



DS-900WN DS-800WN

Príručka správcu

Potrebné nastavenia podľa vhodnosti na daný účel

Nastavenia siete

Potrebné nastavenia pre skenovanie

Základné nastavenia zabezpečenia

Rozšírené nastavenia zabezpečenia

Používanie funkcie Epson Open Platform

Autorské práva

Bez predchádzajúceho písomného súhlasu spoločnosti Seiko Epson Corporation nie je možné žiadnu časť tejto publikácie kopírovať, uchovávať v načítavacom systéme ani prenášať v akejkoľvek forme alebo akýmkoľvek prostriedkami, či už elektronickými, mechanickými, kopírovaním, zaznamenávaním alebo inak. V súvislosti s použitím tu obsiahnutých informácií sa neprijíma žiadna zodpovednosť za porušenie patentu. Žiadna zodpovednosť sa neprijíma ani za škody spôsobené použitím tu uvedených informácií. Informácie uvedené v tejto dokumentácii sú určené iba na použitie s týmto zariadením Epson. Spoločnosť Epson nie je zodpovedná za akékoľvek použitie týchto informácií pri aplikovaní na iných zariadeniach.

Spoločnosť Seiko Epson Corporation ani jej sesterské organizácie nepreberajú zodpovednosť voči kupcovi tohto produktu ani tretím stranám za poškodenia, straty, náklady alebo výdavky, ktoré kupcovi alebo tretím stranám vznikli pri nehode, nesprávnom používaní alebo zneužití tohto produktu alebo pri neoprávnených modifikáciách, opravách alebo zmenách tohto produktu, alebo (okrem USA) nedodržaní pokynov o prevádzke a údržbe od spoločnosti Seiko Epson Corporation.

Spoločnosť Seiko Epson Corporation ani jej sesterské organizácie nie sú zodpovedné za žiadne poškodenia alebo problémy vyplývajúce z použitia akéhokoľvek príslušenstva alebo akýchkoľvek spotrebných produktov, ako sú tie, ktoré sú určené ako originálne produkty Epson alebo schválené produkty Epson spoločnosťou Seiko Epson Corporation.

Spoločnosť Seiko Epson Corporation nenesie zodpovednosť za akékoľvek poškodenie zapríčinené elektromagnetickým rušením, ktoré sa vyskytuje pri používaní niektorých káblov rozhrania iných, ako sú tie, ktoré sú určené ako schválené produkty Epson spoločnosťou Seiko Epson Corporation.

© 2024 Seiko Epson Corporation

Obsah tejto príručky a technické údaje o tomto zariadení sa môžu zmeniť bez predchádzajúceho upozornenia.

Ochranné známky

- Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- Chrome, Chromebook and Android are trademarks of Google LLC.
- Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Všeobecné upozornenie: všetky ostatné ochranné známky sú majetkom príslušných vlastníkov a používajú sa len na identifikačné účely.

Obsah

Autorské práva

Ochranné známky

Úvod

Obsah tohto dokumentu.	7
Používanie tejto príručky.	7
Značky a symboly.	7
Popisy použité v tejto príručke.	7
Odkazy na operačné systémy.	7

Poznámky k heslu správcu

Poznámky k heslu správcu.	10
Prvotné heslo správcu.	10
Činnosti vyžadujúce heslo správcu.	10
Zmena hesla správcu.	10
Vynulovanie hesla správcu.	10

Potrebné nastavenia podľa vhodnosti na daný účel

Potrebné nastavenia podľa vhodnosti na daný účel.	12
---	----

Nastavenia siete

Pripojenie skenera k sieti.	15
Pred vytvorením sieťového pripojenia.	15
Pripojenie k sieti z ovládacieho panela.	17
Pridanie alebo výmena počítača alebo zariadení.	21
Pripojenie k skeneru, ktorý bol pripojený k sieti.	21
Priame pripojenie inteligentného zariadenia a skenera (Wi-Fi Direct).	23
Vynulovanie sieťového pripojenia.	25
Kontrola stavu sieťového pripojenia.	27
Kontrola stavu sieťového pripojenia z ovládacieho panela.	27
Parametre siete.	28
Parametre Wi-Fi.	28
Parametre siete Ethernet.	30
Funkcie siete a podpora IPv4/IPv6.	30
Bezpečnostný protokol.	31
Používanie portu pre skener.	31
Riešenie problémov.	32
Nedá sa pripojiť k sieti.	32

Softvér na nastavenie skenera

Aplikácia na konfiguráciu činností skenera (Web Config).	37
Ako spustiť funkciu Web Config v internetovom prehliadači.	37
Epson Device Admin.	38
Šablóna konfigurácie.	39

Potrebné nastavenia pre skenovanie

Registrácia e-mailového servera.	44
Kontrola pripojenia e-mailového servera.	45
Vytvorenie sieťového priečinka.	47
Sprístupnenie kontaktov.	54
Porovnanie konfigurácie kontaktov.	55
Registrácia cieľa do kontaktov pomocou aplikácie Web Config.	55
Registrovanie cieľov ako skupiny pomocou aplikácie Web Config.	57
Zálohovanie a import kontaktov.	58
Export a hromadná registrácia kontaktov pomocou nástroja.	59
Spolupráca medzi serverom LDAP a používateľmi.	61
Nastavenie funkcie AirPrint.	64
Problémy pri príprave skenovanie cez sieť.	64
Pomôcky k riešeniu problémov.	64
Nedá sa otvoriť aplikácia Web Config.	65

Prispôbenie zobrazenia ovládacieho panela

Registrácia položky Predv. hod..	68
Možnosti ponuky Predv. hod..	69
Úprava hlavnej obrazovky ovládacieho panela.	70
Zmena položky Usporiadanie na hlavnej obrazovke.	70
Pridať ikonu.	71
Odstrániť ikonu.	72
Presunúť ikonu.	73

Základné nastavenia zabezpečenia

Predstavenie funkcií zabezpečenia výrobku.	75
Nastavenia správcu.	75
Konfigurácia hesla správcu.	75

Používanie funkcie Nastavenie zámku pre ovládací panel.	77
Prihlásenie správcu z ovládacieho panela.	80
Obmedzenie dostupných funkcií (Riadenie prístupu).	81
Vytvorenie používateľského konta.	81
Povolenie funkcie Riadenie prístupu.	82
Prihlásenie do skenera, na ktorom je povolená funkcia Riadenie prístupu.	82
Zakázanie externého rozhrania.	83
Povolenie funkcie Overenie programu pri spustení.	83
Zakázanie sieťového skenovania v počítači.	84
Povolenie alebo zakázanie skenovania WSD.	84
Monitorovanie vzdialeného skenera.	85
Overenie údajov pre vzdialený skener.	85
Prijímanie emailových oznámení pri výskyte udalostí.	85
Na ovládanie napájania skenera použite funkciu Web Config.	86
Obnovenie predvolených nastavení.	86
Informácie o službe Epson Remote Services.	87
Riešenie problémov.	87
Zabudnuté heslo správcu.	87

Rozšírené nastavenia zabezpečenia

Nastavenia zabezpečenia a prevencia pred nebezpečenstvom.	89
Nastavenia funkcie zabezpečenia.	90
Riadenie pomocou protokolov.	90
Riadiace protokoly.	90
Protokoly, ktoré môžete zapnúť alebo vypnúť.	90
Položky nastavenia protokolu.	91
Používanie digitálneho certifikátu.	93
O digitálnom certifikáte.	93
Konfigurácia položky CA-podpísaný Certifikát.	93
Aktualizácia vlastného podpísaného certifikátu.	97
Konfigurácia položky Certifikát CA.	97
Komunikácia so skenerom cez protokol SSL/TLS.	98
Konfigurácia základných nastavení SSL/TLS.	98
Konfigurácia certifikátu servera pre skener.	99
Šifrovaná komunikácia pomocou filtrovania IPsec/IP.	99
Čo je IPsec/IP Filtrovanie.	99
Konfigurácia predvolených zásad.	100
Konfigurácia zásad skupiny.	103
Príklady konfigurácie funkcie IPsec/IP Filtrovanie.	109

Konfigurácia certifikátu pre funkciu filtrovania IPsec/IP.	110
Pripojenie skenera k sieti IEEE802.1X.	111
Konfigurácia siete IEEE 802.1X.	111
Konfigurácia certifikátu pre sieť IEEE 802.1X.	112
Riešenie problémov pre rozšírené zabezpečenie.	112
Obnovenie nastavení zabezpečenia.	112
Problémy pri používaní funkcií bezpečnosti siete.	113
Problémy s používaním digitálneho certifikátu.	115

Používanie funkcie Epson Open Platform

Prehľad platformy Epson Open Platform.	120
Konfigurácia režimu Epson Open Platform.	120
Overenie platformy Epson Open Platform.	120

Pripojenie overovacieho zariadenia

Pripojenie overovacieho zariadenia.	123
Kontrola činnosti pre overovacie zariadenie.	123
Potvrdenie rozpoznania overovacej karty.	123
Riešenie problémov s overovacím zariadením.	124
Overovacia karta sa nedá čítať.	124

Údržba

Čistenie vonkajšej časti skenera.	126
Čistenie vnútra skenera.	126
Výmena súpravy valca.	131
Kódy súprav valca.	136
Vynulovanie počtu skenovaní po výmene valcov.	136
Úsporný režim.	137
Preprava skenera.	137
Zálohovanie nastavení.	138
Export nastavení.	138
Import nastavení.	139
Obnoviť štandardné nastavenia.	139
Aktualizácia aplikácií a firmvéru.	140
Aktualizácia firmvéru skenera pomocou ovládacieho panela.	140
Aktualizácia firmvéru pomocou aplikácie Web Config.	141
Aktualizácia firmvéru bez pripojenia k internetu.	141

Úvod

Obsah tohto dokumentu.	7
Používanie tejto príručky.	7

Obsah tohto dokumentu

Tento dokument poskytuje nasledovné informácie pre správcov skenerov.

- Nastavenia siete
- Príprava funkcie skenovania
- Povolenie a riadenie nastavení zabezpečenia
- Vykonávanie každodennej údržby

Informácie o štandardných spôsoboch používania skenera nájdete v dokumente *Používateľská príručka*.

Používanie tejto príručky

Značky a symboly



Upozornenie:

Pokyny, ktoré je potrebné dôsledne dodržiavať, aby nedošlo k zraneniu.



Upozornenie:

Pokyny, ktoré je potrebné dodržiavať, aby nedošlo k poškodeniu zariadenia.

Poznámka:

Poskytuje doplnkové a referenčné informácie.

Súvisiace informácie

- ➔ Prepojenia na príslušné časti.

Popisy použité v tejto príručke

- Snímky obrazoviek aplikácií pochádzajú z Windows 10 alebo macOS High Sierra. Obsah zobrazený na obrazovkách sa mení v závislosti od modelu a situácie.
- Ilustrácie použité v tejto príručke slúžia len ako pomôcka. Aj keď sa môžu mierne líšiť od skutočného výrobku, spôsoby ovládania sú rovnaké.

Odkazy na operačné systémy

Windows

V tejto príručke označujú rôzne výrazy, ako napríklad „Windows 11“, „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Server 2022“, „Windows Server 2019“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“, „Windows Server 2008 R2“ a „Windows Server 2008“, nasledujúce operačné systémy. Výrazom „Windows“ sa označujú všetky verzie.

- Operačný systém Microsoft® Windows® 11
- 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 Server® 2022
- Operačný systém Microsoft® Windows Server® 2019
- 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

Mac OS

V tejto príručke sa výrazom „Mac OS“ označuje systém Mac OS X 10.9 alebo novší, ako aj macOS 11 alebo novší.

Poznámky k heslu správcu

Poznámky k heslu správcu.	10
Prvotné heslo správcu.	10
Činnosti vyžadujúce heslo správcu.	10
Zmena hesla správcu.	10
Vynulovanie hesla správcu.	10

Poznámky k heslu správcu

Zariadenie umožňuje nastaviť heslo správcu a zabrániť tak neoprávneným tretím stranám v prístupe alebo zmene nastavení zariadenia alebo sieťových nastavení uložených v zariadení keď je zariadenie pripojené k sieti.

Ak nastavíte heslo správcu, je potrebné heslo zadať pri zmene nastavení v konfiguračnom softvéri, ako je napríklad aplikácia Web Config.

Prvotné heslo správcu je nastavené na skeneri, ale môžete ho zmeniť na ľubovoľné heslo.

Prvotné heslo správcu

Prvotné heslo správcu sa líši v závislosti od štítku pripevneného na výrobku. Ak je na zadnej strane pripevnený štítok „PASSWORD“, zadajte 8-miestne číslo uvedené na štítku. Ak nie je pripevnený štítok „PASSWORD“, zadajte ako prvotné heslo správcu sériové číslo na štítku pripevnenom na zadnej strane výrobku.

Odporúčame zmeniť pôvodné heslo správcu z predvoleného nastavenia.

Poznámka:

Štandardne nie je nastavené žiadne používateľské meno.

Činnosti vyžadujúce heslo správcu

Ak sa počas nasledujúcich činností zobrazí výzva na zadanie hesla správcu, zadajte heslo správcu nastavené na výrobku.

- Pri prihlasovaní do rozšírených nastavení pre aplikáciu Web Config
- Pri používaní ponuky na ovládacom paneli, ktorá bola uzamknutá správcom
- Keď sa menia nastavenia zariadenia v aplikácii
- Keď sa aktualizuje firmvér pre zariadenie
- Pri zmene alebo vynulovaní hesla správcu

Zmena hesla správcu

Môžete ho zmeniť z ovládacieho panela výrobku alebo v aplikácii Web Config.

Keď meníte heslo, nové heslo musí mať 8 až 20 znakov a môže obsahovať iba jednobajtové alfanumerické znaky a symboly.

Vynulovanie hesla správcu

Heslo správcu môžete vynulovať na počiatočné nastavenie z ovládacieho panela výrobku alebo cez aplikáciu Web Config.

Ak ste zabudli heslo a nemôžete ho obnoviť na predvolené nastavenia, výrobok je potrebné opraviť. Obráťte sa na miestneho predajcu.

Potrebné nastavenia podľa vhodnosti na daný účel

Potrebné nastavenia podľa vhodnosti na daný účel. 12

Potrebné nastavenia podľa vhodnosti na daný účel

Pozrite nasledovné a urobte potrebné nastavenia podľa vhodnosti na daný účel.

Pripojenie skenera k sieti

Účel	Požadované nastavenia
Chcem pripojiť skener k sieti.	Nastavte skener na skenovanie cez sieť. „Pripojenie skenera k sieti“ na strane 15
Chcem pripojiť skener k novému počítaču.	Urobte nastavenia siete pre skener na novom počítači. „Pridanie alebo výmena počítača alebo zariadení“ na strane 21

Nastavenia pre skenovanie

Účel	Požadované nastavenia
Chcem posilať naskenované obrázky e-mailom. (Skenovať do e-mailu)	1. Nastavte e-mailový server, ktorý chcete pripojiť. „Registrácia e-mailového servera“ na strane 44 2. Zaregistrujte e-mailovú adresu príjemcu v položke Kontakty (nepovinné). Po registrácii e-mailovej adresy ju už nebude potrebné zadávať pri každom odosielaní, stačí ju vybrať spomedzi vašich kontaktov. „Sprístupnenie kontaktov“ na strane 54
Chcem ukladať naskenované obrázky do priečinka v sieti. (Skenovať do sieťového priečinka/FTP)	1. Vytvorte priečinku v sieti, kam chcete ukladať naskenované obrázky. „Vytvorenie sieťového priečinka“ na strane 47 2. Zaregistrujte umiestnenie priečinka do položky Kontakty (nepovinné). Po registrácii umiestnenia priečinka ho už nebude potrebné zadávať pri každom odosielaní, stačí ho vybrať spomedzi vašich kontaktov. „Sprístupnenie kontaktov“ na strane 54
Chcem ukladať naskenované obrázky do cloudovej služby. (Skenovať do cloudu)	Nastavte aplikáciu Epson Connect. Podrobnosti o nastavení nájdete na webovom portáli Epson Connect. Pri nastavovaní je potrebné používateľské konto pre online cloudovú službu, na ktorú chcete pripojiť. https://www.epsonconnect.com/ http://www.epsonconnect.eu (len Európa)

Prispôsobenie zobrazenia ovládacieho panela

Účel	Požadované nastavenia
Chcem zmeniť položky zobrazované na ovládacom paneli skenera.	Nastavte položku Predv. hod. alebo Upraviť domovskú obrazovku . Môžete zaregistrovať svoje obľúbené nastavenia skenovania do ovládacieho panela a upraviť zobrazované položky. „Prispôsobenie zobrazenia ovládacieho panela“ na strane 67

Nastavenie základných funkcií zabezpečenia

Účel	Požadované nastavenia
Chcem zabrániť každému okrem správcov meniť nastavenia skenera.	Nastavte heslo správcu pre skener. „Nastavenia správcu“ na strane 75
Chcem zakázať používať skenery s USB pripojeniami.	Zakážete externé rozhranie. „Zakázanie externého rozhrania“ na strane 83

Nastavenie rozšírených funkcií zabezpečenia

Účel	Požadované nastavenia
Chcem ovládať, ktoré protokoly sa používajú.	Povoľte alebo zakážete protokoly. „Riadenie pomocou protokolov“ na strane 90
Chcem šifrovať dráhu komunikácie.	1. Nastavte svoj digitálny certifikát. „Používanie digitálneho certifikátu“ na strane 93 2. Nastavte komunikáciu SSL/TLS. „Komunikácia so skenerom cez protokol SSL/TLS“ na strane 98
Chcem používať šifrovanú komunikáciu (IPsec). Chcem mať možnosť používať softvér len z konkrétneho počítača (filtrovanie IP).	Nastavte zásady filtrovania prenosu údajov. „Šifrovaná komunikácia pomocou filtrovania IPsec/IP“ na strane 99
Chcem používať skener v sieti IEEE802.1X.	Nastavte režim IEEE802.1X pre skener. „Pripojenie skenera k sieti IEEE802.1X“ na strane 111

Synchronizácia skenera so systémom overovania

Získajte produktový kľúč zo špecializovanej webovej lokality a aktivujte stránku Epson Open Platform na svojom skeneri.

[„Používanie funkcie Epson Open Platform“ na strane 119](#)

Používanie možnosti overovania (Epson Print Admin/Epson Print Admin Serverless)

Na používanie tejto možnosti potrebujete licenčný kľúč.

Ďalšie informácie vám poskytne predajca.

Poznámka:

Keď je systém synchronizovaný s aplikáciou Epson Open Platform, nemôžete aplikáciu Epson Print Admin Serverless používať.

Nastavenia siete

Pripojenie skenera k sieti.	15
Pridanie alebo výmena počítača alebo zariadení.	21
Kontrola stavu sieťového pripojenia.	27
Parametre siete.	28
Riešenie problémov.	32

Pripojenie skenera k sieti

V tejto časti je vysvetlené, ako pripojiť skener k sieti pomocou ovládacieho panela skenera.

Poznámka:

Ak sa skener a počítač nachádzajú v rovnakom segmente, môžete sa pripojiť aj pomocou inštalačného programu.

Ak chcete spustiť inštalačný program, prejdite na nasledujúcu webovú stránku a potom zadajte názov výrobku. Prejdite na položku **Nastavenie** a potom spustíte inštaláciu.

<https://epson.sn>

Môžete zobrazit prevádzkové pokyny v možnosti Príručky k webovým filmom. Prejdite na túto adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Pred vytvorením sieťového pripojenia

Ak chcete pripojiť k sieti, skontrolujte spôsob pripojenia a informácie o nastavení pripojenia.

Získanie informácií o nastavení pripojenia

Prpravte si na pripojenie nasledujúce údaje. Skontrolujte nasledujúce údaje.

Rozdelenie	Položky	Poznámka
Spôsob pripojenia zariadenia	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Rozhodnite o spôsobe pripojenia skenera k sieti. Pri káblvej sieti LAN pripojte k prepínaču LAN. Pri sieti Wi-Fi pripojte k sieti (SSID) prístupového bodu.
Informácie o pripojení k sieti LAN	<input type="checkbox"/> IP adresa <input type="checkbox"/> Maska podsiete <input type="checkbox"/> Predvolená brána	Rozhodnite o IP adrese priradenej skeneru. Keď priradíte statickú IP adresu, sú potrebné všetky hodnoty. Keď priradíte IP adresu dynamicky pomocou funkcie DHCP, tieto informácie nie sú potrebné, pretože sú nastavené automaticky.
Informácie o pripojení k sieti Wi-Fi	<input type="checkbox"/> SSID <input type="checkbox"/> Heslo	Je tu SSID (názov siete) a heslo prístupového bodu, ku ktorému sa skener pripája. Ak bolo nastavené filtrovanie adries MAC, zaregistrujte adresu MAC skenera a tak zaregistrujte skener. Informácie o podporovaných normách nájdete ďalej. „Parametre siete“ na strane 28
Informácie o serveri DNS	<input type="checkbox"/> IP adresa primárneho servera DNS <input type="checkbox"/> IP adresa sekundárneho servera DNS	Tie sú potrebné pri určovaní serverov DNS. Sekundárny server DNS je nastavený, keď má systém druhú konfiguráciu a je k dispozícii sekundárny server DNS. Ak ste v malej organizácii a nenastavujete server DNS, nastavte IP adresu smerovača.

Rozdelenie	Položky	Poznámka
Informácie o serveri proxy	<input type="checkbox"/> Názov servera proxy	Nastavte to, keď vaše sieťové prostredie používa server proxy na prístup k internetu z intranetu a používate funkciu, pri ktorej má skener priamy prístup k internetu. Pre nasledujúce funkcie sa skener priamo pripája k internetu. <input type="checkbox"/> Služby Epson Connect <input type="checkbox"/> Cloudové služby iných spoločností <input type="checkbox"/> Aktualizácia firmvéru <input type="checkbox"/> Odosielanie naskenovaných obrazov do SharePoint (WebDAV)
Informácie o čísle portu	<input type="checkbox"/> Číslo portu na uvoľnenie	Skontrolujte číslo portu používaného skenerom a počítačom, potom uvoľnite port blokovaný firewallom, ak je to potrebné. Informácie o čísle portu používaného skenerom nájdete ďalej. „Používanie portu pre skener“ na strane 31

Priradenie IP adresy

Toto sú typy priradenia IP adresy.

Statická IP adresa:

Ručné priradenie vopred určenej IP adresy skeneru (hostiteľovi).

Údaje na pripojenie k sieti (maska podsiete, predvolená brána, server DNS atď) je potrebné nastaviť ručne.

IP adresa sa nezmení ani po vypnutí zariadenia, takže je to užitočné v prípade, že chcete spravovať zariadenia s prostredím, kde sa nemôže meniť IP adresa, prípadne ak chcete spravovať zariadenia pomocou IP adresy. Odporúčame nastavenia pre skener, server atď, ku ktorým má prístup viac počítačov. Aj pri používaní funkcií zabezpečenia, ako sú napríklad Filtrovanie IPsec/IP, priradte pevnú IP adresu, takže sa IP adresa nemení.

Automatické priradenie pomocou funkcie DHCP (dynamická IP adresa):

Automatické priradenie IP adresy skeneru (hostiteľovi) pomocou funkcie DHCP servera DHCP alebo smerovača.

Informácie na pripojenie k sieti (maska podsiete, predvolená brána, server DNS atď.) sú nastavené automaticky, takže môžete zariadenie ľahko pripojiť k sieti.

Ak sa zariadenie alebo smerovač vypnú (prípadne ak to závisí od nastavení servera DHCP), IP adresa sa môže pri opätovnom pripojení zmeniť.

Odporúčame spravovanie zariadení inak než IP adresou a komunikáciu s protokolmi, ktoré sledujú IP adresu.

Poznámka:

Keď použijete funkciu rezervovania IP adresy na serveri DHCP, môžete kedykoľvek priradiť rovnakú IP adresu zariadeniam.

Server DNS a server Proxy

Server DNS má názov hostiteľa, doménový názov alebo e-mailovú adresu atď. v súvislosti s údajmi o IP adrese.

Komunikácia nie je možná, ak je druhá strana popísaná názvom hostiteľa, doménovým názvom atď., keď skener alebo počítač vykonávajú IP komunikáciu.

Posielajú sa dopyty na server DNS k daným údajom a získava sa IP adresa druhej strany. Tento proces sa nazýva rozlišovanie názvu.

Zariadenia (napríklad počítače a skenery) teda dokážu komunikovať pomocou IP adresy.

Rozlišovanie názvu je potrebné pre skener komunikujúci pomocou funkcie e-mailu alebo funkcie internetového pripojenia.

Keď používate tieto funkcie, urobte nastavenia servera DNS.

Keď priradíte IP adresu skenera pomocou funkcie DHCP na serveri DHCP alebo smerovači, nastaví sa automaticky.

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

Keď pripájate k internetu cez server proxy, nakonfigurujte na skeneri server proxy.

Pripojenie k sieti z ovládacieho panela

Pripojte skener k sieti pomocou ovládacieho panela skenera.

Priradenie IP adresy

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

V tejto časti je vysvetlený postup nastavenia statickej IP adresy.

1. Zapnite skener.
2. Vyberte položku **Nastav.** na hlavnej obrazovke na ovládacom paneli skenera.
3. Vyberte položky **Nastavenie siete > Rozšírené > TCP/IP**.
4. Vyberte možnosť **Ručne** pre **Získať IP adresu**.

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 5 až 6 tiež nastavujú automaticky, takže prejdite na krok 7.

5. Zadajte IP adresu.

Presunie dopredu alebo dozadu o segment oddelený bodkou, ak vyberiete ◀ a ▶.

Overte hodnotu zobrazenú na predchádzajúcej obrazovke.

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

Overte hodnotu zobrazenú na predchádzajúcej obrazovke.



Upozornenie:

*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.*

7. Zadajte IP adresu primárneho servera DNS.

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 9.

8. Zadajte IP adresu sekundárneho servera DNS.
Overte hodnotu zobrazenú na predchádzajúcej obrazovke.
9. Klepnite na tlačidlo **Spustiť nastavenie**.

Nastavenie servera Proxy


Nastavte server proxy, ak sú obidve nasledujúce tvrdenia pravdivé.

- Server proxy pre internetové pripojenie je zabudovaný.
- Keď sa používa funkcia, pri ktorej sa skener priamo pripája k internetu, napríklad služba Epson Connect alebo cloudové služby inej spoločnosti.

1. Na hlavnej obrazovke vyberte položku **Nastav.**
Keď robíte nastavenia po nastavení IP adresy, zobrazí sa obrazovka **Rozšírené**. Prejdite na 3. krok.
2. Vyberte položky **Nastavenie siete > Rozšírené**.
3. Vyberte položku **Proxy server**.
4. Vyberte možnosť **Použiť** pre **Nastavenia proxy servera**.
5. Zadajte adresu servera proxy vo formáte IPv4 alebo FQDN.
Overte hodnotu zobrazenú na predchádzajúcej obrazovke.
6. Zadajte číslo portu pre server proxy.
Overte hodnotu zobrazenú na predchádzajúcej obrazovke.
7. Klepnite na tlačidlo **Spustiť nastavenie**.

Pripojenie k sieti Ethernet

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

1. Prepojte skener a rozbočovač (prepínač LAN) káblom siete LAN.
2. Na hlavnej obrazovke vyberte položku .
3. Vyberte položku **Smerovač**.
4. Uistite sa, či sú nastavenia Pripojenie a IP adresa správne.
5. Klepnite na tlačidlo **Zatvoriť**.

Pripojenie k bezdrôtovej sieti LAN (Wi-Fi)

Skener môžete pripojiť k bezdrôtovej sieti LAN (Wi-Fi) viacerými spôsobmi. Vyberte spôsob pripojenia, ktorý vyhovuje prostrediu a podmienkam, ktoré používate.

Ak poznáte údaje bezdrôtového smerovača, ako je napríklad SSID a heslo, môžete urobiť nastavenia ručne.

Ak bezdrôtový smerovač podporuje funkciu WPS, môžete urobiť nastavenia pomocou tlačidla Push Setup.

Po pripojení skenera k sieti pripojíte k skeneru zo zariadenia, ktoré chcete použiť (počítač, inteligentné zariadenie, tablet atď.)

Poznámka pri používaní pripojenia Wi-Fi 5 GHz

Tento produkt bežne používa W52 (36. kanál) ako kanál pri priamom pripojení Wi-Fi Direct (Jednoduchý prístupový bod). Keďže kanál pre pripojenie k bezdrôtovej sieti LAN (Wi-Fi) sa vyberá automaticky, použitý kanál sa môže líšiť, ak sa používa súčasne s pripojením Wi-Fi Direct. Ak sa kanály líšia, dátová komunikácia so skenerom môže byť pomalá. Ak to pri používaní neprekáža, pripojte sa k SSID v pásme 2,4 GHz. Vo frekvenčnom pásme 2,4 GHz sa použité kanály budú zhodovať.

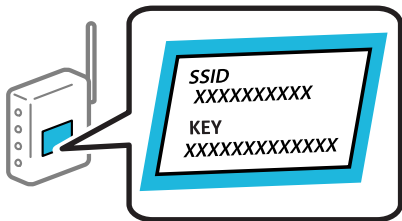
Pri nastavení bezdrôtovej siete LAN na 5 GHz odporúčame vypnúť funkciu priameho pripojenia Wi-Fi Direct.


Vytvorenie nastavení siete Wi-Fi zadaním SSID a hesla

Z ovládacieho panela skenera môžete zadať údaje potrebné na pripojenie k bezdrôtovému smerovaču a nastaviť tak sieť Wi-Fi. Ak chcete nastaviť týmto spôsobom, je potrebné vedieť SSID a heslo pre bezdrôtový smerovač.

Poznámka:

Ak používate bezdrôtový smerovač s jeho predvolenými nastaveniami, SSID a heslo sú na štítku. Ak nepoznáte SSID a heslo, poskytne vám ich osoba, ktorá nainštalovala bezdrôtový smerovač, prípadne si pozrite dokumentáciu k prístupovému bodu.



1. Na hlavnej obrazovke klepnite na .
2. Vyberte položku **Smerovač**.
3. Klepnite na položku **Spustiť nastavenie**.

Ak je už sieťové pripojenie nastavené, zobrazia sa podrobnosti o pripojení. Klepnutím na položku **Zmeň. na prip. Wi-Fi** alebo **Zmeniť nastavenia** zmeníte nastavenia.

4. Vyberte položku **Sprievodca nastavením Wi-Fi**.
5. Podľa pokynov na obrazovke vyberte SSID, zadajte heslo pre bezdrôtový smerovač a spustíte inštaláciu.

Ak chcete po dokončení inštalácie skontrolovať stav sieťového pripojenia skenera, podrobnosti nájdete cez odkaz na súvisiace informácie.

Poznámka:

- Ak nepoznáte SSID, skontrolujte, či nie je napísané na štítku na bezdrôtovom smerovači. Ak používate bezdrôtový smerovač s jeho predvolenými nastaveniami, použite SSID napísané na štítku. Ak nemôžete nájsť žiadne údaje, pozrite dokumentáciu, ktorá bola priložená k bezdrôtovému smerovaču.
- V hesle sa rozlišujú malé/veľké písmená.
- Ak nepoznáte heslo, skontrolujte, či nie je napísané na štítku na bezdrôtovom smerovači. Na štítku môže byť heslo nazvané „Network Key“, „Wireless Password“ atď. Ak používate bezdrôtový smerovač s jeho predvolenými nastaveniami, použite heslo napísané na štítku.
- Ak nevidíte SSID, ku ktorému sa chcete pripojiť, použite softvér alebo aplikáciu na nastavenie Wi-Fi z počítača alebo inteligentného zariadenia, napríklad smartfónu alebo tabletu. Ak chcete získať ďalšie informácie, zadajte do prehliadača adresu „<https://epson.sn>“, aby ste sa dostali na webovú stránku, zadajte názov svojho výrobku a prejdite na **Nastavenie**.

Súvisiace informácie

➔ „Kontrola stavu sieťového pripojenia“ na strane 27

Vytvorenie nastavení siete Wi-Fi tlačidlom Push Button Setup (WPS)


Sieť Wi-Fi môžete nastaviť automaticky stlačením tlačidla na bezdrôtovom smerovači. Ak sú splnené nasledujúce podmienky, môžete nastaviť týmto spôsobom.

- Bezdrôtový smerovač je kompatibilný s funkciou WPS (Wi-Fi Protected Setup).
- Aktuálne pripojenie Wi-Fi bolo nadviazané stlačením tlačidla na bezdrôtovom smerovači.

Poznámka:

Ak nevíete tlačidlo nájsť, prípadne nastavujete pomocou softvéru, pozrite si dokumentáciu dodanú s bezdrôtovým smerovačom.



1. Na hlavnej obrazovke klepnite na .
2. Vyberte položku **Smerovač**.
3. Klepnite na tlačidlo **Spustiť nastavenie**.

Ak je už sieťové pripojenie nastavené, zobrazia sa podrobnosti o pripojení. Klepnutím na položku **Zmeň. na prip. Wi-Fi** alebo **Zmeniť nastavenia** zmeníte nastavenia.

4. Vyberte položku **Nastavenie tlačidla (WPS)**.
5. Postupujte podľa pokynov na obrazovke.

Ak chcete po dokončení inštalácie skontrolovať stav sieťového pripojenia skenera, podrobnosti nájdete cez odkaz na súvisiace informácie.

Poznámka:

Ak sa nepodarí pripojiť, reštartujte bezdrôtový smerovač, premiestnite ho bližšie ku skeneru a skúste to znova.


Súvisiace informácie

➔ „Kontrola stavu sieťového pripojenia“ na strane 27

Vytvorenie nastavení siete Wi-Fi kódom PIN (WPS)

Môžete automaticky pripojiť k bezdrôtovému smerovaču pomocou kódu PIN. Týmto spôsobom nastavte, ak bezdrôtový smerovač podporuje funkciu WPS (Wi-Fi Protected Setup). Pomocou počítača zadajte kód PIN do bezdrôtového smerovača.



1. Na hlavnej obrazovke klepnite na .
2. Vyberte položku **Smerovač**.
3. Klepnite na tlačidlo **Spustiť nastavenie**.

Ak je už sieťové pripojenie nastavené, zobrazia sa podrobnosti o pripojení. Klepnutím na položku **Zmeň. na prip. Wi-Fi**, alebo **Zmeniť nastavenia** zmeníte nastavenia.

4. Vyberte položky **Iné > Nastavenie kódu PIN (WPS)**
5. Postupujte podľa pokynov na obrazovke.

Ak chcete po dokončení inštalácie skontrolovať stav sieťového pripojenia skenera, podrobnosti nájdete cez odkaz na súvisiace informácie.

Poznámka:

Pozrite si dokumentáciu k bezdrôtovému smerovaču, kde nájdete ďalšie podrobnosti o zadávaní kódu PIN.

Súvisiace informácie

➔ „Kontrola stavu sieťového pripojenia” na strane 27

Pridanie alebo výmena počítača alebo zariadení

Pripojenie k skeneru, ktorý bol pripojený k sieti

Keď už bol skener pripojený k sieti, môžete pripojiť k skeneru počítač alebo inteligentné zariadenie cez sieť.

Používanie sieťového skenera z druhého počítača

Na pripojenie skenera k počítaču odporúčame použiť inštaláčny program.

Ak chcete spustiť inštaláčny program, prejdite na nasledujúcu webovú stránku a potom zadajte názov výrobku. Prejdite na položku **Nastavenie** a potom spustíte inštaláciu.

