EPSON
EXCEED YOUR VISION

Руководство администратора

NPD5668-00 RU

Содержание

Содержание

Приложение.

Расширенные настройки безопасности для предприятия

Авторское право

Торговые марки

- ❏ EPSON® является зарегистрированным товарным знаком. EPSON EXCEED YOUR VISION и EXCEED YOUR VISION являются товарными знаками Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Уведомление: прочие названия продуктов упоминаются в документе только в целях идентификации и могут являться товарными знаками соответствующих владельцев. Компания Epson отрицает любые права на владение данными знаками.

Об этом руководстве

Маркировка и обозначения.

> ⚠ ***Предостережение:***
> *Инструкции, которые необходимо соблюдать во избежание травм.*

> ***Важно:***
> *Инструкции, которые необходимо соблюдать во избежание повреждения оборудования.*

Примечание:
Инструкции, содержащие полезные советы и ограничения по работе сканера.

Соответствующая информация

➡ Щелкните этот значок для получения дополнительной информации.

Описания, используемые в данном руководстве

❏ Снимки экранов драйвера сканера и Epson Scan 2 (драйвера сканера) относятся к системам Windows 10 или OS X El Capitan. Содержание, отображающееся на экранах, различается в зависимости от модели и ситуации.

❏ Иллюстрации, используемые в этом руководстве, приведены исключительно в качестве примеров. Несмотря на то, что могут существовать небольшие отличия между моделями, способы их эксплуатации совпадают.

❏ Некоторые из элементов меню на ЖК-экране отличаются в зависимости от модели и настроек.

Обозначение операционных систем

Windows

В данном руководстве такие термины, как Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2 и Windows Server 2003, используются по отношению к следующим операционным системам. Кроме того, термин Windows используется по отношению ко всем версиям.

❏ 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 Vista®

- ❏ Операционная система Microsoft® Windows® XP
- ❏ Операционная система Microsoft® Windows® XP Professional x64 Edition
- ❏ 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
- ❏ Операционная система Microsoft® Windows Server® 2008
- ❏ Операционная система Microsoft® Windows Server® 2003 R2
- ❏ Операционная система Microsoft® Windows Server® 2003

Mac OS

Кроме того, термин Mac OS используется по отношению к macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x и Mac OS X v10.6.8.

Введение

Руководство

Настоящее руководство предназначено для администратора устройств, который несет ответственность за подключение принтера или сканера к сети. Здесь содержатся сведения о том, как настроить использование соответствующих функций.

Изучите *Руководство пользователя*, чтобы получить сведения об использовании функций.

Подготовка

Здесь описываются административные задачи, инструкции по настройке устройств и программное обеспечение для управления.

Подключение

Здесь объясняется, как подключить устройство к сети или телефонной линии. Кроме того, здесь описывается сетевая среда, например использование порта для устройства, а также сведения о DNS-сервере и прокси-сервере.

Настройки функций

Здесь объясняются настройки для каждой функции на устройстве.

Базовые настройки безопасности

Здесь объясняются настройки каждой функции, например печати, сканирования и отправки факсов.

Настройки работы и управления

Здесь описываются действия, которые выполняются после начала использования устройства, например проверка сведений и обслуживание.

Решение проблем

Здесь объясняются настройки инициализации и устранения неисправностей в сети.

Расширенные настройки безопасности для предприятия

Здесь объясняется метод настройки для улучшения безопасности устройства, например использование сертификата ЦС, связи SSL/TLS и IPsec/фильтрации IP.

В зависимости от модели некоторые функции, указанные в этой главе, не поддерживаются.

Термины, используемые в данном руководстве

В данном руководстве используются следующие термины.

Введение

Администратор

Лицо, ответственное за установку и настройку устройства или сети в офисе или организации. В небольших организациях это лицо может нести ответственность за администрирование и устройств, и сети. В крупных организациях администраторы управляют сетью или устройствами в отделе или подразделении, а сетевые администраторы несут ответственность за настройки связи за пределами организации, например за выход в Интернет.

Сетевой администратор

Лицо, ответственное за управление сетевой связью. Лицо, которое настраивает маршрутизатор, прокси-сервер, DNS-сервер и почтовый сервер для управления связью через Интернет или сеть.

Пользователь

Лицо, которое использует такие устройства, как принтеры или сканеры.

Web Config (веб-страница устройства)

Веб-сервер, встроенный в устройство, называется Web Config. В нем с помощью браузера можно проверить состояние устройства.

Инструмент

Общий термин, связанный с программным обеспечением для настройки устройства и управления им, например Epson Device Admin, EpsonNet Config, EpsonNet SetupManager и т. д.

Сканирование с использованием технологии Push

Общий термин, обозначающий сканирование с панели управления устройства.

ASCII (Американский стандартный код для обмена информацией)

Одна из стандартных кодировок символов. Определено 128 символов, включая такие символы, как алфавит (a–z, A–Z), арабские цифры (0–9), обозначения, пустые символы и управляющие символы. При использовании термина ASCII в этом руководстве имеются в виду указанные ниже символы от 0x20 до 0x7E (в шестнадцатеричном формате), управляющие символы не учитываются.

SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* Обозначает пробел.

Юникод (UTF-8)

Международная стандартная кодировка, которая охватывает большинство глобальных языков. При использовании в этом руководстве термина UTF-8 имеются в виду символы кодировки в формате UTF-8.

Подготовка

В этой главе объясняется роль администратора и подготовка к внесению изменений.

Рабочий процесс настройки и обслуживания сканера

Администратор настраивает подключение к сети, выполняет исходную настройку и обслуживание сканера, чтобы эти устройства были доступны пользователям.

1. Подготовка
   - ❏ Сбор сведений о настройке подключения
   - ❏ Решение по методу подключения
2. Подключение
   - ❏ Подключение к сети с панели управления сканера
3. Настройка функций
   - ❏ Настройки драйвера сканера
   - ❏ Прочие расширенные настройки
4. Настройки безопасности
   - ❏ Настройки администратора
   - ❏ SSL/TLS
   - ❏ Управление протоколами
   - ❏ Расширенные настройки безопасности (опция)
5. Эксплуатация и управление
   - ❏ Проверка состояния устройства
   - ❏ Обработка экстренных ситуаций
   - ❏ Резервное копирование настроек устройства

Соответствующая информация

➡ «Подготовка» на стр. 10

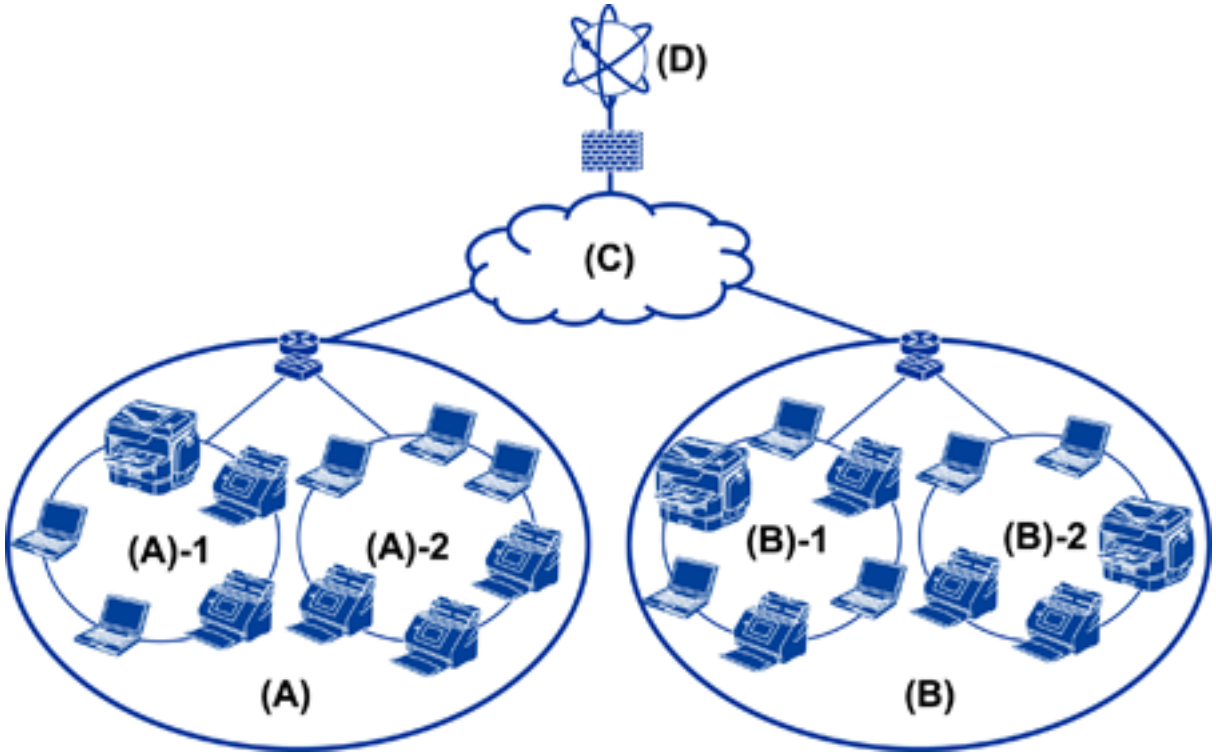
➡ «Подключение» на стр. 15

➡ «Настройки функций» на стр. 22

➡ «Базовые настройки безопасности» на стр. 33

➡ «Настройки работы и управления» на стр. 41

Пример сетевой среды



(A) : офис 1

❏ (A) - 1 : локальная сеть 1

❏ (A) - 2 : локальная сеть 2

(B) : офис 2

❏ (B) - 1 : локальная сеть 1

❏ (B) - 2 : локальная сеть 2

(C) : WAN

(D) : Интернет

Пример настроек подключения сканера

В основном существуют два типа подключения, использование которых зависит от способа применения сканера. Оба служат для подключения сканера к сети, если компьютер подключен через концентратор.

❏ Подключение сервер/клиент (сканер с использованием сервера под управлением Windows, управление заданиями)

❏ Одноранговое подключение (прямое подключение к клиентскому компьютеру)

Соответствующая информация

➡ «Подключение сервера/клиента» на стр. 12

➡ «Одноранговое подключение» на стр. 12

Подключение сервера/клиента

Централизованное управление сканером и заданиями с помощью Document Capture Pro Server, установленного на сервере. Больше всего подходит для заданий, использующих несколько сканеров для сканирования большого количества документов определенного формата.

Соответствующая информация

➡ «Термины, используемые в данном руководстве» на стр. 8

Одноранговое подключение

Использование отдельного сканера с помощью драйвера сканера, например Epson Scan 2, установленного на клиентском компьютере. Установка Document Capture Pro (Document Capture) на клиентском компьютере позволяет выполнять задания на отдельных клиентских компьютерах, подключенных к сканеру.

Соответствующая информация

➡ «Термины, используемые в данном руководстве» на стр. 8

Подготовка подключения к сети

Сбор информации о настройке подключения

Для сетевого подключения необходимо наличие IP-адреса, адреса шлюза и т. д. Заблаговременно проверьте следующие параметры.

Разделы	Параметры	Примечание
Метод подключения устройства	❏ Ethernet	Для подключения Ethernet используйте экранированную витую пару категории 5e и выше.
Сведения о подключении к локальной сети	❏ IP-адрес ❏ Маска подсети ❏ Стандартный шлюз	Если вы автоматически установили IP-адрес с помощью функции DHCP на маршрутизаторе, это значение не является необходимым.
Сведения о DNS-сервере	❏ IP-адрес для основного DNS ❏ IP-адрес для вспомогательного DNS	При использовании в качестве IP-адреса статического IP-адреса настройте DNS-сервер. Настройте при автоматическом назначении с использованием функции DHCP и при невозможности автоматического назначения DNS-сервера.
Сведения о прокси-сервере	❏ Имя прокси-сервера ❏ Номер порта	Настройте при использовании прокси-сервера для подключения к Интернету, а также при использовании службы Epson Connect или функции автоматического обновления микропрограммы.

Характеристики сканера

Характеристика, указывающая, поддерживает ли сканер стандартный режим или режим подключения (см. *Руководство пользователя*).

Использование номера порта

Номер порта, используемого сканером, см. в приложении.

Соответствующая информация

➡ «Использование порта сканера» на стр. 61

Тип назначения IP-адреса

Существует два типа назначения IP-адреса на сканере.

Статический IP-адрес:

Назначьте сканеру предварительно определенный, уникальный IP-адрес.

IP-адрес не меняется даже при отключении сканера или маршрутизатора, поэтому можно управлять устройством через его IP-адрес.

Этот тип подходит для сети, где необходимо управлять большим количеством сканеров, например в большой организации или в учебном заведении.

Автоматическое назначение с использованием функции DHCP:

Надлежащий IP-адрес автоматически назначается, если успешно устанавливается связь между сканером и маршрутизатором, который поддерживает функцию DHCP.

Если изменение IP-адреса для определенного устройства не представляется удобным, зарезервируйте этот IP-адрес, чтобы назначить его впоследствии.

DNS-сервер и прокси-сервер

Если вы используете службу подключения к Интернету, настройте DNS-сервер. Если не настроить его, необходимо указать IP-адрес для доступа, так как это может привести к ошибочному разрешению имен.

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.

Можно запретить доступ к определенному URL-адресу, используя функцию фильтрации, так как прокси-сервер может проверять содержимое канала связи.

Способ настройки подключения к сети

Чтобы настроить IP-адрес, маску подсети и стандартный шлюз на сканере, выполните следующие действия.

Подготовка

Использование панели управления

Настройте параметры с помощью панели управления сканера на каждом сканере. Подключитесь к сети после настройки параметров подключения сканера.

Использование установщика

При использовании установщика сеть сканера и клиентский компьютер устанавливаются автоматически. Настройка осуществляется посредством выполнения инструкций установщика, даже если у вас нет глубоких познаний в области сетевых технологий.

Использование инструмента:

Используйте инструмент на компьютере администратора. Вы можете определить сканер и настроить его или же создать файл SYLK для пакетного внесения изменений на несколько сканеров. Можно настроить несколько сканеров, однако перед настройкой к ним необходимо физически подключать кабель Ethernet. Поэтому рекомендуется построить сеть Ethernet для настройки.

Соответствующая информация

➡ «Подключение к сети с панели управления» на стр. 15

➡ «Подключение к сети с помощью установщика» на стр. 19

➡ «Назначение IP-адресов с помощью EpsonNet Config» на стр. 57

Подключение

В этой главе объясняется среда или процедура для подключения сканера к сети.

Подключение к сети

Подключение к сети с панели управления

Подключите сканер к сети с помощью панели управления сканера.

Дополнительные сведения о панели управления сканера см. в *Руководство пользователя*.

Назначение IP-адреса

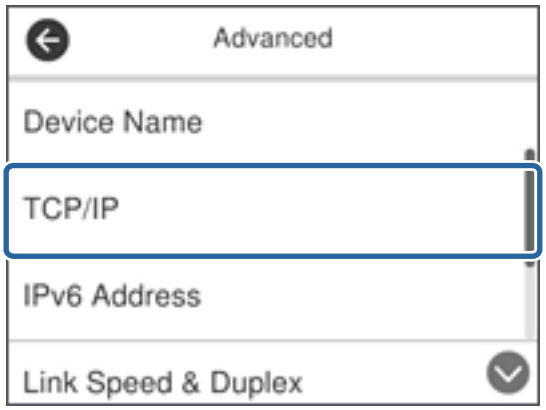
Настройте базовые элементы, такие как IP-адрес, Маска подсети и Шлюз по умолчанию.

1. Включите сканер.
2. Проведите по экрану влево на панели управления сканера, затем нажмите **Настр.**.

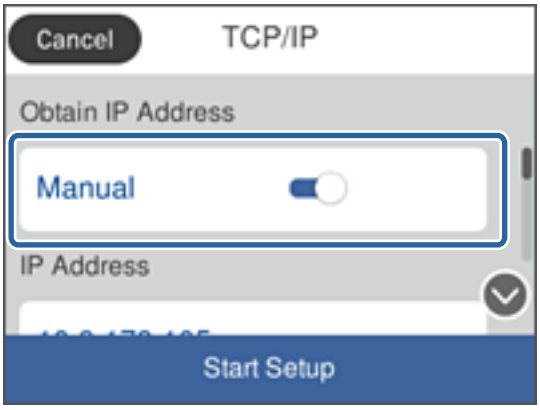
3. Нажмите **Настройки сети** > **Изменить настройки**.

   Если элемент не отображается, прокрутите экран вверх для его отображения.

4. Коснитесь **TCP/IP**.

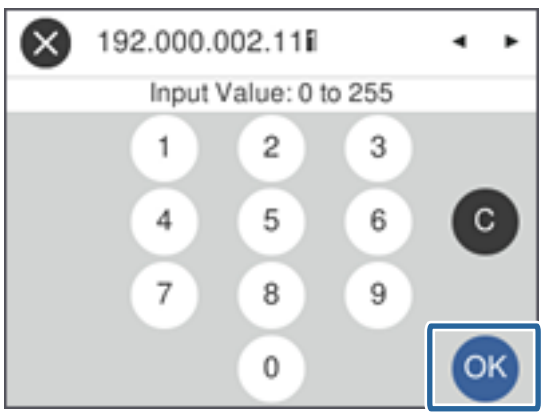


5. Выберите значение **Ручной** для параметра **Получить IP-адрес**.



Примечание:
*Если IP-адрес определяется автоматически с помощью функции DHCP или маршрутизатора, выберите**Авто**. В этом случае **IP-адрес**, **Маска подсети** и **Шлюз по умолчанию** на шагах 6–7 также задаются автоматически, поэтому перейдите к шагу 8.*

6. Нажмите поле **IP-адрес**, введите IP-адрес с помощью клавиатуры, отображаемой на экране, затем нажмите **OK**.



Проверьте значение, отображенное на предыдущем экране.

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

   Проверьте значение, отображенное на предыдущем экране.

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

8. Щелкните поле **Основной DNS-сервер** для **DNS-сервер**, введите IP-адрес для основного DNS-сервера с помощью клавиатуры, отображаемой на экране, затем нажмите **OK**.

   Проверьте значение, отображенное на предыдущем экране.

   Примечание:
   *При выборе **Авто** в качестве настроек назначения IP-адреса можно выбрать настройки DNS-сервера как **Ручной** или **Авто**. Если вы не можете получить адрес DNS-сервера автоматически, выберите **Ручной** и введите адрес DNS-сервера. Затем введите напрямую адрес дополнительного DNS-сервера. Если вы выбрали **Авто**, перейдите к шагу 10.*

9. Щелкните поле **Дополнит. DNS-сервер**, введите IP-адрес для дополнительного DNS-сервера с помощью клавиатуры, отображаемой на экране, затем нажмите **OK**.

   Проверьте значение, отображенное на предыдущем экране.

10. Коснитесь **Запуск настройки**.

11. Нажмите **Закрыть** на экране подтверждения.

    Если вы не нажмете кнопку **Закрыть**, окно автоматически закроется по истечении определенного времени.

Подключение к Ethernet

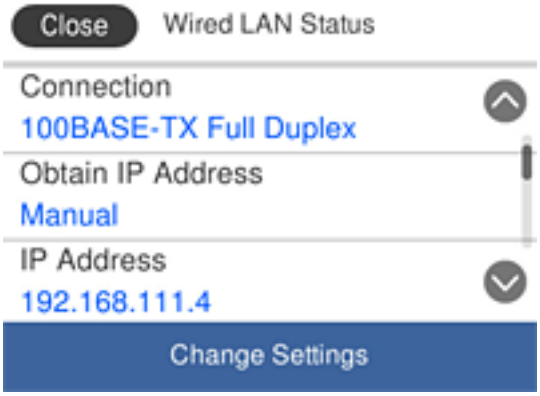
Подключите сканер к сети с помощью кабеля Ethernet и проверьте подключение.

1. Подключите сканер и концентратор (коммутатор L2) кабелем Ethernet.

   Значок на главном экране меняется на  .

2. Нажмите  на главном экране.

3. Прокрутите экран вверх, затем убедитесь, что состояние подключения и IP-адрес указаны верно.



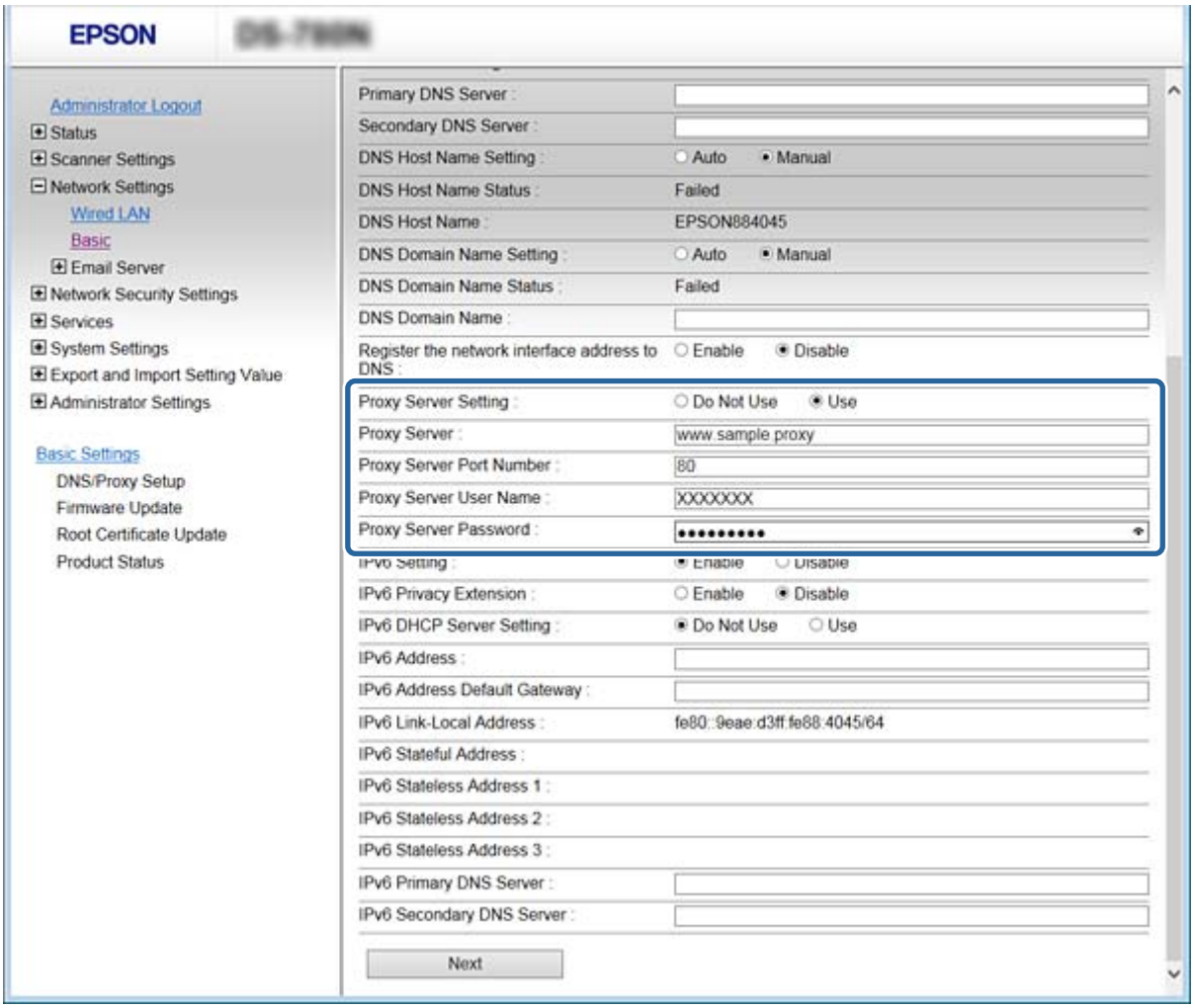
Настройка прокси-сервера

Прокси-сервер не может быть установлен на панели. Выполните настройки с помощью Web Config.

