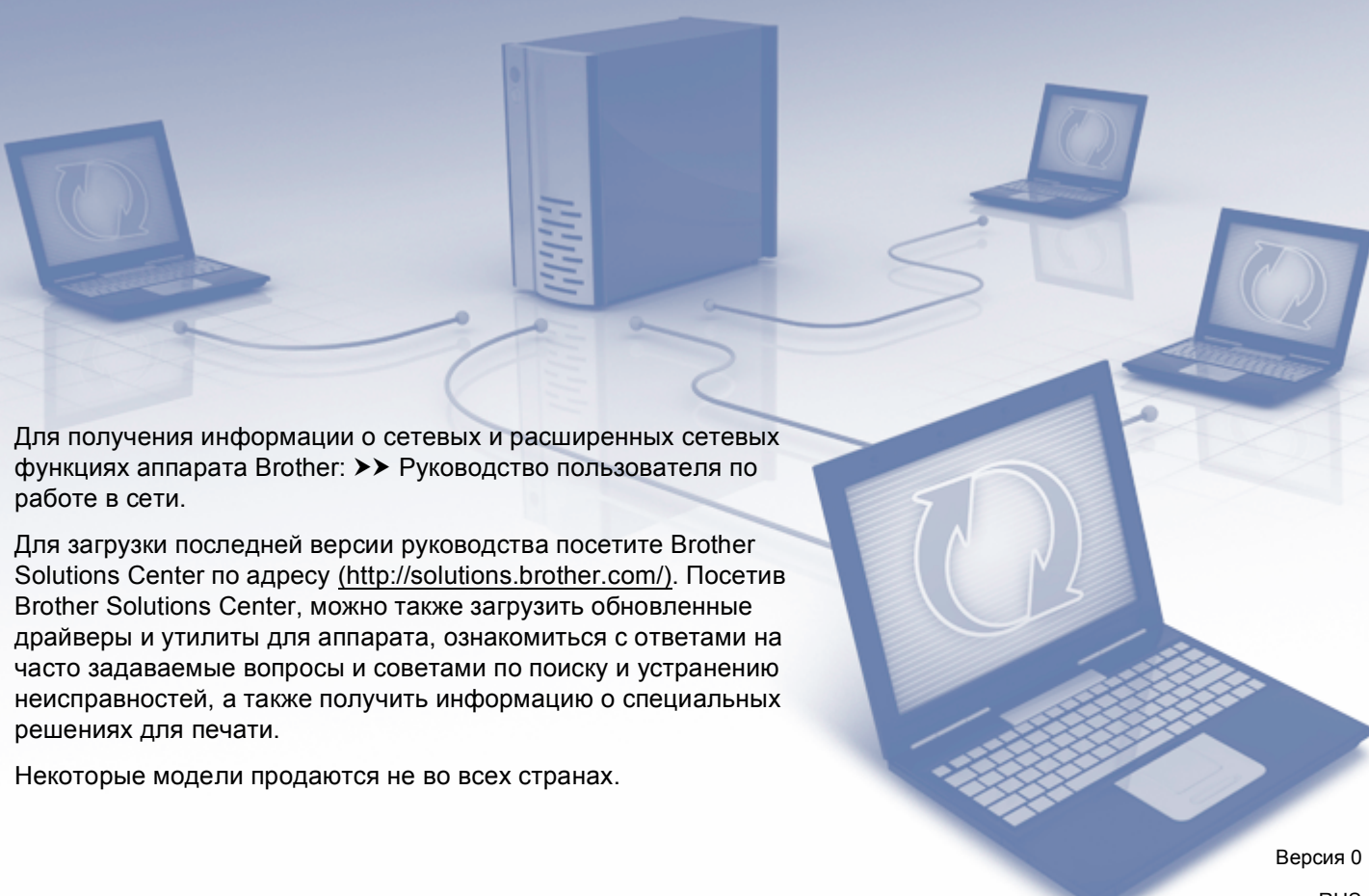


Руководство по SSL

(Secure Socket Layer)

A blue-tinted illustration of a network setup. In the center is a server tower. To its left and right are several laptops. Wavy lines represent network connections between the server and the laptops. Each laptop screen displays a circular arrow icon, symbolizing a network or refresh function.

Для получения информации о сетевых и расширенных сетевых функциях аппарата Brother: ►► Руководство пользователя по работе в сети.

Для загрузки последней версии руководства посетите Brother Solutions Center по адресу (<http://solutions.brother.com/>). Посетив Brother Solutions Center, можно также загрузить обновленные драйверы и утилиты для аппарата, ознакомиться с ответами на часто задаваемые вопросы и советами по поиску и устранению неисправностей, а также получить информацию о специальных решениях для печати.

Некоторые модели продаются не во всех странах.

Применимые модели

Руководство пользователя применяется к следующим моделям.

HL-5450DN(T)/5470DW(T)/6180DW(T)

DCP-8110DN/8150DN/8155DN/8250DN/MFC-8510DN/8710DW/8910DW/8950DW(T)

Обозначение примечаний

В настоящем руководстве пользователя используются следующие значки:

 Примечание	В примечаниях описывается способ действия в возникшей ситуации и содержатся советы по работе той или иной операции с другими функциями.
---	---

Торговые марки

Логотип Brother является зарегистрированным товарным знаком Brother Industries, Ltd.

Microsoft, Windows, Windows Server и Internet Explorer являются зарегистрированными товарными знаками или товарными знаками Microsoft Corporation в США и/или других странах.

Windows Vista является зарегистрированным товарным знаком или товарным знаком Microsoft Corporation в США и/или других странах.

Все компании, программное обеспечение которых упомянуто в данном руководстве, имеют особые лицензионные соглашения для выпускаемых ими программных продуктов.

Все торговые названия и названия продукции компаний, появляющиеся на продукции Brother, сопутствующих документах и любых других материалах, являются товарными знаками или зарегистрированными товарными знаками соответствующих компаний.

ВАЖНОЕ ПРИМЕЧАНИЕ

- Данный продукт утвержден для использования только в стране покупки. Не используйте данный продукт за пределами страны покупки, так как это может привести к нарушению правил беспроводной связи и используемой мощности, установленных в этой стране.
- В данном руководстве используются экраны MFC-8950DW(T), если не указано иного.
- Windows® XP в настоящем документе обозначает Windows® XP Professional, Windows® XP Professional x64 Edition и Windows® XP Home Edition.
- Windows Server® 2003 в настоящем документе обозначает Windows Server® 2003 и Windows Server® 2003 x64 Edition.
- Windows Server® 2008 в настоящем документе обозначает Windows Server® 2008 и Windows Server® 2008 R2.
- Под Windows Vista® в данном документе понимаются все издания ОС Windows Vista®.
- Windows® 7 в настоящем документе обозначает все издания ОС Windows® 7.
- Для загрузки других руководств посетите Brother Solutions Center по адресу <http://solutions.brother.com/> и на странице соответствующей модели нажмите «Руководства».

