EPSON
EXCEED YOUR VISION

DS-790WN

Ръководство на администратора

NPD6726-00 BG

Авторско право

Търговски марки

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION и техните лога са регистрирани търговски марки или търговски марки на Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa и PaSoRi са регистрирани търговски марки на Sony Corporation.
- ❏ MIFARE е регистрирана търговска марка на NXP Semiconductor Corporation.
- ❏ Обща бележка: другите имена на продукти, които се използват тук, са само за целите на идентификация и е възможно да са търговски марки на съответните собственици. Epson не разполага с никакви права над тези марки.

Съдържание

Авторско право

Търговски марки

Въведение

Необходими настройки, които отговарят на Вашите нужди

Мрежови настройки

Софтуер за настройка на скенера

Необходими настройки за сканиране

Персонализиране на дисплея на контролния панел

Основни настройки за сигурност

Разширени настройки за сигурност

Authentication Settings

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

❏ Активиране и управление на Authentication Settings

❏ Извършвайте ежедневна поддръжка

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

Забележка:
В настоящия документ са обяснени Authentication Settings, които осигуряват самостоятелно удостоверяване, без да се налага да се използва сървър за удостоверяване. В допълнение към Authentication Settings, представени в настоящото ръководство, можете да изградите и система за удостоверяване с помощта на сървър за удостоверяване. За изграждане на система използвайте Document Capture Pro Server Authentication Edition (съкратеното име е Document Capture Pro Server AE).

За допълнителна информация се свържете с Вашия местен офис на Epson.

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.

Препратки към операционната система

Windows

В настоящото ръководство термини като „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Server 2019“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“ и „Windows Server 2008 R2“ се отнасят до следните операционни системи. Освен това „Windows“ се използва за справка с всички версии и „Windows Server“ се използва за справка с „Windows Server 2019“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“ и „Windows Server 2008 R2“.

- ❏ 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® 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

Mac OS

В настоящото ръководство „Mac OS“ се отнася до macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan, и OS X Yosemite.

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 14
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 21

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. "Конфигуриране на сървър за електронна поща" на страница 43 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 64
Искам да запиша сканирани изображения в папка в мрежата. (Scan to Network Folder/FTP)	1. Създайте папка в мрежата, където искате да запаметите изображенията. "Настройка на споделена мрежова папка" на страница 46 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 64
Искам да запиша сканирани изображения в облачна услуга. (Scan to Cloud)	Настройте Epson Connect. За подробности относно настройката вижте уеб портала 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 78

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 87
Искам да дезактивирам използването на скенери с USB връзки.	Дезактивирайте външния интерфейс. "Дезактивиране на външния интерфейс" на страница 93

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 99
Искам да криптирам комуникационния път.	1. Настройте Вашия цифров сертификат. "Използване на цифров сертификат" на страница 102 2. Настройте SSL/TLS комуникация. "SSL/TLS комуникация със скенера" на страница 108
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 109
Искам да използвам скенер в мрежа IEEE802.1X.	Задайте IEEE802.1X за скенера. "Свързване на скенера към мрежа IEEE802.1X" на страница 120

Настройка на функциите, които да бъдат удостоверявани от скенера

Цел	Необходими настройки
Искам да активирам Authentication Settings.	Вижте следното за повече информация относно наличните Authentication Settings и Authentication Method. "Относно Authentication Settings" на страница 130 "Относно Authentication Method" на страница 131

Използване на системата за удостоверяване на сървъра

С Document Capture Pro Server Authentication Edition (съкратено Document Capture Pro Server AE), можете да изградите система за удостоверяване, която използва сървър за удостоверяване.

За допълнителна информация се свържете с Вашия местен офис на Epson.

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 ги свържете и с помощта на инсталиращата програма.

❏ *Настройка от уеб сайта*

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

http://epson.sn

❏ *Инсталиране от диска със софтуер (само за модели, които имат диск със софтуер и потребители с компютри с Windows с дискови устройства).*

Поставете диска със софтуера в компютъра, след което следвайте инструкциите на екрана.

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 29

Отдели	Елементи	Забележка
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.
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 31

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.

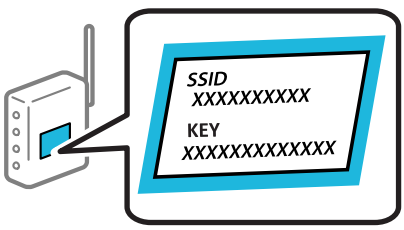
Ако безжичният маршрутизатор поддържа WPS, можете да зададете настройките, като използвате настройка с натискане на бутон.

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

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 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. 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 **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.*

Още по темата

➡ “Проверка на състоянието на мрежовата връзка” на страница 27

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 27

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 27

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. Можете да стартирате инсталиращата програма с помощта на един от следните методи.

❏ Настройка от уебсайта

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

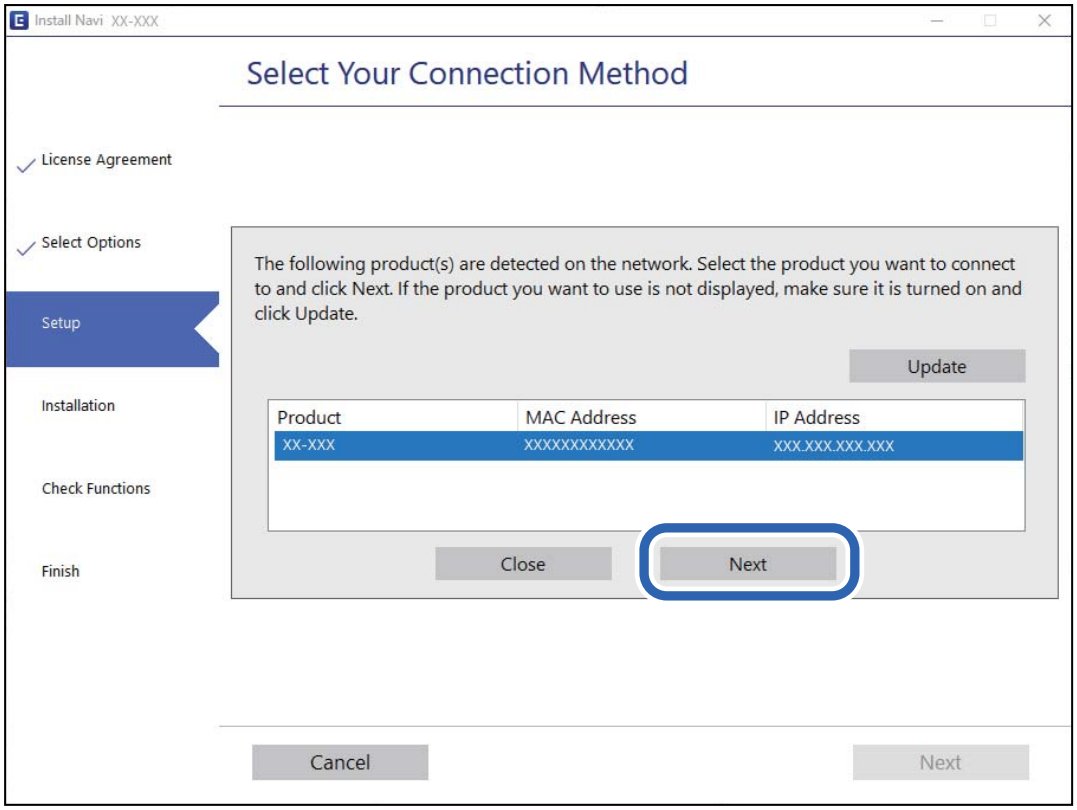
http://epson.sn

❏ Инсталиране от диска със софтуер (само за модели, които имат диск със софтуер и потребители с компютри с Windows с дискови устройства).

Поставете диска със софтуера в компютъра, след което следвайте инструкциите на екрана.

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 25

Свързване чрез Wi-Fi Direct

Свържете смарт устройството директно към скенера без безжичен маршрутизатор.

Вижте следното за повече подробности.

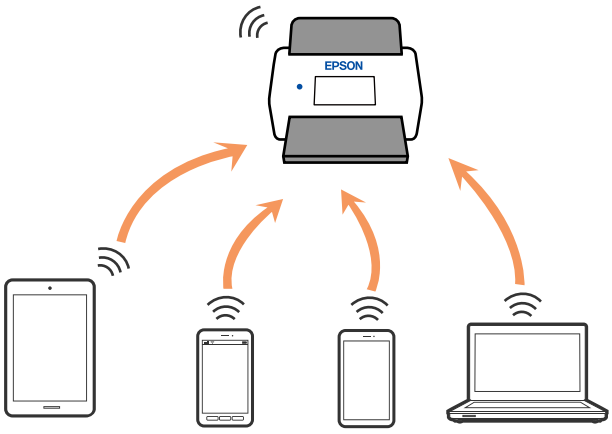
“Директно свързване на смарт устройство и скенер (Wi-Fi Direct)” на страница 22

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. Можете да стартирате инсталиращата програма с помощта на един от следните методи.

❏ Настройка от уебсайта

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

http://epson.sn

❏ Инсталиране от диска със софтуер (само за модели, които имат диск със софтуер и потребители с компютри с Windows с дискови устройства).

Поставете диска със софтуера в компютъра, след което следвайте инструкциите на екрана.

Избиране на методите на свързване

Следвайте инструкциите на екрана. На екрана **Изберете операцията** 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 32

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, влезте в следния уебсайт и след това въведете името на продукта. Отидете на **Конфигуриране**, след което стартирайте настройката.

http://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. Можете да стартирате инсталиращата програма с помощта на следния метод.

❏ Настройка от уебсайта

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

http://epson.sn

❏ Инсталиране от диска със софтуер (само за модели, които имат диск със софтуер и потребители с компютри с Windows с дискови устройства).

Поставете диска със софтуера в компютъра, след което следвайте инструкциите на екрана.

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 18

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.

❏ Настройка от уебсайта

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

http://epson.sn

❏ Инсталиране от диска със софтуер (само за модели, които имат диск със софтуер и потребители с компютри с Windows с дискови устройства).

Поставете диска със софтуера в компютъра, след което следвайте инструкциите на екрана.

Избиране на промяна на метода на свързване

Следвайте инструкциите на екрана. На екрана **Изберете операцията** 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

Wi-Fi спецификации

Вижте следната таблица за спецификации на Wi-Fi.

Държави или региони, освен посочените по-долу	Таблица A
Австралия Нова Зеландия Тайван Южна Корея	Таблица B

Таблица A

Стандарти	IEEE 802.11b/g/n*1
Честотен обхват	2,4 GHz
Максимална радиочестотна мощност на предаване	2400 – 2483,5 MHz: 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 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 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 IPv4/IPv6

Функции	Поддържани
Epson Scan 2	IPv4, IPv6

Функции	Поддържани
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

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
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

Използвайте	Местоназначение (сървър)	Протокол	Номер на порт
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

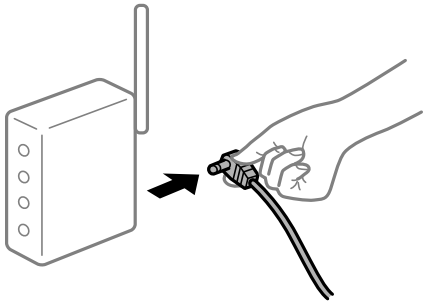
Не може да се свърже към мрежа

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

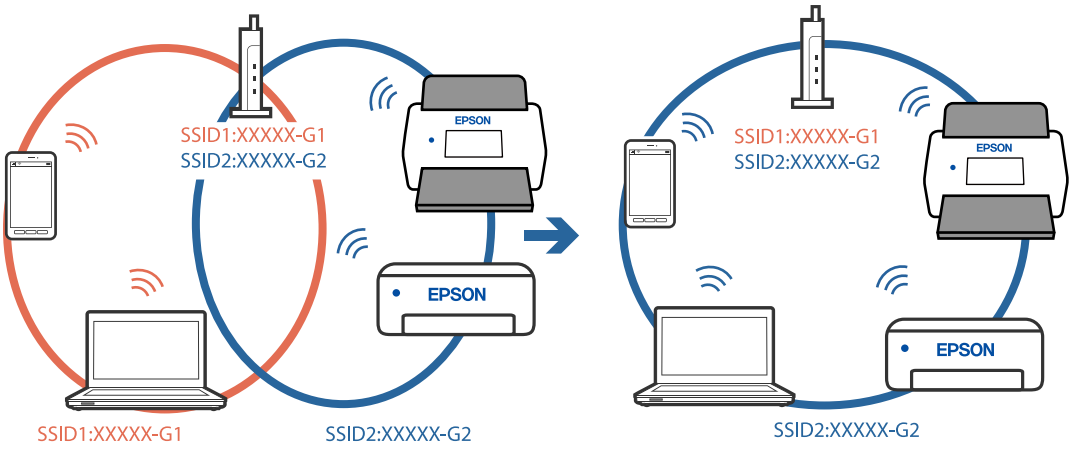
Извършете отново настройките на връзката така, че да съвпадат с новия безжичен маршрутизатор.

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.

   “Пускане на Web Config в уеб браузър” на страница 37
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

Web Config

Web Config е приложение, което работи в уеб браузър, като Internet Explorer и Safari, на компютър. Можете да проверите състоянието на скенера или да промените настройките на мрежата и скенера. Тъй като скенерите са достъпни и управлявани директно от мрежата, то е подходящо за настройка на един скенер в даден момент. За да използвате Web Config, свържете своя компютър към същата мрежа като скенера.

Поддържат се следните браузъри.

Microsoft Edge, Windows Internet Explorer 8 или по-нова версия, Firefox*, Chrome*, Safari*

* Използвайте най-новата версия.

Пускане на Web Config в уеб браузър

1. Проверете IP адреса на скенера.

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

2. Стартирайте уеб браузър от компютъра или смарт устройството и въведете IP адреса на скенера.

   Формат:

   IPv4: http://IP адреса на скенера/

   IPv6: http://[IP адреса на скенера]/

   Примери:

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   Забележка:
   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.

3. Влезте като администратор, за да промените настройките на скенера.

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

   Забележка:
   - ❏ *Следното предоставя първоначалните стойности за информацията за администратора на Web Config.*

     ·Потребителско име: няма (празно)

     ·Парола: серийният номер на скенера

     За да видите серийния номер, проверете етикета на задната страна на скенера.
   - ❏ *Ако в горния десен ъгъл на екрана се вижда **Administrator Logout**, значи вече сте влезли като администратор.*

Работа с Web Config на Windows

Когато свързвате компютър към скенер с помощта на WSD, следвайте стъпките по-долу, за да стартирате Web Config.

1. Отворете списъка със скенери на компютъра.

   ❏ Windows 10

   Щракнете върху бутона за стартиране и изберете **Система Windows** > **Контролен панел** > **Преглед на устройства и принтери** в **Хардуер и звук**.

   ❏ Windows 8.1/Windows 8

   Изберете **Работен плот** > **Настройки** > **Контролен панел** > **Преглед на устройства и принтери** в **Хардуер и звук** (или **Хардуер**).

   ❏ Windows 7

   Щракнете върху бутон Старт и изберете **Контролен панел** > **Преглед на устройства и принтери** в **Хардуер и звук**.

2. Щракнете с десния бутон върху скенера и изберете **Свойства**.

3. Изберете раздела **Уебуслуга** и щракнете върху URL адреса.

   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.

   Забележка:

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

   ·Потребителско име: няма (празно)

   ·Парола: серийният номер на скенера

   За да видите серийния номер, проверете етикета на задната страна на скенера.

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

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.

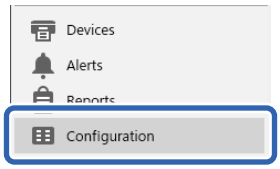
Шаблон за конфигуриране

Създаване на шаблон за конфигуриране

Създайте нов шаблон за конфигуриране.

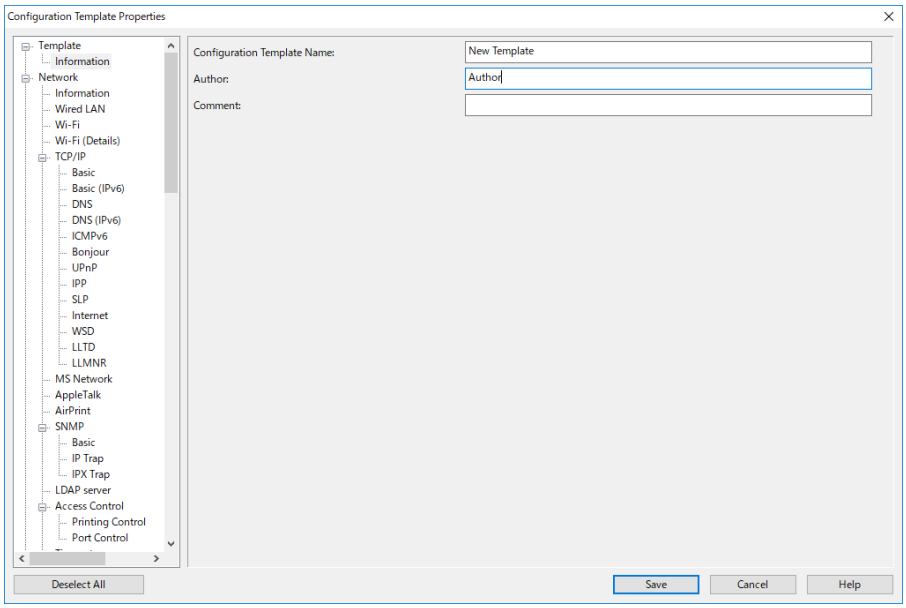
1. Стартирайте Epson Device Admin.

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.

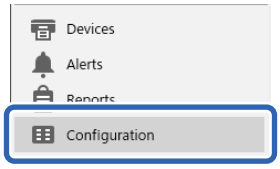
*1. В менюто на лентата на екрана „Списък с устройства“ изберете **Options** > **Password manager**.*

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

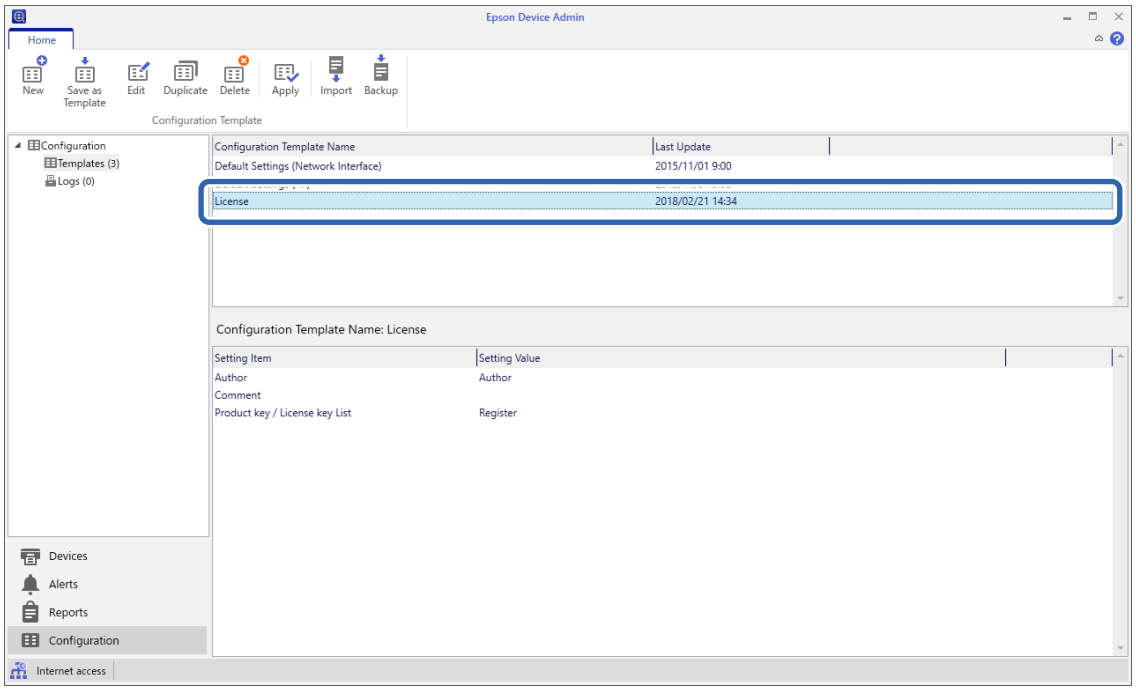
*3. Изберете съответния скенер и след това щракнете **Edit**.*

*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**.



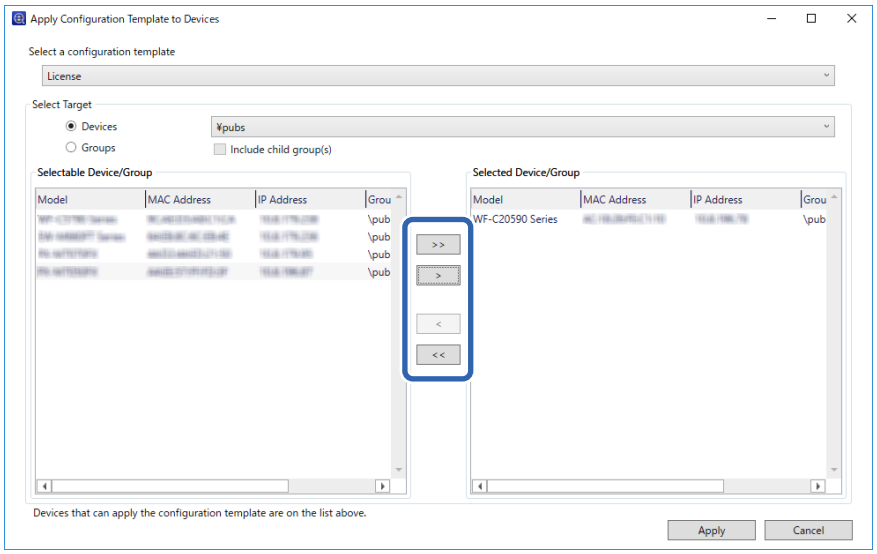
3. Щракнете върху **Apply** от менюто на лентата.

