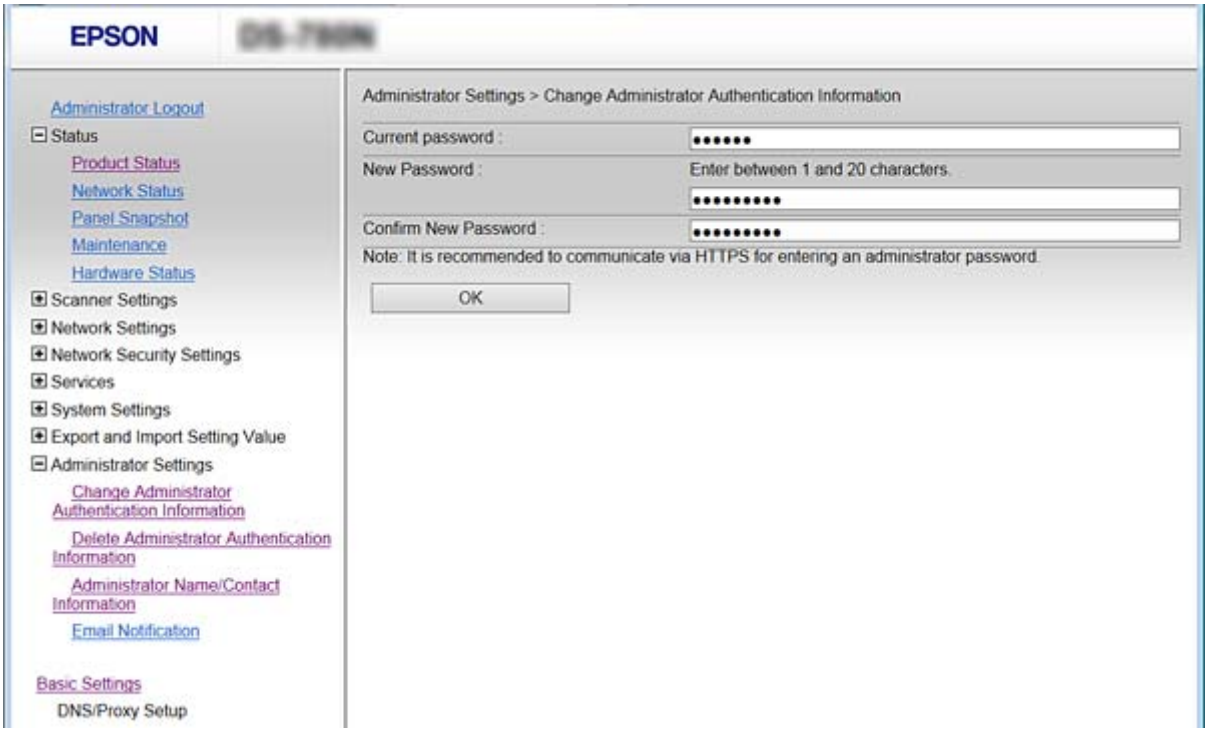
Administratoriaus slaptažodžio konfigūravimas naudojant Web Config

Administratoriaus slaptažodį galite nustatyti naudodami Web Config.

1. Atverkite Web Config ir pasirinkite **Administrator Settings** > **Change Administrator Authentication Information**.

2. Įrašykite slaptažodį į **New Password** ir **Confirm New Password**. Jei reikia, įveskite naudotojo vardą.

   Jeigu norite pakeisti slaptažodį, įveskite esamą slaptažodį.



3. Pasirinkite **OK**.

   Pastaba:

   ❏ *Norėdami nustatyti arba pakeisti užrakintus meniu elementus, paspauskite **Administrator Login**, tada įveskite administratoriaus slaptažodį.*

   ❏ *Norėdami ištrinti administratoriaus slaptažodį, spustelėkite **Administrator Settings** > **Delete Administrator Authentication Information**, tada įveskite administratoriaus slaptažodį.*

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Administratoriaus slaptažodžiu užrakinamas elementas

Administratoriai nustato ir keičia visų įrenginių funkcijų privilegijas.

Be to, jei įrenginyje nustatote administratoriaus slaptažodį, galite jį užrakinti, kad negalėtumėte keisti su įrenginio valdymu susijusių elementų.

Šiuos elementus gali valdyti administratorius.

Elementas	Aprašas
Skaitytuvo nustatymai	Dvigubo tiekimo aptikimo ir mažo greičio režimo nustatymas.

Pagrindiniai saugumo nustatymai

Elementas	Aprašas
Eterneto ryšio nustatymai	Keisti įrenginio pavadinimą ir IP adresą, DNS serverio arba tarpinio serverio sąranką ir keisti nustatymus, susijusius su tinklo ryšiais.
Naudotojo paslaugų nustatymas	Ryšio protokolų valdymo, tinklo nuskaitymo ir Document Capture Pro paslaugų sąranka.
El. pašto serverio nustatymai	El. pašto serverio, su kuriuo tiesiogiai komunikuoja įrenginiai, sąranka.
Saugumo nustatymas	Tinklo saugumo nustatymai, pvz. SSL/TLS ryšio, IPsec / IP filtravimo ir IEEE802.1X.
Šakninio sertifikato atnaujinimas	Atnaujinami šakniniai sertifikatai, reikalingi vykdant Document Capture Pro Server autentifikavimo procesą ir atnaujinant programinę aparatinę įrangą iš Web Config.
Programinės aparatinės įrangos atnaujinimas	Patikrinkite ir atnaujinkite įrenginių programinę aparatinę įrangą.
Laikas, laikmačio nustatymai	Miego perėjimo laikas, automatinis išsijungimas, data / laikas, neveikimo laikas, kiti su laikmačiu susiję nustatymai.
Atkurti numatytuosius nustatymus	Skaitytuvo gamyklinių nustatymų atkūrimo nustatymas.
Administratoriaus nustatymas	Administratoriaus užrakto arba administratoriaus slaptažodžio nustatymas.
Sertifikuoto įrenginio nustatymai	Autentifikavimo įrenginio ID nustatymas. Nustatykite naudodami skaitytuvą su autentifikavimo sistema, palaikančia autentifikavimo įrenginius.

Valdymo protokolai

Galite nuskaityti naudodami įvairius kelius ir protokolus. Taip pat galite naudoti nuskaitymo per tinklą funkciją, pasiekiamą nenurodyto skaičiaus tinklo kompiuteriuose. Pavyzdžiui, galima nuskaityti naudojant tik nurodytus kelius ir protokolus. Galite sumažinti nenumatyto naudojimo pavojus apribodami nuskaitymą naudojant tam tikrus užduočių kelius arba valdydami galimas funkcijas.

Konfigūruokite protokolo parametrus.

1. Atverkite Web Config ir pasirinkite **Services** > **Protocol**.
2. Sukonfigūruokite kiekvieną elementą.
3. Spustelėkite **Next**.
4. Spustelėkite **OK**.

   Parametrai taikomi skaitytuvui.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23
➡ „Protokolai, kuriuos galite įjungti arba išjungti” puslapyje 36
➡ „Protokolo nustatymo elementai” puslapyje 37

Protokolai, kuriuos galite įjungti arba išjungti

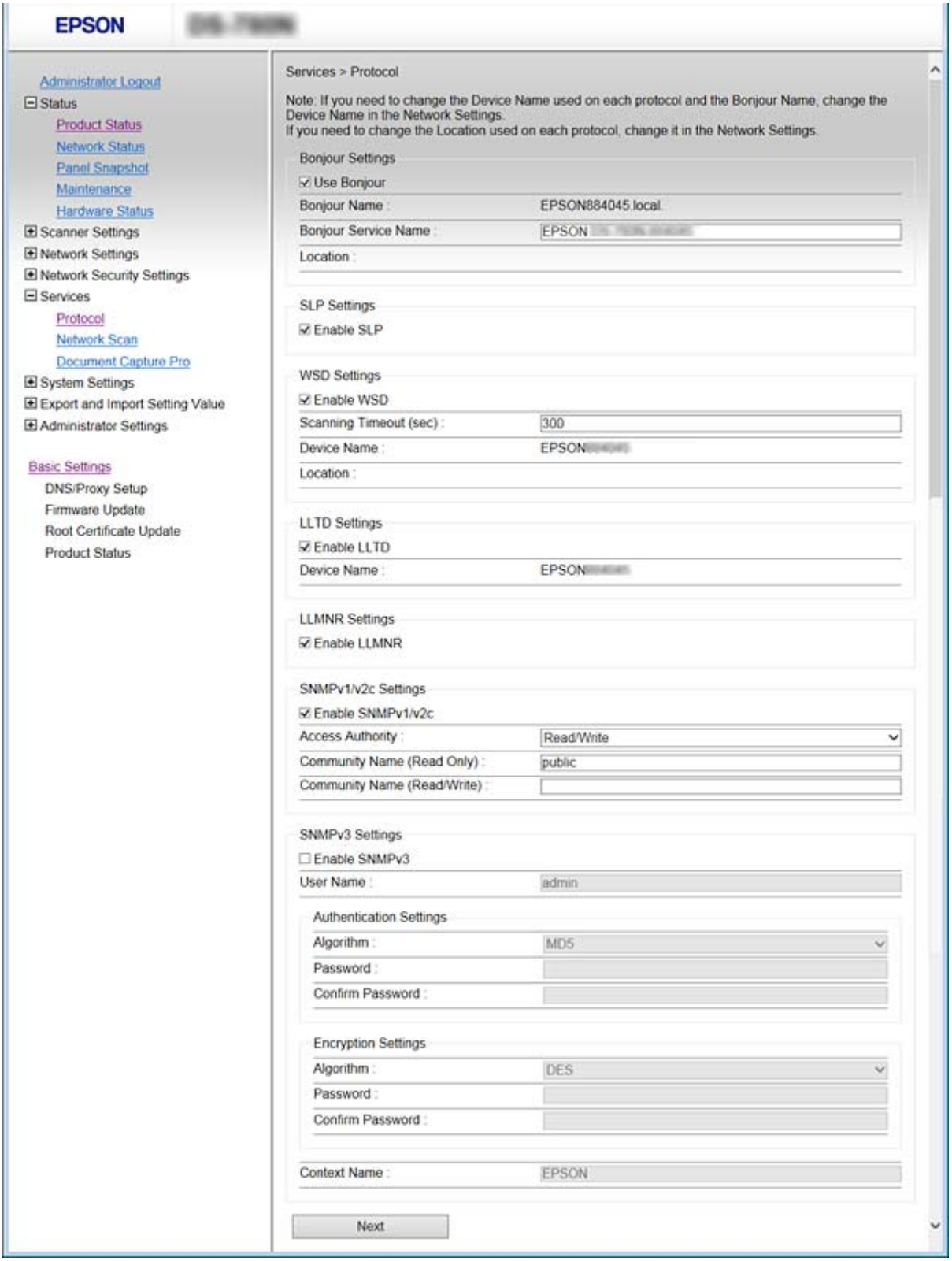
Protokolas	Aprašas
Bonjour Settings	Galite nurodyti, ar naudoti Bonjour. Bonjour naudojama įrenginiams ieškoti, nuskaityti ir pan.
SLP Settings	Galite įjungti arba išjungti SLP funkciją. SLP naudojama Epson Scan 2 ir tinklui ieškoti naudojant EpsonNet Config.
WSD Settings	Galite įjungti arba išjungti WSD funkciją. Įjungę, galite pridėti WSD įrenginius arba nuskaityti iš WSD prievado.
LLTD Settings	Galite įjungti arba išjungti LLTD funkciją. Kai ši funkcija įjungiama, tai rodoma Windows tinklo žemėlapyje.
LLMNR Settings	Galite įjungti arba išjungti LLMNR funkciją. Kai ji įjungta, galite vardus versti be NetBIOS, net jei negalite naudoti DNS.
SNMPv1/v2c Settings	Galite nurodyti įjungti arba neįjungti SNMPv1/v2c. Ši funkcija naudojama įrenginiams, stebėsenai ir pan. nustatyti.
SNMPv3 Settings	Galite nurodyti įjungti arba neįjungti SNMPv3. Ši funkcija naudojama užšifruotiems įrenginiams, stebėsenai ir pan. nustatyti.

Susijusi informacija

➡ „Valdymo protokolai” puslapyje 35

➡ „Protokolo nustatymo elementai” puslapyje 37

Protokolo nustatymo elementai



Elementai	Parametro reikšmė ir aprašas
Bonjour Settings	

Pagrindiniai saugumo nustatymai

Elementai	Parametro reikšmė ir aprašas
Use Bonjour	Pasirinkite, jei norite naršyti arba naudoti įrenginius naudojant Bonjour.
Bonjour Name	Rodomas Bonjour vardas.
Bonjour Service Name	Galite atverti ir nustatyti Bonjour paslaugos pavadinimą.
Location	Rodomas Bonjour vietos vardas.
SLP Settings	
Enable SLP	Pasirinkite, norėdami įjungti SLP funkciją. Ji naudojama tinklui rasti naudojant Epson Scan 2 ir EpsonNet Config.
WSD Settings	
Enable WSD	Pasirinkite, norėdami pridėti įrenginių naudojant WSD, taip pat spausdinti ir nuskaityti iš WSD prievado.
Scanning Timeout (sec)	Nuskaitymui iš WSD įveskite ryšio skirtojo laiko reikšmę nuo 3 iki 3 600 sekundžių.
Device Name	Rodomas WSD įrenginio vardas.
Location	Rodomas WSD vietos vardas.
LLTD Settings	
Enable LLTD	Pasirinkite tai, norėdami įjungti LLTD. Skaitytuvo rodomas Windows tinklo žemėlapyje.
Device Name	Rodomas LLTD įrenginio vardas.
LLMNR Settings	
Enable LLMNR	Pasirinkite tai, norėdami įjungti LLMNR. Galite vardus versti be NetBIOS, net jei negalite naudoti DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Pasirinkite, norėdami įjungti SNMPv1/v2c. Rodomi tik SNMPv3 palaikantys skaitytuvai.
Access Authority	Nustatykite prieigos tarnybą, kai įjungta SNMPv1/v2c. Pasirinkite **Read Only** arba **Read/Write**.
Community Name (Read Only)	Įveskite 0 iki 32 ASCII (0x20 iki 0x7E) ženklus.
Community Name (Read/Write)	Įveskite 0 iki 32 ASCII (0x20 iki 0x7E) ženklus.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 įjungiamas, kai pažymimas langelis.
User Name	Naudodami 1 baito ženklus, įrašykite 1–32 ženklus.
Authentication Settings	
Algorithm	Pasirinkite algoritmą, skirtą SNMPv3 autentifikuoti.

Pagrindiniai saugumo nustatymai

Elementai	Parametro reikšmė ir aprašas
Password	Įveskite slaptažodį, skirtą SNMPv3 autentifikuoti. Įveskite nuo 8 iki 32 simbolių ASCII (0x20–0x7E) formatu. Jei nenorite to nurodyti, palikite tuščią.
Confirm Password	Įveskite sukonfigūruotą slaptažodį patvirtinimui.
Encryption Settings	
Algorithm	Pasirinkite algoritmą, skirtą SNMPv3. užšifruoti.
Password	Įveskite slaptažodį, skirtą SNMPv3 užšifruoti. Įveskite nuo 8 iki 32 simbolių ASCII (0x20–0x7E) formatu. Jei nenorite to nurodyti, palikite tuščią.
Confirm Password	Įveskite sukonfigūruotą slaptažodį patvirtinimui.
Context Name	Įveskite 32 ženklus arba mažiau „Unicode“ (UTF-8) formatu. Jei nenorite to nurodyti, palikite tuščią. Galimų įvesti ženklų skaičius skiriasi priklausomai nuo kalbos.

Susijusi informacija

➡ „Valdymo protokolai” puslapyje 35
➡ „Protokolai, kuriuos galite įjungti arba išjungti” puslapyje 36

Operacijų ir valdymo nustatymai

Šiame skyriuje paaiškinami elementai, susiję su kasdienėmis operacijomis ir įrenginio valdymu.

Patvirtinkite įrenginio informaciją

Galite patikrinti šią veikiančio įrenginio informaciją iš **Status**, naudodami Web Config.

❏ Product Status

Patikrinkite kalbą, būseną, produkto numerį, MAC adresą ir t. t.

❏ Network Status

Patikrinkite tinklo ryšio būsenos informaciją, IP adresą, DNS serverį ir t. t.

❏ Panel Snapshot

Rodyti ekrano vaizdo momentinę nuotrauką įrenginio valdymo skydelyje.

❏ Maintenance

Pradžios datos, nuskaitymo informacijos ir t. t. patikra.

❏ Hardware Status

Patikrinkite skaitytuvo būseną.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Įrenginių valdymas (Epson Device Admin)

Daug įrenginių valdyti ir naudoti galite naudodami Epson Device Admin. Epson Device Admin leidžia valdyti kitame tinkle esančius įrenginius. Toliau aprašomos pagrindinės valdymo funkcijos.

Daugiau informacijos apie funkcijas ir programinės įrangos naudojimą ieškokite Epson Device Admin dokumentacijoje arba žinyne.

❏ Įrenginių atradimas

Galite atrasti tinklo įrenginius ir užregistruoti juos sąraše. Jei „Epson“ įrenginiai, pvz., spausdintuvai arba skaitytuvai, prijungti prie to paties tinklo segmento, kaip ir administratoriaus kompiuteris, galite rasti juos, net jei jiems ir nebuvo priskirtas IP adresas.

Taip pat galite atrasti įrenginius, prijungtus prie tinklo kompiuterių USB laidais. Kompiuteryje reikia įdiegti Epson Device USB Agent.

❏ Įrenginių nustatymas

Galite sukurti šabloną, kuriame yra nustatymo elementai, pvz. tinklo sąsaja ir popieriaus šaltinis, ir taikyti jį kitiems įrenginiams kaip bendrinamus nustatymus. Kai įrenginys prijungtas prie tinklo, galite priskirti jam IP adresą, jei jis nebuvo priskirtas.

❏ Įrenginių stebėjimas

Galite reguliariai gauti tinklo įrenginių būseną ir išsamią informaciją. Galite stebėti prie tinklo kompiuterių USB laidais prijungtus įrenginius ir kitų kompanijų įrenginius, kurie buvo užregistruoti įrenginių sąraše. Norint stebėti USB laidais prijungtus įrenginius, reikia įdiegti Epson Device USB Agent.

❏ Įspėjimų valdymas

Galite stebėti įspėjimus apie įrenginių ir vartojamų reikmenų būseną. Sistema automatiškai administratoriui siunčia pranešimus el. paštu pagal nustatytas sąlygas.

❏ Ataskaitų valdymas

Galite kurti reguliarias ataskaitas, sistemai kaupiant duomenis apie įrenginio naudojimą ir vartojamus reikmenis. Tada galite išsaugoti sukurtas ataskaitas ir siųsti jas el. paštu.

Susijusi informacija

➡ „Epson Device Admin” puslapyje 55

Pranešimų el. paštu gavimas įvykus įvykiams

Apie el. laiško pranešimus

Šią funkciją galite naudoti įspėjimų gavimui įvykus įvykiui. Galite užregistruoti iki 5 el. pašto adresų ir pasirinkti kokių įvykių pranešimus norite gauti.

Norint naudoti šią funkciją turi būti sukonfigūruotas pašto serveris.