Содержание

1	Введение	1
	Обзор	1
	Краткая история SSL	1
	Преимущества SSL.....	1
	Использование сертификатов для защиты устройств.....	2
2	Цифровой сертификат для связи SSL	4
	Установка цифрового сертификата.....	4
	Создание самозаверяющего сертификата.....	6
	Создание запроса CSR (запроса на подпись сертификата)	7
	Установка сертификата на аппарат	10
	Выбор сертификата	11
	Установка самозаверяющего или предварительно установленного сертификата в Windows Vista®, Windows® 7 и Windows Server® 2008 для пользователей с правами администратора.....	13
	Установка самозаверяющего или предварительно установленного сертификата в Windows® XP и Windows Server® 2003.....	15
	Импорт и экспорт сертификата и секретного ключа	18
	Импорт самозаверяющего сертификата, сертификата, выданного сторонним ЦС, и закрытого ключа	18
	Экспорт самозаверяющего сертификата, сертификата, выданного сторонним ЦС, и закрытого ключа	18
	Импорт и экспорт сертификата ЦС	19
	Управление несколькими сертификатами	20
3	Безопасное управление сетевым аппаратом с помощью SSL/TLS	21
	Безопасное управление с помощью системы управления через веб-интерфейс (веб-браузер) ...	21
4	Безопасная печать документов с использованием протокола SSL	22
	Безопасная печать документов с использованием протокола IPPS для Windows®	22
	Windows® XP и Windows Server® 2003.....	22
	Windows Vista®, Windows® 7 и Windows Server® 2008	24
5	Безопасная отправка или получение (для моделей DCP и MFC) сообщений электронной почты	26
	Настройка с помощью системы управления через веб-интерфейс (веб-браузер)	26
	Безопасная отправка или получение (для моделей DCP и MFC) сообщений электронной почты с использованием SSL/TLS	27

6	Устранение неисправностей	28
	Обзор	28
	Определение проблемы	28
	Печать страницы параметров принтера (для модели HL-5450DN(T))	30
	Печать отчёта конфигурации сети (для других моделей)	30
	Сетевые термины и понятия	32
	Технический обзор SSL	32
	Сетевая терминология	33

Обзор

Secure Socket Layer (SSL – уровень защищенных сокетов) является эффективным методом защиты данных при пересылке по локальной или региональной сети. Он работает по принципу шифрования данных, передаваемых по сети, в данном случае, задания печати, чтобы при попытке перехвата документ невозможно было прочитать, т.к. все данные будут зашифрованы.

Его можно настроить как для проводных, так и для беспроводных сетей, и он совместим с другими методами защиты, например, ключами WPA и брандмауэрами.

Краткая история SSL

SSL изначально был создан для защиты передаваемой по Интернету информации, в особенности, данных, передаваемых от веб-браузеров на серверы и обратно. Например, когда вы используете Internet Explorer® для получения банковских услуг через Интернет и в веб-браузере отображается https:// и изображение замка, то вы используете SSL. Затем область его применения расширилась до таких приложений, как Telnet, принтеры и программное обеспечение FTP, сделав SSL универсальным средством он-лайн защиты. Он до сих пор используется по своему исходному предназначению многими интернет-магазинами и банками, обеспечивая защиту таких уязвимых данных, как номера кредитных карт, записи о клиентах и т.п.

SSL использует очень высокие уровни шифрования и снискал доверие банков по всему миру благодаря практически нулевому риску его взлома.

Преимущества SSL

Основное преимущество, которое даёт использование SSL на принтерах Brother, - это гарантированная защита печати через сеть IP за счёт того, что неавторизованные пользователи не смогут читать данные, направляемые на принтер. Главной отличительной чертой является возможность безопасной печати конфиденциальных данных. Например, отдел кадров крупного предприятия может таким образом регулярно распечатывать платёжные ведомости. Если данные из этих платёжных ведомостей не шифровать, то их смогут прочитать другие пользователи в сети. Однако применение SSL приводит к тому, что при попытке перехватить данные пользователь увидит только страницу нечитаемого кода, а не фактическую платёжную ведомость.

Использование сертификатов для защиты устройств

Аппарат Brother поддерживает использование нескольких сертификатов безопасности, позволяющих осуществлять безопасное управление и аутентификацию, а также устанавливать безопасное соединение с аппаратом. Для аппарата можно использовать следующие функции безопасности. Во время печати документа или использования системы управления через веб-интерфейс (веб-браузера) с применением SSL вам необходимо установить сертификат на свой компьютер. См. раздел *Установка цифрового сертификата* >> стр. 4.

- Связь SSL/TLS
- Соединение по протоколу SSL для SMTP/POP3

Аппарат Brother поддерживает следующие сертификаты.

- Предварительно установленный сертификат

На этом аппарате имеется предварительно установленный самозаверяющий сертификат.

Пользуясь этим сертификатом, можно с легкостью использовать соединение по протоколу SSL/TLS без создания или установки сертификата. Если на аппарате требуется использовать функцию Google Cloud Print, то этот предварительно установленный сертификат позволит провести безопасную настройку Google Cloud Print. Чтобы подробнее узнать о Google Cloud Print, посетите Brother Solutions Center по адресу <http://solutions.brother.com/> и на странице соответствующей модели нажмите «Руководства» для загрузки «Руководства по использованию Google Cloud Print».



Примечание

Предварительно установленный самозаверяющий сертификат не обеспечивает защиты от фишинга. Для обеспечения лучшей защиты мы рекомендуем использовать сертификат, выданный надёжной организацией.

- Самозаверяющий сертификат

Сервер печати использует свой собственный сертификат. Пользуясь этим сертификатом, можно с легкостью использовать связь по протоколу SSL/TLS без получения сертификата от центра сертификатов. (См. раздел *Создание самозаверяющего сертификата* >> стр. 6.)

- Сертификат от стороннего ЦС

Существует два способа установки такого сертификата. Если у вас уже имеется сертификат от ЦС или если требуется использовать сертификат от стороннего проверенного ЦС:

- С использованием CSR (запроса на подпись сертификата) от данного сервера печати. (См. раздел *Создание запроса CSR (запроса на подпись сертификата)* >> стр. 7.)
- С импортированием сертификата и секретного ключа. (См. раздел *Импорт и экспорт сертификата и секретного ключа* >> стр. 18.)

■ Сертификат ЦС

Если используется сертификат ЦС, определяющий сам ЦС (центр сертификации), необходимо импортировать сертификат ЦС из центра сертификации до выполнения настройки. (См. раздел *Импорт и экспорт сертификата ЦС* ►► стр. 19.)



Примечание

- При использовании соединения SSL/TLS сначала рекомендуется связаться со своим системным администратором.
- При восстановлении заводских параметров сервера печати установленный сертификат и секретный ключ будут удалены. Если после перезагрузки сервера печати требуется использование того же сертификата и закрытого ключа, следует их экспортировать и установить повторно после перезагрузки. (См. раздел *Импорт самоподписанного сертификата, сертификата, выданного сторонним ЦС, и закрытого ключа* ►► стр. 18.)

Установка цифрового сертификата

Печать по защищённой сети или безопасное управление через веб-интерфейс (веб-браузер) требуют установки цифрового сертификата как на аппарате, так и на устройстве, осуществляющем отправку данных на аппарат, например, компьютере. На этом аппарате имеется предварительно установленный сертификат. Для настройки сертификата пользователь должен произвести удалённый вход в систему аппарата через веб-браузер, используя его IP-адрес.