   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

Конфигуриране на сървър за електронна поща

Задайте сървъра за електронна поща от Web Config.

Когато скенерът може да изпрати имейла чрез настройка на сървъра за електронна поща, е възможно да се случи следното.

❏ Прехвърляне на резултатите от сканиране чрез имейл

❏ Получаване на имейл известие от скенера

Щракнете по-долу преди настройка.

❏ Скенерът е свързан към мрежата, която има достъп до сървъра за електронна поща.

❏ Информация за настройка на имейла на компютъра, която използва същия сървър за електронна поща като на скенера.

Забележка:

❏ *Когато използвате сървъра за електронна поща в интернет, потвърдете информацията за настройка от доставчика или уебсайта.*

❏ *Можете също да зададете сървъра за електронна поща от контролния панел. Влезте по следния начин.*

Настройки > ***Настройки на мрежата*** > ***Разширени*** > ***Имейл сървър*** > ***Настройки на сървър***

1. Влезте в Web Config и изберете раздел **Network** > **Email Server** > **Basic**.
2. Въведете стойност за всеки елемент.
3. Изберете **OK**.

   Избраните от Вас настройки ще бъдат показани.

Още по темата

➡ "Пускане на Web Config в уеб браузър" на страница 37

Елементи за настройка на сървъра за електронна поща

Елементи	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	Изисква се сървърът за електронна поща да поддържа SMTP удостоверяване.
	POP before SMTP	Конфигурирайте POP3 сървъра, когато изберете този метод.
Authenticated Account	Ако изберете **SMTP AUTH** или **POP before SMTP** като **Authentication Method**, въведете име на акаунта за удостоверяване между 0 и 255 символа в ASCII (0x20 – 0x7E).	
Authenticated Password	Ако изберете **SMTP AUTH** или **POP before SMTP** като **Authentication Method**, въведете парола за удостоверяване между 0 и 20 символа в ASCII (0x20 – 0x7E).	

Елементи	Настройки и обяснение	
Sender's Email Address	Въведете имейл адреса на подателя. Въведете между 0 и 255 знака 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**.
Certificate Validation	Сертификатът е проверен при разрешаването му. Препоръчваме тази опция да се зададе на **Enable**.	
POP3 Server Address	Ако изберете **POP before SMTP** като **Authentication Method**, въведете адреса на POP3 сървъра между 0 и 255 знака, като ползвате A – Z, a – z, 0 – 9, ., -. Можете да използвате формат IPv4 или FQDN.	
POP3 Server Port Number	Ако изберете **POP before SMTP** за **Authentication Method**, въведете число между 1 и 65 535.	

Проверка на връзката с пощенския сървър

Можете да проверите връзката към имейл сървъра като извършите проверка на връзката.

1. Влезте в Web Config и изберете раздел **Network** > **Email Server** > **Connection Test**.
2. Изберете **Start**.

   Тестът за свързване към имейл сървъра е стартиран. След теста се показва отчетът за проверката.

   Забележка:
   Можете също да проверите връзката към имейл сървъра от контролния панел. Влезте по следния начин.

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

Позовавания при диагностика на връзката с имейл сървъра

Съобщения	Причина
Connection test was successful.	Това съобщение се показва, когато свързването със сървъра е успешно.

Съобщения	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
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 разрешаване на име за POP3 сървър
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.

Съобщения	Причина
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.

Настройка на споделена мрежова папка

Задайте споделена мрежова папка, за да запишете сканираното изображение.

Когато запазвате файл в папка, скенерът влиза като потребителя на компютъра, за който е създадена папката.

Създаване на споделената папка

Още по темата

- “Преди създаване на споделената папка” на страница 46
- “Проверка на мрежовия профил” на страница 47
- “Местоположение, където е създадена споделената папка, и пример за сигурността” на страница 47
- “Добавяне на група или потребител, която разрешава достъп” на страница 60

Преди създаване на споделената папка

Преди създаване на споделената папка, проверете следното.

❏ Скенерът е свързан към мрежата, от която може да получи достъп до компютъра, където ще бъде създадена споделената папка.

❏ В името на компютъра, където ще бъде създадена споделената папка, не е включен многобайтов знак.

Важно:

Когато в името на компютъра е включен многобайтов знак, записването на файла в споделената папка може да не бъде успешно.

В този случай сменете името на компютъра, като не включвате многобайтов знак в името или сменете името на компютъра.

Когато сменяте името на компютъра, не забравяйте предварително да потвърдите с администратора, защото това може да засегне някои настройки като управление на компютъра, достъп до ресурси и т.н.

Проверка на мрежовия профил

От компютъра, където споделената папка ще бъде създадена, проверете дали споделянето на папка е достъпно.

1. Влезте в компютъра, където ще бъде създадена споделената папка, от потребителския акаунт на администратора.

2. Изберете **Контролен панел** > **Мрежа и интернет** > **Център за мрежи и споделяне**.

3. Щракнете върху **Промяна на разширени настройки за споделяне**, след което щракнете върху за профила с **(текущ профил)** в изведените мрежови профили.

4. Проверете дали **Включване на споделянето на файлове и принтери** е избрано на **Споделяне 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.

Местоположение, където е създадена споделената папка, и пример за сигурността

В зависимост от местоположението, където се създава споделената папка, сигурността и удобството се различават.

За управление на споделената папка от скенерите и други компютри се изискват следните разрешения за четене и промяна за папката.

❏ Раздел **Споделяне** > **Разширено споделяне** > **Разрешения**

Управлява разрешението за достъп до мрежата на споделената папка.

❏ Разрешение за достъп на раздела **Сигурност**

Управлява разрешението за достъп до мрежа и локалния достъп на споделената папка.

Когато зададете **Всеки** на споделената папка, която е създадена на работния плот, като пример за създаване на споделена папка, всички потребители, които имат достъп до компютъра, ще имат разрешение за достъп.

Въпреки това потребителят, който няма разрешение, няма достъп до тях, защото работният плот (папката) е под управлението на потребителската папка и след това настройките за сигурност на потребителската папка се предават към нея. Потребителят, който има разрешение за достъп на раздела **Сигурност** (потребител, който е влязъл и администратор в този случай) може да управлява папката.

Вижте по-долу за създаване на правилното местоположение.

Този пример е при създаване на папка „scan_folder“.

Още по темата

➡ “Пример за конфигурация на файлови сървъри” на страница 48

➡ “Пример за конфигурация на персонален компютър” на страница 54

Пример за конфигурация на файлови сървъри

Това разяснение е пример за създаване на споделената папка в главната директория на устройството на споделения компютър, като например файловия сървър, при следното условие.

Право на достъп до споделената папка имат потребители с контролиран достъп като някой, който има същия домейн на компютъра си за създаване на споделена папка.

Задайте тази конфигурация, когато разрешавате на всеки потребител да чете и пише в споделената папка на компютъра, като например файловият сървър и споделеният компютър.

❏ Място за създаване на споделена папка: главната директория на устройството

❏ Път до папката: C:\scan_folder

❏ Разрешение за достъп през мрежата (Споделяне на разрешения): всеки

❏ Разрешение за достъп на файловата система (сигурност): удостоверени потребители

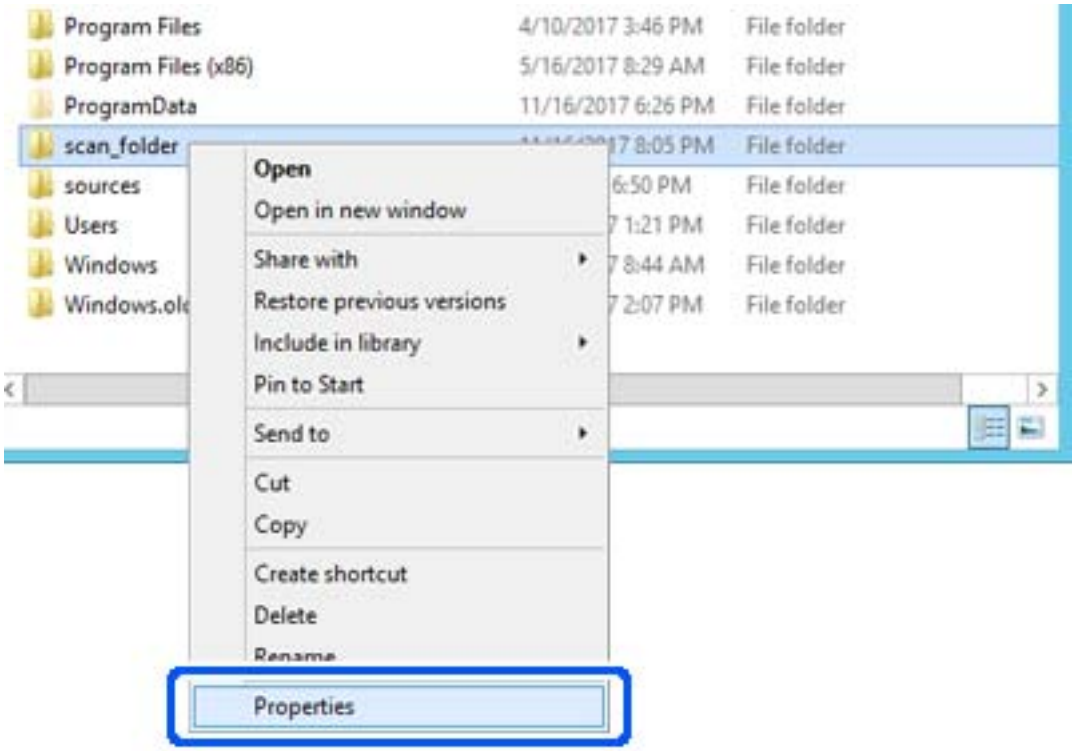
1. Влезте в компютъра, където ще бъде създадена споделената папка, от потребителския акаунт на администратора.

2. Стартирайте Explorer.

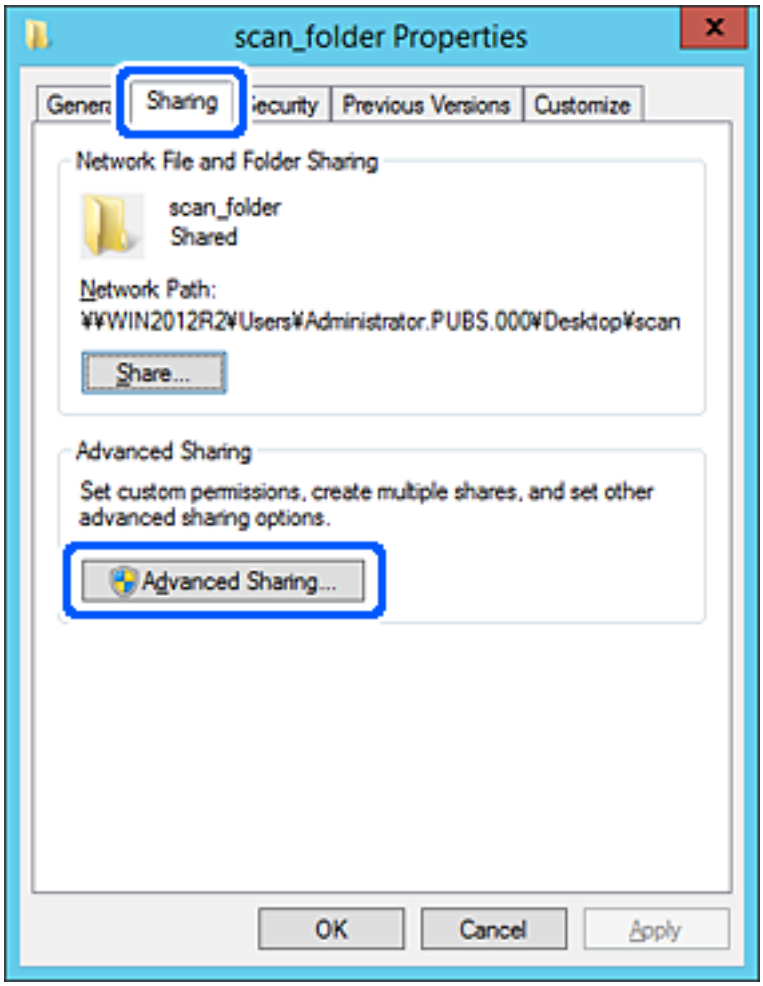
3. Създайте папката в главната директория на устройството и след това я наименувайте „scan_folder“.

   За името на папката въведете между 1 и 12 буквено-цифрови знака. Ако ограничението на знаците за името на папката е надвишено, Вие може да нямате достъп до нея при различни среди.

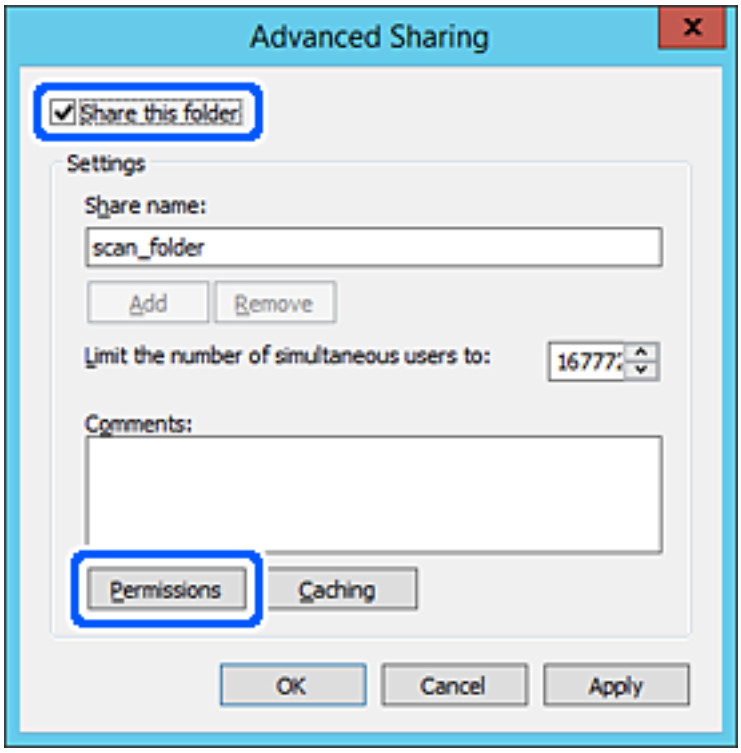
4. Щракнете с десния бутон върху папката и след това изберете **Свойства**.



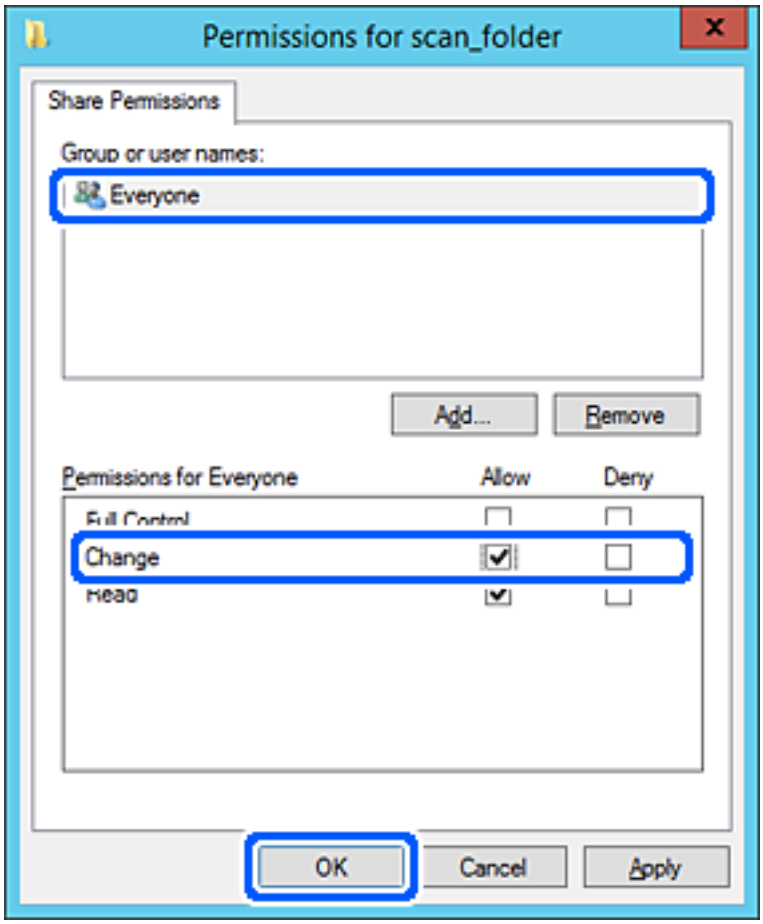
5. Щракнете върху **Разширено споделяне** на раздела **Споделяне**.



6. Изберете **Споделяне на тази папка**, след което щракнете върху **Разрешения**.

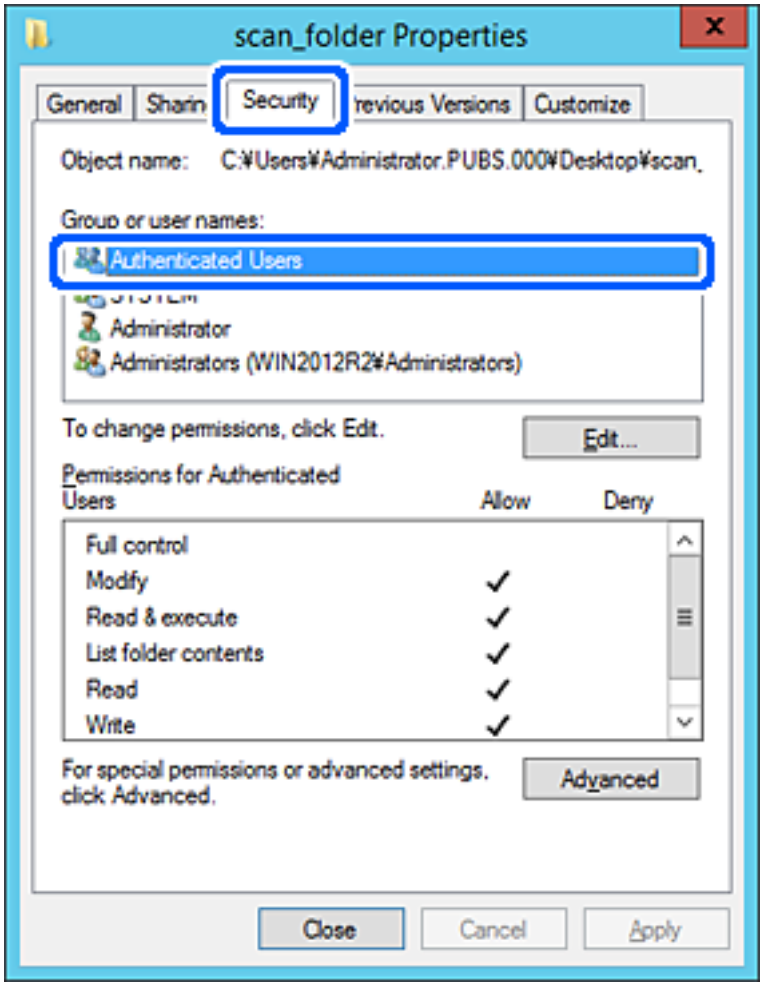


7. Изберете групата **Всеки** на **Имена на група или потребители**, изберете **Разрешаване** на **Промяна**, след което щракнете върху **OK**.



8. Щракнете върху **OK**.

9. Изберете раздела **Сигурност**, след което изберете **Удостоверени потребители** в **Имена на група или потребители**.

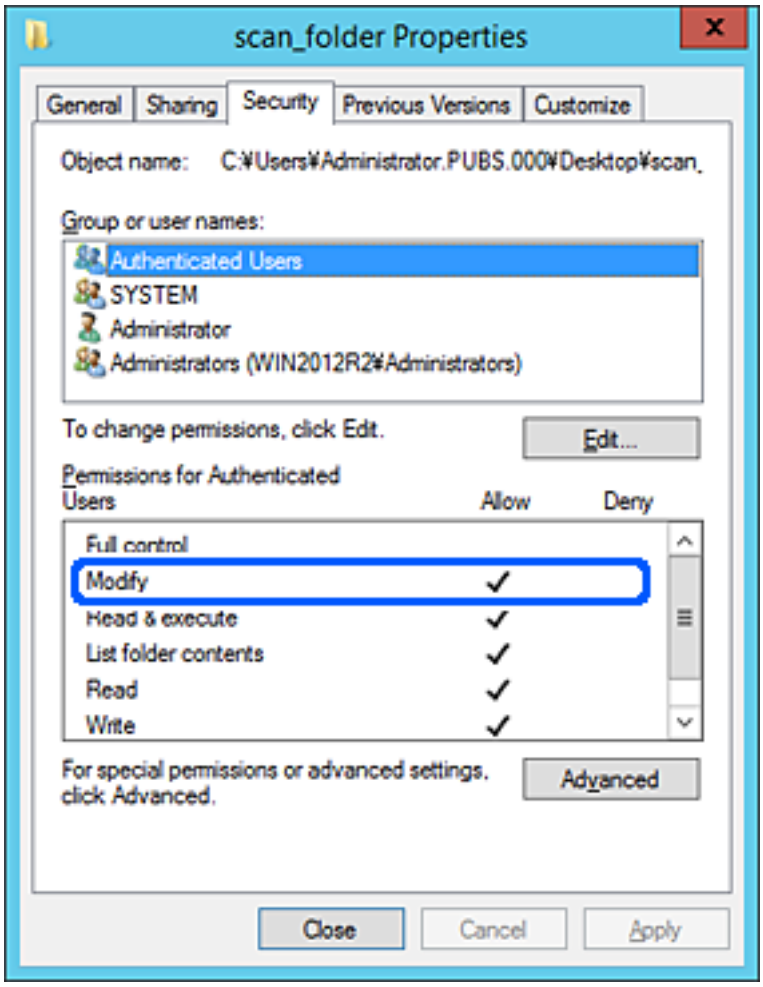


„Удостоверени потребители“ е специалната група, която включва всички потребители, които имат право да влизат в домейна или компютъра. Тази група се извежда само когато папката е създадена точно под главната папка.