Susijusi informacija

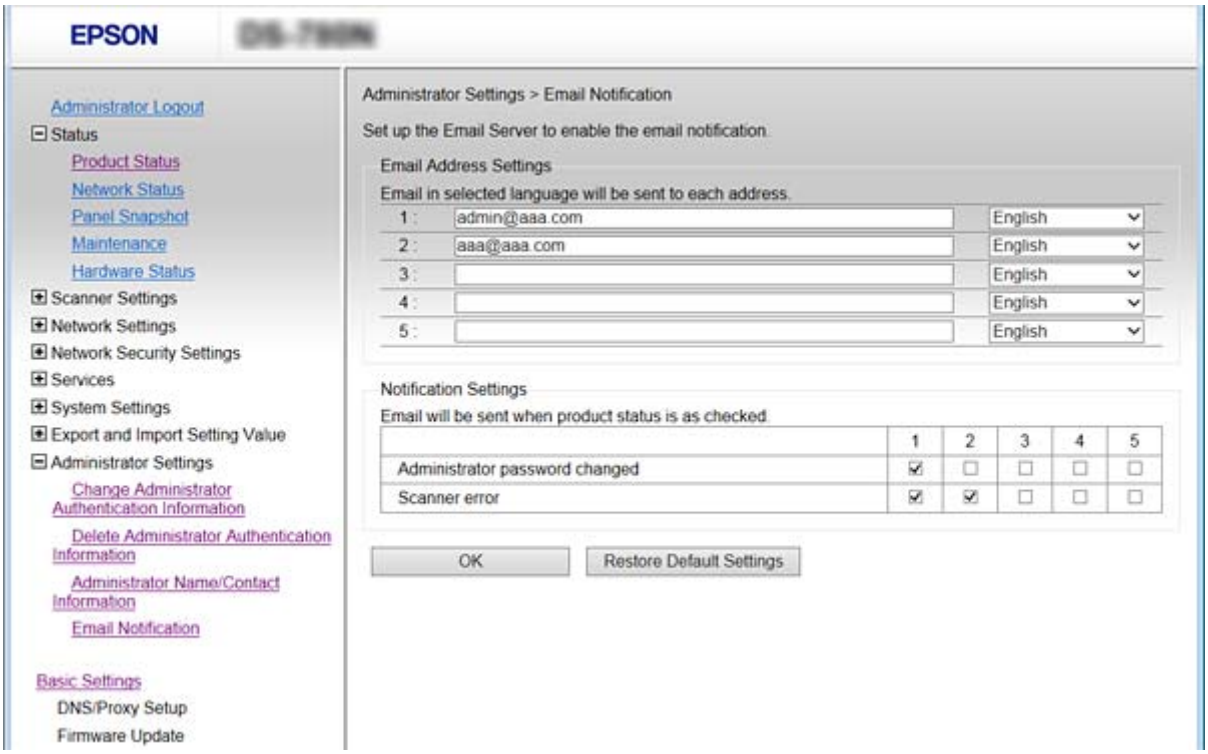
➡ „Pašto serverio konfigūravimas” puslapyje 42

El. laiško pranešimo konfigūravimas

Norėdami naudoti funkciją, turite sukonfigūruoti pašto serverį.

1. Atverkite Web Config ir pasirinkite **Administrator Settings** > **Email Notification**.
2. Įveskite el. pašto adresą, į kurį norite gauti el. laiško pranešimus.
3. Pasirinkite el. laiškų pranešimų kalbą.

4. Pažymėkite tų pranešimų, kuriuos norite gauti, laukelius.



5. Spustelėkite **OK**.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „Pašto serverio konfigūravimas” puslapyje 42

Pašto serverio konfigūravimas

Prieš konfigūruodami, patikrinkite šiuos duomenis.

❏ Ar skaitytuvas prijungtas prie tinklo.

❏ Kompiuterio el.pašto serverio informaciją.

1. Atverkite Web Config ir pasirinkite **Network Settings** > **Email Server** > **Basic**.
2. Įveskite vertę kiekvienam elementui.
3. Pasirinkite **OK**.

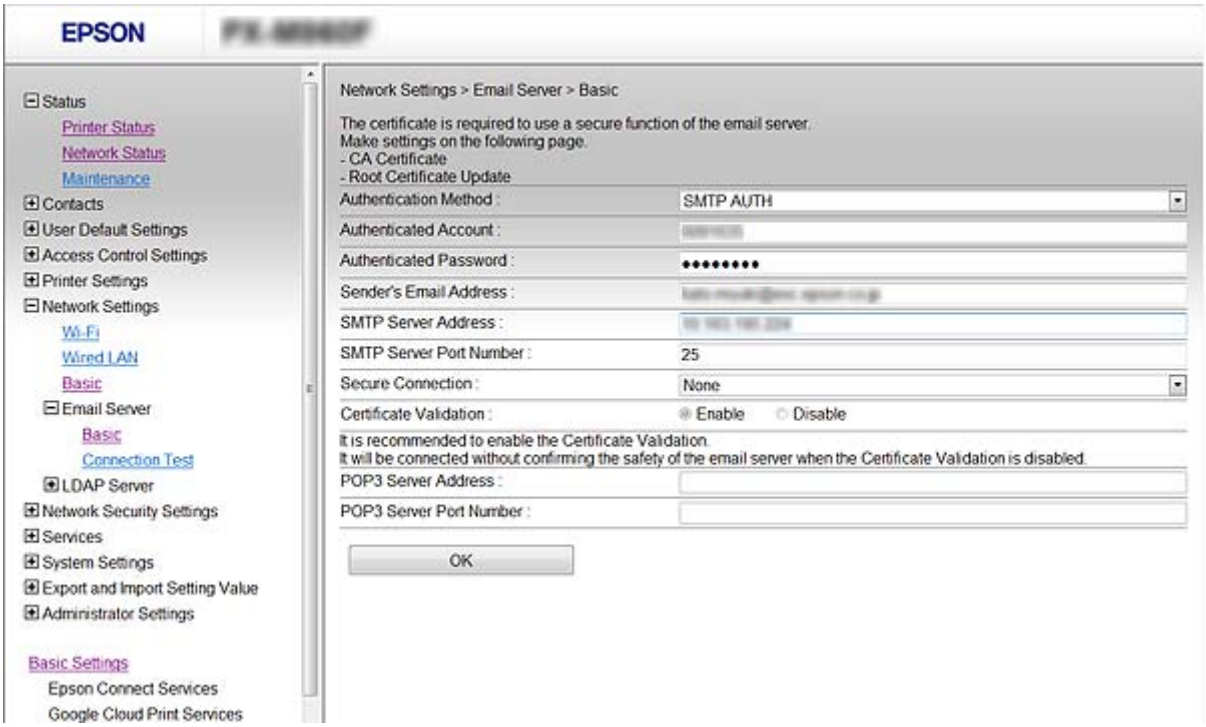
   Rodomos pasirinktos nuostatos.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „Pašto serverio nustatymo elementai” puslapyje 43

Pašto serverio nustatymo elementai



Elementai	Nuostatos ir paaiškinimai	
Authentication Method	Kad būtų galima pasiekti pašto serverį, nurodykite skaitytuvo tapatybės nustatymo metodą.	
	Off	Sukuriant ryšį su pašto serveriu tapatybės nustatymas yra išjungiamas.
	SMTP AUTH	Būtina, kad pašto serveris palaikytų SMTP tapatybės patvirtinimą.
	POP before SMTP	Pasirinkdami šį metodą, sukonfigūruokite POP3 serverį.
Authenticated Account	Jei **SMTP AUTH** arba **POP before SMTP** pasirenkate kaip **Authentication Method**, įveskite 0–255 simbolių paskyros tapatybės patvirtinimo vardą ASCII formatu (0x20 iki 0x7E).	
Authenticated Password	Jei **SMTP AUTH** arba **POP before SMTP** pasirenkate kaip **Authentication Method**, įveskite 0–20 simbolių tapatybės patvirtinimo slaptažodį naudodami A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Įveskite siuntėjo el. pašto adresą. Įveskite nuo 0 iki 255 simbolių ASCII (0x20–0x7E), išskyrus : ( ) < > [ ] ; ¥. Nenaudokite taško „.“ kaip pirmojo simbolio.	
SMTP Server Address	Įrašykite 0–255 simbolius, tarp kurių gali būti A–Z, a–z, 0–9. - . Galite naudoti IPv4 ar FQDN formatą.	
SMTP Server Port Number	Įveskite skaičių nuo 1 iki 65 535.	

Elementai	Nuostatos ir paaiškinimai	
Secure Connection	Nurodykite saugų el. pašto serverio sujungimo metodą.	
	None	Jei **POP before SMTP** pasirenkate skiltyje **Authentication Method**, tapatybės nustatymo metodas nustatomas **None**.
	SSL/TLS	Ši funkcija galima, jei **Authentication Method** nustatytas **Off** arba **SMTP AUTH**.
	STARTTLS	Ši funkcija galima, jei **Authentication Method** nustatytas **Off** arba **SMTP AUTH**.
Certificate Validation	Kai ši funkcija įjungta, sertifikatas tikrinamas. Rekomenduojame nustatyti **Enable**.	
POP3 Server Address	Jeigu **POP before SMTP** pasirenkate kaip **Authentication Method**, įveskite 0–255 simbolių POP3 serverio adresą naudodami A–Z a–z 0–9. - . Galite naudoti IPv4 ar FQDN formatą.	
POP3 Server Port Number	Jeigu **POP before SMTP** pasirenkate kaip **Authentication Method**, įveskite skaičių nuo 1 iki 65 535.	

Susijusi informacija

➡ „Pašto serverio konfigūravimas” puslapyje 42

Pašto serverio ryšio patikrinimas

1. Atverkite Web Config ir pasirinkite **Network Settings** > **Email Server** > **Connection Test**.
2. Pasirinkite **Start**.

   Ryšio su pašto serveriu bandymas pradėtas. Patikrinus, rodoma patikros ataskaita.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23
➡ „Pašto serverio ryšio patikros nuorodos” puslapyje 44

Pašto serverio ryšio patikros nuorodos

Pranešimai	Paaiškinimas
Connection test was successful.	Šis pranešimas yra rodomas, kai prie serverio prisijungta sėkmingai.
SMTP server communication error. Check the following. - Network Settings	Šis pranešimas pasirodo, kai ❏ Skaitytuvas neprijungtas prie tinklo ❏ SMTP serveris išjungtas ❏ Prisijungimo metu tinklo ryšys išjungtas ❏ Gauti nebaigti duomenys

Operacijų ir valdymo nustatymai

Pranešimai	Paaiškinimas
POP3 server communication error. Check the following. - Network Settings	Šis pranešimas pasirodo, kai ❏ Skaitytuvas neprijungtas prie tinklo ❏ POP3 serveris išjungtas ❏ Prisijungimo metu tinklo ryšys išjungtas ❏ Gauti nebaigti duomenys
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Šis pranešimas pasirodo, kai ❏ Prisijungti prie DNS serverio nepavyko ❏ SMTP serverio vardo išversti nepavyko
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Šis pranešimas pasirodo, kai ❏ Prisijungti prie DNS serverio nepavyko ❏ POP3 serverio vardo išversti nepavyko
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Šis pranešimas pasirodo, kai nepavyko atpažinti SMTP serverio.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Šis pranešimas pasirodo, kai nepavyko atpažinti POP3 serverio.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Šis pranešimas pasirodo, kai bandote prisijungti naudodami nepalaikomus protokolus.
Connection to SMTP server failed. Change Secure Connection to None.	Šis pranešimas pasirodo, kai neatitinka serverio ir kliento SMTP arba kai serveris nepalaiko saugaus SMTP ryšio (SSL ryšio).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Šis pranešimas pasirodo, kai neatitinka serverio ir kliento SMTP arba kai serveris reikalauja naudoti SSL/TLS ryšį saugiam SMTP sujungimui.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Šis pranešimas pasirodo, kai neatitinka serverio ir kliento SMTP arba kai serveris reikalauja naudoti STARTTLS ryšį saugiam SMTP sujungimui.
The connection is untrusted. Check the following. - Date and Time	Šis pranešimas pasirodo, kai skaitytuvo datos ir laiko parametrai yra neteisingi arba baigėsi sertifikato galiojimo laikas.
The connection is untrusted. Check the following. - CA Certificate	Šis pranešimas pasirodo, kai skaitytuvas neturi serverį atitinkančio šakninio sertifikato arba CA Certificate nebuvo importuotas.
The connection is not secured.	Šis pranešimas yra rodomas, kai gautas sertifikatas sugadintas.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Šis pranešimas pasirodo, kai nesutampa serverio ir kliento autentiškumo nustatymo metodai. Serveris palaiko SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Šis pranešimas pasirodo, kai nesutampa serverio ir kliento autentiškumo nustatymo metodai. Serveris nepalaiko SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	Šis pranešimas pasirodo, kai nustatyto el. pašto siuntėjo adresas neteisingas.

Pranešimai	Paaiškinimas
Cannot access the product until processing is complete.	Šis pranešimas yra rodomas, kai skaitytuvas yra užimtas.

Susijusi informacija

➡ „Pašto serverio ryšio patikrinimas” puslapyje 44

Mikroprogramininės įrangos naujinimas

Aparatinės programinės įrangos atnaujinimas naudojant Web Config

Mikroprogramininė įranga atnaujinama naudojant Web Config. Įrenginys turi būti prijungtas prie interneto.

1. Atverkite Web Config ir pasirinkite **Basic Settings** > **Firmware Update**.
2. Spustelėkite **Start**.

   Pradedamas mikroprogramininės įrangos patvirtinimas ir, jei yra atnaujinta mikroprogramininė įranga, rodoma informacija apie mikroprogramininę įrangą.
3. Spustelėkite **Start**, ir vadovaukitės ekrane rodomomis instrukcijomis.

Pastaba:
Mikroprogramininę įrangą taip pat galite atnaujinti naudodami Epson Device Admin. Informaciją apie mikroprogramininę įrangą galite patikrinti įrenginių sąraše. Tai naudinga, kai norite atnaujinti kelių įrenginių programinę aparatinę įrangą. Daugiau informacijos žr. Epson Device Admin vadovą arba pagalbą.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23
➡ „Epson Device Admin” puslapyje 55

Mikroprogramininės įrangos naujinimas naudojant Epson Firmware Updater

Įrenginio mikroprogaminę įrangą į kompiuterį galite atsisiųsti „Epson“ tinklavietėje. Tuomet, įrenginį prijungę prie kompiuterio per USB laidą, galite atnaujinti mikroprogramininę įrangą. Jei įrangos naujinti tinkle nepavyksta, pabandykite šį įrangos naujinimo būdą.

1. „Epson“ tinklavietėje atsisiųskite mikroprogramininę įrangą.
2. Kompiuterį su mikroprogramine įranga prijunkite prie įrenginio naudodami USB laidą.
3. Du kartus spustelėkite ant atsisiųsto .exe failo.

   Paleidžiama Epson Firmware Updater programa.

4. Vadovaukitės ekrane rodomomis instrukcijomis.

Nustatymų atsarginių kopijų kūrimas

Eksportuodami Web Config nustatymo elementus, galite nukopijuoti elementus į kitus skaitytuvus.

Parametrų eksportavimas

Eksportuokite visus skaitytuvo parametrus.

1. Atverkite Web Config, tada pasirinkite **Export and Import Setting Value** > **Export**.
2. Pasirinkite parametrus, kuriuos norite eksportuoti.

   Pasirinkite norimus eksportuoti parametrus. Jei pasirenkate pirminę kategoriją, taip pat parenkamos subkategorijos. Tačiau tame pačiame tinkle, dėl dubliavimosi, klaidas sukeliančių subkategorijų (pvz., IP adresų ir pan.) pasirinkti negalima.
3. Norėdami šifruoti eksportuotą failą, įveskite slaptažodį.

   Failui importuoti reikia slaptažodžio. Palikite lauką tuščią, jei nenorite šifruoti failo.
4. Spustelėkite **Export**.

> ***Svarbu:***
>
> *Jei norite eksportuoti skaitytuvo tinklo parametrus, pvz., skaitytuvo vardą ir IP adresą, pasirinkite **Enable to select the individual settings of device** ir pasirinkite daugiau elementų. Keičiamam skaitytuvui naudokite tik pasirinktas reikšmes.*

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Parametrų importavimas

Eksportuotą Web Config failą importuokite į skaitytuvą.

> ***Svarbu:***
>
> *Importuodami su individualia informacija susijusias reikšmes, pvz., skaitytuvo pavadinimą arba IP adresą, įsitikinkite, kad tame pačiame tinkle nėra tokio IP adreso. Jei IP adresas pasikartoja, skaitytuvas nesupranta reikšmės.*

1. Atverkite Web Config, tada pasirinkite **Export and Import Setting Value** > **Import**.
2. Pasirinkite eksportuotą failą, paskui įveskite šifruotą slaptažodį.
3. Spustelėkite **Next**.
4. Pasirinkite norimas importuoti nuostatas, tada spustelėkite **Next**.

5. Spustelėkite **OK**.

Parametrai taikomi skaitytuvui.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Problemų sprendimas

Problemų sprendimo patarimai

Šioje instrukcijoje galite rasti daugiau informacijos.

❏ Vartotojo vadovas

Pateikia skaitytuvo naudojimo, priežiūros ir problemų sprendimo instrukcijas.

Serverio ir tinklo įrenginio žurnalo patikra

Jei kyla problemų dėl tinklo ryšio, jų priežastį galima nustatyti patvirtinant pašto serverio, LDAP serverio ir t. t. žurnalą ir patikrinant būseną naudojant sistemos įrangos žurnalų ir komandų, pvz., maršrutų parinktuvų, tinklo žurnalą.

Tinklo nustatymų inicijavimas

Tinklo būsenos atkūrimas per valdymo skydą

Galite atkurti visus tinklo nustatymus į numatytuosius.

1. Pradžios ekrane palieskite **Nuostatos**.
2. Palieskite **Sistemos administravimas** > **Atkurti numatytuosius parametrus** > **Tinklo nuostatos**.
3. Patikrinkite žinutę ir palieskite **Taip**.
4. Kai parodomas užbaigimo pranešimas, palieskite **Uždaryti**.

   Ekranas automatiškai užsidarys po tam tikro laiko tarpo, jei nepaliesite **Uždaryti**.

Komunikacijos tarp įrenginių ir kompiuterių patikrinimas

Ryšio patikrinimas naudojant ryšio patikrinimo komandą — „Windows“

Naudodami ryšio patikrinimo komandą galite įsitikinti, ar kompiuteris prijungtas prie skaitytuvo. Vykdykite toliau pateiktus žingsnius, norėdami patikrinti ryšį su ryšio patikrinimo komanda.

1. Patikrinkite skaitytuvo, kurį pageidaujate prijungti, IP adresą.

   Tai galite patikrinti naudodami „Epson Scan 2“.

2. Atverkite kompiuterio komandinę eilutę.

   ❏ Windows 10

   Dešiniu klavišu spustelėkite pradžios mygtuką arba paspauskite ir laikykite, tada pasirinkite **Komandinė eilutė**.

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

   Atverkite programėlės langą ir tuomet pasirinkite **Komandinė eilutė**.

