EPSON
EXCEED YOUR VISION

Príručka správcu

NPD5668-00 SK

Obsah

Príloha

Nastavenia rozšíreného zabezpečenia pre firmy

Autorské práva

Ochranné známky

- ❏ EPSON® je registrovaná ochranná známka a EPSON EXCEED YOUR VISION alebo EXCEED YOUR VISION je ochranná známka spoločnosti 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.
- ❏ Všeobecné oznámenie: ďalšie názvy produktov, ktoré sa používajú v tomto dokumente, sú uvedené len z dôvodu identifikácie a môžu byť ochrannými známkami ich príslušných vlastníkov. Spoločnosť Epson odmieta akékoľvek práva na tieto známky.

O tejto príručke

Značky a symboly

> ⚠ ***Upozornenie:***
> *Pokyny, ktoré je potrebné starostlivo dodržiavať, aby nedošlo k zraneniu.*

> ***Upozornenie:***
> *Pokyny, ktoré je potrebné dodržiavať, aby nedošlo k poškodeniu zariadenia.*

Poznámka:
Pokyny obsahujúce užitočné tipy a obmedzenia pri prevádzke skenera.

Súvisiace informácie

➡ Kliknutím na túto ikonu zobrazíte súvisiace informácie.

Popisy použité v tejto príručke

❏ Snímky obrazoviek ovládača skenera a softvéru Epson Scan 2 (ovládač skenera) pochádzajú zo systému Windows 10 alebo OS X El Capitan. Obsah zobrazený na obrazovkách sa líši v závislosti od modelu a situácie.

❏ Obrázky použité v tejto príručke slúžia len ako príklady. Jednotlivé modely sa môžu líšiť, spôsob obsluhy je však rovnaký.

❏ Položky ponuky zobrazené na obrazovkách sa líšia v závislosti od modelu a nastavení.

Odkazy na operačné systémy

Windows

V tejto príručke označujú rôzne výrazy nasledujúce operačné systémy: „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“ a „Windows Server 2003“. Výrazom „Windows“ sa označujú všetky verzie.

❏ Operačný systém Microsoft® Windows® 10

❏ Operačný systém Microsoft® Windows® 8.1

❏ Operačný systém Microsoft® Windows® 8

❏ Operačný systém Microsoft® Windows® 7

❏ Operačný systém Microsoft® Windows Vista®

❏ Operačný systém Microsoft® Windows® XP

❏ Operačný systém Microsoft® Windows® XP Professional x64 Edition

- ❏ Operačný systém Microsoft® Windows Server® 2016
- ❏ Operačný systém Microsoft® Windows Server® 2012 R2
- ❏ Operačný systém Microsoft® Windows Server® 2012
- ❏ Operačný systém Microsoft® Windows Server® 2008 R2
- ❏ Operačný systém Microsoft® Windows Server® 2008
- ❏ Operačný systém Microsoft® Windows Server® 2003 R2
- ❏ Operačný systém Microsoft® Windows Server® 2003

Mac OS

V tejto príručke sa výrazom „Mac OS“ označujú tieto operačné systémy: macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x a Mac OS X v10.6.8.

Úvod

Súčasti príručky

Táto príručka je určená správcom zariadenia, ktorí sa starajú o pripojenie tlačiarne alebo skenera k sieti, a obsahuje informácie o spôsobe vytvorenia nastavení pre používanie funkcií.

Informácie o používaní funkcií nájdete v dokumente *Používateľská príručka*.

Príprava

Vysvetľuje úlohy správcu, spôsob nastavenia zariadení a softvér na spravovanie.

Pripojenie

Vysvetľuje spôsob pripojenia zariadenia k sieti alebo telefónnej linke. Vysvetľuje aj sieťové prostredie, napríklad používanie portu pre zariadenie a informácie o serveroch DNS a Proxy.

Nastavenia funkcií

Vysvetľuje nastavenia jednotlivých funkcií zariadenia.

Základné nastavenia zabezpečenia

Vysvetľuje nastavenia jednotlivých funkcií, napríklad tlače, skenovania a faxovania.

Nastavenia činnosti a riadenia

Vysvetľuje činnosti po začatí používania zariadení, napríklad kontrola informácií a údržba.

Riešenie problémov

Vysvetľuje inicializáciu nastavení a riešenie problémov so sieťou.

Nastavenia rozšíreného zabezpečenia pre firmy

Vysvetľuje spôsob nastavenia v rámci vylepšenia zabezpečenia zariadenia, napríklad používanie certifikátu CA, komunikácia cez protokol SSL/TLS a filtrovanie IPsec/IP.

V závislosti od modelu nie sú niektoré funkcie uvedené v tejto kapitole podporované.

Definícia výrazov používaných v tejto príručke

V tejto príručke sa používajú nasledujúce výrazy.

Správca

Osoba starajúca sa o inštaláciu a nastavenie zariadenia alebo siete v kancelárii alebo organizácii. V malých organizáciách sa môže táto osoba starať o spravovanie zariadenia aj siete. Vo veľkých organizáciách majú správcovia poverenie k sieti alebo zariadeniam v skupinovej jednotke oddelenia alebo odboru a správcovia siete sa zastupujúc organizáciu starajú o nastavenia komunikácie, napríklad o internet.

Správca siete

Osoba starajúca sa o ovládanie sieťovej komunikácie. Osoba, ktorá nastavuje smerovač, server Proxy, server DNS a poštový server, a riadi komunikáciu cez internet alebo sieť.

Používateľ

Osoba, ktorá používa zariadenia, ako sú napríklad tlačiarne alebo skenery.

Web Config (webová stránka zariadenia)

Webový server, ktorý je zabudovaný do zariadenia. Nazýva sa Web Config. Pomocou prehľadávača na nej môžete kontrolovať a meniť stav zariadenia.

Nástroj

Všeobecný výraz pre softvér na nastavenie a spravovanie zariadenia, ako sú napríklad Epson Device Admin, EpsonNet Config, EpsonNet SetupManager atď.

Okamžité skenovanie

Všeobecný výraz pre skenovanie z ovládacieho panela zariadenia.

ASCII (American Standard Code for Information Interchange)

Jedno zo štandardných kódovaní znakov. Je určených 128 znakov vrátane abecedných (a – z, A – Z), arabských číslic (0 – 9), symbolov, prázdnych znakov a riadiacich znakov. Keď sa v tejto príručke uvádza kódovanie „ASCII“, znamená to ďalej uvedené znaky 0x20 – 0x7E (hex number) a nezahŕňa to riadiace znaky.

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	{	|	}	~	

* Znak medzery.

Unicode (UTF-8)

Medzinárodný štandardný kód pokrývajúci hlavné globálne jazyky. Keď sa v tejto príručke uvádza kódovanie „UTF-8“, znamená to znaky kódovania vo formáte UTF-8.

Príprava

V tejto kapitole je vysvetlená úloha správcu a príprava pred vytvorením nastavení.

Postup nastavenia skenera a spravovanie

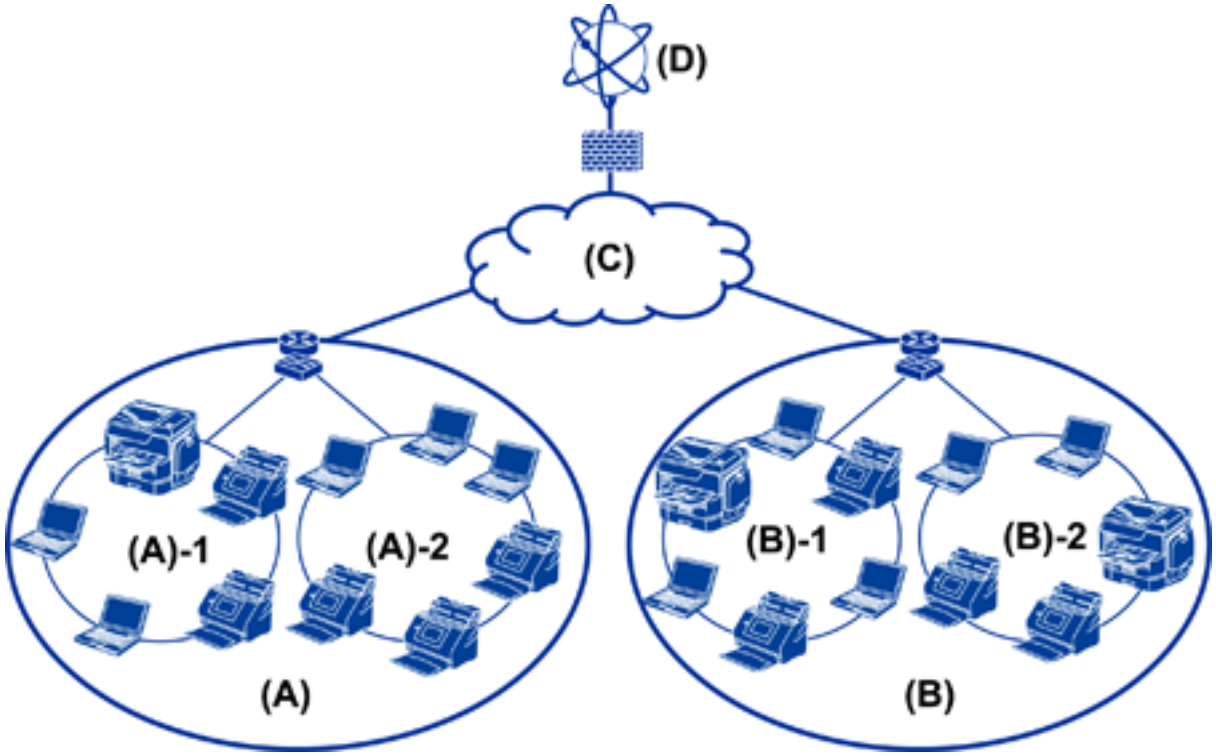
Správca vytvorí nastavenia sieťového pripojenia, prvotné nastavenie a údržbu skenera, aby boli k dispozícii používateľom.

1. Príprava
   - ❏ Zhromaždenie informácií pre nastavenie pripojenia
   - ❏ Rozhodnutie o spôsobe pripojenia
2. Pripojenie
   - ❏ Sieťové pripojenie z ovládacieho panela skenera
3. Nastavenia funkcií
   - ❏ Nastavenia ovládača skenera
   - ❏ Ďalšie rozšírené nastavenia
4. Nastavenia zabezpečenia
   - ❏ Nastavenia správcu
   - ❏ SSL/TLS
   - ❏ Ovládanie protokolov
   - ❏ Rozšírené nastavenia zabezpečenia (voliteľné)
5. Používanie a spravovanie
   - ❏ Kontrola stavu zariadenia
   - ❏ Spracovanie tiesňových situácií
   - ❏ Zálohovanie nastavení zariadenia

Súvisiace informácie

➡ „Príprava” na strane 10
➡ „Pripojenie” na strane 15
➡ „Nastavenia funkcií” na strane 22
➡ „Základné nastavenia zabezpečenia” na strane 32
➡ „Nastavenia činnosti a riadenia” na strane 40

Príklad sieťového prostredia



(A): Kancelária 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Kancelária 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Úvod do príkladu nastavenia pripojenia skenera

V závislosti od spôsobu používania skenera sú dva základné typy pripojenia. Pri oboch je skener pripojený k sieti s počítačom cez rozbočovač.

❏ Pripojenie server/klient (skener používa server Windows, riadenie úloh)

❏ Partnerské pripojenie (priame pripojenie ku klientskemu počítaču)

Súvisiace informácie

➡ „Pripojenie server/klient” na strane 12

➡ „Partnerské pripojenie” na strane 12

Pripojenie server/klient

Centralizácia riadenia skenera a úloh s aplikáciou Document Capture Pro Server nainštalovanou na serveri. Najvhodnejšie na prácu, pri ktorej sa používa viac skenerov na skenovanie veľkého množstva dokumentov v určitom formáte.

Súvisiace informácie

➡ „Definícia výrazov používaných v tejto príručke” na strane 8

Partnerské pripojenie

Použite jednotlivý skener s ovládačom skenera, napríklad s aplikáciou Epson Scan 2 nainštalovanou na klientskom počítači. Inštalácia aplikácie Document Capture Pro (Document Capture) na klientsky počítač umožňuje spúšťať úlohy na jednotlivých klientskych počítačoch skenera.

Súvisiace informácie

➡ „Definícia výrazov používaných v tejto príručke” na strane 8

Príprava na pripojenie k sieti

Získanie informácií o nastavení pripojenia

Pre sieťové pripojenie je potrebné mať IP adresu, adresu brány atď. Skontrolujte nasledujúce.

Rozdelenie	Položky	Poznámka
Spôsob pripojenia zariadenia	❏ Ethernet	Na pripojenie k sieti Ethernet použite kábel STP kategórie 5e alebo vyššej (tienená skrútená dvojlinka).
Informácie o pripojení k sieti LAN	❏ IP adresa ❏ Maska podsiete ❏ Predvolená brána	Ak ste IP adresu nastavili pomocou funkcie DHCP na smerovači, nie je to potrebné.
Informácie o serveri DNS	❏ IP adresa primárneho servera DNS ❏ IP adresa sekundárneho servera DNS	Ak používate statickú IP adresu, nakonfigurujte server DNS. Nakonfigurujte v prípade, že automatické priradenie pomocou funkcie DHCP a keď server DNS nie je možné priradiť automaticky.
Informácie o serveri Proxy	❏ Názov servera Proxy ❏ Číslo portu	Nakonfigurujte, keď na pripojenie k internetu používate server Proxy a keď používate službu Epson Connect alebo funkciu automatickej aktualizácie firmvéru.

Technické údaje skenera

Ak potrebujete technické údaje o tom, ktoré normy a režimy pripojenia skener podporuje, pozrite dokument *Používateľská príručka*.

Používanie čísla portu

Číslo portu, ktorý skener používa, nájdete v časti „Dodatok“.

Súvisiace informácie

➡ „Používanie portu pre skener” na strane 60

Typ priradenia IP adresy

Sú dva typy priradenia IP adresy skeneru.

Statická IP adresa:

Priradenie vopred určenej jedinečnej IP adresy skeneru.

IP adresa sa nemení ani po vypnutí skenera ani smerovača, takže zariadenie môžete spravovať podľa IP adresy.

Tento typ je vhodný pre sieť, kde sa spravuje viac skenerov, napríklad veľká kancelária alebo škola.

Automatické priradenie funkciou DHCP:

Správna IP adresa je priradená automaticky, keď sa úspešne nadviaže komunikácia medzi skenerom a smerovačom, ktorý podporuje funkciu DHCP.

Ak je nepraktické meniť IP adresu pre konkrétne zariadenie, vyhraďte IP adresu a potom ju priraďte.

Server DNS a server Proxy

Ak používate službu internetového pripojenia, nakonfigurujte server DNS. Ak ho nenakonfigurujete, na prístup je potrebné určiť IP adresu, pretože rozpoznanie názvu nemusí byť úspešné.

Server Proxy je umiestnený na bráne medzi sieťou a internetom a komunikuje s počítačom, skenerom a internetom (vzdialený server) v ich zastúpení. Vzdialený server komunikuje len so serverom Proxy. Informácie o skeneri, ako je napríklad IP adresa a číslo portu, sa nedajú prečítať a zabezpečenie je vyššie.

Pomocou funkcie filtrovania môžete zakázať prístup k určitej URL adrese, pretože server Proxy dokáže kontrolovať obsah komunikácie.

Spôsob nastavenia sieťového pripojenia

Pri nastavení pripojenia pre položky IP adresa skenera, maska podsiete a predvolená brána postupujte nasledovne.

Pomocou ovládacieho panela:

Nakonfigurujte nastavenia pre jednotlivé skenery pomocou ovládacieho panela skenera. Po nakonfigurovaní nastavení pripojenia skenera pripojte k sieti.

Pomocou inštalačného programu:

Ak sa používa inštalačný program, sieť skenera a klientsky počítač sa nastavia automaticky. Nastavenie je k dispozícii podľa pokynov inštalačného programu, hoci nemáte hlbšie vedomosti o sieti.

Pomocou nástroja:

Použite nástroj z počítača správcu. Môžete rozpoznať skener a potom ho nastaviť, prípadne vytvorte súbor SYLK, ak chcete vytvoriť hromadné nastavenia pre skenery. Môžete nastaviť viaceré skenery, ale pred nastavením je potrebné, aby boli fyzicky pripojené káblom siete Ethernet. Odporúča sa to teda v prípade, že môžete na nastavenie vytvoriť sieť Ethernet.

Súvisiace informácie

➡ „Pripojenie k sieti z ovládacieho panela” na strane 15

➡ „Pripojenie k sieti pomocou inštalačného programu” na strane 19

➡ „Priradenie IP adresy pomocou aplikácie EpsonNet Config” na strane 56

Pripojenie

V tejto kapitole je vysvetlené prostredie alebo postup pripojenia skenera k sieti.

Pripojenie k sieti

Pripojenie k sieti z ovládacieho panela

Pripojte skener k sieti pomocou ovládacieho panela skenera.

Ďalšie podrobnosti o ovládacom paneli skenera nájdete v dokumente *Používateľská príručka*.

Priradenie IP adresy

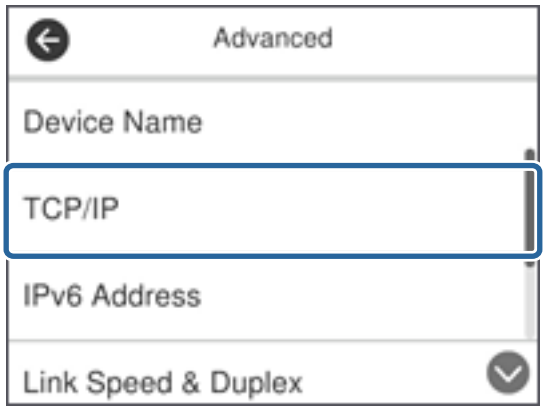
Nastavte základné položky, ako sú IP adresa, Maska podsiete a Predvolená brána.

1. Zapnite skener.
2. Rýchlo potiahnite obrazovku na ovládacom paneli skenera doľava a potom klepnite na položku **Nastav.**.

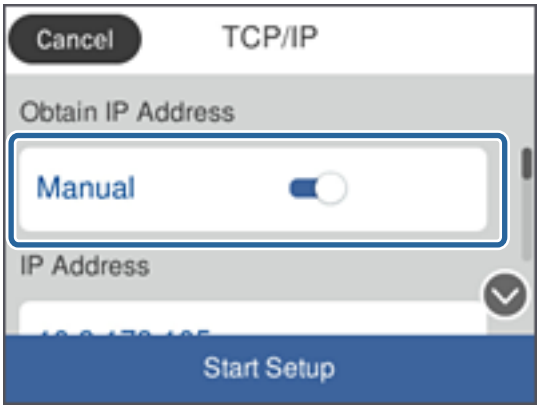
3. Klepnite na položky **Nastavenia siete** > **Zmeniť nastavenia**.

   Ak sa položka nezobrazuje, rýchlym potiahnutím po obrazovke smerom nahor ju zobrazte.

4. Klepnite na položku **TCP/IP**.

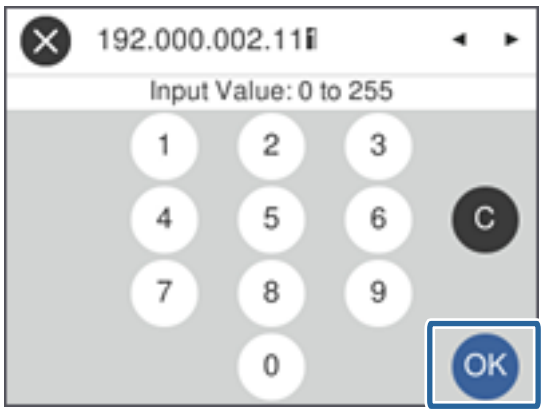


5. Vyberte možnosť **Ručne** pre **Získať IP adresu**.



Poznámka:
*Keď nastavujete IP adresu automaticky pomocou funkcie DHCP alebo smerovačom, vyberte možnosť **Automaticky**. V takom prípade sa položky **IP adresa**, **Maska podsiete** a **Predvolená brána** v krokoch 6 až 7 tiež nastavia automaticky, takže prejdite na krok 8.*

6. Klepnite do políčka **IP adresa**, zadajte IP adresu pomocou klávesnice zobrazenej na obrazovke a potom klepnite na tlačidlo **OK**.



Overte hodnotu zobrazenú na predchádzajúcej obrazovke.

7. Nastavte položky **Maska podsiete** a **Predvolená brána**.

   Overte hodnotu zobrazenú na predchádzajúcej obrazovke.

   Poznámka:
   *Ak je kombinácia položiek IP adresa, Maska podsiete a Predvolená brána nesprávna, položka **Spustiť nastavenie** je neaktívna a nedá sa pokračovať v nastaveniach. Skontrolujte, či nie je v zadaní chyba.*

8. Klepnite do políčka **Primárny DNS** pre položku **Server DNS**, zadajte IP adresu primárneho servera DNS pomocou klávesnice zobrazenej na obrazovke a potom klepnite na tlačidlo **OK**.

   Overte hodnotu zobrazenú na predchádzajúcej obrazovke.

   Poznámka:
   *Keď pre nastavenie priradenia IP adresy vyberiete možnosť **Automaticky**, môžete vybrať nastavenia servera DNS spomedzi možností **Ručne** alebo **Automaticky**. Ak nemôžete získať adresu servera DNS automaticky, vyberte možnosť **Ručne** a zadajte adresu servera DNS. Potom priamo zadajte adresu sekundárneho servera DNS. Ak vyberiete možnosť **Automaticky**, prejdite na krok 10.*

9. Klepnite do políčka **Sekundárny DNS**, zadajte IP adresu sekundárneho servera DNS pomocou klávesnice zobrazenej na obrazovke a potom klepnite na tlačidlo **OK**.

   Overte hodnotu zobrazenú na predchádzajúcej obrazovke.

10. Klepnite na položku **Spustiť nastavenie**.

11. Na obrazovke potvrdenia klepnite na položku **Zatvoriť**.

    Ak neklepnete na tlačidlo **Zatvoriť**, po určitom čase sa obrazovka automaticky zatvorí.

Pripojenie k sieti Ethernet

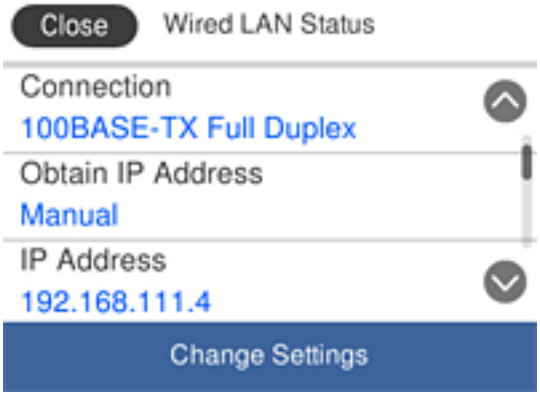
Pripojte skener k sieti pomocou kábla siete Ethernet a skontrolujte pripojenie.

1. Prepojte skener a rozbočovač (prepínač L2) káblom siete Ethernet.

   Ikona na hlavnej obrazovke sa zmení na  .

2. Na hlavnej obrazovke klepnite na  .

3. Potiahnite po obrazovke nahor a potom sa uistite, či sú správne stav zariadenia a IP adresa.



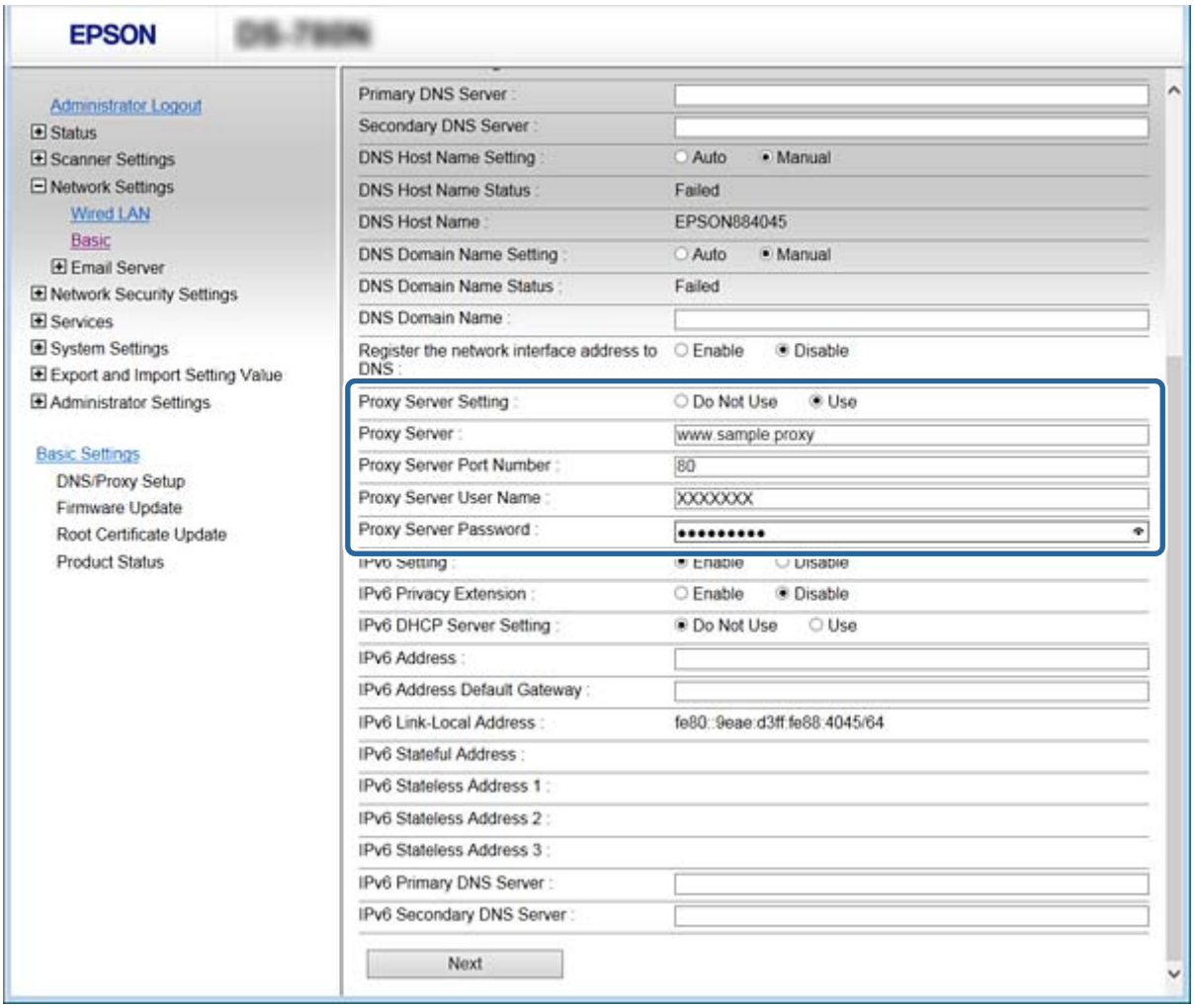
Nastavenie servera Proxy

Server proxy nie je možné nastaviť na paneli. Nakonfigurujte ho pomocou aplikácie Web Config.