Ако не се извежда, можете да я добавите, като щракнете върху **Редактиране**. За повече подробности вижте съответната информация.

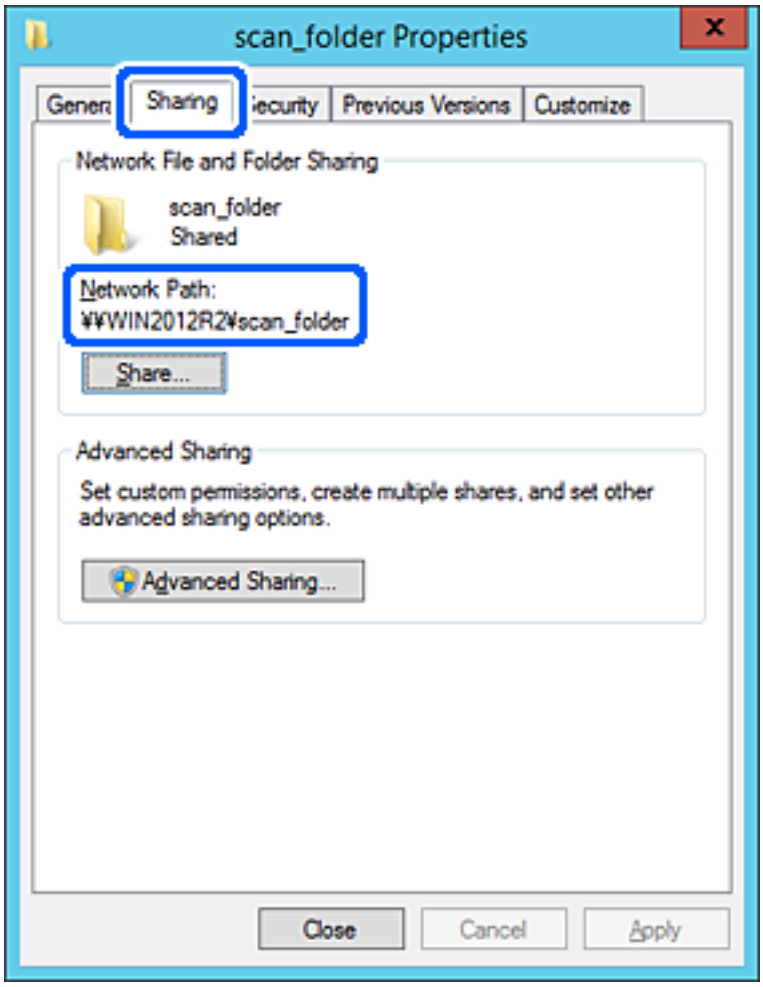
10. Проверете дали сте избрали **Разрешаване** на **Промяна** в **Разрешения за удостоверени потребители**.

    Ако не е избрано, изберете **Удостоверени потребители**, изберете **Редактиране**, изберете **Разрешаване** на **Промяна** в **Разрешения за удостоверени потребители**, след което щракнете върху **OK**.



11. Изберете раздел **Споделяне**.

    Извежда се пътят на споделената папка в мрежата. Това се използва при регистриране в контактите на скенера. Моля, запишете го.



12. Щракнете върху **OK** или **Затваряне**, за да затворите екрана.

    Проверете дали файлът може да бъде записан или прочетен на споделената папка от компютрите със същия домейн.

Още по темата

➡ “Добавяне на група или потребител, която разрешава достъп” на страница 60

➡ “Регистриране на местоназначение към контакти чрез Web Config” на страница 65

Пример за конфигурация на персонален компютър

Това разяснение е пример за създаване на споделена папка на работния плот на потребителя, който в момента е влязъл в компютъра.

Потребителят, който влиза в компютъра и който има администраторски права, може да получи достъп до папката на работния плот и до папката с документи, които са в папка Потребител.

Задайте тази конфигурация, когато НЕ разрешавате четене и писани на друг потребител в споделената папка на персонален компютър.

- ❏ Място за създаване на споделена папка: работен плот
- ❏ Пътя до папката: C:\Users\xxxx\Desktop\scan_folder
- ❏ Разрешение за достъп през мрежата (Споделяне на разрешения): всеки
- ❏ Разрешение за достъп на файлова система (сигурност): да не се добавят или да се добавят имена на потребител/група, на които им е разрешен достъп

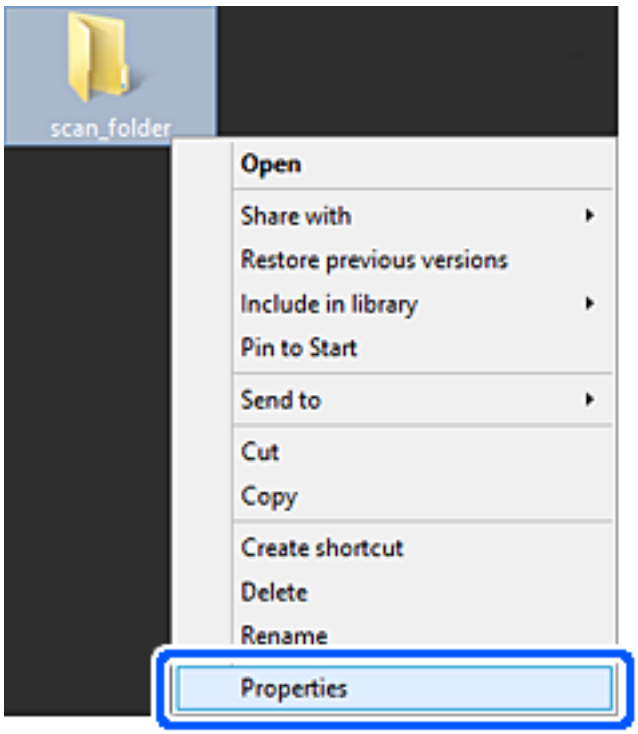
1. Влезте в компютъра, където ще бъде създадена споделената папка, от потребителския акаунт на администратора.

2. Стартирайте Explorer.

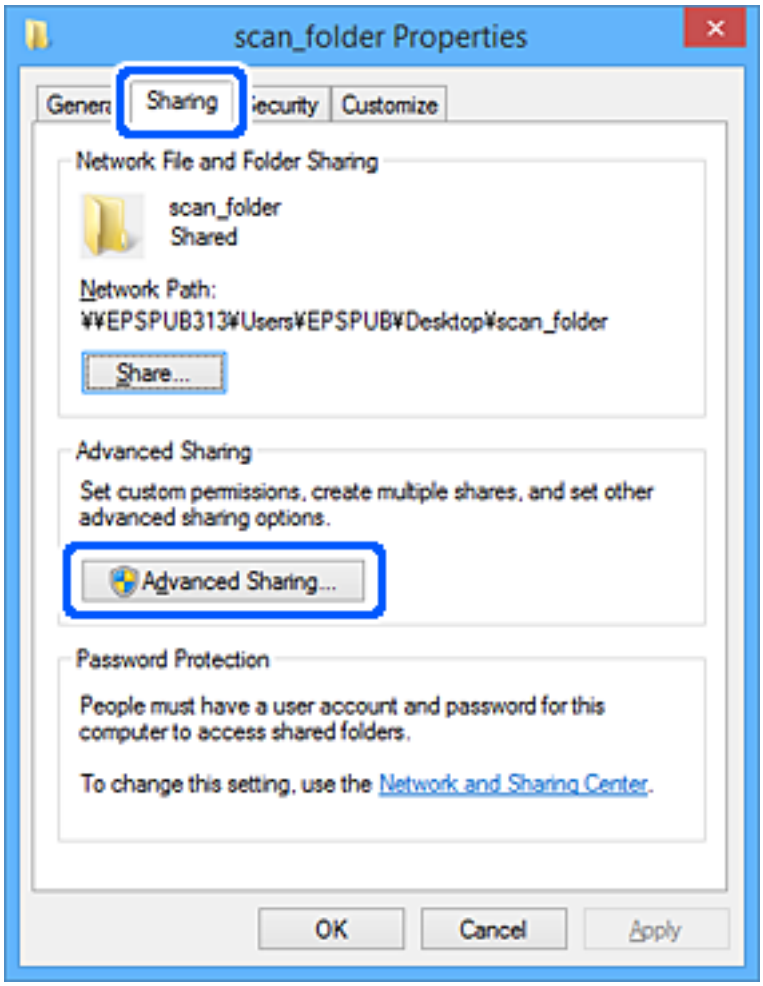
3. Създайте папката на работния плот и след това я наименувайте „scan_folder“.

   За името на папката въведете между 1 и 12 буквено-цифрови знака. Ако ограничението на знаците за името на папката е надвишено, Вие може да нямате достъп до нея при различни среди.

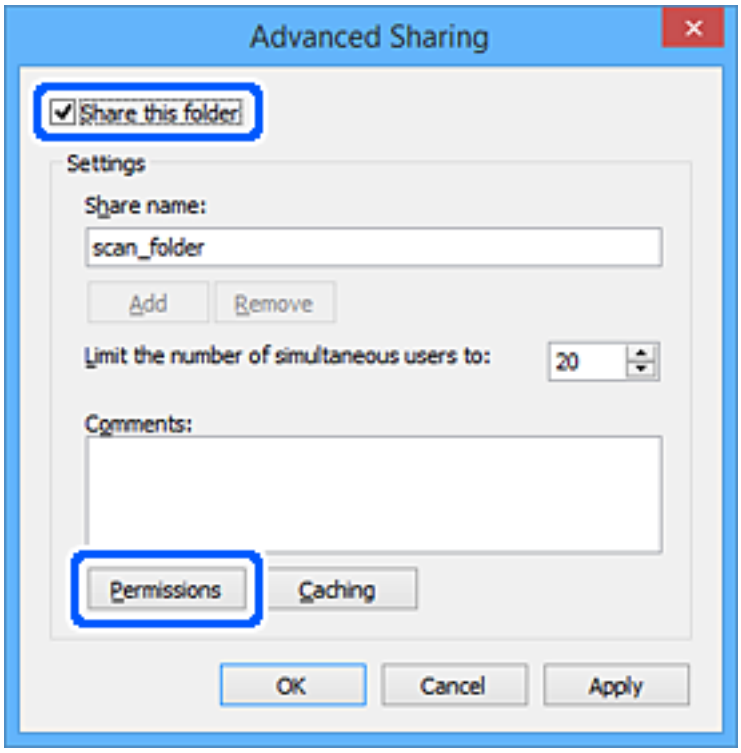
4. Щракнете с десния бутон върху папката и след това изберете **Свойства**.



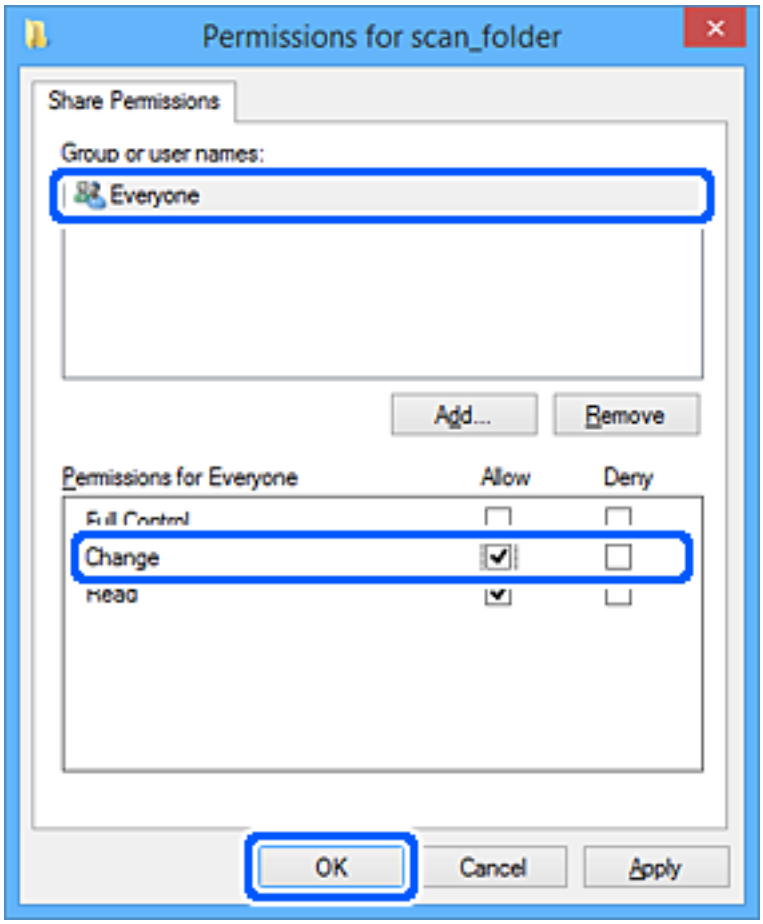
5. Щракнете върху **Разширено споделяне** на раздела **Споделяне**.



6. Изберете **Споделяне на тази папка**, след което щракнете върху **Разрешения**.



7. Изберете групата **Всеки** на **Имена на група или потребители**, изберете **Разрешаване** на **Промяна**, след което щракнете върху **OK**.



8. Щракнете върху **OK**.

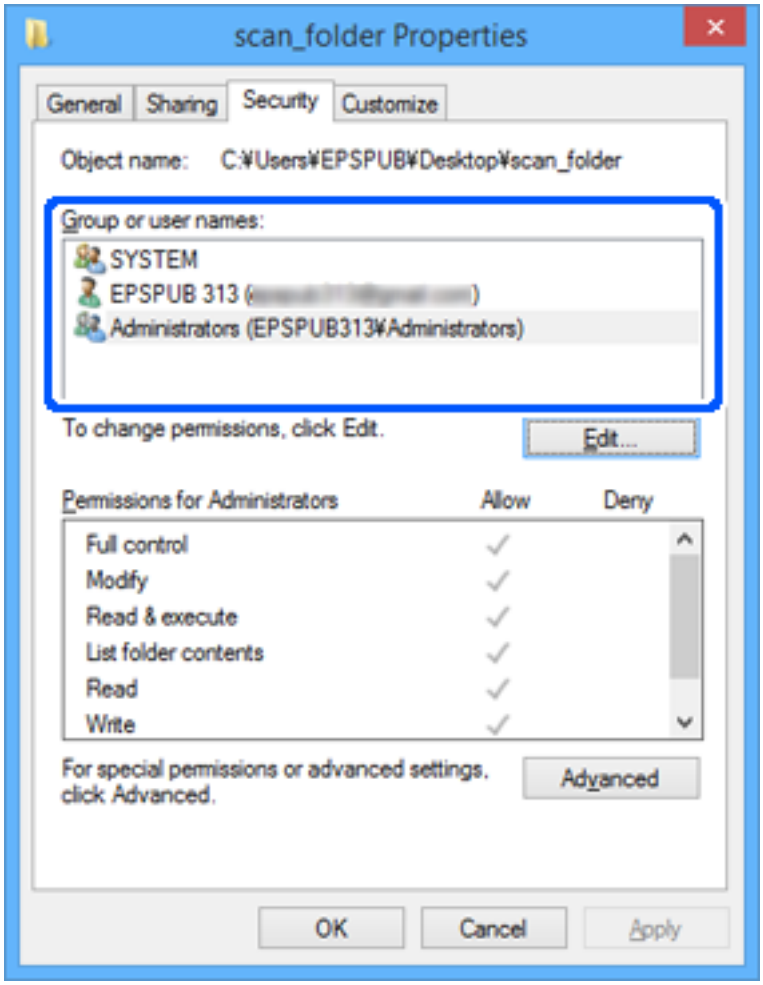
9. Изберете раздел **Сигурност**.

10. Поставете отметка на групата или потребителя в **Имена на група или потребител**.

    Изведените тук група или потребител могат да влизат в споделената папка.

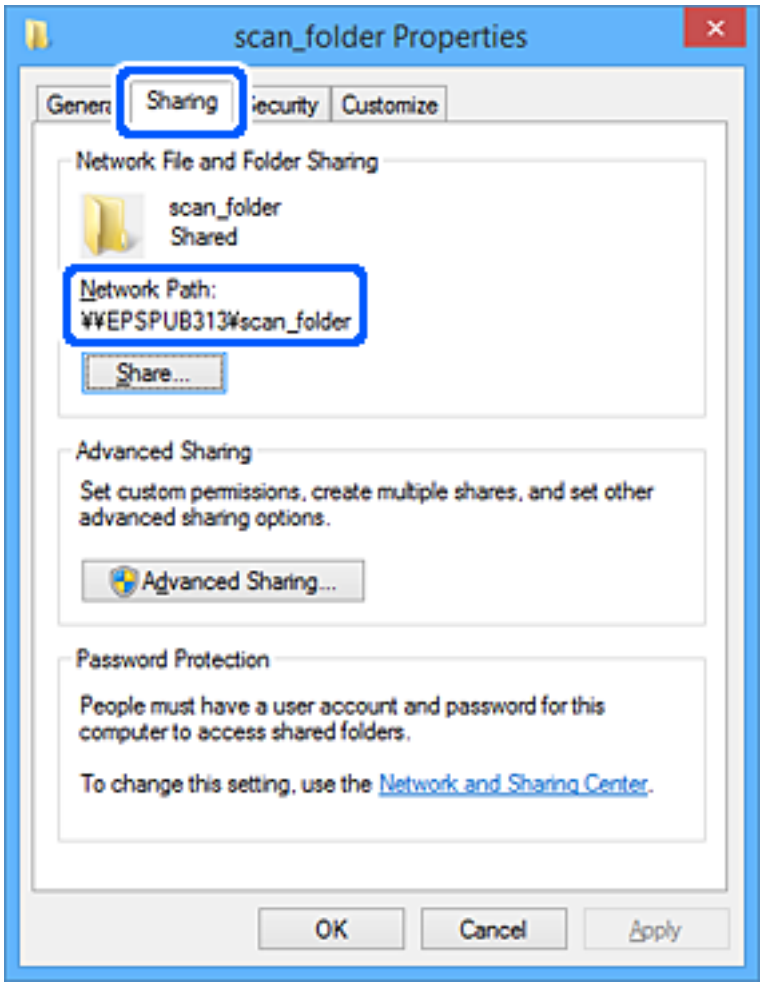
    В този случай потребителят, който влиза в този компютър, и администраторът могат да влизат в споделената папка.

Добавете разрешение за достъп, ако е необходимо. Можете да го добавите, като щракнете върху **Редактиране**. За повече подробности вижте съответната информация.



11. Изберете раздел **Споделяне**.

    Извежда се пътят на споделената папка в мрежата. Това се използва при регистриране в контактите на скенера. Моля, запишете го.



12. Щракнете върху **OK** или **Затваряне**, за да затворите екрана.

    Проверете дали файлът може да бъде записан или прочетен на споделената папка от компютрите на потребителите или групите с разрешение за достъп.

Още по темата

➡ “Добавяне на група или потребител, която разрешава достъп” на страница 60

➡ “Регистриране на местоназначение към контакти чрез Web Config” на страница 65

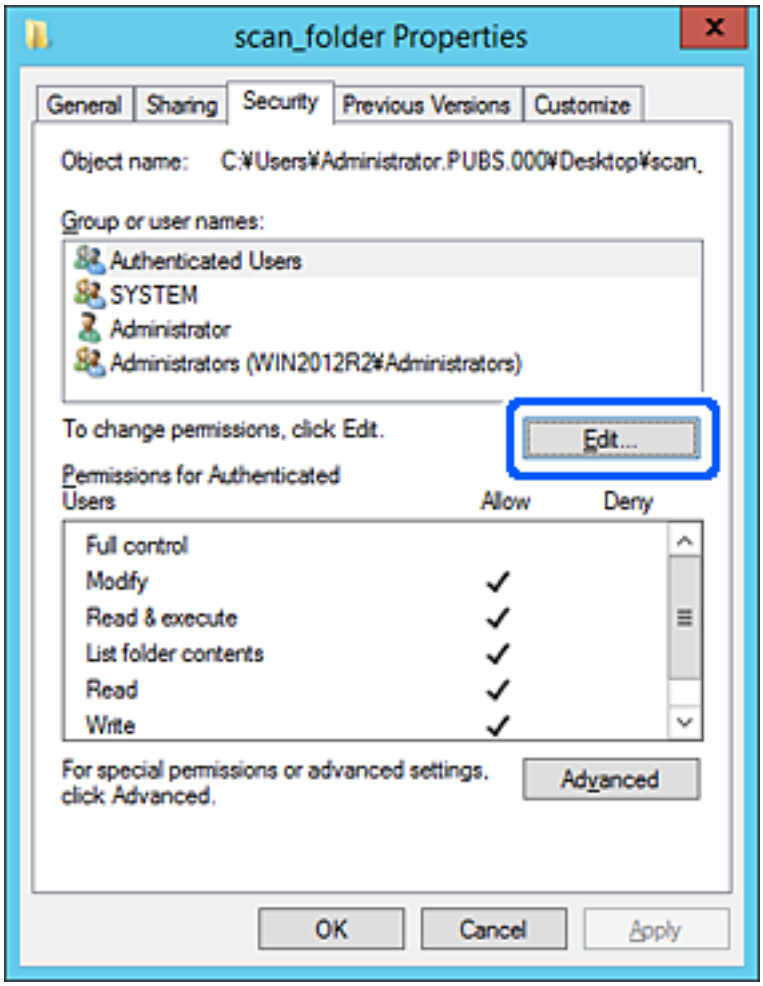
Добавяне на група или потребител, която разрешава достъп

Можете да добавите групата или потребителя, които разрешават достъп.