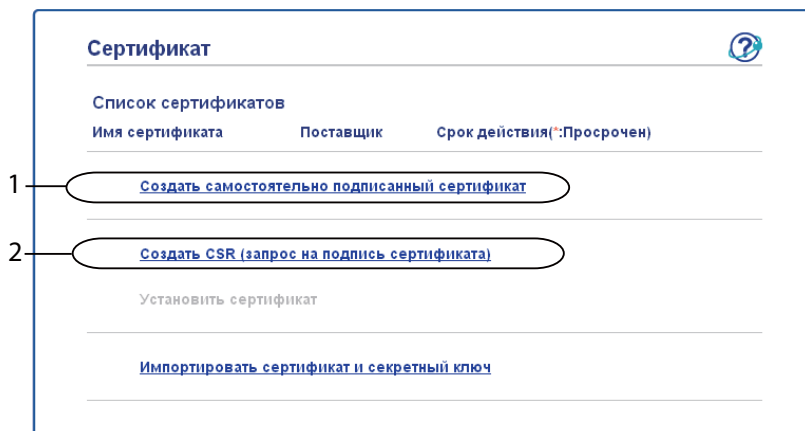


Примечание

Рекомендуется использовать Windows® Internet Explorer® 7.0/8.0 или Firefox® 3.6 для Windows® и Safari 4.0/5.0 для Macintosh. Проследите за тем, чтобы в используемом браузере всегда были разрешены JavaScript и Cookies. Любой другой веб-браузер должен быть совместим с HTTP 1.0 и HTTP 1.1.

- 1 Запустите веб-браузер.
- 2 В адресной строке браузера введите “http://IP-адрес аппарата/” (где “IP-адрес аппарата” соответствует IP-адресу аппарата или имени сервера печати).
 - Например: http://192.168.1.2/
- 3 По умолчанию пароль не требуется. Если вы ранее установили пароль, введите его и нажмите ➔.
- 4 Нажмите **Сеть**.
- 5 Нажмите **Безопасность**.
- 6 Нажмите **Сертификат**.

- 7** Параметры сертификата можно настраивать.
 Для создания самоподписанного сертификата с помощью системы управления через веб-интерфейс перейдите к разделу *Создание самоподписанного сертификата* >> стр. 6.
 Для создания запроса CSR (запроса на подпись сертификата) перейдите к разделу *Создание запроса CSR (запроса на подпись сертификата)* >> стр. 7.



- 1 Создание и установка самоподписанного сертификата
- 2 Использование сертификата от Центра сертификатов (ЦС)



Примечание

- Затененные функции, не оформленные в виде ссылок, недоступны.
- Чтобы получить дополнительную информацию по настройке, обратитесь к справке системы управления через веб-интерфейс.

Создание самозаверяющего сертификата

1 Нажмите **Создать самостоятельно подписанный сертификат**.

2 Введите **Общее название** и **Срок действия**.



Примечание

- Длина поля **Общее название** не должна превышать 64 знака. Введите идентификатор, такой как IP-адрес, имя узла или имя домена, чтобы использовать его при доступе к аппарату через соединение по протоколу SSL/TLS. По умолчанию отображается имя узла.
 - Если используется протокол IPPS или HTTPS, при вводе адреса URL, отличного от указанного в параметре **Общее название**, который был использован для заполнения самозаверяющего сертификата, будет отображаться всплывающее сообщение.
-

3 В выпадающем списке можно выбрать значения параметров **Алгоритм с использованием открытых ключей** и **Алгоритм**. Настройки по умолчанию: **RSA (2048 бит)** для **Алгоритм с использованием открытых ключей** и **SHA-256** для **Алгоритм**.

4 Нажмите **Отправить**.

5 Создание и установка самозаверяющего сертификата в память аппарата завершены успешно.

Создание запроса CSR (запроса на подпись сертификата)

Запрос на подпись сертификата (CSR) - это запрос в ЦС для аутентификации учётных данных, содержащихся в сертификате.



Примечание

Перед созданием запроса на подпись сертификата рекомендуется установить на компьютере корневой сертификат, полученный от ЦС.

2

- 1 Нажмите **Создать CSR (запрос на подпись сертификата)**.
- 2 Введите **Общее название** и свои данные, такие как **Организация**.
Для подтверждения подлинности и доказательства существования вашей компании необходимо предоставить в ЦС сведения о компании.

Создать CSR (запрос на подпись сертификата)

Общее название

BRNxxxxxxxxxx
(Обязательно)
(Введите FQDN, IP-адрес или имя узла)

Организация

Подразделение

Город/район

Штат/область

Страна/регион

(Например, US для США)

☐ Настройка дополнительного раздела

SubjectAltName

☒ Авто (Регистрация IPv4)
☐ Вручную

Алгоритм с использованием открытых ключей

RSA (2048 бит)

Алгоритм выборки

SHA-256

Отмена

Отправить



Примечание

- Длина поля **Общее название** не должна превышать 64 знака. Введите идентификатор, такой как IP-адрес, имя узла или имя домена, чтобы использовать его при доступе к аппарату через соединение по протоколу SSL/TLS. По умолчанию отображается имя узла. Поле **Общее название** является обязательным для заполнения.
- При вводе в адресе URL имени, отличного от имени в поле «Общее название», использованного для сертификата, будет отображаться предупреждающее сообщение.
- Длина полей **Организация**, **Подразделение**, **Город/район** и **Страна/регион** не должна превышать 64 знака.
- В поле **Страна/регион** необходимо указать код страны, состоящий из двух символов, в соответствии со стандартом ISO 3166.
- Если выполняется настройка расширения сертификата X.509v3, установите флажок в поле **Настройка дополнительного раздела**, а затем выберите **Авто (Регистрация IPv4)** или **Вручную**.

- 3 В выпадающем списке можно выбрать значения параметров **Алгоритм с использованием открытых ключей** и **Алгоритм**. Настройки по умолчанию: **RSA (2048 бит)** для **Алгоритм с использованием открытых ключей** и **SHA-256** для **Алгоритм**.
- 4 Нажмите **Отправить**. Откроется следующий экран.

[Создать CSR \(запрос на подпись сертификата\)](#)

Подождите.



- 5 Через несколько секунд вы получите сертификат, который можно сохранить в небольшой файл или скопировать и вставить непосредственно в он-лайн форму CSR, предоставленную Центром сертификации. Нажмите **Сохранить** для сохранения файла CSR на компьютер.

CSR (запрос на подпись сертификата)

```
-----BEGIN CERTIFICATE REQUEST-----
MIICXzCCAUCCAQAwGjEYMBYGA1UEAxMPQ1JOMDAxQkE5OEJCRDUzMIIIBjAMBgkq
hk1G9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlvcaxs9e9F5dKPaasJPL5VAFezhLYf00
URFbcrn+u0tKlvr00dUo/F3xP60AOTWmDMpp5xwGbnqUE+5SPV5tlzc5ciq90k
fIup8jKy190sV7k1oXkg3ad4G2Vi3++ev0tnLgy1iayv0+0aGG9eyHdpp44qWUg
y6mZepBduLS8Q52KjMlHsCHXy2CqjeWEXhniXducP3l5yypxGS/t0kx/WiYTaxB1P
+Qv1v0n1MAqbAVUXoCh855awFTl1g0l1pyUbMdJfKln00ppBi0WscPWLnGpS0escN
bMam3egEM18JgUnlR+77mZsZa18uh508rVvxfwxv3297ahp0K153zQIDAQABoAAw
DQYJKoZIhvcNAQELBQADggEBAE87zHsnUczPpLinkimPhTtxy19RvdLIGt+C38b8
Y0yPho7jT9g4k/CEXDE8GnspOwdTI/SyrAvFXisEn4i9zRvPCE9lwIsmF/xFOEbw
ULAqbAzy+Qm0DVCLc2LF2i6lRr4JNkKFc15Qoa09g4JBG34/6Nh5qt3WqMcXWSf1
hyHJkM4EWfpx2JRh5o+PUst0QTLDo2aAv8KKBKBoNo2syNkurzPr3T0+oJ6K0rW
a1MjY1K00tmdo5mCoiBFb2pvaQcRdJhsvCalovVvadoSpD4TF7UU4e4LA02GQKa
CfkC0zCOTQ2v0zZq2LEKYMPF6Gj6Br0mZdrQPROw0eCWRQ=
-----END CERTIFICATE REQUEST-----
```

Вернуться

Сохранить



Примечание

Чтобы отправить запрос на подпись сертификата в центр сертификатов, выполните соответствующие указания своего ЦС.

