EPSON

DS-900WN DS-800WN

Ръководство на администратора

NPD7398-00 BG

Авторско право

Търговски марки

- ❏ 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.
- ❏ Общо известие: всички други търговски марки са притежание на съответните им собственици и се използват само за целите на идентификация.

Съдържание

Основни настройки за сигурност

Разширени настройки за сигурност

Употреба на Epson Open Platform

Монтиране на устройство за удостоверяване

Поддръжка

Въведение

Съдържанието на този документ

Този документ предоставя следната информация за администраторите на скенера.

❏ Мрежови настройки

❏ Подготовка на функцията на сканиране

❏ Активиране и управление на настройките за сигурност

❏ Извършвайте ежедневна поддръжка

За стандартните методи за използване на скенера вижте *Ръководство на потребителя*.

Използване на това ръководство

Знаци и символи

Внимание:

Инструкции, които трябва да се следват внимателно, за да се избегнат наранявания.

Важно:

Инструкции, които трябва да се спазват внимателно, за да се избегнат повреди на оборудването.

Забележка:
Предоставя допълнителна и справочна информация.

Още по темата

➡ Връзки към свързани раздели.

Описания, използвани в ръководството

❏ Снимките на екраните са от Windows 10 или macOS High Sierra. Съдържанието, показвано на екраните, може да се различава според модела и ситуацията.

❏ Илюстрациите, използвани в ръководството, са само за справка. Въпреки че е възможно те да се различават до известна степен от действителния продукт, методите на работа са едни и същи.

Справки за операционните системи

Windows

Употребените в това ръководство термини, като например "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" и "Windows Server 2008" се отнасят до следните операционни системи. В допълнение, „Windows“ се отнася към всички версии.

- ❏ Операционна система Microsoft® Windows® 11
- ❏ Операционна система Microsoft® Windows® 10
- ❏ Операционна система Microsoft® Windows® 8.1
- ❏ Операционна система Microsoft® Windows® 8
- ❏ Операционна система Microsoft® Windows® 7
- ❏ Операционна система Microsoft® Windows Server® 2022
- ❏ Операционна система Microsoft® Windows Server® 2019
- ❏ Операционна система Microsoft® Windows Server® 2016
- ❏ Операционна система Microsoft® Windows Server® 2012 R2
- ❏ Операционна система Microsoft® Windows Server® 2012
- ❏ Операционна система Microsoft® Windows Server® 2008 R2
- ❏ Операционна система Microsoft® Windows Server® 2008

Mac OS

В настоящото ръководство „Mac OS“ се отнася до Mac OS X 10.9 или по-нови версии, както и до macOS 11 или по-нови версии.

Забележки относно паролата на администратора

Забележки относно паролата на администратора

Това устройство Ви позволява да зададете парола на администратор, за да предотвратите неоторизирани трети страни да осъществяват достъп до и да променят настройките на устройството или на мрежата, съхранени в устройството, когато е свързано към мрежа.

Ако зададете парола на администратор, се налага да въвеждате паролата, когато променяте настройките в софтуера за конфигурация, като например Web Config.

Първоначалната парола на администратор е зададена на скенера, но можете да я смените на всякаква парола.

Първоначална парола на администратор

Първоначалната парола на администратор зависи от етикета, прикрепен на продукта. Ако на гърба има прикрепен етикет „PASSWORD“, въведете 8-цифрения номер, показан на етикета. Ако няма прикрепен етикет „PASSWORD“, въведете серийния номер на етикета, прикрепен на гърба на продукта, за първоначална парола на администратор.

Препоръчваме да промените първоначалната администраторска парола от настройката по подразбиране.

Забележка:
Не е зададено потребителско име по подразбиране.

Операции, които изискват паролата на администратор

Ако от Вас се изисква да въведете паролата на администратор по време на следните операции, въведете паролата на администратор, зададена на продукта.

- ❏ Когато влизате в разширените настройки за Web Config
- ❏ Когато използвате меню в контролния панел, което е било заключено от администратора
- ❏ Когато променяте настройките на устройството в приложението
- ❏ Когато актуализирате фърмуера на устройството
- ❏ Когато променяте или нулирате паролата на администратора

Промяна на парола на администратора

Можете да промените от контролния панел на продукта или в Web Config.

Когато промените паролата, новата парола трябва да е с дължина от 8 до 20 знака и да съдържа само еднобайтови буквено-цифрови знаци и символи.

Нулиране на паролата на администратора

Можете да нулирате паролата на администратора до първоначалните настройки от контролния панел на продукта или в Web Config.

Ако сте забравили паролата и не можете да я нулирате до настройките по подразбиране, продуктът трябва да бъде поправен. Свържете се с Вашия местен дилър.

Необходими настройки, които отговарят на Вашите нужди

Необходими настройки, които отговарят на Вашите нужди

Вижте следното, за да направите необходимите настройки, които да отговарят на Вашата цел.

Свързване на скенера към мрежата

Цел	Необходими настройки
Искам да свържа скенера към мрежата.	Настройте скенера за мрежово сканиране. "Свързване на скенера към мрежата" на страница 17
Искам да свържа скенера към нов компютър.	Задайте мрежовите настройки за Вашия скенер на новия компютър. "Добавяне или подмяна на компютър или устройства" на страница 24

Настройки за сканиране

Цел	Необходими настройки
Искам да изпратя сканирани изображения по имейл. (Scan to Email)	1. Настройте сървъра на електронната поща, който искате да свържете. "Регистриране на имейл сървър" на страница 47 2. Регистрирайте имейл адреса на получателя **Contacts** (опция). Като регистрирате имейл адреса, не е нужно да го въвеждате всеки път, когато искате да изпратите нещо, можете просто да го изберете от Вашите контакти. "Направете контактите достъпни" на страница 57
Искам да запиша сканирани изображения в папка в мрежата. (Scan to Network Folder/FTP)	1. Създайте папка в мрежата, където искате да запаметите изображенията. "Създаване на мрежова папка" на страница 50 2. Регистрирайте пътя към папката в **Contacts** (опция). Като регистрирате пътя към папката, не е нужно да го въвеждате всеки път, когато искате да изпратите нещо, можете просто да го изберете от Вашите контакти. "Направете контактите достъпни" на страница 57
Искам да запиша сканирани изображения в облачна услуга. (Scan to Cloud)	Настройте Epson Connect. За подробности относно настройката вижте уебпортала Epson Connect. Когато настройвате, имате нужда от потребителски акаунт за услугата за онлайн съхранение, към която искате да се свържете. https://www.epsonconnect.com/ http://www.epsonconnect.eu (само за Европа)

Персонализиране на дисплея на контролния панел

Цел	Необходими настройки
Искам да променя елементите, показани на контролния панел на скенера.	Задайте **Предв.настр.** или **Редактиране Нач. екран**. Можете да регистрирате предпочитаните си настройки за сканиране в контролния панел и да редактирате показаните елементи. "Персонализиране на дисплея на контролния панел" на страница 70

Настройка на основни функции за сигурност

Цел	Необходими настройки
Искам да попреча на всеки друг освен администратора да променя настройките на скенера.	Задайте администраторска парола за скенера. "Настройки на администратора" на страница 79
Искам да дезактивирам използването на скенери с USB връзки.	Дезактивирайте външния интерфейс. "Дезактивиране на външния интерфейс" на страница 87

Настройка на разширени функции за сигурност

Цел	Необходими настройки
Искам да контролирам кои протоколи да използвам.	Активирайте или дезактивирайте протоколите. "Управление чрез протоколи" на страница 95
Искам да криптирам комуникационния път.	1. Настройте Вашия цифров сертификат. "Използване на цифров сертификат" на страница 98 2. Настройте SSL/TLS комуникация. "SSL/TLS комуникация със скенера" на страница 104
Искам да използвам криптирана комуникация (IPsec). Искам да мога да използвам софтуера само от конкретен компютър (IP филтриране).	Задайте правила за филтриране на трафика. "Криптирана комуникация с IPsec/IP филтриране" на страница 105
Искам да използвам скенер в мрежа IEEE802.1X.	Задайте IEEE802.1X за скенера. "Свързване на скенера към мрежа IEEE802.1X" на страница 116

Синхронизиране на скенера със система за удостоверяване

Вземете продуктов ключ от специализирания уебсайт и активирайте Epson Open Platform на Вашия скенер.

"Употреба на Epson Open Platform" на страница 125

Използване на опция за удостоверяване (Epson Print Admin/Epson Print Admin Serverless)

Трябва да имате лицензионен ключ, за да използвате опцията.

Свържете се с Вашия търговец за повече информация.

Забележка:
Вие не можете да използвате Epson Print Admin Serverless, когато системата е синхронизирана с Epson Open Platform.

Мрежови настройки

Свързване на скенера към мрежата

В този раздел е разяснено как се свързва скенерът към мрежата чрез контролния панел на скенера.

Забележка:
Ако Вашият скенер и компютър са в един и същи сегмент, можете да се свържете и с помощта на инсталиращата програма.

За да стартирате инсталиращата програма, идете на дадения по-долу уеб сайт, след което въведете името на продукта. Отидете на ***Конфигуриране****, след което стартирайте инсталацията.*

https://epson.sn

Можете да прегледате инструкциите за работа в Уеб филми наръчници. Идете на следния URL.

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

Преди извършване на мрежова връзка

За да се свържете към мрежата, проверете предварително метода на свързване и информацията за настройка за връзката.

Събиране на информация относно настройката за свързване

Подгответе необходимата информация за настройка за свързване. Проверете предварително следната информация.

Отдели	Елементи	Забележка
Метод на свързване на устройство	❏ Ethernet ❏ Wi-Fi	Вземете решение как да свържете скенера към мрежата. За кабелна LAN мрежа, свързва се към LAN комутатора. За Wi-Fi, свързва се към мрежата (SSID) на точката на достъп.
Информация за LAN мрежа	❏ IP адрес ❏ Подмрежова маска ❏ Шлюз по подразбиране	Изберете IP адреса за назначаване към скенера. Когато назначите IP адреса статично, всички стойности са необходими. Когато назначите IP адреса динамично с помощта на функцията DHCP, тази информация не е задължителна, защото се задава автоматично.
Информация за Wi-Fi връзка	❏ SSID ❏ Парола	Това са SSID (име на мрежа) и паролата на точката за достъп, към която се свързва скенерът. Ако има зададено филтриране чрез MAC адрес, регистрирайте предварително MAC адреса на скенера, за да регистрирате скенера. Вижте следното за поддържаните стандарти. "Спецификации на мрежата" на страница 32
Информация за DNS сървър	❏ IP адрес за основен DNS ❏ IP адрес за вторичен DNS	Тези опции са задължителни, когато посочвате DNS сървъри. Вторичният DNS сървър се задава, когато системата разполага с излишна конфигурация и има вторичен DNS сървър. Ако се намирате в малка организация и не задавате DNS сървъра, задайте IP адреса на маршрутизатора.

Отдели	Елементи	Забележка
Информация за прокси сървър	❏ Име на прокси сървър	Задайте го, когато Вашата мрежова среда използва прокси сървър за достъп до интернет от вътрешната мрежа и използвате функцията, с която скенерът директно се свързва към интернет. За следните функции скенерът се свързва директно към интернет. ❏ Epson Connect Services ❏ Облачни услуги на други компании ❏ Актуализиране на фърмуер ❏ Изпращане на сканирани изображения към SharePoint(WebDAV)
Информация за номер на порт	❏ Номер на порт за освобождаване	Проверете номера на порта, използван от скенера и компютъра, след което освободете порта, който е блокиран от защитна стена, ако е необходимо. Вижте следното за номера на порта, използван от скенера. "Използване на порт за скенера" на страница 34

Назначаване на IP адрес

Това са следните типове назначаване на IP адрес.

Статичен IP адрес:

Назначете ръчно предварително определения IP адрес на скенера (хост).

Информацията за свързване към мрежата (маска на подмрежа, шлюз по подразбиране, DNS сървър и т.н.) трябва да бъдат зададени ръчно.

IP адресът не се променя дори когато устройството е изключено, така че това е полезно, когато искате да управлявате устройства със среда, в която не можете да променяте IP адреса или искате да управлявате устройства с помощта на IP адреса. Препоръчваме настройки на скенера, сървъра и т.н., до които имат достъп много компютри. Освен това, когато използвате функции за сигурност, като IPsec/IP филтриране, назначете фиксиран IP адрес, така че IP адресът да не се променя.

Автоматично назначаване с помощта на DHCP функция (динамичен IP адрес):

Назначете IP адреса автоматично към скенера (хост), като използвате DHCP функцията на DHCP сървъра или маршрутизатора.

Информацията за свързване към мрежата (маска на подмрежа, шлюз по подразбиране, DNS сървър и т.н.) се задава автоматично, за да можете лесно да свържете устройството към мрежата.

Ако устройството или маршрутизаторът са изключени или в зависимост от настройките на DHCP сървъра, IP адресът може да се промени при повторно свързване.

Препоръчваме управление на устройства, различни от IP адреса, и комуникация с протоколи, която може да следва IP адреса.

Забележка:
Когато използвате функцията за запазване на IP адрес на DHCP, Вие можете да назначавате по всяко време един и същ IP адрес към устройствата.

DNS сървър и прокси сървър

DNS сървърът има име на хост, име на домейн на имейл адреса и т.н. във връзка с информацията за IP адреса.

Комуникацията е невъзможна, ако другата страна е описана с име на хост, име на домейн и т.н., когато компютърът или скенерът извършват комуникация по IP.

Подава заявки към DNS сървъра за тази информация и получава IP адреса на другата страна. Този процес се нарича преобразуване на име.

Поради това устройствата, като компютри и скенери, могат да комуникират чрез IP адреса.

Преобразуването на име е необходимо, за да може скенерът да комуникира чрез функцията за имейл или с функцията за интернет връзка.

Когато използвате тези функции, извършете настройките на DNS сървъра.

Когато назначите IP адреса на скенера с помощта на функцията DHCP на DHCP сървъра или маршрутизатора, той се конфигурира автоматично.

Прокси сървърът е поставен на шлюза между мрежата и интернет и комуникира с компютъра, скенера и интернет (срещуположен сървър) вместо всеки от тях. Срещуположният сървър комуникира само с прокси сървъра. Следователно, информацията за скенера, например IP адрес и номер на порт, не може да бъде прочетена и се очаква увеличена сигурност.

Когато се свързвате с интернет чрез прокси сървър, конфигурирайте прокси сървъра на скенера.

Свързване към мрежата от контролния панел

Свържете скенера към мрежата с помощта на контролния панел на скенера.

Задаване на IP адрес

Задаване на основни елементи като адрес на хост, Маска на подмрежата, Шлюз по подразбиране.

В този раздел е разяснена процедурата за настройка на статичен IP адрес.

1. Включете скенера.
2. Изберете **Настройки** на началния екран от контролния панел на скенера.
3. Изберете **Настройки на мрежата** > **Разширени** > **TCP/IP**.
4. Изберете **Ръчно** за **Получаване на IP адрес**.

   Когато зададете IP адрес автоматично с помощта на функцията DHCP на маршрутизатора, изберете **Автоматично**. В този случай **IP адрес**, **Маска на подмрежата** и **Шлюз по подразбиране** в стъпка 5 до 6 също се задават автоматично, така че отидете на стъпка 7.
5. Въведете IP адреса.

   Фокусът се премества към предния сегмент или задния сегмент, разделени с точка, ако изберете ◀ и ▶.

   Потвърдете стойността, която е отразена в предишния екран.

6. Задайте **Маска на подмрежата** и **Шлюз по подразбиране**.

   Потвърдете стойността, която е отразена в предишния екран.

   > ***Важно:***
   >
   > *Ако комбинацията на IP адрес, Маска на подмрежата иШлюз по подразбиране е грешна, **Старт на настройката** е неактивна и не можете да продължите с настройките. Потвърдете, че няма грешка в записа.*

7. Въведете IP адреса за основния DNS сървър.

   Потвърдете стойността, която е отразена в предишния екран.

   Забележка:
   *Когато изберете **Автоматично** за настройки на назначаване на IP адреса, можете да изберете настройките за DNS сървър от **Ръчно** или **Автоматично**. Ако не можете да получите автоматично адреса на DNS сървъра, изберете **Ръчно** и въведете адреса на DNS сървъра. След това въведете директно вторичния адрес на DNS сървъра. Ако изберете **Автоматично**, отидете на стъпка 9.*

8. Въведете IP адреса за вторичния DNS сървър.

   Потвърдете стойността, която е отразена в предишния екран.

9. Натиснете **Старт на настройката**.

Настройка на прокси сървъра

Задайте прокси сървъра, ако следните неща са верни.

❏ Прокси сървърът е създаден за интернет връзка.

❏ Когато използвате функция, в която скенер се свързва директно към интернет, като услуга Epson Connect или други облачни услуги на компанията.

1. Изберете **Настройки** от началния екран.

   Когато извършвате настройки след задаване на IP адрес се извежда екранът **Разширени**. Отидете на стъпка 3.

2. Изберете **Настройки на мрежата** > **Разширени**.

3. Изберете **Прокси сървър**.

4. Изберете **Употр.** за **Настройки за прокси сървър**.

5. Въведете адреса за прокси сървъра чрез IPv4 или FQDN формат.

   Потвърдете стойността, която е отразена в предишния екран.

6. Въведете номера на порта за прокси сървъра.

   Потвърдете стойността, която е отразена в предишния екран.

7. Натиснете **Старт на настройката**.

Свързване към Ethernet

Свържете скенера към мрежата с LAN кабел и проверете връзката.

1. Свържете скенера и концентратора (LAN превключвател) с LAN кабел.
2. Изберете  от началния екран.
3. Изберете **Маршрутизатор**.
4. Уверете се, че настройките на Връзка и IP адрес са правилни.
5. Докоснете **Затвори**.

Свързване към безжична LAN (Wi-Fi) мрежа

Можете да свържете скенера към безжична LAN (Wi-Fi) мрежа по няколко начина. Изберете начин на свързване, който отговаря на средата и условията, които използвате.

Ако имате информация за безжичния маршрутизатор, например SSID и парола, можете да зададете настройките ръчно.

Ако безжичният маршрутизатор поддържа WPS, можете да зададете настройките, като използвате настройка с натискане на бутон.

След като свържете скенера към мрежата, свържете се към скенера от устройството, което желаете да използвате (компютър, смарт устройство, таблет и т.н.)

Бележка при използване на Wi-Fi 5 GHz връзка

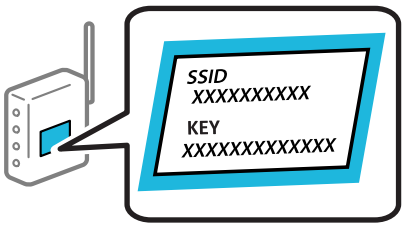
Този продукт обикновено използва W52 (36ch) като канал при свързване към Wi-Fi Direct (обикновена точка за достъп). Тъй като каналът за безжична LAN (Wi-Fi) връзка е автоматично избран, използваният канал може да се различава, когато се използва в същото време като Wi-Fi Direct връзката. Ако каналите се различават, комуникацията на данни със скенера може да е бавна. Ако не смущава използването, свържете към SSID в 2,4 GHz лента. В честотната 2,4 Ghz лента използваните канали ще съвпадат.

Когато задавате безжичната LAN към 5 Ghz, Ви препоръчваме да дезактивирате Wi-Fi Direct.

Извършване на Wi-Fi настройки чрез въвеждане на SSID и парола

Можете да конфигурирате Wi-Fi мрежа, като въведете необходимата информация за свързване към безжичен маршрутизатор от контролния панел на скенера. За да конфигурирате чрез този метод, са необходими SSID и парола за безжичен маршрутизатор.

Забележка:
Ако използвате безжичен маршрутизатор с неговите настройки по подразбиране, ще намерите SSID и паролата на етикета. Ако не знаете SSID и паролата, се свържете се с лицето, конфигурирало безжичния маршрутизатор, или вижте в документацията, предоставена с безжичния маршрутизатор.



1. Докоснете  на началния екран.
2. Изберете **Маршрутизатор**.
3. Докоснете **Начало на настройка**.

   Ако мрежовата връзка е вече зададена, се извежда подробна информация за връзката. Докоснете **Променете на Wi-Fi връзка.** или **Промяна на настройки**, за да промените настройките.
4. Изберете **Съветник за настройка на Wi-Fi**.
5. Следвайте екранните инструкции, за да изберете SSID, въведете паролата за безжичния маршрутизатор и стартирайте настройката.

   Ако желаете да проверите състоянието на мрежовата връзка за скенера след завършване на настройката, вижте съответната връзка с информация по-долу за подробности.

   Забележка:
   - ❏ *Ако SSID не Ви е известен, проверете дали не е изписан на етикета на безжичния маршрутизатор. Ако използвате безжичния маршрутизатор с настройки по подразбиране, използвайте SSID, изписан на етикета. Ако не можете да намерите никаква информация, вижте предоставената с безжичния маршрутизатор документация.*
   - ❏ *Паролата различава малки и главни букви.*
   - ❏ *Ако не знаете паролата, проверете дали информацията не е изписана на етикета на безжичния маршрутизатор. Върху етикета паролата може да е изписано „Network Key“, „Wireless Password“ и т.н. Ако използвате безжичния маршрутизатор с настройки по подразбиране, използвайте паролата, изписана на етикета.*
   - ❏ *Ако не виждате SSID, към който искате да се свържете, използвайте софтуер или приложение, за да конфигурирате Wi-Fi от Вашия компютър или смарт устройство, като смартфон или таблет. За информация въведете „https://epson.sn“ във Вашия браузър за достъп до уебсайта, въведете името на Вашия продукт и отидете на **Конфигуриране**.*

Още по темата

➡ “Проверка на състоянието на мрежовата връзка” на страница 30

Извършване на Wi-Fi настройки посредством бутон за настройка (WPS)

Можете автоматично да конфигурирате Wi-Fi мрежа, като натиснете бутон на безжичния маршрутизатор. Ако са изпълнени следните условия, можете да извършите настройка с помощта на този метод.

❏ Безжичният маршрутизатор е съвместим с WPS (Wi-Fi Protected Setup).

❏ Текущата Wi-Fi връзка е осъществена чрез натискане на бутон на безжичния маршрутизатор.

Забележка:
Ако не намирате бутона или конфигурирате с помощта на софтуер, направете справка в предоставената с безжичния маршрутизатор документация.

1. Докоснете  на началния екран.
2. Изберете **Маршрутизатор**.
3. Натиснете **Начало на настройка**.

   Ако мрежовата връзка е вече зададена, се извежда подробна информация за връзката. Докоснете **Променете на Wi-Fi връзка.** или **Промяна на настройки**, за да промените настройките.
4. Изберете **Настройка на бутон (WPS)**.
5. Следвайте инструкциите на екрана.

   Ако желаете да проверите състоянието на мрежовата връзка за скенера след завършване на настройката, вижте съответната връзка с информация по-долу за подробности.

   Забележка:
   При неуспешно свързване рестартирайте безжичния маршрутизатор, преместете го по-близо до скенера и опитайте отново.

Още по темата

➡ "Проверка на състоянието на мрежовата връзка" на страница 30

Извършване на Wi-Fi настройки посредством въвеждане на PIN код (WPS)

Можете да се свържете автоматично към безжичен маршрутизатор с помощта на PIN код. Можете да използвате този метод, за да определите дали за даден безжичен маршрутизатор е възможна WPS (Wi-Fi защитена настройка). Използвайте компютър за въвеждането на PIN код в безжичния маршрутизатор.

1. Докоснете  на началния екран.
2. Изберете **Маршрутизатор**.
3. Натиснете **Начало на настройка**.

   Ако мрежовата връзка е вече зададена, се извежда подробна информация за връзката. Докоснете **Променете на Wi-Fi връзка.** или **Промяна на настройки**, за да промените настройките.
4. Изберете **Други** > **Настройка на PIN код (WPS)**
5. Следвайте инструкциите на екрана.

   Ако желаете да проверите състоянието на мрежовата връзка за скенера след завършване на настройката, вижте съответната връзка с информация по-долу за подробности.

   Забележка:
   Направете справка в предоставената при покупката на безжичен маршрутизатор документация за подробна информация относно въвеждането на PIN код.

Още по темата

➡ “Проверка на състоянието на мрежовата връзка” на страница 30

Добавяне или подмяна на компютър или устройства

Свързване към скенер, който е бил свързан към мрежата

Когато скенерът вече е бил свързван към мрежата, можете да свържете компютър или смарт устройство към скенера през мрежата.

Използване на мрежов скенер от втори компютър

Нашата препоръка е да използвате инсталиращата програма за свързването на скенера към компютър.

За да стартирате инсталиращата програма, идете на дадения по-долу уеб сайт, след което въведете името на продукта. Отидете на **Конфигуриране**, след което стартирайте инсталацията.

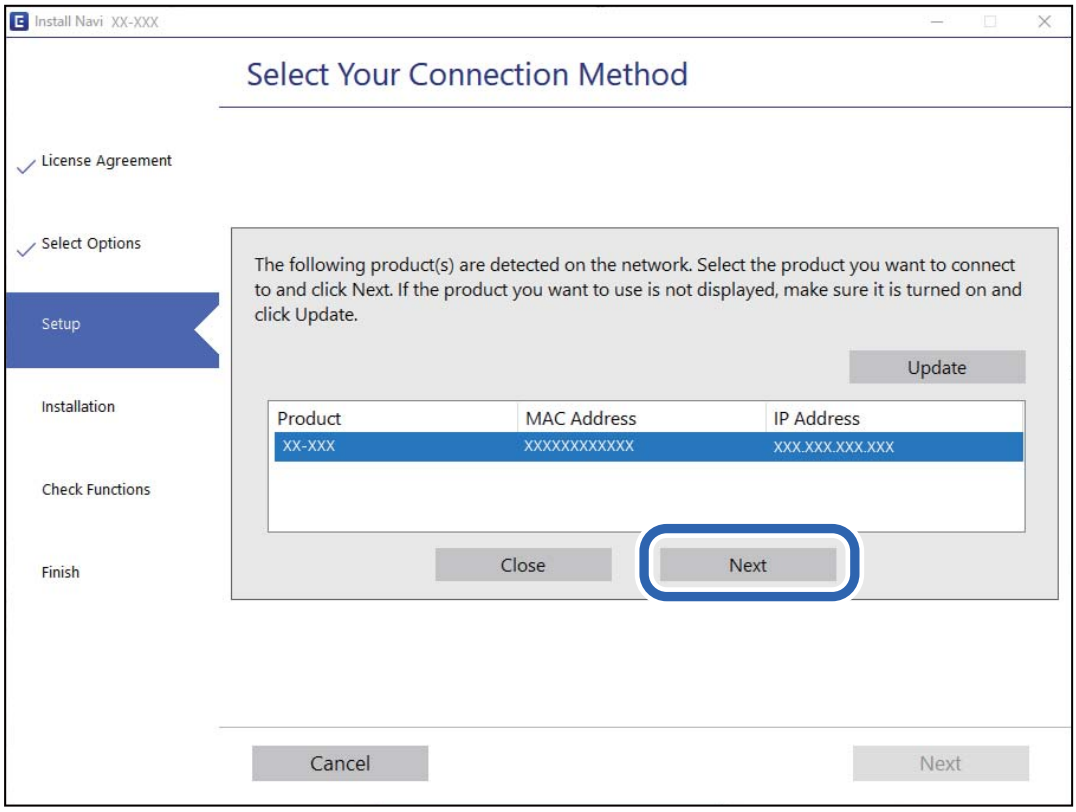
https://epson.sn

Можете да прегледате инструкциите за работа в Уеб филми наръчници. Идете на следния URL.

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

Избор на скенер

Следвайте инструкциите на екрана, докато се покаже следният екран, изберете името на скенера, към който искате да се свържете, след което щракнете върху **Следващ**.



Следвайте инструкциите на екрана.

Използване на мрежов скенер от смарт устройство

Можете да свържете смарт устройство към скенера чрез един от следните методи.

Свързване през безжичен маршрутизатор

Свържете смарт устройството към същата Wi-Fi мрежа (SSID) като скенера.

Вижте следното за повече подробности.

“Извършване на настройки за свързване към смарт устройството” на страница 29

Свързване чрез Wi-Fi Direct

Свържете смарт устройството директно към скенера без безжичен маршрутизатор.

Вижте следното за повече подробности.

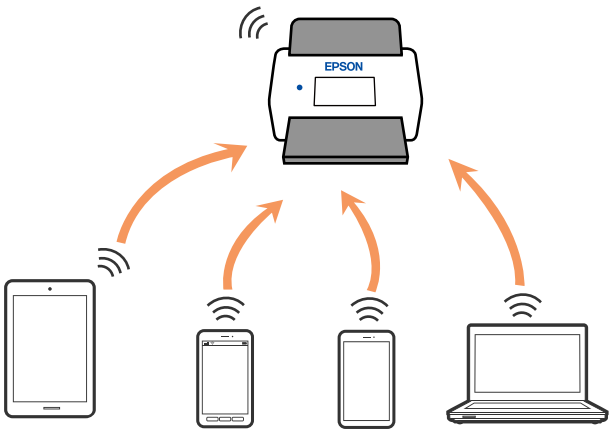
“Директно свързване на смарт устройство и скенер (Wi-Fi Direct)” на страница 26

Директно свързване на смарт устройство и скенер (Wi-Fi Direct)

Wi-Fi Direct (обикновена точка за достъп) Ви позволява да свързвате смарт устройство директно към скенера без безжичен маршрутизатор и да сканирате от смарт устройството.

Относно Wi-Fi Direct

Използвайте този метод на свързване, когато не ползвате Wi-Fi вкъщи или в офиса или когато искате да свържете директно скенера и компютъра или смарт устройството. В този режим скенерът функционира като безжичен маршрутизатор и можете да свържете устройства към скенера, без да се налага да използвате безжичен маршрутизатор. Свързаните директно със скенера устройства обаче не могат да комуникират помежду си чрез скенера.



Скенерът може да бъде свързан едновременно чрез Wi-Fi или Ethernet и Wi-Fi Direct (обикновена точка за достъп) връзка. Ако обаче стартирате мрежова връзка в Wi-Fi Direct (обикновена точка за достъп) връзка, когато скенерът е свързан чрез Wi-Fi, Wi-Fi, връзката временно се прекъсва.

Свързване към смарт устройство с помощта на Wi-Fi Direct

Този метод Ви дава възможност за свързване на скенера директно към смарт устройства без безжичен маршрутизатор.

1. Изберете  от началния екран.
2. Изберете **Wi-Fi Direct**.
3. Изберете **Начало на настройка**.
4. Стартирайте Epson Smart Panel на смарт устройството.
5. Следвайте изведените инструкции на Epson Smart Panel за свързване към скенера.

   Когато смарт устройството се свърже към скенера, преминете към следващата стъпка.
6. От контролния панел на скенера изберете **Завърш.**.

Прекъсване на Wi-Fi Direct (обикновена точка за достъп) връзка

Има два налични метода за дезактивиране на връзката Wi-Fi Direct (обикновена точка за достъп); можете да дезактивирате всички връзки с помощта на контролния панел на скенера или да дезактивирате всяка връзка от компютъра или смарт устройството.

Ако искате да дезактивирате всички връзки, изберете  > **Wi-Fi Direct** > **Начало на настройка** > **Промяна** > **Деактивиране на Wi-Fi Direct**.

Важно:

Когато връзката Wi-Fi Direct (обикновена точка за достъп) е дезактивирана, връзката на всички компютри и смарт устройства, свързани към скенера в Wi-Fi Direct (обикновена точка за достъп), се прекъсва.