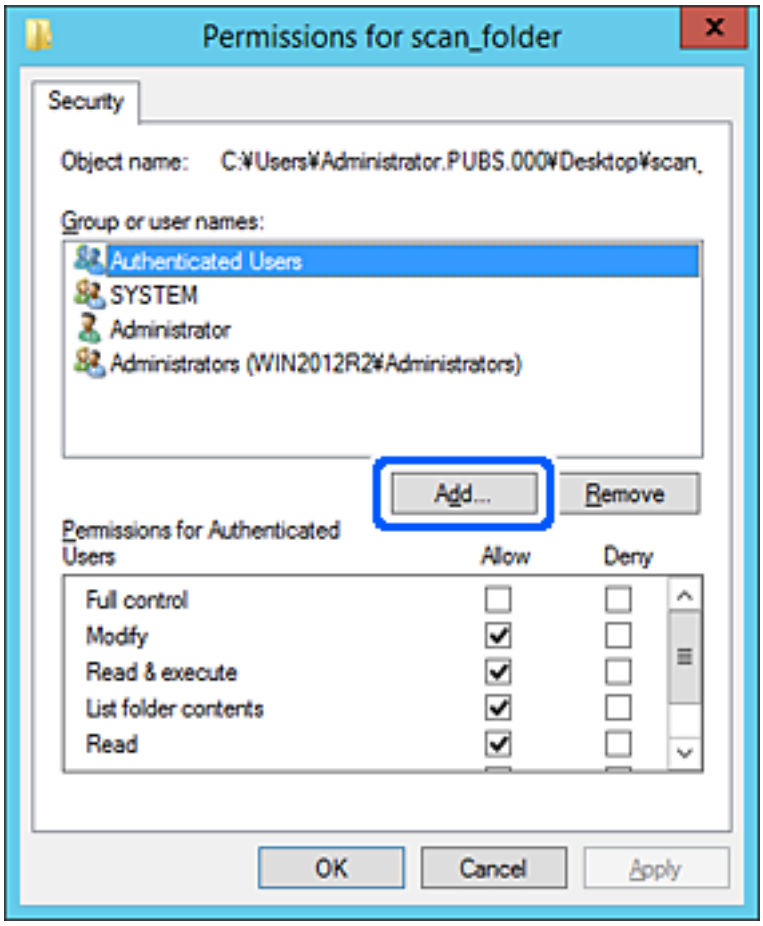
1. Щракнете с десния бутон върху папката и изберете **Свойства**.

2. Изберете раздела **Сигурност**.

3. Щракнете върху **Редактиране**.



4. Щракнете върху **Добавяне** под **Имена на група или потребители**.

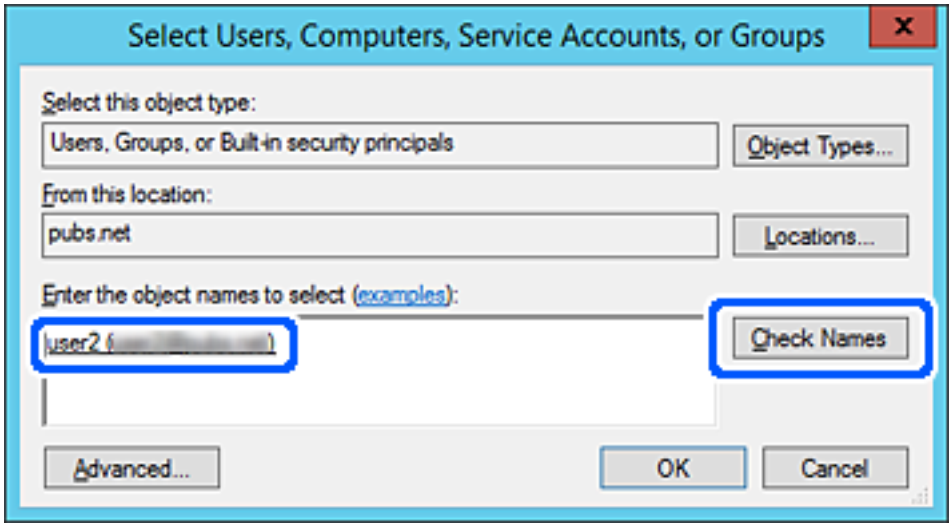


5. Въведете името на групата или потребителя, на които искате да разрешите достъп, след което щракнете върху **Имена за проверка**.

   Към името е добавено подчертаване.

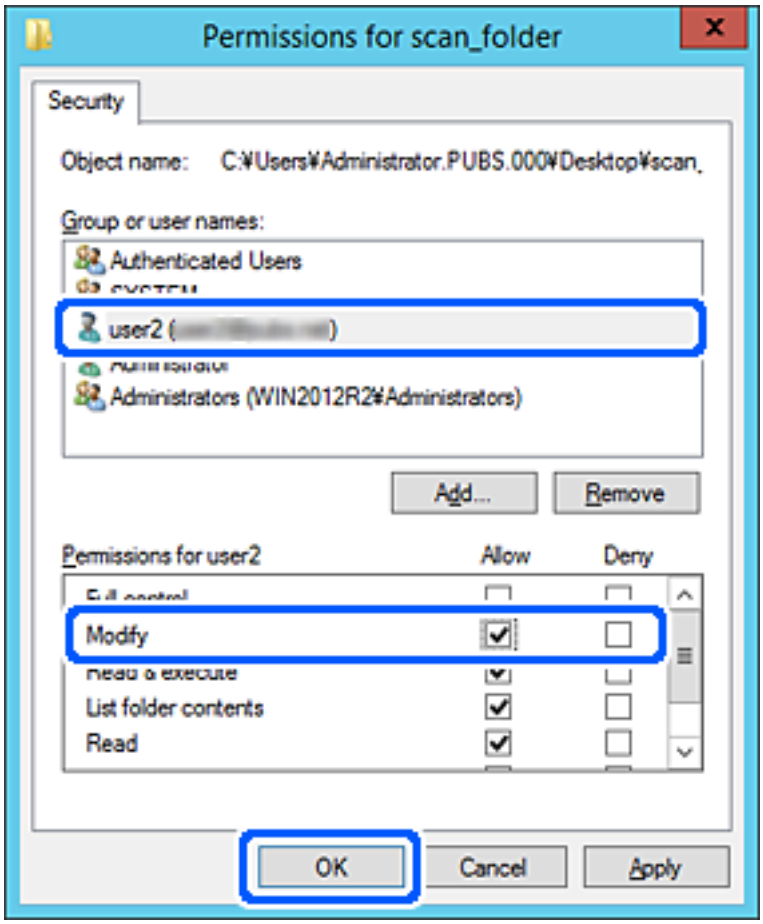
Забележка:
Ако не знаете пълното име на групата или потребителя, въведете част от името, след което щракнете върху ***Имена за проверка****. Имената на групата или потребителските имена, които съвпадат с част от името, са описани и след това можете да изберете пълното име от списъка.*

Ако съвпада само едно име, пълното име с подчертаване се извежда във ***Въведете името на обекта за избор****.*



6. Щракнете върху **OK**.

7. В екрана за разрешение изберете потребителското име, което е въведено в **Имена на група или потребители**, изберете разрешението за достъп в **Смяна**, след което щракнете върху **OK**.



8. Щракнете върху **OK** или **Затваряне**, за да затворите екрана.

   Проверете дали файлът може да бъде записан или прочетен на споделената папка от компютрите на потребителите или групите с разрешение за достъп.

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 71

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

Елементи за настройка на местоназначения

Елементи	Настройки и обяснение
Общи настройки	
Name	Въведете име, показвано в контактите, с максимум 30 знака в Unicode (UTF-8). Ако не го посочите, оставете полето празно.
Index Word	Въведете име с 30 или по-малко символа в Unicode (UTF-8) за търсене на контактите в контролния панел на скенера. Ако не го посочите, 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-8), пропускайки „\\". Въведете пътя на мрежата, изведен на екрана за свойства на папката. Вижте следното за подробности относно настройката на пътя на мрежата. "Пример за конфигурация на персонален компютър" на страница 54
User Name	Въведете потребителското име за достъп до мрежова папка с максимум 30 знака в Unicode (UTF-8). Избягвайте обаче да използвате контролни знаци (от 0x00 до 0x1F, 0x7F).
Password	Въведете парола за достъп до мрежова папка с максимум 20 знака в Unicode (UTF-8). Избягвайте обаче да използвате контролни знаци (от 0x00 до 0x1F, 0x7F).
FTP	

Елементи	Настройки и обяснение
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 ASCII (0x20 – 0x7E), като пропускате „ftp://“ или „ftps://“.
User Name	Въведете потребителското име за достъп до FTP сървър с максимум 30 знака в Unicode (UTF-8). Избягвайте обаче да използвате контролни знаци (от 0x00 до 0x1F, 0x7F). Ако сървърът позволява анонимни връзки, въведете потребителско име, като например „Анонимен“ и „FTP“. Ако не го посочите, оставете полето празно.
Password	Въведете парола за достъп до FTP сървър с максимум 20 знака в Unicode (UTF-8). Избягвайте обаче да използвате контролни знаци (от 0x00 до 0x1F, 0x7F). Ако не го посочите, 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 ASCII (0x20 – 0x7E), като пропускате „http://“ или „https://“.
User Name	Въведете потребителско име за достъп до сървър с максимум 30 знака в Unicode (UTF-8). Избягвайте обаче да използвате контролни знаци (от 0x00 до 0x1F, 0x7F). Ако не го посочите, оставете полето празно.
Password	Въведете парола за достъп до сървър с максимум 20 знака в Unicode (UTF-8). Избягвайте обаче да използвате контролни знаци (от 0x00 до 0x1F, 0x7F). Ако не го посочите, 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.

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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.

Елементи	Настройки и обяснение
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.
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.

Елементи	Настройки и обяснение
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.

Употреба на Document Capture Pro Server

Като използвате Document Capture Pro Server, можете да управлявате начина на сортиране, формата на запис и местоназначението за препращане на резултата от сканиране от контролния панел на скенера. Можете да извиквате и да изпълнявате задание, което е било регистрирано преди това на сървъра от контролния панел на скенера.

Инсталирайте го на сървърния компютър.

За повече информация относно Document Capture Pro Server се свържете с Вашия местен офис на Epson.

Задаване на режим на сървър

За да използвате Document Capture Pro Server, го настройте както следва.

1. Влезте в Web Config и изберете раздел **Scan** > **Document Capture Pro**.
2. Изберете **Server Mode** за **Mode**.
3. Въведете адреса на сървъра с Document Capture Pro Server, инсталиран на него, в **Server Address**.

   Въведете между 2 и 255 знака във формат IPv4, IPv6, име на хост или FQDN. За формат FQDN можете да използвате буквено-цифрени символи в ASCII (0x20 – 0x7E) и „-“, освен в началото и в края на адреса.
4. Щракнете върху **OK**.

   Мрежата се свързва отново, след което настройката се разрешава.

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	Bonjour и AirPrint (Услуга за сканиране) са активирани.

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 **Системни предпочитания** > **Мрежа** > **Разширени** > **Проксита**, след което регистрирайте локалния адрес за **Заобикаляне на прокси настройки за тези хостове и домейни**.

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.

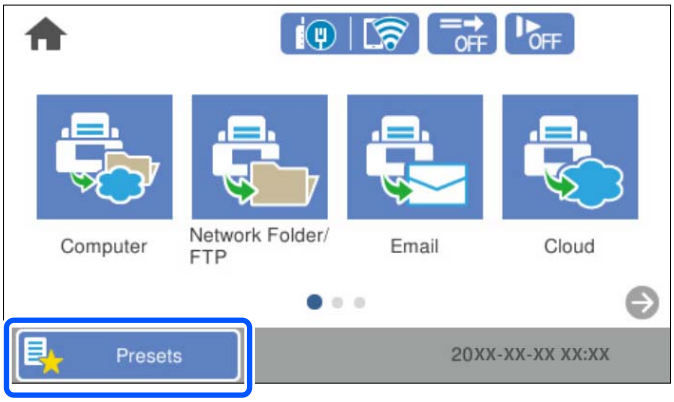
Можете да регистрирате често използвана настройка за сканиране като **Предв.настр.**. Можете да регистрирате до 48 предварителни настройки.

Забележка:

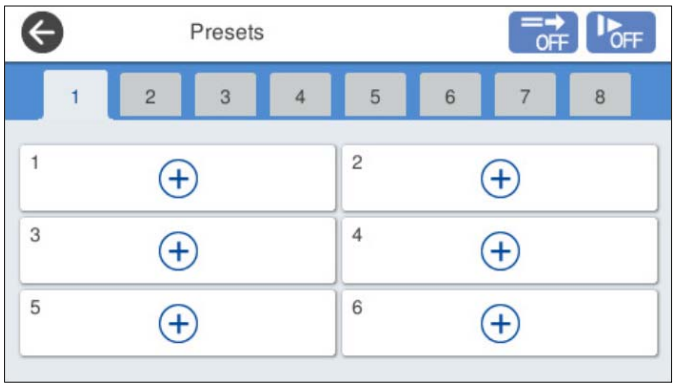
- *Можете да регистрирате текущите настройки чрез избиране на* ☆ *на екрана за стартиране на сканиране.*
- *Можете също да регистрирате **Presets** в Web Config.*

  *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**.*

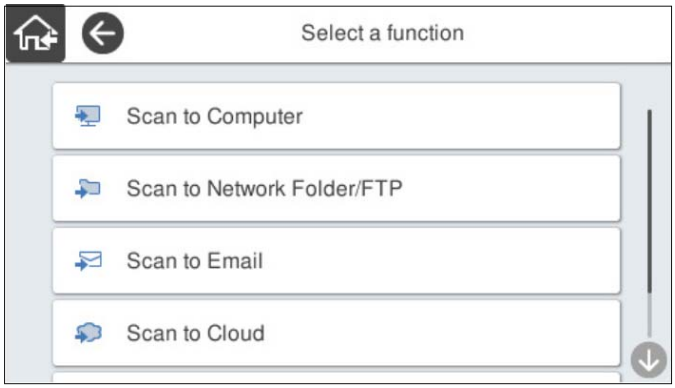
1. Изберете **Предв.настр.** на началния екран от контролния панел на скенера.



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.

  Когато използвате Document Capture Pro Server, дори да сте задали софтуера за потвърждаване на съдържание на задание преди сканиране, **Настройка Бързо изпращане** на предварителната настройка на скенера има приоритет над софтуера.
- ❏ **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 82

❏ 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 82

❏ Отстраняване на икона: премахва икони от началния екран.

"Отстраняване на икона" на страница 83

❏ Преместване на икона: променя реда на показване на иконите.

"Преместване на икона" на страница 84

❏ Възст. показване икони по подразб.: възстановява настройките за извеждане по подразбиране за началния екран.

❏ Тапет: променя цвета на тапета на началния екран.

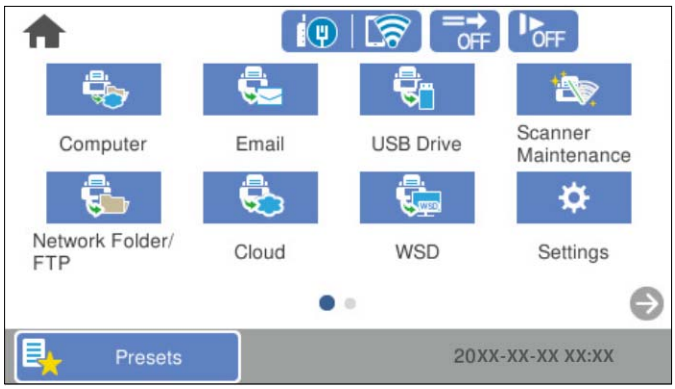
Промяна на Оформление на началния екран

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

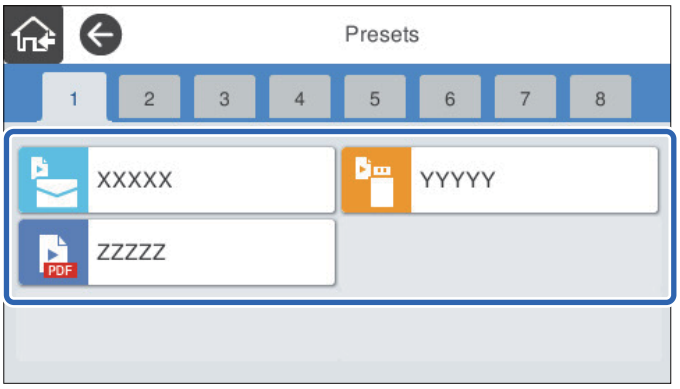
1. Изберете **Настройки** > **Редактиране Нач. екран** > **Добавяне на икона** от контролния панел на скенера.

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

   ❏ Функция: извежда функциите по подразбиране на началния екран.

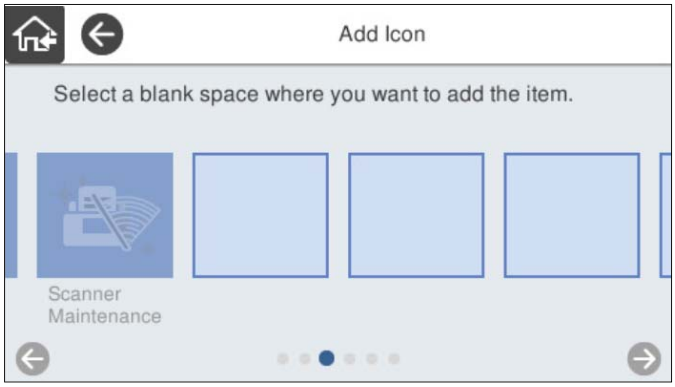
❏ Предв.настр.: извежда регистрираните предварителни настройки.

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.

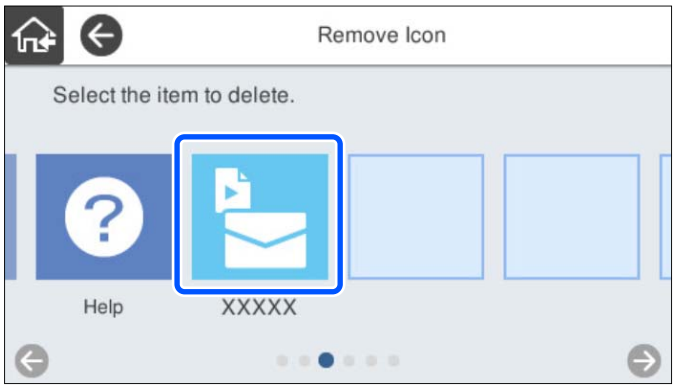


5. Изберете за връщане и проверка на началния екран.

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.

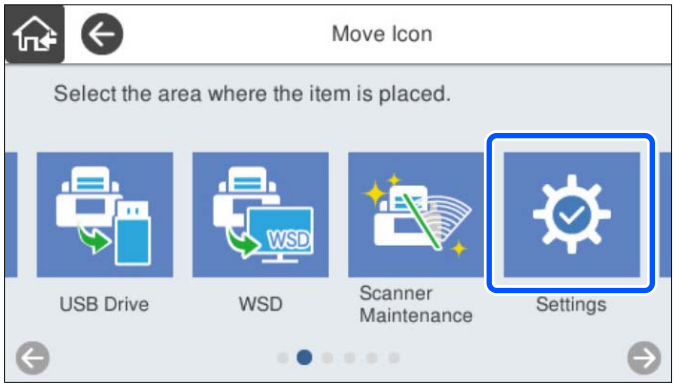
   Ако желаете да премахнете повече икони, повторете процедура 2 до 3.

4. Изберете за връщане и проверка на началния екран.

Преместване на икона

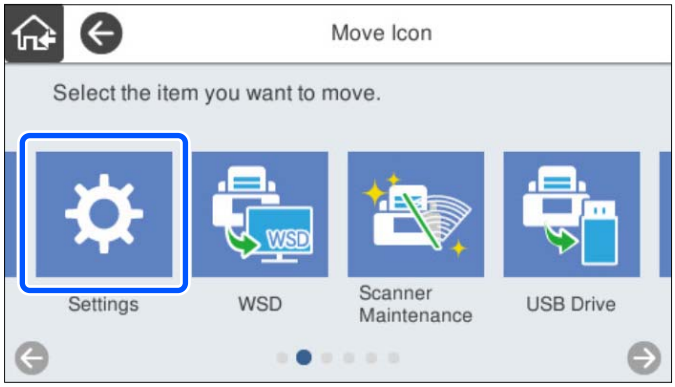
1. Изберете **Настройки** > **Редактиране Нач. екран** > **Преместване на икона** от контролния панел на скенера.