- 6 Запрос на подпись сертификата создан. Инструкции по установке сертификата на аппарат см. в разделе *Установка сертификата на аппарат* ►► стр. 10.

Установка сертификата на аппарат

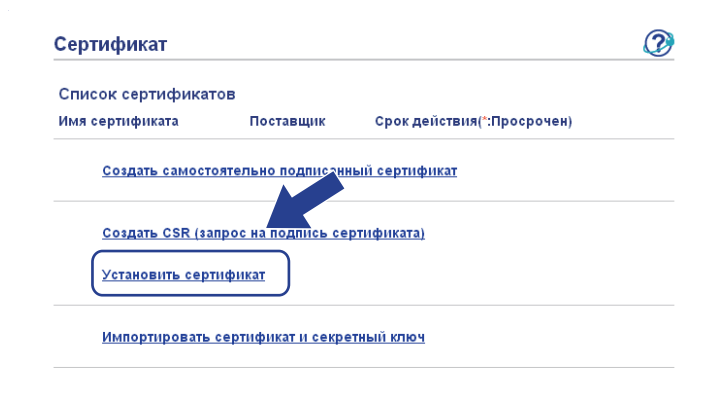
При получении сертификата из ЦС выполните следующие действия, чтобы установить полученный сертификат на сервер печати.



Примечание

Возможна установка только того сертификата, который был получен по запросу, отправленному с этого аппарата. Если необходимо создать еще один запрос на подпись сертификата, перед созданием убедитесь, что сертификат установлен. После установки сертификата на аппарат создайте другой запрос на подпись сертификата. В противном случае созданный перед установкой CSR будет недействительным.

- 1 Нажмите **Установить сертификат** на странице **Сертификат**.



- 2 Укажите файл сертификата, выданный ЦС, и нажмите **Отправить**.
- 3 Теперь создание и установка сертификата в память аппарата завершены успешно. Чтобы использовать связь по протоколу SSL/TLS, на компьютере необходимо установить корневой сертификат, полученный из ЦС. Чтобы получить консультацию по его установке, обратитесь к сетевому администратору. Настройка параметров цифрового сертификата завершена. Для отправки и получения сообщений электронной почты с использованием SSL см. *Безопасная отправка или получение (для моделей DCP и MFC) сообщений электронной почты* >> стр. 26, где указаны необходимые этапы настройки.

Выбор сертификата

После установки сертификата следуйте процедуре, описанной ниже, чтобы выбрать необходимый сертификат.

- 1 Нажмите **Сеть**.
- 2 Нажмите **Протокол**.
- 3 Нажмите **Настройки сервера HTTP** и выберите сертификат из раскрывающегося списка **Выбор сертификата**.

Настройки сервера HTTP

Если требуется безопасное соединение, рекомендуется использовать SSL.
(Рекомендуемые настройки безопасности будут заданы после выбора сертификата.)

Выбор сертификата Предустановка ▾
(Можно выбрать или отменить выбор следующих протоколов для сертификата SSL.)

Система управления через веб-интерфейс

☒ HTTPS(Порт 443)
☒ HTTP(Порт 80)

IPP

☒ HTTPS(Порт 443)
☒ HTTP
☒ Порт 80
☒ Порт 631

Веб-службы

☒ HTTP

[Сертификат](#)

Отмена Отправить



Примечание

- Если открывается данное диалоговое окно, Brother рекомендует отключить протоколы Telnet, FTP, TFTP и сетевое управление со старыми версиями BRAdmin Professional (2.8 и ранее) для защиты связи. Если они будут включены, то аутентификация пользователя будет производиться в небезопасном режиме.

Протокол(Низкий уровень безопасности)

Для обеспечения связи с высокой степенью безопасности рекомендуется отключить протоколы.

Чтобы отключить протокол, снимите соответствующий флажок.

☒ Telnet

☒ FTP(Включая функцию "Сканировать на FTP")

☒ TFTP

Программа BRAdmin использует SNMP.

Использование SNMP обеспечивает "доступ на чтение-запись SNMPv3" для высокой степени защиты.

Если протокол не используется, удалите соответствующий флажок.

☒ SNMP

Отмена

Отправить

- Для моделей DCP и MFC:
Если отключить FTP, функция "Сканировать на FTP" будет также отключена.

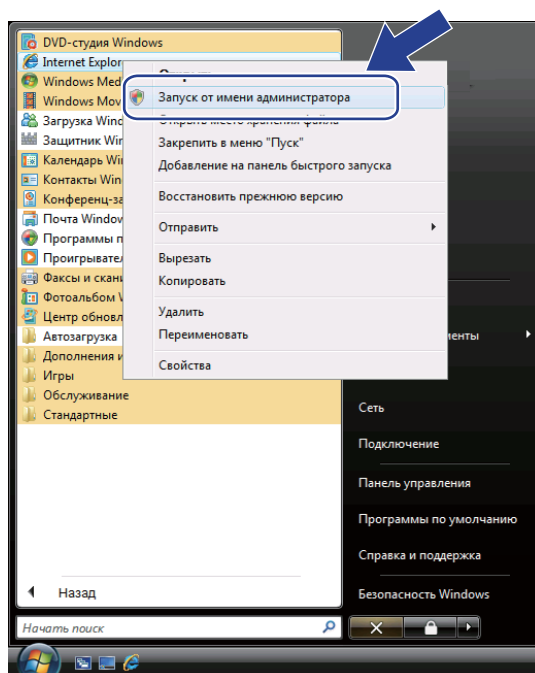
4 Нажмите **Отправить**.

Установка самозаверяющего или предварительно установленного сертификата в Windows Vista®, Windows® 7 и Windows Server® 2008 для пользователей с правами администратора

Примечание

- При работе в программе Windows® Internet Explorer® необходимо выполнить следующие шаги. При использовании другого веб-браузера следует обратиться к справке этого браузера.
- Для установки самозаверяющего или предварительно установленного сертификата необходимо иметь права администратора.

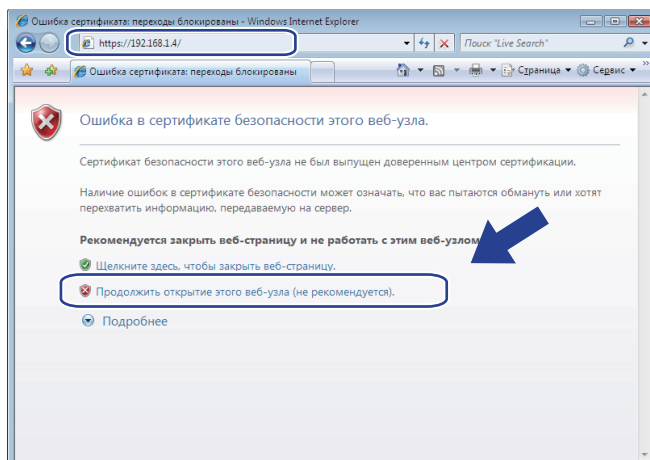
- 1 Нажмите кнопку  и **Все программы**.
- 2 Нажмите правой кнопкой мыши **Internet Explorer**, затем выберите **Запуск от имени администратора**.



