EPSON
EXCEED YOUR VISION

DS-790WN

Руководство администратора

NPD6726-00 RU

Авторское право

Товарные знаки

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION и соответствующие логотипы являются товарными знаками 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 являются зарегистрированными товарными знаками Sony Corporation.
- ❏ MIFARE является зарегистрированным товарным знаком NXP Semiconductor Corporation.
- ❏ Общее примечание. Названия иных продуктов упоминаются в документе только для их идентификации и могут являться товарными знаками соответствующих владельцев. Компания Epson отрицает любые права на владение данными знаками.

Содержание

Расширенные настройки безопасности

Настройки аутентификации

Обслуживание

Введение

Содержание настоящего документа

В этом документе содержится следующая информация для администраторов сканера.

❏ Настройки сети

❏ Подготовка функции сканирования

❏ Включение и контроль настроек безопасности

❏ Включение и контроль Настройки аутентификации

❏ Выполнение ежедневного технического обслуживания

Информацию о стандартных способах использования сканера см. в *Руководство пользователя*.

Примечание:
В данном документе описаны Настройки аутентификации, которые обеспечивают автономную аутентификацию без необходимости использования сервера аутентификации. В дополнение к Настройки аутентификации, описанным в данном руководстве, можно также организовать систему аутентификации с использованием сервера аутентификации. Для создания системы используйте Document Capture Pro Server Authentication Edition (сокращенное название — Document Capture Pro Server AE).

Для получения дополнительной информации свяжитесь с местным отделением Epson.

Использование настоящего руководства

Эмблемы и символы

> ***Предостережение:***
> *Необходимо соблюдать инструкции во избежание получения травм.*

> ***Важно:***
> *Необходимо соблюдать инструкции, чтобы не повредить оборудование.*

Примечание:
Дополнительная и справочная информация.

Соответствующая информация

➡ Ссылки на соответствующие разделы.

Описания в этом руководстве

❏ Снимки экрана приложений взяты из ОС Windows 10 или macOS High Sierra. Содержимое этих экранов различается в зависимости от модели устройства и ситуации.

❏ Иллюстрации, используемые в этом руководстве, предназначены исключительно для справки. Несмотря на то, что они незначительно отличаются от фактического устройства, методы выполнения действий остаются такими же.

Названия операционных систем

Windows

В данном руководстве такие термины, как 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, относятся к следующим операционным системам. Кроме того, Windows используется для ссылки на все версии, а Windows Server используется для ссылки на Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 и Windows Server 2008 R2.

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

Mac OS

В этом руководстве Mac OS используется для ссылки на macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan и OS X Yosemite.

Настройки, необходимые для различных целей

Настройки, необходимые для различных целей

Необходимые настройки для выполнения различных задач приведены ниже.

Подключение сканера к сети

Цель	Требуемые настройки
Необходимо подключить сканер к сети.	Настройте сканер для сканирования по сети. «Подключение сканера к сети» на стр. 14
Необходимо подключить сканер к новому компьютеру.	Задайте сетевые настройки для сканера на новом компьютере. «Добавление или замена компьютера или устройств» на стр. 20

Настройки сканирования

Цель	Требуемые настройки
Необходимо отправлять отсканированные изображения по электронной почте. (Сканирование в электронную почту)	1. Настройте почтовый сервер, с которым будет устанавливаться связь. «Настройка почтового сервера» на стр. 44 2. Зарегистрируйте адрес электронной почты получателя в разделе **Контакты** (необязательное действие). Если вы зарегистрируете адрес электронной почты, вам не придется вводить его каждый раз, когда вы хотите что-то отправить на него. Вы можете просто выбрать его из списка контактов. «Обеспечение доступности контактов» на стр. 66
Необходимо сохранять отсканированные изображения в сетевую папку. (Сканирование в сетевую папку/FTP)	1. Создайте в сети папку, в которую вы планируете сохранять изображения. «Настройка общей сетевой папки» на стр. 47 2. Зарегистрируйте путь к папке в разделе **Контакты** (необязательное действие). Если вы зарегистрируете этот путь к папке, вам не придется вводить его каждый раз, когда вы хотите что-то отправить в папку. Вы можете просто выбрать его из списка контактов. «Обеспечение доступности контактов» на стр. 66
Необходимо сохранять отсканированные изображения в облачную службу. (Сканирование в облако)	Настройте службу Epson Connect. Подробную информацию о настройке см. на сайте-портале Epson Connect. При настройке вам потребуется учетная запись пользователя службы онлайн-хранилища, к которому вы планируете подключаться. https://www.epsonconnect.com/ http://www.epsonconnect.eu (только Европа)

Настройка панели управления

Цель	Требуемые настройки
Необходимо изменить элементы, отображаемые на панели управления сканера.	Задайте настройки **Предустан.** или **Редактировать домашний**. Вы можете зарегистрировать предпочитаемые настройки сканирования на панели управления и изменить отображаемые элементы. «Настройка панели управления» на стр. 80

Настройка основных функций безопасности

Цель	Требуемые настройки
Необходимо запретить изменять настройки сканера всем, кроме администратора.	Установите пароль администратора для сканера. «Настройки администратора» на стр. 89
Необходимо запретить использование сканеров с USB-подключением.	Отключите внешний интерфейс. «Отключение внешнего интерфейса» на стр. 95

Настройка дополнительных функций безопасности

Цель	Требуемые настройки
Необходимо контролировать использование тех или иных протоколов.	Включите или отключите соответствующие протоколы. «Управление использованием протоколов» на стр. 101
Необходимо зашифровать канал передачи данных.	1. Настройте цифровой сертификат. «Использование цифрового сертификата» на стр. 104 2. Настройте соединение по протоколу SSL/TLS. «Связь со сканером через SSL/TLS» на стр. 110
Необходимо использовать зашифрованное соединение (IPsec). Необходимо обеспечить возможность использовать программное обеспечение только с определенного компьютера (с фильтрацией IP-адресов).	Настройте политики фильтрации трафика. «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 111
Необходимо использовать сканер в сети стандарта IEEE802.1X.	Настройте IEEE802.1X для сканера. «Подключение сканера к сети IEEE802.1X» на стр. 123

Настройка функций аутентификации сканера

Цель	Требуемые настройки
Необходимо включить функцию Настройки аутентификации.	Более подробную информацию о доступных функциях Настройки аутентификации и Метод аутентификации см. в следующих разделах. «Сведения о ПО Настройки аутентификации» на стр. 133 «Сведения о ПО Метод аутентификации» на стр. 134

Использование системы аутентификации сервера

С помощью ПО Document Capture Pro Server Authentication Edition (сокр. Document Capture Pro Server AE) можно организовать систему аутентификации, в которой проверка подлинности осуществляется через сервер.

Для получения дополнительной информации свяжитесь с местным отделением Epson.

Настройки сети

Подключение сканера к сети

В этом разделе описывается процедура подключения сканера к сети с помощью панели управления сканера.

Примечание:
Если ваш сканер и компьютер находятся в одном сегменте сети, вы также можете выполнить подключение с помощью программы установки.

❏ *Установка с веб-сайта*

Перейдите на указанный веб-сайт и введите наименование изделия. Откройте раздел ***Настройка****, затем начните настройку.*

http://epson.sn

❏ *Настройка с помощью диска с программным обеспечением (только для моделей, которые поставляются с диском с программным обеспечением, и пользователей компьютеров, работающих под управлением Windows и оснащенных дисковыми приводами).*

Вставьте компакт-диск с ПО в компьютер и следуйте инструкциям на экране.

Перед установкой сетевого подключения

Перед подключением к сети проверьте метод подключения и его параметры.

Сбор информации о настройке подключения

Перед подключением подготовьте необходимую информацию о параметрах сети. Предварительно узнайте следующую информацию.

Разделы	Параметры	Примечание
Метод подключения устройства	❏ Ethernet ❏ Wi-Fi	Выберите способ подключения сканера к сети. При использовании проводной локальной сети подсоедините принтер к коммутатору локальной сети. При использовании Wi-Fi подключитесь к сети (SSID) точки доступа.
Сведения о подключении к локальной сети	❏ IP-адрес ❏ Маска подсети ❏ Стандартный шлюз	Выберите способ назначения IP-адреса сканера. При назначении статического IP-адреса требуются значения всех параметров. При назначении динамического IP-адреса с использованием функции DHCP эта информация не требуется, поскольку настройка происходит автоматически.
Сведения о подключении к Wi-Fi	❏ SSID ❏ Пароль	Это SSID (имя сети) и пароль точки доступа, к которой подключается сканер. Если установлена фильтрация MAC-адресов, перед регистрацией сканера зарегистрируйте на точке доступа его MAC-адрес. Информацию о поддерживаемых стандартах см. в следующем разделе. «Характеристики сети» на стр. 29

Разделы	Параметры	Примечание
Сведения о DNS-сервере	❏ IP-адрес основного DNS-сервера ❏ IP-адрес дополнительного DNS-сервера	Эти параметры необходимы для задания DNS-серверов. Дополнительный DNS-сервер устанавливается при организации в системе избыточной конфигурации и настройке дополнительного DNS-сервера. Если организация небольшая и DNS-сервер не устанавливается, установите IP-адрес маршрутизатора.
Сведения о прокси-сервере	❏ Имя прокси-сервера	Установите этот режим при использовании в сетевой среде прокси-сервера для доступа к Интернету из интрасети и использовании функции, применяемой сканером для доступа к Интернету. При использовании следующих функций сканер подключается к Интернету напрямую. ❏ Службы Epson Connect ❏ Облачные службы других компаний ❏ Обновление микропрограммы ❏ Отправка отсканированных изображений в SharePoint (WebDAV)
Информация о номере порта	❏ Номер порта для освобождения	Проверьте номер порта, используемый сканером и компьютером, затем при необходимости откройте этот порт на брандмауэре, если он заблокирован там. Информацию о номере порта, который используется сканером, см. в следующем разделе. «Использование порта сканера» на стр. 31

Назначение IP-адреса

Существуют следующие типы назначения IP-адресов.

Статический IP-адрес

Назначение вручную сканеру (узлу) фиксированного IP-адреса.

Данные для подключения к сети (маска подсети, шлюз по умолчанию, DNS-сервер и т. д.) должны быть заданы вручную.

Такой IP-адрес не меняется даже при выключении устройства. Это полезно при управлении устройствами в сети, в которой нельзя изменять IP-адреса, или при управлении устройствами с использованием их IP-адресов. Мы рекомендуем настраивать таким образом сканеры, серверы и другие устройства, к которым подключается много компьютеров. При использовании функций безопасности, таких как IPsec/фильтрация IP, также назначайте фиксированные IP-адреса, чтобы они не менялись.

Автоматическое назначение с использованием функции DHCP (динамический IP-адрес):

Автоматическое назначение IP-адреса сканеру (узлу) с использованием функции DHCP соответствующего сервера или маршрутизатора.

Параметры подключения к сети (маска подсети, шлюз по умолчанию, DNS-сервер и т. д.) устанавливаются автоматически, что позволяет легко подключать устройства к сети.

При выключении устройства или маршрутизатора и в зависимости от параметров DHCP-сервера при повторном подключении IP-адреса могут изменяться.

Мы рекомендуем управлять устройствами без использования IP-адресов и использовать протоколы, разрешающие IP-адреса.

Примечание:
При использовании функции DHCP для резервирования IP-адресов можно назначить один IP-адрес нескольким устройствам одновременно.

DNS-сервер и прокси-сервер

DNS-сервер позволяет связывать имя узла, имена домена адреса электронной почты и т. д. с данными IP-адреса.

Если компьютер или сканер связываются по протоколу IP с другой стороной, которая указана именем узла, именем домена и т. д., то такая связь будет невозможна.

Запрашивает эту информацию у DNS-сервера и получает IP-адрес другой стороны. Этот процесс называется разрешением имен.

Поэтому устройства, такие как компьютеры и сканеры, могут обмениваться данными, используя IP-адреса.

Разрешение имен необходимо, чтобы сканер мог отправлять электронную почту и подключаться к Интернету.

При использовании этих функций необходимо настроить DNS-сервер.

При назначении сканеру IP-адреса с использованием функции DHCP соответствующего сервера или маршрутизатора этот адрес устанавливается автоматически.

Прокси-сервер размещается на шлюзе между сетью и Интернетом, а также связывается с компьютером, сканером и Интернетом (противоположный сервер) от имени каждого устройства. Противоположный сервер связывается только с прокси-сервером. Поэтому сведения о сканере, такие как IP-адрес и номер порта, не могут быть считаны, что повышает безопасность.

При подключении к сети Интернет через прокси-сервер настройте на сканере параметры этого сервера.

Подключение к сети с панели управления

Подключите сканер к сети с помощью панели управления сканера.

Назначение IP-адреса

Настройте базовые элементы, такие как адрес узла, Маска подсети, Шлюз по умолчанию.

В этом разделе описывается процедура настройки статического IP-адреса.

1. Включите сканер.
2. Выберите **Настр.** на главном экране или на панели управления сканера.
3. Выберите **Настройки сети** > **Расширенные** > **TCP/IP**.
4. Выберите значение **Ручной** для параметра **Получить IP-адрес**.

   Если IP-адрес определяется автоматически с помощью функции DHCP маршрутизатора, выберите **Авто**. В этом случае параметры **IP-адрес**, **Маска подсети** и **Шлюз по умолчанию** на шагах 5–6 также задаются автоматически, поэтому перейдите к шагу 7.

5. Введите IP-адрес.

   При выборе ◀ и ▶ фокус перемещается к следующему или предыдущему сегменту, отделенному точкой.

   Проверьте значение, отображенное на предыдущем экране.

6. Укажите **Маска подсети** и **Шлюз по умолчанию**.

   Проверьте значение, отображенное на предыдущем экране.

   > ***Важно:***
   > *Если сочетание IP-адрес, Маска подсети и Шлюз по умолчанию является неверным, **Запуск настройки** становится неактивным и продолжить настройку будет невозможно. Убедитесь, что в записи нет ошибки.*

7. Введите IP-адрес основного DNS-сервера.

   Проверьте значение, отображенное на предыдущем экране.

   Примечание:
   *Если в настройках присваивания IP-адреса устройству используется значение **Авто**, для настроек DNS-сервера можно выбрать значение **Ручной** или **Авто**. Если не удается получить адрес DNS-сервера автоматически, выберите вариант **Ручной** и введите адрес DNS-сервера. Затем введите напрямую адрес дополнительного DNS-сервера. Если вы выбрали **Авто**, перейдите к шагу 9.*

8. Введите IP-адрес дополнительного DNS-сервера.

   Проверьте значение, отображенное на предыдущем экране.

9. Нажмите **Запуск настройки**.

Настройка прокси-сервера

Настройте прокси-сервер, если выполняются оба следующих условия.

❏ Прокси-сервер предназначен для подключения к Интернету.

❏ При использовании функции, для которой сканер подключается к Интернету напрямую, например службы Epson Connect или облачных служб другой компании.

1. Выберите **Настр.** на главном экране.

   При проведении настройки после настройки IP-адреса будет выведен экран **Расширенные**. Перейдите к шагу 3.

2. Выберите **Настройки сети** > **Расширенные**.

3. Выберите **Прокси-сервер**.

4. Выберите значение **Исп.** для параметра **Наст. прокси-сервера**.

5. Введите адрес прокси-сервера в формате IPv4 или в формате полного доменного имени.

   Проверьте значение, отображенное на предыдущем экране.

6. Введите номер порта прокси-сервера.

   Проверьте значение, отображенное на предыдущем экране.

7. Нажмите **Запуск настройки**.

Подключение к Ethernet-сети

Подключите сканер к сети с помощью сетевого кабеля и проверьте подключение.

1. Соедините сканер и концентратор (коммутатор локальной сети) сетевым кабелем.

2. Выберите  на главном экране.

3. Выберите **Маршрутизатор**.

4. Убедитесь, что параметры Подключение и IP-адрес заданы верно.

5. Нажмите **Закрыть**.

Подключение к беспроводной локальной сети (Wi-Fi)

Подключить сканер к беспроводной локальной сети (Wi-Fi) можно несколькими способами. Выберите метод подключения, который соответствует среде и условиям использования.

Если у вас есть информация для доступа к беспроводному маршрутизатору (SSID и пароль), настройки можно задать вручную.

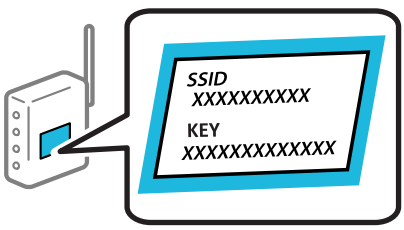
Если беспроводной маршрутизатор поддерживает WPS, задать настройки можно нажатием соответствующей кнопки.

После подключения сканера к сети подключите сканер к устройству, с которым вы хотите его использовать (к компьютеру, интеллектуальному устройству, планшетному компьютеру и т. п.)

Настройка сети Wi-Fi посредством ввода имени сети (SSID) и пароля

Вы можете настроить сеть Wi-Fi, введя с панели управления сканера сведения, необходимые для подключения к беспроводному маршрутизатору. Для этого необходимо знать имя сети (SSID) и пароль для беспроводного маршрутизатора.

Примечание:
Если вы используете беспроводной маршрутизатор с настройками по умолчанию, SSID и пароль указаны на ярлыке. Если вы не знаете SSID и пароль, обратитесь к сотруднику, выполнявшему настройку беспроводного маршрутизатора, или к документации на этот беспроводной маршрутизатор.



1. Нажмите  на начальном экране.
2. Выберите **Маршрутизатор**.
3. Нажмите **Начать установку**.

   Если сетевое подключение уже настроено, отображаются подробные сведения о подключении. Нажмите **Измените реж. на подключение Wi-Fi.** или **Изменить настройки** для изменения настроек.
4. Выберите **Мастер настройки Wi-Fi**.
5. Следуйте инструкциям на экране, чтобы выбрать SSID, ввести пароль беспроводного маршрутизатора и запустить настройку.

   Если необходимо проверить состояние подключения сканера к сети после завершения настройки, обратитесь к ссылке ниже в разделе сопутствующей информации.

   Примечание:
   - ❏ *Если вы не знаете имя сети (SSID), проверьте, не написано ли оно на ярлыке беспроводного маршрутизатора. Если вы используете беспроводной маршрутизатор с настройками по умолчанию, используйте имя сети (SSID), указанное на ярлыке. Если не удалось найти никакой информации, обратитесь к документации на беспроводной маршрутизатор.*
   - ❏ *Пароль чувствителен к регистру.*
   - ❏ *Если вы не знаете пароль, проверьте, не написан ли он на ярлыке беспроводного маршрутизатора. На ярлыке пароль может быть обозначен как «ключ сети», «пароль беспроводной сети» и т. д. Если вы используете беспроводной маршрутизатор с настройками по умолчанию, используйте пароль, указанный на ярлыке.*

Соответствующая информация

➡ «Проверка состояния сетевого соединения» на стр. 27

Настройка соединения Wi-Fi с помощью кнопки настройки WPS

Можно автоматически настроить сеть Wi-Fi, нажав соответствующую кнопку на беспроводном маршрутизаторе. При выполнении следующих условий можно выполнить настройку с помощью этого способа.

- ❏ Беспроводной маршрутизатор поддерживает режим WPS (Wi-Fi Protected Setup).
- ❏ Текущее соединение Wi-Fi было установлено путем нажатия кнопки на беспроводном маршрутизаторе.

Примечание:
Если вы не можете найти кнопку либо выполняете настройку с помощью ПО, обратитесь к документации на беспроводной маршрутизатор.

1. Нажмите  на начальном экране.
2. Выберите **Маршрутизатор**.
3. Нажмите **Начать установку**.

   Если сетевое подключение уже настроено, отображаются подробные сведения о подключении. Нажмите **Измените реж. на подключение Wi-Fi.** или **Изменить настройки** для изменения настроек.

4. Выберите **Настройка кнопкой (WPS)**.

5. Следуйте инструкциям на экране.

   Если необходимо проверить состояние подключения сканера к сети после завершения настройки, обратитесь к ссылке ниже в разделе сопутствующей информации.

   Примечание:
   Если установить соединение не удается, перезапустите беспроводной маршрутизатор, переместите его ближе к сканеру и повторите попытку.

Соответствующая информация

➡ «Проверка состояния сетевого соединения» на стр. 27

Настройка соединения Wi-Fi с помощью установки PIN-кода (WPS)

К беспроводному маршрутизатору можно автоматически подключиться с помощью PIN-кода. Этот способ можно применять, если беспроводной маршрутизатор имеет функцию WPS (защищенная настройка Wi-Fi). Для установки PIN-кода на беспроводном маршрутизаторе используйте компьютер.

1. Нажмите  на начальном экране.

2. Выберите **Маршрутизатор**.

3. Нажмите **Начать установку**.

   Если сетевое подключение уже настроено, отображаются подробные сведения о подключении. Нажмите **Измените реж. на подключение Wi-Fi.** или **Изменить настройки** для изменения настроек.

4. Выберите **Другие** > **Настр. PIN-кода (WPS)**

5. Следуйте инструкциям на экране.

   Если необходимо проверить состояние подключения сканера к сети после завершения настройки, обратитесь к ссылке ниже в разделе сопутствующей информации.

   Примечание:
   Для получения более подробной информации о вводе PIN-кода обратитесь к документации на беспроводной маршрутизатор.

Соответствующая информация

➡ «Проверка состояния сетевого соединения» на стр. 27

Добавление или замена компьютера или устройств

Подключение к сканеру, который уже подключен к сети

Если сканер уже подключен к сети, вы можете через эту сеть подключить к этому сканеру компьютер или интеллектуальное устройство.

Использование сетевого сканера на втором компьютере

При подключении сканера к компьютеру рекомендуется использовать программу установки. Запустить программу установки можно одним из следующих способов.

❏ Установка с веб-сайта

Перейдите на указанный веб-сайт и введите наименование вашей модели. Откройте раздел **Настройка**, затем начните настройку.

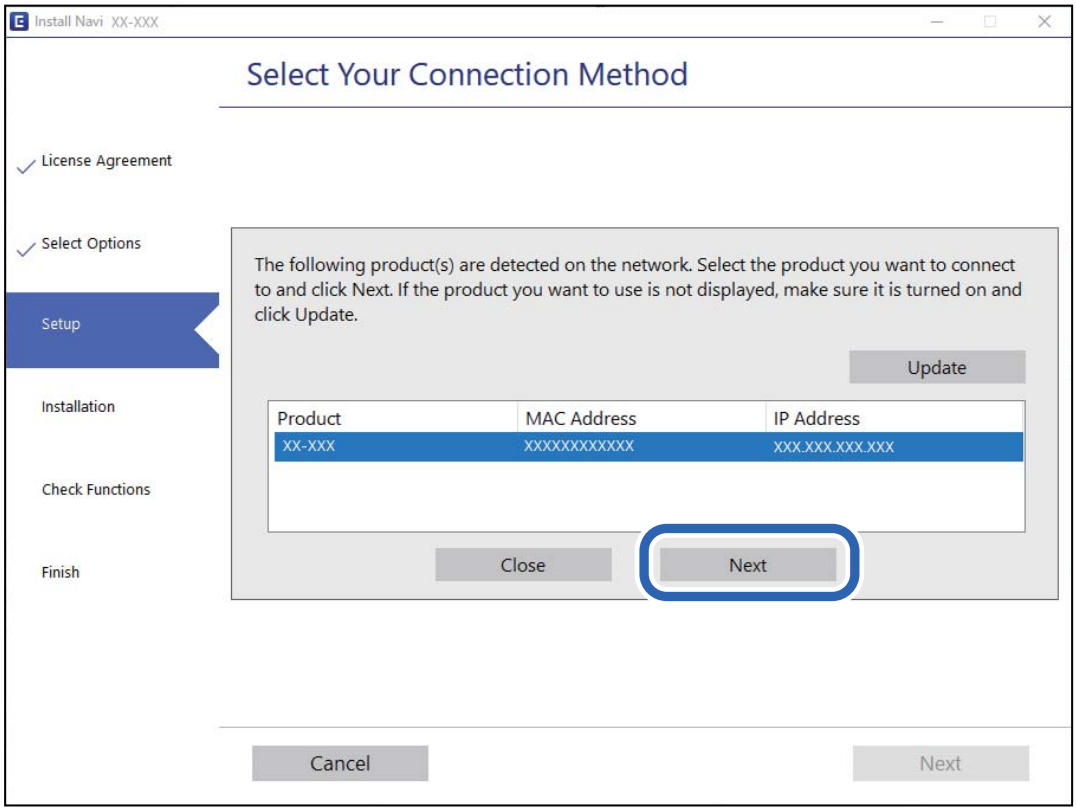
http://epson.sn

❏ Настройка с помощью диска с программным обеспечением (только для моделей, которые поставляются с диском с программным обеспечением, и пользователей компьютеров, работающих под управлением Windows и оснащенных дисковыми приводами).

Вставьте компакт-диск с ПО в компьютер и следуйте инструкциям на экране.

Выбор сканера

Следуйте инструкциям на экране, пока не появится показанный ниже экран, выберите имя сканера, к которому необходимо подключиться, затем нажмите **Далее**.



Следуйте инструкциям на экране.

Использование сетевого сканера на интеллектуальном устройстве

Вы можете подключить интеллектуальное устройство к сканеру с помощью одного из следующих способов.

Подключение через беспроводной маршрутизатор

Подключите интеллектуальное устройство к той же сети Wi-Fi (SSID), к которой подключен сканер.

Подробные сведения см. ниже.

«Настройка подключения к интеллектуальному устройству» на стр. 25

Подключение с помощью Wi-Fi Direct

Вы можете подключить интеллектуальное устройство к сканеру напрямую, без использования маршрутизатора беспроводной сети.

Подробные сведения см. ниже.

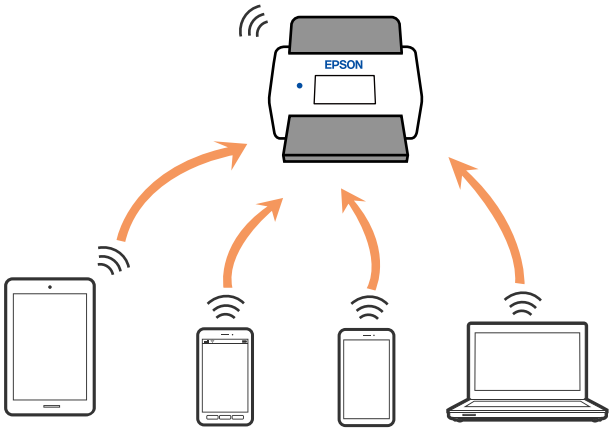
«Подключение интеллектуального устройства напрямую к сканеру (Wi-Fi Direct)» на стр. 22

Подключение интеллектуального устройства напрямую к сканеру (Wi-Fi Direct)

Режим Wi-Fi Direct (простая точка доступа) позволяет подключить интеллектуальное устройство к сканеру напрямую, без использования беспроводного маршрутизатора, и сканировать прямо с устройства.

Сведения о ПО Wi-Fi Direct

Этот способ подключения используется, когда Wi-Fi не используется дома или в офисе или когда нужно подключить сканер к компьютеру или интеллектуальному устройству напрямую. В этом режиме сканер выполняет функции беспроводного маршрутизатора, при этом к сканеру можно подключать устройства без использования стандартного беспроводного маршрутизатора. Однако при этом устройства, подключенные к сканеру, не смогут обмениваться информацией друг с другом через сканер.



Сканер может быть одновременно подключен к сети Wi-Fi или Ethernet и находиться в режиме Wi-Fi Direct (простая точка доступа). Однако при настройке сетевого подключения в режиме Wi-Fi Direct (простая точка доступа), если сканер подключен по Wi-Fi, подключение Wi-Fi будет временно разъединено.

Подключение к интеллектуальному устройству с помощью Wi-Fi Direct

Этот способ позволяет подключить сканер напрямую к интеллектуальным устройствам без использования беспроводного маршрутизатора.

1. Выберите  на главном экране.
2. Выберите **Wi-Fi Direct**.
3. Выберите **Начать установку**.
4. На вашем интеллектуальном устройстве установлено Epson Smart Panel.
5. Выполните инструкции, отображаемые на Epson Smart Panel, чтобы подключиться к сканеру.

   Если интеллектуальное устройство подключено к сканеру, перейдите к следующему шагу.
6. На панели управления сканера выберите **Заверш.**.

Отключение соединения в режиме Wi-Fi Direct (простая точка доступа)

Доступны два способа отключения соединения Wi-Fi Direct (простая точка доступа). Можно отключить все соединения с помощью панели управления сканера либо отключить каждое соединение с компьютера или интеллектуального устройства.

Для отключения всех соединений выберите  > **Wi-Fi Direct** > **Начать установку** > **Изменить** > **Отключить Wi-Fi Direct**.

Важно:

При отключении соединения Wi-Fi Direct (простая точка доступа) все компьютеры и интеллектуальные устройства, подключенные к сканеру через соединение Wi-Fi Direct (простая точка доступа), будут отключены.

Примечание:

Если вы хотите отключить конкретное устройство, выполните отключение на устройстве, а не на сканере. Для отключения соединения Wi-Fi Direct (простая точка доступа) с устройства используйте один из указанных ниже способов.

❏ *Отключите подключение по Wi-Fi к имени сети (SSID) сканера.*

❏ *Выполните подключение к другому имени сети (SSID).*

Изменение параметров режима Wi-Fi Direct (простая точка доступа), таких как SSID

Если включен режим подключения Wi-Fi Direct (простая точка доступа), можно изменить соответствующие параметры, выбрав  > **Wi-Fi Direct** > **Начать установку** > **Изменить**, после чего появятся следующие пункты меню.

Изменить имя сети

Изменение имени сети (SSID), используемого в режиме Wi-Fi Direct (простая точка доступа) для подключения к сканеру, на произвольное значение. Для имени сети (SSID) можно использовать символы ASCII с экранной клавиатуры на панели управления. Введите до 22 символов.

При изменении имени сети (SSID) все подключенные устройства отключаются. Чтобы снова подключить эти устройства, используйте новое имя сети (SSID).

Изменить пароль

Изменение пароля подключения к сканеру по Wi-Fi Direct (простая точка доступа) на произвольное значение. В пароле можно использовать символы ASCII экранной клавиатуры на панели управления. Можно ввести от 8 до 22 символов.

При изменении пароля все подключенные устройства отключаются. Чтобы снова подключить эти устройства, используйте новый пароль.

Изменить частотный диапазон

Измените частотный диапазон Wi-Fi Direct, используемый для подключения к сканеру. Можно выбрать диапазон 2,4 или 5 ГГц.

При изменении частотного диапазона все подключенные устройства отключаются. Повторно подключите устройство.

Учтите, что при выборе частотного диапазона 5 ГГц вы не сможете повторно подключить устройства, не поддерживающие этот частотный диапазон.

В зависимости от региона эта настройка может не отображаться.

Отключить Wi-Fi Direct

Отключение параметров режима Wi-Fi Direct (простая точка доступа) на сканере. При отключении этого режима также будут отключены все устройства, подключенные к сканеру по соединению Wi-Fi Direct (простая точка доступа).

Восст. настр. по ум.

Возврат всех параметров режима Wi-Fi Direct (простая точка доступа) к значениям по умолчанию.

Удаляется сохраненная на сканере информация о подключении интеллектуального устройства в режиме Wi-Fi Direct (простая точка доступа).

Примечание:
*На вкладке **Сеть** > **Wi-Fi Direct** приложения Web Config также можно выполнить следующие настройки.*

- ❏ *Включение или выключение режима Wi-Fi Direct (простая точка доступа)*
- ❏ *Изменение имени сети (SSID)*
- ❏ *Изменение пароля*
- ❏ *Изменение частотного диапазона*

  В зависимости от региона эта настройка может не отображаться.
- ❏ *Восстановление параметров Wi-Fi Direct (простая точка доступа)*

Повторная настройка подключения к сети

В этом разделе описывается, как задать параметры подключения к сети и изменить способ подключения после замены беспроводного маршрутизатора или компьютера.

Когда заменяется беспроводной маршрутизатор

При замене беспроводного маршрутизатора необходимо настроить параметры соединения между компьютером (или интеллектуальным устройством) и сканером.

Эти параметры также необходимо настроить при смене интернет-провайдера и в других случаях.

Настройка подключения к компьютеру

При подключении сканера к компьютеру рекомендуется использовать программу установки. Запустить программу установки можно одним из следующих способов.

❏ Установка с веб-сайта

Перейдите на указанный веб-сайт и введите наименование вашей модели. Откройте раздел **Настройка**, затем начните настройку.

http://epson.sn

❏ Настройка с помощью диска с программным обеспечением (только для моделей, которые поставляются с диском с программным обеспечением, и пользователей компьютеров, работающих под управлением Windows и оснащенных дисковыми приводами).

Вставьте компакт-диск с ПО в компьютер и следуйте инструкциям на экране.

Выбор способа подключения

Следуйте инструкциям на экране. На экране **Выберите операцию** выберите **Установите подключение к Принтер заново (для нового сетевого или переключения с USB на сеть и т.д.)** и нажмите кнопку **Далее**.

Завершите настройку, следуя инструкциям на экране.

Если выполнить подключение не удается, попробуйте решить проблему, используя информацию из следующих разделов.

«Не удается выполнить подключение к сети» на стр. 33

Настройка подключения к интеллектуальному устройству

Вы можете пользоваться сканером с интеллектуального устройства при подключении сканера к сети Wi-Fi с тем же SSID, что и сеть, к которой подключено интеллектуальное устройство. Для использования сканера с интеллектуального устройства зайдите на следующий сайт и введите название устройства. Откройте раздел **Настройка** и начните настройку.

http://epson.sn

Зайдите на веб-сайт с устройства, которое вы хотите подключить к сканеру.

Когда заменяется компьютер

При замене компьютера необходимо настроить параметры соединения между компьютером и сканером.

Настройка подключения к компьютеру

При подключении сканера к компьютеру рекомендуется использовать программу установки. Программу установки можно запустить одним из следующих способов.

❏ Установка с веб-сайта

Перейдите на указанный веб-сайт и введите наименование вашей модели. Откройте раздел **Настройка**, затем начните настройку.

http://epson.sn

❏ Настройка с помощью диска с программным обеспечением (только для моделей, которые поставляются с диском с программным обеспечением, и пользователей компьютеров, работающих под управлением Windows и оснащенных дисковыми приводами).

Вставьте компакт-диск с ПО в компьютер и следуйте инструкциям на экране.

Следуйте инструкциям на экране.

Изменение способа подключения к компьютеру

В этом разделе описано, как можно изменить способ подключения сканера к компьютеру.

Изменение способа подключения к сети — с Ethernet на Wi-Fi

Перейдите с подключения Ethernet на подключение Wi-Fi на панели управления сканера. Изменение способа подключения по сути не отличается от настройки подключения Wi-Fi.

Соответствующая информация

➡ «Подключение к беспроводной локальной сети (Wi-Fi)» на стр. 18

Изменение способа подключения к сети — с Wi-Fi на Ethernet

Чтобы изменить способ подключения к сети с Wi-Fi на Ethernet, выполните указанные ниже инструкции.

1. Выберите **Настр.** на главном экране.
2. Выберите **Настройки сети** > **Настройка проводной ЛВС**.
3. Следуйте инструкциям на экране.

Изменение способа подключения с USB-подключения на сетевое

Используйте программу установки и выберите иной способ подключения.

❏ Установка с веб-сайта

Перейдите на указанный веб-сайт и введите наименование вашей модели. Откройте раздел **Настройка**, затем начните настройку.

http://epson.sn

❏ Настройка с помощью диска с программным обеспечением (только для моделей, которые поставляются с диском с программным обеспечением, и пользователей компьютеров, работающих под управлением Windows и оснащенных дисковыми приводами).

Вставьте компакт-диск с ПО в компьютер и следуйте инструкциям на экране.

Выбор изменения способа подключения

Следуйте инструкциям на экране. На экране **Выберите операцию** выберите **Установите подключение к Принтер заново (для нового сетевого или переключения с USB на сеть и т.д.)** и нажмите кнопку **Далее**.

Выберите нужное сетевое подключение, затем выберите **Подключение по беспроводной сети (Wi-Fi)** или **Подключение через проводную локальную сеть (Ethernet)** и нажмите **Далее**.

Завершите настройку, следуя инструкциям на экране.

Проверка состояния сетевого соединения

Вы можете проверить состояние сетевого подключения следующим способом.

Проверка состояния сетевого соединения с помощью панели управления

Состояние сетевого соединения можно проверить с помощью значка сети или информации о сети на панели управления сканера.

Проверка состояния сетевого соединения с помощью значка сети

Проверить состояние сетевого соединения и мощность радиоволн можно с помощью значка сети на начальном экране сканера.

	Отображает состояние сетевого соединения. Нажмите этот значок для просмотра и изменения текущих настроек. Это ярлык для следующего меню. **Настр.** > **Настройки сети** > **Настройка Wi-Fi**	
		Сканер не подключен к беспроводной сети (Wi-Fi).
		Сканер выполняет поиск SSID, IP-адрес сброшен, или произошла проблема с беспроводной сетью (Wi-Fi).
		Сканер подключен к беспроводной сети (Wi-Fi). Количество полосок указывает на мощность сигнала подключения. Чем больше полосок, тем лучше сигнал.
		Сканер не подключен к беспроводной сети (Wi-Fi) в режиме Wi-Fi Direct (простая точка доступа).
		Сканер подключен к беспроводной сети (Wi-Fi) в режиме Wi-Fi Direct (простая точка доступа).
		Сканер не подключен к проводной (Ethernet) сети, или подключение закрыто.
		Сканер подключен к проводной сети (Ethernet).

Отображение подробных сведений о сети на панели управления

Если сканер подключен к сети, вы можете просмотреть прочую информацию, относящуюся к сети, выбрав соответствующие меню.

1. Выберите **Настр.** на главном экране.
2. Выберите **Настройки сети** > **Статус сети**.
3. Для того чтобы проверить информацию, выберите меню, которые хотели бы проверить.
   - ❏ Состоя. провод. ЛВС/Wi-Fi

     Служит для отображения сведений о сети (имя устройства, подключение, мощность сигнала и т. д.) для подключений Ethernet или Wi-Fi.
   - ❏ Состояние Wi-Fi Direct

     Отображает, включен или выключен Wi-Fi Direct, а также SSID, пароль и т. д. для подключений Wi-Fi Direct.
   - ❏ Статус серв. эл. поч.

     Отображает информацию о сети для сервера электронной почты.

Характеристики сети

Технические характеристики Wi-Fi

Информацию о технических характеристиках Wi-Fi см. в следующей таблице.

Страны и регионы, отличные от указанных ниже	Таблица A
Австралия Новая Зеландия Тайвань Южная Корея	Таблица B

Таблица A

Стандарты	IEEE 802.11b/g/n*1
Частотный диапазон	2,4 ГГц
Максимальная передаваемая мощность радиоизлучения	2400–2483,5 МГц: 20 дБм (EIRP)
Каналы	1/2/3/4/5/6/7/8/9/10/11/12/13
Режимы подключения	Инфраструктура, Wi-Fi Direct (простая точка доступа)*2*3
Протоколы защиты*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Доступно только для HT20.

*2 Не поддерживается для IEEE 802.11b.

*3 Можно одновременно использовать инфраструктуру и режимы Wi-Fi Direct или Ethernet-соединение.

*4 Режим Wi-Fi Direct поддерживает только стандарт WPA2-PSK (AES).

*5 Соответствует стандартам WPA2 с поддержкой WPA/WPA2 Personal.

Таблица B

Стандарты	IEEE 802.11a/b/g/n*1/ac
Частотные диапазоны	IEEE 802.11b/g/n: 2,4 ГГц, IEEE 802.11a/n/ac: 5 ГГц

Каналы	Wi-Fi	2,4 ГГц	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 ГГц*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 ГГц	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 ГГц*3	W52 (36/40/44/48) W58 (149/153/157/161/165)
Режимы подключения	Инфраструктура, Wi-Fi Direct (простая точка доступа)*4*5		
Протоколы защиты*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Доступно только для HT20.

*2 Недоступно в Тайване.

*3 Доступность этих каналов и возможность использования устройств с этими каналами за пределами помещений зависят от региона. Подробности см. по адресу http://support.epson.net/wifi5ghz/.

*4 Не поддерживается для IEEE 802.11b.

*5 Можно одновременно использовать инфраструктуру и режимы Wi-Fi Direct или Ethernet-соединение.

*6 В режиме Wi-Fi Direct поддерживается только стандарт WPA2-PSK (AES).

*7 Соответствует стандартам WPA2 с поддержкой WPA/WPA2 Personal.