1. Откройте Web Config и выберите **Network Settings** > **Basic**.
2. Выберите **Use** в **Proxy Server Setting**.
3. Укажите прокси-сервер в формате IPv4-адреса или полного доменного имени в **Прокси-сервер**, затем введите номер порта в **Proxy Server Port Number**.

   Для прокси-серверов, требующих проверку подлинности, введите имя пользователя и пароль для проверки подлинности на прокси-сервере.

4. Нажмите кнопку **Next**.



5. Проверьте настройки, затем нажмите **Настройки**.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Подключение к сети с помощью установщика

Рекомендуем использовать установщик для подключения сканера к компьютеру. Вы можете запустить установщик с помощью одного из следующих методов.

❏ Настройка с веб-сайта

Откройте следующий веб-сайт и введите имя продукта. Откройте **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, чьи компьютеры оснащены дисковыми приводами).

Вставьте диск с программным обеспечением в компьютер и выполните инструкции на экране.

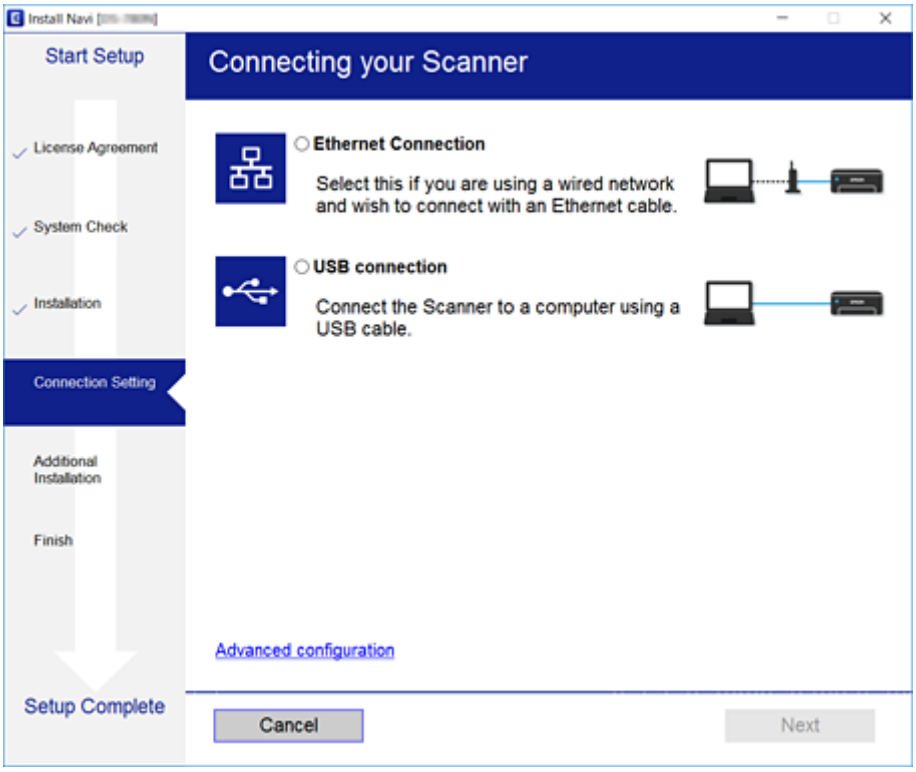
Подключение

Выбор методов подключения

Выполните инструкции на экране, пока не отобразится следующий экран, затем выберите метод подключения сканера к компьютеру.

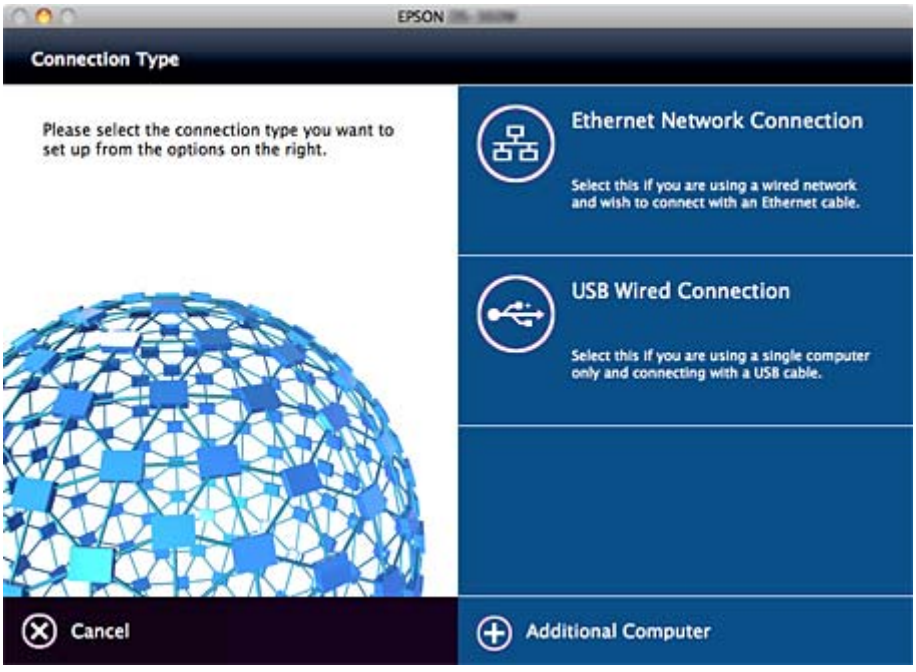
❏ Windows

Выберите тип подключения и нажмите **Далее**.



❏ Mac OS

Выберите тип подключения.



Подключение

Следуйте инструкциям на экране. Установлено необходимое программное обеспечение.

Настройки функций

В этой главе объясняются начальные настройки, которые следует выполнить, чтобы использовать каждую функцию устройства.

Программное обеспечение для настройки

В этом разделе объясняется процедура внесения настроек с компьютера администратора с использованием Web Config.

Web Config (веб-страница для устройства)

Сведения о Web Config

Web Config представляет собой приложение на основе браузера для настройки параметров сканера.

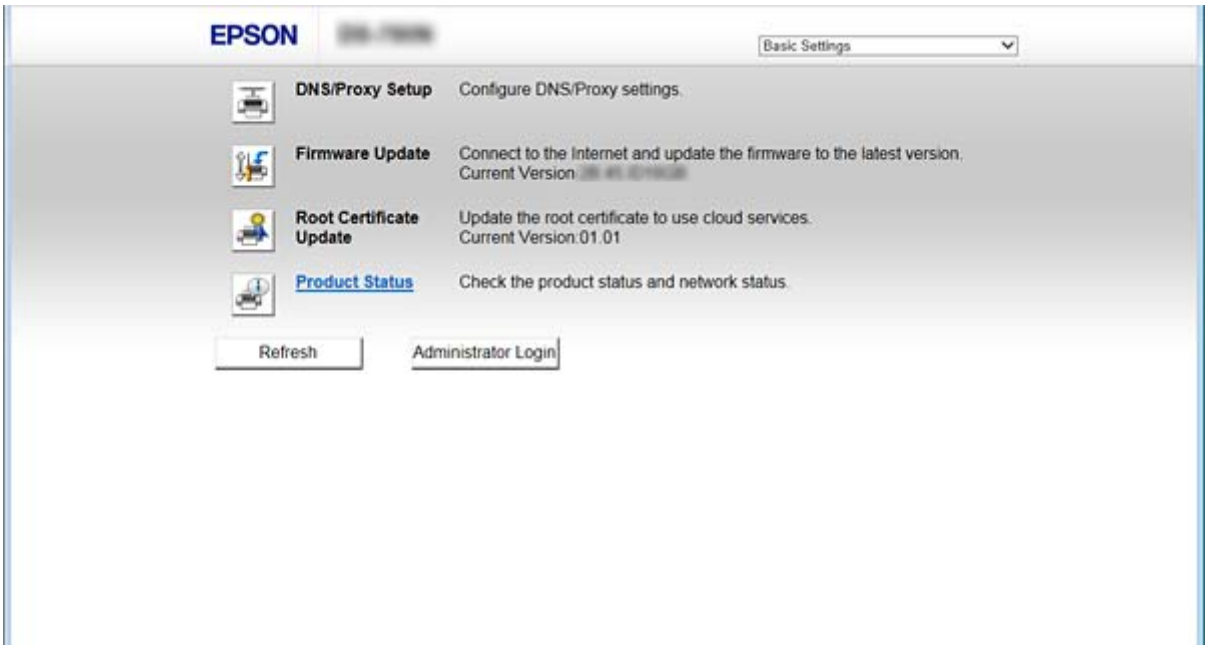
Для получения доступа к приложению Web Config необходимо вначале присвоить сканеру IP-адрес.

Примечание:
Параметры можно заблокировать путем настройки пароля администратора для сканера.

Ниже представлены две страницы настройки.

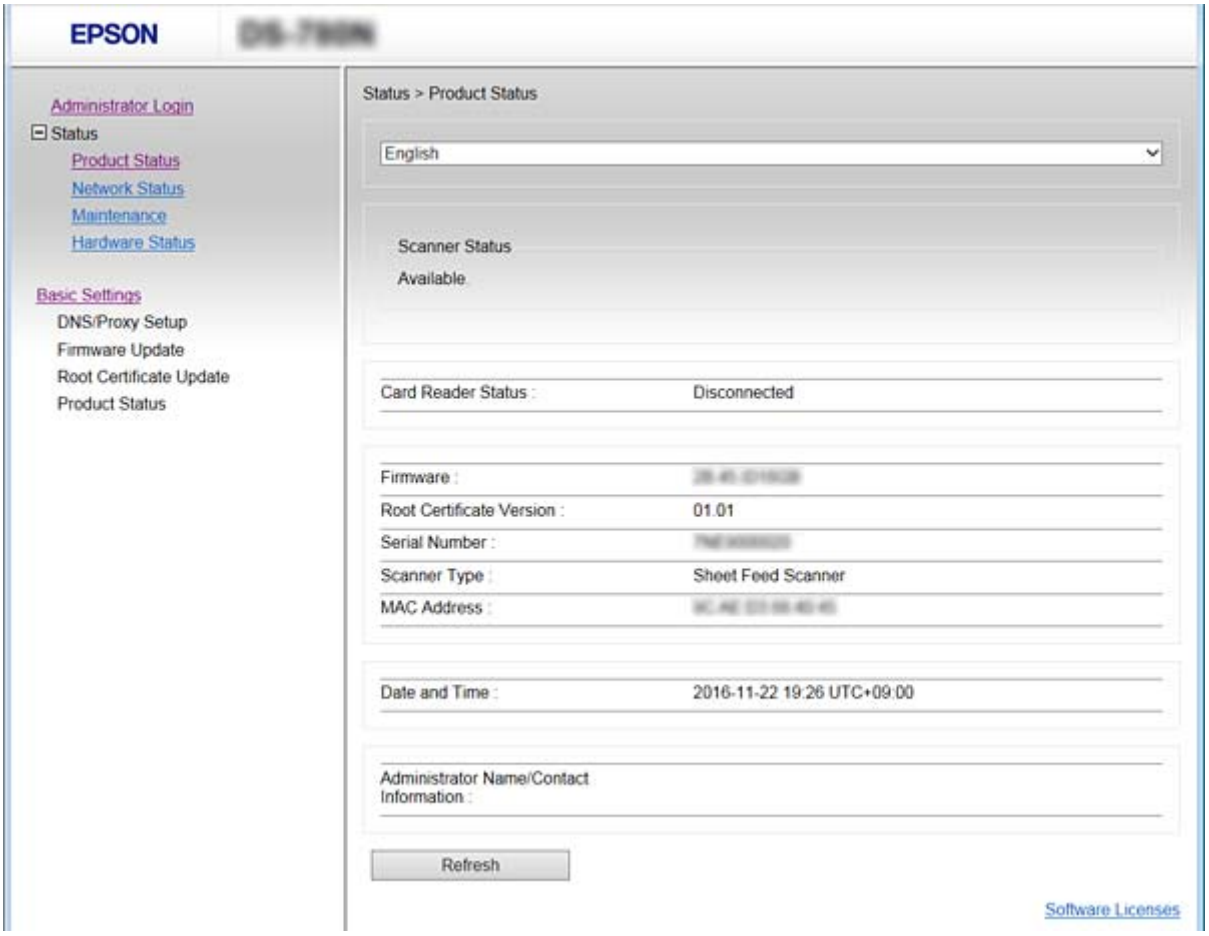
❏ **Basic Settings**

На этой странице можно настроить основные параметры для сканера.



❏ **Advanced Settings**

На этой странице можно настроить дополнительные параметры для сканера. Данная страница предназначена для администратора.



Доступ к приложению Web Config

Введите IP-адрес сканера в веб-браузере. JavaScript должен быть включен. При доступе к Web Config по протоколу HTTPS в браузере появится предупреждение, поскольку при соединении будет использован самозаверяющий сертификат, хранящийся на сканере.

❏ Доступ по HTTPS

IPv4: https://<IP-адрес сканера> (без < >)

IPv6: https://[IP-адрес сканера]/ (с [ ])

❏ Доступ по HTTP

IPv4: http://<IP-адрес сканера> (без < >)

IPv6: http://[IP-адрес сканера]/ (с [ ])

Примечание:

❏ *Примеры*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Имя сканера, зарегистрированного на DNS-сервере, можно использовать вместо его IP-адреса.*

Соответствующая информация

➡ «Связь со сканером через SSL/TLS» на стр. 64

➡ «О цифровом сертификате» на стр. 65

Использование функций сканирования

В зависимости от того, как вы намереваетесь использовать сканер, установите следующее программное обеспечение и внесите необходимые настройки.

❏ **Сканирование с компьютера**

❏ Проверьте правильность настройки сетевой службы сканирования с помощью Web Config (допустимо при поставке с завода).

❏ Установите Epson Scan 2 на компьютере и задайте IP-адрес.

❏ При сканировании с использованием задания установите Document Capture Pro (Document Capture) и задайте настройки задания.

❏ **Сканирование с панели управления**

❏ При использовании Document Capture Pro или Document Capture Pro Server

Установите Document Capture Pro или Document Capture Pro Server.

Настройка DCP (режим сервера, режим клиента).

❏ При использовании протокола WSD

Проверьте правильность WSD в Web Config или на панели управления (допустимо только при поставке с завода).

Дополнительные настройки устройства (компьютер под управлением Windows).

Сканирование с компьютера

Установите программное обеспечение и проверьте, включена ли служба сетевого сканирования для сканирования с компьютера по сети.

Соответствующая информация

➡ «Устанавливаемое программное обеспечение» на стр. 25

➡ «Включение сканирования сети» на стр. 25

Устанавливаемое программное обеспечение

❏ Epson Scan 2

Это драйвер сканера. Если необходимо использовать устройство с компьютера, установите драйвер на каждом клиентском компьютере. Если установлено Document Capture Pro/Document Capture, можно выполнить операции, назначенные кнопкам на устройстве.

Благодаря EpsonNet SetupManager драйверы печати также могут распространяться совместно в пакетах.

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

Установите на клиентском компьютере. Можно вызвать и выполнить задания, зарегистрированные на компьютере, с помощью программного обеспечения Document Capture Pro/Document Capture, установленного в сети, с компьютера или панели управления сканера.

Можно также выполнить сканирование с компьютера через сеть. Для сканирования требуется Epson Scan 2.

Соответствующая информация

➡ «EpsonNet SetupManager» на стр. 57

Настройте IP-адрес сканера в Epson Scan 2

Укажите IP-адрес сканера, чтобы сканер можно было использовать в сети.

1. Запустите **Epson Scan 2 Utility** в меню **Пуск** > **Все программы** > **EPSON** > **Epson Scan 2**.

   Если уже зарегистрирован другой сканер, перейдите к шагу 2.

   Если не зарегистрирован, перейдите к шагу 4.

2. Щелкните ▼ в разделе **Сканер**.
3. Нажмите **Настройки**.
4. Щелкните **Включить изменение**, затем щелкните **Добавить**.
5. Выберите наименование модели сканера в пункте **Модель**.
6. Выберите IP-адрес сканера, который будет использоваться, в пункте **Адрес** раздела **Поиск сети**.

   Щелкните  и  , чтобы обновить список. Если невозможно найти IP-адрес сканера, выберите **&Ручной ввод адреса** и введите IP-адрес.

7. Нажмите **Добавить**.
8. Нажмите **OK**.

Включение сканирования сети

Вы можете включить службу сканирования сети при сканировании с клиентского компьютера по сети. Значение по умолчанию включено.

1. Откройте Web Config и выберите **Services** > **Network Scan**.

2. Убедитесь, что выбран пункт **Enable scanning** для **EPSON Scan**.

   Если он выбран, эта задача выполнена. Закройте Web Config.

   Если пункт не выбран, выберите его и перейдите к следующему шагу.

3. Нажмите **Next**.

4. Нажмите **OK**.

   Сеть подключается повторно, после чего включаются настройки.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Сканирование с использованием панели управления

Функция сканирования в папку и функция сканирования на эл. почту с панели управления сканера, а также передача результатов сканирования на почту, в папки и т. д. выполняются путем запуска задания с компьютера.

При передаче результатов сканирования настройте задание с помощью Document Capture Pro Server или Document Capture Pro.

Сведения о настройках и настройке задания см. в документации или справке по Document Capture Pro Server или Document Capture Pro.

Соответствующая информация

➡ «Настройки Document Capture Pro Server/Document Capture Pro» на стр. 26

➡ «Настройка серверов и папок» на стр. 27

Программное обеспечение для установки на компьютере

❏ **Document Capture Pro Server**

Это версия Document Capture Pro для сервера. Установите его на сервере Windows. Несколько устройств и заданий могут централизованно управляться с сервера. Могут выполняться задания одновременно с нескольких сканеров.

С помощью сертифицированной версии Document Capture Pro Server можно управлять заданиями и историей сканирования с привязкой к группам и пользователям.

Подробные сведения о Document Capture Pro Server можно получить в региональном офисе Epson.

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

Как и при сканировании с компьютера, можно вызвать задания, зарегистрированные на компьютере, с панели управления, а затем выполнить их. Невозможно выполнять задания на компьютере одновременно с нескольких сканеров.

Настройки Document Capture Pro Server/Document Capture Pro

Настройте использование функции сканирования с панели управления сканера.

1. Откройте Web Config и выберите **Services** > **Document Capture Pro**.

2. Выберите **Режим работы**.

   ❏ Server Mode

   Выберите этот режим при использовании Document Capture Pro Server или Document Capture Pro только для заданий, которые были настроены для определенного компьютера.

   ❏ Client Mode

   Установите этот режим, если вы выбрали настройку задания через ПО Document Capture Pro (Document Capture), установленное на каждом клиентском компьютере в сети без указания компьютера.

3. Задайте приведенные ниже настройки в соответствии с выбранным режимом.

   ❏ Server Mode

   В **Server Address** укажите сервер, на котором установлено ПО Document Capture Pro Server. Введите от 2 до 252 символов в формате IPv4, IPv6, имя хоста или полное доменное имя. В формате полного доменного имени можно использовать буквы, цифры, алфавиты и дефисы US — ASCII (кроме пробела в начале и в конце).

   ❏ Client Mode

   Укажите **Group Settings** для использования группы сканеров, указанной в Document Capture Pro (Document Capture).

4. Нажмите **Настройки**.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Настройка серверов и папок

Document Capture Pro и Document Capture Pro Server сохраняют отсканированные данные на сервер или клиентский компьютер только один раз и используют функцию передачи для запуска функции сканирования в папку или сканирования на электронную почту.

Необходимо иметь надлежащие права и нужные сведения для передачи данных с компьютера, на котором установлены Document Capture Pro, Document Capture Pro Server, на другой компьютер или в облачную службу.

Подготовьте сведения о функции, которую намереваетесь использовать, обращая внимание на приведенные ниже сведения.

Можно настроить эти функции с помощью Document Capture Pro или Document Capture Pro Server. Сведения об этих настройках см. в документации или справке по Document Capture Pro Server или Document Capture Pro.

Настройки функций

Название	Настройки	Требование
Сканирование в сетевую папку (SMB)	Создание и настройка общего доступа к папке сохранения	Учетная запись пользователя, являющегося администратором на компьютере, где создаются папки для сохранения.
	Сканирование в сетевую папку (SMB)	Имя пользователя и пароль для входа на компьютер, где размещена папка для сохранения, а также привилегия для обновления папки для сохранения.
Сканирование в сетевую папку (FTP)	Настройка для входа на FTP-сервер	Информация для входа на FTP-сервер и привилегия на обновление папки для сохранения.
Сканирование в эл. почту	Настройка сервера электронной почты	Сведения о настройке сервера эл. почты
Сканирование в Document Capture Pro (при использовании Document Capture Pro Server)	Настройка для входа в облачные службы	Среда интернет-подключения Регистрация учетной записи для облачных служб

Использование сканирования WSD (только в Windows)

Если компьютер работает под управлением Windows Vista и выше, можно использовать сканирование WSD.

Если можно использовать протокол WSD, на панели управления сканера отображается меню **Комп. (WSD)**.