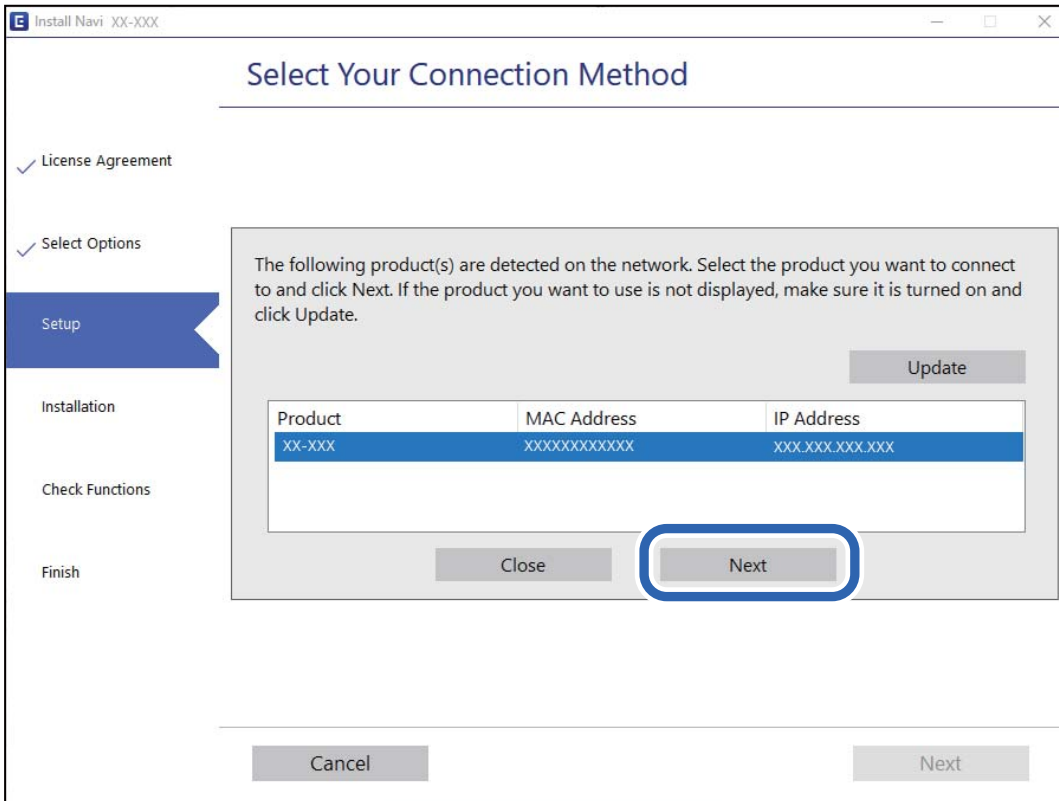
<https://epson.sn>

Môžete zobraziť prevádzkové pokyny v možnosti Príručky k webovým filmom. Prejdite na túto adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Výber skenera

Postupujte podľa pokynov na obrazovke, kým sa nezobrazí nasledujúca obrazovka. Vyberte názov skenera, ku ktorému chcete pripojiť, a potom kliknite na tlačidlo **Ďalej**.



Postupujte podľa pokynov na obrazovke.

Používanie sieťového skenera z inteligentného zariadenia

Inteligentné zariadenie môžete pripojiť k skeneru jedným z nasledujúcich spôsobov.

Pripojenie cez bezdrôtový smerovač

Pripojte inteligentné zariadenie k rovnakej sieti Wi-Fi (SSID) ako skener.

Ďalšie podrobnosti nájdete v nasledujúcej časti.

[„Vytvorenie nastavení na pripojenie k inteligentnému zariadeniu” na strane 26](#)

Pripojenie v režime Wi-Fi Direct

Pripojte inteligentné zariadenie k skeneru priamo bez bezdrôtového smerovača.

Ďalšie podrobnosti nájdete v nasledujúcej časti.

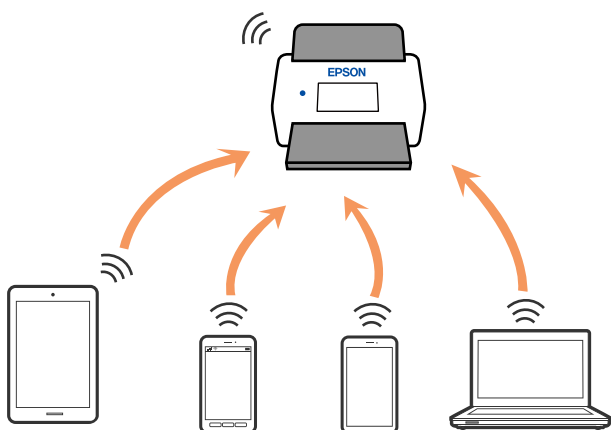
[„Priame pripojenie inteligentného zariadenia a skenera \(Wi-Fi Direct\)” na strane 23](#)

Priame pripojenie inteligentného zariadenia a skenera (Wi-Fi Direct)

Režim Wi-Fi Direct (Jednoduchý prístupový bod) umožňuje pripojiť inteligentné zariadenie priamo k skeneru bez bezdrôtového smerovača a tlačíť z inteligentného zariadenia.

Čo je Wi-Fi Direct


Tento spôsob pripojenia použijete vtedy, keď doma ani v kancelárii nepoužívate sieť Wi-Fi, prípadne ak chcete prepojiť skener a počítač alebo inteligentné zariadenie priamo. V tomto režime funguje skener ako bezdrôtový smerovač a k skeneru môžete pripojiť zariadenia bez toho, aby ste použili bežný bezdrôtový smerovač. Zariadenia, ktoré sú pripojené priamo ku skeneru, však nemôžu medzi sebou komunikovať prostredníctvom skenera.



Skener možno súčasne pripojiť cez pripojenie Wi-Fi alebo Ethernet a Wi-Fi Direct (Jednoduchý prístupový bod). Ak však spustíte pripojenie k sieti cez Wi-Fi Direct (Jednoduchý prístupový bod), keď bude skener pripojený cez sieť Wi-Fi, Wi-Fi sa dočasne odpojí.

Pripojenie k inteligentnému zariadeniu v režime Wi-Fi Direct

Tento spôsob umožňuje pripojiť skener priamo k inteligentným zariadeniam bez bezdrôtového smerovača.

1. Na hlavnej obrazovke vyberte položku .
2. Vyberte položku **Wi-Fi Direct**.
3. Vyberte položku **Spustiť nastavenie**.
4. Spustíte na inteligentnom zariadení aplikáciu Epson Smart Panel.
5. Podľa pokynov zobrazených v aplikácii Epson Smart Panel pripojte k skeneru.
Keď je inteligentné zariadenie pripojené k skeneru, prejdite na ďalší krok.
6. Na ovládacom paneli skenera vyberte položku **Dokonč..**

Odpojenie v režime Wi-Fi Direct (Jednoduchý prístupový bod)

K dispozícii sú dva spôsoby zakázania pripojenia v režime Wi-Fi Direct (Jednoduchý prístupový bod): môžete zakázať všetky pripojenia pomocou ovládacieho panela skenera, prípadne zakázať jednotlivé pripojenia z počítača alebo inteligentného zariadenia.

Keď chcete zakázať všetky pripojenia, vyberte ponuku  > **Wi-Fi Direct** > **Spustiť nastavenie** > **Zmeniť** > **Zakázať Wi-Fi Direct**.

Upozornenie:

Keď je pripojenie v režime Wi-Fi Direct (Jednoduchý prístupový bod) vypnuté, všetky počítače a inteligentné zariadenia pripojené ku skeneru v režime Wi-Fi Direct (Jednoduchý prístupový bod) sú odpojené.


Poznámka:

Ak chcete odpojiť konkrétne zariadenie, odpojte zo zariadenia, nie zo skenera. Pomocou jedného z nasledujúcich spôsobov odpojenie pripojenie v režime Wi-Fi Direct (Jednoduchý prístupový bod) zo zariadenia.

- Odpojte pripojenie Wi-Fi k sieti skenera (SSID).*
- Pripojte k inej sieti (SSID).*

Zmena nastavení režimu Wi-Fi Direct (Jednoduchý prístupový bod), napríklad SSID

Keď je režim Wi-Fi Direct (Jednoduchý prístupový bod) povolený, môžete nastavenia zmeniť cez ponuku

 > **Wi-Fi Direct** > **Spustiť nastavenie** > **Zmeniť**. Potom sa zobrazia nasledujúce položky ponuky.

Zmeniť názov siete

Zmeňte názov siete pre režim pripojenia Wi-Fi Direct (Jednoduchý prístupový bod) (SSID) používanej na pripojenie ku skeneru na svoj povinný názov. Názov siete (SSID) môžete nastaviť v znakoch ASCII, ktoré sa zobrazujú na softvérovej klávesnici na ovládacom paneli. Môžete zadať najviac 22 znakov.

Keď zmeníte názov siete (SSID), všetky pripojené zariadenia sa odpoja. Keď chcete zariadenie znova pripojiť, použite nový názov siete (SSID).

Zmena hesla

Zmeňte heslo režimu Wi-Fi Direct (Jednoduchý prístupový bod) na pripojenie ku skeneru na svoju predvolenú hodnotu. Heslo môžete nastaviť v znakoch ASCII, ktoré sú zobrazené na softvérovej klávesnici na ovládacom paneli. Môžete zadať 8 až 22 znakov.

Keď zmeníte heslo, všetky pripojené zariadenia sa odpoja. Ak chcete zariadenie znova pripojiť, použite nové heslo.

Zmeniť Frequency Range

Zmeňte frekvenčný rozsah režimu Wi-Fi Direct používaného na pripojenie ku skeneru. Môžete vybrať pásmo 2,4 GHz alebo 5 GHz.

Keď zmeníte frekvenčný rozsah, všetky pripojené zariadenia sa odpoja. Znova pripojte zariadenie.

Majte na pamäti, že nie je možné znova pripojiť zo zariadení, ktoré nepodporujú frekvenčný rozsah 5 GHz, keď ho zmeníte na 5 GHz.

V závislosti od regiónu sa nemusí toto nastavenie zobrazovať.

Zakázať Wi-Fi Direct

Zakážte nastavenia režimu Wi-Fi Direct (Jednoduchý prístupový bod) pre skener. Keď režim zakážete, všetky zariadenia pripojené ku skeneru cez pripojenie Wi-Fi Direct (Jednoduchý prístupový bod) sa odpoja.

Obnoviť štand. nastavenia

Môžete obnoviť predvolené hodnoty všetkých nastavení režimu Wi-Fi Direct (Jednoduchý prístupový bod).

Údaje o pripojení v režime Wi-Fi Direct (Jednoduchý prístupový bod) k inteligentnému zariadeniu uložené v skeneri sa odstránia.

Poznámka:

Teraz môžete na karte **Sieť > Wi-Fi Direct** v časti **Web Config** nastaviť nasledovné nastavenia.

- Povolenie či zakázanie režimu Wi-Fi Direct (Jednoduchý prístupový bod)
- Zmena názvu siete (SSID)
- Zmena hesla
- Zmena frekvenčného rozsahu
V závislosti od regiónu sa nemusí toto nastavenie zobrazovať.
- Obnovenie nastavení režimu Wi-Fi Direct (Jednoduchý prístupový bod)

Vynulovanie sieťového pripojenia

V tejto časti je vysvetlené, ako robiť nastavenia sieťového pripojenia a meniť spôsob pripojenia, keď vymeníte bezdrôtový smerovač alebo počítač.

Pri výmene bezdrôtového smerovača

Keď vymeníte bezdrôtový smerovač, urobte nastavenia pripojenia medzi počítačom alebo inteligentným zariadením a skenerom.

Ak zmeníte poskytovateľa internetu a podobne, je potrebné urobiť tieto nastavenia.

Vytvorenie nastavení na pripojenie k počítaču

Na pripojenie skenera k počítaču odporúčame použiť inštalačný program.

Ak chcete spustiť inštalačný program, prejdite na nasledujúcu webovú stránku a potom zadajte názov výrobku. Prejdite na položku **Nastavenie** a potom spustíte inštaláciu.

<https://epson.sn>

Môžete zobraziť prevádzkové pokyny v možnosti Príručky k webovým filmom. Prejdite na túto adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Výber spôsobu pripojenia

Postupujte podľa pokynov na obrazovke. Na obrazovke **Vyberte možnosť Inštalovať** vyberte možnosť **Znova nastavte pripojenie pre Tlačiareň (kvôli novému sieťovému smerovaču alebo zmene z USB na sieťové atď.)** a kliknite na tlačidlo **Ďalej**.

Dokončíte nastavenie podľa pokynov na obrazovke.

Ak sa nedá pripojiť, pozrite nasledujúce spôsoby vyriešenia problému.

„Nedá sa pripojiť k sieti” na strane 32

Vytvorenie nastavení na pripojenie k inteligentnému zariadeniu

Keď pripojíte skener k rovnakej sieti Wi-Fi (SSID) ako inteligentné zariadenie, môžete skener používať z inteligentného zariadenia. Ak chcete spúšťať skener z inteligentného zariadenia, prejdite na nasledujúcu webovú stránku a potom zadajte názov výrobku. Prejdite na položku **Nastavenie** a potom spustíte inštaláciu.

<https://epson.sn>

Otvorte webovú stránku z inteligentného zariadenia, ktoré chcete pripojiť k skeneru.

Pri zmene počítača

Keď zmeníte počítač, urobte nastavenia pripojenia medzi počítačom a skenerom.

Vytvorenie nastavení na pripojenie k počítaču

Na pripojenie skenera k počítaču odporúčame použiť inštalračný program.

Ak chcete spustiť inštalračný program, prejdite na nasledujúcu webovú stránku a potom zadajte názov výrobku. Prejdite na položku **Nastavenie** a potom spustíte inštalračiu.

<https://epson.sn>

Môžete zobrazit' prevádzkové pokyny v možnosti Prírurčky k webovým filmom. Prejdite na túto adresu URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Postupujte podľa pokynov na obrazovke.

Zmena spôsobu pripojenia k počítaču

V tejto časti je vysvetlený spôsob zmeny pripojenia, keď boli počítač a skener pripojené.

Zmena pripojenia tlačiarne zo siete Ethernet na sieť Wi-Fi

Pripojenie cez sieť Ethernet na sieť Wi-Fi zmeníte z ovládacieho panela skenera. Zmena spôsobu pripojenia je v základe rovnaká ako nastavenia pripojenia cez sieť Wi-Fi.

Súvisiace informácie

➔ „Pripojenie k bezdrôtovej sieti LAN (Wi-Fi)” na strane 19

Zmena sieťového pripojenia zo siete Wi-Fi na sieť Ethernet

Podľa ďalej uvedeného postupu zmeníte pripojenie cez sieť Wi-Fi na sieť Ethernet.

1. Na hlavnej obrazovke vyberte položku **Nastav.**
2. Vyberte položky **Nastavenie siete > Nastavenie drôtovej siete LAN**.
3. Postupujte podľa pokynov na obrazovke.

Zmena z pripojenia cez USB na sieťové pripojenie

Použite inštalačný program a znova nastavte iný spôsob pripojenia.

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

<https://epson.sn>

Výber zmeny spôsobov pripojenia

Postupujte podľa pokynov v jednotlivých oknách. Na obrazovke **Vyberte možnosť Inštalovať** vyberte možnosť **Znova nastavte pripojenie pre Tlačiareň (kvôli novému sieťovému smerovaču alebo zmene z USB na sieťové atď.)** a kliknite na tlačidlo **Ďalej**.

Vyberte sieťové pripojenie, ktoré chcete použiť — **Pripojiť cez bezdrôtovú sieť (Wi-Fi)** alebo **Pripojiť cez káblovú sieť LAN (Ethernet)**, potom kliknite na tlačidlo **Ďalej**.

Dokončite nastavenie podľa pokynov na obrazovke.

Kontrola stavu sieťového pripojenia

Podľa nasledujúceho postupu môžete skontrolovať stav sieťového pripojenia.

Kontrola stavu sieťového pripojenia z ovládacieho panela

Stav sieťového pripojenia môžete skontrolovať pomocou ikony siete alebo informácií o sieti na ovládacom paneli skenera.

Kontrola stavu sieťového pripojenia pomocou ikony siete

Stav sieťového pripojenia a intenzitu rádiových vln môžete skontrolovať pomocou ikony siete na hlavnej obrazovke skenera.



	<p>Zobrazuje stav pripojenia k sieti.</p> <p>Klepnutím na ikonu skontrolujete a zmeníte aktuálne nastavenia. Toto je odkaz na nasledujúcu ponuku.</p> <p>Nastav. > Nastavenie siete > Nastavenie Wi-Fi</p>
	<p>Skener nie je pripojený k bezdrôtovej sieti (Wi-Fi).</p>
	<p>Skener vyhľadáva SSID, nie je nastavená IP adresa, prípadne má problém s bezdrôtovou sieťou (Wi-Fi).</p>
	<p>Skener je pripojený k bezdrôtovej sieti (Wi-Fi).</p> <p>Počet prúžkov označuje intenzitu signálu pripojenia. Čím viac čiar, tým silnejšie pripojenie.</p>
	<p>Skener nie je v režime Wi-Fi Direct (Jednoduchý prístupový bod) pripojený k bezdrôtovej sieti (Wi-Fi).</p>
	<p>Skener je pripojený k bezdrôtovej sieti (Wi-Fi) v režime Wi-Fi Direct (Jednoduchý prístupový bod).</p>
	<p>Skener nie je pripojený ku káblovej sieti (Ethernet), prípadne nie je sieť nastavená.</p>
	<p>Skener je pripojený ku káblovej sieti (Ethernet).</p>

Zobrazenie podrobných informácií o sieti z ovládacieho panela

Keď je skener pripojený k sieti, môžete tiež zobraziť informácie týkajúce sa siete zvolením ponúk siete, ktoré chcete skontrolovať.

1. Na hlavnej obrazovke vyberte položku **Nastav.**
2. Vyberte položky **Nastavenie siete > Stav siete**.
3. Ak chcete overiť údaje, vyberte ponuky, ktoré chcete skontrolovať.
 - Stav káblovej siete LAN/Wi-Fi
Zobrazuje informácie o sieti (názov zariadenia, pripojenie, intenzita signálu atď.) pri pripojení k sieti Ethernet alebo Wi-Fi.
 - Stav Wi-Fi Direct
Zobrazuje, či je aktívny alebo deaktivovaný režim Wi-Fi Direct, a položku SSID, heslo a podobne pre pripojenia v režime Wi-Fi Direct.
 - Stav e-mail. servera
Zobrazuje informácie o sieti pre e-mailový server.

Parametre siete

Parametre Wi-Fi

Parametre Wi-Fi nájdete v nasledujúcej tabuľke.

Krajiny alebo oblasti mimo hore uvedených	Tabuľka A
Írsko, Spojené kráľovstvo, Rakúsko, Nemecko, Lichtenštajnsko, Švajčiarsko, Francúzsko, Belgicko, Luxembursko, Holandsko, Taliansko, Portugalsko, Španielsko, Dánsko, Fínsko, Nórsko, Švédsko, Island, Chorvátsko, Cyprus, Grécko, Severné Macedónsko, Srbsko, Slovinsko, Malta, Bosna a Hercegovina, Kosovo, Čierna Hora, Albánsko, Bulharsko, Česká republika, Estónsko, Maďarsko, Lotyšsko, Litva, Poľsko, Rumunsko, Slovensko, Izrael, Austrália, Nový Zéland, Taiwan	Tabuľka B
Turecko	DS-900WN: Sériové čísla začínajúce na XDA8: Tabuľka A Sériové čísla začínajúce na XDA7: Tabuľka B
	DS-800WN: Sériové čísla začínajúce na XDA2: Tabuľka A Sériové čísla začínajúce na XD9Z: Tabuľka B

Tabuľka A

Normy	IEEE 802.11b/g/n* ¹
Frekvenčný rozsah	2 400 až 2 483,5 MHz
Maximálny prenášaný rádiový výkon	20 dBm (EIRP)
Kanály	1/2/3/4/5/6/7/8/9/10/11/12/13
Režimy pripojenia	Infraštruktúra, Wi-Fi Direct (Jednoduchý prístupový bod)* ² * ³
Bezpečnostné protokoly* ⁴	WEP (64/128bit), WPA2-PSK (AES)* ⁵ , WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 K dispozícii len pre model HT20.

*2 Nepodporované pre IEEE 802.11b.

*3 Režimy Infraštruktúra a Wi-Fi Direct alebo pripojenie cez sieť Ethernet sa môžu používať súčasne.

*4 Režim Wi-Fi Direct podporuje len WPA2-PSK (AES).

*5 V súlade so štandardmi WPA2 s podporou zabezpečenia WPA/WPA2 Personal.

Tabuľka B

Normy	IEEE 802.11a/b/g/n* ¹ /ac
Frekvenčné rozsahy	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz

Kanály	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48) W58 (149/153/157/161/165)
Režimy pripojenia	Infraštruktúra, Wi-Fi Direct (Jednoduchý prístupový bod)* ⁴ , * ⁵		
Bezpečnostné protokoly* ⁶	WEP (64/128bit), WPA2-PSK (AES)* ⁷ , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 K dispozícii len pre model HT20.

*2 Nie je k dispozícii na Taiwane

*3 Dostupnosť týchto kanálov a používanie výrobku v exteriéri cez tieto kanály sa líši v závislosti od miesta. Ďalšie informácie nájdete na webovej stránke <http://support.epson.net/wifi5ghz/>

*4 Nepodporované pre IEEE 802.11b.

*5 Režimy Infraštruktúra a Wi-Fi Direct alebo pripojenie cez sieť Ethernet sa môžu používať súčasne.

*6 Wi-Fi Direct podporuje len WPA2-PSK (AES).

*7 V súlade so štandardmi WPA2 s podporou zabezpečenia WPA/WPA2 Personal.

Parametre siete Ethernet

Normy	IEEE802.3i (10BASE-T)* ¹ IEEE802.3u (100BASE-TX)* ¹ IEEE802.3ab (1000BASE-T)* ¹ IEEE802.3az (Energy Efficient Ethernet)* ²
Komunikačný režim	Automaticky, 10 Mb/s úplný duplex, 10 Mb/s polovičný duplex, 100 Mb/s úplný duplex, 100 Mb/s polovičný duplex
Konektor	RJ-45

*1 Na zabránenie nebezpečenstvu rušenia rádiovkej komunikácie používajte kábel kategórie 5e alebo vyššej kategórie STP (tienená skrútená dvojlinka).

*2 Pripojené zariadenie musí spĺňať normy IEEE802.3az.

Funkcie siete a podpora IPv4/IPv6

Funkcie	Podporované
Epson Scan 2	IPv4, IPv6

Funkcie	Podporované
Document Capture Pro/Document Capture	IPv4

Bezpečnostný protokol

IEEE802.1X*	
IPsec/filtrovanie IP	
SSL/TLS	HTTPS server/klient
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Je potrebné použiť pripájacie zariadenie, ktoré spĺňa normu IEEE802.1X.

Používanie portu pre skener

Skener používa nasledujúci port. Tieto porty by mali mať podľa potreby k dispozícii správcovia siete.

Keď odosielateľ (klient) je skener

Použitie	Cieľ (server)	Protokol	Číslo portu	
Odoslanie súboru (keď sa zo skenera využíva skenovanie do priečinka)	Server FTP/FTPS	FTP/FTPS (TCP)	20	
			21	
	Súborový server	SMB (TCP)	445	
			NetBIOS (UDP)	137
				138
	Server WebDAV	NetBIOS (TCP)	139	
Protokol HTTP (TCP)			80	
	Protokol HTTPS (TCP)	443		
Odoslanie e-mailu (keď sa zo skenera využíva skenovanie do e-mailu)		Server SMTP	SMTP (TCP)	25
	SMTP SSL/TLS (TCP)		465	
	SMTP STARTTLS (TCP)		587	
Pripojenie POP pred SMTP (keď sa zo skenera využíva skenovanie do e-mailu)	Server POP	POP3 (TCP)	110	
Keď sa používa aplikácia Epson Connect	Server Epson Connect	HTTPS	443	
		XMPP	5222	

Použitie	Cieľ (server)	Protokol	Číslo portu
Zhromažďovanie používateľských údajov (využívanie kontaktov zo skenera)	Server LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Overenie používateľa pri zhromažďovaní používateľských údajov (keď sa využívajú kontakty zo skenera) Overenie používateľa, keď sa zo skenera využíva skenovanie do sieťového priečinka (SMB)	Server KDC	Kerberos	88
Ovládanie WSD	Klientsky počítač	WSD (TCP)	5357
Vyhľadanie počítača, keď sa využíva okamžité skenovanie z aplikácie	Klientsky počítač	Rozpoznávanie okamžitého skenovania cez sieť	2968

Keď odosielateľ (klient) je klientsky počítač

Použitie	Cieľ (server)	Protokol	Číslo portu
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
Preposielanie naskenovaných údajov z aplikácie	Skener	Skenovanie cez sieť (TCP)	1865
Zhromažďovanie údajov o úlohe, keď sa využíva okamžité skenovanie z aplikácie	Skener	Okamžité skenovanie cez sieť	2968
Web Config	Skener	HTTP (TCP)	80
		HTTPS (TCP)	443

Riešenie problémov

Nedá sa pripojiť k sieti

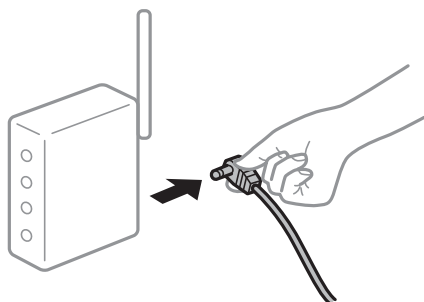
Problém môže byť jeden z nasledovných.

■ So sieťovými zariadeniami pre pripojenie cez Wi-Fi je niečo nesprávne.

Riešenia

Vypnite zariadenia, ktoré chcete pripojiť k sieti. Počkajte asi 10 sekúnd a potom zapnite zariadenia v tomto poradí: bezdrôtový smerovač, počítač alebo inteligentné zariadenia a potom skener. Premiestnite

skener a počítač alebo inteligentné zariadenie bližšie k bezdrôtovému smerovaču, aby sa zlepšila komunikácia rádiovými vlnami, a potom skúste urobiť nastavenia siete znova.



Zariadenia nedokážu prijímať signály z bezdrôtového smerovača, pretože sú príliš ďaleko od seba.

Riešenia

Po premiestnení počítača alebo inteligentného zariadenia a skenera bližšie k bezdrôtovému smerovaču vypnite bezdrôtový smerovač a znova ho zapnite.

Keď vymeníte bezdrôtový smerovač, nastavenia sa nezhodujú s novým smerovačom.

Riešenia

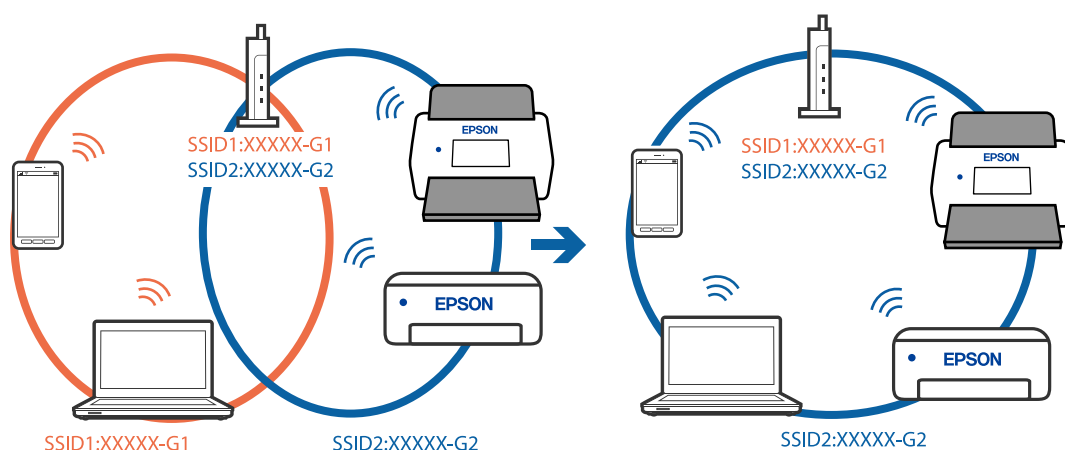
Urobte nastavenia pripojenia znova, aby zodpovedali novému bezdrôtovému smerovaču.

SSID pripojené z počítača alebo inteligentného zariadenia a počítača sú odlišné.

Riešenia

Keď používate viaceré bezdrôtové smerovače súčasne, prípadne má bezdrôtový smerovač viac SSID a zariadenia sú pripojené k rozličným SSID, nie je možné pripojiť k bezdrôtovému smerovaču.

Pripojte počítač alebo inteligentné zariadenie k rovnakému SSID ako skener.



K dispozícii je oddelovač súkromia na bezdrôtovom smerovači.

Riešenia

Väčšina bezdrôtových smerovačov má funkciu oddelovača súkromia, ktorá blokuje komunikáciu medzi pripojenými zariadeniami. Ak komunikácia medzi skenerom a počítačom alebo inteligentným zariadením nie je možná, hoci sú pripojené k rovnakej sieti, deaktivujte na bezdrôtovom smerovači

funkciu oddeľovača súkromia. Pozrite si návod k bezdrôtovému smerovaču, kde nájdete ďalšie podrobnosti.

IP adresa je priradená nesprávne.

Riešenia

Ak je IP adresa pridelená skeneru 169.254.XXX.XXX a maska podsiete je 255.255.0.0, IP adresa nemusí byť priradená správne.

Vyberte položky **Nastav. > Nastavenie siete > Rozšírené > Nastavenie TCP/IP** na ovládacom paneli skenera a potom skontrolujte IP adresu a masku podsiete priradené skeneru.

Reštartujte bezdrôtový smerovač, prípadne vynulujte nastavenia siete pre skener.

Je problém s nastaveniami siete na počítači.

Riešenia

Skúste z počítača otvoriť nejakú webovú stránku, aby ste sa uistili, či sú nastavenia siete na počítači správne. Ak nemôžete otvoriť žiadnu webovú stránku, problém je v počítači.

Skontrolujte sieťové pripojenie počítača. Pozrite si dokumentáciu k počítaču, kde nájdete ďalšie podrobnosti.

Skener bol pripojený cez sieť Ethernet využívajúcu zariadenia podporujúce štandard IEEE 802.3az (Energeticky účinná sieť Ethernet).

Riešenia

Keď pripájate skener cez sieť Ethernet pomocou zariadení podporujúcich normu IEEE 802.3az (Energeticky účinná sieť Ethernet), môžu sa vyskytnúť nasledujúce problémy v závislosti od rozbočovača alebo smerovača, ktoré používate.

- Pripojenie sa stáva nestabilné, skener sa znova a znova pripája a odpája.
- Nedá sa pripojiť k skeneru.
- Rýchlosť pripojenia sa znižuje.

Postupujte podľa ďalej uvedených pokynov, zakážte normu IEEE 802.3az pre skener a potom pripojte.

1. Odpojte kábel siete Ethernet pripojený k počítaču a skeneru.
2. Keď je režim siete IEEE 802.3az pre počítač povolený, zakážte ho.
Pozrite si dokumentáciu k počítaču, kde nájdete ďalšie podrobnosti.
3. Prepojte počítač so skenerom priamo káblom siete Ethernet.
4. Na skeneri skontrolujte nastavenia siete.
Vyberte položky **Nastav. > Nastavenie siete > Stav siete > Stav káblovej siete LAN/Wi-Fi**.
5. Skontrolujte IP adresu skenera.
6. Na počítači otvorte aplikáciu Web Config.
Spustite webový prehľadávač a potom zadajte IP adresu skenera.
[„Ako spustiť funkciu Web Config v internetovom prehliadači”](#) na strane 37
7. Vyberte kartu **Sieť > Drôtová sieť LAN**.

8. Vyberte možnosť **Vyp.** pre **IEEE 802.3az**.
9. Kliknite na položku **Ďalej**.
10. Kliknite na položku **OK**.
11. Odpojte kábel siete Ethernet pripojený k počítaču a skeneru.
12. Ak ste v kroku 2 zakázali režim IEEE 802.3az pre počítač, povoľte ho.
13. Pripojte k počítaču a skeneru káble siete Ethernet, ktoré ste odpojili v kroku 1.
Ak problém pretrváva, môžu problém spôsobovať iné zariadenia okrem skenera.

■ **Skener je vypnutý.**

Riešenia

Skontrolujte, či je skener zapnutý.

Počkajte, kým indikátor stavu prestane blikať, čo znamená, že je skener pripravený na skenovanie.

Softvér na nastavenie skenera

Aplikácia na konfiguráciu činností skenera (Web Config)	37
Epson Device Admin.	38

Aplikácia na konfiguráciu činností skenera (Web Config)

Web Config je aplikácia, ktorá funguje vo webových prehliadačoch, napríklad Microsoft Edge alebo Safari, na počítači alebo na inteligentnom zariadení. Môžete overiť stav skenera alebo zmeniť sieťovú službu a nastavenia skenera. Ak chcete použiť aplikáciu Web Config, pripojte skener a počítač alebo zariadenie do tej istej siete.

Podporované sú nasledujúce prehliadače. Použite najnovšiu verziu.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

Poznámka:

Počas používania tohto zariadenia sa môže objaviť výzva na zadanie hesla správcu. Podrobnosti o hesle správcu pozrite ďalej.

[„Poznámky k heslu správcu” na strane 10](#)

Súvisiace informácie

➔ [„Nedá sa otvoriť aplikácia Web Config” na strane 65](#)

Ako spustiť funkciu Web Config v internetovom prehliadači

Skener sa dodáva so zabudovaným softvérom s názvom Web Config (webová stránka, na ktorej môžete vykonať nastavenia). Ak chcete získať prístup k nástroju Web Config, jednoducho zadajte do prehliadača IP adresu skenera pripojeného k sieti.

1. Skontrolujte IP adresu skenera.

Na ovládacom paneli skenera vyberte položky **Nastav.** > **Nastavenie siete** > **Stav siete**. Potom vyberte spôsob aktívneho pripojenia (**Stav káblovej siete LAN/Wi-Fi** alebo **Stav Wi-Fi Direct**) a overte si tak IP adresu skenera.

Príklad IP adresy: 192.168.100.201

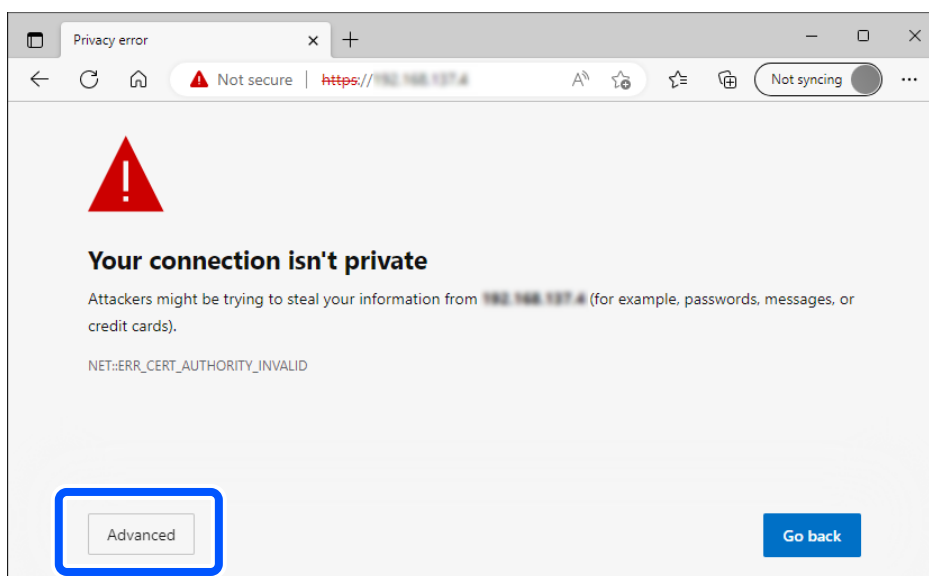
2. Z počítača alebo inteligentného zariadenia spustíte prehľadávač a do riadku adresy zadajte IP adresu skenera.