Характеристики Ethernet

Стандарты	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (энергоэффективный Ethernet)*2
Режим обмена данными	Автоматический, 10 Mbps дуплексный режим, 10 Mbps полудуплексный режим, 100 Mbps дуплексный режим, 100 Mbps полудуплексный режим
Разъем	RJ-45

*1 Используйте кабель STP (экранированная витая пара) категории 5e или более высокой для снижения влияния помех.

*2 Подключенное устройство должно соответствовать стандартам IEEE802.3az.

Сетевые функции и IPv4/IPv6

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

Функции	Поддержка
Document Capture Pro Server	IPv4, IPv6

Протокол безопасности

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

* Необходимо использовать устройство связи, соответствующее стандарту IEEE802.1X.

Использование порта сканера

Сканер использует следующий порт. Эти порты должны быть при необходимости разрешены сетевым администратором.

Если отправитель (клиент) — сканер

Использование	Получатель (сервер)	Протокол	Номер порта
Отправка файла (если сканирование в сетевую папку выполняется со сканера)	FTP-/FTPS-сервер	FTP/FTPS (TCP)	20
			21
	Файловый сервер	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	Сервер WebDAV	Протокол HTTP (TCP)	80
		Протокол HTTPS (TCP)	443
Отправка файла (если сканирование на электронную почту выполняется со сканера)	SMTP-сервер	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
Подключение POP перед SMTP (при использовании сканирования на электронную почту со сканера)	POP-сервер	POP3 (TCP)	110

Использование	Получатель (сервер)	Протокол	Номер порта
Если используется Epson Connect	Сервер Epson Connect	HTTPS	443
		XMPP	5222
Сбор сведений о пользователе (используйте контакты со сканера)	Сервер LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Аутентификация пользователя при сборе сведений о пользователе (при использовании списка контактов со сканера) Аутентификация пользователя при выполнении сканирования в сетевую папку (SMB) со сканера	Сервер KDC	Kerberos	88
Управление WSD	Клиентский компьютер	WSD (TCP)	5357
Поиск компьютера при сканировании по технологии Push из приложения	Клиентский компьютер	Обнаружение устройств, поддерживающих сканирование по технологии Push	2968

Если отправитель (клиент) — клиентский компьютер

Использование	Получатель (сервер)	Протокол	Номер порта
Определите сканер в приложении, например EpsonNet Config, а также драйвер сканера.	Сканер	ENPC (UDP)	3289
Соберите и настройте информацию MIB с приложения, например EpsonNet Config, а также драйвер сканера.	Сканер	SNMP (UDP)	161
Поиск сканера WSD	Сканер	WS-Discovery (UDP)	3702
Переадресация данных сканирования из приложения	Сканер	Сканирование сети (TCP)	1865
Сбор сведений о задании при сканировании с использованием технологии Push из приложения	Сканер	Сетевое сканирование с использованием технологии Push	2968
Web Config	Сканер	HTTP (TCP)	80
		HTTPS (TCP)	443

Решение проблем

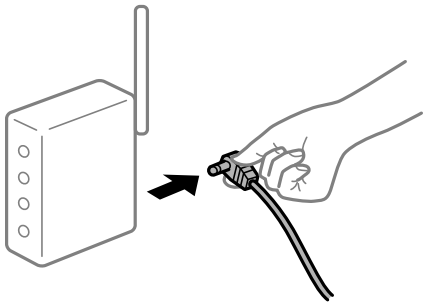
Не удается выполнить подключение к сети

Причиной этого могут быть следующие проблемы.

Возникают проблемы с сетевыми устройствами, подключенными по сети Wi-Fi.

Решения

Выключите устройства, которые вы хотите соединить по сети. Подождите примерно 10 секунд, после чего включите устройства в следующем порядке: беспроводной маршрутизатор, компьютер или интеллектуальное устройство, сканер. Переместите сканер и компьютер или интеллектуальное устройство ближе к беспроводному маршрутизатору для улучшения радиосвязи и попробуйте заново задать сетевые настройки.



Устройства не могут принять сигнал от беспроводного маршрутизатора, так как находятся слишком далеко от него.

Решения

Переместите компьютер, интеллектуальное устройство и сканер ближе к беспроводному маршрутизатору, после чего выключите и снова включите его.

После замены беспроводного маршрутизатора существующие настройки не подходят новому маршрутизатору.

Решения

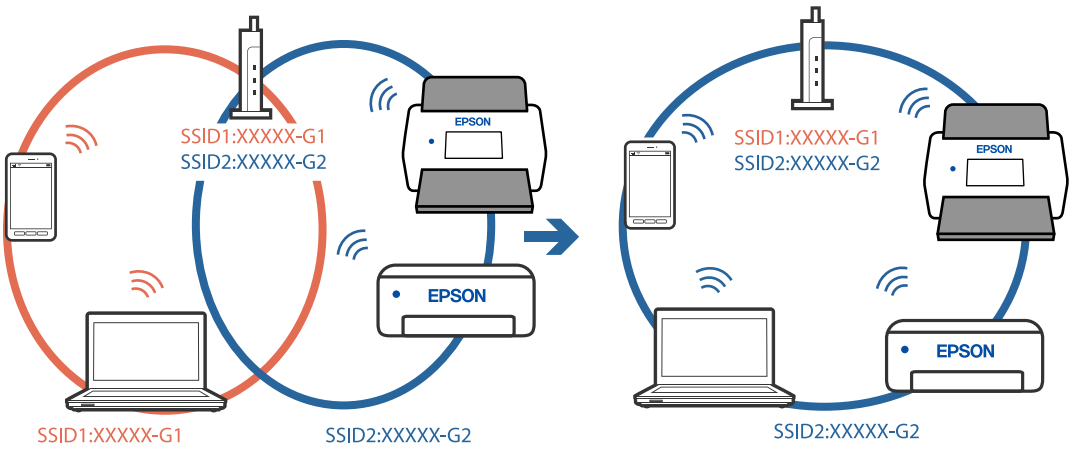
Заново задайте настройки подключения к сети, чтобы они соответствовали новому беспроводному маршрутизатору.

Имена сетей (идентификаторы SSID), к которым подключены компьютер или интеллектуальное устройство, разные.

Решения

Если вы одновременно используете несколько беспроводных маршрутизаторов или на беспроводном маршрутизаторе имеется несколько идентификаторов SSID, а устройства при этом подключены к разным SSID (то есть к сетям с разными именами), вы не сможете подключиться к беспроводному маршрутизатору.

Подключите компьютер или интеллектуальное устройство к сети с тем же SSID, что и сеть, к которой подключен сканер.



На беспроводном маршрутизаторе доступна функция разделения устройств.

Решения

Большинство беспроводных маршрутизаторов поддерживают функцию разделения устройств, которая блокирует связь между подключенными устройствами. Если вы не можете установить связь между сканером и компьютером или интеллектуальным устройством, даже если они подключены к одной сети, отключите функцию разделения устройств на беспроводном маршрутизаторе. За более подробной информацией обратитесь к руководству по беспроводному маршрутизатору.

IP-адрес назначен неправильно.

Решения

Если IP-адрес, назначенный сканеру, имеет вид 169.254.XXX.XXX, а для маски подсети настроено значение 255.255.0.0, то такой IP-адрес может быть назначен неправильно.

На панели управления принтера выберите **Настр.** > **Настройки сети** > **Расширенные** > **Настройка TCP/IP** и проверьте IP-адрес и маску подсети, назначенные сканеру.

Перезагрузите беспроводной маршрутизатор или сбросьте настройки сети на сканере.

На компьютере возникла проблема с настройками сети.

Решения

Попробуйте зайти на любой веб-сайт со своего компьютера, чтобы убедиться, что настройки сети на компьютере верны. Если вы не можете получить доступ ни к одному веб-сайту, это означает, что на компьютере имеются проблемы.

Проверьте сетевое подключение на компьютере. Для получения более подробной информации обратитесь к документации на компьютер.

Сканер подключен через Ethernet с помощью устройств, поддерживающих стандарт IEEE 802.3az (энергосберегающий Ethernet).

Решения

Если сканер подключается через Ethernet с помощью устройств, поддерживающих стандарт IEEE 802.3az (энергосберегающий Ethernet), то в зависимости от используемого концентратора или маршрутизатора могут возникать указанные ниже проблемы.

❏ Соединение становится нестабильным, сканер то подключается, то теряет соединение.

❏ Не удается подключить сканер.

❏ Скорость соединения снижается.

Выполните указанные ниже действия, чтобы отключить IEEE 802.3az для сканера, а затем снова подключите сканер.

1. Отсоедините Ethernet-кабель от компьютера и сканера.
2. Если на компьютере включена поддержка IEEE 802.3az, отключите ее.

   Для получения более подробной информации обратитесь к документации на компьютер.
3. Соедините сканер с компьютером напрямую с помощью кабеля Ethernet.
4. На сканере проверьте сетевые настройки.

   Выберите **Настр.** > **Настройки сети** > **Статус сети** > **Состоя. провод. ЛВС/Wi-Fi**.
5. Проверьте IP-адрес сканера.
6. Откройте на компьютере Web Config.

   Запустите какой-либо веб-браузер и введите IP-адрес сканера.

   «Запуск Web Config в веб-браузере» на стр. 37
7. Выберите вкладку **Сеть** > **Проводная сеть**.
8. Выберите значение **Выкл.** для параметра **IEEE 802.3az**.
9. Нажмите **Следующий**.
10. Нажмите **ОК**.
11. Отсоедините Ethernet-кабель от компьютера и сканера.
12. Если на шаге 2 вы отключили на компьютере поддержку IEEE 802.3az, включите ее снова.
13. Подключите к компьютеру и сканеру кабели Ethernet, которые вы отсоединили на шаге 1.

Если проблема по-прежнему сохраняется, возможно, ее причиной является не сканер, а другие устройства.

Сканер выключен

Решения

Убедитесь, что сканер включен.

Кроме того, подождите, пока индикатор не перестанет мигать светом (готовность к сканированию).

Программное обеспечение для настройки сканера

Web Config

Web Config — это приложение, которое работает в веб-браузере (например, Internet Explorer или Safari) на компьютере. Можно просмотреть состояние сканера или изменить параметры сетевой службы и сканера. Так как доступ к сканерам и управление ими осуществляются непосредственно из сети, это приложение подходит для настройки одного сканера за сеанс. Перед использованием Web Config подключите компьютер и сканер к одной и той же сети.

Поддерживаются следующие браузеры.

Microsoft Edge, Windows Internet Explorer 8 или более поздней версии, Firefox*, Chrome*, Safari*

* Используйте самую новую версию.

Запуск Web Config в веб-браузере

1. Проверьте IP-адрес сканера.

   Выберите **Настр.** > **Настройки сети** > **Статус сети** на панели управления сканера. Затем выберите состояние активного подключения (**Состоя. провод. ЛВС/Wi-Fi** или **Состояние Wi-Fi Direct**) для подтверждения IP-адреса сканера.

2. Откройте веб-браузер на компьютере или интеллектуальном устройстве, затем введите IP-адрес сканера.

   Формат:

   IPv4: http://IP-адрес сканера/

   IPv6: http://[IP-адрес сканера]/

   Например:

   IPv4: http://192.168.100.201/

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

   Примечание:
   Так как для доступа по протоколу HTTPS сканер использует самозаверяющий сертификат, то при запуске Web Config в браузере отображается предупреждение. Эта ситуация не указывает на проблему и может быть проигнорирована.

3. Выполните вход в качестве администратора для изменения настроек сканирования.

   Щелкните **Вход для администратора** в правой верхней части экрана. Введите **Имя пользователя** и **Текущий пароль** и нажмите **ОК**.

   Примечание:
   - ❏ *Ниже приведены первоначальные значения для сведений для администратора Web Config.*

     ·Имя пользователя: нет (пустое)

     ·Пароль: серийный номер сканера

     Серийный номер указан на этикетке снизу сканера.
   - ❏ *Если в правой верхней части экрана отображается **Выход для администратора**, вы уже выполнили вход в качестве администратора.*

Запуск Web Config в Windows

При подключении компьютера к сканеру через WSD выполните приведенные ниже действия, чтобы запустить Web Config.

1. Откройте список сканеров на компьютере.
   - ❏ Windows 10

     Нажмите кнопку «Пуск», затем выберите **Система Windows** > **Панель управления** > **Просмотр устройств и принтеров** в разделе **Оборудование и звук**.
   - ❏ Windows 8.1/Windows 8

     Выберите **Рабочий стол** > **Настройки** > **Панель управления** > **Просмотр устройств и принтеров** в разделе **Оборудование и звук** (или **Оборудование**).
   - ❏ Windows 7

     Нажмите кнопку «Пуск», выберите **Панель управления** > **Просмотр устройств и принтеров** в разделе **Оборудование и звук**.
2. Щелкните правой кнопкой мыши значок нужного сканера и выберите **Свойства**.
3. Выберите вкладку **Веб-служба** и щелкните URL-адрес.

   Так как для доступа по протоколу HTTPS сканер использует самозаверяющий сертификат, то при запуске Web Config в браузере отображается предупреждение. Эта ситуация не указывает на проблему и может быть проигнорирована.

   Примечание:
   - ❏ *Ниже приведены первоначальные значения для сведений для администратора Web Config.*

     ·Имя пользователя: нет (пустое)

     ·Пароль: серийный номер сканера

     Серийный номер указан на этикетке снизу сканера.
   - ❏ *Если в правой верхней части экрана отображается **Выход для администратора**, вы уже выполнили вход в качестве администратора.*

Epson Device Admin

Epson Device Admin — это многофункциональное приложение, позволяющее управлять устройствами в сети.

Для применения единых настроек к нескольким сканерам в сети можно использовать шаблоны конфигурации — это удобный способ установки большого количества сканеров и управления ими.

Приложение Epson Device Admin можно загрузить с сайта технической поддержки Epson. Для получения подробной информации о том, как использовать это приложение, обратитесь к документации или справке Epson Device Admin.

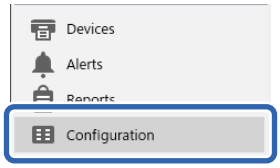
Шаблон конфигурации

Создание шаблона конфигурации

Создайте новый шаблон конфигурации.

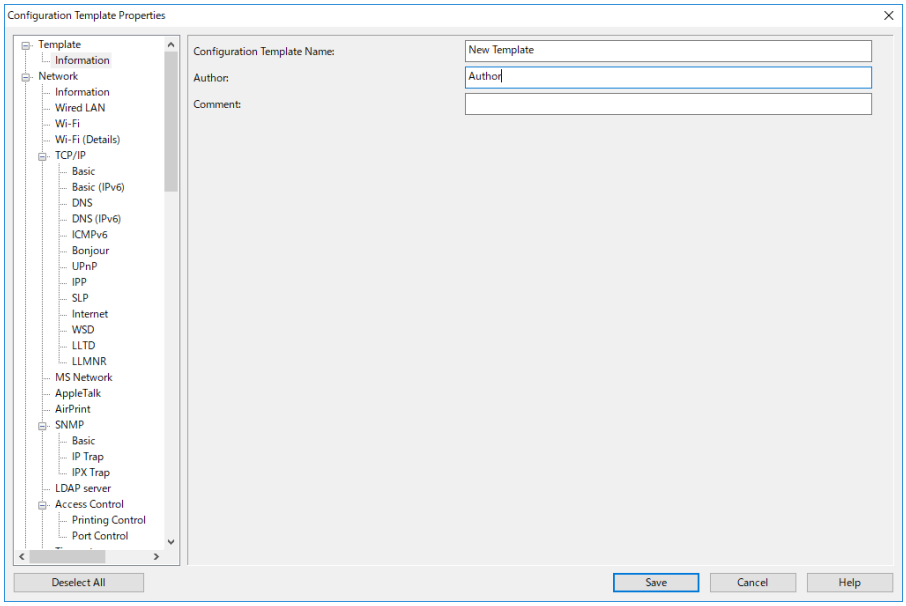
1. Запустите Epson Device Admin.

2. Выберите **Конфигурация** в меню задач боковой панели.



3. В меню-ленте выберите **Новый**.

4. Настройте каждый элемент.



Элемент	Описание
Название шаблона конфигурации	Имя шаблона конфигурации. Введите до 1024 символов в кодировке Юникод (UTF-8).

Элемент	Описание
Автор	Информация о создателе шаблона. Введите до 1024 символов в кодировке Юникод (UTF-8).
Комментарий	Укажите любую дополнительную информацию. Введите до 1024 символов в кодировке Юникод (UTF-8).

5. Слева выберите элементы, которые требуется настроить.

   Примечание:
   Выбирайте элементы меню слева для смены экранов. Заданное значение элемента сохраняется при смене экрана, но не сохраняется при отмене выбора экрана. Завершив настройку элементов, нажмите ***Сохранить****.*

Применение шаблона конфигурации

Применение сохраненного шаблона конфигурации на сканере. Применяются выбранные в шаблоне элементы. Элемент не применяется, если на целевом сканере отсутствует соответствующая функция.

Примечание:
Если на сканере установлен пароль администратора, настройте пароль заранее.

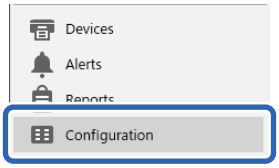
1. В меню-ленте на экране «Список устройств» выберите ***Настройки*** *>* ***Управление паролями****.*

2. Выберите ***Включить автоматическое управление паролями****, после чего щелкните* ***Управление паролями****.*

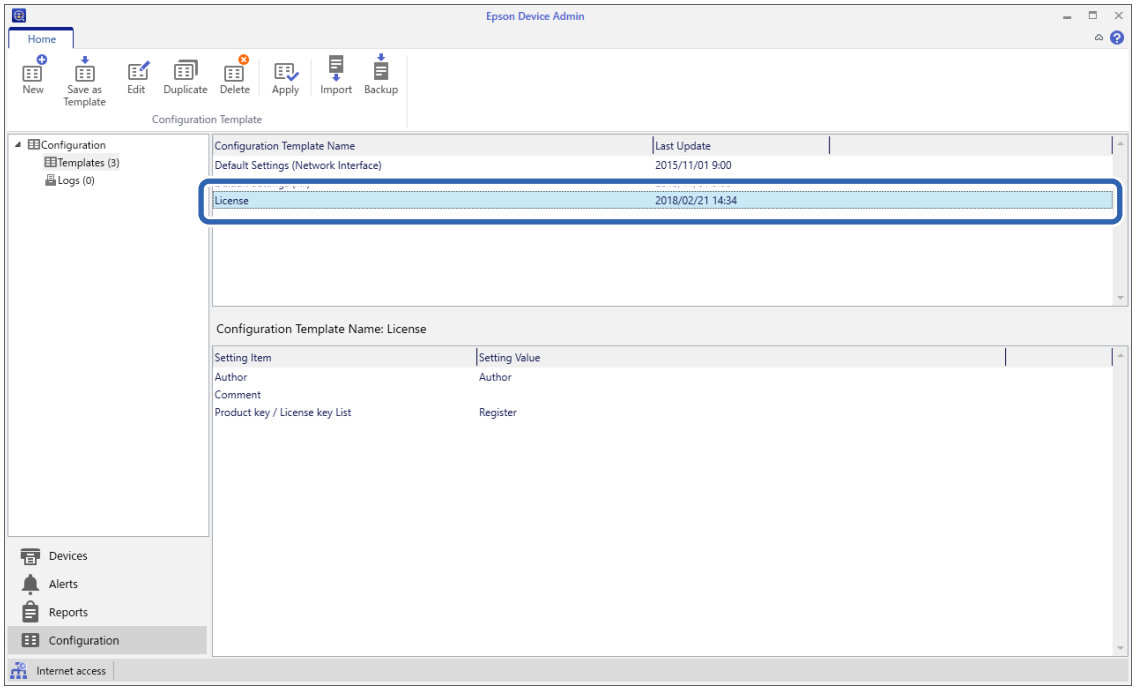
3. Выберите нужный сканер и нажмите ***Редактировать****.*

4. Задайте пароль и нажмите ***OK****.*

1. Выберите **Конфигурация** в меню задач сбоку.



2. В списке **Название шаблона конфигурации** выберите шаблон конфигурации, который необходимо применить.



3. Нажмите **Применить** в меню-ленте.

   Откроется экран выбора устройств.

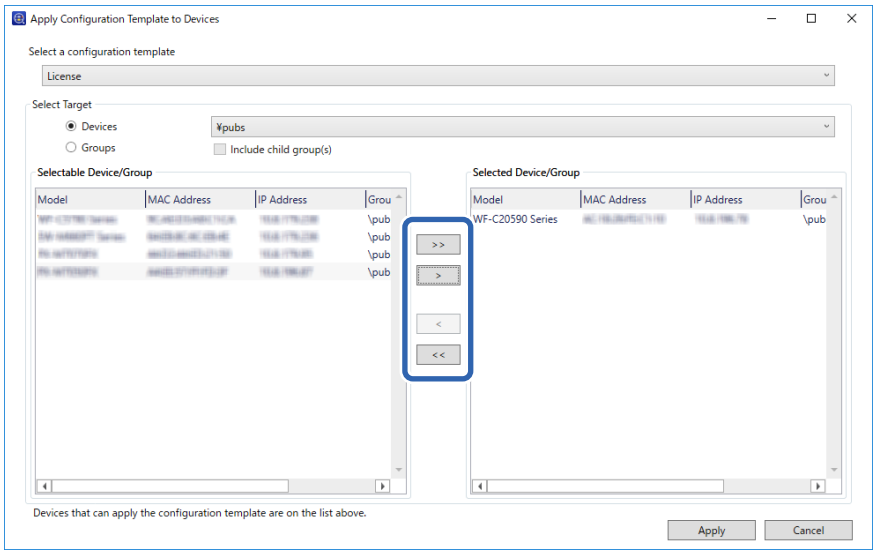
4. Выберите шаблон конфигурации, который необходимо применить.

   Примечание:

   ❏ *Если в раскрывающемся меню выбрать элемент **Устройства** и группы, содержащие устройства, отображается каждое из устройств.*

   ❏ *Группы отображаются, если выбран элемент **Группы**. Выберите элемент **Содержит дочерние группы (группу)**, чтобы автоматически выбрать дочерние группы в указанной группе.*

5. Переместите сканер или группы, к которым необходимо применить шаблон, в раздел **Выбранное устройство (группа)**.



6. Нажмите **Применить**.

   Откроется экран для подтверждения применения шаблона конфигурации.

7. Для применения шаблона конфигурации нажмите **OK**.

8. Когда появится сообщение о завершении процедуры, нажмите кнопку **OK**.

9. Нажмите **Сведения** и проверьте информацию.

   Если возле элементов, к которым применялись шаблоны, появился значок , значит, применение выполнено успешно.

10. Нажмите **Закрыть**.

Необходимые настройки сканирования

Настройка почтового сервера

Настройте в Web Config почтовый сервер.

Если на сканере настроен почтовый сервер и он может отправлять электронную почту, то предоставляются следующие функции.

❏ Передача результатов сканирования по электронной почте

❏ Получение уведомлений от сканера по электронной почте

Перед настройкой проверьте следующее.

❏ Сканер подключен к сети с доступом к почтовому серверу.

❏ Информация о настройке электронной почты на компьютере, использующем тот же почтовый сервер, что и сканер.

Примечание:

❏ *При использовании почтового сервера в Интернете уточните информацию о настройке у поставщика услуг или на веб-сайте.*

❏ *Также можно настроить почтовый сервер на панели управления сканера. Выполните указанные ниже действия.*

Настр. > ***Настройки сети*** > ***Расширенные*** > ***Сервер эл. почты*** > ***Настройки сервера***

1. Войдите в Web Config и выберите вкладку **Сеть** > **Сервер эл. почты** > **Основные**.
2. Введите значение для каждого элемента.
3. Выберите **ОК**.

   Отображаются выбранные параметры.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Параметры настройки почтового сервера

Параметры	Настройки и их описание	
Метод аутентификации	Укажите метод аутентификации для доступа сканера к почтовому серверу.	
	Выкл	При обмене данными с сервером электронной почты аутентификация отключена.
	АУТЕНТИФИКАЦИЯ SMTP	Необходимо, чтобы сервер электронной почты поддерживал аутентификацию SMTP.
	POP до SMTP	При выборе этого метода настройте параметры сервера POP3.
Проверенная учет. запись	Если вы выбрали значение **АУТЕНТИФИКАЦИЯ SMTP** или **POP до SMTP** для параметра **Метод аутентификации**, введите имя учетной записи, прошедшей проверку подлинности, длиной от 0 до 255 символов ASCII (от 0x20 до 0x7E).	

Параметры	Настройки и их описание	
Проверенный пароль	Если вы выбрали значение **АУТЕНТИФИКАЦИЯ SMTP** или **POP до SMTP** для параметра **Метод аутентификации**, введите пароль аутентификации длиной от 0 до 20 символов ASCII (с кодами от 0x20 до 0x7E).	
Адрес эл. почты отправителя	Введите адрес электронной почты отправителя. Введите от 0 до 255 символов ASCII (от 0x20 до 0x7E), за исключением : ( ) < > [ ] ; ¥. Точка (.) не может быть первым символом.	
Адрес сервера SMTP	Введите от 0 до 255 символов, используя символы в диапазоне от A до Z, от a до z, 0–9, а также . - . Используйте формат IPv4 или FQDN.	
Номер порта сервера SMTP	Введите число от 1 до 65535.	
Безопасное подключение	Укажите безопасный метод подключения к серверу электронной почты.	
	Нет	Если выбрать **POP до SMTP** в поле **Метод аутентификации**, для метода подключения будет установлено значение **Нет**.
	SSL/TLS	Это доступно, если для параметра **Метод аутентификации** установлено значение **Выкл** или **АУТЕНТИФИКАЦИЯ SMTP**.
	STARTTLS	Это доступно, если для параметра **Метод аутентификации** установлено значение **Выкл** или **АУТЕНТИФИКАЦИЯ SMTP**.
Проверка подлинности сертификатов	При включении этого режима проверяется сертификат. Рекомендуется задать значение **Включить**.	
Адрес сервера POP3	Если вы выбрали значение **POP до SMTP** для параметра **Метод аутентификации**, введите адрес сервера POP3 длиной от 0 до 255 символов, используя символы в диапазоне от A до Z, от a до z, 0–9, а также . - . Используйте формат IPv4 или FQDN.	
Номер порта сервера POP3	Если значение **POP до SMTP** указано для параметра **Метод аутентификации**, введите число 1 до 65535.	

Проверка соединения почтового сервера

Можно проверить соединение с почтовым сервером, запустив соответствующую процедуру.

1. Войдите в Web Config и выберите вкладку **Сеть** > **Сервер эл. почты** > **Проверка подключения**.
2. Выберите **Пуск**.

   Начнется проверка подключения к почтовому серверу. После завершения проверки отобразится отчет о проверке.

   Примечание:
   Соединение с почтовым сервером также можно проверить на панели управления. Выполните указанные ниже действия.

   Настр. > ***Настройки сети*** > ***Расширенные*** > ***Сервер эл. почты*** > ***Проверка подключения***

Пояснения к сообщениям, отображаемым при проверке соединения с почтовым сервером

Сообщения	Причина
Проверка подключения прошла успешно.	Это сообщение отображается, когда соединение с сервером установлено.
Ошибка связи с сервером SMTP. Проверьте следующее. - Параметры сети	Это сообщение отображается в следующих случаях. ❏ Сканер не подключен к сети. ❏ SMTP-сервер не работает. ❏ Сетевое подключение было прервано во время связи. ❏ Получены неполные данные.
Ошибка связи с сервером POP3. Проверьте следующее. - Параметры сети	Это сообщение отображается в следующих случаях. ❏ Сканер не подключен к сети. ❏ POP3-сервер не работает. ❏ Сетевое подключение было прервано во время связи. ❏ Получены неполные данные.
При подключении к серверу SMTP произошла ошибка. Проверьте следующее. - Адрес сервера SMTP - Сервер DNS	Это сообщение отображается в следующих случаях. ❏ Произошла ошибка при подключении к DNS-серверу. ❏ Произошла ошибка при разрешении имени SMTP-сервера.
При подключении к серверу POP3 произошла ошибка. Проверьте следующее. - Адрес сервера POP3 - Сервер DNS	Это сообщение отображается в следующих случаях. ❏ Произошла ошибка при подключении к DNS-серверу. ❏ Произошла ошибка при разрешении имени POP3-сервера.
Ошибка аутентификации сервера SMTP. Проверьте следующее. - Метод аутентификации - Подтвержденная учетная запись - Подтвержденный пароль	Это сообщение отображается, если произошла ошибка аутентификации на SMTP-сервере.
Ошибка аутентификации сервера POP3. Проверьте следующее. - Метод аутентификации - Подтвержденная учетная запись - Подтвержденный пароль	Это сообщение отображается, если произошла ошибка аутентификации на POP3-сервере.
Неподдерживаемый метод связи. Проверьте следующее. - Адрес сервера SMTP - Номер порта сервера SMTP	Это сообщение отображается при попытке использовать неподдерживаемый протокол.
Не удалось подключиться к серверу SMTP. Измените Безопасное подключение на Нет.	Это сообщение отображается при несоответствии параметров протокола SMTP на сервере и на клиенте или в том случае, если сервер не поддерживает безопасное подключение по SMTP (SSL-подключение).
Не удалось подключиться к серверу SMTP. Измените Безопасное подключение на SSL/TLS.	Это сообщение отображается при несоответствии параметров протокола SMTP на сервере и на клиенте или в том случае, если сервер запрашивает использование подключения по SSL/TLS для установки безопасного подключения SMTP.

Сообщения	Причина
Не удалось подключиться к серверу SMTP. Измените Безопасное подключение на STARTTLS.	Это сообщение отображается при несоответствии параметров протокола SMTP на сервере и на клиенте или в том случае, если сервер запрашивает использование подключения по STARTTLS для установки безопасного подключения SMTP.
Недоверенное соединение. Проверьте следующее. - Дата и время	Это сообщение отображается, если дата и время на сканере настроены неверно или истек срок действия сертификата.
Недоверенное соединение. Проверьте следующее. - Сертификат ЦС	Это сообщение отображается, если на сканере нет корневого сертификата, соответствующего данному серверу, или если Сертификат ЦС не был импортирован.
Подключение небезопасное.	Это сообщение отображается, если полученный сертификат поврежден.
Ошибка аутентификации сервера SMTP. Измените Метод аутентификации на SMTP-AUTH.	Это сообщение отображается, если метод аутентификации на сервере не соответствует методу аутентификации на клиенте. Сервер поддерживает АУТЕНТИФИКАЦИЯ SMTP.
Ошибка аутентификации сервера SMTP. Измените Метод аутентификации на POP перед SMTP.	Это сообщение отображается, если метод аутентификации на сервере не соответствует методу аутентификации на клиенте. Сервер не поддерживает АУТЕНТИФИКАЦИЯ SMTP.
Неверный адрес электронной почты отправителя. Укажите адрес электронной почты своей почтовой службы.	Это сообщение отображается, если указан неверный адрес эл. почты отправителя.
Доступ к устройству невозможен до завершения обработки.	Это сообщение отображается, если сканер занят.

Настройка общей сетевой папки

Задайте общую сетевую папку для сохранения отсканированных изображений.

При сохранении файла в папку сканер выполняет вход от имени пользователя компьютера, на котором была создана эта папка.

Создание общей папки

Соответствующая информация

- «Перед созданием общей папки» на стр. 47
- «Проверка сетевого профиля» на стр. 48
- «Место создания общей папки и пример организации безопасности» на стр. 48
- «Предоставление доступа на уровне групп и пользователей» на стр. 62

Перед созданием общей папки

Перед созданием общей папки проверьте следующее.

❏ Сканер подключен к сети, и у него есть доступ к компьютеру, на котором будет создана эта общая папка.

❏ В имени компьютера, на котором будет создана общая папка, не используются многобайтовые символы.

> ***Важно:***
>
> *Если в имя компьютера входит многобайтовый символ, то при сохранении файла в эту общую папку может произойти ошибка.*
>
> *В этом случае выберите компьютер, в имени которого нет многобайтовых символов, или измените имя компьютера.*
>
> *Изменение имени компьютера необходимо заранее согласовать с администратором, поскольку это может повлиять на некоторые параметры, такие как управление компьютером, доступ к ресурсам и т. д.*

Проверка сетевого профиля

На компьютере, на котором будет создана общая папка, проверьте возможность общего доступа к папкам.

1. Войдите на компьютер, на котором будет создана общая папка, используя учетную запись администратора.

2. Выберите **Панель управления** > **Сеть и Интернет** > **Центр управления сетями и общим доступом**.

3. Щелкните **Изменить дополнительные параметры общего доступа**, затем щелкните для профиля, для которого в текущих сетевых профилях указано **(текущий профиль)**.

4. Проверьте установку параметра **Включить общий доступ к файлам и принтерам** в разделе **Общий доступ к файлам и принтерам**.

   Если этот параметр уже выбран, щелкните **Отмена** и закройте окно.

   При изменении параметра щелкните **Сохранить изменения** и закройте окно.

Место создания общей папки и пример организации безопасности

В зависимости от места создания общей папки баланс защиты и удобства может меняться.

Для использования общей папки со сканеров или других компьютеров требуется настроить для нее следующие разрешения на чтение и изменение.

❏ Вкладка **Общий доступ** > **Дополнительный общий доступ** > **Разрешения**

Это управление разрешениями на сетевой доступ к этой общей папке.

❏ Разрешение доступа на вкладке **Безопасность**

Это управление разрешениями на сетевой и локальный доступ к этой общей папке.

При выборе варианта **Все** для общей папки, созданной для примера на рабочем столе, доступ будет предоставлен всем пользователям, которым доступен этот компьютер.

Однако пользователям без доступа папка будет недоступна, поскольку рабочий стол (папка) принадлежит папке пользователя и наследует параметры безопасности этой папки. Пользователь, которому предоставлен доступ на вкладке **Безопасность** (в данном случае это пользователь, вошедший с правами администратора), может работать с этой папкой.

Правильное местоположение указано ниже.

Это пример создания папки scan_folder.

Соответствующая информация

➡ «Пример конфигурации файловых серверов» на стр. 49

➡ «Пример конфигурации персонального компьютера» на стр. 56

Пример конфигурации файловых серверов

Ниже описан пример создания общей папки в корне диска на общем компьютере, например на файловом сервере, при следующих условиях.

Пользователи, доступ которых контролируется, например пользователи этого же домена компьютера, на котором создается общая папка, должны получать доступ к ней.

Установите эту конфигурацию, чтобы разрешить всем пользователям выполнять чтение и запись в общую папку на компьютере, таком как файловый сервер и общий компьютер.

❏ Место создания общей папки: корень диска

❏ Путь к папке: C:\scan_folder

❏ Разрешение на доступ по сети (разрешения для общего ресурса): все

❏ Разрешение на доступ к файловой системе (безопасность): прошедшие проверку

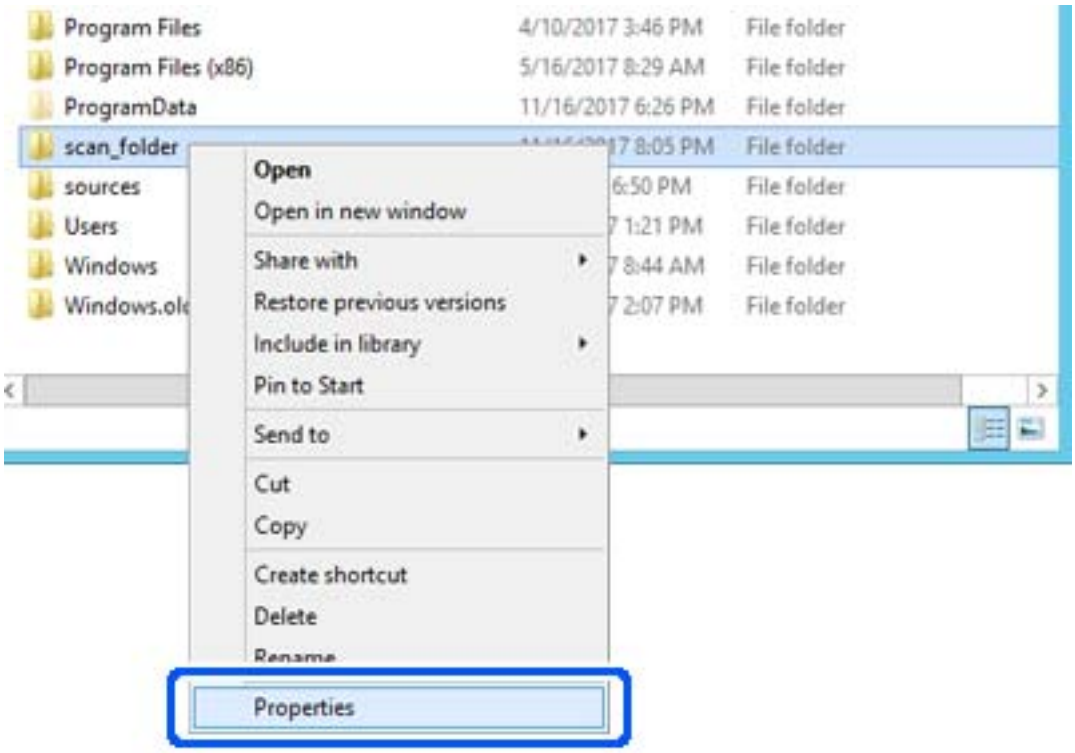
1. Войдите на компьютер, на котором будет создана общая папка, используя учетную запись администратора.

2. Откройте проводник.

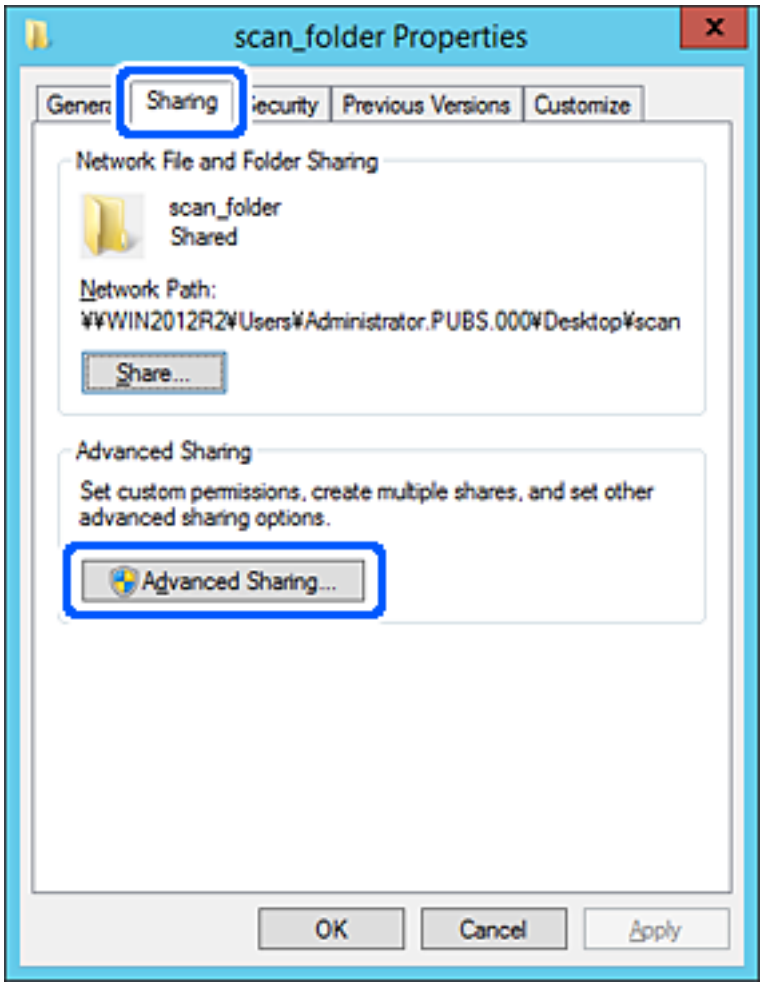
3. Создайте папку в корне диска и присвойте ей имя scan_folder.

   Для имени папки введите от 1 до 12 буквенно-цифровых символов. При превышении ограничения символов для имени папки она будет недоступна.