1. Otvorte aplikáciu Web Config a vyberte položky **Network Settings** > **Basic**.
2. Vyberte možnosť **Use** v položke **Proxy Server Setting**.
3. Stanovte server proxy pomocou adresy IPv4 alebo vo formáte FQDN v položke **Proxy server** a potom zadajte číslo portu v položke **Proxy Server Port Number**.

   Pri serveroch proxy, ktoré vyžadujú overenie, zadajte používateľské meno pre overovanie a heslo pre overovanie na serveri proxy.

4. Kliknite na tlačidlo **Next**.



5. Potvrďte nastavenie a potom kliknite na položku **Nastavenia**.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Pripojenie k sieti pomocou inštalačného programu

Na pripojenie skenera k počítaču odporúčame použiť inštalačný program. Inštalačný program môžete spustiť jedným z nasledujúcich spôsobov.

❏ Inštalácia z webovej stránky

Otvorte nasledujúcu webovú stránku a potom zadajte názov výrobku. Prejdite na položku **Nastavenie** a potom spustite inštaláciu.

http://epson.sn

❏ Inštalácia pomocou disku so softvérom (len pre modely, ku ktorým bol priložený disk so softvérom a pre používateľov s počítačmi vybavenými diskovou mechanikou)

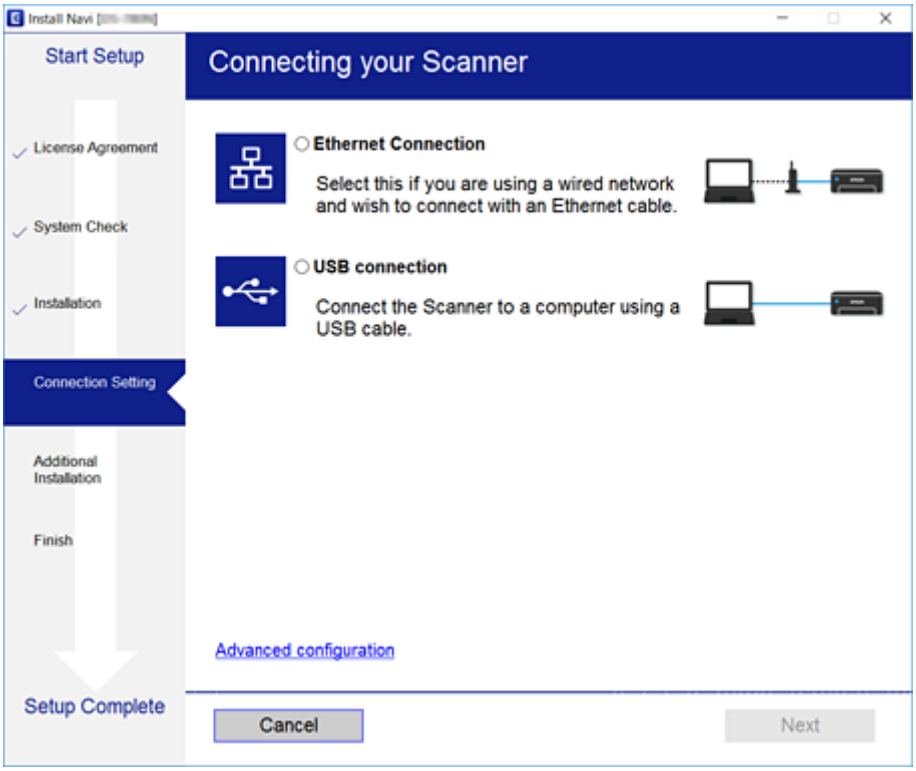
Vložte do počítača disk so softvérom a potom postupujte podľa pokynov na obrazovke.

Výber spôsobov pripojenia

Postupujte podľa pokynov na obrazovke, kým sa nezobrazí nasledujúca obrazovka, a potom vyberte spôsob pripojenia skenera k počítaču.

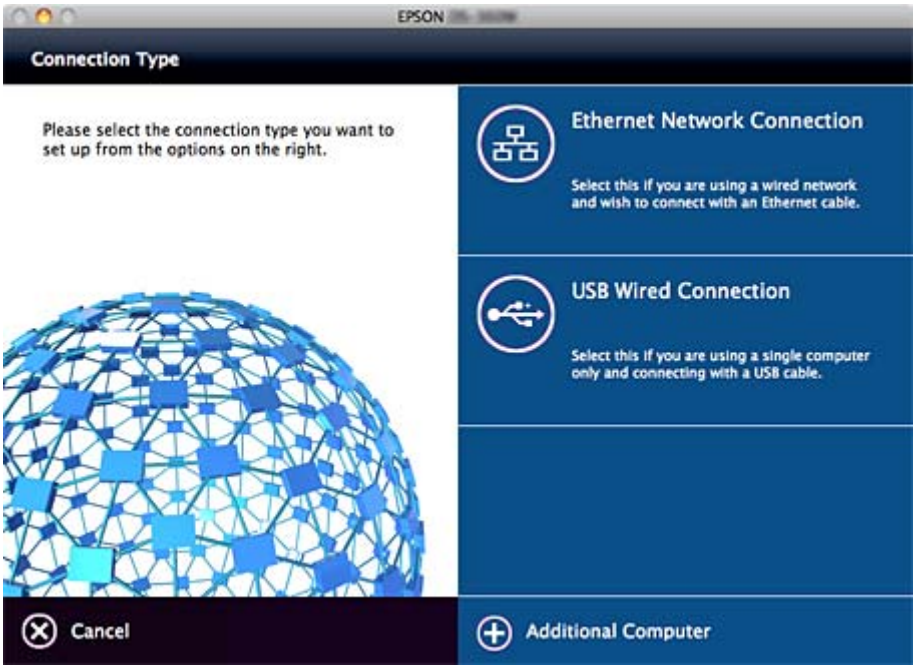
❏ Windows

Vyberte typ pripojenia a potom kliknite na tlačidlo **Ďalej**.



❏ Mac OS

Vyberte typ pripojenia.



Pripojenie

Postupujte podľa pokynov na obrazovke. Nainštaluje sa potrebný softvér.

Nastavenia funkcií

V tejto kapitole sú vysvetlené prvé nastavenia, ktoré treba urobiť pre jednotlivé funkcie zariadenia.

Softvér na nastavenie

V tejto téme je vysvetlený postup vytvárania nastavení zo správcovského počítača pomocou aplikácie Web Config.

Web Config (webová stránka zariadenia)

Čo je Web Config

Web Config je aplikácia spúšťaná v prehľadávači určená na konfiguráciu nastavení skenera.

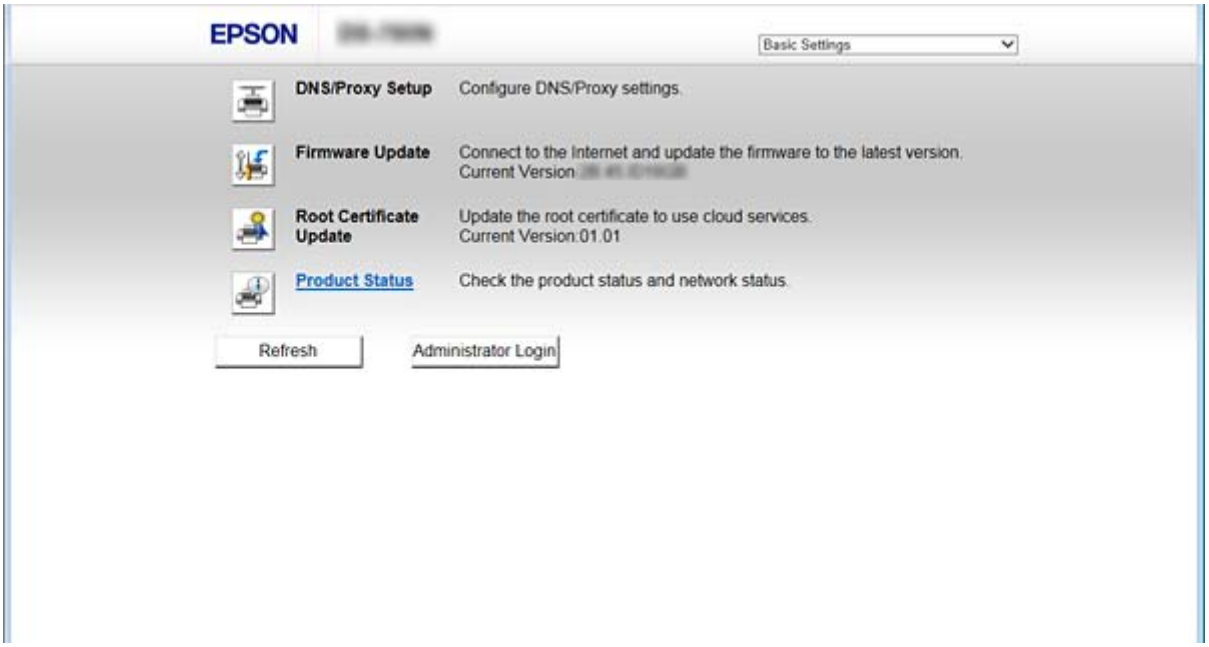
Ak chcete otvoriť aplikáciu Web Config, najskôr musíte skeneru prideliť adresu IP.

Poznámka:
Nastavenia môžete uzamknúť nakonfigurovaním hesla správcu do skenera.

V aplikácii sú dve stránky s nastaveniami, ktoré sú opísané nižšie.

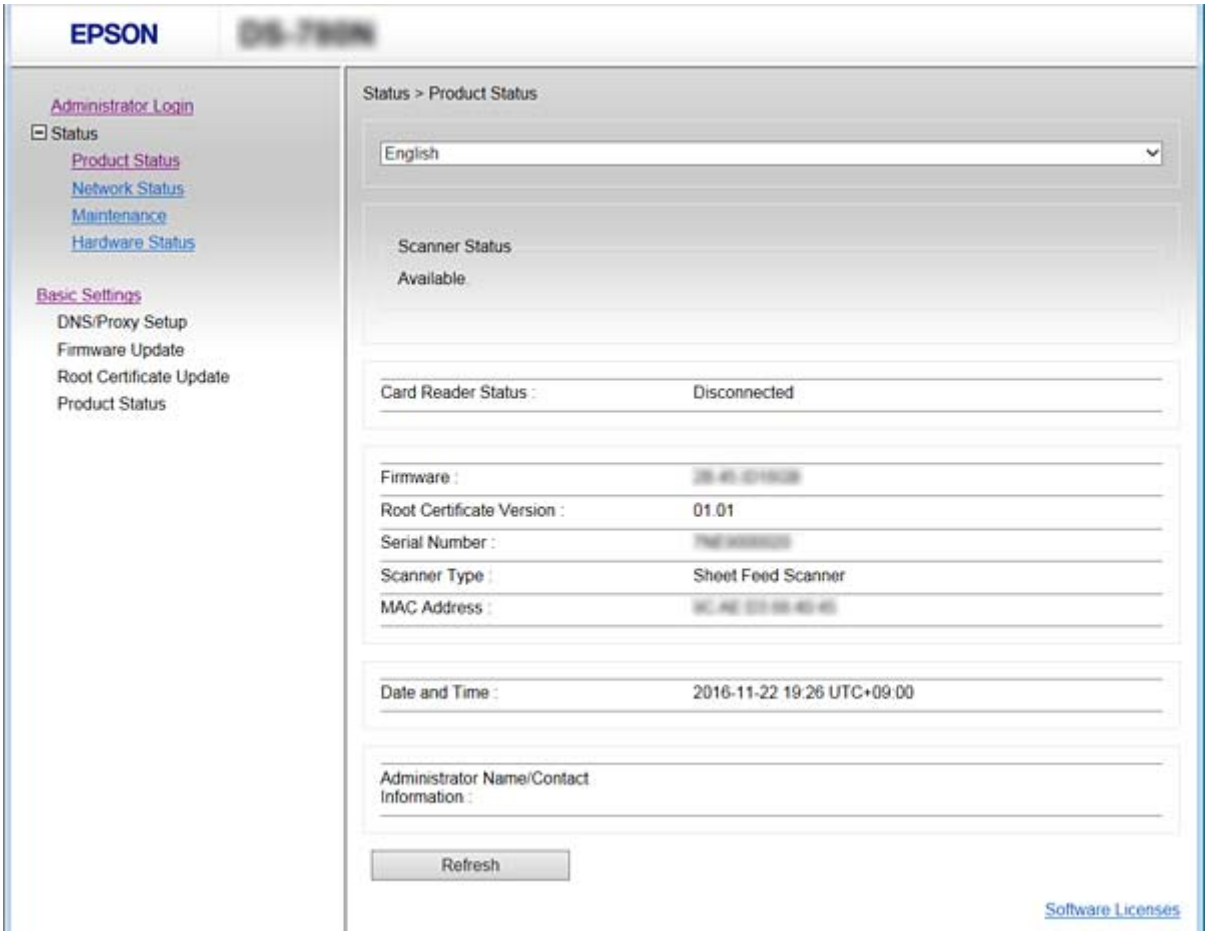
❏ **Basic Settings**

Môžete konfigurovať základné nastavenia skenera.



❏ **Advanced Settings**

Môžete konfigurovať rozšírené nastavenia skenera. Táto stránka je určená hlavne správcovi.



Otvorenie aplikácie Web Config

Zadajte adresu IP skenera do webového prehľadávača. JavaScript musí byť povolený. Keď otvárate aplikáciu Web Config cez protokol HTTPS, v prehľadávači sa zobrazí upozornenie, pretože sa používa certifikát s vlastným podpisom uložený v skeneri.

❏ Otvorenie prostredníctvom protokolu HTTPS

IPv4: https://<adresa IP skenera> (bez znakov < >)

IPv6: https://[adresa IP skenera]/ (so znakmi [ ])

❏ Otvorenie prostredníctvom protokolu HTTP

IPv4: http://<adresa IP skenera> (bez znakov < >)

IPv6: http://[adresa IP skenera]/ (so znakmi [ ])

Poznámka:

❏ *Príklady*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Ak je názov skenera registrovaný v serveri DNS, môžete ho použiť namiesto adresy IP skenera.*

Súvisiace informácie

➡ „Komunikácia so skenerom cez protokol SSL/TLS” na strane 63

➡ „O digitálnom certifikáte” na strane 63

Používanie funkcií skenovania

V závislosti od spôsobu používania skenera nainštalujte nasledujúci softvér a urobte nastavenia jeho používania.

❏ **Skenovanie z počítača**

❏ Overte platnosť služby skenovania cez sieť pomocou aplikácie Web Config (pri dodaní z výroby platné).

❏ Nainštalujte do počítača aplikáciu Epson Scan 2 a nastavte IP adresu.

❏ Keď skenujete pomocou úloh, nainštalujte aplikáciu Document Capture Pro (Document Capture) a urobte nastavenia úlohy.

❏ **Skenovanie z prevádzkového panela**

❏ Keď používate aplikáciu Document Capture Pro alebo Document Capture Pro Server:

Nainštalujte aplikáciu Document Capture Pro alebo Document Capture Pro Server

Nastavenie DCP (režim servera, režim klienta).

❏ Keď používate protokol WSD:

Overte platnosť funkcie WSD v aplikácii Web Config alebo na prevádzkovom paneli (platné pri dodaní z výroby).

Ďalšie nastavenia zariadenia (počítač so systémom Windows).

Skenovanie z počítača

Nainštalujte softvér a skontrolujte, či je povolená služba skenovania cez sieť z počítača.

Súvisiace informácie

➡ „Inštalovaný softvér” na strane 25

➡ „Povolenie skenovania cez sieť” na strane 25

Inštalovaný softvér

❏ Epson Scan 2

Toto je ovládač skenera. Ak používate zariadenie z počítača, nainštalujte ovládač na jednotlivé klientske počítače. Ak je aplikácia Document Capture Pro/Document Capture nainštalovaná, môžete vykonávať činnosti priradené tlačidlám zariadenia.

Pomocou aplikácie EpsonNet SetupManager môžu byť ovládače tlačiarne rozmiestnené spolu v balíkoch.

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

Nainštalujte na klientsky počítač. Z počítača a ovládacieho panela skenera môžete vyvolať a vykonať úlohy zaregistrované na počítači s aplikáciou Document Capture Pro / Document Capture nainštalovanou v sieti.

Môžete aj skenovať z počítača cez sieť. Na skenovanie je potrebná aplikácia Epson Scan 2.

Súvisiace informácie

➡ „EpsonNet SetupManager” na strane 56

Nastavte IP adresu skenera v aplikácii Epson Scan 2

Stanovte IP adresu skenera tak, aby bolo možné skener používať v sieti.

1. Spustite aplikáciu **Epson Scan 2 Utility** z ponuky **Štart** > **Všetky programy** > **EPSON** > **Epson Scan 2**.

   Ak je už zaregistrovaný iný skener, prejdite na 2. krok.

   Ak nie je zaregistrovaný, prejdite na 4. krok.

2. Kliknite na položku ▼ v časti **Skener**.
3. Kliknite na položku **Nastavenie**.
4. Kliknite na možnosť **Povoliť úpravy** a potom kliknite na tlačidlo **Pridať**
5. V položke **Model** vyberte názov modelu skenera.
6. V položke **Adresa** v časti **Vyhľadať sieť** vyberet IP adresu skenera, ktorá sa bude používať.

   Kliknite na  a kliknutím na  aktualizujte zoznam. Ak nemôžete nájsť IP adresu skenera, vyberte možnosť **Zadajte adresu** a zadajte IP adresu.

7. Kliknite na tlačidlo **Pridať**.
8. Kliknite na tlačidlo **OK**.

Povolenie skenovania cez sieť

Keď skenujete z klientskeho počítača cez sieť, môžete nastaviť službu skenovania cez sieť. V predvolenom nastavení je povolená.

1. Otvorte aplikáciu Web Config a vyberte položky **Services** > **Network Scan**.

2. Zaistite, aby bola zvolená možnosť **Enable scanning** pre položku **EPSON Scan**.

   Ak je to zvolené, úloha je dokončená. Zatvorte aplikáciu Web Config.

   Ak nie je zvolená, vyberte ju a prejdite na ďalší krok.

3. Kliknite na tlačidlo **Next**.

4. Kliknite na tlačidlo **OK**.

   Sieť sa znova pripojí a nastavenia sú aktivované.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Skenovanie pomocou ovládacieho panela

Funkcie skenovania do priečinka a skenovania do e-mailu pomocou ovládacieho panela skenera, ako aj prenos výsledkov skenovania do e-mailu, priečinkov atď. sa vykonávajú spustením úlohy z počítača.

Keď prenášate výsledky skenovania, nastavte úlohu pomocou aplikácie Document Capture Pro Server alebo Document Capture Pro.

Podrobnosti o nastaveniach a nastavení úlohy nájdete v dokumentácii alebo v Pomocníkovi k aplikácii Document Capture Pro Server alebo Document Capture Pro.

Súvisiace informácie

➡ „Nastavenia režimu Document Capture Pro Server/Document Capture Pro” na strane 26

➡ „Nastavenie serverov a priečinkov” na strane 27

Softvér inštalovaný do počítača

❏ **Document Capture Pro Server**

Toto je serverová verzia aplikácie Document Capture Pro. Nainštalujte ju na server Windows. Zo servera je možné centrálne riadiť viaceré zariadenia a úlohy. Úlohy sa dajú vykonávať súčasne z viacerých skenerov.

Pomocou aplikácie Document Capture Pro Server s certifikátom môžete riadiť úlohy a históriu skenovania prepojenú na používateľov a skupiny.

Podrobnosti o aplikácii Document Capture Pro Server vám poskytne miestne zastúpenie spoločnosti Epson.

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

Podobne ako pri skenovaní z počítača môžete z ovládacieho panela vyvolať úlohy zaregistrované na počítači a vykonať ich. Počítačové úlohy nie je možné spúšťať súčasne z viacerých skenerov.

Nastavenia režimu Document Capture Pro Server/Document Capture Pro

Urobte nastavenia pomocou funkcie skenovania z ovládacieho panela skenera.

1. Otvorte aplikáciu Web Config a vyberte položky **Services** > **Document Capture Pro**.

2. Vyberte položku **Režim operácie**.

   ❏ Server Mode:

   Vyberte to len vtedy, ak používate režim Document Capture Pro Server alebo Document Capture Pro len pre úlohy, ktoré boli nastavené pre konkrétny počítač.

   ❏ Client Mode:

   Nastavte to, keď vyberáte nastavenie úlohy aplikácie Document Capture Pro (Document Capture) nainštalovanej na jednotlivých klientskych počítačoch v sieti bez určenia počítača.

3. V závislosti od vybraného režimu nastavte nasledujúce.

   ❏ Server Mode:

   V položke **Server Address** stanovte server, na ktorom je nainštalovaná aplikácia Document Capture Pro Server. Môže to byť 2 až 252 znakov v jednom z týchto formátov: IPv4, IPv6, názov hostiteľa alebo FQDN. Vo formáte FQDN možno použiť písmená v kódovaní US – ASCII, čísla, abecedné znaky a pomlčky (nie na začiatku ani na konci).

   ❏ Client Mode:

   Stanovte položku **Group Settings**, ak chcete použiť skupinu skenera určenú z aplikácie Document Capture Pro (Document Capture).

4. Kliknite na tlačidlo **Nastavenia**.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Nastavenie serverov a priečinkov

Režimy Document Capture Pro a Document Capture Pro Server raz uložia naskenované údaje na server alebo do klientskeho počítača a pomocou funkcie prenosu vykonajú funkciu skenovania do priečinka a funkciu skenovania do e-mailu.

Sú potrebné poverenie a informácie na prenos z počítača, na ktorom je nainštalovaná aplikácia Document Capture Pro alebo Document Capture Pro Server, do počítača alebo cloudovej služby.

Pripravte si informácie k funkcii, ktorú použijete. Pozrite nasledujúce.

Nastavenia pre tieto funkcie môžete vytvoriť pomocou aplikácie Document Capture Pro alebo Document Capture Pro Server. Podrobnosti o týchto nastaveniach nájdete v dokumentácii alebo v Pomocníkovi k aplikácii Document Capture Pro Server alebo Document Capture Pro.

Názov	Nastavenie	Požiadavky
Skenovanie do sieťového priečinka (SMB)	Vytvorte a nastavte zdieľanie priečinka na ukladanie	Administratívne používateľské konto na počítači, v ktorom sú vytvorené priečinky na ukladanie.
	Cieľ pre skenovanie do sieťového priečinka (SMB)	Používateľské meno a heslo na prihlásenie do počítača, v ktorom je priečinok na ukladanie, a právo aktualizácie priečinka na ukladanie.
Skenovanie do sieťového priečinka (FTP)	Nastavenie prihlásenia na server FTP	Prihlasovacie údaje k serveru FTP a právo aktualizácie priečinka na ukladanie.

Názov	Nastavenie	Požiadavky
Skenovanie do e-mailu	Nastavenie e-mailového servera	Informácie o nastavení e-mailového servera
Skenovanie do aplikácie Document Capture Pro (keď sa používa Document Capture Pro Server)	Nastavenie prihlasovania do cloudových služieb	Prostredie internetového pripojenia Registrácia konta pre cloudové služby

Používanie skenovania cez WSD (len systém Windows)

Ak je na počítači systém Windows Vista alebo novší, môžete použiť skenovanie cez WSD.

Ak je možné použiť skenovanie cez WSD, na ovládacom paneli skenera sa zobrazuje ponuka **Počítač (WSD)**.

1. Otvorte aplikáciu Web Config a vyberte položky **Services** > **Protocol**.
2. Skontrolujte, či je možnosť **Enable WSD** v položke **WSD Settings** začiarknutá.
   Ak je začiarknutá, úloha je dokončená a môžete zavrieť aplikáciu Web Config.
   Ak nie je začiarknutá, začiarknite ju a pokračujte na ďalší krok.
3. Kliknite na tlačidlo **Next**.
4. Potvrďte nastavenie a kliknite na položku **Nastavenia**.

Vytvorenie systémových nastavení

Vytvorenie systémových nastavení z ovládacieho panela

Nastavenie jasu obrazovky

Nastavte jas LCD obrazovky.

1. Na hlavnej obrazovke klepnite na položku **Nastav.**.
2. Klepnite na položky **Všeob. nastavenia** > **Jas LCD displeja**.
3. Klepnutím na  alebo  nastavte jas.
   Môžete ho nastaviť v rozmedzí od 1 do 9.
4. Klepnite na tlačidlo **OK**.

Nastavenie zvuku

Nastavte zvuky činnosti na paneli alebo chýb.

1. Na hlavnej obrazovke klepnite na položku **Nastav.**.
2. Klepnite na položky **Všeob. nastavenia** > **Zvuk**.
3. V prípade potreby nastavte nasledujúce položky.
   - ❏ Zvuk činnosti
     Nastavte hlasitosť zvuku činnosti prevádzkového panela.
   - ❏ Zvuk chyby
     Nastavte hlasitosť zvuku chyby.
4. Klepnite na tlačidlo **OK**.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Zisťovanie dvojitého podávania originálu

Stanovte funkciu zisťovania dvojitého podávania skenovaného dokumentu a zastavenia skenovania v prípade, že sa zistí viacnásobné podávanie.

Ak chcete skenovať originály, ktoré by mohli byť považované za viacnásobné podávanie (napríklad obálky alebo papier s nálepkami), funkciu vypnite.

Poznámka:
Nastaviť to môžete aj pomocou aplikácie Web Config alebo Epson Scan 2.

1. Na hlavnej obrazovke klepnite na položku **Nastav.**.
2. Klepnite na položky **Externé Nastavenia skenovania** > **Ultrazv. zisťovanie dvojitého pod.**.
3. Klepnutím na položku **Ultrazv. zisťovanie dvojitého pod.** funkciu zapnete alebo vypnete.
4. Klepnite na tlačidlo **Zatvoriť**.