Забележка:

Ако искате да прекъснете връзката за определено устройство, прекъснете я от устройството вместо от скенера. Използвайте един от следните методи, за да прекъснете връзката на Wi-Fi Direct (обикновена точка за достъп) от устройството.

- ❏ *Прекъснете Wi-Fi връзката към името на мрежата (SSID) на скенера.*
- ❏ *Свържете се към друго име на мрежа (SSID).*

Промяна на настройките на Wi-Fi Direct (обикновена точка за достъп) като SSID

Когато е активирана връзката Wi-Fi Direct (обикновена точка за достъп), можете да промените настройките от  > **Wi-Fi Direct** > **Начало на настройка** > **Промяна**, след което се извеждат следните елементи на менюто.

Промяна на името на мрежата

Сменете името на мрежата (SSID) на Wi-Fi Direct (обикновена точка за достъп), която се използва за свързване към скенера с Вашето произволно име. Можете да зададете името на мрежата (SSID) в ASCII знаци, които се извеждат на софтуерната клавиатура на контролния панел. Можете да въвеждате до 22 знака.

Когато променяте името на мрежата (SSID), всички свързани устройства се разкачат. Използвайте новото име на мрежата (SSID), ако искате да свържете повторно устройството.

Промяна на парола

Сменете паролата на Wi-Fi Direct (обикновена точка за достъп) за свързване към скенера с Вашето произволно име. Можете да зададете паролата в ASCII знаци, които се извеждат на софтуерната клавиатура на контролния панел. Можете да въвеждате от 8 до 22 знака.

Когато променяте паролата, всички свързани устройства се разкачат. Използвайте новата парола, ако искате да свържете повторно устройството.

Промяна на честотния диапазон

Сменете честотния обхват на Wi-Fi Direct, използван за свързване към скенера. Можете да изберете 2,4 GHz или 5 GHz.

Когато променяте честотния обхват, всички свързани устройства се разкачат. Свържете повторно устройството.

Имайте предвид, че не можете да свързвате повторно от устройства, които не поддържат честотен обхват от 5 GHz, при смяна на 5 GHz.

В зависимост от региона тази настройка може да не бъде показана.

Деактивиране на Wi-Fi Direct

Дезактивирайте настройките на Wi-Fi Direct (обикновена точка за достъп) на скенера. Когато ги дезактивирате, всички устройства, свързани към скенера в Wi-Fi Direct връзка (обикновена точка за достъп), се разкачат.

Възстановяване на настройки по подразбиране

Възстановява всички настройки на Wi-Fi Direct (обикновена точка за достъп) до техните стойности по подразбиране.

Запазената в скенера информация за Wi-Fi Direct (обикновена точка за достъп) връзката на смарт устройството се изтрива.

Забележка:
*Можете също да конфигурирате от раздел **Network** > **Wi-Fi Direct** на Web Config за следните настройки.*

- ❏ *Активиране или дезактивиране на Wi-Fi Direct (обикновена точка за достъп)*
- ❏ *Промяна на името на мрежата (SSID)*
- ❏ *Промяна на парола*
- ❏ *Промяна на честотния обхват*

  В зависимост от региона тази настройка може да не бъде показана.
- ❏ *Възстановяване на настройките на Wi-Fi Direct (обикновена точка за достъп)*

Нулиране на мрежовата връзка

В този раздел е разяснено как да извършите настройките за мрежовата връзка и да промените метода на свързване, когато сменяте безжичния маршрутизатор или компютъра.

При смяна на безжичния маршрутизатор

Когато смените безжичния маршрутизатор, извършете настройките за връзката между компютъра или смарт устройството и скенера.

Трябва да извършите тези настройки, ако промените своя доставчик на интернет услуга и т.н.

Извършване на настройки за свързване към компютъра

Нашата препоръка е да използвате инсталиращата програма за свързването на скенера към компютър.

За да стартирате инсталиращата програма, идете на дадения по-долу уеб сайт, след което въведете името на продукта. Отидете на **Конфигуриране**, след което стартирайте инсталацията.

https://epson.sn

Можете да прегледате инструкциите за работа в Уеб филми наръчници. Идете на следния URL.

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

Избиране на методите на свързване

Следвайте инструкциите на екрана. На екрана **Избор на опция за инсталиране** изберете **Настройка отново на връзката на Принтер (за нов мрежов рутер или промяна на USB към мрежа и т.н.)** и след това щракнете върху **Следващ**.

Следвайте инструкциите на екрана, за да завършите настройката.

Ако не можете да се свържете, вижте по-долу, за да се опитате да разрешите проблема.

“Не може да се свърже към мрежа” на страница 36

Извършване на настройки за свързване към смарт устройството

Можете да използвате скенера от смарт устройство, когато свързвате скенера към Wi-Fi мрежата (SSID), към която е свързано смарт устройството. За да използвате скенера от смарт устройство, отидете на дадения по-долу уеб сайт, след което въведете името на продукта. Отидете на **Конфигуриране**, след което стартирайте инсталацията.

https://epson.sn

Влезте на уебсайта от смарт устройството, което желаете да свържете към скенера.

При смяна на компютъра

При смяна на компютъра извършете настройки на връзката между компютъра и скенера.

Извършване на настройки за свързване към компютъра

Нашата препоръка е да използвате инсталиращата програма за свързването на скенера към компютър.

За да стартирате инсталиращата програма, идете на дадения по-долу уеб сайт, след което въведете името на продукта. Отидете на **Конфигуриране**, след което стартирайте инсталацията.

https://epson.sn

Можете да прегледате инструкциите за работа в Уеб филми наръчници. Идете на следния URL.

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

Следвайте инструкциите на екрана.

Промяна на начина на свързване към компютър

В този раздел е разяснено как да промените метода на свързване, когато компютърът и скенерът са свързани.

Промяна на мрежовата връзка от Ethernet към Wi-Fi

Променете Ethernet връзката към Wi-Fi връзка от контролния панел на скенера. Методът за промяна на връзка е същият като настройките за Wi-Fi връзка.

Още по темата

➡ “Свързване към безжична LAN (Wi-Fi) мрежа” на страница 21

Промяна на мрежовата връзка от Wi-Fi към Ethernet

Следвайте стъпките по-долу, за да промените от Wi-Fi връзка към Ethernet връзка.

1. Изберете **Настройки** от началния екран.
2. Изберете **Настройки на мрежата** > **Кабелна LAN настройка**.
3. Следвайте инструкциите на екрана.

Промяна от USB към мрежова връзка

Използване на инсталиращата програма и повторна настройка с различен метод на свързване.

Идете на дадения по-долу уеб сайт, след което въведете името на продукта. Отидете на **Конфигуриране**, след което стартирайте инсталацията.

https://epson.sn

Избиране на промяна на метода на свързване

Следвайте инструкциите на всеки прозорец. На екрана **Избор на опция за инсталиране** изберете **Настройка отново на връзката на Принтер (за нов мрежов рутер или промяна на USB към мрежа и т.н.)** и след това щракнете върху **Следващ**.

Изберете мрежовата връзка, която искате да използвате, **Свързване чрез безжична мрежа (Wi-Fi)** или **Свързване чрез кабелна LAN (Ethernet)**, след което щракнете върху **Следващ**.

Следвайте инструкциите на екрана, за да завършите настройката.

Проверка на състоянието на мрежовата връзка

Можете да проверите състоянието на мрежовата връзка по следния начин.

Проверка на състоянието на мрежовата връзка от контролния панел

Можете да проверите състоянието на мрежовата връзка с помощта на иконата на мрежата или информацията за мрежа на контролния панел на скенера.

Проверка на състоянието на мрежовата връзка с помощта на иконата за мрежата

Можете да проверите състоянието на мрежовата връзка и силата на радиосигнала с помощта на иконата за мрежата на началния екран на скенера.

	Извежда състоянието на мрежовата връзка. Изберете иконата, за да проверите и промените текущите настройки. Това е прекият път до следното меню. **Настройки** > **Настройки на мрежата** > **Wi-Fi настройка**	
		Скенерът не е свързан към безжична (Wi-Fi) мрежа.
		Скенерът търси SSID, не е настроен IP адрес или има проблем с безжичната (Wi-Fi) мрежа.
		Скенерът е свързан към безжична (Wi-Fi) мрежа. Броят на чертичките обозначава силата на сигнала на връзката. Колкото повече чертички има, толкова по-силна е връзката.
		Скенерът не е свързан към безжична (Wi-Fi) мрежа в режим Wi-Fi Direct (обикновена точка за достъп).
		Скенерът е свързан към безжична (Wi-Fi) мрежа в Wi-Fi Direct режим (обикновена точка за достъп).
		Скенерът не е свързан към кабелна (Ethernet) мрежа или отменете настройката.
		Скенерът е свързан към кабелна (Ethernet) мрежа.

Извеждане на подробна информация за мрежата на контролния панел

Когато Вашият скенер е свързан в мрежата, можете да прегледате и друга информация, свързана с мрежата, като изберете менютата на мрежата, които искате да проверите.

1. Изберете **Настройки** от началния екран.
2. Изберете **Настройки на мрежата** > **Мрежов статус**.
3. За да видите информацията, изберете менютата, които искате да проверите.
   - ❏ Състояние на кабелна LAN/Wi-Fi връзка

     Показва мрежова информация (име на устройството, връзка, сила на сигнала и др.) за Ethernet или Wi-Fi връзки.

❏ Състояние на Wi-Fi Direct

Показва дали Wi-Fi Direct е активирано или дезактивирано, SSID, парола и др. за Wi-Fi Direct връзки.

❏ Състояние на имейл сървър

Показва мрежова информация за имейл сървъра.

Спецификации на мрежата

Спецификации на Wi-Fi

Вижте следната таблица за спецификации на Wi-Fi.

Държави или региони, освен посочените по-долу	**Таблица A**
Ирландия, Обединеното кралство, Австрия, Германия, Лихтенщайн, Швейцария, Франция, Белгия, Люксембург, Нидерландия, Италия, Португалия, Испания, Дания, Финландия, Норвегия, Швеция, Исландия, Хърватия, Кипър, Гърция, Северна Македония, Сърбия, Словения, Малта, Босна и Херцеговина, Косово, Черна гора, Албания, България, Чехия, Естония, Унгария, Латвия, Литва, Полша, Румъния, Словакия, Израел, Австралия, Нова Зеландия, Тайван	**Таблица B**
Турция	DS-900WN: Серийни номера, започващи с XDA8: **Таблица A** Серийни номера, започващи с XDA7: **Таблица B**
	DS-800WN: Серийни номера, започващи с XDA2: **Таблица A** Серийни номера, започващи с XD9Z: **Таблица B**

Таблица A

Стандарти	IEEE 802.11b/g/n[*1]
Честотен обхват	2400 – 2483,5 MHz
Максимална радиочестотна мощност на предаване	20 dBm (EIRP)
Канали	1/2/3/4/5/6/7/8/9/10/11/12/13
Режими на свързване	Инфраструктура, Wi-Fi Direct (обикновена точка за достъп)[*2][*3]
Протоколи за защита[*4]	WEP (64/128bit), WPA2-PSK (AES)[*5], WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Налични само за HT20

*2 Не се поддържа за IEEE 802.11b

*3 Режимите на инфраструктура и Wi-Fi Direct или Ethernet връзка могат да бъдат използвани едновременно.

*4 Wi-Fi Direct поддържа само WPA2-PSK (AES).

*5 Отговаря на стандартите за WPA2 с поддръжка за WPA/WPA2 Personal.

Таблица B

Стандарти	IEEE 802.11a/b/g/n*1/ac		
Честотни диапазони	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Канали	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)
Режими на свързване	Инфраструктура, Wi-Fi Direct (обикновена точка за достъп)*4*5		
Протоколи за защита*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Налични само за HT20

*2 Не е налично в Тайван

*3 Наличността на тези канали и използването на продукта на открито през тези канали се различава според местоположението. За повече информация вижте http://support.epson.net/wifi5ghz/

*4 Не се поддържа за IEEE 802.11b

*5 Режимите на инфраструктура и Wi-Fi Direct или Ethernet връзка могат да бъдат използвани едновременно.

*6 Wi-Fi Direct поддържа само WPA2-PSK (AES).

*7 Отговаря на стандартите за WPA2 с поддръжка за WPA/WPA2 Personal.

Спецификации за Ethernet

Стандарти	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Енергоефективен Ethernet)*2
Комуникационен режим	Автоматичен, 10 Mbps пълен дуплекс, 10 Mbps половин дуплекс, 100 Mbps пълен дуплекс, 100 Mbps половин дуплекс
Конектор	RJ-45

*1 Използвайте кабел с екранирана усукана двойка (STP) от категория 5e или по-висока, за да се предотврати рискът от радиосмущения.

*2 Свързаното устройство трябва да отговаря на изискванията на стандартите IEEE802.3az.

Мрежови функции и поддържане на IPv4/IPv6

Функции	Поддържани
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Протокол за защита

IEEE802.1X*	
IPsec/IP филтриране	
SSL/TLS	HTTPS сървър/клиент
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Трябва да използвате устройство за свързване, което е в съответствие с IEEE802.1X.

Използване на порт за скенера

Скенерът използва следния порт. Тези портове трябва бъдат направени достъпни от мрежовия администратор, ако е необходимо.

Когато подателят (клиентът) е скенерът

Използвайте	Местоназначение (сървър)	Протокол	Номер на порт
Изпращане на файл (при сканиране в мрежова папка се използва от скенера)	FTP/FTPS сървър	FTP/FTPS (TCP)	20
			21
	Файлов сървър	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	WebDAV сървър	Протокол HTTP (TCP)	80
		Протокол HTTPS (TCP)	443

Използвайте	Местоназначение (сървър)	Протокол	Номер на порт
Изпращане на имейл (при сканиране в имейл се използва от скенера)	SMTP сървър	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP преди SMTP връзка (при сканиране в имейл се използва от скенера)	POP сървър	POP3 (TCP)	110
При използване на Epson Connect	Сървър за Epson Connect	HTTPS	443
		XMPP	5222
Събиране на потребителска информация (Използвайте контактите от скенера)	LDAP сървър	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Удостоверяване на потребител при събиране на потребителска информация (при използване на контактите от скенера) Удостоверяване на потребител при използване на сканиране към мрежова папка (SMB) от скенера	KDC сървър	Kerberos	88
Control WSD	Клиентски компютър	WSD (TCP)	5357
Потърсете компютъра при насочено сканиране от приложение	Клиентски компютър	Откриване на насочено сканиране за мрежа	2968

Когато подателят (клиентът) е клиентският компютър

Използвайте	Местоназначение (сървър)	Протокол	Номер на порт
Откриване на скенера от приложение като EpsonNet Config и драйвер на скенера.	Скенер	ENPC (UDP)	3289
Събиране и настройка на MIB информация от приложения като EpsonNet Config и драйвера на скенера.	Скенер	SNMP (UDP)	161
Търсене на WSD скенер	Скенер	WS-Discovery (UDP)	3702
Препращане на данните за сканиране от приложение	Скенер	Мрежово сканиране (TCP)	1865
Събиране на информацията за задание при насочено сканиране от приложение	Скенер	Насочено мрежово сканиране	2968
Web Config	Скенер	HTTP (TCP)	80
		HTTPS (TCP)	443

Решаване на проблеми

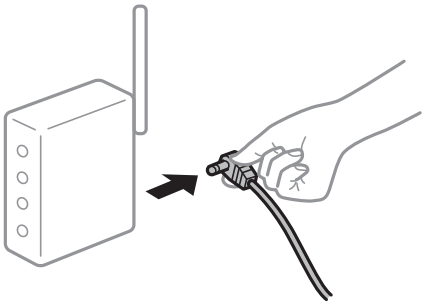
Не може да се свърже към мрежа

Проблемът може да е една от следните грешки.

Възникна грешка с мрежовите устройства за Wi-Fi връзка.

Решения

Изключете устройствата, които искате да свържете към мрежата. Изчакайте около 10 секунди и след това включете устройствата в следната последователност; безжичен маршрутизатор, компютър или смарт устройство, а след това и скенера. Преместете скенера и компютъра или смарт устройството по-близо до безжичния маршрутизатор, за да подпомогнете радиовръзката, и след това се опитайте да зададете мрежовите настройки отново.



Устройствата не могат да получават сигнали от безжичния маршрутизатор, защото са твърде отдалечени.

Решения

След преместване на компютъра или смарт устройството и скенера по-близо до безжичния маршрутизатор, изключете безжичния маршрутизатор, след което отново го включете.

При смяна на безжичния маршрутизатор настройките не съвпадат с новия маршрутизатор.

Решения

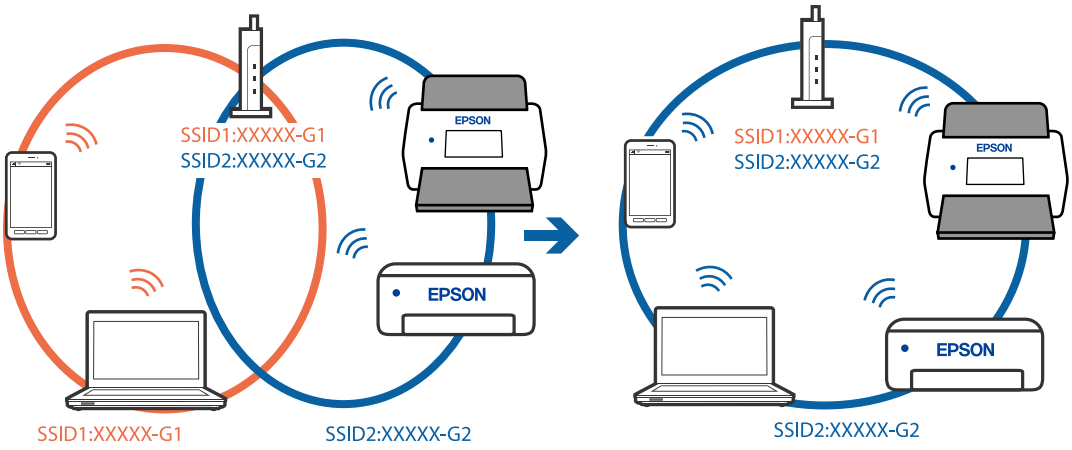
Извършете отново настройките на връзката така, че да съвпадат с новия безжичен маршрутизатор.

SSID, свързани от компютъра или смарт устройството, и компютъра са различни.

Решения

Когато използвате множество безжични маршрутизатори едновременно или ако безжичният маршрутизатор има множество SSID и устройства са свързани към различни SSID, не можете да се свържете към безжичния маршрутизатор.

Свържете компютъра или смарт устройство към същия SSID, към който е свързан скенерът.



В безжичния маршрутизатор има наличен разделител за поверителността.

Решения

Повечето безжични маршрутизатори разполагат с функция за разделител за поверителност, която блокира комуникацията между свързаните устройства. Ако не можете да осъществите комуникация между скенера и компютъра или смарт устройството дори ако са свързани към една и съща мрежа, дезактивирайте разделителя за поверителност на безжичния маршрутизатор. Вижте предоставеното с безжичния маршрутизатор ръководство за подробна информация.

IP адресът е неправилно назначен.

Решения

Ако IP адресът, назначен към скенера, е 169.254.XXX.XXX, а маската на подмрежата е 255.255.0.0, IP адресът може да не е назначен правилно.

Изберете **Настройки** > **Настройки на мрежата** > **Разширени** > **TCP/IP** на контролния панел на скенера, след което проверете IP адреса и назначената към скенера маска на подмрежата.

Рестартирайте безжичния маршрутизатор или нулирайте мрежовите настройки за скенера.

Има проблем с мрежовите настройки на компютъра.

Решения

Опитайте се да отидете на някакъв уебсайт от Вашия компютър, за да се уверите, че настройките на Вашата компютърна мрежа са правилни. Ако не можете да отидете на никакъв уебсайт, тогава има проблем в компютъра.

Проверка на мрежовата връзка на компютъра. Направете справка в предоставената при покупката на компютъра документация за подробна информация.

Скенерът е свързан чрез Ethernet чрез устройства, които поддържат IEEE 802.3az (енергоефективен Ethernet).

Решения

Когато свържете скенерът чрез Ethernet с помощта на устройства, които поддържат IEEE 802.3az (енергоефективен Ethernet), е възможно да възникнат следните проблеми в зависимост от концентратора или маршрутизатора, който използвате.

❏ Връзката става нестабилна, връзката на скенера се установява и прекъсва постоянно.

❏ Не можете да се свържете със скенера.

❏ Скоростта на комуникация става бавна.

Следвайте стъпките по-долу, за да дезактивирате IEEE 802.3az за скенера и след това да се свържете.

1. Отстранете Ethernet кабела, който е свързан към компютъра и скенера.
2. Когато IEEE 802.3az за компютъра е активирана, дезактивирайте я.

   Направете справка в предоставената при покупката на компютъра документация за подробна информация.
3. Свържете директно компютъра и скенера с Ethernet кабел.
4. На скенера проверете мрежовите настройки.

   Изберете **Настройки** > **Настройки на мрежата** > **Мрежов статус** > **Състояние на кабелна LAN/Wi-Fi връзка**.
5. Проверете IP адреса на скенера.
6. От компютъра влезте в Web Config.

   Стартирайте уеб браузър, след което въведете IP адреса на скенера.

   “Как да стартирате Web Config в уеб браузър” на страница 40
7. Изберете раздел **Network** > **Wired LAN**.
8. Изберете **OFF** за **IEEE 802.3az**.
9. Щракнете върху **Next**.
10. Щракнете върху **OK**.
11. Отстранете Ethernet кабела, който е свързан към компютъра и скенера.
12. Ако сте дезактивирали IEEE 802.3az за компютъра в стъпка 2, активирайте го.
13. Свържете Ethernet кабелите, които сте премахнали в стъпка 1, към компютъра и скенера.

Ако проблемът продължи, той може да се дължи на устройства, различни от скенера.

Скенерът е изключен.

Решения

Уверете се, че скенерът е включен.

Също така изчакайте, докато индикаторът за състояние не спре да премигва, т.е. скенерът е готов за сканиране.

Софтуер за настройка на скенера

Приложение за конфигуриране на операции на скенера (Web Config)

Web Config е приложение, което работи в уеббраузъри, като Microsoft Edge и Safari, на компютър или смарт устройство. Можете да проверите състоянието на скенера или да промените настройките на мрежата и скенера. За да използвате Web Config, свържете скенера и компютъра или устройството към същата мрежа.

Поддържат се следните браузъри. Използвайте най-новата версия.

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

Забележка:
От Вас може да се изисква да въведете паролата на администратор, когато използвате това устройство. Вижте следното за подробности относно паролата на администратор.

"Забележки относно паролата на администратора" на страница 11

Още по темата

➡ "Няма достъп до Web Config" на страница 68

Как да стартирате Web Config в уеб браузър

Скенерът се доставя с вграден софтуер, наречен Web Config (уеб страница, където можете да правите настройки). За достъп до Web Config, просто въведете IP адреса на свързан в мрежа скенер във Вашия уеб браузър.

1. Проверете IP адреса на скенера.

   Изберете **Настройки** > **Настройки на мрежата** > **Мрежов статус** от контролния панел на скенера. След това изберете активния метод на свързване (**Състояние на кабелна LAN/Wi-Fi връзка** или **Състояние на Wi-Fi Direct**) за потвърждаване на IP адреса на скенера.

   Пример за IP адрес: 192.168.100.201

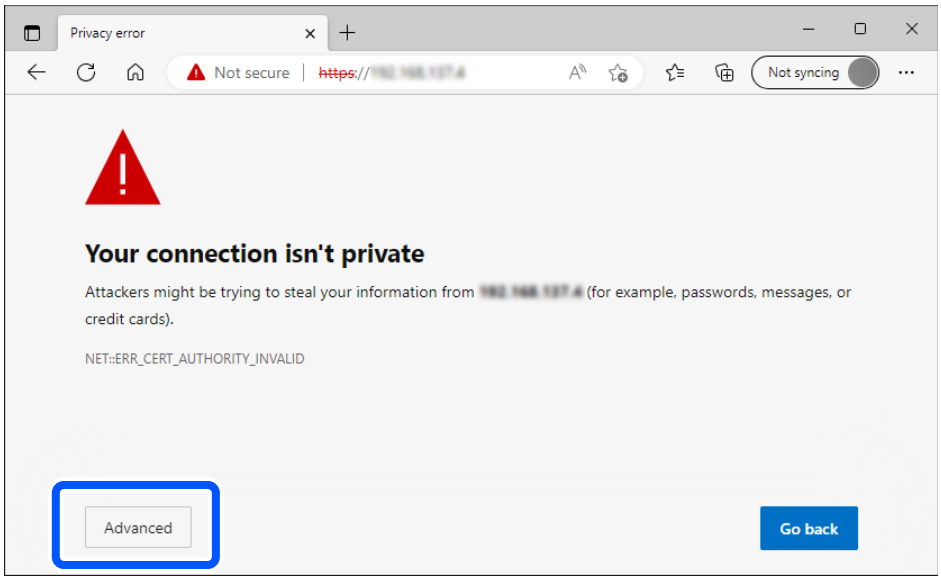
2. Стартирайте браузър от компютъра или смарт устройството и въведете IP адреса на скенера в адресната лента.

   Формат: http://scanner's IP address/

   Пример: http://192.168.100.201/

   Ако в браузъра ви се покаже екран с предупреждение, можете спокойно да пренебрегнете предупреждението и да покажете уеб страницата (Web Config). Тъй като скенерът използва самоподписан сертификат при влизане в HTTPS, на браузъра се извежда предупреждение, когато стартирате Web Config; това не указва проблем и може безопасно да се игнорира. В зависимост от браузъра Ви, може да се наложи да щракнете върху **Разширени настройки**, за да видите уеб страницата.

Пример: за Microsoft Edge



Забележка:

❏ *Ако не се покаже предупредителен екран, преминете към следващата стъпка.*

❏ *За IPv6 адреси използвайте следния формат.*

Формат: http://[scanner's IP address]/

Пример: http://[2001:db8::1000:1]/

3. За да промените настройките на скенера, трябва да се впишете като администратор на Web Config.

   Щракнете върху **Log in** в горния десен ъгъл на екрана. Въведете **User Name** и **Current password**, след което щракнете върху **OK**.

   Следното предоставя първоначалните стойности за информацията за администратора на Web Config.

   ·Потребителско име: няма (празно)

   ·Парола: Зависи от етикета, прикрепен към продукта.

   Ако на гърба има прикрепен етикет „PASSWORD“, въведете 8-цифрения номер, показан на етикета. Ако няма прикрепен етикет „PASSWORD“, въведете серийния номер на етикета, прикрепен на гърба на продукта, за първоначална парола на администратор.

   Забележка:

   ❏ *Ако в горния десен ъгъл на екрана се вижда **Log out**, значи вече сте влезли като администратор.*

   ❏ *След приблизително 20 минути неактивност ще бъдете отписани автоматично.*

Epson Device Admin

Epson Device Admin е многофункционално приложение, което Ви позволява да управлявате устройства в мрежа.

Можете да използвате шаблони за конфигуриране, за да приложите унифицирани настройки към множество скенери в мрежа, което го прави подходящо за инсталиране и управление на множество скенери.

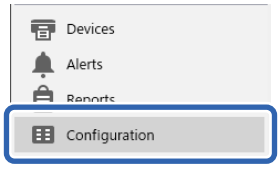
Можете да изтеглите Epson Device Admin от уебсайта за поддръжка на Epson. За подробности относно използването това приложение вижте документацията или помощта за Epson Device Admin.

Шаблон за конфигуриране

Създаване на шаблон за конфигуриране

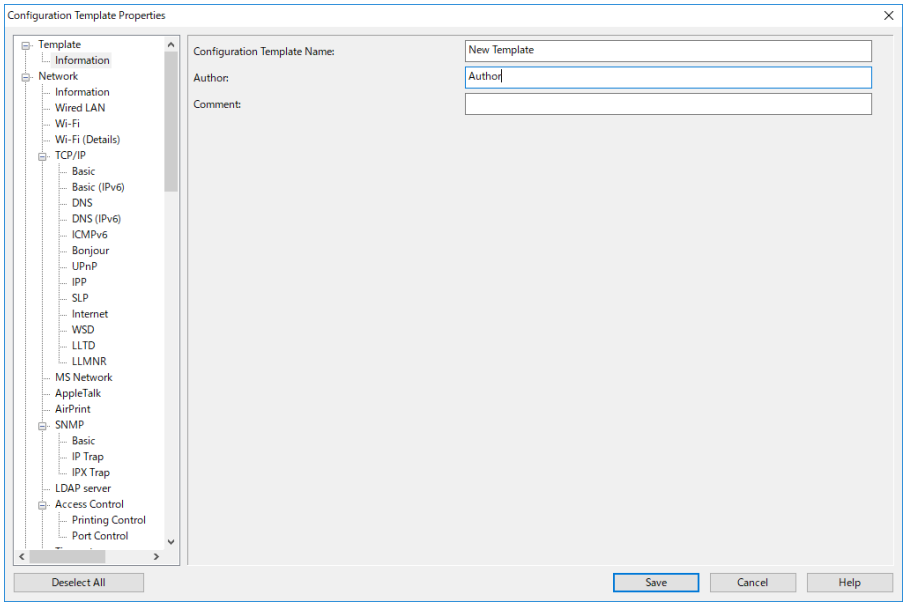
Създайте нов шаблон за конфигуриране.

1. Стартирайте Epson Device Admin.
2. Изберете **Configuration** на менюто със задачи на страничната лента.



3. Изберете **New** от менюто на лентата.

4. Задайте всеки елемент.



Елемент	Разяснение
Configuration Template Name	Име на шаблона за конфигуриране. Въведете до 1024 знака в Unicode (UTF-8).
Author	Информация за създателя на шаблона. Въведете до 1024 знака в Unicode (UTF-8).
Comment	Въведете произволна информация. Въведете до 1024 знака в Unicode (UTF-8).

5. Изберете елементите, които искате да зададете, отляво.

   Забележка:
   Щракнете върху елементите от менюто вляво, за да превключите към всеки екран. Зададената стойност се запазва, ако превключите екрана, но не и ако отмените екрана. Когато завършите всички настройки, щракнете върху ***Save****.*

Прилагане на шаблона за конфигуриране

Приложете запаметения шаблон за конфигуриране към скенера. Избраните в шаблона елементи се прилагат. Ако целевият скенер няма съответната функция, тя не се прилага.

Забележка:
Когато за скенера е зададена администраторска парола, конфигурирайте паролата предварително.