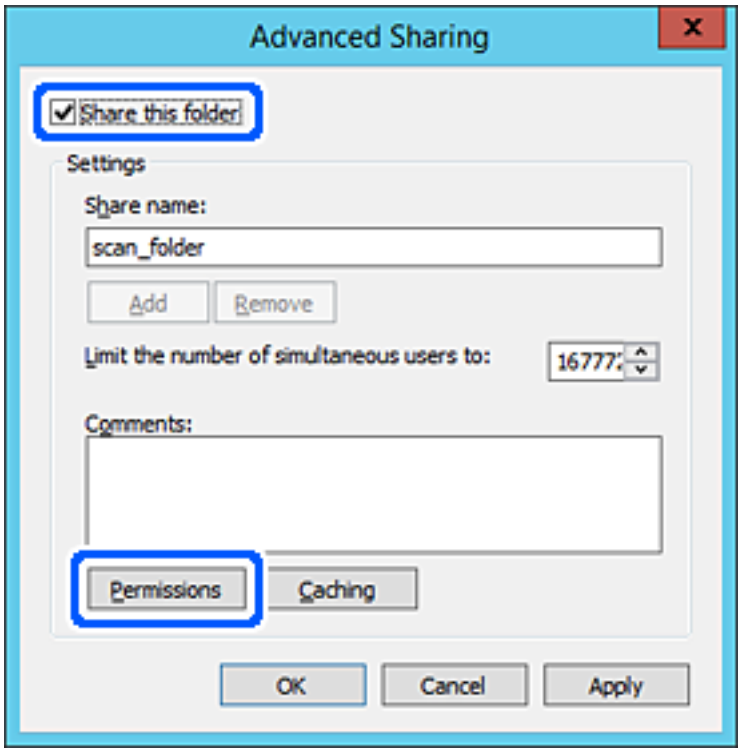
4. Щелкните папку правой кнопкой мыши и выберите **Свойства**.



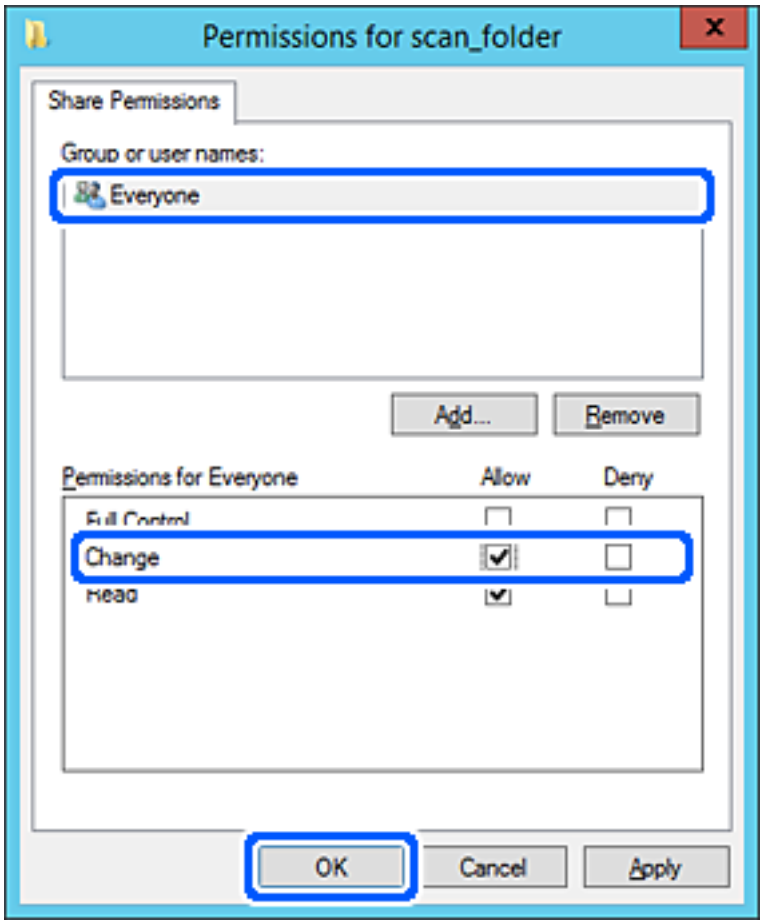
5. Щелкните **Дополнительный общий доступ** на вкладке **Общий доступ**.



6. Выберите **Общий доступ к папке**, затем щелкните **Разрешения**.

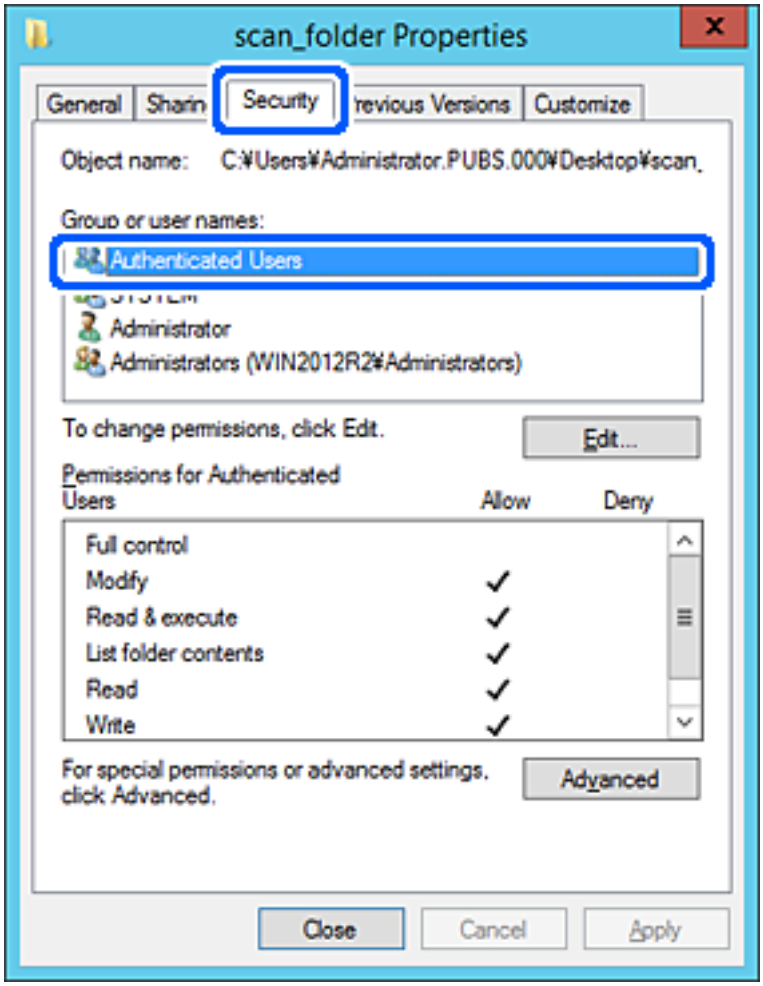


7. Выберите группу **Все** в разделе **Группы или пользователи**, выберите **Разрешить** в разделе **Изменить** и нажмите кнопку **OK**.



8. Нажмите **OK**.

9. Перейдите на вкладку **Безопасность** и выберите **Прошедшие проверку** в разделе **Группа или пользователи**.

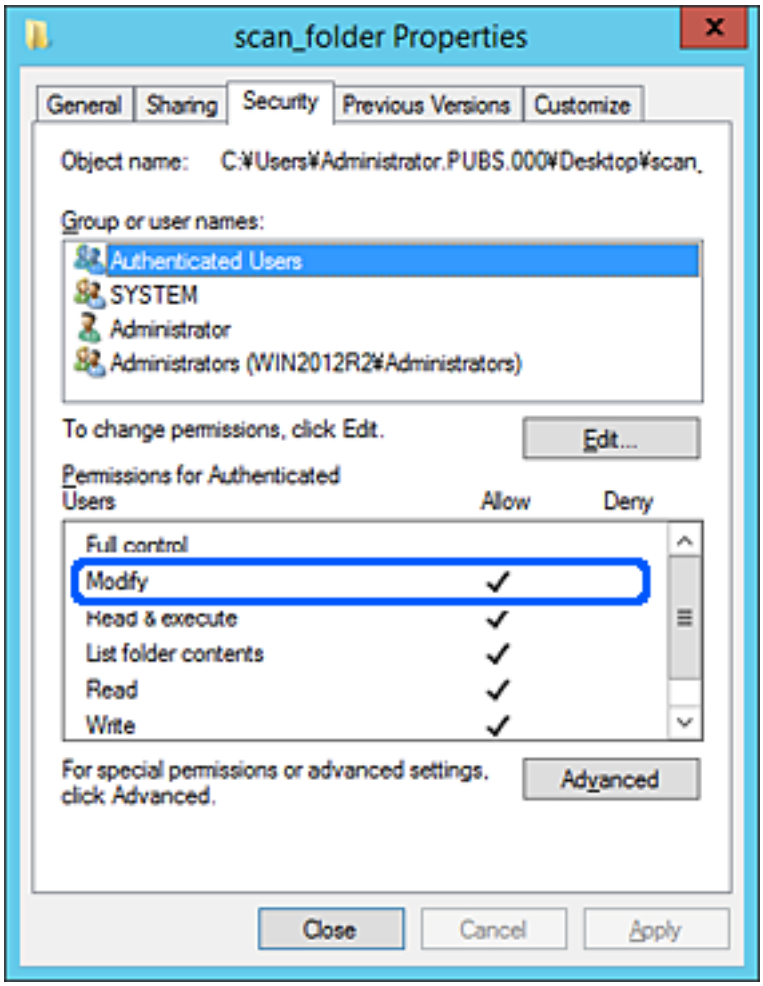


«Прошедшие проверку» — это специальная группа, в которую входят все пользователи, которые могут войти в домен или на компьютер. Эта группа отображается только в том случае, если папка создана непосредственно в корневой папке.

Если она не отображается, ее можно добавить, щелкнув **Изменить**. Дополнительные сведения см. в разделе «Подробная информация».

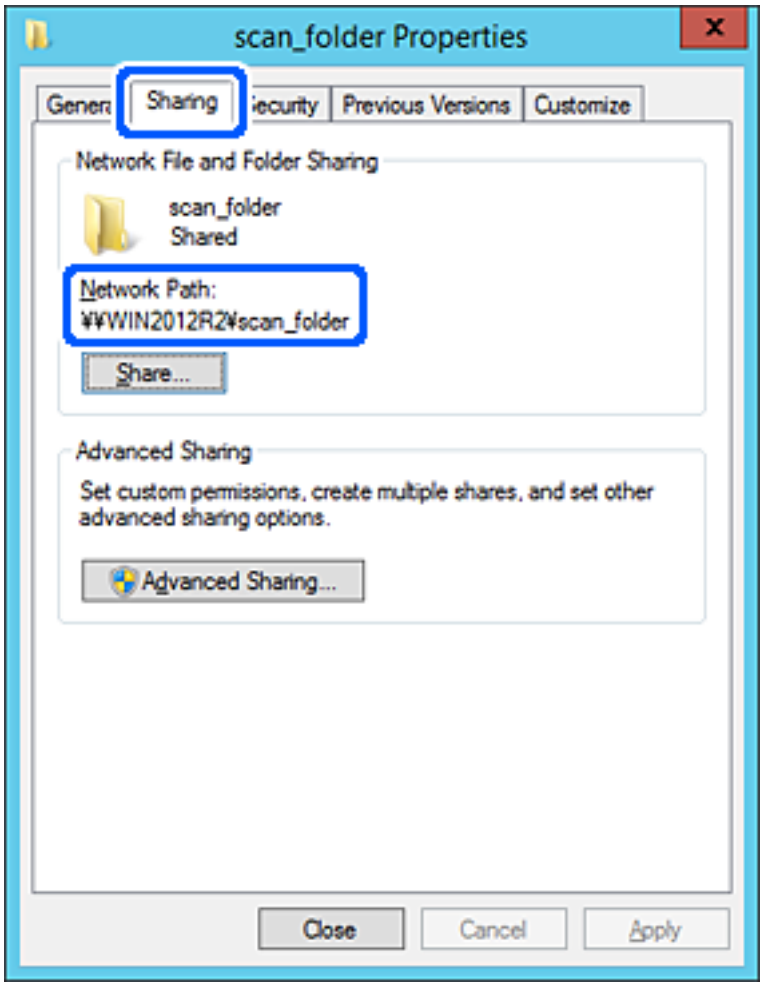
10. Убедитесь, что для параметра **Изменение** выбрано **Разрешить** в разделе **Разрешения для проверенных пользователей**.

    Если этот параметр не выбран, выберите **Проверенные пользователи**, щелкните **Изменить**, выберите **Разрешить** для **Изменить** в разделе **Разрешения для проверенных пользователей** и нажмите кнопку **OK**.



11. Перейдите на вкладку **Общий доступ**.

    Отобразится сетевой путь к данной общей папке. Он используется при регистрации в списке контактов сканера. Запишите его.



12. Нажмите **OK** или **Закрыть**, чтобы закрыть это окно.

    Проверьте возможность чтения или записи файла в этой общей папке с компьютеров в этом же домене.

Соответствующая информация

➡ «Предоставление доступа на уровне групп и пользователей» на стр. 62

➡ «Регистрация получателя в контактах с использованием Web Config» на стр. 67

Пример конфигурации персонального компьютера

Ниже описан пример создания общей папки на рабочем столе пользователя, вошедшего в данный момент в систему компьютера.

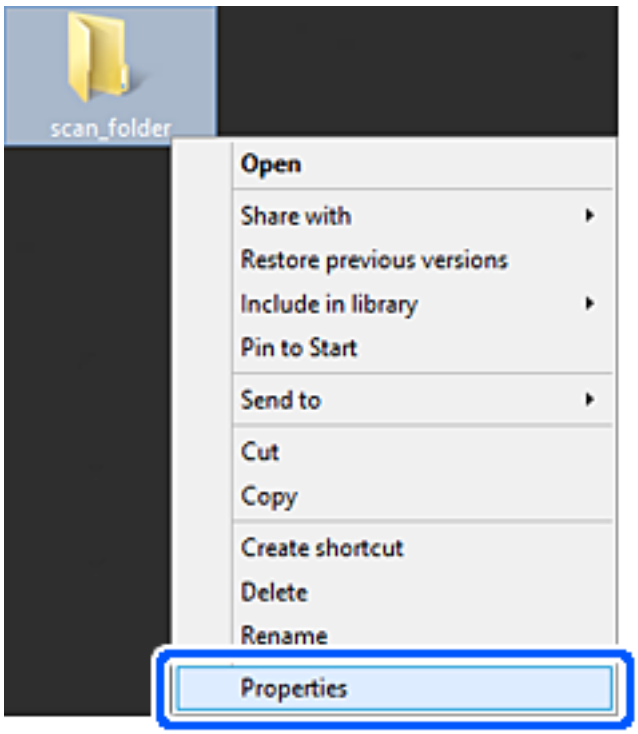
Пользователь, вошедший в систему компьютера и имеющий права администратора, получает доступ к папке на рабочем столе и к папке с документами, которые находятся в папке User.

Установите эту конфигурацию, чтобы НЕ РАЗРЕШИТЬ другим пользователям чтение и запись для этой общей папки на компьютере.

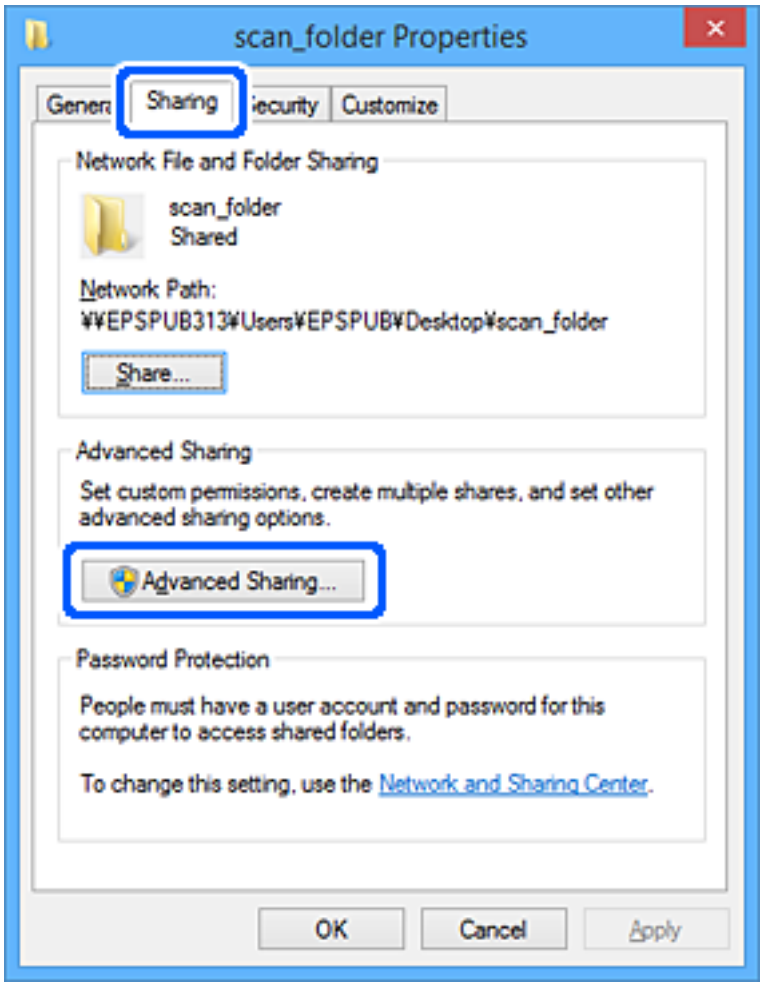
- ❏ Место создания общей папки: рабочий стол
- ❏ Путь к папке: C:\Users\xxxx\Desktop\scan_folder
- ❏ Разрешение на доступ по сети (разрешения для общего ресурса): все
- ❏ Разрешение на доступ к файловой системе (безопасность): для разрешения доступа добавьте соответствующие имена пользователей/групп или не добавляйте их, если доступ следует запретить.

1. Войдите на компьютер, на котором будет создана общая папка, используя учетную запись администратора.
2. Откройте проводник.
3. Создайте папку на рабочем столе и присвойте ей имя scan_folder.

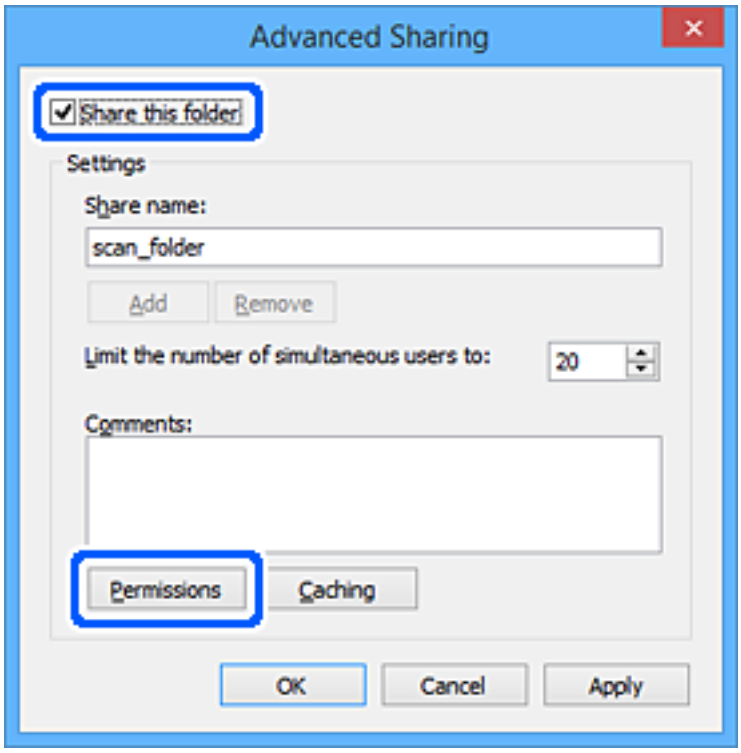
   Для имени папки введите от 1 до 12 буквенно-цифровых символов. При превышении ограничения символов для имени папки она будет недоступна.
4. Щелкните папку правой кнопкой мыши и выберите **Свойства**.



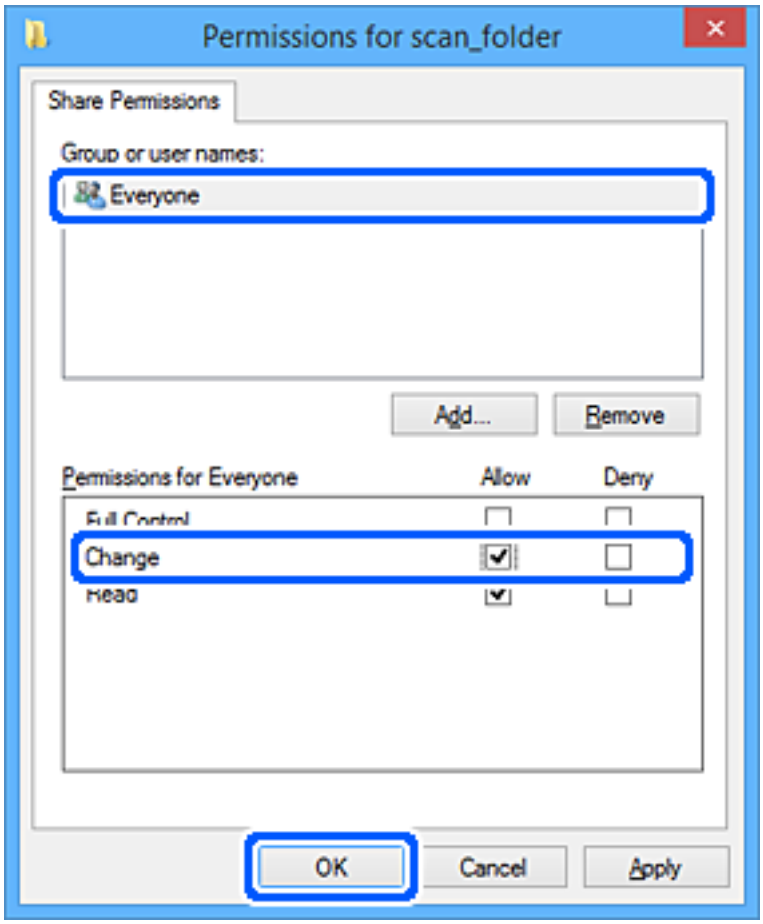
5. Щелкните **Дополнительный общий доступ** на вкладке **Общий доступ**.



6. Выберите **Общий доступ к папке**, затем щелкните **Разрешения**.



7. Выберите группу **Все** в разделе **Группы или пользователи**, выберите **Разрешить** в разделе **Изменить** и нажмите кнопку **OK**.



8. Нажмите **OK**.

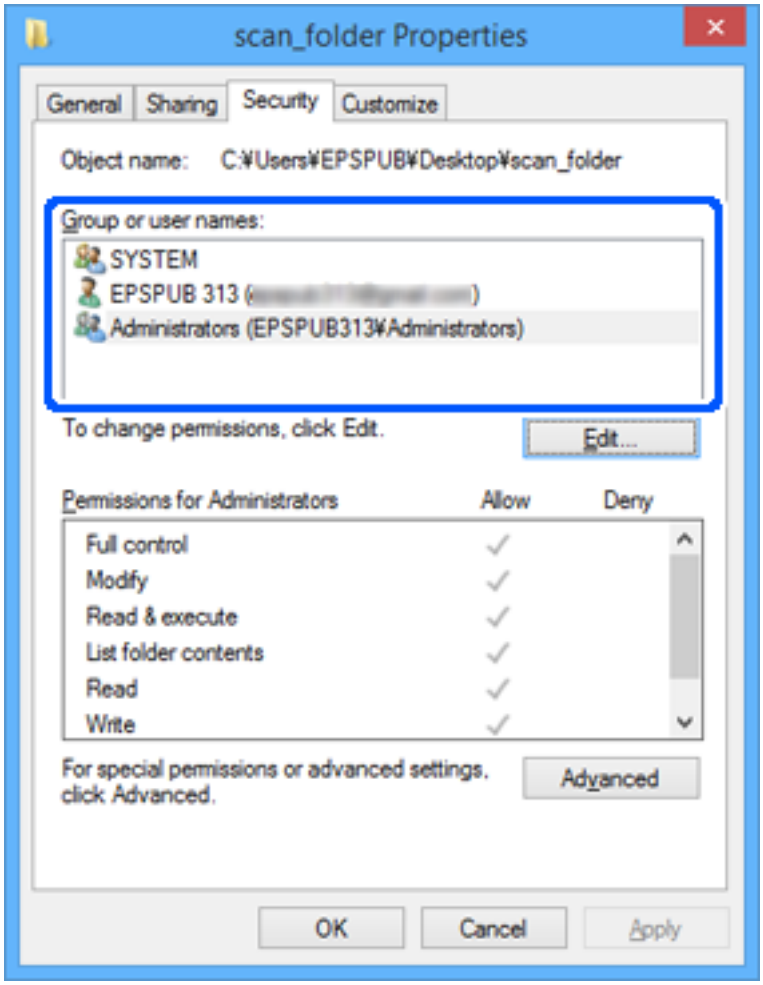
9. Перейдите на вкладку **Безопасность**.

10. Проверьте списки групп или пользователей в разделе **Группа или пользователи**.

    Данные группы и пользователи будут иметь доступ к этой общей папке.

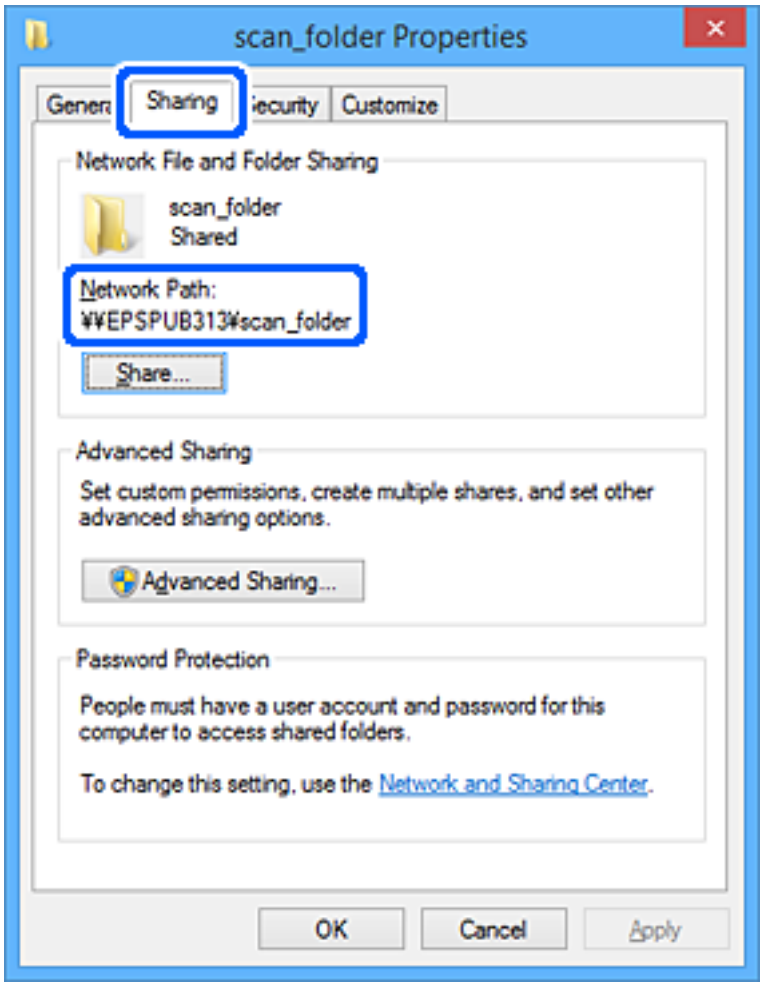
    В данном случае доступ к этой общей папке получат пользователь, вошедший в систему компьютера, и администратор.

При необходимости добавьте разрешение на доступ. Его можно добавить, нажав кнопку **Изменить**. Дополнительные сведения см. в разделе «Подробная информация».



11. Перейдите на вкладку **Общий доступ**.

    Отобразится сетевой путь к данной общей папке. Он используется при регистрации в списке контактов сканера. Запишите его.



12. Нажмите **OK** или **Закрыть**, чтобы закрыть это окно.

    Проверьте возможность чтения или записи файла в данной общей папке на компьютерах пользователей и групп, которым был открыт этот доступ.

Соответствующая информация

➡ «Предоставление доступа на уровне групп и пользователей» на стр. 62

➡ «Регистрация получателя в контактах с использованием Web Config» на стр. 67

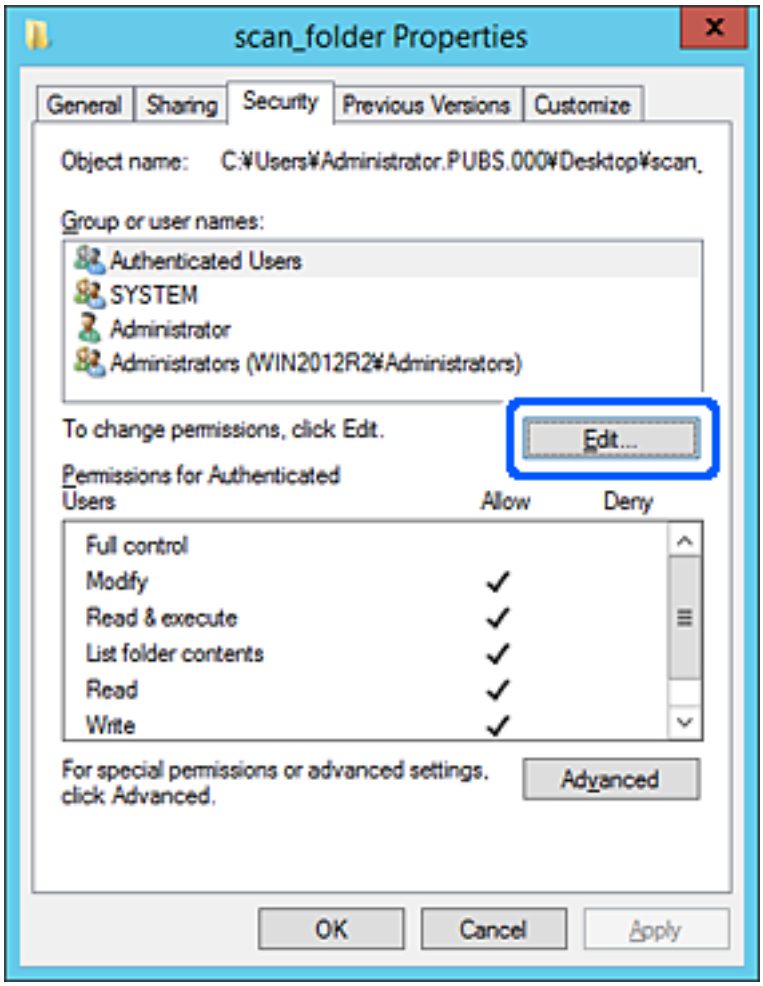
Предоставление доступа на уровне групп и пользователей

Можно предоставлять доступ к устройству, добавляя группы и отдельных пользователей.

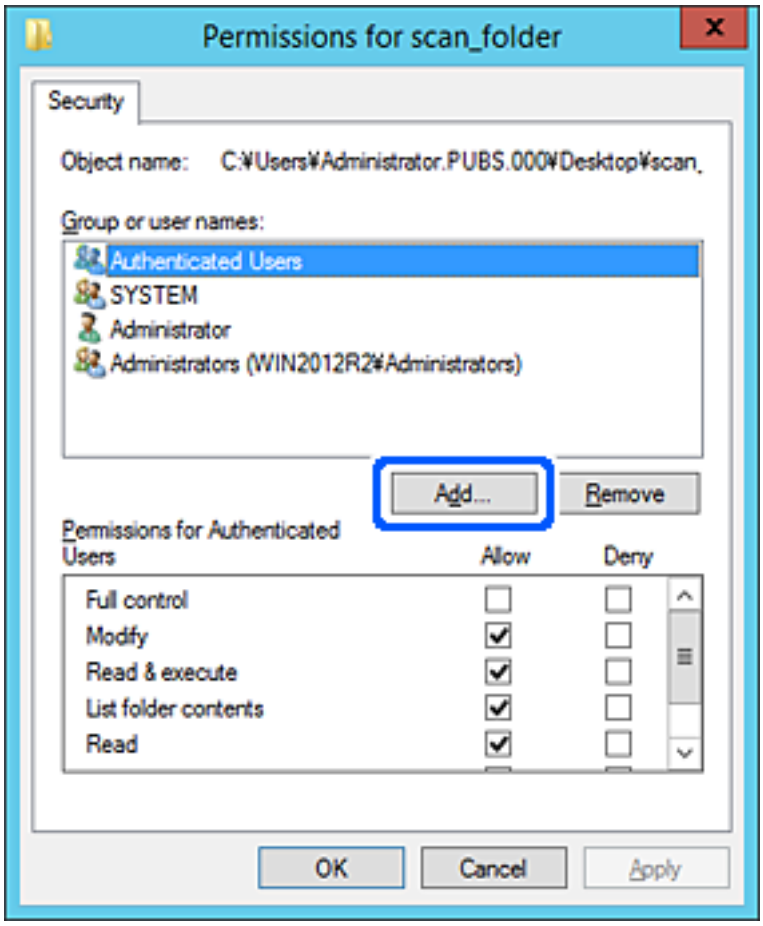
1. Щелкните данную папку правой кнопкой мыши и выберите **Свойства**.

2. Перейдите на вкладку **Безопасность**.

3. Щелкните **Изменить**.



4. Нажмите кнопку **Добавить** в разделе **Группа или пользователи**.

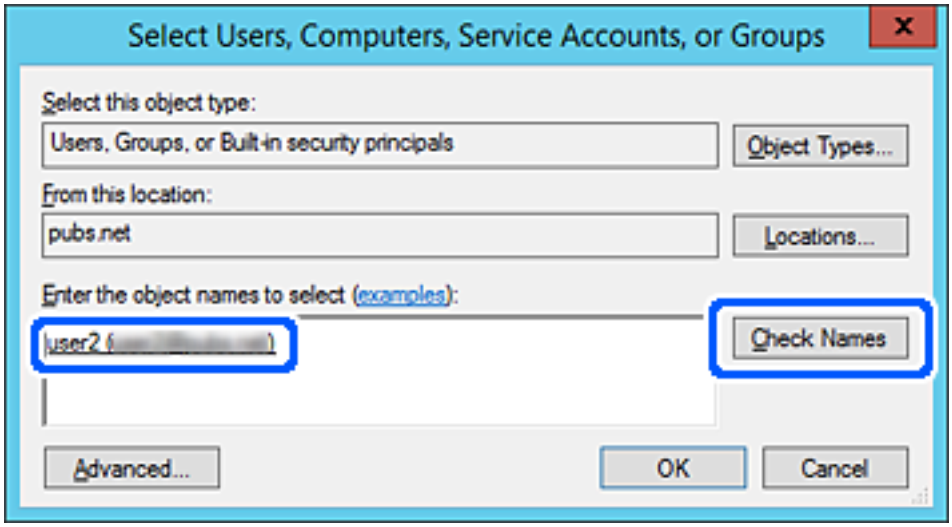


5. Введите имя группы или пользователя, которым необходимо предоставить доступ, и щелкните **Проверить имена**.

   К имени добавляется подчеркивание.

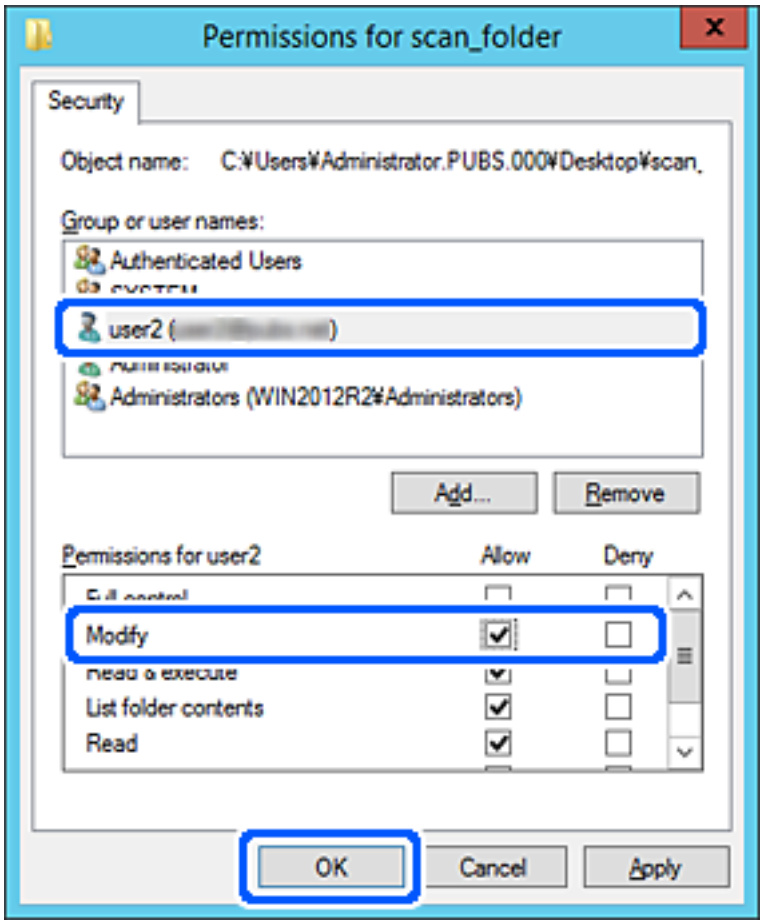
Примечание:
Если вам неизвестно полное имя группы или пользователя, введите часть имени и щелкните ***Проверить имена****. Будет выведен список имен групп или пользователей, соответствующих указанной части имени, в котором можно выбрать полное имя.*

Если указанной части имени соответствует только одно имя, в поле ***Введите имена выбираемых объектов*** *появится полное имя с подчеркиванием.*



6. Щелкните **OK**.

7. На экране «Разрешения» выберите имя пользователя, введенное в разделе **Группа или пользователи**, предоставьте доступ на **Изменение** и нажмите **OK**.



8. Нажмите **OK** или **Закрыть**, чтобы закрыть это окно.

   Проверьте возможность чтения или записи файла в данной общей папке на компьютерах пользователей и групп, которым был открыт этот доступ.

Обеспечение доступности контактов

Зарегистрировав места назначения в списке контактов сканера, вы можете легко вводить эти места назначения при выполнении сканирования.

В списке контактов можно зарегистрировать указанные ниже типы мест назначений. Всего можно зарегистрировать до 300 записей.

Примечание:
Для ввода мест назначения также можно использовать сервер LDAP (поиск LDAP).

Эл. почта	Получатель сообщения электронной почты. Предварительно нужно задать параметры почтового сервера.
Сетевая папка	Место сохранения данных сканирования. Необходимо заблаговременно подготовить сетевую папку.

Соответствующая информация

➡ «Взаимодействие между сервером LDAP и пользователями» на стр. 73

Сравнение настроек контактов

Существуют три инструмента для настройки списка контактов сканера: Web Config, Epson Device Admin и панель управления сканера. Различия между тремя инструментами перечислены в таблице ниже.

Функции	Web Config*	Epson Device Admin	Панель управления сканера
Регистрация получателя	✓	✓	✓
Редактирование получателя	✓	✓	✓
Добавление группы	✓	✓	✓
Редактирование группы	✓	✓	✓
Удаление получателя или групп	✓	✓	✓
Удаление всех получателей	✓	✓	—
Импорт файла	✓	✓	—
Экспорт файла	✓	✓	—

* Войдите в систему как администратор для выполнения настроек.

Регистрация получателя в контактах с использованием Web Config

Примечание:
Также можно зарегистрировать контакты на панели управления сканера.

1. Войдите в Web Config и выберите вкладку **Скан.** > **Контакты**.
2. Выберите номер для регистрации и нажмите **Изменить**.
3. Введите **Имя** и **Ключевое слово**.
4. Выберите тип получателя, используя параметр **Тип**.