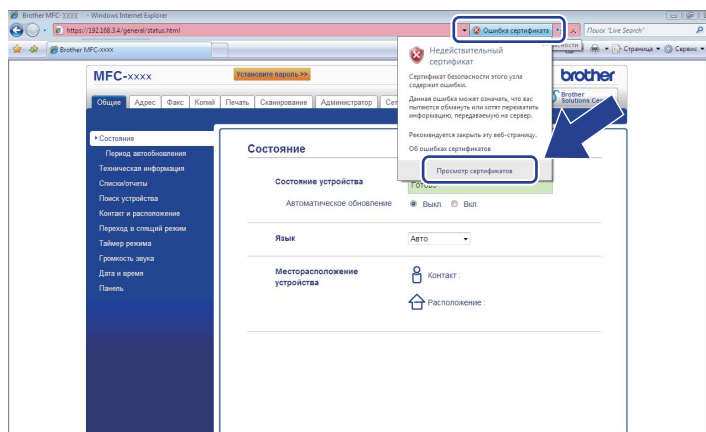
Примечание

Если откроется экран **Контроль учетных записей пользователей**,
(Windows Vista®) Щелкните **Продолжить (Разрешить)**.
(Windows® 7) Щелкните **Да**.

- 3 Чтобы получить доступ к аппарату, введите в браузере “https://IP-адрес аппарата/” (где “IP-адрес аппарата” – это IP-адрес или имя узла, назначенное для сертификата). После этого нажмите **Продолжить открытие этого веб-узла (не рекомендуется)**.

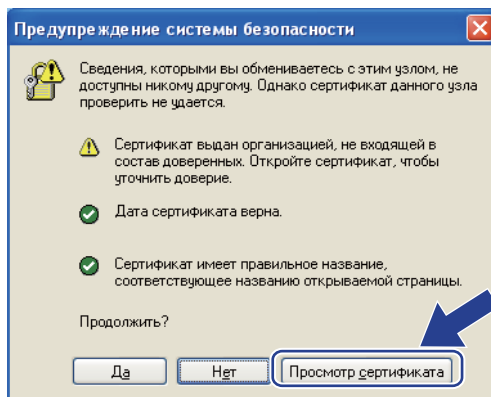


- 4 Нажмите **Ошибка сертификата**, а затем **Просмотр сертификатов**. Чтобы выполнить остальные инструкции, выполните шаги с пункта 4 в разделе *Установка самозаверяющего или предварительно установленного сертификата в Windows® XP и Windows Server® 2003* ➤➤ стр. 15.

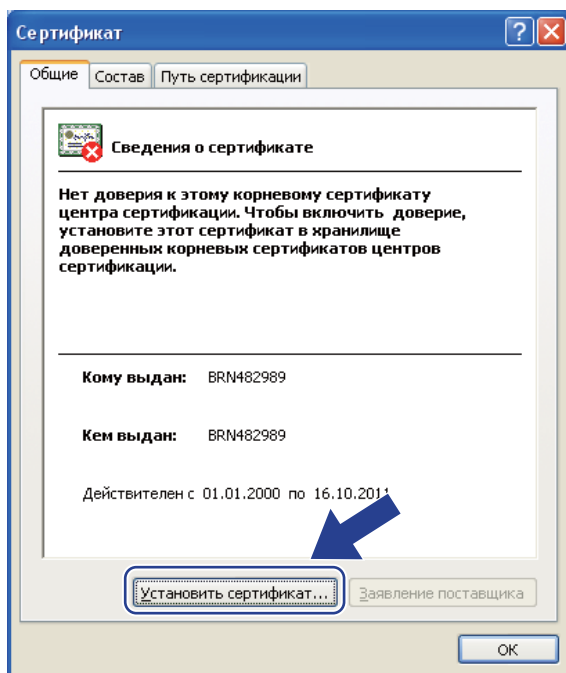


Установка самоверяющего или предварительно установленного сертификата в Windows® XP и Windows Server® 2003

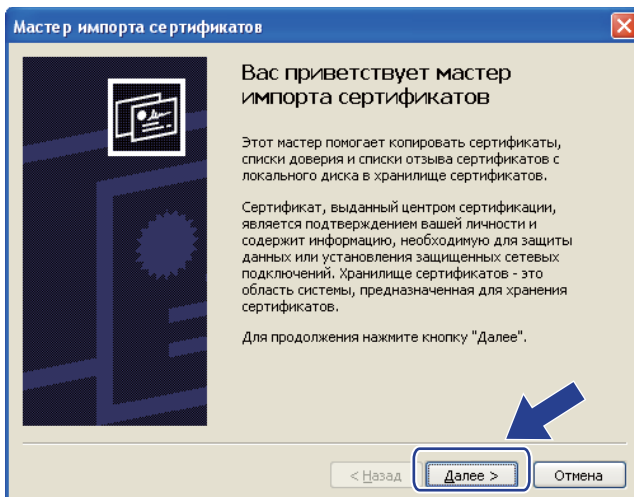
- 1 Запустите веб-браузер.
- 2 Чтобы получить доступ к аппарату, введите в браузере “https://IP-адрес аппарата/” (где “IP-адрес аппарата” – это IP-адрес или имя узла, назначенное для сертификата).
- 3 При появлении диалогового окна с предупредительным сообщением, произведите одно из указанных действий:
 - Нажмите **Продолжить открытие этого веб-узла (не рекомендуется)**.. Нажмите **Ошибка сертификата**, а затем **Просмотр сертификатов**.
 - Если появится указанное диалоговое окно, нажмите **Просмотр сертификата**.



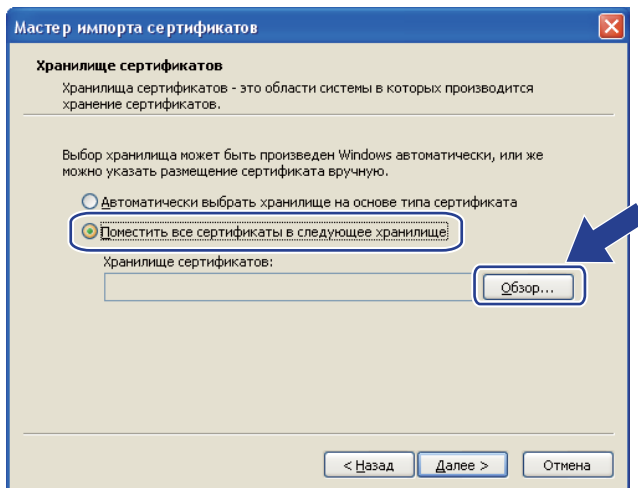
- 4 Нажмите **Установить сертификат...** на вкладке **Общие**.



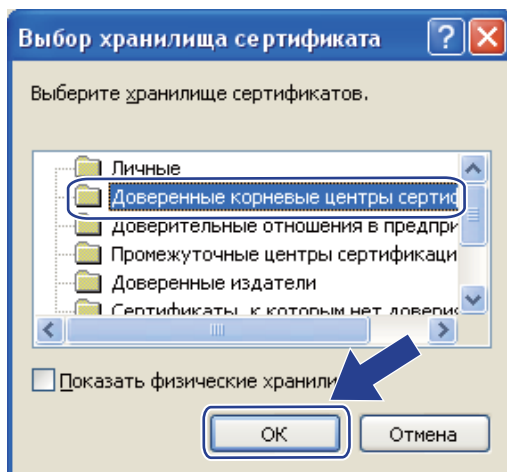
- 5 Когда отобразится **Мастер импорта сертификатов**, нажмите **Далее**.