   ❏ „Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008“ ir ankstesnės versijos

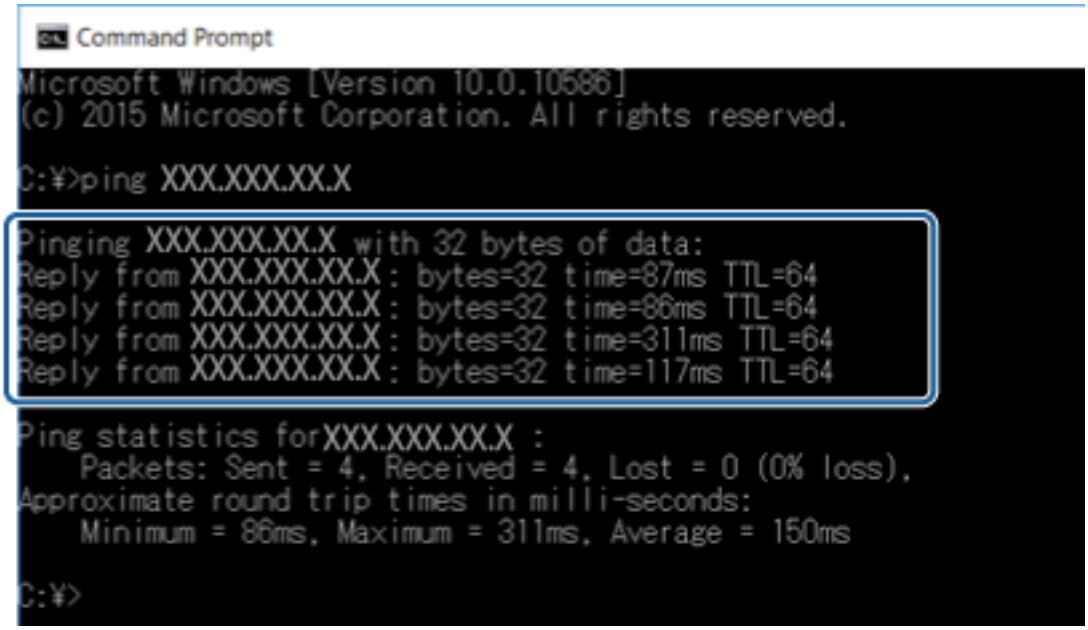
   Paspauskite mygtuką „Pradžia“, pasirinkite **Visos programos** arba **Programos** > **Reikmenys** > **Komandinė eilutė**.

3. Įveskite „ping xxx.xxx.xxx.xxx“ ir tuomet paspauskite mygtuką „Enter“.

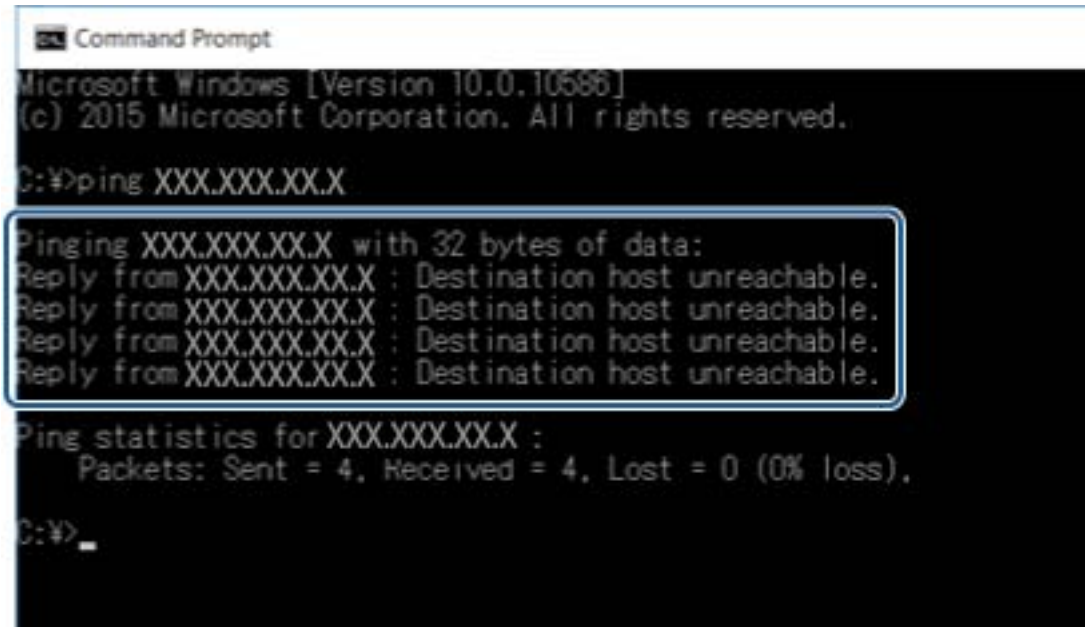
   xxx.xxx.xxx.xxx vietoje įveskite skaitytuvo IP adresą.

4. Patikrinkite komunikacijos būseną.

   Jeigu skaitytuvas komunikuoja su kompiuteriu, rodomas toliau nurodytas pranešimas.



Jeigu skaitytuvas nekomunikuoja su kompiuteriu, rodomas toliau nurodytas pranešimas.



Ryšio patikra naudojant ryšio patikrinimo komandą — „Mac OS“

Naudodami ryšio patikrinimo komandą galite įsitikinti, ar kompiuteris prijungtas prie skaitytuvo. Vykdykite toliau pateiktus žingsnius, norėdami patikrinti ryšį su ryšio patikrinimo komanda.

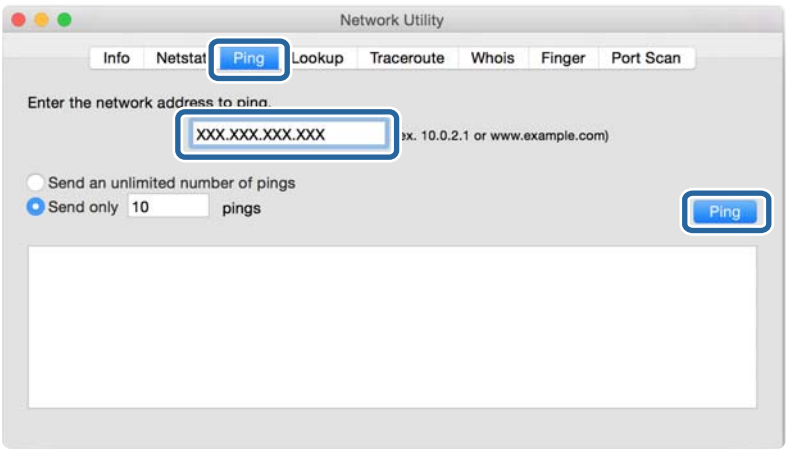
1. Patikrinkite skaitytuvo, kurį pageidaujate prijungti, IP adresą.

   Tai galite patikrinti naudodami „Epson Scan 2“.

2. Paleiskite tinklo paslaugų programą.

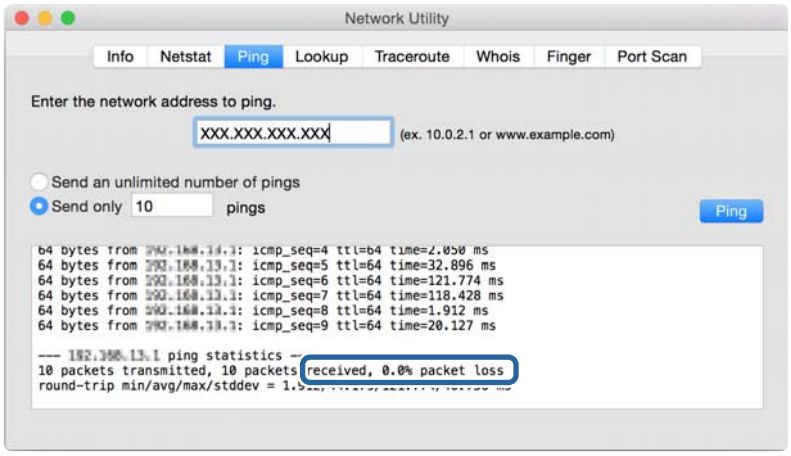
   Atverkite „Tinklo paslaugų programą“, esančią **Spotlight**.

3. Paspauskite skirtuką **Ping**, įveskite IP adresą, kurį patikrinote 1 veiksme, ir tuomet paspauskite **Ping**.

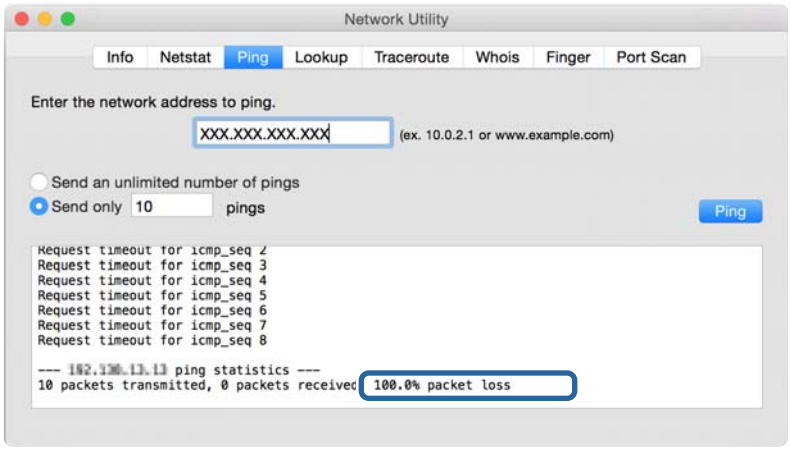


4. Patikrinkite komunikacijos būseną.

   Jeigu skaitytuvas komunikuoja su kompiuteriu, rodomas toliau nurodytas pranešimas.



   Jeigu skaitytuvas nekomunikuoja su kompiuteriu, rodomas toliau nurodytas pranešimas.



Tinklo programinės įrangos naudojimo problemos

Nepavyksta pasiekti tinklo konfigūravimo lango

Ar tinkamai sukonfigūruotas skaitytuvo IP adresas?

IP adresą sukonfigūruokite naudodami Epson Device Admin arba EpsonNet Config.

Ar jūsų naršyklė palaiko masinį šifravimą Encryption Strength, skirtą SSL/TLS?

Toliau yra pateiktas Encryption Strength masinis šifravimas, skirtas SSL/TLS. Prie Web Config galima prisijungti naudojant naršyklę, palaikančią toliau nurodytus masiniu šifravimus. Skaitykite naršyklės šifravimo pagalbos informaciją.

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

❏ 192 bitų: AES256

❏ 256 bitų: AES256

Mėginant pasiekti Web Config, kai naudojamas SSL ryšys (https), parodomas pranešimas „Baigė galioti“.

Jei sertifikatas baigė galioti, jį gaukite iš naujo. Jei pranešimas parodomas nesibaigus galiojimo laikui, įsitikinkite, ar tinkamai sukonfigūruota skaitytuvo data.

Mėginant pasiekti Web Config, kai naudojamas SSL ryšys (https), parodomas pranešimas „Neatitinka saugos sertifikato pavadinimas…“.

Common Name įvestas skaitytuvo IP adresas, skirtas naudoti kuriant vartotojo pasirašomą sertifikatą arba CSR, nesutampa su naršyklėje įvestu adresu. Vėl gaukite ir importuokite sertifikatą arba pakeiskite skaitytuvo pavadinimą.

Skaitytuvą mėginama pasiekti per tarpinį serverį.

Jei kartu su skaitytuvu naudojate tarpinį serverį, turite sukonfigūruoti naršyklės tarpinio serverio nustatymus.

❏ Windows:

Pasirinkite **Valdymo skydas** > **Tinklas ir internetas** > **Interneto parinktys** > **Ryšiai** > **LAN parametrai** > **Tarpinis serveris**, paskui sukonfigūruokite, kad tarpinis serveris nebūtų naudojamas vietos adresams.

❏ Mac OS:

Pasirinkite **Sistemos nuostatos** > **Tinklas** > **Išplėstiniai** > **Tarpinis serveris**, po to užregistruokite **Pagrindiniams kompiuteriams ir domenams skirtos apėjimo tarpinio serverio nuostatos** vietinį adresą.

Pavyzdys:

192.168.1.*: vietos adresas 192.168.1.XXX, potinklio kaukė 255.255.255.0

192.168.*.*: vietos adresas 192.168.XXX.XXX, potinklio kaukė 255.255.0.0

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „IP adreso priskyrimas” puslapyje 15

➡ „IP adreso priskyrimas naudojant EpsonNet Config” puslapyje 56

Modelio pavadinimas ir (arba) IP adresas nėra rodomi EpsonNet Config

Ar pasirinkote Blokuoti, Atšaukti arba Išjungti, kai buvo rodomas „Windows“ saugos priminimas arba užkardos langas?

Jei pasirinkote **Blokuoti**, **Atšaukti** arba **Išjungti**, IP adresas ir modelio pavadinimas EpsonNet Config arba EpsonNet Setup nebus rodomi.

Norėdami tai ištaisyti, užregistruokite EpsonNet Config kaip išimtį. Naudokite Windows ugniasienę ir komercinę saugos programinę įrangą. Jeigu naudojate antivirusinę ar saugos programą, ją užverkite ir mėginkite naudoti EpsonNet Config.

Ar ryšio klaidos skirtojo laiko nuostata yra per trumpa?

Paleiskite EpsonNet Config ir pasirinkite **Tools** > **Options** > **Timeout**, paskui pailginkite **Communication Error** nuostatoje užfiksuojamą laiko trukmę. Atkreipkite dėmesį, kad tai atlikus, EpsonNet Config gali veikti lėčiau.

Susijusi informacija

➡ „EpsonNet Config — Windows paleidimas” puslapyje 56

➡ „EpsonNet Config — Mac OS paleidimas” puslapyje 56

Priedas

Tinklo programinės įrangos įvadas

Toliau aprašoma programinė įranga, konfigūruojanti ir valdanti įrenginius.

Epson Device Admin

Epson Device Admin yra programa, leidžianti įdiegti įrenginius tinkle, tada konfigūruoti ir valdyti juos. Galite gauti išsamią įrenginių informaciją, pvz. būseną ir vartojamus reikmenis, siųsti įspėjimų pranešimus ir kurti įrenginio naudojimo ataskaitas. Taip pat galite sukurti šabloną, kuriame yra nustatymo elementai, ir taikyti jį kitiems įrenginiams kaip bendrinamus nustatymus. Epson Device Admin galite atsisiųsti iš Epson palaikymo žiniatinklio svetainės. Norėdami gauti daugiau informacijos, žr. Epson Device Admin dokumentaciją arba žinyną.

Epson Device Admin paleidimas (tik Windows)

Pasirinkite **Visos programos** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Pastaba:
Parodžius ugniasienės perspėjimui, suteikite prieigą Epson Device Admin.

„EpsonNet Config“

EpsonNet Config leidžia administratoriui sukonfigūruoti skaitytuvo tinklo nuostatas, pvz., priskirti IP adresą ir pakeisti ryšio režimą. Partijos nuostatos režimą palaiko Windows. Norėdami gauti daugiau informacijos, žr. EpsonNet Config dokumentaciją arba žinyną.

EpsonNet Config — Windows paleidimas

Pasirinkite **Visos programos** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Pastaba:
Parodžius ugniasienės perspėjimui, suteikite prieigą EpsonNet Config.

EpsonNet Config — Mac OS paleidimas

Pasirinkite **Eiti** > **Programos** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager yra programinė įranga, skirta paprasto skaitytuvo įdiegimo paketui kurti, pvz., paketui, skirtam skaitytuvo tvarkyklę diegti ir konfigūruoti, bei diegti Document Capture Pro. Programinė įranga suteikia galimybę administratoriui sukurti išskirtinius programinės įrangos paketus ir platinti juos tarp grupių.

Daugiau informacijos rasite apsilankę savo regiono Epson svetainėje.

IP adreso priskyrimas naudojant EpsonNet Config

Galite priskirti IP adresą skaitytuvui, naudodami EpsonNet Config. EpsonNet Config leidžia priskirti IP adresą skaitytuvui, kuriam jis nebuvo priskirtas, prijungus eterneto laidu.

IP adreso priskyrimas naudojant partijos nustatymus

Failo partijos nustatymams sukūrimas

Kaip raktus naudodami MAC adresą ir modelio pavadinimą, galite sukurti naują SYLK failą IP adreso nustatymui.

1. Atidarykite skaičiuoklės programą (pvz. „Microsoft Excel“) arba teksto redaktorių.
2. Įveskite „Info_MACAddress“, „Info_ModelName“ ir „TCPIP_IPAddress“ pirmoje eilutėje kaip nustatymo elementų pavadinimus.

   Įveskite nustatymų elementus šioms teksto eilutėms. Norint skirti didžiąsias ir mažąsias raides ir dviejų baitų ir vieno baito simboliu, jei bent vienas simbolis skiriasi, elementas nebus atpažintas.

   Įveskite nustatymo elemento pavadinimą kaip parašyta toliau, priešingu atveju EpsonNet Config negalės atpažinti nustatymų elementų.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Kiekvienai tinklo sąsajai įveskite MAC adresą, modelio pavadinimą ir IP adresą.

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. Įveskite pavadinimą ir išsaugokite kaip SYLK failą (*.slk).

Partijos nustatymų pasirinkimas naudojant konfigūracijos failą

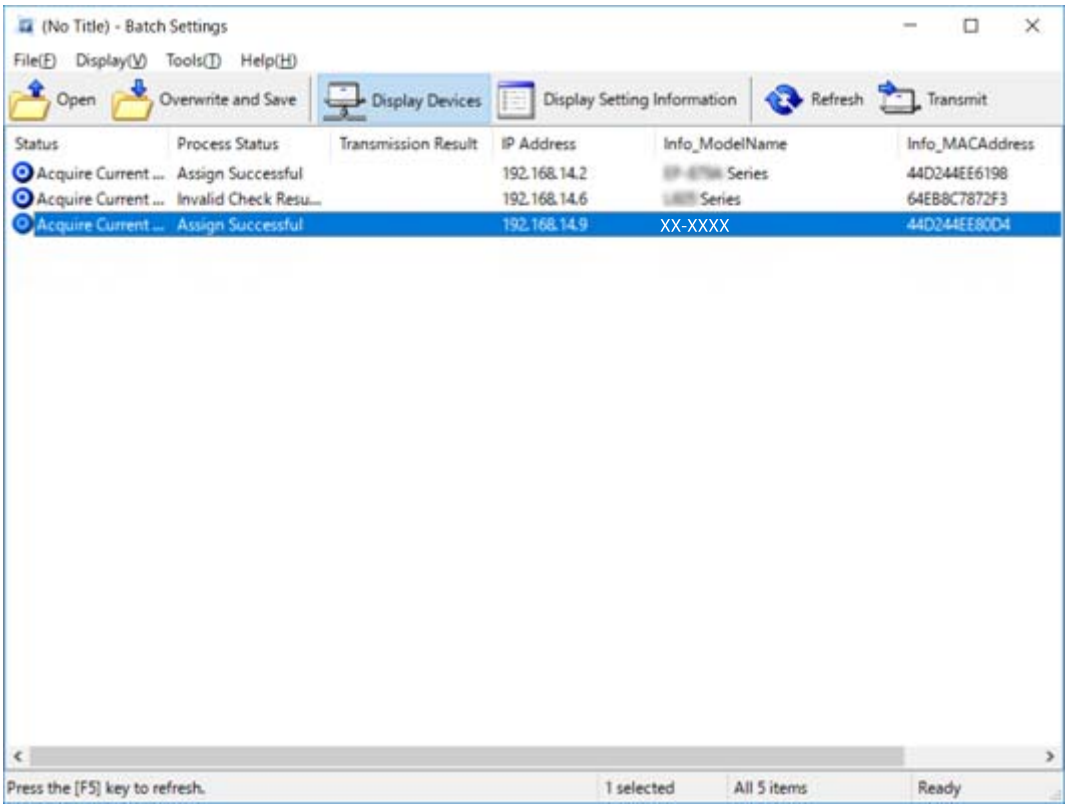
Priskirkite IP adresus konfigūracijos faile (SYLK faile) vienu metu. Prieš priskyrimą reikia sukurti konfigūracijos failą.