Formát: `http://IP adresa skenera/`

Príklad: `http://192.168.100.201/`

Ak sa v prehliadači zobrazí obrazovka s upozornením, môžete toto upozornenie bezpečne ignorovať a zobrazíť webovú stránku (Web Config). Pretože skener pri prístupe k protokolu HTTPS používa vlastný podpísaný certifikát, v prehľadávači sa pri spustení aplikácie Web Config zobrazuje upozornenie. To neznamená problém a možno to bezpečne ignorovať. V závislosti od vášho prehliadača môže byť potrebné kliknúť na možnosť **Rozšírené nastavenia**, aby ste si mohli zobrazíť webovú stránku.

Príklad: pre Microsoft Edge



Poznámka:

Ak sa nezobrazí výstražná obrazovka, prejdite na ďalší krok.

Pre adresy IPv6 použite tento formát.

Formát: `http://[IP adresa skenera]/`

Príklad: `http://[2001:db8::1000:1]/`

3. Ak chcete zmeniť nastavenia skenera, musíte sa prihlásiť ako správca aplikácie Web Config.

Kliknite na položku **prihlásiť sa** vpravo hore na obrazovke. Zadaťte položku **Názov používateľa** a **Aktuálne heslo** a kliknite na tlačidlo **OK**.

Nasledujúce informácie poskytujú úvodné hodnoty pre správcovské informácie v aplikácii Web Config.

·Používateľské meno: žiadne (prázdne)

·Heslo: závisí od štítka pripevneného na výrobku.

Ak je na zadnej strane pripevnený štítok „PASSWORD“, zadajte 8-miestne číslo uvedené na štítku. Ak nie je pripevnený štítok „PASSWORD“, zadajte ako prvotné heslo správcu sériové číslo na štítku pripevnenom na zadnej strane výrobku.

Poznámka:

Ak je v pravom hornom rohu obrazovky zobrazená položka **odhlásiť sa**, už ste prihlásení ako správca.

Približne po 20 minútach nečinnosti automaticky prebehne odhlásenie.

Epson Device Admin

Epson Device Admin je multifunkčná aplikácia umožňujúca spravovať zariadenia v sieti.

Šablóny konfigurácie môžete použiť na použitie zjednotených nastavení na viacero skenerov v sieti, vďaka čomu sú vhodné na inštaláciu a správu viacerých skenerov.

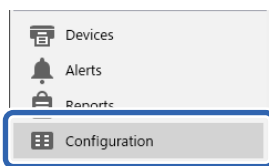
Aplikáciu Epson Device Admin si môžete prevziať z webovej stránky podpory spoločnosti Epson. Podrobnosti o spôsobe používania tejto aplikácie nájdete v dokumentácii k aplikácii Epson Device Admin.

Šablóna konfigurácie

Vytvorenie šablóny konfigurácie

Vytvorte nanovo šablónu konfigurácie.

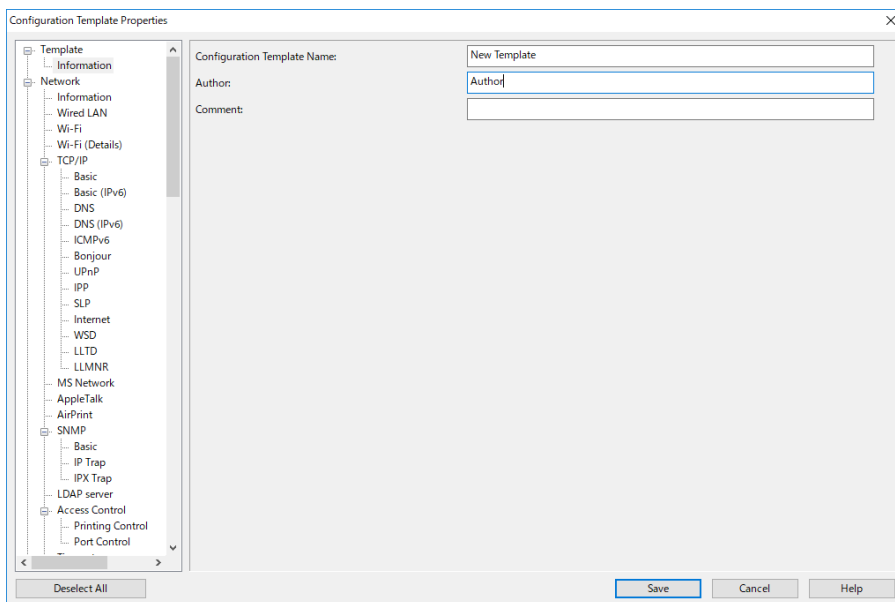
1. Spustíte aplikáciu Epson Device Admin.
2. Vyberte položku **Configuration** z ponuky úloh na bočnom paneli.



3. V ponuke vyberte položku **New**.



4. Nastavte jednotlivé položky.



Položka	Vysvetlenie
Configuration Template Name	Názov šablóny konfigurácie. Zadajte max. 1024 znakov v kódovaní Unicode (UTF-8).
Author	Informácie o tvorcovi šablóny. Zadajte max. 1024 znakov v kódovaní Unicode (UTF-8).

Položka	Vysvetlenie
Comment	Zadajte povinné údaje. Zadajte max. 1024 znakov v kódovaní Unicode (UTF-8).

5. Vľavo vyberte položky, ktoré chcete nastaviť.

Poznámka:

Kliknutím na položky ponuky naľavo prepnete na jednotlivé obrazovky. Ak prepnete obrazovku, nastavená hodnota zostane zachovaná. Nie však vtedy, ak obrazovku zrušíte. Po dokončení všetkých nastavení kliknite na položku **Save**.

Použitie šablóny konfigurácie

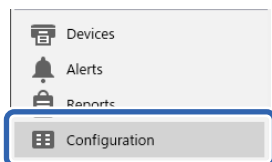
Použite uloženú šablónu konfigurácie do skenera. Použijú sa položky zvolené na šablóne. Ak cieľový skener nemá príslušnú funkciu, nepoužije sa.

Poznámka:

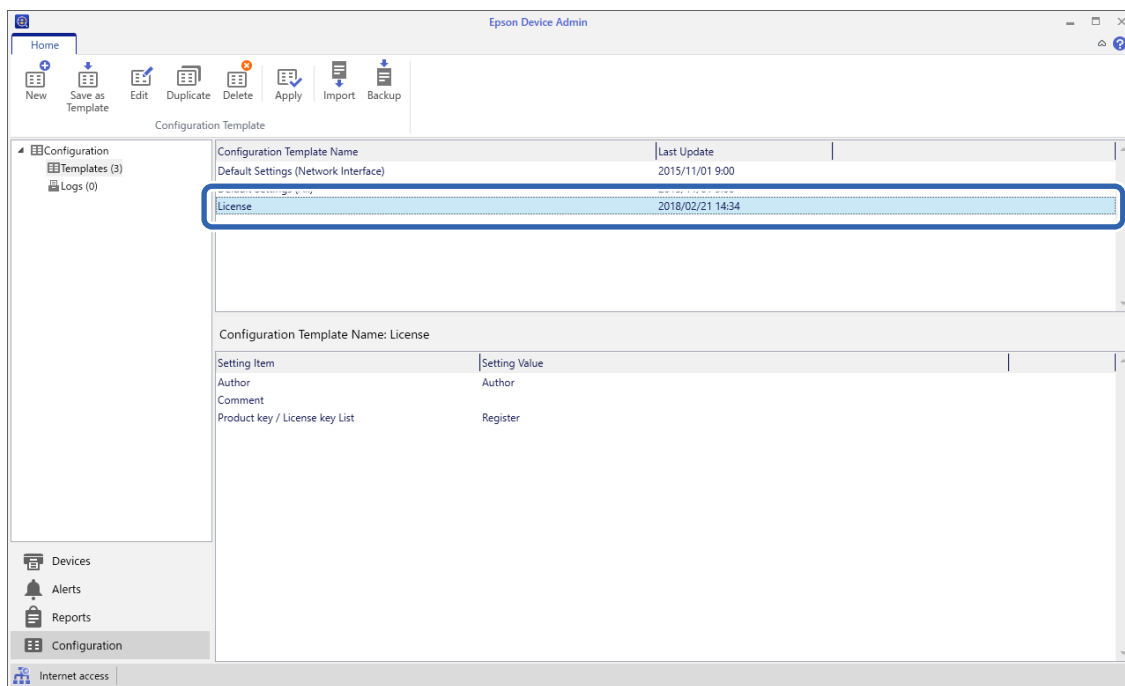
Keď je do skenera nastavené heslo správcu, nakonfigurujte heslo.

1. V pruhovej ponuke na obrazovke Zoznam zariadení vyberte položky **Options** > **Password manager**.
2. Vyberte možnosť **Enable automatic password management** a potom kliknite na položku **Password manager**.
3. Vyberte príslušný skener a kliknite na položku **Edit**.
4. Nastavte heslo a potom kliknite na tlačidlo **OK**.

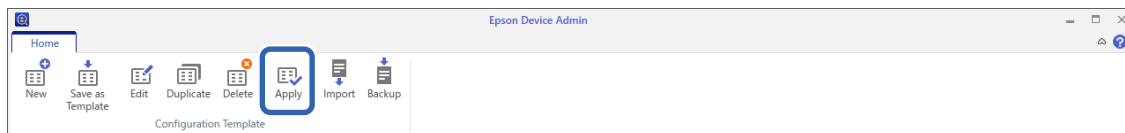
1. Vyberte položku **Configuration** z ponuky úloh na bočnom paneli.



2. V položke **Configuration Template Name** vyberte šablónu konfigurácie, ktorú chcete použiť.



3. V ponuke kliknite na položku **Apply**.
Zobrazí sa obrazovka voľby zariadenia.

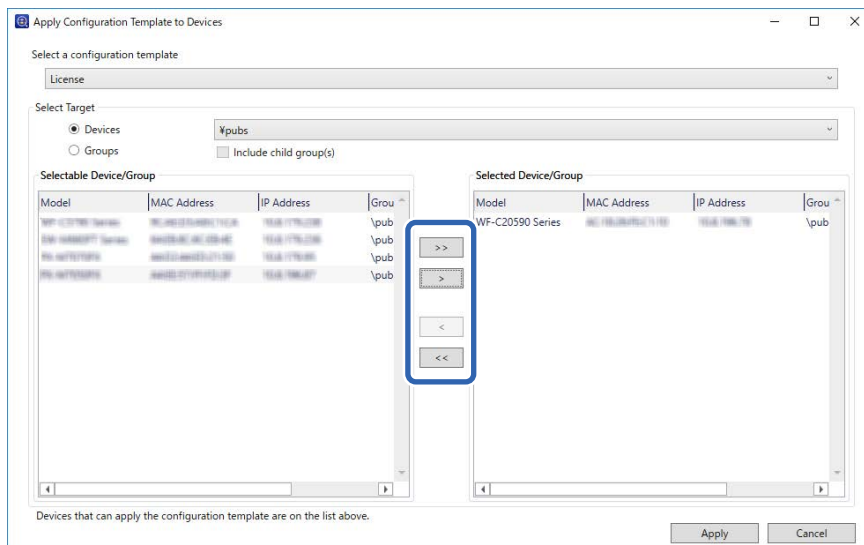



4. Vyberte šablónu konfigurácie, ktorú chcete použiť.

Poznámka:

- Keď vyberiete možnosť **Devices** a skupiny obsahujúce zariadenia v rozbalovacej ponuke, zobrazia sa jednotlivé zariadenia.
- Skupiny sa zobrazia, keď zvolíte možnosť **Groups**. Vyberte možnosť **Include child group(s)**, ak chcete automaticky vybrať podriadené skupiny v rámci vybranej skupiny.

5. Presuňte do časti **Selected Device/Group** skener alebo skupiny, na ktoré chcete použiť šablónu.



6. Kliknite na položku **Apply**.
Zobrazí sa obrazovka s potvrdením pre šablónu konfigurácie, ktorú chcete použiť.
7. Kliknutím na tlačidlo **OK** použijete šablónu konfigurácie.
8. Keď je zobrazené hlásenie s informáciou o dokončení postupu, kliknite na tlačidlo **OK**.
9. Kliknite na položku **Details** a skontrolujte informácie.
Keď sa na použitých položkách zobrazí symbol , použitie bolo dokončené úspešne.
10. Kliknite na položku **Close**.

Potrebné nastavenia pre skenovanie

Registrácia e-mailového servera.	44
Vytvorenie sieťového priečinka.	47
Sprístupnenie kontaktov.	54
Nastavenie funkcie AirPrint.	64
Problémy pri príprave skenovanie cez sieť.	64

Registrácia e-mailového servera

Pred konfigurovaním e-mailového servera skontrolujte nasledujúce položky.

- Skener je pripojený k sieti
- Údaje k nastaveniu e-mailového servera
 - Ak používate internetový e-mailový server, skontrolujte informácie o nastavení u poskytovateľa alebo na webovej lokalite.

Ako zaregistrovať

Otvorte aplikáciu Web Config, vyberte kartu **Sieť > E-mailový server > Základné**.

„Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Nastavenia môžete urobiť aj na ovládacom paneli skenera. Vyberte položky **Nastav. > Nastavenie siete > Rozšírené > E-mailový server > Nastavenia servera**.

Položky nastavenia e-mailového servera

Položka	Nastavenia a vysvetlenie	
Spôsob overenia	Vyberte metódu overenia skenera na prístup k e-mailovému serveru.	
	Vyp.	Pri komunikácii s e-mailovým serverom je overovanie vypnuté.
	Overenie servera SMTP	E-mailový server vyžaduje podporu overovania SMTP.
	POP pred SMTP	Keď vyberiete túto položku, nastavte server POP3.
Overený účet	Ak vyberiete Overenie servera SMTP alebo POP pred SMTP ako Spôsob overenia , zadajte názov overovaného účtu. Zadajte 0 až 255 znakov v kódovaní ASCII (0x20 – 0x7E).	
Overené heslo	Ak vyberiete Overenie servera SMTP alebo POP pred SMTP ako Spôsob overenia , zadajte overené heslo. Zadajte 0 až 20 znakov v kódovaní ASCII (0x20 – 0x7E).	
E-mailová adresa odosielateľa	Nastavte e-mailovú adresu, ktorá sa bude používať na odosielanie e-mailov zo skenera. Hoci môžete použiť existujúcu e-mailovú adresu, odporúčame vám získať a nastaviť vyhradenú e-mailovú adresu, aby ju bolo možné odlišiť od e-mailov odoslaných zo skenera. Zadajte 0 až 255 znakov v kódovaní ASCII (0x20 – 0x7E), okrem znakov : () < > [] ; ¥. Prvý znak nemôže byť bodka „.”.	
Adresa servera SMTP	Zadajte 0 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 . - . Môžete použiť formát IPv4 alebo FQDN.	
Číslo portu servera SMTP	Zadajte číslo medzi 1 a 65535.	
Zabezpečené pripojenie	Pre e-mailový server určite bezpečný spôsob pripojenia.	
	Žiadna	Ak vyberiete položku POP pred SMTP v možnosti Spôsob overenia , spôsob pripojenia je nastavený na Žiadna .
	SSL/TLS	Táto možnosť je dostupná, keď je položka Spôsob overenia nastavená na možnosť Vyp. alebo Overenie servera SMTP .
	STARTTLS	Táto možnosť je dostupná, keď je položka Spôsob overenia nastavená na možnosť Vyp. alebo Overenie servera SMTP .
Overenie certifikátu (iba systém Web Config)	Keď je povolená táto možnosť, certifikát je overený. Odporúčame nastaviť túto hodnotu na Povoliť keď Zabezpečené pripojenie je nastavená na inú hodnotu ako Žiadna .	

Položka	Nastavenia a vysvetlenie
Adresa servera POP3	Ak vyberiete POP pred SMTP ako Spôsob overenia , zadajte adresu servera POP3. Môžete zadať 0 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9. Môžete použiť formát IPv4 alebo FQDN.
Číslo portu servera POP3	Nastavte, keď ste vybrali možnosť POP pred SMTP v položke Spôsob overenia . Zadajte číslo medzi 1 a 65535.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Kontrola pripojenia e-mailového servera

1. Vyberte ponuku testu pripojenia.

Pri nastavení z aplikácie Web Config:

Vyberte kartu **Sieť > E-mailový server > Test pripojenia > Spustiť**.

Pri nastavovaní z ovládacieho panela:

Vyberte položky **Nastav. > Nastavenie siete > Rozšírené > E-mailový server > Kontrola pripojenia**.

Skúška pripojenia k e-mailovému serveru je spustená.

2. Skontrolujte výsledky testov.

Test je úspešný, keď sa zobrazí správa **Test pripojenia bol úspešný**. sa zobrazí.

Ak sa zobrazí chyba, postupujte podľa pokynov v správe a chybu odstráňte.

„Správy testu pripojenia servera pošty” na strane 45

Správy testu pripojenia servera pošty

Hlásenie	Príčina
Chyba komunikácie servera SMTP. Skontrolujte nasledujúcu položku. - Nastavenia siete	Toto hlásenie sa zobrazí, keď <ul style="list-style-type: none"> <input type="checkbox"/> Skener nie je pripojený k sieti <input type="checkbox"/> Server SMTP má výpadok <input type="checkbox"/> Počas komunikácie došlo k odpojeniu siete <input type="checkbox"/> Prijali sa neúplné údaje
Chyba komunikácie servera POP3. Skontrolujte nasledujúcu položku. - Nastavenia siete	Toto hlásenie sa zobrazí, keď <ul style="list-style-type: none"> <input type="checkbox"/> Skener nie je pripojený k sieti <input type="checkbox"/> Server POP3 má výpadok <input type="checkbox"/> Počas komunikácie došlo k odpojeniu siete <input type="checkbox"/> Prijali sa neúplné údaje
Počas pripájania k serveru SMTP sa vyskytla chyba. Skontrolujte nasledujúce položky. - Adresa servera SMTP - Server DNS	Toto hlásenie sa zobrazí, keď <ul style="list-style-type: none"> <input type="checkbox"/> Pripojenie k serveru DNS nebolo úspešné <input type="checkbox"/> Rozlíšenie názvu pre server SMTP nebolo úspešné

Hlásenie	Príčina
Počas pripájania k serveru POP3 sa vyskytla chyba. Skontrolujte nasledujúce položky. - Adresa servera POP3 - Server DNS	Toto hlásenie sa zobrazí, keď <ul style="list-style-type: none"> <input type="checkbox"/> Pripojenie k serveru DNS nebolo úspešné <input type="checkbox"/> Rozlíšenie názvu pre server POP3 nebolo úspešné
Chyba pri autentifikácii servera SMTP. Skontrolujte nasledujúce položky. - Spôsob autentifikácie - Autentifikované konto - Autentifikované heslo	Toto hlásenie sa zobrazí, keď nebolo overenie na serveri SMTP úspešné.
Chyba pri autentifikácii servera POP3. Skontrolujte nasledujúce položky. - Spôsob autentifikácie - Autentifikované konto - Autentifikované heslo	Toto hlásenie sa zobrazí, keď nebolo overenie na serveri POP3 úspešné.
Nepodporovaný spôsob komunikácie. Skontrolujte nasledujúce položky. - Adresa servera SMTP - Číslo portu servera SMTP	Toto hlásenie sa zobrazí, keď sa pokúšate komunikovať s nepodporovanými protokolmi.
Pripojenie k serveru SMTP zlyhalo. Zmeňte Zabezpečené pripojenie na možnosť Žiadna.	Toto hlásenie sa zobrazí, keď medzi serverom a klientom dôjde k nesúladu SMTP alebo ak tento server nepodporuje bezpečné pripojenie SMTP (pripojenie SSL).
Pripojenie k serveru SMTP zlyhalo. Zmeňte Zabezpečené pripojenie na možnosť SSL/TLS.	Toto hlásenie sa zobrazí, keď sa medzi serverom a klientom vyskytne nesúlad SMTP, prípadne ak server vyžaduje pre SSL/TLS zabezpečené pripojenie cez SMTP (pripojenie SSL).
Pripojenie k serveru SMTP zlyhalo. Zmeňte Zabezpečené pripojenie na možnosť STARTTLS.	Toto hlásenie sa zobrazí, keď sa medzi serverom a klientom vyskytne nesúlad SMTP, prípadne ak server vyžaduje pre STARTTLS zabezpečené pripojenie cez SMTP (pripojenie SSL).
Pripojenie nie je dôveryhodné. Skontrolujte nasledujúcu položku. - Dátum a čas	Toto hlásenie sa objaví, keď je nastavenie dátumu a času na skeneri nesprávne, prípadne uplynula platnosť certifikátu.
Pripojenie nie je dôveryhodné. Skontrolujte nasledujúcu položku. - Certifikát CA	Toto hlásenie sa objaví, keď skener nemá koreňový certifikát zodpovedajúci serveru, prípadne nebol importovaný Certifikát CA.
Pripojenie nie je zabezpečené.	Toto hlásenie sa objaví, keď je získaný certifikát poškodený.
Autentifikácia servera SMTP zlyhala. Zmeňte spôsob autentifikácie na SMTP-AUTH.	Toto hlásenie sa objaví, keď sa medzi serverom a klientom vyskytne nesúlad v spôsobe overovania. Server podporuje funkciu Overenie servera SMTP.
Autentifikácia servera SMTP zlyhala. Zmeňte spôsob autentifikácie na POP pred SMTP.	Toto hlásenie sa objaví, keď sa medzi serverom a klientom vyskytne nesúlad v spôsobe overovania. Server nepodporuje funkciu Overenie servera SMTP.
E-mailová adresa odosielateľa je nesprávna. Zmeňte na e-mailovú adresu vašej e-mailovej služby.	Toto hlásenie sa objaví, keď je určená e-mailová adresa odosielateľa nesprávna.
K výrobku nemožno získať prístup, kým nebude dokončené spracovanie.	Toto hlásenie sa objaví, keď je skener zaneprázdnený.

Vytvorenie sieťového priečinka

Vytvorte sieťový priečinok v počítači. Počítač musí byť pripojený k rovnakej sieti ako skener.


Spôsob nastavenia sieťového priečinka sa líši v závislosti od prostredia. Toto je príklad vytvorenia sieťového priečinka na pracovnej ploche počítača v nasledujúcom prostredí.

- Operačný systém: Windows 10
- Miesto vytvorenia zdieľaného priečinka: pracovná plocha
- Cesta k priečinku: C:\Users\xxxx\Plocha\scan_folder (vytvorte sieťový priečinok s názvom „scan_folder“ na ploche)

1. Prihláste sa do počítača, v ktorom chcete vytvoriť sieťový priečinok, pomocou používateľského konta s oprávnením správcu.

Poznámka:

Ak nevíete, ktoré používateľské konto má oprávnenie správcu, obráťte sa na správcu počítača.

2. Uistite sa, že názov zariadenia (názov počítača) neobsahuje dvojbytové znaky. Kliknite na tlačidlo Štart systému Windows a potom vyberte možnosť  **Nastavenia** > **Systém** > **Informácie**.

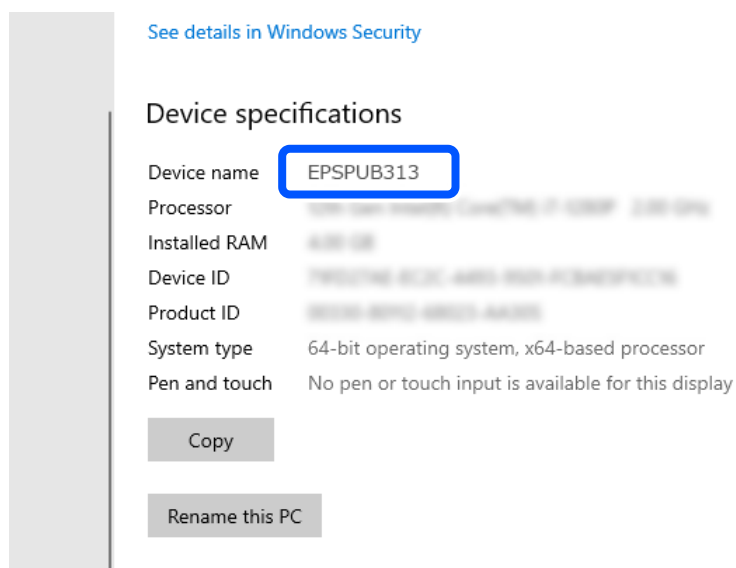
Poznámka:

Ak sú v názve zariadenia dvojbytové znaky, ukladanie súborov môže zlyhať.

3. Skontrolujte, či reťazec zobrazený v ponuke **Špecifikácie zariadenia** > **Názov zariadenia** neobsahuje žiadne dvojbytové znaky.

Ak názov zariadenia obsahuje iba jednobajtové znaky, nemali by sa vyskytnúť žiadne problémy. Zatvorte obrazovku.

Príklad: EPSPUB313



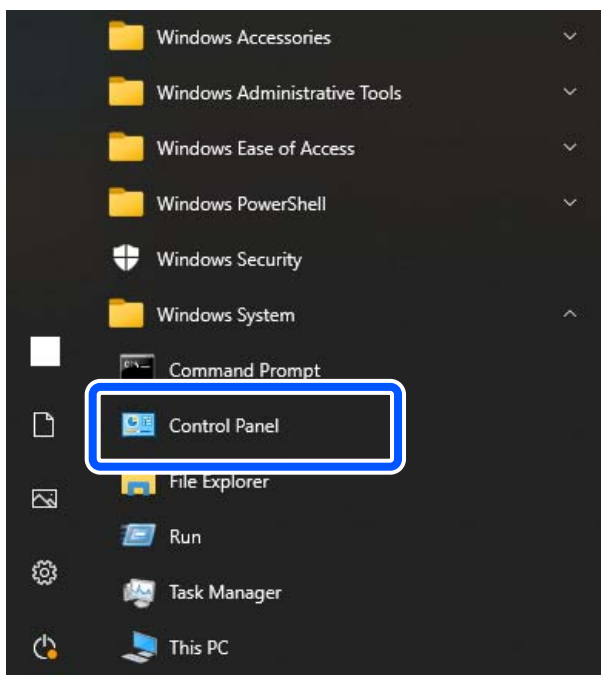
! **Upozornenie:**

Ak názov zariadenia obsahuje dvojbytové znaky, použite počítač, ktorý nepoužíva dvojbytové znaky, alebo zariadenie premenujte.

Ak potrebujete zmeniť názov zariadenia, vopred sa poraďte so správcom počítača, pretože to môže ovplyvniť správu počítača a prístup k prostriedkom.

Potom skontrolujte nastavenia počítača.

4. Kliknite na tlačidlo Štart systému Windows a vyberte položky **Systém Windows > Ovládací panel**.



5. Na Ovládacom paneli kliknite na položky **Sieť a internet > Centrum sietí a zdieľania > Zmeniť rozšírené nastavenia zdieľania**.

Zobrazí sa profil siete.

6. Skontrolujte, či je v časti **Zdieľanie súborov a tlačiarňí** pre sieťový profil (aktuálny profil) vybratá možnosť **Zapnúť zdieľanie súborov a tlačiarňí**.

Ak už je to zvolené, kliknite na tlačidlo **Zrušiť** a zatvorte okno.

Keď zmeníte nastavenie, kliknite na tlačidlo **Uložiť zmeny** a zatvorte okno.

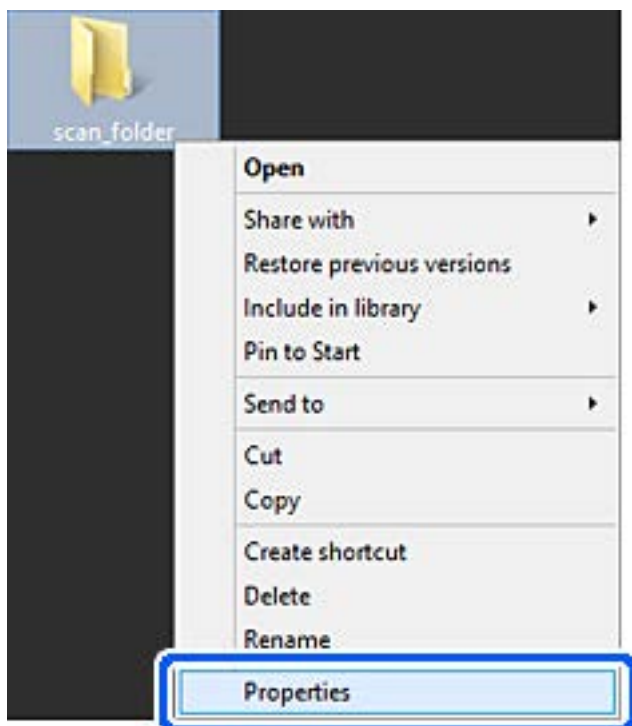
Potom vytvorte sieťový priečinok.

7. Vytvorte a pomenujte priečinok na pracovnej ploche.

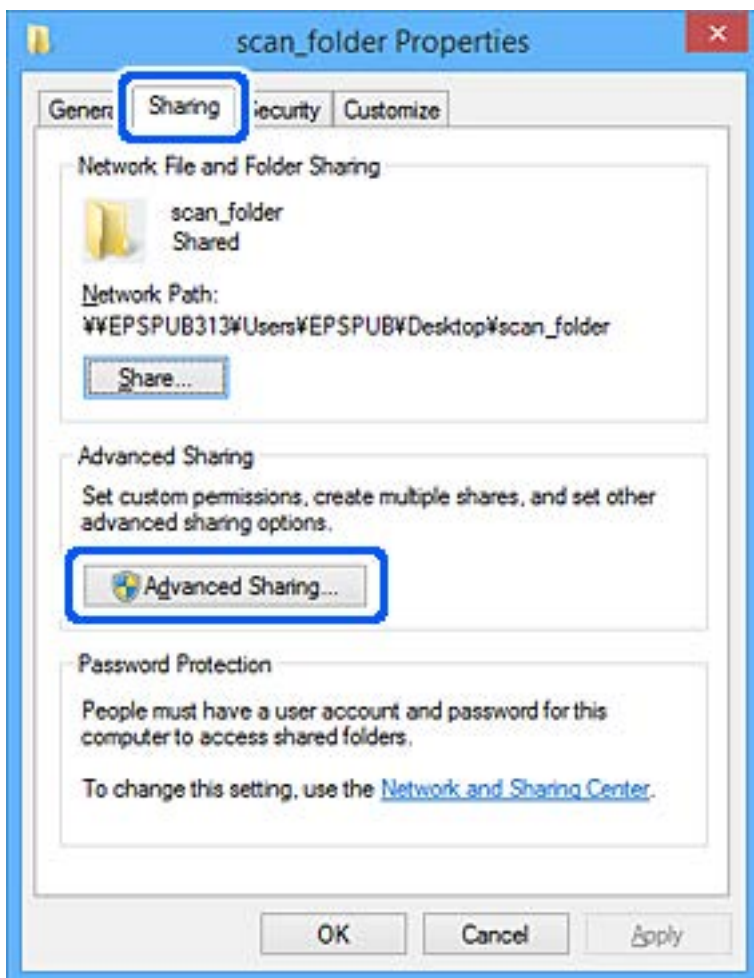
V názve priečinka môžete zadať 1 až 12 abecedných a číselných znakov. Ak je v názve viac ako 12 znakov, v závislosti od vášho zariadenia sa môže stať, že nebudete mať prístup k priečinku.

Príklad: scan_folder

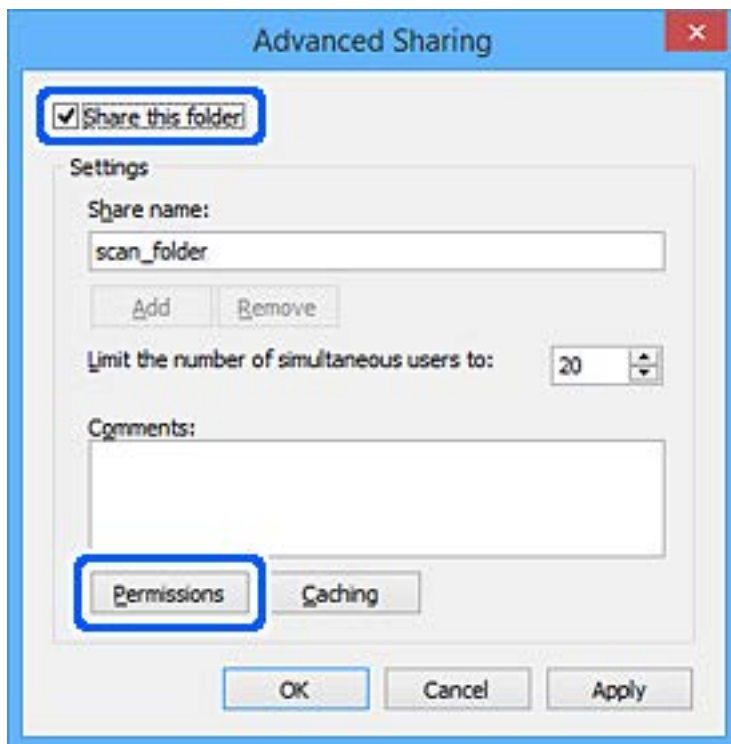
8. Kliknite pravým tlačidlom myši na priečinok a vyberte položku **Vlastnosti**.



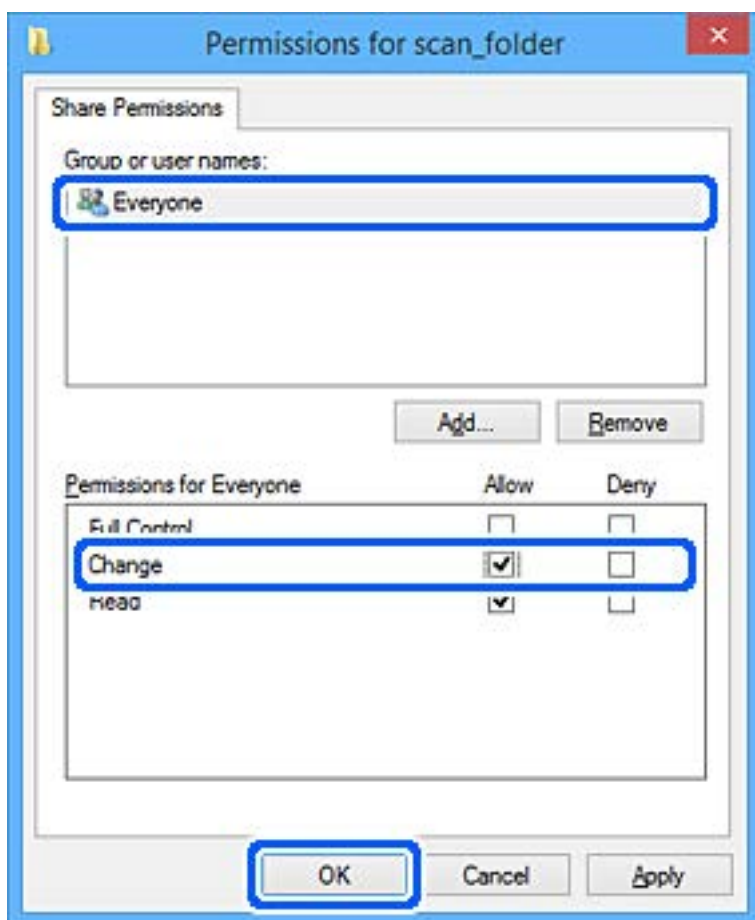
9. Kliknite na položku **Rozšírené zdieľanie** na karte **Zdieľanie**.



10. Vyberte možnosť **Zdieľať tento priečink** a potom kliknite na položku **Povolenia**.



11. Vyberte skupinu **Všetci** v položke **Skupina alebo používateľské mená**, vyberte možnosť **Povoliť** na položke **Zmeniť** a potom kliknite na tlačidlo **OK**.