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
Настройка за 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.
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 87
➡ “Дезактивиране на външния интерфейс” на страница 93

Настройки на администратора

Конфигуриране на парола на администратора

Когато зададете паролата на администратор, Вие можете да предотвратите потребителите да променят настройките за управление на системата. Стойностите по подразбиране се задават в момента на покупката. Променете ги, ако е необходимо.

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

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

❏ *Парола: серийният номер на скенера*

За да видите серийния номер, проверете етикета на задната страна на скенера.

Можете да промените паролата на администратора чрез 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 администраторска парола с Web Config

Сменете паролата на администратора в Web Config.

1. Влезте в Web Config и изберете раздел **Product Security** > **Change Administrator Password**.

2. Въведете необходимата информация в **Current password**, **User Name**, **New Password** и **Confirm New Password**.

   Въведете поне един знак за новата парола.

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

   ❏ *Потребителско име: няма (празно)*

   ❏ *Парола: серийният номер на скенера*

   За да видите серийния номер, проверете етикета на задната страна на скенера.

   > ***Важно:***
   > *Не забравяйте да запомните администраторската парола, която сте задали. Ако забравите паролата си, няма да можете да я зададете отново и ще трябва да поискате помощ от сервизен персонал.*

3. Изберете **OK**.

Още по темата

➡ "Пускане на Web Config в уеб браузър" на страница 37

Промяна на администраторската парола от контролния панел

Можете да промените паролата на администратора 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 настоящата парола.

   Забележка:
   Настройката в момента на покупката (стойност по подразбиране) за администраторска парола е серийният номер на скенера.

   За да видите серийния номер, проверете етикета на задната страна на скенера.

5. Въведете новата си парола.

   Въведете поне един знак.

> ***Важно:***
>
> *Не забравяйте да запомните администраторската парола, която сте задали. Ако забравите паролата си, няма да можете да я зададете отново и ще трябва да поискате помощ от сервизен 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.

Забележка:
Ако активирате Authentication Settings на скенера, Заключване на настройка също се активира на контролния панел. Контролният панел не може да бъде отключен, когато Authentication Settings са активирани.

Дори ако дезактивирате Authentication Settings, Заключване на настройка остава активирана. Ако искате да я дезактивирате, можете да направите настройки от контролния панел или Web Config.

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

Елементи на Заключване на настройка в менюто Настройки

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

✓: да бъде заключено.

– : да не бъде заключено.

Меню Настройки		**Заключване на настройка**
Осн. Настройки		–
	Яркост на LCD	–
	Звуци	–
	Таймер за сън	✓
	Таймер за изключване	✓
	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	✓
	Директно вкл.	✓
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.	✓
	Тапет	✓
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		✓
	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.		–
	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			✓
	Настр. предупр. за бр.		✓
Настройки за предупреждение за редовно почистване			✓

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

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

Влизане като администратор от контролния панел

Можете да използвате някой от следните методи, за да влезете като администратор от контролния панел на скенера.

1. Докоснете в горния десен ъгъл на екрана.
   - ❏ Когато Authentication Settings са активирани, иконата се показва на екрана **Добре дошли** (екран за готовност за удостоверяване).
   - ❏ Когато Authentication Settings са дезактивирани, иконата се извежда на началния екран.
2. Докоснете **Да**, когато се изведе екранът за потвърждение.
3. Въведете паролата на администратора.

   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 началния екран.

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ "Конфигуриране на сървър за електронна поща" на страница 43

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

Елементи за имейл известие

Елементи	Настройки и обяснение
Administrator password changed	Известие, когато паролата на администратора е сменена.

Елементи	Настройки и обяснение
Scanner error	Известие при възникване на грешка на скенера.
Грешка на Wi-Fi	Известие при възникване на грешка на безжичния LAN интерфейс.

Решаване на проблеми

Забравена администраторска парола

Имате нужда от помощ от персонал по обслужване. Свържете се с местния търговец.

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

❏ *Потребителско име: няма (празно)*

❏ *Парола: серийният номер на скенера*

За да видите серийния номер, проверете етикета на задната страна на скенера. Ако възстановите настройките по подразбиране за паролата на администратора, тя се нулира до първоначалните стойности.

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 99
➡ “SSL/TLS комуникация със скенера” на страница 108
➡ “Криптирана комуникация с IPsec/IP филтриране” на страница 109
➡ “Свързване на скенера към мрежа IEEE802.1X” на страница 120

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

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 103
➡ "Актуализиране на самоподписан сертификат" на страница 106
➡ "Конфигуриране на CA Certificate" на страница 107

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

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

➡ “Пускане на Web Config в уеб браузър” на страница 37
➡ “Конфигуриране на CA-signed Certificate” на страница 103
➡ “Конфигуриране на CA Certificate” на страница 107

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ “Пускане на Web Config в уеб браузър” на страница 37
➡ “Конфигуриране на CA-signed Certificate” на страница 103
➡ “Конфигуриране на CA Certificate” на страница 107

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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.	
Certificate Validation	Можете да зададете удостоверяване на сертификат независимо от метода на удостоверяване. Импортирайте сертификата в **CA Certificate**.	

Елементи	Настройки и обяснение	
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

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

➡ “Криптирана комуникация с IPsec/IP филтриране” на страница 109

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 109

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

➡ “Пускане на Web Config в уеб браузър” на страница 37

➡ “Криптирана комуникация с IPsec/IP филтриране” на страница 109

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 109

Няма достъп до скенера 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.

Свържете скенера и компютъра и след това конфигурирайте отново IEEE 802.1X.

Още по темата

➡ “Конфигуриране на мрежа IEEE802.1X” на страница 120

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 104

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 106

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 103

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 102

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.

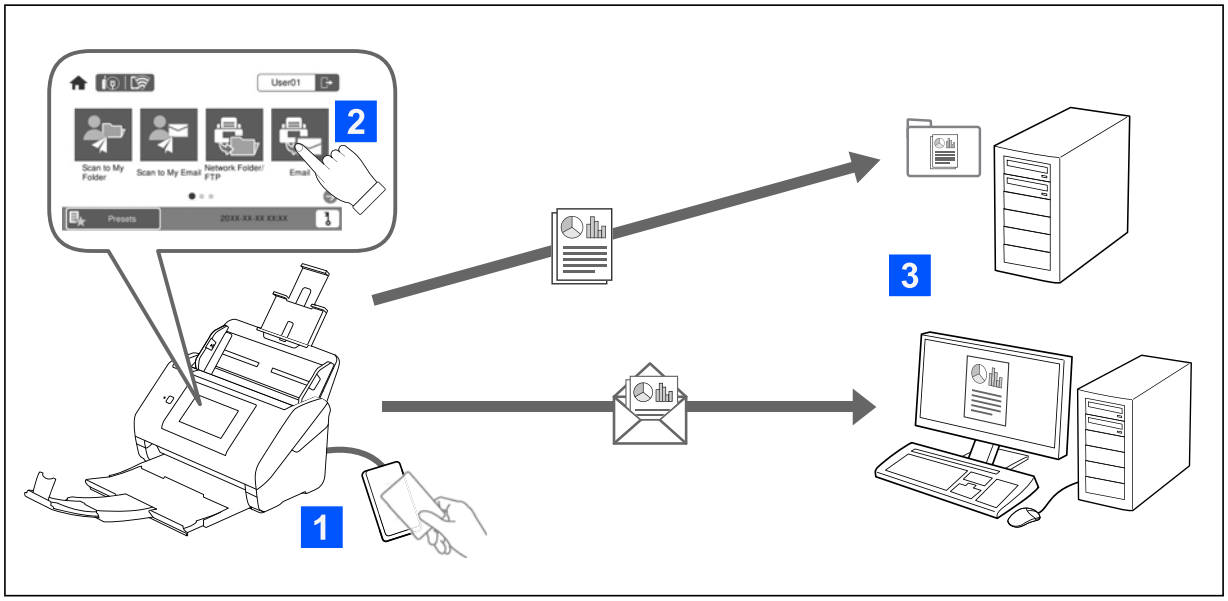
Още по темата

➡ “Импортиране на подписан от сертифициращ орган сертификат” на страница 104

➡ “Изтриване на сертификат, подписан от сертифициращ орган” на страница 106

Authentication Settings

Относно Authentication Settings



Когато Authentication Settings са активирани, се изисква удостоверяване на потребителя, за да започне сканирането. Можете да зададете методите за сканиране, които могат да се използват от всеки потребител, и да предотвратите случайни операции.

Можете да посочите имейл адреса на удостоверения потребител като местоназначение за сканиране (Scan to My Email) или да запаметите данните на всеки потребител в лична папка (Scan to My Folder). Можете също да посочите други методи за сканиране.

Забележка:

❏ *Не можете да сканирате от компютър или смарт устройство, когато са активирани Authentication Settings.*

❏ *В допълнение към Authentication Settings, представени в настоящото ръководство, можете да изградите и система за удостоверяване с помощта на сървър за удостоверяване. За изграждане на система използвайте Document Capture Pro Server Authentication Edition (съкратеното име е Document Capture Pro Server AE). За допълнителна информация се свържете с Вашия местен офис на Epson.*

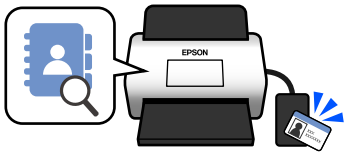
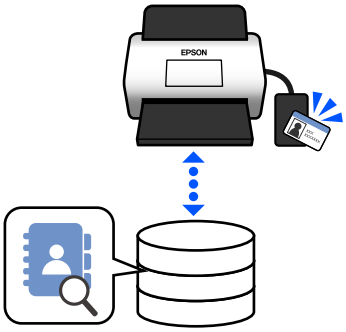
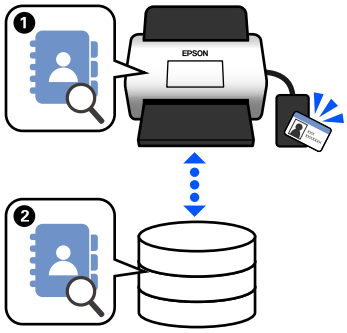
Налични функции за Authentication Settings

Функции за сканиране на контролния панел	Authentication Settings	
	Когато са активирани	Когато са дезактивирани
Сканир. в Моята папка Записва изображения в папката, назначена за удостоверения потребител.	✓	–
Сканиране в Моя имейл Изпраща изображения в имейл адреса на удостоверения потребител.	✓	–
Сканиране към мрежова папка/FTP Записва изображения в папка в мрежата.	✓	✓

Функции за сканиране на контролния панел	Authentication Settings	
	Когато са активирани	Когато са дезактивирани
Сканиране на компютър Записва изображения в свързан компютър с помощта на задания, създадени в Document Capture Pro (Windows)/Document Capture (Mac OS). * Когато Authentication Settings са активирани, можете да използвате само задания, регистрирани в **Предв.настр.**.	✓*	✓
Сканиране към имейл Изпраща изображения на имейл адреса, който сте задали.	✓	✓
Сканиране в облак Изпраща изображения в облака, който сте задали.	✓	✓
Сканиране в USB памет Записва изображения на USB устройство, свързано към скенера. Тази опция е налична само когато към скенера няма свързано устройство за удостоверяване.	✓	✓
Сканиране към WSD Записва изображения на свързан компютър с помощта на функцията WSD.	–	✓
Предв.настр. Можете да регистрирате до 48 предварително зададени функции за сканиране. Можете да разпределите до пет Предв.настр. на потребители, регистрирани в Local DB. Разпределените Предв.настр. са достъпни само за този потребител. Предв.настр., които не са разпределени на нито един потребител, могат да се използват от всички потребители.	✓	✓

Относно Authentication Method

Този скенер може да осигури удостоверяване със следните методи, без да се налага да се създава сървър за удостоверяване.

	Local DB	LDAP	Local DB and LDAP
Местоположение на потребителска информация	**Памет на скенера** Този метод за удостоверяване проверява потребителската информация, регистрирана в скенера, и я сравнява с потребителя, който използва функцията за сканиране.	**LDAP сървър*** Този метод за удостоверяване проверява потребителската информация на LDAP сървъра, синхронизиран със скенера. Тъй като до 300 елемента потребителска информация от LDAP сървъра могат временно да бъдат съхранени в скенера като кеш, удостоверяването може да се извърши с помощта на кеша, ако LDAP сървърът не сработи. * Сървър, който предоставя услуга с директории, която може да комуникира с LDAP.	**Памет на скенера и LDAP сървър** Първо проверете потребителската информация, регистрирана в скенера (❶), и ако няма съвпадение, проверете потребителската информация спрямо LDAP сървъра (❷).
			
Брой регистрирани потребители	50 (памет на скенера)	Неограничен (LDAP сървър)	50 (памет на скенера) Неограничен (LDAP сървър)
Кеш памет на скенера	–	300	Макс. 300 (50 от слотовете за кеш памет се споделят с User Settings в Local DB)
Методи за влизане	Можете да използвате някой от следните методи. ❏ Поддържайте карта за удостоверяване или въведете **User ID** и **Password** ❏ Поддържайте карта за удостоверяване или въведете **ID Number** ❏ Въведете **User ID** и **Password** ❏ Въведете **User ID** ❏ Въведете **ID Number**		
Ограничения на функцията „Сканиране към“	Задайте индивидуално за всеки потребител	Едни и същи настройки за всички LDAP потребители	Local DB потребители: индивидуално задаване LDAP потребители: едни и същи настройки за всички потребители

	Local DB	LDAP	Local DB and LDAP
Разпределяне на Предв.настр. на потребители	До 5 за всеки потребител	– (Не може да се задава индивидуално)	Local DB потребители: до 5 за всеки потребител LDAP потребители: –

Софтуер за настройка

Настройте с помощта на Web Config или Epson Device Admin.

❏ Когато използвате Web Config, можете да настроите скенера само с помощта на уеб браузър.

"Web Config" на страница 37

❏ Когато използвате Epson Device Admin, можете да настроите няколко скенера наведнъж с помощта на шаблон за конфигуриране.

"Epson Device Admin" на страница 38

Актуализиране на фърмуера на скенера

Преди да активирате Authentication Settings, актуализирайте фърмуера на скенера до най-новата версия. Свържете предварително скенера с интернет.

Важно:

Не изключвайте компютъра или скенера, докато актуализирате.

При настройка от Web Config:

Изберете раздела **Device Management** > **Firmware Update**, след което следвайте инструкциите на екрана, за да актуализирате фърмуера.

При настройка от Epson Device Admin:

Изберете **Home** > **Firmware** > **Update** на екрана със списъка с устройства и след това следвайте инструкциите на екрана, за да актуализирате фърмуера.

Забележка:

Ако най-новият фърмуер вече е инсталиран, не е необходимо да актуализирате.

Свързване и конфигуриране на устройство за удостоверяване

Ако искате да свържете и използвате устройство за удостоверяване като четец на IC карти, първо трябва да конфигурирате устройството. Това не е необходимо, ако не използвате устройство за удостоверяване.

Още по темата

➡ “Свързване на устройство за удостоверяване” на страница 136

➡ “Настройки на устройството за удостоверяване” на страница 137

Списък на съвместими с четец на карти

Този списък не гарантира операции за четците на карти в списъка.

Да: поддържа се (идентификационната информация може да се чете със стандартни настройки на четеца на карти.)

Не: не е съвместим

Производител	Модел	Номер на модела	Карта за удостоверяване							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Да	Да*1	Да*1	Да*1	Не	Не	Не	Клавиатура
RF IDEAS	pcProx	RDR-7081BKU	Да*1	Не	Да	Да	Не	Не	Не	Клавиатура
RF IDEAS	pcProx	RDR-7581AKU	Да	Не	Да*1	Да*1	Не	Не	Не	Клавиатура
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Не	Не	Да	Да	Не	Не	Не	Клавиатура
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Да	Не	Да	Да	Да	Да	Да	Клавиатура
ELATEC	TWN4 MULTITECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Да	Да	Да	Да	Да	Да	Да	Клавиатура

Производител	Модел	Номер на модела	Карта за удостоверяване							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ELATEC	TWN4 MultiTech 2 BLE-PI	T4LK-FB4BLZ-PI	Да	Да	Да	Да	Да	Да	Да	Клавиатура
ELATEC	TWN4 Slim	T4QC-FC3B7	Да	Да	Да	Да	Да	Да	Да	Клавиатура
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Да	Да	Да	Да	Да	Не	Да	Клавиатура[*1]
ACS	ACR122U	ACR122U	Не	Не	Да[*2]	Да[*2]	Да	Не	Да[*2]	PC/SC
ACS	ACR1252	ACR1252	Не	Не	Да[*2]	Да[*2]	Да	Да	Да[*2]	PC/SC
Sony	PaSoRi	RC-S330/S	Не	Не	Да[*2]	Да[*2]	Да[*2]	Да[*2]	Да[*2]	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Не	Не	Да[*2]	Да[*2]	Да[*2]	Да[*2]	Да[*2]	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Да	Да	Да	Да	Да	Да	Да	Клавиатура
DMZ	Leitor RFID Multi-125	DMZ087	Не	Да	Не	Не	Не	Не	Не	Клавиатура
DMZ	Leitor RFID Mifare	DMZ088	Не	Не	Да	Да	Не	Не	Не	Клавиатура
DMZ	Biometric & RFID Reader	DMZ073	Не	Да	Не	Не	Не	Не	Не	Клавиатура

Производител	Модел	Номер на модела	Карта за удостоверяване							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
inepro	SCR708	SCR708	Да*1	Да*1	Да*1	Да*1	Да*1	Да*1	Да*1	Клавиатура
Y Soft	YU03088 001	MU0388	Да	Да	Да	Да	Да	Да	Да	Клавиатура
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Не	Не	Да	Да	Не	Не	Да	Клавиатура
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Не	Не	Да	Да	Не	Не	Да	Клавиатура
NT-ware	MiCard MultiTech4-PI	T4DT-FB4WUF-PI	Да	Да	Да	Да	Да	Да	Да	Клавиатура
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Да*1	Да*1	Да*1	Да*1	Не	Не	Не	Клавиатура
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Да	Да	Да	Да	Да	Да	Не	Клавиатура

*1 Трябва да промените настройките на четеца на карти, като използвате собствения софтуер, предоставен от производителя на четеца на карти.

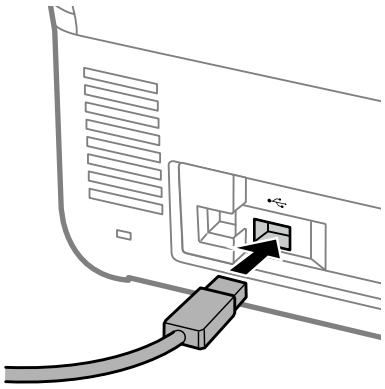
*2 Ако трябва да използвате данни в определена област на картата, различна от стандартния идентификатор на картата като идентификатор за удостоверяване, като конфигурирате настройките на продукта, моля, свържете се с Вашия партньор на Epson или местен представител за повече информация относно начина за настройка на продукта.

Свързване на устройство 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**.

Настройки на устройството за удостоверяване

Задайте формата за четене на информацията за удостоверяване, получена от карта за удостоверяване.

Можете да зададете следния метод за четене за устройството за удостоверяване.

❏ Прочетете конкретната област на картата за удостоверяване, като например номер на служител или личен идентификационен номер.

❏ Използвайте информацията на картата за удостоверяване с изключение на UID (информация на картата за удостоверяване, като серийния номер.)

Можете да използвате инструмент за генериране на работни параметри. Попитайте Вашия дилър за подробности.

Забележка:
Използване на карти за удостоверяване от различни производители:

Когато използвате UID информация за карта (информация за идентификатор на картата, като серийния номер), можете да използвате комбинация от различни типове карти за удостоверяване. Те не могат да се смесват, когато се използва друга информация за картата.

При настройка от Web Config:

Изберете раздел **Device Management** > **Card Reader**.

При настройка от Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Card Reader** от шаблона за конфигуриране.

Елемент	Разяснение
Vendor ID	Задайте идентификатора на доставчика на устройството за удостоверяване, който ограничава употребата от 0000 до FFFF, като използвате 4 буквено-цифрови знака. Ако не искате да я ограничавате, въведете 0000.

Елемент	Разяснение
Product ID	Задайте продуктовия идентификатор на устройството за удостоверяване, който ограничава употребата от 0000 до FFFF, като използвате 4 буквено-цифрови знака. Ако не искате да я ограничавате, въведете 0000.
Operational parameter	Задайте оперативния параметър на устройството за удостоверяване между 0 и 8192 знака. Налични са A~Z, a~z, 0~9, +, /, =, интервал и подаване на нов ред.
Card Reader	Изберете формат за преобразуване за устройство за удостоверяване. Можете да проверите подробностите за формата. Вижте връзката, предоставена в описанието на елемента.
Authentication Card ID save format	Изберете формат за преобразуване за информация за удостоверяване на ID картата. Можете да проверите подробностите за формата. Вижте връзката, предоставена в описанието на елемента.
Set card ID range	Активирайте спецификацията на позицията за четене.
Text Start Position	Посочете началната позиция на текста за четене на идентификационната информация. Можете да посочите между 1 и 4096.
Number of Characters	Посочете броя на знаците, които да бъдат прочетени от началната позиция на идентификационната информация. Можете да посочите между 1 и 4096.

Информация за регистриране и настройка

Настройка

Направете необходимите настройки в зависимост от Authentication Method и метода на сканиране, който използвате.

Важно:

Преди да започнете настройката, проверете дали настройката на времето за скенера е правилна.

Ако настройката на времето е неправилна, се показва съобщението за грешка „Лицензът е изтекъл“, което може да доведе до неуспешна настройка на скенера. Също така, за да използвате функция за сигурност, като SSL/TLS комуникация или IPsec, трябва да бъде настроено правилното време. Можете да настроите времето по следния начин.