1. Prijunkite visus įrenginius prie tinklo eterneto kabeliais.
2. Įjunkite skaitytuvą.
3. Paleiskite „EpsonNet Config“.

   Rodomas tinklo skaitytuvų sąrašas. Gali užtrukti, kol jie bus parodyti.
4. Spustelėkite **Tools** > **Batch Settings**.
5. Spustelėkite **Open**.
6. Failo pasirinkimo ekrane pasirinkite SYLK failą (*.slk), kuriame yra nustatymai, tada spustelėkite **Open**.

7. Pasirinkite įrenginius, kuriems norite pasirinkti partijos nustatymus su **Status** stulpeliu nustatytu ties **Unassigned** ir **Process Status** nustatytu ties **Assign Successful**.

   Pasirinkdami kelis pasirinkimus, paspauskite „Ctrl“ arba „Shift“ ir spustelėkite arba vilkite pelę.



8. Spustelėkite **Transmit**.

9. Kai rodomas slaptažodžio įvedimo ekranas, įveskite slaptažodį, tada spustelėkite **OK**.

   Siųskite nustatymus.

   Pastaba:
   Informacija siunčiama į tinklo sąsają, kol eigos matuokliu nurodoma, kad procesas baigtas. Neišjunkite įrenginio arba bevielio adapterio ir nesiųskite jokių duomenų į įrenginį.

10. Ekrane **Transmitting Settings** spustelėkite **OK**.

11. Patikrinkite nustatyto įrenginio būseną.

    Įrenginių, rodančių  arba  atveju, patikrinkite nustatymų failo turinį arba ar įrenginys įprastai įsijungė iš naujo.

Piktograma	Status	Process Status	Paaiškinimas
	Setup Complete	Setup Successful	Sąranka užbaigta įprastai.
	Setup Complete	Rebooting	Nusiuntus informaciją kiekvienas įrenginys turi įsijungti iš naujo, norint įgalinti nustatymus. Atliekama patikra, nustatanti, ar prie įrenginio galima prisijungti po pakartotinio įjungimo.
	Setup Complete	Reboot Failed	Negalima patvirtinti įrenginio po nustatymų nusiuntimo. Patikrinkite, ar įrenginys įjungtas arba ar įprastai įsijungė iš naujo.
	Setup Complete	Searching	Nustatymų faile inicijuoto įrenginio paieška.*
	Setup Complete	Search Failed	Negalima patikrinti įrenginių, kurių sąranka jau atlikta. Patikrinkite, ar įrenginys įjungtas arba ar įprastai įsijungė iš naujo.*

    * Tik kai rodoma nustatymo informacija.

Susijusi informacija

➡ „EpsonNet Config — Windows paleidimas” puslapyje 56

➡ „EpsonNet Config — Mac OS paleidimas” puslapyje 56

IP adreso kiekvienam įrenginiui priskyrimas

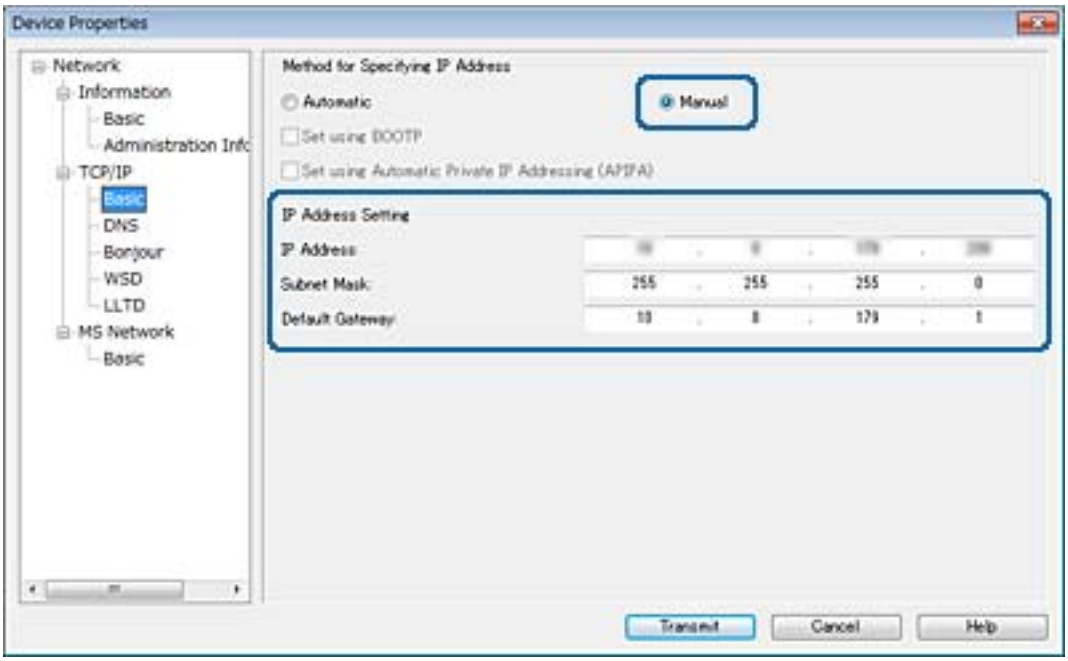
Priskirkite IP adresą skaitytuvui, naudodami EpsonNet Config.

1. Įjunkite skaitytuvą.
2. Eterneto kabeliu prijunkite skaitytuvą prie tinklo.
3. Paleiskite „EpsonNet Config“.

   Rodomas tinklo skaitytuvų sąrašas. Gali užtrukti, kol jie bus parodyti.
4. Dukart spustelėkite skaitytuvą, kuriam norite priskirti.

   Pastaba:
   Jei prijungėte kelis to paties modelio skaitytuvus, galite identifikuoti skaitytuvą, naudodami MAC adresą.
5. Pasirinkite **Network** > **TCP/IP** > **Basic**.

6. Įveskite **IP Address**, **Subnet Mask**, ir **Default Gateway** adresus.



Pastaba:
Įveskite statinį adresą, kai prijungiate skaitytuvą prie saugaus tinklo.

7. Spustelėkite **Transmit**.

   Ekrane rodomas informacijos perdavimo patvirtinimas.

8. Spustelėkite **OK**.

   Rodomas užbaigto perdavimo ekranas.

   Pastaba:
   Informacija perduodama į įrenginį ir rodomas pranešimas „Konfigūracija sėkmingai atlikta“. Neišjunkite įrenginio ir nesiųskite jokių duomenų į paslaugos tarnybą.

9. Spustelėkite **OK**.

Susijusi informacija

➡ „EpsonNet Config — Windows paleidimas” puslapyje 56
➡ „EpsonNet Config — Mac OS paleidimas” puslapyje 56

Skaitytuvo prievado naudojimas

Skaitytuve naudojamas toliau nurodytas prievadas. Kai reikia, prieigą prie šių prievadų turi įgalinti tinklo administratorius.

Priedas

Siuntėjas (klientas)	Paskirtis	Vieta (serveris)	Protokolas	Prievado numeris
Skaitytuvas	El. laiškų siuntimas (el. pašto pranešimas)	SMTP serveris	SMTP (TCP)	25
			SMTP SSL / TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP prieš SMTP ryšys (el. pašto pranešimas)	POP serveris	POP3 (TCP)	110
	WSD valdymas	Kliento kompiuteris	WSD (TCP)	5357
	Suraskite kompiuterį ir paspauskite nuskaitymo mygtuką iš Document Capture Pro	Kliento kompiuteris	„Network Push Scan Discovery“	2968
	Darbo informacijos gavimas skenuojant mygtuko paspaudimu iš Document Capture Pro	Kliento kompiuteris	„Network Push Scan“	2968
Kliento kompiuteris	Raskite skaitytuvą taikomojoje programoje, pvz., EpsonNet Config, ir skaitytuvo tvarkyklėje.	Skaitytuvas	ENPC (UDP)	3289
	Surinkite ir nustatykite MIB informaciją taikomojoje programoje, pvz., EpsonNet Config, ir skaitytuvo tvarkyklėje.	Skaitytuvas	SNMP (UDP)	161
	Ieškoma WSD skaitytuvo	Skaitytuvas	„WS-Discovery“ (UDP)	3702
	Skenavimo duomenų peradresavimas iš Document Capture Pro	Skaitytuvas	„Network Scan“ (TCP)	1865

Išplėstiniai saugumo nustatymai verslui

Šiame skyriuje aprašomos išplėstinės saugumo funkcijos.

Saugumo nustatymai ir pavojaus prevencija

Kai įrenginys prijungtas prie tinklo, galite jį pasiekti nuotoliniu būdu. Be to, įrenginiu gali dalintis keli žmonės, todėl veikla tampa efektyvesnė ir patogesnė. Tačiau padidėja nelegalios prieigos, nelegalaus naudojimo ir duomenų klastojimo rizika. Jei įrenginį naudojate aplinkoje, kurioje yra prieiga prie interneto, rizika dar išauga.

Kad išvengtumėte šios rizikos, „Epson“ įrenginiuose įdiegta įvairių saugumo technologijų.

Nustatykite įrenginį taip, kaip reikia, pagal aplinkos sąlygas, sukurtas naudojant kliento aplinkos informaciją.

Pavadinimas	Funkcijos tipas	Ką nustatyti	Ko saugotis
SSL / TLS ryšys	Kompiuterio ir įrenginio ryšio kelias yra užšifruotas naudojant SSL / TLS ryšį. Naudojant naršyklę, ryšio turinys yra apsaugotas.	Nustatykite serverio CA sertifikatą — įrenginio sertifikatą, pasirašytą CA (sertifikavimo institucijos).	Saugokitės, kad nustatymo informacija ir perduodamų duomenų turinys nebūtų perduoti iš kompiuterio į skaitytuvą. Prieiga prie „Epson“ interneto serverio iš įrenginio taip pat gali būti apsaugoma naudojant programinės aparatinės įrangos atnaujinimo funkciją ir t. t.
„IPsec“ / „IP Filtering“	Galite nustatyti, kad būtų leidžiama išjungti arba nutraukti duomenis, kurie yra konkretaus tipo arba gaunami iš tam tikro kliento. Kadangi „IPsec“ apsaugo duomenis IP paketo elementu (šifravimo ir autentifikavimo funkcijomis), galite saugiai perduoti neapsaugotą nuskaitymo protokolą.	Kad nustatytumėte klientą arba duomenų tipą, galinčius pasiekti įrenginį, sukurkite pagrindinę politiką ir individualią politiką.	Apsaugokite įrenginį nuo neleistinos prieigos, ryšio duomenų klastojimo ir perėmimo.
SNMPv3	Pridėtos funkcijos, pvz., prisijungusių įrenginių stebėjimas tinkle, duomenų vientisumo su SNMP protokolu stebėjimas kontrolei, užšifravimui, naudotojo autentifikavimui ir t. t. atlikti.	Įjunkite SNMPv3, tada nustatykite autentifikavimo ir užšifravimo metodą.	Įsitikinkite, kad duomenys tinkle pakeisti ir kad būsenos stebėjimas konfidencialus.
IEEE802.1X	Prisijungti leidžiama tik vartotojui, kuris autentifikuojamas per eternetą. Naudotis įrenginiu leidžiama tik naudotojui, kuriam suteikta prieiga.	RADIUS serverio (autentifikavimo serverio) autentifikavimo nustatymas.	Apsaugokite įrenginį nuo neleistinos prieigos ir naudojimo.

Pavadinimas	Funkcijos tipas	Ką nustatyti	Ko saugotis
ID kortelės nuskaitymas	Įrenginį galite naudoti palaikę ID kortelę virš prijungto autentifikuoto įrenginio. Galite apriboti kiekvieno naudotojo ir įrenginio žurnalų gavimą bei apriboti kiekvieno naudotojo ir grupės galimą įrenginių naudojimą ir galimas funkcijas.	Prijunkite prie įrenginio autentifikuotą įrenginį ir autentifikavimo sistemoje nustatykite naudotojo informaciją.	Neleiskite, kad įrenginys būtų naudojamas neteisėtai arba apsimetant kitu vartotoju.

Susijusi informacija

➡ „SSL / TLS ryšys su skaitytuvu” puslapyje 63
➡ „Užkoduota komunikacija naudojant „IPsec“ / IP filtravimą” puslapyje 71
➡ „„SNMPv3“ protokolo naudojimas” puslapyje 82
➡ „Skaitytuvo prijungimas prie IEEE802.1X tinklo” puslapyje 84

Saugumo funkcijos nustatymai

Nustatant „IPsec“ / IP filtravimą arba IEEE802.1X, rekomenduojama atverti Web Config naudojant SSL/TLS, norint pranešti nustatymų informaciją, kad sumažėtų saugumo rizikos, pvz. klastojimas arba perėmimas.

SSL / TLS ryšys su skaitytuvu

Kai serverio sertifikatas nustatytas naudojant SSL / TLS (saugiųjų jungčių lygmens / transportavimo lygmens saugos) ryšį su skaitytuvu, galite užšifruoti ryšio kelią tarp kompiuterių. Atlikite tai, jei norite užkirsti kelią nuotoliniai ir neleistinai prieigai.

Apie skaitmeninį sertifikatą

❏ SI pasirašytas sertifikatas

SI (sertifikavimo institucijos) pasirašytą sertifikatą būtina gauti iš sertifikavimo institucijos. Saugų ryšį galite užtikrinti naudodami SI pasirašytą sertifikatą. Kiekvienai saugos funkcijai galite naudoti SI pasirašytą sertifikatą.

❏ SI sertifikatas

SI sertifikatas rodo, kad trečioji šalis patvirtino serverio tapatybę. Tai yra pagrindinis patikimo žiniatinklio saugos stiliaus komponentas. SI sertifikatą serverio autentiškumui patvirtinti turite gauti iš jį išduodančios SI.

❏ Naudotojo pasirašyto sertifikatas

Naudotojo pasirašytas sertifikatas — tai toks sertifikatas, kurį išduoda skaitytuvas ir pasirašo pats naudotojas. Šis sertifikatas yra nepatikimas ir negalės padėti išvengti apsimetimo kitu naudotoju rizikos. Jei šį sertifikatą naudosite SSL / TLS sertifikatui, naršyklėje gali būti rodomas saugos perspėjimas. Šį sertifikatą galite naudoti tik SSL / TLS ryšiui.

Susijusi informacija

➡ „SI pasirašyto sertifikato gavimas ir importavimas” puslapyje 64

➡ „SI pasirašyto sertifikato šalinimas” puslapyje 67
➡ „Naudotojo pasirašyto sertifikato atnaujinimas” puslapyje 68

SI pasirašyto sertifikato gavimas ir importavimas

SI pasirašyto sertifikato gavimas

Norėdami gauti SI pasirašytą sertifikatą, sukurkite CSR (sertifikato pasirašymo užklausą) ir pateikite ją sertifikavimo institucijai. CSR galite sukurti naudodami Web Config ir kompiuterį.

Vykdykite žingsnius ir sukurkite CSR bei, naudodami Web Config, gaukite SI pasirašytą sertifikatą. Naudojant Web Config ir kuriant CSR, sertifikatas yra PEM / DER formato.

1. Atverkite Web Config, tada pasirinkite **Network Security Settings**. Toliau pasirinkite **SSL/TLS** > **Certificate** arba **IPsec/IP Filtering** > **Client Certificate** arba **IEEE802.1X** > **Client Certificate**.

2. Spustelėkite **Generate**, esančią **CSR**.

   Atveriamas CSR kūrimo puslapis.

3. Įveskite vertę kiekvienam elementui.

   Pastaba:
   Atsižvelgiant į sertifikavimo instituciją, skiriasi galimas rakto ilgis ir santrumpos. Užklausą sukurkite pagal kiekvienos sertifikavimo institucijos taisykles.

4. Spustelėkite **OK**.

   Rodomas baigimo pranešimas.

5. Pasirinkite **Network Security Settings**. Toliau pasirinkite **SSL/TLS** > **Certificate** arba **IPsec/IP Filtering** > **Client Certificate**, arba **IEEE802.1X** > **Client Certificate**.

6. Spustelėkite vieną iš **CSR** siuntimo mygtukų (pagal kiekvienos sertifikavimo institucijos formatą) ir atsisiųskite CSR į kompiuterį.

   > ***Svarbu:***
   > *CSR atnaujinti nereikia. Atnaujinus, gali nepavykti importuoti išduoto CA-signed Certificate sertifikato.*

7. Siųskite CSR sertifikavimo institucijai ir gaukite CA-signed Certificate sertifikatą.

   Laikykitės kiekvienos sertifikavimo institucijos taisyklių dėl siuntimo metodo ir formos.

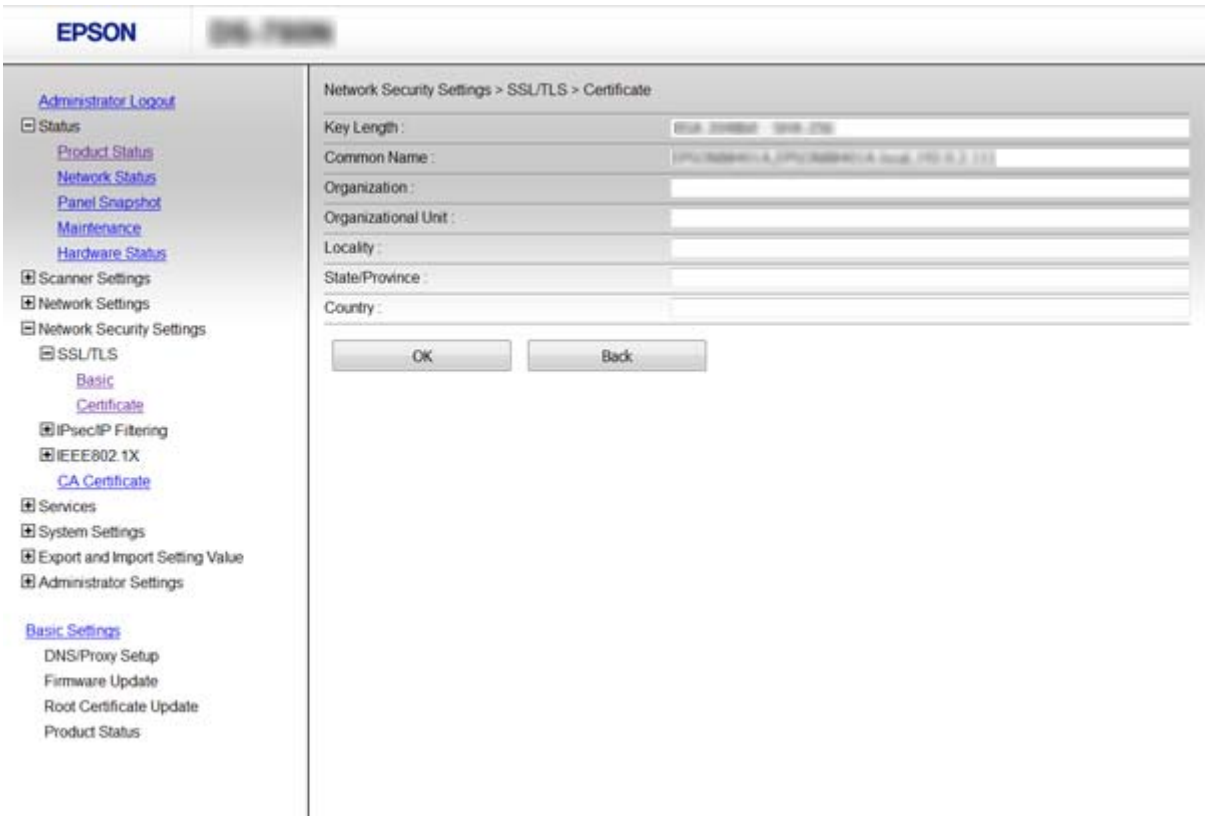
8. Išduotą CA-signed Certificate sertifikatą išsaugokite prie skaitytuvo prijungtame kompiuteryje.