   Примечание:
   *После завершения регистрации изменить параметр **Тип** невозможно. Для изменения типа удалите получателя, а затем повторно его зарегистрируйте.*
5. Введите значение для каждого элемента и затем нажмите **Применить**.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Настройка параметров получателя

Параметры	Настройки и их описание
Общие настройки	
Имя	Введите имя, отображаемое в контактах, длиной не более 30 символов Юникода (UTF-8). Если не нужно указывать это значение, оставьте поле пустым.
Ключевое слово	Введите имя длиной не более 30 символов Юникода (UTF-8) для поиска контактов на панели управления принтера. Если не нужно указывать это значение, оставьте поле пустым.
Тип	Выберите тип адреса, который следует зарегистрировать.
Отнести к часто использ.	Выберите для определения зарегистрированного адреса в качестве часто используемого. Если этот адрес задается в качестве часто используемого адреса, он будет отображаться в верхней части экрана сканирования и целевой адрес можно будет выбрать без отображения списка контактов.
Эл. почта	
Адрес эл. почты	Введите от 1 до 255 символов, используя символы от A до Z, от a до z, цифры от 0 до 9 и символы ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Сетевая папка (SMB)	
Сохранить в	\\«Путь к папке» Введите местоположение, где располагается сетевая папка, длиной от 1 до 253 символов Юникода (UTF-8), не вводите символы «\\». Введите сетевой путь, отображаемый на экране свойств папки. Информацию об установке сетевого пути см. ниже. «Пример конфигурации персонального компьютера» на стр. 56
Имя пользователя	Введите имя пользователя для доступа к сетевой папке длиной не более 30 символов Юникода (UTF-8). Не используйте при этом управляющие символы (от 0x00 до 0x1f, 0x7F).
Пароль	Введите пароль для доступа к сетевой папке длиной не более 20 символов Юникода (UTF-8). Не используйте при этом управляющие символы (от 0x00 до 0x1f, 0x7F).
FTP	
Безопасное подключение	Выберите FTP или FTPS в соответствии с протоколом, поддерживаемым FTP-сервером. Выберите **FTPS**, чтобы сканер поддерживал связь с применением мер безопасности.
Сохранить в	Введите имя сервера без указания префикса ftp:// или ftps://. Можно ввести от 1 до 253 символов в кодировке ASCII (символы с кодами от 0x20 до 0x7E).

Параметры	Настройки и их описание
Имя пользователя	Введите имя пользователя для доступа к FTP-серверу длиной не более 30 символов Юникода (UTF-8). Не используйте при этом управляющие символы (от 0x00 до 0x1f, 0x7F). Если сервер допускает анонимное подключение, введите любое имя пользователя, например Anonymous или FTP. Если не нужно указывать это значение, оставьте поле пустым.
Пароль	Введите пароль для доступа к FTP-серверу длиной не более 20 символов Юникода (UTF-8). Не используйте при этом управляющие символы (от 0x00 до 0x1f, 0x7F). Если не нужно указывать это значение, оставьте поле пустым.
Режим подключения	Выберите режим подключения из меню. Если брандмауэр установлен между сканером и FTP-сервером, выберите **Пассивный режим**.
Номер порта	Введите номер порта FTP-сервера в диапазоне от 1 до 65535.
Проверка подлинности сертификатов	При включении этого параметра проверяется сертификат FTP-сервера. Этот режим доступен, если для параметра **FTPS** выбрано значение **Безопасное подключение**. Для такой настройки на сканер должен быть импортирован Сертификат ЦС.
SharePoint(WebDAV)	
Безопасное подключение	Выберите HTTP или HTTPS в соответствии с протоколом, поддерживаемым сервером. Выберите **HTTPS**, чтобы сканер поддерживал связь с применением мер безопасности.
Сохранить в	Введите имя сервера без указания префикса http:// или https://. Можно ввести от 1 до 253 символов в кодировке ASCII (символы с кодами от 0x20 до 0x7E).
Имя пользователя	Введите имя пользователя для доступа к серверу длиной не более 30 символов Юникода (UTF-8). Не используйте при этом управляющие символы (от 0x00 до 0x1f, 0x7F). Если не нужно указывать это значение, оставьте поле пустым.
Пароль	Введите пароль для доступа к серверу длиной не более 20 символов Юникода (UTF-8). Не используйте при этом управляющие символы (от 0x00 до 0x1f, 0x7F). Если не нужно указывать это значение, оставьте поле пустым.
Проверка подлинности сертификатов	При включении этого параметра проверяется сертификат сервера. Этот режим доступен, если для параметра **Безопасное подключение** выбрано значение **HTTPS**. Для такой настройки на сканер должен быть импортирован Сертификат ЦС.
Прокси-сервер	Выберите, использовать или нет прокси-сервер.

Регистрация мест назначения (получателей) в виде группы с помощью Web Config

Если в качестве типа места назначения используется **Эл. почта**, несколько мест назначения можно зарегистрировать как группу.

1. Войдите в Web Config и выберите вкладку **Скан.** > **Контакты**.

2. Выберите номер для регистрации и нажмите **Изменить**.

3. Выберите группу в разделе **Тип**.
4. Нажмите **Выбрать** для **Контакт(ы) для Группы**.

   Отобразится список доступных получателей.
5. Выберите получателей для регистрации в группе и нажмите **Выбрать**.
6. Введите **Имя** и **Ключевое слово**.
7. Выберите, следует ли назначать зарегистрированную группу в группу часто используемых получателей.

   Примечание:
   Получателя можно зарегистрировать в нескольких группах.
8. Нажмите **Применить**.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Резервное копирование и импорт контактов

С помощью Web Config и других средств можно импортировать список контактов или сделать его резервную копию.

С помощью Web Config можно сделать резервную копию списка контактов, экспортировав параметры сканера, которые включают и контакты. Файл экспортируется как двоичный, поэтому его нельзя будет изменить.

При импорте такого файла параметров на сканер контакты переписываются.

При использовании Epson Device Admin с экрана свойств устройства могут быть экспортированы только контакты. Кроме того, если связанные с безопасностью элементы не экспортируются, можно изменить экспортированные контакты и импортировать их, поскольку их можно сохранить как файл SYLK или CSV.

Импорт контактов с помощью Web Config

Если у вас есть сканер, который поддерживает резервное копирование контактов и совместим с данным сканером, вы легко можете зарегистрировать контакты путем импорта файла резервной копии.

Примечание:
Инструкции по резервному копированию контактов сканера см. в руководстве по сканеру.

Для импорта контактов на сканер выполните следующие действия.

1. Откройте Web Config, выберите вкладку **Управление устройствами** > **Значение настройки экспорта и импорта** > **Импорт**.
2. Выберите файл резервной копии, созданный в разделе **Файл**, введите пароль и щелкните **Следующий**.
3. Установите флажок **Контакты** и щелкните **Следующий**.

Резервное копирование контактов с помощью Web Config

Из-за сбоя в работе сканера контакты могут быть потеряны. Мы рекомендуем выполнять резервное копирование после каждого обновления данных. Компания Epson не несет ответственности за какую-либо потерю и восстановление данных или настроек даже во время гарантийного периода.

С помощью Web Config можно также создать на компьютере резервную копию контактов, хранящихся на сканере.

1. Войдите в Web Config и выберите вкладку **Управление устройствами** > **Значение настройки экспорта и импорта** > **Экспорт**.
2. Установите флажок **Контакты** в категории **Скан.**.
3. Введите пароль для шифрования экспортированного файла.

   Для импорта файла необходим пароль. Оставьте поле пароля пустым, если не требуется шифрование файла.
4. Нажмите **Экспорт**.

Экспорт и массовая регистрация контактов с использованием инструмента

При использовании Epson Device Admin можно создать резервную копию только списка контактов, изменить экспортированные файлы, а затем зарегистрировать весь список за один раз.

Это полезно, если нужна резервная копия только списка контактов или если заменяется сканер и необходимо перенести на него контакты со старого сканера.

Экспорт контактов

Сохранение информации о контактах в файл.

Файлы, сохраненные в форматах SYLK и CSV, можно отредактировать с помощью программы для работы с таблицами или текстового редактора. После удаления или добавления этой информации ее можно зарегистрировать всю за один раз.

Информация, содержащая элементы безопасности, например пароли и личную информацию, может быть сохранена в двоичном формате, защищенном паролем. Такой файл изменить будет нельзя. Он может использоваться в качестве резервной копии информации, в том числе элементов безопасности.

1. Запустите Epson Device Admin.
2. Выберите **Устройства** в меню задач сбоку.
3. Выберите устройство для настройки в списке устройств.
4. Щелкните **Конфигурация устройства** на вкладке **Главная** меню ленты.

   После установки пароля администратора введите его и нажмите **OK**.
5. Щелкните **Общий** > **Контактная информация**.

6. Выберите формат экспорта в **Экспорт** >**Экспорт элементов**.

   ❏ Все элементы

   Экспортируйте зашифрованный двоичный файл. Выберите, должны ли быть включены элементы безопасности, такие как пароль и личная информация. Такой файл изменить будет нельзя. При выборе этого варианта необходимо установить пароль. Щелкните **Конфигурация** и установите пароль длиной от 8 до 63 символов в ASCII. Этот пароль требуется при импорте двоичного файла.

   ❏ Элементы кроме информации о безопасности

   Экспортируйте файлы в формате SYLK или CSV. Выберите этот вариант, если будет нужно изменить информацию в экспортированном файле.

7. Нажмите **Экспорт**.

8. Укажите место сохранения файла, выберите тип файла и щелкните **Сохранить**.

   Отображается сообщение о завершении.

9. Нажмите **OK**.

   Убедитесь, что файл сохранен в указанном месте.

Импорт контактов

Импорт списка контактов из файла.

Можно импортировать файлы, сохраненные в формате SYLK или CSV, или двоичный файл резервной копии с параметрами безопасности.

1. Запустите Epson Device Admin.

2. Выберите **Устройства** в меню задач сбоку.

3. Выберите устройство для настройки в списке устройств.

4. Щелкните **Конфигурация устройства** на вкладке **Главная** меню ленты.

   После установки пароля администратора введите его и нажмите **OK**.

5. Щелкните **Общий** > **Контактная информация**.

6. Щелкните **Обзор** в разделе **Импорт**.

7. Выберите файл для импорта и щелкните **Открыть**.

   При выборе двоичного файла в поле **Пароль** введите пароль, установленный при экспорте этого файла.

8. Нажмите **Импорт**.

   Отображается экран подтверждения.

9. Нажмите **OK**.

   Отображается результат подтверждения.

❏ Отредактировать загруженные данные

Щелкните, если необходимо изменить отдельную информацию.

❏ Загрузить еще файл

Щелкните для импорта нескольких файлов.

10. Щелкните **Импорт**, затем нажмите **OK** на экране завершения импорта.

Вернитесь к экрану свойств устройства.

11. Нажмите **Передача**.

12. Нажмите **OK** в сообщении с подтверждением.

Параметры будут отправлены на сканер.

13. На экране завершения отправки нажмите **OK**.

Данные на сканере обновятся.

Откройте контакты в Web Config или на панели управления сканера и убедитесь, что они обновлены.

Взаимодействие между сервером LDAP и пользователями

При взаимодействии с сервером LDAP можно использовать информацию об адресе, зарегистрированную на сервере LDAP, как параметры получателя электронной почты.

Настройка LDAP-сервера

Для использования информации LDAP-сервера зарегистрируйте этот сервер на сканере.

1. Войдите в Web Config и выберите вкладку **Сеть** > **Сервер LDAP** > **Основные**.

2. Введите значение для каждого элемента.

3. Выберите **OK**.

Отображаются выбранные параметры.

Параметры настройки LDAP-сервера

Параметры	Настройки и их описание
Использование сервера LDAP	Выберите **Использовать** или **Не использовать**.
Адрес сервера LDAP	Введите адрес LDAP-сервера. Введите от 1 до 255 символов в формате IPv4, IPv6 или полного доменного имени (FQDN). Для формата FQDN можно использовать буквенно-цифровые символы в ASCII (от 0x20 до 0x7E) и «-», за исключением начала и конца адреса.
Номер порта сервера LDAP	Введите номер порта LDAP-сервера в диапазоне от 1 до 65535.
Безопасное подключение	Укажите метод аутентификации для доступа сканера к LDAP-серверу.

Параметры	Настройки и их описание
Проверка подлинности сертификатов	При включении подтверждается сертификат LDAP-сервера. Рекомендуется задать значение **Включить**. Для такой настройки на сканер должен быть импортирован **Сертификат ЦС**.
Таймаут поиска (с.)	Задайте продолжительность поиска до возникновения тайм-аута (число от 5 до 300).
Метод аутентификации	Выберите один из способов. При выборе **Аутентификация Kerberos** выберите **Настройки Kerberos** для настройки Kerberos. Для использования Аутентификация Kerberos требуется следующая среда. ❏ Сканер и DNS-сервер могут связываться друг с другом. ❏ Время сканера, сервера KDC и сервера, необходимого для аутентификации (LDAP-сервера, SMTP-сервера, файлового сервера), синхронизируется. ❏ Если сервер службы назначен через IP-адрес, полное доменное имя сервера службы регистрируется в зоне обратного просмотра DNS-сервера.
Область Kerberos для использования	При выборе значения **Аутентификация Kerberos** для параметра **Метод аутентификации** выберите область Kerberos, которую следует использовать.
Доменное имя администратора / Имя пользователя	Введите имя пользователя для LDAP-сервера. Длина имени не должна превышать 128 символов Юникода (UTF-8). Нельзя использовать управляющие символы, например символы с кодами от 0x00 до 0x1F и код 0x7F. Если для параметра **Метод аутентификации** выбрано значение **Анонимная аутентификация**, этот параметр не используется. Если не нужно указывать это значение, оставьте поле пустым.
Пароль	Введите пароль для проверки подлинности на LDAP-сервере. Длина пароля не должна превышать 128 символов Юникода (UTF-8). Нельзя использовать управляющие символы, например символы с кодами от 0x00 до 0x1F и код 0x7F. Если для параметра **Метод аутентификации** выбрано значение **Анонимная аутентификация**, этот параметр не используется. Если не нужно указывать это значение, оставьте поле пустым.

Настройки Kerberos

Если выбрано значение **Аутентификация Kerberos** параметра **Метод аутентификации** для **Сервер LDAP** > **Основные**, внесите следующие настройки Kerberos на вкладке **Сеть** > **Настройки Kerberos**. Можно зарегистрировать до 10 настроек Kerberos.

Параметры	Настройки и их описание
Область (домен)	Введите область проверки подлинности Kerberos длиной не более 255 символов ASCII (от 0x20 до 0x7E). В противном случае оставьте это поле пустым.
Адрес KDC	Введите адрес сервера аутентификации Kerberos. Введите не более 255 символов в формате IPv4, IPv6 или полного доменного имени. В противном случае оставьте это поле пустым.
Номер порта (Kerberos)	Введите номер порта сервера Kerberos в диапазоне от 1 до 65535.

Настройка параметров поиска LDAP-сервера

При установке параметров поиска можно использовать адрес электронной почты, зарегистрированный для LDAP-сервера.

1. Войдите в Web Config и выберите вкладку **Сеть** > **Сервер LDAP** > **Параметры поиска**.
2. Введите значение для каждого элемента.
3. Нажмите **OK** для отображения результата настройки.

   Отображаются выбранные параметры.

Элементы настройки поиска данных LDAP-сервера

Параметры	Настройки и их описание
Поиск в базе (Уникальное имя)	Для поиска произвольного домена задайте доменное имя LDAP-сервера. Введите от 0 до 128 символов в кодировке Юникод (UTF-8). Если не требуется поиск произвольного атрибута, оставьте это поле пустым. Пример для каталога локального сервера: dc=server,dc=local
Число элементов поиска	Укажите количество записей для поиска от 5 до 500. Указанное количество записей для поиска сохраняется и отображается временно. Даже если количество записей поиска превышает заданное число и появляется сообщение об ошибке, то поиск можно завершить.
Атрибут имени пользователя	Укажите имя атрибута для отображения при поиске имен пользователей. Введите от 1 до 255 символов в кодировке Юникод (UTF-8). Первым символом должен быть символ в диапазоне от a до z или от A до Z. Пример: cn, uid
Атрибут просмотра имени пользователя	Укажите имя атрибута для отображения в качестве имени пользователя. Введите от 0 до 255 символов в кодировке Юникод (UTF-8). Первым символом должен быть символ в диапазоне от a до z или от A до Z. Пример: cn, sn
Атрибут адреса электронной почты	Укажите имя атрибута для отображения при поиске адреса электронной почты. Введите комбинацию от 1 до 255 символов, используя символы в диапазоне от A до Z, от a до z, 0–9, и -. Первым символом должен быть символ в диапазоне от a до z или от A до Z. Пример: mail
Произвольный атрибут 1 - Произвольный атрибут 4	Можно указать другие произвольные атрибуты для поиска. Введите от 0 до 255 символов в кодировке Юникод (UTF-8). Первым символом должен быть символ в диапазоне от a до z или от A до Z. Если не требуется поиск произвольных атрибутов, оставьте это поле пустым. Пример: o, ou

Проверка соединения с LDAP-сервером

Проверка подключения к LDAP-серверу с использованием параметров, установленных в меню **Сервер LDAP** > **Параметры поиска**.

1. Войдите в Web Config и выберите вкладку **Сеть** > **Сервер LDAP** > **Проверка подключения**.
2. Выберите **Пуск**.

   Проверка соединения началась. После завершения проверки отобразится отчет о проверке.

Пояснения сообщений, отображаемых при проверке соединения с LDAP-сервером

Сообщения	Описание
Проверка подключения прошла успешно.	Это сообщение отображается, когда соединение с сервером установлено.
Сбой проверки подключения. Проверьте настройки.	Это сообщение отображается по следующим причинам. ❏ Адрес или номер порта LDAP-сервера неверен. ❏ Истекло время ожидания. ❏ Значение **Не использовать** задано для параметра **Использование сервера LDAP**. ❏ Если значение **Аутентификация Kerberos** задано для параметра **Метод аутентификации**, такие параметры, как **Область (домен)**, **Адрес KDC** и **Номер порта (Kerberos)**, неверны.
Сбой проверки подключения. Проверьте дата и время на устройстве или сервере.	Это сообщение отображается, когда не удается установить соединение, потому что параметры времени для сканера и LDAP-сервера не совпадают.
Ошибка аутентификации. Проверьте настройки.	Это сообщение отображается по следующим причинам. ❏ Параметры **Имя пользователя** и **Пароль** неверны. ❏ Если значение **Аутентификация Kerberos** задано для параметра **Метод аутентификации**, дату и время будет невозможно изменить.
Доступ к устройству невозможен до завершения обработки.	Это сообщение отображается, если сканер занят.

Использование Document Capture Pro Server

С помощью Document Capture Pro Server вы можете управлять методом сортировки, форматом сохранения и назначением переадресации результатов сканирования с панели управления сканера. Вы можете вызывать и выполнять ранее зарегистрированное задание на сервере с панели управления сканера.

Установите это программное обеспечение на сервере.

Дополнительные сведения о Document Capture Pro Server можно получить в местном офисе Epson.

Настройка режима сервера

Чтобы использовать Document Capture Pro Server, выполните следующую настройку.

1. Войдите в Web Config и выберите вкладку **Скан.** > **Document Capture Pro**.
2. Выберите значение **Режим сервера** для параметра **Режим**.

3. Введите адрес сервера, где установлен Document Capture Pro Server, используя это значение в качестве **Адрес сервера**.

   Введите от 2 до 255 символов в любом из форматов: IPv4, IPv6, имя хоста или полное доменное имя. Для формата полного доменного имени можно использовать буквенно-цифровые символы в ASCII (от 0x20 до 0x7E) и «-», за исключением начала и конца адреса.

4. Нажмите **OK**.

   Сеть подключается повторно, после чего включаются настройки.

Настройка AirPrint

Откройте приложение Web Config и выберите вкладку **Сеть**, затем выберите **Настройка AirPrint**.

Параметры	Описание
Служебное имя Bonjour	Введите имя службы Bonjour — не более 41 символа в кодировке ASCII (символы с кодами от 0x20 до 0x7E).
Местоположение Bonjour	Введите описание расположения сканера — до 127 символов в кодировке Unicode (UTF-8).
Wide-Area Bonjour	Укажите, следует ли использовать Wide-Area Bonjour. При использовании этой функции сканер должен пройти регистрацию на сервере DNS для возможности поиска сканера в сегменте.
Вкл. AirPrint	Службы Bonjour и AirPrint (служба сканирования) включены.

Проблемы при подготовке сетевого сканирования

Советы по решению проблем

❏ Просмотр сообщения об ошибке

При возникновении неполадки сначала проверьте, есть ли какие-нибудь сообщения на панели управления сканера или экране драйвера. Если настроена отправка уведомлений по электронной почте в случае каких-либо событий, то вы своевременно узнаете о произошедшем.

❏ Проверка состояния соединения

Проверьте состояние связи с сервером или клиентским компьютером, используя такие команды, как ping и ipconfig.

❏ Проверка подключения

Для проверки подключения сканера и почтового сервера выполните на сканере проверку подключения. Кроме того, проверьте подключение клиентского компьютера к серверу, чтобы проверить состояние связи.

❏ Инициализация параметров

Если проблема не связана с текущими параметрами и состоянием связи, она может быть решена путем отключения или сброса сетевых параметров сканера и их последующей перенастройки.

Нет доступа к Web Config

Сканеру не назначен IP-адрес.

Решения

Возможно, сканеру не назначен допустимый IP-адрес. Настройте IP-адрес, используя панель управления сканера. Текущие значения параметров можно проверить на панели управления сканера.

Браузер не поддерживает стойкость шифрования для SSL/TLS.

Решения

Для SSL/TLS установлен режим Криптографическая стойкость. Web Config можно открыть с помощью веб-браузера, который поддерживает указанные ниже алгоритмы массового шифрования. Убедитесь, что используете поддерживаемый браузер.

- ❏ 80 бит: AES256/AES128/3DES
- ❏ 112 бит: AES256/AES128/3DES
- ❏ 128 бит: AES256/AES128
- ❏ 192 бита: AES256
- ❏ 256 бит: AES256

Срок действия Сертификат, подписанный ЦС истек.

Решения

Если имеется проблема с истечением срока действия сертификата, при подключении к Web Config через соединение SSL/TLS (https) отображается сообщение «Срок действия сертификата истек». Если это сообщение отображается до истечения срока действия сертификата, убедитесь, что дата на сканере настроена правильно.

Общее имя в сертификате и на сканере не совпадает.

Решения

Если общее имя в сертификате и на сканере не совпадает, при доступе к Web Config через соединение SSL/TLS (https) отображается сообщение «Имя сертификата безопасности не совпадает с···». Это происходит потому, что не совпадают следующие IP-адреса.

- ❏ IP-адрес сканера, введенный для общего имени при создании Самоподписанный сертификат или CSR.
- ❏ IP-адрес, введенный в веб-браузере при запуске Web Config

Если используется Самоподписанный сертификат, обновите сертификат.

Если используется Сертификат, подписанный ЦС, еще раз получите сертификат для сканера.

В веб-браузере не настроены параметры прокси-сервера для локальных адресов.

Решения

Если сканер использует прокси-сервер, настройте веб-браузер так, чтобы он не подключался к локальным адресам через прокси-сервер.

❏ Windows:

выберите **Панель управления** > **Сеть и Интернет** > **Свойства обозревателя** > **Подключения** > **Настройка сети** > **Прокси-сервер**, после чего отключите использование прокси-сервера для сети (локальные адреса).

❏ Mac OS:

выберите **Системные настройки** > **Сеть** > **Дополнительно** > **Прокси** и зарегистрируйте локальный адрес в разделе **Обход прокси-сервера для этих хостов и доменов**.

Пример:

192.168.1.*: локальный адрес 192.168.1.XXX, маска подсети 255.255.255.0

192.168.*.*: локальный адрес 192.168.XXX.XXX, маска подсети 255.255.0.0

В настройках компьютера отключено DHCP.

Решения

Если DHCP для автоматического получения IP-адреса отключено на компьютере, Web Config недоступна. Включите DHCP.

Пример для Windows 10:

Откройте панель управления и щелкните **Сеть и Интернет** > **Центр управления сетями и общим доступом** > **Изменение параметров адаптера**. Откройте экран «Свойства» используемого соединения, затем откройте экран свойств **IP версии 4 (TCP/IPv4)** или **IP версии 6 (TCP/IPv6)**. Убедитесь, что на отображаемом экране установлен флажок **Получить IP-адрес автоматически**.

Настройка панели управления

Регистрация Предустан.

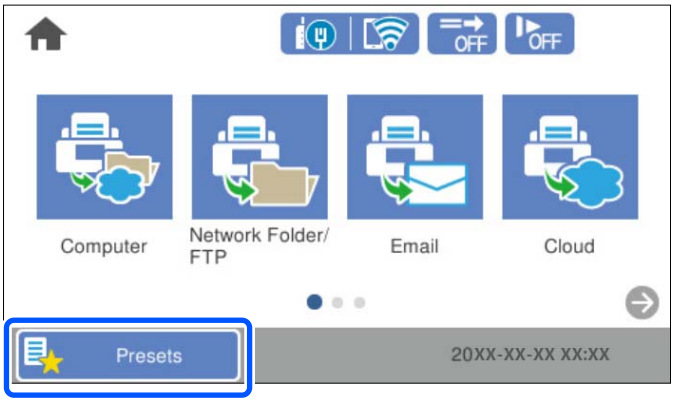
Можно регистрировать часто используемые настройки сканирования в качестве предустановок (**Предустан.**). Разрешается зарегистрировать до 48 предустановок.

Примечание:

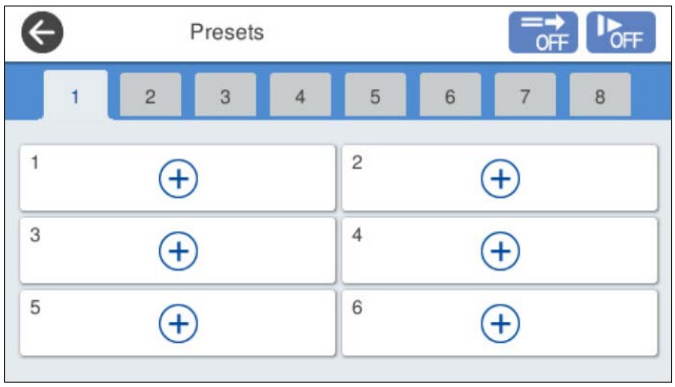
- *Можно зарегистрировать текущие настройки, выбрав* ☆ *на экране начала сканирования.*
- *Можно также зарегистрировать* ***Предустановки*** *в Web Config.*

  Выберите вкладку ***Скан.*** *>* ***Предустановки****.*
- *При выборе* ***Сканиров. на компьютер*** *во время регистрации можно зарегистрировать задание, созданное в Document Capture Pro, как* ***Предустановки****. Это доступно только для компьютеров, подключенных по сети. Заранее зарегистрируйте задание в Document Capture Pro.*
- *Если включена функция аутентификации, администратор может зарегистрировать* ***Предустановки****.*

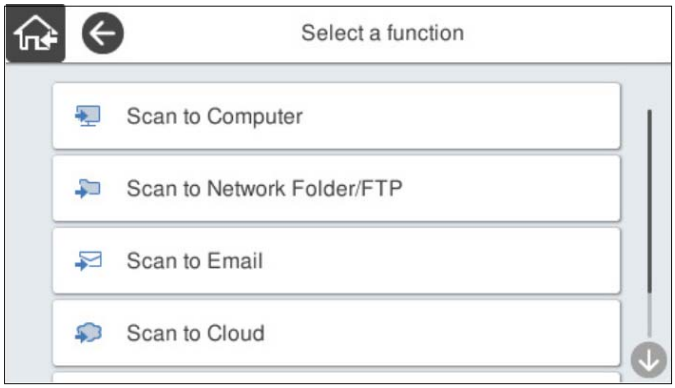
1. Выберите **Предустан.** на главном экране или на панели управления сканера.



2. Выберите ⊕.



3. Выберите меню, которое следует использовать для регистрации предустановки.



4. Настройте каждый элемент, затем выберите ☆+.

Примечание:
При выборе ***Сканиров. на компьютер*** *выберите компьютер, на котором установлено приложение Document Capture Pro, затем выберите зарегистрированное задание. Это доступно только для компьютеров, подключенных по сети.*

5. Измените настройки предустановки.

- ❏ **Имя**: определение имени.
- ❏ **Настроить Иконку**: определение изображения и цвета значка, который следует отобразить.
- ❏ **Настройка быстрой отправки**: незамедлительный запуск сканирования без подтверждения, если выбрана предустановка.

  При использовании Document Capture Pro Server, даже при установке подтверждения содержимого задания перед сканированием, настройка **Настройка быстрой отправки** предустановки сканера имеет приоритет перед программным обеспечением.
- ❏ **Содержимое**: проверка настроек сканирования.

6. Выберите **OK**.

Параметры меню Предустан.

Настройки предустановки можно изменить, выбрав › в соответствующей предустановке.

Переименовать:

изменение названия предустановки.

Изменить Иконку:

изменение значка и цвета предустановки.

Настройка быстрой отправки:

незамедлительный запуск сканирования без подтверждения при выборе предустановки.

Изменить положение:

изменение порядка отображения предустановок.

Удалить:

удаление выбранной предустановки.

Добавить или удалить Иконку вкл. В начало:

добавление или удаление значка предустановки на главном экране.

Подтвердить Сведения:

просмотр настроек предустановки. Загрузить предустановку можно путем выбора пункта **Использ. эту настр.**.

Изменение главного экрана панели управления

Главный экран можно настроить, выбрав на панели управления сканера пункт **Настр.** > **Редактировать домашний**.

- Макет: меняет метод отображения значков меню.

  «Изменение Макет на главном экране» на стр. 83

- Добавить значок: добавляет значки во внесенные настройки **Предустан.** или восстанавливает значки, которые были удалены с экрана.

  «Добавить значок» на стр. 84

- Удалить значок: удаляет значки с главного экрана.

  «Удалить значок» на стр. 85

- Переместить значок: меняет порядок отображения значков.

  «Переместить значок» на стр. 86

- Восстан. отображ. значков по умолчанию: восстанавливает настройки главного экрана по умолчанию.
- Фон экрана: изменение фонового изображения главного экрана.

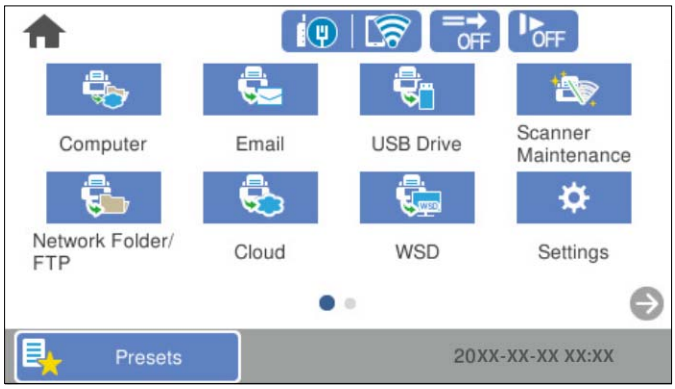
Изменение Макет на главном экране

1. Выберите **Настр.** > **Редактировать домашний** > **Макет** на панели управления сканера.

2. Выберите **Линия** или **Матрица**.

   Линия:

   Матрица:



3. Выберите , чтобы вернуться и проверить главный экран.

Добавить значок

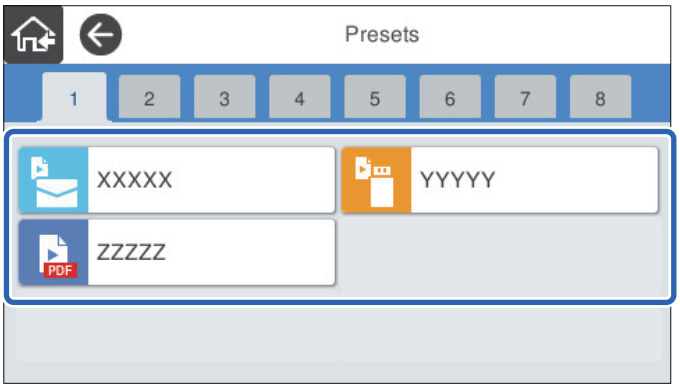
1. Выберите **Настр.** > **Редактировать домашний** > **Добавить значок** на панели управления сканера.

2. Выберите **Функция** или **Предустан.**.

   ❏ Функция: отображает функции по умолчанию, которые приведены на главном экране.

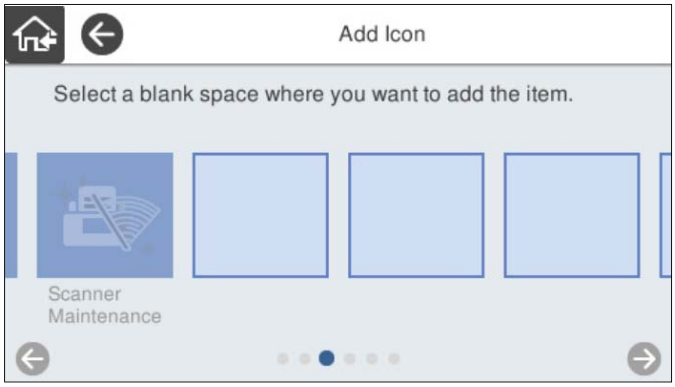
❏ Предустан.: отображает зарегистрированные предустановки.

3. Выберите элемент, который следует добавить на главный экран.



4. Выберите пустое место, на которое следует добавить элемент.

   Если необходимо добавить несколько значков, повторите шаги 3 и 4.

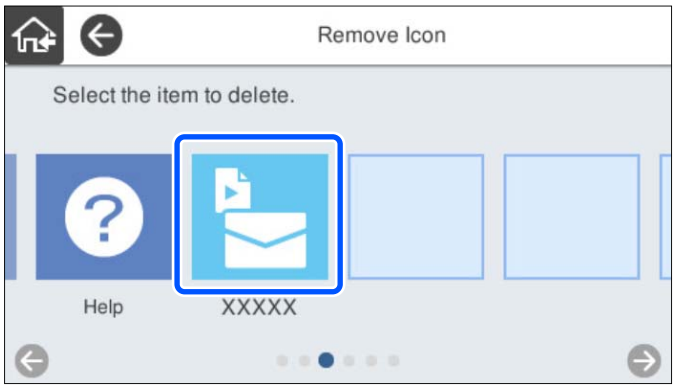


5. Выберите  , чтобы вернуться и проверить главный экран.

Удалить значок

1. Выберите **Настр.** > **Редактировать домашний** > **Удалить значок** на панели управления сканера.

2. Выберите значок, который необходимо удалить.



3. Для завершения нажмите **Да**.

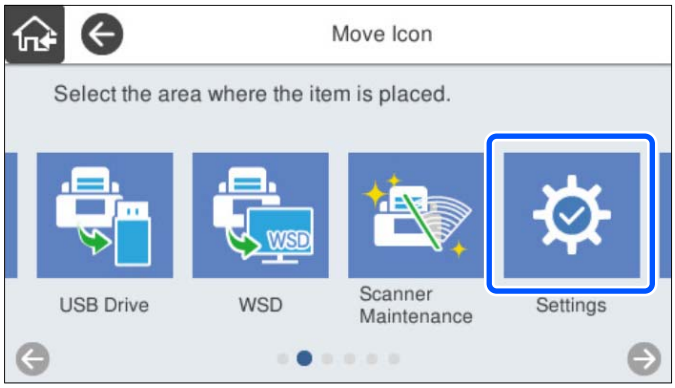
   Если необходимо удалить несколько значков, выполните процедуру 2 и 3.

4. Выберите , чтобы вернуться и проверить главный экран.

Переместить значок

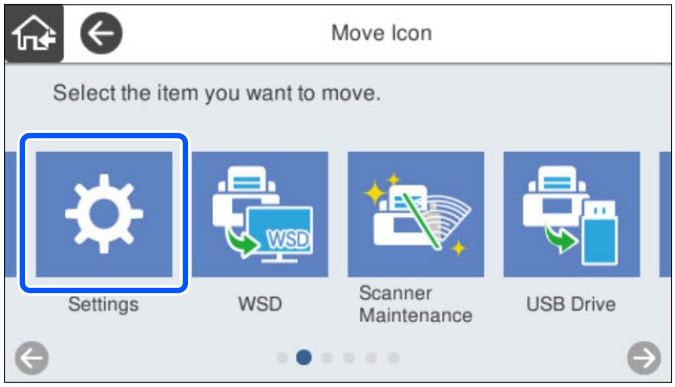
1. Выберите **Настр.** > **Редактировать домашний** > **Переместить значок** на панели управления сканера.

2. Выберите значок, который необходимо переместить.



3. Выберите рамку места назначения.

   Если другой значок уже задан в рамке места назначения, этот значок будет заменен.



4. Выберите , чтобы вернуться и проверить главный экран.

Базовые настройки безопасности

Общие сведения о функциях безопасности устройства

В этом разделе приводятся общие сведения о функциях безопасности устройств Epson.

Название функции	Тип функции	Что определять	Что предотвращать
Настройка пароля администратора	Блокирует настройки системы, такие как настройка подключения к сети или USB.	Администратор задает пароль для устройства. Установить и изменить этот режим можно в Web Config и на панели управления сканера.	Можно предотвратить незаконное чтение и изменение информации, которая хранится на устройстве, например идентификаторов, паролей, настроек сети и т. д. Кроме того, можно снизить широкий спектр рисков безопасности, таких как утечка информации о сетевой среде или политике безопасности.
Настройка внешнего интерфейса	Управление интерфейсом для подключения к устройству.	Включите или отключите соединение с компьютером по протоколу USB.	USB-подключение компьютера: предотвращает несанкционированное использование устройства, запрещая сканирование без подключения по сети.

Соответствующая информация

➡ «Настройка пароля администратора» на стр. 89
➡ «Отключение внешнего интерфейса» на стр. 95

Настройки администратора

Настройка пароля администратора

Установив пароль администратора, можно предотвратить изменение пользователями параметров управления системой. После покупки устройства установлены значения по умолчанию. При необходимости измените их.

Примечание:
Значения по умолчанию для администраторских учетных данных приведены ниже.

❏ *Имя пользователя (используется только в Web Config): отсутствует (пустое имя)*

❏ *Пароль: серийный номер сканера*

Серийный номер указан на этикетке снизу сканера.

Изменить пароль администратора можно с помощью Web Config, панели управления сканера или ПО Epson Device Admin. При использовании Epson Device Admin обратитесь к руководству или справке по Epson Device Admin.

Изменение пароля администратора с помощью Web Config

Измените пароль администратора в приложении Web Config.

1. Войдите в Web Config и выберите вкладку **Безопасность устройства** > **Изменить Пароль администратора**.

2. Введите необходимую информацию в поля **Текущий пароль**, **Имя пользователя**, **Новый пароль** и **Подтвердить новый пароль**.

   Введите как минимум один символ для нового пароля.

   Примечание:
   Значения по умолчанию для администраторских учетных данных приведены ниже.

   ❏ *Имя пользователя: отсутствует (пустое имя)*

   ❏ *Пароль: серийный номер сканера*

   Серийный номер указан на этикетке снизу сканера.

   > ***Важно:***
   > *Обязательно запомните установленный пароль администратора. Если вы забудете пароль, вы не сможете его сбросить и вам придется обратиться за помощью к персоналу технической поддержки.*

3. Выберите **OK**.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Изменение пароля администратора с панели управления

Пароль администратора можно изменить с панели управления сканера.

1. Выберите **Настр.** на панели управления сканера.

2. Выберите **Администрир. системы** > **Настройки администратора**.

3. Выберите **Пароль администратора** > **Изменить**.

4. Введите текущий пароль.

   Примечание:
   После покупки сканера для пароля администратора установлено значение по умолчанию — серийный номер данного сканера.

   Серийный номер указан на этикетке снизу сканера.

5. Введите новый пароль.

   Нужно ввести не менее одного символа.

> ***Важно:***
>
> *Обязательно запомните установленный пароль администратора. Если вы забудете пароль, вы не сможете его сбросить и вам придется обратиться за помощью к персоналу технической поддержки.*

6. Для подтверждения еще раз введите новый пароль.

Отобразится сообщение о завершении операции.

Использование функции Функция блокировки для панели управления

Вы можете использовать Функция блокировки для блокировки панели управления, чтобы пользователи не могли изменять элементы, связанные с системными настройками.

Примечание:
При включении Настройки аутентификации на сканере функция Функция блокировки также включается для панели управления. Панель управления не может быть разблокирована, если включена функция Настройки аутентификации.

Даже при отключении Настройки аутентификации функция Функция блокировки остается включенной. Если вы хотите отключить ее, вы можете сделать соответствующие настройки с панели управления или из приложения Web Config.

Настройка функции Функция блокировки с панели управления

1. Если вы хотите отменить функцию **Функция блокировки** после ее включения, нажмите значок  в правом верхнем углу главного экрана, чтобы выполнить вход как администратор.

   Значок  не отображается, если функция **Функция блокировки** отключена. Если вы хотите включить этот параметр, перейдите к следующему шагу.

2. Выберите **Настр.**.

3. Выберите **Администрир. системы** > **Настройки администратора**.

4. Установите **Вкл.** или **Вык.** для параметра **Функция блокировки**.

Настройка функции Функция блокировки с помощью Web Config

1. Выберите вкладку **Управление устройствами** > **Панель управления**.

2. Выберите значение **Вкл.** или **Выкл.** для параметра **Блокировка панели**.

3. Нажмите **OK**.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Элементы Функция блокировки в меню Настр.