1. Откройте Web Config и выберите **Services** > **Protocol**.
2. Убедитесь, что включен параметр **Enable WSD** в меню **WSD Settings**.

   Если он включен, задача выполнена и можно закрывать Web Config.

   Если он не включен, включите его и перейдите к следующему шагу.
3. Нажмите кнопку **Next**.
4. Проверьте настройки, затем щелкните **Настройки**.

Внесение системных настроек

Настройка системы на панели управления

Установка яркости экрана

Установите яркость ЖК-экрана.

1. Нажмите **Настр.** на главном экране.
2. Нажмите **Общие настройки** > **Яркость дисп.**.
3. Нажмите  или  для регулировки яркости экрана.

   Можно изменить от 1 до 9.
4. Коснитесь **OK**.

Установка звука

Установите звуки панели управления и звуки ошибок.

1. Нажмите **Настр.** на главном экране.
2. Нажмите **Общие настройки** > **Звук**.
3. При необходимости настройте следующие элементы.
   - ❏ Звук работы

     Установите громкость звуков, которые слышны при работе с панелью управления.
   - ❏ Звук ошибки

     Установите громкость звука ошибок.
4. Коснитесь **OK**.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Определение двойной подачи оригинала

Включите функцию определения двойной подачи документа для сканирования и остановки сканирования при нескольких подачах.

Чтобы отсканировать оригиналы, которые могут определяться как многократные подачи, например конверты или бумага с наклейками, отключите функцию.

Примечание:
Можно также установить настройки с помощью Web Config или Epson Scan 2.

1. Нажмите **Настр.** на главном экране.
2. Нажмите **Внешние настройки сканирования** > **Ультразвук. обнар. двойн. под.**.
3. Нажмите **Ультразвук. обнар. двойн. под.** для включения или отключения функции.
4. Коснитесь **Закрыть**.

Установка низкоскоростного режима

Установите для сканирования на низкой скорости, чтобы замятия бумаги не возникали при сканировании тонких документов, таких как чеки.

1. Нажмите **Настр.** на главном экране.
2. Нажмите **Внешние настройки сканирования** > **Медленно**.
3. Нажмите **Медленно** для включения или отключения функции.
4. Коснитесь **Закрыть**.

Внесение настроек системы с помощью веб-конфигурации

Настройки энергосбережения во время бездействия

Установите настройку энергосбережения на время бездействия сканера. Задайте время в зависимости от среды использования.

Примечание:
Можно также внести изменения в настройки энергосбережения на панели управления сканера.

1. Откройте Web Config и выберите **System Settings** > **Power Saving**.
2. Введите время для **Sleep Timer**, чтобы переключиться в режим энергосбережения на период бездействия.

   Можно настроить вплоть до 240 минут с шагом в одну минуту.
3. Выберите время отключения для **Power Off Timer**.
4. Нажмите **OK**.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Настройка панели управления

Выполните настройку панели управления сканера. Настройку можно выполнить следующим образом.

1. Откройте Web Config и выберите **System Settings** > **Control Panel**.
2. При необходимости настройте следующие элементы.

   ❏ Language

   Выберите отображаемый язык на панели управления.

❏ Panel Lock

Если вы выберите значение **ON** при выполнении операций, требующих прав администратора, необходимо будет вводить пароль администратора. Если пароль администратора не задан, блокировка панели отключена.

❏ Operation Timeout

Если выбрать **ON** при входе в качестве администратора, выполняется автоматический выход из системы и переход на начальный экран при отсутствии активности в течение определенного периода времени.

Можно задать значение от 10 секунд до 240 минут с шагом в одну секунду.

3. Нажмите **OK**.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Настройка ограничения для внешнего интерфейса

Вы можете ограничить использование порта USB для подключения с компьютера. Задайте его для ограничения сканирования, кроме как через сеть.

1. Откройте Web Config и выберите **System Settings** > **External Interface**.
2. Выберите **Enable** или **Disable**.

   Для ограничения выберите **Disable**.
3. Коснитесь **OK**.

Синхронизация даты и времени с помощью сервера времени

Если вы используете сертификат ЦС, можно предотвратить возникновение проблем со временем.

1. Откройте Web Config и выберите **System Settings** > **Date and Time** > **Time Server**.
2. Выберите значение **Use** для параметра **Use Time Server**.
3. Введите адрес сервера времени в качестве значения параметра **Time Server Address**.

   Используйте формат IPv4, IPv6 или полного доменного имени. Вводите не более 252 символов. Оставьте поле пустым, если не нужно указывать значение.
4. Введите **Update Interval (min)**.

   Можно настроить вплоть до 10 800 минут с шагом в одну минуту.
5. Нажмите **OK**.

   Примечание:
   *Вы можете проверить состояние подключения к серверу времени в разделе **Time Server Status**.*

Настройки функций

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Базовые настройки безопасности

В этой главе объясняются базовые настройки безопасности, которые не требуют особой среды.

Введение в базовые функции безопасности

Здесь представлены базовые функции безопасности устройств Epson.

Название функции	Тип функции	Что определять	Что предотвращать
Настройка пароля администратора	Заблокируйте настройки, связанные с системой, например настройки сети и подключения по USB, чтобы никто не мог их изменять, кроме администратора.	Администратор задает пароль для устройства. Настройка или обновление доступны в любом месте Web Config, на панели управления, в Epson Device Admin и EpsonNet Config.	Можно предотвратить незаконное чтение и изменение информации, которая хранится на устройстве, например таких данных, как идентификаторы, пароли, сетевые настройки и контакты. Кроме того, можно снизить широкий спектр рисков безопасности, таких как утечка информации о сетевой среде или политике безопасности.
Соединения SSL/TLS	При получении доступа к серверу Epson в Интернете с устройства, например при связи с компьютера через браузер или обновление микропрограммы, передаваемые данные шифруются посредством соединения SSL/TLS.	Получите сертификат, подписанный ЦС, а затем импортируйте его на сканер.	Сброс идентификации на устройстве с помощью сертификата, подписанного ЦС, препятствует выдаче себя за другое лицо и незаконному доступу. Кроме того, данные, передаваемые по каналу SSL/TLS, являются защищенными, что препятствует утечке данных о печати и настройке.
Протоколы управления	Протоколы управления используются для связи между устройствами и компьютерами, а также для включения и выключения функций.	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.

Соответствующая информация

➡ «Сведения о Web Config» на стр. 22

➡ «EpsonNet Config» на стр. 56

➡ «Epson Device Admin» на стр. 56

➡ «Настройка пароля администратора» на стр. 34

➡ «Управление протоколами» на стр. 36

Настройка пароля администратора

При установке пароля администратора пользователи, отличные от администраторов, не смогут изменять настройки, предназначаемые для администрирования системы. Можно задать и изменить пароль администратора с помощью Web Config, панели управления сканера или программного обеспечения (Epson Device Admin или EpsonNet Config). При использовании программного обеспечения изучите документацию каждой программы.

Соответствующая информация

➡ «Настройка пароля администратора на панели управления» на стр. 34

➡ «Настройка пароля администратора с помощью Web Config» на стр. 34

➡ «EpsonNet Config» на стр. 56

➡ «Epson Device Admin» на стр. 56

Настройка пароля администратора на панели управления

Можно настроить пароль администратора на панели управления сканера.

1. Нажмите **Настр.** на главном экране.
2. Нажмите **Администрир. системы** > **Настройки администратора**.

   Если элемент не отображается, прокрутите экран вверх для его отображения.
3. Нажмите **Пароль администратора** > **Регистрация**.
4. Введите пароль и нажмите **OK**.
5. Повторно введите пароль и нажмите **OK**.
6. Нажмите **OK** на экране подтверждения.

   Отображается экран настроек администратора.
7. Нажмите **Функция блокировки**, затем нажмите **OK** на экране подтверждения.

   Для параметра Функция блокировки задано значение **Вкл.**, поэтому для управления заблокированным меню будет необходим пароль администратора.

Примечание:

❏ *Если настроить для параметра **Настр.** > **Общие настройки** > **Вр. ож. оп.** значение **Вкл.**, сканер выполнит выход текущего пользователя после определенного периода бездействия на панели управления.*

❏ *Можно изменить или удалить пароль администратора при выборе **Изменить** или **Сброс** на экране **Пароль администратора** и вводе пароля администратора.*

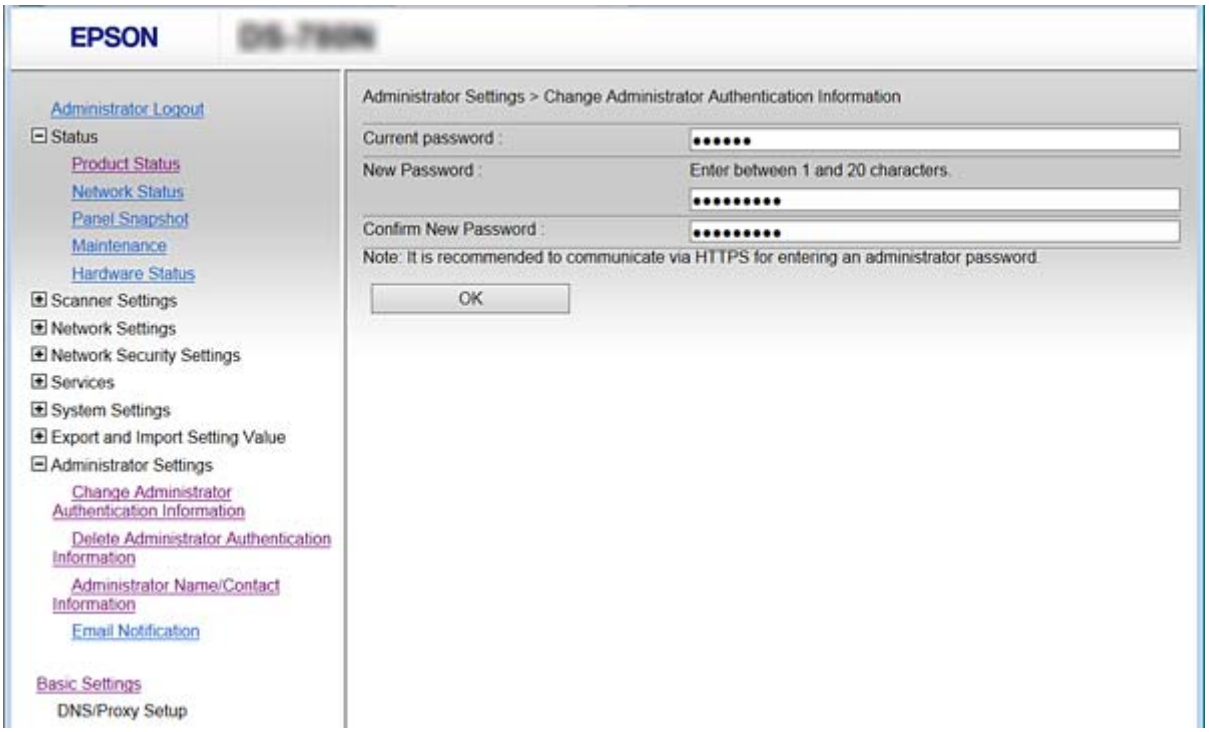
Настройка пароля администратора с помощью Web Config

С помощью Web Config можно настроить пароль администратора.

1. Откройте Web Config и выберите **Administrator Settings** > **Change Administrator Authentication Information**.

2. Введите пароль в поле **New Password** и нажмите **Confirm New Password**. Если необходимо, введите имя пользователя.

   При необходимости смены пароля введите текущий пароль.



3. Выберите **OK**.

   Примечание:
   - ❏ *Чтобы установить или изменить заблокированные элементы меню, щелкните **Administrator Login**, затем введите пароль администратора.*
   - ❏ *Чтобы удалить пароль администратора, щелкните **Administrator Settings** > **Delete Administrator Authentication Information**, затем введите пароль администратора.*

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Элементы, которые блокируются паролем администратора

Администраторы имеют права на настройку и изменение любых функций на устройствах.

Кроме того, если задать пароль администратора на этом устройстве, можно заблокировать устройство, чтобы невозможно было изменять параметры, связанные с управлением устройством.

Ниже приведены элементы, управляемые администратором.

Базовые настройки безопасности

Элемент	Описание
Настройка сканера	Настройка определения двойной подачи и низкий скоростной режим.
Настройки подключения по Ethernet	Здесь можно изменить имя и IP-адрес устройства, настроить DNS-сервер или прокси-сервер, а также настроить изменения, связанные с подключением к сети.
Настройка пользовательских служб	Здесь можно выполнить настройку протоколов связи, сетевого сканирования и служб Document Capture Pro.
Настройка сервера эл. почты	Настройте сервер электронной почты, с которым непосредственно связываются устройства.
Настройка безопасности	Настройки сетевой безопасности, например связи SSL/TLS, IPsec/фильтрации IP, а также IEEE802.1X.
Обновление корневого сертификата	Обновление корневого сертификата необходимо для проверки подлинности Document Capture Pro Server и обновления микропрограммы в Web Config.
Обновление микропрограммы	Проверьте и обновите микропрограмму на устройствах.
Время, настройки таймера	Время перехода в спящий режим, автоматическое выключение питания, дата/время, таймер нерабочего времени, прочие настройки, связанные с таймером.
Восстановление настроек по умолчанию	Настройка сканера для сброса до заводских настроек.
Настройка администратора	Настройка блокировки администратора или пароля администратора.
Настройка сертифицированного устройства	Настройка идентификатора устройства проверки подлинности. Укажите, когда использовать сканер в системе проверки подлинности, которая поддерживает устройства проверки подлинности.

Управление протоколами

Можно сканировать, используя различные способы и протоколы. Можно также использовать сканирование по сети с неограниченного количества сетевых компьютеров. Например, допустимо сканирование с использованием только указанных способов и протоколов. Можно снизить вероятность возникновения непредусмотренных рисков безопасности, ограничив возможность сканирования тем или иным способом, а также управляя доступными функциями.

Настройте параметры протоколов.

1. Откройте Web Config и выберите **Services** > **Protocol**.
2. Выполните настройку каждого элемента.
3. Нажмите **Next**.
4. Нажмите **OK**.

   Настройки будут применены на сканере.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Протоколы, которые можно включить и выключить» на стр. 37

➡ «Элементы настройки протоколов» на стр. 38

Протоколы, которые можно включить и выключить

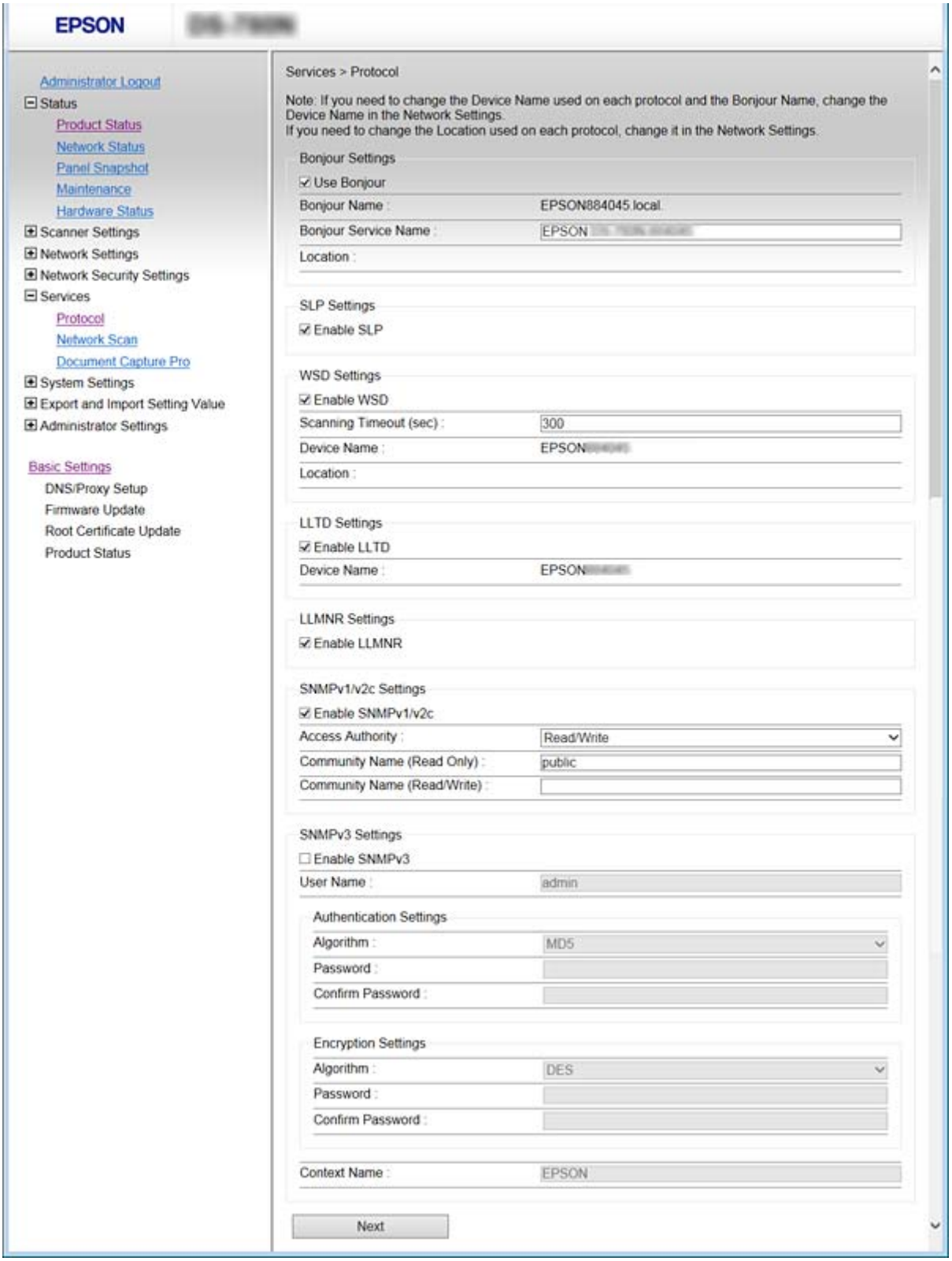
Протокол	Описание
Bonjour Settings	Можно указать, следует ли использовать Bonjour. Bonjour используется для поиска устройств, сканирования и пр.
SLP Settings	Можно включить или отключить функцию SLP. SLP используется для Epson Scan 2 и поиска в сети EpsonNet Config.
WSD Settings	Можно включить или отключить функцию WSD. Если функция включена, можно добавлять устройства WSD или сканировать с порта WSD.
LLTD Settings	Можно включить или отключить функцию LLTD. Если функция включена, она отображается на карте сети Windows.
LLMNR Settings	Можно включить или отключить функцию LLMNR. Если функция включена, можно разрешать имена без использования NetBIOS, даже если невозможно использовать DNS.
SNMPv1/v2c Settings	Можно указать, следует ли включить или выключить SNMPv1/v2c. Этот протокол используется для настройки устройств, их мониторинга и т. д.
SNMPv3 Settings	Можно указать, следует ли включить или выключить SNMPv3. Этот протокол используется для настройки шифрованных устройств, их мониторинга и пр.

Соответствующая информация

➡ «Управление протоколами» на стр. 36

➡ «Элементы настройки протоколов» на стр. 38

Элементы настройки протоколов



Параметры	Значение и описание параметров
Bonjour Settings	

Базовые настройки безопасности

Параметры	Значение и описание параметров
Use Bonjour	Выберите для поиска или использования устройств с помощью Bonjour.
Bonjour Name	Отображает имя Bonjour.
Bonjour Service Name	Можно отобразить и установить имя службы Bonjour.
Location	Отображает имя местоположения Bonjour.
SLP Settings	
Enable SLP	Выберите этот параметр для включения функции SLP. Используется для сетевого обнаружения в Epson Scan 2 и EpsonNet Config.
WSD Settings	
Enable WSD	Выберите для включения добавления устройств с помощью WSD, а также печати и сканирования с порта WSD.
Scanning Timeout (sec)	Введите значение времени ожидания связи для сканирования WSD от 3 до 3600 секунд.
Device Name	Отображает имя устройства WSD.
Location	Отображает имя местоположения WSD.
LLTD Settings	
Enable LLTD	Выберите этот параметр для включения LLTD. Сканер отображается на карте сети Windows.
Device Name	Отображает имя устройства LLTD.
LLMNR Settings	
Enable LLMNR	Выберите этот параметр для включения LLMNR. Можно разрешать имена без использования NetBIOS, даже если невозможно использовать DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Выберите этот параметр для включения SNMPv1/v2c. Отображаются только сканеры, поддерживающие SNMPv3.
Access Authority	Установите права доступа, если включен параметр SNMPv1/v2c. Выберите **Read Only** или **Read/Write**.
Community Name (Read Only)	Введите символы ASCII от 0 до 32 (от 0x20 до 0x7E).
Community Name (Read/Write)	Введите символы ASCII от 0 до 32 (от 0x20 до 0x7E).
SNMPv3 Settings	
Enable SNMPv3	Протокол SNMPv3 включен, если установлен флажок.
User Name	Введите от 1 до 32 1-байтовых символов.
Authentication Settings	
Algorithm	Выберите алгоритм проверки подлинности для SNMPv3.

Базовые настройки безопасности

Параметры	Значение и описание параметров
Password	Введите пароль для проверки подлинности SNMPv3. Введите от 8 до 32 символов в ASCII (от 0x20 до 0x7E). Оставьте поле пустым, если не нужно указывать значение.
Confirm Password	Введите выбранный вами пароль для подтверждения.
Encryption Settings	
Algorithm	Выберите алгоритм шифрования для SNMPv3..
Password	Введите пароль для шифрования SNMPv3. Введите от 8 до 32 символов в ASCII (от 0x20 до 0x7E). Оставьте поле пустым, если не нужно указывать значение.
Confirm Password	Введите выбранный вами пароль для подтверждения.
Context Name	Введите не более 32 символов в кодировке Unicode (UTF-8). Оставьте поле пустым, если не нужно указывать значение. Количество символов для ввода зависит от языка.

Соответствующая информация

➡ «Управление протоколами» на стр. 36

➡ «Протоколы, которые можно включить и выключить» на стр. 37

Настройки работы и управления

В этой главе объясняются элементы, связанные с ежедневной работой и управлением устройством.

Проверка сведений об устройстве

Можно проверить следующие сведения об операционной системе в разделе **Status**, используя для этого Web Config.

❏ Product Status

Проверьте язык, статус, номер продукта, MAC-адрес и т. д.