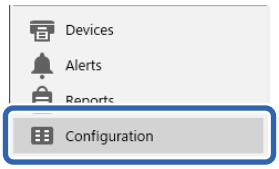
1. В менюто на лентата на екрана „Списък с устройства“ изберете ***Options*** *>* ***Password manager****.*

2. Изберете ***Enable automatic password management****, след което щракнете върху* ***Password manager****.*

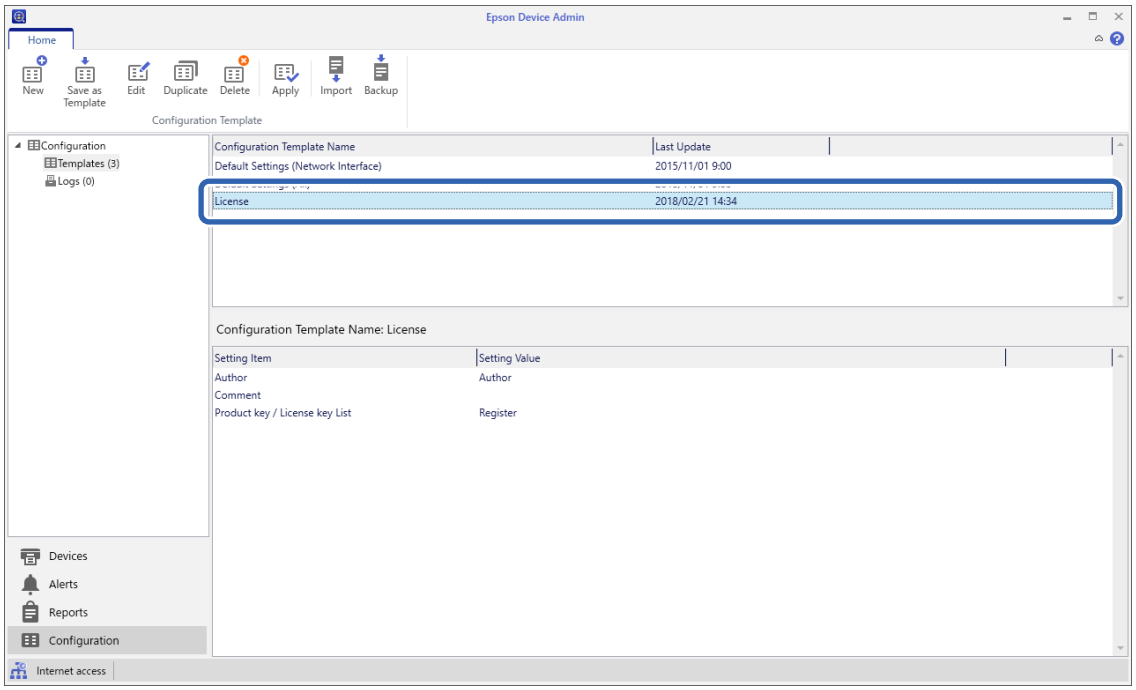
3. Изберете съответния скенер и след това щракнете ***Edit****.*

4. Задайте паролата, след което щракнете върху ***OK****.*

1. Изберете **Configuration** на менюто със задачи на страничната лента.



2. Изберете шаблона за конфигуриране, който искате да приложите от **Configuration Template Name**.



3. Щракнете върху **Apply** от менюто на лентата.

   Показва се екранът за избор на устройство.

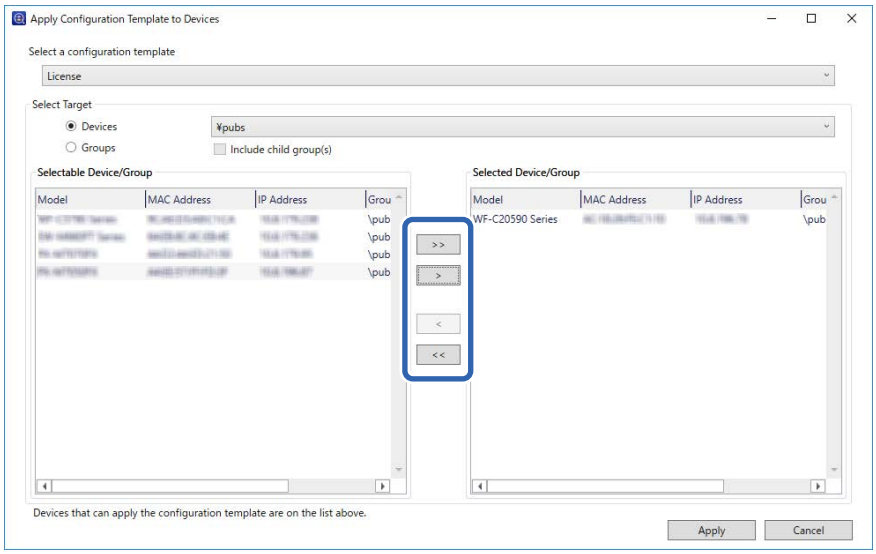
4. Изберете шаблона за конфигуриране, който искате да приложите.

   Забележка:

   ❏ *Когато изберете **Devices** и групи, съдържащи устройства, от падащото меню, се показва всяко устройство.*

   ❏ *Групите се показват, когато изберете **Groups**. Изберете **Include child group(s)** за автоматично избиране на дъщерни групи в рамките на избраната група.*

5. Преместете скенера или групите, към които искате да приложите шаблона, в **Selected Device/Group**.



6. Щракнете върху **Apply**.

   Показва се екран за потвърждение на шаблона за конфигуриране, който трябва да бъде приложен.

7. Щракнете върху **OK**, за да приложите шаблона за конфигуриране.

8. Когато се покаже съобщение, че процедурата е завършена, щракнете върху **OK**.

9. Щракнете върху **Details** и проверете информацията.

   Когато върху елементите, които сте приложили, се покаже , приложението е завършено успешно.

10. Щракнете върху **Close**.

Необходими настройки за сканиране

Регистриране на имейл сървър

Проверете следното преди да конфигурирате имейл сървъра.

❏ Скенерът е свързан към мрежата

❏ Информация за настройка за имейл сървър

Когато използвате имейл сървър, базиран на интернет, проверете информацията за настройките от доставчика или уебсайта.

Как да регистрирате

Влезте в Web Config, изберете раздел **Network** > **Email Server** > **Basic**.

"Как да стартирате Web Config в уеб браузър" на страница 40

Можете да извършвате настройки и на контролния панел на скенера. Изберете **Настройки** > **Настройки на мрежата** > **Разширени** > **Имейл сървър** > **Настройки на сървър**.

Елементи за настройка на имейл сървъра

Елемент	Настройки и обяснение	
Authentication Method	Посочете метода на удостоверяване за скенера за достъп до сървъра за електронна поща.	
	Off	Удостоверяването е изключено, когато тече комуникация със сървъра за електронна поща.
	SMTP AUTH	Имейл сървърът трябва да поддържа SMTP удостоверяване.
	POP before SMTP	Когато изберете този елемент, задайте POP3 сървър.
Authenticated Account	Ако изберете **SMTP AUTH** или **POP before SMTP** като **Authentication Method**, въведете името на акаунта за удостоверяване. Въведете от 0 до 255 знака в ASCII (0x20 – 0x7E).	
Authenticated Password	Ако изберете **SMTP AUTH** или **POP before SMTP** като **Authentication Method**, въведете паролата за удостоверяване. Въведете между 0 и 20 знака в ASCII (0x20 – 0x7E).	
Sender's Email Address	Задайте имейл адреса, който ще се използва за изпращане на имейли от скенера. Въпреки че можете да използвате съществуващ имейл адрес, препоръчваме ви да създадете и настроите специален имейл адрес, така че да можете да разграничавате имейлите, изпратени от скенера. Въведете от 0 до 255 символа в ASCII (0x20 – 0x7E) с изключение на: ( ) < > [ ] ; ¥. Първият знак не може да бъде точка „.".	
SMTP Server Address	Въведете между 0 и 255 знака, като използвате A – Z a – z 0 – 9. -. Можете да използвате формат IPv4 или FQDN.	
SMTP Server Port Number	Въведете число между 1 и 65 535.	
Secure Connection	Посочете защитен метод за свързване за имейл сървъра.	
	None	Ако изберете **POP before SMTP** в **Authentication Method**, методът за свързване е зададен да бъде **None**.
	SSL/TLS	Тази опция е достъпна, когато **Authentication Method** е **Off** или **SMTP AUTH**.
	STARTTLS	Тази опция е достъпна, когато **Authentication Method** е **Off** или **SMTP AUTH**.

Елемент	Настройки и обяснение
Certificate Validation (само за Web Config)	Сертификатът е проверен при разрешаването му. Когато **Secure Connection** е настроена на стойност различна от **None**, Ви препоръчваме да го настроите на **Enable**.
POP3 Server Address	Ако изберете **POP before SMTP** като **Authentication Method**, въведете адреса на POP3 сървъра. Можете да въведете между 0 и 255 знака, като използвате A – Z a – z 0 – 9. Можете да използвате формат IPv4 или FQDN.
POP3 Server Port Number	Задайте го, когато избирате **POP before SMTP** в **Authentication Method**. Въведете число между 1 и 65 535.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Проверка на връзката с имейл сървъра

1. Изберете менюто за тестване на връзката.

   ❏ **Когато настройвате от Web Config:**

   Изберете раздел **Network** > **Email Server** > **Connection Test** > **Start**.

   ❏ **При настройване от контролния панел:**

   Изберете **Настройки** > **Настройки на мрежата** >**Разширени** > **Имейл сървър** > **Проверка на връзката**.

   Тестът за свързване към имейл сървъра е стартиран.

2. Проверете резултатите от теста.

   ❏ Тестът се смята за успешен, когато бъде изведено съобщението **Connection test was successful.**.

   ❏ Ако се покаже грешка, следвайте инструкциите в съобщението, за да изчистите грешката.

   "Позоваванията при диагностика на връзката с имейл сървъра" на страница 48

Позоваванията при диагностика на връзката с имейл сървъра

Съобщение	Причина
SMTP server communication error. Check the following. - Network Settings	Това съобщение се показва, когато ❏ Скенерът не е свързан към мрежа ❏ Няма връзка с SMTP сървъра ❏ Връзката с мрежата е прекъсната по време на комуникация ❏ Получени са непълни данни
POP3 server communication error. Check the following. - Network Settings	Това съобщение се показва, когато ❏ Скенерът не е свързан към мрежа ❏ Няма връзка с POP3 сървъра ❏ Връзката с мрежата е прекъсната по време на комуникация ❏ Получени са непълни данни

Съобщение	Причина
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Това съобщение се показва, когато ❏ Свързването с DNS сървър е неуспешно ❏ Разрешаването на имената за SMTP сървър е неуспешно
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Това съобщение се показва, когато ❏ Свързването с DNS сървър е неуспешно ❏ Неуспешно преобразуване на име за сървъра на POP3
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Това съобщение се показва, когато удостоверяването в SMTP сървър е неуспешно.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Това съобщение се показва, когато удостоверяването в POP3 сървър е неуспешно.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Това съобщение се показва, когато се опитате да комуникирате с неподдържани протоколи.
Connection to SMTP server failed. Change Secure Connection to None.	Това съобщение се показва, когато възникне несъответствие в SMTP между сървър и клиент или когато сървърът не поддържа защитена SMTP връзка (SSL връзка).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Това съобщение се показва, когато възникне несъответствие в SMTP между сървър и клиент или когато сървърът изисква използване на SSL/TLS връзка за защитена SMTP връзка.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Това съобщение се показва, когато възникне несъответствие в SMTP между сървър и клиент или когато сървърът изисква използване на STARTTLS връзка за защитена SMTP връзка.
The connection is untrusted. Check the following. - Date and Time	Това съобщение се показва, когато настройката за дата и час на скенера е неправилна или сертификатът е изтекъл.
The connection is untrusted. Check the following. - CA Certificate	Това съобщение се показва, когато скенерът няма главен сертификат, съответстващ на сървъра, или не е бил импортиран CA Certificate.
The connection is not secured.	Това съобщение се показва, когато полученият сертификат е повреден.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Това съобщение се показва, когато възникне несъответствие в метода на удостоверяване между сървър и клиент. Сървърът поддържа SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Това съобщение се показва, когато възникне несъответствие в метода на удостоверяване между сървър и клиент. Сървърът не поддържа SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	Това съобщение се показва, когато имейл адресът на посочения подател е грешен.
Cannot access the product until processing is complete.	Това съобщение се показва, когато скенерът е зает.

Създаване на мрежова папка

Създайте мрежова папка на Вашия компютър. Компютърът трябва да е свързан към същата мрежа като скенера.

Методът за задаване на мрежовата папка варира в зависимост от средата. Това е пример за създаване на мрежова папка на работния плот на компютър в следната среда.

- ❏ Операционна система: Windows 10
- ❏ Място за създаване на мрежовата папка: работен плот
- ❏ Път към папката: C:\Users\xxxx\Desktop\scan_folder (създайте на работния плот мрежова папка с име „scan_folder“)

1. Впишете се в компютъра, на който искате да създадете мрежовата папка, с потребителски акаунт с администраторски права.

   Забележка:
   Ако не знаете кой потребителски акаунт има администраторски права, проверете при администратора на Вашия компютър.

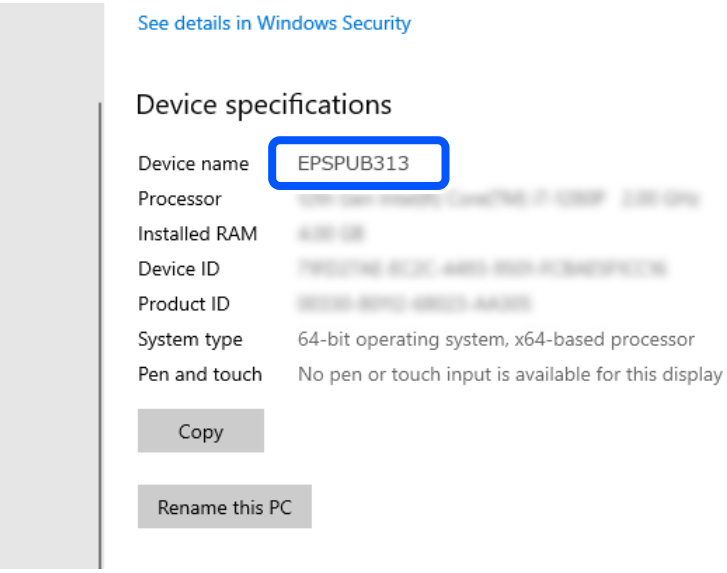
2. Уверете се, че името на устройството (името на компютъра) не съдържа двубайтови знаци. Щракнете върху бутона Старт на Windows, след което изберете **Настройки** > **Системни** > **Относно**.

   Забележка:
   Ако в името на устройството има двубайтови знаци, записът на файла може да е неуспешен.

3. Проверете дали текстовият низ в **Спецификации на устройството** > **Име на устройството** не съдържа двубайтови символи.

   Ако името на устройството съдържа само еднобайтови знаци, не би трябвало да има проблеми. Затворете екрана.

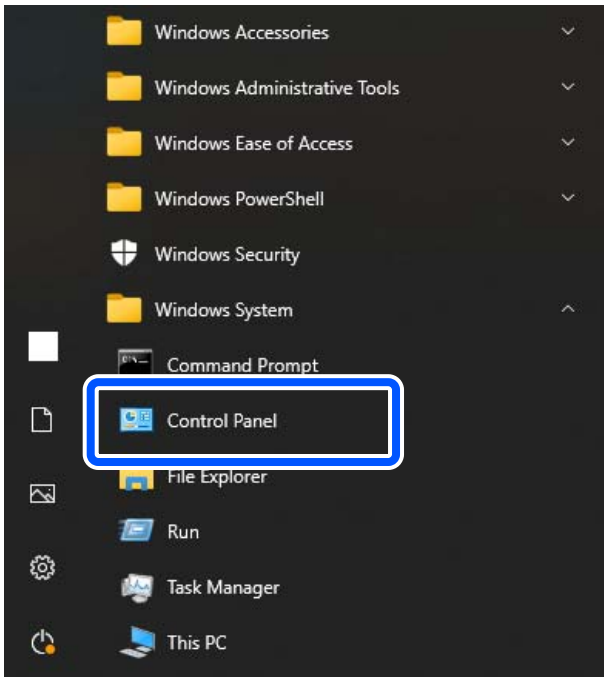
   Пример: EPSPUB313



> ***Важно:***
>
> *Ако името на устройството съдържа двубайтови знаци, използвайте компютър, който не използва двубайтови знаци, или сменете името на устройството.*
>
> *Ако трябва да промените името на устройството, предварително се консултирайте с администратора на вашия компютър, тъй като това може да повлияе на управлението на компютъра и достъпа до ресурси.*

След това, проверете настройките на Вашия компютър.

4. Щракнете върху бутона Старт на Windows, след което изберете **Система на Windows** > **Контролен панел**.



5. В контролния панел щракнете върху > **Мрежа и интернет** > **Център за мрежи и споделяне** > **Промяна на разширените настройки за споделяне**.

   Показва се мрежовия профил.

6. Уверете се, че за мрежовия профил (текущия профил) под **Споделяне на файлове и принтери** е избрано **Включване на споделянето на файлове и принтери**.

   Ако вече е избрано, щракнете върху **Отмяна** и затворете прозореца.

   Когато промените настройките, щракнете върху **Записване на промените** и затворете прозореца.

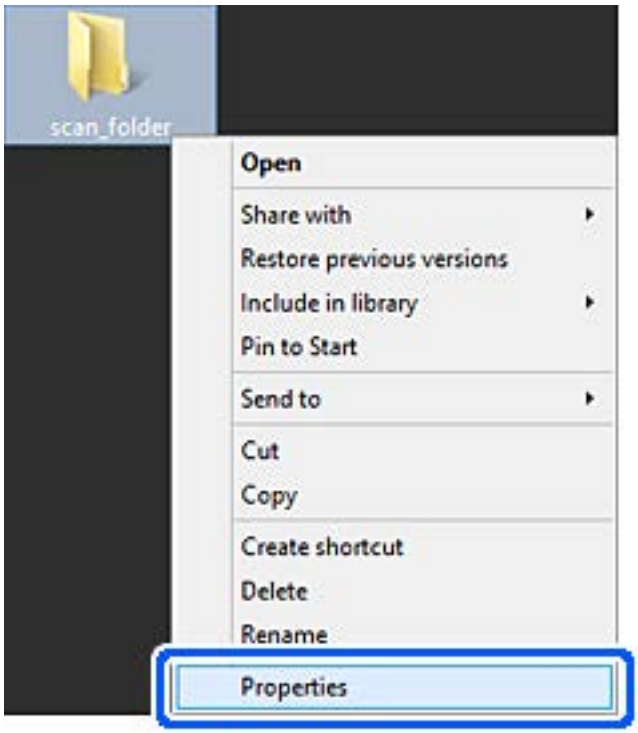
   След това, създайте мрежова папка.

7. Създайте и дайте име на папка на Вашия работен плот.

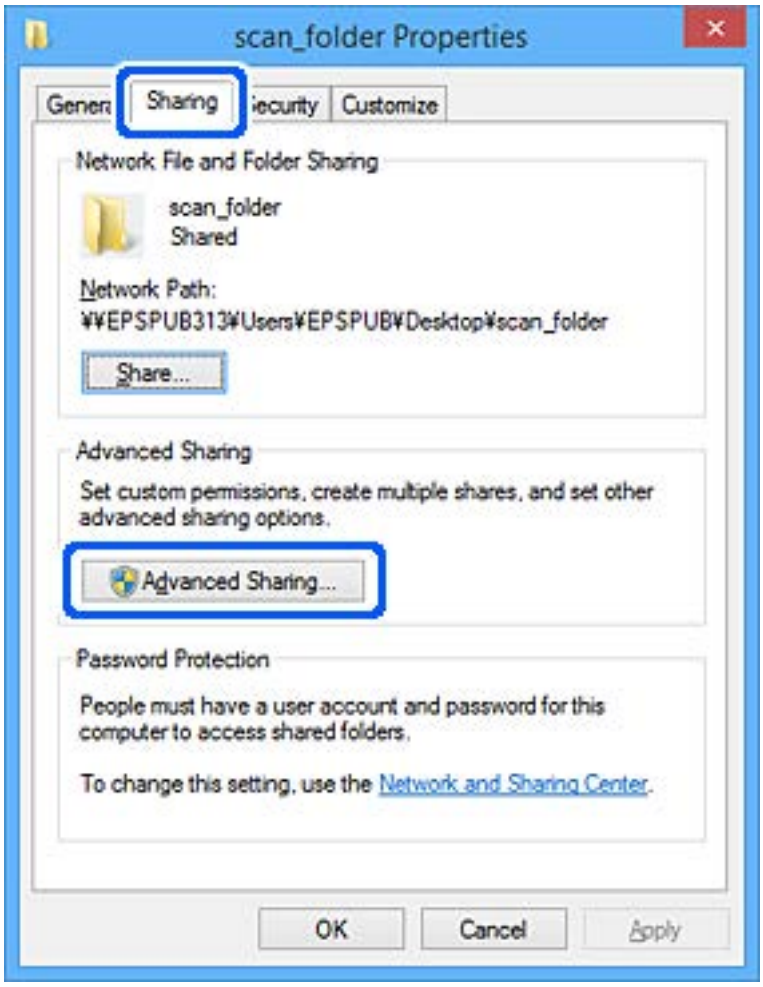
   Въведете име на папката от 1 до 12 буквено-цифрови символа. Ако името надвишава 12 знака, може да не успеете да получите достъп до папката в зависимост от Вашата среда.

   Пример: scan_folder

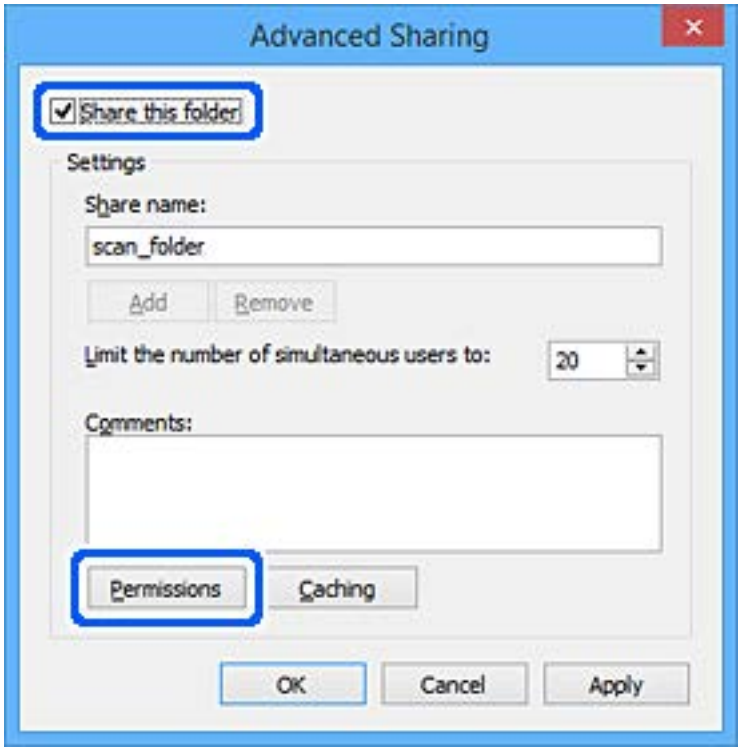
8. Щракнете с десния бутон върху папката и след това изберете **Свойства**.



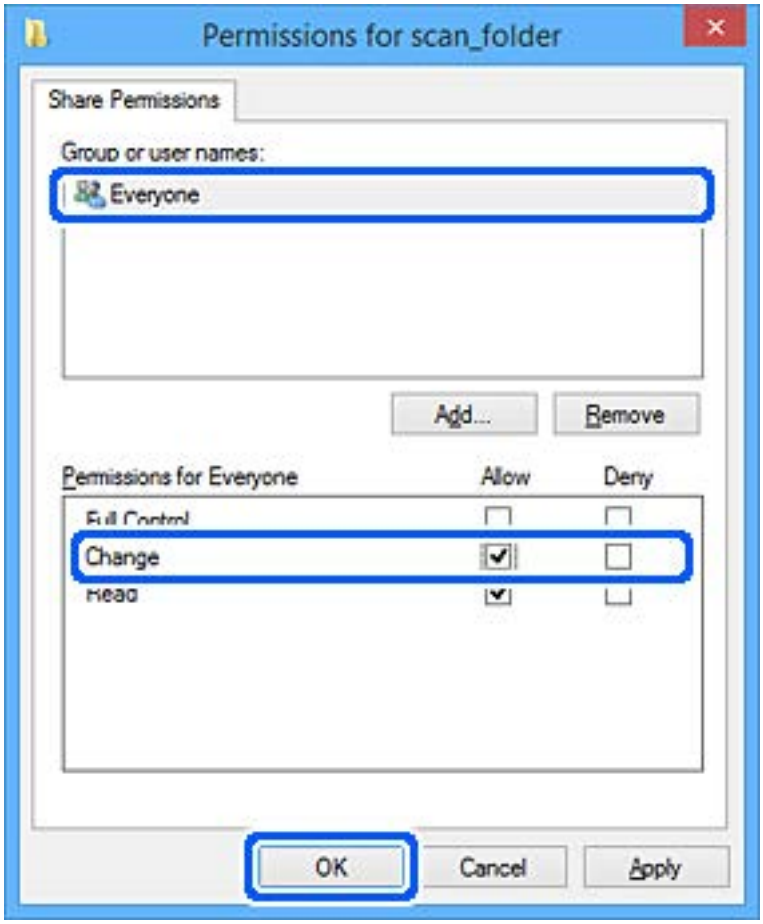
9. Щракнете върху **Разширено споделяне** на раздела **Споделяне**.



10. Изберете **Сподели тази папка**, след което щракнете върху **Разрешения**.



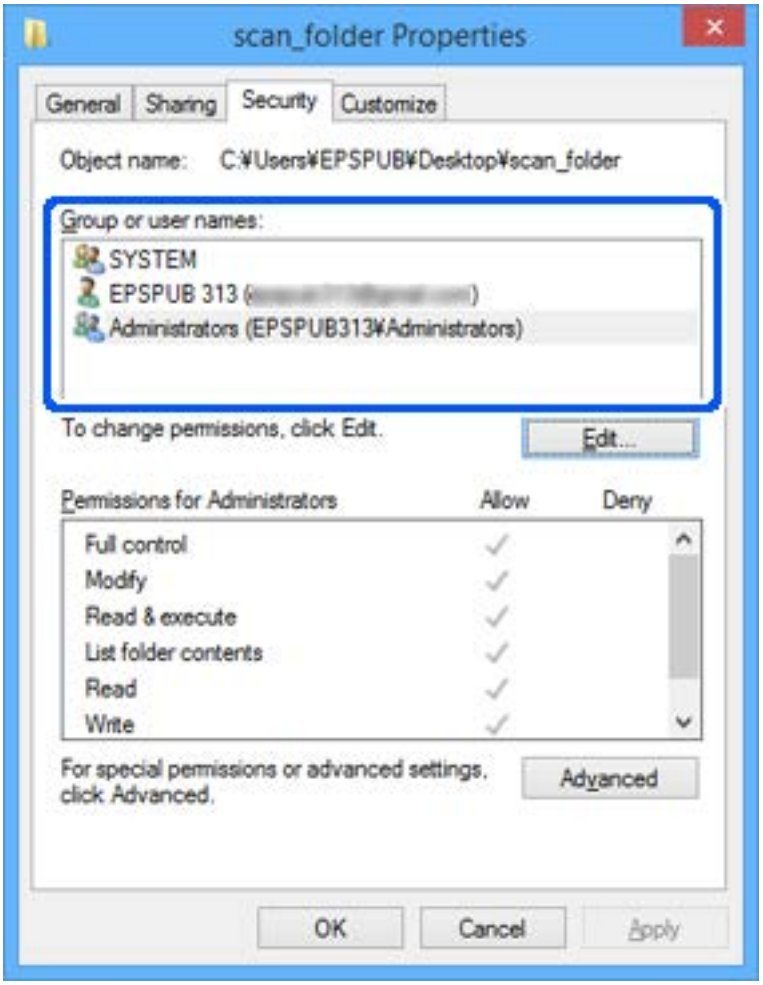
11. В **Имена на потребители или групи** изберете **Всички**, в **Промяна** изберете **Разрешаване**, след което щракнете върху **OK**.



12. Щракнете върху **OK**, за да затворите екрана и да се върнете към прозореца със свойства.

    Забележка:
    Можете да проверите, кои групи или потребители имат достъп до мрежовата папка в раздела ***Защита*** > ***Имена на потребители или групи****.*

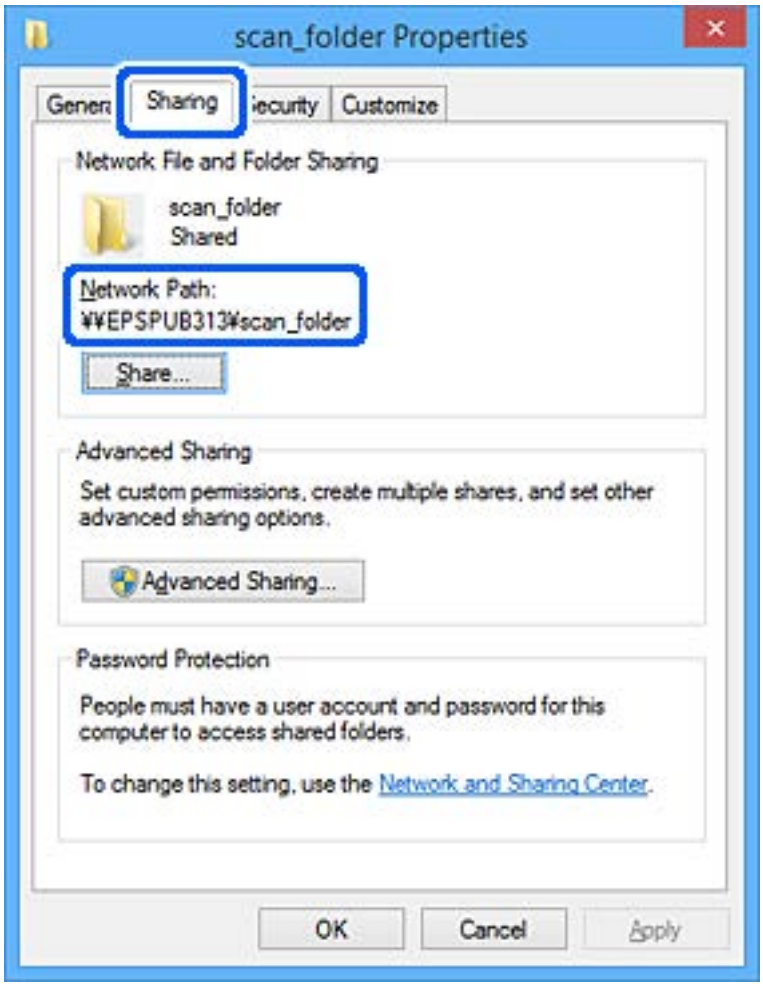
    Пример: Когато потребителят влезе в компютъра, както и администраторите да имат достъп до мрежовата папка



13. Изберете раздела **Споделяне**.

    Извежда се мрежовият път за мрежовата папка. Това се използва, когато се регистрирате към вашите контакти за скенера. Моля, запишете го.

Пример: \\EPSPUB313\scan_folder



14. Щракнете върху **Затваряне** или **OK**, за да затворите прозореца.

С това приключва създаването на мрежовата папка.

Направете контактите достъпни

Регистриране на местоназначения в списъка с контакти на скенера Ви позволява лесно да въведете местоназначението при сканиране.

Можете да регистрирате следните типове местоназначения в списъка с контакти. Можете да регистрирате до 300 записа общо.

Забележка:
Можете също да използвате LDAP сървър (търсене с LDAP), за да въведете местоназначението.

Имейл	Местоназначение за имейл. Трябва да конфигурирате предварително настройките на имейл сървъра.
Мрежова папка	Местоназначение на данни за сканиране. Трябва предварително да подготвите мрежовата папка.

Още по темата

➡ "Съвместна работа между LDAP сървър и потребители" на страница 64

Сравнение между конфигурациите на контакти

Има три инструмента за конфигуриране на контактите на скенера: Web Config, Epson Device Admin и контролния панел на скенера. Разликите между трите инструмента са изброени в таблицата по-долу.