Это список элементов, заблокированных в меню **Настр.** панели управления с помощью функции Функция блокировки.

✓: блокируется.

—: не блокируется.

Меню Настр.		**Функция блокировки**
Основ. настройки		—
	Яркость дисп.	—
	Звуки	—
	Таймер откл.	✓
	Таймер выключения	✓
	Настр. даты и времени	✓
	Язык/Language	✓/—*
	Клавиатура (В некоторых регионах эта функция может быть недоступна.)	—
	Время ожид. операции	✓
	USB-подключение к PC	✓
	Прямое включение питания	✓
Параметры сканера		—
	Медленно	—
	Время остан. при двойной подаче	✓
	Функция DFDS	—
	Защита бумаги	✓
	Определение загрязнения стекла	✓
	Ультразвук. обнар. двойн. под.	✓
	Время ожидания Режима автоматической подачи	✓
	Подтвердить Получателя	✓
Редактировать домашний		✓

Меню Настр.		**Функция блокировки**
	Макет	✓
	Добавить значок	✓
	Удалить значок	✓
	Переместить значок	✓
	Восстан. отображ. значков по умолчанию	✓
	Фон экрана	✓
Параметры пользователя		✓
	Сетевая папка/FTP	✓
	Эл. почта	✓
	Облако	✓
	USB-накопитель	✓
Настройки сети		✓
	Настройка Wi-Fi	✓
	Настройка проводной ЛВС	✓
	Статус сети	✓
	Расширенные	✓
Настройки веб-службы		✓
	Служба Epson Connect	✓
Document Capture Pro		—
	Изменить настройки	✓
Диспетчер Контакты		—
	Регистрация/Удалить	✓/—*
	Частые	—
	Параметры просмотра	—
	Параметры поиска	—
Администрир. системы		✓

Меню Настр.			**Функция блокировки**
	Диспетчер Контакты		✓
	Настройки администратора		✓
	Ограничения		✓
	Шифрование пароля		✓
	Сбор информации о клиенте		✓
	Настройки WSD		✓
	Восст. настр. по ум.		✓
	Обновление встроенного ПО		✓
Информация об устройстве			—
	Серийный номер		—
	Текущая версия		—
	Суммарное число копий		—
	Число 1-сторонних копий		—
	Число 2-сторонних копий		—
	Число копий конверта для сканир.		—
	Число копий после замены рол.		—
	Число копий после регул. очист.		—
	Сброс числа копий		✓
Техобслуж. Сканера			—
	Чистка роликов		—
	Замена роликов		—
		Сброс числа копий	✓
		Замена	—
	Регул. очист		—
		Сброс числа копий	✓
		Как выполнить очистку	—
	Очистка стекла		—
Настройка уведомления о замене роликов			✓
	Настро оповещ счетчи		✓
Настройка оповещений о регулярной очистке			✓

Меню Настр.		Функция блокировки
	Настройка предупреждений	✓
	Настро оповещ счетчи	✓

* Можно указать, разрешены или нет изменения в разделе **Администрир. системы** > **Ограничения**.

Вход в качестве администратора с панели управления

Для входа в качестве администратора с панели управления сканера можно использовать следующие методы.

1. Нажмите значок в правой верхней части экрана.
   - ❏ Если функция Настройки аутентификации включена, этот значок отображается на экране **Добро пожаловать** (экране ожидания авторизации).
   - ❏ Если функция Настройки аутентификации отключена, значок отображается на главном экране.
2. На экране подтверждения нажмите **Да**.
3. Введите пароль администратора.

   Отобразится сообщение о завершении процедуры входа, после чего на панели управления отобразится главный экран.

Чтобы выполнить выход, нажмите значок в правой верхней части главного экрана.

Отключение внешнего интерфейса

Можно отключить интерфейс, используемый для подключения устройства к сканеру. Выполните настройку ограничений, чтобы разрешить сканирование только по сети.

Примечание:
Можно также изменить настройки ограничений на панели управления сканера.

USB-подключение к PC: ***Настр.*** > ***Основ. настройки*** > ***USB-подключение к PC***

1. Войдите в Web Config и выберите вкладку **Безопасность устройства** > **Внешний интерфейс**.
2. Выберите **Отключить** для функций, которые необходимо установить.

   Выберите **Включить**, чтобы отключить управление.

   USB-подключение к PC

   Вы можете запретить использование подключения по USB с компьютера. Для того чтобы сделать это, выберите пункт **Отключить**.
3. Нажмите **OK**.

4. Убедитесь, что отключенный порт не будет использоваться.

   USB-подключение к PC

   Если на компьютере был установлен драйвер

   Подключите сканер к компьютеру с помощью кабеля USB и убедитесь, что сканер не сканирует.

   Если на компьютере не был установлен драйвер

   Windows

   Откройте диспетчер устройств, затем подключите сканер к компьютеру с помощью кабеля USB и убедитесь, что содержимое диспетчера устройств не меняется.

   Mac OS

   Подключите сканер к компьютеру с помощью кабеля USB и убедитесь, что невозможно добавить сканер в разделе **Принтеры и сканеры**.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Мониторинг удаленного сканера

Проверка информации об удаленном сканере

В разделе **Состояние** с помощью средства Web Config можно просмотреть следующие сведения о работе сканера.

❏ Состояние устройства

Просмотр сведений о статусе, облачной службе, номере продукта, MAC-адресе и т. д.

❏ Статус сети

Просмотр сведений о состоянии сетевого подключения, IP-адресе, DNS-сервере и т. д.

❏ Состояние использования

Просмотр даты первого сканирования, счетчика операций сканирования и т. д.

❏ Статус оборудования

Просмотр состояния каждой функции сканера.

❏ Панель "Снимок"

Отображение снимка экрана панели управления сканера.

Получение уведомлений по электронной почте, когда происходят события

Информация об оповещениях по электронной почте

Это функция уведомления, которая при возникновении таких событий, как остановка сканирования и ошибка сканера, отправляет сообщение электронной почты на указанный адрес.

Можно зарегистрировать до пяти адресов и настроить параметры уведомлений для каждого из них.

Чтобы использовать эту функцию, перед настройкой уведомлений необходимо настроить сервер электронной почты.

Соответствующая информация

➡ «Настройка почтового сервера» на стр. 44

Настройка оповещений по электронной почте

Настройте оповещения по электронной почте с помощью Web Config.

1. Войдите в Web Config и выберите вкладку **Управление устройствами** > **Уведомление по электронной почте**.

2. Установите тему для уведомлений электронной почты.

   Выберите содержимое, отображаемое в теме, при помощи следующих двух раскрывающихся меню.

   ❏ Выбранное содержимое отображается рядом с полем **Тема**.

   ❏ Слева и справа нельзя установить одинаковое содержимое.

   ❏ Если число символов в поле **Расположение** превышает 32 байта, символы, выходящие за границу 32 байтов, отбрасываются.

3. Введите адрес электронной почты для отправки уведомлений.

   Используйте символы от A до Z, от a до z, от 0 до 9, а также ! # $ % & ' * + - . / = ? ^ _ { | } ~ @; длина может составлять от 1 до 255 символов.

4. Выберите язык оповещений.

5. Установите флажок для событий, о которых необходимо получать уведомления.

   Номер **Настройки уведомлений** связан с номером назначения **Параметры адреса электронной почты**.

   Пример:

   Если при смене пароля администратора необходимо отправить уведомление на адрес электронной почты, заданный для числа 1 в **Параметры адреса электронной почты**, установите флажок для столбца **1** в строке **Пароль администратора изменен**.

6. Нажмите **OK**.

   Подтвердите отправку уведомления по электронной почте в случае каких-либо событий.

   Пример: был изменен пароль администратора.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Параметры уведомлений по электронной почте

Параметры	Настройки и их описание
Пароль администратора изменен	Уведомление об изменении пароля администратора.
Ошибка сканера	Уведомление об ошибке сканера.
Ошибка Wi-Fi	Уведомление об ошибке интерфейса беспроводной локальной сети.

Решение проблем

Вы забыли пароль администратора

Требуется помощь специалистов по техническому обслуживанию. Обратитесь к локальному дилеру.

Примечание:
Ниже приведены первоначальные значения для администратора Web Config.

❏ *Имя пользователя: нет (пустое)*

❏ *Пароль: серийный номер сканера*

Серийный номер указан на этикетке снизу сканера. При восстановлении пароля администратора по умолчанию будут восстановлены первоначальные значения.

Расширенные настройки безопасности

Настройки безопасности и предотвращение опасных ситуаций

Если сканер подключен к сети, можно получить к нему доступ из удаленного местоположения. Кроме того, сразу несколько пользователей смогут совместно использовать этот сканер, что позволяет повысить эффективность и удобство работы. Однако увеличиваются такие риски, как незаконный доступ, нелегальное использование и взлом данных. При использовании сканера в среде, где есть доступ к Интернету, риски становятся еще выше.

Если сканеры не защищены от доступа извне, можно будет получить доступ к этому сканеру из Интернета и просмотреть журналы заданий печати, которые хранятся на сканере.

Во избежание этих рисков сканеры Epson оснащены различными технологиями безопасности.

Настройте сканер в соответствии с требованиями условий окружающей среды, которые были сформированы на основе информации, указанной клиентом.

Название	Тип функции	Что определять	Что предотвращать
Управление протоколами	Позволяет управлять протоколами и службами, которые используются для связи между сканерами и компьютерами, а также включает и отключает соответствующие функции.	Протокол или служба, которая применяется к функциям, могут быть отдельно включены или отключены.	Снижение рисков безопасности, которые могут возникнуть вследствие непреднамеренного использования, путем предотвращения доступа пользователей к ненужным функциям.
Соединения SSL/TLS	При доступе со сканера к серверу Epson в Интернете (например, при обращении с компьютера через веб-браузер с использованием Epson Connect или обновлении программного обеспечения) все данные, передаваемые по каналу связи, шифруются с использованием протокола SSL/TLS.	Получите сертификат, подписанный ЦС, а затем импортируйте его на сканер.	Сброс идентификации на сканере с помощью сертификата, подписанного ЦС, не позволяет выдавать себя за другое лицо и получать несанкционированный доступ. Кроме того, данные, передаваемые по каналу SSL/TLS, надежно защищены, что препятствует утечке данных сканирования и параметров настройки.
IPsec/фильтрация IP	Можно настроить блокирование и фильтрацию данных определенного типа или данных, которые поступают от определенного клиента. Так как протокол IPsec обеспечивает защиту данных на уровне IP-пакетов (шифрование и аутентификация), незащищенный протокол можно безопасно использовать для передачи данных.	Создайте базовую политику и индивидуальную политику, чтобы задать тип клиента, который может обращаться к сканеру, или тип данных, которые могут передаваться на сканер.	Обеспечьте защиту от несанкционированного доступа, а также взлома и перехвата данных, передаваемых на сканер.

Название	Тип функции	Что определять	Что предотвращать
IEEE 802.1X	Позволяет подключаться к сети только тем пользователям, которые прошли аутентификацию. Позволяет использовать сканер только авторизованному пользователю.	Настройка проверки подлинности на сервере RADIUS (сервер проверки подлинности).	Защита от неавторизованного доступа к сканеру и его нецелевого использования.

Соответствующая информация

- «Управление использованием протоколов» на стр. 101
- «Связь со сканером через SSL/TLS» на стр. 110
- «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 111
- «Подключение сканера к сети IEEE802.1X» на стр. 123

Настройки функций безопасности

При настройке IPsec/фильтрации IP или IEEE802.1X рекомендуется открыть Web Config с использованием SSL/TLS для передачи данных по настройкам, чтобы снизить риски безопасности, такие как взлом или перехват данных.

Перед настройкой IPsec/фильтрации IP или IEEE802.1X убедитесь, что задан пароль администратора.

Управление использованием протоколов

Можно выполнять сканирование, используя различные способы и протоколы. Можно также использовать сканирование по сети с неограниченного количества сетевых компьютеров.

Ограничивая использование определенных способов сканирования и контролируя доступные функции, вы можете снизить вероятность возникновения непредвиденных угроз безопасности.

Управление протоколами

Настройте параметры протокола, поддерживаемого сканером.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** tab > **Протокол**.
2. Выполните настройку каждого элемента.
3. Нажмите **Следующий**.
4. Нажмите **ОК**.

   Выбранные настройки будут применены на сканере.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Протоколы, которые можно включить и выключить

Протокол	Описание
Параметры Bonjour	Можно указать, следует ли использовать Bonjour. Bonjour используется для поиска устройств, сканирования и пр.
Параметры SLP	Можно включить или отключить функцию SLP. SLP используется для сканирования по технологии push и сетевого поиска в EpsonNet Config.
Параметры WSD	Можно включить или отключить функцию WSD. Если эта функция включена, можно добавлять устройства WSD или сканировать с использованием порта WSD.
Параметры LLTD	Можно включить или отключить функцию LLTD. Если функция включена, она отображается на карте сети Windows.
Параметры LLMNR	Можно включить или отключить функцию LLMNR. Если функция включена, можно разрешать имена без использования NetBIOS, даже если невозможно использовать DNS.
Параметры SNMPv1/v2c	Можно указать, следует ли включить или выключить SNMPv1/v2c. Этот протокол используется для настройки устройств, их мониторинга и т. д.
Настройки SNMPv3	Можно указать, следует ли включить или выключить SNMPv3. Этот протокол используется для настройки шифрованных устройств, их мониторинга и пр.

Элементы настройки протоколов

Параметры Bonjour

Параметры	Значение и описание параметров
Использовать Bonjour	Выберите этот параметр для поиска или использования устройств с помощью Bonjour.
Имя Bonjour	Отображает имя Bonjour.
Служебное имя Bonjour	Отображает имя службы Bonjour.
Расположение	Отображает имя местоположения Bonjour.
Wide-Area Bonjour	Установите, необходимо ли использовать режим Wide-Area Bonjour.

Параметры SLP

Параметры	Значение и описание параметров
Включить SLP	Выберите этот параметр для включения функции SLP. Этот параметр используется, например, функцией поиска в сети EpsonNet Config.

Параметры WSD

Параметры	Значение и описание параметров
Включить WSD	Выберите этот параметр, чтобы включить добавление устройств с помощью WSD, а также для сканирования с использованием порта WSD.
Время ожидания сканирования (с.)	Введите значение времени ожидания связи для сканирования WSD от 3 до 3600 секунд.
Имя устройства	Отображает имя устройства WSD.
Расположение	Отображает имя местоположения WSD.

Параметры LLTD

Параметры	Значение и описание параметров
Включить LLTD	Выберите этот параметр для включения LLTD. Сканер отображается на карте сети Windows.
Имя устройства	Отображает имя устройства LLTD.

Параметры LLMNR

Параметры	Значение и описание параметров
Включить LLMNR	Выберите этот параметр для включения LLMNR. Можно разрешать имена без использования NetBIOS, даже если невозможно использовать DNS.

Параметры SNMPv1/v2c

Параметры	Значение и описание параметров
Включить SNMPv1/v2c	Выберите этот параметр для включения SNMPv1/v2c.
Полномочия доступа	Установите права доступа, если включен параметр SNMPv1/v2c. Выберите **Только для чтения** или **Чтение/Запись**.
Имя сообщества (только для чтения)	Введите символы ASCII от 0 до 32 (от 0x20 до 0x7E).
Имя сообщества (чтение/запись)	Введите символы ASCII от 0 до 32 (от 0x20 до 0x7E).

Настройки SNMPv3

Параметры	Значение и описание параметров
Включить SNMPv3	Протокол SNMPv3 включен, если установлен флажок.
Имя пользователя	Введите от 1 до 32 1-байтовых символов.
Настройки аутентификации	

Параметры		Значение и описание параметров
	Алгоритм	Выберите алгоритм проверки подлинности для SNMPv3.
	Пароль	Введите пароль для проверки подлинности SNMPv3. Введите от 8 до 32 символов в ASCII (от 0x20 до 0x7E). Если не нужно указывать это значение, оставьте поле пустым.
	Подтверждение пароля	Введите выбранный вами пароль для подтверждения.
Настройки шифрования		
	Алгоритм	Выберите алгоритм шифрования для SNMPv3.
	Пароль	Введите пароль для шифрования SNMPv3. Введите от 8 до 32 символов в ASCII (от 0x20 до 0x7E). Если не нужно указывать это значение, оставьте поле пустым.
	Подтверждение пароля	Введите выбранный вами пароль для подтверждения.
Контекстное имя		Введите не более 32 символов в кодировке Unicode (UTF-8). Если не нужно указывать это значение, оставьте поле пустым. Количество символов для ввода зависит от языка.

Использование цифрового сертификата

О цифровом сертификате

❏ Сертификат, подписанный ЦС

Это сертификат, подписанный ЦС (центром сертификации). Его можно получить, чтобы отправить в центр сертификации. Этот сертификат подтверждает существование данного сканера и используется для соединения SSL/TLS, позволяя обеспечить безопасность передачи данных.

Для соединения SSL/TLS он используется как сертификат сервера.

Для IPsec/фильтрации IP или связи IEEE 802.1x он используется как сертификат клиента.

❏ Сертификат ЦС

Этот сертификат входит в цепочку Сертификат, подписанный ЦС и называется также промежуточным сертификатом ЦС. Он используется веб-браузером для подтверждения пути сертификата сканера при доступе к серверу третьей стороны или к средству Web Config.

В параметрах сертификата ЦС необходимо установить, когда должен подтверждаться путь сертификата сервера при доступе со сканера. В настройках сканера необходимо установить режим подтверждения пути Сертификат, подписанный ЦС для соединения SSL/TLS.

Сертификат ЦС сканера можно получить в центре сертификации, выпустившем этот сертификат.

Кроме того, сертификат ЦС для подтверждения сервера третьей стороны можно получить в центре сертификации, выпустившем Сертификат, подписанный ЦС другого сервера.

❏ Самоподписанный сертификат

Этот сертификат сканер подписывает и выпускает самостоятельно. Он также называется корневым сертификатом. Поскольку издатель сертифицирует самого себя, этот вариант ненадежен и не предотвращает выдачу себя за других лиц.

Используйте его при установке настроек безопасности и установке простой связи SSL/TLS без механизма Сертификат, подписанный ЦС.

При использовании данного сертификата для связи SSL/TLS в веб-браузере могут отображаться сообщения системы безопасности, поскольку сертификат не зарегистрирован в браузере. Самоподписанный сертификат можно использовать только для связи SSL/TLS.

Соответствующая информация

➡ «Настройка Сертификат, подписанный ЦС» на стр. 105

➡ «Обновление самозаверяющего сертификата» на стр. 108

➡ «Настройка Сертификат ЦС» на стр. 109

Настройка Сертификат, подписанный ЦС

Получение сертификата, подписанного ЦС

Для получения сертификата, подписанного ЦС, создайте запрос на подписание сертификата (CSR) и отправьте его в центр сертификации.Создать CSR можно с помощью Web Config и компьютера.

Для создания CSR и получения сертификата, подписанного ЦС, при помощи Web Config выполните следующие действия.При создании CSR с помощью приложения Web Config сертификат имеет формат PEM/DER.

1. Войдите в Web Config и выберите вкладку **Безопасность сети**.Далее выберите **SSL/TLS** > **Сертификат**, или **IPsec/Фильтрация IP** > **Сертификат клиента**, или **IEEE802.1X** > **Сертификат клиента**.

   Независимо от выбранного параметра, вы получите один и тот же сертификат, который можно использовать во всех случаях.

2. Нажмите **Сформировать** в разделе **CSR**.

   Отображается страница для создания CSR.

3. Введите значение для каждого элемента.

   Примечание:
   Доступная длина ключа и сокращения различаются в зависимости от центра сертификации.Создайте запрос в соответствии с правилами каждого центра сертификации.

4. Нажмите **OK**.

   Отображается сообщение о завершении.

5. Выберите вкладку **Безопасность сети**.Далее выберите **SSL/TLS** > **Сертификат**, или **IPsec/Фильтрация IP** > **Сертификат клиента**, или **IEEE802.1X** > **Сертификат клиента**.

6. Нажмите на одну из кнопок загрузки из **CSR** в соответствии с заданным форматом каждого центра сертификации для загрузки CSR на компьютер.

> ***Важно:***
>
> *Не создавайте CSR повторно,так как импорт Сертификат, подписанный ЦС может оказаться невозможным.*

7. Отправьте CSR в центр сертификации и получите Сертификат, подписанный ЦС.

   Соблюдайте метод и форму отправки, установленные каждым центром сертификации.

8. Сохраните полученный Сертификат, подписанный ЦС на компьютере, подключенном к сканеру.

   Процедура получения Сертификат, подписанный ЦС будет завершена при сохранении сертификата получателем.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Параметры настройки CSR

Параметры	Настройки и их описание
Длина ключа	Выберите длину ключа для CSR.
Общее имя	Длина может составлять от 1 до 128 символов. Если это IP-адрес, то он должен быть статическим. Можно ввести от 1 до 5 IPv4-адресов, IPv6-адресов, имен хоста, полных доменных имен, разделяя их запятыми. Первый элемент сохраняется в общем имени, а другие элементы сохраняются в поле псевдонима темы сертификата. Пример: IP-адрес сканера: 192.0.2.123, имя сканера: EPSONA1B2C3 Общее имя: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Организация/ Организационное подразделение/ Населенный пункт/ Штат/Провинция	Введите от 0 до 64 символов в ASCII (0x20-0x7E). Различающиеся имена можно отделять запятыми.
Страна	Введите код страны как двузначное число по стандарту ISO 3166.
Адрес эл. почты отправителя	Можно указать адрес электронной почты отправителя для соответствующего параметра почтового сервера. Адрес электронной почты указывается в параметре **Адрес эл. почты отправителя** (вкладка **Сеть** > **Сервер эл. почты** > **Основные**).

Импорт сертификата, подписанного ЦС

Импортируйте полученный Сертификат, подписанный ЦС на сканер.

Важно:

❏ *Убедитесь, что дата и время сканера установлены правильно. Сертификат может быть недействительным.*

❏ *Импортируйте сертификат единожды в случае, если он был создан в Web Config.*

1. Войдите в Web Config и выберите вкладку **Безопасность сети**. Далее выберите **SSL/TLS** > **Сертификат**, или **IPsec/Фильтрация IP** > **Сертификат клиента**, или **IEEE802.1X** > **Сертификат клиента**.

2. Нажмите **Импорт**.

   Отображается страница импорта сертификата.

3. Введите значение для каждого элемента. Если для доступа к сканеру используется веб-браузер, то при проверке пути сертификата установите **Сертификат ЦС 1** и **Сертификат ЦС 2**.

   Обязательные настройки различаются в зависимости от формата файла сертификата и от того, где был создан CSR. Введите значения необходимых параметров в соответствии со следующими указаниями.

   ❏ Сертификат формата PEM/DER получен из Web Config.

   ❏ **Закрытый ключ**: не настраивайте, поскольку сканер содержит секретный ключ.

   ❏ **Пароль**: не настраивайте.

   ❏ **Сертификат ЦС 1/Сертификат ЦС 2**: необязательно.

   ❏ Сертификат формата PEM/DER получен от компьютера

   ❏ **Закрытый ключ**: установите.

   ❏ **Пароль**: не настраивайте.

   ❏ **Сертификат ЦС 1/Сертификат ЦС 2**: необязательно.

   ❏ Сертификат формата PKCS#12 получен от компьютера

   ❏ **Закрытый ключ**: не настраивайте.

   ❏ **Пароль**: необязательно.

   ❏ **Сертификат ЦС 1/Сертификат ЦС 2**: не настраивайте.

4. Нажмите **OK**.

   Отображается сообщение о завершении.

Примечание:
*Нажмите **Подтвердить** для проверки информации о сертификате.*

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Параметры настройки импорта сертификата, подписанного ЦС

Параметры	Настройки и их описание
Сертификат сервера или Сертификат клиента	Выберите формат сертификата. Для соединения SSL/TLS отображается Сертификат сервера. Для IPsec/фильтрации IP или IEEE802.1x отображается Сертификат клиента.
Закрытый ключ	Если получен сертификат в формате PEM/DER с помощью запроса CSR, созданного на компьютере, необходимо указать файл секретного ключа, который соответствует сертификату.
Пароль	Если формат этого файла — **Сертификат с закрытым ключом (PKCS#12)**, введите пароль для шифра секретного ключа, предоставленный вам вместе с этим сертификатом.
Сертификат ЦС 1	Если формат этого сертификата — **Сертификат (PEM/DER)**, импортируйте сертификат ЦС, который выдает Сертификат, подписанный ЦС, используемый как сертификат сервера. Укажите файл, если необходимо.
Сертификат ЦС 2	Если формат этого сертификата — **Сертификат (PEM/DER)**, импортируйте сертификат ЦС, который выдает сертификат Сертификат ЦС 1. Укажите файл, если необходимо.

Удаление сертификата, подписанного ЦС

Импортированный сертификат можно удалить, если срок действия сертификата истек или когда нет необходимости шифровать соединение.

> ***Важно:***
> *Невозможно повторно импортировать удаленный сертификат, если он был получен с помощью CSR из приложения Web Config.В этом случае создайте CSR заново и повторно получите сертификат.*

1. Войдите в Web Config и выберите вкладку **Безопасность сети**.Далее выберите **SSL/TLS** > **Сертификат**, или **IPsec/Фильтрация IP** > **Сертификат клиента**, или **IEEE802.1X** > **Сертификат клиента**.
2. Нажмите **Удалить**.
3. В отображаемом сообщении подтвердите удаление сертификата.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Обновление самозаверяющего сертификата

Поскольку Самоподписанный сертификат выпущен сканером, его можно обновить при истечении срока действия или при изменении соответствующего содержимого.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** tab > **SSL/TLS** > **Сертификат**.

2. Нажмите **Обновить**.

3. Введите **Общее имя**.

   Можно ввести до 5 IPv4-адресов, IPv6-адресов, имен хоста, полных доменных имен длиной от 1 до 128 символов, разделяя их запятыми. Первый параметр сохраняется в общем имени, а другие параметры сохраняются в поле псевдонима темы сертификата.

   Пример:

   IP-адрес сканера: 192.0.2.123, имя сканера: EPSONA1B2C3

   Общее имя: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Укажите срок действия сертификата.

5. Нажмите **Следующий**.

   Отображается запрос подтверждения.

6. Нажмите **ОК**.

   Настройки сканера обновлены.

Примечание:
*Сертификат можно проверить на вкладке **Безопасность сети** > **SSL/TLS** > **Сертификат** > **Самоподписанный сертификат**, щелкнув **Подтвердить**.*

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Настройка Сертификат ЦС

При настройке Сертификат ЦС можно проверить путь к сертификату ЦС сервера, к которому обращается сканер. Это может предотвратить мошенничество, связанное с выдачей себя за других лиц.

Сертификат ЦС можно получить в центре сертификации, выпустившем Сертификат, подписанный ЦС.

Импорт Сертификат ЦС

Импортируйте Сертификат ЦС на сканер.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **Сертификат ЦС**.

2. Нажмите **Импорт**.

3. Укажите Сертификат ЦС, который необходимо импортировать.

4. Нажмите **ОК**.

После завершения импорта вы вернетесь на экран **Сертификат ЦС**, где будет отображаться импортированный Сертификат ЦС.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Удаление Сертификат ЦС

Можно удалить импортированный Сертификат ЦС.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **Сертификат ЦС**.
2. Щелкните **Удалить** рядом с Сертификат ЦС, который необходимо удалить.
3. В появившемся сообщении подтвердите удаление сертификата.
4. Щелкните **Перезагрузка сети** и убедитесь, что удаленный сертификат ЦС отсутствует на обновленном экране.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Связь со сканером через SSL/TLS

Если сертификат сервера задан с использованием протоколов SSL/TLS, вы можете шифровать канал связи между компьютерами. Это следует применять в случаях, когда необходимо предотвратить удаленный и неавторизованный доступ.

Настройка основных параметров SSL/TLS

Протоколы SSL/TLS можно использовать для шифрования связи, если сканер поддерживает функцию HTTPS-сервера. Настройку сканера и управление им можно осуществлять, используя Web Config. При этом одновременно обеспечивается безопасность.

Настройте уровень шифрования и функцию переадресации.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **SSL/TLS** > **Основные**.
2. Выберите значение для каждого элемента.
   - ❏ Криптографическая стойкость

     Выберите уровень строгости шифрования.
   - ❏ Перенаправление HTTP на HTTPS

     При получении доступа к HTTP выполните перенаправление на HTTPS.
3. Нажмите **Следующий**.

   Отображается запрос подтверждения.

4. Нажмите **OK**.

   Настройки сканера будут обновлены.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Настройка сертификата сервера для сканера

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **SSL/TLS** > **Сертификат**.
2. Укажите сертификат для использования в параметре **Сертификат сервера**.
   - ❏ Самоподписанный сертификат

     Сканером был сформирован самозаверяющий сертификат. Выберите этот пункт, если сертификат, подписанный центром сертификации (ЦС), не получен.
   - ❏ Сертификат, подписанный ЦС

     Выберите этот пункт, если сертификат, подписанный ЦС, был получен и импортирован заранее.
3. Нажмите **Следующий**.

   Отображается запрос подтверждения.
4. Нажмите **OK**.

   Настройки сканера обновлены.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37
➡ «Настройка Сертификат, подписанный ЦС» на стр. 105
➡ «Настройка Сертификат ЦС» на стр. 109

Шифрованный канал связи с использованием IPsec/фильтрации IP

Сведения о IPsec/Фильтрация IP

Можно организовать фильтрацию трафика на основе IP-адресов, служб и портов, используемых функцией IPsec/фильтрации IP.Сканер можно настроить на прием или блокировку определенных клиентов и данных, объединяя разные фильтры.Кроме того, уровень безопасности можно повысить, используя протокол IPsec.

Примечание:
Компьютеры, работающие под управлением Windows Vista и более поздних версий или Windows Server 2008 и более поздних версий, поддерживают работу с протоколом IPsec.

Настройка политики по умолчанию

Настройте политику по умолчанию (действия по умолчанию) для фильтрации трафика.Политика по умолчанию распространяется на каждого пользователя или группу пользователей, имеющую подключение к сканеру.Настройте групповую политику для более точного контроля над пользователями и группами пользователей.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **IPsec/Фильтрация IP** > **Основные**.
2. Введите значение для каждого элемента.
3. Нажмите **Следующий**.

   Отображается запрос подтверждения.
4. Нажмите **OK**.

   Настройки сканера обновлены.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Параметры настройки в разделе Стандартная политика

Стандартная политика

Параметры	Настройки и их описание
IPsec/Фильтрация IP	Функцию IPsec/фильтрацию IP можно включить или выключить.

❏ **Управление доступом**

Настройте способ управления трафиком IP-пакетов.

Параметры	Настройки и их описание
Разрешить доступ	Выберите этот параметр, чтобы разрешить прохождение настроенных IP-пакетов.
Запретить доступ	Выберите этот параметр, чтобы запретить прохождение настроенных IP-пакетов.
IPsec	Выберите этот параметр, чтобы запретить прохождение настроенных пакетов IPsec.

❏ **Версия IKE**

Выберите значения **IKEv1** или **IKEv2** для параметра **Версия IKE**. Выберите одно из значений в соответствии с устройством, к которому подключен сканер.

❏ IKEv1

При выборе значения **IKEv1** для параметра **Версия IKE** отображаются следующие элементы.

Параметры	Настройки и их описание
Метод аутентификации	Выберите пункт **Сертификат** для получения и импорта сертификата, подписанного ЦС.
Предварительный ключ	Если значение **Предварительный ключ** указано для параметра **Метод аутентификации**, то введите предварительный ключ длиной от 1 до 127 символов.
Подтвердить Предварительный ключ	Введите выбранный вами ключ для подтверждения.

❏ IKEv2

При выборе значения **IKEv2** для параметра **Версия IKE** отображаются следующие элементы.

Параметры		Настройки и их описание
Локально	Метод аутентификации	Выберите пункт **Сертификат** для получения и импорта сертификата, подписанного ЦС.
	Тип ID	При выборе значения **Предварительный ключ** для параметра **Метод аутентификации** выберите тип идентификатора сканера.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа нельзя использовать символы @, # и =. **Отличительное имя**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ =. **IP-адрес**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя символы от A до Z, от a до z, 0–9, дефис (-) и точку (.). **Адрес эл. почты**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ @. **ID ключа**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Предварительный ключ	Если значение **Предварительный ключ** указано для параметра **Метод аутентификации**, то введите предварительный ключ длиной от 1 до 127 символов.
	Подтвердить Предварительный ключ	Введите выбранный вами ключ для подтверждения.

Параметры		Настройки и их описание
Удаленно	Метод аутентификации	Выберите пункт **Сертификат** для получения и импорта сертификата, подписанного ЦС.
	Тип ID	Если для параметра **Метод аутентификации** было выбрано значение **Предварительный ключ**, выберите тип идентификатора для устройства, подлинность которого следует проверить.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа нельзя использовать символы @, # и =. **Отличительное имя**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ =. **IP-адрес**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя символы от A до Z, от a до z, 0–9, дефис (-) и точку (.). **Адрес эл. почты**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ @. **ID ключа**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Предварительный ключ	Если значение **Предварительный ключ** указано для параметра **Метод аутентификации**, то введите предварительный ключ длиной от 1 до 127 символов.
	Подтвердить Предварительный ключ	Введите выбранный вами ключ для подтверждения.

❏ Формирование пакетов данных

Настройте режим инкапсуляции при выборе значения **IPsec** для параметра **Управление доступом**.

Параметры	Настройки и их описание
Режим передачи	Выберите этот пункт, если сканер используется в рамках одной ЛВС. IP-пакеты четвертого или более высокого уровня шифруются.
Туннельный режим	Выберите этот параметр, если вы используете сканер в сети с выходом в Интернет, например IPsec — VPN. Заголовок и данные IP-пакетов шифруются. **Удаленный шлюз(Туннельный режим)**: если для параметра **Формирование пакетов данных** указано значение **Туннельный режим**, введите адрес шлюза длиной от 1 до 39 символов.

❏ Протокол безопасности

Если выбрано значение **IPsec** для параметра **Управление доступом**, выберите нужный параметр.

Параметры	Настройки и их описание
ESP	Выберите этот пункт для обеспечения целостности, аутентификации и шифрования данных.
AH	Выберите этот пункт для обеспечения целостности и аутентификации данных. Даже если шифрование данных запрещено, можно использовать протокол IPsec.

❏ **Настройки алгоритма**

Рекомендуется выбирать значение **Любой** для всех параметров или значение, отличное от **Любой**, для каждого параметра. Если для некоторых параметров выбрать **Любой**, а для остальных параметров вариант, отличный от **Любой**, устройство может не поддерживать связь: это зависит от другого устройства, аутентификацию которого вы хотите выполнить.

Параметры		Настройки и их описание
IKE	Шифрование	Выберите алгоритм шифрования для IKE. Элементы различаются в зависимости от версии IKE.
	Аутентификация	Выберите алгоритм проверки подлинности для IKE.
	Обмен ключами	Выберите алгоритм обмена ключами для IKE. Элементы различаются в зависимости от версии IKE.
ESP	Шифрование	Выберите алгоритм шифрования для ESP. Этот режим доступен, если для параметра **Протокол безопасности** выбрано значение **ESP**.
	Аутентификация	Выберите алгоритм проверки подлинности для ESP. Этот режим доступен, если для параметра **Протокол безопасности** выбрано значение **ESP**.
AH	Аутентификация	Выберите алгоритм шифрования для AH. Этот режим доступен, если для параметра **Протокол безопасности** выбрано значение **AH**.

Настройка политики групп

Групповая политика — это одно или несколько правил, которые применимы к пользователю или группе пользователей.Сканер управляет IP-пакетами, которые соответствуют настроенной политике.Аутентификация IP-пакетов выполняется сначала в соответствии с групповой политикой с 1 по 10, далее применяется политика по умолчанию.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **IPsec/Фильтрация IP** > **Основные**.
2. Щелкните вкладку с номером, которую необходимо настроить.
3. Введите значение для каждого элемента.
4. Нажмите **Следующий**.

   Отображается запрос подтверждения.
5. Нажмите **OK**.

   Настройки сканера обновлены.

Параметры настройки в разделе Групповая политика

Параметры	Настройки и их описание
Включить эту Групповую политику	Групповую политику можно включить или выключить.

Управление доступом

Настройте способ управления трафиком IP-пакетов.

Параметры	Настройки и их описание
Разрешить доступ	Выберите этот параметр, чтобы разрешить прохождение настроенных IP-пакетов.
Запретить доступ	Выберите этот параметр, чтобы запретить прохождение настроенных IP-пакетов.
IPsec	Выберите этот параметр, чтобы запретить прохождение настроенных пакетов IPsec.

Локальный адрес (сканер)

Выберите адрес IPv4 или IPv6, соответствующий вашему сетевому окружению. Если IP-адрес назначается автоматически, можно выбрать параметр **Использовать полученный автоматически адрес IPv4**.

Примечание:
Если адрес IPv6 присваивается автоматически, соединение может быть недоступно. Настройте статический адрес IPv6.

Удаленный адрес(узел)

Введите IP-адрес устройства для контроля доступа. IP-адрес должен иметь длину не более 43 символов. Если IP-адрес не введен, контролируются все адреса.

Примечание:
Если IP-адрес присваивается автоматически (например, сервером DHCP), то соединение может быть недоступно. Настройте статический IP-адрес.

Способ выбора порта

Выберите способ указания портов.

❏ Имя службы

Если выбрано значение **Имя службы** для параметра **Способ выбора порта**, выберите нужный параметр.

❏ Протокол передачи

Настройте режим инкапсуляции при выборе значения **Номер порта** для параметра **Способ выбора порта**.

Параметры	Настройки и их описание
Любой протокол	Выберите этот параметр для управления всеми типами протоколов.
TCP	Выберите этот параметр для управления одноадресными данными.
UDP	Выберите этот параметр для управления данными при широковещательной и многоадресной рассылке.
ICMPv4	Выберите этот параметр для контроля выполнения команды ping.

❏ Локальный порт

При выборе **Номер порта** для **Способ выбора порта** и **TCP** или **UDP** для **Протокол передачи** необходимо через запятую ввести номера портов для управления входящими пакетами. Введите максимум 10 номеров портов.

Например: 20,80,119,5220

Если номер порта не введен, контролируются все порты.

❏ Удаленный порт

При выборе **Номер порта** для **Способ выбора порта** и **TCP** или **UDP** для **Протокол передачи** необходимо через запятую ввести номера портов для управления исходящими пакетами. Введите максимум 10 номеров портов.

Например: 25,80,143,5220

Если номер порта не введен, контролируются все порты.

Версия IKE

Выберите значения **IKEv1** или **IKEv2** для параметра **Версия IKE**. Выберите одно из значений в соответствии с устройством, к которому подключен сканер.

❏ IKEv1

При выборе значения **IKEv1** для параметра **Версия IKE** отображаются следующие элементы.

Параметры	Настройки и их описание
Метод аутентификации	Если выбрано значение **IPsec** для параметра **Управление доступом**, выберите нужный параметр. Используемый сертификат соответствует политике по умолчанию.
Предварительный ключ	Если значение **Предварительный ключ** указано для параметра **Метод аутентификации**, то введите предварительный ключ длиной от 1 до 127 символов.
Подтвердить Предварительный ключ	Введите выбранный вами ключ для подтверждения.

❏ IKEv2

При выборе значения **IKEv2** для параметра **Версия IKE** отображаются следующие элементы.

Параметры		**Настройки и их описание**
Локально	Метод аутентификации	Если выбрано значение **IPsec** для параметра **Управление доступом**, выберите нужный параметр. Используемый сертификат соответствует политике по умолчанию.
	Тип ID	При выборе значения **Предварительный ключ** для параметра **Метод аутентификации** выберите тип идентификатора сканера.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа нельзя использовать символы @, # и =. **Отличительное имя**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ =. **IP-адрес**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя символы от A до Z, от a до z, 0–9, дефис (-) и точку (.). **Адрес эл. почты**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ @. **ID ключа**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Предварительный ключ	Если значение **Предварительный ключ** указано для параметра **Метод аутентификации**, то введите предварительный ключ длиной от 1 до 127 символов.
	Подтвердить Предварительный ключ	Введите выбранный вами ключ для подтверждения.