Nastavenie režimu malej rýchlosti

Nastavte skenovanie malou rýchlosťou, ak chcete, aby pri skenovaní tenkých dokumentov (napríklad ústrižkov) nedochádzalo k zaseknutiu papiera.

1. Na hlavnej obrazovke klepnite na položku **Nastav.**.
2. Klepnite na položky **Externé Nastavenia skenovania** > **Pomaly**.
3. Klepnutím na položku **Pomaly** funkciu zapnete alebo vypnete.
4. Klepnite na tlačidlo **Zatvoriť**.

Vytvorenie systémových nastavení pomocou aplikácie Web Config

Nastavenia úspory energie počas nečinnosti

Urobte nastavenie úspory energie po dobu nečinnosti skenera. Nastavte čas v závislosti od prostredia používania.

Poznámka:
Na ovládacom paneli skenera môžete urobiť aj nastavenia úspory energie.

1. Otvorte aplikáciu Web Config a vyberte položky **System Settings** > **Power Saving**.
2. Zadajte čas pre položku **Sleep Timer**, po uplynutí ktorého sa v prípade nečinnosti prejde do úsporného režimu.

   Môžete nastaviť maximálne 240 minút v intervaloch po jednej minúte.
3. Pre položku **Power Off Timer** vyberte čas vypnutia.
4. Kliknite na tlačidlo **OK**.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Nastavenie ovládacieho panela

Nastavte ovládací panel skenera. Môžete nastaviť nasledovné.

1. Otvorte aplikáciu Web Config a vyberte položky **System Settings** > **Control Panel**.
2. V prípade potreby nastavte nasledujúce položky.
   - ❏ Language

     Vyberte jazyk zobrazovaný na ovládacom paneli.
   - ❏ Panel Lock

     Ak vyberiete možnosť **ON**, pri vykonávaní úkonu, ktorý vyžaduje práva správcu, je potrebné zadať heslo správcu. Ak heslo správcu nie je nastavené, zámok panela je vypnutý.
   - ❏ Operation Timeout

     Ak vyberiete možnosť **ON**, keď sa prihlásite ako správca, automaticky budete odhlásení a otvorí sa úvodná obrazovka, ak po určitú dobu nie je vykonaná žiadna činnosť.

     Môžete nastaviť limit od 10 sekúnd do 240 minút v krokoch po jednej sekunde.
3. Kliknite na tlačidlo **OK**.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Nastavenie obmedzenia pre externé rozhranie

Môžete obmedziť používanie pripojenia cez USB z počítača. Nastavte to na zakázanie iného skenovania než cez sieť.

1. Otvorte aplikáciu Web Config a vyberte položky **System Settings** > **External Interface**.
2. Vyberte možnosť **Enable** alebo **Disable**.

   Ak chcete obmedziť, vyberte možnosť **Disable**.
3. Klepnite na tlačidlo **OK**.

Synchronizácia dátumu a času s časovým serverom

Ak používate ceritifkát CA, môžete zabrániť problémom s časom.

1. Otvorte aplikáciu Web Config a vyberte položky **System Settings** > **Date and Time** > **Time Server**.
2. Vyberte možnosť **Use** pre **Use Time Server**.
3. Pre položku **Time Server Address** zadajte adresu časového servera.

   Môžete použiť jeden z týchto formátov: IPv4, IPv6 alebo FQDN. Zadajte maximálne 252 znakov. Ak to neurčujete, nechajte prázdne.
4. Zadajte položku **Update Interval (min)**.

   Môžete nastaviť maximálne 10 800 minút v intervaloch po jednej minúte.
5. Kliknite na položku **OK**.

   Poznámka:
   *V položke **Time Server Status** môžete overiť stav pripojenia k časovému serveru.*

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Základné nastavenia zabezpečenia

V tejto kapitole sú vysvetlené základné nastavenia zabezpečenia, ktoré nevyžadujú špeciálne prostredie.

Úvod do základných bezpečnostných funkcií

Predstavujeme vám základné bezpečnostné funkcie zariadení Epson.

Názov funkcie	Typ funkcie	Čo sa nastavuje	Čomu sa zabráni
Nastavenie hesla správcu	Môžete uzamknúť nastavenia týkajúce sa systému, ako sú napríklad nastavenia pripojenia k sieti alebo cez rozhranie USB, takže ich môže zmeniť len správca.	Správca nastaví heslo k zariadeniu. Konfigurácia alebo aktualizácia je k dispozícii kdekoľvek z aplikácie Web Config, ovládacieho panela, aplikácie Epson Device Admin a aplikácie EpsonNet Config.	Chráni pred nezákonným čítaním a zmenou údajov uložených v zariadení, ako sú napríklad ID, heslo, nastavenia siete a kontakty. Znižuje tiež široký rozsah bezpečnostných rizík, ako je napríklad únik informácií pre sieťové prostredie alebo bezpečnostné zásady.
Komunikácie SSL/TLS	Keď sa zo zariadenia pripájate k serveru Epson na internete, napríklad pri komunikácii s počítačom cez prehľadávač alebo pri aktualizácii firmvéru, obsah komunikácie ja zašifrovaný pomocou protokolu SSL/TLS.	Zadovážte si certifikát podpísaný autoritou CA a potom ho importujte do skenera.	Vymazanie identifikácie zariadenia certifikáciou s podpisom autoritou CA zabráni v prevzatí identity a nepovolenom prístupe. Okrem toho je obsah komunikácie cez protokol SSL/TLS chránený a zabraňuje úniku obsahu tlačových údajov a údajov nastavenia.
Ovládacie protokoly	Ovládacie protokoly používané na komunikáciu medzi zariadeniami a počítačmi a povolenie alebo zakázanie funkcií.	Protokol alebo služba, ktoré sa používajú na funkcie, sú povolené alebo zakázané samostatne.	Zníženie bezpečnostných rizík, ktoré sa môžu vyskytnúť pri nežiaducom používaní vďaka tomu, že sa používateľom zabráni používať nepotrebné funkcie.

Súvisiace informácie

➡ „Čo je Web Config” na strane 22
➡ „EpsonNet Config” na strane 55
➡ „Epson Device Admin” na strane 55
➡ „Nastavenie hesla správcu” na strane 32
➡ „Riadiace protokoly” na strane 35

Nastavenie hesla správcu

Keď nastavíte heslo správcu, ostatní používatelia, ktorí nei sú správcovia, nebudú môcť meniť nastavenia správy systému. Nastaviť a zmeniť heslo správcu môžete buď pomocou aplikácie Web Config, alebo z ovládacieho panela

skenera, prípadne softvérom (Epson Device Admin alebo EpsonNet Config). Pri použití softvéru si pozrite dokumentáciu k jednotlivým softvérom.

Súvisiace informácie

➡ „Konfigurácia hesla správcu z ovládacieho panela” na strane 33
➡ „Konfigurácia hesla správcu pomocou aplikácie Web Config” na strane 33
➡ „EpsonNet Config” na strane 55
➡ „Epson Device Admin” na strane 55

Konfigurácia hesla správcu z ovládacieho panela

Heslo správcu môžete nastaviť z ovládacieho panela skenera.

1. Na hlavnej obrazovke klepnite na položku **Nastav.**.
2. Klepnite na položky **Správa systému** > **Nastavenia správy**.

   Ak sa položka nezobrazuje, rýchlym potiahnutím po obrazovke smerom nahor ju zobrazte.
3. Klepnite na položky **Heslo správcu** > **Zaregistrovať**.
4. Zadajte nové heslo a potom klepnite na tlačidlo **OK**.
5. Zadajte znova heslo a potom klepnite na tlačidlo **OK**.
6. Na obrazovke potvrdenia klepnite na položku **OK**.

   Zobrazí sa obrazovka s nastaveniami správcu.
7. Klepnite na položku **Nastavenie zámku**, a potom na obrazovke s potvrdením klepnite na tlačidlo **OK**.

   Položka Nastavenie zámku je nastavená na možnosť **Zap.** a pri použití uzamknutej položky ponuky bude potrebné heslo správcu.

Poznámka:

❏ *Ak nastavíte položku **Nastav.** > **Všeob. nastavenia** > **Časový limit prevádzky** na možnosť **Zap.**, skener vás po určitej dobe nečinnosti ovládacieho panela odhlási.*

❏ *Heslo správcu môžete zmeniť alebo odstrániť, ak vyberiete možnosť **Zmeniť** alebo **Resetovať** na obrazovke **Heslo správcu** a zadáte heslo správcu.*

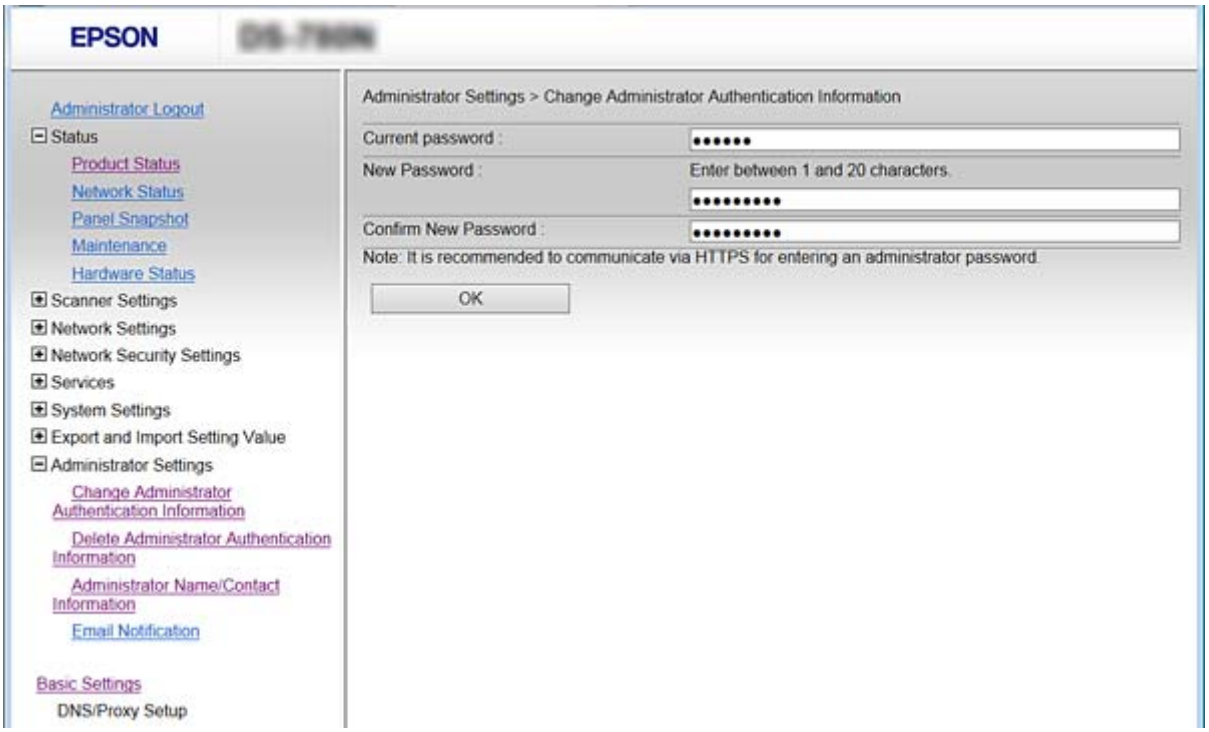
Konfigurácia hesla správcu pomocou aplikácie Web Config

Pomocou aplikácie Web Config môžete nastaviť heslo správcu.

1. Otvorte aplikáciu Web Config a vyberte položky **Administrator Settings** > **Change Administrator Authentication Information**.

2. Do polí **New Password** a **Confirm New Password** zadajte heslo. Ak je to potrebné, zadajte používateľské meno.

   Ak chcete zmeniť heslo na nové, zadajte aktuálne heslo.



3. Vyberte položku **OK**.

   Poznámka:

   ❏ *Ak chcete nastaviť alebo zmeniť uzamknuté položky ponuky, kliknite na položku* ***Administrator Login*** *a potom zadajte heslo správcu.*

   ❏ *Ak chcete odstrániť heslo správcu, kliknite na položky* ***Administrator Settings*** *>* ***Delete Administrator Authentication Information*** *a potom zadajte heslo správcu.*

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Položky uzamknuté heslom správcu

Správcovia majú oprávnenia na nastavenie a zmeny pre všetky funkcie na zariadeniach.

Ak na zariadení nastavíte heslo správcu, môžete ho aj uzamknúť, takže nikto nemôže meniť položky týkajúce sa riadenia zariadenia.

Nasleduje zoznam položiek, ktoré môže správca ovládať.

Položka	Popis
Nastavenie skenera	Nastavenie zisťovania dvojitého podávania a režimu malej rýchlosti.
Nastavenia pripojenia cez sieť Ethernet	Zmena názvu zariadení a IP adresy, nastavenie servera DNS alebo servera Proxy a zmeny nastavenia týkajúce sa sieťových pripojení.

Základné nastavenia zabezpečenia

Položka	Popis
Nastavenie používateľských služieb	Nastavenie pre ovládanie komunikačných protokolov, skenovania cez sieť a služieb Document Capture Pro.
Nastavenie e-mailového servera	Nastavenie e-mailového servera, s ktorým zariadenia komunikujú.
Nastavenie zabezpečenia	Nastavenia pre zabezpečenie siete, ako je napríklad komunikácia cez protokol SSL/TLS, filtrovanie IPsec/IP a IEEE802.1X.
Aktualizácia koreňového certifikátu	Aktualizácia koreňových certifikátov potrebných pri overovaní v režime Document Capture Pro Server a aktualizácii firmvéru z aplikácie Web Config.
Aktualizácia firmvéru	Kontrola a aktualizácia firmvéru zariadení.
Čas, nastavenie času	Čas prechodu do režimu spánku, automatické vypnutie, dátum/čas, časovač nečinnosti, ďalšie nastavenia týkajúce sa časovača.
Obnovenie predvolených nastavení	Obnovenie predvolených nastavení skenera.
Nastavenie správcu	Nastavenie zámku správcu alebo hesla správcu.
Nastavenie certifikovaného zariadenia	Nastavenie identifikácie overovacieho zariadenia. Nastavte, keď používate skener v systéme overovania, ktorý podporuje overovacie zariadenia.

Riadiace protokoly

Môžete skenovať prostredníctvom rôznych ciest a protokolov. Môžete použiť aj skenovanie cez sieť z neurčeného počtu sieťových počítačov. Napríklad je povolené len skenovanie pomocou určených ciest a protokolov. Nežiaduce riziká pre zabezpečenie môžete znížiť obmedzením skenovania z určených ciest alebo riadením dostupných funkcií.

Konfigurácia nastavení protokolu.

1. Otvorte aplikáciu Web Config a vyberte položky **Services** > **Protocol**.
2. Nakonfigurujte každú položku.
3. Kliknite na položku **Next**.
4. Kliknite na tlačidlo **OK**.

   Nastavenia sú uplatnené v skeneri.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23
➡ „Protokoly, ktoré môžete zapnúť alebo vypnúť” na strane 36
➡ „Položky nastavenia protokolu” na strane 37

Protokoly, ktoré môžete zapnúť alebo vypnúť

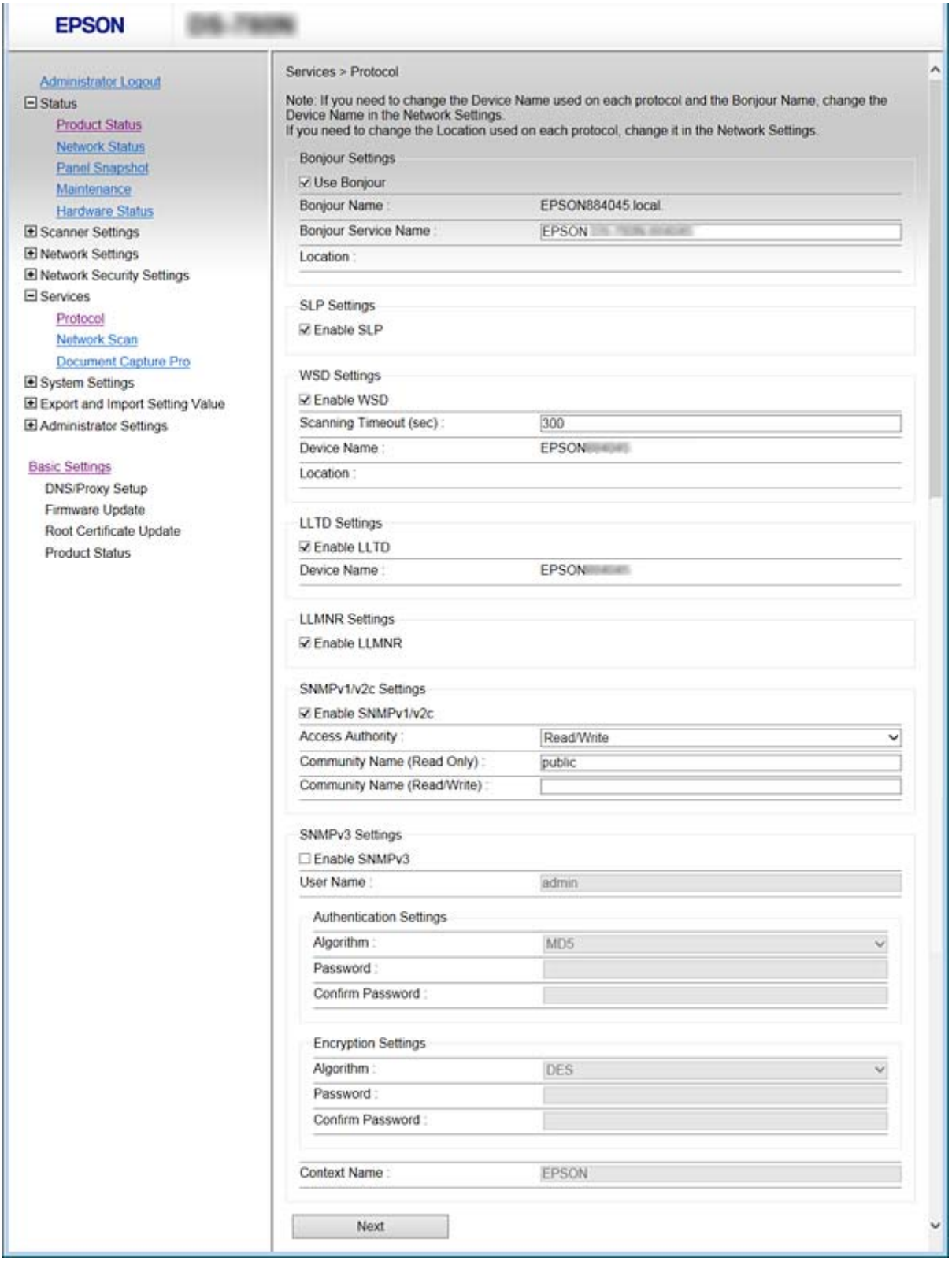
Protokol	Popis
Bonjour Settings	Môžete určiť, či sa chcete použiť funkciu Bonjour. Bonjour sa používa na vyhľadávanie zariadení, skenovanie atď.
SLP Settings	Môžete zapnúť alebo vypnúť funkciu SLP. Funkcia SLP sa používa v aplikácii Epson Scan 2 a na vyhľadávanie v sieti v aplikácii EpsonNet Config.
WSD Settings	Môžete zapnúť alebo vypnúť funkciu WSD. Keď je zapnutá, môžete pridať zariadenia WSD alebo skenovať z portu WSD.
LLTD Settings	Môžete zapnúť alebo vypnúť funkciu LLTD . Keď je zapnutá, zobrazí sa na mape siete vo Windows.
LLMNR Settings	Môžete zapnúť alebo vypnúť funkciu LLMNR . Keď je zapnutá, názov rozlíšenia môžete použiť bez NetBIOS aj vtedy, keď nemôžete použiť DNS.
SNMPv1/v2c Settings	Môžete určiť, či sa SNMPv1/v2c má alebo nemá povoliť. Táto funkcia sa používa na nastavenie zariadení, monitorovanie a tak ďalej.
SNMPv3 Settings	Môžete určiť, či sa SNMPv3 má alebo nemá povoliť. Táto funkcia sa používa na nastavenie šifrovaných zariadení, monitorovanie atď.

Súvisiace informácie

➡ „Riadiace protokoly” na strane 35

➡ „Položky nastavenia protokolu” na strane 37

Položky nastavenia protokolu



Položky	Nastavenie hodnoty a popis
Bonjour Settings	

Základné nastavenia zabezpečenia

Položky	Nastavenie hodnoty a popis
Use Bonjour	Túto možnosť vyberte, ak chcete zariadenia použiť pomocou služby Bonjour.
Bonjour Name	Zobrazí názov Bonjour.
Bonjour Service Name	Môžete zobraziť a nastaviť názov služby Bonjour.
Location	Zobrazí názov umiestnenia zariadenia Bonjour.
SLP Settings	
Enable SLP	Túto možnosť vyberte, ak chcete zapnúť funkciu SLP. Používa sa na rozpoznávanie siete v aplikácii Epson Scan 2 a EpsonNet Config.
WSD Settings	
Enable WSD	Túto funkciu vyberte, ak chcete povoliť pridávanie zariadení pomocou WSD a tlačiť a skenovať z portu WSD.
Scanning Timeout (sec)	Zadajte hodnotu časového limitu komunikácie pre skenovanie pomocou WSD v rozsahu od 3 do 3 600 sekúnd.
Device Name	Zobrazí názov zariadenia WSD.
Location	Zobrazí názov umiestnenia zariadenia WSD.
LLTD Settings	
Enable LLTD	Túto možnosť vyberte, ak chcete povoliť LLTD. Skener je zobrazená na mape siete Windows.
Device Name	Zobrazí názov zariadenia LLTD.
LLMNR Settings	
Enable LLMNR	Túto možnosť vyberte, ak chcete povoliť LLMNR. Rozlíšenie názvu môžete použiť bez NetBIOS aj v prípade, ak nemôžete použiť DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Túto možnosť vyberte, ak chcete povoliť SNMPv1/v2c. Zobrazené sú iba tlačiarne skenery, ktoré podporujú SNMPv3.
Access Authority	Keď je povolené, vyberte prístupovú autoritu. Vyberte možnosť **Read Only** alebo **Read/Write**.
Community Name (Read Only)	Zadajte znaky od 0 do 32 ASCII (0x20 až 0x7E).
Community Name (Read/Write)	Zadajte znaky od 0 do 32 ASCII (0x20 až 0x7E).
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 je povolené, keď je políčko začiarknuté.
User Name	Zadajte 1 až 32 znakov pomocou 1-bajtových znakov.
Authentication Settings	
Algorithm	Vyberte algoritmus pre overovanie protokolu SNMPv3.

Základné nastavenia zabezpečenia

Položky	Nastavenie hodnoty a popis
Password	Zadajte heslo pre overovanie protokolu SNMPv3. Zadajte 8 až 32 znakov v kódovaní ASCII (0x20 – 0x7E). Ak to neurčujete, nechajte prázdne.
Confirm Password	Zadajte nastavené heslo, aby sa vykonalo jeho potvrdenie.
Encryption Settings	
Algorithm	Vyberte algoritmus pre šifrovanie protokolu SNMPv3..
Password	Zadajte heslo pre šifrovanie protokolu SNMPv3. Zadajte 8 až 32 znakov v kódovaní ASCII (0x20 – 0x7E). Ak to neurčujete, nechajte prázdne.
Confirm Password	Zadajte nastavené heslo, aby sa vykonalo jeho potvrdenie.
Context Name	Zadajte najviac 32 znakov v kódovaní Unicode (UTF-8). Ak to neurčujete, nechajte prázdne. Počet znakov, ktoré možno zadať, sa líši v závislosti od jazyka.

Súvisiace informácie

➡ „Riadiace protokoly” na strane 35
➡ „Protokoly, ktoré môžete zapnúť alebo vypnúť” na strane 36

Nastavenia činnosti a riadenia

V tejto kapitole sú vysvetlené položky týkajúce sa každodenných činností a spravovania zariadenia.

Overenie údajov zariadenia

V položke **Status** pomocou aplikácie Web Config môžete overiť nasledujúce informácie o používanom zariadení.

❏ Product Status

Skontrolujte jazyk, stav, číslo výrobku, adresu MAC atď.

❏ Network Status

Skontrolujte informácie o stave sieťového pripojenia, IP adresu, server DNS atď.

❏ Panel Snapshot

Zobrazte snímku obrazovky, ktorá je zobrazená na ovládacom paneli zariadenia.

❏ Maintenance

Skontrolujte dátum spustenia, informácie o skenovaní atď.

❏ Hardware Status

Skontrolujte stav skenera.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Spravovanie zariadení (Epson Device Admin)

Pomocou aplikácie Epson Device Admin môžete spravovať a ovládať viaceré zariadenia. Aplikácia Epson Device Admin vám umožňuje spravovať zariadenia umiestnené v inej sieti. V nasledujúcej časti sú načrtnuté základné funkcie spravovania.

Ďalšie informácie o funkciách a používaní softvéru nájdete v dokumentácii alebo v Pomocníkovi k aplikácii Epson Device Admin.

❏ Rozpoznávanie zariadení

Môžete rozpoznať zariadenia v sieti a potom ich zaregistrovať do zoznamu. Ak sú zariadenia Epson, ako sú napríklad tlačiarne a skenery, pripojené k rovnakému segmentu siete ako počítač správcu, môžete ich nájsť aj vtedy, ak nemajú priradenú IP adresu.

Môžete tiež rozpoznať zariadenia, ktoré sú pripojené k počítačom v sieti káblami USB. Do počítača je potrebné nainštalovať aplikáciu Epson Device USB Agent.

❏ Nastavenie zariadení

Môžete vytvoriť šablónu obsahujúcu položky nastavenia, ako je napríklad sieťové rozhranie a zdroj papiera, a použiť ju na iné zariadenia ako zdieľané nastavenie. Keď je zariadenie pripojené k sieti, môžete priradiť IP adresu na zariadenie, ktorému nebola priradená IP adresa.

❏ Monitorovanie zariadení

Pravidelne môžete zisťovať stav a podrobné informácie o zariadeniach v sieti. Môžete tiež monitorovať zariadenia, ktoré sú pripojené k počítačom v sieti káblami USB a zariadenia z iných spoločností, ktoré boli zaregistrované do zoznamu zariadení. Ak chcete monitorovať zariadenia pripojené káblami USB, je potrebné nainštalovať aplikáciu Epson Device USB Agent.