   Išsaugojus sertifikatą paskirties vietoje, CA-signed Certificate sertifikatas yra gautas.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23
➡ „CSR nustatymo elementai” puslapyje 65
➡ „SI pasirašyto sertifikato importavimas” puslapyje 65

CSR nustatymo elementai



Elementai	Nuostatos ir paaiškinimai
Key Length	Pasirinkite rakto ilgį, skirtą CSR.
Common Name	Galite įvesti nuo 1 iki 128 simbolių. Jei tai IP adresas, jis turėtų būti nekintamas. Pavyzdys: URL adresas, skirtas Web Config pasiekti: https://10.152.12.225 Bendrasis pavadinimas: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Galite įvesti nuo 0 iki 64 simbolių ASCII (0x20–0x7E) formatu. Išskirtinus pavadinimus galite atskirti kableliais.
Country	Įveskite šalies kodą, kurį nustatė ISO-3166 (kaip dviejų skaičių numerį).

Susijusi informacija

➡ „SI pasirašyto sertifikato gavimas” puslapyje 64

SI pasirašyto sertifikato importavimas

Svarbu:

❏ *Įsitikinkite, ar skaitytuvo data ir laikas nustatyti tinkamai.*

❏ *Naudodami Web Config sukurtą CSR ir gavę sertifikatą, vieną kartą jį galėsite importuoti.*

1. Atverkite Web Config tada pasirinkite **Network Security Settings**. Toliau pasirinkite **SSL/TLS** > **Certificate** arba **IPsec/IP Filtering** > **Client Certificate**, arba **IEEE802.1X** > **Client Certificate**.

2. Spustelėkite **Import**.

   Atveriamas sertifikato importavimo puslapis.

3. Įveskite vertę kiekvienam elementui.

   Privalomos nuostatos skiriasi priklausomai nuo to, ar kursite CSR ir failo formato sertifikatą. Pagal toliau pateiktus nurodymus, įveskite reikšmes į privalomus užpildyti laukelius.

   - ❏ PEM / DER formato sertifikatas, gautas iš Web Config
     - ❏ **Private Key**: nekonfigūruokite, kadangi skaitytuvas turi asmeninį raktą.
     - ❏ **Password**: nekonfigūruokite.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: pasirenkama
   - ❏ PEM / DER formato sertifikatas, gautas iš kompiuterio
     - ❏ **Private Key**: turite nustatyti.
     - ❏ **Password**: nekonfigūruokite.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: pasirenkama
   - ❏ PKCS#12 formato sertifikatas, gautas iš kompiuterio
     - ❏ **Private Key**: nekonfigūruokite.
     - ❏ **Password**: pasirenkama
     - ❏ **CA Certificate 1**/**CA Certificate 2**: nekonfigūruokite.

4. Spustelėkite **OK**.

   Rodomas baigimo pranešimas.

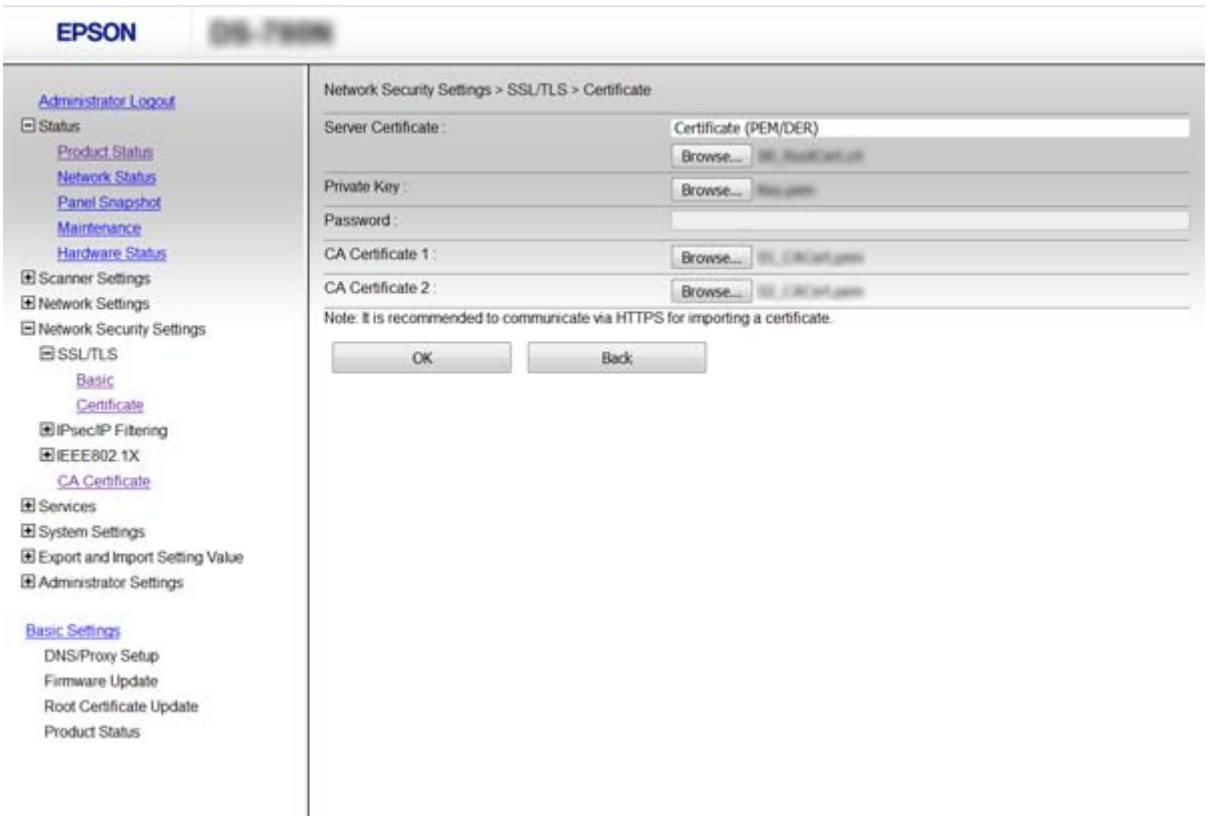
Pastaba:
Spustelėkite ***Confirm*** *ir patikrinkite sertifikato informaciją.*

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „SI pasirašyto sertifikato importavimo nustatymo elementai” puslapyje 67

SI pasirašyto sertifikato importavimo nustatymo elementai



Elementai	Nuostatos ir paaiškinimai
Server Certificate arba Client Certificate	Pasirinkite sertifikato formatą.
Private Key	Jei naudodami kompiuteryje sukurtą CSR gausite PEM / DER formato sertifikatą, nurodykite asmeniško rakto failą, atitinkantį sertifikatą.
Password	Norėdami šifruoti asmenišką raktą, įveskite slaptažodį.
CA Certificate 1	Jei jūsų sertifikato formatas yra **Certificate (PEM/DER)**, importuokite sertifikatą, kurį išdavė sertifikavimo institucija, išduodanti serverio sertifikatą. Jei reikia, nurodykite failą.
CA Certificate 2	Jei jūsų sertifikato formatas yra **Certificate (PEM/DER)**, importuokite sertifikatą, kurį išdavė **CA Certificate 1** išduodanti sertifikavimo institucija. Jei reikia, nurodykite failą.

Susijusi informacija

➡ „SI pasirašyto sertifikato importavimas” puslapyje 65

SI pasirašyto sertifikato šalinimas

Pasibaigus sertifikato galiojimo laikui ar kai nebereikalingas šifruojamas ryšys, galite pašalinti importuotą sertifikatą.

> ***Svarbu:***
> *Jei sertifikatą gausite naudodami Web Config, sukurtą CSR, negalėsite vėl importuoti pašalinto sertifikato. Tokiu atveju sukurkite CSR ir vėl gaukite sertifikatą.*

1. Atverkite Web Config, tada pasirinkite **Network Security Settings**. Toliau pasirinkite **SSL/TLS** > **Certificate** arba **IPsec/IP Filtering** > **Client Certificate** arba **IEEE802.1X** > **Client Certificate**.
2. Spustelėkite **Delete**.
3. Pateiktame pranešime patvirtinkite, kad norite panaikinti sertifikatą.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Naudotojo pasirašyto sertifikato atnaujinimas

Jei skaitytuvas palaiko HTTPS serverio funkciją, galite atnaujinti naudotojas pasirašomą sertifikatą. Kai naudojant naudotojo pasirašomą sertifikatą įjungiama Web Config, rodomas įspėjamasis pranešimas.

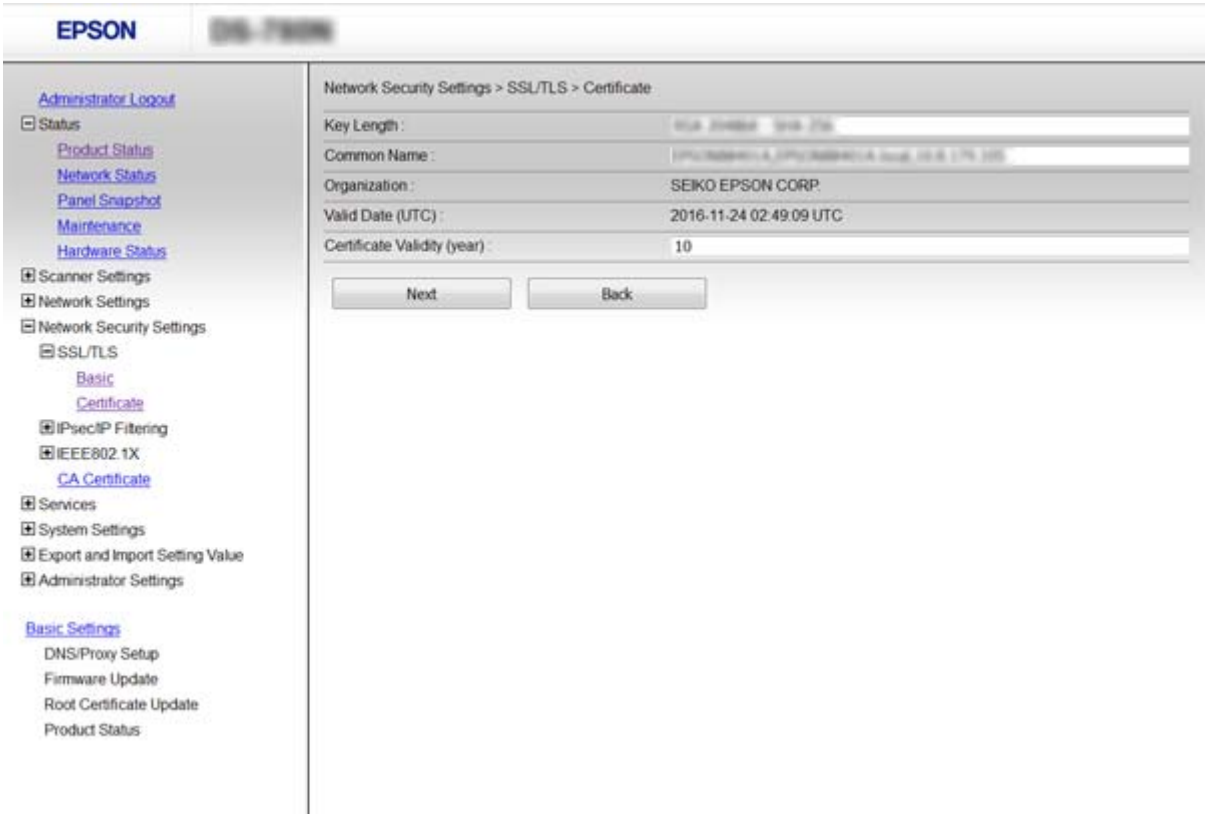
Naudotojo pasirašomą sertifikatą naudokite laikinai, kol gausite ir importuosite SI pasirašytą sertifikatą.

1. Atverkite Web Config ir pasirinkite **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Spustelėkite **Update**.
3. Įjunkite **Common Name**.

   Įveskite IP adresą arba identifikatorių, pvz., skaitytuvo FQDN pavadinimą. Galite įvesti nuo 1 iki 128 simbolių.

   Pastaba:
   Pavadinimą (CN) galite atskirti kableliais.

4. Nurodykite sertifikato galiojimo laikotarpį.



5. Spustelėkite **Next**.

   Rodomas patvirtinimo pranešimas.

6. Spustelėkite **OK**.

   Skaitytuvas yra atnaujintas.

Pastaba:
*Spustelėkite **Confirm** ir patikrinkite sertifikato informaciją.*

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

CA Certificate konfigūravimas

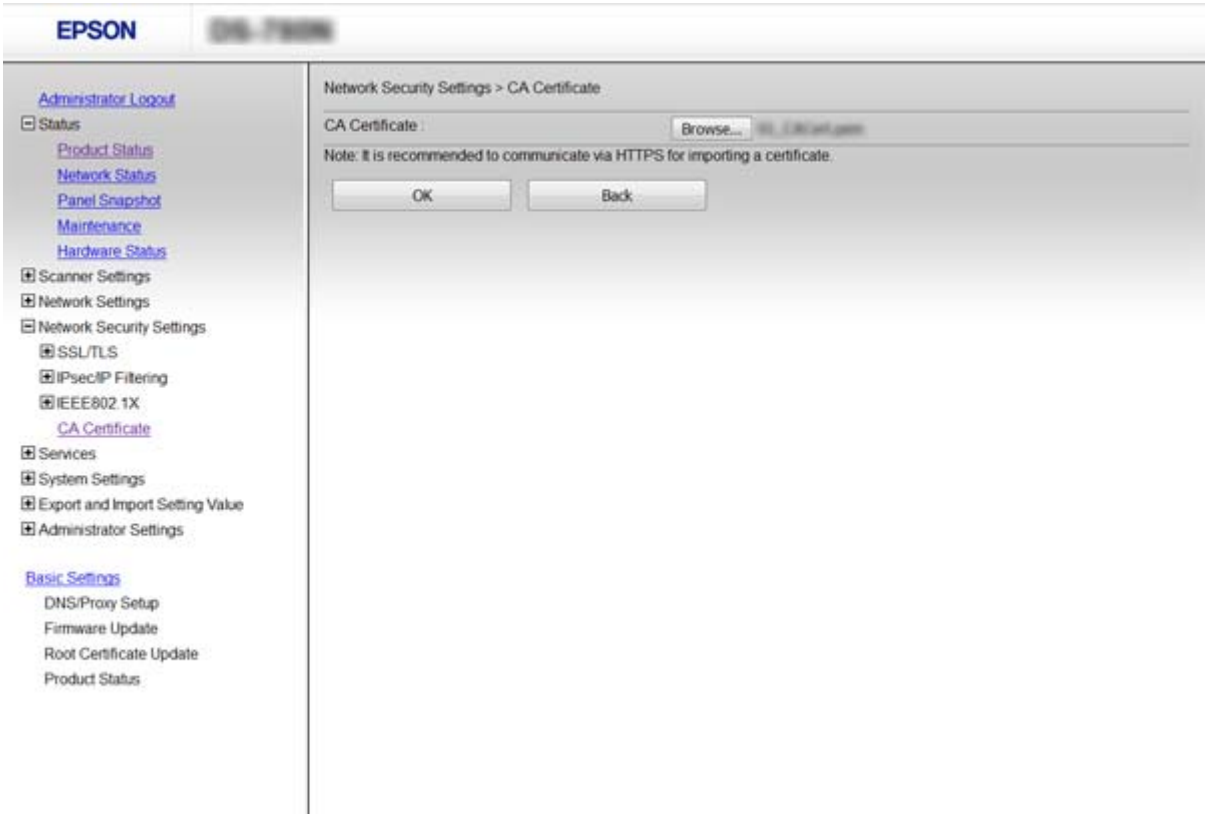
CA Certificate galite importuoti, rodyti arba panaikinti.

CA Certificate importavimas

1. Atverkite Web Config, tada pasirinkite **Network Security Settings** > **CA Certificate**.

2. Spustelėkite **Import**.

3. Nurodykite norimą importuoti CA Certificate.



4. Spustelėkite **OK**.

Importavimui pasibaigus, vėl atidaromas **CA Certificate** ekranas ir rodomas importuotas CA Certificate.

Susijusi informacija

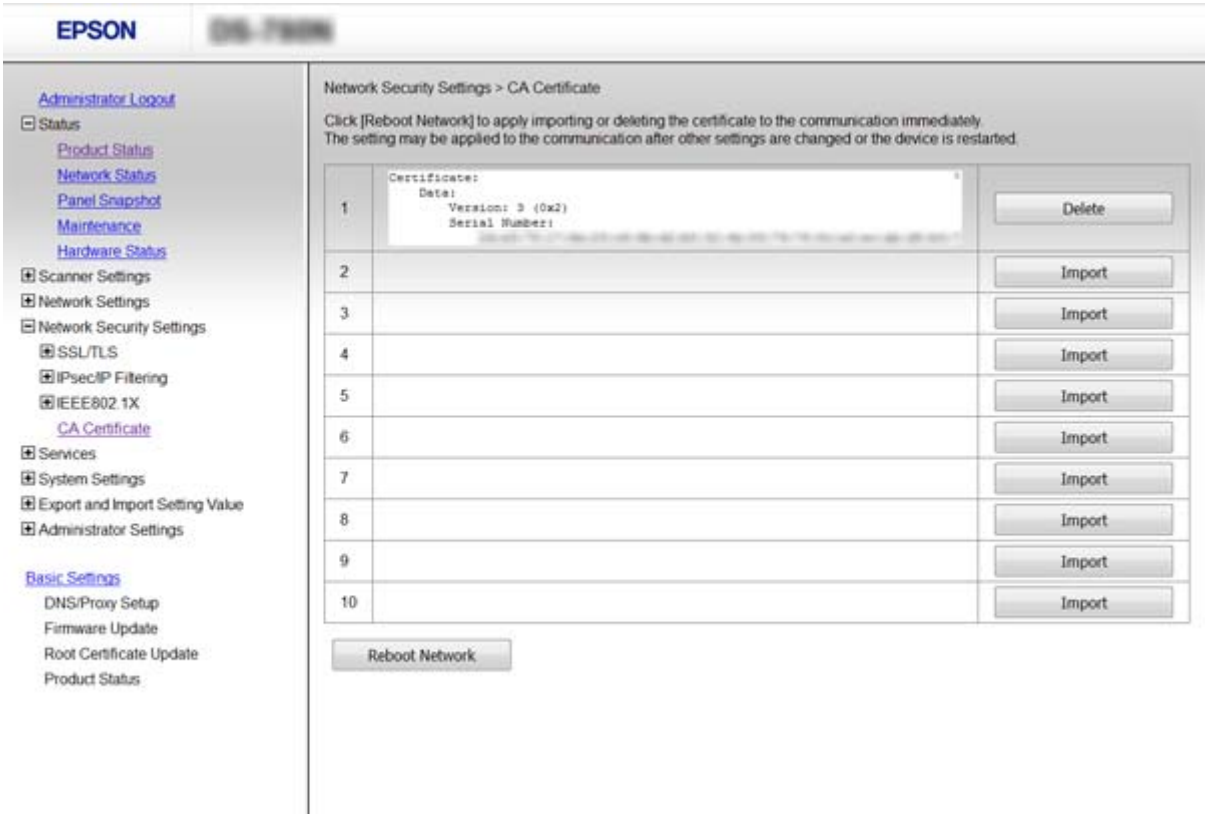
➡ „Prieiga prie Web Config” puslapyje 23

CA Certificate panaikinimas

Importuotą CA Certificate galite panaikinti.