Функции	Web Config*	Epson Device Admin	Контролен панел на скенера
Регистриране на местоназначение	✓	✓	✓
Редактиране на местоназначение	✓	✓	✓
Добавяне на група	✓	✓	✓
Редактиране на група	✓	✓	✓
Изтриване на местоназначение или групи	✓	✓	✓
Изтриване на всички местоназначения	✓	✓	–
Импортиране на файл	✓	✓	–
Експортиране на файл	✓	✓	–

* Впишете се като администратор, за да правите настройки.

Регистриране на местоназначение към контакти чрез Web Config

Забележка:
Можете също да регистрирате контактите на контролния панел на скенера.

1. Влезте в Web Config и изберете раздел **Scan** > **Contacts**.
2. Изберете номера, който искате да регистрирате, след което щракнете върху **Edit**.
3. Въведете **Name** и **Index Word**.
4. Изберете типа на местоназначението за опцията **Type**.

   Забележка:
   *Няма да можете да промените опцията **Type**, след като регистрирането приключи. Ако искате да промените типа, изтрийте местоназначението и регистрирайте отново.*
5. Въведете стойност за всеки елемент, след което щракнете върху **Apply**.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Елементи за настройка на местоназначения

Елементи	Настройки и обяснение
Общи настройки	
Name	Въведете име, показвано в контактите, с максимум 30 знака в Unicode (UTF-16). Ако не посочите това, оставете полето празно.
Index Word	Въведете име с 30 или по-малко знака в Unicode (UTF-16) за търсене на контактите в контролния панел на скенера. Ако не посочите това, оставете полето празно.
Type	Изберете типа на адреса, който искате да регистрирате.
Assign to Frequent Use	Изберете дали да зададете регистрирания адрес като често използван адрес. Когато го зададете като често използван адрес, местоназначението ще се показва в горния екран за сканиране и ще можете да го избирате, без да показвате контактите.
Email	
Email Address	Въведете между 1 и 255 знака, като използвате A – Z, a – z, 0 – 9! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Network Folder (SMB)	
Save to	\\„Път до папка" Въведете местоположението, където се намира целевата папка, като използвате между 1 и 253 знака в Unicode (UTF-16), пропускайки „\\". Въведете пътя на мрежата, изведен на екрана за свойства на папката. Вижте следното за подробности относно настройката на пътя на мрежата. "Създаване на мрежова папка" на страница 50
User Name	Въведете потребителското име за достъп до мрежова папка с максимум 30 знака в Unicode (UTF-16). Все пак избягвайте да използвате контролни знаци (от 0x00 до 0x1f, 0x7F).
Password	Въведете парола за достъп до мрежова папка от 0 до 20 знака в Unicode (UTF-16). Все пак избягвайте да използвате контролни знаци (от 0x00 до 0x1f, 0x7F).
FTP	
Secure Connection	Изберете FTP или FTPS спрямо протокола за прехвърляне на файлове, който се поддържа от FTP сървъра. Изберете **FTPS**, за да позволите на скенера да комуникира с мерките за сигурност.
Save to	Въведете името на сървъра, като използвате между 1 и 253 знака в Unicode (UTF-16), като пропускате „ftp://" или „ftps://".

Елементи	Настройки и обяснение
User Name	Въведете потребителското име за достъп до FTP сървър с максимум 30 знака в Unicode (UTF-16). Все пак избягвайте да използвате контролни знаци (от 0x00 до 0x1f, 0x7F). Ако сървърът позволява анонимни връзки, въведете потребителско име, като например „Анонимен“ и „FTP“. Ако не посочите това, оставете полето празно.
Password	Въведете парола за достъп до FTP сървър от 0 до 20 знака в Unicode (UTF-16). Все пак избягвайте да използвате контролни знаци (от 0x00 до 0x1f, 0x7F). Ако не посочите това, оставете полето празно.
Connection Mode	Изберете режима на свързване от менюто. Ако е настроена защитна стена между скенера и FTP сървъра, изберете **Passive Mode**.
Port Number	Въведете номера на порта на FTP сървъра, като използвате стойност между 1 и 65535.
Certificate Validation	Сертификатът на FTP сървъра се валидира, когато това е активирано. Това е налично, когато сте избрали **FTPS** за **Secure Connection**. За настройка трябва да импортирате CA Certificate в скенера.
SharePoint(WebDAV)*	
Secure Connection	Изберете HTTP или HTTPS спрямо протокола за прехвърляне на файлове, който се поддържа от сървъра. Изберете **HTTPS**, за да позволите на скенера да комуникира с мерките за сигурност.
Save to	Въведете името на сървъра, като използвате между 1 и 253 знака в Unicode (UTF-16), като пропускате „http://“ или „https://“.
User Name	Въведете потребителско име за достъп до сървър с максимум 30 знака в Unicode (UTF-16). Все пак избягвайте да използвате контролни знаци (от 0x00 до 0x1f, 0x7F). Ако не посочите това, оставете полето празно.
Password	Въведете парола за достъп до сървър от 0 до 20 знака в Unicode (UTF-16). Все пак избягвайте да използвате контролни знаци (от 0x00 до 0x1f, 0x7F). Ако не посочите това, оставете полето празно.
Certificate Validation	Сертификатът на сървъра се валидира, когато това е активирано. Това е налично, когато сте избрали **HTTPS** за **Secure Connection**. За настройка трябва да импортирате CA Certificate в скенера.
Proxy Server	Изберете дали да използвате прокси сървър.

* SharePoint Online не се поддържа, когато сканирате в мрежова папка от контролния панел на скенера.

Ако искате да запазите сканираното изображение на SharePoint Online, използвайте Document Capture Pro, след като инсталирате SharePoint Online Connector. За подробности вижте ръководството Document Capture Pro.

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

Регистриране на местоназначения като група чрез Web Config

Ако типът на местоназначението е зададен на **Email**, можете да регистрирате местоназначенията като група.

1. Влезте в Web Config и изберете раздел **Scan** > **Contacts**.

2. Изберете номера, който искате да регистрирате, след което щракнете върху **Edit**.
3. Изберете група от **Type**.
4. Щракнете върху **Select** за **Contact(s) for Group**.

   Достъпните местоназначения се показват.
5. Изберете местоназначението, което искате да регистрирате в групата, след което щракнете върху **Select**.
6. Въведете **Name** и **Index Word**.
7. Изберете дали искате да назначите регистрираната група към групата на често използваните или не.

   Забележка:
   Местоназначенията могат да бъдат регистрирани в множество групи.
8. Щракнете върху **Apply**.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Архивиране и импортиране на контакти

С помощта на Web Config или други инструменти Вие можете да архивирате и импортирате контакти.

За Web Config Вие можете да архивирате контакти, като експортирате настройките на скенера, които включват контакти. Експортираният файл не може да бъде редактиран, защото е експортиран като двоичен файл.

Когато импортирате настройките на скенера към скенера, контактите се презаписват.

За Epson Device Admin могат да бъдат експортирани само контакти от екрана със свойства на устройството. Освен това, ако не експортирате елементите за сигурност, Вие можете да редактирате експортираните контакти и да ги импортирате, защото могат да бъдат записани като SYLK или CSV файлове.

Импортиране на контакти чрез Web Config

Ако имате скенер, който Ви позволява да архивирате контакти и е съвместим с този скенер, можете лесно да регистрирате контактите, като импортирате архивния файл.

Забележка:
За инструкции относно архивиране на контактите на скенера вижте предоставеното със скенера ръководство.

Следвайте стъпките по-долу, за да импортирате контактите към този скенер.

1. Влезте в Web Config, изберете раздел **Device Management** > **Export and Import Setting Value** > **Import**.
2. Изберете архивния файл, който сте създали във **File**, въведете паролата, след което щракнете върху **Next**.
3. Изберете квадратчето за отметка **Contacts**, след което щракнете върху **Next**.

Архивиране на контакти с помощта на Web Config

Данните за контакти могат да бъдат изгубени при повреда на скенера. Препоръчваме Ви да правите резервно копие на данните при всяко актуализиране. Epson не носи отговорност за загуба на данни, за архивиране или възстановяване на данни и/или настройки дори по време на гаранционния период.

С помощта на Web Config можете да архивирате в компютъра данните, съхранени на скенера.

1. Влезте в Web Config, след което изберете раздел **Device Management** > **Export and Import Setting Value** > **Export**.
2. Сложете отметка в квадратчето за **Contacts** от категорията **Scan**.
3. Въведете парола, за да шифровате експортирания файл.

   Паролата ще Ви е необходима, за да импортирате файла. Оставете това поле празно, ако не искате да шифровате файла.
4. Щракнете върху **Export**.

Експортиране и групова регистрация на контакти с помощта на инструмент

Ако използвате Epson Device Admin, Вие можете да архивирате само контактите и да редактирате експортираните файлове, след което да ги регистрирате всички наведнъж.

Това е полезно, ако искате да архивирате само контактите или когато подмените скенера и искате да прехвърлите контактите от стария към новия скенер.

Експортиране на контакти

Запис на информацията за контакти във файла.

Можете да редактирате файлове, които са записани в SYLK или csv формат, с помощта на приложение за електронни таблици или текстов редактор. Можете да регистрирате всички наведнъж след изтриване или добавяне на информацията.

Информация, която включва елементи за сигурност, като парола и лична информация, може да бъде записана в двоичен формат с парола. Не можете да редактирате файла. Това може да се използва като архивен файл на информацията, включително елементите за сигурност.

1. Стартирайте Epson Device Admin.
2. Изберете **Devices** на менюто със задачи на страничната лента.
3. Изберете устройството, което искате да конфигурирате, от списъка с устройства.
4. Щракнете върху **Device Configuration** на раздела **Home** на менюто на лентата.

   Когато паролата на администратора е зададена, въведете паролата и щракнете върху **OK**.
5. Щракнете върху **Common** > **Contacts**.

6. Изберете формата за експортиране от **Export** > **Export items**.

   ❏ All Items

   Експортирайте криптирания двоичен файл. Изберете кога искате да включите елементите за сигурност като парола и лична информация. Не можете да редактирате файла. Ако го изберете, Вие трябва да зададете паролата. Щракнете върху **Configuration** и задайте парола с дължина между 8 и 63 знака в ASCII. Тази парола е задължителна при импортиране на двоичен файл.

   ❏ Items except Security Information

   Експортирайте файловете в SYLK или csv формат. Изберете кога искате да редактирате информацията на експортирания файл.

7. Щракнете върху **Export**.

8. Посочете мястото за запис на файла, изберете типа файл, след което щракнете върху **Save**.

   Извежда се съобщение за завършване.

9. Щракнете върху **OK**.

   Проверете дали файлът е записан в посоченото място.

Импортиране на контакти

Импортирайте информацията за контакти от файла.

Можете да импортирате файловете, записани в SYLK или csv формат или архивиран двоичен файл, който включва елементите за сигурност.

1. Стартирайте Epson Device Admin.

2. Изберете **Devices** на менюто със задачи на страничната лента.

3. Изберете устройството, което искате да конфигурирате, от списъка с устройства.

4. Щракнете върху **Device Configuration** на раздела **Home** на менюто на лентата.

   Когато паролата на администратора е зададена, въведете паролата и щракнете върху **OK**.

5. Щракнете върху **Common** > **Contacts**.

6. Щракнете върху **Browse** на **Import**.

7. Изберете файла, който искате да импортирате, и щракнете върху **Open**.

   Когато изберете двоичен файл въведете в **Password** паролата, която сте задали при експортирането на файла.

8. Щракнете върху **Import**.

   Извежда се екранът за потвърждение.

9. Щракнете върху **OK**.

   Извежда се резултатът от потвърждението.

   ❏ Edit the information read

   Щракнете, когато искате да редактирате информацията поотделно.

❏ Read more file

Щракнете, когато искате да импортирате няколко файла.

10. Щракнете върху **Import**, след което натиснете **OK** на екрана за завършване на импортирането.

    Върнете се на екрана със свойства на устройството.

11. Щракнете върху **Transmit**.

12. Щракнете върху **OK** върху съобщението за потвърждение.

    Настройките се изпращат към скенера.

13. На екрана за завършване на изпращането щракнете върху **OK**.

    Информацията на скенера се актуализира.

    Отворете контактите от Web Config или от контролния панел на скенера, след което проверете дали контактът е актуализиран.

Съвместна работа между LDAP сървър и потребители

Когато работите с LDAP сървър, Вие можете да използвате информацията за адрес, регистрирана на LDAP сървъра като местоназначение на имейл.

Конфигуриране на LDAP сървъра

За да използвате информацията за LDAP сървъра, регистрирайте го на скенера.

1. Влезте в Web Config и изберете раздела **Network** > **LDAP Server** > **Basic**.

2. Въведете стойност за всеки елемент.

3. Изберете **OK**.

   Избраните от Вас настройки ще бъдат показани.

Елементи за настройка на LDAP сървър

Елементи	Настройки и обяснение
Use LDAP Server	Изберете **Use** или **Do Not Use**.
LDAP Server Address	Въведете адреса на LDAP сървъра. Въведете между 1 и 255 знака във формат IPv4, IPv6 или FQDN. За формат FQDN можете да използвате букви и цифри в ASCII (0x20 – 0x7E) и „-“, освен за началото и края на адреса.
LDAP server Port Number	Въведете номера на порта на LDAP сървъра, като използвате стойност между 1 и 65 535.
Secure Connection	Определете метода за удостоверяване, когато скенерът се опитва да осъществи достъп до LDAP сървъра.

Елементи	Настройки и обяснение
Certificate Validation	Когато това е активирано, сертификатът на LDAP сървъра се валидира. Препоръчваме тази опция да се зададе на **Enable**. За да конфигурирате, **CA Certificate** трябва да се импортира в скенера.
Search Timeout (sec)	Задайте периода за търсене, преди времето на изчакване да изтече, в диапазона от 5 до 300.
Authentication Method	Изберете един от методите. Ако изберете **Kerberos Authentication**, изберете **Kerberos Settings** за извършване на настройки за Kerberos. За да извършите Kerberos Authentication, е необходима следната среда. ❏ Скенерът и DNS сървърът могат да комуникират. ❏ Времето на скенера, KDC сървърът и сървърът, който е необходим за удостоверяване (LDAP сървър, SMTP сървър, файлов сървър), се синхронизират. ❏ Когато сървърът на услугата е назначен като IP адрес, FQDN на сървъра на услугата се регистрира на обратната зона за търсене на DNS сървъра.
Kerberos Realm to be Used	Ако изберете **Kerberos Authentication** за **Authentication Method**, изберете областта на Kerberos, която искате да използвате.
Administrator DN / User Name	Въведете потребителското име за LDAP сървъра с максимум 128 знака в Unicode (UTF-8). Не можете да използвате контролни знаци като 0x00 – 0x1F и 0x7F. Тази настройка не се използва, когато сте избрали **Anonymous Authentication** като **Authentication Method**. Ако не искате да посочвате нищо, оставете полето празно.
Password	Въведете паролата за удостоверяването чрез LDAP сървър с максимум 128 знака в Unicode (UTF-8). Не можете да използвате контролни знаци като 0x00 – 0x1F и 0x7F. Тази настройка не се използва, когато сте избрали **Anonymous Authentication** като **Authentication Method**. Ако не искате да посочвате нищо, оставете полето празно.

Настройки за Kerberos

Ако изберете **Kerberos Authentication** за **Authentication Method** на **LDAP Server** > **Basic**, направете следните настройки Kerberos от раздела **Network** > **Kerberos Settings**. Можете да регистрирате до 10 настройки за Kerberos.

Елементи	Настройки и обяснение
Realm (Domain)	Въведете областта за удостоверяване с Kerberos, като използвате максимум 255 знака във формат ASCII (0x20 – 0x7E). Ако не го регистрирате, оставете полето празно.
KDC Address	Въведете адреса на сървъра за удостоверяване с Kerberos. Въведете максимум 255 знака във формат IPv4, IPv6 или FQDN. Ако не го регистрирате, оставете полето празно.
Port Number (Kerberos)	Въведете номера на порта на сървъра за Kerberos, като използвате стойност между 1 и 65 535.

Конфигуриране на настройките за търсене на LDAP сървъра

Когато конфигурирате настройките за търсене, Вие можете да използвате имейл адреса, регистриран към LDAP сървъра.

1. Влезте в Web Config и изберете раздел **Network** > **LDAP Server** > **Search Settings**.
2. Въведете стойност за всеки елемент.
3. Щракнете върху бутона **OK**, за покажете резултата от настройването.

   Избраните от Вас настройки ще бъдат показани.

Елементи за настройка на търсене в LDAP сървър

Елементи	Настройки и обяснение
Search Base (Distinguished Name)	Ако искате да потърсите в произволен домейн, посочете името на домейна на LDAP сървъра. Въведете между 0 и 128 знака в Unicode (UTF-8). Ако не търсите произволен атрибут, оставете този елемент празен. Пример за директорията на локалния сървър: dc=server,dc=local
Number of search entries	Посочете броя на записите за търсене в диапазона от 5 до 500. Посоченият брой на записите за търсене се записва и показва временно. Дори ако броят на записите за търсене е над посочения брой и се покаже съобщение за грешка, търсенето може да бъде изпълнено.
User name Attribute	Посочете името на атрибута, който да се покаже при търсене на потребителски имена. Въведете между 1 и 255 знака в Unicode (UTF-8). Първият знак трябва да е измежду a – z или A – Z. Пример: cn, uid
User name Display Attribute	Посочете името на атрибута, който да се покаже като потребителското име. Въведете между 0 и 255 знака в Unicode (UTF-8). Първият знак трябва да е измежду a – z или A – Z. Пример: cn, sn
Email Address Attribute	Посочете името на атрибута, който да се покаже при търсене на имейл адреси. Въведете комбинация от 1 – 255 знака, включващи A – Z, a – z, 0 – 9 и -. Първият знак трябва да е измежду a – z или A – Z. Пример: mail
Arbitrary Attribute 1 - Arbitrary Attribute 4	Можете да посочите други произволни атрибути за търсене. Въведете между 0 и 255 знака в Unicode (UTF-8). Първият знак трябва да е измежду a – z или A – Z. Ако не търсите произволни атрибути, оставете този елемент празен. Пример: o, ou

Проверка на връзката с LDAP сървъра

Извършва тест на връзката към LDAP сървъра с помощта на параметъра, зададен на **LDAP Server** > **Search Settings**.

1. Влезте в Web Config и изберете раздел **Network** > **LDAP Server** > **Connection Test**.

2. Изберете **Start**.

   Тестването на връзката е стартирано. След теста се показва отчетът за проверката.

Предпочитания за тестване на връзка с LDAP сървър

Съобщения	Разяснение
Connection test was successful.	Това съобщение се показва, когато свързването със сървъра е успешно.
Connection test failed. Check the settings.	Това съобщение се показва поради следните причини: ❏ Адресът или номерът на порта на LDAP сървъра е неправилен. ❏ Времето на изчакване е изтекло. ❏ Опцията **Do Not Use** е избрана за **Use LDAP Server**. ❏ Ако опцията **Kerberos Authentication** е избрана за **Authentication Method**, настройките, като например **Realm (Domain)**, **KDC Address** и **Port Number (Kerberos)**, са неправилни.
Connection test failed. Check the date and time on your product or server.	Това съобщение се показва, когато осъществяването на връзка е неуспешно поради несъответствие между настройките за време на скенера и LDAP сървъра.
Authentication failed. Check the settings.	Това съобщение се показва поради следните причини: ❏ **User Name** и/или **Password** са неправилни. ❏ Ако опцията **Kerberos Authentication** е избрана за **Authentication Method**, часът/датата може да не са конфигурирани.
Cannot access the product until processing is complete.	Това съобщение се показва, когато скенерът е зает.

Настройване на AirPrint

Влезте в Web Config и изберете раздела **Network**, след което изберете **AirPrint Setup**.

Елементи	Разяснение
Bonjour Service Name	Въведете име на услугата Bonjour, като използвате ASCII текст (0x20 – 0x7E) и до 41 знака.
Bonjour Location	Въведете описание на местоположението на скенера, като използвате Unicode (UTF-8) текст и до 127 байта.
Wide-Area Bonjour	Задайте дали искате да използвате Wide-Area Bonjour. Ако го използвате, скенерът трябва да бъде регистриран на DNS сървъра, за да търси скенера в сегмента.
Enable AirPrint	Активира Bonjour и AirPrint (услуга за сканиране). Този бутон е наличен само когато сте активирали AirPrint. ***Забележка:*** *Ако AirPrint е дезактивирано, Mopria сканирането от Chromebooks, Windows и от Mopria Scan също е дезактивирано.*

Проблеми при подготовка на мрежово сканиране

Съвети за разрешаване на проблеми

❏ Проверка на съобщението за грешка

При възникването на проблем, първо проверете дали има съобщения на контролния панел на скенера или на екрана на драйвера. Ако сте задали имейл известие при възникване на събития, Вие можете незабавно да научите състоянието.

❏ Проверка на състоянието на комуникацията

Проверете състоянието на комуникацията на сървъра или на клиентския компютър с помощта на команда като ping и ipconfig.

❏ Тестване на връзката

За проверка на връзката между скенера и имейл сървъра извършете тест на връзката от скенера. Освен това проверете връзката от клиентския компютър към сървъра, за да проверите състоянието на комуникацията.

❏ Инициализиране на настройките

Ако няма проблем в настройките и състоянието на комуникация, проблемите могат да бъдат разрешени чрез дезактивиране или инициализиране на настройките на мрежата на скенера, след което отново да извършите настройка.

Няма достъп до Web Config

IP адресът не е назначен към скенера.

Решения

Валиден IP адрес може да не е назначен към скенера. Конфигурирайте IP адреса, като използвате контролния панел на скенера. Можете да потвърдите текущата информация за настройка от контролния панел на скенера.

Уеб браузърът не поддържа сила на криптиране за SSL/TLS.

Решения

SSL/TLS има Encryption Strength. Можете да отворите Web Config с помощта на уеб браузър, който поддържа групово криптиране, както е посочено по-долу. Проверете дали използвате поддържан браузър.

❏ 80 бита: AES256/AES128/3DES

❏ 112 бита: AES256/AES128/3DES

❏ 128 бита: AES256/AES128

❏ 192 бита: AES256

❏ 256 бита: AES256

CA-signed Certificate е изтекъл.

Решения

Ако има проблем с датата на изтичане на сертификата, се извежда съобщението „Сертификатът е изтекъл“ при свързване към Web Config с SSL/TLS комуникация (https). Ако съобщението се изведе преди датата на изтичане, се уверете, че датата на скенера е правилно конфигурирана.

Използваното име на сертификата и скенера не съвпадат.

Решения

Ако общото име на сертификата и на скенера не съвпадат, се извежда съобщението „Името на сертификата за сигурност не съвпада с…“ при достъп до Web Config чрез SSL/TLS комуникация (https). Това се случва, защото следните IP адреси не съвпадат.

- ❏ Въведеният IP адрес на скенера за използвано име за създаване на Self-signed Certificate или CSR
- ❏ IP адрес, въведен в уеббраузър при изпълнение на Web Config

За Self-signed Certificate, актуализирайте сертификата.

За CA-signed Certificate вземете отново сертификата за скенера.

Настройката на прокси сървъра на локален адрес не е зададена в уеб браузъра.

Решения

Когато скенерът е зададен да използва прокси сървър, конфигурирайте уеб браузъра да не се свързва към локалния адрес чрез прокси сървъра.

- ❏ Windows:

  Изберете **Контролен панел** > **Мрежа и интернет** > **Интернет опции** > **Връзки** > **Настройки на LAN** > **Прокси сървър**, след което конфигурирайте да не използвате прокси сървъра за LAN (локални адреси).

- ❏ Mac OS:

  Изберете **System Preferences** (или **System Settings**) > **Network** > **Advanced** > **Proxies**, след което регистрирайте локалния адрес за **Bypass proxy settings for these Hosts & Domains**.

  Пример:

  192.168.1.*: Локален адрес 192.168.1.XXX, подмрежова маска 255.255.255.0

  192.168.*.*: Локален адрес 192.168.XXX.XXX, подмрежова маска 255.255.0.0

DHCP е дезактивирано в настройките на компютъра.

Решения

Ако DHCP за получаване на IP адрес автоматично е дезактивирано на компютъра, нямате достъп до Web Config. Активирайте DHCP.

Пример за Windows 10:

Отворете контролния панел и щракнете върху **Мрежа и интернет** > **Център за мрежи и споделяне** > **Промяна на настройките на адаптера**. Отворете екрана със свойства на връзката, която използвате, и след това отворете екрана със свойства за **Интернет протокол версия 4 (TCP/IPv4)** или **Интернет протокол версия 6 (TCP/IPv6)**. Проверете дали **Получаване на IP адрес автоматично** е избрано на изведения екран.

Персонализиране на дисплея на контролния панел

Регистриране на Предв.настр.

Можете да регистрирате често използвана настройка за сканиране като **Предв.настр.**. Можете да регистрирате до 48 предварителни настройки.

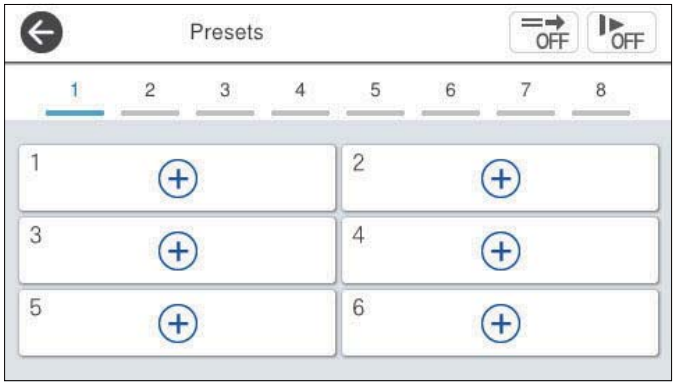
Забележка:

- *Можете да регистрирате текущите настройки чрез избиране на ★ на екрана за стартиране на сканиране.*
- *Можете също да регистрирате **Presets** в Web Config.*

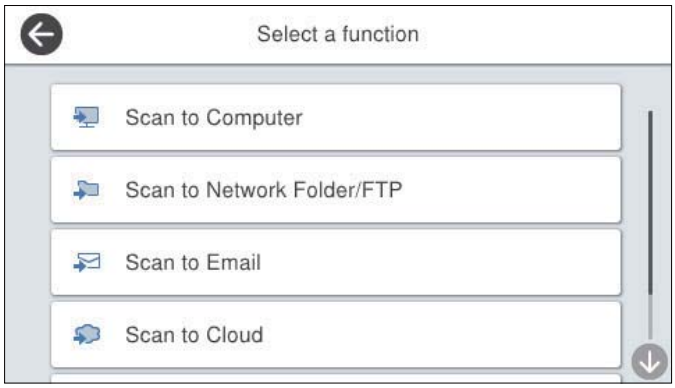
  *Изберете раздел **Scan** > **Presets**.*
- *Ако изберете **Сканиране на компютър** при регистриране, можете да регистрирате заданието, създадено в Document Capture Pro като **Presets**. Това е налично само за компютри, свързани в мрежа. Регистрирайте заданието в Document Capture Pro предварително.*
- *При активирана функция за удостоверяване само администраторът може да регистрира **Presets**.*

1. Изберете **Предв.настр.** на началния екран от контролния панел на скенера.

2. Изберете ⊕.



3. Изберете менюто, което желаете да използвате за регистриране на предварителна настройка.



4. Задайте всеки елемент и изберете ☆+.

   Забележка:
   При избор на ***Сканиране на компютър*** *изберете компютъра, на който е инсталирано Document Capture Pro, след което изберете регистрирано задание. Това е налично само за компютри, свързани в мрежа.*

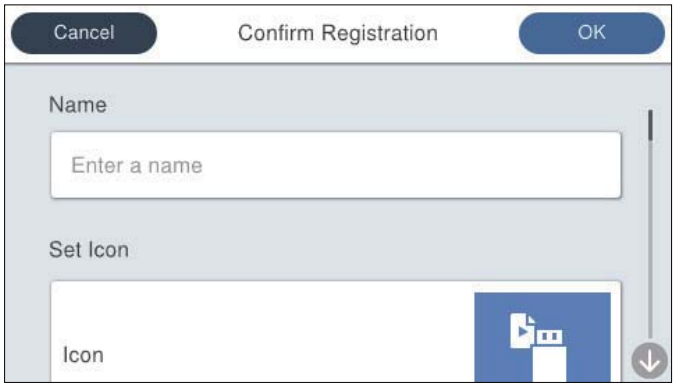
5. Направете предварителните настройки.

   ❏ **Име**: задайте името.

   ❏ **Задаване на Икона**: задава изображението и цвета на иконата за извеждане.

   ❏ **Настройка Бързо изпращане**: незабавно започва сканирането без потвърждение, когато е избрана предварителната настройка.

   ❏ **Съдържание**: проверете настройките за сканиране.



6. Изберете **OK**.

Опции на менюто на Предв.настр.

Можете да промените настройките на предварителна настройка, като изберете › във всяка предварителна настройка.

Промяна на Име:

Променя името на предварителната настройка.

Промяна на Икона:

Променя изображението на иконата и цвета на предварителната настройка.

Настройка Бързо изпращане:

Незабавно започва сканирането без потвърждение, когато е избрана предварителната настройка.

Промяна на позиция:

Променя реда на показване на предварителните настройки.

Изтриване:

Изтрива предварителната настройка.

Добавяне или премахване на Икона в Начало:

Добавя или изтрива иконата на предварителната настройка от началния екран.

Потвърдете Детайли:

Преглежда настройките на предварителна настройка. Можете да заредите предварителната настройка, като изберете **Използ. т. настро.**.

Редактиране на началния екран на контролния панел

Можете да персонализирате началния екран, като изберете **Настройки** > **Редактиране Нач. екран** от контролния панел на скенера.

- ❏ Оформление: променя метода на показване на иконите на менютата.
  "Промяна на Оформление на началния екран" на страница 73
- ❏ Добавяне на икона: добавя икони към настройките на **Предв.настр.**, които сте направили, или възстановява икони, които са били премахнати от екрана.
  "Добавяне на икона" на страница 74
- ❏ Отстраняване на икона: премахва икони от началния екран.
  "Отстраняване на икона" на страница 75
- ❏ Преместване на икона: променя реда на показване на иконите.
  "Преместване на икона" на страница 76
- ❏ Възст. показване икони по подразб.: възстановява настройките за извеждане по подразбиране за началния екран.

Промяна на Оформление на началния екран

1. Изберете **Настройки** > **Редактиране Нач. екран** > **Оформление** от контролния панел на скенера.

2. Изберете **Линия** или **Матрица**.

   Линия:

   Матрица:

3. Изберете за връщане и проверка на началния екран.

Добавяне на икона

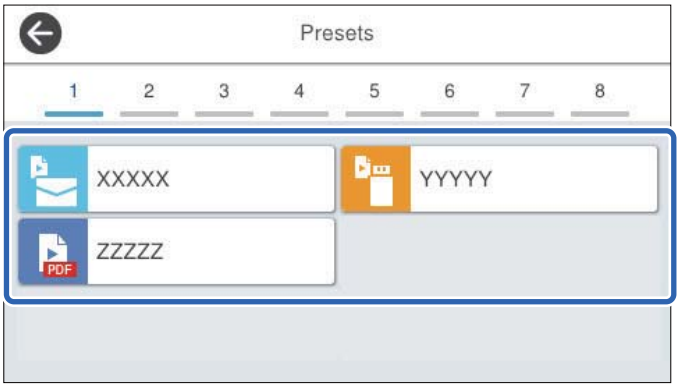
1. Изберете **Настройки** > **Редактиране Нач. екран** > **Добавяне на икона** от контролния панел на скенера.

2. Изберете **Функция** или **Предв.настр.**.

   ❏ Функция: извежда функциите по подразбиране на началния екран.