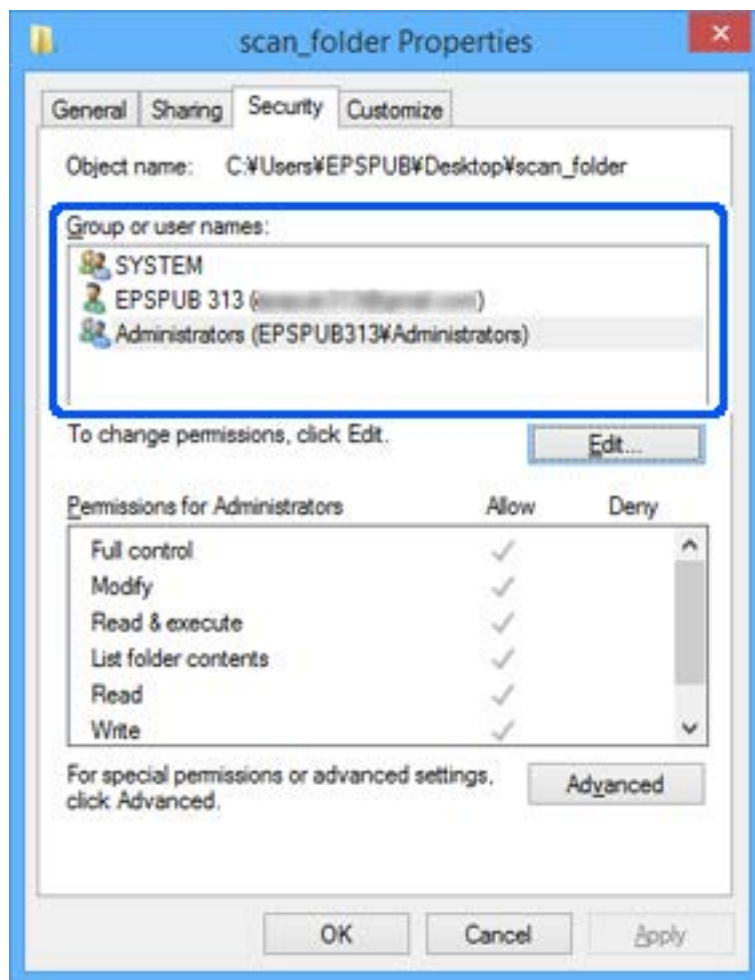


12. Kliknutím na tlačidlo **OK** zatvorte obrazovku a vráťte sa do okna Vlastnosti.

Poznámka:

Na karte **Zabezpečenie** > **Názvy skupín alebo používateľov** môžete skontrolovať, ktoré skupiny alebo používatelia majú prístup k sieťovému priečinku.

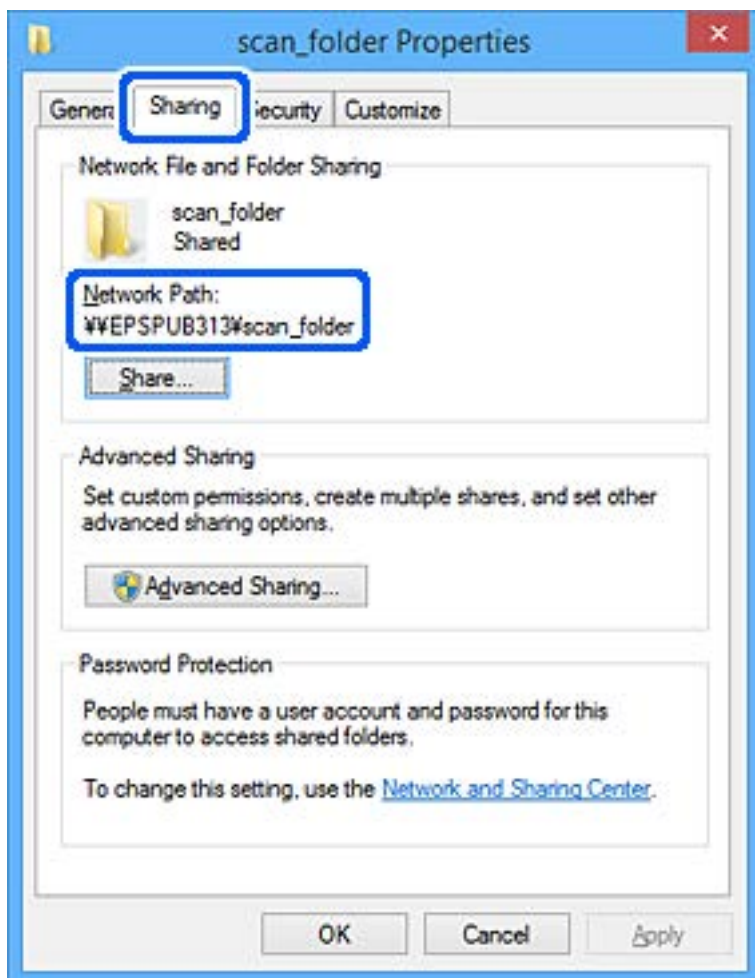
Príklad: keď používateľ prihlásený do počítača, ako aj administrátori majú prístup k sieťovému priečinku



13. Vyberte kartu **Zdieľanie**.

Zobrazuje sa umiestnenie sieťového priečinka v sieti. To sa používa pri registrácii vašich kontaktov v skeneri. Zapište si to.

Príklad: \\EPSPUB313\scan_folder



14. Kliknutím na tlačidlo **Zatvoriť** alebo **OK** zatvorte okno.

Tým sa dokončí vytváranie sieťového priečinka.

Sprístupnenie kontaktov

Po registrácii cieľov do zoznamu kontaktov v skeneri budete môcť ľahko zadávať cieľ pri skenovaní.

Do zoznamu kontaktov môžete zaregistrovať nasledujúce typy cieľov. Môžete zaregistrovať celkovo až 300 položiek.

Poznámka:

Na zadanie cieľa môžete použiť server LDAP (vyhľadávanie cez LDAP).

E-mail	Cieľ pre e-mail. Najprv je potrebné nakonfigurovať nastavenia e-mailového servera.
Sieťový priečinok	Cieľ pre údaje skenovania. Vopred je potrebné sieťový priečinok nastaviť.

Súvisiace informácie

➔ „Spolupráca medzi serverom LDAP a používateľmi” na strane 61

Porovnanie konfigurácie kontaktov

Na konfiguráciu kontaktov skenera existujú tri nástroje: aplikácia Web Config, aplikácia Epson Device Admin a ovládací panel tlačiarne. Rozdiely medzi týmito tromi nástrojmi sú uvedené v tabuľke nižšie.

Funkcie	Web Config*	Epson Device Admin	Ovládací panel skenera
Registrácia cieľa	✓	✓	✓
Úprava cieľa	✓	✓	✓
Pridanie skupiny	✓	✓	✓
Úprava skupiny	✓	✓	✓
Odstránenie cieľa alebo skupiny	✓	✓	✓
Odstránenie všetkých cieľov	✓	✓	–
Import súboru	✓	✓	–
Export do súboru	✓	✓	–

* Ak chcete robiť nastavenia, prihláste sa ako správca.

Registrácia cieľa do kontaktov pomocou aplikácie Web Config

Poznámka:

Na ovládacom paneli skenera môžete tiež zaregistrovať kontakty.

1. Otvorte aplikáciu Web Config a vyberte kartu **Skenov.** > **Kontakty**.
2. Vyberte číslo, ktoré chcete zaregistrovať, a potom kliknite na tlačidlo **Upraviť**.
3. Zadajte položky **Názov** a **Indexové slovo**.
4. V možnosti **Typ** vyberte typ cieľa.

Poznámka:

Možnosť **Typ** nie je možné po registrácii zmeniť. Ak chcete zmeniť typ, odstráňte cieľ a vykonajte novú registráciu.

5. Zadajte hodnoty pre všetky položky a kliknite na položku **Použiť**.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Položky nastavenia cieľa

Položky	Nastavenia a vysvetlenie
Spoločné nastavenia	
Názov	Zadajte meno zobrazené v kontaktoch — najviac 30 znakov v kódovaní Unicode (UTF-16). Ak to neurčujete, nechajte prázdne.
Indexové slovo	Zadajte názov pomocou maximálne 30 znakov v kódovaní Unicode (UTF-16), ak chcete vyhľadať kontakty na ovládacom paneli skenera. Ak to neurčujete, nechajte prázdne.
Typ	Vyberte typ adresy, ktorú chcete zaregistrovať.
Priradiť k najp.	Vyberte, či chcete zaregistrovanú adresu nastaviť ako často používanú. Keď je nastavená ako často používaná adresa, zobrazuje sa vo vrchnej časti obrazovky skenovania a môžete určiť cieľ bez zobrazenia kontaktov.
E-mail	
E-mailová adresa	Zadajte 1 až 255 znakov. Môžete použiť znaky A – Z a – z 0 – 9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Priečinko siete (SMB)	
Uložiť do	\\„Cesta k priečinku“ Zadajte umiestnenie cieľového priečinka — 1 až 253 znakov v kódovaní Unicode (UTF-16) (nepočítajte do toho „\\“). Zadajte sieťovú cestu zobrazenú na obrazovke vlastností priečinka. Podrobnosti o nastavení sieťovej cesty nájdete ďalej. „Vytvorenie sieťového priečinka“ na strane 47
Názov používateľa	Zadajte používateľské meno pre prístup k sieťovému priečinku — najviac 30 znakov v kódovaní Unicode (UTF-16). Nepoužívajte však riadiace znaky (0x00 až 0x1F, 0x7F).
Heslo	Zadajte heslo prístupu k sieťovému priečinku dlhé 0 až 20 znakov v štandarde Unicode (UTF-16). Nepoužívajte však riadiace znaky (0x00 až 0x1F, 0x7F).
FTP	
Zabezpečené pripojenie	Vyberte možnosť FTP alebo FTPS podľa toho, ktorý protokol prenosu súborov podporuje server FTP. Vyberte možnosť FTPS , ak chcete povoliť skeneru komunikáciu s bezpečnostnými opatreniami.
Uložiť do	Zadajte názov servera v dĺžke 1 až 253 znakov v kódovaní Unicode (UTF-16) (nepočítajte do toho „ftp://“ ani „ftps://“).
Názov používateľa	Zadajte používateľské meno pre prístup k serveru FTP — najviac 30 znakov v kódovaní Unicode (UTF-16). Nepoužívajte však riadiace znaky (0x00 až 0x1F, 0x7F). Ak server umožňuje zadať anonymné pripojenia, zadajte meno používateľa, ako napríklad Anonymný a FTP. Ak to neurčujete, nechajte prázdne.
Heslo	Zadajte heslo prístupu na server FTP dlhé 0 až 20 znakov v kódovaní Unicode (UTF-16). Nepoužívajte však riadiace znaky (0x00 až 0x1F, 0x7F). Ak to neurčujete, nechajte prázdne.
Režim pripojenia	V ponuke vyberte režim pripojenia. Ak je medzi skenerom a serverom FTP nastavená brána firewall, vyberte položku Pasívny režim .

Položky	Nastavenia a vysvetlenie
Číslo portu	Zadajte číslo portu servera FTP v rozmedzí od 1 do 65535.
Overenie certifikátu	Keď je táto možnosť aktivovaná, overuje sa certifikát servera FTP. To je k dispozícii, keď je možnosť FTPS zvolená pre položku Zabezpečené pripojenie . Ak chcete nastaviť, je potrebné do skenera importovať certifikát Certifikát CA.
SharePoint(WebDAV)*	
Zabezpečené pripojenie	Vyberte možnosť HTTP alebo HTTPS podľa toho, ktorý protokol prenosu súborov podporuje server. Vyberte možnosť HTTPS , ak chcete povoliť skeneru komunikáciu s bezpečnostnými opatreniami.
Uložiť do	Zadajte názov servera v dĺžke 1 až 253 znakov v kódovaní Unicode (UTF-16) (nepočítajte do toho „http://“ ani „https://“).
Názov používateľa	Zadajte používateľské meno pre prístup k serveru — najviac 30 znakov v kódovaní Unicode (UTF-16). Nepoužívajte však riadiace znaky (0x00 až 0x1F, 0x7F). Ak to neurčujete, nechajte prázdne.
Heslo	Zadajte heslo prístupu na server dlhé 0 až 20 znakov v kódovaní Unicode (UTF-16). Nepoužívajte však riadiace znaky (0x00 až 0x1F, 0x7F). Ak to neurčujete, nechajte prázdne.
Overenie certifikátu	Keď je táto možnosť aktivovaná, overuje sa certifikát servera. To je k dispozícii, keď je možnosť HTTPS zvolená pre položku Zabezpečené pripojenie . Ak chcete nastaviť, je potrebné do skenera importovať certifikát Certifikát CA.
Proxy server	Vyberte, či chcete používať server proxy.

* SharePoint Online nie je podporované, keď sa skenuje do sieťového priečinka z ovládacieho panela skenera.

Ak chcete uložiť naskenovaný obraz v službe SharePoint Online, použite program Document Capture Pro po inštalácii aplikácie SharePoint Online Connector. Podrobnosti nájdete v návode k aplikácii Document Capture Pro.

<https://support.epson.net/dcp/>

Registrovanie cieľov ako skupiny pomocou aplikácie Web Config

Ak je typ cieľa nastavený na možnosť **E-mail**, ciele môžete registrovať ako skupinu.

1. Otvorte aplikáciu Web Config a vyberte kartu **Skenov.** > **Kontakty**.
2. Vyberte číslo, ktoré chcete zaregistrovať, a potom kliknite na tlačidlo **Upraviť**.
3. V položke **Typ** vyberte skupinu.
4. Kliknite na možnosť **Vybrať** pre položku **Kontakt(y) Skupiny**.
Zobrazia sa dostupné ciele.
5. Vyberte cieľ, ktorý chcete zaregistrovať do skupiny, a potom kliknite na položku **Vybrať**.
6. Zadajte položky **Názov** a **Indexové slovo**.

7. Vyberte, či chcete priradiť registrovanú skupinu do často používaných skupín.

Poznámka:

Ciele je možné zaregistrovať do viacerých skupín.

8. Kliknite na položku **Použiť**.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Zálohovanie a import kontaktov

Pomocou aplikácie Web Config alebo inými nástrojmi môžete zálohovať a importovať kontakty.

S aplikáciou Web Config môžete zálohovať kontakty exportovaním nastavení skenera, ktoré zahŕňajú aj kontakty. Exportovaný súbor sa nedá upraviť, pretože ide o binárny súbor.

Keď do skenera nainportujete nastavenia skenera, kontakty sa prepíšu.

S aplikáciou Epson Device Admin je možné z obrazovky vlastností zariadenia exportovať len kontakty. Ak neexportujete aj položky týkajúce sa zabezpečenia, môžete exportované kontakty upraviť, pretože sú uložené v súbore vo formáte SYLK alebo CSV.

Import kontaktov pomocou aplikácie Web Config

Ak máte skener umožňujúci zálohovanie kontaktov, ktoré je kompatibilné s týmto skenerom, môžete kontakty ľahko zaregistrovať importom súboru so zálohou.

Poznámka:

Pokyny na zálohovanie kontaktov v skeneri nájdete v návode, ktorý bol priložený ku skeneru.

Podľa nasledujúceho postupu importujte kontakty do tohto skenera.

1. Otvorte aplikáciu Web Config a vyberte kartu **Správa zariadenia > Hodnota nastavenia exportu a importu > Importovať**.
2. V ponuke **Súbor** vyberte vytvorený súbor so zálohou, zadajte heslo a potom kliknite na tlačidlo **Ďalej**.
3. Vyberte políčko **Kontakty** a potom kliknite na tlačidlo **Ďalej**.

Zálohovanie kontaktov pomocou aplikácie Web Config

Údaje kontaktov sa môžu stratiť z dôvodu poruchy skenera. Odporúčame vám, aby ste si pri akejkoľvek aktualizácii údajov urobili zálohu týchto údajov. Spoločnosť Epson nezodpovedá za stratu akýchkoľvek údajov ani za zálohovanie a/alebo obnovenie údajov alebo nastavení, a to ani počas záručného obdobia.

Pomocou aplikácie Web Config môžete zálohovať údaje kontaktov uložené v skeneri do počítača.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Správa zariadenia > Hodnota nastavenia exportu a importu > Exportovať**.
2. Začiarknite políčko **Kontakty** v kategórii **Skenov..**

3. Zadajte heslo na zašifrovanie exportovaného súboru.
Na import súboru je potrebné heslo. Ak nechcete súbor zašifrovať, nechajte to prázdne.
4. Kliknite na položku **Exportovať**.

Export a hromadná registrácia kontaktov pomocou nástroja

Ak použijete aplikáciu Epson Device Admin, môžete zálohovať len kontakty a upraviť exportované súbory, potom ich môžete zaregistrovať naraz.

Je to užitočné, ak chcete zálohovať len kontakty, prípadne ak vymieňate skener a chcete preniesť kontakty zo starého do nového.

Export kontaktov

Uložte údaje o kontaktoch do súboru.

Pomocou tabuľkovej aplikácie alebo textového editora môžete upraviť súbory uložené vo formáte SYLK alebo CSV. Po odstránení alebo pridaní údajov môžete zaregistrovať všetko naraz.

Údaje obsahujúce položky zabezpečenia, napríklad heslá a osobné údaje, môžu byť uložené v binárnom formáte s heslom. Súbor sa nedá upravovať. Môže sa využiť ako záložný súbor údajov vrátane položiek zabezpečenia.

1. Spustíte softvér Epson Device Admin.
2. Vyberte položku **Devices** z ponuky úloh na bočnom paneli.
3. Zo zoznamu zariadení vyberte zariadenie, ktoré chcete nakonfigurovať.
4. Kliknite na položku **Device Configuration** na karte **Home** v ponuke.
Keď bolo nastavené heslo správcu, zadajte heslo a kliknite na tlačidlo **OK**.
5. Kliknite na položky **Common > Contacts**.
6. Vyberte formát exportu v ponuke **Export > Export items**.
 - All Items
Exportujte zašifrovaný binárny súbor. Vyberte, či chcete zahrnúť položky zabezpečenia, napríklad heslo a osobné údaje. Súbor sa nedá upravovať. Ak ho zvolíte, je potrebné nastaviť heslo. Kliknite na položku **Configuration** a nastavte heslo: 8 až 63 znakov v kódovaní ASCII. Toto heslo je potrebné pri importe binárneho súboru.
 - Items except Security Information
Exportujte súbory vo formáte SYLK alebo CSV. Vyberte, keď chcete upraviť údaje v exportovanom súbore.
7. Kliknite na položku **Export**.
8. Stanovte miesto na uloženie súboru, vyberte typ súboru a potom kliknite na možnosť **Save**.
Zobrazí sa hlásenie o dokončení.
9. Kliknite na položku **OK**.
Skontrolujte, či je súbor uložený na určenom mieste.

Import kontaktov

Naimportujte údaje o kontaktoch zo súboru.

Importovať môžete súbory uložené vo formáte SYLK alebo CSV, prípadne binárny súbor obsahujúci položky zabezpečenia.

1. Spustíte softvér Epson Device Admin.
2. Vyberte položku **Devices** z ponuky úloh na bočnom paneli.
3. Zo zoznamu zariadení vyberte zariadenie, ktoré chcete nakonfigurovať.
4. Kliknite na položku **Device Configuration** na karte **Home** v ponuke.
Keď bolo nastavené heslo správcu, zadajte heslo a kliknite na tlačidlo **OK**.
5. Kliknite na položky **Common > Contacts**.
6. Kliknite na tlačidlo **Browse** v časti **Import**.
7. Vyberte súbor, ktorý chcete importovať, a potom kliknite na tlačidlo **Open**.
Keď vyberiete binárny súbor, v položke **Password** zadajte heslo nastavené pri exporte súboru.
8. Kliknite na položku **Import**.
Zobrazí sa obrazovka s potvrdením.
9. Kliknite na položku **OK**.
Zobrazí sa výsledok overenia.
 - Edit the information read
Kliknite, keď chcete upraviť jednotlivé informácie.
 - Read more file
Kliknite, keď chcete importovať viac súborov.
10. Kliknite na položku **Import** a potom kliknite na tlačidlo **OK** na obrazovke dokončenia importu.
Vráťte sa na obrazovku vlastností zariadenia.
11. Kliknite na položku **Transmit**.
12. Kliknite na tlačidlo **OK** v hlásení o potvrdení.
Nastavenia sú odoslané do skenera.
13. Na obrazovke dokončenia odosielania kliknite na tlačidlo **OK**.
Informácie o skeneri sú aktualizované.
Otvorte kontakty z aplikácie Web Config alebo ovládacieho panela skenera a potom skontrolujte, či je kontakt aktualizovaný.

Spolupráca medzi serverom LDAP a používateľmi

Keď spolupracujete so serverom LDAP, môžete použiť informácie o adresách zaregistrované na serveri LDAP ako cieľ e-mailu.

Konfigurácia servera LDAP

Ak chcete používať údaje zo servera LDAP, zaregistrujte ho na skeneri.

1. Otvorte aplikáciu Web Config a vyberte kartu **Sieť > Server LDAP > Základné**.
2. Zadáajte hodnoty pre všetky položky.
3. Vyberte položku **OK**.
Zobrazia sa nastavenia, ktoré ste vybrali.

Položky nastavenia servera LDAP

Položky	Nastavenia a vysvetlenie
Použiť server LDAP	Vyberte možnosť Použiť alebo Nepoužívajte .
Adresa servera LDAP	Zadáajte adresu servera LDAP. Zadáajte 1 až 255 znakov vo formáte IPv4, IPv6 alebo FQDN. Pre formát FQDN môžete použiť alfanumerické znaky v kódovaní ASCII (0x20 – 0x7E) a znak „-“, ktorý nemôže byť na začiatku a konci adresy.
Číslo portu servera LDAP	Zadáajte číslo portu servera LDAP v rozmedzí od 1 do 65535.
Zabezpečené pripojenie	Stanovte metódu overovania, keď má skener prístup k serveru LDAP.
Overenie certifikátu	Keď to je aktivované, overuje sa certifikát servera LDAP. Odporúčame nastaviť túto položku na Povoliť . Ak to chcete nastaviť, do skenera je potrebné importovať certifikát Certifikát CA .
Časový limit vyhľadávania (sek.)	Nastavte dobu vyhľadávania pred vypršaním časového limitu — 5 až 300.
Spôsob overenia	Vyberte jednu z metód. Ak vyberiete možnosť Autentifikácia prostredníctvom protokolu Kerberos , vyberte položku Nastavenia Kerberos a urobte nastavenia pre Kerberos. Ak sa má vykonávať funkcia Autentifikácia prostredníctvom protokolu Kerberos, je potrebné nasledujúce prostredie. <input type="checkbox"/> Skener a server DNS môžu medzi sebou komunikovať. <input type="checkbox"/> Čas na skeneri, serveri KDC a serveri potrebnom na overenie (server LDAP, server SMTP, súborový server) je synchronizovaný. <input type="checkbox"/> Keď je servisný server priradený ako IP adresa FQDN servisného servera je zaregistrovaná v zóne reverzného vyhľadávania servera DNS.
Použije sa oblasť Kerberos	Ak vyberiete možnosť Autentifikácia prostredníctvom protokolu Kerberos pre položku Spôsob overenia , vyberte oblasť Kerberos, ktorú chcete použiť.

Položky	Nastavenia a vysvetlenie
DN správcu / Názov používateľa	Zadajte používateľské meno pre server LDAP — najviac 128 znakov v kódovaní Unicode (UTF-8). Nemôžete použiť riadiace znaky, ako sú napríklad 0x00 – 0x1F a 0x7F. Toto nastavenie sa nepoužíva, keď je možnosť Anonymná autentifikácia zvolená pre položku Spôsob overenia . Ak to neurčujete, nechajte prázdne.
Heslo	Zadajte heslo pre server LDAP — najviac 128 znakov v kódovaní Unicode (UTF-8). Nemôžete použiť riadiace znaky, ako sú napríklad 0x00 – 0x1F a 0x7F. Toto nastavenie sa nepoužíva, keď je možnosť Anonymná autentifikácia zvolená pre položku Spôsob overenia . Ak to neurčujete, nechajte prázdne.

Nastavenia Kerberos

Ak vyberiete možnosť **Autentifikácia prostredníctvom protokolu Kerberos** pre položku **Spôsob overenia** v ponuke **Server LDAP > Základné**, urobte nasledujúce nastavenia Kerberos na karte **Sieť > Nastavenia Kerberos**. Môžete zaregistrovať až 10 nastavení pre Kerberos.

Položky	Nastavenia a vysvetlenie
Oblasť (Doména)	Zadajte oblasť overovania Kerberos — najviac 255 znakov v kódovaní ASCII (0x20 – 0x7E). Ak to neregistrujete, nechajte prázdne.
Adresa KDC	Zadajte adresu overovacieho servera Kerberos. Zadajte najviac 255 znakov v jednom z týchto formátov: IPv4, IPv6 alebo FQDN. Ak to neregistrujete, nechajte prázdne.
Číslo portu (Kerberos)	Zadajte číslo portu servera Kerberos v rozmedzí od 1 do 65535.

Konfigurácia nastavení vyhľadávania v serveri LDAP

Keď nastavíte vyhľadávanie, môžete používať e-mailovú adresu zaregistrovanú na serveri LDAP.

- Otvorte aplikáciu Web Config a vyberte kartu **Sieť > Server LDAP > Nastavenia vyhľadávania**.
- Zadajte hodnoty pre všetky položky.
- Kliknutím na položku **OK** sa zobrazí výsledok nastavení.
Zobrazia sa nastavenia, ktoré ste vybrali.

Položky nastavenia vyhľadávania v serveri LDAP

Položky	Nastavenia a vysvetlenie
Báza vyhľadávania (odlišujúci názov)	Ak chcete vyhľadávať v ľubovoľnej doméne, zadajte názov domény servera LDAP. Zadajte 0 až 128 znakov v kódovaní Unicode (UTF-8). Ak nechcete vyhľadávať absolútny atribút, nechajte to prázdne. Príklad pre adresár lokálneho servera: dc=server,dc=local
Počet položiek vyhľadávania	Stanovte počet hľadaných položiek od 5 do 500. Určený počet hľadaných položiek sa uloží a dočasne zobrazí. Hoci je počet hľadaných položiek vyšší než stanovený počet a objaví sa hlásenie o chybe, vyhľadávanie môže byť dokončené.

Položky	Nastavenia a vysvetlenie
Atribút Používateľské meno	Stanovte názov atribútu, ktorý sa bude zobrazovať pri vyhľadávaní mena používateľa. Zadaťte 1 až 255 znakov v kódovaní Unicode (UTF-8). Prvý znak musí byť a – z alebo A – Z. Príklad: cn, uid
Atribút zobrazenia používateľského mena	Stanovte názov atribútu, ktorý sa bude zobrazovať ako meno používateľa. Zadaťte 0 až 255 znakov v kódovaní Unicode (UTF-8). Prvý znak musí byť a – z alebo A – Z. Príklad: cn, sn
Atribút E-mailová adresa	Stanovte názov atribútu, ktorý sa bude zobrazovať pri vyhľadávaní e-mailovej adresy. Zadaťte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a -. Prvý znak musí byť a – z alebo A – Z. Príklad: mail
Ľubovoľný atribút 1 - Ľubovoľný atribút 4	Môžete stanoviť ďalšie atribúty, ktoré vyhľadávať. Zadaťte 0 až 255 znakov v kódovaní Unicode (UTF-8). Prvé znaky by mali byť a – z alebo A – Z. Ak nechcete vyhľadávať ľubovoľné atribúty, nechajte túto položku prázdnu. Príklad: o, ou

Kontrola pripojenia servera LDAP

Vykonáva test pripojenia k serveru LDAP pomocou parametra nastaveného v ponuke **Server LDAP > Nastavenia vyhľadávania**.

- Otvorte aplikáciu Web Config a vyberte kartu **Sieť > Server LDAP > Test pripojenia**.
- Vyberte položku **Spustiť**.
Začal sa test pripojenia. Po teste skontrolujte zobrazenú správu.

Správy testu pripojenia servera LDAP

Hlásenia	Vysvetlenie
Test pripojenia bol úspešný.	Toto hlásenie sa zobrazí, ak bolo pripojenie k serveru úspešné.
Test pripojenia zlyhal. Skontrolujte nastavenia.	Toto hlásenie sa objaví z nasledujúcich dôvodov: <ul style="list-style-type: none"> <input type="checkbox"/> Adresa servera LDAP alebo číslo portu sú nesprávne. <input type="checkbox"/> Vypršal časový limit. <input type="checkbox"/> Je zvolená možnosť Nepoužívajte pre položku Použiť server LDAP. <input type="checkbox"/> Ak je možnosť Autentifikácia prostredníctvom protokolu Kerberos zvolená pre položku Spôsob overenia, nastavenia (ako sú napríklad Oblasť (Doména), Adresa KDC a Číslo portu (Kerberos)) sú nesprávne.
Test pripojenia zlyhal. Skontrolujte Dátum a čas na vašom zariadení alebo serveri.	Toto hlásenie sa zobrazí, keď pripojenie zlyhá z dôvodu nezhody nastavení času skenera a servera LDAP.

Hlásenia	Vysvetlenie
Autentifikácia zlyhala. Skontrolujte nastavenia.	Toto hlásenie sa objaví z nasledujúcich dôvodov: <input type="checkbox"/> Položka Názov používateľa a/alebo Heslo je nesprávna. <input type="checkbox"/> Ak je zvolená možnosť Autentifikácia prostredníctvom protokolu Kerberos pre položku Spôsob overenia , čas/dátum možno nie je nakonfigurované.
K výrobku nemožno získať prístup, kým nebude dokončené spracovanie.	Toto hlásenie sa objaví, keď je skener zaneprázdnený.

Nastavenie funkcie AirPrint

Otvorte aplikáciu Web Config, vyberte kartu **Sieť** a vyberte možnosť **Nastavenie aplikácie AirPrint**.

Položky	Vysvetlenie
Servisný názov Bonjour	Zadajte názov služby Bonjour. Použiť môžete text vo formáte ASCII (0x20 – 0x7E) a najviac 41 znakov.
Miesto Bonjour	Zadajte popis umiestnenia skenera. Použiť môžete text v kódovaní Unicode (UTF-8) a najviac 127 bajtov.
Wide-Area Bonjour	Nastavenie, či sa má alebo nemá používať Wide-Area Bonjour. Ak ho použijete, skener musí byť zaregistrovaný na serveri DNS, aby sa skener dal vyhľadať v segmente.
Povoliť AirPrint	Povolí Bonjour a AirPrint (služba skenovania). Toto tlačidlo je k dispozícii len vtedy, keď je funkcia AirPrint vypnutá. Poznámka: <i>Mopria Ak je vypnutá funkcia AirPrint, je vypnuté aj skenovanie z počítačov Chromebook, Windows a aplikácia Mopria Scan.</i>

Problémy pri príprave skenovanie cez sieť

Pomôcky k riešeniu problémov

Kontrola hlásenia o chybe

Keď sa vyskytne problém, najprv skontrolujte, či na ovládacom paneli skenera alebo na obrazovke ovládača nie sú nejaké hlásenia. Ak máte nastavené upozornenie e-mailom pri výskyte chyby, môžete mať okamžité prehľad o stave.

Kontrola stavu komunikácie

Skontrolujte stav komunikácie serverového počítača alebo klientskeho počítača pomocou príkazu, ako sú napríklad ping a ipconfig.

Test pripojenia

Na kontrolu pripojenia medzi skenerom a poštovým serverom, vykonajte test pripojenia zo skenera. Rovnako aj skontrolujte pripojenie z klientskeho počítača k serveru a overte tak stav komunikácie.

Inicializácia nastavení

Ak sa v nastaveniach a stave komunikácie nejaví žiadny problém, problémy sa dajú vyriešiť zakázaním alebo inicializáciou sieťových nastavení skenera a potom opätovným nastavením.

Nedá sa otvoriť aplikácia Web Config

Skeneru nie je priradená IP adresa.

Riešenia

Skeneru možno nie je priradená platná IP adresa. Nakonfigurujte IP adresu pomocou ovládacieho panela skenera. Aktuálne nastavenie môžete skontrolovať pomocou ovládacieho panela skenera.

Webový prehľadávač nepodporuje silu šifrovania pre protokol SSL/TLS.

Riešenia

Protokol SSL/TLS má funkciu Sila šifrovania. Aplikáciu Web Config môžete otvoriť pomocou webového prehľadávača, ktorý podporuje dávkové šifrovanie, ako je uvedené ďalej. Skontrolujte, či používate podporovaný prehľadávač.

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

Uplynula platnosť CA-podpísaný Certifikát.

Riešenia

Ak je problém s uplynutím platnosti dátumu certifikátu, zobrazuje sa pri pripájaní k aplikácii Web Config cez protokol SSL/TLS (https) hlásenie „Platnosť certifikátu uplynula“. Ak sa hlásenie objavuje pred uplynutím jeho platnosti, uistite sa, či je správne nakonfigurovaný dátum na skeneri.

Všeobecný názov certifikátu a skenera sa nezhodujú.

Riešenia

Ak sa všeobecný názov certifikátu a skenera nezhodujú, pri otváraní aplikácie Web Config pomocou komunikácie SSL/TLS (https) sa zobrazuje hlásenie „Názov bezpečnostného certifikátu sa nezhoduje...“. Dochádza k tomu, pretože sa nezhodujú nasledujúce IP adresy.

- IP adresa skenera zadaná do všeobecného názvu pre vytvorenie položky Certifikát s vlastným podpisom alebo CSR.
- IP adresa zadaná do webového prehľadávača pri spustenej aplikácii Web Config

Pri položke Certifikát s vlastným podpisom aktualizujte certifikát.

Pre položku CA-podpísaný Certifikát znova získajte certifikát pre skener.

Vo webovom prehľadávači nie je nastavená položka nastavenia servera proxy lokálnej adresy.

Riešenia

Keď je na skeneri nastavené používanie servera proxy, nakonfigurujte webový prehľadávač tak, aby sa nepripájal k lokálnej adrese cez server proxy.

Windows:

Vyberte ponuku **Ovládací panel > Sieť a internet > Možnosti internetu > Pripojenia > Nastavenie siete LAN > Server proxy** a nakonfigurujte, aby sa nepoužíval server proxy pre sieť LAN (lokálne adresy).

Mac OS:

Vyberte ponuky **Preferencie systému > (alebo Systémové nastavenia) > Sieť > Rozšírené > Servery proxy** a potom zaregistrujte lokálnu adresu pre funkciu **Obísť nastavenia servera 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

DHCP je v nastaveniach počítača zakázané.

Riešenia

Ak je na počítači zakázaná funkcia DHCP na automatické získanie IP adresy, nie je možný prístup do aplikácie Web Config. Povoľte funkciu DHCP.

Príklad pre systém Windows 10:

Otvorte Ovládací panel a kliknite na položky **Sieť a internet > Centrum sietí a zdieľania > Zmeniť nastavenie adaptéra**. Otvorte obrazovku Vlastnosti pre používané pripojenie a otvorte obrazovku vlastností pre **Internetový protokol verzia 4 (TCP/IPv4)** alebo **Internetový protokol verzia 6 (TCP/IPv6)**. Skontrolujte, či je na zobrazenej obrazovke začiarknutá možnosť **Získať IP adresu automaticky**.