1. Atverkite Web Config, tada pasirinkite **Network Security Settings** > **CA Certificate**.

2. Spustelėkite **Delete** prie CA Certificate, kurį norite panaikinti.



3. Pateiktame pranešime patvirtinkite, kad norite panaikinti sertifikatą.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Užkoduota komunikacija naudojant „IPsec“ / IP filtravimą

Apie IPsec/IP Filtering

Skaitytuvui palaikant „IPsec“ / „IP Filtering“, galite filtruoti srautą pagal IP adresus, paslaugas ir prievadą. Derinant filtravimą, galima sukonfigūruoti skaitytuvą taip, kad priimtų arba blokuotų nurodytus klientus ir duomenis. Be to, naudodami „IPsec“, galite pagerinti saugos lygį.

Norėdami filtruoti srautą, sukonfigūruokite numatytąją politiką. Numatytoji politika taikoma kiekvienam vartotojui ar grupei, kuri jungiasi prie skaitytuvo. Kad galėtumėte dar išsamiau valdyti vartotojus ir vartotojų grupes, sukonfigūruokite grupės politikas. Grupės politika yra viena ar daugiau taisyklių, taikomų vartotojui ar vartotojų grupei. Skaitytuvas valdo IP paketus, kurie atitinka sukonfigūruotas politikas. IP paketų autentiškumas yra patvirtintas grupės politikos nuo 1 iki 10 tvarka, paskui pritaikant numatytąją politiką.

Pastaba:
Windows Vista arba naujesnę, Windows Server 2008 arba naujesnę OS turintis kompiuteris palaiko „IPsec“.

Default Policy konfigūravimas

1. Atverkite Web Config ir pasirinkite **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Įveskite vertę kiekvienam elementui.
3. Spustelėkite **Next**.

   Rodomas patvirtinimo pranešimas.
4. Spustelėkite **OK**.

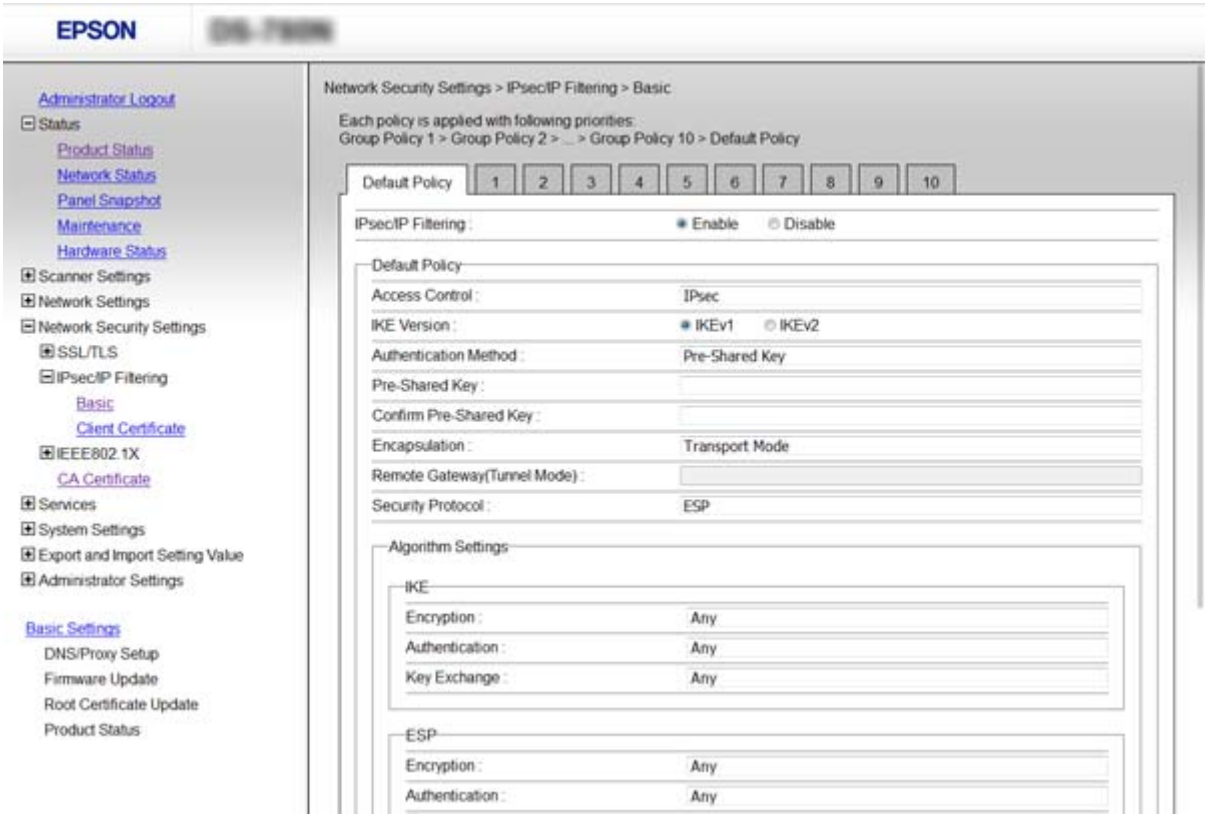
   Skaitytuvas yra atnaujintas.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „Default Policy nustatymo elementai” puslapyje 72

Default Policy nustatymo elementai



Elementai	Nuostatos ir paaiškinimai
IPsec/IP Filtering	Galite įjungti ar išjungti „IPsec“ / „IP Filtering“ funkciją.

Išplėstiniai saugumo nustatymai verslui

Elementai	Nuostatos ir paaiškinimai	
Access Control	Sukonfigūruokite IP paketų srauto valdymo metodą.	
	Permit Access	Pažymėkite, norėdami suteikti prieigą sukonfigūruotiems IP paketams.
	Refuse Access	Pažymėkite, norėdami uždrausti prieigą sukonfigūruotiems IP paketams.
	IPsec	Pažymėkite, norėdami suteikti prieigą sukonfigūruotiems „IPsec“ paketams.
IKE Version	IKE versijai pasirinkite IKEv1 arba IKEv2. Pasirinkite vieną iš jų pagal įrenginį, prie kurio prijungtas skaitytuvas.	
IKEv1	Šie elementai rodomi pasirinkus **IKEv1**, skirtą **IKE Version**.	
	Authentication Method	Norėdami pažymėti **Certificate**, turite iš anksto gauti ir importuoti SI pasirašytą sertifikatą.
	Pre-Shared Key	Pažymėję **Pre-Shared Key** kaip **Authentication Method**, įveskite 1–127 simbolių ilgio iš anksto bendrinamą raktą.
	Confirm Pre-Shared Key	Įveskite sukonfigūruotą raktą patvirtinimui.
IKEv2	Šie elementai rodomi pasirinkus **IKEv2**, skirtą **IKE Version**.	
Local	Authentication Method	Norėdami pažymėti **Certificate**, turite iš anksto gauti ir importuoti SI pasirašytą sertifikatą.
	ID Type	Pasirinkite skaitytuvo ID tipą.
	ID	Įveskite skaitytuvo ID, atitinkantį ID tipą. Pirmas simbolis negali būti „@“, „#“ ir „=“. **Distinguished Name**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „=“. **IP Address**: įveskite IPv4 arba IPv6 formatą. **FQDN**: įveskite 1–255 simbolių derinį, naudodami A–Z, a–z, 0–9 ir „-“ ir tašką (.). **Email Address**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „@“. **Key ID**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius.
	Pre-Shared Key	Pažymėję **Pre-Shared Key** kaip **Authentication Method**, įveskite 1–127 simbolių ilgio iš anksto bendrinamą raktą.
	Confirm Pre-Shared Key	Įveskite sukonfigūruotą raktą patvirtinimui.

Išplėstiniai saugumo nustatymai verslui

Elementai	Nuostatos ir paaiškinimai	
Remote	Authentication Method	Norėdami pažymėti **Certificate**, turite iš anksto gauti ir importuoti SI pasirašytą sertifikatą.
	ID Type	Pasirinkite įrenginio, kurį norite autentifikuoti, ID tipą.
	ID	Įveskite skaitytuvo ID, atitinkantį ID tipą. Pirmas simbolis negali būti „@“, „#“ ir „=“. **Distinguished Name**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „=“. **IP Address**: įveskite IPv4 arba IPv6 formatą. **FQDN**: įveskite 1–255 simbolių derinį, naudodami A–Z, a–z, 0–9 ir „-“ ir tašką (.). **Email Address**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „@“. **Key ID**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius.
	Pre-Shared Key	Pažymėję **Pre-Shared Key** kaip **Authentication Method**, įveskite 1–127 simbolių ilgio iš anksto bendrinamą raktą.
	Confirm Pre-Shared Key	Įveskite sukonfigūruotą raktą patvirtinimui.
Encapsulation	Pažymėję **IPsec** kaip **Access Control**, turėsite sukonfigūruoti paketų formavimo režimą.	
	Transport Mode	Pažymėkite, jei skaitytuvą naudosite tame pačiame LAN. 4 ar naujesnio lygio IP paketai yra užšifruoti.
	Tunnel Mode	Jeigu skaitytuvą naudojate prie interneto prijungtame tinkle, pvz., IPsec-VPN, pasirinkite šią parinktį. IP paketų antraštė ir duomenys yra užšifruoti.
Remote Gateway(Tunnel Mode)	Pažymėję **Tunnel Mode** kaip **Encapsulation**, įveskite 1–39 simbolių tinklų sąsajos adresą.	
Security Protocol	**IPsec**, skirtas **Access Control**, pasirinkite parinktį.	
	ESP	Pasirinkite, norėdami užtikrinti autentiškumo patvirtinimo ir duomenų vientisumą bei užšifruoti duomenis.
	AH	Pasirinkite, norėdami užtikrinti autentiškumo patvirtinimo ir duomenų vientisumą. Net jei draudžiama šifruoti duomenis, galite naudoti „IPsec“.
Algorithm Settings		
IKE	Encryption	Pasirinkite kodavimo algoritmą, skirtą IKE. Elementai skiriasi priklausomai nuo IKE versijos.
	Authentication	Pasirinkite autentifikavimo algoritmą, skirtą IKE.
	Key Exchange	Pasirinkite raktų mainų algoritmą, skirtą IKE. Elementai skiriasi priklausomai nuo IKE versijos.

Elementai	Nuostatos ir paaiškinimai	
ESP	Encryption	Pasirinkite kodavimo algoritmą, skirtą ESP. Tai prieinama, kai **ESP** yra pasirinkta **Security Protocol**.
	Authentication	Pasirinkite autentifikavimo algoritmą, skirtą ESP. Tai prieinama, kai **ESP** yra pasirinkta **Security Protocol**.
AH	Authentication	Pasirinkite kodavimo algoritmą, skirtą AH. Tai prieinama, kai **AH** yra pasirinkta **Security Protocol**.

Susijusi informacija

➡ „Default Policy konfigūravimas” puslapyje 72

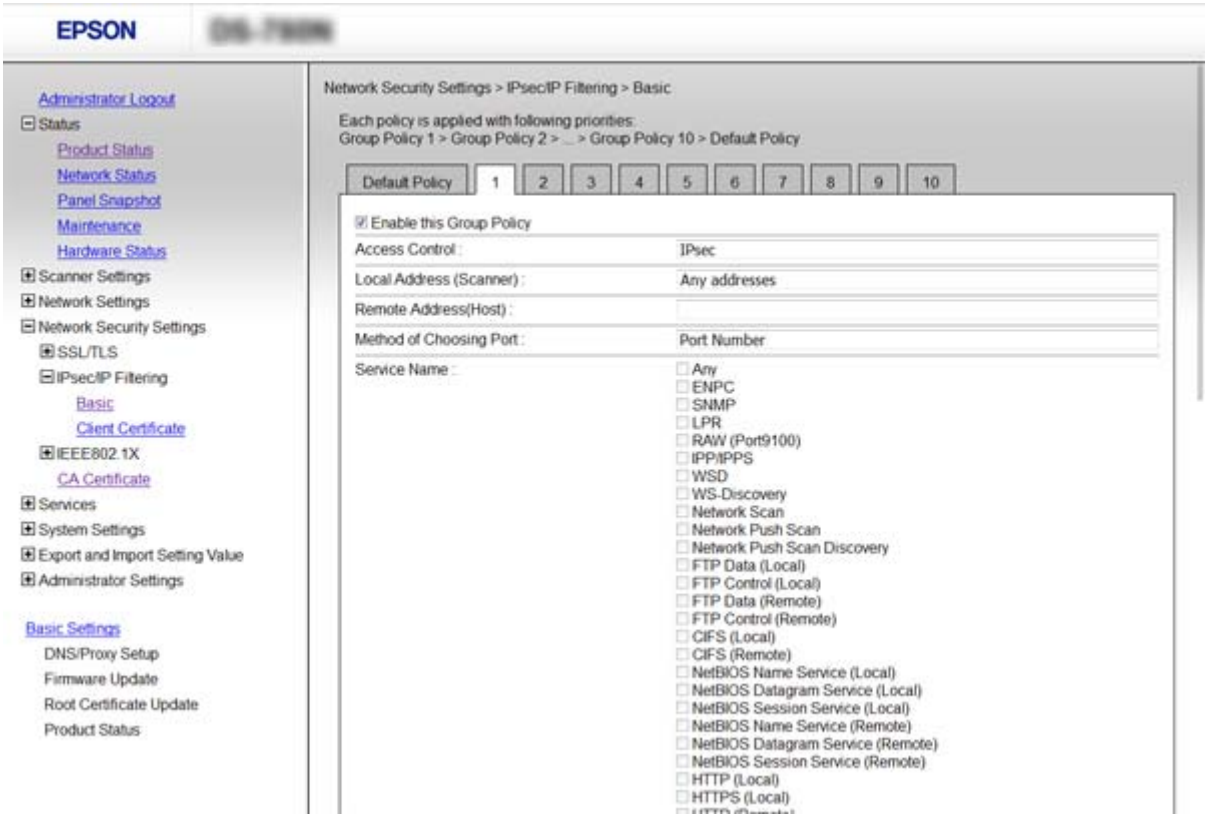
Group Policy konfigūravimas

1. Atverkite Web Config ir pasirinkite **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Spustelėkite norimos konfigūruoti kortelės numerį.
3. Įveskite vertę kiekvienam elementui.
4. Spustelėkite **Next**.
   Rodomas patvirtinimo pranešimas.
5. Spustelėkite **OK**.
   Skaitytuvas yra atnaujintas.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23
➡ „Group Policy nustatymo elementai” puslapyje 76

Group Policy nustatymo elementai



Elementai	Nuostatos ir paaiškinimai	
Enable this Group Policy	Galite įjungti arba išjungti grupės politiką.	
Access Control	Sukonfigūruokite IP paketų srauto valdymo metodą.	
	Permit Access	Pažymėkite, norėdami suteikti prieigą sukonfigūruotiems IP paketams.
	Refuse Access	Pažymėkite, norėdami uždrausti prieigą sukonfigūruotiems IP paketams.
	IPsec	Pažymėkite, norėdami suteikti prieigą sukonfigūruotiems „IPsec“ paketams.
Local Address (Scanner)	Pasirinkite IPv4 adresą arba IPv6 adresą, atitinkantį savo tinklo aplinką. Jeigu IP adresas yra priskiriamas automatiškai, galite pasirinkti **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Norėdami valdyti prieigą, įveskite įrenginio IP adresą. IP adresas turi būti 43 simbolių arba trumpesnis. Neįvedus IP adreso, bus valdomi visi adresai. ***Pastaba:*** *Jei IP adresas yra priskiriamas automatiškai (pvz., jį priskiria DHCP), ryšys gali būti neprieinamas. Sukonfigūruokite statinį IP adresą.*	
Method of Choosing Port	Pasirinkite prievadų nurodymų metodą.	
Service Name	Pasirinkę **Service Name** kaip **Method of Choosing Port**, pažymėkite parinktį.	

Išplėstiniai saugumo nustatymai verslui

Elementai	Nuostatos ir paaiškinimai	
Transport Protocol	Pažymėję **Port Number** kaip **Method of Choosing Port**, turėsite sukonfigūruoti paketų formavimo režimą.	
	Any Protocol	Pažymėkite, norėdami valdyti visus protokolų tipus.
	TCP	Pažymėkite, norėdami valdyti duomenų perdavimą vienu adresu.
	UDP	Pažymėkite, norėdami valdyti duomenų transliaciją ir perdavimą daugybe adresų.
	ICMPv4	Pažymėkite, norėdami valdyti ryšio užklausos komandą.
Local Port	Jeigu pasirinksite **Port Number**, skirtą **Method of Choosing Port** ir pasirinksite **TCP** arba **UDP**, skirtą **Transport Protocol**, įveskite prievado numerius gaunamų paketų valdymui, atskirdami juos kableliais. Daugiausia galite įvesti 10 prievado numerių. Pavyzdžiui: 20,80,119,5220 Neįvedus prievado numerio, bus valdomi visi prievadai.	
Remote Port	Jeigu pasirinksite **Port Number**, skirtą **Method of Choosing Port** ir pasirinksite **TCP** arba **UDP**, skirtą **Transport Protocol**, įveskite prievado numerius siunčiamų paketų valdymui, atskirdami juos kableliais. Daugiausia galite įvesti 10 prievado numerių. Pavyzdžiui: 25,80,143,5220 Neįvedus prievado numerio, bus valdomi visi prievadai.	
IKE Version	IKE versijai pasirinkite IKEv1 arba IKEv2. Pasirinkite vieną iš jų pagal įrenginį, prie kurio prijungtas skaitytuvas.	
IKEv1	Šie elementai rodomi pasirinkus **IKEv1**, skirtą **IKE Version**.	
	Authentication Method	Pasirinkę **IPsec** kaip **Access Control**, pažymėkite parinktį. Naudojamas sertifikatas atitinka numatytąją politiką.
	Pre-Shared Key	Pažymėję **Pre-Shared Key** kaip **Authentication Method**, įveskite 1–127 simbolių ilgio iš anksto bendrinamą raktą.
	Confirm Pre-Shared Key	Įveskite sukonfigūruotą raktą patvirtinimui.
IKEv2	Šie elementai rodomi pasirinkus **IKEv2**, skirtą **IKE Version**.	