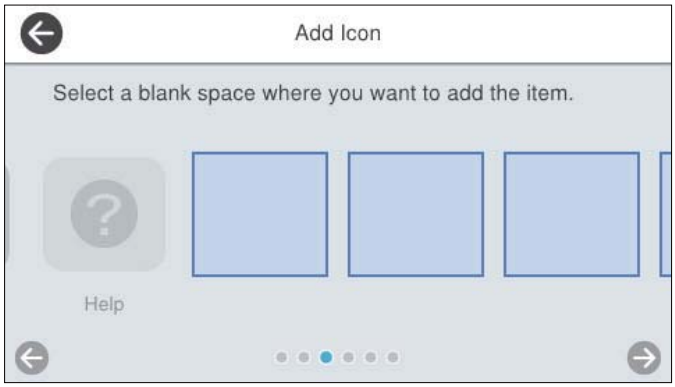
❏ Предв.настр.: извежда регистрираните предварителни настройки.

3. Изберете елемента, който искате да добавите на началния екран.



4. Изберете свободното пространство, на което желаете да добавите елемента.

   Ако желаете да добавите повече икони, повторете стъпки 3 до 4.

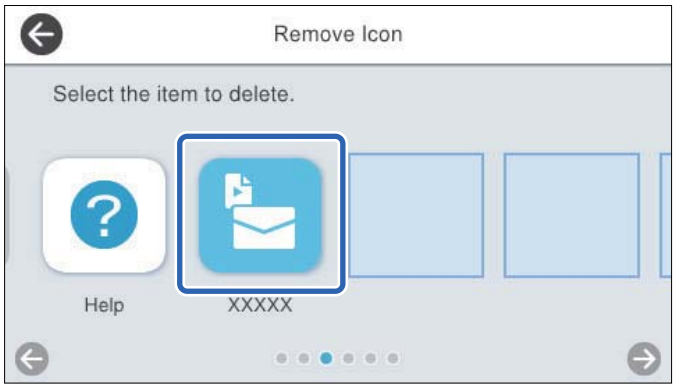


5. Изберете за връщане и проверка на началния екран.

Отстраняване на икона

1. Изберете **Настройки** > **Редактиране Нач. екран** > **Отстраняване на икона** от контролния панел на скенера.

2. Изберете иконата, която желаете да премахнете.



3. Изберете **Да**, за да завършите.

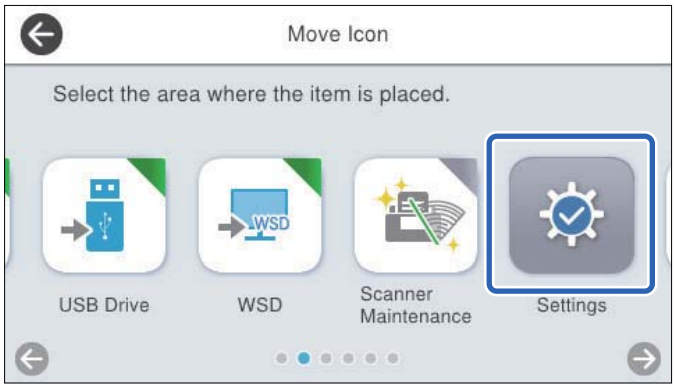
   Ако желаете да премахнете повече икони, повторете процедура 2 до 3.

4. Изберете за връщане и проверка на началния екран.

Преместване на икона

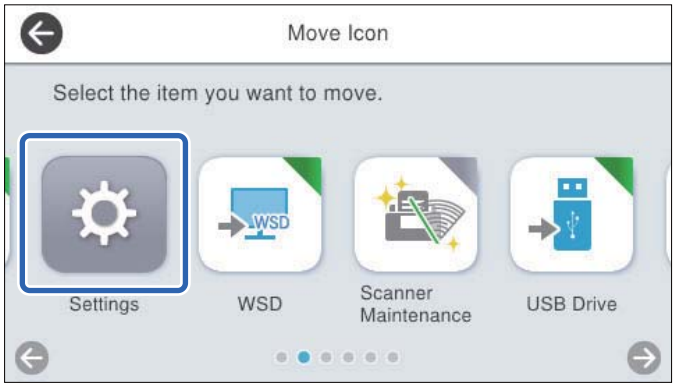
1. Изберете **Настройки** > **Редактиране Нач. екран** > **Преместване на икона** от контролния панел на скенера.

2. Изберете иконата, която желаете да преместите.



3. Изберете рамката на местоназначението.

   Ако друга икона вече е поставена в рамката на местоназначението, иконите се заменят.



4. Изберете за връщане и проверка на началния екран.

Основни настройки за сигурност

Представяне на функции за защита на продукта

Този раздел представя функцията за защита на устройствата Epson.

Име на функция	Тип функция	Какво да зададете	Какво да предотвратите
Конфигуриране на парола на администратора	Заключва системните настройки, като например настройка на връзка за мрежа или USB.	Администратор задава парола към устройството. Можете да зададете или промените от Web Config и от контролния панел на скенера.	Предотвратяване на незаконно прочитане или промяна на информация, съхранена в устройството, като ИД, парола, мрежови настройки и т.н. Освен това намалява широка гама рискове за сигурността като изтичане на информация за мрежовата среда или политиката за сигурност.
Access Control Settings	Ако влезете в устройството с потребителски акаунт, който е предварително регистриран, Вие имате право да използвате устройството.	Регистрирайте потребителски акаунт. Можете да регистрирате до 10 потребителски акаунта.	Ограничаването на потребители предотвратява неоторизирано използване на устройството.
Настройка за външен интерфейс	Управлява интерфейса, който се свързва към устройството.	Активирайте или дезактивирайте USB връзката с компютъра.	USB връзка към компютър: предотвратява неупълномощен достъп на устройството, като забранява сканирането, без да преминава през мрежата.

Още по темата

➡ “Конфигуриране на парола на администратора” на страница 79

➡ “Дезактивиране на външния интерфейс” на страница 87

Настройки на администратора

Конфигуриране на парола на администратора

Когато зададете парола на администратор, Вие можете да предотвратите потребителите да променят настройките за управление на системата. Стойностите по подразбиране са вече зададени по време на покупката. Променете ги, както е нужно.

Забележка:
Следното предоставя стойностите по подразбиране за информацията за администратора.

❏ *Потребителско име (използвано само за Web Config): няма (празно)*

❏ *Парола: Зависи от етикета, прикрепен към продукта.*

Ако на гърба има прикрепен етикет „PASSWORD“, въведете 8-цифрения номер, показан на етикета. Ако няма прикрепен етикет „PASSWORD“, въведете серийния номер на етикета, прикрепен на гърба на продукта, за първоначална парола на администратор.

Можете да промените паролата на администратор, като използвате Web Config, контролния панел на скенера или Epson Device Admin. Когато използвате Epson Device Admin, вижте ръководството на Epson Device Admin или помощта.

Промяна на паролата на администратор с Web Config

Променете паролата на администратора в Web Config.

1. Влезте в Web Config и изберете раздел **Product Security** > **Change Administrator Password**.
2. Въведете нужната информация в **Current password**, **User Name**, **New Password** и **Confirm New Password**.

   Новата парола трябва да е с дължина от 8 до 20 знака и да съдържа само еднобайтови буквено-цифрови знаци и символи.

   Забележка:
   Следното предоставя стойностите по подразбиране за информацията за администратора.

   ❏ *Потребителско име: няма (празно)*

   ❏ *Парола: Зависи от етикета, прикрепен към продукта.*

   Ако на гърба има прикрепен етикет „PASSWORD“, въведете 8-цифрения номер, показан на етикета. Ако няма прикрепен етикет „PASSWORD“, въведете серийния номер на етикета, прикрепен на гърба на продукта, за първоначална парола на администратор.

   > ***Важно:***
   > *Погрижете се да запомните паролата на администратор, която зададете. Ако забравите паролата си, няма да имате възможност да я нулирате и ще се наложи да потърсите помощ от сервизния персонал.*

3. Изберете **OK**.

Още по темата

➡ “Как да стартирате Web Config в уеб браузър” на страница 40

Промяна на паролата на администратор от контролния панел на скенера

Можете да промените паролата на администратор от контролния панел на скенера.

1. Изберете **Настройки** от контролния панел на скенера.
2. Изберете **Системна администрация** > **Администраторски настройки**.
3. Изберете **Администраторска парола** > **Промяна**.
4. Въведете текущата си парола.

   Забележка:
   Първоначалната парола на администратор (по подразбиране) по време на покупката зависи от етикета, прикрепен към продукта. Ако на гърба има прикрепен етикет „PASSWORD“, въведете 8-цифрения номер, показан на етикета. Ако няма прикрепен етикет „PASSWORD“, въведете серийния номер на етикета, прикрепен на гърба на продукта, за първоначална парола на администратор.

5. Въведете новата Ви парола.

   Новата парола трябва да е с дължина от 8 до 20 знака и да съдържа само еднобайтови буквено-цифрови знаци и символи.

   > ***Важно:***
   >
   > *Погрижете се да запомните паролата на администратор, която зададете. Ако забравите паролата си, няма да имате възможност да я нулирате и ще се наложи да потърсите помощ от сервизния персонал.*

6. Въведете отново новата парола за потвърждение.

Извежда се съобщение за завършване.

Използване на Заключване на настройка за контролния панел

Можете да използвате Заключване на настройка, за да заключите контролния панел, за да попречите на потребителите да променят елементи, свързани със системните настройки.

Настройка на Заключване на настройка от контролния панел

1. Ако искате да отмените **Заключване на настройка**, след като е активирана, докоснете в горния десен ъгъл на началния екран, за да влезете като администратор.

   не се показва, когато **Заключване на настройка** е дезактивирана. Ако искате да активирате тази настройка, преминете към следващата стъпка.

2. Изберете **Настройки**.

3. Изберете **Системна администрация** > **Администраторски настройки**.

4. Изберете **Вкл.** или **Изкл.** като **Заключване на настройка**.

Настройка Заключване на настройка от Web Config

1. Изберете раздел **Device Management** > **Control Panel**.

2. Изберете **ON** или **OFF** за **Panel Lock**.

3. Щракнете върху **OK**.

Още по темата

➡ “Как да стартирате Web Config в уеб браузър” на страница 40

Елементи Заключване на настройка в менюто Настройки

Това е списък с елементи, които са заключени в менюто **Настройки** на контролния панел от Заключване на настройка.

✓: да бъде заключено.

- : Да не се заключва.

Меню Настройки		**Заключване на настройка**
Осн. Настройки		–
	Яркост на LCD	–
	Звуци	–
	Таймер за сън	✓
	Таймер за изключване	✓
	Директно вкл.	✓
	Настройки на дата/час	✓
	Език/Language	✓/-*
	Клавиатура (Тази функция може да не е налична в зависимост от Вашия регион.)	-
	Време на изчакване на работа	✓
	Свързване с компютър чрез USB	✓
Настр. на скенера		–
	Бавно	–
	Вр. спиране за дв. подаване	✓
	DFDS функция	–
	Защита на хартия	✓
	Откриване на замърсяване на стъклото	✓
	Откр. на двойно подав.	✓
	Изтичане на времето на Режим на автоматично подаване	✓
	Потвърждаване на получател	✓
Редактиране Нач. екран		✓

Меню Настройки		**Заключване на настройка**
	Оформление	✓
	Добавяне на икона	✓
	Отстраняване на икона	✓
	Преместване на икона	✓
	Възст. показване икони по подразб.	✓
Потребителски настройки		✓
	Мрежова папка/FTP	✓
	Имейл	✓
	Облак	✓
	USB памет	✓
Настройки на мрежата		✓
	Wi-Fi настройка	✓
	Кабелна LAN настройка	✓
	Мрежов статус	✓
	Разширени	✓
Услуги на уеб настройки		✓
	Услуги Epson Connect	✓
Document Capture Pro		–
	Промяна на настройки	✓
Диспечер на Контакти		–
	Регистриране/изтриване	✓/-*
	Често срещан	–
	Опции на преглед	–
	Опции на търсене	–
Системна администрация		✓

Меню Настройки			**Заключване на настройка**
	Диспечер на Контакти		✓
	Администраторски настройки		✓
	Ограничения		✓
	Управление на достъпа		✓
	Шифроване на парола		✓
	Клиентско проучване		✓
	WSD настройки		✓
	възст. на наст. по подразбиране		✓
	Актуализация на фърмуера		✓
Информация за устройството			–
	Сериен номер		–
	Текуща версия		–
	Общ брой сканирания		–
	Брой 1-странни сканирания		–
	Брой 2-странни сканирания		–
	Брой сканир. на Подложка		–
	Бр. ск. след см. ролка		–
	Бр. скан. след Ред. почиств.		–
	Състояние на удостоверяване на устройство		–
	Информация за Epson Open Platform		–
	Menu (Нулиране на брой сканирания)		✓
Техническо обсл. Скенера			–
	Почистване на ролки		–
	Смяна на поддържаща ролка		–
		Нулиране на брой сканирания	✓
		Как се сменя	–
	Ред. почиств.		–
		Нулиране на брой сканирания	✓
		Как да почистите	–
	Почиств. стъкло		–
Настр. на аларма за подмяна на ролката			✓

Меню Настройки		Заключване на настройка
	Настр. предупр. за бр.	✓
Настройки за предупреждение за редовно почистване		✓
	Настройка за предупреждение	✓
	Настр. предупр. за бр.	✓

* Можете да посочите дали да разрешите печат в **Системна администрация** > **Ограничения**.

Влизане като администратор от контролния панел

Когато сте активирали **Заключване на настройка**, Вие можете да използвате някои от следните методи, за да влезете от контролния панел на скенера.

1. Докоснете в горния десен ъгъл на екрана.
2. Когато е изведен екранът **Избор на потребител**, изберете **Администратор**.
3. Въведете паролата за влизане.

   Показва се съобщение за завършено влизане и след това се показва началният екран на контролния панел.

За да излезете, докоснете в горния десен ъгъл на екрана и натиснете бутона .

Ограничаване на наличните функции (Управление на достъпа)

Можете да ограничите потребителите, като регистрирате потребителски акаунти на скенера.

Когато сте активирали Управление на достъпа, потребителят може да използва функциите за сканиране, като въведе паролата на контролния панел на скенера и се впише. Вие не можете да сканирате, ако не сте вписани.

Можете да сканирате от компютър, като регистрирате своето Потребителско име и Парола в драйвера на скенера (Epson Scan 2). Вижте помощта за Epson Scan 2 или *Ръководство на потребителя* на продукта за подробности относно извършване на настройките.

Създаване на потребителски акаунт

Можете да създадете акаунт в Управление на достъпа.

1. Влезте в Web Config, след което изберете раздел **Product Security** > **Access Control Settings** > **User Settings**.

2. Щракнете върху **Add** за номера, който искате да регистрирате.

> ***Важно:***
>
> *Когато използвате скенера със система за удостоверяване от Epson или от друга компания, регистрирайте User Name в Access Control Settings в номер на слот 2 до 10.*
>
> *Софтуерът на приложението като системата за удостоверяване използва слот номер 1, така че потребителското име не се извежда на контролния панел на скенера.*

3. Задайте всеки елемент.

   ❏ User Name:

   Въведете името, което се извежда в списъка с потребителски имена, с дължина между 1 и 14 знака чрез буквено-цифрени знаци.

   ❏ Password:

   Въведете парола с дължина до 20 знака в ASCII (0x20-0x7E). Когато инициализирате паролата, оставете я празна.

   ❏ Select the check box to enable or disable each function.

   Изберете **Scan**, ако искате да разрешите функциите за сканиране.

4. Щракнете върху **Apply**.

Редактиране на потребителския акаунт

Можете да редактирате регистрирания акаунт в Управление на достъпа.

1. Влезте в Web Config, след което изберете раздел **Product Security** > **Access Control Settings** > **User Settings**.
2. Щракнете върху **Edit** за номера, който искате да редактирате.
3. Променете всеки елемент.
4. Щракнете върху **Apply**.

Изтриване на потребителския акаунт

Можете да изтриете регистрирания акаунт в Управление на достъпа.

1. Влезте в Web Config, след което изберете раздел **Product Security** > **Access Control Settings** > **User Settings**.
2. Щракнете върху **Edit** за номера, който искате да изтриете.
3. Щракнете върху **Delete**.

> ***Важно:***
>
> *Когато щракнете върху **Delete**, потребителският акаунт ще бъде изтрит без съобщение за потвърждение. Бъдете внимателни, когато изтривате акаунта.*

Активиране на Управление на достъпа

Когато активирате Управление на достъпа, само регистрираният потребител ще може да използва скенера.

Забележка:
Когато сте активирали Access Control Settings, трябва да уведомите потребителя относно информацията за неговия акаунт.

1. Влезте в Web Config, след което изберете раздел **Product Security** > **Access Control Settings** > **Basic**.
2. Изберете **Enables Access Control**.

   Ако активирате Access Control Settings и сканирате от компютър, който не разполага с информация за удостоверяване, изберете **Allow printing and scanning without authentication information from a computer**.
3. Щракнете върху **OK**.

Влизане в скенер, на който е активирано Управление на достъпа

Когато сте активирали **Управление на достъпа**, Вие можете да използвате някои от следните методи, за да влезете от контролния панел на скенера.

1. Докоснете в горния десен ъгъл на екрана.
2. Когато се появи екранът **Избор на потребител**, изберете потребителя.
3. Въведете паролата за влизане.

   Показва се съобщение за завършено влизане и след това се показва началният екран на контролния панел.

За да излезете, докоснете в горния десен ъгъл на екрана и натиснете бутона .

Дезактивиране на външния интерфейс

Можете да дезактивирате интерфейса, който се използва за свързване на устройството към скенера. Извършете настройките за ограничение, за да ограничите сканирането освен през интернет.

Забележка:
Можете също така да извършите настройките за ограничение от контролния панел на скенера.

*Свързване с компютър чрез USB: **Настройки** > **Осн. Настройки** > **Свързване с компютър чрез USB***

1. Влезте в Web Config и изберете раздел **Product Security** > **External Interface**.
2. Изберете **Disable** за функциите, които желаете да настроите.

   Изберете **Enable**, когато искате да отмените контролирането.

   Свързване с компютър чрез USB

   Можете да ограничите употребата на USB връзката от компютъра. Ако искате да го направите, изберете **Disable**.

3. Щракнете върху **OK**.
4. Проверете дали дезактивираният порт не може да се използва.

   Свързване с компютър чрез USB

   Ако драйверът е бил инсталиран на компютъра

   Свържете скенера към компютъра с помощта на USB кабел, след което потвърдете, че скенерът не сканира.

   Ако драйверът не е бил инсталиран на компютъра

   Windows:

   Отворете диспечера на устройства и го запазете, свържете скенера към компютъра с помощта на USB кабел, след което потвърдете, че съдържанието на дисплея на диспечера на устройството остава непроменено.

   Mac OS:

   Свържете скенера към компютъра с помощта на USB кабел, след което потвърдете, че не можете да добавите скенера от **Принтери и скенери**.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Активиране на потвърждение на програма при стартиране

Ако активирате функцията за потвърждение на програма, скенерът изпълнява потвърждение при стартиране, за да провери дали има намеса в програмата на неупълномощени трети страни. При откриване на проблеми скенерът не стартира.

Забележка:
Активирането на тази функция повишава времето за стартиране на скенера.

1. Отидете на Web Config, след което изберете раздел **Product Security** > **Program Verification on Start Up**.

   Забележка:
   Можете да извършвате настройки и на контролния панел на скенера.

   Настройки > ***Системна администрация*** > ***Проверка при зареждане***

2. Изберете **ON**, за да активирате **Program Verification on Start Up**.
3. Щракнете върху **OK**.

Дезактивиране на мрежовото сканиране от Вашия компютър

Можете да направите следните настройки в Web Config за да деактивирате мрежовото сканиране с помощта на Epson Scan 2 от Вашия компютър.

1. Отидете на Web Config, след което изберете раздел **Scan** > **Network Scan**.
2. В **Epson Scan 2** изчистете полето с отметка **Enable scanning**.
3. Щракнете върху **Next**.

   Извежда се екранът за потвърждение на настройките.
4. Щракнете върху **OK**.

Активиране или дезактивиране на WSD сканиране

Забележка:
Можете да извършвате настройки и на контролния панел на скенера. Изберете ***Настройки*** *>****Системна администрация*** *>* ***WSD настройки****.*

Можете да активирате или дезактивирате WSD сканирането.

Ако не искате Вашият компютър да конфигурира скенера като WSD сканиращо устройство, дезактивирайте WSD настройките.

1. Отидете на Web Config, след което изберете раздел **Network Security** > **Protocol**.
2. В **WSD Settings** променете полето с отметка **Enable WSD**.
3. Щракнете върху **Next**.

   Извежда се екранът за потвърждение на настройките.
4. Щракнете върху **OK**.

Забележка:
Ако компютърът Ви все още конфигурира скенера като WSD сканиращо устройство, изберете раздела ***Scan*** *>* ***Network Scan****, след което махнете отметката от* ***Enable scanning*** *в* ***AirPrint****.*

Ако AirPrint е дезактивирано, Mopria сканирането от Chromebooks, Windows и от Mopria Scan също е дезактивирано.

Наблюдение на отдалечен скенер

Проверка на информация за отдалечен скенер

Можете да проверите следната информация на работещия скенер от **Status** с помощта на Web Config.

- ❏ Product Status

  Проверете състоянието, облачната услуга, номера на продукта, MAC адреса и т.н.
- ❏ Network Status

  Проверете информацията на състоянието на мрежовата връзка, IP адреса, DNS сървъра и т.н.
- ❏ Usage Status

  Проверете първия ден на сканиране, брой сканирания и т.н.

❏ Hardware Status

Проверете състоянието на всяка функция на скенера.

❏ Panel Snapshot

Извежда се моментална снимка на екрана на контролния панел на скенера.

Получаване на имейл известия при възникване на събития

Относно известяванията по имейл

Това е функцията за известяване, която при събития като спиране на сканиране и грешка при сканиране изпраща имейла до посочения адрес.

Можете да регистрирате до пет местоназначения и да задавате настройки за известяване за всяко местоназначение.

За да използвате тази функция, Вие трябва да зададете имейл сървъра преди да зададете известявания.

Още по темата

➡ "Регистриране на имейл сървър" на страница 47

Конфигуриране на имейл известие

Конфигурирайте имейл известие с помощта на Web Config.

1. Влезте в Web Config и изберете раздел **Device Management** > **Email Notification**.
2. Задайте темата на имейл известието.

   Изберете съдържанието, изведено на темата от двете падащи менюта.

   ❏ Избраното съдържание се извежда до **Subject**.

   ❏ Едно и също съдържание не може да се задава отляво и отдясно.

   ❏ Когато броят на знаците в **Location** надвишава 32 байта, знаците, които надвишават 32 байта, ще бъдат пропуснати.
3. Въведете имейл адреса за изпращане на имейл известието.

   Използвайте A – Z a – z 0 – 9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @ и въведете между 1 и 255 знака.
4. Изберете езика за имейл известията.
5. Изберете квадратчето за отметка на събитието, за което искате да получавате известие.

   Броят на **Notification Settings** е свързан към номера на местоназначение на **Email Address Settings**.

   Пример:

   Ако желаете да се изпрати известие към имейл адреса, зададен за номер 1 в **Email Address Settings**, когато администраторската парола е променена, сложете отметка в квадратчето за колона **1** в ред **Administrator password changed**.

6. Щракнете върху **OK**.

   Потвърдете, че ще бъде изпратено имейл известие чрез причиняване на събитие.

   Пример: паролата на администратора е сменена.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Елементи за имейл известие

Елементи	Настройки и обяснение
Administrator password changed	Известие, когато паролата на администратора е сменена.
Scanner error	Известие при възникване на грешка на скенера.
Грешка на Wi-Fi	Известие при възникване на грешка на безжичния LAN интерфейс.

Използване на Web Config за управление на захранването на скенера

Ако Вашият компютър е отдалечен от скенера, Вие можете да използвате Web Config, за да изключите или рестартирате скенера.

1. Отидете на Web Config, след което изберете раздел **Device Management** > **Power**.
2. Изберете **Power Off** или **Reboot**.
3. Щракнете върху **Execute**.

Възстановяване на настройките по подразбиране

Можете да изберете мрежовите настройки или други настройки, съхранени в скенера, и да ги възстановите до стойностите им по подразбиране.

1. Отидете на Web Config, след което изберете раздел **Device Management** > **Restore Default Settings**.

   Забележка:
   Можете да извършвате настройки и на контролния панел на скенера.

   Настройки** > **Системна администрация** > **Възстановяване на настройки по подразбиране

2. Изберете елементите, които желаете да възстановите.
3. Щракнете върху **Execute**.

   Най-накрая следвайте инструкциите на екрана.

Информация за Epson Remote Services

Epson Remote Services е услуга, която периодично събира информация за скенера през интернет. Това може да се използва за прогнозиране кога ще бъде необходима смяна или повторно снабдяване с консумативи и резервни части, както и за бързо разрешаване на възникнали грешки или проблеми.

Свържете се с Вашия търговец за повече информация относно Epson Remote Services.

Решаване на проблеми

Забравена администраторска парола

Имате нужда от помощ от персонал по обслужване. Свържете се с Вашия местен дилър.

Забележка:
Следното предоставя първоначалните стойности за администратора на Web Config.

❏ *Потребителско име: няма (празно)*

❏ *Парола: Зависи от етикета, прикрепен към продукта.*

Ако на гърба има прикрепен етикет „PASSWORD“, въведете 8-цифрения номер, показан на етикета.

Ако няма прикрепен етикет „PASSWORD“, въведете серийния номер на етикета, прикрепен на гърба на продукта, за първоначална парола на администратор.

Ако възстановите паролата на администратора, тя се нулира до първоначалната стойност от времето на закупуване.

Разширени настройки за сигурност

Настройки за защита и предотвратяване на опасност

Когато даден скенер е свързан към мрежа, Вие можете да влезете в нея от отдалечено място. В допълнение много хора могат да споделят скенера, което е полезно при подобряване на ефективността и удобството. Въпреки това се увеличават рисковете като незаконен достъп, незаконна употреба и подправяне на данни. Ако използвате скенера в среда, в която имате достъп до интернет, рисковете са още по-големи.

За скенери, които не разполагат със защита на достъпа от външна среда, има възможност да прочетете от интернет контактите, които са съхранени в скенера.

За да избегнете този риск, скенерите Epson разполагат с различни технологии за защита.

Конфигурирайте скенера, ако е необходимо, в съответствие с условията на средата, която е била изградена с информацията за среда на клиента.

Име	Тип функция	Какво да зададете	Какво да предотвратите
Управление на протокол	Управлява протоколите и услугите, които ще се използват за комуникация между скенери и компютри, и активира и дезактивира функциите.	Протокол или услуга, която е приложена към функции, които се разрешават или забраняват поотделно.	Намаляване на рискове за сигурността, които могат да възникнат чрез непреднамерено използване, като не позволява на потребителите да използват ненужни функции.
SSL/TLS комуникации	Съдържанието за комуникация се шифрова със SSL/TLS комуникации при влизане в сървъра на Epson в интернет от скенера, като комуникация към компютъра чрез уеббраузър с помощта на Epson Connect и актуализиране на фърмуера.	Получаване на подписан от сертифициращ орган сертификат и импортиране в скенера.	Изчистване на идентификация на скенера от подписания от сертифициращ орган сертификат предотвратява въплъщаване и неупълномощен достъп. В допълнение съдържанието на комуникацията на SSL/TLS е защитено и не позволява изтичането на съдържание за данни за сканиране и информация за настройка.
IPsec/IP филтриране	Можете да конфигурирате разрешаването на изтриването или изрязването на данни, които са от определен клиент или от конкретен тип. Тъй като IPsec предпазва данните чрез IP пакети (шифроване и удостоверяване), Вие можете безопасно да предавате незащитен протокол.	Създавайте основна политика и индивидуална политика, за да конфигурирате клиента или типа данни, които имат право на достъп до скенера.	Защитете от неупълномощен достъп, подправяне и прихващане на комуникационни данни към скенера.

Име	Тип функция	Какво да зададете	Какво да предотвратите
IEEE 802.1X	Позволява свързване към мрежата само на удостоверени потребители. Позволява само на потребител с разрешение да използва скенера.	Настройка за удостоверяване към RADIUS сървъра (сървър за удостоверяване).	Защита от неупълномощен достъп и използване на скенера.

Още по темата

- "Управление чрез протоколи" на страница 95
- "SSL/TLS комуникация със скенера" на страница 104
- "Криптирана комуникация с IPsec/IP филтриране" на страница 105
- "Свързване на скенера към мрежа IEEE802.1X" на страница 116

Настройки на функция за защита

Когато задавате IPsec/IP филтриране или IEEE 802.1X, препоръчително е да влезете в Web Config чрез SSL/TLS за предаване на настройки за комуникация с цел намаляване на рисковете за защита като подправяне или прихващане.

Не забравяйте да конфигурирате паролата на администратора, преди да зададете IPsec/IP филтриране или IEEE 802.1X.

Управление чрез протоколи

Можете да сканирате, като използвате разнообразни пътища и протоколи. Също така можете да използвате мрежово сканиране от неопределен брой компютри в мрежа.

Можете да намалите случайните рискове за сигурността, като ограничите сканирането от определени пътища или чрез управление на достъпните функции.

Управляващи протоколи

Конфигурирайте поддържаните от скенера настройки на протоколите.

1. Влезте в Web Config и след това изберете раздела **Network Security** tab > **Protocol**.
2. Конфигурирайте всеки елемент.
3. Щракнете върху **Next**.
4. Щракнете върху **OK**.

   Настройките се прилагат към скенера.

Още по темата

- "Как да стартирате Web Config в уеб браузър" на страница 40

Протоколи, които можете да активирате или дезактивирате

Протокол	Описание
Bonjour Settings	Можете да посочите дали да използвате Bonjour. Bonjour се използва за търсене на устройства, сканиране и др.
SLP Settings	Можете да активирате или дезактивирате функцията SLP. SLP се използва за насочено сканиране и мрежово търсене в EpsonNet Config.
WSD Settings	Можете да активирате или дезактивирате функцията WSD. Когато тази опция е активирана, можете да добавяте WSD устройства и да сканирате от порта WSD.
LLTD Settings	Можете да активирате или дезактивирате функцията LLTD. Когато тази опция е активирана, това се извежда на мрежовата карта Windows.
LLMNR Settings	Можете да активирате или дезактивирате функцията LLMNR. Когато е активирана, можете да използвате име на разделителна способност без NetBIOS дори ако не можете да използвате DNS.
SNMPv1/v2c Settings	Можете да посочите дали разрешавате SNMPv1/v2c. Това се използва за настройка на устройства, наблюдение и т.н.
SNMPv3 Settings	Можете да посочите дали разрешавате SNMPv3. Това се използва за настройка на шифровани устройства, наблюдение и т.н.

Елементи за настройка на протокол

Bonjour Settings

Елементи	Стойност и описание на настройка
Use Bonjour	Изберете това за търсене на или използване на устройства чрез Bonjour.
Bonjour Name	Извежда името на Bonjour.
Bonjour Service Name	Извежда името на услуга Bonjour.
Location	Извежда името на местоположение на Bonjour.
Wide-Area Bonjour	Задайте дали да се използва Wide-Area Bonjour.

SLP Settings

Елементи	Стойност и описание на настройка
Enable SLP	Изберете това, за да активирате функцията SLP. Това се използва като търсене на мрежа в EpsonNet Config.