Prispôsobenie zobrazenia ovládacieho panela


Registrácia položky Predv. hod.. 68

Úprava hlavnej obrazovky ovládacieho panela. 70

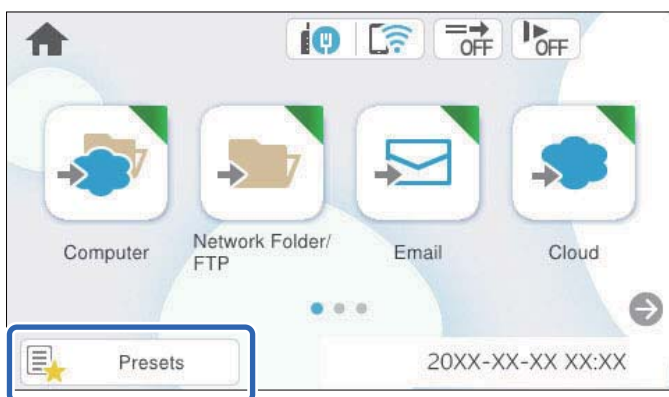
Registrácia položky Predv. hod.


Môžete zaregistrovať často používané nastavenia skenovania ako **Predv. hod.**. Môžete zaregistrovať až 48 predvolieb.

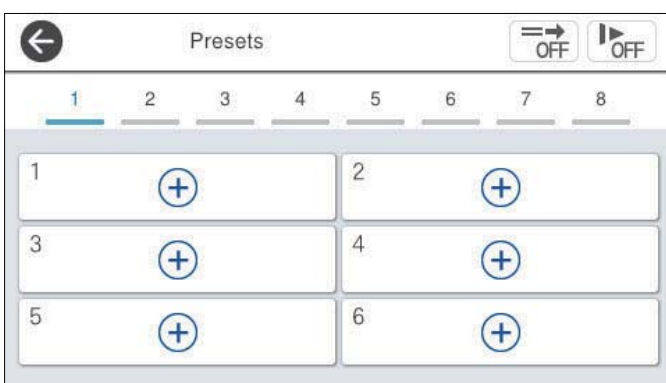
Poznámka:

- Aktuálne nastavenia môžete zaregistrovať voľbou položky  na obrazovke spustenia skenovania.
- Predvolené hodnoty** môžete zaregistrovať aj v aplikácii Web Config.
Vyberte kartu **Skenov.** > **Predvolené hodnoty**.
- Ak pri registrácii vyberiete možnosť **Skenovať do počítača**, môžete zaregistrovať úlohu vytvorenú v aplikácii Document Capture Pro ako **Predvolené hodnoty**. To je k dispozícii len pre počítače pripojené cez sieť. Zaregistrujte najprv úlohu v aplikácii Document Capture Pro.
- Ak je funkcia overovania povolená, len správca môže registrovať položku **Predvolené hodnoty**.

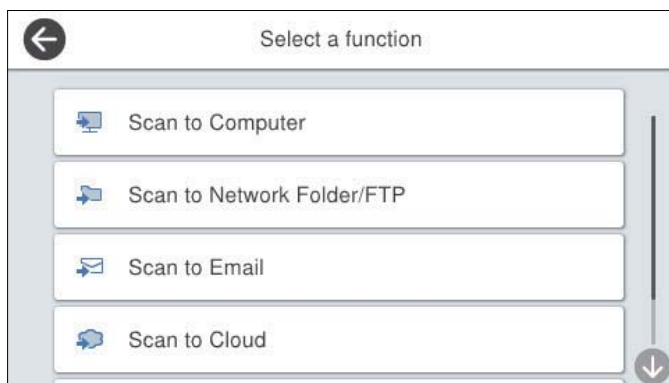
1. Vyberte položku **Predv. hod.** na hlavnej obrazovke na ovládacom paneli skenera.



2. Vyberte položku .



3. Vyberte ponuku, ktorú chcete zaregistrovať ako predvoľbu.



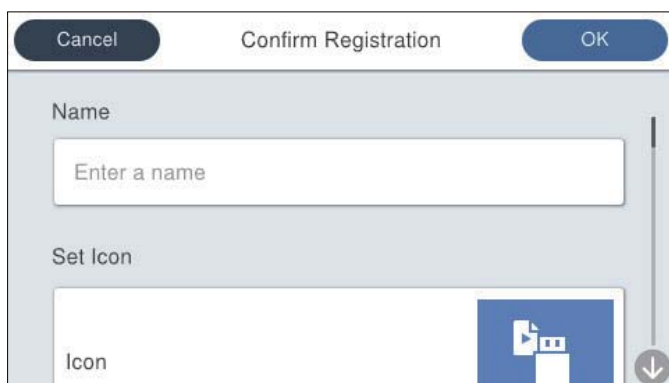
4. Nastavte jednotlivé položky a vyberte položku .

Poznámka:

Keď vyberiete možnosť **Skenovať do počítača**, vyberte počítač s nainštalovaným programom Document Capture Pro a potom vyberte zaregistrovanú úlohu. To je k dispozícii len pre počítače pripojené cez sieť.


5. Urobte nastavenia predvoľby.

- Názov:** Nastavte názov.
- Nastavená Ikona:** Nastavte obrázok a farbu ikony, ktorú chcete zobraziť.
- Nastavenie položky Rýchlo odoslať:** Keď sa zvolí táto predvoľba, okamžite sa spustí skenovanie bez potvrdzovania.
- Obsah:** Skontrolujte nastavenia skenovania.



6. Vyberte položku **OK**.

Možnosti ponuky Predv. hod.

Pomocou položky  v jednotlivých predvoľbách môžete zmeniť nastavenia.

Zmeniť Názov:

Zmena názvu predvoľby.

Zmeniť Ikonu:

Zmena obrázka ikony a farby predvoľby.

Nastavenie položky Rýchlo odoslať:

Keď sa zvolí táto predvoľba, okamžite sa spustí skenovanie bez potvrdzovania.

Zmeniť umiestnenie:

Zmena poradia zobrazovania predvoľieb.

Odstrániť:

Odstránenie predvoľby.

Pridať alebo odstrániť Ikonu z obrazovky Domov:

Pridanie alebo odstránenie ikony predvoľby z hlavnej obrazovky.

Potvrdiť podrobnosti:

Zobrazenie nastavení predvoľby. Predvoľbu môžete načítať cez položku **Použiť toto nastavenie**.

Úprava hlavnej obrazovky ovládacieho panela

Hlavnú obrazovku si môžete prispôbiť cez ponuku **Nastav. > Upraviť domovskú obrazovku** na ovládacom paneli skenera.

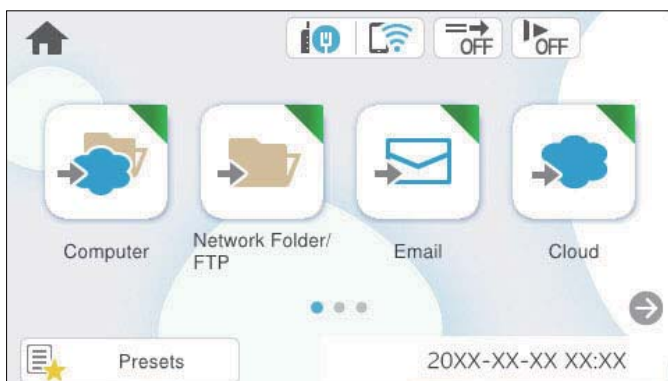
- Usporiadanie:** Zmena spôsobu zobrazovania ikon ponuky.
[„Zmena položky Usporiadanie na hlavnej obrazovke” na strane 70](#)
- Pridať ikonu:** Pridáva ikony do nastavenia **Predv. hod.**, ktoré ste vytvorili, prípadne slúži na obnovenie ikon odstránených z obrazovky.
[„Pridať ikonu” na strane 71](#)
- Odstrániť ikonu:** Odstraňuje ikony z hlavnej obrazovky.
[„Odstrániť ikonu” na strane 72](#)
- Presunúť ikonu:** Zmena poradia zobrazovania ikon.
[„Presunúť ikonu” na strane 73](#)
- Obnoviť predvolené zobrazenie ikon:** Slúži na obnovenie predvoleného nastavenia zobrazenia hlavnej obrazovky.

Zmena položky Usporiadanie na hlavnej obrazovke

1. Na ovládacom paneli skenera vyberte položky **Nastav. > Upraviť domovskú obrazovku > Usporiadanie**.


2. Vyberte možnosť **Riadok** alebo **Matica**.

Riadok:



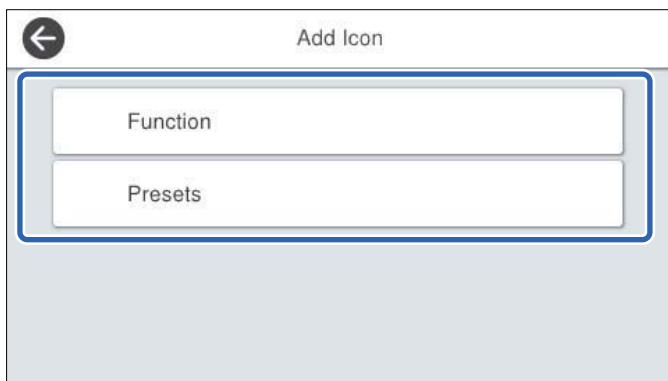
Matica:



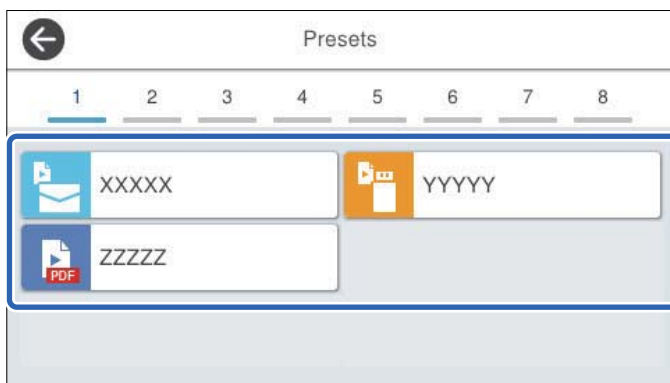
3. Položkou  sa vrátite a skontrolujte hlavnú obrazovku.

Pridať ikonu

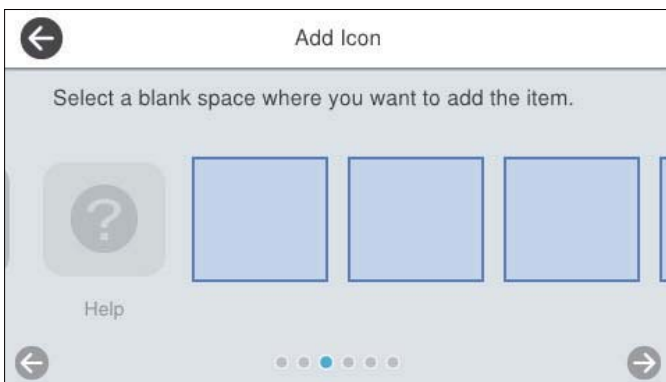
1. Na ovládacom paneli skenera vyberte položky **Nastav.** > **Upraviť domovskú obrazovku** > **Pridať ikonu**.
2. Vyberte možnosť **Funkcia** alebo **Predv. hod.**.
 - Funkcia:** Zobrazuje predvolené funkcie znázornené na hlavnej obrazovke.
 - Predv. hod.:** Zobrazuje zaregistrované predvoľby.




3. Vyberte položku, ktorú chcete pridať na hlavnú obrazovku.



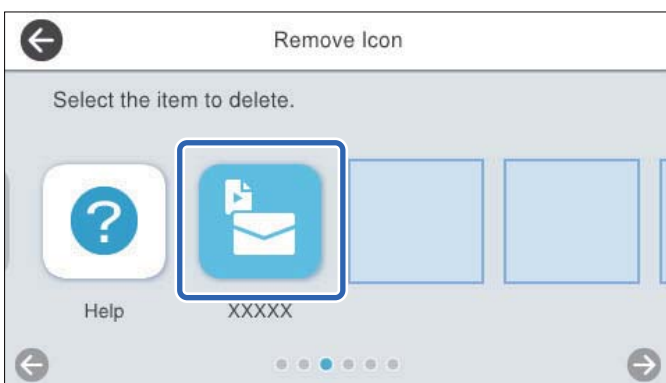
4. Vyberte prázdne miesto, kam chcete položku pridať.
Ak chcete pridať viac ikon, opakujte kroky 3 až 4.




5. Položkou  sa vrátite a skontrolujete hlavnú obrazovku.

Odstrániť ikonu

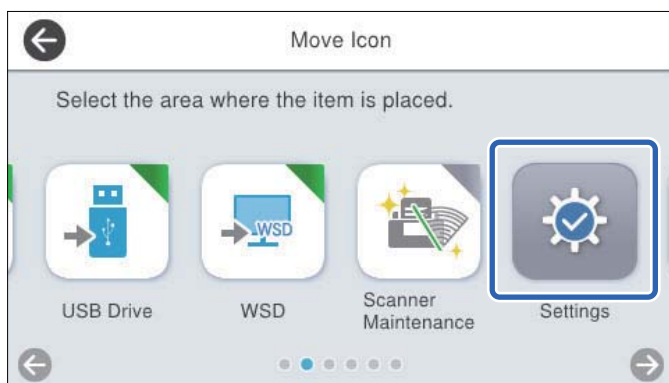
1. Na ovládacom paneli skenera vyberte položky **Nastav.** > **Upraviť domovskú obrazovku** > **Odstrániť ikonu.**
2. Vyberte ikonu, ktorú chcete odstrániť.



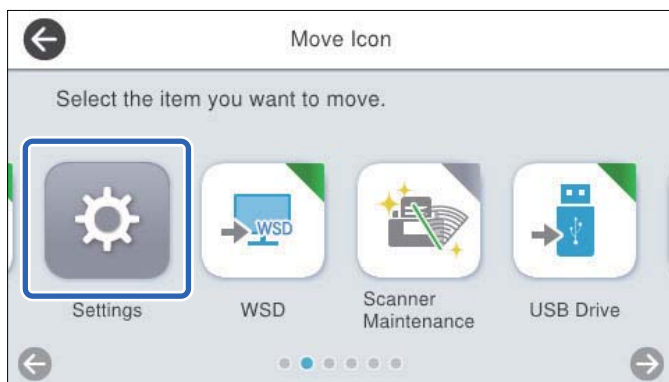
3. Pre dokončenie vyberte položku **Áno**.
Ak chcete odstrániť viac ikon, opakujte postup 2 až 3.
4. Položkou  sa vráťte a skontrolujte hlavnú obrazovku.


Presunúť ikonu

1. Na ovládacom paneli skenera vyberte položky **Nastav.** > **Upraviť domovskú obrazovku** > **Presunúť ikonu**.
2. Vyberte ikonu, ktorú chcete presunúť.



3. Vyberte cieľový rámček.
Ak je už pre cieľový rámček nastavená iná ikona, ikony sa nahradia.



4. Položkou  sa vráťte a skontrolujte hlavnú obrazovku.

Základné nastavenia zabezpečenia

Predstavenie funkcií zabezpečenia výrobku.	75
Nastavenia správcu.	75
Obmedzenie dostupných funkcií (Riadenie prístupu).	81
Zakázanie externého rozhrania.	83
Povolenie funkcie Overenie programu pri spustení.	83
Zakázanie sieťového skenovania v počítači.	84
Povolenie alebo zakázanie skenovania WSD.	84
Monitorovanie vzdialeného skenera.	85
Obnovenie predvolených nastavení.	86
Informácie o službe Epson Remote Services.	87
Riešenie problémov.	87

Predstavenie funkcií zabezpečenia výrobu

V tejto časti vám predstavíme funkciu zabezpečenia zariadení Epson.

Názov funkcie	Typ funkcie	Čo nastavíte	Čomu zabránite
Konfigurácia hesla správcu	Zablokujú sa nastavenia systému, ako je napríklad nastavenie pripojenia k sieti alebo USB.	Administrátor nastaví heslo k zariadeniu. Môžete ho nastaviť alebo zmeniť z aplikácie Web Config aj z ovládacieho panela skenera.	Chráni pred nezákonným čítaním a zmenou údajov uložených v zariadení, ako sú napríklad ID, heslo, nastavenia siete a podobne. Redukuje aj širokú paletu bezpečnostných rizík, ako je napríklad únik údajov pre sieťové prostredie alebo bezpečnostné zásady.
Nastavenia riadenia prístupu	Ak sa do zariadenia prihlásite pomocou vopred zaregistrovaného používateľského účtu, môžete zariadenie používať.	Zaregistrujte ľubovoľný používateľský účet. Môžete zaregistrovať až 10 používateľských kont.	Obmedzenie používateľov zabraňuje neoprávnenému používaniu zariadenia.
Nastavenie pre externé rozhranie	Riadi rozhranie, ktorým sa pripája k zariadeniu.	Povoľte alebo zakážete USB pripojenie k počítaču.	USB pripojenie počítača: zabraňuje nepovolenému použitiu zariadenia prostredníctvom zakázania skenovania bez prístupu cez sieť.

Súvisiace informácie

- ➔ „Konfigurácia hesla správcu” na strane 75
- ➔ „Zakázanie externého rozhrania” na strane 83

Nastavenia správcu

Konfigurácia hesla správcu

Keď nastavíte heslo správcu, môžete zabrániť používateľom meniť nastavenia riadenia systému. Predvolené hodnoty sú nastavené pri zakúpení. V prípade potreby ich zmeňte.

Poznámka:

Nasledujúce informácie poskytujú predvolené hodnoty pre údaje správcu.

- Používateľské meno (používa sa len pre aplikáciu Web Config): žiadne (prázdne)
- Heslo: závisí od štítku pripevneného na výrobku.

Ak je na zadnej strane pripevnený štítok „PASSWORD“, zadajte 8-miestne číslo uvedené na štítku. Ak nie je pripevnený štítok „PASSWORD“, zadajte ako prvotné heslo správcu sériové číslo na štítku pripevnenom na zadnej strane výrobu.

Heslo správcu môžete zmeniť pomocou aplikácie Web Config, na ovládacom paneli skenera alebo cez aplikáciu Epson Device Admin. Keď používate aplikáciu Epson Device Admin, pozrite príručku Epson Device Admin alebo Pomocníka.

Zmena hesla správcu pomocou aplikácie Web Config

Zmeňte heslo správcu v aplikácii Web Config.

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie produktu > Zmeniť Heslo správcu**.
2. Zadajte potrebné údaje do položiek **Aktuálne heslo**, **Názov používateľa**, **Nové heslo** a **Potvrďte nové heslo**.
Nové heslo musí mať 8 až 20 znakov a môže obsahovať iba jednobajtové alfanumerické znaky a symboly.

Poznámka:

Nasledujúce informácie poskytujú predvolené hodnoty pre údaje správcu.

- Používateľské meno: žiadne (prázdne)*
- Heslo: závisí od štítka pripevneného na výrobku.*

Ak je na zadnej strane pripevnený štítok „PASSWORD“, zadajte 8-miestne číslo uvedené na štítku. Ak nie je pripevnený štítok „PASSWORD“, zadajte ako prvotné heslo správcu sériové číslo na štítku pripevnenom na zadnej strane výrobku.



Upozornenie:

Nezabudnite si zapamätať nastavené heslo správcu. Ak zabudnete heslo, nebudete ho môcť obnoviť a budete musieť požiadať o pomoc servisný personál.

3. Vyberte položku **OK**.

Súvisiace informácie

➔ [„Ako spustiť funkciu Web Config v internetovom prehliadači“](#) na strane 37

Zmena hesla správcu z ovládacieho panela skenera

Heslo správcu môžete zmeniť z ovládacieho panela skenera.

1. Na ovládacom paneli skenera vyberte možnosť **Nastav.**
2. Vyberte položky **Správa systému > Nastavenia správy**.
3. Vyberte položky **Heslo správcu > Zmeniť**.
4. Zadajte aktuálne heslo.

Poznámka:

Prvotné heslo správcu (predvolené) v čase zakúpenia sa líši v závislosti od štítka pripevneného na výrobku. Ak je na zadnej strane pripevnený štítok „PASSWORD“, zadajte 8-miestne číslo uvedené na štítku. Ak nie je pripevnený štítok „PASSWORD“, zadajte ako prvotné heslo správcu sériové číslo na štítku pripevnenom na zadnej strane výrobku.

5. Zadajte nové heslo.

Nové heslo musí mať 8 až 20 znakov a môže obsahovať iba jednobajtové alfanumerické znaky a symboly.



Upozornenie:

Nezabudnite si zapamätať nastavené heslo správcu. Ak zabudnete heslo, nebudete ho môcť obnoviť a budete musieť požiadať o pomoc servisný personál.



6. Potvrďte opätovným zadaním nového hesla.

Zobrazí sa správa o vytvorení.

Používanie funkcie Nastavenie zámku pre ovládací panel

Funkciu Nastavenie zámku môžete použiť na uzamknutie ovládacieho panela, aby ste zabránili používateľom v zmene položiek týkajúcich sa nastavenia systému.

Nastavenie možnosti Nastavenie zámku z ovládacieho panela

1. Ak chcete zrušiť nastavenie **Nastavenie zámku** po tom, čo bolo povolené, ťuknite v pravom hornom rohu hlavnej obrazovky na položku  a prihláste sa ako správca.
 sa nezobrazuje, keď je možnosť **Nastavenie zámku** zakázaná. Ak chcete povoliť toto nastavenie, prejdite na ďalší krok.
2. Vyberte položku **Nastav.**
3. Vyberte položky **Správa systému > Nastavenia správy**.
4. Vyberte možnosť **Zap.** alebo **Vyp.** pre nastavenie **Nastavenie zámku**.

Nastavenie položky Nastavenie zámku z aplikácie Web Config

1. Vyberte kartu **Správa zariadenia > Ovládací panel**.
2. Vyberte možnosť **Zap.** alebo **Vyp.** pre **Uzamknutie panela**.
3. Kliknite na položku **OK**.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Položky Nastavenie zámku v ponuke Nastav.

Toto je zoznam položiek, ktoré sú v ponuke **Nastav.** na ovládacom paneli zamknuté pomocou Nastavenie zámku.


✓: bude uzamknuté.

- : nebude uzamknuté.

Ponuka Nastav.	Nastavenie zámku
Zákl. nastavenia	-

Ponuka Nastav.		Nastavenie zámku
	Jas LCD displeja	–
	Zvuky	–
	Časovač režimu spánku	✓
	Časovač vypnutia	✓
	Priame zapnutie	✓
	Nastavenia dátumu/času	✓
	Jazyk/Language	✓/!-*
	Klávesnica (V závislosti od oblasti nemusí byť táto funkcia k dispozícii.)	–
	Časový limit prevádzky	✓
	Pripojenie PC pomocou USB	✓
Nastavenia skenera		–
	Pomaly	–
	Časovanie zas. pri dvojitom podávaní	✓
	Funkcia DFDS	–
	Ochrana papiera	✓
	Zisťovanie znečistenia skla	✓
	Ultrazv. zisťovanie dvojitého pod.	✓
	Časový limit Režim automatického podávania	✓
	Potvrdiť príjemcu	✓
Upraviť domovskú obrazovku		✓
	Usporiadanie	✓
	Pridať ikonu	✓
	Odstrániť ikonu	✓
	Presunúť ikonu	✓
	Obnoviť predvolené zobrazenie ikon	✓
Používateľské nastavenia		✓
	Sieťový prieč./FTP	✓
	E-mail	✓
	Cloud	✓
	USB jednotka	✓
Nastavenie siete		✓

Ponuka Nastav.		Nastavenie zámku
	Nastavenie Wi-Fi	✓
	Nastavenie drôtovej siete LAN	✓
	Stav siete	✓
	Rozšírené	✓
Nastavenia webovej služby		✓
	Služby Epson Connect	✓
Document Capture Pro		-
	Zmeniť nastavenia	✓
Správa kontaktov		-
	Zaregistrovať/Odstrániť	✓/!*
	Najčastejšie používané	-
	Zobraziť možnosti	-
	Možnosti hľadania	-
Správa systému		✓
	Správa kontaktov	✓
	Nastavenia správy	✓
	Obmedzenia	✓
	Riadenie prístupu	✓
	Šifrovanie hesla	✓
	Zákaznícky prieskum	✓
	Nastavenia WSD	✓
	Obnoviť štand. nastavenia	✓
	Aktualizácia firmvéru	✓
Informácie o zariadení		-

Ponuka Nastav.		Nastavenie zámku
	Sériové číslo	–
	Aktuálna verzia	–
	Celkový počet skenovaní	–
	Počet jednostr. skenovaní	–
	Počet obojstr. skenovaní	–
	Počet skenov. držiaka na hárky	–
	Počet skenov po výmene valčeka	–
	Počet skenov po Pravid. čistení	–
	Stav overenia zariadenia	–
	Informácie o Epson Open Platform	–
	 (Vynulovať počet skenovaní)	✓
Údržba skenera		–
	Čistenie valčekov	–
	Výmena servisných valčekov	–
	Vynulovať počet skenovaní	✓
	Ako vymeniť	–
	Pravidelné čistenie	–
	Vynulovať počet skenovaní	✓
	Spôsob čistenia	–
	Čistenie skla	–
Nastavenie upozornenia na výmenu valca		✓
	Nastave počtu upozorn	✓
Nastavenie upozornenia na pravidelné čistenie		✓
	Nastavenie výstr. upozornenia	✓
	Nastave počtu upozorn	✓

* Môžete nastaviť, či majú byť povolené zmeny v ponuke **Správa systému > Obmedzenia**.

Prihlásenie správcu z ovládacieho panela

Keď je povolená funkcia **Nastavenie zámku**, môžete použiť niektorý z nasledujúcich spôsobov prihlásenia z ovládacieho panela skenera.

1. Ťuknite na položku  vpravo hore na obrazovke.

2. Keď sa zobrazí obrazovka **Zvoľte používateľa**, vyberte možnosť **Správca**.

3. Zadajte heslo na prihlásenie.

Zobrazí sa hlásenie o dokončení prihláseniam, a potom sa na ovládacom paneli zobrazí hlavná obrazovka.

Ak sa chcete odhlásiť, ťuknite na položku  v pravom hornom rohu obrazovky alebo stlačte tlačidlo .

Obmedzenie dostupných funkcií (Riadenie prístupu)

Používateľov môžete obmedziť registráciou používateľských účtov na skeneri.

Keď je aktivovaná stránka Riadenie prístupu, používateľ môže používať funkcie skenovania zadaním hesla na ovládacom paneli skenera a prihlásením sa. Ak sa neprihlásite, nemôžete skenovať.

Skenovať z počítača môžete tak, že zaregistrujete svoje Uživatelské meno a Heslo v ovládači skenera (Epson Scan 2). Pozrite si pomocníka Epson Scan 2 alebo v *Používateľská príručka* výrobku, kde nájdete viac informácií o nastaveniach.

Vytvorenie používateľského konta

Môžete si vytvoriť účet Riadenie prístupu.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie produktu** > **Nastavenia riadenia prístupu** > **Nastavenia používateľa**.
2. Kliknite na možnosť **Pridať** pre číslo, ktoré chcete zaregistrovať.



Upozornenie:

*Pri používaní skenera s overovacím systémom od spoločnosti Epson alebo inej spoločnosti zaregistrujte položku **Názov používateľa** v časti **Nastavenia riadenia prístupu** v sloty číslo 2 až 10.*

Aplikačný softvér, ako je napríklad systém overovania, používa slot číslo jeden, takže meno používateľa sa nezobrazuje na ovládacom paneli tlačiarne.

3. Nastavte jednotlivé položky.

Názov používateľa:

Zadajte meno zobrazené v zozname používateľov. Použite 1 až 14 abecedných a číselných znakov.

Heslo:

Zadajte heslo, použite najviac 20 znakov ASCII (0x20 – 0x7E). Pri inicializácii hesla ho nechajte prázdne.

Na zapnutie/vypnutie každej funkcie zaškrtnite začiarkavacie políčko.

Vyberte možnosť **Skenov.**, ak chcete povoliť funkcie skenovania.

4. Kliknite na položku **Použiť**.

Úprava používateľského účtu

Zaregistrovaný účet Riadenie prístupu môžete upraviť.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie produktu > Nastavenia riadenia prístupu > Nastavenia používateľa**.
2. Kliknite na možnosť **Upraviť** pre číslo, ktoré chcete upraviť.
3. Zmeňte jednotlivé položky.
4. Kliknite na tlačidlo **Použiť**.

Odstránenie používateľského účtu

Zaregistrovaný účet Riadenie prístupu môžete vymazať.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie produktu > Nastavenia riadenia prístupu > Nastavenia používateľa**.
2. Kliknite na možnosť **Upraviť** pre číslo, ktoré chcete odstrániť.
3. Kliknite na tlačidlo **Odstrániť**.



Upozornenie:

Keď kliknete na možnosť **Odstrániť**, používateľský účet sa odstráni bez potvrdzovacieho hlásenia. Pri odstraňovaní účtu dávajte pozor.

Povolenie funkcie Riadenie prístupu

Keď aktivujete funkciu Riadenie prístupu, skener môže využívať len registrovaný používateľ.


Poznámka:

Keď je povolená položka *Nastavenia riadenia prístupu*, je potrebné používateľovi oznámiť údaje o jeho účte.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie produktu > Nastavenia riadenia prístupu > Základné**.
2. Vyberte položku **Aktivuje kontrolu prístupu**.
Ak povolíte možnosť *Nastavenia riadenia prístupu* a skenovanie z počítača, ktorý nemá overovacie informácie, vyberte možnosť **Povolíť tlač a skenovanie bez overovacích informácií z počítača**.
3. Kliknite na položku **OK**.

Prihlásenie do skenera, na ktorom je povolená funkcia Riadenie prístupu

Keď je povolená funkcia **Riadenie prístupu**, môžete použiť niektorý z nasledujúcich spôsobov prihlásenia z ovládacieho panela skenera.

1. Ťuknite na položku  vpravo hore na obrazovke.
2. Ak sa zobrazí obrazovka **Zvoľte používateľa**, vyberte používateľa.

3. Zadajte heslo na prihlásenie.

Zobrazí sa hlásenie o dokončení prihláseniam, a potom sa na ovládacom paneli zobrazí hlavná obrazovka.

Ak sa chcete odhlásiť, ťuknite na položku  v pravom hornom rohu obrazovky alebo stlačte tlačidlo .

Zakázanie externého rozhrania

Môžete zakázať rozhranie, ktoré sa používa na pripojenie zariadenia k skeneru. Urobte nastavenia obmedzenia, ak chcete obmedziť skenovanie iným spôsobom než cez sieť.

Poznámka:

Nastavenia obmedzenia môžete urobiť aj na ovládacom paneli skenera.

Pripojenie PC pomocou USB: **Nastav.** > **Zákl. nastavenia** > **Pripojenie PC pomocou USB**

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie produktu** > **Externé rozhranie**.

2. Vyberte možnosť **Zakázať** pri funkciách, ktoré chcete nastaviť.

Vyberte možnosť **Povoliť**, ak chcete zrušiť ovládanie.

Pripojenie PC pomocou USB

Môžete obmedziť využívanie pripojenie cez USB z počítača. Ak ho chcete obmedziť, vyberte možnosť **Zakázať**.

3. Kliknite na položku **OK**.

4. Skontrolujte, či sa zakázaný port nedá použiť.

Pripojenie PC pomocou USB

Ak bol do počítača nainštalovaný ovládač

Pripojte skener k počítaču pomocou kábla USB, a potom skontrolujte, či skener neskenuje.

Ak nebol do počítača nainštalovaný ovládač

Windows:

Otvorte správca zariadení a nechajte ho otvorený. Pripojte skener k počítaču káblom USB a skontrolujte, či zostal správca zariadení nezmenený.

Mac OS:

Pripojte skener k počítaču pomocou kábla USB a skontrolujte, či sa skener nedá pridať cez funkciu **Tlačiarne a skenery**.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Povolenie funkcie Overenie programu pri spustení

Ak povolíte funkciu Overenie programu, skener pri spustení vykoná overenie, aby skontrolovala, či s programom nemanipulovali neoprávnené tretie strany. Ak sa zistia nejaké problémy, skener sa nespustí.

Poznámka:

Aktivácia tejto funkcie predlžuje čas spustenia skenera.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie produktu > Overenie programu pri spustení**.

Poznámka:

Nastavenia môžete urobiť aj na ovládacom paneli skenera.

Nastav. > **Správa systému** > **Overenie programu pri spustení**

2. Vyberte možnosť **Zap.**, ak chcete povoliť funkciu **Overenie programu pri spustení**.
3. Kliknite na tlačidlo **OK**.

Zakázanie sieťového skenovania v počítači

Na stránke Web Config môžete vykonať nasledujúce nastavenia, aby ste zakázali skenovanie siete pomocou stránky Epson Scan 2 z vášho počítača.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Skenov.** > **Skenovanie cez sieť**.
2. V položke **Epson Scan 2**, zrušte začiarknutie políčka **Zapnúť skenovanie**.
3. Kliknite na tlačidlo **Ďalej**.
Zobrazí sa obrazovka s potvrdením nastavenia.
4. Kliknite na tlačidlo **OK**.

Povolenie alebo zakázanie skenovania WSD

Poznámka:

Nastavenia môžete urobiť aj na ovládacom paneli skenera. Vyberte položky **Nastav.** > **Správa systému** > **Nastavenia WSD**.

Skenovanie WSD môžete povoliť alebo zakázať.

Ak nechcete, aby počítač nakonfiguroval skener ako skenovacie zariadenie WSD, vypnite nastavenia WSD.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie siete** > **Protokol**.
2. V položke **Nastavenia WSD** zmeňte začiarkavacie políčko **Zapnúť WSD**.
3. Kliknite na položku **Ďalej**.
Zobrazí sa obrazovka s potvrdením nastavenia.
4. Kliknite na tlačidlo **OK**.

Poznámka:

Ak počítač stále konfiguruje skener ako skenovacie zariadenie WSD, vyberte kartu **Skenov.** > **Skenovanie cez sieť**, a potom zrušte zaškrtnutie políčka **Zapnúť skenovanie** začiarkavacie políčko na stránke **AirPrint**.

Mopria Ak je vypnutá funkcia AirPrint, je vypnuté aj skenovanie z počítačov Chromebook, Windows a aplikácia Mopria Scan.

Monitorovanie vzdialeného skenera

Overenie údajov pre vzdialený skener

V položke **Stav** pomocou aplikácie Web Config môžete overiť nasledujúce informácie o používanom skeneri.

- Stav výrobku
Skontrolujte stav, cloudovú službu, číslo výrobku, adresu MAC atď.
- Stav siete
Skontrolujte informácie o stave sieťového pripojenia, IP adresu, server DNS atď.
- Stav využitia
Skontrolujte prvý deň skenovania, počet skenovaní atď.
- Stav hardvéru
Skontrolujte stav jednotlivých funkcií skenera.
- Snímka panela
Zobrazuje snímku obrazovky, ktorá sa zobrazuje na ovládacom paneli skenera.

Prijímanie emailových oznámení pri výskyte udalostí

Čo sú e-mailové upozornenia

Je to funkcia upozorňovania, ktorá na určenú adresu odošle e-mail, keď sa vyskytne udalosť, napríklad zastavenie skenovania a chyba skenera.

Môžete zaregistrovať najviac päť cieľov a pre jednotlivé ciele určiť nastavenia upozornenia.

Ak chcete používať túto funkciu, je pred nastavením upozornení potrebné nastaviť poštový server.

Súvisiace informácie

➔ [„Registrácia e-mailového servera” na strane 44](#)

Konfigurácia e-mailového upozornenia

Nakonfigurujte e-mailové upozornenie pomocou aplikácie Web Config.

1. Otvorte aplikáciu Web Config a vyberte kartu **Správa zariadenia > E-mailové upozornenie**.
2. Nastavte predmet e-mailového upozornenia.
Z dvoch rozbaľovacích ponúk vyberte obsah zobrazený v predmete.
 - Vybraný obsah sa zobrazuje vedľa položky **Predmet**.
 - Rovnaký obsah nie je možné nastaviť na ľavú a pravú stranu.
 - Keď počet znakov v položke **Umiestnenie** prekračuje 32 bajtov, znaky nad 32 bajtov sa vynechajú.