❏ Network Status

Проверьте сведения о состоянии сетевого подключения, IP-адресе, DNS-сервере и т. д.

❏ Panel Snapshot

Отображения снимка экрана панели управления устройства.

❏ Maintenance

Проверьте дату начала, сведения о сканировании и т. д.

❏ Hardware Status

Проверьте состояние сканера.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Управление устройствами (Epson Device Admin)

С помощью Epson Device Admin вы можете управлять любым количеством устройств. Epson Device Admin позволяет управлять устройствами, расположенными в другой сети. Ниже приведены основные функции управления.

Дополнительные сведения о функциях и использовании программного обеспечения см. в документации или в справке по Epson Device Admin.

❏ Обнаружение устройств

Вы можете определять устройства в сети и регистрировать их в списке. Если устройства Epson, такие как принтеры и сканеры, подключены к тому же сегменту сети, что и компьютер администратора, эти устройства можно найти, даже если им не был назначен IP-адрес.

Можно также обнаружить устройства, которые подключены к компьютеру в сети с помощью кабеля USB. Необходимо установить Epson Device USB Agent на компьютере.

❏ Настройка устройств

Можно создать шаблон, содержащий параметры настройки, например сетевой интерфейс и источник бумаги, и применять его к другим устройствам в качестве общих настроек. При подключении к сети можно назначить IP-адрес устройству, которому не был назначен IP-адрес.

❏ Мониторинг устройств

Вы можете регулярно получать данные о состоянии и подробную информацию об устройствах в сети. Можно также отслеживать устройства, которые подключены к компьютерам в сети с помощью кабелей USB, а также устройства других компаний, которые были зарегистрированы в списке устройств. Чтобы отслеживать устройства, подключенные с помощью кабелей USB, необходимо установить Epson Device USB Agent.

❏ Управление оповещениями

Можно отслеживать оповещения о состоянии устройств и расходных материалов. Система автоматически отправляет сообщения эл. почты с уведомлениями администратору на основе заданных условий.

❏ Управление отчетами

Можно создавать регулярные отчеты по мере накопления системой данных по использованию устройства и расходных материалов. Можно сохранить эти созданные отчеты и передать их по электронной почте.

Соответствующая информация

➡ «Epson Device Admin» на стр. 56

Получение уведомлений по электронной почте, когда происходят события

Информация об оповещениях по электронной почте

Эту функцию можно использовать для получения оповещений по электронной почте при возникновении определенных событий. Можно зарегистрировать до 5 адресов электронной почты и выбрать определенные события, по наступлению которых будут отправляться оповещения.

Для использования этой функции необходимо настроить почтовый сервер.

Соответствующая информация

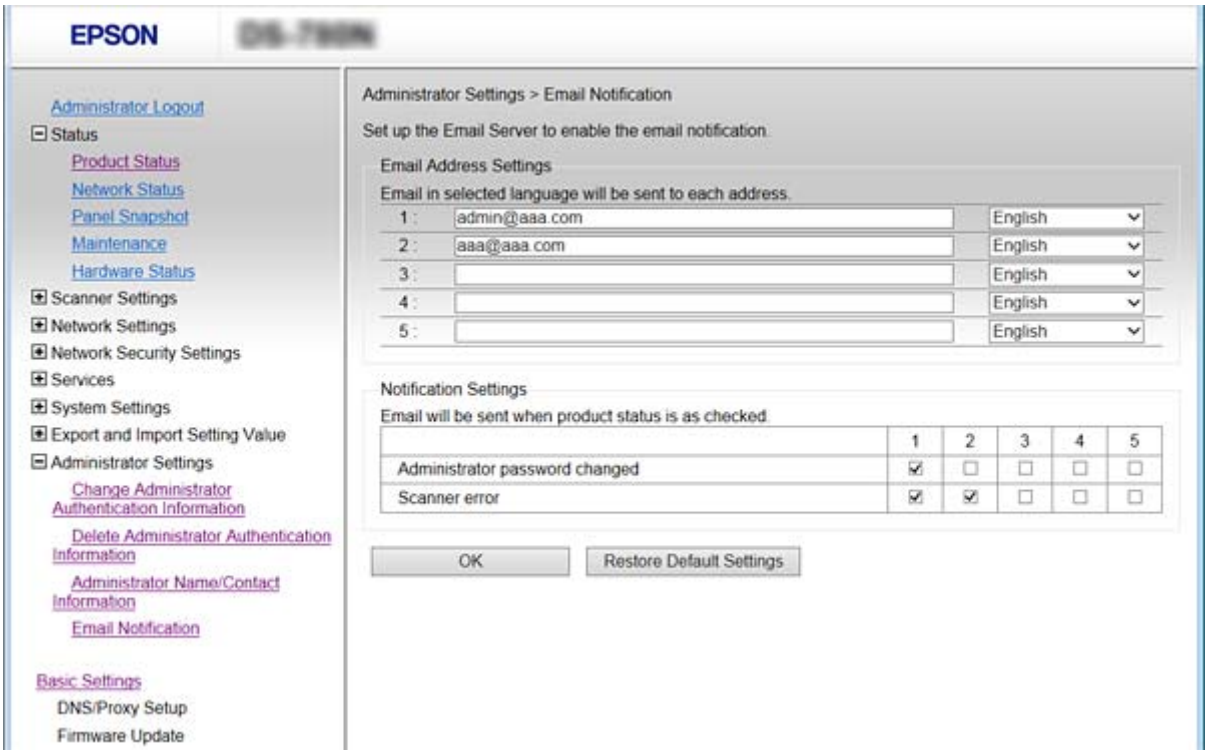
➡ «Настройка почтового сервера» на стр. 43

Настройка оповещений по электронной почте

Для использования этой функции нужно настроить почтовый сервер.

1. Откройте приложение Web Config и выберите **Administrator Settings** > **Email Notification**.
2. Введите адрес электронной почты, на который должны приходить оповещения.
3. Выберите язык оповещений.

4. Установите флажки в соответствии с тем, какие оповещения вы хотели бы получать.



5. Нажмите **OK**.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Настройка почтового сервера» на стр. 43

Настройка почтового сервера

Перед настройкой проверьте следующее.

❏ Сканер подключен к сети.

❏ Сведения о почтовом сервере на компьютере.

1. Откройте приложение Web Config и выберите **Network Settings** > **Email Server** > **Basic**.

2. Введите значение для каждого элемента.

3. Выберите **OK**.

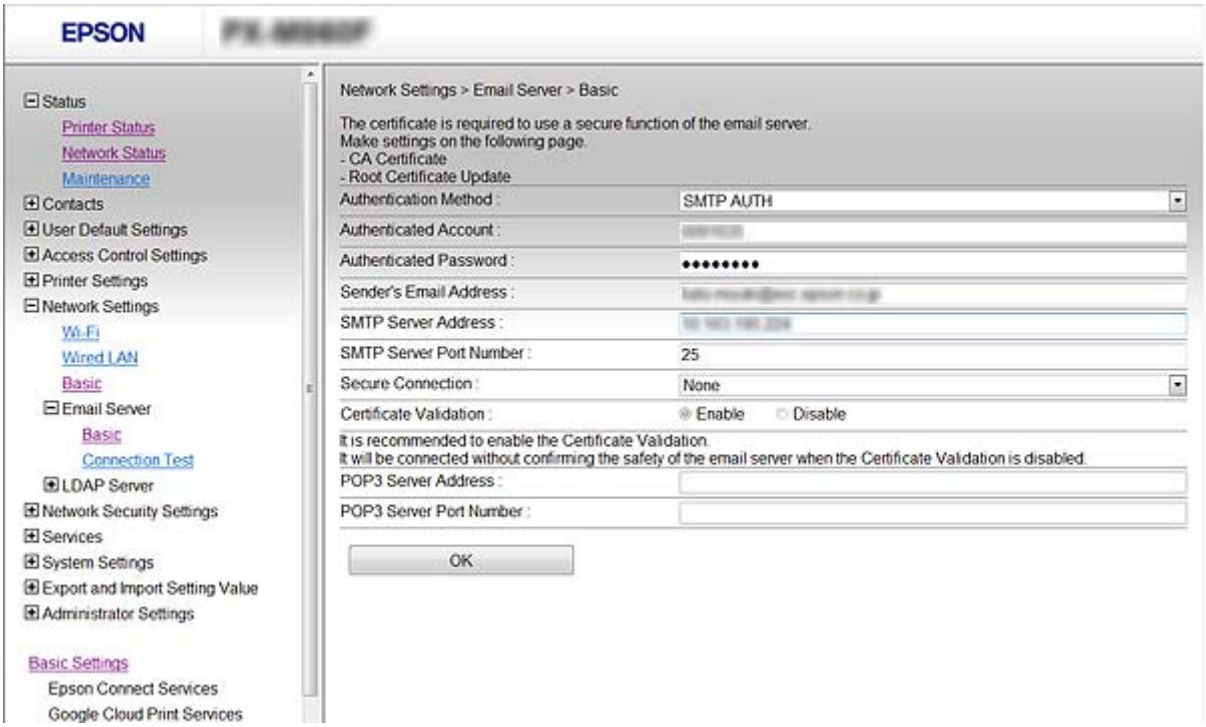
   Отображаются выбранные параметры.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Параметры настройки почтового сервера» на стр. 44

Параметры настройки почтового сервера



Элементы	Настройки и объяснения	
Authentication Method	Укажите метод аутентификации для доступа сканера к почтовому серверу.	
	Off	При обмене данными с сервером электронной почты аутентификация отключена.
	SMTP AUTH	Необходимо, чтобы сервер электронной почты поддерживал аутентификацию SMTP.
	POP before SMTP	Настройка сервера POP3 при выборе этого метода.
Authenticated Account	Если вы выбрали значение **SMTP AUTH** или **POP before SMTP** для параметра **Authentication Method**, введите имя учетной записи, прошедшей проверку подлинности, длиной от 0 до 255 символов ASCII (от 0x20 до 0x7E).	
Authenticated Password	Если вы выбрали значение **SMTP AUTH** или **POP before SMTP** для параметра **Authentication Method**, введите имя учетной записи, прошедшей проверку подлинности, длиной от 0 до 20 символов, используя A–Z, a–z, 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Введите адрес электронной почты отправителя. Введите от 0 до 255 символов ASCII (от 0x20 до 0x7E), за исключением : ( ) < > [ ] ; ¥. Точка «.» не может быть первым символом.	
SMTP Server Address	Введите от 0 до 255 символов, используя A–Z, a–z, 0–9. - . Используйте формат IPv4 или FQDN.	
SMTP Server Port Number	Введите число от 1 до 65535.	

Элементы	Настройки и объяснения	
Secure Connection	Укажите безопасный метод подключения к серверу электронной почты.	
	None	Если выбрать **POP before SMTP** в поле **Authentication Method**, метод подключения будет установлен как **None**.
	SSL/TLS	Это доступно, если параметр **Authentication Method** имеет значение **Off** или **SMTP AUTH**.
	STARTTLS	Это доступно, если параметр **Authentication Method** имеет значение **Off** или **SMTP AUTH**.
Certificate Validation	Сертификат проверяется при включении этой функции. Рекомендуется задать значение **Enable**.	
POP3 Server Address	Если вы выбрали значение **POP before SMTP** для параметра **Authentication Method**, введите адрес сервера POP3 длиной от 0 до 255 символов, используя A–Z, a–z, 0–9 . - . Используйте формат IPv4 или FQDN.	
POP3 Server Port Number	Если значение **POP before SMTP** указано для параметра **Authentication Method**, введите число 1 до 65535.	

Соответствующая информация

➡ «Настройка почтового сервера» на стр. 43

Проверка соединения почтового сервера

1. Откройте приложение Web Config и выберите **Network Settings** > **Email Server** > **Connection Test**.
2. Выберите **Start**.

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

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Пояснения к сообщениям, отображаемым при проверке соединения с почтовым сервером» на стр. 45

Пояснения к сообщениям, отображаемым при проверке соединения с почтовым сервером

Сообщения	Объяснения
Connection test was successful.	Это сообщение отображается, когда соединение с сервером установлено.
SMTP server communication error. Check the following. - Network Settings	Это сообщение отображается в следующих случаях. ❏ Сканер не подключен к сети. ❏ SMTP-сервер не работает. ❏ Сетевое подключение было прервано в процессе передачи данных. ❏ Получены неполные данные.

Настройки работы и управления

Сообщения	Объяснения
POP3 server communication error. Check the following. - Network Settings	Это сообщение отображается в следующих случаях. ❏ Сканер не подключен к сети. ❏ POP3-сервер не работает. ❏ Сетевое подключение было прервано в процессе передачи данных. ❏ Получены неполные данные.
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Это сообщение отображается в следующих случаях. ❏ Произошла ошибка при подключении к DNS-серверу. ❏ Произошла ошибка при разрешении имени SMTP-сервера.
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Это сообщение отображается в следующих случаях. ❏ Произошла ошибка при подключении к DNS-серверу. ❏ Произошла ошибка при разрешении имени POP3-сервера.
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Это сообщение отображается, если произошла ошибка аутентификации на SMTP-сервере.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Это сообщение отображается, если произошла ошибка аутентификации на POP3-сервере.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Это сообщение отображается, если вы пытаетесь связаться по неподдерживаемым протоколам.
Connection to SMTP server failed. Change Secure Connection to None.	Это сообщение отображается при возникновении несоответствия по протоколу SMTP между сервером и клиентом или в том случае, если сервер не поддерживает безопасное подключение по SMTP (SSL-подключение).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Это сообщение отображается при возникновении несоответствия по протоколу SMTP между сервером и клиентом или в том случае, если сервер запрашивает использование подключения по SSL/TLS для установки безопасного подключения SMTP.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Это сообщение отображается при возникновении несоответствия по протоколу SMTP между сервером и клиентом или в том случае, если сервер запрашивает использование подключения по STARTTLS для установки безопасного подключения SMTP.
The connection is untrusted. Check the following. - Date and Time	Это сообщение отображается, если параметры даты и времени сканера являются недопустимыми или истек срок действия сертификата.
The connection is untrusted. Check the following. - CA Certificate	Это сообщение отображается, если сканер не имеет корневого сертификата, соответствующего серверу, или если CA Certificate не был импортирован.
The connection is not secured.	Это сообщение отображается, если полученный сертификат поврежден.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Это сообщение отображается, если возникает несоответствие в методе аутентификации между сервером и клиентом. Сервер поддерживает SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Это сообщение отображается, если возникает несоответствие в методе аутентификации между сервером и клиентом. Сервер не поддерживает SMTP AUTH.

Сообщения	Объяснения
Sender's Email Address is incorrect. Change to the email address for your email service.	Это сообщение отображается, если указан неверный адрес эл. почты отправителя.
Cannot access the product until processing is complete.	Это сообщение отображается, если сканер занят.

Соответствующая информация

➡ «Проверка соединения почтового сервера» на стр. 45

Обновление микропрограммы

Обновление микропрограммы с помощью Web Config

Выполняет обновление микропрограммы с помощью Web Config. Устройство должно быть подключено к Интернету.

1. Откройте Web Config и выберите **Basic Settings** > **Firmware Update**.
2. Нажмите **Start**.

   Запускается подтверждение микропрограммы, после чего отображаются сведения о микропрограмме, если существует обновление микропрограммы.
3. Щелкните **Start** и выполните инструкции на экране.

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

➡ «Доступ к приложению Web Config» на стр. 23
➡ «Epson Device Admin» на стр. 56

Обновление программного обеспечения с использованием Epson Firmware Updater

Вы можете загрузить микропрограмму устройства с веб-сайта Epson на компьютере, а затем подключить устройство и компьютер с помощью кабеля USB для обновления микропрограммы. Если вы не можете выполнить обновление через сеть, воспользуйтесь следующим методом.

1. Получите доступ к веб-сайту и загрузите микропрограмму.
2. Подключите компьютер, который содержит загруженное программное обеспечение, к устройству через кабель USB.

3. Дважды щелкните загруженный файл exe.

   Запускается Epson Firmware Updater.

4. Следуйте инструкциям на экране.

Резервное копирование настроек

Экспорт элементов настройки в Web Config позволяет копировать эти элементы на другие сканеры.

Экспорт настроек

Выполните экспорт каждой настройки для сканера.

1. Откройте приложение Web Config и выберите **Export and Import Setting Value** >**Export**.

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, дупликация 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 **Export**.

   > ***Важно:***
   >
   > *Если необходимо экспортировать сетевые настройки сканера, например имя и IP-адрес сканера, выберите **Enable to select the individual settings of device** и затем выберите дополнительные элементы. Используйте выбранные значения только для сканера на замену.*

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Импорт настроек

Импортируйте экспортированный файл Web Config на сканер.

> ***Важно:***
>
> *При импорте значений, содержащих индивидуальные сведения, например имени или IP-адреса сканера, убедитесь, что в сети нет такого же IP-адреса. При совпадении IP-адресов сканер не отражает это значение.*

1. Откройте приложение Web Config и выберите **Export and Import Setting Value** >**Import**.

2. Выберите экспортированный файл и введите зашифрованный пароль.

3. Нажмите **Next**.
4. Выберите настройки, которые необходимо импортировать, затем нажмите **Next**.
5. Нажмите **OK**.

Настройки будут применены на сканере.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Устранение неполадок

Советы по устранению неполадок

Более подробная информация содержится в следующем руководстве.

❏ Руководство пользователя

Содержит инструкции по эксплуатации сканера, техническому обслуживанию и устранению неполадок.

Проверка журнала сервера и сетевого устройства

В случае возникновения проблем с подключением к сети можно идентифицировать причину, проверив журнал на почтовом сервере, сервере LDAP и т. д., а также проверив состояние с помощью сетевого журнала или журналов и команд такого оборудования, как маршрутизаторы.

Инициализация сетевых настроек

Восстановление сетевых настроек с помощью панели управления

Вы можете выполнить сброс всех настроек сети на значения по умолчанию.

1. Нажмите **Настр.** на главном экране.
2. Нажмите **Администрир. системы** > **Восст. настр. по ум.** > **Настройки сети**.
3. Прочтите сообщение, затем выберите **Да**.
4. После появления предупреждения нажмите **Закрыть**.

   Если вы не нажмете кнопку **Закрыть**, окно автоматически закроется по истечении определенного времени.

Проверка связи между устройствами и компьютерами

Проверка подключения с помощью команды Ping — Windows

Вы можете использовать команду Ping, чтобы убедиться в подключении компьютера к сканеру. Выполните приведенные ниже действия, чтобы проверить подключение с помощью команды Ping.

1. Проверьте IP-адрес сканера, соединение с которым хотите проверить.

   Проверку можно выполнить с помощью Epson Scan 2.

2. Запуск командной строки на компьютере.

   ❏ Windows 10

   Щелкните правой кнопкой мыши кнопку «Пуск» или нажмите ее и удерживайте, затем выберите **Командная строка**.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Запустите экран приложения и выберите **Командная строка**.

   ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 или более ранняя версия

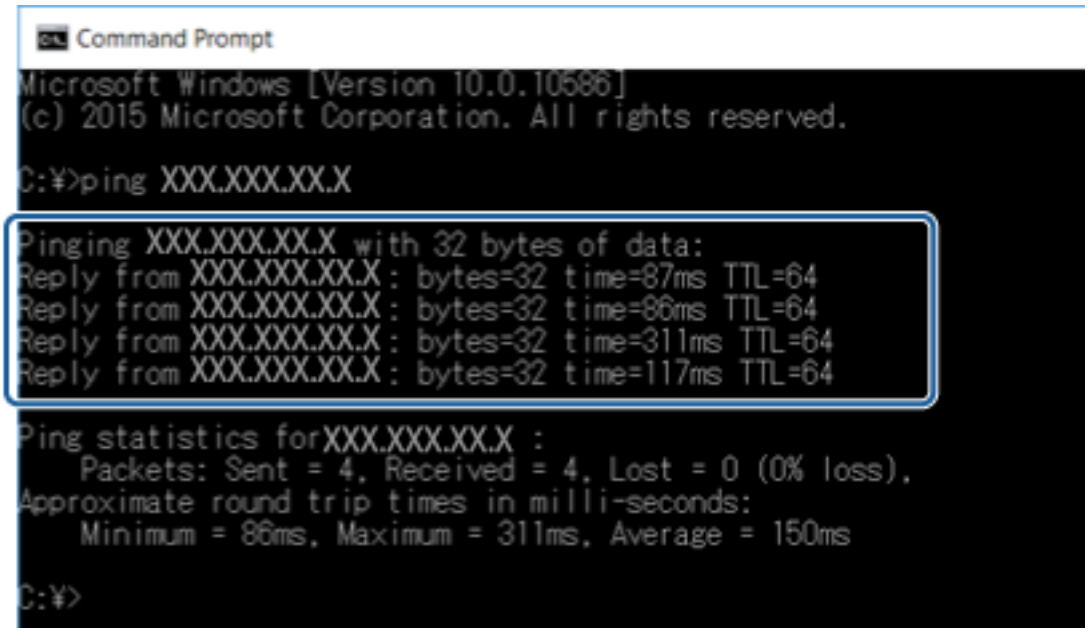
   Щелкните кнопку «Пуск», выберите **Все программы** или **Программы** > **Стандартные** > **Командная строка**.

3. Введите «ping xxx.xxx.xxx.xxx» и нажмите клавишу «Ввод».

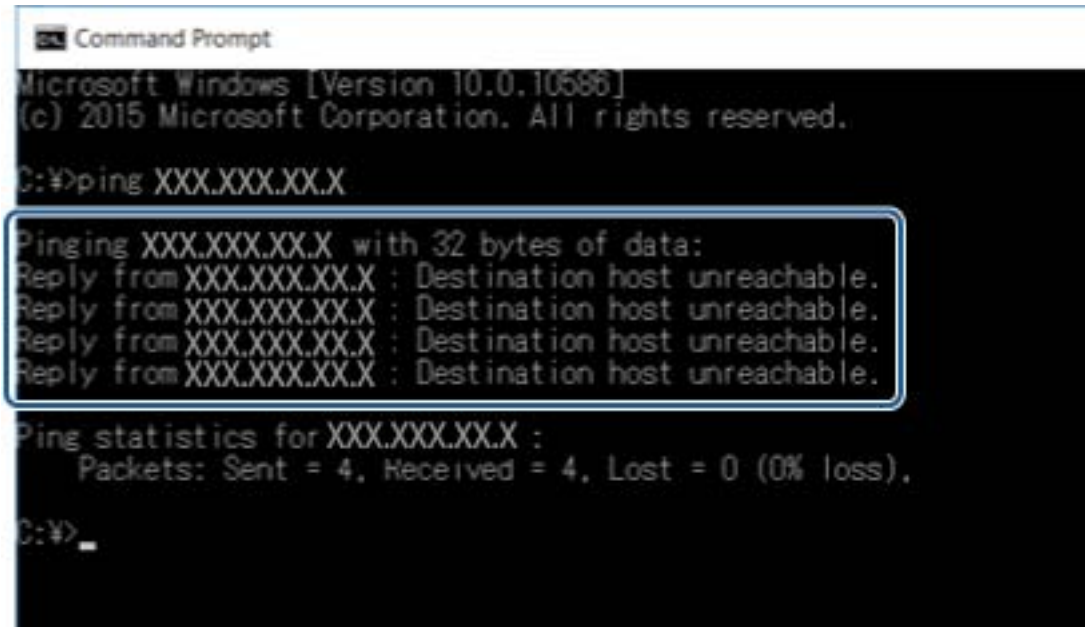
   Вместо «xxx.xxx.xxx.xxx» введите IP-адрес сканера.