WSD Settings

Елементи	Стойност и описание на настройка
Enable WSD	Изберете го за активиране на добавяне на устройства чрез WSD и сканиране от порта WSD.
Scanning Timeout (sec)	Въведете стойността за изтичане на време на комуникация за сканиране с WSD между 3 и 3600 секунди.
Device Name	Извежда името на устройство на WSD.
Location	Извежда името на местоположение на WSD.

LLTD Settings

Елементи	Стойност и описание на настройка
Enable LLTD	Изберете това, за да активирате LLTD. Скенерът е показан в Windows карта на мрежата.
Device Name	Извежда името на устройство на LLTD.

LLMNR Settings

Елементи	Стойност и описание на настройка
Enable LLMNR	Изберете това, за да активирате LLMNR. Можете да използвате име на разделителна способност без NetBIOS дори ако не можете да използвате DNS.

SNMPv1/v2c Settings

Елементи	Стойност и описание на настройка
Enable SNMPv1/v2c	Изберете за активиране на SNMPv1/v2c.
Access Authority	Задайте органа за достъп, когато е активирано SNMPv1/v2c. Изберете **Read Only** или **Read/Write**.
Community Name (Read Only)	Въведете 0 до 32 ASCII (0x20 до 0x7E) знаци.
Community Name (Read/Write)	Въведете 0 до 32 ASCII (0x20 до 0x7E) знаци.

SNMPv3 Settings

Елементи	Стойност и описание на настройка
Enable SNMPv3	SNMPv3 е активирано, когато е поставена отметка в квадратчето.
User Name	Въведете между 1 и 32 знака, като използвате знаци от 1 байт.
Authentication Settings	

Елементи		Стойност и описание на настройка
	Algorithm	Изберете алгоритъм за удостоверяване на SNMPv3.
	Password	Въведете паролата за удостоверяване на SNMPv3. Въведете между 8 и 32 знака в ASCII (0x20 – 0x7E). Ако не искате да посочвате нищо, оставете полето празно.
	Confirm Password	Въведете паролата, която сте конфигурирали за потвърждение.
Encryption Settings		
	Algorithm	Изберете алгоритъм за шифроване на SNMPv3.
	Password	Въведете паролата за шифроване на SNMPv3. Въведете между 8 и 32 знака в ASCII (0x20 – 0x7E). Ако не искате да посочвате нищо, оставете полето празно.
	Confirm Password	Въведете паролата, която сте конфигурирали за потвърждение.
Context Name		Въведете в рамките на 32 знака или по-малко в Unicode (UTF-8). Ако не искате да посочвате нищо, оставете полето празно. Броят на знаците, които можете да въведете, варира в зависимост от езика.

Използване на цифров сертификат

Относно цифровото сертифициране

❏ CA-signed Certificate

Това е сертификат, подписан от сертифициращия орган (Орган за сертификати). Можете да го получите, за да подадете молба пред органа за сертификати. Този сертификат сертифицира наличието на скенера и се използва за SSL/TLS комуникация, за да се гарантира безопасността на комуникацията на данни.

Когато се използва за SSL/TLS комуникация, той се използва като сертификат за сървър.

Когато е зададен на IPsec/IP филтриране или IEEE 802.1X комуникация, той се използва като клиентски сертификат.

❏ Сертификат от сертифициращ орган

Това е сертификат, който е свързан със CA-signed Certificate, наричан също така междинен сертификат от сертифициращ орган. Използва се от уеббраузъра за валидиране на пътя на сертификата на скенера при достъп до сървъра от трета страна или от Web Config.

За сертификата от сертифициращ орган, задава се кога да валидира пътя до сертификата на сървъра, който осъществява достъп от скенера. За скенера задайте сертифициране на пътя до CA-signed Certificate за SSL/TLS връзка.

Можете да получите сертификата от сертифициращ орган на скенера от органа за сертификати, където е издаден сертификатът от сертифициращ орган.

Освен това можете да получите сертификата от сертифициращ орган, използван за валидиране на сървъра на другата страна, от органа за сертификати, който е издал CA-signed Certificate на другия сървър.

❏ Self-signed Certificate

Това е сертификат, че скенерът се подписва и издава. Нарича се също главен сертификат. Тъй като издателят сертифицира себе си, той не е надежден и не може да предотврати въплъщаване.

Използвайте го, когато извършвате настройката за сигурност и изпълнявате проста SSL/TLS комуникация без CA-signed Certificate.

Ако използвате този сертификат за SSL/TLS комуникация, на уеббраузъра може да бъде изведено предупреждение за сигурността, тъй като сертификатът не е регистриран в уеббраузъра. Можете да използвате Self-signed Certificate само за SSL/TLS комуникация.

Още по темата

➡ “Конфигуриране на CA-signed Certificate” на страница 99

➡ “Актуализиране на самоподписан сертификат” на страница 102

➡ “Конфигуриране на CA Certificate” на страница 103

Конфигуриране на CA-signed Certificate

Получаване на сертификат, подписан от сертифициращ орган

За да получите сертификат, подписан от сертифициращ орган, създайте CSR (заявка за подписване на сертификат) и я приложете по отношение на сертифициращия орган.Можете да създадете CSR с помощта на Web Config и компютър.

Следвайте стъпките, за да създадете CSR и да получите сертификат, подписан от сертифициращ орган, с помощта на Web Config.Когато създавате CSR с помощта на Web Config, сертификатът е във формат PEM/DER.

1. Влезте в Web Config и след това изберете раздела **Network Security**.След това изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate**, или **IEEE802.1X** > **Client Certificate**.

   Каквото и да изберете, Вие можете да получите същия сертификат и да го използвате общо.

2. Щракнете върху **Generate** на **CSR**.

   Отваря се страница за създаване на CSR.

3. Въведете стойност за всеки елемент.

   Забележка:
   Наличната дължина на ключа и съкращенията варират според сертифициращия орган.Създайте заявка съгласно правилата на всеки сертифициращ орган.

4. Щракнете върху **OK**.

   Показва се съобщение за завършване.

5. Изберете раздел **Network Security**.След това изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate**, или **IEEE802.1X** > **Client Certificate**.

6. Щракнете върху един от бутоните за изтегляне на **CSR** в съответствие с определения формат от всеки сертифициращ орган, за да изтеглите CSR на компютър.

> ***Важно:***
>
> *Не генерирайте CSR отново.Ако направите това, възможно е да не можете да импортирате издаден CA-signed Certificate.*

7. Изпратете CSR до сертифициращ орган и получете CA-signed Certificate.

   Следвайте правилата на всеки сертифициращ орган относно метода и формата на изпращане.

8. Запазете издадения CA-signed Certificate на компютър, свързан към скенера.

   Получаването на CA-signed Certificate е завършено, когато запазите сертификата в определена дестинация.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Елементи за настройка на CSR

Елементи	Настройки и обяснение
Key Length	Изберете дължина на ключ за CSR.
Common Name	Можете да въвеждате между 1 и 128 знака. Ако това е IP адрес, той трябва да бъде статичен IP адрес. Можете да въвеждате 1 до 5 IPv4 адреси, IPv6 адреси, имена на хостове, FQDN, като ги разделяте със запетаи. Първият елемент се съхранява в общото име, а другите елементи се съхраняват в полето за псевдоним на темата на сертификата. Пример: IP адрес на скенера: 192.0.2.123, име на скенера: EPSONA1B2C3 Common Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organization/ Organizational Unit/ Locality/ State/Province	Можете да въвеждате между 0 и 64 знака в ASCII (0x20 – 0x7E). Можете да разделите разграничени имена със запетаи.
Country	Въведете код на държавата в двуцифрен номер, посочен от ISO-3166.
Sender's Email Address	Можете да въведете имейл адреса на подателя за настройката на сървъра за електронна поща. Въведете същия имейл адрес като **Sender's Email Address** за раздела **Network** > **Email Server** > **Basic**.

Импортиране на подписан от сертифициращ орган сертификат

Импортирайте получения CA-signed Certificate в скенера.

Важно:

❏ *Уверете се, че датата и часът на скенера са правилно зададени. Възможно е сертификатът да е невалиден.*

❏ *Ако получите сертификат чрез CSR, създаден от Web Config, Вие можете да импортирате сертификат еднократно.*

1. Влезте в Web Config, след което изберете раздел **Network Security**. След това изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate**, или **IEEE802.1X** > **Client Certificate**.

2. Щракнете върху **Import**

   Отваря се страница за импортиране на сертификат.

3. Въведете стойност за всеки елемент. Задайте **CA Certificate 1** и **CA Certificate 2**, когато потвърждавате пътя на сертификата в уеббраузъра, който има достъп до скенера.

   В зависимост от това къде сте създали CSR и файловия формат на сертификата, необходимите настройки може да варират. Въведете стойности в необходимите елементи в съответствие със следното.

   ❏ Сертификат с PEM/DER формат, получен от Web Config

   ❏ **Private Key**: не конфигурирайте, защото скенерът съдържа личен ключ.

   ❏ **Password**: не конфигурирайте.

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

   ❏ Сертификат с PEM/DER формат, получен от компютър

   ❏ **Private Key**: трябва да зададете.

   ❏ **Password**: не конфигурирайте.

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

   ❏ Сертификат с PKCS#12 формат, получен от компютър

   ❏ **Private Key**: не конфигурирайте.

   ❏ **Password**: опционално

   ❏ **CA Certificate 1**/**CA Certificate 2**: не конфигурирайте.

4. Щракнете върху **OK**.

   Извежда се съобщение за завършване.

Забележка:
*Щракнете върху **Confirm**, за да потвърдите информацията за сертификата.*

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Подписан от сертифициращ орган сертификат импортиране на елементи за настройки

Елементи	Настройки и обяснение
Server Certificate илиClient Certificate	Изберете формат на сертификата. За SSL/TLS връзка се извежда Server Certificate. За IPsec/IP филтриране или IEEE 802.1X се извежда Client Certificate.
Private Key	Ако получите сертификат от формат PEM/DER с помощта на създаден от компютър CSR, посочете файл на личен ключ, който съвпада със сертификат.
Password	Ако форматът на файла е **Certificate with Private Key (PKCS#12)**, въведете паролата за шифроване на личния ключ, която е зададена при получаване на сертификата.
CA Certificate 1	Ако форматът на Вашия сертификат е **Certificate (PEM/DER)**, импортирайте сертификат от орган за сертификати, който издава CA-signed Certificate, използван като сертификат на сървър. Ако е необходимо, посочете файл.
CA Certificate 2	Ако форматът на Вашия сертификат е **Certificate (PEM/DER)**, импортирайте сертификат от орган за сертификати, който издава CA Certificate 1. Ако е необходимо, посочете файл.

Изтриване на сертификат, подписан от сертифициращ орган

Можете да изтриете импортиран сертификат, когато сертификатът е изтекъл или когато вече не е необходима криптирана връзка.

Важно:

Ако получите сертификат с помощта на CSR, създадена от Web Config, не можете да импортирате изтрит сертификат отново. В този случай създайте CSR и получете сертификат отново.

1. Влезте в Web Config и след това изберете раздела **Network Security**. След това изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.
2. Щракнете върху **Delete**.
3. Потвърдете, че искате да изтриете сертификата в показаното съобщение.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Актуализиране на самоподписан сертификат

Тъй като Self-signed Certificate се издава от скенера, Вие можете да го актуализирате, когато изтече или при промяна на описаното съдържание.

1. Влезте в Web Config и изберете **Network Security** tab > **SSL/TLS** > **Certificate**.
2. Щракнете върху **Update**.

3. Въведете **Common Name**.

   Можете да въвеждате до 5 IPv4 адреса, IPv6 адреса, имена на хостове, FQDN между 1 и 128 знака и да ги разделяте със запетаи. Първият параметър се съхранява в общото име, а другите елементи се съхраняват в полето за псевдоним на темата на сертификата.

   Пример:

   IP адрес на скенера: 192.0.2.123, име на скенера: EPSONA1B2C3

   Общо име: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Посочете период на валидност за сертификата.

5. Щракнете върху **Next**.

   Извежда се съобщение за потвърждение.

6. Щракнете върху **OK**.

   Скенерът е актуализиран.

Забележка:
*Можете да проверите информацията за сертификата от раздела **Network Security** > **SSL/TLS** > **Certificate** > **Self-signed Certificate** и щракнете върху **Confirm**.*

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Конфигуриране на CA Certificate

Когато зададете CA Certificate, Вие можете да удостоверите пътя до сертификата от сертифициращ орган на сървъра, до който има достъп скенерът. Това може да предотврати въплъщаване.

Можете да получите CA Certificate от сертифициращия орган, където е издаден CA-signed Certificate.

Импортиране на CA Certificate

Импортирайте CA Certificate в скенера.

1. Влезте в Web Config, след което изберете раздел **Network Security** > **CA Certificate**.

2. Щракнете върху **Import**.

3. Посочете CA Certificate, който искате да импортирате.

4. Щракнете върху **OK**.

Когато импортирането завърши, Вие ще бъдете върнати на екрана **CA Certificate** и ще се изведе импортираният CA Certificate.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Изтриване на CA Certificate

Можете да изтриете импортирания CA Certificate.

1. Влезте в Web Config, след което изберете раздел **Network Security** > **CA Certificate**.
2. Щракнете върху **Delete** до CA Certificate, който искате да изтриете.
3. Потвърдете че искате да изтриете сертификата в изведеното съобщение.
4. Щракнете върху **Reboot Network**, след което проверете дали изтрият сертификат на сертифициращ орган не е посочен в актуализирания екран.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

SSL/TLS комуникация със скенера

Когато се настрои сертификат на сървъра чрез SSL/TLS (Слой със защитени сокети/Защита на транспортния слой) комуникация към скенера, можете да криптирате пътя на комуникация между компютрите. Направете това, ако искате да предотвратите дистанционен и неупълномощен достъп.

Конфигуриране на основни настройки на SSL/TLS

Ако скенерът поддържа грешката на HTTPS сървъра, Вие можете да използвате SSL/TLS комуникация за шифроване на съобщения. Можете да конфигурирате и управлявате скенера с помощта на Web Config, като същевременно гарантирате сигурност.

Конфигуриране на сила на шифроване и функция за пренасочване.

1. Влезте в Web Config и изберете раздел **Network Security** > **SSL/TLS** > **Basic**.
2. Изберете стойност за всеки елемент.
   - ❏ Encryption Strength

     Изберете нивото на сила на шифроване.
   - ❏ Redirect HTTP to HTTPS

     При влизане в HTTP, пренасочете към HTTPS.
3. Щракнете върху **Next**.

   Извежда се съобщение за потвърждение.
4. Щракнете върху **OK**.

   Скенерът е актуализиран.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Конфигуриране на сертификат на сървъра за скенера

1. Влезте в Web Config и изберете раздел **Network Security** > **SSL/TLS** > **Certificate**.
2. Посочете сертификат за използване на **Server Certificate**.
   - ❏ Self-signed Certificate

     От скенера се генерира самоподписан сертификат. Изберете го, ако не сте получили подписан от сертифициращ орган сертификат.
   - ❏ CA-signed Certificate

     Ако получите и импортирате подписан от сертифициращ орган сертификат предварително, можете да го посочите.
3. Щракнете върху **Next**.

   Извежда се съобщение за потвърждение.
4. Щракнете върху **OK**.

   Скенерът е актуализиран.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40
➡ "Конфигуриране на CA-signed Certificate" на страница 99
➡ "Конфигуриране на CA Certificate" на страница 103

Криптирана комуникация с IPsec/IP филтриране

Относно IPsec/IP Filtering

Можете да филтрирате трафика на базата на IP адреси, услуги и порт с помощта на функцията за IPsec/IP филтриране.Чрез комбиниране на филтрирането можете да конфигурирате скенера да приема или да блокира определени клиенти и определени данни.Освен това можете да подобрите нивото на защита, като използвате IPsec.

Забележка:
Компютри, които работят под Windows Vista или по-нова версия или под Windows Server 2008 или по-нова версия, поддържат IPsec.

Конфигуриране на политика по подразбиране

За да филтрирате трафика, конфигурирайте политиката по подразбиране.Политиката по подразбиране се прилага за всеки потребител или група, които се свързват към скенера.За по-фин контрол върху потребители и групи от потребители конфигурирайте групови политики.

1. Влезте в Web Config, след което изберете раздела **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Въведете стойност за всеки елемент.

3. Щракнете върху **Next**.

   Показва се съобщение за потвърждение.

4. Щракнете върху **OK**.

   Скенерът се актуализира.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Елементи за настройка на Default Policy

Default Policy

Елементи	Настройки и обяснение
IPsec/IP Filtering	Можете да активирате или дезактивирате функция за IPsec/IP филтриране.

❏ **Access Control**

Конфигурирайте метод за контрол за трафик на IP пакети.

Елементи	Настройки и обяснение
Permit Access	Изберете това за разрешаване на преминаване на конфигурирани IP пакети.
Refuse Access	Изберете това за отказ на преминаване на конфигурирани IP пакети.
IPsec	Изберете това за разрешаване на конфигурирани IPsec пакети за преминаване.

❏ **IKE Version**

Изберете **IKEv1** или **IKEv2** за **IKE Version**. Изберете един от тях спрямо устройството, към което е свързан скенерът.

❏ IKEv1

Следните елементи се извеждат, когато изберете **IKEv1** за **IKE Version**.

Елементи	Настройки и обяснение
Authentication Method	За да изберете **Certificate**, Вие трябва предварително да получите и импортирате подписан от сертифициращ орган сертификат.
Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, въведете предварително споделен ключ между 1 и 127 знака.
Confirm Pre-Shared Key	Въведете конфигурирания ключ за потвърждение.

❏ IKEv2

Следните елементи се извеждат, когато изберете **IKEv2** за **IKE Version**.

Елементи		Настройки и обяснение
Local	Authentication Method	За да изберете **Certificate**, Вие трябва предварително да получите и импортирате подписан от сертифициращ орган сертификат.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете типа ИД за скенера.
	ID	Въведете ИД на скенера, който съвпада с типа ИД. Не можете да използвате „@“, „#“, и „=“ за първия знак. **Distinguished Name**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „=“. **IP Address**: въведете IPv4 или IPv6 формат. **FQDN**: въведете комбинация между 1 и 255 знака, включващи A – Z, a – z, 0 – 9, „-“, и точка (.). **Email Address**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „@“. **Key ID**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете конфигурирания ключ за потвърждение.

Елементи		Настройки и обяснение
Remote	Authentication Method	За да изберете **Certificate**, Вие трябва предварително да получите и импортирате подписан от сертифициращ орган сертификат.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете типа ИД за устройството, което искате да удостоверите.
	ID	Въведете ИД на скенера, който съвпада с типа ИД. Не можете да използвате „@“, „#“, и „=“ за първия знак. **Distinguished Name**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „=“. **IP Address**: въведете IPv4 или IPv6 формат. **FQDN**: въведете комбинация между 1 и 255 знака, включващи A – Z, a – z, 0 – 9, „-“, и точка (.). **Email Address**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „@“. **Key ID**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете конфигурирания ключ за потвърждение.

❏ Encapsulation

Ако изберете **IPsec** за **Access Control**, Вие трябва да конфигурирате режим на капсулиране.

Елементи	Настройки и обяснение
Transport Mode	Ако използвате скенера в една и съща LAN мрежа, изберете това. IP пакети от слой 4 или по-нов се шифроват.
Tunnel Mode	Ако използвате скенера в мрежа, която може да се свързва с интернет, като IPsec-VPN, изберете тази опция. Заглавната част и данните на IP пакетите са шифровани. **Remote Gateway(Tunnel Mode)**: ако изберете **Tunnel Mode** за **Encapsulation**, въведете адрес на шлюз между 1 и 39 знака.

❏ Security Protocol

Ако изберете **IPsec** за **Access Control**, изберете опция.

Елементи	Настройки и обяснение
ESP	Изберете тази опция, за да осигурите целостта на удостоверяване и данни и за шифроване на данни.
AH	Изберете тази опция, за да осигурите целостта на удостоверяване и данни. Дори ако шифроването на данни е забранено, Вие можете да използвате IPsec.

❏ **Algorithm Settings**

Препоръчително е да изберете **Any** за всички настройки или да изберете елемент, различен от **Any**, за всяка настройка. Ако изберете **Any** за някои от настройките и изберете елемент, различен от **Any**, за другите настройки, устройството може да не комуникира в зависимост от другото устройство, което искате да удостоверите.

Елементи		Настройки и обяснение
IKE	Encryption	Изберете алгоритъма на шифроване за IKE. Елементите са различни в зависимост от версията на IKE.
	Authentication	Изберете алгоритъма за удостоверяване за IKE.
	Key Exchange	Изберете алгоритъма за обмен на ключове за IKE. Елементите са различни в зависимост от версията на IKE.
ESP	Encryption	Изберете алгоритъма на шифроване за ESP. Това е налично, когато сте избрали **ESP** за **Security Protocol**.
	Authentication	Изберете алгоритъма за удостоверяване за ESP. Това е налично, когато сте избрали **ESP** за **Security Protocol**.
AH	Authentication	Изберете алгоритъма на шифроване за AH. Това е налично, когато сте избрали **AH** за **Security Protocol**.

Конфигуриране на групова политика

Групова политика представлява едно или повече правила, приложени към потребител или група потребители.Скенерът контролира IP пакетите, които съответстват на конфигурирани политики.IP пакетите се удостоверяват по реда на групова политика 1 до 10, след това политика по подразбиране.

1. Влезте в Web Config, след което изберете раздела **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Щракнете върху номериран раздел, който искате да конфигурирате.
3. Въведете стойност за всеки елемент.
4. Щракнете върху **Next**.

   Показва се съобщение за потвърждение.
5. Щракнете върху **OK**.

   Скенерът се актуализира.

Елементи за настройка на Group Policy

Елементи	Настройки и обяснение
Enable this Group Policy	Можете да активирате или дезактивирате групова политика.

Access Control

Конфигурирайте метод за контрол за трафик на IP пакети.

Елементи	Настройки и обяснение
Permit Access	Изберете това за разрешаване на преминаване на конфигурирани IP пакети.
Refuse Access	Изберете това за отказ на преминаване на конфигурирани IP пакети.
IPsec	Изберете това за разрешаване на конфигурирани IPsec пакети за преминаване.

Local Address (Scanner)

Изберете IPv4 адрес или IPv6 адрес, който съответства на Вашата мрежова среда. Ако IP адресът е автоматично назначен, Вие можете да изберете **Use auto-obtained IPv4 address**.

Забележка:
При автоматично назначаване на IPv6 адрес, връзката може да е недостъпна. Конфигурирайте IPv6 адрес.

Remote Address(Host)

Въведете IP адреса на устройството за управление на достъпа. IP адресът трябва да бъде с 43 знака или по-малко. Ако не въведете IP адрес, всички адреси се контролират.

Забележка:
При автоматично назначаване на IP адрес (напр. назначен от DHCP), връзката може да е недостъпна. Конфигурирайте статичен IP адрес.

Method of Choosing Port

Изберете метод, за да посочите портове.

❏ Service Name

Ако изберете **Service Name** за **Method of Choosing Port**, изберете опция.

❏ Transport Protocol

Ако изберете **Port Number** за **Method of Choosing Port**, Вие трябва да конфигурирате режим на капсулиране.

Елементи	Настройки и обяснение
Any Protocol	Изберете това за управление на всички типове протоколи.
TCP	Изберете това за управление на данните за уникаст.
UDP	Изберете това за управление на данните за излъчване и мултикаст.
ICMPv4	Изберете това за управление на ping команда.

❏ Local Port

Ако изберете **Port Number** за **Method of Choosing Port** и ако изберете **TCP** или **UDP** за **Transport Protocol**, въведете номера на портове за управление на получаването на пакети, като ги разделяте със запетаи. Можете да въвеждате най-много 10 номера на портове.

Пример: 20,80,119,5220

Ако не въведете номер на порт, всички портове се контролират.

❏ Remote Port

Ако изберете **Port Number** за **Method of Choosing Port** и ако изберете **TCP** или **UDP** за **Transport Protocol**, въведете номерата на портове за управление на изпращането на пакети, като ги разделяте със запетаи. Можете да въвеждате най-много 10 номера на портове.

Пример: 25,80,143,5220

Ако не въведете номер на порт, всички портове се контролират.

IKE Version

Изберете **IKEv1** или **IKEv2** за **IKE Version**. Изберете един от тях спрямо устройството, към което е свързан скенерът.

❏ IKEv1

Следните елементи се извеждат, когато изберете **IKEv1** за **IKE Version**.

Елементи	Настройки и обяснение
Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опция. Използваният сертификат е общ с политика по подразбиране.
Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, въведете предварително споделен ключ между 1 и 127 знака.
Confirm Pre-Shared Key	Въведете конфигурирания ключ за потвърждение.

❏ IKEv2

Следните елементи се извеждат, когато изберете **IKEv2** за **IKE Version**.

Елементи		Настройки и обяснение
Local	Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опция. Използваният сертификат е общ с политика по подразбиране.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете типа ИД за скенера.
	ID	Въведете ИД на скенера, който съвпада с типа ИД. Не можете да използвате „@“, „#“, и „=“ за първия знак. **Distinguished Name**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „=“. **IP Address**: въведете IPv4 или IPv6 формат. **FQDN**: въведете комбинация между 1 и 255 знака, включващи A – Z, a – z, 0 – 9, „-“, и точка (.). **Email Address**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „@“. **Key ID**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете конфигурирания ключ за потвърждение.
Remote	Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опция. Използваният сертификат е общ с политика по подразбиране.
	ID Type	Ако изберете **Pre-Shared Key** за **Authentication Method**, изберете типа ИД за устройството, което искате да удостоверите.
	ID	Въведете ИД на скенера, който съвпада с типа ИД. Не можете да използвате „@“, „#“, и „=“ за първия знак. **Distinguished Name**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „=“. **IP Address**: въведете IPv4 или IPv6 формат. **FQDN**: въведете комбинация между 1 и 255 знака, включващи A – Z, a – z, 0 – 9, „-“, и точка (.). **Email Address**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака. Трябва да включите „@“. **Key ID**: въведете 1 до 255 1-байтови ASCII (0x20 до 0x7E) знака.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете конфигурирания ключ за потвърждение.

Encapsulation

Ако изберете **IPsec** за **Access Control**, Вие трябва да конфигурирате режим на капсулиране.

Елементи	Настройки и обяснение
Transport Mode	Ако използвате скенера в една и съща LAN мрежа, изберете това. IP пакети от слой 4 или по-нов се шифроват.
Tunnel Mode	Ако използвате скенера в мрежа, която може да се свързва с интернет, като IPsec-VPN, изберете тази опция. Заглавната част и данните на IP пакетите са шифровани. **Remote Gateway(Tunnel Mode)**: ако изберете **Tunnel Mode** за **Encapsulation**, въведете адрес на шлюз между 1 и 39 знака.

Security Protocol

Ако изберете **IPsec** за **Access Control**, изберете опция.

Елементи	Настройки и обяснение
ESP	Изберете тази опция, за да осигурите целостта на удостоверяване и данни и за шифроване на данни.
AH	Изберете тази опция, за да осигурите целостта на удостоверяване и данни. Дори ако шифроването на данни е забранено, Вие можете да използвате IPsec.

Algorithm Settings

Препоръчително е да изберете **Any** за всички настройки или да изберете елемент, различен от **Any**, за всяка настройка. Ако изберете **Any** за някои от настройките и изберете елемент, различен от **Any**, за другите настройки, устройството може да не комуникира в зависимост от другото устройство, което искате да удостоверите.

Елементи		Настройки и обяснение
IKE	Encryption	Изберете алгоритъма на шифроване за IKE. Елементите са различни в зависимост от версията на IKE.
	Authentication	Изберете алгоритъма за удостоверяване за IKE.
	Key Exchange	Изберете алгоритъма за обмен на ключове за IKE. Елементите са различни в зависимост от версията на IKE.
ESP	Encryption	Изберете алгоритъма на шифроване за ESP. Това е налично, когато сте избрали **ESP** за **Security Protocol**.
	Authentication	Изберете алгоритъма за удостоверяване за ESP. Това е налично, когато сте избрали **ESP** за **Security Protocol**.
AH	Authentication	Изберете алгоритъма на шифроване за AH. Това е налично, когато сте избрали **AH** за **Security Protocol**.

Комбинация от Local Address (Scanner) и Remote Address(Host) на Group Policy

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

Настройка на Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Празен	✓	✓	✓

*1 Ако **IPsec** е избрано за **Access Control**, не можете да определяте в дължината на префикса.

*2 Ако **IPsec** е избрано за **Access Control**, можете да изберете локален адрес за връзката (fe80::), но груповата политика ще бъде деактивирана.

*3 Освен локални за връзката IPv6 адреси.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Справки за име на услуга на групова политика

Забележка:
Извеждат се недостъпни услуги, но не се избират.

Име на услуга	Тип протокол	Номер на локален порт	Номер на отдалечен порт	Контролирани функции
Any	–	–	–	Всички услуги
ENPC	UDP	3289	Всеки порт	Търсене на скенер от приложения като Epson Device Admin и драйвера на скенера
SNMP	UDP	161	Всеки порт	Получаване и конфигуриране на MIB от приложения като Epson Device Admin и драйвера на скенера Epson
WSD	TCP	Всеки порт	5357	Контролиране на WSD
WS-Discovery	UDP	3702	Всеки порт	Търсене на WSD скенери
Network Scan	TCP	1865	Всеки порт	Препращане на сканираните данни от Document Capture Pro
Network Push Scan	TCP	Всеки порт	2968	Получаване на информация за задание за насочено сканиране от Document Capture Pro
Network Push Scan Discovery	UDP	2968	Всеки порт	Търсене на компютър от скенер
FTP Data (Remote)	TCP	Всеки порт	20	FTP клиент (препращане на сканирани данни) Това може да се контролира само на FTP сървър, който използва номер 20 на отдалечен порт.
FTP Control (Remote)	TCP	Всеки порт	21	FTP клиент (управление на препратени сканирани данни)

Име на услуга	Тип протокол	Номер на локален порт	Номер на отдалечен порт	Контролирани функции
CIFS (Remote)	TCP	Всеки порт	445	CIFS клиент (препращане на сканирани данни в папка)
NetBIOS Name Service (Remote)	UDP	Всеки порт	137	CIFS клиент (препращане на сканирани данни в папка)
NetBIOS Datagram Service (Remote)	UDP	Всеки порт	138	
NetBIOS Session Service (Remote)	TCP	Всеки порт	139	
HTTP (Local)	TCP	80	Всеки порт	HTTP(S) сървър (препращане на данни на Web Config и WSD)
HTTPS (Local)	TCP	443	Всеки порт	
HTTP (Remote)	TCP	Всеки порт	80	HTTP(S) клиент (актуализиране на фърмуера и коренния сертификат)
HTTPS (Remote)	TCP	Всеки порт	443	

Конфигуриране на примери на IPsec/IP Filtering

Получаване само на IPsec пакети

Този пример е само за конфигуриране на политика по подразбиране.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: въведете до 127 знака.

Group Policy: не конфигурирайте.

Получаване на данни за сканиране и настройки на скенер

Този пример позволява комуникация на данни за сканиране и конфигурация на скенера от указани услуги.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: поставете отметка в полето.

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

❏ **Remote Address(Host)**: IP адрес на клиент

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

❏ **Service Name**: поставете отметка в полето **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)** и **Network Scan**.

Получаване на достъп само от указан IP адрес

Този пример позволява достъп на указан IP адрес до скенера.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: поставете отметка в полето.

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

❏ **Remote Address(Host)**: IP адрес на клиент на администратор

Забележка:
Независимо от конфигурацията на политиката, клиентът ще може да получава достъп до и да конфигурира скенера.