3. Zadaťte e-mailovú adresu na odosielanie e-mailového upozornenia.
Použite znaky A – Z a – z 0 – 9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @. Môžete zadať 1 až 255 znakov.
4. Vyberte jazyk pre e-mailové upozornenia.
5. Začiarknite políčko pri udalosti, pre ktorú chcete prijímať upozornenie.
Číslo položky **Nastavenia upozornení** je prepojené na číslo cieľa v položke **Nastavenia e-mailovej adresy**.
Príklad:
Ak chcete odosielať upozornenie na e-mailovú adresu nastavenú pre číslo 1 v položke **Nastavenia e-mailovej adresy**, keď sa zmení heslo správcu, začiarknite políčko pre stĺpec **1** v riadku **Heslo správcu sa zmenilo**.
6. Kliknite na položku **OK**.
Vyvolaním udalosti overte, či bude e-mailové upozornenie odoslané.
Príklad: Heslo správcu bolo zmenené.

Súvisiace informácie

➔ „Ako spustiť funkciu **Web Config** v internetovom prehliadači” na strane 37

Položky pre e-mailové oznámenie

Položky	Nastavenia a vysvetlenie
Heslo správcu sa zmenilo	Oznamuje, že bolo zmenené heslo administrátora.
Chyba skenera	Oznamuje, že sa vyskytla chyba skenera.
Chyba súčasti Wi-Fi	Oznámenie, že sa vyskytla chyba rozhrania bezdrôtovej siete LAN.

Na ovládanie napájania skenera použite funkciu **Web Config**

Ak je váš počítač vzdialený od skenera, stále môžete použiť funkciu **Web Config** na vypnutie alebo reštartovanie skenera.

1. Otvorte aplikáciu **Web Config** a potom vyberte kartu **Správa zariadenia > Napájanie**.
2. Vyberte možnosť **Vypnúť** alebo **Reštartovať**.
3. Kliknite na tlačidlo **Vykonať**.

Obnovenie predvolených nastavení

Môžete vybrať sieťové nastavenia alebo iné nastavenia uložené v skeneri a obnoviť ich na predvolené hodnoty.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Správa zariadenia > Obn. predv. nast.**

Poznámka:

Nastavenia môžete urobiť aj na ovládacom paneli skenera.

Nastav. > **Správa systému** > **Obnoviť štand. nastavenia**

2. Vyberte položky, ktoré chcete obnoviť.

3. Kliknite na položku **Vykonať**.

Nakoniec postupujte podľa pokynov na obrazovke.

Informácie o službe Epson Remote Services

Epson Remote Services je služba, ktorá cez internet pravidelne zhromažďuje informácie o skeneri. Dá sa využiť na predvídanie potreby výmeny alebo obnovy spotrebného materiálu alebo náhradných dielov a na rýchle riešenie akýchkoľvek chýb alebo problémov.

Ďalšie informácie o Epson Remote Services vám poskytne predajca.

Riešenie problémov

Zabudnuté heslo správcu

Potrebujete pomoc od servisného personálu. Obráťte sa na miestneho predajcu.

Poznámka:

Nasledujúce informácie poskytujú úvodné hodnoty pre správcu v aplikácii Web Config.

Používateľské meno: žiadne (prázdne)

Heslo: závisí od štítka pripevneného na výrobku.

Ak je na zadnej strane pripevnený štítok „PASSWORD“, zadajte 8-miestne číslo uvedené na štítku.

Ak nie je pripevnený štítok „PASSWORD“, zadajte ako prvotné heslo správcu sériové číslo na štítku pripevnenom na zadnej strane výrobku.

Ak obnovíte heslo správcu, obnoví sa na pôvodnú hodnotu, ktorá bola pri zakúpení.

Rozšírené nastavenia zabezpečenia

Nastavenia zabezpečenia a prevencia pred nebezpečenstvom.	89
Riadenie pomocou protokolov.	90
Používanie digitálneho certifikátu.	93
Komunikácia so skenerom cez protokol SSL/TLS.	98
Šifrovaná komunikácia pomocou filtrovania IPsec/IP.	99
Pripojenie skenera k sieti IEEE802.1X.	111
Riešenie problémov pre rozšírené zabezpečenie.	112

Nastavenia zabezpečenia a prevencia pred nebezpečenstvom

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

Pri skeneroch, ktoré nemajú ochranu pred prístupom zvonka, bude možné z internetu čítať kontakty uložené v skeneri.

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

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

Názov	Typ funkcie	Čo sa nastavuje	Pred čím chráni
Ovládanie protokolu	Ovláda protokoly a služby používané na komunikáciu medzi skenermi a počítačmi a aktivuje a deaktivuje funkcie.	Protokol alebo služba, ktoré sa používajú na funkcie, sú povolené alebo zakázané samostatne.	Zníženie bezpečnostných rizík, ktoré sa môžu vyskytnúť pri nežiadanom používaní vďaka tomu, že sa používateľom zabráni používať nepotrebné funkcie.
Komunikácie SSL/TLS	Obsah komunikácie je pri prístupe k serveru Epson na internete zo skenera zašifrovaný komunikačným protokolom SSL/TLS, napríklad ak komunikujete s počítačom cez webový prehliadač pomocou aplikácie Epson Connect a pri aktualizácii firmvéru.	Zadovážte si certifikát podpísaný autoritou CA a potom ho importujte do skenera.	Vymazanie identifikácie skenera 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 skenovaných údajov a údajov nastavenia.
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.	Vytvorte základné zásady a individuálne zásady nastavenia klienta alebo typu údajov, ktoré majú prístup ku skeneru.	Zabráňte nepovolenému prístupu, sabotáži a odpočúvaniu komunikačných údajov v skeneri.
IEEE 802.1X	Len overení používateľia majú prístup k sieti. Umožnite skener používať iba povolenému používateľovi.	Nastavenie overovania na serveri RADIUS (overovací server).	Chráňte pred nepovoleným prístupom a používaním skenera.

Súvisiace informácie

- ➔ „Riadenie pomocou protokolov” na strane 90
- ➔ „Komunikácia so skenerom cez protokol SSL/TLS” na strane 98
- ➔ „Šifrovaná komunikácia pomocou filtrovania IPsec/IP” na strane 99

➔ „Pripojenie skenera k sieti IEEE802.1X” na strane 111

Nastavenia funkcie zabezpečenia

Keď nastavujete funkciu filtrovania IPsec/IP alebo sieť IEEE 802.1X, odporúča sa, aby ste aplikáciu Web Config otvárali pomocou protokolu SSL/TLS, cez ktorý sa budú komunikovať údaje nastavenia, aby sa znížilo bezpečnostné riziko, napríklad pri manipulácii alebo odpočúvaní.

Pred nastavením funkcie filtrovania IPsec/IP alebo siete IEEE 802.1X nezabudnite nakonfigurovať heslo správcu.

Riadenie pomocou protokolov

Môžete skenovať prostredníctvom rôznych ciest a protokolov. Môžete použiť aj skenovanie cez sieť z neurčeného počtu sieťových počítačov.

Nežiaduce riziká pre zabezpečenie môžete znížiť obmedzením skenovania z určených ciest alebo riadením dostupných funkcií.

Riadiace protokoly

Nakonfigurujte nastavenie protokolu podporovaného skenerom.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie siete** tab > **Protokol**.
2. Nakonfigurujte každú položku.
3. Kliknite na položku **Ďalej**.
4. Kliknite na položku **OK**.

Nastavenia sú uplatnené v skeneri.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Protokoly, ktoré môžete zapnúť alebo vypnúť

Protokol	Popis
Nastavenia služby Bonjour	Môžete určiť, či sa chcete použiť funkciu Bonjour. Bonjour sa používa na vyhľadávanie zariadení, skenovanie atď.
Nastavenia SLP	Môžete zapnúť alebo vypnúť funkciu SLP. Funkcia SLP sa používa na zobrazovanie vyhľadávania a skenovanie siete v aplikácii EpsonNet Config.
Nastavenia WSD	Môžete zapnúť alebo vypnúť funkciu WSD. Keď je to zapnuté, môžete pridať zariadenia WSD a skenovať z portu WSD.
Nastavenia LLTD	Môžete zapnúť alebo vypnúť funkciu LLTD. Keď je zapnutá, zobrazí sa na mape siete vo Windows.

Protokol	Popis
Nastavenia LLMNR	Môžete zapnúť alebo vypnúť funkciu LLMNR. Keď je zapnutá, rozlišovanie názvu môžete použiť bez funkcie NetBIOS aj vtedy, keď nemôžete použiť DNS.
Nastavenia SNMPv1/v2c	Môžete určiť, či sa SNMPv1/v2c má alebo nemá povoliť. Táto funkcia sa používa na nastavenie zariadení, monitorovanie a tak ďalej.
Nastavenia SNMPv3	Môžete určiť, či sa SNMPv3 má alebo nemá povoliť. Táto funkcia sa používa na nastavenie šifrovaných zariadení, monitorovanie atď.

Položky nastavenia protokolu

Nastavenia služby Bonjour

Položky	Nastavenie hodnoty a popis
Použiť službu Bonjour	Túto možnosť vyberte, ak chcete zariadenia použiť pomocou služby Bonjour.
Názov Bonjour	Zobrazí názov Bonjour.
Servisný názov Bonjour	Zobrazí názov služby Bonjour.
Umiestnenie	Zobrazí názov umiestnenia zariadenia Bonjour.
Wide-Area Bonjour	Nastavte, či chcete používať funkciu Wide-Area Bonjour.

Nastavenia SLP

Položky	Nastavenie hodnoty a popis
Zapnúť SLP	Túto možnosť vyberte, ak chcete zapnúť funkciu SLP. Používa sa napríklad na sieťové vyhľadávanie v aplikácii EpsonNet Config.

Nastavenia WSD

Položky	Nastavenie hodnoty a popis
Zapnúť WSD	Túto funkciu vyberte, ak chcete povoliť pridávanie zariadení pomocou WSD a skenovať z portu WSD.
Časový limit skenovania (sek.)	Zadajte hodnotu časového limitu komunikácie pre skenovanie pomocou WSD v rozsahu od 3 do 3 600 sekúnd.
Názov zariadenia	Zobrazí názov zariadenia WSD.
Umiestnenie	Zobrazí názov umiestnenia zariadenia WSD.

Nastavenia LLTD

Položky	Nastavenie hodnoty a popis
Zapnúť LLTD	Túto možnosť vyberte, ak chcete povoliť LLTD. Skener je zobrazený na mape siete Windows.

Položky	Nastavenie hodnoty a popis
Názov zariadenia	Zobrazí názov zariadenia LLTD.

Nastavenia LLMNR

Položky	Nastavenie hodnoty a popis
Zapnúť LLMNR	Túto možnosť vyberte, ak chcete povoliť LLMNR. Rozlíšenie názvu môžete použiť bez NetBIOS aj v prípade, ak nemôžete použiť DNS.

Nastavenia SNMPv1/v2c

Položky	Nastavenie hodnoty a popis
Zapnúť SNMPv1/v2c	Túto možnosť vyberte, ak chcete povoliť SNMPv1/v2c.
Prístupové práva	Keď je povolené SNMPv1/v2c, vyberte prístupovú autoritu. Vyberte možnosť Iba na čítanie alebo Čítať/zapisovať .
Názov komunity (len na čítanie)	Zadajte znaky od 0 do 32 ASCII (0x20 až 0x7E).
Názov komunity (čítanie/zápis)	Zadajte znaky od 0 do 32 ASCII (0x20 až 0x7E).

Nastavenia SNMPv3

Položky	Nastavenie hodnoty a popis
Zapnúť SNMPv3	SNMPv3 je povolené, keď je políčko začiarknuté.
Názov používateľa	Zadajte 1 až 32 znakov pomocou 1-bajtových znakov.
Nastavenia autentifikácie	
Algoritmus	Vyberte algoritmus pre overovanie protokolu SNMPv3.
Heslo	Vyberte heslo pre overovanie protokolu SNMPv3. Zadajte 8 až 32 znakov v kódovaní ASCII (0x20 – 0x7E). Ak to neurčujete, nechajte prázdne.
Potvrdiť heslo	Zadajte nastavené heslo, aby sa vykonalo jeho potvrdenie.
Nastavenia šifrovania	
Algoritmus	Vyberte algoritmus pre šifrovanie protokolu SNMPv3.
Heslo	Vyberte heslo pre šifrovanie protokolu SNMPv3. Zadajte 8 až 32 znakov v kódovaní ASCII (0x20 – 0x7E). Ak to neurčujete, nechajte prázdne.
Potvrdiť heslo	Zadajte nastavené heslo, aby sa vykonalo jeho potvrdenie.
Názov kontextu	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.

Používanie digitálneho certifikátu

O digitálnom certifikáte

CA-podpísaný Certifikát

Toto je certifikát podpísaný certifikačnou autoritou CA (Certificate Authority.) Môžete ho získať a použiť na certifikačnú autoritu. Tento certifikát potvrdzuje existenciu skenera a používa sa pri komunikácii SSL/TLS, aby sa zaistila bezpečnosť komunikácie údajov.

Keď sa používa pre komunikáciu SSL/TLS, používa sa ako serverový certifikát.

Keď je nastavený na komunikáciu IPsec/IP Filtering alebo IEEE 802.1X, používa sa ako klientsky certifikát.

Certifikát CA

Toto je certifikát, ktorý je v reťazení s certifikátom CA-podpísaný Certifikát. Nazýva sa bezprostredný certifikát CA. Používa sa webovým prehľadávačom na overenie cesty k certifikátu skenera pri prístupe servera inej strany alebo aplikácie Web Config.

Pre certifikát CA nastavte, keď sa overuje cesta prístupu serverového certifikátu zo skenera. Pre skener nastavte na certifikáciu cesty CA-podpísaný Certifikát pre pripojenie SSL/TLS.

Certifikát CA pre skener môžete získať od certifikačnej autority, ktorá certifikát CA vydala.

Certifikát CA používaný na overovanie servera inej strany môžete získať aj od certifikačnej autority, ktorá vydala CA-podpísaný Certifikát iného servera.

Certifikát s vlastným podpisom

Toto je certifikát, ktorý podpísal a vydal samotný skener. Nazýva sa aj koreňový certifikát. Pretože vydavateľ certifikuje sám seba, nie je spoľahlivý a nedokáže zabrániť falošnej identifikácii.

Používa sa pri vytváraní nastavenia zabezpečenia a vykonávaní jednoduchej komunikácie SSL/TLS bez certifikátu CA-podpísaný Certifikát.

Ak tento certifikát použijete na komunikáciu SSL/TLS, vo webovom prehľadávači sa môže zobrazíť upozornenie zabezpečenia, pretože certifikát nie je zaregistrovaný vo webovom prehľadávači. Certifikát Certifikát s vlastným podpisom môžete použiť iba na komunikáciu SSL/TLS.

Súvisiace informácie

➔ „Konfigurácia položky CA-podpísaný Certifikát” na strane 93

➔ „Aktualizácia vlastného podpísaného certifikátu” na strane 97

➔ „Konfigurácia položky Certifikát CA” na strane 97

Konfigurácia položky CA-podpísaný Certifikát

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 kartu **Zabezpečenie siete**. Potom vyberte položky **SSL/TLS > Certifikát** alebo **IPsec/IP Filtrovanie > Certifikát klienta** alebo **IEEE802.1X > Certifikát klienta**.

Bez ohľadu na voľbu môžete získať rovnaký certifikát a použiť ho všeobecne.

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

Otvorí sa stránka vytvorenia žiadosti CSR.

3. Zadaťte 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 kartu **Zabezpečenie siete**. Potom vyberte položky **SSL/TLS > Certifikát** alebo **IPsec/IP Filtrovanie > Certifikát klienta** alebo **IEEE802.1X > Certifikát klienta**.

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-podpísaný Certifikát nebudete môcť importovať.

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

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

8. Vydaný certifikát CA-podpísaný Certifikát uložte do počítača, ktorý je pripojený ku skeneru.

Získanie podpísaného certifikátu CA-podpísaný Certifikát je dokončené, keď certifikát uložíte do cieľového umiestnenia.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Položky nastavenia žiadosti CSR

Položky	Nastavenia a vysvetlenie
Dĺžka kľúča	Vyberte dĺžku kľúča pre žiadosť CSR.

Položky	Nastavenia a vysvetlenie
Všeobecný názov	Môžete zadať 1 až 128 znakov. Ak je to adresa IP, mala by to byť statická adresa IP. Môžete zadať 1 až 5 adries IPv4, adries IPv6, názvov hostiteľa a FQDN, oddelíte ich čiarkami. Prvý prvok je uložený do všeobecného názvu a ostatné prvky sú uložené do políčka alias pre certifikovaný subjekt. Príklad: IP adresa skenera: 192.0.2.123, názov skenera: EPSONA1B2C3 Všeobecný názov: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organizácia/ Organizačná jednotka/ Lokalita/ Štát/Provincia	Môžete zadať 0 až 64 znakov v kódovaní ASCII (0x20 – 0x7E). Rozlíšené názvy môžete oddeliť čiarkami.
Krajina	Zadajte dvojciferný kód krajiny podľa normy ISO-3166.
E-mailová adresa odosielateľa	Môžete zadať e-mailovú adresu odosielateľa pre nastavenie poštového servera. Zadajte rovnakú e-mailovú adresu ako v položke E-mailová adresa odosielateľa pre kartu Sieť > E-mailový server > Základné .

Import certifikátu s podpisom CA

Importujte získaný certifikát CA-podpísaný Certifikát do skenera.



Upozornenie:

- Skontrolujte, či je dátum a čas skenera nastavený správne. Certifikát je možno neplatný.
- Ak ste certifikát získali prostredníctvom žiadosti CSR vytvorenej v aplikácii Web Config, môžete ho naimportovať raz.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie siete**. Potom vyberte položky **SSL/TLS > Certifikát** alebo **IPsec/IP Filtrovanie > Certifikát klienta** alebo **IEEE802.1X > Certifikát klienta**.
2. Kliknite na tlačidlo **Importovať**
Otvorí sa stránka importu certifikátu.
3. Zadajte hodnoty pre všetky položky. Nastavte položky **Certifikát CA 1** a **Certifikát CA 2**, keď sa overuje cesta k certifikátu vo webovom prehľadávači, cez ktorý sa pristupuje ku skeneru.

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
 - Súkromný kľúč:** Nekonfigurujte, pretože skener obsahuje súkromný kľúč.
 - Heslo:** Nekonfigurujte.
 - Certifikát CA 1/Certifikát CA 2:** Nepovinné
- Certifikát vo formáte PEM/DER získaný z počítača
 - Súkromný kľúč:** Je potrebné nastaviť.
 - Heslo:** Nekonfigurujte.
 - Certifikát CA 1/Certifikát CA 2:** Nepovinné

- Certifikát vo formáte PKCS#12 získaný z počítača
 - Súkromný kľúč:** Nekonfigurujte.
 - Heslo:** Nepovinné
 - Certifikát CA 1/Certifikát CA 2:** Nekonfigurujte.

4. Kliknite na položku **OK**.

Zobrazí sa správa o vytvorení.

Poznámka:

Kliknutím na položku **Potvrdiť** potvrdíte údaje certifikátu.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Položky nastavenia importu podpísaného certifikátu CA

Položky	Nastavenia a vysvetlenie
Certifikát servera alebo Certifikát klienta	Vyberte formát certifikátu. Pri pripojení cez protokol SSL/TLS sa zobrazuje položka Certifikát servera. Pri funkcii filtrovania IPsec/IP alebo sieti IEEE 802.1X sa zobrazuje položka Certifikát klienta.
Súkromný kľúč	Ak získate certifikát formátu PEM/DER pomocou CSR vytvoreného z počítača, stanovte súbor so súkromným kľúčom, ktorý zodpovedá certifikátu.
Heslo	Ak je formát súboru Certifikát so súkromným kľúčom (PKCS#12) , zadajte heslo na šifrovanie súkromného kľúča, ktoré ste nastavili pri získavaní certifikátu.
Certifikát CA 1	Ak je formát certifikátu Certifikát (PEM/DER) , importujte certifikačnú autoritu, ktorá vydala CA-podpísaný Certifikát používaný ako serverový certifikát. Ak je to potrebné, vyberte súbor.
Certifikát CA 2	Ak je formát certifikátu Certifikát (PEM/DER) , importujte certifikát certifikačnej autority, ktorá vydala Certifikát CA 1. Ak je to potrebné, vyberte súbor.

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 kartu **Zabezpečenie siete**. Potom vyberte položky **SSL/TLS > Certifikát** alebo **IPsec/IP Filtrovanie > Certifikát klienta** alebo **IEEE802.1X > Certifikát klienta**.
2. Kliknite na tlačidlo **Odstrániť**.

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

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Aktualizácia vlastného podpísaného certifikátu

Pretože položka Certifikát s vlastným podpisom je vydaná skenerom, môžete to aktualizovať, keď uplynie platnosť, prípadne ak sa opísaný obsah zmení.

1. Otvorte aplikáciu Web Config a vyberte položky **Zabezpečenie siete** tab > **SSL/TLS** > **Certifikát**.
2. Kliknite na položku **Aktualizovať**.
3. Zadajte položku **Všeobecný názov**.

Môžete zadať až 5 adries IPv4, adries IPv6, názvov hostiteľa a FQDN. Zadať môžete 1 až 128 znakov a položky oddelíte čiarkami. Prvý parameter sa uloží do bežného názvu a ďalšie sa uložia do políčka aliasu subjektu certifikátu.

Príklad:

IP adresa skenera: 192.0.2.123, Názov skenera: EPSONA1B2C3

Bežný názov: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Stanovte dobu platnosti certifikátu.
5. Kliknite na položku **Ďalej**.
Zobrazí sa hlásenie s potvrdením.
6. Kliknite na tlačidlo **OK**.
Skener je aktualizovaný.

Poznámka:

Informácie o certifikáte môžete overiť cez kartu **Zabezpečenie siete** > **SSL/TLS** > **Certifikát** > **Certifikát s vlastným podpisom** a kliknite na tlačidlo **Potvrdiť**.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Konfigurácia položky Certifikát CA

Keď nastavíte certifikát Certifikát CA, môžete overiť platnosť cesty k certifikátu CA servera, ktorá má prístup ku skeneru. Tým zabránite falošnej identifikácii.

Certifikát CA môžete získať od overovacej authority, kde je CA-podpísaný Certifikát vydaný.

Importovanie certifikátu Certifikát CA

Importujte certifikát Certifikát CA do skenera.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie siete** > **Certifikát CA**.
2. Kliknite na položku **Importovať**.
3. Určite certifikát Certifikát CA, ktorý chcete importovať.
4. Kliknite na položku **OK**.

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

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Odstránenie položky Certifikát CA

Môžete odstrániť importovanú položku Certifikát CA.

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie siete** > **Certifikát CA**.
2. Kliknite na možnosť **Odstrániť** vedľa položky Certifikát CA, ktorú chcete odstrániť.
3. V zobrazenom hlásení potvrdte, že chcete certifikát odstrániť.
4. Kliknite na možnosť **Reštartovať sieť** a skontrolujte, či odstránený certifikát nie je uvedený na aktualizovanej obrazovke.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

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.

Konfigurácia základných nastavení SSL/TLS

Ak skener podporuje funkciu servera HTTPS, môžete na šifrovanie komunikácie použiť komunikáciu SSL/TLS. Môžete nakonfigurovať a spravovať skener pomocou aplikácie Web Config, pričom bude bezpečnosť zaistená.

Nakonfigurujte silu šifrovania a funkciu presmerovania.

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie siete** > **SSL/TLS** > **Základné**.
2. Nastavte hodnotu pre jednotlivé položky.
 - Sila šifrovania
Vyberte úroveň sily šifrovania.

- Presmerovať HTTP na HTTPS

Presmerujte na protokol HTTPS, keď sa otvára cez protokol HTTP.

3. Kliknite na položku **Ďalej**.

Zobrazí sa hlásenie s potvrdením.

4. Kliknite na položku **OK**.

Skener je aktualizovaný.

Súvisiace informácie

➔ [„Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37](#)

Konfigurácia certifikátu servera pre skener

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie siete > SSL/TLS > Certifikát**.

2. V položke **Certifikát servera** zadajte certifikát, ktorý sa má použiť.

- Certifikát s vlastným podpisom

Certifikát s vlastným podpisom je vygenerovaný skenerom. Vyberte ho, ak nezískavate certifikát s podpisom certifikačnej autority (CA).

- CA-podpísaný Certifikát

Ak ste vopred získali a nainportovali certifikát s podpisom CA, môžete vybrať tento certifikát.

3. Kliknite na položku **Ďalej**.

Zobrazí sa potvrdzujúca správa.

4. Kliknite na položku **OK**.

Skener je aktualizovaný.

Súvisiace informácie

➔ [„Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37](#)

➔ [„Konfigurácia položky CA-podpísaný Certifikát” na strane 93](#)

➔ [„Konfigurácia položky Certifikát CA” na strane 97](#)

Šifrovaná komunikácia pomocou filtrovania IPsec/IP

Čo je IPsec/IP Filtrovanie

Prenos údajov môžete pomocou funkcie IPsec/IP Filtering filtrovať podľa 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.

Poznámka:

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

Konfigurácia predvolených zásad

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.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie siete > IPsec/IP Filtrovanie > Základné**.
2. Zadajte hodnoty pre všetky položky.
3. Kliknite na položku **Ďalej**.
Zobrazí sa potvrdzujúca správa.
4. Kliknite na položku **OK**.
Skener je aktualizovaný.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Položky nastavenia Predvolené zásady

Predvolené zásady

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

Kontrola prístupu

Nakonfigurujte metódu riadenia komunikácie prostredníctvom paketov IP.

Položky	Nastavenia a vysvetlenie
Povoliť prístup	Vybratím tejto možnosti povolíte, aby sa nakonfigurované pakety IP dostali do tlačiarne.
Odmietnuť prístup	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.

Verzia IKE

Vyberte možnosť **IKEv1** alebo **IKEv2** pre **Verzia IKE**. Vyberte jednu z nich v závislosti od zariadenia, ku ktorému je skener pripojený.

IKEv1

Keď vyberiete možnosť **IKEv1** pre položku **Verzia IKE**, zobrazia sa nasledujúce položky.

Položky	Nastavenia a vysvetlenie
Spôsob overenia	Ak chcete vybrať možnosť Certifikát , musíte najskôr získať a naimportovať certifikát s podpisom CA.
Vopred zdieľaný kľúč	Ak vyberiete možnosť Vopred zdieľaný kľúč v položke Spôsob overenia , zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
Potvrdiť Vopred zdieľaný kľúč	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.

IKEv2

Keď vyberiete možnosť **IKEv2** pre položku **Verzia IKE**, zobrazia sa nasledujúce položky.

Položky	Nastavenia a vysvetlenie	
Lokálne	Spôsob overenia	Ak chcete vybrať možnosť Certifikát , musíte najskôr získať a naimportovať certifikát s podpisom CA.
	Typ ID	Ak vyberiete možnosť Vopred zdieľaný kľúč pre položku Spôsob overenia , vyberte typ ID pre skener.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. Rozlišujúci názov: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „=“. Adresa IP: zadajte formát IPv4 alebo IPv6. FQDN: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). E-mailová adresa: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „@“. ID kľúča: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255.
	Vopred zdieľaný kľúč	Ak vyberiete možnosť Vopred zdieľaný kľúč v položke Spôsob overenia , zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Potvrdiť Vopred zdieľaný kľúč	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.

Položky		Nastavenia a vysvetlenie
Vzdialené	Spôsob overenia	Ak chcete vybrať možnosť Certifikát , musíte najskôr získať a naimportovať certifikát s podpisom CA.
	Typ ID	Ak vyberiete možnosť Vopred zdieľaný kľúč pre položku Spôsob overenia , vyberte typ ID pre zariadenie, ktoré chcete overiť.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. Rozlišujúci názov: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „=“. Adresa IP: zadajte formát IPv4 alebo IPv6. FQDN: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). E-mailová adresa: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „@“. ID kľúča: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255.
	Vopred zdieľaný kľúč	Ak vyberiete možnosť Vopred zdieľaný kľúč v položke Spôsob overenia , zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Potvrdiť Vopred zdieľaný kľúč	Zadajte nakonfigurovaný kľúč, aby sa vykonal jeho potvrdenie.

Zapuzdrenie

Ak v položke **Kontrola prístupu** vyberiete možnosť **IPsec**, musíte nakonfigurovať režim zapuzdrovania.

Položky	Nastavenia a vysvetlenie
Režim transportu	Ak skener používate iba v rovnakej sieti LAN, vyberte túto možnosť. Pakety IP vrstvy 4 alebo vyššej sú šifrované.
Režim tunela	Ak používate skener v sieti s pripojením k internetu, ako je napríklad IPsec-VPN, vyberte túto možnosť. Hlavičky a údaje paketov IP sú šifrované. Vzdialená brána (Režim tunela): Ak vyberiete možnosť Režim tunela pre Zapuzdrenie , zadajte adresu brány dlhú 1 až 39 znakov.

Protokol zabezpečenia

Ak v položke **IPsec** vyberiete možnosť **Kontrola prístupu**, vyberte niektorú možnosť.

Položky	Nastavenia a vysvetlenie
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.

☐ Nastavenia algoritmu

Odporúča sa vybrať položku **Akýkoľvek** pre všetky nastavenia, alebo vybrať pre všetky nastavenia inú položku ako **Akýkoľvek**. Ak pre niektoré nastavenia vyberiete možnosť **Akýkoľvek** a pre ostatné nastavenia vyberiete inú možnosť než **Akýkoľvek**, zariadenie nemusí komunikovať. Závisí to od druhého zariadenia, ktoré chcete overiť.

Položky		Nastavenia a vysvetlenie
IKE	Šifrovanie	Vyberte algoritmus šifrovania pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.
	Overenie	Vyberte algoritmus overovania pre IKE.
	Výmena kľúčov	Vyberte algoritmus výmeny kľúča pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.
ESP	Šifrovanie	Vyberte algoritmus šifrovania pre ESP. To je k dispozícii, keď je možnosť ESP zvolená pre položku Protokol zabezpečenia .
	Overenie	Vyberte algoritmus overovania pre ESP. To je k dispozícii, keď je možnosť ESP zvolená pre položku Protokol zabezpečenia .
AH	Overenie	Vyberte algoritmus šifrovania pre AH. To je k dispozícii, keď je možnosť AH zvolená pre položku Protokol zabezpečenia .

Konfigurácia zásad skupiny

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.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie siete > IPsec/IP Filtrovanie > Základné**.
2. Kliknite na očíslovanú kartu, ktorú chcete konfigurovať.
3. Zadajte hodnoty pre všetky položky.
4. Kliknite na položku **Ďalej**.
Zobrazí sa potvrdzujúca správa.
5. Kliknite na položku **OK**.
Skener je aktualizovaný.

Položky nastavenia Zásady skupiny

Položky	Nastavenia a vysvetlenie
Zapnúť tieto Zásady skupiny	Môžete zapnúť alebo vypnúť skupinovú politiku.

Kontrola prístupu

Nakonfigurujte metódu riadenia komunikácie prostredníctvom paketov IP.

Položky	Nastavenia a vysvetlenie
Povolit' prístup	Vybratím tejto možnosti povolíte, aby sa nakonfigurované pakety IP dostali do tlačiarne.
Odmietnuť prístup	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.

Lokálna adresa (skener)

Vyberte adresu IPv4 alebo IPv6, ktoré zodpovedajú vášmu sieťovému prostrediu. Ak je IP adresa priradená automaticky, môžete vybrať možnosť **Použiť automaticky získanú adresu IPv4**.

Poznámka:

Ak je adresa IPv6 pridelená automaticky, pripojenie nemusí byť k dispozícii. Nakonfigurujte statickú adresu IPv6.

Vzdialená adresa (hostiteľ)

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.

Spôsob výberu portu

Vyberte spôsob určenia portov.

- Názov služby

Ak v položke **Názov služby** vyberiete možnosť **Spôsob výberu portu**, vyberte niektorú možnosť.

- Transportný protokol

Ak v položke **Spôsob výberu portu** vyberiete možnosť **Číslo portu**, musíte nakonfigurovať režim zapuzdrovania.

Položky	Nastavenia a vysvetlenie
Akýkoľvek protokol	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.

- Lokálny port

Ak vyberiete možnosť **Číslo portu** pre položku **Spôsob výberu portu** a ak vyberiete možnosť **TCP** alebo **UDP** pre položku **Transportný protokol**, zadajte čísla portov na riadenie prichádzajúcich paketov. Oddelíte ich čiarkami. Môžete zadať maximálne 10 čísel portov.

Príklad: 20,80,119,5220

Ak nezadáte číslo portu, budú sa riadiť všetky porty.

Vzdialený port

Ak vyberiete možnosť **Číslo portu** pre položku **Spôsob výberu portu** a ak vyberiete možnosť **TCP** alebo **UDP** pre položku **Transportný protokol**, zadajte čísla portov na riadenie odosielaných paketov. Oddelte ich čiarkami. Môžete zadať maximálne 10 čísel portov.

Príklad: 25,80,143,5220

Ak ne zadáte číslo portu, budú sa riadiť všetky porty.

Verzia IKE

Vyberte možnosť **IKEv1** alebo **IKEv2** pre **Verzia IKE**. Vyberte jednu z nich v závislosti od zariadenia, ku ktorému je skener pripojený.

IKEv1

Keď vyberiete možnosť **IKEv1** pre položku **Verzia IKE**, zobrazia sa nasledujúce položky.

Položky	Nastavenia a vysvetlenie
Spôsob overenia	Ak v položke IPsec vyberiete možnosť Kontrola prístupu , vyberte niektorú možnosť. Pri predvolenej politike sa zvyčajne používa certifikát.
Vopred zdieľaný kľúč	Ak vyberiete možnosť Vopred zdieľaný kľúč v položke Spôsob overenia , zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
Potvrdiť Vopred zdieľaný kľúč	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.

IKEv2

Keď vyberiete možnosť **IKEv2** pre položku **Verzia IKE**, zobrazia sa nasledujúce položky.

Položky		Nastavenia a vysvetlenie
Lokálne	Spôsob overenia	Ak v položke IPsec vyberiete možnosť Kontrola prístupu , vyberte niektorú možnosť. Pri predvolenej politike sa zvyčajne používa certifikát.
	Typ ID	Ak vyberiete možnosť Vopred zdieľaný kľúč pre položku Spôsob overenia , vyberte typ ID pre skener.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. Rozlišujúci názov: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „=“. Adresa IP: zadajte formát IPv4 alebo IPv6. FQDN: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). E-mailová adresa: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „@“. ID kľúča: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255.
	Vopred zdieľaný kľúč	Ak vyberiete možnosť Vopred zdieľaný kľúč v položke Spôsob overenia , zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Potvrdiť Vopred zdieľaný kľúč	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.
Vzdialené	Spôsob overenia	Ak v položke IPsec vyberiete možnosť Kontrola prístupu , vyberte niektorú možnosť. Pri predvolenej politike sa zvyčajne používa certifikát.
	Typ ID	Ak vyberiete možnosť Vopred zdieľaný kľúč pre položku Spôsob overenia , vyberte typ ID pre zariadenie, ktoré chcete overiť.
	ID	Zadajte ID skenera, ktoré zodpovedá typu identifikácie. Ako prvý znak nie je možné použiť „@“, „#“ a „=“. Rozlišujúci názov: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „=“. Adresa IP: zadajte formát IPv4 alebo IPv6. FQDN: zadajte kombináciu 1 až 255 znakov. Môžete použiť znaky A – Z, a – z, 0 – 9 a bodku (.). E-mailová adresa: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255. Je potrebné, aby obsahovalo znak „@“. ID kľúča: zadajte jednobajtové znaky ASCII (0x20 až 0x7E) 1 až 255.
	Vopred zdieľaný kľúč	Ak vyberiete možnosť Vopred zdieľaný kľúč v položke Spôsob overenia , zadajte vopred zdieľaný kľúč dlhý 1 až 127 znakov.
	Potvrdiť Vopred zdieľaný kľúč	Zadajte nakonfigurovaný kľúč, aby sa vykonalo jeho potvrdenie.