❏ Spravovanie výstrah

Môžete monitorovať výstrahy na stav zariadení a spotrebného materiálu. Systém automaticky posiela e-mailom upozornenia správcovi na základe nastavených podmienok.

❏ Riadenie správ

Môžete vytvárať pravidelné správy, keď systém zhromaždí údaje o využívaní zariadenia a spotrebného materiálu. Tieto vytvorené správy potom môžete uložiť a odoslať ich e-mailom.

Súvisiace informácie

➡ „Epson Device Admin” na strane 55

Prijímanie emailových oznámení pri výskyte udalostí

Čo sú e-mailové upozornenia

Túto funkciu môžete využiť na prijímanie upozornení e-mailov pri výskyte udalostí. Môžete zaregistrovať až 5 e-mailových adries a vybrať, na ktoré udalosti chcete dostávať upozornenia.

Ak chcete použiť túto funkciu, musí byť nakonfigurovaný poštový server.

Súvisiace informácie

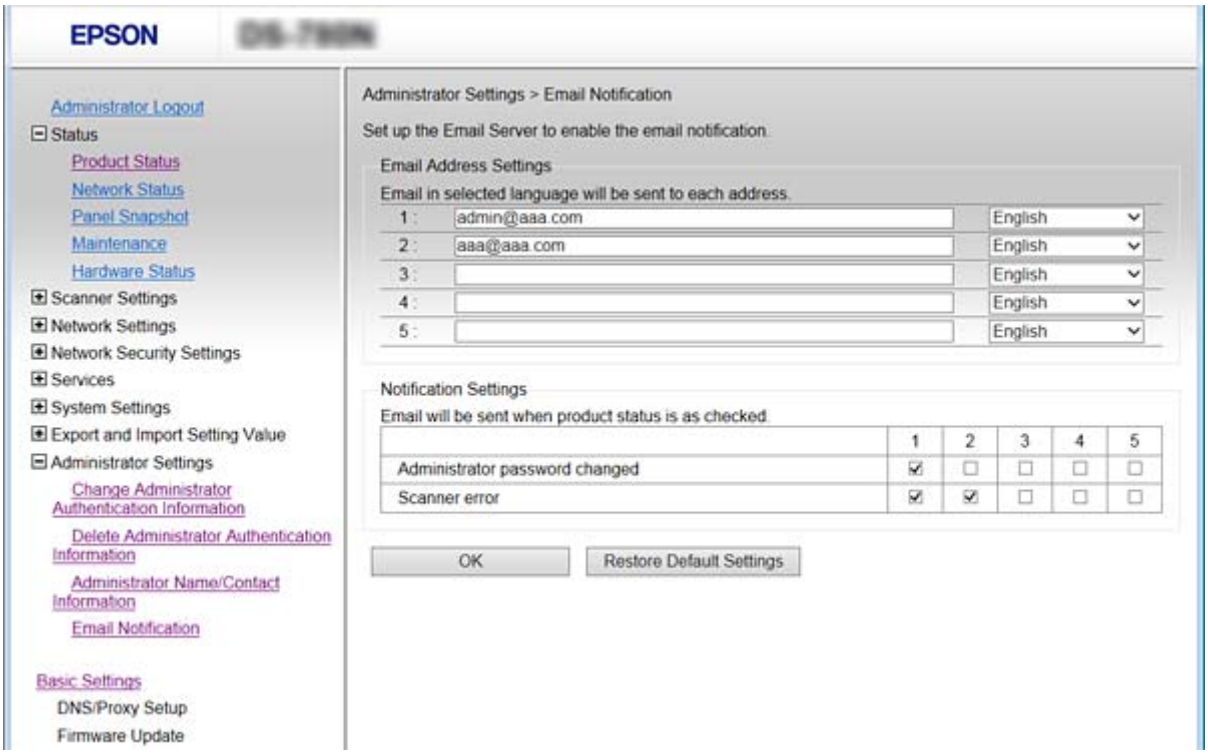
➡ „Konfigurácia servera pošty” na strane 42

Konfigurácia e-mailového upozornenia

Ak chcete používať funkciu, je potrebné nakonfigurovať e-mailový server.

1. Otvorte aplikáciu Web Config a vyberte položky **Administrator Settings** > **Email Notification**.
2. Zadajte e-mailovú adresu, na ktorú chcete prijímať e-mailové upozornenia.
3. Vyberte jazyk pre e-mailové upozornenia.

4. Začiarknite políčka upozornení, ktoré chcete prijímať.



5. Kliknite na položku **OK**.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23
➡ „Konfigurácia servera pošty” na strane 42

Konfigurácia servera pošty

Pred konfiguráciou skontrolujte nasledujúce položky.

❏ Skener je pripojený k sieti.

❏ Informácie o e-mailovom serveri počítača.

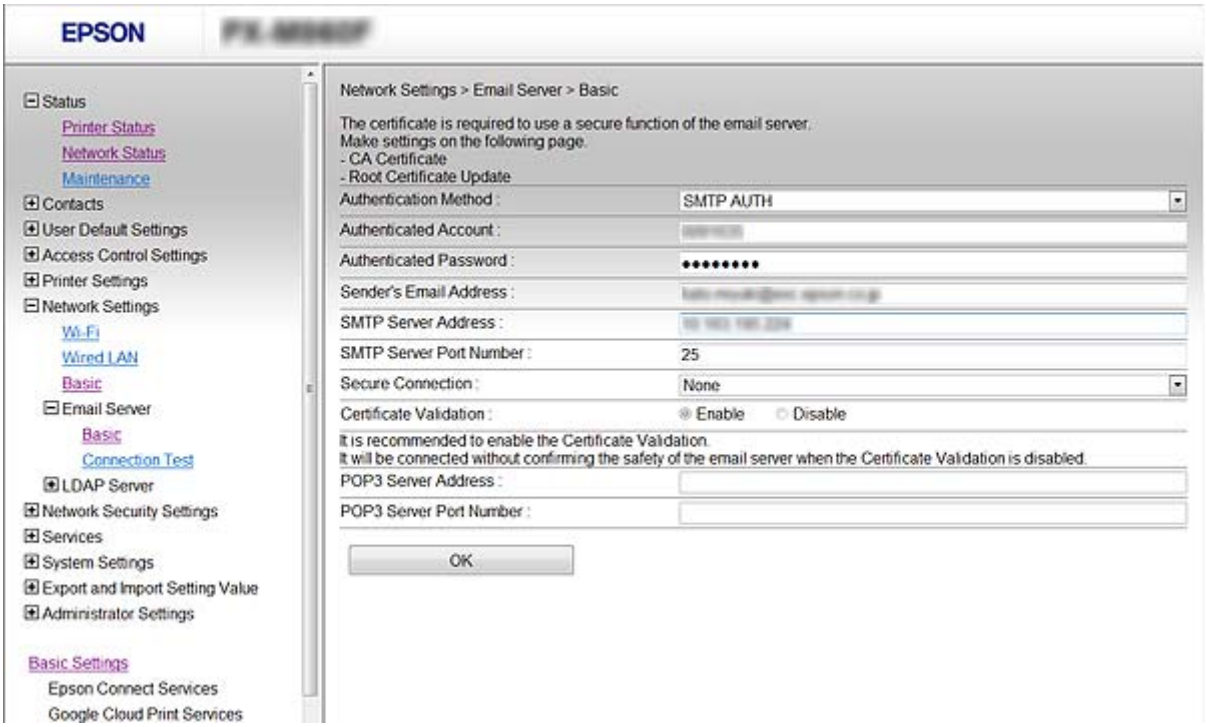
1. Otvorte aplikáciu Web Config a vyberte položky **Network Settings** > **Email Server** > **Basic**.
2. Zadajte hodnoty pre všetky položky.
3. Vyberte položku **OK**.

   Zobrazia sa nastavenia, ktoré ste vybrali.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23
➡ „Položky nastavenia servera pošty” na strane 43

Položky nastavenia servera pošty



Položky	Nastavenia a vysvetlenie	
Authentication Method	Vyberte metódu overenia skenera na prístup k e-mailovému serveru.	
	Off	Pri komunikácii s e-mailovým serverom je overovanie vypnuté.
	SMTP AUTH	Vyžaduje, aby e-mailový server podporoval overovanie cez SMTP.
	POP before SMTP	Ak vyberiete túto metódu, nakonfigurujte server POP3.
Authenticated Account	Ak vyberiete položku **SMTP AUTH** alebo **POP before SMTP** ako **Authentication Method**, zadajte overený názov konta s dĺžkou 0 až 255 znakov v štandarde ASCII (0x20–0x7E).	
Authenticated Password	Ak vyberiete možnosť **SMTP AUTH** alebo **POP before SMTP** pre položku **Authentication Method**, zadajte overené heslo s dĺžkou 0 až 20 znakov A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Zadajte e-mailovú adresu odosielateľa. Zadajte 0 až 255 znakov v kódovaní ASCII (0x20–0x7E), okrem znakov : ( ) < > [ ] ; ¥. Prvý znak nemôže byť bodka „.“.	
SMTP Server Address	Zadajte 0 až 255 znakov. Môžete použiť znaky A–Z a–z 0–9. - . Môžete použiť formát IPv4 alebo FQDN.	
SMTP Server Port Number	Zadajte číslo medzi 1 a 65535.	

Položky	Nastavenia a vysvetlenie	
Secure Connection	Pre e-mailový server určite bezpečný spôsob pripojenia.	
	None	Ak vyberiete položku **POP before SMTP** v možnosti **Authentication Method**, spôsob pripojenia je nastavený na **None**.
	SSL/TLS	Táto možnosť je dostupná, keď je položka **Authentication Method** nastavená na možnosť **Off** alebo **SMTP AUTH**.
	STARTTLS	Táto možnosť je dostupná, keď je položka **Authentication Method** nastavená na možnosť **Off** alebo **SMTP AUTH**.
Certificate Validation	Keď je povolená táto možnosť, certifikát je overený. Odporúčame nastaviť túto položku na **Enable**.	
POP3 Server Address	Ak vyberiete možnosť **POP before SMTP** pre položku **Authentication Method**, zadajte adresu servera POP3 s dĺžkou 0 až 255 znakov A–Z a–z 0–9. - . Môžete použiť formát IPv4 alebo FQDN.	
POP3 Server Port Number	Ak vyberiete možnosť **POP before SMTP** v položke **Authentication Method**, zadajte číslo dlhé 1 až 65535 znakov.	

Súvisiace informácie

➡ „Konfigurácia servera pošty” na strane 42

Kontrola pripojenia servera pošty

1. Otvorte aplikáciu Web Config a vyberte položky **Network Settings** > **Email Server** > **Connection Test**.
2. Vyberte položku **Start**.

   Skúška pripojenia k e-mailovému serveru je spustená. Po teste skontrolujte zobrazenú správu.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23
➡ „Správy testu pripojenia servera pošty” na strane 44

Správy testu pripojenia servera pošty

Správy	Vysvetlenie
Connection test was successful.	Táto správa sa zobrazí, ak bolo pripojenie k serveru úspešné.
SMTP server communication error. Check the following. - Network Settings	Toto hlásenie sa zobrazí, keď ❏ Skener nie je pripojený k sieti ❏ Server SMTP je vypnutý ❏ Sieťové pripojenie je počas komunikácie odpojené ❏ Sú prijaté neúplné údaje

Nastavenia činnosti a riadenia

Správy	Vysvetlenie
POP3 server communication error. Check the following. - Network Settings	Toto hlásenie sa zobrazí, keď ❏ Skener nie je pripojený k sieti ❏ Server POP3 je vypnutý ❏ Sieťové pripojenie je počas komunikácie odpojené ❏ Sú prijaté neúplné údaje
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Toto hlásenie sa zobrazí, keď ❏ Nepodarilo sa pripojiť k serveru DNS ❏ Nepodarilo sa rozlíšiť názov servera SMTP
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Toto hlásenie sa zobrazí, keď ❏ Nepodarilo sa pripojiť k serveru DNS ❏ Nepodarilo sa rozlíšiť názov servera POP3
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Toto hlásenie sa zobrazí po zlyhaní overenia servera SMTP.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Toto hlásenie sa zobrazí po zlyhaní overenia servera POP3.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Toto hlásenie sa zobrazí, keď chcete komunikovať s nepodporovanými protokolmi.
Connection to SMTP server failed. Change Secure Connection to None.	Toto hlásenie sa zobrazí, keď medzi serverom a klientom dôjde k nesúladu SMTP alebo ak tento server nepodporuje bezpečné pripojenie SMTP (pripojenie SSL).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Toto hlásenie sa zobrazí, keď medzi serverom a klientom dôjde k nesúladu SMTP, alebo ak tento server vyžaduje použiť pripojenie SSL/TLS na bezpečné pripojenie servera SMTP.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Toto hlásenie sa zobrazí, keď medzi serverom a klientom dôjde k nesúladu SMTP, alebo ak tento server vyžaduje použiť pripojenie STARTTLS na bezpečné pripojenie servera SMTP.
The connection is untrusted. Check the following. - Date and Time	Toto hlásenie sa zobrazí vtedy, keď je nastavenie dátumu a času skenera nesprávne alebo ak skončila platnosť certifikátu.
The connection is untrusted. Check the following. - CA Certificate	Toto hlásenie sa zobrazí, keď v skeneri nie je koreňový certifikát zodpovedajúci serveru, alebo keď nebol naimportovaný certifikát CA Certificate.
The connection is not secured.	Toto hlásenie sa zobrazí vtedy, keď je poškodený získaný certifikát.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Toto hlásenie sa zobrazí vtedy, keď dôjde k nesúladu spôsobu overenia medzi serverom a klientom. Server podporuje funkciu SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Toto hlásenie sa zobrazí vtedy, keď dôjde k nesúladu spôsobu overenia medzi serverom a klientom. Server nepodporuje SMTP AUTH.

Správy	Vysvetlenie
Sender's Email Address is incorrect. Change to the email address for your email service.	Toto hlásenie sa zobrazí vtedy, keď je zadaná e-mailová adresa odosielateľa nesprávna.
Cannot access the product until processing is complete.	Toto hlásenie sa zobrazí vtedy, keď je skener zaneprázdnený.

Súvisiace informácie

➡ „Kontrola pripojenia servera pošty” na strane 44

Aktualizácia firmvéru

Aktualizácia firmvéru pomocou aplikácie Web Config

Aktualizuje firmvér pomocou aplikácie Web Config. Zariadenie musí byť pripojené k internetu.

1. Otvorte aplikáciu Web Config a vyberte položky **Basic Settings** > **Firmware Update**.
2. Kliknite na položku **Start**.

   Spustí sa overenie firmvéru. Ak existuje aktualizovaný firmvér, zobrazia sa informácie o firmvéri.
3. Kliknite na tlačidlo **Start** a postupujte podľa pokynov na obrazovke.

Poznámka:
Firmvér môžete aktualizovať aj pomocou aplikácie Epson Device Admin. V zozname zariadení môžete vizuálne overiť údaje o firmvéri. Je to užitočné v prípade, že chcete aktualizovať firmvér viacerých zariadení. Ďalšie podrobnosti nájdete v príručke k aplikácii Epson Device Admin alebo jej Pomocníkovi.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23
➡ „Epson Device Admin” na strane 55

Aktualizácia firmvéru pomocou programu Epson Firmware Updater

Do počítača si môžete prevziať firmvér zariadenia z webovej stránky Epson a potom prepojiť zariadenie a počítač káblom USB a aktualizovať firmvér. Ak nemôžete aktualizovať cez sieť, skúste tento spôsob.

1. Otvorte webovú stránku spoločnosti Epson a prevezmite si firmvér.
2. Pripojte počítač obsahujúci prevzatý firmvér k zariadeniu káblom USB.
3. Dvakrát kliknite na prevzatý súbor .exe.

   Spustí sa aplikácia Epson Firmware Updater.
4. Postupujte podľa pokynov na obrazovke.

Zálohovanie nastavení

Exportovaním položiek nastavenia v aplikácii Web Config môžete skopírovať položky do iných skenerov.

Export nastavení

Exportujte každé nastavenie skenera.

1. Otvorte aplikáciu Web Config a potom vyberte položky **Export and Import Setting Value** > **Export**.
2. Vyberte nastavenia, ktoré chcete exportovať.

   Vyberte nastavenia, ktoré chcete exportovať. Ak vyberiete nadradenú kategóriu, vedľajšie kategórie budú tiež vybrané. Vedľajšie kategórie, ktoré spôsobujú chyby ich kopírovaním v rámci rovnakej siete (ako napríklad adresy IP a podobne), nemôžu byť vybrané.
3. Na zakódovanie exportovaného súboru zadajte heslo.

   Na importovanie súboru potrebujete heslo. Toto pole nechajte prázdne, ak nechcete súbor zakódovať.
4. Kliknite na položku **Export**.

> ***Upozornenie:***
>
> *Ak chcete exportovať nastavenia siete skenera, ako napríklad názov skenera a adresa IP, vyberte možnosť* ***Enable to select the individual settings of device*** *a potom vyberte ďalšie položky. Pre náhradný skener vyberte iba vybrané hodnoty.*

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Import nastavení

Exportovaný Web Config súbor importujte do skenera.

> ***Upozornenie:***
>
> *Pri importovaní hodnôt, ktoré obsahujú jednotlivé informácie, ako napríklad názov skenera alebo adresa IP, sa uistite, že v rovnakej sieti neexistuje rovnaká adresa IP. Ak sa adresa IP prekrýva, skener neodzrkadľuje túto hodnotu.*

1. Otvorte aplikáciu Web Config a potom vyberte položky **Export and Import Setting Value** > **Import**.
2. Vyberte exportovaný súbor a potom zadajte zašifrované heslo.
3. Kliknite na položku **Next**.
4. Vyberte nastavenia, ktoré chcete importovať, a potom kliknite na tlačidlo **Next**.
5. Kliknite na položku **OK**.

Nastavenia sú uplatnené v skeneri.

Nastavenia činnosti a riadenia

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Riešenie problémov

Tipy na riešenie problémov

Ďalšie informácie nájdete v nasledujúcej príručke.

❏ Používateľská príručka

Nachádzajú sa tu pokyny na používanie skenera a riešenie problémov.

Kontrola protokolu pre server a sieťové zariadenie

V prípade problému so sieťovým pripojením je možné identifikovať príčinu overením protokolu na poštovom serveri, serveri LDAP atď., kontrolou stavu pomocou protokolu o sieti v denníkoch a príkazoch systémových zariadení, napríklad smerovačov.

Inicializácia nastavení siete

Obnovenie nastavení siete z ovládacieho panela

Môžete obnoviť všetky nastavenia siete na predvolené hodnoty.

1. Na hlavnej obrazovke klepnite na položku **Nastav.**.
2. Klepnite na položky **Správa systému** > **Obnoviť štand. nastavenia** > **Nastavenia siete**.
3. Skontrolujte hlásenie a potom klepnite na položku **Áno**.
4. Keď sa zobrazí hlásenie o dokončení, klepnite na položku **Zatvoriť**.

   Ak neklepnete na tlačidlo **Zatvoriť**, po určitom čase sa obrazovka automaticky zatvorí.

Overenie komunikácie medzi zariadeniami a počítačmi

Kontrola pripojenia pomocou príkazu Ping — Windows

Môžete použiť príkaz Ping a uistiť sa, či je počítač pripojený k skeneru. Postupujte podľa ďalej uvedených pokynov a skontrolujte pripojenie pomocou príkazu Ping.

1. Overte IP adresu skenera pre pripojenie, ktoré chcete skontrolovať.

   Môžete to overiť pomocou aplikácie Epson Scan 2.

2. Zobrazte na počítači obrazovku s príkazovým riadkom.
   - ❏ Windows 10

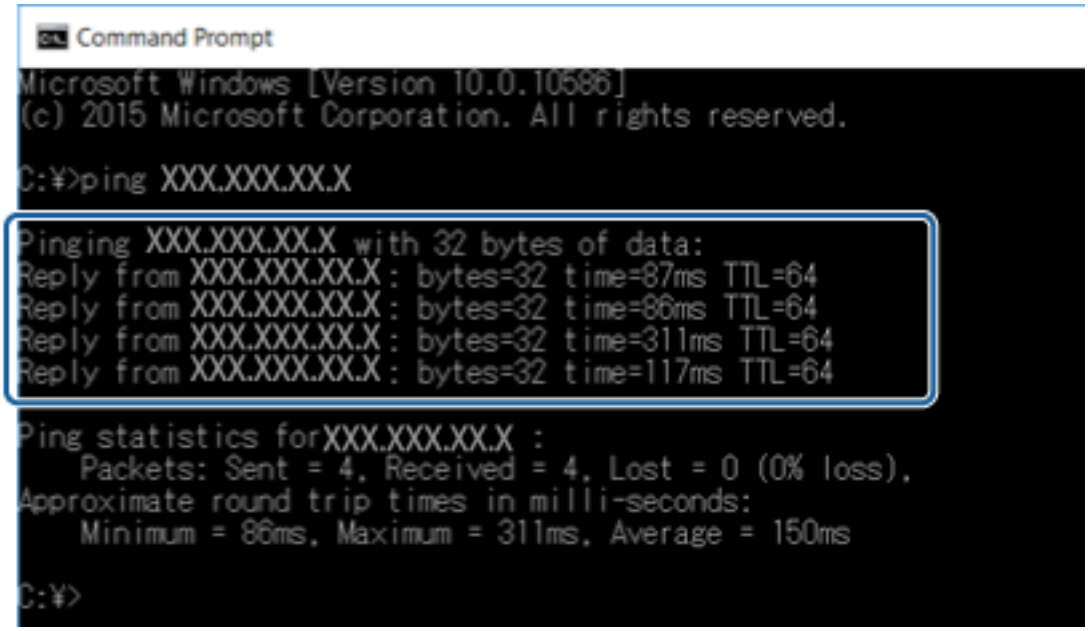
     Kliknite pravým tlačidlom myši na tlačidlo Štart (prípadne ho stlačte a podržte) a potom vyberte položku **Príkazový riadok**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

     Zobrazte obrazovku aplikácie a potom vyberte položku **Príkazový riadok**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 alebo starší

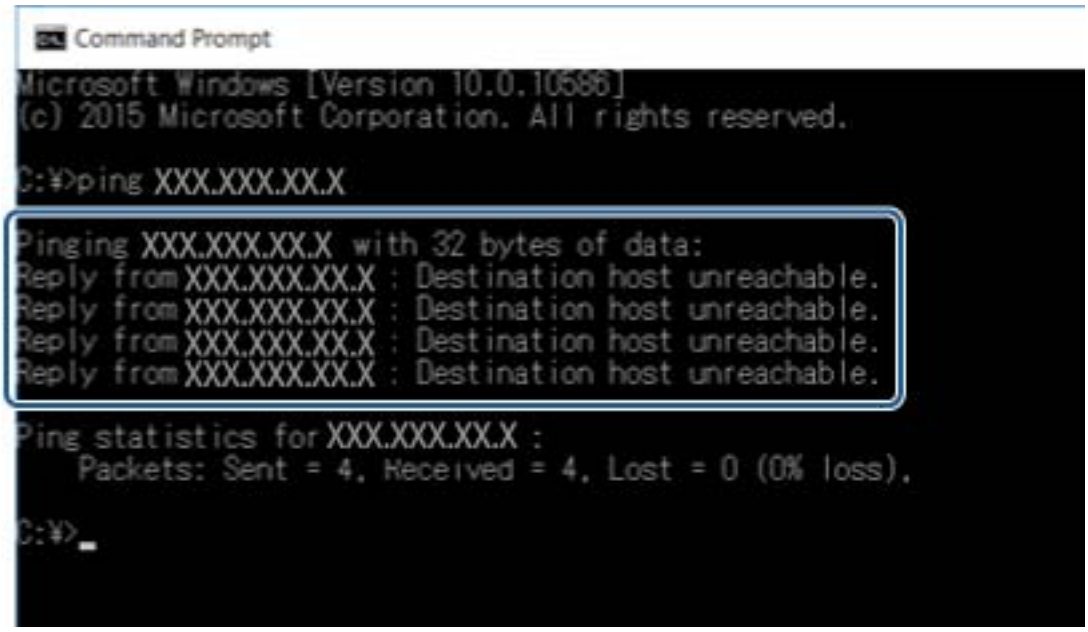
     Kliknite na tlačidlo Štart, vyberte položku **Všetky programy** alebo **Programy** > **Príslušenstvo** > **Príkazový riadok**.
3. Zadajte „ping xxx.xxx.xxx.xxx“ a potom stlačte kláves Enter.

   Pre xxx.xxx.xxx.xxx zadajte IP adresu skenera.
4. Skontrolujte stav komunikácie.

   Ak skener a počítač komunikujú, zobrazí sa nasledujúce hlásenie.



Ak skener a počítač nekomunikujú, zobrazí sa nasledujúce hlásenie.



Kontrola pripojenia pomocou príkazu Ping – Mac OS

Môžete použiť príkaz Ping a uistiť sa, či je počítač pripojený k skeneru. Postupujte podľa ďalej uvedených pokynov a skontrolujte pripojenie pomocou príkazu Ping.

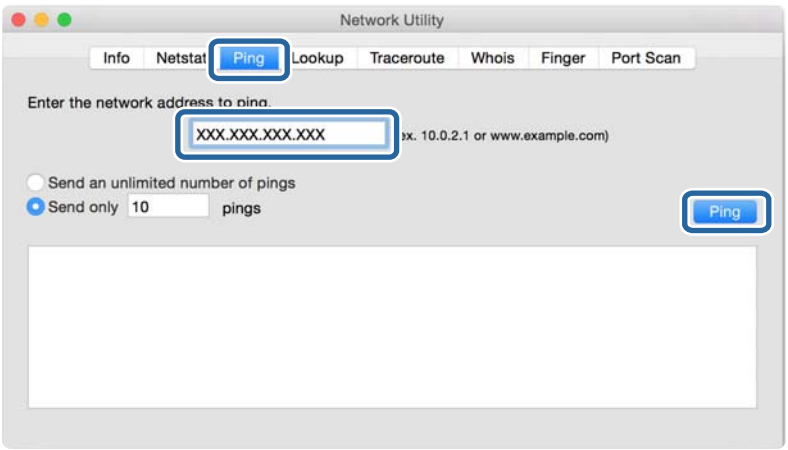
1. Overte IP adresu skenera pre pripojenie, ktoré chcete skontrolovať.

   Môžete to overiť pomocou aplikácie Epson Scan 2.