Конфигуриране на сертификат за IPsec/IP филтриране

Конфигуриране на клиентски сертификат за IPsec/IP филтриране. Когато го зададете, можете да използвате сертификата като метод на удостоверяване за IPsec/IP филтриране. Ако желаете да конфигурирате органа за сертификати, отидете на **CA Certificate**.

1. Влезте в Web Config след което изберете раздел **Network Security** > **IPsec/IP Filtering** > **Client Certificate**.

2. Импортирайте сертификата в **Client Certificate**.

   Ако вече сте импортирали сертификат, публикуван от орган за сертификати, Вие можете да копирате сертификата и да го използвате при IPsec/IP филтриране. За да копирате, изберете сертификата от **Copy From**, след което щракнете върху **Copy**.

Още по темата

➡ “Как да стартирате Web Config в уеб браузър” на страница 40

➡ “Конфигуриране на CA-signed Certificate” на страница 99

➡ “Конфигуриране на CA Certificate” на страница 103

Свързване на скенера към мрежа IEEE802.1X

Конфигуриране на мрежа IEEE802.1X

Когато зададете IEEE802.1X на скенера, Вие можете да го използвате на мрежата, която е свързана към сървъра RADIUS, LAN превключвател с функция за удостоверяване или точка на достъп.

1. Влезте в Web Config, след което изберете раздела **Network Security** > **IEEE802.1X** > **Basic**.

2. Въведете стойност за всеки елемент.

   Ако искате да използвате скенера в Wi-Fi мрежа, щракнете върху **Wi-Fi Setup** и изберете или въведете SSID.

   Забележка:
   Можете да споделяте настройки между Ethernet и Wi-Fi.

3. Щракнете върху **Next**.

   Показва се съобщение за потвърждение.

4. Щракнете върху **OK**.

   Скенерът се актуализира.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Елементи за настройка на мрежа IEEE 802.1X

Елементи	Настройки и обяснение	
IEEE802.1X (Wired LAN)	Можете да активирате или дезактивирате настройките на страницата (**IEEE802.1X** > **Basic**) за IEEE802.1X (кабелна LAN).	
IEEE802.1X (Wi-Fi)	Извежда се състоянието на връзката IEEE802.1X (Wi-Fi).	
Connection Method	Извежда се методът на връзка на текуща мрежа.	
EAP Type	Изберете опция за метод на удостоверяване между скенера и сървъра RADIUS.	
	EAP-TLS	Вие трябва да получите и импортирате подписан от сертифициращ орган сертификат.
	PEAP-TLS	
	PEAP/MSCHAPv2	Трябва да конфигурирате парола.
	EAP-TTLS	
User ID	Конфигурирайте ИД за използване за удостоверяване на сървъра RADIUS. Въведете 1 до 128 1-байтови ASCII (0x20 до 0x7E) знака.	
Password	Конфигурирайте парола за удостоверяване на скенера. Въведете 1 до 128 1-байтови ASCII (0x20 до 0x7E) знака. Ако използвате Windows сървър като сървър RADIUS, можете да въвеждате до 127 знака.	
Confirm Password	Въведете паролата, която сте конфигурирали за потвърждение.	
Server ID	Можете да конфигурирате ИД на сървър за удостоверяване с определен RADIUS сървър. Приложение за удостоверяване потвърждава дали дадено ИД на сървър се съдържа в полето subject/subjectAltName на сертификат на сървър, който е изпратен от RADIUS сървър или не. Въведете 0 до 128 1-байтови ASCII (0x20 до 0x7E) знака.	

Елементи	Настройки и обяснение	
Certificate Validation (кабелна локална мрежа)	Ако искате да извършите **Certificate Validation** чрез **IEEE802.1X (Wired LAN)**, изберете **Enable**. Ако изберете Активиране, вижте съответната информация и импортирайте **CA Certificate**. Обърнете внимание, че Certificate Validation е винаги активирано в IEEE802.1X (Wi-Fi). Не забравяйте да импортирате CA Certificate.	
Anonymous Name	Ако изберете **PEAP-TLS** или **PEAP/MSCHAPv2** за **EAP Type**, Вие можете да конфигурирате анонимно име вместо ИД на потребител за фаза 1 на удостоверяване с PEAP. Въведете 0 до 128 1-байтови ASCII (0x20 до 0x7E) знака.	
Encryption Strength	Можете да изберете едно от следните неща.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Още по темата

➡ "Конфигуриране на CA Certificate" на страница 103

Конфигуриране на сертификат за IEEE 802.1X

Конфигурирайте клиентския сертификат за IEEE802.1X. Когато го зададете, можете да използвате **EAP-TLS** и **PEAP-TLS** като метод за удостоверяване на IEEE 802.1X. Ако желаете да конфигурирате сертификата на сертифициращия орган, отидете на **CA Certificate**.

1. Влезте в Web Config след което изберете раздел **Network Security** > **IEEE802.1X** > **Client Certificate**.
2. Въведете сертификат в **Client Certificate**.

   Ако вече сте импортирали сертификат, публикуван от орган за сертификати, Вие можете да копирате сертификата и да го използвате при IEEE802.1X. За да копирате, изберете сертификата от **Copy From**, след което щракнете върху **Copy**.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Решаване на проблеми за повишена защита

Възстановяване на настройките за сигурност

Когато установите силно защитена среда, например IPsec/IP филтриране, е възможно да не можете да комуникирате с устройствата поради неправилни настройки или проблеми с устройството или сървъра. В този случай възстановете настройките за сигурност, за да направите отново настройките за устройството или за да получите временен достъп.

Дезактивиране на функцията за сигурност чрез Web Config

Можете да дезактивирате IPsec/IP Filtering чрез Web Config.

1. Влезте в Web Config и изберете раздел **Network Security** > **IPsec/IP Filtering** > **Basic**.
2. Дезактивирайте **IPsec/IP Filtering**.

Проблеми при използване на функциите за мрежова сигурност

Забравен предварително споделен ключ

Повторно конфигуриране на предварително споделен ключ.

За да промените ключа, влезте в Web Config и изберете раздела **Network Security** > **IPsec/IP Filtering** > **Basic** > **Default Policy** или **Group Policy**.

Когато промените предварително споделения ключ, конфигурирайте го за компютри.

Още по темата

➡ “Как да стартирате Web Config в уеб браузър” на страница 40
➡ “Криптирана комуникация с IPsec/IP филтриране” на страница 105

Не може да комуникира с IPsec комуникация

Посочете алгоритъма, който скенерът или компютърът не поддържат.

Скенерът поддържа следните алгоритми. Проверка на настройките на компютъра.

Методи за защита	Алгоритми
IKE алгоритъм за криптиране	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE алгоритъм за удостоверяване	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE алгоритъм за размяна на ключове	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP алгоритъм за криптиране	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP алгоритъм за удостоверяване	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH алгоритъм за удостоверяване	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Възможно само за IKEv2

Още по темата

➡ “Криптирана комуникация с IPsec/IP филтриране” на страница 105

Не може да комуникира внезапно

IP адресът на скенера е променен или не може да се използва.

Когато IP адресът, регистриран в локалния адрес на Group Policy, е променен или не може да се използва, IPsec комуникация не може да се извършва. Дезактивирайте IPsec от контролния панел на скенера.

Ако DHCP е остарял, рестартирането или IPv6 адресът е остарял или не е получен, регистрираният за скенера IP адрес за раздела Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) може да не бъде намерен.

Използвайте статичен IP адрес.

IP адресът на компютъра е променен или не може да се използва.

Когато IP адресът, регистриран в дистанционния адрес на Group Policy, е променен или не може да се използва, IPsec комуникация не може да се извършва.

Дезактивирайте IPsec от контролния панел на скенера.

Ако DHCP е остарял, рестартирането или IPv6 адресът е остарял или не е получен, регистрираният за скенера IP адрес за раздела Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) може да не бъде намерен.

Използвайте статичен IP адрес.

Още по темата

➡ “Как да стартирате Web Config в уеб браузър” на страница 40

➡ “Криптирана комуникация с IPsec/IP филтриране” на страница 105

Не може да се установи връзка след конфигуриране на IPsec/IP филтриране

Настройките за IPsec/IP филтриране са грешни.

Забранете IPsec/IP филтриране от контролния панел на скенера.Свържете скенера и компютъра и отново конфигурирайте настройките за IPsec/IP филтриране.

Още по темата

➡ “Криптирана комуникация с IPsec/IP филтриране” на страница 105

Няма достъп до устройството след конфигуриране на IEEE 802.1X

Настройките на IEEE 802.1X са грешни.

Дезактивирайте IEEE 802.1X и Wi-Fi от контролния панел на скенера. Свържете скенера и компютъра и след това конфигурирайте отново IEEE 802.1X.

Още по темата

➡ "Конфигуриране на мрежа IEEE802.1X" на страница 116

Проблеми при използване на цифров сертификат

Не може да се импортира CA-signed Certificate

CA-signed Certificate и информацията относно CSR не съвпадат.

Ако на CA-signed Certificate и CSR няма еднаква информация, CSR не може да се импортира.Проверете следното:

❏ Опитвате ли се да импортирате сертификата към устройство, което няма същата информация?

Проверете информацията на CSR и след това импортирайте сертификата към устройство, което има същата информация.

❏ Презаписахте ли запазената в скенера CSR след изпращането ѝ на сертифициращ орган?

Получете сертификата, подписан от сертифициращ орган, отново с CSR.

CA-signed Certificate е повече от 5 KB.

Не можете да импортирате CA-signed Certificate, който е по-голям от 5 KB.

Паролата за импортиране на сертификата е грешна.

Въведете правилната парола.Ако забравите паролата си, не можете да импортирате сертификата.Повторно получаване на CA-signed Certificate.

Още по темата

➡ "Импортиране на подписан от сертифициращ орган сертификат" на страница 100

Не може да се актуализира самоподписан сертификат

Common Name не е въведено.

Трябва да е въведено **Common Name**.

Въведени са неподдържани знаци за Common Name.

Въведете между 1 и 128 знака във формат IPv4, IPv6, име на хост или FQDN в ASCII (0x20–0x7E).

Включени са запетая или интервал в използваното име.

Ако е въведена запетая, **Common Name** се разделя в тази точка.Ако е въведен само интервал преди или след запетая, възниква грешка.

Още по темата

➡ "Актуализиране на самоподписан сертификат" на страница 102

Не може да се създаде CSR

Common Name не е въведено.

Трябва да е въведено **Common Name**.

Въведени са неподдържани знаци за Common Name, Organization, Organizational Unit, Locality и State/Province.

Въведете знаци във формат IPv4, IPv6, име на хост или FQDN в ASCII (0x20–0x7E).

Включени са запетая или интервал в Common Name.

Ако е въведена запетая, **Common Name** се разделя в тази точка.Ако е въведен само интервал преди или след запетая, възниква грешка.

Още по темата

➡ "Получаване на сертификат, подписан от сертифициращ орган" на страница 99

Появява се предупреждение за цифров сертификат

Съобщения	Причина/Какво да се направи
Enter a Server Certificate.	**Причина:** Не сте избрали файл за импортиране. **Какво да се направи:** Изберете файл и щракнете върху **Import**.
CA Certificate 1 is not entered.	**Причина:** Сертификат на сертифициращ орган 1 не е въведен, а е въведен само сертификат на сертифициращ орган 2. **Какво да се направи:** Импортирайте първо сертификат на сертифициращ орган 1.
Invalid value below.	**Причина:** Неподдържани знаци се съдържат в пътя до файла и/или паролата. **Какво да се направи:** Уверете се, че знаците за елемента са въведени правилно.
Invalid date and time.	**Причина:** Не са зададени дата и час на скенера. **Какво да се направи:** Задайте дата и час с помощта на Web Config или EpsonNet Config.
Invalid password.	**Причина:** Зададената за сертификат на сертифициращ орган парола и въведената парола не съвпадат. **Какво да се направи:** Въведете правилната парола.

Съобщения	Причина/Какво да се направи
Invalid file.	**Причина:** Не импортирате файл със сертификат в X509 формат. **Какво да се направи:** Уверете се, че сте избрали правилния сертификат, изпратен от надежден сертифициращ орган.
	Причина: Импортираният файл е твърде голям. Максималният размер на файла е 5 KB. **Какво да се направи:** Ако сте избрали правилния файл, сертификатът може да е повреден или подправен.
	Причина: Веригата, съдържаща се в сертификата, е невалидна. **Какво да се направи:** За повече информация относно сертификата вижте уеб сайта на сертифициращия орган.
Cannot use the Server Certificates that include more than three CA certificates.	**Причина:** Файлът на сертификата в PKCS#12 формат съдържа повече от 3 сертификата на сертифициращ орган. **Какво да се направи:** Импортирайте всеки сертификат, като го конвертирате от PKCS#12 формат в PEM формат, или импортирайте файла със сертификата в PKCS#12 формат, който съдържа до 2 сертификата на сертифициращ орган.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Причина:** Сертификатът е изтекъл. **Какво да се направи:** ❏ Ако сертификатът е изтекъл, получете и импортирайте нов сертификат. ❏ Ако сертификатът не е изтекъл, се уверете, че датата и часът на скенера са настроени правилно.
Private key is required.	**Причина:** Няма сдвоен личен ключ със сертификата. **Какво да се направи:** ❏ Ако сертификатът е в PEM/DER формат и е получен от CSR с помощта на компютър, посочете файла с личен ключ. ❏ Ако сертификатът е в PKCS#12 формат и е получен от CSR с помощта на компютър, създайте файл, който съдържа личния ключ.
	Причина: Импортирали сте повторно PEM/DER сертификата, получен от CSR с помощта на Web Config. **Какво да се направи:** Ако сертификатът е в PEM/DER формат и е получен от CSR с помощта на Web Config, можете да го импортирате само веднъж.

Съобщения	Причина/Какво да се направи
Setup failed.	**Причина:** Конфигурацията не може да се завърши, тъй като комуникацията между скенера и компютъра е неуспешна или файлът не може да се прочете поради някакви грешки. **Какво да се направи:** След проверка на дадения файл и комуникацията, импортирайте файла отново.

Още по темата

➡ "Относно цифровото сертифициране" на страница 98

Изтриване на сертификат, подписан от сертифициращ орган, по погрешка

Няма резервно копие за сертификат, подписан от сертифициращ орган.

Ако имате резервно копие на файла, импортирайте сертификата отново.

Ако получите сертификат с помощта на CSR, създадена от Web Config, не можете да импортирате изтрит сертификат отново.Създайте CSR и получете нов сертификат.

Още по темата

➡ "Импортиране на подписан от сертифициращ орган сертификат" на страница 100
➡ "Изтриване на сертификат, подписан от сертифициращ орган" на страница 102

Употреба на Epson Open Platform

Общ преглед на Epson Open Platform

Epson Open Platform е платформа, която Ви позволява да използвате системи за удостоверяване с този скенер.

Може да се използва с Epson Print Admin (Система за удостоверяване на Epson) или със система за удостоверяване на трета страна. Можете да извличате регистри по устройство и потребител, да конфигурирате устройства, които могат да се използват от потребители и групи, да задавате ограничения за функции и т.н.

Ако свържете устройство за удостоверяване, можете също да извършвате удостоверяване на потребител с помощта на ИД карта.

Конфигуриране на Epson Open Platform

Активирайте Epson Open Platform, за да можете да използвате устройството от системата за удостоверяване.

1. Вземете ключ от специализирания уебсайт.

   Вижте ръководството на Epson Open Platform за подробности относно получаване на продуктовия ключ.

2. Отидете на Web Config, след което изберете раздел **Epson Open Platform** > **Product Key or License Key**.

3. Проверете и задайте всеки елемент.

   ❏ Serial Number

   Извежда се серийният номер на устройството.

   ❏ Epson Open Platform Version

   Изберете версията на Epson Open Platform. Съответната версия варира в зависимост от системата за удостоверяване.

   ❏ Product Key or License Key

   Въведете продуктовия ключ, който сте получили.

4. Щракнете върху **Next**.

   Извежда се екранът за потвърждение на настройките.

5. Щракнете върху **OK**.

   Настройките се прилагат към скенера.

   Забележка:
   Вие не можете да използвате Epson Print Admin Serverless, когато системата е синхронизирана с Epson Open Platform.

Валидиране на Epson Open Platform

Можете да проверите валидността на Epson Open Platform чрез един от следните методи.

❏ Web Config

Въведен е продуктов ключ в раздела **Epson Open Platform** > **Product Key or License Key** > **Product Key or License Key** и се извежда разделът **Epson Open Platform** > **Authentication System** от лявата страна на дървовидния изглед на менюто.

❏ Контролен панел на скенера

Проверете дали продуктовият ключ е изведен в **Настройки** > **Информация за устройството** > **Информация за Epson Open Platform**.

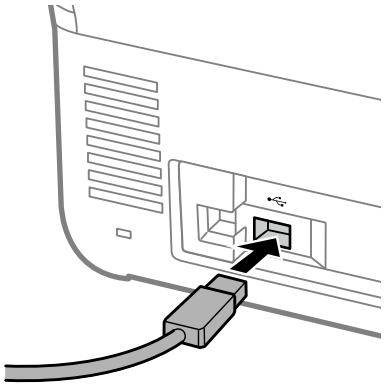
Монтиране на устройство за удостоверяване

Свързване на устройство за удостоверяване

Забележка:
Устройството за удостоверяване се използва, когато използвате система за удостоверяване.

> ***Важно:***
> *Когато свържете устройството за удостоверяване към няколко скенера, използвайте продукт със същия номер на модел.*

Свържете USB кабела на четеца на карти към USB порта за външен интерфейс на скенера.



Проверка на работата на устройството за удостоверяване

Можете да проверите състоянието на връзката и разпознаването на картата за удостоверяване за устройството за удостоверяване от контролния панел на скенера.

Информацията се извежда, когато изберете **Настройки** > **Информация за устройството** > **Състояние на удостоверяване на устройство**.

Потвърждение, че картата за удостоверяване е разпозната

Можете да проверите дали картите за удостоверяване могат да бъдат разпознати с помощта на Web Config.

1. Отидете на Web Config, след което изберете раздел **Device Management** > **Card Reader**.
2. Задръжте картата за удостоверяване над четеца на карти за удостоверяване.
3. Щракнете върху **Check**.
   Резултатът се извежда.

Отстраняване на неизправности от устройство за удостоверяване

Не може да се чете картата за удостоверяване

Проверете посоченото по-долу.

❏ Проверете дали устройството за удостоверяване е свързано към скенера правилно.

Свържете устройството за удостоверяване към USB порта за външен интерфейс на гърба на скенера.

❏ Проверете дали устройството за удостоверяване и картата за удостоверяване са сертифицирани.

Свържете се с Вашия търговец за информация относно поддържани устройства и карти за удостоверяване.

Поддръжка

Почистване на скенера отвън

Забършете всички петна от външната част на корпуса със суха кърпа или с кърпа, навлажнена с мек почистващ препарат и вода.

Важно:

- ❏ *Никога не използвайте алкохол, разредител или какъвто и да било корозивен препарат за почистване на скенера. Може да се получи деформация или обезцветяване.*
- ❏ *Не допускайте проникването на вода вътре в продукта. Това би могло да предизвика неизправност.*
- ❏ *Никога не отваряйте корпуса на скенера.*

1. Натиснете бутон ⏻, за да изключите скенера.
2. Изключете AC адаптера от скенера.
3. Почистете външната част на корпуса с кърпа, навлажнена с мек почистващ препарат и вода.

   Забележка:
   Почистете сензорния екран с помощта на мека и суха кърпа.

Почистване на скенера отвътре

След като използвате скенера за известно време, полепването на хартия или прах от стаята върху валяка или стъклената част отвътре на скенера може да предизвика проблеми с подаването на хартията или с качеството на изображението. Почиствайте вътрешността на скенера на всеки 5,000 сканирания.

Можете да проверите последния брой сканирания на контролния панел или в Epson Scan 2 Utility.

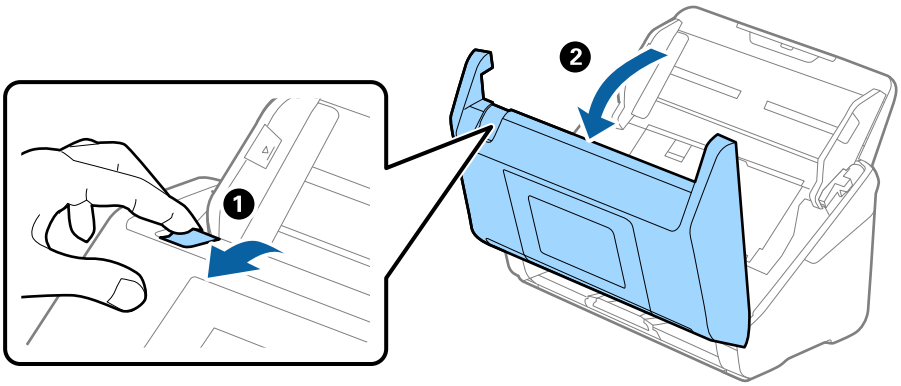
Ако повърхността е замърсена с труден за почистване материал, използвайте оригинален комплект за почистване на Epson за отстраняване на петната. Използвайте малко количество от почистващия препарат върху почистващата кърпа, за да отстраните петната.

Важно:

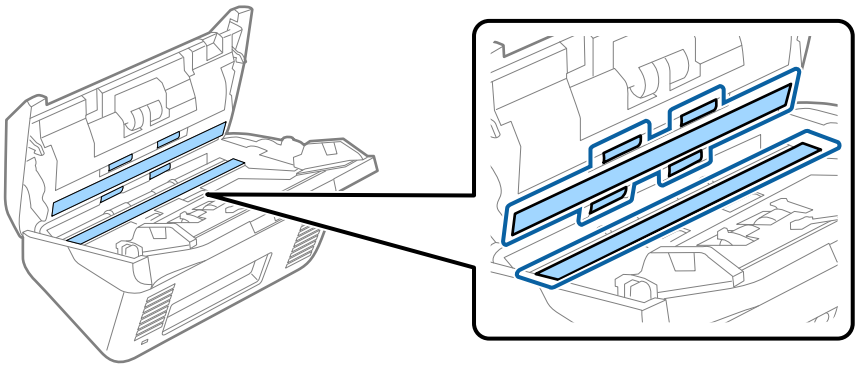
- ❏ *Никога не използвайте алкохол, разредител или какъвто и да било корозивен препарат за почистване на скенера. Може да се получи деформация или обезцветяване.*
- ❏ *Никога не пръскайте каквато и да е течност или смазочно средство върху скенера. При повреда на оборудването или електрическите вериги е възможно необичайно функциониране на скенера.*
- ❏ *Никога не отваряйте корпуса на скенера.*

1. Натиснете бутон ⏻, за да изключите скенера.
2. Изключете адаптера за променлив ток от скенера.

3. Дръпнете лоста и отворете капака на скенера.



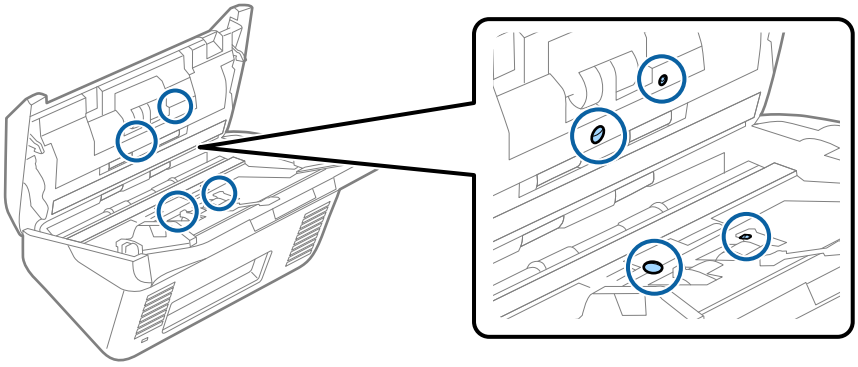
4. Избършете всички петна от пластмасовата ролка (4 места) и стъклената повърхност в долната вътрешна част на капака на скенера. Избършете с мека, неотделяща влакна кърпа, навлажнена с малко специален почистващ препарат или вода.



Важно:

- *Не използвайте прекомерна сила при почистването на стъклената повърхност.*
- *Не използвайте четка или твърд инструмент. Всякакви драскотини по стъклото може да окажат влияние върху качеството при сканиране.*
- *Не пръскайте почистващ препарат върху стъклената повърхност.*

5. Избършете всякакви петна от сензорите с памучен тампон.

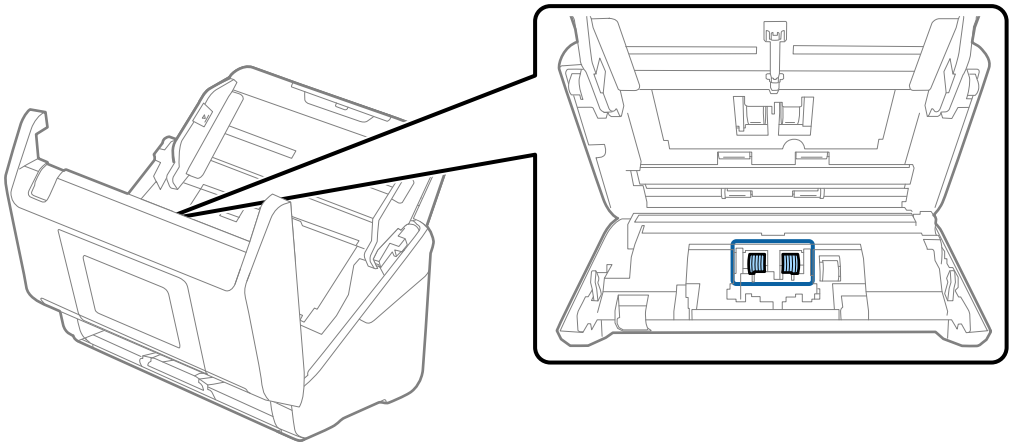


Важно:

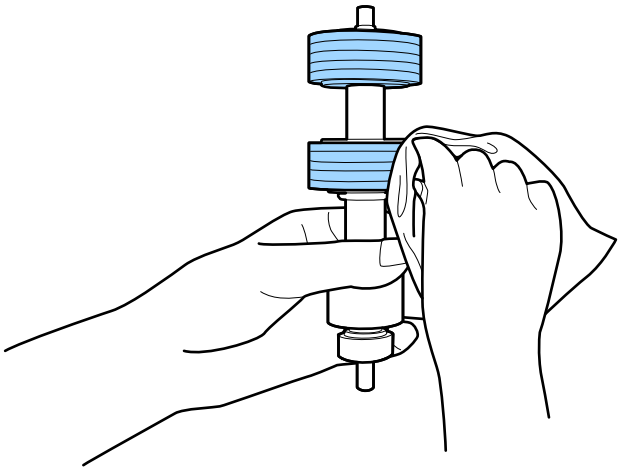
Не използвайте течност, като например почистващ препарат, върху памучен тампон.

6. Отворете капака, след което извадете разделителната ролка.

   За повече подробности вижте „Смяна на комплекта ролки“.



7. Избърсване на разделителната ролка. Избършете с мека, неотделяща влакна кърпа, навлажнена с малко специален почистващ препарат или вода.

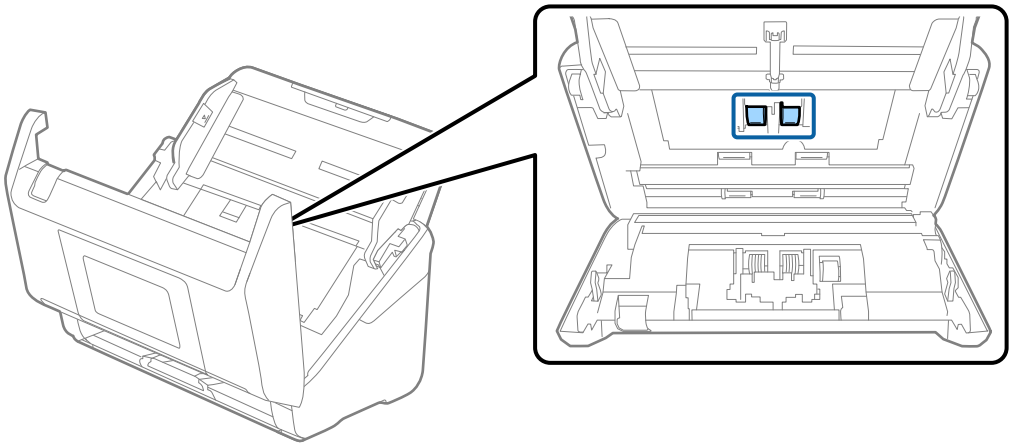


Важно:

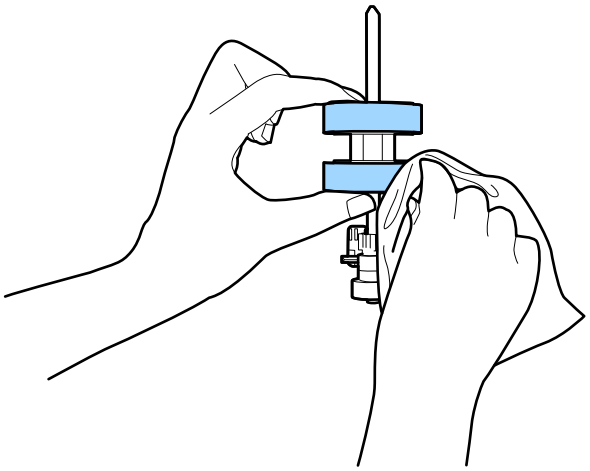
Използвайте само оригинален комплект за почистване на Epson или мека влажна кърпа за почистване на ролката. Използването на суха кърпа може да повреди повърхността на ролката.

8. Отворете капака, след което извадете листоподаващата ролка.

   За повече подробности вижте „Смяна на комплекта ролки“.



9. Избърсване на листоподаващата ролка. Избършете с мека, неотделяща влакна кърпа, навлажнена с малко специален почистващ препарат или вода.

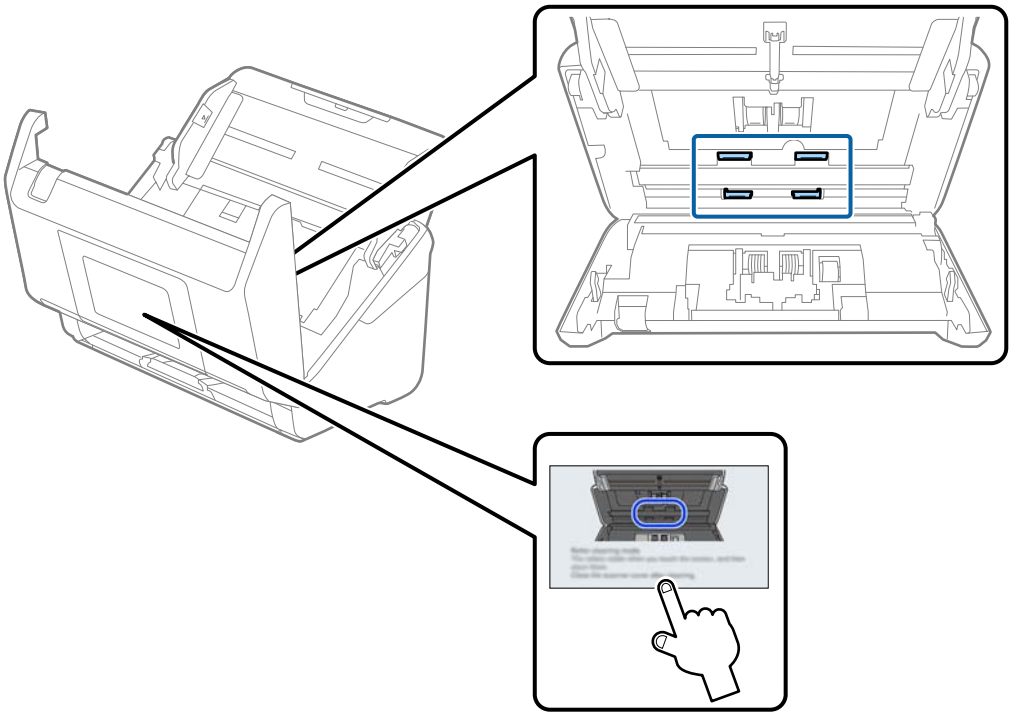


> ***Важно:***
>
> *Използвайте само оригинален комплект за почистване на Epson или мека влажна кърпа за почистване на ролката. Използването на суха кърпа може да повреди повърхността на ролката.*

10. Затворете капака на скенера.
11. Включете AC адаптера в мрежата, след което включете скенера.
12. Изберете **Техническо обсл. Скенера** от началния екран.
13. От екран **Техническо обсл. Скенера** изберете **Почистване на ролки**.
14. Дръпнете лоста, за да отворите капака на скенера.