4. Проверьте состояние соединения.

   Если обмен данными между компьютером и сканером происходит, появится следующее сообщение.



Если обмен данными между компьютером и сканером не происходит, появится следующее сообщение.



Проверка подключения с помощью команды Ping — Mac OS

Вы можете использовать команду Ping, чтобы убедиться в подключении компьютера к сканеру. Выполните приведенные ниже действия, чтобы проверить подключение с помощью команды Ping.

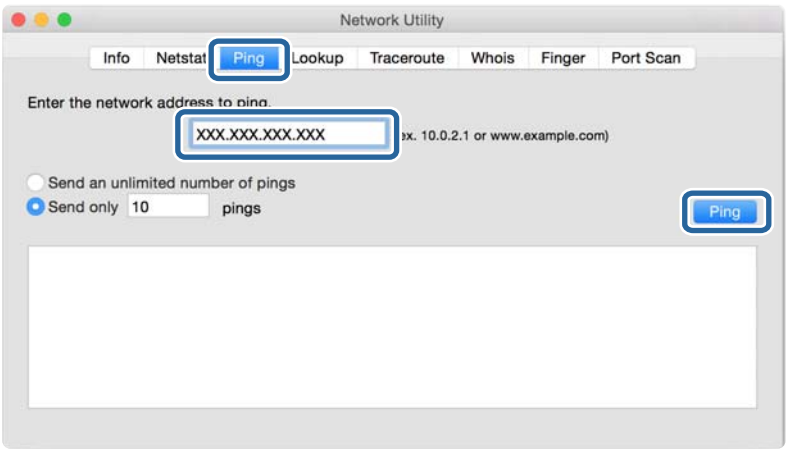
1. Проверьте IP-адрес сканера, соединение с которым хотите проверить.

   Проверку можно выполнить с помощью Epson Scan 2.

2. Запустите программу Network Utility.

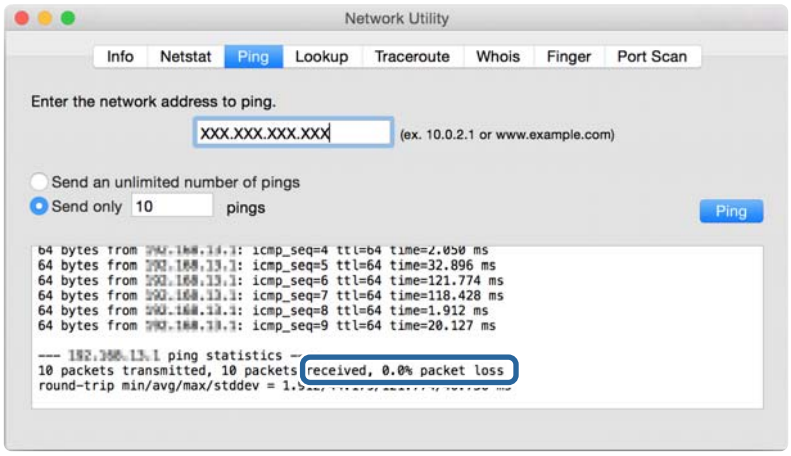
   Введите Network Utility в **Spotlight**.

3. Щелкните по вкладке **Ping**, введите проверяемый IP-адрес из шага 1 и щелкните **Ping**.

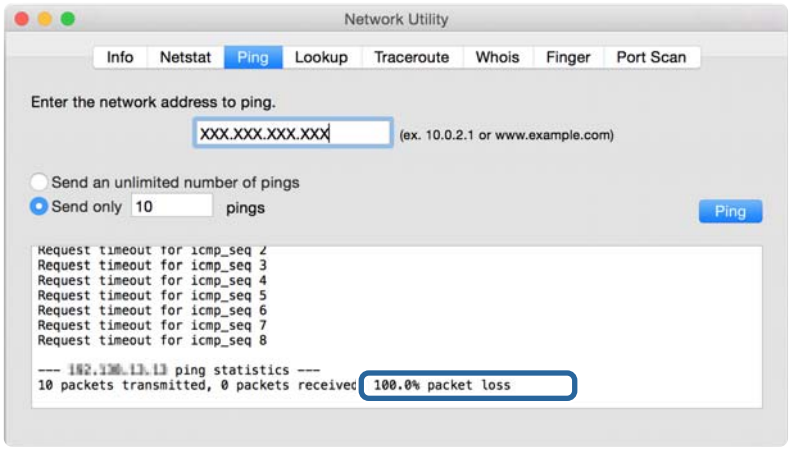


4. Проверьте состояние соединения.

   Если обмен данными между компьютером и сканером происходит, появится следующее сообщение.



   Если обмен данными между компьютером и сканером не происходит, появится следующее сообщение.



Неполадки при использовании программного обеспечения сети.

Не удается получить доступ к Web Config

Правильно ли настроен IP-адрес сканера?

Укажите IP-адрес с помощью Epson Device Admin или EpsonNet Config.

Поддерживает ли ваш браузер массовое шифрование Encryption Strength для SSL/TLS?

Алгоритмы массового шифрования Encryption Strength для SSL/TLS приведены ниже. К приложению Web Config можно получить доступ только через браузер, поддерживающий следующие алгоритмы массового шифрования. Проверьте, поддерживает ли браузер такое шифрование.

❏ 80 бит: AES256/AES128/3DES

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

Сообщение «Устарело» отображается при доступе к Web Config с использованием SSL-соединения (https).

Если сертификат устарел, то получите сертификат заново. Если сообщение отображается до истечения срока годности, то убедитесь, что дата на сканере настроена правильно.

Сообщение «Имя сертификата безопасности не совпадает…» отображается при доступе к Web Config с использованием SSL-соединения (https).

IP-адрес сканера, введенный для параметра **Common Name** для самозаверяющего сертификата или CSR, не совпадает с адресом, введенным в браузере. Получите и импортируйте сертификат заново или измените имя сканера.

Доступ к сканеру осуществляется через прокси-сервер.

При использовании прокси-сервера для сканера требуется выполнить настройки прокси-сервера в браузере.

- ❏ Windows

  Выберите **Панель управления** > **Сеть и Интернет** > **Свойства обозревателя** > **Подключения** > **Настройка сети** > **Прокси-сервер**, а затем отключите использование прокси-сервера для локальных адресов.

- ❏ Mac OS

  Выберите **Системные настройки** > **Сеть** > **Дополнительно** > **Прокси**, зарегистрируйте локальный адрес для **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

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Назначение IP-адреса» на стр. 15

➡ «Назначение IP-адресов с помощью EpsonNet Config» на стр. 57

Название модели и/или IP-адрес не отображаются в EpsonNet Config.

Был ли выбран вариант "Блокировать", "Отмена" или "Закрыть", когда на экране отобразилось важное уведомление Windows или окно брандмауэра?

При выборе **Блокировать**, **Отмена** или **Закрыть**, IP-адрес или имя модели не будут отображены в EpsonNet Config или EpsonNet Setup.

Для исправления этой проблемы зарегистрируйте EpsonNet Config в виде исключения, используя брандмауэр Windows и защитное программное обеспечение. При использовании антивируса или программы защиты закройте их, а затем попробуйте использовать EpsonNet Config.

Задано ли слишком малое время ожидания ошибки связи?

Запустите EpsonNet Config принтера и выберите **Tools** > **Options** > **Timeout**, а затем увеличьте значение времени для настройки **Communication Error**. Обратите внимание, что это может замедлить запуск EpsonNet Config.

Соответствующая информация

➡ «Запуск EpsonNet Config — Windows» на стр. 57

➡ «Запуск EpsonNet Config — Mac OS» на стр. 57

Приложение.

Введение в сетевое программное обеспечение

Ниже описано программное обеспечение, которое позволяет настраивать и управлять устройствами.

Epson Device Admin

Epson Device Admin — приложение, позволяющее выполнять установку устройств в сети, настраивать устройства и управлять ими. Вы можете получать подробные сведения об устройствах, например их состояние и расходные материалы, отправлять уведомления о предупреждениях и создавать отчеты об использовании устройств. Можно также создать шаблон, содержащий параметры настройки, и применять его к другим устройствам в качестве общих настроек. Вы можете загрузить приложение Epson Device Admin с веб-сайта поддержки Epson. Подробную информацию см. в документации или справке по Epson Device Admin.

Запуск Epson Device Admin (только Windows)

Выберите **Все программы** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Примечание:
Разрешите доступ для Epson Device Admin, если появляется предупреждение брандмауэра.

EpsonNet Config

Приложение EpsonNet Config позволяет администратору настраивать такие сетевые параметры сканера, как присвоение IP-адресов и изменение режима подключения. Функция пакетной настройки поддерживается в ОС Windows. Подробную информацию см. в документации или справке по EpsonNet Config.

Запуск EpsonNet Config — Windows

Выберите **Все программы** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Примечание:
Разрешите доступ для EpsonNet Config, если появляется предупреждение брандмауэра.

Запуск EpsonNet Config — Mac OS

Нажмите **Перейти** > **Приложения** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager — приложение для создания пакета для простой установки сканера, например установки и настройки драйвера сканера и установки программы Document Capture Pro. Данное программное обеспечение позволяет администратору создавать уникальные программные пакеты и распределять их между группами.

Для получения дополнительной информации перейдите на региональный веб-сайт Epson.

Назначение IP-адресов с помощью EpsonNet Config

Можно назначить IP-адрес сканеру с помощью EpsonNet Config. EpsonNet Config позволяет назначить IP-адрес для сканера без назначенного IP-адреса после подключения кабеля Ethernet.

Назначение IP-адреса с помощью пакетных настроек

Создание файла для пакетных настроек

Используя MAC-адрес и имя модели в качестве ключей, можно создать новый файл SYLK для настройки IP-адреса.

1. Откройте приложение для работы с электронными таблицами (например, Microsoft Excel) или текстовый редактор.

2. Введите Info_MACAddress, Info_ModelName и TCPIP_IPAddress в первой строке для определения названий элементов.

   Введите элементы настройки для следующих текстовых строк. Вследствие разделения между верхним и нижним регистром, а также двухбайтовыми и однобайтовыми символами разница даже в одном символе приведет к невозможности распознания элемента.

   Введите название настройки, как показано ниже; в противном случае EpsonNet Config не сможет распознать элементы настройки.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Введите MAC-адрес, название модели и IP-адрес для каждого сетевого интерфейса.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Введите имя и сохраните в качестве SYLK-файла (*.slk).

Внесение пакетных изменений с помощью файла конфигурации

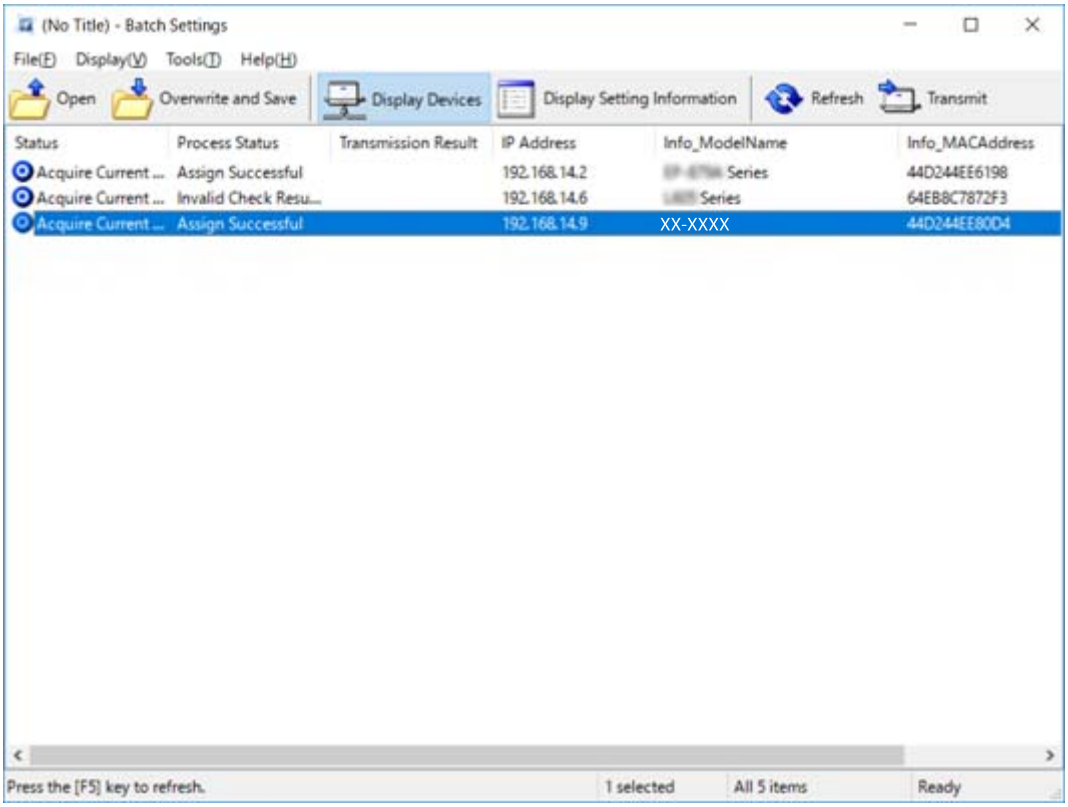
Назначьте IP-адреса в файле конфигурации (SYLK-файл) одновременно. Необходимо создать файл конфигурации перед его назначением.

1. Подключите все устройства к сети с помощью кабелей Ethernet.
2. Включите сканер.
3. Запустите EpsonNet Config.

   Отображается список сканеров в сети. На их отображение может потребоваться некоторое время.
4. Щелкните **Tools** > **Batch Settings**.
5. Нажмите **Open**.
6. На экране выбора файлов вберите SYLK-файл (*.slk), содержащий настройки, затем щелкните **Open**.

7. Выберите устройства, для которых необходимо выполнить пакетные настройки, используя для этого столбец **Status**, установленный в значение **Unassigned**, и столбец **Process Status**, установленный в значение **Assign Successful**.

   При внесении нескольких изменений нажмите Ctrl или Shift, затем щелкните мышкой или перетащите ее.



8. Нажмите **Transmit**.

9. При отображении экрана входа введите пароль, затем щелкните **OK**.

   Выполните передачу настроек.

   Примечание:
   Информация передается на сетевой интерфейс до завершения операции. Не отключайте устройство или беспроводной адаптер и не передавайте какие-либо данные на устройство.

10. На экране **Transmitting Settings** щелкните **OK**.

11. Проверьте состояние настроенного устройства.

    Для устройств, которые отображают  или  проверьте содержимое файла настроек и надлежащую перезагрузку устройства.

Значок	Status	Process Status	Объяснения
	Setup Complete	Setup Successful	Настройка завершается без ошибок.
	Setup Complete	Rebooting	Если информация была передана, каждое устройство должно быть перезагружено для включения настроек. Выполняется проверка для определения, можно ли подключить устройство после перезагрузки.
	Setup Complete	Reboot Failed	Не удается проверить устройство после переноса настроек. Убедитесь, что устройство включено и что оно перезапустилось без ошибок.
	Setup Complete	Searching	Поиск устройства, отмеченного в файле настроек*.
	Setup Complete	Search Failed	Не удается проверить устройства, которые уже были настроены. Убедитесь, что устройство включено и что оно перезапустилось без ошибок*.

    * Только при отображении сведений о настройке.

Соответствующая информация

➡ «Запуск EpsonNet Config — Windows» на стр. 57

➡ «Запуск EpsonNet Config — Mac OS» на стр. 57

Назначение IP-адреса для каждого устройства

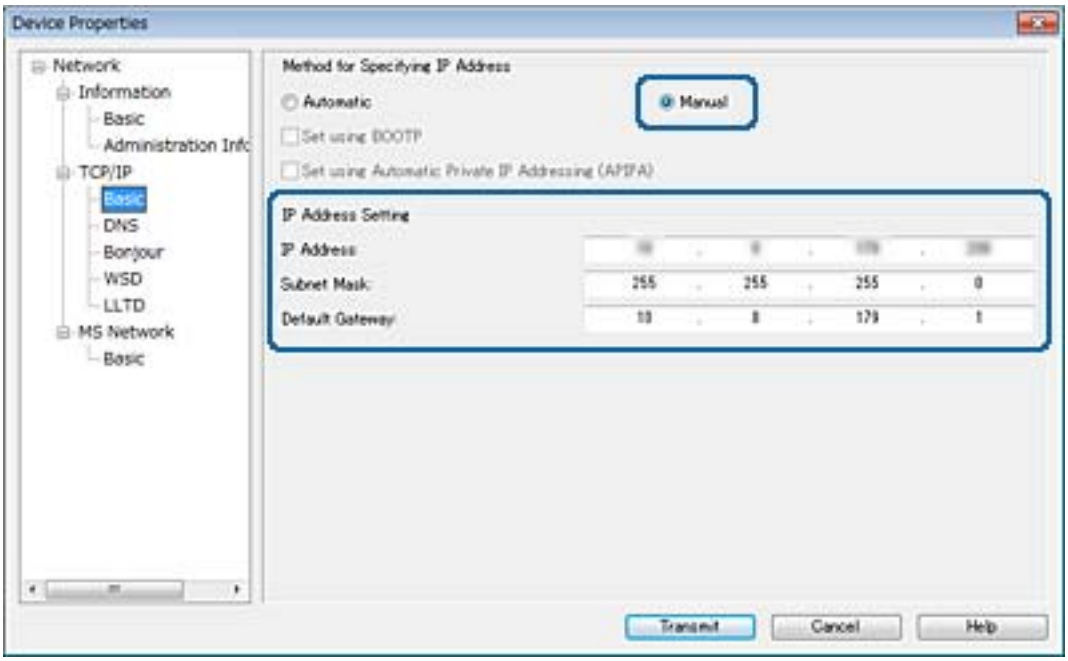
Назначение IP-адреса сканеру с использованием EpsonNet Config.

1. Включите сканер.
2. Подключите сканер к сети с помощью кабеля Ethernet.
3. Запустите EpsonNet Config.

   Отображается список сканеров в сети. На их отображение может потребоваться некоторое время.
4. Дважды щелкните сканер, для которого необходимо выполнить назначение.

   Примечание:
   При подключении нескольких сканеров одной модели можно определить сканер по MAC-адресу.
5. Выберите **Network** > **TCP/IP** > **Basic**.

6. Введите адреса для **IP Address**, **Subnet Mask** и **Default Gateway**.



Примечание:
Введите статический адрес при подключении сканера к безопасной сети.

7. Нажмите **Transmit**.

   Отображается экран, подтверждающий передачу информации.

8. Нажмите **OK**.

   Отображается экран, подтверждающий завершение передачи.

   Примечание:
   Информация передается на устройство, после чего отображается сообщение «Конфигурация успешно завершена». Не отключайте устройство и не передавайте какие-либо данные в службу.

9. Нажмите **OK**.

Соответствующая информация

➡ «Запуск EpsonNet Config — Windows» на стр. 57

➡ «Запуск EpsonNet Config — Mac OS» на стр. 57

Использование порта сканера

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

Приложение.

Отправитель (клиент)	Использование	Получатель (сервер)	Протокол	Номер порта
Сканер	Отправка электронной почты (уведомление по эл. почте)	SMTP-сервер	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	Подключение POP перед SMTP (уведомление по эл. почте	POP-сервер	POP3 (TCP)	110
	Управление WSD	Клиентский компьютер	WSD (TCP)	5357
	Поиск компьютера при сканировании по технологии push из программы Document Capture Pro	Клиентский компьютер	Обнаружение устройств, поддерживающих сканирование по технологии Push	2968
	Сбор сведений при сканировании в Document Capture Pro с использованием технологии Push	Клиентский компьютер	Сканирование в сети с использованием технологии Push	2968
Клиентский компьютер	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
	Пересылка данных сканирования из Document Capture Pro	Сканер	Сканирование сети (TCP)	1865

Расширенные настройки безопасности для предприятия

В этой главе описываются расширенные функции безопасности.

Настройки безопасности и предотвращение опасных ситуаций

Если устройство подключено к сети, можно зайти на него с удаленного местоположения. Кроме того, многие люди могут совместно использовать устройство, что позволяет повысить эффективность и удобство работы. Однако увеличиваются такие риски, как незаконный доступ, нелегальное использование и взлом данных. При использовании устройства в среде, где есть доступ к Интернету, риски растут еще больше.

Во избежание этих рисков устройства Epson оснащены различными технологиями безопасности.

Настройте устройство надлежащим образом в соответствии с условиями окружающей среды, которые были сформированы на основе информации, указанной клиентом.

Название	Тип функции	Что определять	Что предотвращать
Соединение SSL/TLS	Канал связи между компьютером и устройством шифруется с помощью SSL/TLS. Содержимое передаваемых через браузер данных защищено.	Укажите на устройстве сертификат ЦС для сервера, то есть сертификат, подписанный центром сертификации.	Предотвратите утечку информации о настройках и содержимого передаваемых данных на сканер с компьютера. Доступ к серверу Epson в Интернете с устройства также может быть защищен с помощью обновления микропрограммы и т. д.
IPsec/фильтрация IP	Вы можете настроить разделение и обрезку данных, которые поступают с определенного клиента определенного типа. Так как IPsec защищает данные в IP-пакетах (шифрование и проверка подлинности), можно безопасно связывать незащищенный протокол сканирования.	Создайте базовую политику и индивидуальную политику для настройки клиента или типа данных, которые могут передаваться на устройство.	Обеспечьте защиту от неавторизованного доступа, а также взлома и перехвата данных на канале связи с устройством.
SNMPv3	Добавлены такие функции, как мониторинг подключенных устройств в сети, целостность данных на протоколе SNMP для контроля, шифрования проверки подлинности пользователей и т. д.	Включите SNMPv3, затем задайте метод проверки подлинности и шифрования.	Обеспечение изменения настроек в сети и конфиденциальности при мониторинге состояния.