Параметры		Настройки и их описание
Удаленно	Метод аутентификации	Если выбрано значение **IPsec** для параметра **Управление доступом**, выберите нужный параметр. Используемый сертификат соответствует политике по умолчанию.
	Тип ID	Если для параметра **Метод аутентификации** было выбрано значение **Предварительный ключ**, выберите тип идентификатора для устройства, подлинность которого следует проверить.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа нельзя использовать символы @, # и =. **Отличительное имя**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ =. **IP-адрес**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя символы от A до Z, от a до z, 0–9, дефис (-) и точку (.). **Адрес эл. почты**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E). В строке должен присутствовать символ @. **ID ключа**: введите от 1 до 255 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Предварительный ключ	Если значение **Предварительный ключ** указано для параметра **Метод аутентификации**, то введите предварительный ключ длиной от 1 до 127 символов.
	Подтвердить Предварительный ключ	Введите выбранный вами ключ для подтверждения.

Формирование пакетов данных

Настройте режим инкапсуляции при выборе значения **IPsec** для параметра **Управление доступом**.

Параметры	Настройки и их описание
Режим передачи	Выберите этот пункт, если сканер используется в рамках одной ЛВС. IP-пакеты четвертого или более высокого уровня шифруются.
Туннельный режим	Выберите этот параметр, если вы используете сканер в сети с выходом в Интернет, например IPsec — VPN. Заголовок и данные IP-пакетов шифруются. **Удаленный шлюз(Туннельный режим)**: если для параметра **Формирование пакетов данных** указано значение **Туннельный режим**, введите адрес шлюза длиной от 1 до 39 символов.

Протокол безопасности

Если выбрано значение **IPsec** для параметра **Управление доступом**, выберите нужный параметр.

Параметры	Настройки и их описание
ESP	Выберите этот пункт для обеспечения целостности, аутентификации и шифрования данных.
AH	Выберите этот пункт для обеспечения целостности и аутентификации данных. Даже если шифрование данных запрещено, можно использовать протокол IPsec.

Настройки алгоритма

Рекомендуется выбирать значение **Любой** для всех параметров или значение, отличное от **Любой**, для каждого параметра. Если для некоторых параметров выбрать **Любой**, а для остальных параметров вариант, отличный от **Любой**, устройство может не поддерживать связь: это зависит от другого устройства, аутентификацию которого вы хотите выполнить.

Параметры		Настройки и их описание
IKE	Шифрование	Выберите алгоритм шифрования для IKE. Элементы различаются в зависимости от версии IKE.
	Аутентификация	Выберите алгоритм проверки подлинности для IKE.
	Обмен ключами	Выберите алгоритм обмена ключами для IKE. Элементы различаются в зависимости от версии IKE.
ESP	Шифрование	Выберите алгоритм шифрования для ESP. Этот режим доступен, если для параметра **Протокол безопасности** выбрано значение **ESP**.
	Аутентификация	Выберите алгоритм проверки подлинности для ESP. Этот режим доступен, если для параметра **Протокол безопасности** выбрано значение **ESP**.
AH	Аутентификация	Выберите алгоритм шифрования для AH. Этот режим доступен, если для параметра **Протокол безопасности** выбрано значение **AH**.

Сочетание Локальный адрес (сканер) и Удаленный адрес(узел) в Групповая политика

		Настройка Локальный адрес (сканер)		
		IPv4	IPv6*2	Любые адреса*3
Настройка Удаленный адрес(узел)	IPv4*1	✓	–	✓
	IPv6*1*2	–	✓	✓
	Пусто	✓	✓	✓

*1 Если для **Управление доступом** выбран **IPsec**, вы не можете указать длину префикса.

*2 Если для **Управление доступом** выбран **IPsec**, вы можете выбрать адрес локального соединения (fe80::), однако групповая политика будет отключена.

*3 Кроме адресов локального соединения IPv6.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Ссылки на название службы в групповой политике

Примечание:
Недоступные службы отображаются, но не могут быть выбраны.

Название службы	Тип протокола	Номер локального порта	Номер удаленного порта	Контролируемые функции
Любой	—	—	—	Все службы
ENPC	UDP	3289	Любой порт	Поиск сканера из приложений, таких как Epson Device Admin и драйвер сканера
SNMP	UDP	161	Любой порт	Получение данных и настройка конфигурации административной базы данных (MIB) из приложений, таких как Epson Device Admin и драйвер сканера Epson.
WSD	TCP	Любой порт	5357	Управление WSD
WS-Discovery	UDP	3702	Любой порт	Поиск сканеров WSD
Network Scan	TCP	1865	Любой порт	Пересылка отсканированных данных из Document Capture Pro
Network Push Scan	TCP	Любой порт	2968	Получение информации о задании при сканировании по технологии push из приложения Document Capture Pro
Network Push Scan Discovery	UDP	2968	Любой порт	Поиск компьютера со сканера
Данные FTP (удаленные)	TCP	Любой порт	20	Клиент FTP (пересылка отсканированных данных) Управление может осуществляться, только если сервер FTP использует удаленный порт 20.
Управление FTP (удаленное)	TCP	Любой порт	21	Клиент FTP (контроль пересылаемых отсканированных данных)
CIFS (удаленный)	TCP	Любой порт	445	Клиент CIFS (пересылка отсканированных данных в папку)
NetBIOS Name Service (удаленные)	UDP	Любой порт	137	Клиент CIFS (пересылка отсканированных данных в папку)
NetBIOS Datagram Service (удаленные)	UDP	Любой порт	138	
NetBIOS Session Service (удаленные)	TCP	Любой порт	139	

Название службы	Тип протокола	Номер локального порта	Номер удаленного порта	Контролируемые функции
HTTP (локальный)	TCP	80	Любой порт	Сервер HTTP(S) (пересылка данных Web Config и WSD)
HTTPS (локальный)	TCP	443	Любой порт	
HTTP (удаленный)	TCP	Любой порт	80	HTTP(S)-клиент (обновление встроенного ПО и корневого сертификата)
HTTPS (удаленный)	TCP	Любой порт	443	

Примеры конфигурации IPsec/Фильтрация IP

Получение только пакетов IPsec.

Данный пример представляет собой настройку только политики по умолчанию.

Стандартная политика:

❏ **IPsec/Фильтрация IP**: **Включить**

❏ **Управление доступом**: **IPsec**

❏ **Метод аутентификации**: **Предварительный ключ**

❏ **Предварительный ключ**: введите до 127 символов.

Групповая политика: не настраивайте.

Получение данных сканирования и настроек сканера

В приведенном примере разрешается обмен данными сканирования и конфигурации сканера между указанными службами.

Стандартная политика:

❏ **IPsec/Фильтрация IP**: **Включить**

❏ **Управление доступом**: **Запретить доступ**

Групповая политика:

❏ **Включить эту Групповую политику**: установите флажок.

❏ **Управление доступом**: **Разрешить доступ**

❏ **Удаленный адрес(узел)**: IP-адрес клиента.

❏ **Способ выбора порта**: **Имя службы**

❏ **Имя службы**: установите флажок **ENPC**, **SNMP**, **HTTP (локальный)**, **HTTPS (локальный)** и **Network Scan**.

Разрешение доступа только с заданного IP-адреса

Этот пример обеспечивает заданному IP-адресу доступ к сканеру.

Стандартная политика:

❏ **IPsec/Фильтрация IP**: **Включить**

❏ **Управление доступом**:**Запретить доступ**

Групповая политика:

❏ **Включить эту Групповую политику**: установите флажок.

❏ **Управление доступом**: **Разрешить доступ**

❏ **Удаленный адрес(узел)**: IP-адрес клиента администратора.

Примечание:
Независимо от настроек политики, клиент будет иметь возможность настройки и доступа к сканеру.

Настройка сертификата для IPsec/фильтрации IP

Настройте клиентский сертификат для IPsec/фильтрации IP. После настройки сертификата его можно использовать в качестве метода аутентификации для IPsec/фильтрации IP. Если необходимо настроить центр сертификации, перейдите к разделу **Сертификат ЦС**.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **IPsec/Фильтрация IP** > **Сертификат клиента**.

2. Импортируйте сертификат в поле **Сертификат клиента**.

   Если вы уже импортировали сертификат, опубликованный центром сертификации, можно скопировать этот сертификат и использовать его в IPsec/фильтрации IP. Чтобы скопировать сертификат, выберите его в списке **Копировать из** и щелкните **Копир.**.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

➡ «Настройка Сертификат, подписанный ЦС» на стр. 105

➡ «Настройка Сертификат ЦС» на стр. 109

Подключение сканера к сети IEEE802.1X

Настройка сети IEEE802.1X

При настройке IEEE802.1X на сканере его можно использовать в сети, подключенной к серверу RADIUS, на коммутаторе локальной сети или в качестве точки доступа.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **IEEE802.1X** > **Основные**.

2. Введите значение для каждого элемента.

   Если вы хотите использовать сканер в сети Wi-Fi, щелкните **Настройка Wi-Fi** и выберите или введите SSID.

   Примечание:
   Настройки сети могут совместно использоваться для Ethernet и Wi-Fi.

3. Нажмите **Следующий**.

   Отображается запрос подтверждения.

4. Нажмите **OK**.

   Настройки сканера обновлены.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Параметры настройки сети IEEE 802.1X

Параметры	Настройки и их описание	
IEEE802.1X (проводная ЛВС)	Можно включить или отключить параметры страницы (**IEEE802.1X** > **Основные**) для IEEE802.1X (проводная сеть LAN).	
IEEE802.1X (Wi-Fi)	Отображается состояние подключения IEEE802.1X (Wi-Fi).	
Способ подключения	Отображает метод подключения к текущей сети.	
Тип EAP	Выберите параметр для метода аутентификации между сканером и сервером RADIUS.	
	EAP-TLS	Необходимо получить и импортировать сертификат, подписанный ЦС.
	PEAP-TLS	
	PEAP/MSCHAPv2	Необходимо настроить пароль.
	EAP-TTLS	
Идентификатор пользователя	Укажите идентификатор (ID) для использования при аутентификации сервера RADIUS. Введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).	
Пароль	Укажите пароль для аутентификации сканера. Введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). При использовании сервера Windows в качестве сервера RADIUS можно ввести до 127 символов.	
Подтверждение пароля	Введите выбранный вами пароль для подтверждения.	
Идентификатор сервера	Можно указать идентификатор сервера для аутентификации с определенным сервером RADIUS. Аутентификатор проверяет наличие ID сервера в поле subject/subjectAltName сертификата сервера, который либо отправляется с сервера RADIUS, либо нет. Введите от 0 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).	
Проверка подлинности сертификатов	Можно задать проверку сертификата независимо от метода аутентификации. Импортируйте сертификат в **Сертификат ЦС**.	
Анонимное имя	При выборе значения **PEAP-TLS** или **PEAP/MSCHAPv2** для параметра **Тип EAP** можно задать анонимное имя вместо идентификатора пользователя для первой фазы PEAP-аутентификации. Введите от 0 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).	

Параметры	Настройки и их описание	
Криптографическая стойкость	Можно выбрать один из уровней, указанных ниже.	
	Высокий	AES256/3DES
	Средняя	AES256/3DES/AES128/RC4

Настройка сертификата для IEEE802.1X

Настройте клиентский сертификат для IEEE802.1X. Если он настроен, **EAP-TLS** и **PEAP-TLS** можно использовать в качестве метода аутентификации IEEE802.1x. Если необходимо настроить сертификат центра сертификации, перейдите к разделу **Сертификат ЦС**.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **IEEE802.1X** > **Сертификат клиента**.
2. Укажите сертификат в поле **Сертификат клиента**.

   Если вы уже импортировали сертификат, опубликованный центром сертификации, можно скопировать этот сертификат и использовать его в IEEE802.1X. Чтобы скопировать сертификат, выберите его в списке **Копировать из** и щелкните **Копир.**.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Решение проблем, связанных с расширенной безопасностью

Восстановление настроек безопасности

При создании среды с повышенным уровнем безопасности, например IPsec/фильтрации IP, может быть невозможно связаться с устройствами вследствие недопустимых настроек или проблем с устройством или сервером. В этом случае восстановите настройки безопасности, чтобы повторно внести настройки на устройстве или разрешить временное использование.

Отключение функции безопасности с помощью ПО Web Config

Можно отключить IPsec/Фильтрация IP с помощью Web Config.

1. Войдите в Web Config и выберите вкладку **Безопасность сети** > **IPsec/Фильтрация IP** > **Основные**.
2. Отключите параметр **IPsec/Фильтрация IP**.

Неполадки при использовании функций защиты сети

Забыт предварительный ключ

Снова настройте предварительный ключ.

Чтобы изменить ключ, откройте Web Config и выберите вкладку **Безопасность сети** > **IPsec/Фильтрация IP** > **Основные** > **Стандартная политика** или **Групповая политика**.

Изменение общего ключа подразумевает настройку общего ключа для компьютеров.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

➡ «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 111

Не удается соединиться по протоколу IPsec

Укажите алгоритм, не поддерживаемый сканером или компьютером.

Сканер поддерживает следующие алгоритмы. Проверьте параметры компьютера.

Методы обеспечения безопасности	Алгоритмы
Алгоритм шифрования IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Алгоритм проверки подлинности IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Алгоритм обмена ключами IKE	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
Алгоритм шифрования ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Алгоритм проверки подлинности ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Алгоритм проверки подлинности AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Доступно только для IKEv2.

Соответствующая информация

➡ «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 111

Неожиданная потеря соединения

IP-адрес сканера изменен или не может использоваться.

Если IP-адрес, зарегистрированный для локального адреса в Групповая политика, изменен или не может использоваться, связь IPsec будет невозможна. Отключите протокол IPsec с помощью панели управления сканера.

Если данные DHCP устарели, DHCP-сервер перезагружается или IPv6-адрес устарел либо не был получен, то сканер может не найти IP-адрес, зарегистрированный для приложения Web Config (вкладка **Безопасность сети** > **IPsec/Фильтрация IP** > **Основные** > **Групповая политика** > **Локальный адрес (сканер)**).

Используйте статический IP-адрес.

IP-адрес компьютера изменен или не может использоваться.

Если IP-адрес, зарегистрированный для удаленного адреса в Групповая политика, изменен или не может использоваться, связь IPsec будет невозможна.

Отключите протокол IPsec с помощью панели управления сканера.

Если данные DHCP устарели, DHCP-сервер перезагружается или IPv6-адрес устарел либо не был получен, то сканер может не найти IP-адрес, зарегистрированный для приложения Web Config (вкладка **Безопасность сети** > **IPsec/Фильтрация IP** > **Основные** > **Групповая политика** > **Удаленный адрес(узел)**).

Используйте статический IP-адрес.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

➡ «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 111

Не удается подключиться после настройки IPsec/фильтрации IP

Неверные параметры IPsec/фильтрации IP.

Отключите IPsec/фильтрацию IP на панели управления сканера.Подключите сканер и компьютер и снова настройте параметры IPsec/фильтрации IP.

Соответствующая информация

➡ «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 111

Не удается получить доступ к сканеру после настройки IEEE 802.1X

Неверные параметры IEEE 802.1X.

Отключите IEEE 802.1X и Wi-Fi на панели управления сканера. Подключите сканер и компьютер, затем повторно настройте IEEE 802.1X.

Подключите сканер и компьютер, затем повторно настройте IEEE 802.1X.

Соответствующая информация

➡ «Настройка сети IEEE802.1X» на стр. 123

Неполадки при использовании цифрового сертификата

Невозможно импортировать Сертификат, подписанный ЦС

Сертификат, подписанный ЦС и информация в CSR не совпадают.

Если информация в Сертификат, подписанный ЦС и в CSR не совпадают, CSR не удастся импортировать.Проверьте следующее.

❏ Импорт сертификата выполняется на устройство, которое не имеет аналогичной информации?

Проверьте информацию CSR, а затем импортируйте сертификат на устройство, которое имеет ту же информацию.

❏ Перезаписан ли сохраненный сканером CSR после отправки CSR в центр сертификации?

Получите снова сертификат, подписанный ЦС, с помощью CSR.

Сертификат, подписанный ЦС больше 5 КБ.

Нельзя импортировать сертификат Сертификат, подписанный ЦС размером больше чем 5 КБ.

Неверный пароль для импорта сертификата.

Введите правильный пароль.Если пароль забыт, то импортировать сертификат невозможно.Еще раз получите Сертификат, подписанный ЦС.

Соответствующая информация

➡ «Импорт сертификата, подписанного ЦС» на стр. 106

Невозможно обновить самозаверяющий сертификат

Не введен параметр Общее имя.

Нужно ввести **Общее имя**.

В параметре Общее имя использованы неподдерживаемые символы.

Введите от 1 до 128 символов или в форматах IPv4, IPv6, имени хоста, или в формате FQDN в ASCII (от 0x20 до 0x7E).

В общем имени использованы запятая или пробел.

Если введена запятая, то **Общее имя** разделяется в этой точке.Если до или после запятой введен только пробел, то возникает ошибка.

Соответствующая информация

➡ «Обновление самозаверяющего сертификата» на стр. 108

Невозможно создать CSR

Не введен параметр Общее имя.

Нужно ввести **Общее имя**.

В параметрах Общее имя, Организация, Организационное подразделение, Населенный пункт и Штат/Провинция использованы неподдерживаемые символы.

Введите символы или в форматах IPv4, IPv6, имени хоста, или в формате FQDN в ASCII (от 0x20 до 0x7E).

В параметре Общее имя использованы запятая или пробел.

Если введена запятая, то **Общее имя** разделяется в этой точке.Если до или после запятой введен только пробел, то возникает ошибка.

Соответствующая информация

➡ «Получение сертификата, подписанного ЦС» на стр. 105

Появление предупреждения, касающегося цифрового сертификата

Сообщения	Причина/действия для устранения
Введите сертификат сервера.	**Причина** Не выбран файл для импорта. **Действия для устранения** Выберите файл и нажмите **Импорт**.
Сертификат ЦС 1 не введен.	**Причина** Сертификат ЦС 1 не введен, введен только сертификат ЦС 2. **Действия для устранения** Импортируйте сертификат ЦС 1.
Недопустимое значение внизу.	**Причина** Неподдерживаемые символы содержатся в пути к файлу и (или) в пароле. **Действия для устранения** Убедитесь, что символы для данного параметра введены правильно.
Недопустимые дата и время.	**Причина** Дата и время сканера не установлены. **Действия для устранения** Установите дату и время, используя Web Config или EpsonNet Config.
Недопустимый пароль.	**Причина** Пароль, установленный для сертификата ЦС, и введенный пароль не совпадают. **Действия для устранения** Введите правильный пароль.

Сообщения	Причина/действия для устранения
Недопустимый файл.	**Причина** Сертификат в формате X509 не импортируется. **Действия для устранения** Убедитесь, что выбран правильный сертификат, присланный надежным центром сертификации.
	Причина Импортируемый файл слишком большой. Максимальный размер файла 5 КБ. **Действия для устранения** Выбран правильный файл, однако сертификат может быть поврежден или подделан.
	Причина Цепочка, содержащаяся в сертификате, является недопустимой. **Действия для устранения** Для получения дополнительной информации о сертификате см. сайт центра сертификации.
Нельзя использовать сертификат сервера, включающий более трех сертификатов ЦС.	**Причина** Файл сертификата в формате PKCS#12 содержит более чем 3 сертификата ЦС. **Действия для устранения** Выполните импорт каждого сертификата путем конвертации из формата PKCS#12 в формат PEM или выполните импорт файла сертификата в формате PKCS#12, который содержит до двух сертификатов ЦС.
Срок действия сертификата истек. Проверьте действительность сертификата или значение дата и время в устройстве.	**Причина** Сертификат устарел. **Действия для устранения** ❏ Если сертификат устарел, то получите и импортируйте новый сертификат. ❏ Если сертификат не устарел, то убедитесь, что дата и время сканера установлены правильно.
Требуется закрытый ключ.	**Причина** Отсутствует парный секретный ключ с сертификатом. **Действия для устранения** ❏ Если сертификат представлен в формате PEM/DER и получен из CSR при помощи компьютера, то укажите файл с секретным ключом. ❏ Если сертификат представлен в формате PKCS#12 и получен из CSR при помощи компьютера, то создайте файл, содержащий секретный ключ.
	Причина Был повторно импортирован сертификат в формате PEM/DER, полученный из CSR при помощи Web Config. **Действия для устранения** Если сертификат в формате PEM/DER и получен из CSR при помощи Web Config, то его можно импортировать только раз.

Сообщения	Причина/действия для устранения
Не удалось выполнить настройку.	**Причина** Невозможно завершить настройку из-за потери соединения между сканером и компьютером, невозможно считать файл по причине возникших ошибок. **Действия для устранения** После проверки указанного файла и соединения импортируйте файл снова.

Соответствующая информация

➡ «О цифровом сертификате» на стр. 104

Ошибочное удаление сертификата, подписанного ЦС

Для сертификата, подписанного ЦС, не создается резервной копии.

При наличии резервной копии файла импортируйте сертификат снова.

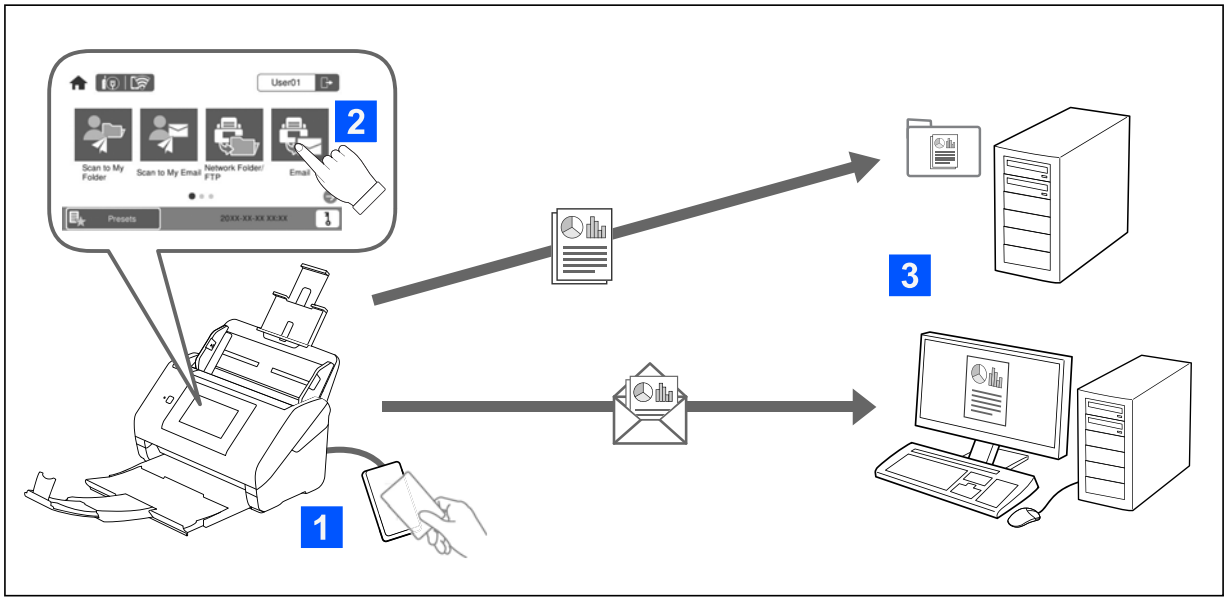
Невозможно повторно импортировать удаленный сертификат, если он был получен с помощью CSR из приложения Web Config.Создайте CSR и получите новый сертификат.

Соответствующая информация

➡ «Импорт сертификата, подписанного ЦС» на стр. 106
➡ «Удаление сертификата, подписанного ЦС» на стр. 108

Настройки аутентификации

Сведения о ПО Настройки аутентификации



Если включены Настройки аутентификации, перед началом сканирования требуется выполнить аутентификацию пользователя. Вы можете задать способы сканирования, которые могут использоваться каждым из пользователей, и таким образом предотвратить случайные операции.

Можно указать адрес электронной почты авторизованного пользователя в качестве целевого места сканирования (Скан. в Мою эл. почту) или сохранять данные каждого пользователя в личных папках (Сканир. в Мою папку). Можно также указать другие методы сканирования.

Примечание:

❏ *Если включены Настройки аутентификации, сканирование с компьютера или смарт-устройства выполнять нельзя.*

❏ *В дополнение к Настройки аутентификации, описанным в данном руководстве, можно также организовать систему аутентификации с использованием сервера аутентификации. Для создания системы используйте Document Capture Pro Server Authentication Edition (сокращенное название — Document Capture Pro Server AE). Для получения дополнительной информации свяжитесь с местным отделением Epson.*

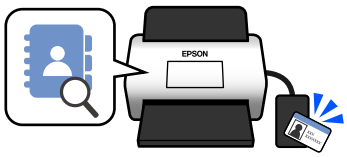
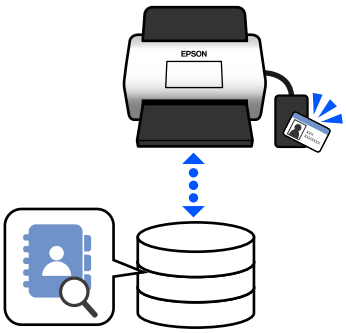
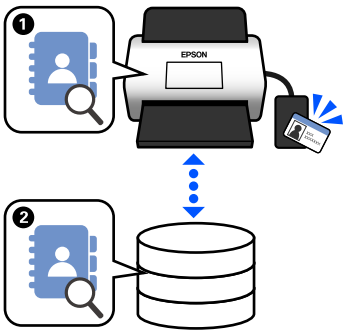
Доступные функции для Настройки аутентификации

Функция сканирования на панели управления	Настройки аутентификации	
	При включении	При выключении
Скан. в Мою папку Сохранение изображений в папку, назначенную авторизованному пользователю.	✓	—
Скан. в Мою эл. Почту Отправка изображений на адрес электронной почты авторизованного пользователя.	✓	—

Функция сканирования на панели управления	Настройки аутентификации	
	При включении	При выключении
Сканир. в сет. папку/FTP Сохранение изображений в сетевую папку.	✓	✓
Сканиров. на компьютер Сохранение изображений на подключенный компьютер с использованием заданий, созданных в ПО Document Capture Pro (Windows)/Document Capture (Mac OS). * Если Настройки аутентификации включены, вы можете использовать только задания, зарегистрированные в разделе **Предустан.**.	✓*	✓
Сканирование в эл. почту Отправка изображений на заданный адрес электронной почты.	✓	✓
Сканирование в облако Отправка изображений в указанную облачную службу.	✓	✓
Скан. на USB-накопитель Сохранение изображений на USB-накопитель, подключенный к сканеру. Эта функция доступна только при подключении устройства аутентификации к сканеру.	✓	✓
Сканировать в WSD Сохранение изображений на подключенный компьютер с помощью функции WSD.	—	✓
Предустан. Разрешается зарегистрировать до 48 предустановок функции сканирования. Можно выделить до пяти Предустан. пользователям, зарегистрированным в Локальная БД. Выделенные Предустан. доступны только соответствующим пользователям. Предустан., не выделенные никаким конкретным пользователям, доступны для всех пользователей.	✓	✓

Сведения о ПО Метод аутентификации

Этот сканер позволяет реализовать аутентификацию с помощью следующих методов без необходимости создания сервера аутентификации.

	Локальная БД	LDAP	Локальная БД и LDAP
Расположение информации о пользователе	**Память сканера** При этом методе аутентификации зарегистрированная на сканере информация о пользователе проверяется и сравнивается с информацией о пользователе, который использует функцию сканирования.	**LDAP-сервер*** При этом виде аутентификации проверяется информация о пользователе, зарегистрированная на LDAP-сервере, который синхронизирован с принтером. Так как в кэше сканера можно временно сохранить до 300 элементов пользовательской информации с LDAP-сервера, то при недоступности LDAP-сервера аутентификация может выполняться с использованием кэша. * Сервер, предоставляющий службу каталогов, которая может обеспечивать связь с использованием протокола LDAP.	**Память сканера и LDAP-сервер** Сначала проверяется информация о пользователе, зарегистрированная в сканере (❶), и если соответствие не обнаруживается, проверяется информация о пользователе на LDAP-сервере (❷).
			
Количество зарегистрированных пользователей	50 (в памяти сканера)	Не ограничено (при использовании LDAP-сервера)	50 (в памяти сканера) Не ограничено (при использовании LDAP-сервера)
Кэш-память сканера	—	300	До 300 (50 слотов кэш-памяти используются совместно с Пользовательские настройки в Локальная БД)
Способы входа	Доступны следующие способы. ❏ Поднимите карту аутентификации или введите **Идентификатор пользователя** и **Пароль**. ❏ Поднимите карту аутентификации или введите **Идентификационный номер**. ❏ Введите **Идентификатор пользователя** и **Пароль**. ❏ Введите **Идентификатор пользователя**. ❏ Введите **Идентификационный номер**.		

	Локальная БД	LDAP	Локальная БД и LDAP
Ограничения функции «Сканирование в...»	Индивидуальная настройка для каждого пользователя	Одинаковые настройки для всех пользователей LDAP	Пользователи Локальная БД: индивидуальная настройка Пользователи LDAP: одинаковые настройки для всех пользователей
Выделение Предустан. для пользователей	До пяти на пользователя	— (индивидуальная настройка невозможна)	Пользователи Локальная БД: до пяти на пользователя Пользователи LDAP: —

Программное обеспечение для настройки

Настройка осуществляется с помощью программного обеспечения Web Config или Epson Device Admin.

❏ При использовании Web Config настройку сканера можно выполнить только через браузер.

«Web Config» на стр. 37

❏ При использовании Epson Device Admin можно выполнить настройку нескольких сканеров с использованием шаблона конфигурации.

«Epson Device Admin» на стр. 38

Обновление встроенного программного обеспечения сканера

Перед включением Настройки аутентификации обновите встроенное ПО сканера до последней версии. Предварительно подключите сканер к Интернету.

Важно:

Не отключайте компьютер или сканер во время обновления.

При выполнении настройки с помощью Web Config:

Выберите вкладку **Управление устройствами** > **Обновление встроенной программы**, а затем следуйте инструкциям на экране для обновления встроенного ПО.

При выполнении настройки с помощью Epson Device Admin:

На экране со списком устройств выберите **Главная** > **Прошивка** > **Обновить**, а затем следуйте инструкциям для обновления встроенного ПО.

Примечание:

Если уже установлена последняя версия встроенного программного обеспечения, обновлять его не нужно.

Подключение и настройка устройства аутентификации

Если вы хотите подключить и использовать устройство аутентификации, например устройство чтения IC-карт, сначала необходимо настроить это устройство. Это не является обязательным, если для проведения аутентификации устройство аутентификации не используется.

Соответствующая информация

➡ «Подключение устройства аутентификации» на стр. 140

➡ «Параметры устройства аутентификации» на стр. 140

Список совместимых устройств чтения карт

Нахождение устройства в этом списке не может гарантировать выполнение необходимых операций этим устройством.

Если указано «Да»: устройство поддерживается (идентификационная информация может быть считана с использованием стандартных настроек устройства чтения карт).

Если указано «Нет»: совместимость отсутствует.

Производитель	Модель	Номер модели	Карта аутентификации							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	Нет	Нет	Нет	Клавиатура
RF IDEAS	pcProx	RDR-7081BKU	Да*1	Нет	Да	Да	Нет	Нет	Нет	Клавиатура
RF IDEAS	pcProx	RDR-7581AKU	Да	Нет	Да*1	Да*1	Нет	Нет	Нет	Клавиатура
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Нет	Нет	Да	Да	Нет	Нет	Нет	Клавиатура

Производитель	Модель	Номер модели	Карта аутентификации							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Да	Нет	Да	Да	Да	Да	Да	Клавиатура
ELATEC	TWN4 MULTITECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Да	Да	Да	Да	Да	Да	Да	Клавиатура
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	Нет	Да	Клавиатура*1
ACS	ACR122U	ACR122U	Нет	Нет	Да*2	Да*2	Да	Нет	Да*2	PC/SC
ACS	ACR1252	ACR1252	Нет	Нет	Да*2	Да*2	Да	Да	Да*2	PC/SC
Sony	PaSoRi	RC-S330/S	Нет	Нет	Да*2	Да*2	Да*2	Да*2	Да*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Нет	Нет	Да*2	Да*2	Да*2	Да*2	Да*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Да	Да	Да	Да	Да	Да	Да	Клавиатура

Производитель	Модель	Номер модели	Карта аутентификации							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
DMZ	Leitor RFID Multi-125	DMZ087	Нет	Да	Нет	Нет	Нет	Нет	Нет	Клавиатура
DMZ	Leitor RFID Mifare	DMZ088	Нет	Нет	Да	Да	Нет	Нет	Нет	Клавиатура
DMZ	Biometric & RFID Reader	DMZ073	Нет	Да	Нет	Нет	Нет	Нет	Нет	Клавиатура
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	Нет	Нет	Да	Да	Нет	Нет	Да	Клавиатура
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Нет	Нет	Да	Да	Нет	Нет	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	Нет	Нет	Нет	Клавиатура
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Да	Да	Да	Да	Да	Да	Нет	Клавиатура

*1 Необходимо изменить настройки устройства чтения карт с помощью оригинального программного обеспечения, предоставляемого производителем устройства.

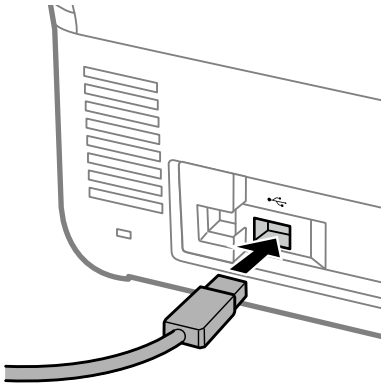
*2 Если в качестве идентификатора аутентификации вам необходимо использовать данные в определенной области карты, отличной от стандартного расположения идентификационной информации на карте, и необходимо соответствующим образом настроить параметры вашего изделия, за информацией о способах такой настройки обратитесь к торговому партнеру или местному представителю Epson.

Подключение устройства аутентификации

Важно:

При подключении устройства аутентификации к нескольким сканерам необходимо использовать устройство с тем же номером модели.

Подключите USB-кабель устройства чтения карт к USB-порту для подключения внешнего интерфейса на сканере.



Проверка работы устройства аутентификации

Вы можете проверить состояние подключения и распознавание карты аутентификации для устройства аутентификации с панели управления сканера.

Информация отображается при выборе **Настр.** > **Информация об устройстве** > **Состояние аутентификации устройства**.

Параметры устройства аутентификации

Выберите формат чтения для данных аутентификации, полученных с карты аутентификации.

Для устройства аутентификации можно задать следующие способы чтения данных.

❏ Чтение данных из определенной области карты аутентификации, например номера сотрудника или персонального идентификатора.

❏ Использование данных карты аутентификации (например, серийного номера), за исключением UID.

Вы можете использовать соответствующий инструмент для генерации рабочих параметров. Для получения дополнительной информации обратитесь к вашему дилеру.

Примечание:
Использование карт проверки подлинности других изготовителей:

При использовании данных UID (идентификационных данных карты, например серийного номера) можно одновременно использовать карты аутентификации различного типа. Совместное использование таких карт невозможно, если используется другая информация с них.

При выполнении настройки с помощью Web Config:

Выберите вкладку **Управление устройствами** > **Картридер**.

При выполнении настройки с помощью Epson Device Admin:

Выберите **Настройки администратора** > **Настройки аутентиф-ции** > **Картридер** из шаблона конфигурации.

Элемент	Описание
Vendor ID	Ограничивает использование устройств аутентификации путем указания идентификатора поставщика устройства (4 буквенно-цифровых символа; диапазон значений — от 0000 до FFFF). Если нет необходимости ограничивать использование устройств аутентификации, введите значение 0000.
Product ID	Ограничивает использование устройств аутентификации путем указания идентификатора продукта (4 буквенно-цифровых символа; диапазон значений — от 0000 до FFFF). Если нет необходимости ограничивать использование устройств аутентификации, введите значение 0000.
Рабочий параметр	Задает эксплуатационный параметр устройства аутентификации (от 0 до 8192 символов). Можно использовать следующие символы: A–Z, a–z, 0–9, +, /, =, пробел и перевод строки.
Картридер	Выбор формата преобразования для устройства аутентификации. Можно проверить данные о формате. См. ссылку, указанную в описании элемента.
Формат сохранения идентификатора опознавательной карточки	Выбор формата преобразования для данных аутентификации ID-карты. Можно проверить данные о формате. См. ссылку, указанную в описании элемента.
Установить диапазон идентификаторов карты	Включает возможность указания положения считывания.
Исходное положение текста	Указание позиции начала текста для чтения идентификационных данных. Можно указать значение от 1 до 4096.
Кол-во символов	Указание количества символов, которые будут считываться, начиная с позиции начала идентификационных данных. Можно указать значение от 1 до 4096.

Регистрация и настройка информации

Настройка

Задайте необходимые настройки в зависимости от используемых Метод аутентификации и способа сканирования.

Важно:

Перед началом настройки убедитесь, что время на сканере настроено правильно.

Если время настроено неправильно, появится сообщение «Срок действия лицензии истек», из-за которого может не получиться настроить сканер. Кроме того, правильные настройки времени необходимы для использования защитных функций, например связи по протоколам SSL/TLS или IPsec. Время можно настроить следующим образом.

- ❏ *Web Config: вкладка **Управление устройствами** > **Дата и время** > **Дата и время**.*
- ❏ *Панель управления сканера: **Настр.** > **Основ. настройки** > **Настр. даты и времени**.*

Настройки	Локальная БД	LDAP	Локальная БД и LDAP
Включение аутентификации Необходимо включить аутентификацию перед настройкой ее параметров. «Включение аутентификации» на стр. 143	✓	✓	✓
Настройки аутентификации Настройка Метод аутентификации и вариантов авторизации пользователей. «Настройки аутентификации» на стр. 143	✓	✓	✓
Регистрация Пользовательские настройки Регистрация настроек для каждого пользователя. Также можно осуществлять групповую регистрацию пользователей с помощью CSV-файла. «Регистрация Пользовательские настройки» на стр. 145	✓	—	✓
Синхронизация с Сервер LDAP Настройка параметров синхронизации LDAP-сервера. «Синхронизация с Сервер LDAP» на стр. 152	—	✓	✓
Настройка Сервер эл. почты Настройка параметров почтового сервера. Задайте эти параметры при использовании функций, требующих настройки почтового сервера (например, Скан. в Мою эл. почту). «Настройка почтового сервера» на стр. 156	✓	✓	✓
Настройка функции Сканир. в Мою папку Указание целевых папок. Их необходимо указать при использовании функции Сканир. в Мою папку. «Настройка функции Сканир. в Мою папку» на стр. 157	✓	✓	✓

Настройки	Локальная БД	LDAP	Локальная БД и LDAP
Настройка функций One-touch (Одно касание) Эти настройки задаются при изменении элементов, отображаемых на панели управления сканера. Вы можете оставить на панели управления только те значки, которые вам нужны, а также изменить порядок расположения значков. «Настройка функций One-touch (Одно касание)» на стр. 159	✓	✓	✓

Включение аутентификации

Необходимо включить аутентификацию перед настройкой ее параметров.

При выполнении настройки с помощью Web Config:

Выберите **Вкл (Устройство/Сервер LDAP)** на вкладке **Безопасность устройства** > **Основные** > **Аутентификация**.

При выполнении настройки с помощью Epson Device Admin:

В шаблоне конфигурации выберите **Вкл (Устройство/Сервер LDAP)** на вкладке **Настройки администратора** > **Настройки аутентиф-ции** > **Основные** > **Аутентификация**.

Примечание:
При включении Настройки аутентификации на сканере функция Функция блокировки также включается для панели управления. Панель управления не может быть разблокирована, если включена функция Настройки аутентификации.

Даже при отключении Настройки аутентификации функция Функция блокировки остается включенной. Если вы хотите отключить ее, вы можете сделать соответствующие настройки с панели управления или из приложения Web Config.

Соответствующая информация

➡ «Настройка функции Функция блокировки с панели управления» на стр. 91

➡ «Настройка функции Функция блокировки с помощью Web Config» на стр. 91

Настройки аутентификации

Настройка Метод аутентификации и вариантов авторизации пользователей.

При выполнении настройки с помощью Web Config:

Выберите вкладку **Безопасность устройства** > **Настройки аутентификации**.

При выполнении настройки с помощью Epson Device Admin:

Выберите **Настройки администратора** > **Настройки аутентиф-ции** > **Настройки аутентификации** из шаблона конфигурации.