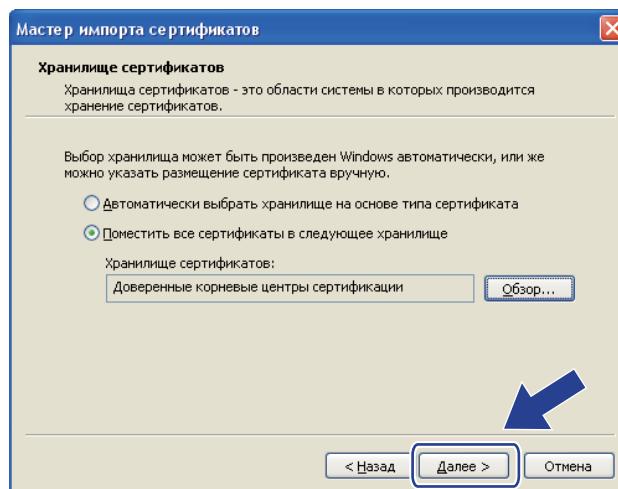
- 6 Для установки сертификата надо указать местоположение. Рекомендуем выбрать **Поместить все сертификаты в следующее хранилище**, и затем нажать **Обзор...**



- 7 Выберите **Доверенные корневые центры сертификации**, а затем нажмите **ОК**.



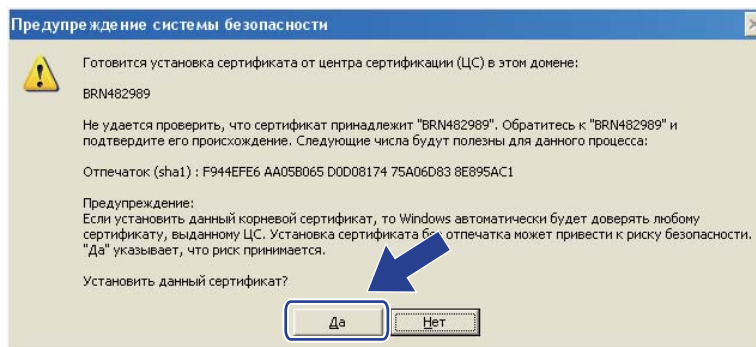
8 Нажмите **Далее**.



9 В следующем окне нажмите **Готово**.

10 Появится запрос установить сертификат. Выполните одно из следующих действий:

- При установке самозаверяющего сертификата подтвердите отпечаток пальца (отпечаток большого пальца) и нажмите **Да**.
- При установке предварительно установленного сертификата нажмите **Да**.



Примечание

- Отпечаток пальца (отпечаток большого пальца) для самозаверяющего сертификата печатается в отчёте конфигурации сети.

Для получения информации о печати отчёта конфигурации сети см. раздел *Печать страницы параметров принтера (для модели HL-5450DN(T))* >> стр. 30 или *Печать отчёта конфигурации сети (для других моделей)* >> стр. 30.

- Отпечаток пальца для предварительно установленного сертификата не печатается в Отчёте конфигурации сети.

11 Нажмите **ОК**.

12 Теперь самозаверяющий или предварительно установленный сертификат установлен на компьютере, и имеется возможность осуществлять связь по протоколу SSL/TLS.

Эту процедуру нужно производить на каждом компьютере, с которого должна вестись безопасная печать. Однако после установки эти действия повторять уже не нужно, если сертификат не изменяется.

Импорт и экспорт сертификата и секретного ключа

В аппарате можно хранить сертификат и секретный ключ и управлять ими с помощью импорта и экспорта.

Импорт самозаверяющего сертификата, сертификата, выданного сторонним ЦС, и закрытого ключа

- 1 Нажмите **Импортировать сертификат и секретный ключ** на странице **Сертификат**.
- 2 Укажите файл, который необходимо импортировать.
- 3 Введите пароль, если файл зашифрован, и нажмите **Отправить**.
- 4 Теперь сертификат и секретный ключ успешно импортированы в аппарат.

Экспорт самозаверяющего сертификата, сертификата, выданного сторонним ЦС, и закрытого ключа

- 1 Нажмите **Экспорт** рядом с полем **Список сертификатов** на странице **Сертификат**.
- 2 Введите пароль, если необходимо зашифровать файл.



Примечание

Если пароль не используется, то шифровка файла не будет выполнена.

- 3 Введите пароль повторно для подтверждения и нажмите **Отправить**.
- 4 Укажите, где необходимо сохранить файл.
- 5 Теперь сертификат и секретный ключ экспортированы в компьютер.

Импорт и экспорт сертификата ЦС

В аппарате можно хранить сертификат ЦС и осуществлять их импорт и экспорт.

Импорт сертификата ЦС

- 1 Нажмите **Сертификата ЦС** на странице **Безопасность**.
- 2 Нажмите **Импорт сертификата ЦС** и выберите сертификат. Нажмите **Отправить**.

Экспорт сертификата ЦС

- 1 Нажмите **Сертификата ЦС** на странице **Безопасность**.
- 2 Выберите сертификат, который требуется экспортировать, и нажмите **Экспорт**. Нажмите **Отправить**.
- 3 Нажмите **Сохранить** для выбора целевой папки.
- 4 Выберите путь сохранения экспортируемого сертификата и произведите его сохранение.

Управление несколькими сертификатами

Функция управления несколькими сертификатами позволяет управлять каждым сертификатом, установленным с помощью системы управления через веб-интерфейс. После установки сертификатов можно видеть, какие сертификаты установлены со страницы **Сертификат**, а затем просмотреть содержимое каждого сертификата, удалить и или экспортировать сертификат. Для получения информации о доступе к стр. **Сертификат** см. раздел *Установка цифрового сертификата* >> стр. 4.

■ Для моделей принтеров

Аппарат Brother позволяет хранить до трех самозаверяющих сертификатов или до трёх сертификатов, выданных ЦС. Сохранённые сертификаты можно использовать для работы с протоколом HTTPS/IPPS или аутентификации IEEE 802.1x.

■ Для моделей DCP и MFC

Аппарат Brother позволяет хранить до четырёх самозаверяющих сертификатов или до четырёх сертификатов, выданных ЦС. Сохранённые сертификаты можно использовать для работы с протоколом HTTPS/IPPS, аутентификации IEEE 802.1x или PDF с цифровой подписью.

Можно также хранить до четырех сертификатов ЦС для использования аутентификации IEEE 802.1x и протокола SSL для SMTP/POP3.

Рекомендуется хранить на один сертификат меньше максимального числа, чтобы иметь одно свободное место в случае истечения срока действия сертификата. Например, если необходимо хранить сертификат ЦС, храните три сертификата и оставьте одну ячейку хранения в качестве резервной. В этом случае при повторной выдаче сертификата, например в случае истечения срока его действия, можно будет импортировать новый сертификат в резервную ячейку, а затем удалить истекший сертификат, чтобы избежать сброса настроек.



Примечание

- При использовании HTTPS/IPPS, IEEE 802.1x или PDF с цифровой подписью (для моделей DCP и MFC) необходимо выбрать сертификат, который будет использоваться.
- При использовании SSL для связи SMTP/POP3 (для моделей DCP и MFC) выбирать сертификат не требуется. Необходимый сертификат будет выбран автоматически.

Для безопасного управления сетевым аппаратом необходимо использовать утилиты управления с протоколами безопасности.