Расширенные настройки безопасности для предприятия

Название	Тип функции	Что определять	Что предотвращать
IEEE802.1X	Позволяет подключаться только пользователю, который прошел проверку подлинности в сети Ethernet. Позволяет использовать устройство только пользователю, имеющему надлежащие права.	Настройка проверки подлинности на сервере RADIUS (сервер проверки подлинности).	Защита от неавторизованного доступа и использования устройства.
Чтение карты идентификации	Устройством можно пользоваться только после поднесения карты идентификации к подключенному устройству проверки подлинности. Можно ограничить получение журналов для каждого пользователя и устройства, а также ограничить доступное использование устройств и функций для каждого пользователя и группы.	Подключите устройство проверки подлинности к данному устройству, а затем настройте сведения о пользователе в системе проверки подлинности.	Предотвратите неавторизованное использование устройства и его спуфинг.

Соответствующая информация

- «Связь со сканером через SSL/TLS» на стр. 64
- «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 72
- «Использование протокола SNMPv3» на стр. 84
- «Подключение сканера к сети IEEE802.1X» на стр. 86

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.

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.

О цифровом сертификате

❏ Сертификат подписан центром сертификации.

От центра сертификации нужно получить сертификат, подписанный ЦС. Обеспечить безопасное соединение можно, используя сертификат, подписанный ЦС. Сертификат, подписанный ЦС, можно использовать для всех функций безопасности.

❏ Сертификат ЦС

Сертификат ЦС свидетельствует о том, что третья сторона подтвердила идентичность сервера. Это является ключевым компонентом в безопасности «сети доверия» (web of trust). Для проверки подлинности сервера получите сертификат ЦС в центре сертификации.

❏ Самозаверяющий сертификат

Самозаверяющий сертификат представляет собой сертификат, выпущенный и подписанный сканером. Этот сертификат является недостоверным и не гарантирует предотвращения спуфинга. При использовании данного сертификата для сертификации SSL/TLS в браузере могут отображаться оповещения системы безопасности. Данный сертификат можно использовать только для соединений SSL/TLS.

Соответствующая информация

➡ «Получение и импорт сертификата, подписанного ЦС» на стр. 65

➡ «Удаление сертификата, подписанного ЦС» на стр. 69

➡ «Обновление самозаверяющего сертификата» на стр. 69

Получение и импорт сертификата, подписанного 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. Откройте приложение Web Config и выберите **Network Security Settings**. Далее выберите **SSL/TLS** > **Certificate**, или **IPsec/IP Filtering** > **Client Certificate**, или **IEEE802.1X** > **Client Certificate**.

2. Нажмите **Generate 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 **Network Security Settings**. Далее выберите **SSL/TLS** > **Certificate**, или **IPsec/IP Filtering** > **Client Certificate**, или **IEEE802.1X** > **Client Certificate**.

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 CA-signed Certificate может оказаться невозможным.*

7. Отправьте CSR в центр сертификации и получите CA-signed Certificate.

   Соблюдайте метод и форму отправки, установленные каждым центром сертификации.

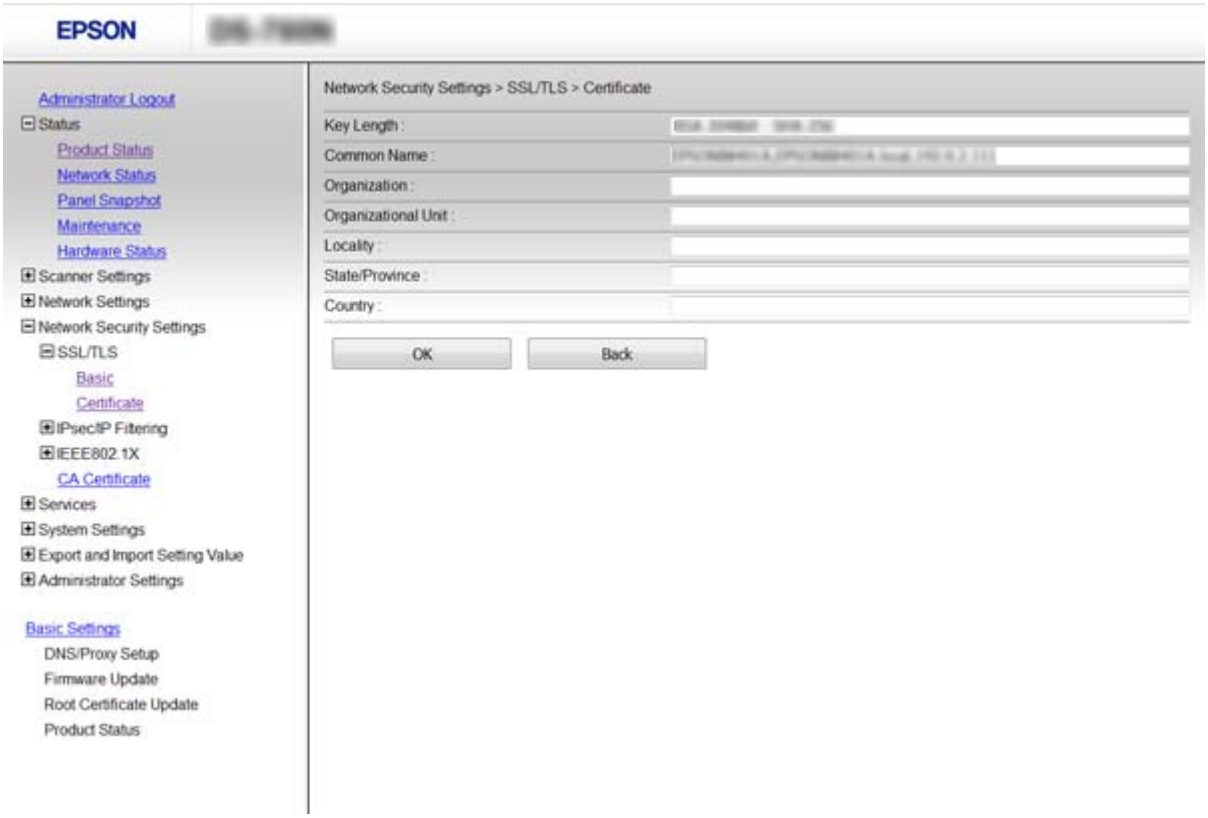
8. Сохраните полученный CA-signed Certificate на компьютере, подключенном к сканеру.

   Процедура получения CA-signed Certificate будет завершена при сохранении сертификата получателем.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23
➡ «Параметры настройки CSR» на стр. 66
➡ «Импорт сертификата, подписанного ЦС» на стр. 67

Параметры настройки CSR



Параметры	Настройки и объяснения
Key Length	Выберите длину ключа для CSR.
Common Name	Длина может составлять от 1 до 128 символов. Если это IP-адрес, то он должен быть статическим. Пример: URL для доступа к Web Config: https://10.152.12.225 Общее имя: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Введите от 0 до 64 символов в ASCII (от 0x20 до 0x7E). Различающиеся имена (CN) можно отделять запятыми.
Country	Введите код страны как двузначное число по стандарту ISO 3166.

Соответствующая информация

➡ «Получение сертификата, подписанного ЦС» на стр. 65

Импорт сертификата, подписанного ЦС

Важно:

❏ *Убедитесь, что дата и время сканера установлены правильно.*

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

1. Откройте приложение Web Config и выберите **Network Security Settings**. Далее выберите **SSL/TLS** > **Certificate**, или **IPsec/IP Filtering** > **Client Certificate**, или **IEEE802.1X** > **Client Certificate**.

2. Нажмите **Import**.

   Отображается страница импорта сертификата.

3. Введите значение для каждого элемента.

   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.

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

   ❏ **Password**: не настраивайте.

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

   ❏ Сертификат формата PEM/DER получен от компьютера.

   ❏ **Private Key**: установите.

   ❏ **Password**: не настраивайте.

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

❏ Сертификат формата PKCS#12 получен от компьютера.

❏ **Private Key**: не настраивайте.

❏ **Password**: необязательно.

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

4. Нажмите **OK**.

Отображается сообщение о завершении.

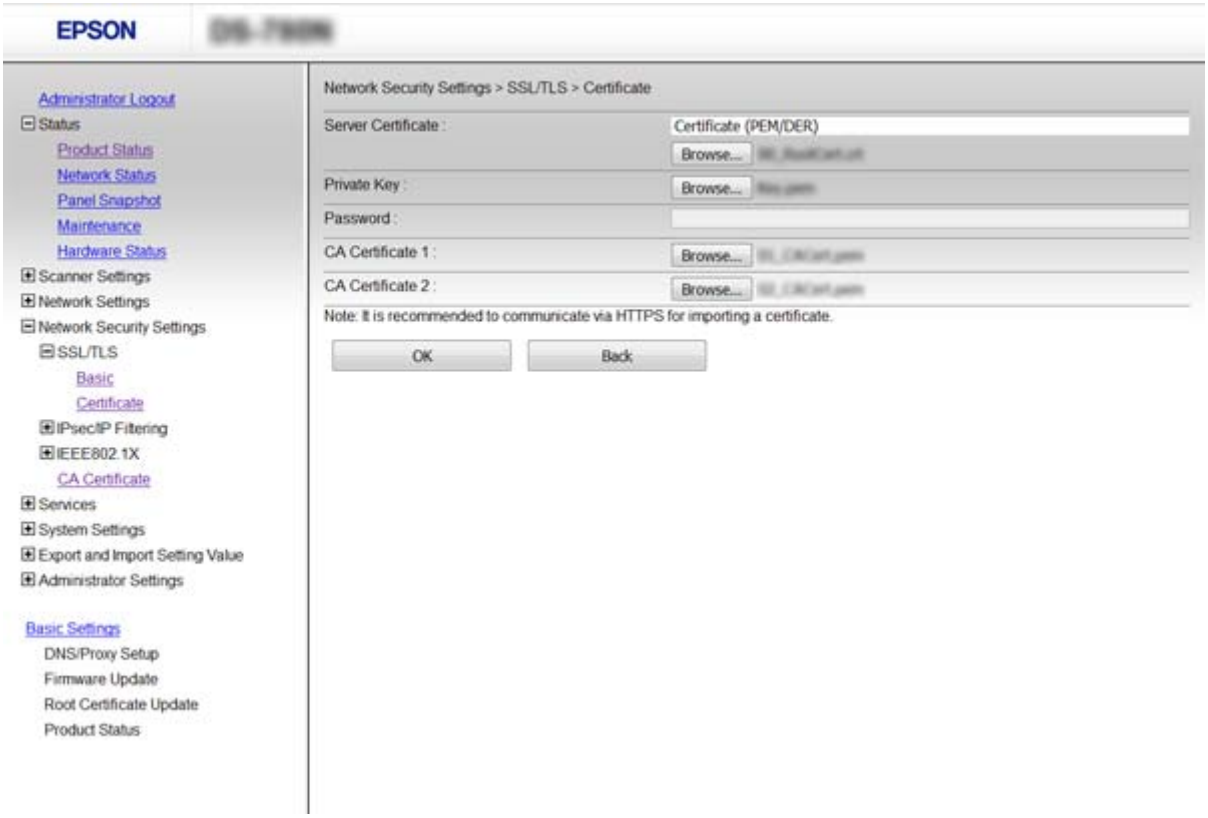
Примечание:
*Нажмите **Confirm** для проверки информации о сертификате.*

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Параметры настройки импорта сертификата, подписанного ЦС» на стр. 68

Параметры настройки импорта сертификата, подписанного ЦС



Параметры	Параметры и объяснения
Server Certificate или Client Certificate	Выберите формат сертификата.
Private Key	Если получен сертификат в формате PEM/DER с помощью запроса CSR, созданного на компьютере, необходимо указать файл секретного ключа, который соответствует сертификату.
Password	Введите пароль для шифрования секретного ключа.

Параметры	Параметры и объяснения
CA Certificate 1	Если сертификат имеет формат **Certificate (PEM/DER)**, то импортируйте сертификат ЦС, который выдает сертификат сервера. Укажите файл, если необходимо.
CA Certificate 2	Если сертификат имеет формат **Certificate (PEM/DER)**, то импортируйте сертификат ЦС, который выдает сертификат **CA Certificate 1**. Укажите файл, если необходимо.

Соответствующая информация

➡ «Импорт сертификата, подписанного ЦС» на стр. 67

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. Откройте приложение Web Config и выберите **Network Security Settings**. Далее выберите **SSL/TLS** > **Certificate**, или **IPsec/IP Filtering** > **Client Certificate**, или **IEEE802.1X** > **Client Certificate**.
2. Нажмите **Delete**.
3. В отображаемом сообщении подтвердите удаление сертификата.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Обновление самозаверяющего сертификата

Самозаверяющий сертификат можно обновить, если сканер поддерживает функцию HTTPS-сервера. При доступе к Web Config с использованием самозаверяющего сертификата отобразится предупреждение.

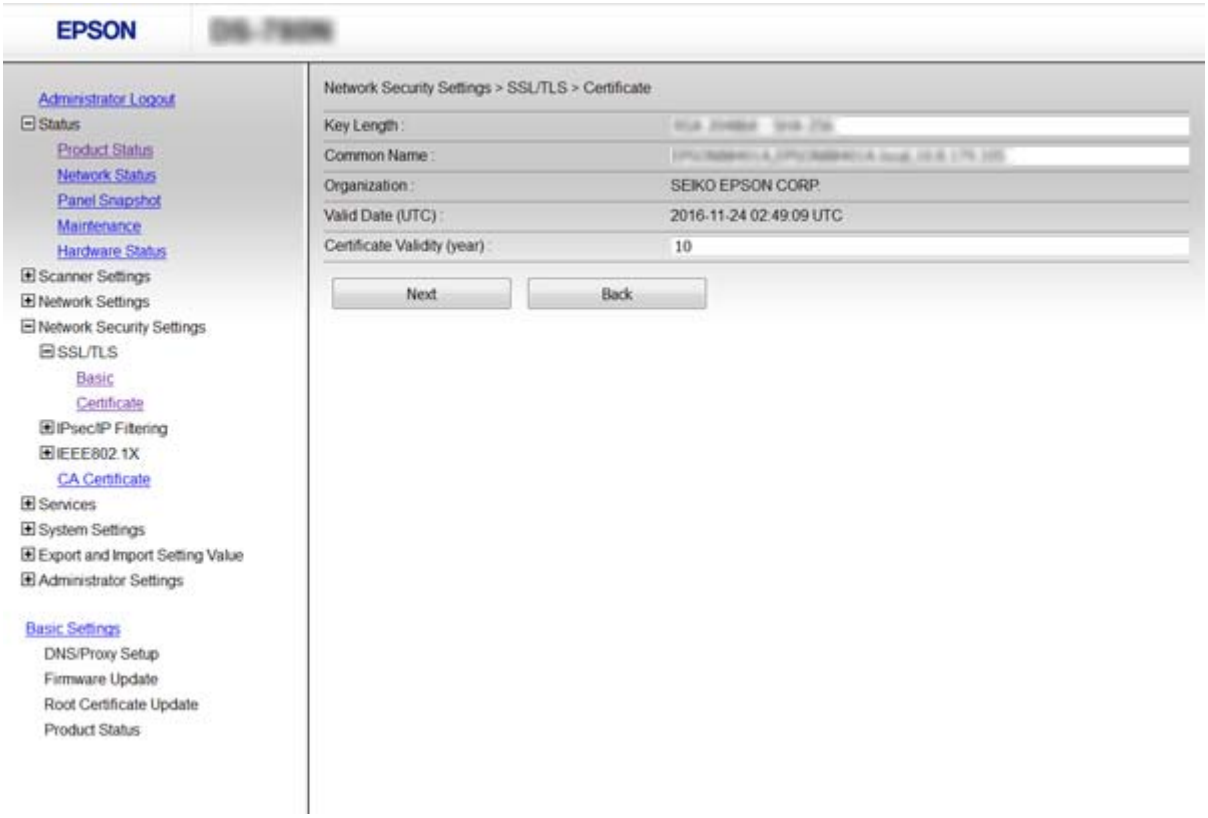
Используйте самозаверяющий сертификат временно, пока не получите и не импортируете сертификат, подписанный ЦС.

1. Откройте приложение Web Config и выберите **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Нажмите **Update**.
3. Введите **Common Name**.

   Введите IP-адрес или идентификатор, такой как имя FQDN для сканера. Длина может составлять от 1 до 128 символов.

   Примечание:
   Отличительное имя (CN) можно отделять запятыми.

4. Укажите срок действия сертификата.



5. Нажмите **Next**.

   Отображается запрос подтверждения.

6. Нажмите **OK**.

   Настройки сканера обновлены.

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

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Настройка CA Certificate

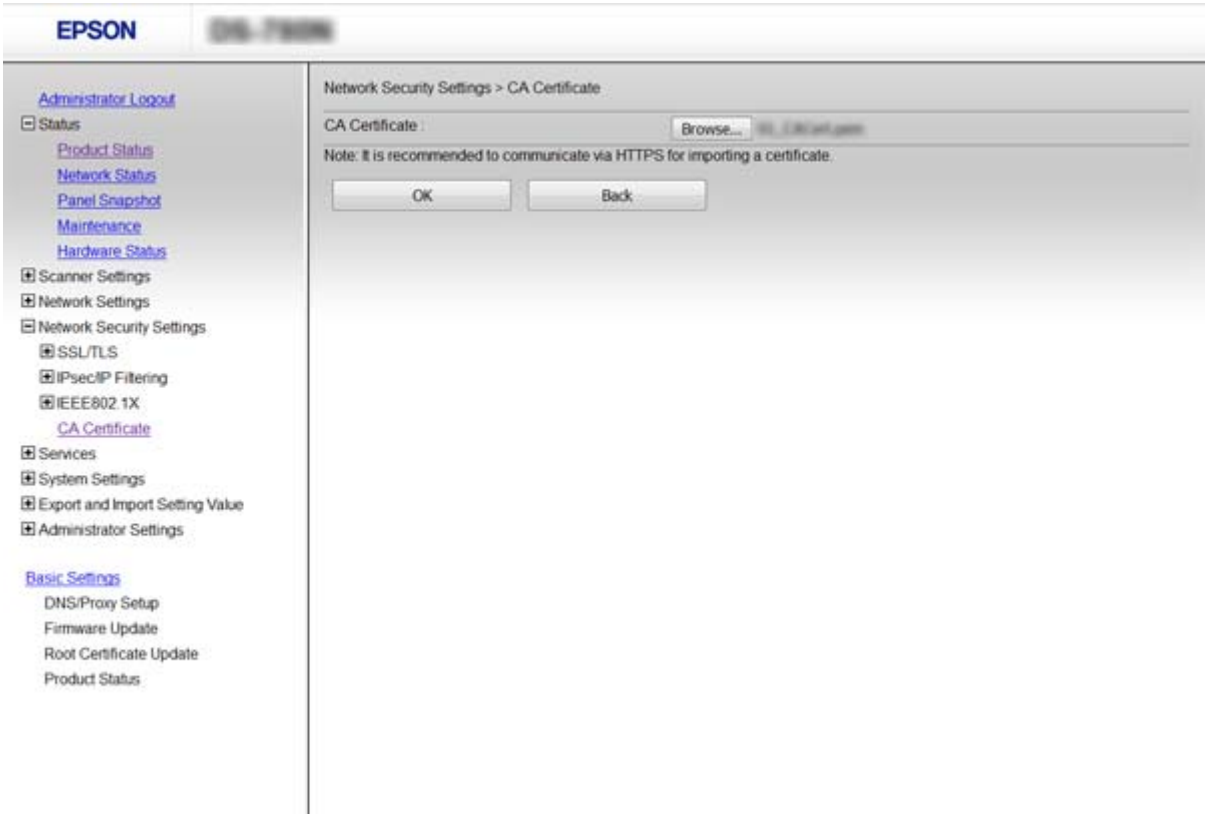
Можно импортировать, отобразить или удалить CA Certificate.

Импорт CA Certificate

1. Откройте приложение Web Config и выберите **Network Security Settings** > **CA Certificate**.

2. Нажмите **Import**.

3. Укажите CA Certificate, который необходимо импортировать.



4. Нажмите **OK**.

После завершения импорта вы вернетесь на экран **CA Certificate**, где будет отображаться импортированный CA Certificate.

Соответствующая информация

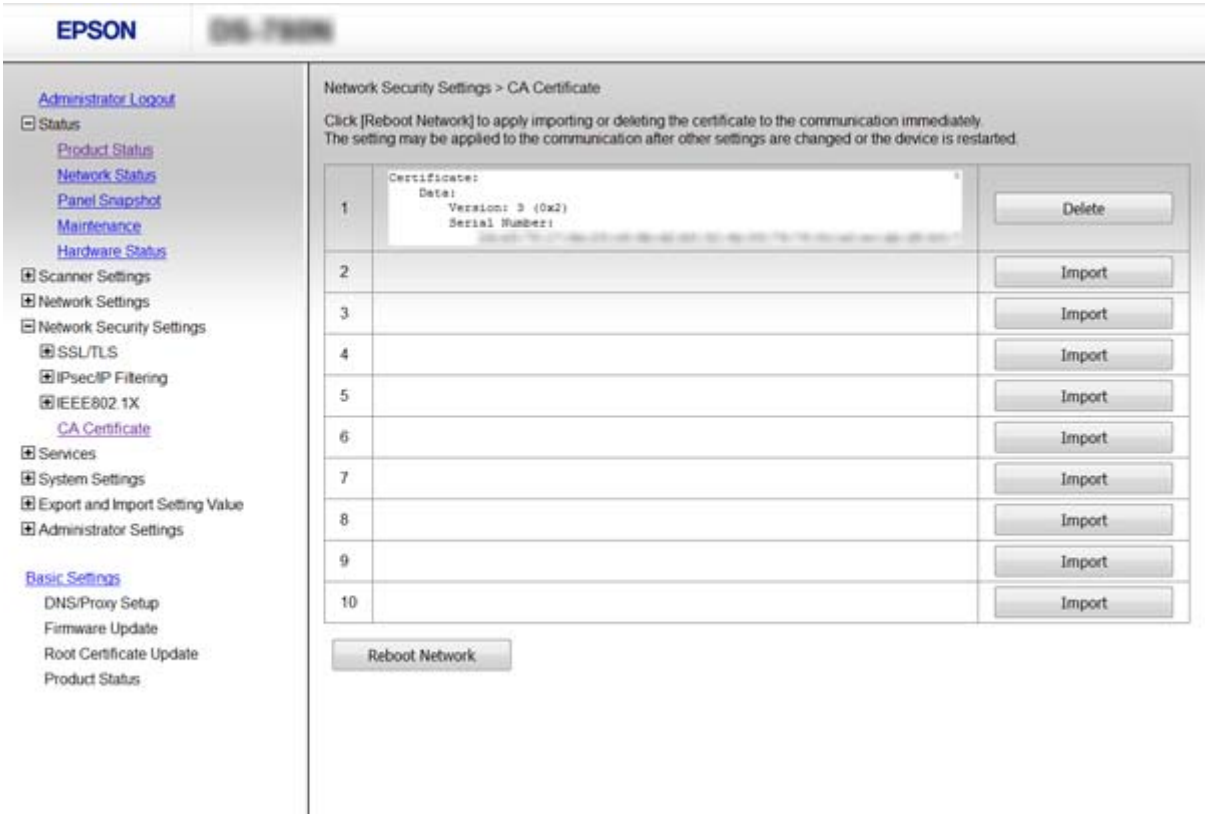
➡ «Доступ к приложению Web Config» на стр. 23

Удаление CA Certificate

Можно удалить импортированный CA Certificate.