Элемент	Описание
Метод аутентификации	Выбор Метод аутентификации. ❏ Локальная БД Аутентификация с использованием Пользовательские настройки, зарегистрированных на сканере. Необходимо, чтобы пользователь был зарегистрирован на сканере. ❏ LDAP Аутентификация с использованием информации о пользователе, хранящейся на LDAP-сервере, который синхронизирован со сканером. Параметры LDAP-сервера должны быть настроены заранее. ❏ Локальная БД и LDAP Аутентификация с использованием информации о пользователе, зарегистрированной на сканере или хранящейся на LDAP-сервере, синхронизированном со сканером. Информация о пользователе должна быть зарегистрирована на сканере, а LDAP-сервер должен быть настроен.
Как выполняется проверка подлинности пользователя	Выбор варианта аутентификации пользователя. ❏ Карта или идент. польз. и пароль Для аутентификации пользователя применяется карта аутентификации. Также аутентификацию можно выполнять с помощью идентификатора пользователя и пароля. ❏ Идент. польз. и пароль Аутентификация пользователя выполняется с помощью идентификатора пользователя и пароля. Если выбрана эта функция, карту аутентификации применять для аутентификации нельзя. ❏ Идентификатор пользователя Аутентификация пользователя выполняется только с помощью идентификатора пользователя. Пароль задавать не нужно. ❏ Карта или идентификационный номер Для аутентификации пользователя применяется карта аутентификации. Также можно использовать Идентификационный номер. ❏ Идентификационный номер Аутентификация пользователя выполняется только с помощью идентификационного номера.
Разрешить пользователям регистрировать карты аутентификации	Установите этот параметр, чтобы разрешить пользователям регистрировать в системе карты доступа. Если выбрано значение **LDAP** для параметра **Метод аутентификации**, то данный параметр установить нельзя. Подробнее о том, как пользователи могут зарегистрировать свои карты аутентификации, см. разделе «Регистрация карты аутентификации» в *Руководство пользователя*.
Минимальное число цифр в идентификационном номере	Установка минимального количества цифр для идентификационного номера.
Кэширование для прошедших проверку пользователей LDAP	При использовании аутентификации через LDAP-сервер можно включить или выключить кэширование пользовательской информации.

Элемент	Описание
Использовать пользовательские данные для аутентификации SMTP	При использовании идентификатора и пароля пользователя для аутентификации можно задать использование пользовательской информации для аутентификации SMTP. Системой используются последний идентификатор и пароль пользователя, которые использовались для входа в систему.
Ограничения для аутентифицированных по LDAP пользователей	Если используется LDAP, можно задать функции, доступные пользователю.

Регистрация Пользовательские настройки

Регистрация Пользовательские настройки, используемых для авторизации пользователей. Доступны следующие способы регистрации.

❏ Регистрация Пользовательские настройки по одному (Web Config)

❏ Регистрация нескольких Пользовательские настройки в пакетном режиме с помощью CSV-файла (Web Config)

❏ Регистрация Настройки пользователя на нескольких сканерах в пакетном режиме с помощью шаблона конфигурации (Epson Device Admin)

Соответствующая информация

➡ «Индивидуальная регистрация Пользовательские настройки (Web Config)» на стр. 145

➡ «Регистрация нескольких Пользовательские настройки с помощью CSV-файла (Web Config)» на стр. 146

➡ «Регистрация Настройки пользователя на нескольких сканерах в пакетном режиме (Epson Device Admin)» на стр. 150

Индивидуальная регистрация Пользовательские настройки (Web Config)

Откройте Web Config и выберите вкладку **Безопасность устройства** > **Пользовательские настройки** > **Добавить**, затем выберите Пользовательские настройки.

Элемент	Описание
Идентификатор пользователя	Введите идентификатор пользователя, который необходимо использовать для аутентификации (от 1 до 83 символов в кодировке Unicode (UTF-8)). Поскольку идентификатор пользователя нечувствителен к регистру, при входе можно вводить буквы любого регистра.
Отображение имени пользователя	Введите имя пользователя, отображаемое на панели управления сканера (до 32 символов в кодировке Unicode (UTF-16)). Этот параметр можно оставить пустым.
Пароль	Введите пароль, который будет использоваться для аутентификации (до 32 символов в кодировке ASCII). Пароль чувствителен к регистру. Оставьте этот параметр пустым, если для параметра **Как выполняется проверка подлинности пользователя** выбрано значение **Идентификатор пользователя**.

Элемент	Описание
Идентификатор опознавательной карточки	Введите идентификатор карты аутентификации (до 116 символов в кодировке ASCII). Этот параметр можно оставить пустым. Если включен параметр **Разрешить пользователям регистрировать карты аутентификации** в разделе **Настройки аутентификации**, отображается результат, зарегистрированный пользователями.
Идентификационный номер	Этот элемент отображается, когда в разделе **Настройки аутентификации** > **Как выполняется проверка подлинности пользователя** выбран элемент **Карта или идентификационный номер** или **Идентификационный номер**. Введите число, длина которого не более 8 символов и не менее значения, заданного в разделе **Настройки аутентификации** > **Минимальное число цифр в идентификационном номере**.
Автоматическое создание	Этот элемент отображается, когда в разделе **Настройки аутентификации** > **Как выполняется проверка подлинности пользователя** выбран элемент **Карта или идентификационный номер** или **Идентификационный номер**. Нажмите, чтобы автоматически сгенерировать идентификационный номер с тем количеством цифр, которое указано в разделе **Минимальное число цифр в идентификационном номере**.
Отдел	Введите имя отдела или другие данные, идентифицирующие пользователя (до 40 символов в кодировке Unicode (UTF-16)). Этот параметр можно оставить пустым.
Адрес эл. почты	Введите адрес электронной почты пользователя (до 200 символов в кодировке ASCII). Это целевой адрес при использовании функции **Скан. в Мою эл. почту**. Этот параметр можно оставить пустым.
Сканир. в Мою папку	Если вы выбрали параметр **Индивидуально** в разделе **Сканир. в Мою папку** > **Настройка типа**, место сохранения данных настраивается индивидуально. Дополнительные сведения о настройке элементов см. ниже. «Настройка функции Сканир. в Мою папку» на стр. 157
Ограничения	Вы можете ограничить функции для каждого пользователя. Выберите функцию, разрешенную для использования.
Предустановки	Из Предустановки, зарегистрированных на сканере, можно задать не более пяти предустановок, доступных только выбранному пользователю. ❏ Предустановки, выделенные конкретному пользователю, доступны только ему. Предустановки, не выделенные никаким конкретным пользователям, доступны для всех пользователей. ❏ Если пользователю доступна только одна предустановка Предустановки, она автоматически загружается после аутентификации. Если доступно несколько Предустановки, после аутентификации будет отображен список Предустановки. ❏ Вы не можете создавать или отображать Предустановки, использующие функции, которые были ограничены в разделе **Ограничения**.

Регистрация нескольких Пользовательские настройки с помощью CSV-файла (Web Config)

Укажите настройки для каждого пользователя в CSV-файле и зарегистрируйте их в пакетном режиме.

Создание CSV-файла

Создание файла CSV для импорта Пользовательские настройки.

Примечание:
Если вы заранее зарегистрируете нужные Пользовательские настройки, а затем экспортируете отформатированный файл (CSV), вы сможете использовать зарегистрированную настройку в качестве образца для ввода параметров.

1. Войдите в Web Config и выберите вкладку **Безопасность устройства** > **Пользовательские настройки**.
2. Нажмите **Экспорт**.
3. Выберите формат файла для элемента **Формат файла**.

   Для выбора формата используйте приведенную ниже информацию.

Элемент	Описание
CSV UTF-16 (разделитель - табуляция)	Выберите этот элемент, если файл редактируется с помощью программы Microsoft Excel. Каждый параметр заключается в квадратные скобки — [ ]. Введите параметры, заключенные в квадратные скобки — [ ]. При обновлении файла мы рекомендуем перезаписать его. При первом сохранении файла в качестве формата выберите «Текст Юникод (*.txt)».
CSV UTF-8 (разделитель - запятая)	Выберите этот элемент, если файл редактируется с помощью текстового редактора или макроса без Microsoft Excel.
CSV UTF-8 (разделитель - точка с запятой)	

4. Нажмите **Экспорт**.
5. Отредактируйте и сохраните этот CSV-файл с помощью программы для работы с электронными таблицами (например, Microsoft Excel) или текстового редактора.

> ***Важно:***
> *При редактировании файла не изменяйте кодировку и информацию заголовка.*

Параметры CSV-файлов

Элемент	Настройки и их описание
UserID	Идентификатор пользователя, применяемый для аутентификации (от 1 до 83 символов в кодировке Unicode).
UserName	Имя пользователя, отображаемое на панели управления принтера (до 32 символов в кодировке Unicode). Этот параметр можно оставить пустым.

Элемент	Настройки и их описание
Password	Пароль, используемый для аутентификации (до 32 символов ASCII). При выполнении импорта это значение используется в качестве пароля вместо **EncPassword**. Оставьте этот параметр пустым, если для параметра **Как выполняется проверка подлинности пользователя** выбрано значение **Идентификатор пользователя**. При выполнении экспорта это поле остается пустым.
AuthenticationCardID	Установка результата чтения карты аутентификации. Если включен параметр **Разрешить пользователям регистрировать карты аутентификации** в разделе **Настройки аутентификации**, отображается результат, зарегистрированный пользователями. Введите не более 116 символов ASCII. Этот параметр можно оставить пустым.
IDNumber	Этот элемент отображается, когда в разделе **Настройки аутентификации** > **Как выполняется проверка подлинности пользователя** выбран элемент **Карта или идентификационный номер** или **Идентификационный номер**. Введите число, длина которого не более 8 символов и не менее значения, заданного в разделе **Настройки аутентификации** > **Минимальное число цифр в идентификационном номере**. Идентификационный номер не может дублироваться. Если он дублируется, то при импорте файла возникнет ошибка. Если поле оставлено пустым, ему автоматически присваивается номер.
Department	Введите название отдела — произвольный параметр, помогающий различать пользователей. Введите не более 40 символов в кодировке Unicode. Этот параметр можно оставить пустым.
MailAddress	Адрес электронной почты пользователя. Это целевой адрес при использовании функции **Скан. в Мою эл. почту**. Можно использовать символы A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Вводите не более 200 символов. В качестве первого символа нельзя использовать запятую (,). Этот параметр можно оставить пустым.
FolderProtocol	Установка типа функции Сканир. в Мою папку. Сетевая папка/FTP (SMB): 0; FTP: 1
FolderPath	Установка папки сохранения для функции Сканир. в Мою папку.
FolderUserName	Установка имени пользователя для функции Сканир. в Мою папку.
FolderPassword	Установите пароль для проверки подлинности к целевой папке функции Сканир. в Мою папку длиной не более 32 символов ASCII. При выполнении импорта это значение используется в качестве пароля вместо **EncPassword**. При выполнении экспорта это поле остается пустым.
FtpPassive	Установка режима соединения с сервером FTP, если значение **FTP** выбрано для параметра **Тип** для функции Сканир. в Мою папку. Активный режим: 0; пассивный режим: 1
FtpPort	Установка номера порта для отправки сканированных данных на сервер FTP от 0 до 65535, если значение **FTP** выбрано для параметра **Тип** для функции Сканир. в Мою папку.

Элемент	Настройки и их описание
ScanToMemory	Установка ограничений для функции Скан. на USB-накопитель. Не разрешено: 0; разрешено: 1
ScanToMail	Установка ограничений для функции Сканирование в электронную почту. Включить параметр **Скан. в Мою эл. Почту** можно, только если включена функция **Сканирование в электронную почту**. Не разрешено: 0; разрешено: 1
ScanToFolder	Установка ограничений для функции Сканирование в сетевую папку/FTP. Включить параметр **Скан. в Мою папку** можно, только если включена функция **Сканирование в сетевую папку/FTP**. Не разрешено: 0; разрешено: 1
ScanToCloud	Установка ограничений для функции Сканирование в облако. Не разрешено: 0; разрешено: 1
ScanToComputer	Установка ограничений для функции Сканиров. на компьютер. Не разрешено: 0; разрешено: 1
PresetIndex	Установка Предустановки, которые необходимо связать с пользователем. Можно указать не более пяти регистрационных номеров Предустановки, разделенных запятыми.
EncPassword	При экспорте пользовательских настроек значение, заданное для параметра **Password**, шифруется, затем это значение кодируется по стандарту BASE64 и выводится. Если импорт выполняется при наличии нового пароля, указанного в параметре **Password**, данное значение игнорируется. Если параметр **Password** не задан, используется данное значение и пароль принимает значение, которое было до экспорта.
EncFolderPassword	При выполнении экспорта значение, заданное для параметра **FolderPassword**, шифруется, затем кодируется по стандарту BASE64 и выводится. Если импорт выполняется при наличии нового пароля, указанного в параметре **FolderPassword**, данное значение игнорируется. Если параметр **FolderPassword** не задан, используется данное значение и пароль принимает значение, которое было до экспорта.

Импорт CSV-файла

1. Войдите в Web Config и выберите вкладку **Безопасность устройства** > **Пользовательские настройки**.
2. Нажмите **Импорт**.
3. Выберите файл, который необходимо импортировать.
4. Нажмите **Импорт**.
5. После проверки отображенной информации нажмите **OK**.

Регистрация Настройки пользователя на нескольких сканерах в пакетном режиме (Epson Device Admin)

Настройки пользователя, используемые в Локальная БД, можно зарегистрировать в пакетном режиме через LDAP-сервер или с помощью CSV/ENE-файла.

Примечание:
*ENE-файл — это бинарный файл, предоставленный компанией Epson, в котором в зашифрованном виде хранятся **Контактная информация**, в частности персональные данные и Пользовательские настройки. В него можно экспортировать данные из Epson Device Admin и установить пароль. Этот файл будет полезен в случае, когда необходимо импортировать Пользовательские настройки из файла резервной копии.*

Импорт из файлов CSV/ENE

1. Выберите **Настройки администратора** > **Настройки аутентиф-ции** > **Настройки пользователя** из шаблона конфигурации.
2. Нажмите **Импорт**.
3. Выберите **Файл CSV или ENE** в **Источник импорта**.
4. Нажмите **Обзор**.

   Откроется экран выбора файлов.
5. Чтобы открыть файл, который необходимо импортировать, выберите его.
6. Выберите способ импорта.
   - ❏ Перезаписать или добавить: если уже существует такой же идентификатор пользователя, данные перезаписываются, иначе добавляется новый идентификатор.
   - ❏ Заменить все: заменяет все на пользовательские настройки, которые вы хотите импортировать.
7. Нажмите **Импорт**.

   Откроется экран подтверждения настроек.
8. Нажмите **OK**.

   Отображается результат подтверждения.

   Примечание:
   - ❏ *Если количество импортированных пользовательских настроек превышает допустимое количество настроек, которое можно импортировать, появится сообщение с предложением удалить некоторые пользовательские настройки. Удалите все лишние пользовательские настройки перед импортом.*
   - ❏ *Выберите пользовательские настройки, которые необходимо удалить перед импортом, затем нажмите **Удалить**.*
9. Нажмите **Импорт**.

   Пользовательские настройки будут импортированы в шаблон конфигурации.

Импорт данных с LDAP-сервера.

1. Выберите **Настройки администратора** > **Настройки аутентиф-ции** > **Настройки пользователя** из шаблона конфигурации.

2. Нажмите **Импорт**.

3. Выберите **LDAP** в **Источник импорта**.

4. Нажмите **Настройки**.

   Отобразятся настройки **Сервер LDAP**.

   Примечание:
   Эти настройки LDAP-сервера используются для импорта пользовательских настроек с LDAP-сервера. Импортированные (скопированные) пользовательские настройки применяются для аутентификации пользователей при работе со сканером.

   *Если же вы выбираете **LDAP** или **Локальная БД и LDAP** в качестве метода аутентификации, пользователи проходят авторизацию через LDAP-сервер.*

5. Настройте каждый элемент.

   Выполняя импорт пользовательских настроек с LDAP-сервера, вы также можете задать следующие настройки в дополнение к настройкам LDAP.

   Информацию о других элементах см. в разделе «Сопутствующая информация».

Элемент			Описание
Настройки LDAP-сервера	Тип LDAP-сервера		Позволяет выбрать тип LDAP-сервера.
Настройки поиска	Фильтр поиска		Можно задать текст, используемый для фильтрации результатов поиска LDAP. Выберите **Настройка**, чтобы изменить текст поискового запроса.
	Настройки	Тип	Для функции **Сканировать в мою папку** можно установить тип места сохранения.
		Режим соединения	Если для параметра **Тип** установлено значение **FTP**, можно задать режим подключения к FTP.
		Номер порта	Если для параметра **Тип** установлено значение **FTP**, можно также указать нужный номер порта.

6. При необходимости выполните проверку соединения, нажав кнопку **Тест соединения**.

   Получает и отображает 10 пользовательских настроек с LDAP-сервера.

7. Нажмите **OK**.

8. Выберите способ импорта.

   ❏ Перезаписать или добавить: если уже существует такой же идентификатор пользователя, данные перезаписываются, иначе добавляется новый идентификатор.

   ❏ Заменить все: заменяет все на пользовательские настройки, которые вы хотите импортировать.

9. Нажмите **Импорт**.

   Откроется экран подтверждения настроек.

10. Нажмите **OK**.

    Отображается результат подтверждения.

11. Нажмите **Импорт**.

    Пользовательские настройки будут импортированы в шаблон конфигурации.

Соответствующая информация

➡ «Настройка LDAP-сервера» на стр. 152
➡ «Настройка параметров поиска LDAP-сервера» на стр. 154

Синхронизация с Сервер LDAP

Настройте параметр Сервер LDAP для сканера.

Задайте необходимые настройки для основного и дополнительного серверов.

Примечание:
*Настройки **Сервер LDAP** также используются функцией **Контакты**.*

Доступные службы

Поддерживаются следующие службы каталогов.

Название службы	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

Настройка LDAP-сервера

Для использования LDAP-сервера его необходимо настроить.

При выполнении настройки с помощью Web Config:

Выберите вкладку **Сеть** > **Сервер LDAP** > **Основные (Основной сервер)** или **Основные (Дополнительный сервер)**.

Если для параметра **Метод аутентификации** выбрано значение **Аутентификация Kerberos**, выберите **Сеть** > **Настройки Kerberos**, чтобы задать настройки Kerberos.

При выполнении настройки с помощью Epson Device Admin:

В шаблоне конфигурации выберите **Сеть** > **Сервер LDAP** > **Настройки сервера (Основной сервер)** или **Настройки сервера (Дополнительный сервер)**.

Если для параметра **Метод аутентификации** выбрано значение **Аутентификация Kerberos**, выберите **Сеть — Безопасность** > **Настройки Kerberos**, чтобы задать настройки Kerberos.

Элемент	Настройки и их описание
Использование сервера LDAP	Выберите **Использовать** или **Не использовать**.
Адрес сервера LDAP	Введите адрес LDAP-сервера. Введите от 1 до 255 символов в формате IPv4, IPv6 или полного доменного имени (FQDN). Для формата FQDN можно использовать буквенно-цифровые символы ASCII (с кодами от 0x20 до 0x7E) и знаки дефиса (за исключением начала и конца адреса).
Номер порта сервера LDAP (Номер порта)	Введите номер порта LDAP-сервера в диапазоне от 1 до 65535.
Безопасное подключение	Укажите метод аутентификации для доступа сканера к LDAP-серверу.
Проверка подлинности сертификатов	При включении этого параметра проверяется сертификат LDAP-сервера. Рекомендуем установить для этого параметра значение **Включить**. Для такой настройки на сканер должен быть импортирован **Сертификат ЦС**.
Таймаут поиска (с.)	Задайте продолжительность поиска до возникновения тайм-аута (от 5 до 300 секунд).
Метод аутентификации	Выберите метод аутентификации. Если выбран вариант **Аутентификация Kerberos**, предварительно задайте настройки Kerberos. Для использования Аутентификация Kerberos требуется следующая среда. ❏ Сканер и DNS-сервер могут связываться друг с другом. ❏ Значения времени сканера, сервера KDC и сервера, необходимого для аутентификации (LDAP-сервера, SMTP-сервера, файлового сервера), синхронизируются. ❏ Если сервер службы назначен через IP-адрес, полное доменное имя (FQDN) сервера службы регистрируется в зоне обратного просмотра DNS-сервера.
Область Kerberos для использования	При выборе значения **Аутентификация Kerberos** для параметра **Метод аутентификации** выберите область Kerberos, которую следует использовать.
Доменное имя администратора / Имя пользователя	Введите имя пользователя для LDAP-сервера. Длина имени не должна превышать 128 символов Юникода (UTF-8). Нельзя использовать управляющие символы, например символы с кодами от 0x00 до 0x1F и код 0x7F. Если для параметра **Метод аутентификации** выбрано значение **Анонимная аутентификация**, этот параметр не используется. Если не нужно указывать это значение, оставьте поле пустым.
Пароль	Введите пароль для проверки подлинности на LDAP-сервере — не более 128 символов в кодировке Юникод (UTF-8). Нельзя использовать управляющие символы, например символы с кодами от 0x00 до 0x1F и код 0x7F. Если для параметра **Метод аутентификации** выбрано значение **Анонимная аутентификация**, этот параметр не используется. Если не нужно указывать это значение, оставьте поле пустым.

Настройки Kerberos

Если в качестве **Метод аутентификации** выбран вариант **Аутентификация Kerberos**, необходимо задать настройки Kerberos. Допускается регистрация до 10 настроек Kerberos.

При выполнении настройки с помощью Web Config:

Выберите вкладку **Сеть** > **Настройки Kerberos**.

При выполнении настройки с помощью Epson Device Admin:

Выберите **Сеть** > **Безопасность** > **Настройки Kerberos** из шаблона конфигурации.

Элемент	Настройки и их описание
Область (домен)	Введите область проверки подлинности Kerberos длиной не более 255 символов ASCII (от 0x20 до 0x7E). Если регистрация этого параметра не требуется, оставьте его пустым.
Адрес KDC	Введите адрес сервера аутентификации Kerberos. Введите не более 255 символов в формате IPv4, IPv6 или полного доменного имени. Если регистрация этого параметра не требуется, оставьте его пустым.
Номер порта (Kerberos)	Введите номер порта сервера Kerberos в диапазоне от 1 до 65535.

Настройка параметров поиска LDAP-сервера

Здесь задаются атрибуты поиска для пользовательских настроек.

При выполнении настройки с помощью Web Config:

Выберите вкладку **Сеть** > **Сервер LDAP** > **Настройки поиска (Аутентификация)**.

При выполнении настройки с помощью Epson Device Admin:

В шаблоне конфигурации выберите **Настройки администратора** > **Настройки аутентиф-ции** > **Сервер LDAP** > **Параметры поиска (Аутентификация)**.

Элемент	Настройки и их описание
Поиск в базе (Уникальное имя)	Укажите начальную позицию для поиска информации о пользователе на LDAP-сервере. Введите от 0 до 128 символов в кодировке Юникод (UTF-8). Если не требуется поиск произвольного атрибута, оставьте это поле пустым. Пример для каталога локального сервера: dc=server,dc=local
Атрибут идентификатора пользователя	Укажите имя атрибута для отображения при поиске идентификационного номера. Введите от 1 до 255 символов в кодировке ASCII. Первым символом должен быть символ в диапазоне от a до z или от A до Z. Пример: cn, uid
Атрибут просмотра имени пользователя	Укажите имя атрибута для отображения в качестве имени пользователя. Введите от 0 до 255 символов в кодировке ASCII. Первым символом должен быть символ в диапазоне от a до z или от A до Z. Это поле можно оставить пустым. Пример: cn, name
Атрибут идентификатора карты аутентификации	Укажите имя атрибута для отображения в качестве идентификатора карты аутентификации. Введите от 0 до 255 символов в кодировке ASCII. Первым символом должен быть символ в диапазоне от a до z или от A до Z. Это поле можно оставить пустым. Пример: cn, sn
Атрибут идентификатора	Укажите имя атрибута для отображения при поиске идентификационного номера. Введите от 1 до 255 символов в кодировке ASCII. Первым символом должен быть символ в диапазоне от a до z или от A до Z. Пример: cn, id

Элемент	Настройки и их описание
Атрибут отдела	Укажите имя атрибута для отображения в качестве названия отдела. Введите от 0 до 255 символов в кодировке ASCII. Первым символом должен быть символ в диапазоне от a до z или от A до Z. Это поле можно оставить пустым. Пример: ou, ou-cl
Атрибут адреса электронной почты	Укажите имя атрибута для отображения при поиске адреса электронной почты. Введите от 1 до 255 символов в кодировке ASCII. Первым символом должен быть символ в диапазоне от a до z или от A до Z. Пример: mail
Атрибут "Сохранить в"	Укажите имя атрибута, указывающего место сохранения для функции Сканировать в мою папку. Введите от 0 до 255 символов в кодировке ASCII. Пример: homeDirectory

Проверка соединения с LDAP-сервером

Проверка подключения к LDAP-серверу с использованием параметров, установленных в меню **Сервер LDAP** > **Параметры поиска**.

1. Войдите в Web Config и выберите вкладку **Сеть** > **Сервер LDAP** > **Проверка подключения**.
2. Выберите **Пуск**.

   Проверка соединения началась. После завершения проверки отобразится отчет о проверке.

Пояснения сообщений, отображаемых при проверке соединения с LDAP-сервером

Сообщения	Описание
Проверка подключения прошла успешно.	Это сообщение отображается, когда соединение с сервером установлено.
Сбой проверки подключения. Проверьте настройки.	Это сообщение отображается по следующим причинам. ❏ Адрес или номер порта LDAP-сервера неверен. ❏ Истекло время ожидания. ❏ Значение **Не использовать** задано для параметра **Использование сервера LDAP**. ❏ Если значение **Аутентификация Kerberos** задано для параметра **Метод аутентификации**, такие параметры, как **Область (домен)**, **Адрес KDC** и **Номер порта (Kerberos)**, неверны.
Сбой проверки подключения. Проверьте дата и время на устройстве или сервере.	Это сообщение отображается, когда не удается установить соединение, потому что параметры времени для сканера и LDAP-сервера не совпадают.
Ошибка аутентификации. Проверьте настройки.	Это сообщение отображается по следующим причинам. ❏ Параметры **Имя пользователя** и **Пароль** неверны. ❏ Если значение **Аутентификация Kerberos** задано для параметра **Метод аутентификации**, дату и время будет невозможно изменить.

Сообщения	Описание
Доступ к устройству невозможен до завершения обработки.	Это сообщение отображается, если сканер занят.

Настройка почтового сервера

При использовании функции **Скан. в Мою эл. почту** необходимо настроить почтовый сервер.

Примечание:
*Включить параметр **Скан. в Мою эл. почту** можно, только если включена функция **Сканирование в электронную почту**.*

При выполнении настройки с помощью Web Config:

Выберите вкладку **Сеть** > **Сервер эл. почты** > **Основные**.

При выполнении настройки с помощью Epson Device Admin:

Выберите **Общий** > **Сервер эл. почты** > **Настройки почтового сервера** из шаблона конфигурации.

Элемент	Настройки и их описание	
Метод аутентификации	Укажите метод аутентификации для доступа сканера к почтовому серверу.	
	Выкл	При обмене данными с почтовым сервером аутентификация отключена.
	АУТЕНТИФИКАЦИЯ SMTP	Почтовый сервер должен поддерживать аутентификацию по протоколу SMTP.
	POP до SMTP	При выборе этого элемента задайте настройки сервера POP3.
Проверенная учет. запись	Если вы выбрали вариант **АУТЕНТИФИКАЦИЯ SMTP** или **POP до SMTP** в качестве значения параметра **Метод аутентификации**, введите имя аутентифицированной учетной записи. Введите от 0 до 255 символов в кодировке ASCII (символы с кодами от 0x20 до 0x7E).	
Проверенный пароль	Если вы выбрали вариант **АУТЕНТИФИКАЦИЯ SMTP** или **POP до SMTP** в качестве значения параметра **Метод аутентификации**, введите пароль аутентификации. Введите от 0 до 20 символов в кодировке ASCII (символы с кодами от 0x20 до 0x7E).	
Адрес эл. почты отправителя	Введите адрес электронной почты отправителя. Введите от 0 до 255 символов в кодировке ASCII (символы с кодами от 0x20 до 0x7E), за исключением символов — : ( ) < > [ ] ; ¥. Точка (.) не может быть первым символом.	
Адрес сервера SMTP	Введите от 0 до 255 символов. Можно использовать буквы в диапазоне от A до Z и от a до z, цифры от 0 до 9 и символы . - . Используйте формат IPv4 или FQDN.	
Номер порта сервера SMTP	Введите число от 1 до 65535.	

Элемент	Настройки и их описание	
Безопасное подключение	Укажите безопасный метод подключения к почтовому серверу.	
	Нет	Если выбрать **POP до SMTP** в поле **Метод аутентификации**, для метода подключения будет установлено значение **Нет**.
	SSL/TLS	Это доступно, если для параметра **Метод аутентификации** установлено значение **Выкл** или **АУТЕНТИФИКАЦИЯ SMTP**.
	STARTTLS	Это доступно, если для параметра **Метод аутентификации** установлено значение **Выкл** или **АУТЕНТИФИКАЦИЯ SMTP**.
Проверка подлинности сертификатов	При включении этого параметра проверяется сертификат. Рекомендуем установить для этого параметра значение **Включить**.	
Адрес сервера POP3	Если вы выбрали вариант **POP до SMTP** в качестве значения параметра **Метод аутентификации**, введите адрес сервера POP3. Введите от 0 до 255 символов. Можно использовать буквы в диапазоне от A до Z и от a до z, цифры от 0 до 9. Используйте формат IPv4 или FQDN.	
Номер порта сервера POP3	Если вы выбрали вариант **POP до SMTP** в качестве значения параметра **Метод аутентификации**, укажите номер порта. Введите число от 1 до 65535.	

Настройка функции Сканир. в Мою папку

Сохранение отсканированных изображений в папки, назначенные пользователям. Можно установить следующую специальную папку.

Примечание:
*Включить параметр **Сканировать в мою папку** можно, только если включена функция **Сканирование в сетевую папку/FTP**.*

Сохранение в настройки	Метод аутентификации	Расположение настройки «Путь к папке»
Укажите одну сетевую папку для всех Настройки аутентификации, чтобы в ней автоматически создавались личные подкаталоги с именами, соответствующими идентификаторам пользователей.	❏ Локальная БД ❏ LDAP ❏ Локальная БД и LDAP	Сканер (настройка Сканир. в Мою папку)
Назначить пользователям различные сетевые папки.	Локальная БД	Сканер (Пользовательские настройки)
	LDAP	Атрибуты LDAP
	Локальная БД и LDAP	Сканер (Пользовательские настройки) или атрибуты LDAP

При выполнении настройки с помощью Web Config:

Выберите вкладку **Безопасность устройства** > **Сканирование в сетевую папку/FTP**.

При выполнении настройки с помощью Epson Device Admin:

В шаблоне конфигурации выберите **Настройки администратора** > **Настройки аутентиф-ции** > **Сканирование в сетевую папку/FTP** > **Сканир. в Мою папку**.

Элемент		Описание
Настройка "Сохранить в"	Настройка типа	❏ **Общие**: Уровнем ниже папки или URL-адреса, указанных в параметре **Сохранить в**, автоматически создается подкаталог, имя которого соответствует идентификатору пользователя, и отсканированные изображения сохраняются в этом каталоге. ❏ **Индивидуально**: Установка папки для сохранения результатов сканирования для каждого пользователя. Пользователи Локальная БД могут быть заданы в пользовательских настройках. Для пользователей LDAP используется место хранения, полученное из атрибутов поиска LDAP-сервера.
	Тип	Выберите протокол передачи данных в соответствии с местом сохранения результатов сканирования. Для сетевой папки: **Сетевая папка (SMB)** Для FTP-сервера: **FTP**
	Сохранить в	Укажите путь или URL-адрес папки для сохранения результатов. Введите не более 160 символов в кодировке Unicode (UTF-16).
	Режим подключения	Задайте этот параметр, если для параметра **Тип** выбрано значение **FTP**. Выберите режим подключения к FTP-серверу.
	Номер порта	Задайте этот параметр, если для параметра **Тип** выбрано значение **FTP**. Укажите номер порта в диапазоне от 0 до 65535 для отправки результатов сканирования на FTP-сервер.

Элемент		Описание
Настройки аутентификации	Настройка типа	Задайте этот параметр, если вы установили значение **Индивидуально** для параметра **Настройка типа** в разделе **Настройка "Сохранить в"**. Задайте значения Имя пользователя и Пароль для доступа к папке. ❏ **Общие**: Используйте общие значения **Имя пользователя** и **Пароль** для всех пользователей. ❏ **Индивидуально**: Для пользователей Локальная БД индивидуально задайте значения **Имя пользователя** и **Пароль** в разделе **Параметры пользователя**. Пользователи LDAP не могут быть настроены индивидуально. Значения **Имя пользователя** и **Пароль**, установленные с помощью этого параметра, используются в групповом режиме.
	Имя пользователя	Укажите имя пользователя для доступа к папке, используемой для сохранения результатов сканирования. Введите не более 30 символов в кодировке Unicode (UTF-16). Задайте этот параметр, если вы используете вариант **Общие** или LDAP-сервер.
	Пароль	Введите пароль, соответствующий имени пользователя **Имя пользователя**. Введите не более 20 символов в кодировке Unicode (UTF-16). Задайте этот параметр, если вы используете вариант **Общие** или LDAP-сервер.

Запрет изменения целевой папки для функции Сканирование в сетевую папку/FTP

Элемент	Описание
Запретить ручной ввод адреса	Если параметр включен, пользователь не может изменить целевую папку по умолчанию.

Настройка функций One-touch (Одно касание)

Можно вывести только необходимые значки, отредактировав конфигурацию значков, отображающихся на главном экране панели управления.

При выполнении настройки с помощью Web Config:

Выберите вкладку **Безопасность устройства** > **Настройка функций One-touch (Одно касание)**.

При выполнении настройки с помощью Epson Device Admin:

Выберите **Настройки администратора** > **Настройки аутентиф-ции** > **Настройка функций One-touch (Одно касание)** из шаблона конфигурации.

Примечание:
В перечисленных ниже случаях значки указанных функций не отображаются на главном экране.

❏ *Если выбраны функции, не разрешенные из-за наличия **Ограничения**.*

❏ *Если адрес электронной почты выполнившего вход пользователя не зарегистрирован. (Скан. в Мою эл. почту)*

❏ *Если не указана целевая папка. (Сканир. в Мою папку)*

Элемент	Описание
Максимальное число функций на экране	Выбор конфигурации значков, отображаемых на панели управления. Изображение изменится в соответствии с выбранной конфигурацией.
Экран(ы)	Выбор количества страниц.
Число	Выбор функций, которые необходимо отобразить для каждой пронумерованной позиции.

Создание отчетов История заданий с помощью ПО Epson Device Admin

С помощью Epson Device Admin можно создать отчет История заданий по каждому пользователю или каждой группе пользователей. В сканере можно сохранить до 3000 экземпляров истории использования устройства. Для создания отчета можно указать период или настроить расписание.

Чтобы вывести История заданий в форме отчета, в меню-ленте на экране «Список устройств» выберите **Настройки** > **Настройки Epson Print Admin Serverless/Аутентификация** > **Управление совместимыми с Epson Print Admin Serverless/Аутентификация устройствами**.

Подробнее о создании отчета о пользователях см. в документации по Epson Device Admin.

Элементы, которые можно включить в отчет

В отчет о пользователях можно включить следующие данные.

Дата/Идентификатор задания/Операция/Идентификатор пользователя/Отдел/Результат/Сведения о результате/Сканирование: тип получателя/Сканирование: получатель/Сканирование: Размер бумаги/Сканирование: 2-сторонняя/Сканирование: Цветной/Сканирование: Страниц/Устройства: Модель/Устройства: IP-адрес/Устройства: Серийный номер/Устройства: Отдел/Устройства: Расположение/Устройства: Заметка/Устройства: Примечание

Вход в качестве администратора с панели управления

Для входа в качестве администратора с панели управления сканера можно использовать следующие методы.

1. Нажмите значок  в правой верхней части экрана.
   - ❏ Если функция Настройки аутентификации включена, этот значок отображается на экране **Добро пожаловать** (экране ожидания авторизации).
   - ❏ Если функция Настройки аутентификации отключена, значок отображается на главном экране.
2. На экране подтверждения нажмите **Да**.

3. Введите пароль администратора.

   Отобразится сообщение о завершении процедуры входа, после чего на панели управления отобразится главный экран.

Чтобы выполнить выход, нажмите значок в правой верхней части главного экрана.

Отключение Настройки аутентификации.

Можно отключить Настройки аутентификации с помощью Web Config.

Примечание:
Пользовательские настройки, зарегистрированные на сканере, сохранятся, даже если отключены Настройки аутентификации. Их можно удалить, восстановив настройки сканера по умолчанию.

1. Откройте Web Config.
2. Выберите вкладку **Безопасность устройства** > **Основные** > **Аутентификация**.
3. Выберите **Выкл.**.
4. Нажмите **Следующий**.
5. Нажмите **ОК**.

Примечание:
Даже при отключении Настройки аутентификации функция Функция блокировки остается включенной. Если вы хотите отключить ее, вы можете сделать соответствующие настройки с панели управления или из приложения Web Config.

Соответствующая информация

➡ «Настройка функции Функция блокировки с панели управления» на стр. 91
➡ «Настройка функции Функция блокировки с помощью Web Config» на стр. 91

Удаление информации об Настройки аутентификации (Восст. настр. по ум.)

Чтобы удалить все данные Настройки аутентификации (Картридер, Метод аутентификации, Пользовательские настройки и пр.), восстановите все настройки сканера до значений по умолчанию на момент покупки.

На панели управления выберите **Настр.** > **Администрир. системы** > **Восст. настр. по ум.** > **Все настройки**.

Важно:
Все контакты и другие сетевые настройки также будут удалены. Удаленные настройки восстановить нельзя.

Решение проблем

Не удается прочитать аутентификационную карту

Проверьте, выполняются ли следующие условия.

❏ Убедитесь, что устройство аутентификации правильно подключено к сканеру.

Подключите устройство аутентификации к USB-порту для подключения внешнего интерфейса, расположенному на задней панели сканера.

❏ Убедитесь, что устройство аутентификации и карта аутентификации поддерживаются.

Обслуживание

Очистка внешних частей сканера

Удалите все загрязнения с внутренней поверхности корпуса с помощью сухой ткани или ткани, смоченной мягким чистящим средством и водой.

Важно:

- ❏ *Никогда не очищайте сканер спиртом, разбавителем или любыми едкими растворителями. В противном случае может произойти деформирование или изменение цвета поверхности устройства.*
- ❏ *Не допускайте попадания воды внутрь устройства. Это может привести к неисправности.*
- ❏ *Никогда не вскрывайте корпус сканера.*

1. Нажмите кнопку ⏻, чтобы выключить сканер.
2. Отсоедините от сканера адаптер переменного тока.
3. Протрите внешнюю поверхность сканера тканью, смоченной мягким моющим средством и водой.

   Примечание:
   Протрите сенсорный экран мягкой сухой тканью.

Очистка внутренних областей сканера

После определенного периода использования сканера бумажная и комнатная пыль, оседающая на роликах или стекле внутри сканера, может привести к ухудшению качества сканирования и к проблемам подачи бумаги. Очистку внутренности сканера следует выполнять через каждые 5,000 сканирований.

Узнать количество выполненных сканирований можно на панели управления или в программе Epson Scan 2 Utility.

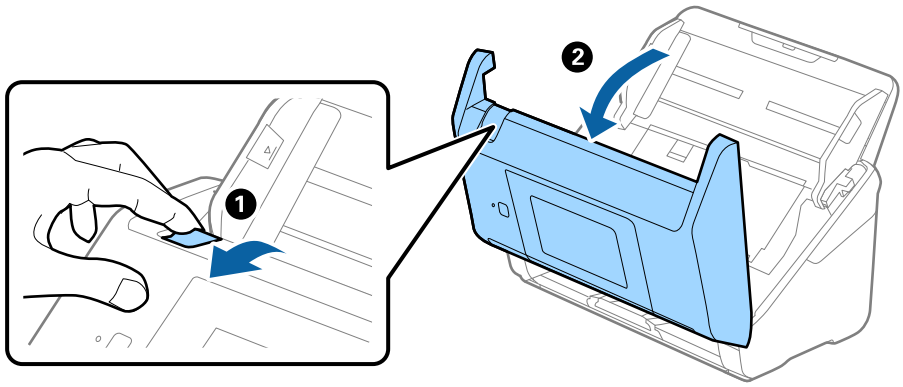
Если на поверхности имеются трудноудаляемые загрязнения, воспользуйтесь оригинальным чистящим набором Epson. Для удаления пятен нанесите небольшое количество очистителя на чистящую салфетку.