Безопасное управление с помощью системы управления через веб-интерфейс (веб-браузер)

Для безопасного управления рекомендуется использовать протокол HTTPS. Чтобы использовать эти протоколы, необходимо настроить следующие параметры аппарата.



Примечание

- По умолчанию протокол HTTPS включен.

Параметры протокола HTTPS и необходимый для использования сертификат можно изменить на экране управления через веб-интерфейс, нажав **Сеть**, **Протокол**, и затем нажав **Настройки сервера HTTP**.

- Вы также должны установить сертификат, установленный на аппарат, на свой компьютер. См. раздел *Установка самоподписанного или предварительно установленного сертификата в Windows Vista®*, *Windows® 7* и *Windows Server® 2008 для пользователей с правами администратора* >> стр. 13 или раздел *Установка самоподписанного или предварительно установленного сертификата в Windows® XP* и *Windows Server® 2003* >> стр. 15.

- 1 Запустите веб-браузер.
- 2 Введите в браузере “http://IP-адрес аппарата/”. (При использовании созданного сертификата, введите в браузер “https://стандартное имя”. Где “стандартное имя” – это имя, назначенное сертификату в поле «Общее название», например IP-адрес, имя узла или имя домена. О назначении стандартного имени для сертификата см. раздел *Использование сертификатов для защиты устройств* >> стр. 2.)

■ Пример:

https://192.168.1.2/ (если стандартным именем является IP-адрес аппарата)

- 3 По умолчанию пароль не требуется. Введите пароль, если он установлен, и нажмите кнопку ➡.

Безопасная печать документов с использованием протокола IPPS для Windows®

Для безопасного управления рекомендуется использовать протокол IPPS. Чтобы использовать протокол IPPS, необходимо настроить следующие параметры аппарата.



Примечание

- Соединение с использованием протокола IPPS не может предотвратить несанкционированный доступ к серверу печати.
- Вы также должны установить сертификат, установленный на аппарат, на свой компьютер. См. раздел *Установка самозаверяющего или предварительно установленного сертификата в Windows Vista®, Windows® 7 и Windows Server® 2008 для пользователей с правами администратора* >> стр. 13 или раздел *Установка самозаверяющего или предварительно установленного сертификата в Windows® XP и Windows Server® 2003* >> стр. 15.
- Протокол IPPS должен быть включен. Активированы настройки по умолчанию. Параметры протокола IPPS и необходимый для использования сертификат можно изменить на экране управления через веб-интерфейс, нажав **Сеть**, **Протокол**, и затем нажав **Настройки сервера HTTP**.

Windows® XP и Windows Server® 2003

- 1 Нажмите кнопку **Пуск**, затем выберите **Принтеры и факсы**.
- 2 Нажмите **Установка принтера** для запуска **Мастер установки принтеров**.
- 3 После отображения экрана **Далее** нажмите **Мастер установки принтеров**.
- 4 Выберите **Сетевой принтер или принтер, подключенный к другому компьютеру**.
- 5 Нажмите **Далее**.
- 6 Выберите **Подключиться к принтеру в Интернете, в домашней сети или в интрасети** и в поле URL введите следующее:
“https://IP-адрес/ipp аппарата” (где “IP-адрес аппарата” - это IP-адрес аппарата или имя узла).



Примечание

- Важно использовать “https://”, а не “http://”, иначе печать по IPP не будет безопасной.
- Если на компьютере отредактирован файл хостов или используется Domain Name System (DNS – система имен доменов), для сервера печати можно ввести имя DNS. Поскольку сервер печати поддерживает имена TCP/IP и NetBIOS, для него можно указать и имя NetBIOS сервера печати. Имя NetBIOS отображается в Отчёте конфигурации сети. (Для получения информации о печати отчёта конфигурации сети см. раздел *Печать страницы параметров принтера (для модели HL-5450DN(T))* >> стр. 30 или *Печать отчёта конфигурации сети (для других моделей)* >> стр. 30). Назначенное имя NetBIOS состоит из первых 15 символов имени узла и по умолчанию оно имеет вид “BRNxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxx” – это MAC-адрес / адрес Ethernet аппарата.)

7

Если нажать **Далее**, Windows® XP и Windows Server® 2003 установят соединение с указанным URL-адресом.

- Если драйвер принтера уже установлен:

В окне **Мастер установки принтеров** появится экран выбора принтера.

Перейдите к шагу 11.

- Если драйвер принтера НЕ установлен

Одним из преимуществ протокола печати IPP является то, что при соединении он определяет название модели принтера. После успешного соединения название модели принтера отобразится автоматически. Следовательно, в Windows® XP и Windows Server® 2003 не требуется указывать тип используемого драйвера принтера.

Перейдите к шагу 8.



Примечание

Если устанавливаемый драйвер принтера не имеет цифрового сертификата, появится предупреждающее сообщение. Чтобы продолжить установку, нажмите **Все равно продолжить**.

8

Нажмите **Установить с диска**. Появится запрос диска с драйвером.

9

Нажмите **Обзор** и выберите соответствующий драйвер принтера Brother с прилагаемого компакт-диска или общей сетевой папки.

Нажмите **ОК**.

10

Нажмите **ОК**.

11

Выберите аппарат и нажмите **ОК**.

12

Выберите **Да**, если данный аппарат будет использоваться в качестве принтера по умолчанию. Нажмите **Далее**.

13

Нажмите **Готово**, и аппарат будет настроен и готов к печати. Чтобы проверить подключение принтера, распечатайте тестовую страницу.

Windows Vista®, Windows® 7 и Windows Server® 2008

- 1 (ОС Windows Vista®)
Нажмите кнопку , выберите **Панель управления, Оборудование и звук, а затем Принтеры.**
(ОС Windows® 7)
Нажмите кнопку , а затем **Устройства и принтеры.**
(ОС Windows Server® 2008)
Нажмите кнопку **Пуск, Панель управления, Оборудование и звук и затем Принтеры.**
- 2 Нажмите **Установка принтера.**
- 3 Выберите **Добавить сетевой, беспроводной или Bluetooth-принтер.**
- 4 Нажмите **Нужный принтер отсутствует в списке.**
- 5 Выберите **Выбрать общий принтер по его имени**, после чего введите следующий адрес в поле URL: “https://IP-адрес/ipp аппарата” (где “IP-адрес аппарата” - это IP-адрес аппарата или имя узла).



Примечание

- Важно использовать “https://”, а не “http://”, иначе печать по IPP не будет безопасной.
- Если на компьютере отредактирован файл хостов или используется Domain Name System (DNS – система имен доменов), для сервера печати можно ввести имя DNS. Поскольку сервер печати поддерживает имена TCP/IP и NetBIOS, для него можно указать и имя NetBIOS сервера печати. Имя NetBIOS отображается в Отчёте конфигурации сети. (Для получения информации о печати отчёта конфигурации сети см. раздел *Печать страницы параметров принтера (для модели HL-5450DN(T))* >> стр. 30 или *Печать отчёта конфигурации сети (для других моделей)* >> стр. 30). Назначенное имя NetBIOS состоит из первых 15 символов имени узла и по умолчанию оно имеет вид “BRNxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxx” – это MAC-адрес / адрес Ethernet аппарата.)

- 6 Нажмите кнопку **Далее** и ОС Windows Vista® и Windows Server® 2008 установит соединение с указанным URL-адресом.

- Если драйвер принтера уже установлен:

В окне мастера установки принтеров появится экран выбора принтера. Нажмите **ОК**.