- *Web Config: раздел **Device Management** > **Date and Time** > **Date and Time**.*
- *Контролен панел на скенера: **Настройки** > **Осн. Настройки** > **Настройки на дата/час**.*

Настройки	Local DB	LDAP	Local DB and LDAP
Активиране на удостоверяване Преди да направите настройки за удостоверяване, трябва да активирате удостоверяването. “Активиране на удостоверяване” на страница 139	✓	✓	✓

Настройки	Local DB	LDAP	Local DB and LDAP
Authentication Settings Задаване на Authentication Method и начин на удостоверяване на потребителя. "Authentication Settings" на страница 140	✓	✓	✓
Регистриране на User Settings Регистрирайте настройките за всеки потребител. Можете също да регистрирате потребители групово, като използвате CSV файл. "Регистриране на User Settings" на страница 141	✓	–	✓
Синхронизиране с LDAP Server Извършете настройките за синхронизиране на LDAP сървъра. "Синхронизиране с LDAP Server" на страница 148	–	✓	✓
Настройка на Email Server Задайте настройките на сървъра на електронната поща. Задайте това, когато използвате функции, които изискват настройки на сървъра на електронната поща, като например Scan to My Email. "Настройка на сървъра на електронната поща" на страница 152	✓	✓	✓
Настройка Scan to My Folder Задайте папките на местоназначение. Настройте това, когато използвате функцията Scan to My Folder. "Настройка Scan to My Folder" на страница 153	✓	✓	✓
Customize One-touch Functions Настройте това, когато променяте елементите, показани на контролния панел на скенера. На контролния панел можете да покажете само иконите, от които се нуждаете, или да промените реда на иконите. "Customize One-touch Functions" на страница 155	✓	✓	✓

Активиране на удостоверяване

Преди да направите настройки за удостоверяване, трябва да активирате удостоверяването.

При настройка от Web Config:

Изберете **Вкл. (Устройство/LDAP сървър)** от раздела **Product Security** > **Basic** > **Authentication**.

При настройка от Epson Device Admin:

В шаблона за конфигуриране изберете **Вкл. (Устройство/LDAP сървър)** от **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Забележка:
Ако активирате Authentication Settings на скенера, Заключване на настройка също се активира на контролния панел. Контролният панел не може да бъде отключен, когато Authentication Settings са активирани.

Дори ако дезактивирате Authentication Settings, Заключване на настройка остава активирана. Ако искате да я дезактивирате, можете да направите настройки от контролния панел или Web Config.

Още по темата

➡ "Настройка на Заключване на настройка от контролния панел" на страница 89

➡ "Настройка Заключване на настройка от Web Config" на страница 89

Authentication Settings

Задаване на Authentication Method и начин на удостоверяване на потребителя.

При настройка от Web Config:

Изберете раздел **Product Security** > **Authentication Settings**.

При настройка от Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Authentication Settings** от шаблона за конфигуриране.

Елемент	Разяснение
Authentication Method	Изберете Authentication Method. ❏ Local DB Удостоверете с помощта на User Settings, регистрирани в скенера. Необходимо е да регистрирате потребителя в скенера. ❏ LDAP Удостоверете с помощта на потребителската информация на LDAP сървъра, синхронизиран със скенера. Трябва да конфигурирате предварително настройките на LDAP сървъра. ❏ Local DB and LDAP Удостоверете с помощта на потребителската информация, регистрирана в скенера или на LDAP сървъра, синхронизиран със скенера. Трябва да регистрирате потребителя в скенера и да настроите LDAP сървъра.

Елемент	Разяснение
How to Authenticate User	Изберете как да удостоверите даден потребител. ❏ Card or User ID and Password Използвайте карта за удостоверяване, за да удостоверите потребители. Можете също да използвате потребителски идентификатор и парола за удостоверяване. ❏ User ID and Password Използвайте потребителски идентификатор и парола, за да удостоверите потребители. Когато изберете тази функция, не можете да използвате карта за удостоверяване. ❏ User ID Използвайте само потребителски идентификатор за удостоверяване на потребителите. Не е нужно да задавате парола. ❏ Card or ID Number Използвайте карта за удостоверяване, за да удостоверите потребители. Можете да използвате и ID Number. ❏ ID Number Използвайте само идентификационен номер за удостоверяване на потребителите.
Allow users to register authentication cards	Активирайте го, ако разрешите на потребителите да регистрират картата за удостоверяване в системата. Ако изберете **LDAP** за **Authentication Method**, не можете да го задавате. За повече информация как потребителите могат да регистрират своите карти за удостоверяване вижте „Регистриране на карта за удостоверяване“ в *Ръководство на потребителя*.
The Minimum Digit Number of ID Number	Изберете минималния брой цифри за идентификационния номер.
Caching for LDAP authenticated users	Когато използвате удостоверяване на LDAP сървър, можете да зададете дали да използвате кеширане за потребителска информация.
Use user information in SMTP authentication	Когато използвате потребителски идентификатор и парола за удостоверяване, можете да зададете дали да използвате потребителска информация за SMTP удостоверяване. Системата използва последния потребителски идентификатор и парола, с които е влизано.
Restrictions for LDAP authenticated users	Ако използвате LDAP, можете да зададете функциите, които са достъпни за потребителя.

Регистриране на User Settings

Регистрирайте User Settings, използвани за удостоверяване. Можете да регистрирате, като използвате един от следните методи.

❏ Регистриране на User Settings една по една (Web Config)

❏ Регистриране на няколко User Settings като партида с помощта на CSV файл (Web Config)

❏ Регистриране на User Settings в няколко скенера като партида с помощта на шаблон за конфигуриране (Epson Device Admin)

Още по темата

➡ “Регистриране на User Settings Индивидуално (Web Config)” на страница 142

➡ “Регистриране на няколко User Settings с помощта на CSV файл (Web Config)” на страница 143

➡ "Регистриране на User Settings в няколко скенера като партида (Epson Device Admin)" на страница 146

Регистриране на User Settings Индивидуално (Web Config)

Влезте в Web Config и изберете раздела **Product Security** > **User Settings** > **Add** и след това въведете User Settings.

Елемент	Разяснение
User ID	Въведете потребителския идентификатор, който искате да използвате за удостоверяване в диапазон от 1 до 83 байта, който може да бъде изразен в Unicode (UTF-8). Тъй като потребителският идентификатор не е чувствителен към малки и големи букви, можете да влезете с главни или малки букви.
User name Display	Въведете потребителското име, показано на контролния панел на скенера в рамките на 32 знака, които могат да бъдат изразени Unicode (UTF-16). Можете да оставите това празно.
Password	Въведете паролата, която искате да използвате за удостоверяване, в рамките на 32 знака в ASCII. Паролата различава малки и главни букви. Оставете това празно, ако изберете **User ID** за **How to Authenticate User**.
Authentication Card ID	Въведете идентификационния номер на картата за удостоверяване в рамките на 116 знака в ASCII. Можете да оставите това празно. Когато разрешите **Allow users to register authentication cards** за **Authentication Settings**, регистрираният от потребителите резултат се отразява.
ID Number	Този елемент се показва, когато **Card or ID Number** или **ID Number** е избран в **Authentication Settings** > **How to Authenticate User**. Въведете номер, който попада някъде между номера, зададен в **Authentication Settings** > **The Minimum Digit Number of ID Number** и е до 8 цифри.
Auto Generate	Този елемент се показва, когато **Card or ID Number** или **ID Number** е избран в **Authentication Settings** > **How to Authenticate User**. Щракнете, за да генерирате автоматично идентификационен номер със същия брой цифри, който сте избрали в **The Minimum Digit Number of ID Number**.
Department	Въведете името на отдела и т.н., което идентифицира потребителя в рамките на 40 знака, които могат да бъдат изразени в Unicode (UTF-16). Можете да оставите това празно.
Email Address	Въведете имейл адреса на потребителя в рамките на 200 знака в ASCII. Това се използва като местоназначение за **Scan to My Email**. Можете да оставите това празно.
Scan to My Folder	Когато изберете **Individual** в **Scan to My Folder** > **Setting Type**, задайте местоназначенията за запис индивидуално. Вижте следното за повече информация относно елементите на настройка. "Настройка Scan to My Folder" на страница 153
Restrictions	Можете да ограничите функциите за всеки потребител. Изберете функцията, който позволявате да се използва.

Елемент	Разяснение
Presets	Можете да зададете до пет предварително зададени настройки, които са достъпни само за избрания потребител от Presets, регистрирани в скенера. ❏ Presets, които са разпределени на потребител, могат да се използват само от този потребител. Presets, които не са разпределени на нито един потребител, могат да се използват от всички потребители. ❏ Ако потребителят има само една налична Presets, тя автоматично се зарежда след удостоверяването. Ако са налични няколко Presets, след удостоверяването се извежда списък на Presets. ❏ Не можете да създавате или показвате Presets, която използва функции, които са ограничени в **Restrictions**.

Регистриране на няколко User Settings с помощта на CSV файл (Web Config)

Въведете настройките за всеки потребител в CSV файл и ги регистрирайте като партида.

Създаване на CSV файл

Създайте CSV файл, за да импортирате User Settings.

Забележка:
Ако регистрирате една или повече User Settings предварително и след това експортирате форматиран файл (CSV файл), можете да използвате регистрираната настройка като справка за въвеждане на елементи от настройките.

1. Влезте в Web Config и изберете раздел **Product Security** > **User Settings**.
2. Щракнете върху **Export**.
3. Изберете файловия формат за **File Format**.

   Изберете го, като направите справка по-долу.

Елемент	Разяснение
CSV UTF-16 (Tab delimited)	Изберете, когато редактирате файла с помощта на Microsoft Excel. Всеки параметър е затворен с [ ] (квадратни скоби). Въведете параметрите в [ ]. Когато актуализирате файла, препоръчваме да го презапишете. Ако за първи път записвате файла, изберете Unicode text (*.txt) за файловия формат.
CSV UTF-8 (Comma delimited)	Изберете, когато редактирате файла с текстов редактор или макрос без Microsoft Excel.
CSV UTF-8 (Semicolon delimited)	

4. Щракнете върху **Export**.

5. Редактирайте и запазете този CSV файл в приложение за електронни таблици, като например Microsoft Excel, или в текстов редактор.

> ***Важно:***
>
> *Когато редактирате файла, не променяйте кодирането и информацията в заглавието.*

Елементи за настройка на CSV файл

Елемент	Настройки и обяснение
UserID	Въведете потребителския идентификатор, за да използвате удостоверяване между 1 и 83 байта в Unicode.
UserName	Въведете потребителското име, показано на контролния панел на скенера в рамките на 32 знака в Unicode. Можете да оставите това празно.
Password	Въведете паролата, която ще използвате за удостоверяване в рамките на 32 знака в ASCII. При импортиране тя се задава като парола вместо **EncPassword**. Оставете това празно, ако изберете **User ID** за **How to Authenticate User**. Когато експортирате, това винаги е празно.
AuthenticationCardID	Задайте резултата от четенето на картата за удостоверяване. Когато разрешите **Allow users to register authentication cards** в **Authentication Settings**, регистрираният от потребителите резултат се отразява. Въведете до 116 знака в ASCII. Можете да оставите това празно.
IDNumber	Този елемент се показва, когато **Card or ID Number** или **ID Number** е избран в **Authentication Settings** > **How to Authenticate User**. Въведете номер, който попада някъде между номера, зададен в **Authentication Settings** > **The Minimum Digit Number of ID Number** и е до 8 цифри. Идентификационният номер не може да бъде дублиран. Ако е дублиран, ще бъдете предупредени за грешката при импортиране на файла. Когато се остави празен, автоматично се присвоява номер.
Department	Въведете името на отдела произволно, за да разграничите потребителите. Въведете в рамките на 40 знака в Unicode. Можете да оставите това празно.
MailAddress	Задайте имейл адреса за потребителите. Това се използва като местоназначение за **Scan to My Email**. Можете да използвате A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Въведете 200 знака или по-малко. Не можете да използвате „,“ (запетая) като първи знак. Можете да оставите това празно.
FolderProtocol	Задайте типа на функцията Scan to My Folder. Мрежова папка/FTP (SMB): 0, FTP: 1
FolderPath	Задайте местоназначението за запис за функцията Scan to My Folder.
FolderUserName	Задайте потребителско име за функцията Scan to My Folder.
FolderPassword	Задайте парола за удостоверяване на папката на местоназначение за функцията Scan to My Folder в рамките на 32 ASCII знака. При импортиране тя се задава като парола вместо **EncPassword**. Когато експортирате, това винаги е празно.

Елемент	Настройки и обяснение
FtpPassive	Задайте режима на връзка за FTP сървъра, когато **FTP** е избрано като **Type** за функцията Scan to My Folder. Активен режим: 0, Пасивен режим: 1
FtpPort	Задайте номера на порта за изпращане на сканирани данни към FTP сървъра от 0 до 65535, когато **FTP** е избрано като **Type** за функцията Scan to My Folder.
ScanToMemory	Задайте ограниченията за Scan to USB Drive. Не е позволено: 0, Позволено: 1
ScanToMail	Задайте ограниченията за Scan to Email. Можете да зададете **Сканиране в Моя имейл** само когато **Scan to Email** е активирано. Не е позволено: 0, Позволено: 1
ScanToFolder	Задайте ограниченията за Scan to Network Folder/FTP. Можете да зададете **Сканир. в Моята папка** само когато **Scan to Network Folder/FTP** е активирано. Не е позволено: 0, Позволено: 1
ScanToCloud	Задайте ограниченията за Scan to Cloud. Не е позволено: 0, Позволено: 1
ScanToComputer	Задайте ограниченията за Сканиране на компютър. Не е позволено: 0, Позволено: 1
PresetIndex	Задайте Presets, които искате да свържете с потребителя. Можете да зададете до пет регистрационни номера на Presets, разделени със запетая.
EncPassword	Когато експортирате потребителски настройки, параметърът, зададен за **Password**, е криптиран, тогава стойността се кодира от BASE64 и се извежда. При импортиране с новата парола за **Password** тази стойност се игнорира. Ако **Password** е празна, тази стойност се използва и паролата остава, както е била преди експортирането.
EncFolderPassword	Когато експортирането на параметъра, зададен за **FolderPassword**, е криптирано, тогава стойността се кодира от BASE64 и се извежда. При импортиране с новата парола за **FolderPassword** тази стойност се игнорира. Ако **FolderPassword** е празна, тази стойност се използва и паролата остава, както е била преди експортирането.

Импортиране на CSV файл

1. Влезте в Web Config и изберете раздел **Product Security** > **User Settings**.
2. Щракнете върху **Import**.
3. Изберете файла, който желаете да импортирате.
4. Щракнете върху **Import**.

5. След като проверите показаната информация, щракнете върху **OK**.

Регистриране на User Settings в няколко скенера като партида (Epson Device Admin)

Можете да регистрирате User Settings, използвани в Local DB като партида с помощта на LDAP сървър или CSV/ENE файл.

Забележка:
ENE файлът е двоичен файл, предоставен от Epson, който криптира и записва информация за ***Contacts****, като лична информация и User Settings. Той може да се експортира от Epson Device Admin и можете да зададете парола. Това е полезно, когато искате да импортирате User Settings от резервен файл.*

Импортиране от CSV/ENE файл

1. Изберете **Administrator Settings** > **Authentication Settings** > **User Settings** от шаблона за конфигуриране.
2. Щракнете върху **Import**.
3. Изберете **CSV or ENE File** от **Import Source**.
4. Щракнете върху **Browse**.

   Показва се екранът за избор на файл.
5. Изберете файла, който искате да импортирате, за да го отворите.
6. Изберете метод на импортиране.
   - ❏ Overwrite and Add: презаписва, ако същият потребителски идентификатор съществува; добавя нов идентификатор, ако не съществува.
   - ❏ Replace All: заменя всичко с потребителските настройки, които искате да импортирате.
7. Щракнете върху **Import**.

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

   Извежда се резултатът от потвърждението.

   Забележка:
   - ❏ *Ако броят на импортираните потребителски настройки надвишава броя, който може да бъде импортиран, съобщение ще Ви подкани да изтриете някои потребителски настройки. Изтрийте всички излишни потребителски настройки, преди да импортирате.*
   - ❏ *Преди импортиране изберете потребителските настройки, които искате да изтриете, след което щракнете върху* ***Delete****.*
9. Щракнете върху **Import**.

   Потребителските настройки се импортират в шаблона за конфигуриране.

Импортиране от LDAP сървър

1. Изберете **Administrator Settings** > **Authentication Settings** > **User Settings** от шаблона за конфигуриране.

2. Щракнете върху **Import**.

3. Изберете **LDAP** от **Import Source**.

4. Щракнете върху **Settings**.

   Показват се настройките на **LDAP Server**.

   Забележка:
   Тази настройка на LDAP сървъра е за импортиране на потребителските настройки от LDAP сървъра. Импортираните (копираните) потребителски настройки се използват за удостоверяване на потребители с помощта на самия скенер.

   *От друга страна, когато изберете **LDAP** или **Local DB and LDAP** като метод за удостоверяване, потребителите се удостоверяват чрез комуникация с LDAP сървъра.*

5. Задайте всеки елемент.

   Когато импортирате потребителски настройки от LDAP сървър, можете да конфигурирате и следните настройки в допълнение към LDAP настройките.

   За други елементи вижте „Свързана информация“.

Елемент			Разяснение
LDAP Server Settings	LDAP Server Type		Позволява Ви да изберете типа LDAP сървър.
Search Settings	Search Filter		Можете да зададете текста, използван за филтъра за търсене на LDAP. Изберете **Custom**, за да редактирате текста за търсене.
	Options	Type	Можете да зададете типа местоназначение за запис за **Scan To My Folder**.
		Connection Mode	Когато **Type** е зададен на **FTP**, можете да зададете режима на FTP връзка.
		Port Number	Когато **Type** е зададен на **FTP**, можете да зададете номера на порта, който искате да използвате.

6. Извършете проверка на връзката, ако е необходимо, като щракнете върху **Connection Test**.

   Получава и показва 10 потребителски настройки от LDAP сървъра.

7. Щракнете върху **OK**.

8. Изберете метод на импортиране.

   ❏ Overwrite and Add: презаписва, ако същият потребителски идентификатор съществува; добавя нов идентификатор, ако не съществува.

   ❏ Replace All: заменя всичко с потребителските настройки, които искате да импортирате.

9. Щракнете върху **Import**.

   Извежда се екранът за потвърждение на настройките.

10. Щракнете върху **OK**.

    Извежда се резултатът от потвърждението.

11. Щракнете върху **Import**.

    Потребителските настройки се импортират в шаблона за конфигуриране.

Още по темата

➡ "Конфигуриране на LDAP сървър" на страница 148
➡ "Конфигуриране на настройките за търсене на LDAP сървъра" на страница 150

Синхронизиране с LDAP Server

Извършете настройки на LDAP Server за скенера.

Направете настройки както за основния сървър, така и за вторичния сървър, ако е необходимо.

Забележка:
*Настройките на **LDAP Server** се споделят с **Contacts**.*

Налични услуги

Поддържат се следните услуги на директории.

Име на услуга	Версия
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Конфигуриране на LDAP сървър

За да използвате LDAP сървър, трябва да конфигурирате LDAP сървър.

При настройка от Web Config:

Изберете раздел **Network** > **LDAP Server** > **Basic (Primary Server)** или **Basic (Secondary Server)**.

Ако изберете **Kerberos Authentication** като **Authentication Method**, изберете **Network** > **Kerberos Settings**, за да извършите настройки за Kerberos.

При настройка от Epson Device Admin:

Изберете **Network** > **LDAP server** > **Server Settings (Primary Server)** или **Server Settings (Secondary Server)** от шаблона за конфигуриране.

Ако изберете **Kerberos Authentication** като **Authentication Method**, изберете **Network — Security** > **Kerberos Settings**, за да извършите настройки за Kerberos.

Елемент	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 тирета освен в началото и края на адреса.
LDAP server Port Number (Port number)	Въведете номера на порта на LDAP сървъра, като използвате стойност между 1 и 65535.
Secure Connection	Посочете метода на удостоверяване за скенера за достъп до LDAP сървъра.
Certificate Validation	Сертификатът на LDAP сървъра се удостоверява, когато това е активирано. Препоръчваме да зададете това 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 секунди.
Authentication Method	Изберете метода на удостоверяване. Ако изберете **Kerberos Authentication**, направете настройки за Kerberos предварително. За да извършите Kerberos Authentication, е необходима следната среда. ❏ Скенерът и DNS сървърът могат да комуникират. ❏ Времето за скенера, KDC сървъра и сървъра, необходимо за удостоверяване (LDAP сървър, SMTP сървър, файлов сървър), се синхронизира. ❏ Когато сървърът на услугата е назначен като IP адрес, FQDN за 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 до 0x1F и 0X7F. Тази настройка не се използва, когато сте избрали **Anonymous Authentication** като **Authentication Method**. Ако не искате да го посочите, 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 до 0x1F и 0X7F. Тази настройка не се използва, когато сте избрали **Anonymous Authentication** като **Authentication Method**. Ако не искате да го посочите, оставете полето празно.

Настройки за Kerberos

Ако изберете **Kerberos Authentication** като **Authentication Method**, трябва да направите настройки за Kerberos. Можете да регистрирате до 10 настройки за Kerberos.

При настройка от Web Config:

Изберете раздел **Network** > **Kerberos Settings**.

При настройка от Epson Device Admin:

Изберете **Network** > **Security** > **Kerberos Settings** от шаблона за конфигуриране.