2. Spustite sieťovú pomôcku.

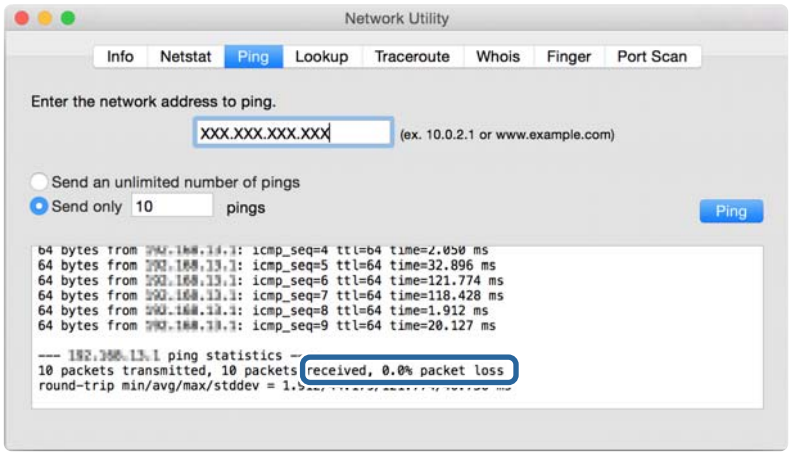
   Zadajte výraz „Network Utility“ (Sieťová pomôcka) v aplikácii **Spotlight**.

3. Kliknite na kartu **Ping**, zadajte IP adresu, ktorú ste overili v 1. kroku, a potom kliknite na tlačidlo **Ping**.

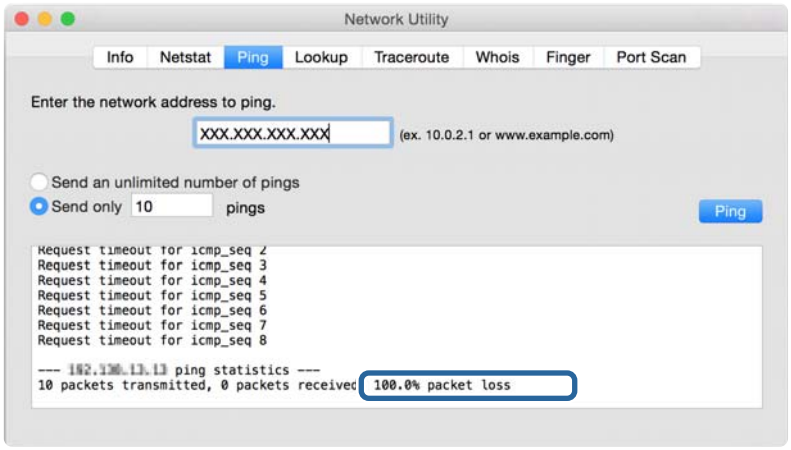


4. Skontrolujte stav komunikácie.

   Ak skener a počítač komunikujú, zobrazí sa nasledujúce hlásenie.



   Ak skener a počítač nekomunikujú, zobrazí sa nasledujúce hlásenie.



Problémy pri používaní sieťového softvéru

Aplikácia Web Config sa nedá otvoriť

Je adresa IP skenera nakonfigurovaná správne?

Nakonfigurujte adresu IP pomocou aplikácie Epson Device Admin alebo EpsonNet Config.

Podporuje váš prehľadávač hromadné šifrovanie pre položku Encryption Strength protokolu SSL/TLS?

Hromadné šifrovanie pre položku Encryption Strength protokolu SSL/TLS je nasledujúce. Aplikácia Web Config sa dá otvoriť len v prehľadávači, ktorý podporuje hromadné šifrovanie. Skontrolujte podporu šifrovania vo svojom prehľadávači.

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

❏ 192-bitové: AES256

❏ 256-bitové: AES256

Pri otváraní aplikácie Web Config prostredníctvom komunikácie SSL (https) sa zobrazí hlásenie „Neaktuálne“.

Ak je certifikát neaktuálny, získajte ho znova. Ak sa hlásenie zobrazí pred dátumom uplynutia platnosti, skontrolujte, či je dátum skenera nastavený správne.

Pri otváraní aplikácie Web Config prostredníctvom komunikácie SSL (https) sa zobrazí hlásenie „Názov bezpečnostného certifikátu sa nezhoduje…“.

Adresa IP skenera zadaná v položke **Common Name** pri vytváraní certifikátu s vlastným podpisom alebo žiadosti CSR sa nezhoduje s adresou zadanou do prehľadávača. Opätovne získajte a naimportujte certifikát alebo zmeňte názov skenera.

Skener je prístupný cez server proxy.

Ak pri používaní skenera používate server proxy, je potrebné v prehľadávači nakonfigurovať nastavenia servera proxy.

❏ Windows:

Vyberte položku **Ovládací panel** > **Sieť a internet** > **Možnosti siete internet** > **Pripojenia** > **Nastavenia siete LAN** > **Server proxy** a nastavte, aby sa pre lokálne adresy nepoužíval server proxy.

❏ Mac OS:

Vyberte položku **Systémové nastavenia** > **Sieť** > **Rozšírené** > **Proxy** a zaregistrujte lokálne adresy v položke **Obísť nastavenia proxy pre týchto hostiteľov a domény**.

Príklad:

192.168.1.*: Lokálna adresa 192.168.1.XXX, maska podsiete 255.255.255.0

192.168.*.*: Lokálna adresa 192.168.XXX.XXX, maska podsiete 255.255.0.0

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Priradenie IP adresy” na strane 15

➡ „Priradenie IP adresy pomocou aplikácie EpsonNet Config” na strane 56

Názov modelu alebo adresa IP sa nezobrazuje v aplikácii EpsonNet Config

Vybrali ste možnosť Block, Cancel alebo Shut down, keď sa zobrazila bezpečnostná obrazovka systému Windows alebo obrazovka brány firewall?

Ak ste vybrali možnosť **Blokovať**, **Zrušiť** alebo **Vypnúť**, adresa IP a názov modelu sa nezobrazia v aplikáciách EpsonNet Config a EpsonNet Setup.

Na nápravu tohto problému zaregistrujte aplikáciu EpsonNet Config ako výnimku pomocou brány firewall systému Windows a komerčného bezpečnostného softvéru. Ak používate antivírusový alebo bezpečnostný program, zatvorte ho a potom skúste použiť aplikáciu EpsonNet Config.

Je nastavený príliš krátky časový limit chyby komunikácie?

Spustite aplikáciu EpsonNet Config, vyberte položku **Tools** > **Options** > **Timeout** a zvýšte časový limit v nastavení **Communication Error**. Upozorňujeme, že to môže zapríčiniť pomalší beh aplikácie EpsonNet Config.

Súvisiace informácie

➡ „Spustenie aplikácie EpsonNet Config – systém Windows” na strane 56

➡ „Spustenie aplikácie EpsonNet Config – systém Mac OS” na strane 56

Príloha

Úvod do sieťového softvéru

Ďalej sa opisuje softvér, ktorý konfiguruje a spravuje zariadenia.

Epson Device Admin

Epson Device Admin je aplikácia, ktorá vám umožňuje inštaláciu zariadení v sieti a potom ich môžete zariadenia konfigurovať a spravovať. Môžete zistiť podrobné informácie pre zariadenia, ako je napríklad stav a spotrebný materiál, odosielať výstražné upozornenia a vytvárať správy pre využitie zariadenia. Môžete vytvoriť aj šablónu obsahujúcu položky nastavenia a použiť ju na iné zariadenia ako zdieľané nastavenie. Aplikáciu Epson Device Admin si môžete prevziať z webovej stránky podpory spoločnosti Epson. Ďalšie informácie nájdete v dokumentácii alebo Pomocníkovi k aplikácii Epson Device Admin.

Spustenie aplikácie Epson Device Admin (len systém Windows)

Vyberte položky **Všetky programy** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Poznámka:
Ak sa zobrazí upozornenie brány firewall, povoľte prístup pre aplikáciu Epson Device Admin.

EpsonNet Config

Aplikácia EpsonNet Config umožňuje správcovi konfigurovať sieťové nastavenia skenera, ako je napríklad priradenie adresy IP, a zmeniť režim pripojenia. Funkcia hromadného nastavenia je podporovaná v systéme Windows. Ďalšie informácie nájdete v dokumentácii alebo Pomocníkovi k aplikácii EpsonNet Config.

Spustenie aplikácie EpsonNet Config – systém Windows

Vyberte položky **Všetky programy** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Poznámka:
Ak sa zobrazí upozornenie brány firewall, povoľte prístup pre aplikáciu EpsonNet Config.

Spustenie aplikácie EpsonNet Config – systém Mac OS

Vyberte položky **Prejsť** > **Aplikácie** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager je softvér na vytvorenie balíka na jednoduchú inštaláciu tlačiarne, napríklad inštaláciu a konfiguráciu ovládača a inštaláciu aplikácie Document Capture Pro. Tento softvér umožňuje správcom vytvárať jedinečné softvérové balíky a ich distribúciu v skupinách.

Ďalšie informácie nájdete na oblastnej webovej stránke spoločnosti Epson.

Priradenie IP adresy pomocou aplikácie EpsonNet Config

Skeneru môžete priradiť IP adresu pomocou aplikácie EpsonNet Config. Aplikácia EpsonNet Config vám umožňuje po pripojení pomocou kábla siete Ethernet priradiť skeneru IP adresu, ktorá nebola priradená.

Priradenie IP adresy pomocou hromadných nastavení

Vytvorenie súboru pre hromadné nastavenia

Pomocou adresy MAC a názvu modelu ako kľúčov môžete vytvoriť nový súbor SYLK na nastavenie IP adresy.

1. Otvorte tabuľkovú aplikáciu (napríklad Microsoft Excel) alebo textový editor.

2. Do prvého riadka ako názvy položky nastavenia napíšte „Info_MACAddress“, „Info_ModelName“ a „TCPIP_IPAddress“.

   Zadajte položky nastavenia pre nasledujúce textové reťazce. Aby sa rozlíšili veľké/malé písmená a dvojbajtové/jednobajtové znaky, ak je jeden znak iný, položka nebude rozpoznaná.

   Zadajte názov položky nastavenia, ako je vysvetlené ďalej. V opačnom prípade aplikácia EpsonNet Config nedokáže rozpoznať položky nastavenia.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Zadajte adresu MAC, názov modelu a IP adresu jednotlivých sieťových rozhraní.

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. Zadajte názov a uložte ako súbor SYLK (*.slk).

Vytvorenie hromadných nastavení pomocou konfiguračného súboru

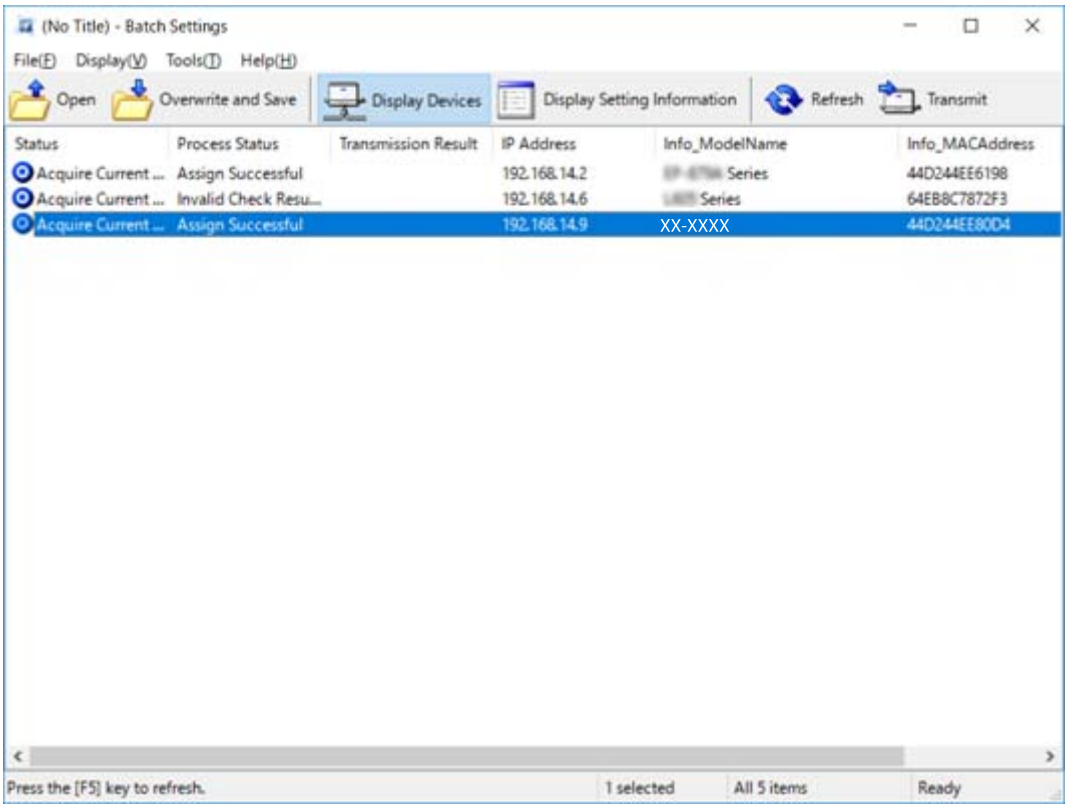
Priraďte naraz IP adresy v konfiguračnom súbore (SYLK). Pred priradením je potrebné vytvoriť konfiguračný súbor.

1. Pomocou kábla siete Ethernet pripojte všetky zariadenia k sieti.
2. Zapnite skener.
3. Spustite aplikáciu EpsonNet Config.

   Zobrazí sa zoznam skenerov v sieti. Kým sa zobrazia, môže to chvíľu trvať.
4. Kliknite na položky **Tools** > **Batch Settings**.
5. Kliknite na položku **Open**.
6. Na obrazovke výberu súboru vyberte súbor SYLK (*.slk) obsahujúci nastavenia a potom kliknite na položku **Open**.

7. Vyberte zariadenia, pre ktoré chcete vykonať hromadné nastavenia so stĺpčekom **Status** nastaveným na možnosť **Unassigned** a položkou **Process Status** nastavenou na možnosť **Assign Successful**.

   Keď vyberáte viac položiek, stlačte kláves Ctrl alebo Shift a kliknite alebo potiahnite myšou.



8. Kliknite na položku **Transmit**.

9. Keď sa zobrazí obrazovka na zadanie hesla, zadajte heslo a potom kliknite na tlačidlo **OK**.

   Preneste nastavenia.

   Poznámka:
   Informácie sa prenášajú do sieťového prostredia, kým sa priebeh nenaplní. Nevypínajte zariadenie ani bezdrôtový adaptér a neodosielajte do zariadenia žiadne údaje.

10. Na obrazovke **Transmitting Settings** kliknite na tlačidlo **OK**.

11. Skontrolujte stav zariadenia, ktoré ste nastavili.

    Pri zariadeniach, na ktorých sa zobrazuje  alebo  skontrolujte obsah súboru s nastaveniami, prípadne overte, či sa zariadenie ako reštartovalo normálne.

Ikona	Status	Process Status	Vysvetlenie
	Setup Complete	Setup Successful	Nastavenie dokončené normálne.
	Setup Complete	Rebooting	Keď sa informácie prenesú, jednotlivé zariadenia sa musia reštartovať, aby sa nastavenia použili. Vykoná sa kontrola, či sa dajú zariadenia po reštartovaní pripojiť.
	Setup Complete	Reboot Failed	Po prenesení nastavení sa nedá zariadenie overiť. Skontrolujte, či je zariadenie zapnuté, prípadne či sa reštartovalo normálne.
	Setup Complete	Searching	Vyhľadanie zariadenia označeného v súbore s nastaveniami.*
	Setup Complete	Search Failed	Nedajú sa skontrolovať zariadenia, ktoré už boli nastavené. Skontrolujte, či je zariadenie zapnuté, prípadne či sa reštartovalo normálne.*

* Len v prípade, že sa informácie o nastavení zobrazujú.

Súvisiace informácie

➡ „Spustenie aplikácie EpsonNet Config – systém Windows” na strane 56

➡ „Spustenie aplikácie EpsonNet Config – systém Mac OS” na strane 56

Priradenie IP adresy jednotlivým zariadeniam

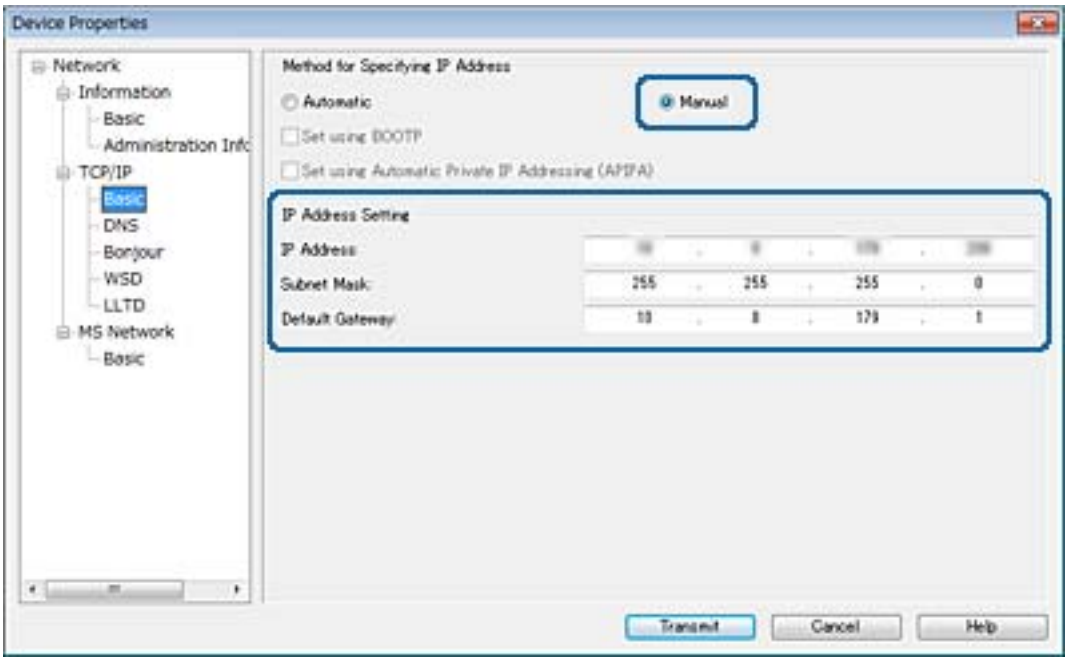
Priraďte IP adresu skeneru pomocou aplikácie EpsonNet Config.

1. Zapnite skener.
2. Pripojte skener k sieti pomocou kábla siete Ethernet.
3. Spustite aplikáciu EpsonNet Config.

   Zobrazí sa zoznam skenerov v sieti. Kým sa zobrazia, môže to chvíľu trvať.
4. Dvakrát kliknite na skener, ktorý chcete priradiť.

   Poznámka:
   Ak máte pripojených viac skenerov rovnakého modelu, môžete skener identifikovať pomocou adresy MAC.
5. Vyberte položky **Network** > **TCP/IP** > **Basic**.

6. Zadajte adresy pre **IP Address**, **Subnet Mask** a **Default Gateway**.



Poznámka:
Zadajte statickú adresu, ak pripájate skener k zabezpečenej sieti.

7. Kliknite na tlačidlo **Transmit**.

   Zobrazí sa obrazovka s potvrdením prenosu informácií.

8. Kliknite na tlačidlo **OK**.

   Zobrazí sa obrazovka dokončenia prenosu.

   Poznámka:
   Informácie sa prenesú do zariadenia a potom sa zobrazí hlásenie „Konfigurácia úspešne dokončená“. Nevypínajte zariadenie a neodosielajte do služby žiadne údaje.

9. Kliknite na tlačidlo **OK**.

Súvisiace informácie

➡ „Spustenie aplikácie EpsonNet Config – systém Windows” na strane 56
➡ „Spustenie aplikácie EpsonNet Config – systém Mac OS” na strane 56

Používanie portu pre skener

Skener používa nasledujúci port. Tieto porty musia byť povolené, aby boli v prípade potreby k dispozícii správcovi siete.

Príloha

Odosielateľ (klient)	Použitie	Cieľ (Server)	Protokol	Číslo portu
Skener	Odosielanie e-mailov (upozornenie e-mailom)	Server SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	Pripojenie POP pred SMTP (upozornenie e-mailom)	Server POP	POP3 (TCP)	110
	Ovládanie WSD	Klientsky počítač	WSD (TCP)	5357
	Vyhľadávanie počítača, keď sa vykonáva okamžité skenovanie z aplikácie Document Capture Pro	Klientsky počítač	Rozpoznanie v sieti pri okamžitom skenovaní	2968
	Zhromaždenie informácií o úlohe pri okamžitom skenovaní z aplikácie Document Capture Pro	Klientsky počítač	Okamžité skenovanie v sieti	2968
Klientsky počítač	Rozpoznanie skenera z aplikácie, ako je napríklad EpsonNet Config a ovládač skenera.	Skener	ENPC (UDP)	3289
	Zhromaždenie a nastavenie informácií MIB z aplikácie, ako je napríklad EpsonNet Config a ovládač skenera.	Skener	SNMP (UDP)	161
	Vyhľadanie skenera WSD	Skener	WS-Discovery (UDP)	3702
	Presmerovanie údajov skenovania z aplikácie Document Capture Pro	Skener	Skenovanie cez sieť (TCP)	1865

Nastavenia rozšíreného zabezpečenia pre firmy

V tejto kapitole sú opísané funkcie rozšíreného zabezpečenia.

Nastavenia zabezpečenia a prevencia pred nebezpečenstvom

Keď je zariadenie pripojené k sieti, môžete mať k nemu prístup na diaľku. Okrem toho mnohí ľudia môžu zdieľať zariadenia, čo je užitočné pre vylepšenie prevádzkovej účinnosti a praktické. Zvyšuje sa však riziko nezákonného prístupu, nezákonného používania a odcudzenia údajov. Ak používate zariadenie v prostredí, kde je možný prístup na internet, riziko je ešte vyššie.

Ak sa tomuto riziku chcete vyhnúť, zariadenia Epson ponúkajú množstvo technológií zabezpečenia.

Nastavte zariadenie tak, ako je potrebné podľa podmienok prostredia, ktoré boli vybudované s informáciami o prostredí zákazníka.

Názov	Typ funkcie	Čo sa nastavuje	Čomu sa zabráni
Komunikácia SSL/TLS	Komunikačná cesta medzi počítačom a zariadením je zašifrovaná pomocou komunikácie v protokole SSL/TLS. Obsah komunikácie cez prehľadávač je chránený.	Nastavte do zariadenia certifikát CA pre server, čo je certifikát podpísaný autoritou CA (Certificate Authority).	Zabráňte úniku informácií o nastavení a obsahu prenášaných údajov do skenera z počítača. Prístup k serveru Epson na internete zo zariadenia môže byť chránený aj aktualizáciou firmvéru atď.
Filtrovanie IPsec/IP	Môžete povoliť oddelenie a eliminovanie údajov, ktoré pochádzajú od určitého klienta alebo sú konkrétneho typu. Pretože protokol IPsec chráni údaje podľa paketových IP jednotiek (šifrovanie a overenie), môžete bezpečne komunikovať nezabezpečený protokol skenovania.	Vytvorte základné zásady a individuálne zásady nastavenia klienta alebo typu údajov, ktoré majú prístup do zariadenia.	Zabráňte nepovolenému prístupu, sabotáži a odpočúvaniu komunikačných údajov v zariadení.
SNMPv3	Pridané sú funkcie, ako je napríklad monitorovanie pripojených zariadení v sieti, celistvosť údajov, ktoré protokol SNMP ovláda, šifrovanie, overovanie používateľov atď.	Povoľte protokol SNMPv3 a potom nastavte spôsob overovania šifrovania.	Zaistite monitorovanie zmeny nastavení cez sieť a dôvernosť.

Nastavenia rozšíreného zabezpečenia pre firmy

Názov	Typ funkcie	Čo sa nastavuje	Čomu sa zabráni
IEEE802.1X	Umožnite pripojenie len používateľovi, ktorý má povolenie prístupu do siete Ethernet. Umožnite zariadenie používať iba povolenému používateľovi.	Nastavenie overovania na serveri RADIUS (overovací server).	Chráňte pred nepovoleným prístupom a používaním zariadenia.
Čítacia identifikačná karta	Môžete používať zariadenie po podržaní identifikačnej karty na pripojenom overovacom zariadení. Môžete obmedziť získavanie protokolov jednotlivých používateľov a zariadení a obmedziť dostupné využívanie zariadení a dostupné funkcie jednotlivých používateľov a skupín.	Pripojte k zariadeniu overovacie zariadenie a potom nastavte v overovacom systéme informácie o používateľovi.	Chráňte pred nepovoleným používaním zariadenia a odcudzením údajov.

Súvisiace informácie

➡ „Komunikácia so skenerom cez protokol SSL/TLS” na strane 63

➡ „Šifrovaná komunikácia pomocou filtrovania IPsec/IP” na strane 71

➡ „Používanie protokolu SNMPv3” na strane 83

➡ „Pripojenie skenera k sieti IEEE802.1X” na strane 85

Nastavenia funkcie zabezpečenia

Keď nastavujete funkciu filtrovania IPsec/IP alebo zabezpečenie IEEE802.1X, odporúča sa, aby ste otvorili aplikáciu Web Config pomocou protokolu SSL/TLS a komunikovali údaje nastavenia takto, aby sa znížili bezpečnostné riziká, ako sú napríklad falšovanie a zachytenie.

Komunikácia so skenerom cez protokol SSL/TLS

Keď je certifikát servera nastavený do skenera pomocou komunikačného protokolu SSL/TLS (Secure Sockets Layer/Transport Layer Security), môžete šifrovať komunikačnú cestu medzi počítačmi. Urobte to, ak chcete zabrániť vzdialenému a nepovolenému prístupu.

O digitálnom certifikáte

❏ Certifikát podpísaný CA

Certifikát podpísaný CA (certifikačnou autoritou) je potrebné získať od certifikačnej autority. Používaním certifikátu s podpisom CA môžete zaistiť bezpečnú komunikáciu. Certifikát s podpisom CA môžete použiť pre všetky bezpečnostné funkcie.

❏ Certifikát CA

Certifikát CA indikuje, že identitu servera overila tretia strana. Je to kľúčový prvok dôveryhodného webu. Certifikát CA na overenie servera je potrebné získať od CA, ktorá ho vydáva.

❏ Certifikát s vlastným podpisom

Certifikát s vlastným podpisom je certifikát vydaný a podpísaný samotným skenerom. Tento certifikát je nespoľahlivý a nemôže zabrániť predstieraniu iného zdroja (spoofing). Ak tento certifikát použijete ako certifikát SSL/TLS, v prehliadači sa môže zobraziť bezpečnostné upozornenie. Tento certifikát môžete použiť iba na komunikáciu SSL/TLS.