Zapuzdrenie

Ak v položke **Kontrola prístupu** vyberiete možnosť **IPsec**, musíte nakonfigurovať režim zapuzdrovania.

Položky	Nastavenia a vysvetlenie
Režim transportu	Ak skener používate iba v rovnakej sieti LAN, vyberte túto možnosť. Pakety IP vrstvy 4 alebo vyššej sú šifrované.
Režim tunela	Ak používate skener v sieti s pripojením k internetu, ako je napríklad IPsec-VPN, vyberte túto možnosť. Hlavičky a údaje paketov IP sú šifrované. Vzdialená brána (Režim tunela): Ak vyberiete možnosť Režim tunela pre Zapuzdrenie , zadajte adresu brány dlhú 1 až 39 znakov.

Protokol zabezpečenia

Ak v položke **IPsec** vyberiete možnosť **Kontrola prístupu**, vyberte niektorú možnosť.

Položky	Nastavenia a vysvetlenie
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.

Nastavenia algoritmu

Odporúča sa vybrať položku **Akýkoľvek** pre všetky nastavenia, alebo vybrať pre všetky nastavenia inú položku ako **Akýkoľvek**. Ak pre niektoré nastavenia vyberiete možnosť **Akýkoľvek** a pre ostatné nastavenia vyberiete inú možnosť než **Akýkoľvek**, zariadenie nemusí komunikovať. Závisí to od druhého zariadenia, ktoré chcete overiť.

Položky	Nastavenia a vysvetlenie	
IKE	Šifrovanie	Vyberte algoritmus šifrovania pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.
	Overenie	Vyberte algoritmus overovania pre IKE.
	Výmena kľúčov	Vyberte algoritmus výmeny kľúča pre IKE. Položky sa môžu líšiť v závislosti od verzie IKE.
ESP	Šifrovanie	Vyberte algoritmus šifrovania pre ESP. To je k dispozícii, keď je možnosť ESP zvolená pre položku Protokol zabezpečenia .
	Overenie	Vyberte algoritmus overovania pre ESP. To je k dispozícii, keď je možnosť ESP zvolená pre položku Protokol zabezpečenia .
AH	Overenie	Vyberte algoritmus šifrovania pre AH. To je k dispozícii, keď je možnosť AH zvolená pre položku Protokol zabezpečenia .

Kombinácia Lokálna adresa (skener) a Vzdialená adresa (hostiteľ) v položke Zásady skupiny

		Nastavenie položky Lokálna adresa (skener)		
		IPv4	IPv6* ²	Akkoľvek adresy* ³
Nastavenie položky Vzdialená adresa (hostiteľ)	IPv4* ¹	✓	–	✓
	IPv6* ¹ , * ²	–	✓	✓
	Prázdne	✓	✓	✓

*1 Ak je vybraná možnosť **IPsec** pre položku **Kontrola prístupu**, nemôžete určiť dĺžku predpony.

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

*3 Okrem prepojení na lokálne adresy IPv6.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

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
Akkoľvek	–	–	–	Všetky služby
ENPC	UDP	3289	Akkoľvek port	Vyhľadávanie skenera z aplikácií, ako je napríklad Epson Device Admin a ovládača skenera
SNMP	UDP	161	Akkoľvek port	Získanie a nakonfigurovanie MIB z aplikácií, ako je napríklad Epson Device Admin, a ovládača skenera Epson
WSD	TCP	Akkoľvek port	5357	Ovládanie WSD
WS-Discovery	UDP	3702	Akkoľvek port	Vyhľadávanie skenerov WSD
Network Scan	TCP	1865	Akkoľvek port	Presmerovanie naskenovaných údajov z aplikácie Document Capture Pro
Network Push Scan	TCP	Akkoľvek port	2968	Získanie informácií úlohy okamžitého skenovania z aplikácie Document Capture Pro
Network Push Scan Discovery	UDP	2968	Akkoľvek port	Vyhľadanie počítača zo skenera

Názov služby	Typ protokolu	Číslo lokálneho portu	Číslo vzdialeného portu	Ovládané funkcie
FTP údaje (vzdialené)	TCP	Akýkoľvek port	20	Klient FTP (presmerovanie naskenovaných údajov) Dá sa to však ovládať iba vtedy, ak server FTP využíva číslo vzdialeného portu 20.
Riadenie FTP (vzdialené)	TCP	Akýkoľvek port	21	Klient FTP (riadenie presmerovaných naskenovaných údajov)
CIFS (vzdialené)	TCP	Akýkoľvek port	445	Klient CIFS (presmerovanie naskenovaných údajov do priečinka)
NetBIOS Name Service (vzdialené)	UDP	Akýkoľvek port	137	Klient CIFS (presmerovanie naskenovaných údajov do priečinka)
NetBIOS Datagram Service (vzdialené)	UDP	Akýkoľvek port	138	
NetBIOS Session Service (vzdialené)	TCP	Akýkoľvek port	139	
HTTP (lokálne)	TCP	80	Akýkoľvek port	Server HTTP(S) (presmerovanie údajov aplikácie Web Config a WSD)
HTTPS (lokálne)	TCP	443	Akýkoľvek port	
HTTP (vzdialené)	TCP	Akýkoľvek port	80	Klient HTTP(S) (aktualizácia firmvéru a koreňového certifikátu)
HTTPS (vzdialené)	TCP	Akýkoľvek port	443	

Príklady konfigurácie funkcie IPsec/IP Filtrovanie

Príjem iba paketov IPsec

Toto je príklad iba na konfiguráciu predvolených zásad.

Predvolené zásady:

- IPsec/IP Filtrovanie: Povolit'**
- Kontrola prístupu: IPsec**
- Spôsob overenia: Vopred zdieľaný kľúč**
- Vopred zdieľaný kľúč:** Zadajte max. 127 znakov.

Zásady skupiny: Nekonfigurujte.

Prijímanie údajov skenovania a nastavení skenera

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

Predvolené zásady:

- IPsec/IP Filtrovanie: Povolit'
- Kontrola prístupu: Odmietnuť prístup

Zásady skupiny:

- Zapnúť tieto Zásady skupiny: Začiarknite políčko.
- Kontrola prístupu: Povolit' prístup
- Vzdialená adresa (hostiteľ): Adresa IP klienta
- Spôsob výberu portu: Názov služby
- Názov služby: Začiarknite políčko ENPC, SNMP, HTTP (lokálne), HTTPS (lokálne) a Network Scan.

Prístup k prijímaniu iba z určenej adresy IP

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

Predvolené zásady:

- IPsec/IP Filtrovanie: Povolit'
- Kontrola prístupu: Odmietnuť prístup

Zásady skupiny:

- Zapnúť tieto Zásady skupiny: Začiarknite políčko.
- Kontrola prístupu: Povolit' prístup
- Vzdialená adresa (hostiteľ): Adresa IP klienta správcu

Poznámka:

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

Konfigurácia certifikátu pre funkciu filtrovania IPsec/IP

Nakonfigurujte certifikát pre funkciu filtrovania IPsec/IP. Keď to nastavíte, môžete certifikát použiť ako spôsob overovania pre funkciu filtrovania IPsec/IP. Ak chcete nakonfigurovať certifikačnú autoritu, prejdite na položku **Certifikát CA**.

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie siete > IPsec/IP Filtrovanie > Certifikát klienta**.
2. Importujte certifikát v položke **Certifikát klienta**.

Ak ste už importovali certifikát vydaný certifikačnou autoritou, môžete certifikát skopírovať a použiť ho vo funkcii filtrovania IPsec/IP. Ak chcete kopírovať, vyberte certifikát v položke **Kopírovať z** a kliknite na tlačidlo **Kopírovať**.

Súvisiace informácie

- ➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37
- ➔ „Konfigurácia položky CA-podpísaný Certifikát” na strane 93
- ➔ „Konfigurácia položky Certifikát CA” na strane 97

Pripojenie skenera k sieti IEEE802.1X

Konfigurácia siete IEEE 802.1X

Keď nastavíte sieť IEEE 802.1X pre skener, môžete ho používať v sieti pripojenej k serveru RADIUS, prepínaču LAN s funkciou overovania alebo prístupovému bodu.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Zabezpečenie siete > IEEE802.1X > Základné**.

2. Zadajte hodnoty pre všetky položky.

Ak chcete používať skener v sieti Wi-Fi, kliknite na položku **Nastavenie bezdr. siete** a vyberte alebo zadajte SSID.

Poznámka:

Môžete zdieľať nastavenia medzi sieťami Ethernet a Wi-Fi.

3. Kliknite na položku **Ďalej**.

Zobrazí sa potvrdzujúca správa.

4. Kliknite na položku **OK**.

Skener je aktualizovaný.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Položky nastavenia siete IEEE 802.1X

Položky	Nastavenia a vysvetlenie	
IEEE802.1X (drôtová sieť LAN)	Môžete aktivovať alebo deaktivovať nastavenia stránky (IEEE802.1X > Základné) pre sieť IEEE802.1X (káblková sieť LAN).	
IEEE802.1X (Wi-Fi)	Zobrazuje sa stav pripojenia siete IEEE802.1X (Wi-Fi).	
Spôsob pripojenie	Zobrazuje sa spôsob pripojenia aktuálnej siete.	
Typ EAP	Vyberte možnosť pre spôsob overovania medzi skenerom a serverom RADIUS.	
	EAP-TLS	Je potrebné získať a naimportovať podpísaný certifikát CA.
	PEAP-TLS	
	PEAP/MSCHAPv2	Je potrebné nakonfigurovať heslo.
	EAP-TTLS	
ID používateľa	Nakonfigurujte ID, ktoré bude používané pre overovanie servera RADIUS. Zadajte 1 až 128 jednobajtových znakov ASCII (0x20 – 0x7E).	
Heslo	Nakonfigurujte heslo pre overovanie skenera. Zadajte 1 až 128 jednobajtových znakov ASCII (0x20 – 0x7E). Ak používate server Windows ako server RADIUS, môžete zadať najviac 127 znakov.	

Položky	Nastavenia a vysvetlenie
Potvrdiť heslo	Na overenie zadajte nakonfigurované heslo.
ID servera	Môžete nakonfigurovať ID servera na overovanie s konkrétnym serverom RADIUS. Overovateľ skontroluje, či je ID servera v políčku subject/subjectAltName v serverovom certifikáte, ktorý je odoslaný zo servera RADIUS. Zadajte 0 až 128 jednobajtových znakov ASCII (0x20 – 0x7E).
Overenie certifikátu (káblová sieť LAN)	Ak to chcete vykonať Overenie certifikátu pomocou IEEE802.1X (drôtová sieť LAN) , vyberte možnosť Povoliť . Ak vyberiete možnosť Povoliť , pozrite si súvisiace informácie a importujte Certifikát CA . Všimnite si, že funkcia Overenie certifikátu je v položke IEEE802.1X (Wi-Fi) vždy povolená. Nezapodme importovať Certifikát CA.
Anonymné meno	Ak vyberiete možnosť PEAP-TLS alebo PEAP/MSCHAPv2 pre položku Typ EAP , môžete nakonfigurovať anonymný názov namiesto ID používateľa pre fázu 1 overovania PEAP. Zadajte 0 až 128 jednobajtových znakov ASCII (0x20 – 0x7E).
Sila šifrovania	Môžete vybrať jednu z nasledujúcich možností.
	Vysoký AES256/3DES
	Stredný AES256/3DES/AES128/RC4

Súvisiace informácie

➔ „Konfigurácia položky Certifikát CA” na strane 97

Konfigurácia certifikátu pre sieť IEEE 802.1X

Nakonfigurujte klientsky certifikát pre sieť IEEE802.1X. Keď to nastavíte, môžete použiť **EAP-TLS** a **PEAP-TLS** ako spôsob overovania pre sieť IEEE 802.1X. Ak chcete nakonfigurovať certifikát certifikačnej autority, prejdite na položku **Certifikát CA**.

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie siete > IEEE802.1X > Certifikát klienta**.
2. Zadajte certifikát v položke **Certifikát klienta**.

Ak ste už importovali certifikát vydaný certifikačnou autoritou, môžete certifikát skopírovať a použiť ho v sieti IEEE802.1X. Ak chcete kopírovať, vyberte certifikát v položke **Kopírovať z** a kliknite na tlačidlo **Kopírovať**.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Riešenie problémov pre rozšírené zabezpečenie

Obnovenie nastavení zabezpečenia

Keď nastavíte prostredie s vysokým zabezpečením, ako je napríklad filtrovanie IPsec/IP, 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.

Deaktivovanie bezpečnostnej funkcie pomocou aplikácie Web Config

Funkciu IPsec/IP Filtrovanie môžete vypnúť pomocou aplikácie Web Config.

1. Otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie siete > IPsec/IP Filtrovanie > Základné**.
2. Vypnite režim **IPsec/IP Filtrovanie**.

Problémy pri používaní funkcií bezpečnosti siete

Zabudnutý vopred zdieľaný kľúč

Znova nakonfigurujte vopred zdieľaný kľúč.

Ak chcete kľúč zmeniť, otvorte aplikáciu Web Config a vyberte kartu **Zabezpečenie siete > IPsec/IP Filtrovanie > Základné > Predvolené zásady** alebo **Zásady skupiny**.

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

Súvisiace informácie

- ➔ [„Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37](#)
- ➔ [„Šifrovaná komunikácia pomocou filtrovania IPsec/IP” na strane 99](#)

Nie je možné komunikovať prostredníctvom komunikácie IPsec

Stanovte algoritmus, ktorý skener alebo počítač nepodporujú.

Skener podporuje nasledujúce algoritmy. Skontrolujte nastavenia počítača.

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 99

Náhle nie je možné komunikovať

IP adresa skenera sa zmenila, prípadne sa nedá použiť.

Keď sa IP adresa zaregistrovaná v lokálnej adrese položky Zásady skupiny zmenila, prípadne sa nedá použiť, komunikácia IPsec nie je možná. 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 (**Zabezpečenie siete > IPsec/IP Filtrovanie > Základné > Zásady skupiny > Lokálna adresa (skener)**).

Použite statickú adresu IP.

IP adresa počítača sa zmenila, prípadne sa nedá použiť.

Keď sa IP adresa zaregistrovaná vo vzdialenej adrese položky Zásady skupiny zmenila, prípadne sa nedá použiť, komunikácia IPsec nie je možná.

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 (**Zabezpečenie siete > IPsec/IP Filtrovanie > Základné > Zásady skupiny > Vzdialená adresa (hostiteľ)**).

Použite statickú adresu IP.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

➔ „Šifrovaná komunikácia pomocou filtrovania IPsec/IP” na strane 99

Po konfigurácii funkcie IPsec/IP Filtering sa nedá pripojiť

Nastavenia funkcie IPsec/IP Filtering sú nesprávne.

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 99

Prístup k zariadeniu nie je po konfigurácii funkcie IEEE 802.1X možný

Nastavenia IEEE 802.1X sú nesprávne.

Z ovládacieho panela skenera vypnite funkciu IEEE 802.1X a Wi-Fi. Pripojte skener k počítaču a potom znova nakonfigurujte funkciu IEEE 802.1X.

Súvisiace informácie

➔ [„Konfigurácia siete IEEE 802.1X” na strane 111](#)

Problémy s používaním digitálneho certifikátu

Nedá sa importovať CA-podpísaný Certifikát

CA-podpísaný Certifikát a údaje CSR sa nezhodujú.

Ak CA-podpísaný Certifikát a CSR nemajú rovnaké údaje, 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.

CA-podpísaný Certifikát je väčší než 5 kB.

CA-podpísaný Certifikát väčší ako 5 kB nie je možné naimportovať.

Heslo na import certifikátu je nesprávne.

Zadajte správne heslo. Ak ste zabudli heslo, nemôžete certifikát naimportovať. Znova získajte CA-podpísaný Certifikát.

Súvisiace informácie

➔ [„Import certifikátu s podpisom CA” na strane 95](#)

Nie je možné aktualizovať certifikát s vlastným podpisom

Položka Všeobecný názov nebola zadaná.

Položku Všeobecný názov je potrebné zadať.

V položke Všeobecný názov boli zadané nepodporované znaky.

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

Položka Common Name obsahuje čiarku alebo medzeru.

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

Súvisiace informácie

➔ [„Aktualizácia vlastného podpísaného certifikátu” na strane 97](#)

Nie je možné vytvoriť žiadosť CSR

Položka Všeobecný názov nebola zadaná.

Položku Všeobecný názov je potrebné zadať.

V položkách Všeobecný názov, Organizácia, Organizačná jednotka, Lokalita a Štát/Provincia boli zadané nepodporované znaky.

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

Položka Všeobecný názov obsahuje čiarku alebo medzeru.

Ak obsahuje čiarku, položka Všeobecný názov 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 93

Zobrazuje sa upozornenie týkajúce sa digitálneho certifikátu

Správy	Príčina/riešenie
Zadajte Certifikát servera.	<p>Príčina: Nevybrali ste súbor na import.</p> <p>Riešenie: Vyberte súbor a kliknite na položku Importovať.</p>
Certifikát CA 1 nie je zadaný.	<p>Príčina: Certifikát CA 1 nie je zadaný a je zadaný iba certifikát CA 2.</p> <p>Riešenie: Naimportujte najskôr certifikát CA 1.</p>
Neplatná hodnota zadaná nižšie.	<p>Príčina: Cesta k súboru alebo heslo obsahuje nepodporované znaky.</p> <p>Riešenie: Skontrolujte, či sú v položke správne zadané znaky.</p>
Neplatný dátum a čas.	<p>Príčina: Nie je nastavený dátum a čas skenera.</p> <p>Riešenie: Nastavte dátum a čas pomocou aplikácie Web Config alebo EpsonNet Config.</p>
Neplatné heslo.	<p>Príčina: Heslo nastavené pre certifikát CA a zadané heslo sa nezhodujú.</p> <p>Riešenie: Zadajte správne heslo.</p>

Správy	Príčina/riešenie
Neplatný súbor.	<p>Príčina:</p> <p>Neimportujete súbor certifikátu vo formáte X509.</p> <p>Riešenie:</p> <p>Skontrolujte, či ste vybrali správny certifikát odoslaný dôveryhodnou certifikačnou autoritou.</p>
	<p>Príčina:</p> <p>Naimportovaný súbor je priveľký. Maximálna veľkosť súboru je 5 kB.</p> <p>Riešenie:</p> <p>Ak ste vybrali správny súbor, certifikát môže byť poškodený alebo falošný.</p>
	<p>Príčina:</p> <p>Reťazec nachádzajúci sa v certifikáte je neplatný.</p> <p>Riešenie:</p> <p>Ďalšie informácie o certifikáte nájdete na webovej lokalite certifikačnej autority.</p>
Nemožno použiť Certifikáty servera, ktoré obsahujú viac než tri Certifikáty CA.	<p>Príčina:</p> <p>Súbor certifikátu vo formáte PKCS#12 obsahuje viac ako 3 certifikáty CA.</p> <p>Riešenie:</p> <p>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.</p>
Platnosť certifikátu uplynula. Skontrolujte, či je certifikát platný alebo skontrolujte dátum a čas v zariadení.	<p>Príčina:</p> <p>Certifikát je neaktuálny.</p> <p>Riešenie:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ak je certifikát neaktuálny, získajte a naimportujte nový certifikát. <input type="checkbox"/> Ak certifikát nie je neaktuálny, skontrolujte, či je správne nastavený dátum a čas skenera.
Vyžaduje sa súkromný kľúč.	<p>Príčina:</p> <p>Certifikát nie je spárovaný so súkromným kľúčom.</p> <p>Riešenie:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ak je certifikát vo formáte PEM/DER a bol získaný na základe žiadosti CSR pomocou počítača, zadajte súbor súkromného kľúča. <input type="checkbox"/> Ak je certifikát vo formáte PKCS#12 a bol získaný na základe žiadosti CSR pomocou počítača, vytvorte súbor obsahujúci súkromný kľúč.
	<p>Príčina:</p> <p>Znova ste naimportovali certifikát PEM/DER získaný na základe žiadosti CSR pomocou aplikácie Web Config.</p> <p>Riešenie:</p> <p>Ak je certifikát vo formáte PEM/DER a bol získaný na základe žiadosti CSR pomocou aplikácie Web Config, môžete ho naimportovať iba raz.</p>

Správy	Príčina/riešenie
Nastavenie zlyhalo.	<p>Príčina:</p> <p>Nie je možné dokončiť konfiguráciu, pretože komunikácia medzi skenerom a počítačom zlyhala alebo súbor nie je možné prečítať kvôli chybám.</p> <p>Riešenie:</p> <p>Po kontrole zadaného súboru a komunikácie naimportujte súbor znova.</p>

Súvisiace informácie

➔ [„O digitálnom certifikáte” na strane 93](#)

Omylom odstránený certifikát s podpisom CA

Nie je žiadny záložný súbor pre certifikát s podpisom CA.

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

➔ [„Import certifikátu s podpisom CA” na strane 95](#)

➔ [„Odstránenie certifikátu s podpisom CA” na strane 96](#)

Používanie funkcie Epson Open Platform

Prehľad platformy Epson Open Platform.	120
Konfigurácia režimu Epson Open Platform.	120
Overenie platformy Epson Open Platform.	120

Prehľad platformy Epson Open Platform

Epson Open Platform je platforma, ktorá umožňuje používať autentifikačné systémy s týmto skenerom.

Môže sa používať so systémom Epson Print Admin (overovací systém Epson) alebo externým overovacím systémom. Môžete získavať protokoly podľa zariadení a používateľov, konfigurovať zariadenia, ktoré môžu používatelia a skupiny používať, nastavovať limity pre funkcie atď.

Ak pripojíte overovacie zariadenie, môžete robiť aj overovanie používateľov pomocou identifikačnej karty.

Konfigurácia režimu Epson Open Platform

Povoľte režim Epson Open Platform, aby ste mohli používať zariadenie z overovacieho systému.

1. Získajte produktový kľúč zo špecializovanej webovej stránky.
Ďalšie údaje o získaní produktového kódu nájdete v návode pre Epson Open Platform.
2. Otvorte aplikáciu Web Config a potom vyberte kartu **Epson Open Platform > Kód Product Key alebo Licenčný kľúč**.
3. Skontrolujte a nastavte každú položku.
 - Výrobné číslo
Zobrazí sa sériové číslo zariadenia.
 - Verzia Epson Open Platform
Vyberte verziu režimu Epson Open Platform. Príslušná verzia sa líši v závislosti od overovacieho systému.
 - Kód Product Key alebo Licenčný kľúč
Zadajte získaný produktový kľúč.
4. Kliknite na položku **Ďalej**.
Zobrazí sa obrazovka s potvrdením nastavenia.
5. Kliknite na tlačidlo **OK**.
Nastavenia sa použijú v skeneri.

Poznámka:

Keď je systém synchronizovaný s aplikáciou Epson Open Platform, nemôžete aplikáciu Epson Print Admin Serverless používať.

Overenie platformy Epson Open Platform

Platnosť funkcie Epson Open Platform môžete skontrolovať pomocou niektorej z nasledujúcich metód.

- Web Config
Produktový kód bol zadaný na karte **Epson Open Platform > Kód Product Key alebo Licenčný kľúč > Kód Product Key alebo Licenčný kľúč** a karta **Epson Open Platform > Autentifikačný systém** sa zobrazuje na ľavej strane štruktúry ponuky.

Ovládací panel skenera

Skontrolujte, či je kľúč produktu zobrazený v **Nastav.** > **Informácie o zariadení** > **Informácie o Epson Open Platform**.

Pripojenie overovacieho zariadenia

Pripojenie overovacieho zariadenia.	123
Kontrola činnosti pre overovacie zariadenie.	123
Potvrdenie rozpoznania overovacej karty.	123
Riešenie problémov s overovacím zariadením.	124

Pripojenie overovacieho zariadenia

Poznámka:

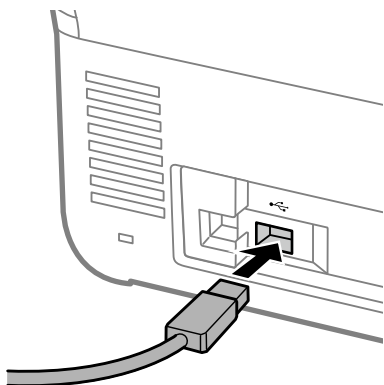
Pri používaní overovacieho systému sa používa overovacie zariadenie.



Upozornenie:

Keď pripájate overovacie zariadenie k viacerým skenerom, použite výrobok s rovnakým číslom modelu.

Pripojte USB kábel čítačky kariet k USB portu externého rozhrania na skeneri.



Kontrola činnosti pre overovacie zariadenie

Stav pripojenia a rozpoznávanie overovacej karty pre overovacie zariadenie môžete skontrolovať z ovládacieho panela skenera.

Keď vyberiete položky **Nastav.** > **Informácie o zariadení** > **Stav overenia zariadenia**, zobrazia sa informácie.

Potvrdenie rozpoznania overovacej karty

Rozpoznanie overovacích kariet môžete skontrolovať pomocou aplikácie Web Config.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Správa zariadenia** > **Čítačka kariet**.
2. Podržte overovaciu kartu na čítačke overovacích kariet.
3. Kliknite na položku **Začiarknuť**.

Zobrazí sa výsledok.

Riešenie problémov s overovacím zariadením

Overovacia karta sa nedá čítať

Skontrolujte nasledujúce.

- Skontrolujte, či je overovacie zariadenie správne pripojené k skeneru.
Pripojte overovacie zariadenie k USB portu externého rozhrania na zadnej strane skenera.
- Skontrolujte, či majú overovacie zariadenia a overovacia karta certifikát.
Informácie o podporovaných overovacích zariadeniach a kartách vám poskytne predajca.

Údržba

Čistenie vonkajšej časti skenera.	126
Čistenie vnútra skenera.	126
Výmena súpravy valca.	131
Vynulovanie počtu skenovaní po výmene valcov.	136
Úsporný režim.	137
Preprava skenera.	137
Zálohovanie nastavení.	138
Obnoviť štand. nastavenia.	139
Aktualizácia aplikácií a firmvéru.	140


Čistenie vonkajšej časti skenera

Utrite všetky škvرنy na vonkajšom obale suchou handričkou alebo handričkou navlhčenou saponátom a vodou.



Upozornenie:

- Na čistenie skenera nikdy nepoužívajte alkohol, riedidlo ani iný korozívny roztok. Môže dôjsť k deformácii alebo zblednutiu farieb.
- Nedovoľte, aby sa do výrobku dostala voda. Mohlo by dôjsť k poškodeniu.
- Nikdy neotvárajte kryt skenera.

1. Stlačením tlačidla  vypnite skener.
2. Odpojte sieťový napájací adaptér od skenera.
3. Vonkajší kryt utrite utierkou navlhčenou v roztoku mierneho čistiaceho prostriedku a vody.

Poznámka:

Utrite dotykovú obrazovku mäkkou suchou handričkou.

Čistenie vnútra skenera

Po určitej dobe používania skenera môže prach z papiera a miestnosti na valci alebo na sklenenej časti vo vnútri skenera spôsobovať problémy s podávaním papiera alebo kvalitou naskenovaného obrazu. Vyčistíte vnútro skenera po každých 5,000 skenovaní.


Aktuálny počet skenovaní zistíte na ovládacom paneli alebo v pomôcke Epson Scan 2 Utility.

Ak je povrch znečistený ťažko odstrániteľným materiálom, použite na odstránenie škvرن čistiacu súpravu Epson. Pomocou malého množstva čistiaceho prostriedku na čistiacej handričke odstráňte škvرنy.

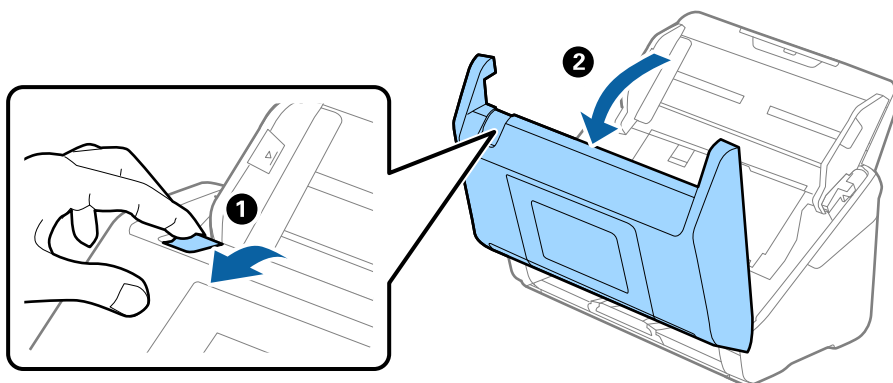


Upozornenie:

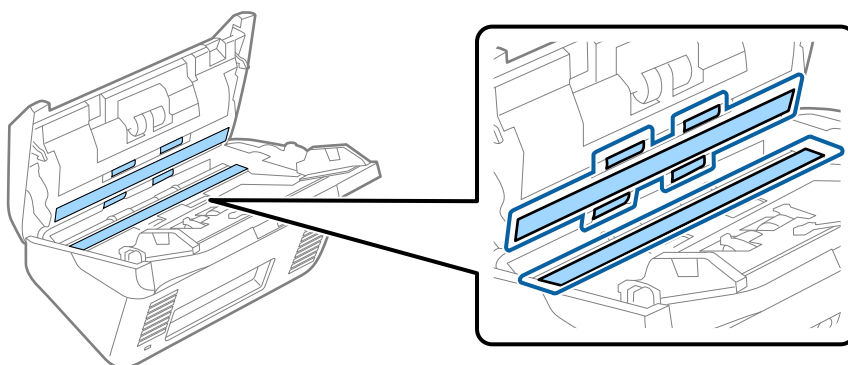
- Na čistenie skenera nikdy nepoužívajte alkohol, riedidlo ani iný korozívny roztok. Môže dôjsť k deformácii alebo zblednutiu farieb.
- Nikdy nestriekajte žiadnu tekutinu ani mazivo na skener. Pri poškodení zariadenia alebo obvodov môže dôjsť k nezvyčajným činnostiam.
- Nikdy neotvárajte kryt skenera.

1. Stlačením tlačidla  vypnite skener.
2. Odpojte sieťový napájací adaptér od skenera.

3. Potiahnite páčku a otvorte kryt skenera.



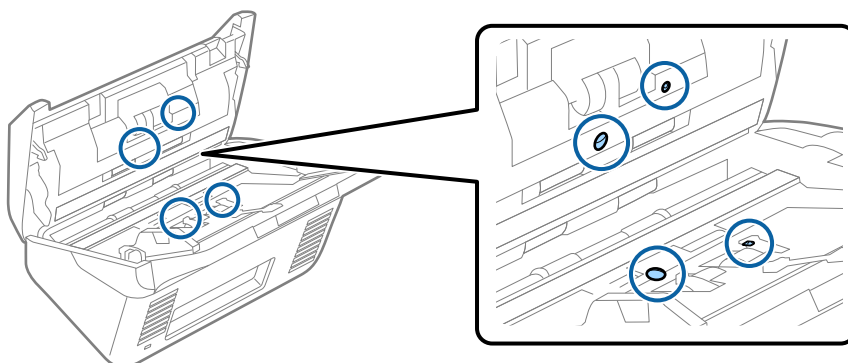
4. Utrite všetky škrvy na plastovom valci (4 miesta) a sklenenom povrchu na spodnej strane vnútra skenera. Utrite mäkkou handričkou bez chlôpk navlhčenou malým množstvom čistiaceho prostriedku alebo vodou.



! **Upozornenie:**

- Na sklenený povrch netlačte príliš silno.
- Nepoužívajte kefu ani tvrdé nástroje. Akékoľvek poškrabanie skla môže ovplyvniť kvalitu skenovania.
- Čistiaci prostriedok nestriekajte priamo na sklenený povrch.

5. Vatovou tyčinkou utrite všetky škrvy na snímačoch.

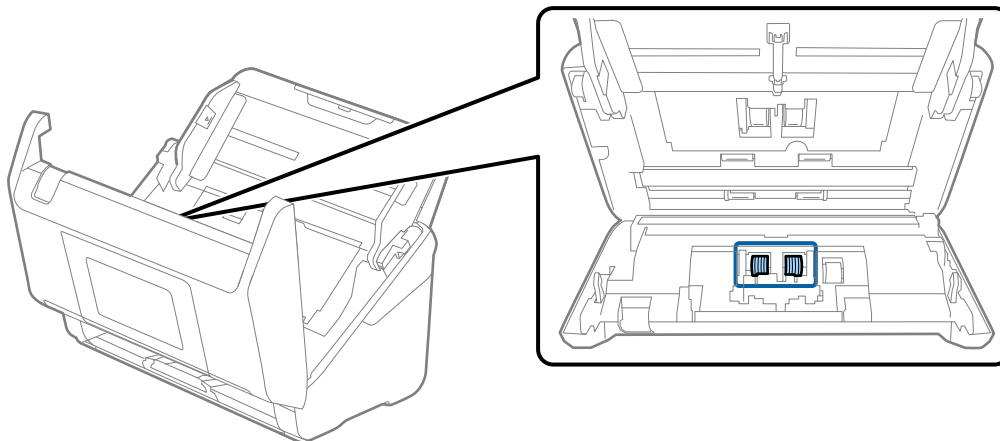




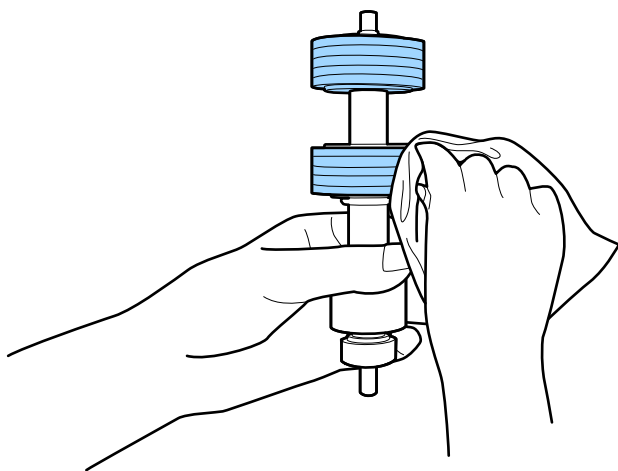
Upozornenie:

Na vatovej tyčinke nepoužívajte žiadne tekutiny, napríklad čistiace prostriedky.

6. Otvorte kryt a potom vytiahnite oddeľovací valec.
Ďalšie podrobnosti nájdete v časti „Výmena súpravy valca“.



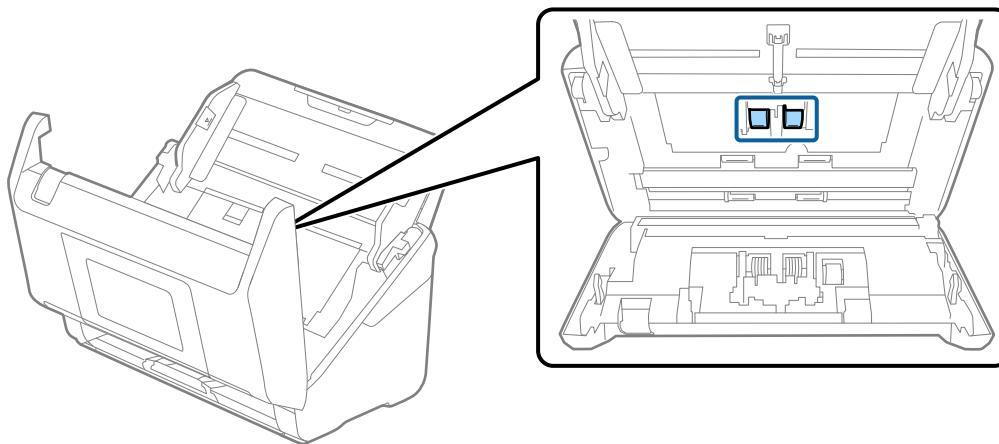
7. Utrite oddeľovací valec. Utrite mäkkou handričkou bez chĺpkov navlhčenou malým množstvom čistiaceho prostriedku alebo vodou.