Елемент	Настройки и обяснение
Realm (Domain)	Въведете областта за удостоверяване с Kerberos, като използвате максимум 255 знака във формат ASCII (0x20 – 0x7E). Ако не искате да 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 искате да го регистрирате, оставете полето празно.
Port Number (Kerberos)	Въведете номера на порта на сървъра за Kerberos, като използвате стойност между 1 и 65535.

Конфигуриране на настройките за търсене на LDAP сървъра

Задава атрибутите за търсене за потребителски настройки.

При настройка от Web Config:

Изберете раздел **Network** > **LDAP Server** > **Search Settings (Authentication)**.

При настройка от Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** от шаблона за конфигуриране.

Елемент	Настройки и обяснение
Search Base (Distinguished Name)	При търсене на потребителска информация от LDAP сървъра посочете началната позиция. 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
User ID Attribute	Посочете името на атрибута, който да се покаже при търсене на идентификационния номер. Въведете между 1 и 255 знака в ASCII. 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 ASCII. Първият знак трябва да е от a – z или A – Z. Можете да оставите този елемент празен. Пример: cn, name
Authentication Card ID Attribute	Посочете името на атрибута, който да се покаже като идентификатор на карта за удостоверяване. Въведете между 0 и 255 знака в ASCII. Първият знак трябва да е от a – z или A – Z. Можете да оставите този елемент празен. Пример: cn, sn
ID Number Attribute	Посочете името на атрибута, който да се покаже при търсене на идентификационния номер. Въведете между 1 и 255 знака в ASCII. Първият знак трябва да е измежду a – z или A – Z. Пример: cn, id
Department Attribute	Посочете името на атрибута, който да се покаже като име на отдела. Въведете между 0 и 255 знака в ASCII. Първият знак трябва да е от a – z или A – Z. Можете да оставите този елемент празен. Пример: ou, ou-cl

Елемент	Настройки и обяснение
Email Address Attribute	Посочете името на атрибута, който да се покаже при търсене на имейл адреси. Въведете между 1 и 255 знака в ASCII. Първият знак трябва да е измежду a – z или A – Z. Пример: mail
Save To Attribute	Посочете името на атрибута, което сочи към местоназначението за Scan To My Folder. Въведете между 0 и 255 знака в ASCII. Пример: homeDirectory

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.

Настройка на сървъра на електронната поща

Когато използвате **Scan to My Email**, задайте сървъра на електронната поща.

Забележка:
*Можете да зададете **Scan to My Email** само когато **Scan to Email** е активирано.*

При настройка от Web Config:

Изберете раздел **Network** > **Email Server** > **Basic**.

При настройка от Epson Device Admin:

Изберете **Common** > **Email Server** > **Mail Server Settings** от шаблона за конфигуриране.

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	Сървърът на електронната поща 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 удостоверения акаунт. Въведете между 0 и 255 знака в ASCII (0x20 – 0x7E).	
Authenticated Password	Ако изберете **SMTP AUTH** или **POP before SMTP** като **Authentication Method**, въведете удостоверената парола. Въведете между 0 и 20 знака в ASCII (0x20 – 0x7E).	
Sender's Email Address	Въведете имейл адреса на подателя. Въведете между 0 и 255 знака в ASCII (0x20 – 0x7E) с изключение на: ( ) < > [ ] ; ¥. Първият знак не може да бъде точка „.“.	
SMTP Server Address	Въведете между 0 и 255 знака с помощта на A – Z, a – z, 0 – 9 . -. Можете да използвате формат IPv4 или FQDN.	
SMTP Server Port Number	Въведете число между 1 и 65535.	
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**.
Certificate Validation	Сертификатът е удостоверен при разрешаването му. Препоръчваме да зададете това 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 с помощта на A – Z, a – z, 0 – 9. Можете да използвате формат IPv4 или FQDN.	
POP3 Server Port Number	Ако изберете **POP before SMTP** като **Authentication Method**, посочете номера на порта. Въведете число между 1 и 65535.	

Настройка Scan to My Folder

Запазва сканираните изображения в папката, присвоена на всеки потребител. Можете да зададете следното като специализирана папка.

Забележка:
*Можете да зададете **Scan To My Folder** само когато **Scan to Network Folder/FTP** е активирано.*

Настройка „Запаметяване в“	Authentication Method	Местоположение за настройка на пътя към папката
Посочете една мрежова папка за всички Authentication Settings за автоматично създаване на лична папка под посочената папка, използвайки името на потребителския идентификатор.	❏ Local DB ❏ LDAP ❏ Local DB and LDAP	Скенер (настройка Scan to My Folder)
Назначете различни мрежови папки индивидуално на всеки потребител.	Local DB	Скенер (User Settings)
	LDAP	LDAP атрибути
	Local DB and LDAP	Скенер (User Settings) или LDAP атрибути

При настройка от Web Config:

Изберете раздел **Product Security** > **Scan to Network Folder/FTP**.

При настройка от Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Scan to Network Folder/FTP** > **Scan to My Folder** от шаблона за конфигуриране.

Елемент		Разяснение
Save To Setting	Setting Type	❏ **Shared**: Автоматично създава папка с името на идентификатора на потребителя под пътя на папката или URL адреса, посочени в **Save to**, и записва сканираните изображения в тази папка. ❏ **Individual**: Задава местоназначението за записване на резултатите от сканирането за всеки потребител. Потребителите на Local DB могат да бъдат зададени в потребителските настройки. Потребителите на LDAP използват местоположението за съхранение, получено от атрибутите за търсене на LDAP сървъра.
	Type	Изберете протокола за предаване според местоназначението на резултата от сканиране. За мрежова папка: **Network Folder (SMB)** За FTP сървър: **FTP**
	Save to	Посочете пътя или URL адреса на изходния път. Въведете в рамките на 160 знака в Unicode (UTF-16).
	Connection Mode	Задайте, когато изберете **FTP** в **Type**. Изберете режим на връзка с FTP сървъра.
	Port Number	Задайте, когато изберете **FTP** в **Type**. Въведете номера на порта за изпращане на сканираните данни към FTP сървър между 0 и 65535.
Authentication Settings	Setting Type	Задайте, когато изберете **Individual** като **Setting Type** в **Save To Setting**. Задайте User Name и Password за достъп до папката. ❏ **Shared**: Използвайте общо **User Name** и **Password** за всички потребители. ❏ **Individual**: За потребители на Local DB задайте **User Name** и **Password** индивидуално в **Потребителски настройки**. Потребителите на LDAP не могат да бъдат индивидуално конфигурирани. **User Name** и **Password**, зададени от този елемент, се използват като партида.
	User Name	Въведете потребителското име за достъп до папката на местоназначение на резултата от сканиране. Въведете в рамките на 30 знака в Unicode (UTF-16). Задайте това, когато използвате **Shared** или LDAP сървър.
	Password	Въведете паролата, съответстваща на **User Name**. Въведете в рамките на 20 знака в Unicode (UTF-16). Задайте това, когато използвате **Shared** или LDAP сървър.

Забрана на промяната на местоназначението за Scan to Network Folder/FTP

Елемент	Разяснение
Prohibit manual entry of destination	Когато е активирано, потребителят не може да промени местоназначението по подразбиране.

Customize One-touch Functions

Можете да покажете само необходимите икони, като редактирате разположението на иконите, показано на началния екран за контролния панел.

При настройка от Web Config:

Изберете раздел **Product Security** > **Customize One-touch Functions**.

При настройка от Epson Device Admin:

Изберете **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** от шаблона за конфигуриране.

Забележка:
В следните случаи иконите за посочените функции не се показват на началния екран.

- ❏ *Когато изберете функции, които не са разрешени поради **Restrictions**.*
- ❏ *Когато имейл адресът на влязъл потребител не е регистриран. (Scan to My Email)*
- ❏ *Когато папката на местоназначение не е зададена. (Scan to My Folder)*

Елемент	Разяснение
Maximum functions per screen	Изберете разположението на иконите, показано на контролния панел. Изображението се променя според избраното разположение.
Screen(s)	Изберете броя на страниците.
Number	Изберете функциите, които искате да показвате за всяка номерирана позиция.

Job History Отчети с помощта на Epson Device Admin

Можете да създадете Job History отчет за всяка група и всеки потребител с помощта на Epson Device Admin. Можете да запишете до 3000 случая на употреба в скенера. Можете да създадете отчета, като посочите период или зададете редовен график.

За да изведете Job History като отчет, изберете **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** от менюто на лентата на екрана със списък с устройства.

За подробности относно създаването на този отчет вижте документацията за Epson Device Admin.

Елементи, които могат да бъдат включени в отчета

Можете да изведете следните елементи в потребителския отчет.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Влизане като администратор от контролния панел

Можете да използвате някой от следните методи, за да влезете като администратор от контролния панел на скенера.

1. Докоснете  в горния десен ъгъл на екрана.
   - ❏ Когато Authentication Settings са активирани, иконата се показва на екрана **Добре дошли** (екран за готовност за удостоверяване).
   - ❏ Когато Authentication Settings са дезактивирани, иконата се извежда на началния екран.
2. Докоснете **Да**, когато се изведе екранът за потвърждение.
3. Въведете паролата на администратора.

   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 началния екран.

Дезактивиране на Authentication Settings

Можете да дезактивирате Authentication Settings чрез Web Config.

Забележка:
User Settings, регистрирани в скенера, ще бъдат запазени дори ако Authentication Settings са дезактивирани. Можете да ги премахнете, като възстановите настройките по подразбиране на скенера.

1. Отидете в Web Config.
2. Изберете раздел **Product Security** > **Basic** > **Authentication**.
3. Изберете **OFF**.
4. Щракнете върху **Next**.
5. Щракнете върху **OK**.

Забележка:
Дори ако дезактивирате Authentication Settings, Заключване на настройка остава активирана. Ако искате да я дезактивирате, можете да направите настройки от контролния панел или Web Config.

Още по темата

➡ "Настройка на Заключване на настройка от контролния панел" на страница 89
➡ "Настройка Заключване на настройка от Web Config" на страница 89

Изтриване на информация за Authentication Settings (възст. на наст. по подразбиране)

За да изтриете цялата информация за Authentication Settings (Card Reader, Authentication Method, User Settings и т. н.), възстановете всички настройки на скенера до настройките по подразбиране към момента на покупката.

Изберете **Настройки** > **Системна администрация** > **възст. на наст. по подразбиране** > **Всички настройки** на контролния панел.

Важно:

Всички контакти и други мрежови настройки също ще бъдат изтрити. Изтритите настройки не могат да се възстановят.

Решаване на проблеми

Картата за удостоверяване не може да се прочете

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 се поддържат.

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 ролката 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.

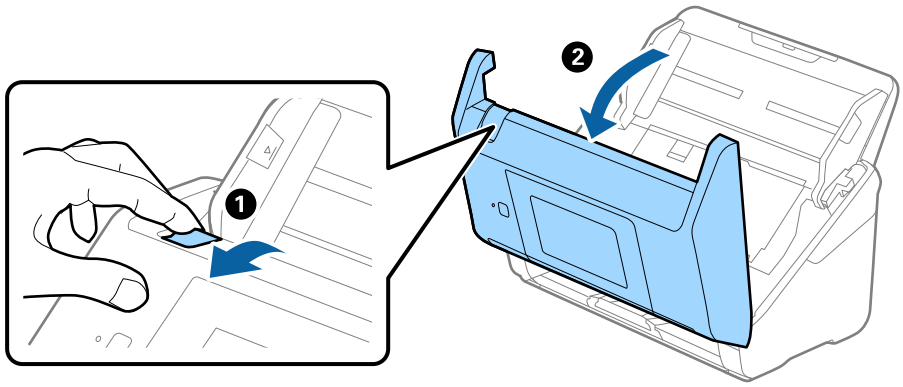
Ако повърхността е замърсена с труден за почистване материал, използвайте оригинален комплект за почистване на Epson за отстраняване на петната. Използвайте малко количество от почистващия препарат върху почистващата кърпа, за да отстраните петната.

Важно:

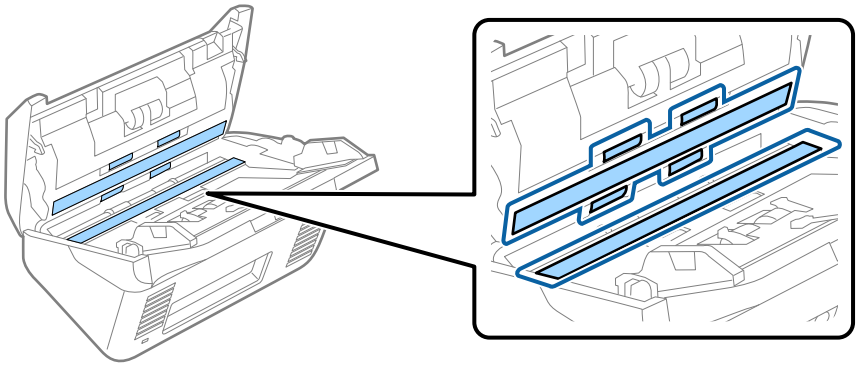
- ❏ *Никога не използвайте алкохол, разредител или какъвто и да било корозивен препарат за почистване на скенера. Може да се получи деформация или обезцветяване.*
- ❏ *Никога не пръскайте каквато и да е течност или смазочно средство върху скенера. При повреда на оборудването или електрическите вериги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

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

3. Дръпнете лоста и отворете капака на скенера.



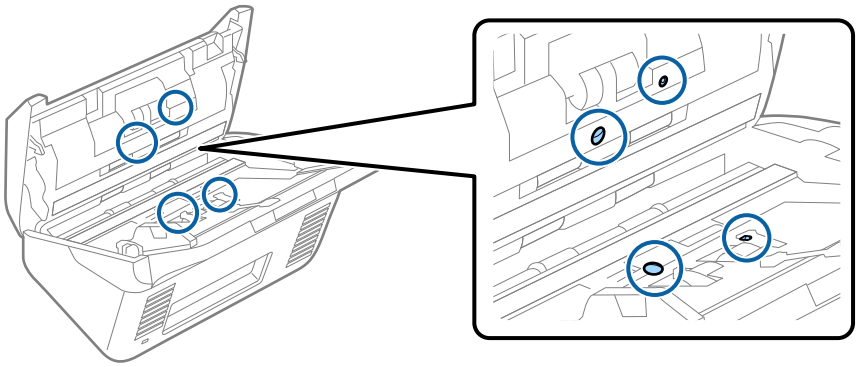
4. Избършете всякакви петна от пластмасовата ролка и стъклената повърхност в долната вътрешна част на капака на скенера, като използвате мека кърпа или оригинален комплект за почистване на Epson.



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.*

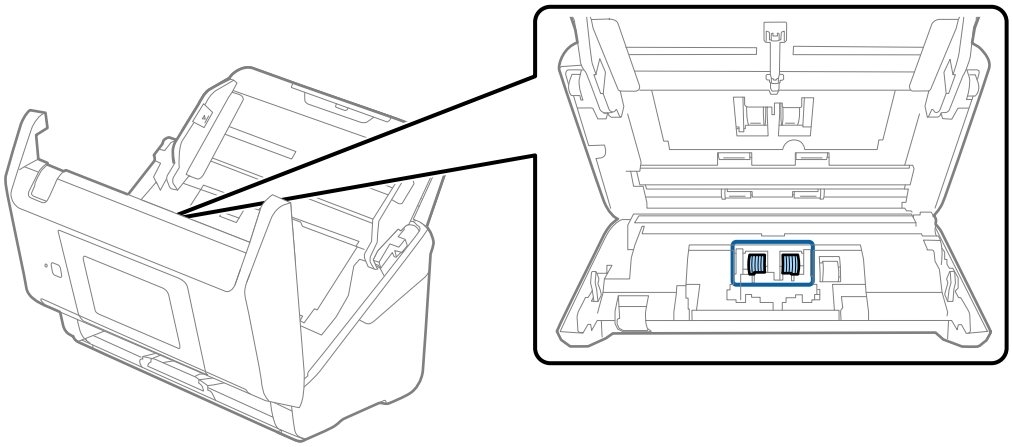
5. Избършете всякакви петна от сензорите с памучен тампон.



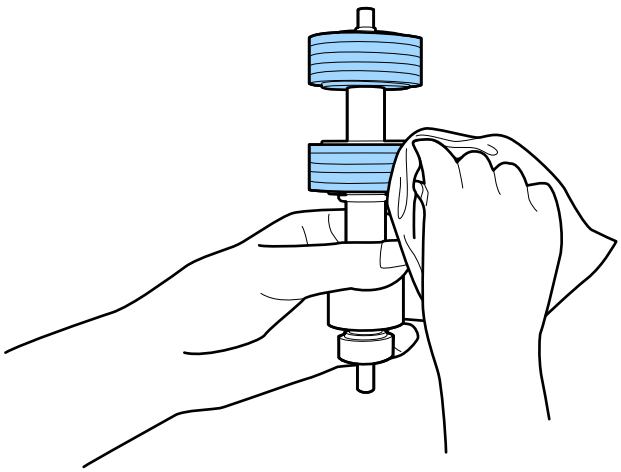
> ***Важно:***
>
> *Не използвайте течност, като например почистващ препарат, върху памучен тампон.*

6. Отворете капака, след което извадете разделителната ролка.

   За повече подробности вижте „Смяна на комплекта ролки“.



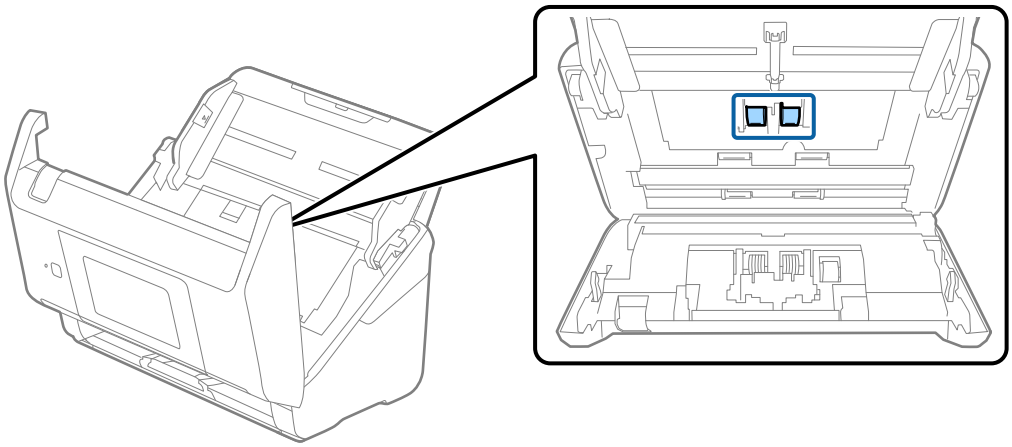
7. Избършете прах или замърсявания от разделителната ролка с помощта на оригинален комплект за почистване на Epson или мека влажна кърпа.



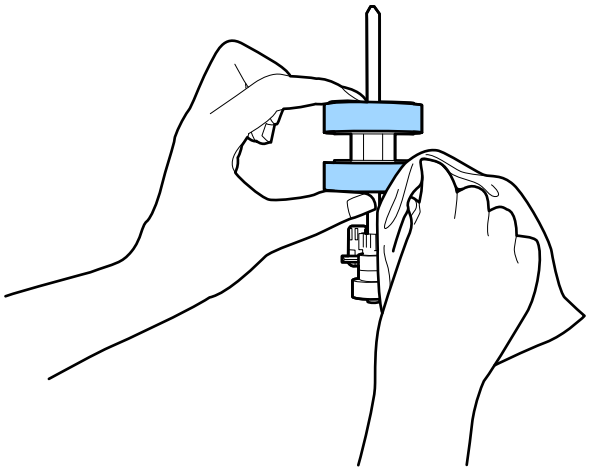
> ***Важно:***
>
> *Използвайте само оригинален комплект за почистване на Epson или мека влажна кърпа за почистване на ролката. Използването на суха кърпа може да повреди повърхността на ролката.*

8. Отворете капака, след което извадете листоподаващата ролка.

   За повече подробности вижте „Смяна на комплекта ролки“.



9. Избършете прах или замърсявания от повдигащата ролка с помощта на оригинален комплект за почистване на Epson или мека влажна кърпа.



> ***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.

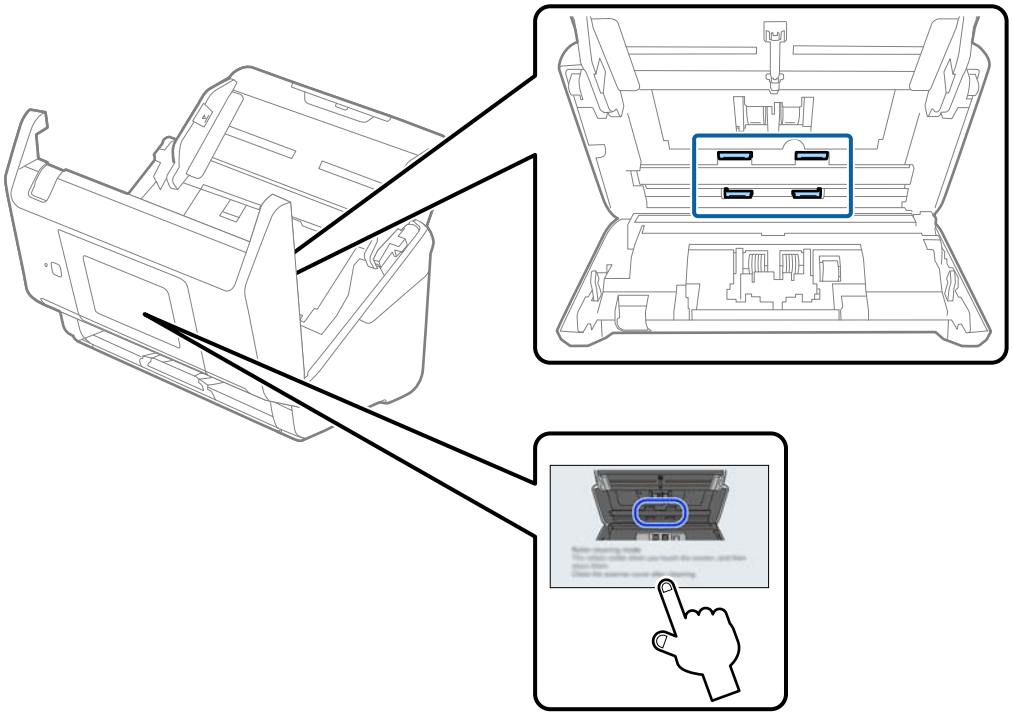
12. Изберете **Техническо обсл. Скенера** от началния екран.