Súvisiace informácie

➡ „Získanie a import certifikátu s podpisom certifikačnej autority (CA)" na strane 64

➡ „Odstránenie certifikátu s podpisom CA" na strane 67

➡ „Aktualizácia certifikátu s vlastným podpisom" na strane 68

Získanie a import certifikátu s podpisom certifikačnej autority (CA)

Získanie certifikátu s podpisom CA

Ak chcete získať certifikát s podpisom CA, vytvorte žiadosť CSR (Certificate Signing Request — žiadosť o podpis certifikátu) a odošlite ju certifikačnej autorite. Žiadosť CSR môžete vytvoriť pomocou aplikácie Web Config a počítača.

Postupujte podľa pokynov na vytvorenie žiadosti CSR a získanie certifikátu s podpisom CA pomocou aplikácie Web Config. Ak sa žiadosť CSR vytvorí pomocou aplikácie Web Config, certifikát bude vo formáte PEM/DER.

1. Otvorte aplikáciu Web Config a potom vyberte položku **Network Security Settings**. Potom vyberte položky **SSL/TLS** > **Certificate** alebo **IPsec/IP Filtering** > **Client Certificate** alebo **IEEE802.1X** > **Client Certificate**.

2. Kliknite na možnosť **Generate** v položke **CSR**.

   Otvorí sa stránka vytvorenia žiadosti CSR.

3. Zadajte hodnoty pre všetky položky.

   Poznámka:
   Dĺžka kľúča a skratky sa líšia v závislosti od certifikačnej autority. Vytvorte žiadosť podľa pravidiel príslušnej certifikačnej autority.

4. Kliknite na položku **OK**.

   Zobrazí sa správa o vytvorení.

5. Vyberte položku **Network Security Settings**. Potom vyberte položky **SSL/TLS** > **Certificate** alebo **IPsec/IP Filtering** > **Client Certificate** alebo **IEEE802.1X** > **Client Certificate**.

6. Kliknutím na jedno z tlačidiel prevzatia žiadosti **CSR** podľa formátu stanoveného jednotlivými certifikačnými autoritami prevezmite žiadosť CSR do počítača.

   > ***Upozornenie:***
   > *Certifikát CSR znova nevytvárajte. Ak ho vytvoríte, vydaný certifikát CA-signed Certificate nebudete môcť importovať.*

7. Certifikát CSR pošlite certifikačnej autorite a získajte podpísaný certifikát CA-signed Certificate.

   Postupujte podľa pravidiel jednotlivých certifikačných autorít týkajúcich sa formy a metódy odoslania.

8. Vydaný certifikát CA-signed Certificate uložte do počítača, ktorý je pripojený ku skeneru.

   Získanie podpísaného certifikátu CA-signed Certificate je dokončené, keď certifikát uložíte do cieľového umiestnenia.

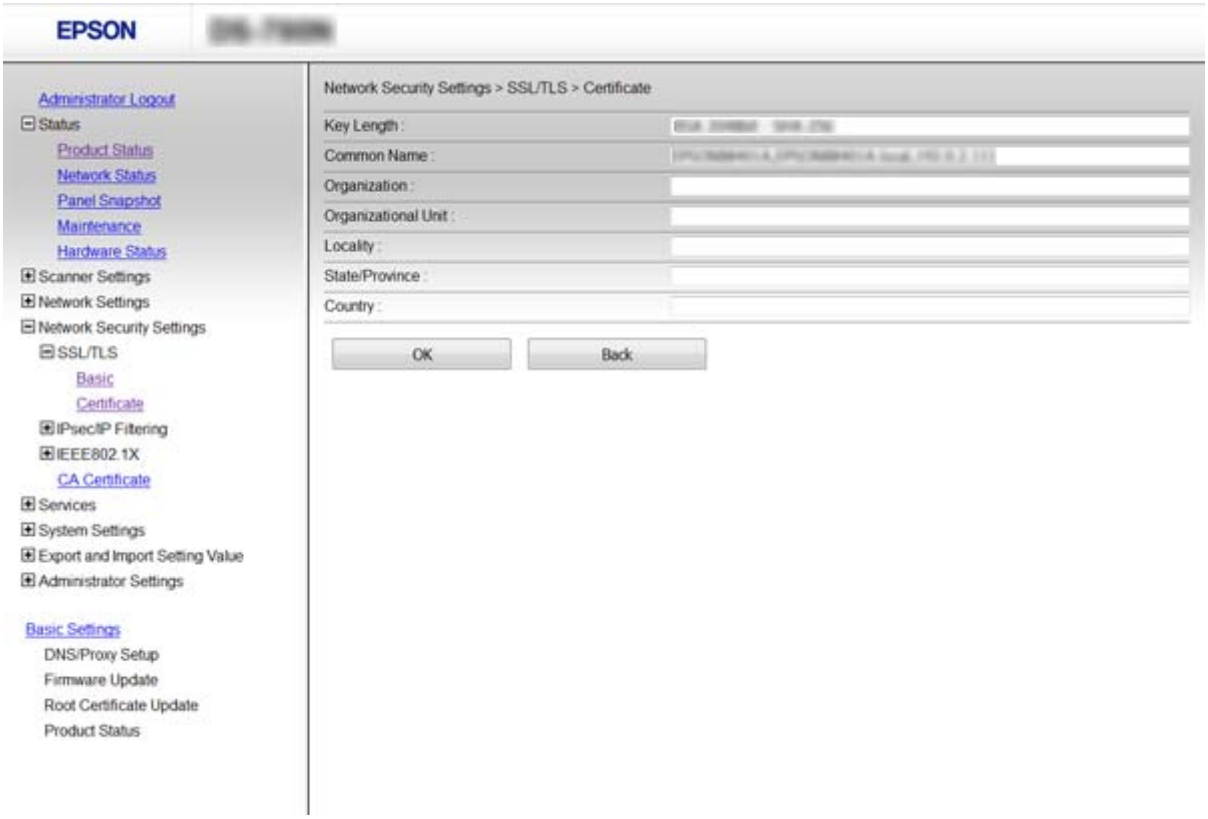
Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Položky nastavenia žiadosti CSR” na strane 65

➡ „Import certifikátu s podpisom CA” na strane 66

Položky nastavenia žiadosti CSR



Položky	Nastavenia a vysvetlenie
Key Length	Vyberte dĺžku kľúča pre žiadosť CSR.
Common Name	Môžete zadať 1 až 128 znakov. Ak je to adresa IP, mala by to byť statická adresa IP. Príklad: Adresa URL na otvorenie aplikácie Web Config: https://10.152.12.225 Bežný názov: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Môžete zadať 0 až 64 znakov v kódovaní ASCII (0x20 – 0x7E). Rozlíšené názvy môžete oddeliť čiarkami.
Country	Zadajte dvojciferný kód krajiny podľa normy ISO-3166.

Súvisiace informácie

➡ „Získanie certifikátu s podpisom CA” na strane 64

Import certifikátu s podpisom CA

Upozornenie:

❏ *Skontrolujte, či je dátum a čas skenera nastavený správne.*

❏ *Ak ste certifikát získali prostredníctvom žiadosti CSR vytvorenej v aplikácii Web Config, môžete ho naimportovať raz.*

1. Otvorte aplikáciu Web Config a potom vyberte položku **Network Security Settings**. Potom vyberte položky **SSL/TLS** > **Certificate** alebo **IPsec/IP Filtering** > **Client Certificate** alebo **IEEE802.1X** > **Client Certificate**.

2. Kliknite na položku **Import**.

   Otvorí sa stránka importu certifikátu.

3. Zadajte hodnoty pre všetky položky.

   Požadované položky nastavenia sa líšia v závislosti od miesta vytvorenia žiadosti CSR a formátu súboru certifikátu. Do požadovaných položiek zadajte hodnoty podľa nasledujúceho návodu.

   ❏ Certifikát vo formáte PEM/DER získaný z aplikácie Web Config

      ❏ **Private Key**: Nekonfigurujte, pretože skener obsahuje súkromný kľúč.

      ❏ **Password**: Nekonfigurujte.

      ❏ **CA Certificate 1**/**CA Certificate 2**: Nepovinné

   ❏ Certifikát vo formáte PEM/DER získaný z počítača

      ❏ **Private Key**: Je potrebné nastaviť.

      ❏ **Password**: Nekonfigurujte.

      ❏ **CA Certificate 1**/**CA Certificate 2**: Nepovinné

   ❏ Certifikát vo formáte PKCS#12 získaný z počítača

      ❏ **Private Key**: Nekonfigurujte.

      ❏ **Password**: Nepovinné

      ❏ **CA Certificate 1**/**CA Certificate 2**: Nekonfigurujte.

4. Kliknite na položku **OK**.

   Zobrazí sa správa o vytvorení.

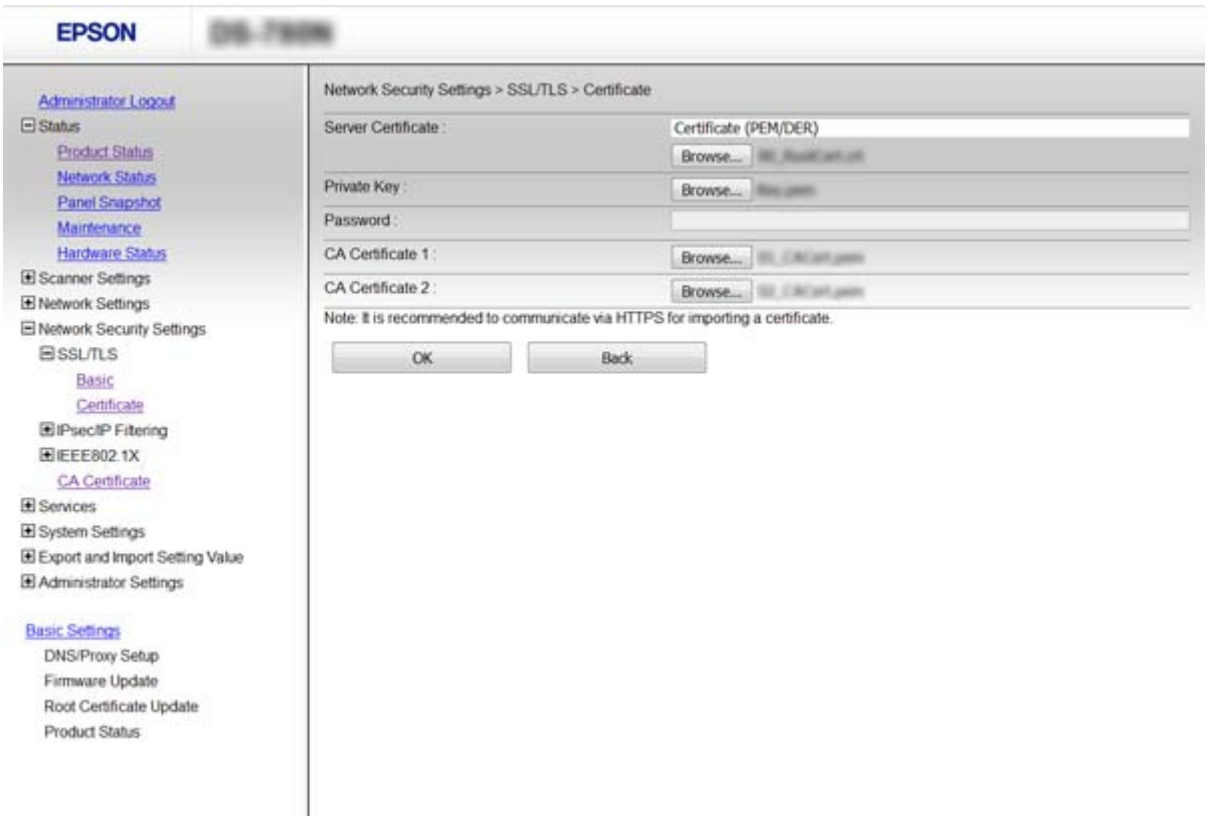
Poznámka:
*Kliknutím na položku **Confirm** potvrďte údaje certifikátu.*

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Položky nastavenia importu certifikátu s podpisom CA” na strane 67

Položky nastavenia importu certifikátu s podpisom CA



Položky	Nastavenia a vysvetlenie
Server Certificate alebo Client Certificate	Vyberte formát certifikátu.
Private Key	Ak získate certifikát vo formáte PEM/DER prostredníctvom žiadosti CSR vytvorenej v počítači, zadajte súbor súkromného kľúča zodpovedajúceho certifikátu.
Password	Zadajte heslo na šifrovanie súkromného kľúča.
CA Certificate 1	Ak je certifikát vo formáte **Certificate (PEM/DER)**, naimportujte certifikát certifikačnej autority, ktorá ho vydala. V prípade potreby zadajte súbor.
CA Certificate 2	Ak je certifikát vo formáte **Certificate (PEM/DER)**, naimportujte certifikát certifikačnej autority, ktorá vydala certifikát **CA Certificate 1**. V prípade potreby zadajte súbor.

Súvisiace informácie

➡ „Import certifikátu s podpisom CA” na strane 66

Odstránenie certifikátu s podpisom CA

Naimportovaný certifikát môžete odstrániť, keď skončí jeho platnosť alebo keď už nie je potrebné šifrované pripojenie.

> ***Upozornenie:***
> *Ak ste certifikát získali prostredníctvom žiadosti CSR vytvorenej v aplikácii Web Config, odstránený certifikát nemôžete znova naimportovať. V takom prípade vytvorte žiadosť CSR a certifikát získajte znova.*

1. Otvorte aplikáciu Web Config a potom vyberte položku **Network Security Settings**. Potom vyberte položky **SSL/TLS** > **Certificate** alebo **IPsec/IP Filtering** > **Client Certificate** alebo **IEEE802.1X** > **Client Certificate**.
2. Kliknite na položku **Delete**.
3. V zobrazenom hlásení potvrďte, že certifikát chcete odstrániť.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Aktualizácia certifikátu s vlastným podpisom

Ak skener podporuje funkciu servera HTTPS, môžete aktualizovať certifikát s vlastným podpisom. Pri otvorení aplikácie Web Config prostredníctvom certifikátu s vlastným podpisom sa zobrazí správa s upozornením.

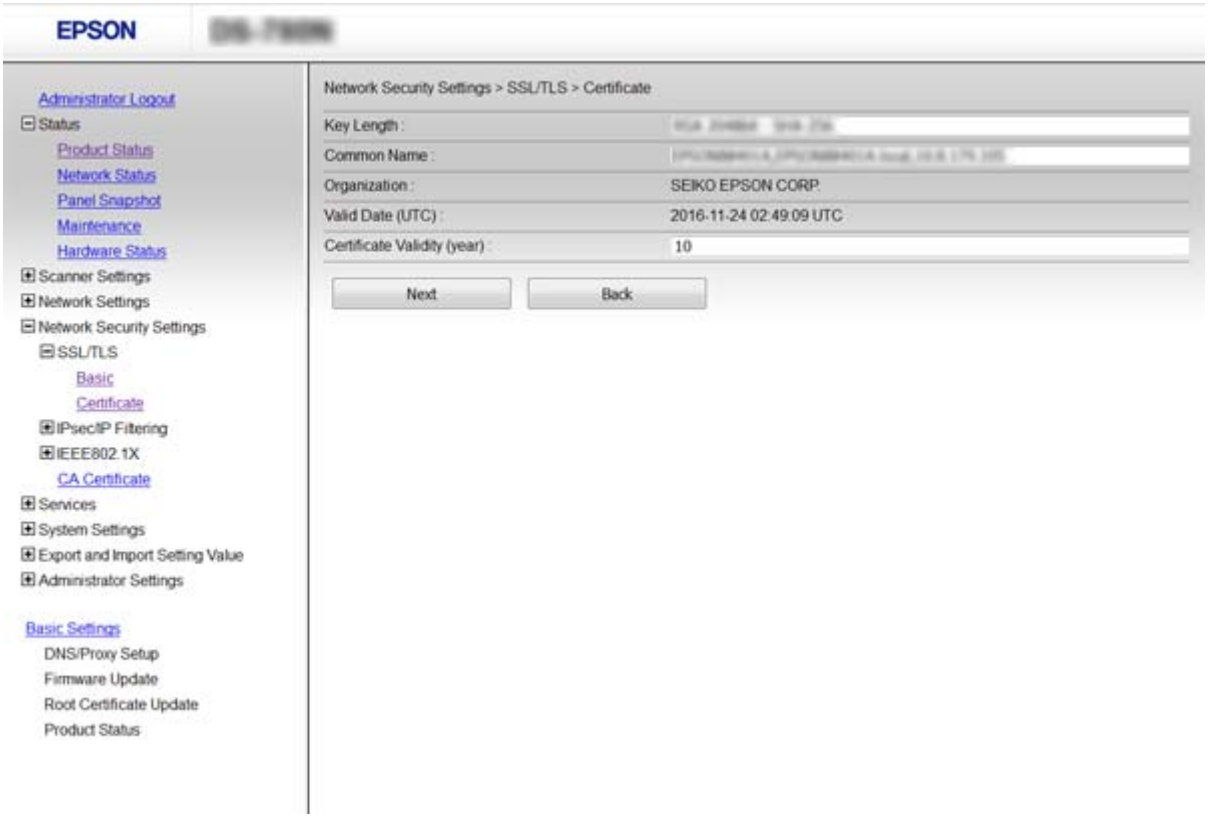
Certifikát s vlastným podpisom používajte dočasne, kým získate a naimportujte certifikát s podpisom CA.

1. Otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Kliknite na položku **Update**.
3. Zadajte položku **Common Name**.

   Zadajte IP adresu alebo identifikátor skenera, ako napríklad názov FQDN. Môžete zadať 1 až 128 znakov.

   Poznámka:
   Rozlišujúci názov (CN) môžete oddeliť čiarkami.

4. Zadajte dobu platnosti certifikátu.



5. Kliknite na položku **Next**.

   Zobrazí sa potvrdzujúca správa.

6. Kliknite na položku **OK**.

   Skener je aktualizovaný.

Poznámka:
*Kliknutím na položku **Confirm** potvrďte údaje certifikátu.*

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Nakonfigurujte položku CA Certificate

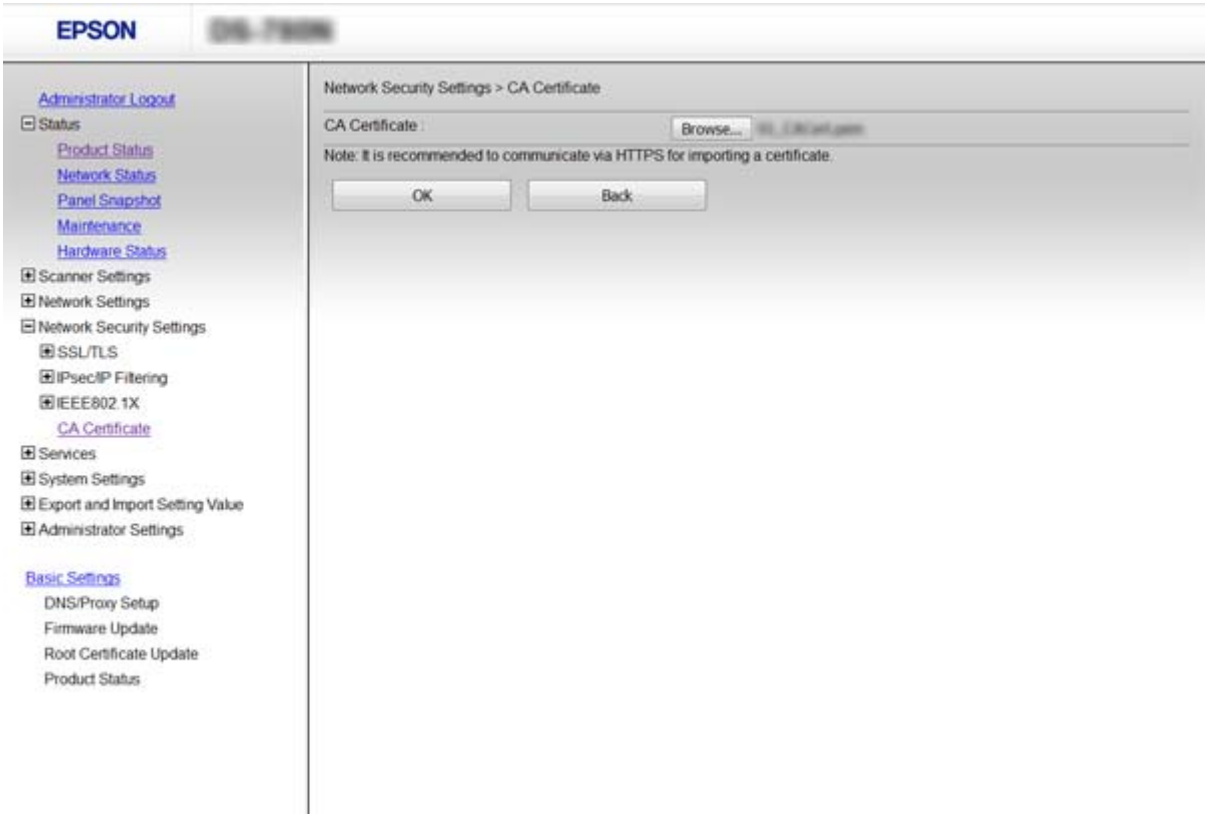
Certifikát CA Certificate môžete importovať, zobraziť alebo odstrániť.

Importovanie certifikátu CA Certificate

1. Otvorte aplikáciu Web Config a potom vyberte položky **Network Security Settings** > **CA Certificate**.

2. Kliknite na položku **Import**.

3. Určite certifikát CA Certificate, ktorý chcete importovať.



4. Kliknite na položku **OK**.

Po dokončení importovania sa môžete vrátiť na obrazovku **CA Certificate**, na ktorej je zobrazený certifikát CA Certificate.

Súvisiace informácie

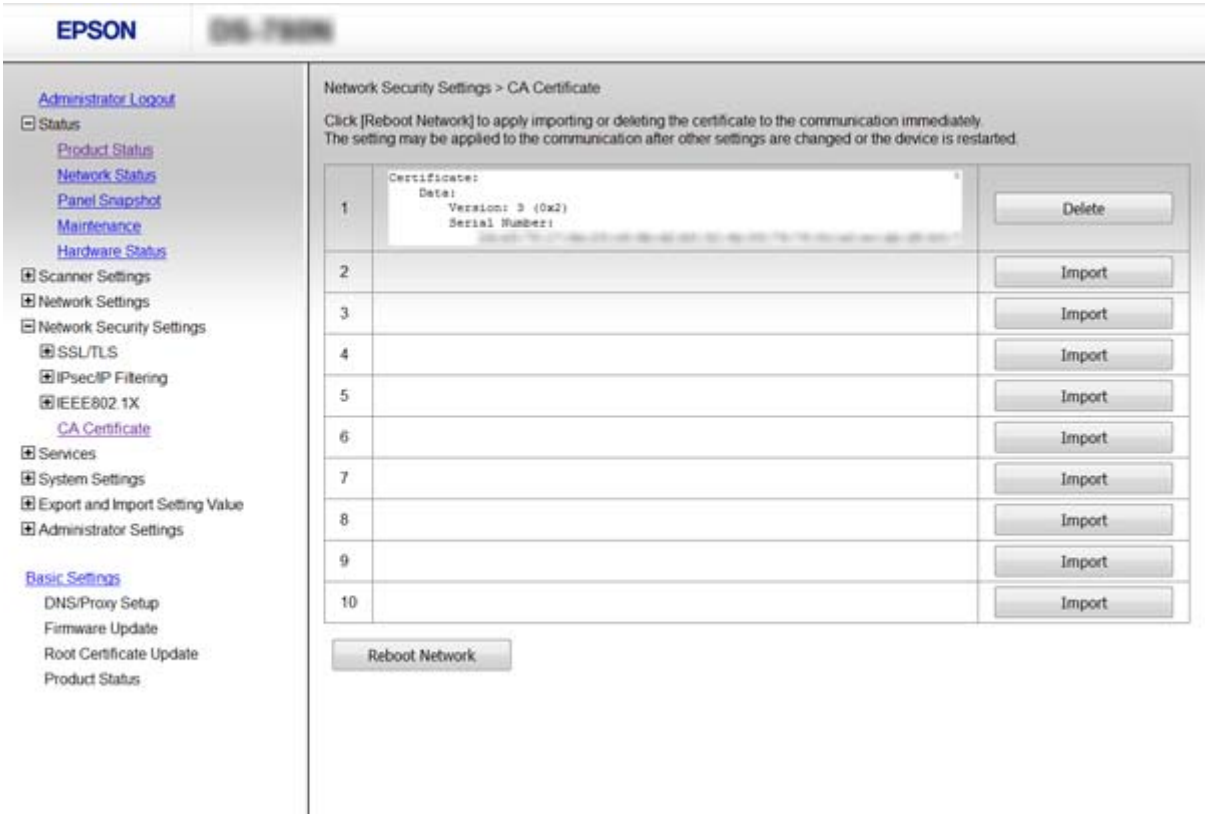
➡ „Otvorenie aplikácie Web Config” na strane 23

Odstránenie certifikátu CA Certificate

Importovaný certifikát CA Certificate môžete odstrániť.

1. Otvorte aplikáciu Web Config a potom vyberte položky **Network Security Settings** > **CA Certificate**.

2. Kliknite na možnosť **Delete** vedľa položky CA Certificate, ktorú chcete odstrániť.



3. V zobrazenom hlásení potvrďte, že certifikát chcete odstrániť.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Šifrovaná komunikácia pomocou filtrovania IPsec/IP

Čo je IPsec/IP Filtering

Ak skener podporuje filtrovanie IPsec/IP, môžete filtrovať prenos údajov na základe IP adries, služieb a portu. Kombináciou kritérií filtrovania môžete nakonfigurovať skener na akceptáciu alebo blokovanie určených klientov a údajov. Okrem toho môžete zlepšiť úroveň bezpečnosti používaním služby IPsec.

Ak chcete filtrovať komunikáciu, nakonfigurujte predvolenú politiku. Predvolené zásady sa vzťahujú na všetkých používateľov a skupiny pripájajúce sa ku skeneru. Ak chcete mať podrobnejšiu kontrolu nad používateľmi a používateľskými skupinami, nakonfigurujte skupinové politiky. Skupinová politika je jedno alebo viac pravidiel vzťahujúcich sa na používateľa alebo skupinu používateľov. Skener riadi pakety IP, ktoré zodpovedajú nakonfigurovaným zásadám. Pakety IP sa overujú v poradí skupinovej politiky 1 až 10 a potom predvolenej politiky.