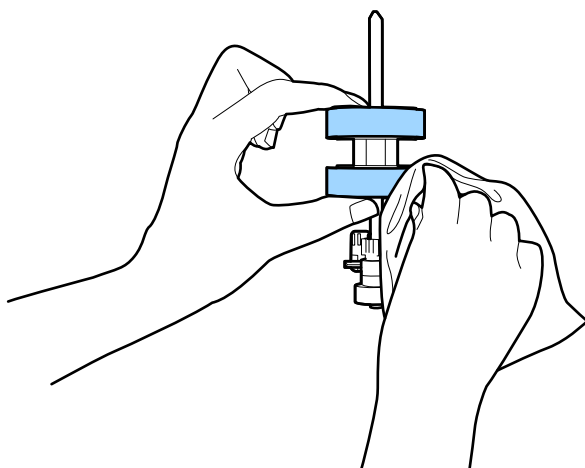
Upozornenie:

Na čistenie valca používajte iba originálnu čistiacu súpravu Epson alebo mäkkú navlhčenú handričku. Suchou handričkou by ste mohli poškodiť povrch valca.

- Otvorte kryt a potom vytiahnite podávací valec.
Ďalšie podrobnosti nájdete v časti „Výmena súpravy valca“.



- Utrite podávací valec. Utrite mäkkou handričkou bez chĺpkov navlhčenou malým množstvom čistiaceho prostriedku alebo vodou.

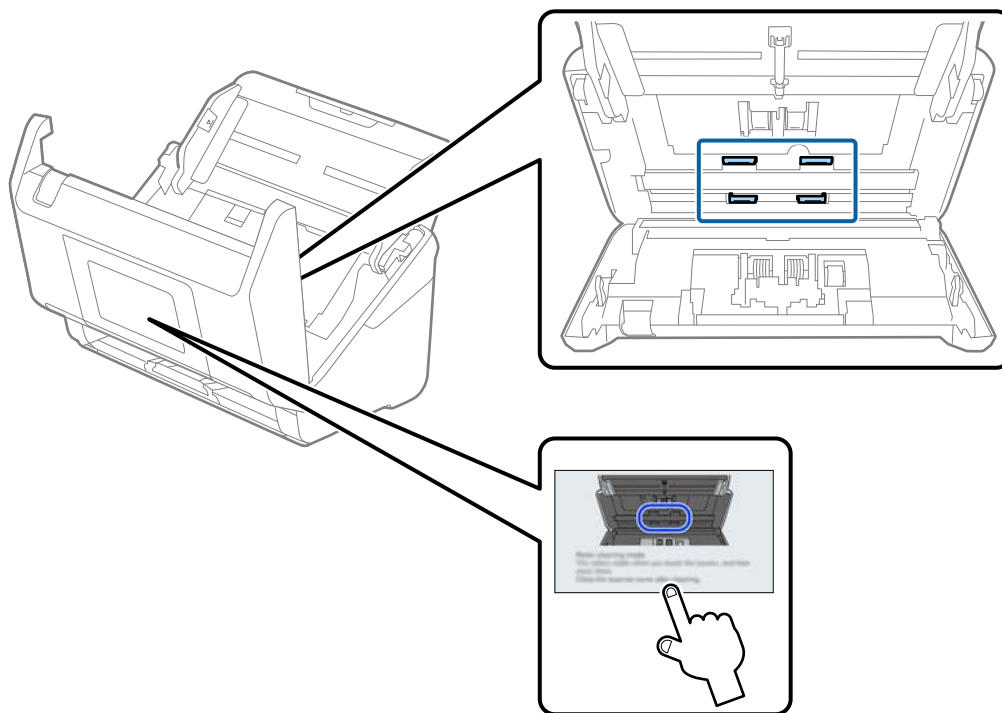


Upozornenie:

Na čistenie valca používajte iba originálnu čistiacu súpravu Epson alebo mäkkú navlhčenú handričku. Suchou handričkou by ste mohli poškodiť povrch valca.

- Zatvorte kryt skenera.
- Zapojte sieťový napájací adaptér a potom zapnite skener.
- Na hlavnej obrazovke vyberte položku **Údržba skenera**.
- Na obrazovke **Údržba skenera** vyberte možnosť **Čistenie valčekov**.
- Potiahnutím páčky otvorte kryt skenera.
Skener prejde do režimu čistenia valcov.

15. Pomaly otáčajte valcami za spodok klepnutím kdekoľvek na LCD obrazovke. Utrite valce pomocou originálnej čistiacej súpravy Epson alebo mäkkou a vodou navlhčenou handričkou. Opakujte, kým nebudú valce čisté.



Upozornenie:

Pri činnosti valca si dávajte pozor na zachytenie rúk alebo vlasov do mechanizmu. Mohlo by dôjsť k úrazu.

16. Zatvorte kryt skenera.

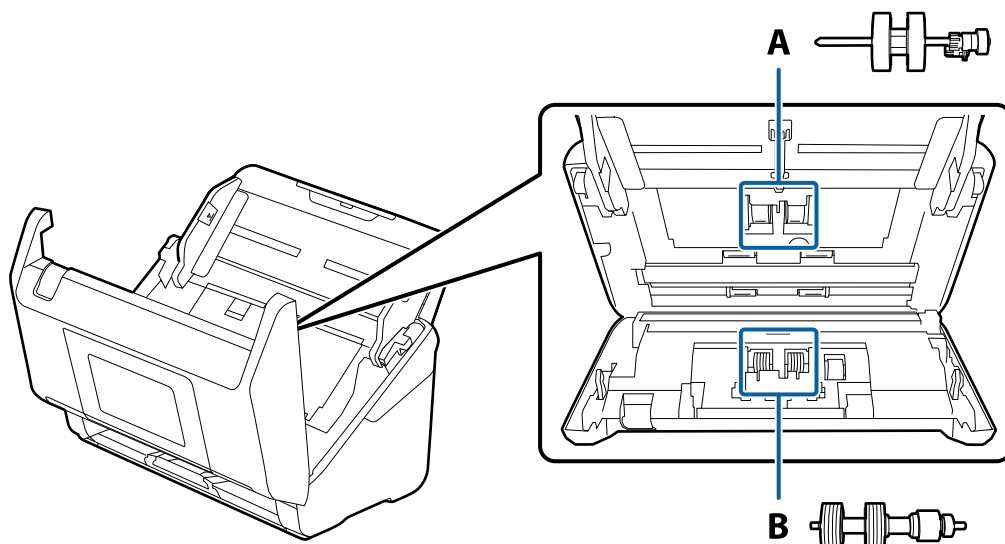
Skener ukončí režim čistenia valcov.

Súvisiace informácie


➔ „Výmena súpravy valca” na strane 131

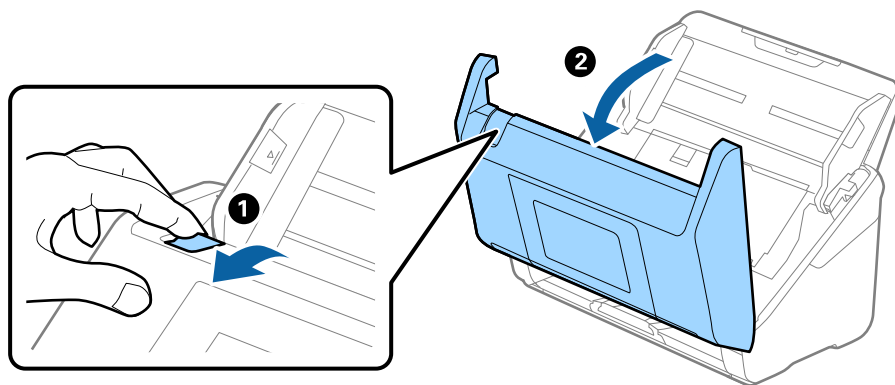
Výmena súpravy valca

Súpravu valca (podávací valec a oddeľovací valec) je potrebné vymeniť, keď počet skenovaní prekročí životný cyklus valcov. Keď sa na ovládacom paneli alebo na obrazovke počítača zobrazí hlásenie o výmene, vymeňte ich podľa nasledujúceho postupu.

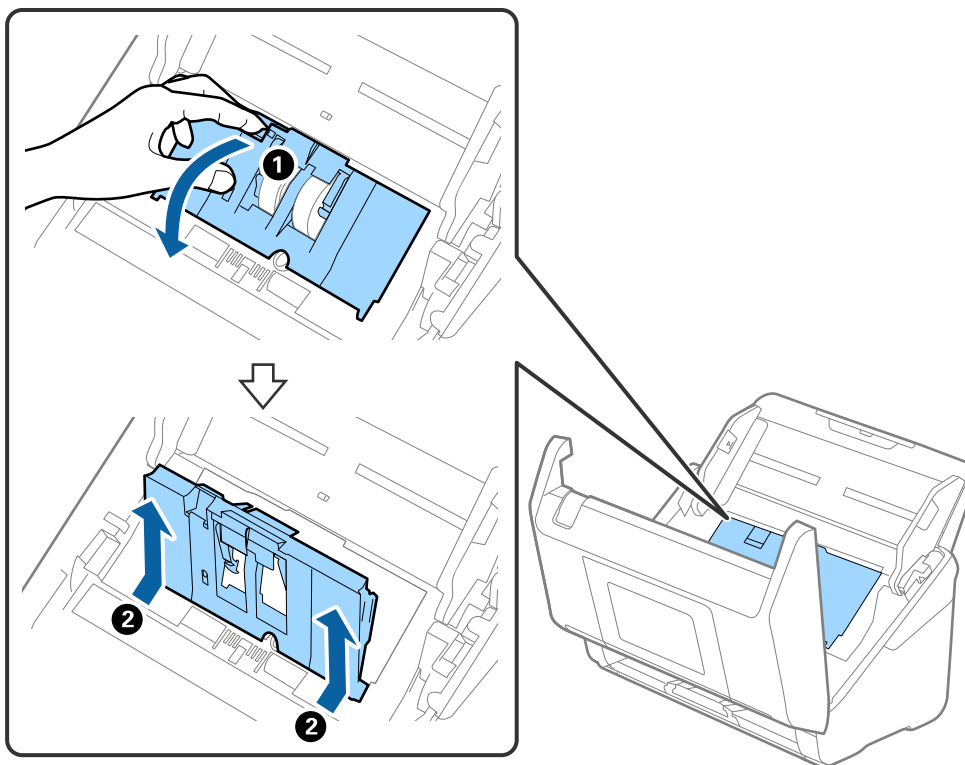


A: podávací valec, B: oddeľovací valec

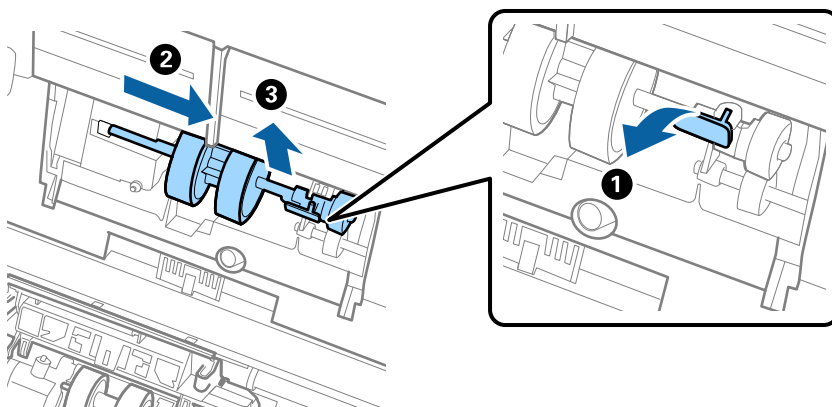
1. Stlačením tlačidla  vypnite skener.
2. Odpojte sieťový napájací adaptér od skenera.
3. Potiahnite páčku a otvorte kryt skenera.



4. Otvorte kryt podávacieho valca a potom ho posuňte a vytiahnite.



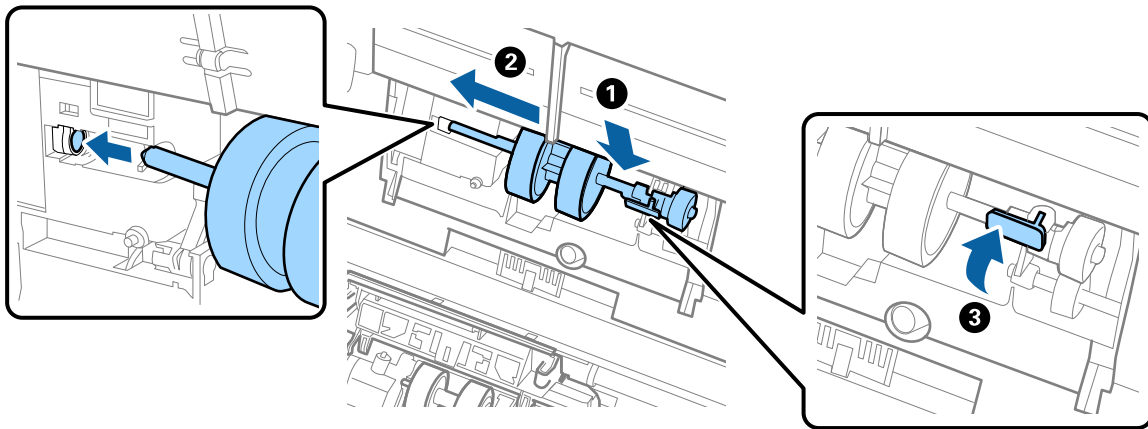
5. Zatlačte úchytku osi valca a potom posuňte a vytiahnite nainštalované podávacie valce.



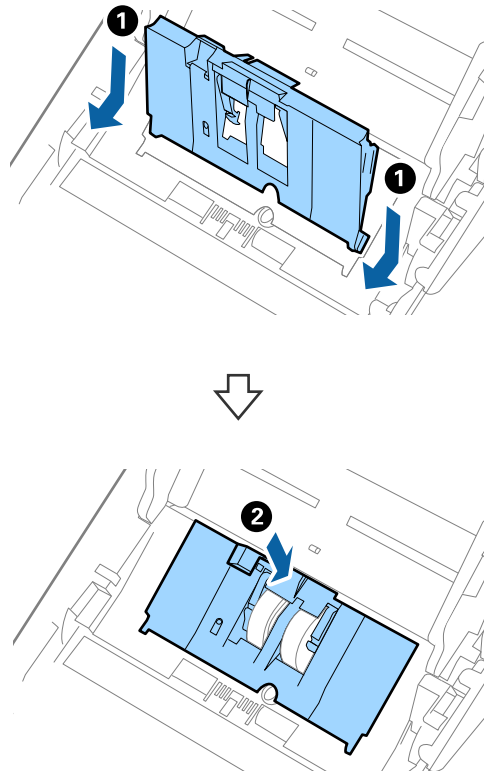
Upozornenie:

Nevytahujte podávací valec násilím. Mohlo by dôjsť k poškodeniu vnútra skenera.

6. Súčasne zatlačte úchytku a zasuňte nový podávací valec doľava, potom ho vložte do otvoru v skeneri. Zatlačením úchytky to zaistíte.

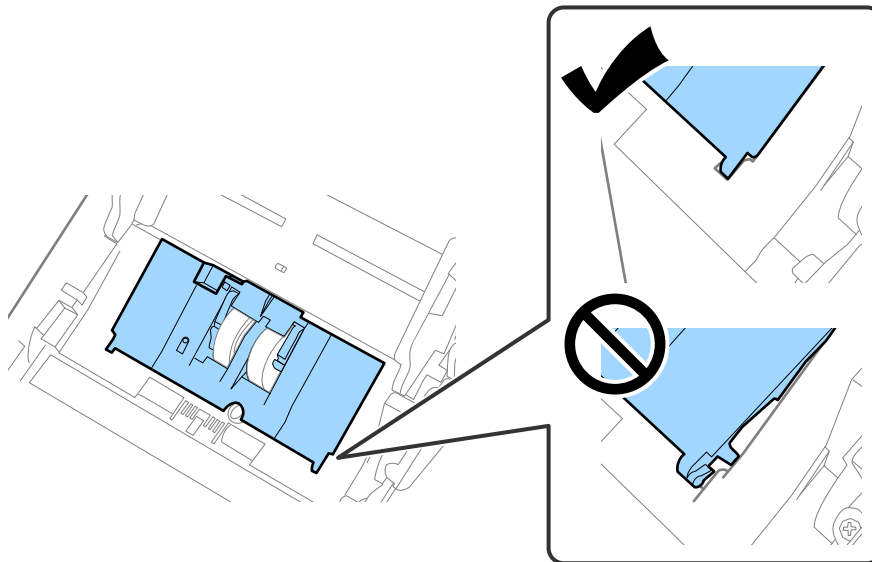


7. Vložte hranu krytu podávacieho valca do drážky a zasuňte. Pevne zatvorte kryt.

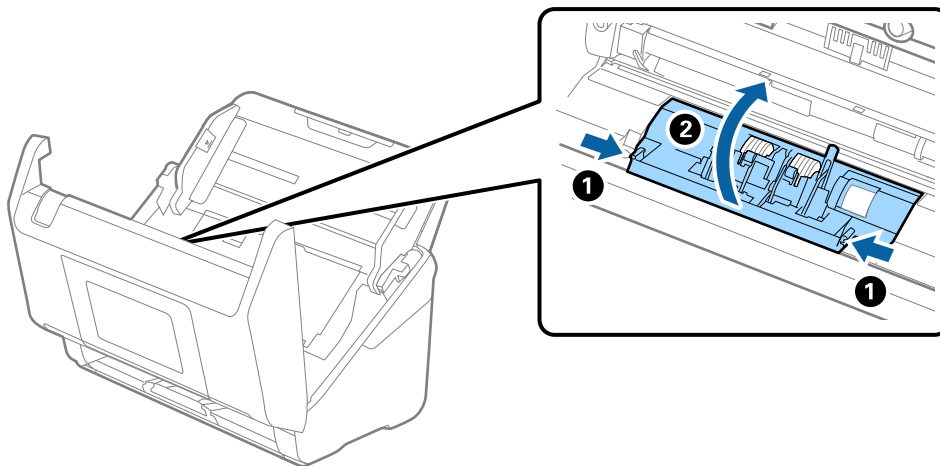


! **Upozornenie:**

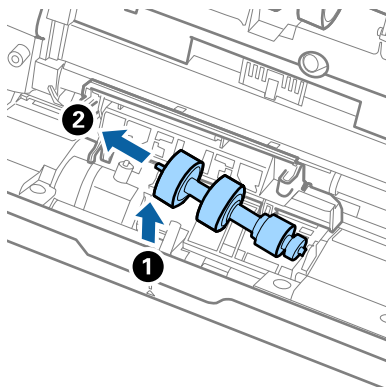
- Skontrolujte, či je kryt podávacieho valca správne zatvorený.
- Ak sa kryt ťažko zatvára, uistite sa, či sú podávacie valce nainštalované správne.
- Neinštalujte kryt, kým je to nadvihnuté.



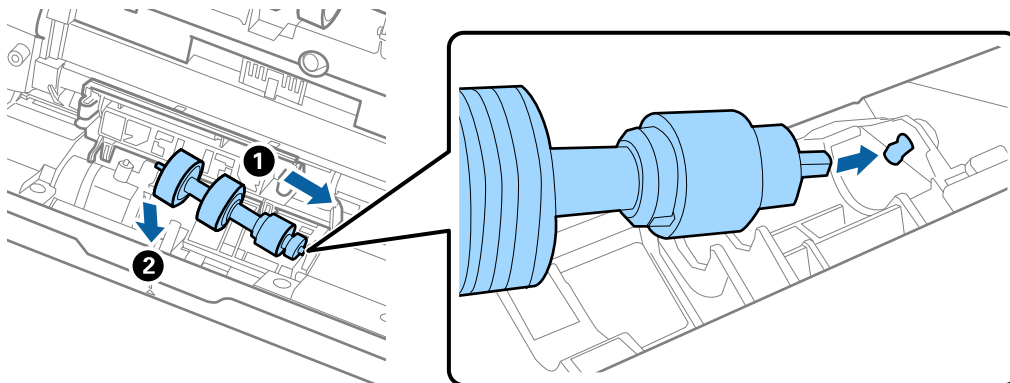
8. Stlačte háčiky na oboch koncoch oddeľovacieho valca, čím otvoríte kryt.



9. Nadvihnite ľavú stranu oddeľovacieho valca a potom posuňte a vytiahnite nainštalované oddeľovacie valce.



10. Vložte os nového oddeľovacieho valca do otvoru na pravej strane a potom dajte valec dole.



11. Zatvorte kryt oddeľovacieho valca.



Upozornenie:

Ak sa kryt zatvára ťažko, uistite sa, či sú oddeľovacie valce nainštalované správne.

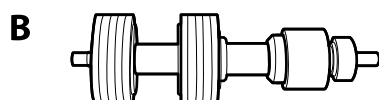
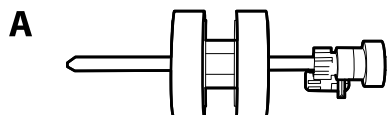
12. Zatvorte kryt skenera.
13. Zapojte sieťový napájací adaptér a potom zapnite skener.
14. Vynulujte počet skenovaní na ovládacom paneli.

Poznámka:

Zlikvidujte podávací valec a oddeľovací valec podľa predpisov a smerníc miestnych úradov. Nerozoberajte ich.

Kódy súprav valca

Súčasti (podávací valec a oddeľovací valec) je potrebné vymeniť, keď počet skenovaní prekročí servisné číslo. Aktuálny počet skenovaní zistíte na ovládacom paneli alebo v pomôcke Epson Scan 2 Utility.



A: podávací valec, B: oddeľovací valec

Názov súčasti	Kódy	Životný cyklus
Súprava valca 2	B12B819711 B12B819721 (len pre Indiu)	200,000*

* Toto číslo bolo dosiahnuté postupným skenovaním pomocou testovacích originálnych papierov značky Epson a slúži ako pomôcka pre cyklus výmeny. Cyklus výmeny sa môže líšiť v závislosti od rozličných typov papiera. Napríklad papier, ktorý vytvára množstvo papierového prachu alebo papier s drsným povrchom, môžu životný cyklus skracovať.

Vynulovanie počtu skenovaní po výmene valcov

Po výmene súpravy valcov vynulujte počet skenovaní pomocou ovládacieho panela alebo nástroja Epson Scan 2 Utility.

V tejto časti je vysvetlené, ako resetovať pomocou ovládacieho panela.

1. Na hlavnej obrazovke klepnite na položku **Údržba skenera**.
2. Klepnite na tlačidlo **Výmena servisných valčekov**.
3. Klepnite na tlačidlo **Vynulovať počet skenovaní**.
4. Vyberte **Počet skenov po výmene valčeka** a potom klepnite na položku **Áno**.

Poznámka:

Ak chcete obnoviť kontrolu v položke Epson Scan 2 Utility, spustíte aplikáciu Epson Scan 2 Utility, kliknite na kartu **Počítadlo** a potom skontrolujte **Obnoviť** v položke **Súprava valca**.

Súvisiace informácie

➔ „Výmena súpravy valca” na strane 131

Úsporný režim

Energiu môžete šetriť pomocou režimu spánku alebo režimu automatického vypnutia, ak sa skenerom nevykonávajú žiadne činnosti. Môžete nastaviť časový limit, po uplynutí ktorého skener prejde do režimu spánku a automaticky sa vypne. Každé zvýšenie má vplyv na energetickú účinnosť výrobku. Pred vykonaním akýchkoľvek zmien zohľadnite dopad na životné prostredie.


1. Na hlavnej obrazovke vyberte položku **Nastav.**
2. Vyberte položku **Zákl. nastavenia**.
3. Vyberte možnosť **Časovač režimu spánku** alebo **Nast. vyp. napáj.** a potom vykonajte nastavenia.

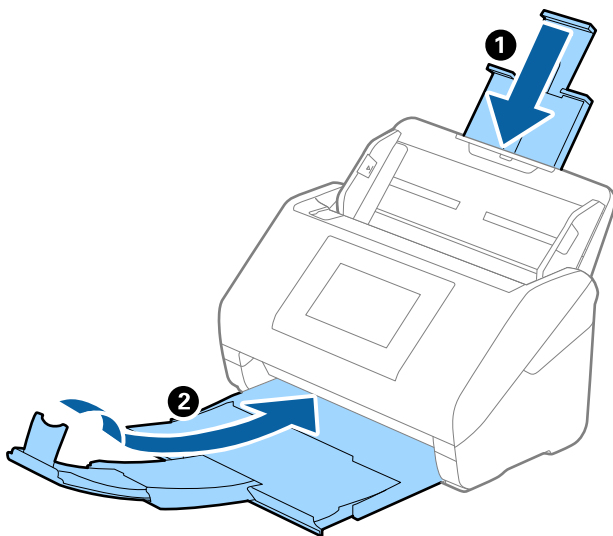
Poznámka:

Dostupné funkcie sa môžu líšiť v závislosti od miesta zakúpenia.

Preprava skenera

Ak je potrebné prepraviť skener na určitú vzdialenosť alebo do opravy, zabaľte skener podľa nasledujúceho postupu.

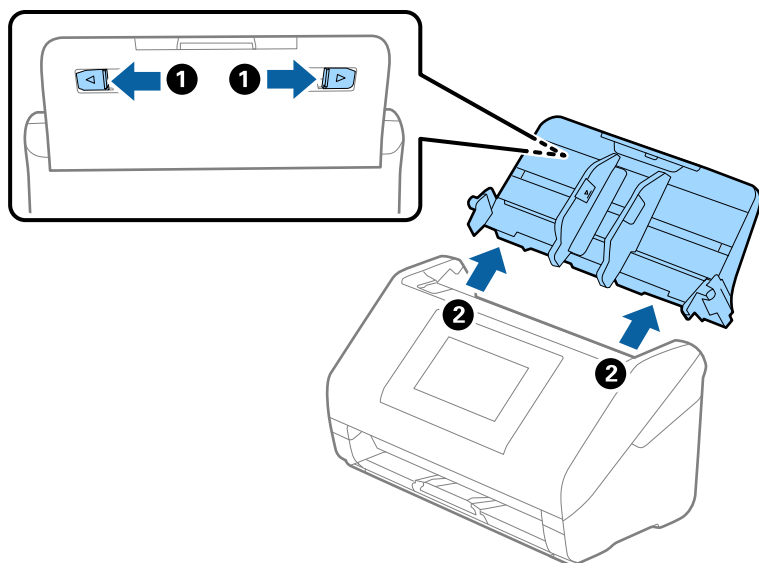
1. Stlačením tlačidla  vypnite skener.
2. Odpojte sieťový napájací adaptér.
3. Odpojte káble a zariadenia.
Odstráňte voliteľnú alebo dodanú stránku Paper Alignment Plate, ak je pripojená.
4. Zatvorte predĺženie vstupného zásobníka a výstupný zásobník.



Upozornenie:

Nezabudnite poriadne zavrieť výstupný zásobník, inak by sa mohol počas prenášania poškodiť.

5. Odnímte vstupný zásobník.



6. Nasadte obalové materiály dodané so skenerom a potom ho zabalte do pôvodnej alebo podobnej škatule.

Zálohovanie nastavení

Hodnotu nastavenia môžete exportovať z aplikácie Web Config do súboru. Môžete to použiť na zálohovanie kontaktov, hodnôt nastavenia, výmenu skenera atď.

Exportovaný súbor sa nedá upraviť, pretože ide o binárny súbor.

Export nastavení

Export nastavenia skenera.

1. Otvorte aplikáciu Web Config a potom vyberte kartu **Správa zariadenia > Hodnota nastavenia exportu a importu > Exportovať**.
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. Zadajte heslo na zašifrovanie exportovaného súboru.
Na import súboru je potrebné heslo. Ak nechcete súbor zašifrovať, nechajte to prázdne.
4. Kliknite na položku **Exportovať**.

! **Upozornenie:**

*Ak chcete exportovať nastavenia siete skenera, ako napríklad názov tlačiarne a adresa IPv6, vyberte možnosť **Zapnite**, ak chcete vybrať jednotlivé nastavenia zariadenia a potom vyberte ďalšie položky. Pre náhradný skener vyberte iba vybrané hodnoty.*

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Import nastavení

Importujte vyexportovaný súbor aplikácie Web Config do skenera.



Upozornenie:

Keď importujete hodnoty obsahujúce individuálne údaje, ako sú napríklad názov skenera alebo IP adresa, uistite sa, či rovnaká IP adresa v tej istej sieti neexistuje.

1. Otvorte aplikáciu Web Config a vyberte kartu **Správa zariadenia > Hodnota nastavenia exportu a importu > Importovať**.
2. Vyberte exportovaný súbor a potom zadajte zašifrované heslo.
3. Kliknite na položku **Ďalej**.
4. Vyberte nastavenia, ktoré chcete importovať, a potom kliknite na tlačidlo **Ďalej**.
5. Kliknite na položku **OK**.

Nastavenia sa použijú v skeneri.

Súvisiace informácie

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači” na strane 37

Obnoviť štand. nastavenia

Na ovládacom paneli vyberte položky **Nastav. > Správa systému > Obnoviť štand. nastavenia**, a potom vyberte položky, ktoré chcete obnoviť na predvolené voľby.

- Nastavenie siete: obnovenie prvotného stavu nastavení týkajúcich sa siete.
- Všetky okrem Nastavení siete: obnovenie prvotného stavu nastavení, okrem nastavení týkajúcich sa siete.
- Všetky nastavenia: obnovenie všetkých nastavení do prvotného stavu pri zakúpení.



Upozornenie:

*Ak vyberiete možnosť **Všetky nastavenia**, všetky údaje nastavenia zaregistrované na skeneri (vrátane kontaktov) sa odstránia. Odstránené nastavenia nemožno obnoviť.*

Poznámka:

Nastavenia môžete vykonať aj v položke Web Config.

Karta **Správa zariadenia > Obn. predv. nast.**

Aktualizácia aplikácií a firmvéru

Aktualizáciou aplikácií a firmvéru je možné odstrániť určité problémy a zlepšiť alebo pridať niektoré funkcie. Uistite sa, že používate najnovšiu verziu aplikácií a firmvéru.



Upozornenie:

- Počas aktualizácie nevypínajte počítač ani skener.

Poznámka:

Ak sa dá skener pripojiť k internetu, môžete aktualizovať firmvér z aplikácie Web Config. Vyberte kartu **Správa zariadenia** > **Aktualizácia firmvéru**, skontrolujte zobrazené hlásenie a kliknite na tlačidlo **Spustiť**.

- Uistite sa, že je skener pripojený k počítaču a že je počítač pripojený k internetu.
- Spustite EPSON Software Updater a aktualizujte aplikácie alebo firmvér.

Poznámka:

Operačné systémy Windows Server nie sú podporované.

- Windows 11

Kliknite na tlačidlo Štart a vyberte položky **Všetky aplikácie** > **Epson Software** > **EPSON Software Updater**.

- Windows 10

Kliknite na tlačidlo Štart a potom vyberte položky **Epson Software** > **EPSON Software Updater**.

- Windows 8.1/Windows 8

Zadajte názov aplikácie do kľúčového tlačidla Vyhľadávanie, a potom vyberte zobrazenú ikonu.

- Windows 7

Kliknite na tlačidlo Štart a potom vyberte položky **Všetky programy** alebo **Programy** > **Epson Software** > **EPSON Software Updater**.

- Mac OS

Zvoľte položku **Finder** > **Prejsť** > **Aplikácie** > **Epson Software** > **EPSON Software Updater**.

Poznámka:

Ak sa v zozname nenachádza aplikácia, ktorú chcete aktualizovať, jej aktualizácia pomocou nástroja EPSON Software Updater nie je možná. Skontrolujte dostupnosť najnovších verzií aplikácií na lokálnej webovej lokalite spoločnosti Epson.

<http://www.epson.com>

Aktualizácia firmvéru skenera pomocou ovládacieho panela

Ak sa dá skener pripojiť k internetu, môžete aktualizovať firmvér skenera pomocou ovládacieho panela. Môžete tiež nastaviť, aby skener pravidelne overoval aktualizácie firmvéru a upozornil vás, ak sú nejaké k dispozícii.

- Na hlavnej obrazovke vyberte položku **Nastav.**
- Vyberte položky **Správa systému** > **Aktualizácia firmvéru** > **Aktualizovať**.

Poznámka:

Vyberte možnosť **Oznámenie** > **Zap.**, čím nastavíte, aby skener pravidelne overoval dostupné aktualizácie firmvéru.

3. Skontrolujte hlásenie zobrazené na obrazovke a spustíte vyhľadávanie dostupných aktualizácií.
4. Ak sa na LCD obrazovke zobrazí hlásenie s informáciou, že je k dispozícii aktualizácia, postupujte podľa pokynov na obrazovke a spustíte aktualizáciu.



Upozornenie:

- Kým nebude aktualizácia dokončená, nevypínajte ani neodpájajte skener. V opačnom prípade by mohlo dôjsť k poruche skenera.*
- Ak sa aktualizácia firmvéru nedokončí, prípadne nepodarí, skener sa nespustí normálne a na LCD obrazovke sa pri nasledujúcom zapnutí skenera zobrazí hlásenie „Recovery Mode“. V takom prípade je potrebné aktualizovať firmvér znova pomocou počítača. Pripojte skener k počítaču pomocou USB kábla. Dokým je na skeneri zobrazený nápis „Recovery Mode“, nie je možné aktualizovať firmvér cez sieťové pripojenie. Na počítači otvorte svoju webovú stránku spoločnosti Epson a potom si prevezmite najnovší firmvér skenera. Ďalšie kroky nájdete v pokynoch na webovej stránke.*

Aktualizácia firmvéru pomocou aplikácie Web Config

Ak sa dá skener pripojiť k internetu, môžete aktualizovať firmvér z aplikácie Web Config.

1. Otvorte aplikáciu Web Config a vyberte kartu **Správa zariadenia > Aktualizácia firmvéru**.
2. Kliknite na tlačidlo **Spustiť** a potom postupujte podľa pokynov na obrazovke.

Spustí sa overenie firmvéru. Ak existuje aktualizovaný firmvér, zobrazia sa informácie o firmvéri.

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

➔ „Ako spustiť funkciu Web Config v internetovom prehliadači“ na strane 37

Aktualizácia firmvéru bez pripojenia k internetu

Do počítača si môžete prevziať firmvér zariadenia z webovej stránky Epson a potom prepojiť zariadenie a počítač káblom USB a aktualizovať firmvér. If you cannot update over the network, try this method.

Poznámka:

Pred aktualizáciou sa uistite, že je v počítači nainštalovaný ovládač skenera Epson Scan 2. Ak aplikácia Epson Scan 2 nie je nainštalovaná, nainštalujte ju znova.

1. Najnovšie aktualizácie firmvéru nájdete na webovej lokalite spoločnosti Epson.
<http://www.epson.com>
 - Ak je k dispozícii firmvér pre váš skener, stiahnite ho a prejdite na ďalší krok.
 - Ak na webovej lokalite nie sú žiadne informácie o firmvéri, používate už najnovší firmvér.
2. Pripojte počítač obsahujúci prevzatý firmvér k skeneru káblom USB.

3. Dvakrát kliknite na prevzatý súbor .exe.
Spustí sa aplikácia Epson Firmware Updater.
4. Postupujte podľa pokynov na obrazovke.