    Скенерът влиза в режима на почистване на ролките.

15. Завъртете бавно ролките в долната част, като натиснете на произволно място върху LCD екрана. Избършете повърхността на ролките с помощта на оригинален комплект за почистване на Epson или мека кърпа, навлажнена във вода. Повторете тази процедура, докато почистите ролките.



> ***Внимание:***
>
> *Внимавайте ръцете или косата Ви да не бъдат захванати в механизма, докато работите с ролката. Това би могло да причини нараняване.*

16. Затворете капака на скенера.

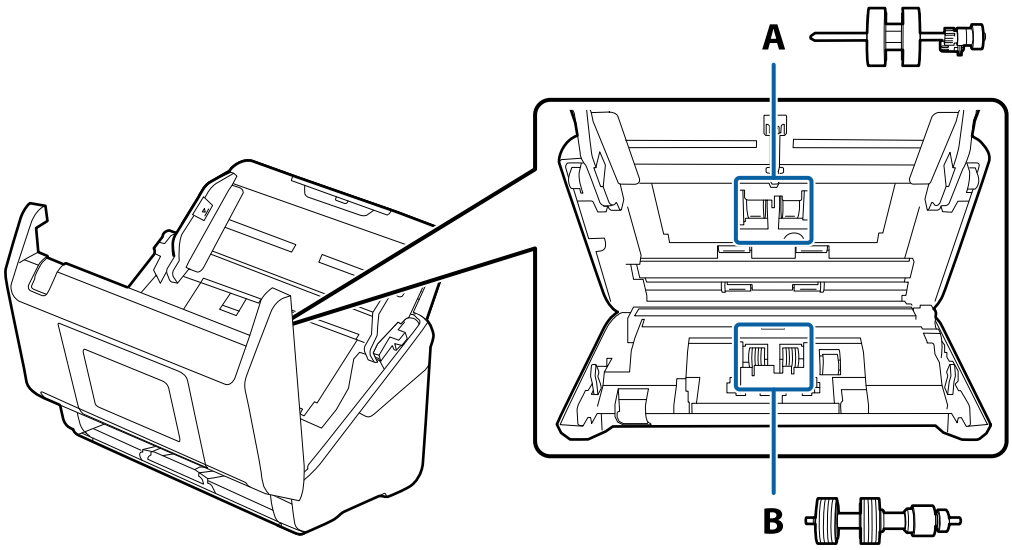
    Скенерът излиза от режима на почистване на ролките.

Още по темата

➡ “Смяна на комплекта ролки” на страница 137

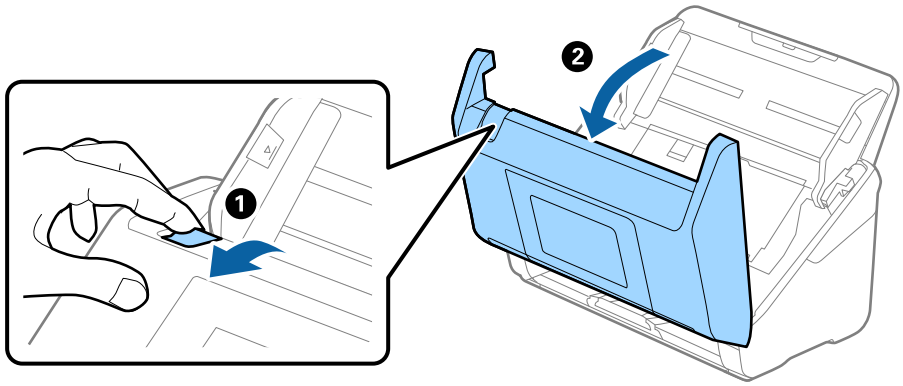
Смяна на комплекта ролки

Комплектът ролки (листоподаващата ролка и разделителната ролка) следва да бъде сменен, когато броят на сканиранията превиши жизнения цикъл на ролките. Когато на контролния панел или на екрана на компютъра се появи съобщение за смяна, следвайте стъпките по-долу, за да я извършите.

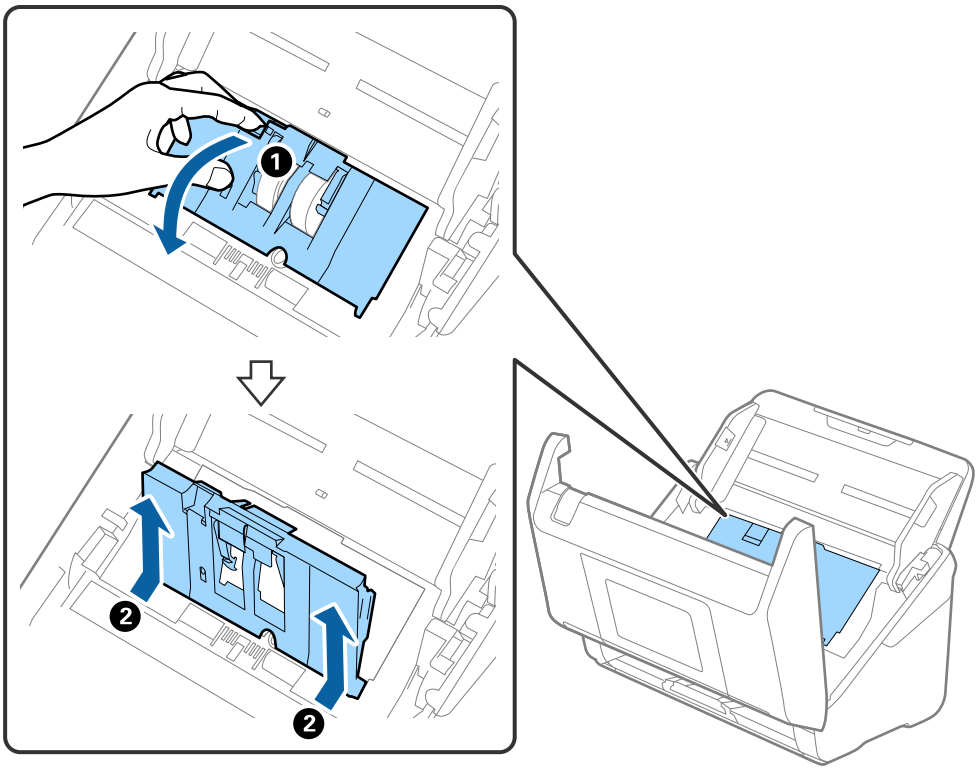


A: листоподаваща ролка, B: разделителна ролка

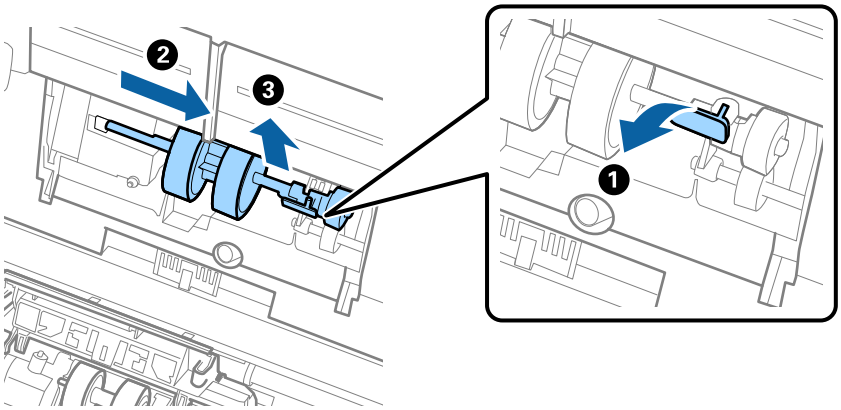
1. Натиснете бутон ⏻, за да изключите скенера.
2. Изключете AC адаптера от скенера.
3. Дръпнете лоста и отворете капака на скенера.



4. Отворете капака на повдигащата ролка, след което го плъзнете и извадете.



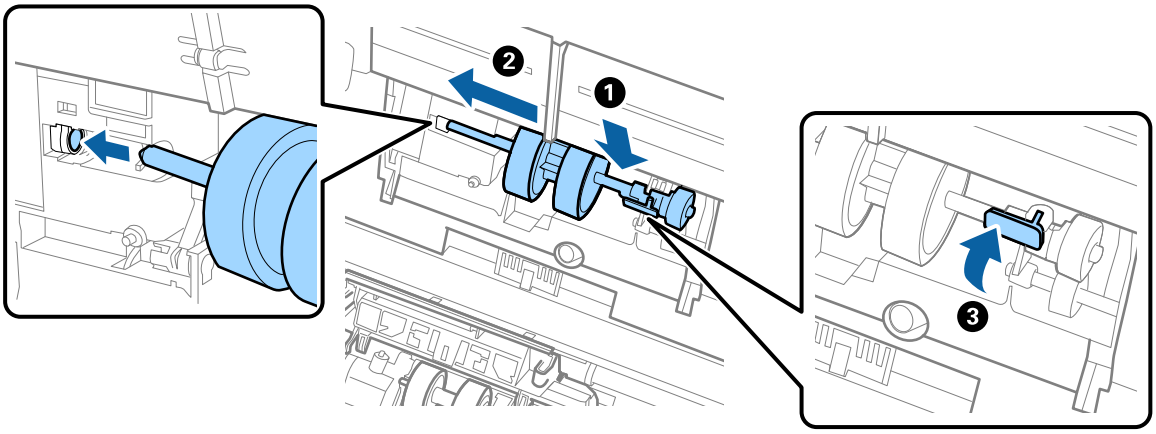
5. Дръпнете фиксиращия механизъм на вала на ролките, след което плъзнете и извадете монтираните повдигащи ролки.



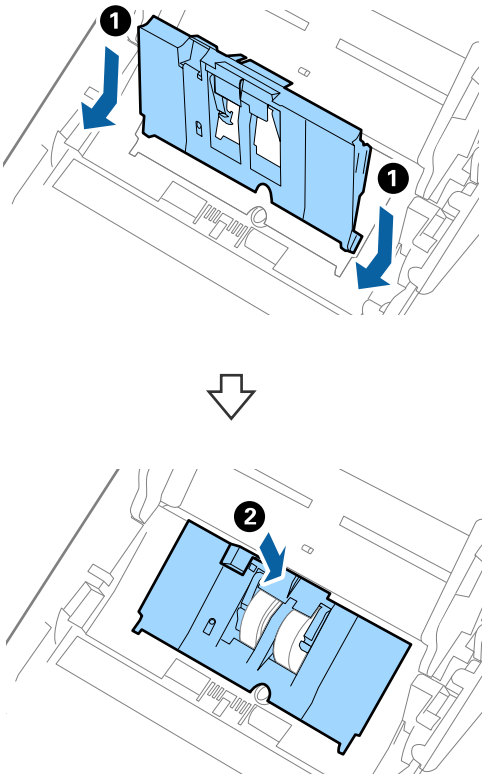
Важно:

Не издърпвайте със сила повдигащите ролки. Това би могло да повреди вътрешните части на скенера.

6. Като държите натиснат фиксиращия механизъм, плъзнете новата повдигаща ролка наляво и я вкарайте в отвора на скенера. Натиснете фиксиращия механизъм, за да я фиксирате.

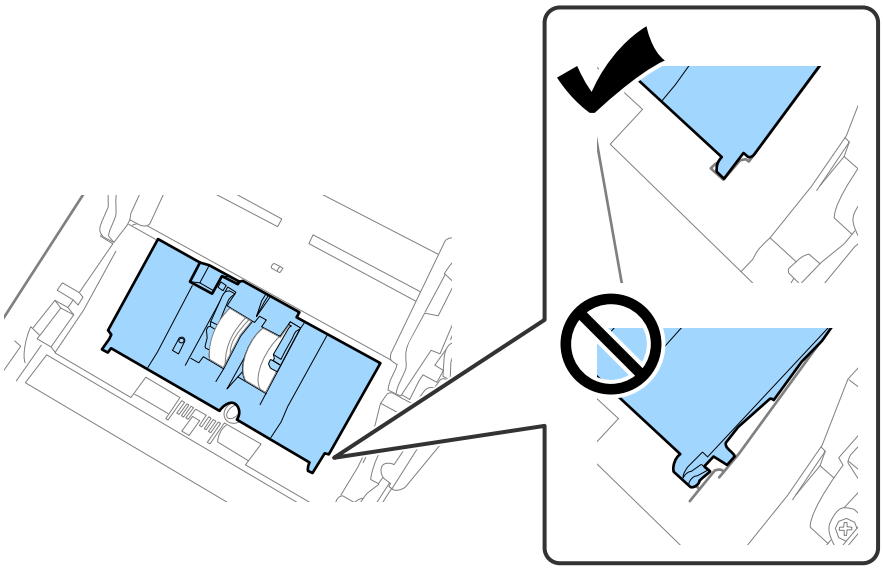


7. Поставете ръба на капака на повдигащата ролка в жлеба и го плъзнете. Затворете плътно капака.

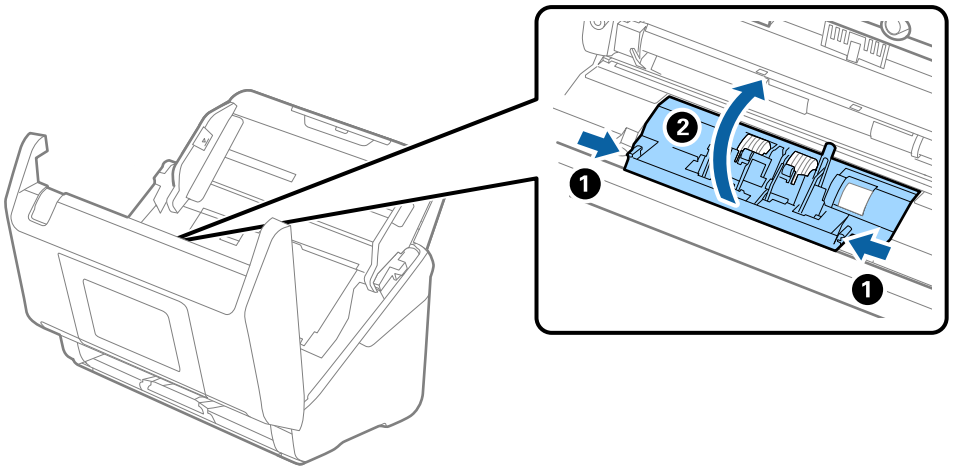


Важно:

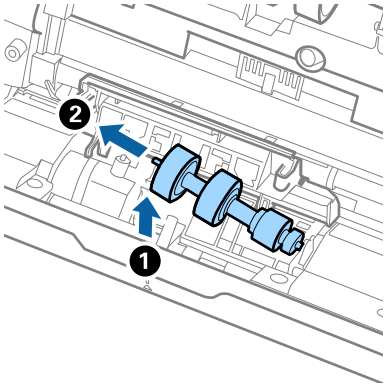
- ❏ *Уверете се, че капакът на повдигащата ролка е затворен правилно.*
- ❏ *Ако капакът се затваря трудно, проверете дали повдигащите ролки са монтирани правилно.*
- ❏ *Не монтирайте капака, докато е повдигнат.*



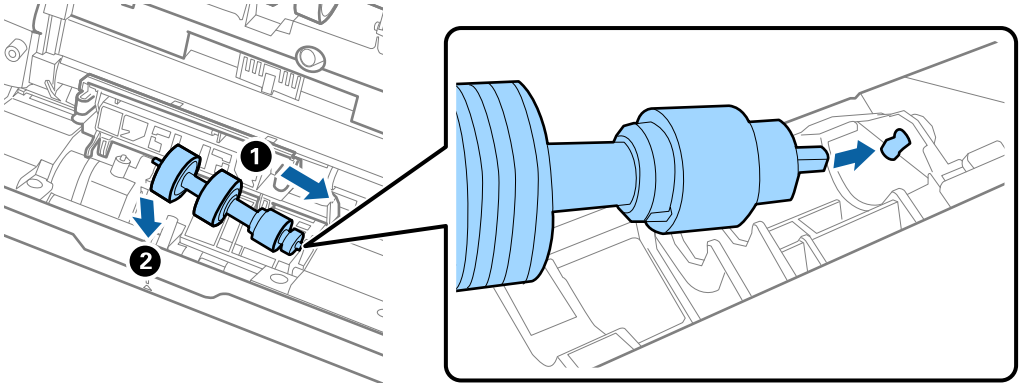
8. Натиснете захващащите куки от двете страни на капака на разделителната ролка, за да го отворите.



9. Повдигнете лявата страна на разделителната ролка, след което плъзнете и извадете монтираните разделителни ролки.



10. Вкарайте вала на новата разделителна ролка в отвора отдясно, след което я натиснете надолу.



11. Затворете капака на разделителната ролка.

> ***Важно:***
>
> *Ако затварянето на капака е затруднено, се уверете, че разделителните ролки са поставени правилно.*

12. Затворете капака на скенера.

13. Включете AC адаптера в мрежата, след което включете скенера.

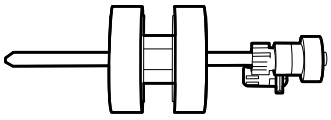
14. Нулирайте броя сканирания на контролния панел.

Забележка:
Изхвърлете повдигащата и разделителната ролка, като следвате правилата и разпоредбите на Вашите местни власти. Не ги разглобявайте.

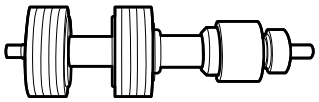
Кодове на комплекта ролки

Частите (листоподаваща ролка и разделителната ролка) трябва да бъдат сменени, когато броят на сканиранията превиши броя за сервизно обслужване. Можете да проверите последния брой сканирания на контролния панел или в Epson Scan 2 Utility.

A



B



A: листоподаваща ролка, B: разделителна ролка

Наименование на частта	Кодове	Жизнен цикъл
Комплект ролки 2	B12B819711 B12B819721 (само за Индия)	200,000*

* Този брой е бил постигнат чрез последователно сканиране при използване на оригинални хартии за тестване на Epson и служи като ориентир за цикъла на смяна. Цикълът на смяна може да варира в зависимост от различните типове хартия, като например хартия, която отделя много хартиен прах, или хартия с груба повърхност, която би могла да съкрати жизнения цикъл.

Нулиране на броя сканирания след смяна на ролките

Нулирайте броя на сканиранията с помощта на контролния панел или Epson Scan 2 Utility след смяната на комплекта ролки.

Този раздел обяснява как да нулирате броя с помощта на контролния панел.

1. Докоснете **Техническо обсл. Скенера** на началния екран.
2. Докоснете **Смяна на поддържаща ролка**.
3. Докоснете **Нулиране на брой сканирания**.
4. Изберете **Бр. ск. след см. ролка**, след което докоснете **Да**.

Забележка:
За да нулирате от Epson Scan 2 Utility, стартирайте Epson Scan 2 Utility, щракнете върху раздела ***Брояч****, след което щракнете върху* ***Възстановяване*** *в* ***Комплект за валяк****.*

Още по темата

➡ “Смяна на комплекта ролки” на страница 137

Пестене на енергия

Можете да пестите енергия чрез използване на спящия режим или режима за автоматично изключване на захранването, когато не се извършват операции от скенера. Можете да зададете времевия период, преди скенерът да влезе в спящ режим и да се изключи автоматично. Всяко едно увеличение ще окаже влияние върху енергийната ефективност на продукта. Мислете за околната среда, преди да направите каквито и да било промени.

1. Изберете **Настройки** от началния екран.
2. Изберете **Осн. Настройки**.
3. Изберете **Таймер за сън** или **Настр. за изкл.** и задайте необходимите настройки.

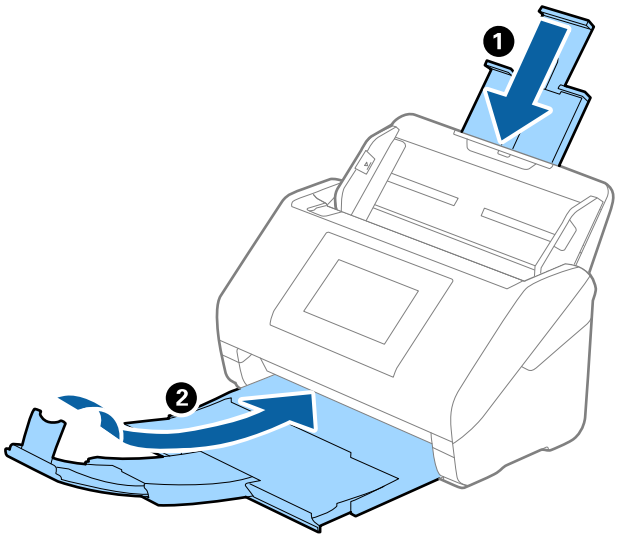
   Забележка:
   Наличните функции може да се различават в зависимост от местоположението на закупуване.

Транспортиране на скенера

Когато се налага транспортиране на скенера за преместване на друго място или за ремонт, следвайте описаните по-долу стъпки, за да го опаковате.

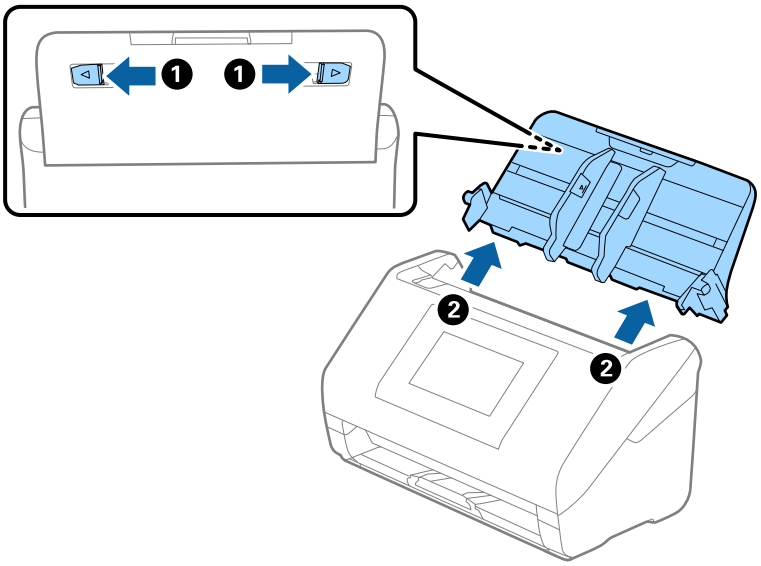
1. Натиснете бутон ⏻, за да изключите скенера.
2. Извадете AC адаптера.
3. Извадете кабелите и устройствата.

   Отстранете допълнителната или доставената Paper Alignment Plate, ако е закрепена.
4. Затворете удължението на входната и изходната тава.



> ***Важно:***
>
> *Уверете се, че сте затворили надеждно изходната тава. В противен случай тя може да бъде повредена по време на транспортирането.*

5. Извадете входната тава.



6. Закрепете опаковъчните материали, с които е бил доставен скенера, след което го поставете в оригиналната му кутия или в друга здрава кутия.

Архивиране на настройките

Можете да експортирате стойността на настройката, зададена от Web Config към файла.Можете да я използвате за архивиране на контактите, стойностите за настройка, като замените скенера и т.н.

Експортираният файл не може да бъде редактиран, защото е експортиран като двоичен файл.

Експортиране на настройки

Експортиране на настройката за скенера.

1. Влезте в Web Config, след което изберете раздела **Device Management** > **Export and Import Setting Value** > **Export**.

2. Изберете настройките, които искате да експортирате.

   Изберете настройките, които искате да експортирате.Ако изберете основна категория, подкатегориите също ще бъдат избрани.Обаче, подкатегориите, които водят до грешки чрез дублиране в рамките на една и съща мрежа (като IP адрес и др.) не могат да бъдат избрани.

3. Въведете парола, за да шифровате експортирания файл.

   Паролата ще Ви е необходима, за да импортирате файла.Оставете това поле празно, ако не искате да шифровате файла.

4. Щракнете върху **Export**.

> ***Важно:***
>
> *Ако искате да експортирате мрежовите настройки на скенера, като име на устройството и IPv6 адрес, изберете **Enable to select the individual settings of device** и изберете още елементи.Използвайте само избраните стойности на новия скенер.*

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

Импортирайте настройките

Импортирайте експортирания Web Config файл в скенера.

> ***Важно:***
>
> *Когато импортирате стойности, които включват индивидуална информация, като име на скенера или IP адрес, се уверете, че същият IP адрес не съществува в същата мрежа.*

1. Влезте в Web Config, след което изберете раздел **Device Management** > **Export and Import Setting Value** > **Import**.
2. Изберете експортирания файл, след което въведете шифрованата парола.
3. Щракнете върху **Next**.
4. Изберете настройките, които искате да импортирате, след което щракнете върху **Next**.
5. Щракнете върху **OK**.

Настройките се прилагат към скенера.

Още по темата

➡ "Как да стартирате Web Config в уеб браузър" на страница 40

възст. на наст. по подразбиране

На контролния панел изберете **Настройки** > **Системна администрация** > **възст. на наст. по подразбиране** и изберете елементите, които искате да върнете към стойностите по подразбиране.

- ❏ Настройки на мрежата: възстановява свързани с мрежа настройки до първоначалното им състояние.
- ❏ Всички освен Настройки на мрежата: възстановява други настройки до първоначалното им състояние, с изключение на свързаните с мрежа настройки.
- ❏ Всички настройки: възстановява всички настройки до първоначалното им състояние при закупуване.

Важно:

*Ако изберете и изпълните **Всички настройки**, всички данни за настройки, регистрирани на скенера, включително контактите, ще бъдат изтрити. Изтритите настройки не могат да се възстановят.*

Забележка:
Можете също да промените настройките на Web Config.

*Раздел **Device Management** > **Restore Default Settings***

Актуализиране на приложения и на фърмуера

Възможно е да изчистите някои проблеми и да подобрите или добавите функции, като актуализирате приложенията и фърмуера. Уверете се, че използвате най-новите версии на приложенията и фърмуера.

Важно:

❏ *Не изключвайте компютъра или скенера, докато актуализирате.*

Забележка:
*Когато скенерът може да се свързва към интернет, можете да актуализирате фърмуера от Web Config. Изберете раздел **Device Management** > **Firmware Update**, проверете изведеното съобщение и след това щракнете върху **Start**.*

1. Уверете се, че скенерът и компютърът са свързани и че компютърът е свързан с интернет.

2. Стартирайте EPSON Software Updater и актуализирайте приложенията или фърмуера.

   Забележка:
   Не се поддържат операционни системи Windows Server.

   ❏ Windows 11

   Щракнете върху бутона за стартиране, след което изберете **Всички приложения** > **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 10

   Щракнете върху бутона за стартиране, след което изберете **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Въведете името на приложението в препратката за търсене, след което изберете показаната икона.

   ❏ Windows 7

   Щракнете върху бутона за стартиране, след което изберете **Всички програми** или **Програми** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Изберете **Finder** > **Отиди** > **Приложения** > **Epson Software** > **EPSON Software Updater**.

Забележка:
Ако не можете да намерите приложението, което искате да актуализирате, в списъка, не можете да осъществите актуализация, използвайки EPSON Software Updater. Проверете за най-новите версии на приложенията в местния уеб сайт на Epson.

http://www.epson.com

Актуализиране на фърмуера на скенера с помощта на контролния панел

Ако скенерът може да се свързва към интернет, можете да актуализирате фърмуера на скенера с помощта на контролния панел. Можете също да настроите скенера редовно да проверява за актуализации на фърмуера и да Ви уведомява, когато има налични.

1. Изберете **Настройки** от началния екран.
2. Изберете **Системна администрация** > **Актуализация на фърмуера** > **Актуализация**.

   Забележка:
   *Изберете **Известие** > **Вкл.**, за да настроите скенера редовно да проверява за актуализации на фърмуера.*
3. Вижте съобщението, което се извежда на екрана, и започнете да търсите налични актуализации.
4. Ако на LCD екрана се появи съобщения за налична актуализация на фърмуера, следвайте инструкциите на екрана, за да стартирате актуализацията.

> ***Важно:***
> - *Не изключвайте скенера или захранващия кабел, докато актуализацията не приключи; в противен случай скенерът може да не функционира правилно.*
> - *Ако актуализацията на фърмуера не е напълно завършена или е неуспешна, скенерът няма да стартира нормално и при последващото му включване на LCD екрана ще се появи „Recovery Mode“. В този случай трябва отново да извършите актуализацията на фърмуера с помощта на компютър. Свържете скенера към компютъра с USB кабел. Докато „Recovery Mode“ се показва на скенера, няма да можете да актуализирате фърмуера през мрежова връзка. От компютъра влезте на уебсайта на Epson и изтеглете най-новата версия на фърмуера за скенера. Вижте инструкциите на уебсайта за последващите стъпки.*

Актуализиране на фърмуер чрез Web Config

Когато скенерът може да се свързва към интернет, можете да актуализирате фърмуера от Web Config.

1. Влезте в Web Config и изберете раздела **Device Management** > **Firmware Update**.
2. Щракнете върху **Start**, след което следвайте инструкциите на екрана.

   Стартира потвърждението на фърмуера и информацията за фърмуера се извежда, ако съществува актуализираният фърмуер.

Забележка:
Можете също да актуализирате фърмуера чрез Epson Device Admin. Можете визуално да потвърдите информацията за фърмуера в списъка с устройства. Това е полезно, когато искате да актуализирате фърмуера на множество устройства. Вижте ръководството на Epson Device Admin или помощта за повече подробности.

Още по темата

➡ “Как да стартирате Web Config в уеб браузър” на страница 40

Актуализиране на фърмуера без свързване към интернет

Можете да изтеглите фърмуера на устройството от уебсайта на Epson на компютър, след което да свържете устройството и компютъра чрез USB кабел, за да обновите фърмуера. If you cannot update over the network, try this method.

Забележка:
Преди да актуализирате, уверете се, че драйверът на скенера Epson Scan 2 е инсталиран на Вашия компютър. Ако Epson Scan 2 не е инсталиран, инсталирайте го отново.

1. Проверете уебсайта на Epson за най-новите версии за актуализиране на фърмуера.

   http://www.epson.com

   ❏ Ако има фърмуер за Вашия скенер, изтеглете го и преминете към следващата стъпка.

   ❏ Ако на уебсайта няма информация за фърмуера, вие вече използвате най-новия фърмуер.

2. Свържете компютъра, който съдържа изтегления фърмуер, към скенера с помощта на USB кабел.

3. Щракнете двукратно върху изтегления .exe файл.

   Epson Firmware Updater се стартира.

4. Следвайте инструкциите на екрана.