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.

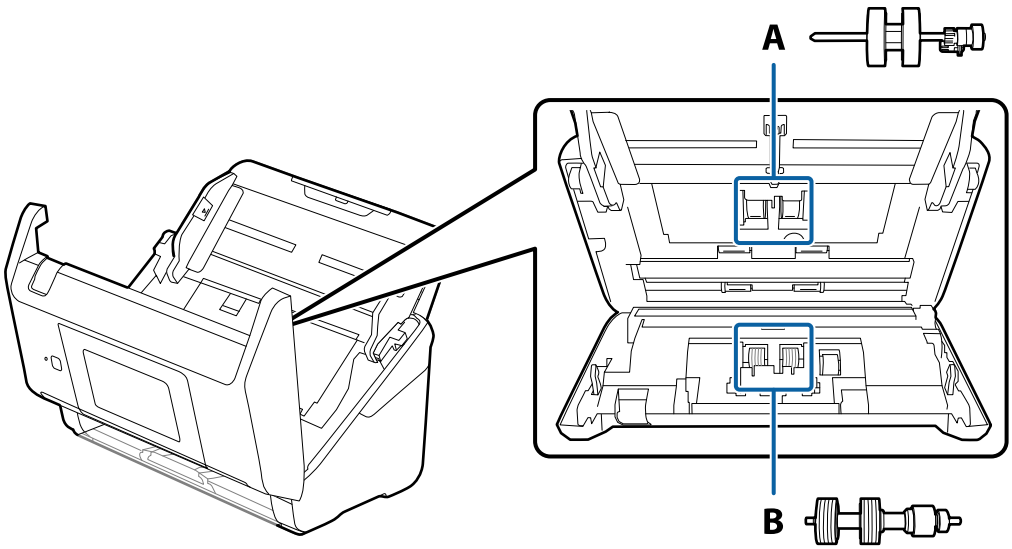
    Скенерът излиза от режима на почистване на ролките.

Още по темата

➡ “Смяна на комплекта ролки” на страница 164

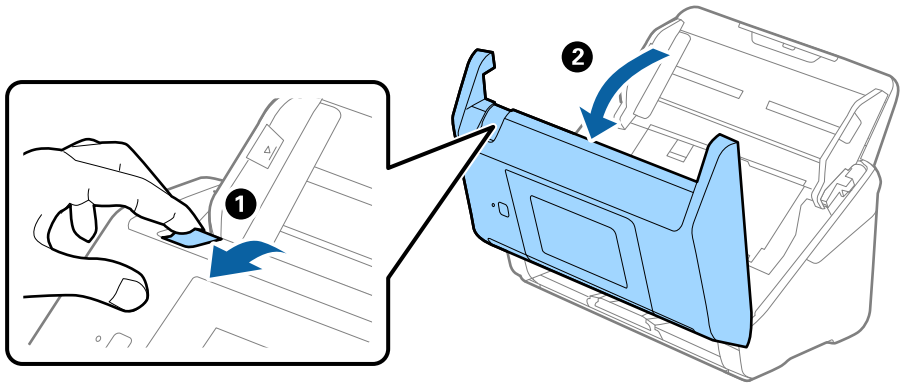
Смяна на комплекта ролки

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.

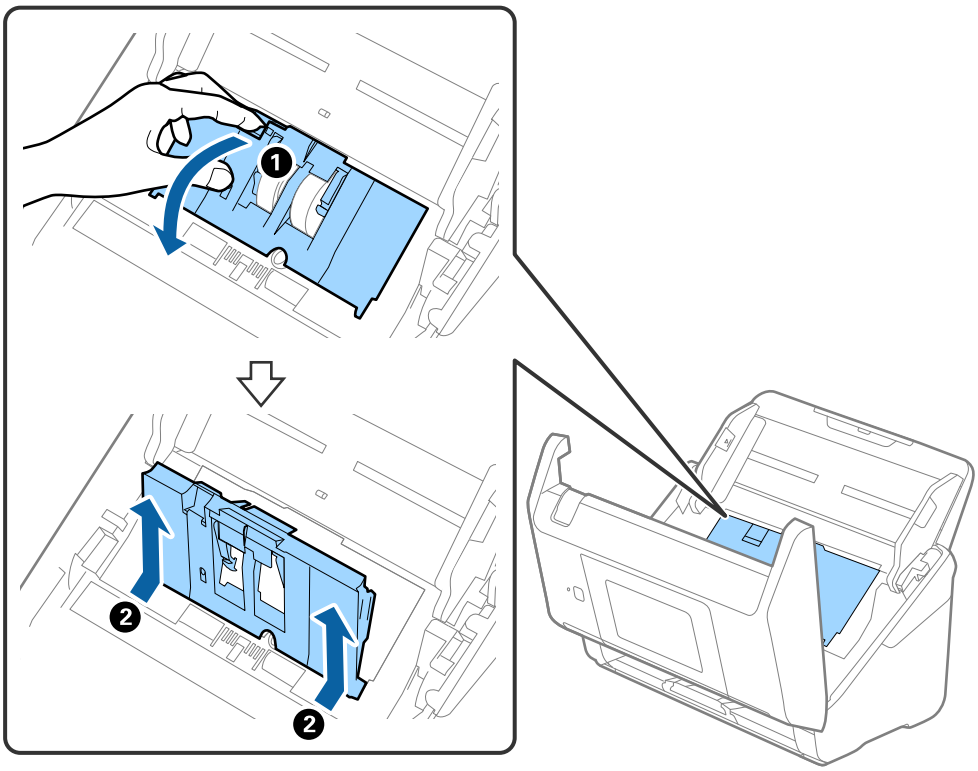


A: листоподаваща ролка, B: разделителна ролка

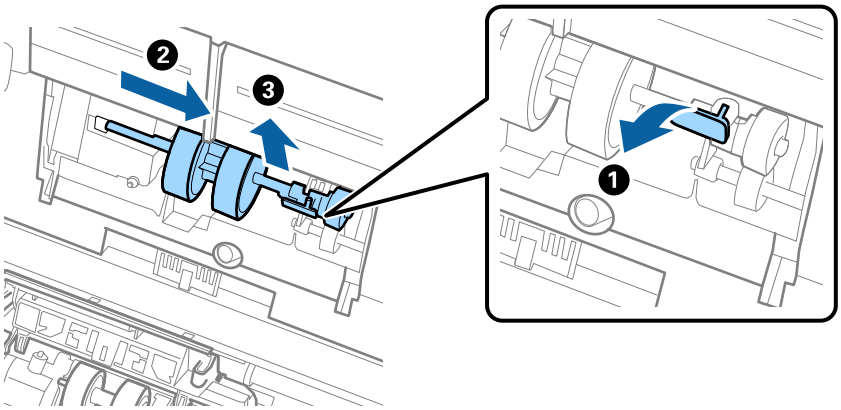
1. Натиснете бутон ⏻, за да изключите скенера.
2. Изключете AC адаптера от скенера.
3. Дръпнете лоста и отворете капака на скенера.



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



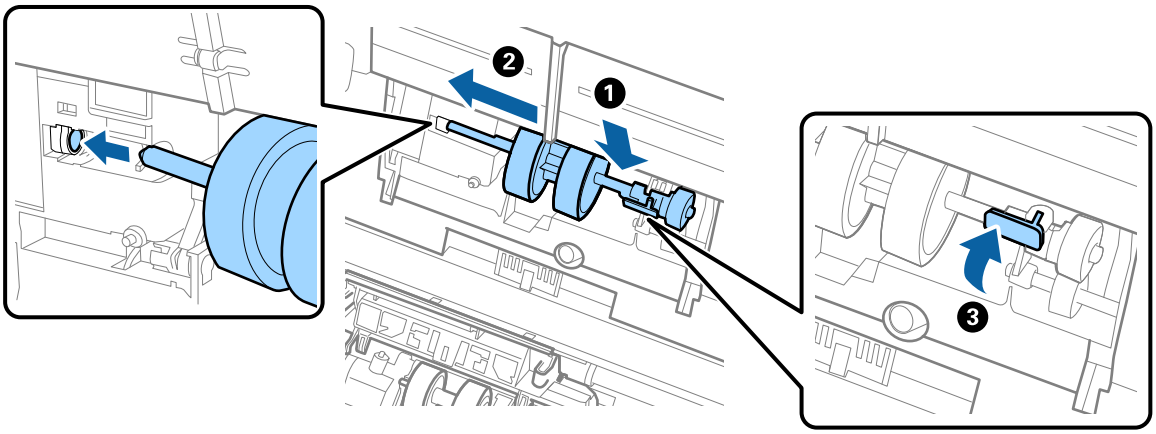
5. Дръпнете фиксиращия механизъм на вала на ролките, след което плъзнете и извадете монтираните повдигащи ролки.



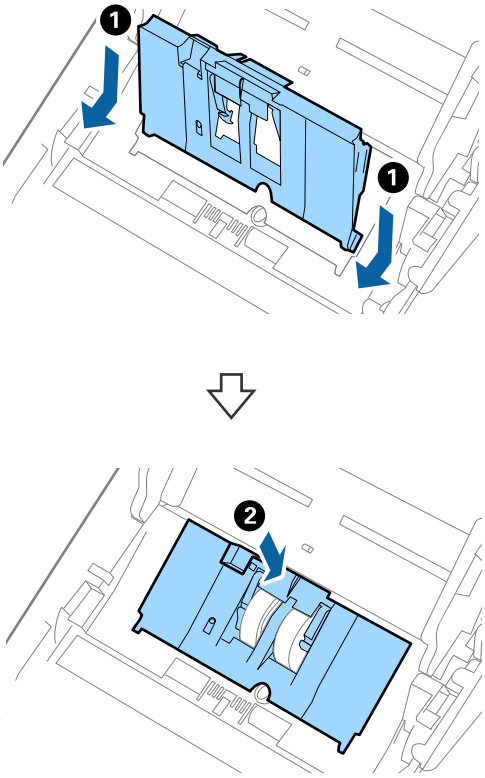
Важно:

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.

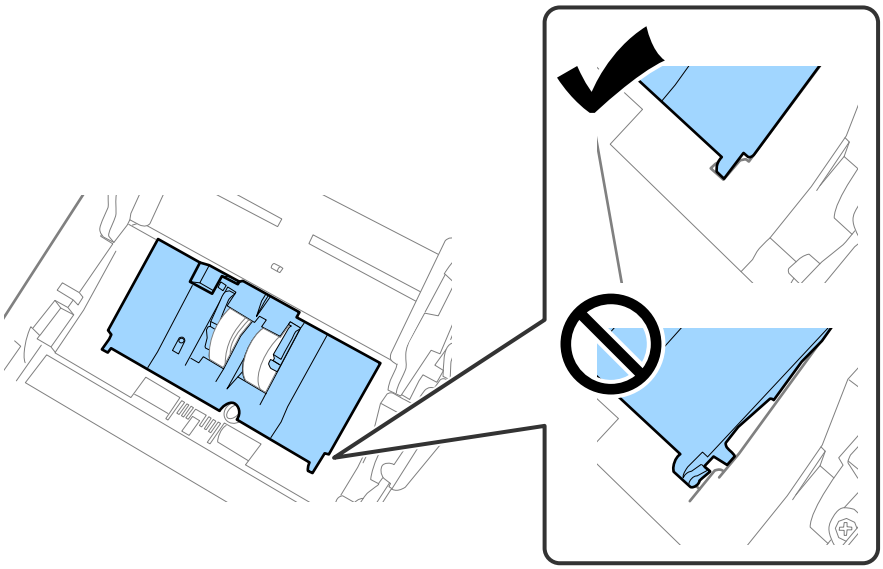


7. Поставете ръба на капака на повдигащата ролка в жлеба и го плъзнете. Затворете плътно капака.

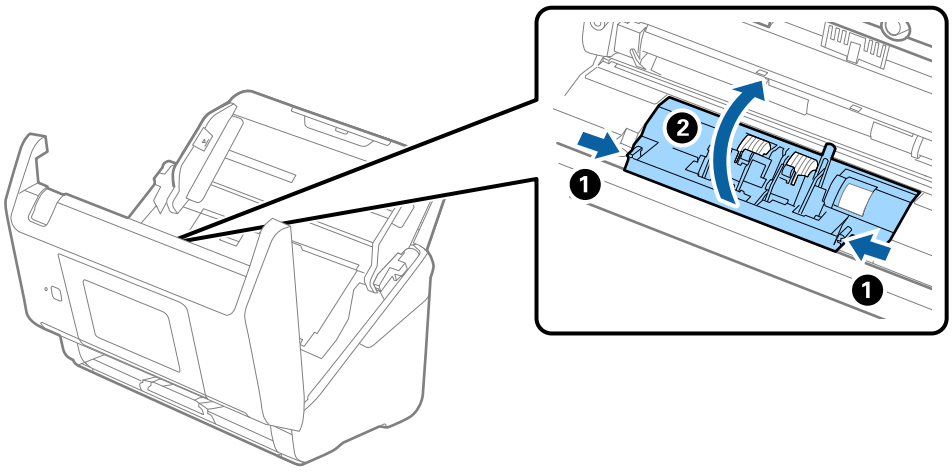


Важно:

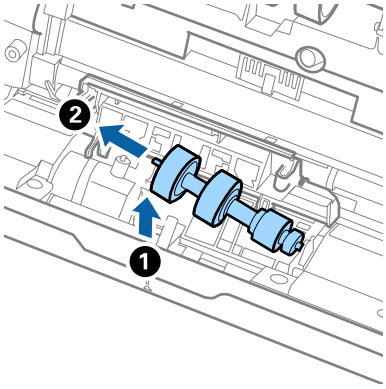
- ❏ *Уверете се, че капакът на повдигащата ролка е затворен правилно.*
- ❏ *Ако капакът се затваря трудно, проверете дали повдигащите ролки са монтирани правилно.*
- ❏ *Не монтирайте капака, докато е повдигнат.*



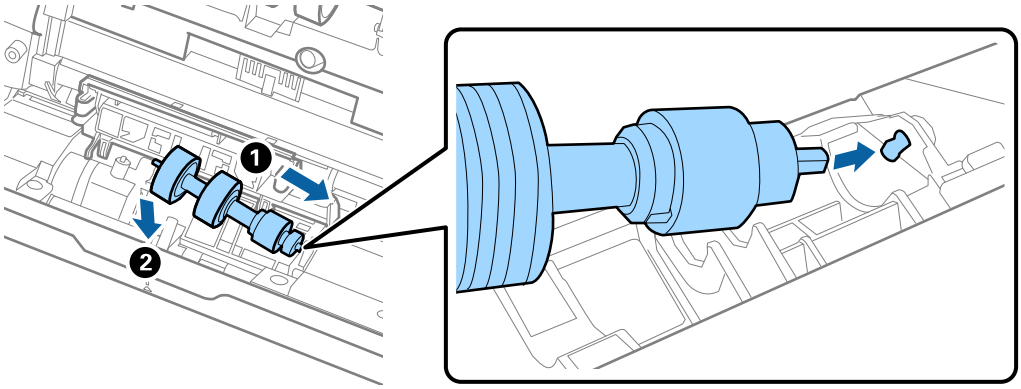
8. Натиснете захващащите куки от двете страни на капака на разделителната ролка, за да го отворите.



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.

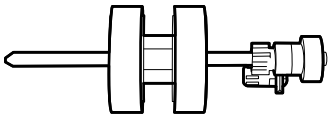
14. Нулирайте броя сканирания на контролния панел.

Забележка:
Изхвърлете повдигащата и разделителната ролка, като следвате правилата и разпоредбите на Вашите местни власти. Не ги разглобявайте.

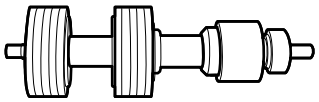
Кодове на комплекта ролки

Частите (листоподаващата 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 помощната програма на Epson Scan 2.

A



B



A: листоподаваща ролка, B: разделителна ролка

Номер на частта	Кодове	Жизнен цикъл
Комплект ролки	B12B819671 B12B819681 (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 хартии, като например хартия, която генерира много хартиен прах, или хартия с груба повърхност, която би могла да съкрати жизнения цикъл.

Нулиране на броя сканирания

Нулирайте броя на сканиранията след смяната на комплекта ролки.

1. Изберете **Настройки** > **Информация за устройството** > **Нулиране на брой сканирания** > **Бр. ск. след см. ролка** от началния екран.

2. Натиснете **Да**.

Още по темата

➡ "Смяна на комплекта ролки" на страница 164

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. Помислете за околната среда, преди да извършвате каквито и да било промени.

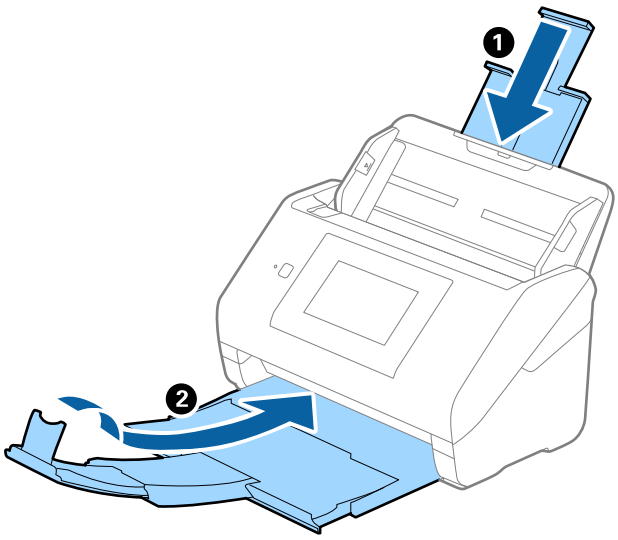
1. Изберете **Настройки** от началния екран.
2. Изберете **Осн. Настройки**.
3. Изберете **Настр. за изкл.**, след което направете настройки.

   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.

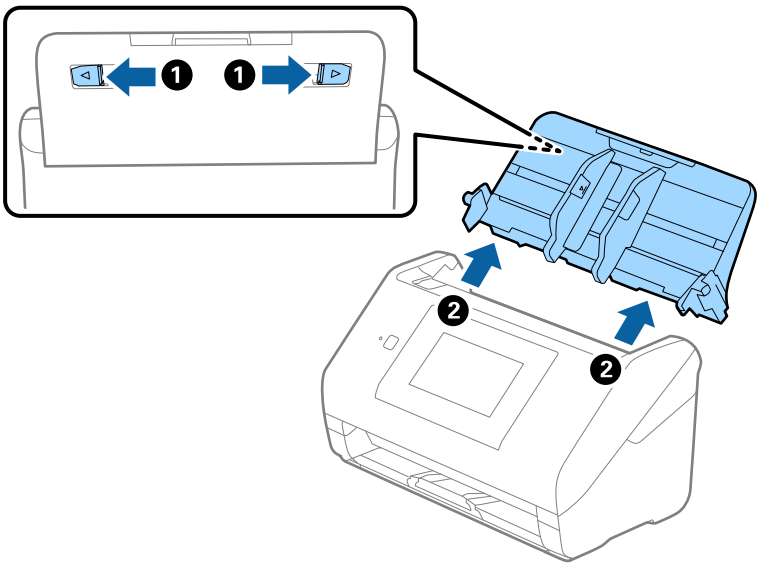
1. Натиснете бутон ⏻, за да изключите скенера.
2. Извадете адаптера за променлив ток.
3. Извадете кабелите и устройствата.
4. Затворете удължението на входната и изходната тава.



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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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

➡ "Пускане на Web Config в уеб браузър" на страница 37

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 стартирате **Всички настройки**, всички данни за настройки, регистрирани на скенера, включително контактите и настройките за удостоверяване на потребител, ще бъдат изтрити. Изтритите настройки не могат да се възстановят.*

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 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 10

   Щракнете върху бутона за стартиране и 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 „Старт“, след което изберете **Всички програми** или **Програми** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Изберете **Търсачка** > **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 приложението 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

➡ “Пускане на Web Config в уеб браузър” на страница 37

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. Ако не можете да обновите по мрежата, опитайте този начин.

Забележка:
Преди да актуализирате, се уверете, че драйверът на скенераEpson Scan 2 е инсталиран на Вашия компютър. Ако Epson Scan 2 не е инсталирано, инсталирайте го отново.

1. Проверете уебсайта на Epson за последните версии на актуализации на фърмуера.

   http://www.epson.com

   ❏ Ако има фърмуер за Вашия скенер, изтеглете го и преминете към следващата стъпка.

   ❏ Ако няма информация за фърмуер на уебсайта, 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.