Важно:

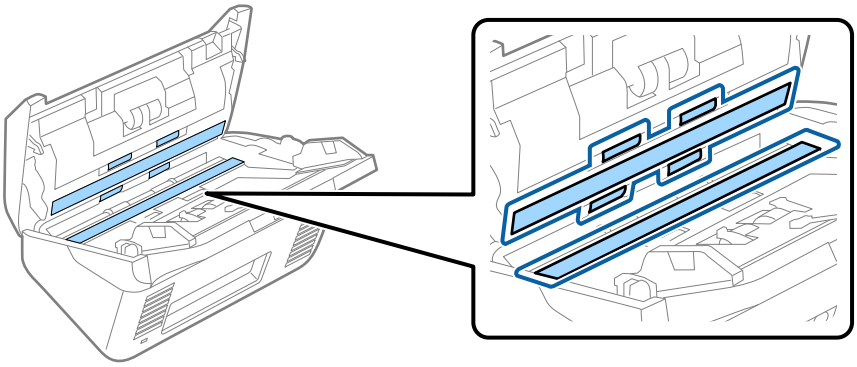
- ❏ *Никогда не очищайте сканер спиртом, разбавителем или любыми едкими растворителями. В противном случае может произойти деформирование или изменение цвета поверхности устройства.*
- ❏ *Никогда не распыляйте жидкости или смазывающие вещества над сканером. В противном случае возможно неправильное функционирование сканера вследствие повреждения оборудования или электрических цепей.*
- ❏ *Никогда не вскрывайте корпус сканера.*

1. Нажмите кнопку ⏻, чтобы выключить сканер.
2. Отсоедините от сканера адаптер переменного тока.

3. Потяните за рычаг и откройте крышку сканера.



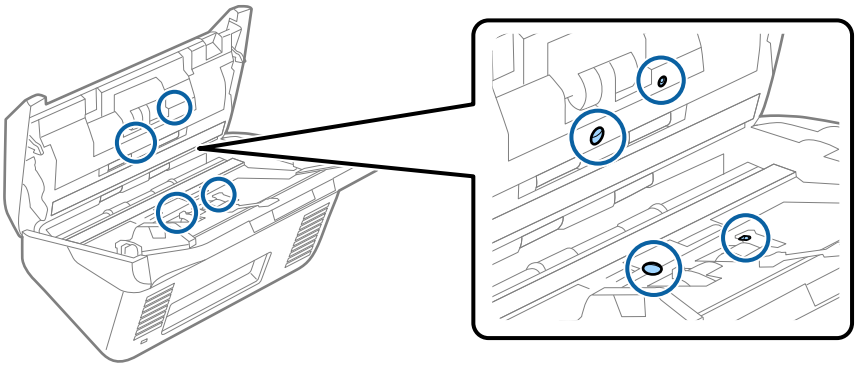
4. Удалите пятна на пластиковом ролике и на нижней поверхности стекла внутри крышки сканера с помощью мягкой ткани или оригинального комплекта для очистки Epson.



Важно:

- ❏ *При очистке поверхности стекла не прикладывайте больших усилий.*
- ❏ *Не пользуйтесь щеткой или твердыми инструментами. Царапины на стекле могут ухудшить качество сканирования.*
- ❏ *Не распыляйте чистящее средство непосредственно на поверхность стекла.*

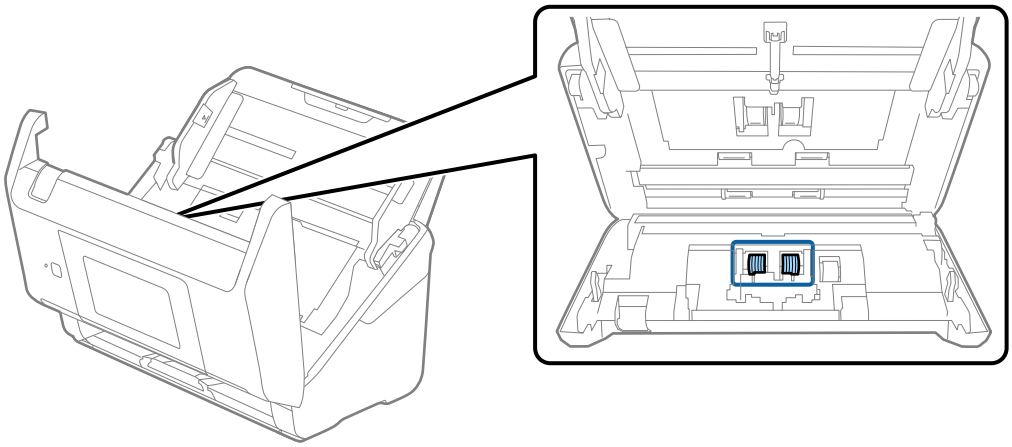
5. Загрязнения на датчиках следует удалять ватной палочкой.



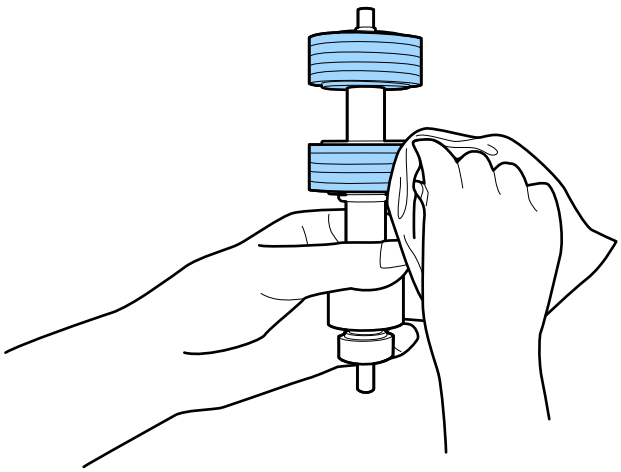
> ***Важно:***
>
> *Не смачивайте при этом ватную палочку (например, чистящим средством).*

6. Откройте крышку сканера и извлеките ролик разделения.

   Для получения дополнительной информации см. раздел «Замена узла роликов».



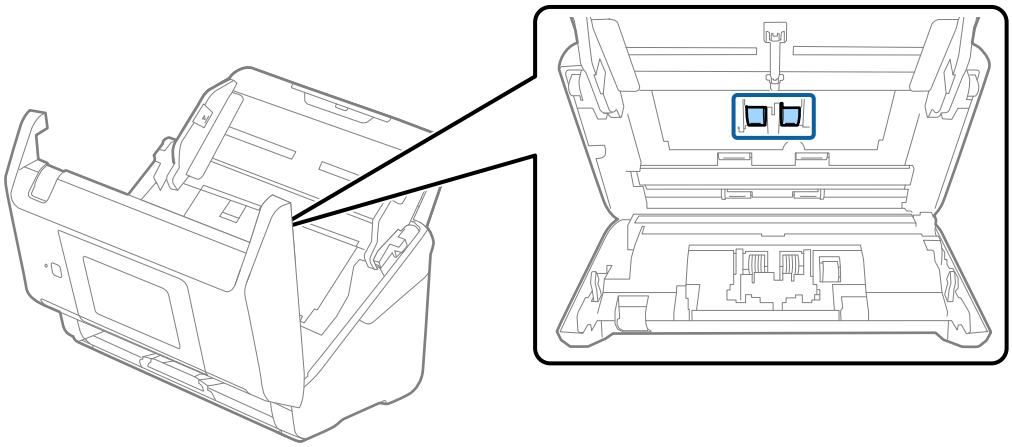
7. Удалите пыль и грязь с ролика разделения с помощью оригинального чистящего набора Epson или мягкой увлажненной ткани.



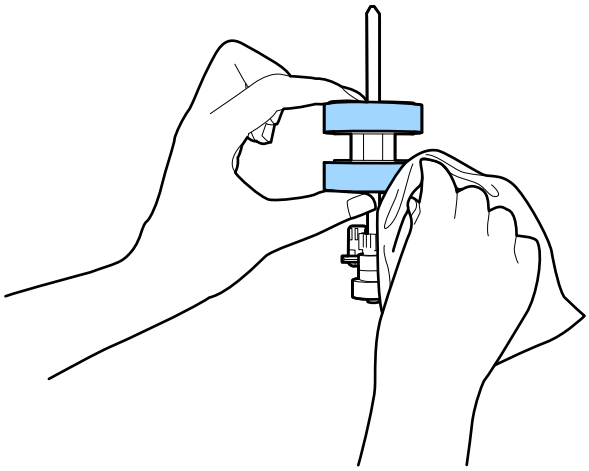
> ***Важно:***
>
> *Для очистки ролика используйте только оригинальный чистящий набор Epson или мягкую увлажненную ткань. Сухая ткань может повредить поверхность ролика.*

8. Откройте крышку сканера и извлеките приемный ролик.

   Для получения дополнительной информации см. раздел «Замена узла роликов».



9. Удалите пыль и грязь с приемного ролика с помощью оригинального чистящего набора Epson или мягкой увлажненной ткани.



> ***Важно:***
>
> *Для очистки ролика используйте только оригинальный чистящий набор Epson или мягкую увлажненную ткань. Сухая ткань может повредить поверхность ролика.*

10. Закройте крышку сканера.

11. Подключите адаптер переменного тока и включите сканер.

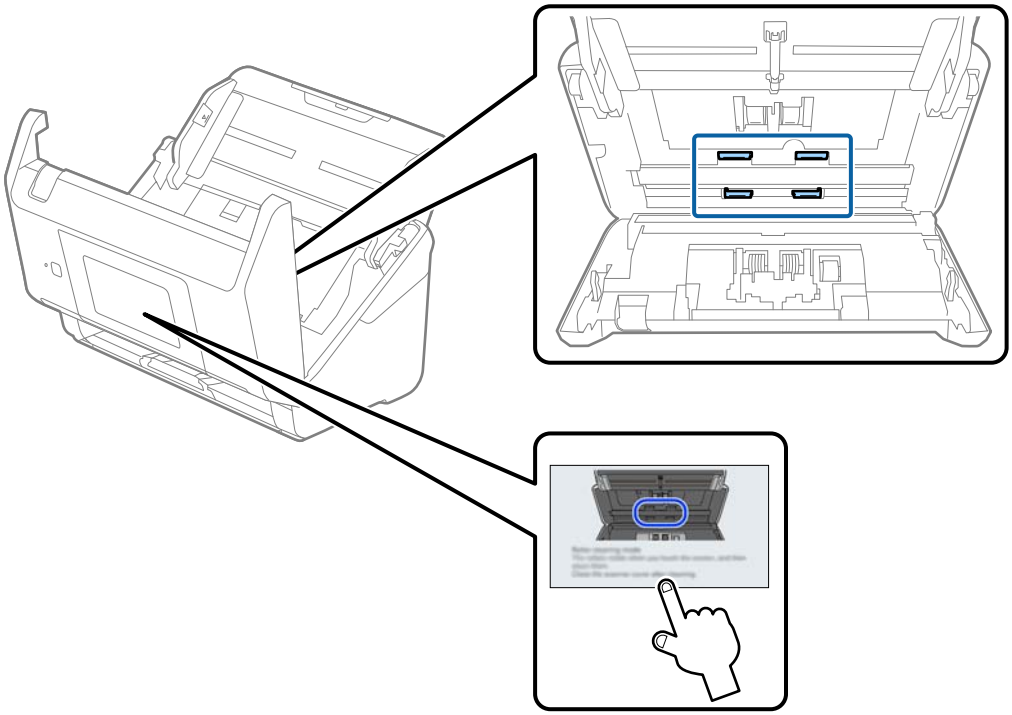
12. Выберите **Техобслуж. Сканера** на главном экране.

13. На экране **Техобслуж. Сканера** выберите **Чистка роликов**.

14. Потяните за рычаг, чтобы открыть крышку сканера.

    Сканер войдет в режим очистки роликов.

15. Медленно проворачивайте ролики внизу, нажимая в любом месте ЖК-дисплея. Протрите поверхность роликов с помощью оригинального чистящего набора Epson или мягкой ткани, смоченной водой. Повторяйте процедуру до тех пор, пока ролики не станут чистыми.



> ⚠ ***Предостережение:***
>
> *При работе с роликами следите за тем, чтобы руки или волосы не попали в механизм. Это может привести к травме.*

16. Закройте крышку сканера.

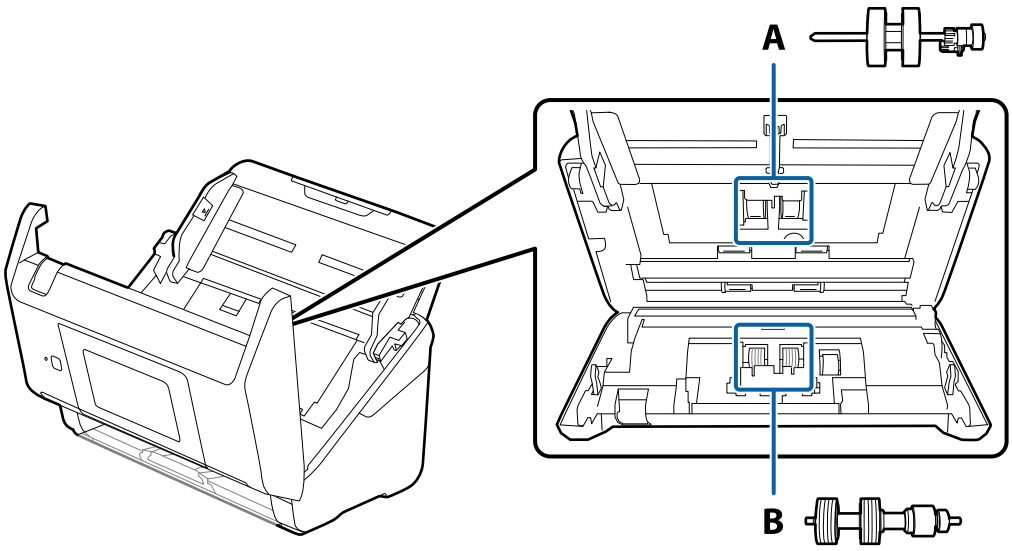
    Сканер выйдет из режима очистки роликов.

Соответствующая информация

➡ «Замена узла роликов» на стр. 169

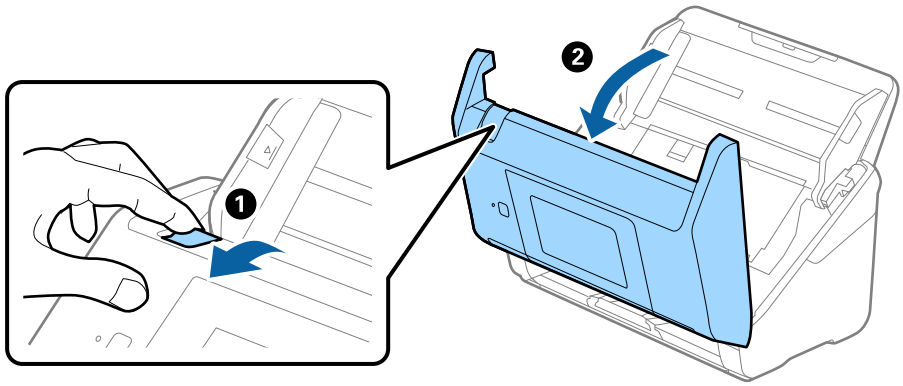
Замена узла роликов

Если количество выполненных сканирований превысит срок службы роликов, необходимо выполнить замену узла роликов (приемного ролика и ролика разделения). При появлении на экране компьютера или панели управления сообщения о необходимости замены выполните следующие действия.

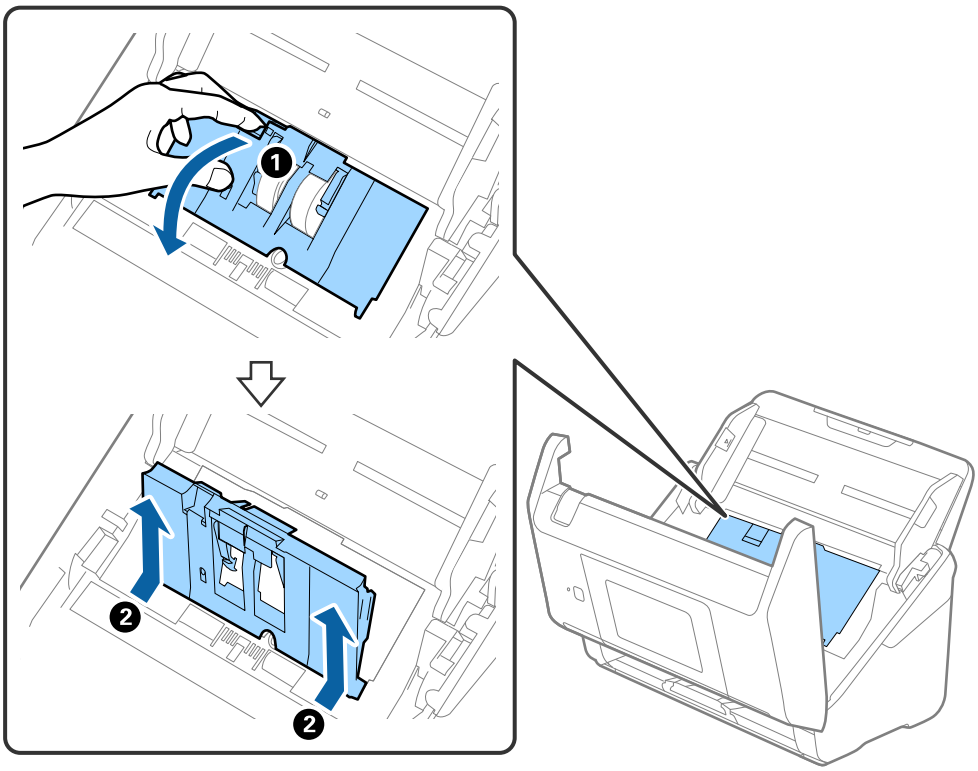


A: приемный ролик, B: ролик разделения

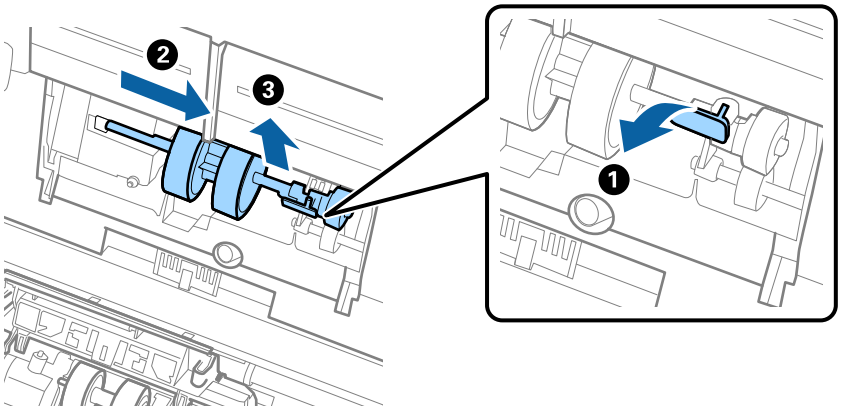
1. Нажмите кнопку ⏻, чтобы выключить сканер.
2. Отсоедините от сканера адаптер переменного тока.
3. Потяните за рычаг и откройте крышку сканера.



4. Откройте крышку приемного ролика захвата, сдвиньте и извлеките ее.

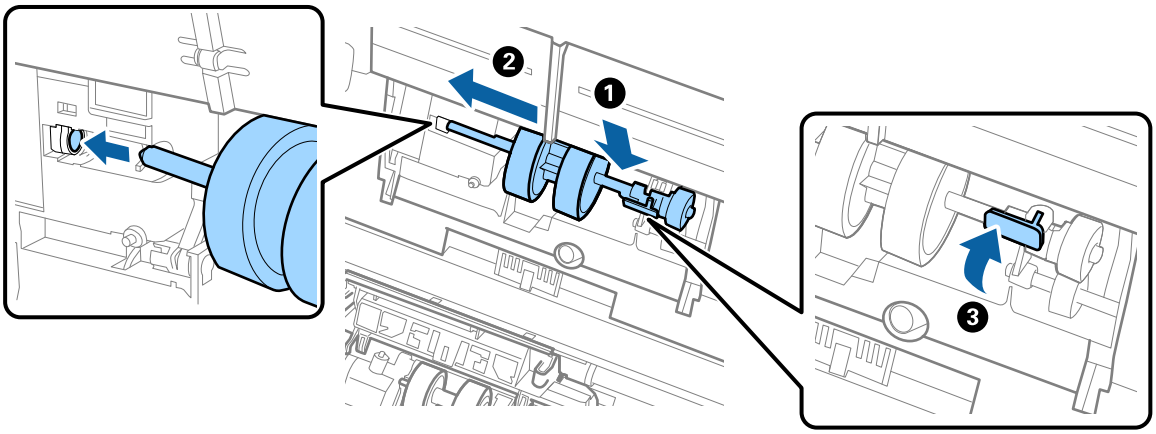


5. Нажмите на крепления оси ролика, сдвиньте и извлеките приемные ролики.

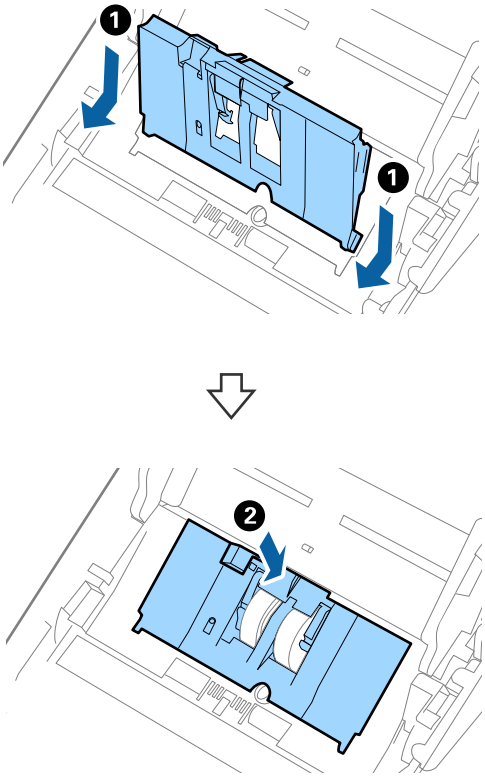


> ***Важно:***
>
> *Не прикладывайте больших усилий при извлечении приемного ролика. Это может привести к повреждению внутренних частей сканера.*

6. Удерживая крепление, сдвиньте новый приемный ролик влево и вставьте его в отверстие в сканере. Нажмите на крепление, чтобы зафиксировать его.

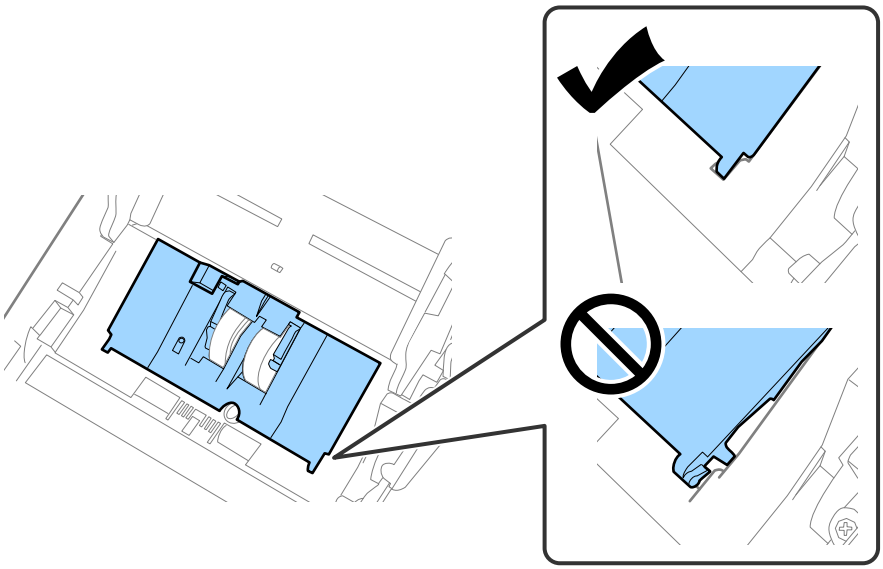


7. Вставьте край крышки приемного ролика в канавку и вдвиньте крышку. Плотно закройте крышку.

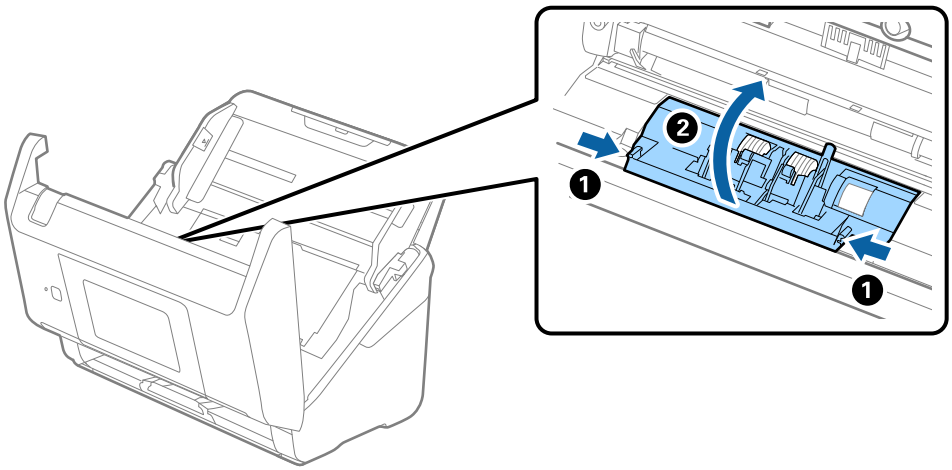


Важно:

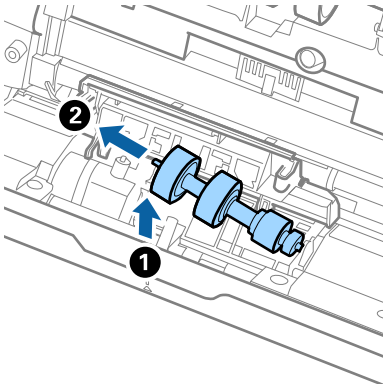
- ❏ *Убедитесь, что крышка захвата закрыта правильно.*
- ❏ *Если крышка закрывается с трудом, проверьте правильность установки приемных роликов бумаги.*
- ❏ *Не устанавливайте крышку, если ролики приподняты.*



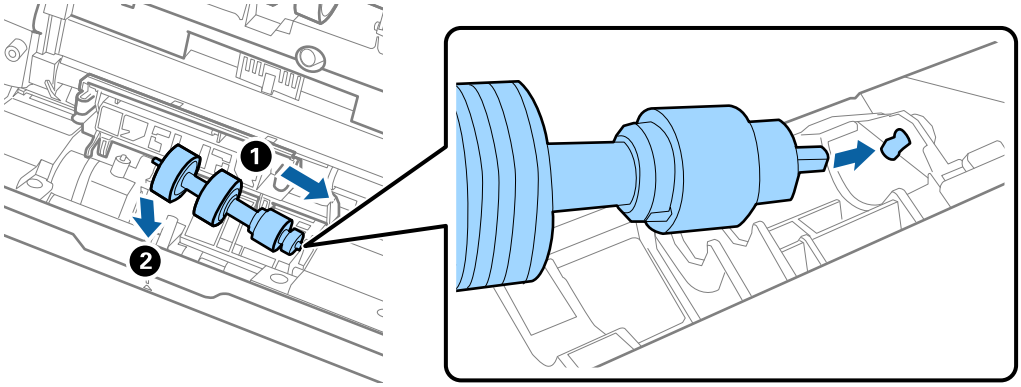
8. Нажмите на защелки по обеим сторонам крышки ролика разделения, чтобы открыть крышку.



9. Приподнимите левую сторону ролика разделения, затем сдвиньте и извлеките их.



10. Вставьте ось нового ролика разделения в отверстие на правой стороне и опустите ролик.



11. Закройте крышку ролика разделения.

> ***Важно:***
>
> *Если крышка закрывается с трудом, убедитесь, что ролики разделения установлены правильно.*

12. Закройте крышку сканера.

13. Подключите адаптер переменного тока и включите сканер.

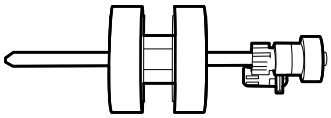
14. Выполните сброс количества сканирований на панели управления.

Примечание:
Утилизацию ролика разделения и приемного ролика следует производить в соответствии с местными нормами. Не разбирайте эти компоненты.

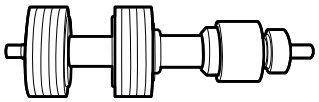
Коды узла роликов

Когда количество сканирований превысит установленное значение, необходимо заменить ролики (приемный ролик и ролик разделения). Узнать количество выполненных сканирований можно на панели управления или в программе Epson Scan 2 Utility.

A



B



A: приемный ролик, B: ролик разделения

Наименование детали	Коды	Срок службы
Узел роликов	B12B819671 B12B819681 (только для Индии)	200,000*

* Это количество было определено с использованием тестовых оригиналов Epson и является значением, определяющим периодичность замены деталей. Периодичность замены может варьироваться в зависимости от типа бумаги: например, при работе с бумагой, создающей много пыли, либо с бумагой с грубой поверхностью необходимость замены деталей может возникнуть раньше.

Сброс количества сканирований

Сбрасывает число сканирований, выполненных после замены узла роликов.

1. Выберите на начальном экране пункт **Настр.** > **Информация об устройстве** > **Сброс числа копий** > **Число копий после замены рол.**.
2. Нажмите **Да**.

Соответствующая информация

➡ «Замена узла роликов» на стр. 169

Экономия электроэнергии

Когда сканер не выполняет никаких операций, можно использовать спящий режим или режим автоматического выключения для экономии электроэнергии. Можно задать период времени, по истечении которого сканер будет переходить в спящий режим и автоматически отключаться. Любое увеличение этого значения повлияет на энергопотребление данного устройства. При внесении каких-либо изменений учитывайте их влияние на окружающую среду.

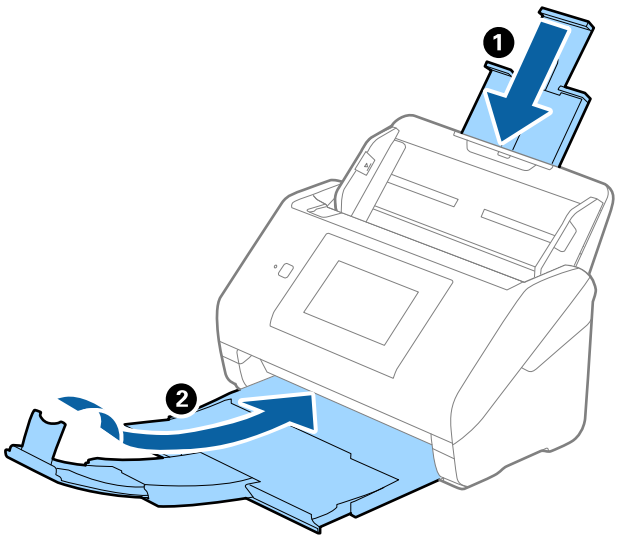
1. Выберите **Настр.** на главном экране.
2. Выберите **Основ. настройки**.
3. Выберите **Настройки выкл.** и задайте настройки.

   Примечание:
   Доступные функции могут различаться в зависимости от места покупки.

Транспортировка сканера

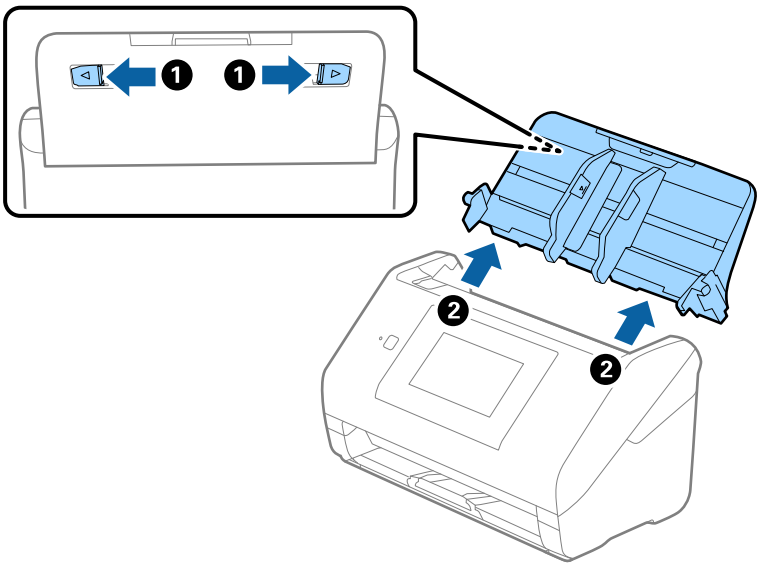
Если необходимо перевезти сканер в другое место или отправить его в ремонт, выполните приведенные ниже действия для его упаковки.

1. Нажмите кнопку ⏻, чтобы выключить сканер.
2. Отключите адаптер переменного тока.
3. Извлеките кабели и устройства.
4. Закройте удлинитель подающего лотка и выходной лоток.



> ***Важно:***
> *Выходной лоток должен быть надежно закрыт, в противном случае он может быть поврежден в процессе транспортировки.*

5. Снимите подающий лоток.



6. Упакуйте сканер в оригинальный упаковочный материал и оригинальную или иную прочную коробку.

Резервное копирование настроек

Можно экспортировать установленное значение параметра из Web Config в файл.Это можно использовать для резервного копирования контактов, установки значений, замены сканера и т. д.

Файл экспортируется как двоичный, поэтому его нельзя будет изменить.

Экспорт настроек

Экспортируйте параметры для сканера.

1. Войдите в Web Config и выберите вкладку **Управление устройствами** > **Значение настройки экспорта и импорта** > **Экспорт**.

2. Выберите настройки, которые необходимо экспортировать.

   Выберите настройки для экспорта.Если выбрать родительскую категорию, также будут выбраны все подкатегории.Однако для выбора становятся недоступными те подкатегории, которые приводят к ошибкам дупликации в рамках одной сети (например, дупликации IP-адресов и т. д.).

3. Введите пароль для шифрования экспортированного файла.

   Для импорта файла необходим пароль.Оставьте поле пароля пустым, если не требуется шифрование файла.

4. Нажмите **Экспорт**.

> ***Важно:***
> *Если необходимо экспортировать сетевые настройки сканера, например имя и IPv6-адрес устройства, выберите **Включите для выбора отдельных параметров устройства** и затем выберите дополнительные элементы.Используйте выбранные значения только для сканера на замену.*

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Импорт настроек

Импортируйте экспортированный файл Web Config на сканер.

> ***Важно:***
> *При импорте значений, содержащих индивидуальные сведения (например, имя или IP-адрес сканера), убедитесь, что в сети нет такого же IP-адреса.*

1. Войдите в Web Config и выберите вкладку **Управление устройствами** > **Значение настройки экспорта и импорта** > **Импорт**.
2. Выберите экспортированный файл и введите зашифрованный пароль.
3. Нажмите **Следующий**.
4. Выберите настройки, которые необходимо импортировать, затем нажмите **Следующий**.
5. Нажмите **ОК**.

Настройки будут применены на сканере.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Восст. настр. по ум.

На панели управления выберите **Настр.** > **Администрир. системы** > **Восст. настр. по ум.**, а затем выберите параметры, которые необходимо вернуть к значениям по умолчанию.

- ❏ Настройки сети: восстановление заводских значений сетевых настроек.
- ❏ Все, кроме Настройки сети: восстановление заводских значений всех настроек (кроме сетевых настроек).
- ❏ Все настройки: восстановление заводских значений всех настроек.

Важно:

*При выборе и выполнении **Все настройки** все зарегистрированные для сканера данные настроек, в том числе контакты и параметры пользователей аутентификации, будут удалены. Удаленные настройки восстановить нельзя.*

Обновление приложений и микропрограммного обеспечения

Обновление приложений и микропрограммного обеспечения позволяет устранить некоторые проблемы и улучшить или добавить функции. Следите за тем, чтобы всегда использовать самую новую версию приложений и микропрограммного обеспечения.

Важно:

❏ *Не отключайте компьютер или сканер во время обновления.*

Примечание:
*Если сканер может быть подключен к Интернету, можно обновить встроенное ПО принтера с помощью Web Config. Выберите вкладку **Управление устройствами** > **Обновление встроенной программы**, проверьте отображаемое сообщение, затем щелкните **Пуск**.*

1. Убедитесь, что сканер и компьютер подсоединены друг к другу, а компьютер подключен к Интернету.

2. Запустите EPSON Software Updater и обновите приложения или микропрограммное обеспечение.

   Примечание:
   Операционные системы семейства Windows Server не поддерживаются.

   ❏ Windows 10

   Нажмите кнопку «Пуск» и выберите **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   С помощью кнопки «Поиск» введите название приложения, после чего нажмите появившийся значок.

   ❏ Windows 7

   Щелкните кнопку «Пуск» и выберите **Все программы** или **Программы** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Выберите **Finder** > **Перейти** > **Приложения** > **Epson Software** > **EPSON Software Updater**.

Примечание:
Если приложение, которое необходимо обновить, невозможно найти в списке, значит, его невозможно обновить при помощи EPSON Software Updater. Проверьте наличие самых новых версий приложений на локальном веб-сайте Epson.

http://www.epson.com

Обновление встроенного программного обеспечения сканера с помощью панели управления

Если сканер может быть подключен к Интернету, можно обновить встроенное ПО сканера с помощью панели управления. Кроме того, сканер можно настроить на регулярную проверку наличия обновлений встроенного ПО и выдачу соответствующих оповещений.

1. Выберите **Настр.** на главном экране.

2. Выберите **Администрир. системы** > **Обновление встроенного ПО** > **Обновление**.

   Примечание:
   *Выберите **Уведомление** > **Вкл.**, чтобы настроить сканер на регулярную проверку доступных обновлений встроенного программного обеспечения.*

3. Просмотрите сообщение на экране и запустите поиск доступных обновлений.

4. Если на ЖК-экране отображается сообщение о наличии обновления встроенного ПО, следуйте инструкциям на экране, чтобы начать процедуру обновления.

   Важно:
   - ❏ *Не выключайте сканер и не отключайте его от сети до тех пор, пока не завершится обновление. В противном случае сканер может перестать работать.*
   - ❏ *Если обновление встроенного ПО не было завершено или было завершено с ошибкой, сканер не запустится в обычном режиме и при следующем его включении на ЖК-экране отобразится надпись Recovery Mode. В таком случае необходимо обновить встроенное ПО с помощью компьютера. Соедините сканер и компьютер с помощью USB-кабеля. Пока на сканере отображается надпись Recovery Mode, вы не сможете обновить встроенное ПО через сетевое соединение. Откройте на компьютере сайт Epson для вашего региона и загрузите последнюю версию встроенного ПО для сканера. Для обновления следуйте инструкциям на веб-сайте.*

Обновление микропрограммы с помощью Web Config

Если сканер может быть подключен к Интернету, можно обновить встроенное ПО принтера с помощью Web Config.

1. Войдите в Web Config и выберите вкладку **Управление устройствами** > **Обновление встроенной программы**.

2. Щелкните **Пуск** и следуйте инструкциям на экране.

   Запускается процесс подтверждения микропрограммы, после чего отображаются сведения о микропрограмме, если существует обновление для нее.

Примечание:
Можно также обновить микропрограмму с помощью Epson Device Admin. Можно визуально подтвердить сведения о микропрограмме в списке устройств. Это оказывается полезным, если необходимо обновить микропрограмму на нескольких устройствах. Дополнительные сведения можно найти в руководстве Epson Device Admin или в справке.

Соответствующая информация

➡ «Запуск Web Config в веб-браузере» на стр. 37

Обновление микропрограммы без подключения к Интернету

Можно загрузить микропрограмму устройства на компьютер с веб-сайта Epson, а затем подключить устройство и компьютер с помощью кабеля USB и обновить микропрограмму. Если вы не можете выполнить обновление через сеть, сделайте следующее.

Примечание:
Перед обновлением убедитесь, что драйвер сканера Epson Scan 2 установлен на вашем компьютере. Если приложение Epson Scan 2 не установлено, установите его.

1. На веб-сайте Epson можно узнать о последних выпусках обновлений микропрограммного обеспечения.

   http://www.epson.com

   ❏ Если для вашего сканера доступно микропрограммное обеспечение, загрузите его и перейдите к следующему шагу.

   ❏ Если на сайте нет информации о микропрограммном обеспечении, это значит, что вы уже используете последнюю версию микропрограммного обеспечения.

2. Через USB-кабель подключите к сканеру компьютер, на который загружено микропрограммное обеспечение.

3. Дважды щелкните загруженный исполняемый файл (EXE).

   Запустится Epson Firmware Updater.

4. Следуйте инструкциям на экране.