1. Откройте приложение Web Config и выберите **Network Security Settings** > **CA Certificate**.

2. Щелкните **Delete** рядом с CA Certificate, который необходимо удалить.



3. В отображаемом сообщении подтвердите удаление сертификата.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Шифрованный канал связи с использованием IPsec/фильтрации IP

Сведения о IPsec/IP Filtering

Если сканер поддерживает протоколы IPsec/IP-фильтрации, можно осуществлять фильтрацию трафика по IP-адресам, службам и по порту. Сканер можно настроить на прием или блокировку определенных клиентов и данных, объединив фильтрации. Кроме того, уровень безопасности можно повысить с помощью протокола IPsec.

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. 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.

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 Default Policy

1. Откройте приложение Web Config и выберите **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Введите значение для каждого элемента.
3. Нажмите **Next**.

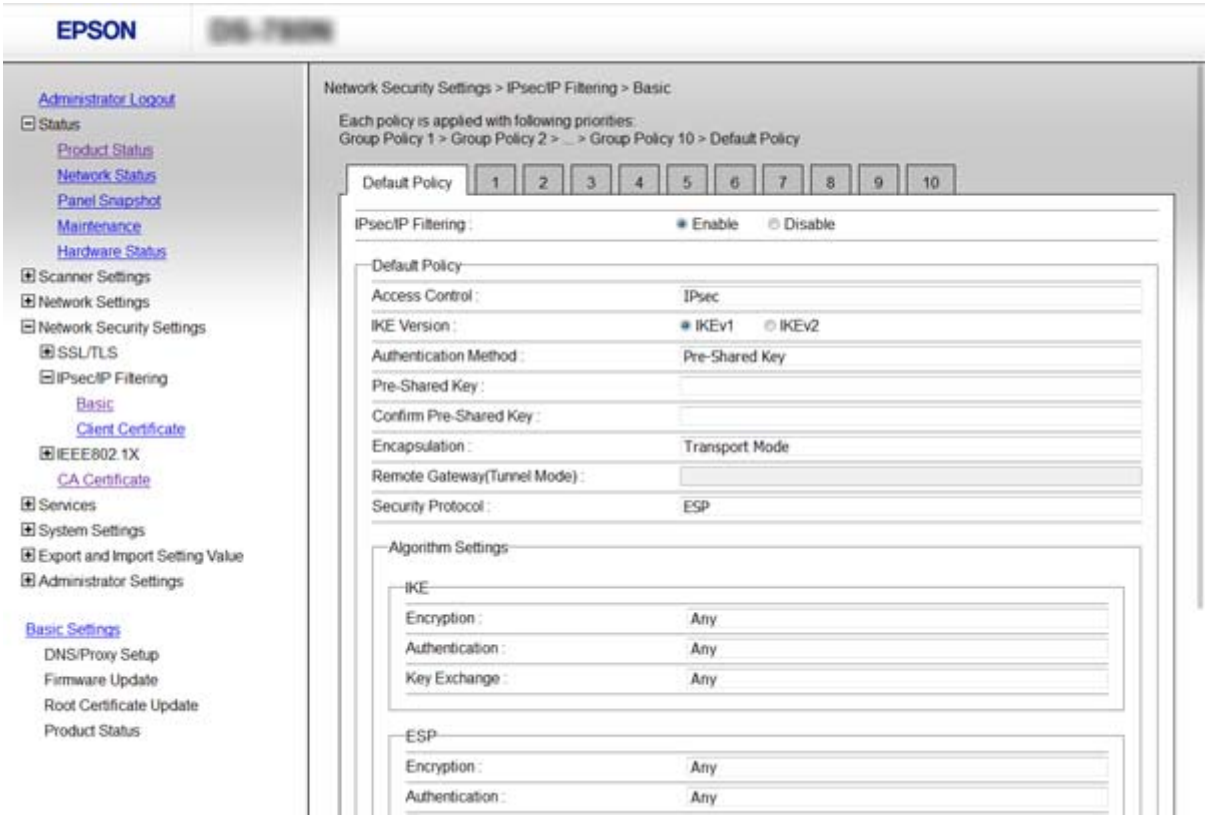
   Отображается запрос подтверждения.
4. Нажмите **OK**.

   Настройки сканера обновлены.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23
➡ «Параметры настройки в разделе Default Policy» на стр. 73

Параметры настройки в разделе Default Policy



Расширенные настройки безопасности для предприятия

Параметры	Настройки и объяснения	
IPsec/IP Filtering	Функцию IPsec/фильтрацию IP можно включить или выключить.	
Access Control	Настройте способ управления трафиком IP-пакетов.	
	Permit Access	Выберите этот параметр, чтобы разрешить прохождение настроенных IP-пакетов.
	Refuse Access	Выберите этот параметр, чтобы запретить прохождение настроенных IP-пакетов.
	IPsec	Выберите этот параметр, чтобы запретить прохождение настроенных пакетов IPsec.
IKE Version	Выберите IKEv1 или IKEv2 в качестве версии IKE. Выберите одно из значений в соответствии с устройством, к которому подключен сканер.	
IKEv1	При выборе **IKEv1** для **IKE Version** отображаются следующие элементы.	
	Authentication Method	Выберите пункт **Certificate** для получения и импорта сертификата, подписанного ЦС.
	Pre-Shared Key	Если значение **Pre-Shared Key** указано для параметра **Authentication Method**, то введите предварительный ключ длиной от 1 до 127 символов.
	Confirm Pre-Shared Key	Введите выбранный вами ключ для подтверждения.
IKEv2	При выборе **IKEv2** для **IKE Version** отображаются следующие элементы.	
Local	Authentication Method	Выберите пункт **Certificate** для получения и импорта сертификата, подписанного ЦС.
	ID Type	Выберите тип идентификатора для сканера.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа вы можете использовать @, # и =. **Distinguished Name**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «=». **IP Address**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя A–Z, a–z, 0–9, дефис (-) и точку (.). **Email Address**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «@». **Key ID**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Pre-Shared Key	Если значение **Pre-Shared Key** указано для параметра **Authentication Method**, то введите предварительный ключ длиной от 1 до 127 символов.
	Confirm Pre-Shared Key	Введите выбранный вами ключ для подтверждения.

Расширенные настройки безопасности для предприятия

Параметры	Настройки и объяснения	
Remote	Authentication Method	Выберите пункт **Certificate** для получения и импорта сертификата, подписанного ЦС.
	ID Type	Выберите тип идентификатора для устройства, подлинность которого следует проверить.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа вы можете использовать @, # и =. **Distinguished Name**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «=». **IP Address**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя A–Z, a–z, 0–9, дефис (-) и точку (.). **Email Address**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «@». **Key ID**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Pre-Shared Key	Если значение **Pre-Shared Key** указано для параметра **Authentication Method**, то введите предварительный ключ длиной от 1 до 127 символов.
	Confirm Pre-Shared Key	Введите выбранный вами ключ для подтверждения.
Encapsulation	Настройте режим инкапсуляции при выборе значения **IPsec** для параметра **Access Control**.	
	Transport Mode	Выберите этот пункт, если сканер используется в рамках одной ЛВС. IP-пакеты 4 слоя или более поздней версии шифруются.
	Tunnel Mode	Выберите этот параметр, если вы используете сканер в сети с выходом в Интернет, например IPsec — VPN. Заголовок и данные IP-пакетов шифруются.
Remote Gateway(Tunnel Mode)	Если значение **Tunnel Mode** указано для параметра **Encapsulation**, то введите адрес шлюза длиной от 1 до 39 символов.	
Security Protocol	**IPsec** для **Access Control**, выберите параметр.	
	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.
Algorithm Settings		

Параметры	Настройки и объяснения	
IKE	Encryption	Выберите алгоритм шифрования для IKE. Элементы различаются в зависимости от версии IKE.
	Authentication	Выберите алгоритм проверки подлинности для IKE.
	Key Exchange	Выберите алгоритм обмена ключами для IKE. Элементы различаются в зависимости от версии IKE.
ESP	Encryption	Выберите алгоритм шифрования для ESP. Это доступно, если **ESP** выбран в качестве **Security Protocol**.
	Authentication	Выберите алгоритм проверки подлинности для ESP. Это доступно, если **ESP** выбран в качестве **Security Protocol**.
AH	Authentication	Выберите алгоритм шифрования для AH. Это доступно, если **AH** выбран в качестве **Security Protocol**.

Соответствующая информация

➡ «Настройка Default Policy» на стр. 73

Настройка Group Policy

1. Откройте приложение Web Config и выберите **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Щелкните вкладку с номером, которую необходимо настроить.
3. Введите значение для каждого элемента.
4. Нажмите **Next**.

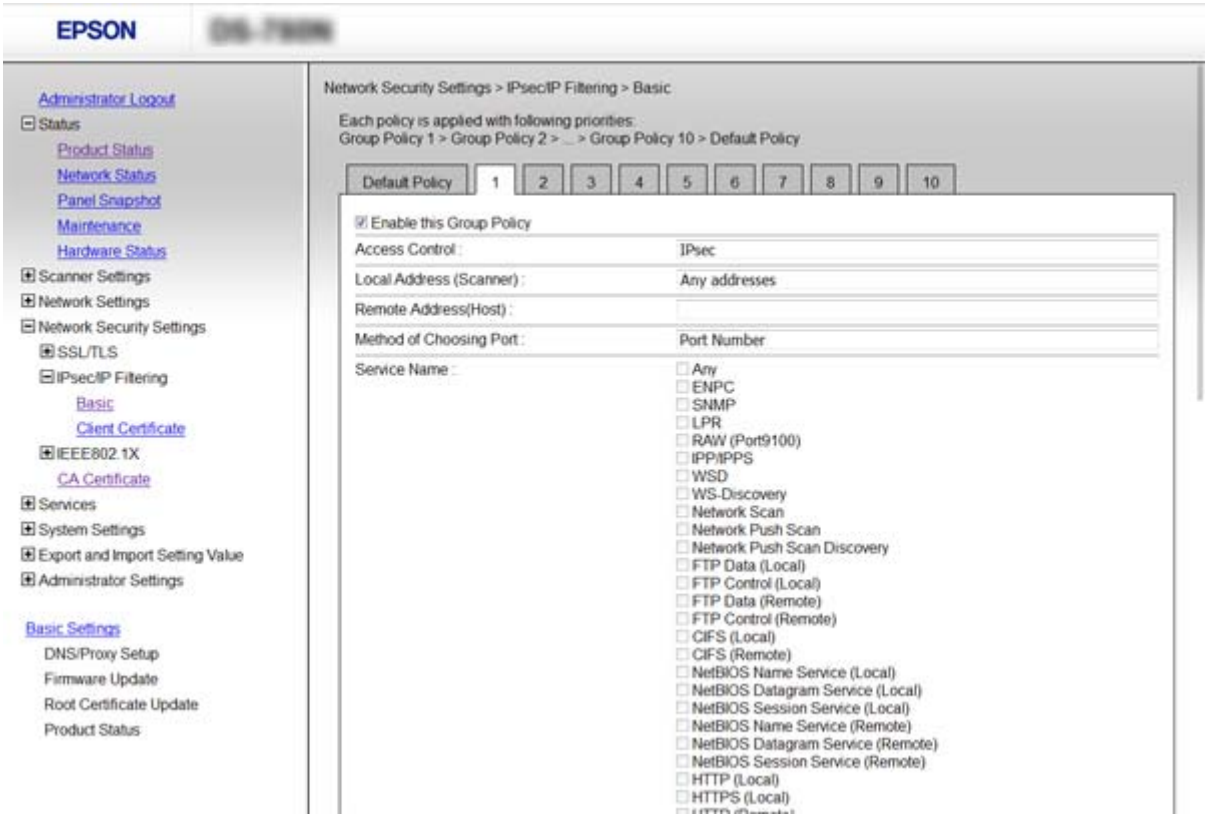
   Отображается запрос подтверждения.
5. Нажмите **OK**.

   Настройки сканера обновлены.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23
➡ «Параметры настройки в разделе Group Policy» на стр. 77

Параметры настройки в разделе Group Policy



Параметры	Настройки и объяснения	
Enable this Group Policy	Групповую политику можно включать или выключать.	
Access Control	Настройте способ управления трафиком IP-пакетов.	
	Permit Access	Выберите этот параметр, чтобы разрешить прохождение настроенных IP-пакетов.
	Refuse Access	Выберите этот параметр, чтобы запретить прохождение настроенных IP-пакетов.
	IPsec	Выберите этот параметр, чтобы запретить прохождение настроенных пакетов IPsec.
Local Address (Scanner)	Выберите адрес IPv4 или IPv6, соответствующий вашему сетевому окружению. Если IP-адрес назначается автоматически, можно выбрать параметр **Use auto-obtained IPv4 address**.	
Remote Address(Host)	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.*	
Method of Choosing Port	Выберите способ указания портов.	
Service Name	Если выбрано значение **Service Name** для параметра **Method of Choosing Port**, то выберите нужный параметр.	

Расширенные настройки безопасности для предприятия

Параметры	Настройки и объяснения	
Transport Protocol	Настройте режим инкапсуляции при выборе значения **Port Number** для параметра **Method of Choosing Port**.	
	Any Protocol	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.
Local Port	При выборе **Port Number** для **Method of Choosing Port** и **TCP** или **UDP** для **Transport Protocol** 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.	
Remote Port	При выборе **Port Number** для **Method of Choosing Port** и **TCP** или **UDP** для **Transport Protocol** 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.	
IKE Version	Выберите IKEv1 или IKEv2 в качестве версии IKE. Выберите одно из значений в соответствии с устройством, к которому подключен сканер.	
IKEv1	При выборе **IKEv1** для **IKE Version** отображаются следующие элементы.	
	Authentication Method	Если выбрано значение **IPsec** для параметра **Access Control**, то выберите нужный параметр. Используемый сертификат соответствует политике по умолчанию.
	Pre-Shared Key	Если значение **Pre-Shared Key** указано для параметра **Authentication Method**, то введите предварительный ключ длиной от 1 до 127 символов.
	Confirm Pre-Shared Key	Введите выбранный вами ключ для подтверждения.
IKEv2	При выборе **IKEv2** для **IKE Version** отображаются следующие элементы.	

Расширенные настройки безопасности для предприятия

Параметры	Настройки и объяснения	
Local	Authentication Method	Если выбрано значение **IPsec** для параметра **Access Control**, то выберите нужный параметр. Используемый сертификат соответствует политике по умолчанию.
	ID Type	Выберите тип идентификатора для сканера.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа вы можете использовать @, # и =. **Distinguished Name**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «=». **IP Address**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя A–Z, a–z, 0–9, дефис (-) и точку (.). **Email Address**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «@». **Key ID**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Pre-Shared Key	Если значение **Pre-Shared Key** указано для параметра **Authentication Method**, то введите предварительный ключ длиной от 1 до 127 символов.
	Confirm Pre-Shared Key	Введите выбранный вами ключ для подтверждения.
Remote	Authentication Method	Если выбрано значение **IPsec** для параметра **Access Control**, то выберите нужный параметр. Используемый сертификат соответствует политике по умолчанию.
	ID Type	Выберите тип идентификатора для устройства, подлинность которого следует проверить.
	ID	Введите идентификатор сканера, который соответствует типу идентификатора. В качестве первого символа вы можете использовать @, # и =. **Distinguished Name**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «=». **IP Address**: укажите в формате IPv4 или IPv6. **FQDN**: введите комбинацию от 1 до 255 символов, используя A–Z, a–z, 0–9, дефис (-) и точку (.). **Email Address**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E). Необходимо включить «@». **Key ID**: введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).
	Pre-Shared Key	Если значение **Pre-Shared Key** указано для параметра **Authentication Method**, то введите предварительный ключ длиной от 1 до 127 символов.
	Confirm Pre-Shared Key	Введите выбранный вами ключ для подтверждения.

Расширенные настройки безопасности для предприятия

Параметры	Настройки и объяснения	
Encapsulation	Настройте режим инкапсуляции при выборе значения **IPsec** для параметра **Access Control**.	
	Transport Mode	Выберите этот пункт, если сканер используется в рамках одной ЛВС. IP-пакеты 4 слоя или более поздней версии шифруются.
	Tunnel Mode	Выберите этот параметр, если вы используете сканер в сети с выходом в Интернет, например IPsec — VPN. Заголовок и данные IP-пакетов шифруются.
Remote Gateway(Tunnel Mode)	Если значение **Tunnel Mode** указано для параметра **Encapsulation**, то введите адрес шлюза длиной от 1 до 39 символов.	
Security Protocol	Если выбрано значение **IPsec** для параметра **Access Control**, то выберите нужный параметр.	
	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.
Algorithm Settings		
IKE	Encryption	Выберите алгоритм шифрования для IKE. Элементы различаются в зависимости от версии IKE.
	Authentication	Выберите алгоритм проверки подлинности для IKE.
	Key Exchange	Выберите алгоритм обмена ключами для IKE. Элементы различаются в зависимости от версии IKE.
ESP	Encryption	Выберите алгоритм шифрования для ESP. Это доступно, если **ESP** выбран в качестве **Security Protocol**.
	Authentication	Выберите алгоритм проверки подлинности для ESP. Это доступно, если **ESP** выбран в качестве **Security Protocol**.
AH	Authentication	Выберите алгоритм проверки подлинности для AH. Это доступно, если **AH** выбран в качестве **Security Protocol**.

Соответствующая информация

➡ «Настройка Group Policy» на стр. 76

➡ «Сочетание Local Address (Scanner) и Remote Address(Host) в Group Policy» на стр. 81

➡ «Ссылки на название службы в групповой политике» на стр. 81

Сочетание Local Address (Scanner) и Remote Address(Host) в Group Policy

		Настройка Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Настройка Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1*2	–	✓	✓
	Пусто	✓	✓	✓

*1 Если для **Access Control** выбран **IPsec**, вы не можете указать длину префикса.

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

*3 Кроме адресов локального соединения IPv6.

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
Any	–	–	–	Все службы
ENPC	UDP	3289	Любой порт	Поиск сканера из приложений, таких как EpsonNet Config и драйвер сканера.
SNMP	UDP	161	Любой порт	Получение данных и конфигурирование административной базы данных (MIB) из приложений, таких как EpsonNet Config и драйвер сканера Epson.
WSD	TCP	Любой порт	5357	Управление WSD
WS-Discovery	UDP	3702	Любой порт	Поиск сканера из WSD
Network Scan	TCP	1865	Любой порт	Пересылка данных сканирования из Document Capture Pro
Network Push Scan Discovery	UDP	2968	Любой порт	Поиск компьютера со сканера.
Network Push Scan	TCP	Любой порт	2968	Получение информации о задании или сканирование по технологии push из приложения Document Capture Pro или Document Capture
HTTP (Local)	TCP	80	Любой порт	Сервер HTTP(S) (пересылка данных Web Config и WSD)
HTTPS (Local)	TCP	443	Любой порт	

Название службы	Тип протокола	Номер локального порта	Номер удаленного порта	Контролируемые функции
HTTP (Remote)	TCP	Любой порт	80	Клиент HTTP(S) (обмен данными при обновлении встроенного микропрограммного обеспечения и обновлении корневых сертификатов)
HTTPS (Remote)	TCP	Любой порт	443	

Примеры конфигурации IPsec/IP Filtering

Получение только пакетов IPsec.

Данный пример представляет собой настройку только политики по умолчанию.

Default Policy

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: введите до 127 символов.

Group Policy:

не настраивайте.

Принятие отсканированных изображений с использованием Epson Scan 2 и параметров сканера

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

Default Policy

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy

❏ **Enable this Group Policy**: установите флажок.

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

❏ **Remote Address(Host)**: IP-адрес клиента.

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

❏ **Service Name**: установите флажок на **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** и **HTTPS (Local)**.

Получение доступа только от заданного IP-адреса

Этот пример обеспечивает заданному IP-адресу доступ к сканеру.

Default Policy

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy

❏ **Enable this Group Policy**: установите флажок.

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

❏ **Remote Address(Host)**: IP-адрес клиента администратора.