Išplėstiniai saugumo nustatymai verslui

Elementai	Nuostatos ir paaiškinimai	
Local	Authentication Method	Pasirinkę **IPsec** kaip **Access Control**, pažymėkite parinktį. Naudojamas sertifikatas atitinka numatytąją politiką.
	ID Type	Pasirinkite skaitytuvo ID tipą.
	ID	Įveskite skaitytuvo ID, atitinkantį ID tipą. Pirmas simbolis negali būti „@“, „#“ ir „=“. **Distinguished Name**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „=“. **IP Address**: įveskite IPv4 arba IPv6 formatą. **FQDN**: įveskite 1–255 simbolių derinį, naudodami A–Z, a–z, 0–9 ir „-“ ir tašką (.). **Email Address**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „@“. **Key ID**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius.
	Pre-Shared Key	Pažymėję **Pre-Shared Key** kaip **Authentication Method**, įveskite 1–127 simbolių ilgio iš anksto bendrinamą raktą.
	Confirm Pre-Shared Key	Įveskite sukonfigūruotą raktą patvirtinimui.
Remote	Authentication Method	Pasirinkę **IPsec** kaip **Access Control**, pažymėkite parinktį. Naudojamas sertifikatas atitinka numatytąją politiką.
	ID Type	Pasirinkite įrenginio, kurį norite autentifikuoti, ID tipą.
	ID	Įveskite skaitytuvo ID, atitinkantį ID tipą. Pirmas simbolis negali būti „@“, „#“ ir „=“. **Distinguished Name**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „=“. **IP Address**: įveskite IPv4 arba IPv6 formatą. **FQDN**: įveskite 1–255 simbolių derinį, naudodami A–Z, a–z, 0–9 ir „-“ ir tašką (.). **Email Address**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius. Būtina įtraukti „@“. **Key ID**: įveskite 1–128 1 baito ASCII (0x20–0x7E) simbolius.
	Pre-Shared Key	Pažymėję **Pre-Shared Key** kaip **Authentication Method**, įveskite 1–127 simbolių ilgio iš anksto bendrinamą raktą.
	Confirm Pre-Shared Key	Įveskite sukonfigūruotą raktą patvirtinimui.
Encapsulation	Pažymėję **IPsec** kaip **Access Control**, turėsite sukonfigūruoti paketų formavimo režimą.	
	Transport Mode	Pažymėkite, jei skaitytuvą naudosite tame pačiame LAN. 4 ar naujesnio lygio IP paketai yra užšifruoti.
	Tunnel Mode	Jeigu skaitytuvą naudojate prie interneto prijungtame tinkle, pvz., IPsec-VPN, pasirinkite šią parinktį. IP paketų antraštė ir duomenys yra užšifruoti.
Remote Gateway(Tunnel Mode)	Pažymėję **Tunnel Mode** kaip **Encapsulation**, įveskite 1–39 simbolių tinklų sąsajos adresą.	

Išplėstiniai saugumo nustatymai verslui

Elementai	Nuostatos ir paaiškinimai	
Security Protocol	Pasirinkę **IPsec** kaip **Access Control**, pažymėkite parinktį.	
	ESP	Pasirinkite, norėdami užtikrinti autentiškumo patvirtinimo ir duomenų vientisumą bei užšifruoti duomenis.
	AH	Pasirinkite, norėdami užtikrinti autentiškumo patvirtinimo ir duomenų vientisumą. Net jei draudžiama šifruoti duomenis, galite naudoti „IPsec“.
Algorithm Settings		
IKE	Encryption	Pasirinkite kodavimo algoritmą, skirtą IKE. Elementai skiriasi priklausomai nuo IKE versijos.
	Authentication	Pasirinkite autentifikavimo algoritmą, skirtą IKE.
	Key Exchange	Pasirinkite raktų mainų algoritmą, skirtą IKE. Elementai skiriasi priklausomai nuo IKE versijos.
ESP	Encryption	Pasirinkite kodavimo algoritmą, skirtą ESP. Tai prieinama, kai **ESP** yra pasirinkta **Security Protocol**.
	Authentication	Pasirinkite autentifikavimo algoritmą, skirtą ESP. Tai prieinama, kai **ESP** yra pasirinkta **Security Protocol**.
AH	Authentication	Pasirinkite autentifikavimo algoritmą, skirtą AH. Tai prieinama, kai **AH** yra pasirinkta **Security Protocol**.

Susijusi informacija

➡ „Group Policy konfigūravimas” puslapyje 75

➡ „Local Address (Scanner) ir Remote Address(Host) derinys Group Policy” puslapyje 79

➡ „Paslaugos pavadinimo nuorodos grupės politikoje” puslapyje 80

Local Address (Scanner) ir Remote Address(Host) derinys Group Policy

		Local Address (Scanner) nuostata		
		IPv4	IPv6*2	Any addresses*3
Remote Address(Host) nuostata	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Tuščias	✓	✓	✓

*1 Jeigu **IPsec** pasirenkamas **Access Control**, negalite nustatyti prefikso ilgio.

*2 Jeigu **IPsec** pasirenkamas **Access Control**, galite pasirinkti nuorodos vietos adresą (fe80::), tačiau grupės politika bus išjungta.

*3 Išskyrus IPv6 nuorodos vietos adresus.

Paslaugos pavadinimo nuorodos grupės politikoje

Pastaba:
Rodomos negalimos paslaugos, tačiau jų negalima pasirinkti.

Paslaugos pavadinimas	Protokolo tipas	Vietinio prievado numeris	Nuotolinio prievado numeris	Valdomos funkcijos
Any	–	–	–	Visos paslaugos
ENPC	UDP	3289	Bet kuris prievadas	Ieškoma skaitytuvo iš tokių programų, kaip EpsonNet Config ir skaitytuvo tvarkyklė
SNMP	UDP	161	Bet kuris prievadas	Gaunama ir konfigūruojama MIB iš tokių programų, kaip EpsonNet Config ir Epson skaitytuvo tvarkyklė
WSD	TCP	Bet kuris prievadas	5357	Valdomas WSD
WS-Discovery	UDP	3702	Bet kuris prievadas	Ieškoma skaitytuvo iš WSD
Network Scan	TCP	1865	Bet kuris prievadas	Persiunčiami nuskaitymo duomenys iš Document Capture Pro
Network Push Scan Discovery	UDP	2968	Bet kuris prievadas	Skaitytuve ieškoma kompiuterio.
Network Push Scan	TCP	Bet kuris prievadas	2968	Gaunama nuskaitymo paspaudus mygtuką užduoties informacija iš Document Capture Pro arba Document Capture
HTTP (Local)	TCP	80	Bet kuris prievadas	HTTP(S) serveris (persiunčiami Web Config ir WSD duomenys)
HTTPS (Local)	TCP	443	Bet kuris prievadas	
HTTP (Remote)	TCP	Bet kuris prievadas	80	HTTP(S) klientas (ryšys tarp programinės aparatinės įrangos atnaujinimo ir šakninio sertifikato atnaujinimo)
HTTPS (Remote)	TCP	Bet kuris prievadas	443	

IPsec/IP Filtering konfigūracijos pavyzdžiai

Tik „IPsec“ paketų gavimas

Šis pavyzdys rodo, kaip sukonfigūruoti tik numatytąją politiką.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: įveskite iki 127 simbolių.

Group Policy:

nekonfigūruokite.

Nuskaitymo duomenų priėmimas naudojant Epson Scan 2 ir skaitytuvo nustatymus

Šis pavyzdys suteikia galimybę perduoti nurodytų paslaugų nuskaitymo duomenis ir skaitytuvo konfigūracijas.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: pažymėkite langelį.

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

❏ **Remote Address(Host)**: kliento IP adresas

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

❏ **Service Name**: pažymėkite langelį **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** ir **HTTPS (Local)**.

Prieigos tik iš nurodyto IP adreso gavimas

Šiame pavyzdyje leidžiama nustatytam IP adresui pasiekti skaitytuvą.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: pažymėkite langelį.

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

❏ **Remote Address(Host)**: administratoriaus kliento IP adresas

Pastaba:
Nepaisant konfigūracijos politikos, klientas galės pasiekti ir sukonfigūruoti skaitytuvą.

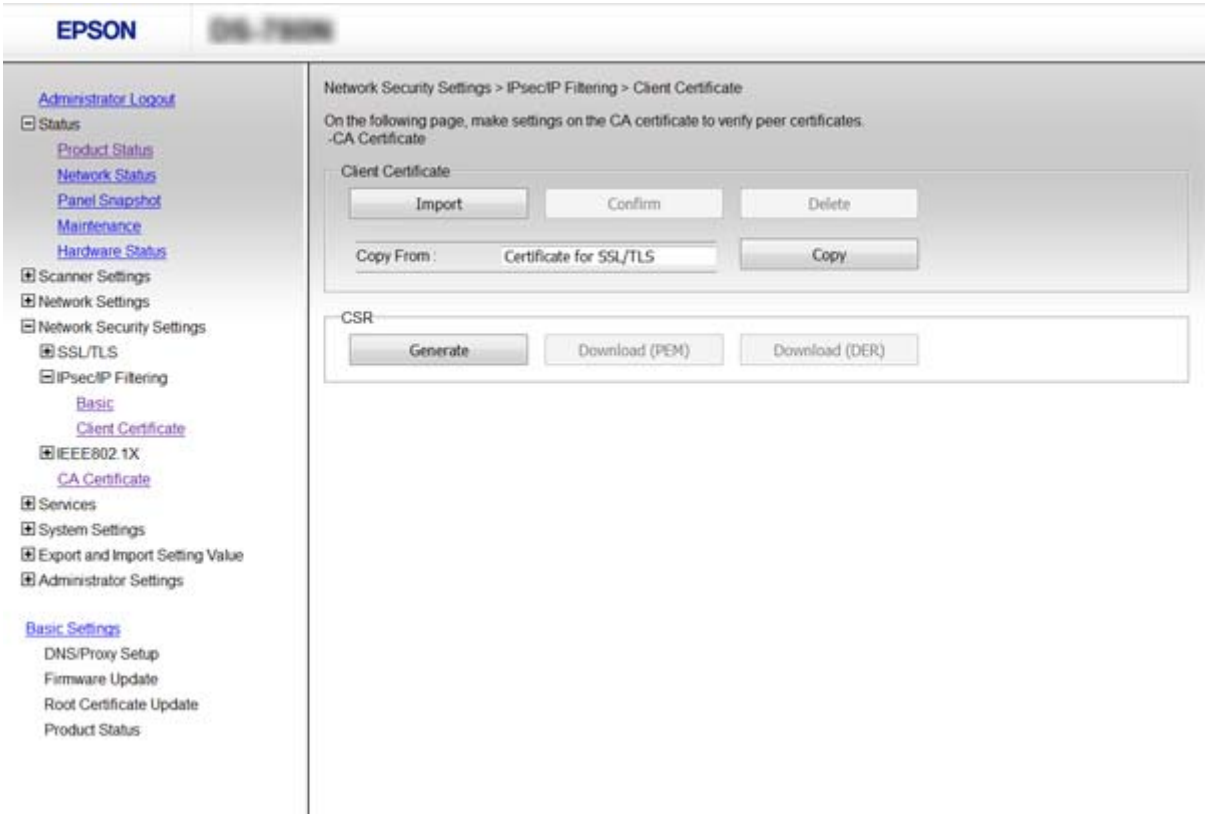
IPsec/IP Filtering sertifikato konfigūravimas

Konfigūruokite kliento „IPsec“ / „IP Filtering“ sertifikatą. Jei norite konfigūruoti sertifikavimo tarnybą, eikite į **CA Certificate**.

1. Atverkite Web Config ir pasirinkite **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importuokite sertifikatą skiltyje **Client Certificate**.

   Jei jau importavote sertifikatą, išleistą IEEE802.1X arba SSL / TLS Sertifikavimo institucijos, galite jį nukopijuoti ir naudoti „IPsec“ / „IP Filtering“ operacijai. Norėdami nukopijuoti, pasirinkite sertifikatą iš **Copy From**, paskui spustelėkite **Copy**.



Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „SI pasirašyto sertifikato gavimas ir importavimas” puslapyje 64

„SNMPv3“ protokolo naudojimas

Apie SNMPv3

SNMP yra protokolas, vykdantis stebėjimą ir valdantis įrenginių, prijungtų prie tinklo, informacijos rinkimą. SNMPv3 yra patobulinta valdymo saugumo funkcijos versija.

Naudojant SNMPv3, SNMP komunikacijos (paketo) būsenos stebėjimą ir nustatymo pakeitimus galima autentifikuoti ir užkoduoti, norint apsaugoti SNMP komunikaciją (paketą) nuo tinklo grėsmių, pvz. pasiklausymo, apsimetinėjimo ir klastojimo.

SNMPv3 konfigūravimas

Jeigu skaitytuvas palaiko SNMPv3 protokolą, galite stebėti ir valdyti prieigą prie skaitytuvo.

1. Atverkite Web Config ir pasirinkite **Services** > **Protocol**.
2. Įveskite vertę kiekvienam **SNMPv3 Settings** priklausančiam elementui.
3. Spustelėkite **Next**.

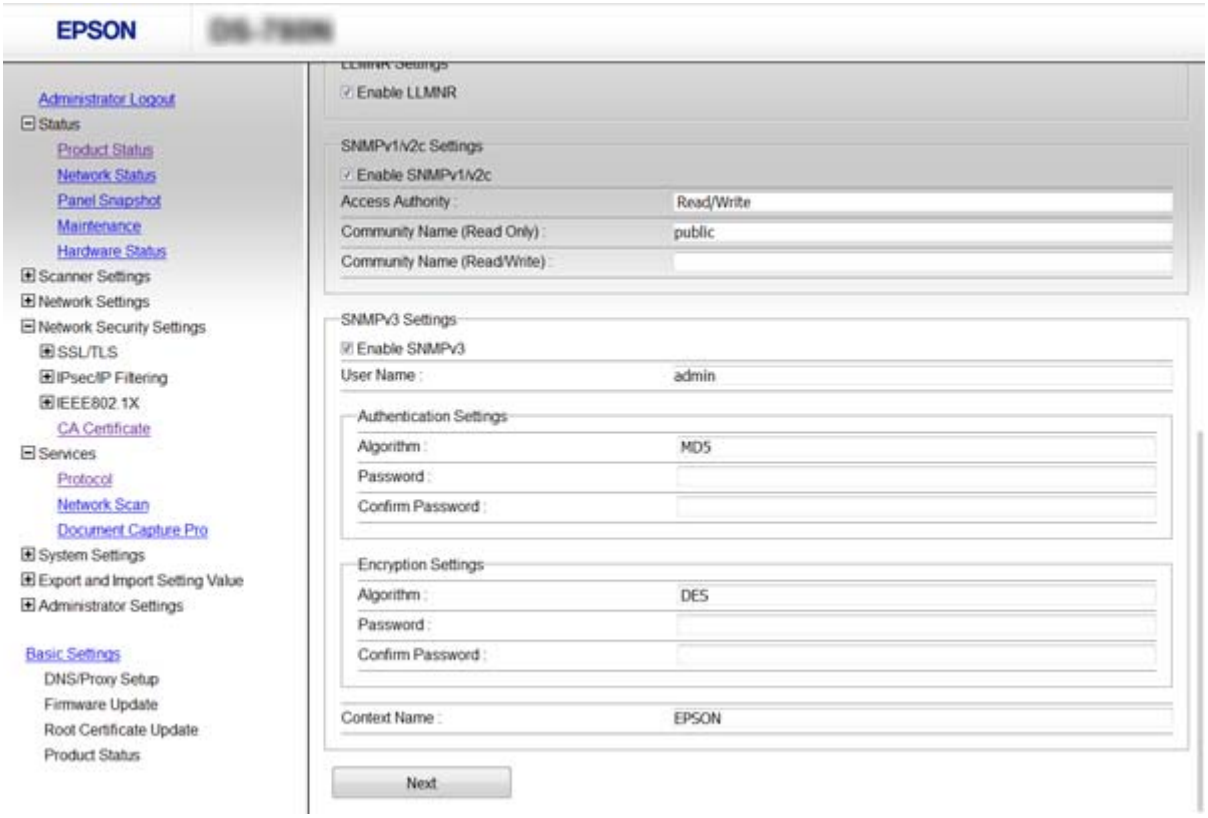
   Rodomas patvirtinimo pranešimas.
4. Spustelėkite **OK**.

   Skaitytuvas yra atnaujintas.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23
➡ „„SNMPv3“ nustatymo elementai” puslapyje 83

„SNMPv3“ nustatymo elementai



Elementai	Nuostatos ir paaiškinimai
Enable SNMPv3	Pažymėjus langelį, „SNMPv3“ yra įjungta.
User Name	Įrašykite 1–32 ženklus, naudodami 1 bito ženklus.
Authentication Settings	
Algorithm	Pasirinkite patvirtinimo algoritmą.

Elementai	Nuostatos ir paaiškinimai
Password	Įrašykite 8–32 ženklų ilgio unikodą ASCII (0x20-0x7E).
Confirm Password	Įveskite slaptažodį, kurį sukonfigūravote patvirtinimui.
Encryption Settings	
Algorithm	Pasirinkite šifravimo algoritmą.
Password	Įrašykite 8–32 ženklų ilgio unikodą ASCII (0x20-0x7E).
Confirm Password	Įveskite slaptažodį, kurį sukonfigūravote patvirtinimui.
Context Name	Įrašykite 1–32 ženklus, naudodami 1 bito ženklus.

Susijusi informacija

➡ „SNMPv3 konfigūravimas” puslapyje 82

Skaitytuvo prijungimas prie IEEE802.1X tinklo

IEEE802.1X tinklo sukonfigūravimas

Jei skaitytuvas palaiko IEEE802.1X, skaitytuvą galite naudoti tinkle su autentiškumo patvirtinimu, kuris yra prijungtas prie RADIUS serverio, o šakotuvas turi autentiškumo patvirtinimo įrenginį.

1. Atverkite Web Config ir pasirinkite **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Įveskite vertę kiekvienam elementui.
3. Spustelėkite **Next**.

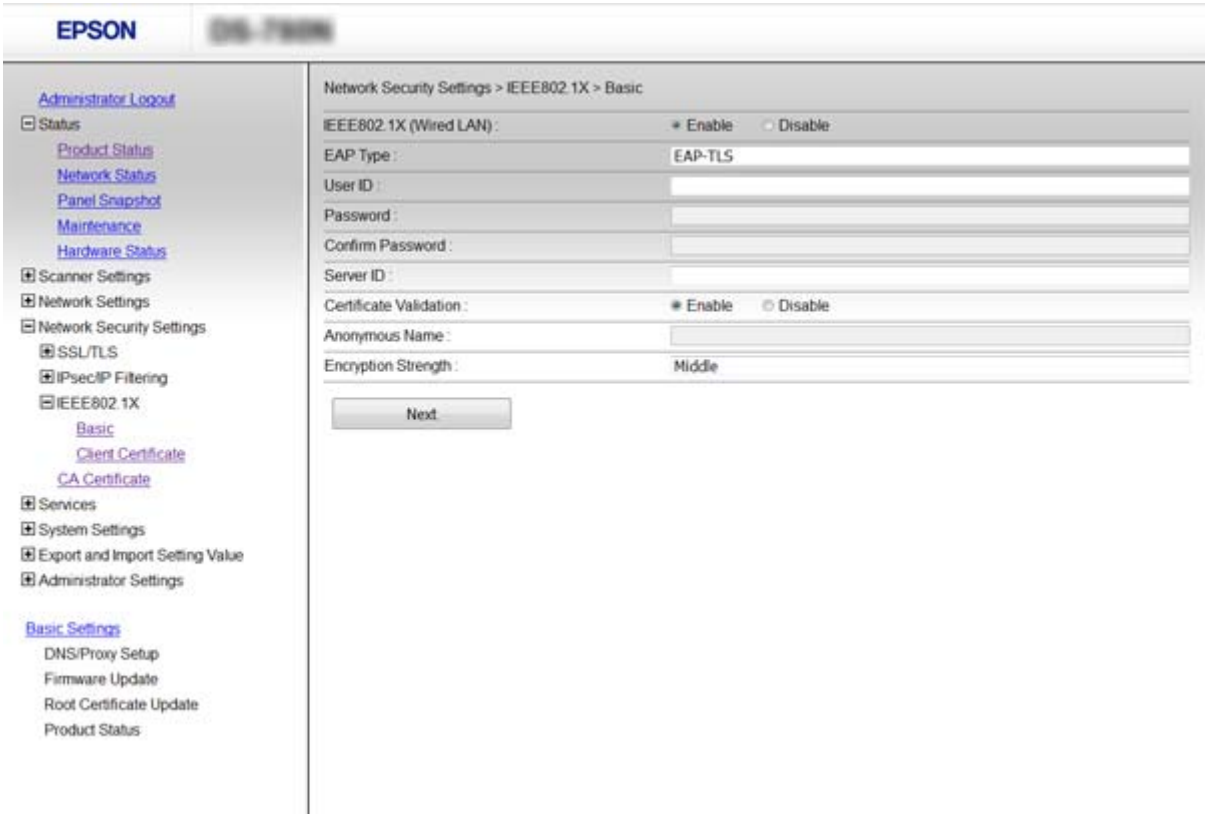
   Rodomas patvirtinimo pranešimas.
4. Spustelėkite **OK**.