Poznámka:
Počítače so systémom Windows Vista alebo novším, prípadne systémom Windows Server 2008 alebo novším, podporujú funkciu IPsec.

Konfigurácia položky Default Policy

1. Otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Zadajte hodnoty pre všetky položky.
3. Kliknite na položku **Next**.

   Zobrazí sa potvrdzujúca správa.
4. Kliknite na položku **OK**.

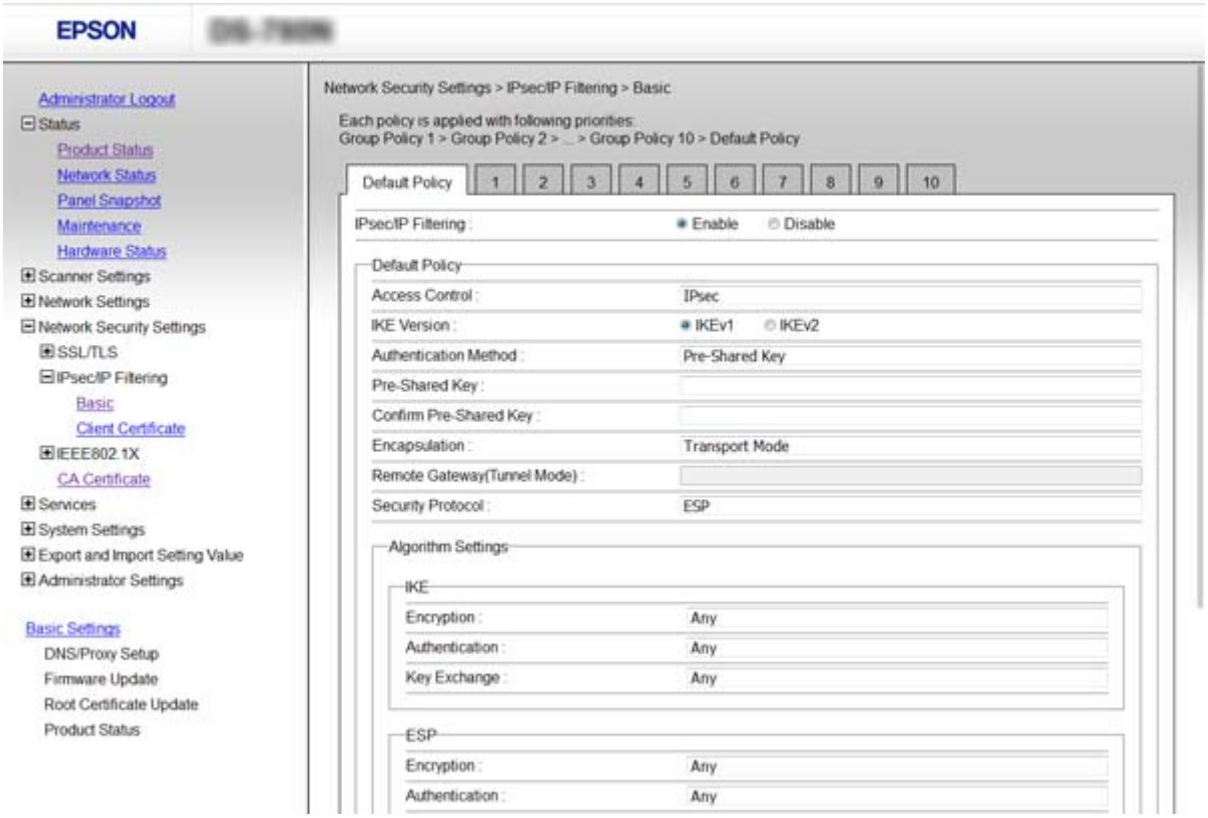
   Skener je aktualizovaný.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Nastavenie možností položky Default Policy” na strane 72

Nastavenie možností položky Default Policy



Položky	Nastavenia a vysvetlenie
IPsec/IP Filtering	Môžete zapnúť alebo vypnúť funkciu filtrovania IPsec/IP.

Nastavenia rozšíreného zabezpečenia pre firmy

Položky	Nastavenia a vysvetlenie	
Access Control	Nakonfigurujte metódu riadenia komunikácie prostredníctvom paketov IP.	
	Permit Access	Vybratím tejto možnosti povolíte, aby sa nakonfigurované pakety IP dostali do tlačiarne.
	Refuse Access	Vybratím tejto možnosti zakážete, aby sa nakonfigurované pakety IP dostali do tlačiarne.
	IPsec	Vybratím tejto možnosti povolíte, aby sa nakonfigurované pakety IPsec dostali do tlačiarne.
IKE Version	Vyberte možnosť IKEv1 alebo IKEv2 pre verziu IKE. Vyberte jednu z nich v závislosti od zariadenia, ku ktorému je skener pripojený.	
IKEv1	Keď vyberiete možnosť **IKEv1** pre položku **IKE Version**, zobrazia sa nasledujúce položky.	
	Authentication Method	Ak chcete vybrať možnosť **Certificate**, musíte najskôr získať a naimportovať certifikát s podpisom CA.
	Pre-Shared Key	Ak vyberiete možnosť **Pre-Shared Key** v položke **Authentication Method**, zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Confirm Pre-Shared Key	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.
IKEv2	Keď vyberiete možnosť **IKEv2** pre položku **IKE Version**, zobrazia sa nasledujúce položky.	
Local	Authentication Method	Ak chcete vybrať možnosť **Certificate**, musíte najskôr získať a naimportovať certifikát s podpisom CA.
	ID Type	Vyberte typ identifikácie pre skener.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. **Distinguished Name**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „=“. **IP Address**: zadajte formát IPv4 alebo IPv6. **FQDN**: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). **Email Address**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „@“. **Key ID**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E).
	Pre-Shared Key	Ak vyberiete možnosť **Pre-Shared Key** v položke **Authentication Method**, zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Confirm Pre-Shared Key	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.

Nastavenia rozšíreného zabezpečenia pre firmy

Položky	Nastavenia a vysvetlenie	
Remote	Authentication Method	Ak chcete vybrať možnosť **Certificate**, musíte najskôr získať a naimportovať certifikát s podpisom CA.
	ID Type	Vyberte typ identifikácie pre zariadenie, ktoré chcete overiť.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. **Distinguished Name**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „=“. **IP Address**: zadajte formát IPv4 alebo IPv6. **FQDN**: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). **Email Address**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „@“. **Key ID**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E).
	Pre-Shared Key	Ak vyberiete možnosť **Pre-Shared Key** v položke **Authentication Method**, zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Confirm Pre-Shared Key	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.
Encapsulation	Ak v položke **IPsec** vyberiete možnosť **Access Control**, musíte nakonfigurovať režim zapuzdrovania.	
	Transport Mode	Ak skener používate iba v rovnakej sieti LAN, vyberte túto možnosť. Pakety IP vrstvy 4 alebo vyššej sú šifrované.
	Tunnel Mode	Ak používate skener v sieti s pripojením k internetu, ako je napríklad IPsec-VPN, vyberte túto možnosť. Hlavičky a údaje paketov IP sú šifrované.
Remote Gateway(Tunnel Mode)	Ak vyberiete možnosť **Tunnel Mode** v položke **Encapsulation**, zadajte adresu brány dlhú 1 až 39 znakov.	
Security Protocol	**IPsec** pre položku **Access Control**. Vyberte možnosť.	
	ESP	Túto položku vyberte na zabezpečenie integrity overovania a údajov a na šifrovanie údajov.
	AH	Túto položku vyberte na zabezpečenie integrity overovania a údajov. Službu IPsec môžete používať, aj keď je šifrovanie údajov zakázané.
Algorithm Settings		
IKE	Encryption	Vyberte algoritmus šifrovania pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.
	Authentication	Vyberte algoritmus overovania pre IKE.
	Key Exchange	Vyberte algoritmus výmeny kľúča pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.

Nastavenia rozšíreného zabezpečenia pre firmy

Položky	Nastavenia a vysvetlenie	
ESP	Encryption	Vyberte algoritmus šifrovania pre ESP. To je k dispozícii, keď je možnosť **ESP** zvolená pre položku **Security Protocol**.
	Authentication	Vyberte algoritmus overovania pre ESP. To je k dispozícii, keď je možnosť **ESP** zvolená pre položku **Security Protocol**.
AH	Authentication	Vyberte algoritmus šifrovania pre AH. To je k dispozícii, keď je možnosť **AH** zvolená pre položku **Security Protocol**.

Súvisiace informácie

➡ „Konfigurácia položky Default Policy” na strane 72

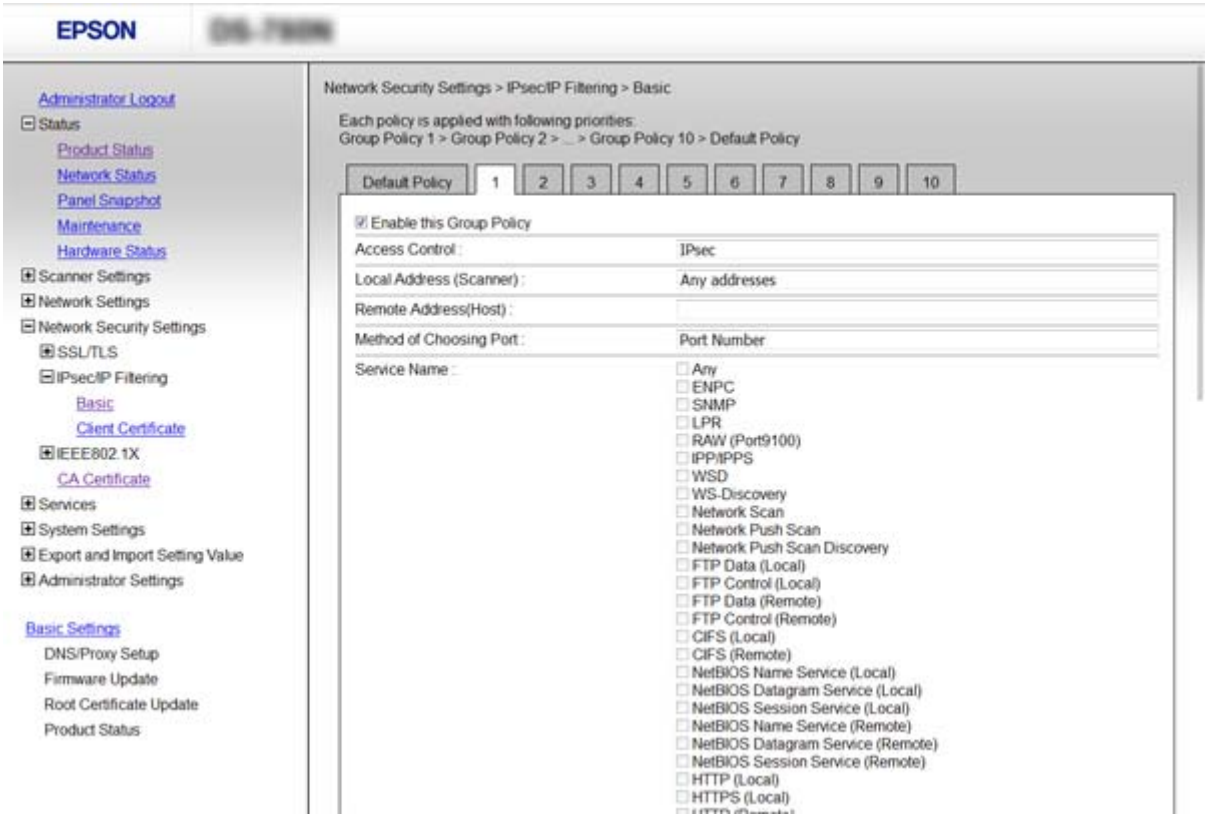
Konfigurácia položky Group Policy

1. Otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Kliknite na očíslovanú kartu, ktorú chcete konfigurovať.
3. Zadajte hodnoty pre všetky položky.
4. Kliknite na položku **Next**.
   Zobrazí sa potvrdzujúca správa.
5. Kliknite na položku **OK**.
   Skener je aktualizovaný.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23
➡ „Položky nastavenia Group Policy” na strane 76

Položky nastavenia Group Policy



Položky	Nastavenia a vysvetlenie	
Enable this Group Policy	Môžete zapnúť alebo vypnúť skupinovú politiku.	
Access Control	Nakonfigurujte metódu riadenia komunikácie prostredníctvom paketov IP.	
	Permit Access	Vybratím tejto možnosti povolíte, aby sa nakonfigurované pakety IP dostali do tlačiarne.
	Refuse Access	Vybratím tejto možnosti zakážete, aby sa nakonfigurované pakety IP dostali do tlačiarne.
	IPsec	Vybratím tejto možnosti povolíte, aby sa nakonfigurované pakety IPsec dostali do tlačiarne.
Local Address (Scanner)	Vyberte adresu IPv4 alebo IPv6, ktoré zodpovedajú vášmu sieťovému prostrediu. Ak je IP adresa priraďovaná automaticky, môžete vybrať možnosť **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Zadajte IP adresu na riadenie prístupu. IP adresa môže mať najviac 43 znakov. Ak nezadáte IP adresu, budú sa riadiť všetky adresy. ***Poznámka:*** *Ak je adresa IP pridelená automaticky (napríklad službou DHCP), pripojenie nemusí byť k dispozícii. Nakonfigurujte statickú adresu IP.*	
Method of Choosing Port	Vyberte spôsob určenia portov.	
Service Name	Ak v položke **Service Name** vyberiete možnosť **Method of Choosing Port**, vyberte niektorú možnosť.	

Nastavenia rozšíreného zabezpečenia pre firmy

Položky	Nastavenia a vysvetlenie	
Transport Protocol	Ak v položke **Port Number** vyberiete možnosť **Method of Choosing Port**, musíte nakonfigurovať režim zapuzdrovania.	
	Any Protocol	Túto možnosť vyberte na riadenie všetkých typov protokolu.
	TCP	Túto možnosť vyberte na riadenie údajov pri vysielaní typu unicast.
	UDP	Túto možnosť vyberte na riadenie údajov pri vysielaní typu broadcast a multicast.
	ICMPv4	Túto možnosť vyberte na riadenie príkazu ping.
Local Port	Ak vyberiete možnosť **Port Number** pre položku **Method of Choosing Port** a ak vyberiete možnosť **TCP** alebo **UDP** pre položku **Transport Protocol**, zadajte čísla portov na riadenie prichádzajúcich paketov. Oddeľte ich čiarkami. Môžete zadať maximálne 10 čísel portov. Príklad: 20,80,119,5220 Ak nezadáte číslo portu, budú sa riadiť všetky porty.	
Remote Port	Ak vyberiete možnosť **Port Number** pre položku **Method of Choosing Port** a ak vyberiete možnosť **TCP** alebo **UDP** pre položku **Transport Protocol**, zadajte čísla portov na riadenie odosielaných paketov. Oddeľte ich čiarkami. Môžete zadať maximálne 10 čísel portov. Príklad: 25,80,143,5220 Ak nezadáte číslo portu, budú sa riadiť všetky porty.	
IKE Version	Vyberte možnosť IKEv1 alebo IKEv2 pre verziu IKE. Vyberte jednu z nich v závislosti od zariadenia, ku ktorému je skener pripojený.	
IKEv1	Keď vyberiete možnosť **IKEv1** pre položku **IKE Version**, zobrazia sa nasledujúce položky.	
	Authentication Method	Ak v položke **IPsec** vyberiete možnosť **Access Control**, vyberte niektorú možnosť. Pri predvolenej politike sa zvyčajne používa certifikát.
	Pre-Shared Key	Ak vyberiete možnosť **Pre-Shared Key** v položke **Authentication Method**, zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Confirm Pre-Shared Key	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.
IKEv2	Keď vyberiete možnosť **IKEv2** pre položku **IKE Version**, zobrazia sa nasledujúce položky.	

Nastavenia rozšíreného zabezpečenia pre firmy

Položky	Nastavenia a vysvetlenie	
Local	Authentication Method	Ak v položke **IPsec** vyberiete možnosť **Access Control**, vyberte niektorú možnosť. Pri predvolenej politike sa zvyčajne používa certifikát.
	ID Type	Vyberte typ identifikácie pre skener.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. **Distinguished Name**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „=“. **IP Address**: zadajte formát IPv4 alebo IPv6. **FQDN**: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). **Email Address**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „@“. **Key ID**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E).
	Pre-Shared Key	Ak vyberiete možnosť **Pre-Shared Key** v položke **Authentication Method**, zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Confirm Pre-Shared Key	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.
Remote	Authentication Method	Ak v položke **IPsec** vyberiete možnosť **Access Control**, vyberte niektorú možnosť. Pri predvolenej politike sa zvyčajne používa certifikát.
	ID Type	Vyberte typ identifikácie pre zariadenie, ktoré chcete overiť.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. **Distinguished Name**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „=“. **IP Address**: zadajte formát IPv4 alebo IPv6. **FQDN**: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). **Email Address**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Je potrebné, aby obsahovalo znak „@“. **Key ID**: zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E).
	Pre-Shared Key	Ak vyberiete možnosť **Pre-Shared Key** v položke **Authentication Method**, zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Confirm Pre-Shared Key	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.

Nastavenia rozšíreného zabezpečenia pre firmy

Položky	Nastavenia a vysvetlenie	
Encapsulation	Ak v položke **IPsec** vyberiete možnosť **Access Control**, musíte nakonfigurovať režim zapuzdrovania.	
	Transport Mode	Ak skener používate iba v rovnakej sieti LAN, vyberte túto možnosť. Pakety IP vrstvy 4 alebo vyššej sú šifrované.
	Tunnel Mode	Ak používate skener v sieti s pripojením k internetu, ako je napríklad IPsec-VPN, vyberte túto možnosť. Hlavičky a údaje paketov IP sú šifrované.
Remote Gateway(Tunnel Mode)	Ak vyberiete možnosť **Tunnel Mode** v položke **Encapsulation**, zadajte adresu brány dlhú 1 až 39 znakov.	
Security Protocol	Ak v položke **IPsec** vyberiete možnosť **Access Control**, vyberte niektorú možnosť.	
	ESP	Túto položku vyberte na zabezpečenie integrity overovania a údajov a na šifrovanie údajov.
	AH	Túto položku vyberte na zabezpečenie integrity overovania a údajov. Službu IPsec môžete používať, aj keď je šifrovanie údajov zakázané.
Algorithm Settings		
IKE	Encryption	Vyberte algoritmus šifrovania pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.
	Authentication	Vyberte algoritmus overovania pre IKE.
	Key Exchange	Vyberte algoritmus výmeny kľúča pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.
ESP	Encryption	Vyberte algoritmus šifrovania pre ESP. To je k dispozícii, keď je možnosť **ESP** zvolená pre položku **Security Protocol**.
	Authentication	Vyberte algoritmus overovania pre ESP. To je k dispozícii, keď je možnosť **ESP** zvolená pre položku **Security Protocol**.
AH	Authentication	Vyberte algoritmus overovania pre AH. To je k dispozícii, keď je možnosť **AH** zvolená pre položku **Security Protocol**.

Súvisiace informácie

➡ „Konfigurácia položky Group Policy” na strane 75

➡ „Kombinácia Local Address (Scanner) a Remote Address(Host) v položke Group Policy” na strane 80

➡ „Odkazy na názvy služieb v Zásadách skupiny” na strane 80

Kombinácia Local Address (Scanner) a Remote Address(Host) v položke Group Policy

		Nastavenie položky Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Nastavenie položky Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Prázdne	✓	✓	✓

*1 Ak je vybraná možnosť **IPsec** pre položku **Access Control**, nemôžete určiť dĺžku predpony.

*2 Ak je vybraná možnosť **IPsec** pre položku **Access Control**, môžete vybrať prepojenie na lokálnu adresu (fe80::), ale skupinové zásady budú deaktivované.

*3 Okrem prepojení na lokálne adresy IPv6.

Odkazy na názvy služieb v Zásadách skupiny

Poznámka:
Nedostupné služby sa zobrazujú, ale nedajú sa vybrať.

Názov služby	Typ protokolu	Číslo lokálneho portu	Číslo vzdialeného portu	Ovládané funkcie
Any	–	–	–	Všetky služby
ENPC	UDP	3289	Akýkoľvek port	Vyhľadávanie skenera z aplikácií, ako je napríklad EpsonNet Config a ovládača skenera
SNMP	UDP	161	Akýkoľvek port	Získanie a nakonfigurovanie MIB z aplikácií, ako je napríklad EpsonNet Config, a ovládača skenera Epson
WSD	TCP	Akýkoľvek port	5357	Ovládanie WSD
WS-Discovery	UDP	3702	Akýkoľvek port	Vyhľadávanie skenera z WSD
Network Scan	TCP	1865	Akýkoľvek port	Presmerovanie údajov skenovania z režimu Document Capture Pro
Network Push Scan Discovery	UDP	2968	Akýkoľvek port	Vyhľadanie počítača zo skenera.
Network Push Scan	TCP	Akýkoľvek port	2968	Získanie informácií úlohy okamžitého skenovania z režimu Document Capture Pro alebo Document Capture
HTTP (Local)	TCP	80	Akýkoľvek port	Server HTTP(S) (presmerovanie údajov aplikácie Web Config a WSD)
HTTPS (Local)	TCP	443	Akýkoľvek port	

Názov služby	Typ protokolu	Číslo lokálneho portu	Číslo vzdialeného portu	Ovládané funkcie
HTTP (Remote)	TCP	Akýkoľvek port	80	Klient HTTP(S) (komunikácia medzi aktualizáciou firmvéru a aktualizáciou koreňového certifikátu)
HTTPS (Remote)	TCP	Akýkoľvek port	443	

Príklady konfigurácie funkcie IPsec/IP Filtering

Príjem iba paketov IPsec

Toto je príklad iba na konfiguráciu predvolených zásad.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: Zadajte max. 127 znakov.

Group Policy:

Nekonfigurujte.

Prijatie skenovania pomocou aplikácie Epson Scan 2 a nastavení skenera

Tento príklad umožňuje komunikáciu údajov skenovania a nastavení skenera z určených služieb.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Začiarknite políčko.

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

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

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

❏ **Service Name**: Začiarknite políčko **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** a **HTTPS (Local)**.

Prístup k prijímaniu iba z určenej adresy IP

V tomto príklade je prístup ku skeneru povolený iba zo zadanej adresy IP.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Začiarknite políčko.

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

❏ **Remote Address(Host)**: Adresa IP klienta správcu

Poznámka:
Bez ohľadu na konfiguráciu zásad bude mať klient prístup ku skeneru a bude ho môcť konfigurovať.

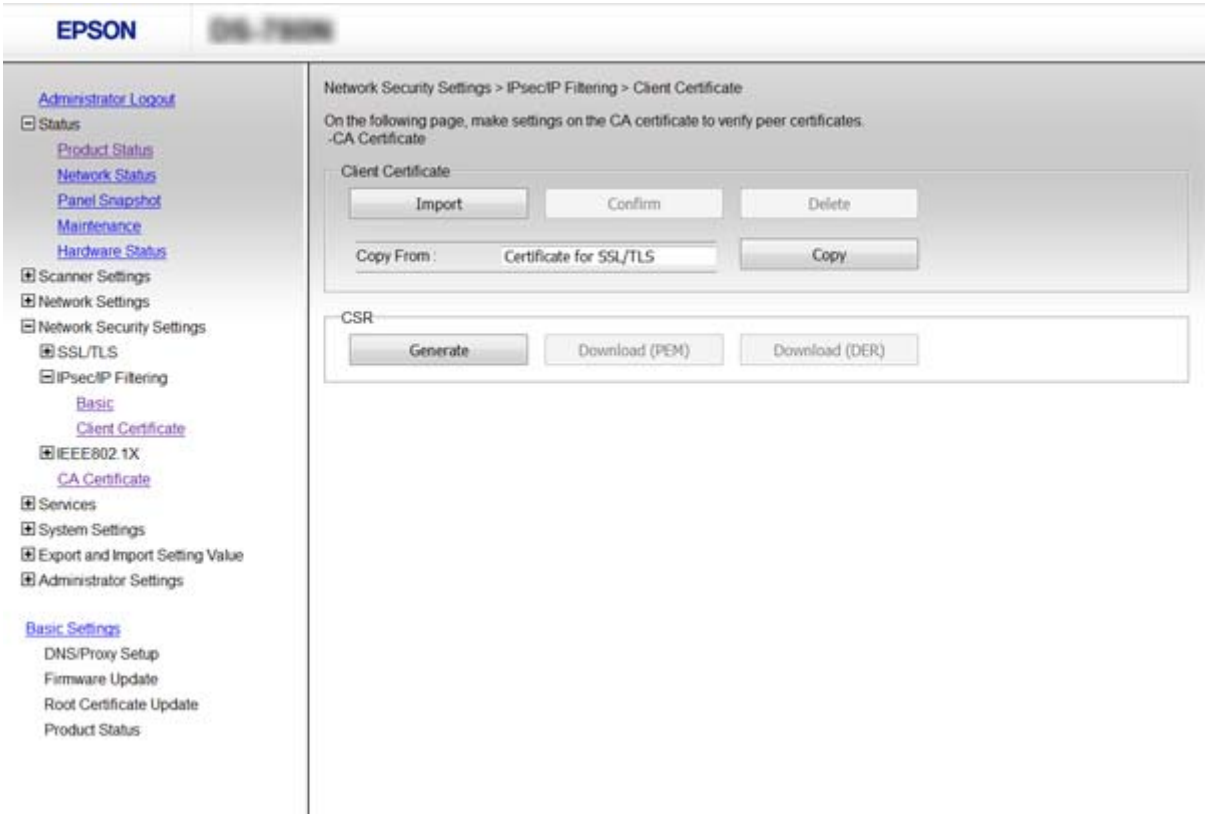
Konfigurácia certifikátu pre IPsec/IP Filtering

Nakonfigurujte aplikáciu Certifikát klienta pre IPsec/IP Filtering. Ak chcete nakonfigurovať certifikačnú autoritu, prejdite do **CA Certificate**.

1. Otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Certifikát importujte v položke **Client Certificate**.

   Ak ste už importovali certifikát, ktorý certifikačná autorita vydala v IEEE802.1X alebo SSL/TLS, tento certifikát môžete skopírovať a používať v IPsec/IP Filtering. Ak chcete certifikát skopírovať, vyberte ho z položky **Copy From** a potom kliknite na možnosť **Copy**.



Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Získanie a import certifikátu s podpisom certifikačnej autority (CA)” na strane 64

Používanie protokolu SNMPv3

Čo je protokol SNMPv3

SNMP je protokol, ktorý sa stará o monitorovanie a riadenie zhromažďovania údajov zariadení, ktoré s pripojené k sieti. SNMPv3 je verzia funkcie riadenia zabezpečenia, ktorá bola vylepšená.

Keď sa používa protokol SNMPv3, zmeny stavu monitorovania a nastavenia komunikácie SNMP (paket) môžu byť overované a šifrované s cieľom chrániť komunikáciu cez protokol SNMP (paket) pred sieťovými rizikami, ako sú napríklad odpočúvanie, zosobnenie a manipulácia.

Konfigurácia protokolu SNMPv3

Ak skener podporuje protokol SNMPv3, môžete monitorovať a riadiť prístupy ku skeneru.

1. Otvorte aplikáciu Web Config a vyberte položky **Services** > **Protocol**.
2. Zadajte hodnoty pre všetky položky **SNMPv3 Settings**.
3. Kliknite na položku **Next**.

   Zobrazí sa potvrdzujúca správa.
4. Kliknite na položku **OK**.

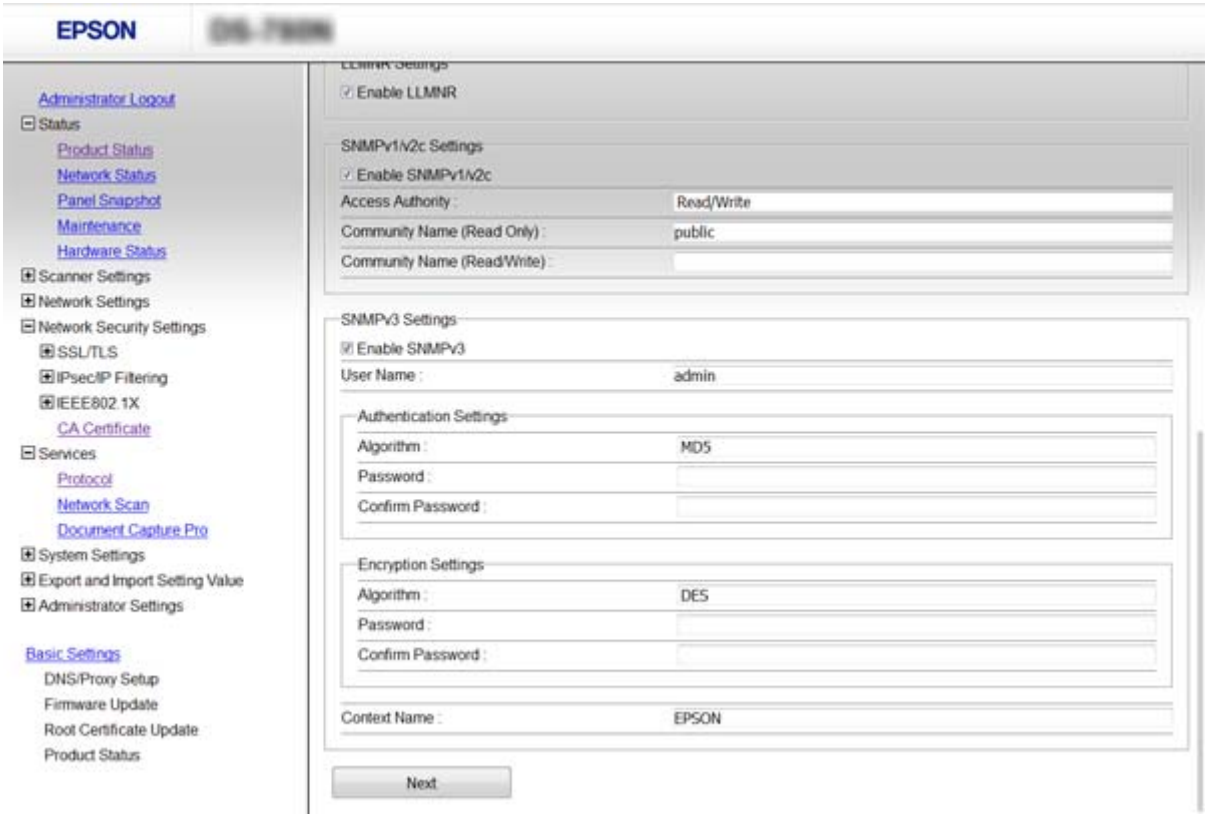
   Skener je aktualizovaný.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Položky nastavenia protokolu SNMPv3” na strane 84

Položky nastavenia protokolu SNMPv3



Položky	Nastavenia a vysvetlenie
Enable SNMPv3	Protokol SNMPv3 je povolený, keď je toto políčko začiarknuté.
User Name	Zadajte 1 až 32 1-bajtových znakov.
Authentication Settings	
Algorithm	Vyberte algoritmus overovania.
Password	Zadajte 8 až 32 znakov v kódovaní ASCII (0x20-0x7E).
Confirm Password	Zadajte heslo, ktoré ste nastavili na potvrdenie.
Encryption Settings	
Algorithm	Vyberte algoritmus šifrovania.
Password	Zadajte 8 až 32 znakov v kódovaní ASCII (0x20-0x7E).
Confirm Password	Zadajte heslo, ktoré ste nastavili na potvrdenie.
Context Name	Zadajte 1 až 32 1-bajtových znakov.

Súvisiace informácie

➡ „Konfigurácia protokolu SNMPv3” na strane 83

Pripojenie skenera k sieti IEEE802.1X

Konfigurácia siete IEEE802.1X

Ak skener podporuje sieť IEEE802.1X, môžete ho použiť v sieti s overovaním pripojenej k serveru RADIUS a k rozbočovaču ako overovateľovi.

1. Otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Zadajte hodnoty pre všetky položky.
3. Kliknite na položku **Next**.

   Zobrazí sa potvrdzujúca správa.
4. Kliknite na položku **OK**.

   Skener je aktualizovaný.

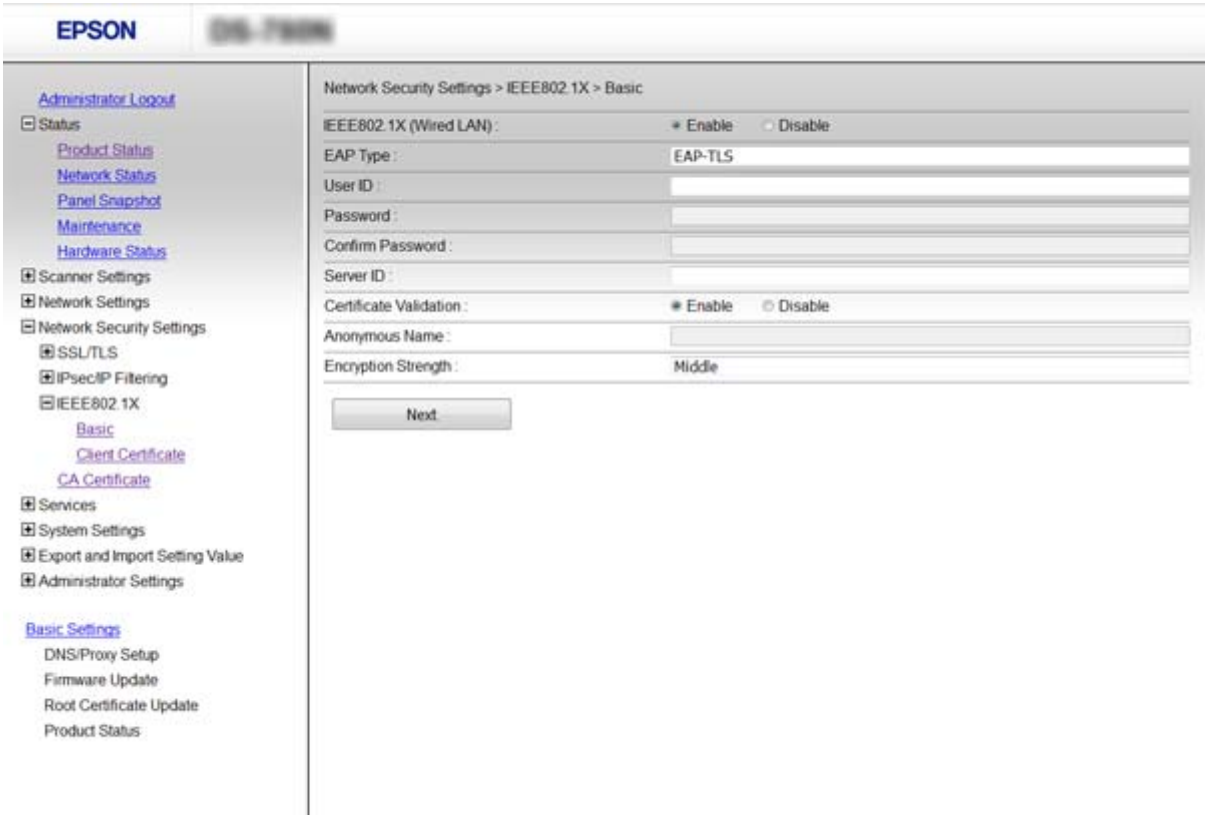
Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Položky nastavenia siete IEEE802.1X” na strane 85

➡ „Prístup k tlačiarni alebo ku skeneru nie je po konfigurácii funkcie IEEE802.1X možný” na strane 90

Položky nastavenia siete IEEE802.1X



Nastavenia rozšíreného zabezpečenia pre firmy

Položky	Nastavenia a vysvetlenie	
IEEE802.1X (Wired LAN)	Nastavenia stránky (**IEEE802.1X** > **Basic**) pre IEEE802.1X (káblová sieť LAN) môžete povoliť alebo zakázať.	
EAP Type	Vyberte spôsob overovania medzi skenerom a serverom RADIUS.	
	EAP-TLS	Treba získať a naimportovať certifikát s podpisom certifikačnej autority (CA).
	PEAP-TLS	
	PEAP/MSCHAPv2	Treba nakonfigurovať heslo.
User ID	Nastavte ID, ktoré sa použije na overenie servera RADIUS. Zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E).	
Password	Nakonfigurujte heslo pre overovanie skenera. Zadajte znaky od 1 do 128, 1-bitový ASCII (0x20 až 0x7E). Ak používate server Windows ako server RADIUS, môžete zadať až 127 znakov.	
Confirm Password	Zadajte nastavené heslo, aby sa vykonalo jeho potvrdenie.	
Server ID	Môžete nakonfigurovať ID servera, ktorým sa overuje v rámci určeného servera RADIUS. Overovací modul overí, či je alebo nie je v poli subject/subjectAltName zadané ID servera, ktoré je odoslané zo server RADIUS. Zadajte znaky od 0 do 128, 1-bitový ASCII (0x20 až 0x7E).	
Certificate Validation	Overenie certifikátu môžete nastaviť bez ohľadu na spôsob overovania. Certifikát importujte v položke **CA Certificate**.	
Anonymous Name	Ak vyberiete možnosť **PEAP-TLS** alebo **PEAP/MSCHAPv2** pre položku **Authentication Method**, vo fáze 1 overenia PEAP môžete namiesto ID používateľa nastaviť anonymné meno. Zadajte znaky od 0 do 128, 1-bitový ASCII (0x20 až 0x7E).	
Encryption Strength	Môžete vybrať jednu z nasledujúcich možností.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Súvisiace informácie

➡ „Konfigurácia siete IEEE802.1X” na strane 85

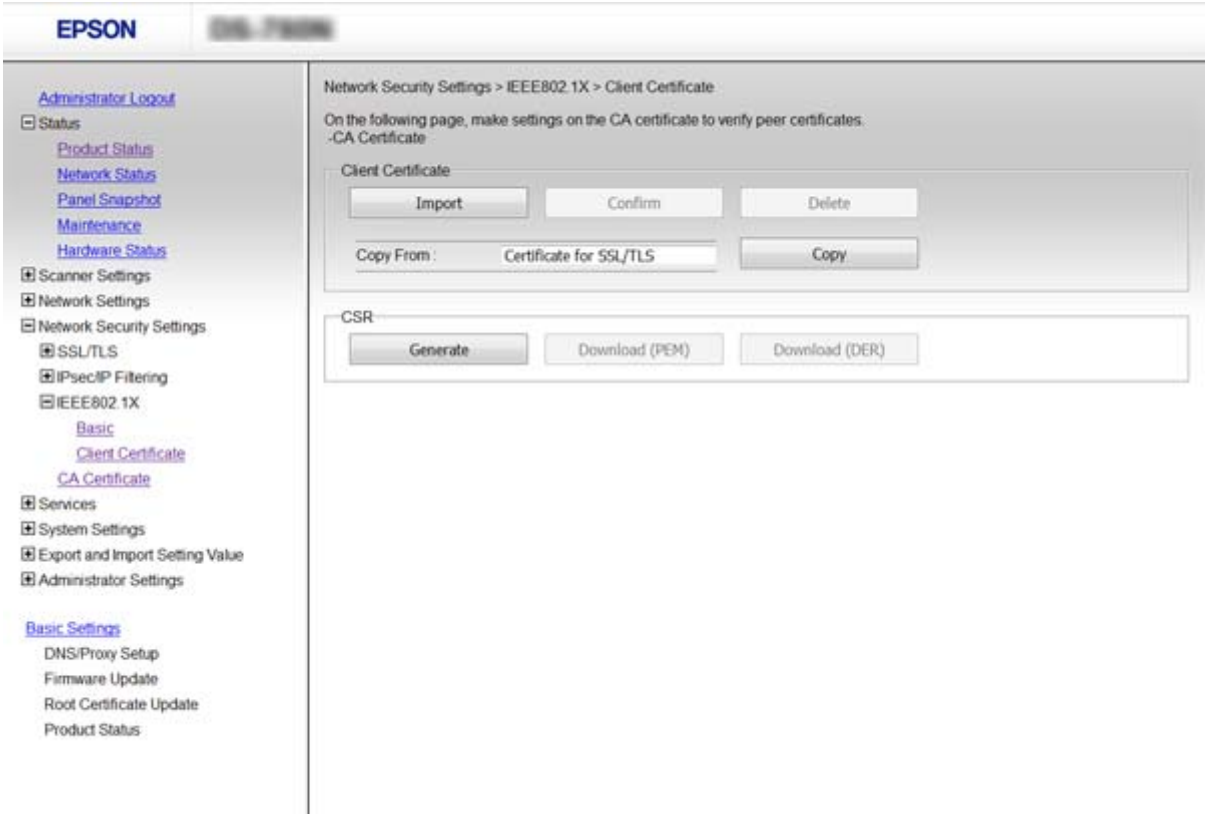
Konfigurácia certifikátu pre IEEE802.1X

Nakonfigurujte certifikát klienta pre IEEE802.1X. Ak chcete nakonfigurovať certifikačnú autoritu, prejdite do **CA Certificate**.

1. Otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. Certifikát zadajte v položke **Client Certificate**.

   Ak chcete, aby certifikačná autorita vydala certifikát, môžete ho skopírovať. Ak chcete certifikát skopírovať, vyberte ho z položky **Copy From** a potom kliknite na možnosť **Copy**.



Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Získanie a import certifikátu s podpisom certifikačnej autority (CA)” na strane 64

Riešenie problémov pre rozšírené zabezpečenie

Obnovenie nastavení zabezpečenia

Keď nastavíte prostredie s vysokým zabezpečením, ako je napríklad filtrovanie IPsec/IP alebo IEEE802.1X, možno sa nebude dať komunikovať so zariadeniami kvôli nesprávnym nastaveniam alebo problémom so zariadením alebo serverom. V takom prípade obnovte nastavenia zabezpečenia, aby bolo možné znova vytvoriť nastavenia, prípadne dočasne používať.

Vypnutie funkcie zabezpečenia pomocou ovládacieho panela

Pomocou ovládacieho panela skenera môžete vypnúť funkciu filtrovania IPsec/IP alebo IEEE802.1X.

1. Klepnite na položky **Nastav.** > **Nastavenia siete**.

2. Klepnite na položku **Zmeniť nastavenia**.
3. Klepnite na položky, ktoré chcete vypnúť.
   - ❏ **IPsec/IP Filtrovanie**
   - ❏ **IEEE802.1X**
4. Keď sa zobrazí hlásenie o dokončení, klepnite na položku **Pokračovať**.

Obnovenie funkcie zabezpečenia pomocou aplikácie Web Config

Pri zabezpečení IEEE802.1X nemusia byť zariadenia v sieti rozpoznané. V takom prípade vypnite funkciu pomocou ovládacieho panela skenera.

Pri funkcii filtrovania IPsec/IP môžete funkciu vypnúť, ak máte k zariadeniu prístup z počítača.

Vypnutie filtrovania IPsec/IP pomocou aplikácie Web Config

1. Otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Vyberte možnosť **Disable** pre **IPsec/IP Filtering** v časti **Default Policy**.
3. Kliknite na položku **Next** a potom zrušte začiarknutie položky **Enable this Group Policy** pre všetky zásady skupiny.
4. Kliknite na tlačidlo **OK**.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Problémy pri používaní funkcií bezpečnosti siete

Zabudnutý vopred zdieľaný kľúč

Nakonfigurujte kľúč znova pomocou aplikácie Web Config.

Ak chcete kľúč zmeniť, otvorte aplikáciu Web Config a vyberte položky **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** alebo **Group Policy**.

Keď zmeníte vopred zdieľaný kľúč, nakonfigurujte vopred zdieľaný kľúč pre počítače.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

Nie je možné komunikovať prostredníctvom komunikácie IPsec

Používate v nastaveniach počítača nepodporovaný algoritmus?

Skener podporuje nasledujúce algoritmy.

Bezpečnostné metódy	Algoritmy
Algoritmus šifrovania IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Algoritmus overovania IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmus výmeny kľúča IKE	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*
Algoritmus šifrovania ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Algoritmus overovania ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmus overovania AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* k dispozícii len pre IKEv2

Súvisiace informácie

➡ „Šifrovaná komunikácia pomocou filtrovania IPsec/IP” na strane 71

Náhle nie je možné komunikovať

Je adresa IP skenera neplatná alebo sa zmenila?

Vypnite službu IPsec pomocou ovládacieho panela skenera.

Ak je protokol DHCP zastaraný, reštartovalo sa alebo je zastaraná adresa IPv6, prípadne nebola zistená, IP adresa zaregistrovaná v aplikácii Web Config pre skener sa nemusí nájsť (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**)

Použite statickú adresu IP.

Je adresa IP počítača neplatná alebo sa zmenila?

Vypnite službu IPsec pomocou ovládacieho panela skenera.

Ak je protokol DHCP zastaraný, reštartovalo sa alebo je zastaraná adresa IPv6, prípadne nebola zistená, IP adresa zaregistrovaná v aplikácii Web Config pre skener sa nemusí nájsť (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**)

Použite statickú adresu IP.

Súvisiace informácie

➡ „Otvorenie aplikácie Web Config” na strane 23

➡ „Šifrovaná komunikácia pomocou filtrovania IPsec/IP” na strane 71

Po konfigurácii IPsec/IP Filtering sa nedá pripojiť

Nastavená hodnota môže byť nesprávna.

Položky IPsec/IP Filtering zablokujte z ovládacieho panela skenera. Pripojte skener a počítač a IPsec/IP Filtering znova nastavte.

Súvisiace informácie

➡ „Šifrovaná komunikácia pomocou filtrovania IPsec/IP” na strane 71

Prístup k tlačiarni alebo ku skeneru nie je po konfigurácii funkcie IEEE802.1X možný

Nastavenia sú možno nesprávne.

Z ovládacieho panela skenera vypnite funkciu IEEE802.1X. Pripojte skener k počítaču a potom znova nakonfigurujte funkciu IEEE802.1X.

Súvisiace informácie

➡ „Konfigurácia siete IEEE802.1X” na strane 85

Problémy s používaním digitálneho certifikátu

Nie je možné naimportovať certifikát s podpisom CA

Zhodujú sa údaje v certifikáte s podpisom CA a žiadosti CSR?

Ak v certifikáte s podpisom CA a žiadosti CSR nie sú rovnaké údaje, žiadosť CSR nie je možné naimportovať. Skontrolujte nasledujúce body:

❏ Pokúšate sa naimportovať certifikát do zariadenia, ktoré nemá rovnaké údaje?

Skontrolujte údaje v žiadosti CSR a potom naimportujte certifikát do zariadenia, ktoré má rovnaké údaje.

❏ Nahradili ste žiadosť CSR uloženú do skenera po odoslaní žiadosti CSR certifikačnej autorite?

Získajte certifikát s podpisom CA znova s použitím tejto žiadosti CSR.

Je certifikát s podpisom CA väčší ako 5 kB?

Certifikát väčší ako 5 kB nie je možné naimportovať.

Je heslo na import certifikátu správne?

Ak ste zabudli heslo, nemôžete certifikát naimportovať.

Súvisiace informácie

➡ „Import certifikátu s podpisom CA” na strane 66

Nie je možné aktualizovať certifikát s vlastným podpisom

Zadali ste položku Common Name?

Položku **Common Name** je potrebné zadať.

Zadali ste do položky Common Name nepodporované znaky? Napríklad japončina nie je podporovaná.

Zadajte 1 až 128 znakov vo formáte IPv4, IPv6, názvu hostiteľa alebo FQDN v kódovaní ASCII (0x20-0x7E).

Obsahuje položka Common Name čiarku alebo medzeru?

Ak obsahuje čiarku, položka **Common Name** sa na danom mieste rozdelí. Ak sa pred alebo za čiarkou nachádza iba medzera, vyskytne sa chyba.

Súvisiace informácie

➡ „Aktualizácia certifikátu s vlastným podpisom” na strane 68

Nie je možné vytvoriť žiadosť CSR

Zadali ste položku Common Name?

Položku **Common Name** je potrebné zadať.

Zadali ste do položiek Common Name, Organization, Organizational Unit, Locality, State/Province nepodporované znaky? Napríklad japončina nie je podporovaná.

Zadajte znaky vo formáte IPv4, IPv6, názvu hostiteľa alebo FQDN v kódovaní ASCII (0x20-0x7E).

Obsahuje položka Common Name čiarku alebo medzeru?

Ak obsahuje čiarku, položka **Common Name** sa na danom mieste rozdelí. Ak sa pred alebo za čiarkou nachádza iba medzera, vyskytne sa chyba.

Súvisiace informácie

➡ „Získanie certifikátu s podpisom CA” na strane 64

Zobrazuje sa upozornenie týkajúce sa digitálneho certifikátu

Správy	Príčina/riešenie
Enter a Server Certificate.	**Príčina:** Nevybrali ste súbor na import. **Riešenie:** Vyberte súbor a kliknite na položku **Import**.

Nastavenia rozšíreného zabezpečenia pre firmy

Správy	Príčina/riešenie
CA Certificate 1 is not entered.	**Príčina:** Certifikát CA 1 nie je zadaný a je zadaný iba certifikát CA 2. **Riešenie:** Naimportujte najskôr certifikát CA 1.
Invalid value below.	**Príčina:** Cesta k súboru alebo heslo obsahuje nepodporované znaky. **Riešenie:** Skontrolujte, či sú v položke správne zadané znaky.
Invalid date and time.	**Príčina:** Nie je nastavený dátum a čas skenera. **Riešenie:** Nastavte dátum a čas pomocou aplikácie Web Config alebo EpsonNet Config.
Invalid password.	**Príčina:** Heslo nastavené pre certifikát CA a zadané heslo sa nezhodujú. **Riešenie:** Zadajte správne heslo.
Invalid file.	**Príčina:** Neimportujete súbor certifikátu vo formáte X509. **Riešenie:** Skontrolujte, či ste vybrali správny certifikát odoslaný dôveryhodnou certifikačnou autoritou.
	Príčina: Naimportovaný súbor je priveľký. Maximálna veľkosť súboru je 5 kB. **Riešenie:** Ak ste vybrali správny súbor, certifikát môže byť poškodený alebo falošný.
	Príčina: Reťazec nachádzajúci sa v certifikáte je neplatný. **Riešenie:** Ďalšie informácie o certifikáte nájdete na webovej lokalite certifikačnej autority.
Cannot use the Server Certificates that include more than three CA certificates.	**Príčina:** Súbor certifikátu vo formáte PKCS#12 obsahuje viac ako 3 certifikáty CA. **Riešenie:** Naimportujte každý certifikát pomocou konverzie z formátu PKCS#12 do formátu PEM alebo naimportujte súbor certifikátu vo formáte PKCS#12, ktorý obsahuje max. 2 certifikáty.

Správy	Príčina/riešenie
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Príčina:** Certifikát je neaktuálny. **Riešenie:** ❏ Ak je certifikát neaktuálny, získajte a naimportujte nový certifikát. ❏ Ak certifikát nie je neaktuálny, skontrolujte, či je správne nastavený dátum a čas skenera.
Private key is required.	**Príčina:** Certifikát nie je spárovaný so súkromným kľúčom. **Riešenie:** ❏ Ak je certifikát vo formáte PEM/DER a bol získaný na základe žiadosti CSR pomocou počítača, zadajte súbor súkromného kľúča. ❏ Ak je certifikát vo formáte PKCS#12 a bol získaný na základe žiadosti CSR pomocou počítača, vytvorte súbor obsahujúci súkromný kľúč.
	Príčina: Znova ste naimportovali certifikát PEM/DER získaný na základe žiadosti CSR pomocou aplikácie Web Config. **Riešenie:** Ak je certifikát vo formáte PEM/DER a bol získaný na základe žiadosti CSR pomocou aplikácie Web Config, môžete ho naimportovať iba raz.
Setup failed.	**Príčina:** Nie je možné dokončiť konfiguráciu, pretože komunikácia medzi skenerom a počítačom zlyhala alebo súbor nie je možné prečítať kvôli chybám. **Riešenie:** Po kontrole zadaného súboru a komunikácie naimportujte súbor znova.

Súvisiace informácie

➡ „O digitálnom certifikáte” na strane 63

Omylom odstránený certifikát s podpisom CA

Existuje záložný súbor certifikátu?

Ak máte záložný súbor, naimportujte certifikát znova.

Ak ste certifikát získali prostredníctvom žiadosti CSR vytvorenej v aplikácii Web Config, odstránený certifikát nemôžete znova naimportovať. Vytvorte žiadosť CSR a získajte nový certifikát.

Súvisiace informácie

➡ „Odstránenie certifikátu s podpisom CA” na strane 67

➡ „Import certifikátu s podpisom CA” na strane 66