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

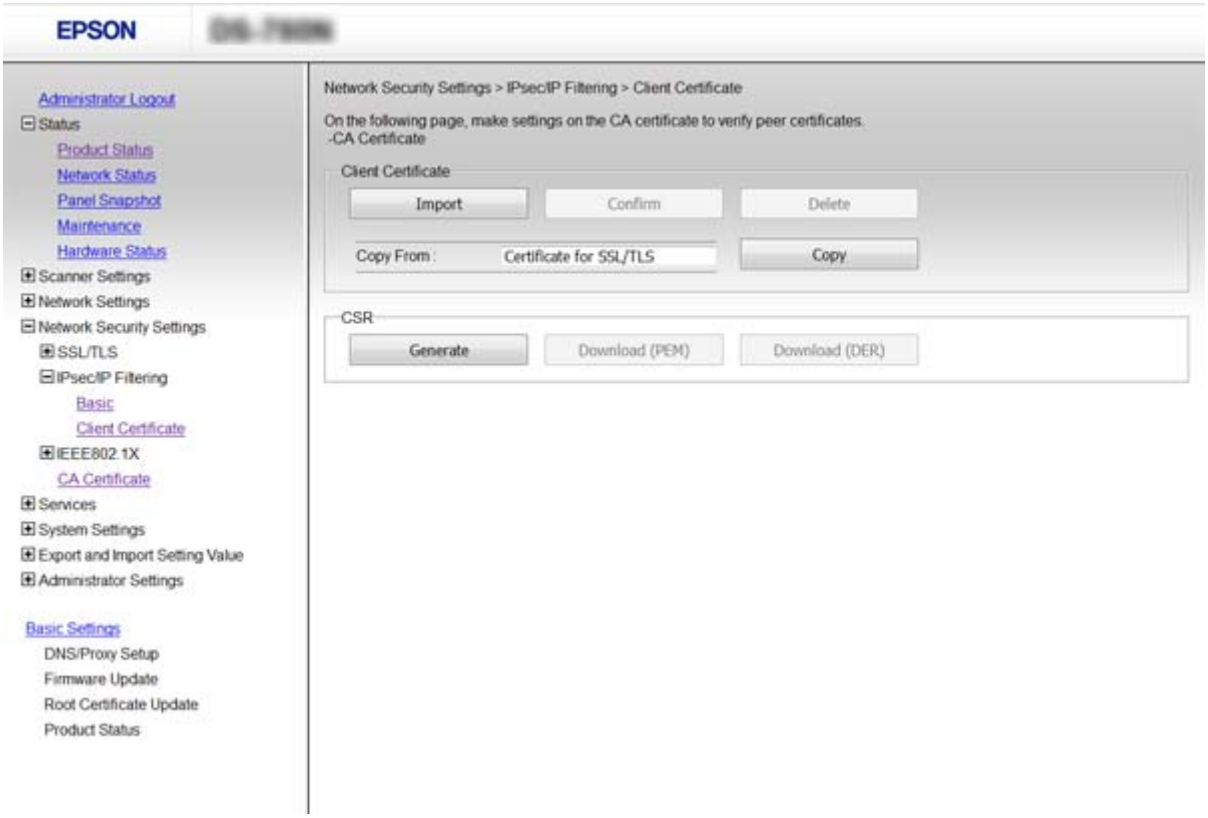
Настройка сертификата для протокола IPsec/IP Filtering

Настройте клиентский сертификат для IPsec/фильтрации IP. Если необходимо настроить центр сертификации, перейдите к разделу **CA Certificate**.

1. Откройте приложение Web Config и выберите **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Импортируйте сертификат в **Client Certificate**.

   Если вы уже импортировали сертификат, опубликованный центром сертификации, в IEEE802.1X или SSL/TLS, можно скопировать этот сертификат и использовать его для IPsec/фильтрации IP. Чтобы скопировать сертификат, выберите его в списке **Copy From** и щелкните **Copy**.



Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Получение и импорт сертификата, подписанного ЦС» на стр. 65

Использование протокола SNMPv3

Сведения о SNMPv3

SNMP – это протокол, который позволяет осуществлять мониторинг и контроль для сбора информации с устройств, подключенных к сети. SNMPv3 – это улучшенная версия функции управления безопасности.

При использовании SNMPv3 мониторинг состояния и изменения настроек связи SNMP (пакет) подлежит проверке подлинности и шифрованию для защиты связи SNMP (пакет) от сетевых рисков, таких как перехват пакетов, выдача себя за другое лицо и взлом.

Настройка SNMPv3

Если сканер поддерживает протокол SNMPv3, вы можете отслеживать и контролировать доступ к принтеру.

1. Откройте приложение Web Config и выберите **Services** > **Protocol**.
2. Введите значение для каждого элемента **SNMPv3 Settings**.
3. Нажмите **Next**.

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

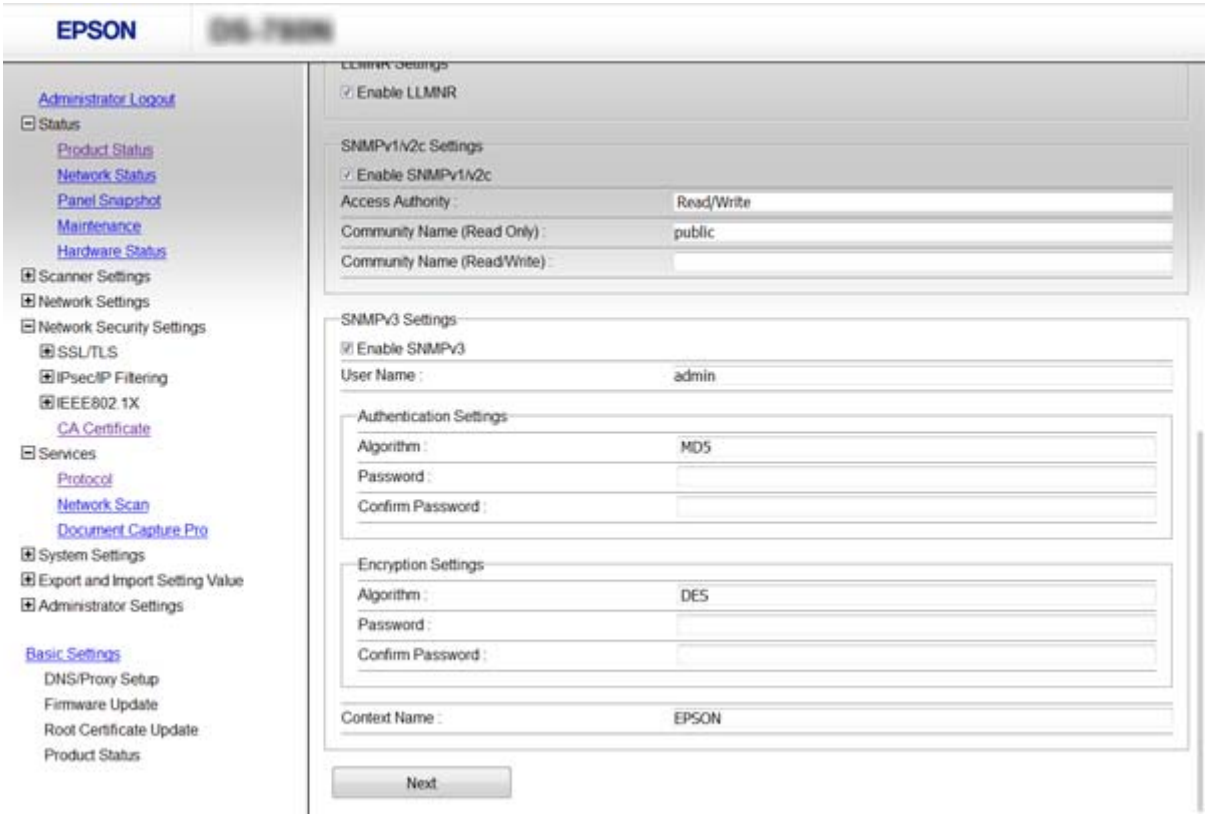
   Настройки сканера обновлены.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Параметры настройки SNMPv3» на стр. 85

Параметры настройки SNMPv3



Параметры	Параметры и объяснения
Enable SNMPv3	Протокол SNMPv3 включается при установке флажка в соответствующей ячейке.
User Name	Введите от 1 до 32 символов, используя 1-байтовые символы.
Authentication Settings	
Algorithm	Выберите алгоритм для аутентификации.
Password	Введите от 8 до 32 символов в формате ASCII (0x20-0x7E).
Confirm Password	Для подтверждения введите настроенный пароль.
Encryption Settings	
Algorithm	Выберите алгоритм для шифрования.
Password	Введите от 8 до 32 символов в формате ASCII (0x20-0x7E).
Confirm Password	Для подтверждения введите настроенный пароль.
Context Name	Введите от 1 до 32 символов, используя 1-байтовые символы.

Соответствующая информация

➡ «Настройка SNMPv3» на стр. 84

Подключение сканера к сети IEEE802.1X

Настройка сети IEEE802.1X

Сканер можно использовать в сети, соединенной с RADIUS-сервером и сетевым концентратором в качестве аутентификатора, если сканер поддерживает сеть IEEE802.1X.

1. Откройте приложение Web Config и выберите **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Введите значение для каждого элемента.
3. Нажмите **Next**.

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

   Настройки сканера обновлены.

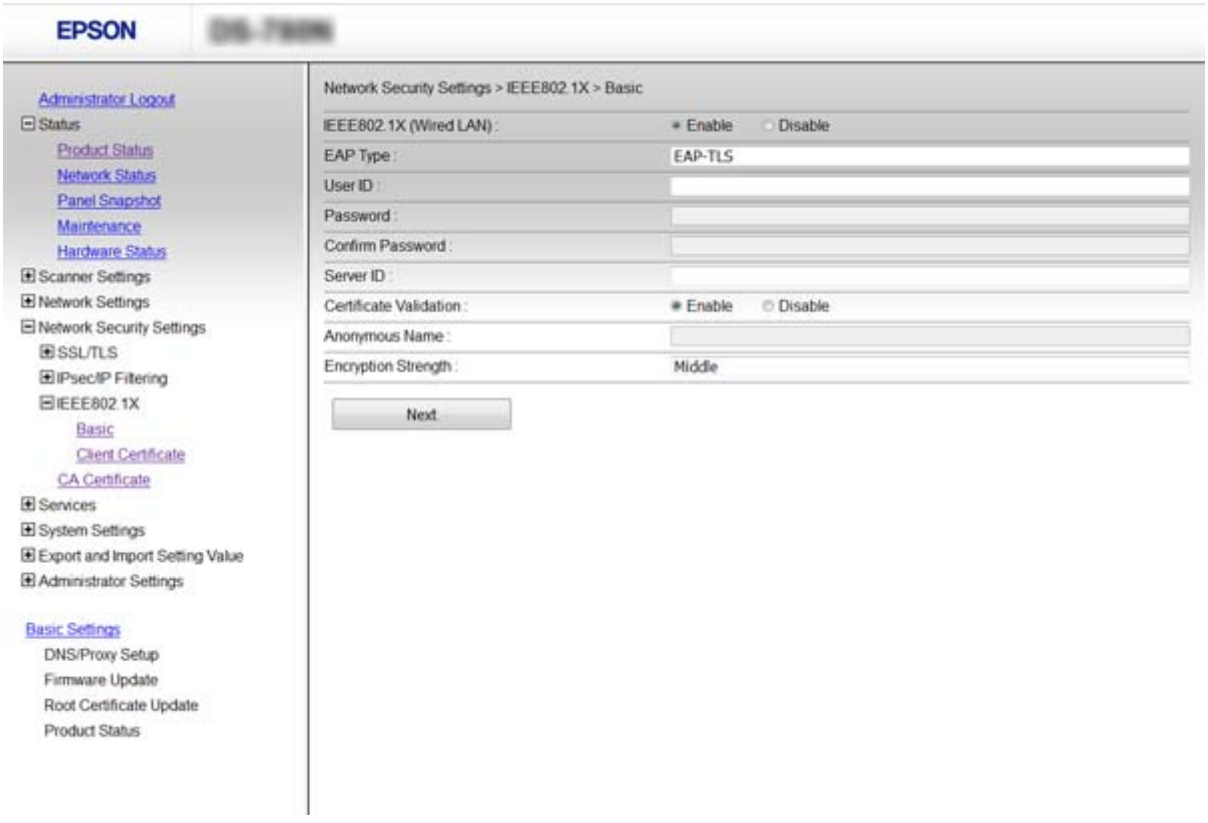
Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Параметры настройки сети IEEE802.1X» на стр. 86

➡ «Не удается получить доступ к принтеру или сканеру после настройки IEEE802.1X» на стр. 91

Параметры настройки сети IEEE802.1X



Расширенные настройки безопасности для предприятия

Параметры	Настройки и объяснения	
IEEE802.1X (Wired LAN)	Можно включить или отключить параметры страницы (**IEEE802.1X** > **Basic**) для IEEE802.1X (проводная сеть LAN).	
EAP Type	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.
User ID	Укажите идентификатор (ID) для использования при аутентификации сервера RADIUS. Введите от 1 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).	
Password	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.	
Confirm Password	Введите выбранный вами пароль для подтверждения.	
Server ID	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).	
Certificate Validation	Можно задать проверку сертификата независимо от метода аутентификации. Импортируйте сертификат в **CA Certificate**.	
Anonymous Name	Если выбран вариант **PEAP-TLS** или **PEAP/MSCHAPv2** для параметра **Authentication Method**, то нужно настроить анонимное имя вместо идентификатора пользователя для фазы 1 PEAP-аутентификации. Введите от 0 до 128 1-байтовых символов ASCII (от 0x20 до 0x7E).	
Encryption Strength	Можно выбрать один из уровней, указанных ниже.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Соответствующая информация

➡ «Настройка сети IEEE802.1X» на стр. 86

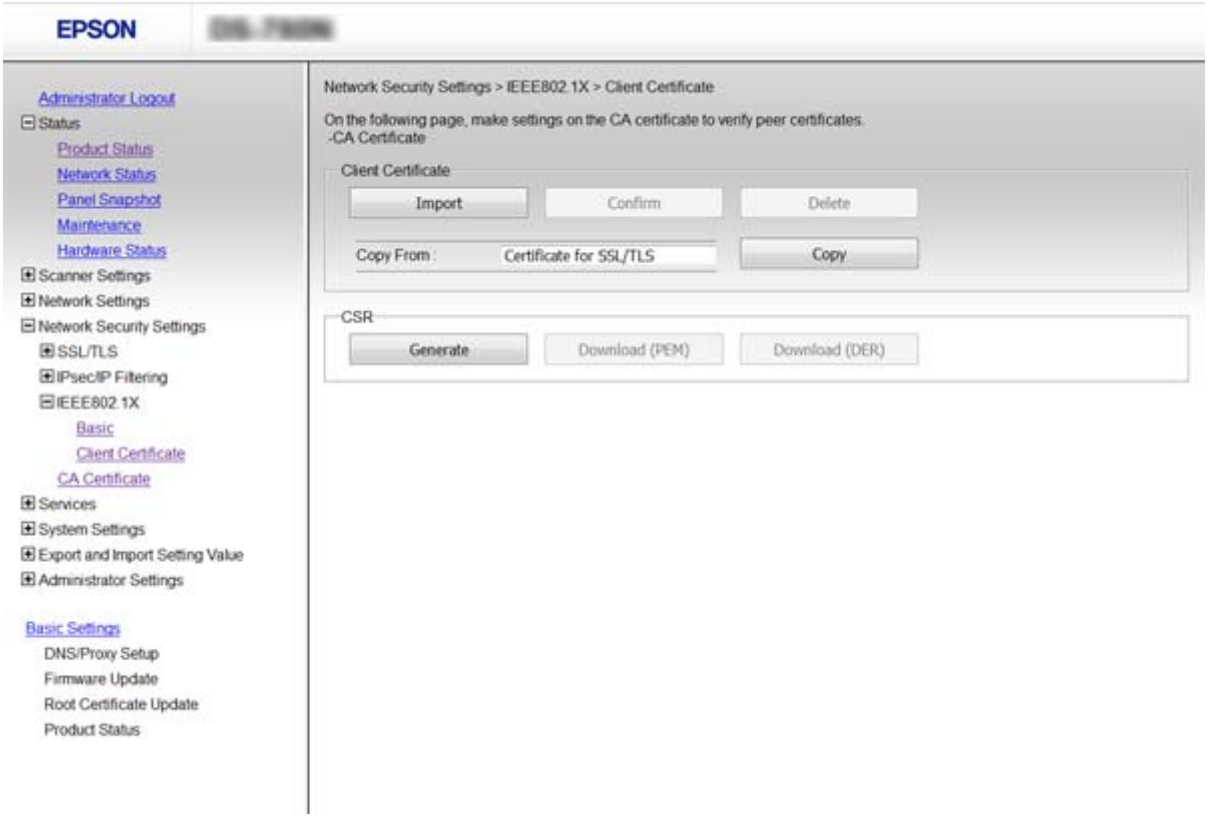
Настройка сертификата для протокола IEEE802.1X

Настройте клиентский сертификат для IEEE802.1X. Если необходимо настроить сертификат центра сертификации, перейдите к разделу **CA Certificate**.

1. Откройте приложение Web Config и выберите **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. Укажите сертификат в поле **Client Certificate**.

   Можно скопировать сертификат, если он опубликован центром сертификации. Чтобы скопировать сертификат, выберите его в списке **Copy From** и щелкните **Copy**.



Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Получение и импорт сертификата, подписанного ЦС» на стр. 65

Решение проблем, связанных с расширенной безопасностью

Восстановление настроек безопасности

При создании среды с повышенным уровнем безопасности, например IPsec/фильтрация IP или IEEE802.1X, может понадобится 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 панели управления

Можно отключить IPsec/фильтрацию IP или IEEE802.1X на панели управления сканера.

1. Нажмите **Настр.** > **Настройки сети**.
2. Коснитесь **Изменить настройки**.
3. Нажмите элементы, которые следует отключить.
   - ❏ **IPsec/Фильтрация IP**
   - ❏ **IEEE802.1X**
4. После появления предупреждения нажмите **Далее**.

Восстановление функции безопасности с помощью Web Config

Устройства, использующие IEEE802.1X, могут не распознаваться в сети. В этом случае отключите эту функцию с помощью панели управления сканера.

Что касается IPsec/фильтрации IP можно отключить эту функцию, если получить доступ на устройство с компьютера.

Отключение фильтрации IPsec/IP с использованием Web Config

1. Откройте Web Config и выберите **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Выберите **Disable** для **IPsec/IP Filtering** в **Default Policy**.
3. Щелкните **Next**, затем снимите флажок **Enable this Group Policy** для всех групповых политик.
4. Нажмите **OK**.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Неполадки при использовании функций защиты сети

Забыт предварительный ключ

Настройте ключ заново, используя Web Config.

Для того чтобы изменить ключ, откройте Web Config и выберите **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** или **Group Policy**.

Изменение общего ключа подразумевает настройку общего ключа для компьютеров.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

Не удается соединиться по протоколу IPsec

В параметрах компьютера используется неподдерживаемый алгоритм?

Сканер поддерживает следующие алгоритмы.

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	Группа DH 1, группа DH 2, группа DH 5, группа DH 14, группа DH 15, группа DH 16, группа DH 17, группа DH 18, группа DH 19, группа DH 20, группа DH 21, группа DH 22, группа DH 23, группа DH 24, группа DH 25, группа DH 26, группа DH 27*, группа DH 28*, группа DH 29*, группа DH 30*
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. 72

Неожиданная потеря соединения

IP-адрес сканера неправильный или изменился?

Отключите протокол IPsec с помощью панели управления сканера.

Если данные DHCP устарели, DHCP-сервер перезагружается или устарел либо не был получен IPv6-адрес, то может оказаться ненайденным IP-адрес, зарегистрированный для приложения Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) на сканере.

Используйте статический IP-адрес.

IP-адрес компьютера неправильный или изменился?

Отключите протокол IPsec с помощью панели управления сканера.

Если данные DHCP устарели, DHCP-сервер перезагружается или устарел либо не был получен IPv6-адрес, то может оказаться ненайденным IP-адрес, зарегистрированный для приложения Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) на сканере.

Используйте статический IP-адрес.

Соответствующая информация

➡ «Доступ к приложению Web Config» на стр. 23

➡ «Шифрованный канал связи с использованием IPsec/фильтрации IP» на стр. 72

Не удается подключиться после настройки IPsec/фильтрации IP

Возможно, указано неверное значение

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. 72

Не удается получить доступ к принтеру или сканеру после настройки IEEE802.1X

Настройки могут быть неверными.

Отключите IEEE802.1X на панели управления сканера. Подключите сканер и компьютер, затем повторно настройте IEEE802.1X.

Соответствующая информация

➡ «Настройка сети IEEE802.1X» на стр. 86

Неполадки при использовании цифрового сертификата

Невозможно импортировать сертификат, подписанный ЦС.

Совпадает ли информация в сертификате, подписанном ЦС, и в CSR?

Если информация в сертификате, подписанном ЦС, и в CSR не совпадает, то CSR нельзя 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?

Невозможно импортировать сертификат, подписанный ЦС, размером больше чем 5 КБ.

Верен ли пароль для импорта сертификата?

Если пароль забыт, то импортировать сертификат невозможно.

Соответствующая информация

➡ «Импорт сертификата, подписанного ЦС» на стр. 67

Невозможно обновить самозаверяющий сертификат.

Введено ли Common Name?

Нужно ввести **Common Name**.

Были ли введены в Common Name неподдерживаемые символы? Например, японский язык не поддерживается.

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

Включена ли запятая или пробел в Common Name?

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

Соответствующая информация

➡ «Обновление самозаверяющего сертификата» на стр. 69

Невозможно создать CSR.

Введено ли Common Name?

Нужно ввести **Common Name**.

Были ли введены неподдерживаемые символы в параметры Common Name, Organization, Organizational Unit, Locality, State/Province? Например, японский язык не поддерживается.

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

Включена ли запятая или пробел в Common Name?

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

Соответствующая информация

➡ «Получение сертификата, подписанного ЦС» на стр. 65

Появление предупреждения, касающегося цифрового сертификата

Сообщения	Причина/действия для устранения
Enter a Server Certificate.	**Причина** Не выбран файл для импорта. **Действия для устранения** Выберите файл и нажмите **Import**.
CA Certificate 1 is not entered.	**Причина** Сертификат ЦС 1 не введен, введен только сертификат ЦС 2. **Действия для устранения** Импортируйте сертификат ЦС 1.
Invalid value below.	**Причина** Неподдерживаемые символы содержатся в пути к файлу и (или) в пароле. **Действия для устранения** Убедитесь, что символы для данного параметра введены правильно.
Invalid date and time.	**Причина** Дата и время сканера не установлены. **Действия для устранения** Установите дату и время, используя Web Config или EpsonNet Config.
Invalid password.	**Причина** Пароль, установленный для сертификата ЦС, и введенный пароль не совпадают. **Действия для устранения** Введите правильный пароль.
Invalid file.	**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.

Сообщения	Причина/действия для устранения
Cannot use the Server Certificates that include more than three CA certificates.	**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.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**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.
Private key is required.	**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.
Setup failed.	**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. 65

Ошибочное удаление сертификата, подписанного ЦС

Существует ли файл резервной копии для сертификата?

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

➡ «Удаление сертификата, подписанного ЦС» на стр. 69

➡ «Импорт сертификата, подписанного ЦС» на стр. 67