   Skaitytuvas yra atnaujintas.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23
➡ „IEEE802.1X tinklo nustatymo elementai” puslapyje 85
➡ „Sukonfigūravus IEEE802.1X, negalima pasiekti spausdintuvo arba skaitytuvo” puslapyje 89

IEEE802.1X tinklo nustatymo elementai



Elementai	Nuostatos ir paaiškinimai	
IEEE802.1X (Wired LAN)	Galite įjungti arba išjungti puslapio parametrus (**IEEE802.1X** > **Basic**), skirtus IEEE802.1X (Laidinis LAN).	
EAP Type	Pasirinkite autentiškumo patvirtinimo tarp skaitytuvo ir RADIUSserverio metodo parinktį.	
	EAP-TLS	Jums reikia gauti ir importuoti SI pasirašytą sertifikatą.
	PEAP-TLS	
	PEAP/MSCHAPv2	Jums reikia sukonfigūruoti slaptažodį.
User ID	Sukonfigūruokite ID, kuris bus naudojamas RADIUS serverio autentiškumui patvirtinti. Įveskite 1–128 1 baito ASCII (0x20 iki 0x7E) simbolius.	
Password	Norėdami patvirtinti skaitytuvo autentiškumą, sukonfigūruokite slaptažodį. Įveskite 1–128 1 baito ASCII (0x20 iki 0x7E) simbolius. Jei Windows serverį naudojate kaip RADIUS serverį, galite įvesti iki 127 simbolių.	
Confirm Password	Įveskite sukonfigūruotą slaptažodį patvirtinimui.	
Server ID	Galite sukonfigūruoti serverio ID, kad galėtumėte autentiškumą patvirtinti nustatytu RADIUS serveriu. Autentiškumo patvirtinimo įrenginys patikrina, ar iš RADIUS serverio atsiųsto serverio sertifikato laukelyje „subject / subjectAltName“ yra serverio ID. Įveskite 0–128 1 baito ASCII (0x20 iki 0x7E) simbolius.	
Certificate Validation	Galite nustatyti sertifikato tikrinimą nepaisant autentiškumo patvirtinimo metodo. Importuokite sertifikatą skiltyje **CA Certificate**.	

Elementai	Nuostatos ir paaiškinimai	
Anonymous Name	Pasirinkus **PEAP-TLS** arba **PEAP/MSCHAPv2** kaip **Authentication Method**, vietoj PEAP autentifikavimo 1 etapo vartotojo ID galima sukonfigūruoti anonimišką pavadinimą. Įveskite 0–128 1 baito ASCII (0x20 iki 0x7E) simbolius.	
Encryption Strength	Galite pasirinkti vieną iš pateiktų toliau.	
	High	AES256 / 3DES
	Middle	AES256 / 3DES / AES128 / RC4

Susijusi informacija

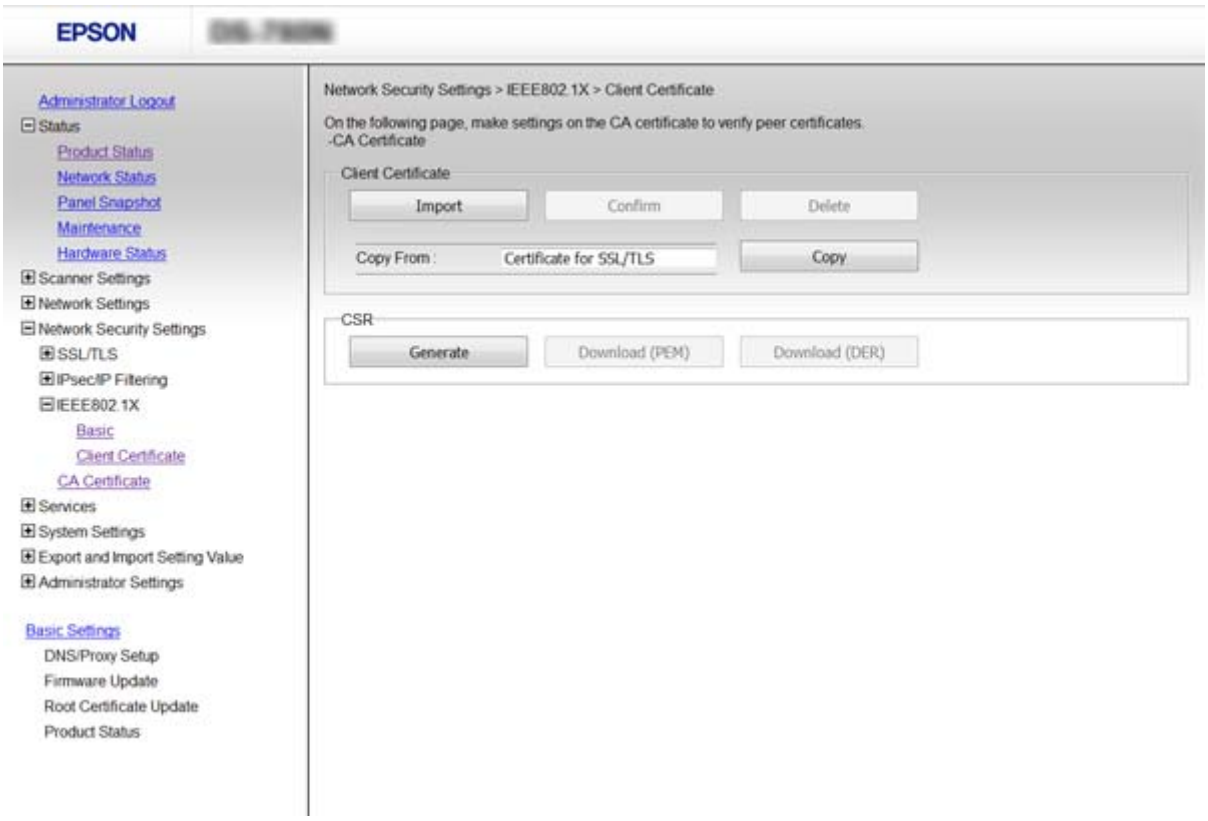
➡ „IEEE802.1X tinklo sukonfigūravimas” puslapyje 84

IEEE802.1X sertifikato konfigūravimas

Sukonfigūruokite kliento IEEE802.1X sertifikatą. Jei norite konfigūruoti sertifikavimo institucijos sertifikatą, eikite į **CA Certificate**.

1. Atverkite Web Config ir pasirinkite **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Eikite į sertifikatą skiltyje **Client Certificate**.

   Galite nukopijuoti sertifikatą, jei jį išduoda sertifikavimo institucija. Norėdami nukopijuoti, pasirinkite sertifikatą iš **Copy From**, paskui spustelėkite **Copy**.



Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „SI pasirašyto sertifikato gavimas ir importavimas” puslapyje 64

Papildomos saugos problemų sprendimas

Saugumo nustatymų atkūrimas

Sukūrus labai saugią aplinką, pvz. „IPsec“ / IP filtravimą arba IEEE802.1X, gali nepavykti komunikuoti su įrenginiais dėl neteisingų nustatymų arba problemų dėl įrenginio arba serverio. Tokiu atveju atkurkite saugumo nustatymus, norėdami iš naujo nustatyti įrenginio nustatymus arba norėdami leisti laikiną naudojimą.

Saugumo funkcijos išjungimas valdymo skydelyje

Galite išjungti „IPsec“ / IP filtravimo funkciją arba IEEE802.1X naudodami skaitytuvo valdymo skydelį.

1. Palieskite **Nuostatos** > **Tinklo nuostatos**.
2. Palieskite „**Keisti nuostatas**“.
3. Palieskite norimus išjungti elementus.
   - ❏ **IPsec/IP filtravimas**
   - ❏ **IEEE802.1X**
4. Kai parodomas užbaigimo pranešimas, palieskite **Tęsti**.

Saugumo funkcijos atkūrimas naudojant tinklo konfigūravimą

IEEE802.1X atveju įrenginiai gali būti neatpažįstami tinkle. Tokiu atveju išjunkite funkciją naudodami skaitytuvo valdymo skydelį.

„IPsec“ / IP filtravimo atveju galite išjungti funkciją, jei galite pasiekti įrenginį iš kompiuterio.

„IPsec“ / IP filtravimo išjungimas, naudojant Web Config

1. Atverkite Web Config ir pasirinkite **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Pasirinkite **Disable** funkcijai **IPsec/IP Filtering** ties **Default Policy**.
3. Paspauskite **Next**, tada išvalykite **Enable this Group Policy** visoms grupių politikoms.
4. Spustelėkite **OK**.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Tinklo saugos funkcijų naudojimo problemos

Pamiršti iš anksto bendrinimą raktą

Naudodami Web Config, vėl sukonfigūruokite raktą.

Norėdami pakeisti raktą, atverkite Web Config ir pasirinkite **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** arba **Group Policy**.

Kai pakeičiate iš anksto bendrinamą raktą, sukonfigūruokite kompiuterių iš anksto bendrinamą raktą.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

Nepavyko užmegzti ryšio su „IPsec“

Ar naudojate nepalaikomą kompiuterio nuostatų algoritmą?

Skaitytuvas palaiko šiuos algoritmus.

Saugos metodai	Algoritmai
IKE kodavimo algoritmas	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE autentifikavimo algoritmas	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE raktų mainų algoritmas	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 kodavimo algoritmas	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP autentifikavimo algoritmas	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH autentifikavimo algoritmas	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* galima tik su IKEv2

Susijusi informacija

➡ „Užkoduota komunikacija naudojant „IPsec“ / IP filtravimą” puslapyje 71

Staiga nepavyko užmegzti ryšio

Skaitytuvo IP adresas negalioja arba buvo pakeistas?

Naudodamiesi skaitytuvo valdymo skydeliu, išjunkite „IPsec“.

Jei DHCP pasenęs, prietaisas įjungiamas iš naujo, IPv6 adresas pasenęs arba nebuvo gautas, skaitytuvo Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) užregistruoto IP adreso gali nepavykti rasti.

Naudokite nekintamą IP adresą.

Kompiuterio IP adresas negalioja arba buvo pakeistas?

Naudodamiesi skaitytuvo valdymo skydeliu, išjunkite „IPsec“.

Jei DHCP pasenęs, prietaisas įjungiamas iš naujo, IPv6 adresas pasenęs arba nebuvo gautas, skaitytuvo Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) užregistruoto IP adreso gali nepavykti rasti.

Naudokite nekintamą IP adresą.

Susijusi informacija

➡ „Prieiga prie Web Config” puslapyje 23

➡ „Užkoduota komunikacija naudojant „IPsec“ / IP filtravimą” puslapyje 71

Negalima prisijungti sukonfigūravus IPsec / IP filtravimą

Reikšmė gali būti neteisinga.

Skaitytuvo valdymo skydelyje išjunkite „IPsec“ / IP filtravimo funkciją. Prijunkite skaitytuvą ir kompiuterį ir vėl nustatykite „IPsec“ / IP filtravimo nustatymus.

Susijusi informacija

➡ „Užkoduota komunikacija naudojant „IPsec“ / IP filtravimą” puslapyje 71

Sukonfigūravus IEEE802.1X, negalima pasiekti spausdintuvo arba skaitytuvo

Nuostatos gali būti neteisingos.

Skaitytuvo valdymo skydelyje išjunkite IEEE802.1X. Prijunkite skaitytuvą ir kompiuterį ir vėl sukonfigūruokite IEEE802.1X.

Susijusi informacija

➡ „IEEE802.1X tinklo sukonfigūravimas” puslapyje 84

Skaitmeninio sertifikato naudojimo problemos

Nepavyko importuoti SI pasirašyto sertifikato

Ar sutampa SI pasirašyto sertifikato ir CSR informacija?

Jei SI pasirašytame sertifikate ir CSR informacija nebus vienoda, nebus galima importuoti CSR. Patikrinkite:

❏ Ar mėginate importuoti SI pasirašytą sertifikatą į įrenginį, kurio informacija skiriasi?
Patikrinkite CSR informaciją, paskui importuokite sertifikatą į įrenginį, kurio informacija yra tokia pati.

❏ Ar perrašėte skaitytuve įrašytą CSR, kai CSR nusiuntėte sertifikavimo institucijai?
Vėl gaukite SI pasirašytą sertifikatą, sutampantį su CSR.

Ar SI pasirašytas sertifikatas yra didesnis nei 5 KB?

Negalite importuoti SI pasirašyto sertifikato, jei jis didesnis nei 5 KB.

Ar teisingas slaptažodis, kurį įvedus galima importuoti sertifikatą?

Jei slaptažodį pamiršite, negalėsite importuoti sertifikatą.

Susijusi informacija

➡ „SI pasirašyto sertifikato importavimas” puslapyje 65

Nepavyksta atnaujinti vartotojo pasirašyto sertifikato

Ar buvo įvestas Common Name?

Būtina įvesti **Common Name**.

Ar į Common Name buvo įvesti nepalaikomi ženklai? Pavyzdžiui, japonų k. raidės nepalaikomos.

IPv4, IPv6, pagrindinio kompiuterio arba FQDN formatu į ASCII (0x20-0x7E) įrašykite 1–128 ženklus.

Ar Common Name įvestas kablelis ar tarpas?

Įvedus kablelį, ties ta vieta atskiriamas **Common Name**. Jei prieš ar po kablelio įvedamas tik tarpas, įvyksta klaida.

Susijusi informacija

➡ „Naudotojo pasirašyto sertifikato atnaujinimas” puslapyje 68

Nepavyko sukurti CSR

Ar buvo įvestas Common Name?

Būtina įvesti **Common Name**.

Ar į Common Name, Organization, Organizational Unit, Locality, State/Province buvo įvesti nepalaikomi ženklai? Pavyzdžiui, japonų k. raidės nepalaikomos.

IPv4, IPv6, pagrindinio kompiuterio arba FQDN formatu į ASCII (0x20-0x7E) įrašykite ženklus.

Ar Common Name įvestas kablelis ar tarpas?

Įvedus kablelį, ties ta vieta atskiriamas **Common Name**. Jei prieš ar po kablelio įvedamas tik tarpas, įvyksta klaida.

Susijusi informacija

➡ „SI pasirašyto sertifikato gavimas” puslapyje 64

Rodomas įspėjimas dėl skaitmeninio sertifikato

Pranešimai	Priežastis / sprendimas
Enter a Server Certificate.	**Priežastis:** Nepasirinkote failo, kurį norite importuoti. **Sprendimas:** Pasirinkite failą ir spustelėkite **Import**.
CA Certificate 1 is not entered.	**Priežastis:** Neimportuotas 1 SI sertifikatas — importuotas tik 2 SI sertifikatas. **Sprendimas:** Pirmiausia importuokite 1 SI sertifikatą.
Invalid value below.	**Priežastis:** Failo kelyje ir (arba) slaptažodyje yra nepalaikomų ženklų. **Sprendimas:** Įsitikinkite, ar elementui įvesti tinkami ženklai.
Invalid date and time.	**Priežastis:** Nebuvo nustatyta skaitytuvo data ir laikas. **Sprendimas:** Naudodami Web Config arba EpsonNet Config, nustatykite datą ir laiką.
Invalid password.	**Priežastis:** SI sertifikatui nustatytas slaptažodis ir įvestas slaptažodis nesutampa. **Sprendimas:** Įveskite teisingą slaptažodį.

Išplėstiniai saugumo nustatymai verslui

Pranešimai	Priežastis / sprendimas
Invalid file.	**Priežastis:** Importuojate sertifikato failą X509 formatu. **Sprendimas:** Įsitikinkite, ar pasirinkote tinkamą sertifikatą, kurį atsiuntė patikima sertifikavimo institucija.
	Priežastis: Importuotas per didelis failas. Failas gali būti daugiausiai 5 KB. **Sprendimas:** Jei pasirinkote tinkamą failą, sertifikatas gali būti sugadintas arba suklastotas.
	Priežastis: Negalioja sertifikate įdiegta grandinė. **Sprendimas:** Norėdami gauti daugiau informacijos, žr. sertifikavimo institucijos žiniatinklio svetainę.
Cannot use the Server Certificates that include more than three CA certificates.	**Priežastis:** PKCS#12 formatu paruošto sertifikato faile yra daugiau nei 3 SI sertifikatai. **Sprendimas:** Konvertuodami iš PKCS#12 į PEM formatą, importuokite kiekvieną sertifikatą arba importuokite sertifikatą, kuriame yra iki 2 SI sertifikatų, PKCS#12 formatu.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Priežastis:** Baigė galioti SI sertifikatas. **Sprendimas:** ❏ Jei sertifikatas baigė galioti, gaukite ir importuokite naują sertifikatą. ❏ Jei sertifikatas dar nebaigė galioti, įsitikinkite, ar tinkamai nustatyta skaitytuvo data ir laikas.
Private key is required.	**Priežastis:** Nėra su sertifikatu sujungto asmeninio rakto. **Sprendimas:** ❏ Jei sertifikatas yra PEM / DER formato ir buvo gautas iš CSR, naudojant kompiuterį, nurodykite asmeninio rakto failą. ❏ Jei sertifikatas yra PKCS#12 formato ir buvo gautas iš CSR, naudojant kompiuterį, sukurkite failą, kuriame yra asmeninis raktas.
	Priežastis: Naudodami Web Config, iš naujo importavote PEM / DER sertifikatą, kurį gavote iš CSR. **Sprendimas:** Jei sertifikatas yra PEM / DER formato ir buvo gautas iš CSR naudojant Web Config, jį galite importuoti tik vieną kartą.

Pranešimai	Priežastis / sprendimas
Setup failed.	**Priežastis:** Nepavyko sukonfigūruoti, kadangi nutrūko ryšys tarp skaitytuvo ir kompiuterio arba dėl tam tikrų klaidų nepavyko perskaityti failo. **Sprendimas:** Patikrinę nurodytą failą ir ryšį, failą importuokite iš naujo.

Susijusi informacija

➡ „Apie skaitmeninį sertifikatą” puslapyje 63

Atsitiktinai pašalinote SI pasirašytą sertifikatą

Ar yra sertifikato atsarginis failas?

Jei turite atsarginį failą, vėl importuokite sertifikatą.

Jei sertifikatą gausite naudodami Web Config, sukurtą CSR, negalėsite vėl importuoti pašalinto sertifikato. Sukurkite CSR ir gaukite naują sertifikatą.

Susijusi informacija

➡ „SI pasirašyto sertifikato šalinimas” puslapyje 67

➡ „SI pasirašyto sertifikato importavimas” puslapyje 65