Если соответствующий драйвер принтера уже установлен на компьютере, ОС Windows Vista® и Windows Server® 2008 будут автоматически использовать этот драйвер. В этом случае появится запрос на установку этого драйвера по умолчанию, после чего работа мастера установки драйверов будет завершена. После этого принтер готов к печати.

Перейдите к шагу 11.

■ Если драйвер принтера НЕ установлен

Одним из преимуществ протокола печати IPP является то, что при соединении он определяет название модели принтера. После успешного соединения название модели принтера отобразится автоматически. Следовательно, в ОС Windows Vista® и Windows Server® 2008 не требуется указывать тип используемого драйвера принтера.

Перейдите к шагу 7.

- 7 Если аппарат отсутствует в списке поддерживаемых принтеров, нажмите **Установить с диска**. Появится запрос диска с драйвером.
- 8 Нажмите **Обзор** и выберите соответствующий драйвер принтера Brother с прилагаемого компакт-диска или общей сетевой папки. Нажмите **Открыть**.
- 9 Нажмите **ОК**.
- 10 Укажите название модели аппарата. Нажмите **ОК**.



Примечание

- Когда отобразится экран контроля учетных записей пользователей, нажмите **Продолжить**.
 - Если устанавливаемый драйвер принтера не имеет цифрового сертификата, появится предупреждающее сообщение. Чтобы продолжить установку, нажмите **Все равно установить этот драйвер**. После этого работа **установка принтера** будет завершена.
-
- 11 В мастере **Установка принтера** появится экран **Введите имя принтера**. Установите флажок в поле **Использовать этот принтер по умолчанию**, если нужно использовать данный аппарат в качестве принтера по умолчанию, после чего нажмите **Далее**.
 - 12 Чтобы проверить подключение принтера, нажмите **Печать пробной страницы**, а затем **Готово**. Аппарат настроен и готов к печати.

Безопасная отправка или получение (для моделей DCP и MFC) сообщений электронной почты

Настройка с помощью системы управления через веб-интерфейс (веб-браузер)

На экране системы управления через веб-интерфейс можно настроить безопасную отставку электронной почты с помощью аутентификации пользователя или отставку и получение (для моделей DCP и MFC) электронной почты с помощью SSL/TLS.

- 1 Запустите веб-браузер.
- 2 В браузере введите “http://IP-адрес аппарата/” (где “IP-адрес аппарата” соответствует IP-адресу аппарата).
 - Пример:
http://192.168.1.2/
- 3 По умолчанию пароль не требуется. Введите пароль, если он установлен, и нажмите кнопку ➡.
- 4 Нажмите **Сеть**.
- 5 Нажмите **Протокол**.
- 6 Нажмите **Дополнительные параметры** в **POP3/SMTP** и убедитесь, что для параметра **POP3/SMTP** установлено значение **Включено**.
- 7 На этой странице можно настроить параметры **POP3/SMTP**.



Примечание

- Для получения дополнительной информации обратитесь к справке системы управления через веб-интерфейс.
 - Можно подтвердить правильность параметров электронной почты после их настройки, отправив тестовое сообщение электронной почты.
 - Если настройки POP3-/SMTP-сервера неизвестны, для получения дополнительной информации обратитесь к системному администратору или провайдеру Интернета.
-
- 8 После настройки нажмите **Отправить**. Появится экран **Проверить конфигурацию отправки электронной почты** или **Проверить конфигурацию отправки/получения электронной почты**.
 - 9 При необходимости выполнения теста с текущими параметрами следуйте инструкциям, отображаемым на экране.

Безопасная отправка или получение (для моделей DCP и MFC) сообщений электронной почты с использованием SSL/TLS

Данный аппарат поддерживает методы SSL/TLS для отправки или получения (для моделей DCP и MFC) электронной почты через сервер электронной почты, требующий наличия защиты связи SSL/TLS. Для отправки или получения электронной почты через сервер электронной почты, использующий связь SSL/TLS, необходимо правильно настроить SMTP с использованием SSL/TLS или POP3 с использованием SSL/TLS.

Проверка подлинности сертификата сервера

- Если для параметра **SMTP через SSL/TLS** или **POP3 через SSL/TLS** установлено значение SSL или TLS, произойдет автоматическая установка флажка **Проверять сертификат сервера** для проверки подлинности сертификата сервера.
 - Перед проверкой подлинности сертификата сервера необходимо импортировать сертификат ЦС, выданный тем ЦС, который подписал сертификат сервера. При необходимости импорта сертификата ЦС обратитесь к администратору сети или к поставщику услуг Интернета. Для получения информации об импорте сертификата см. раздел *Импорт и экспорт сертификата ЦС* >> стр. 19.
 - Если нет необходимости проверять подлинность сертификата сервера, снимите флажок **Проверять сертификат сервера**.

Номер порта

- При выборе SSL или TLS значения параметров **Порт SMTP** или **Порт POP3** автоматически изменятся, чтобы соответствовать протоколу. Если необходимо изменить номер порта вручную, введите номер порта после выбора параметра **SMTP через SSL/TLS** или **POP3 через SSL/TLS**.
- Протокол соединения POP3/SMTP необходимо настроить так, чтобы он совпадал с протоколом сервера электронной почты. Для получения подробной информации о параметрах сервера электронной почты обратитесь к администратору сети или поставщику услуг Интернета. В большинстве случаев для служб защищенной передачи электронной почты требуется установка следующих параметров.
 - **SMTP**
 - Порт SMTP: 587
 - Способ аутентификации сервера SMTP: SMTP-AUTH
 - SMTP с использованием SSL/TLS: TLS
 - **POP3**
 - Порт POP3: 995
 - POP3 с использованием SSL/TLS: SSL

Обзор

В этой главе рассказывается об устранении возможных проблем сети, с которыми можно столкнуться при эксплуатации аппарата Brother. Если после прочтения этой главы возникшая проблема не будет решена, посетите веб-сайт Brother Solutions Center по адресу: (<http://solutions.brother.com/>).

Для загрузки других руководств посетите Brother Solutions Center по адресу (<http://solutions.brother.com/>) и на странице соответствующей модели нажмите «Руководства».

Определение проблемы

Перед чтением этой главы выполните следующие действия.

Сначала проверьте следующее:

Кабель питания подсоединен правильно и аппарат Brother включен.

Вся защитная упаковка снята с аппарата.

Тонер-картриджи и фотобарабан установлены правильно.

Передняя и задняя крышки плотно закрыты.

Бумага правильно вставлена в лоток для бумаги.

Аппарат подключен к сети надлежащим образом.

Перейдите на страницы решения проблем, указанные ниже

- Не получается напечатать документ по Интернету с использованием IPPS.

См. раздел *Не получается напечатать документ по Интернету с использованием IPPS*.
 >> стр. 29.

- Необходимо проверить надлежащее функционирование используемых сетевых устройств.

См. раздел *Необходимо проверить надлежащее функционирование используемых сетевых устройств*. >> стр. 29.

Не получается напечатать документ по Интернету с использованием IPPS.

Вопрос	Решение
Не получается связаться с аппаратом Brother с использованием SSL.	■ Получите действующий сертификат и установите его ещё раз на аппарате и компьютере. ■ Убедитесь, что настройки порта для аппарата корректны. Параметры порта вашего аппарата можно подтвердить на экране управления через веб-интерфейс, нажав Сеть, Протокол, а затем нажав Настройки сервера HTTP.

Необходимо проверить надлежащее функционирование используемых сетевых устройств.

Вопрос	Решение
Включен ли ваш аппарат Brother?	Убедитесь, что соблюдены все инструкции в разделе <i>Сначала проверьте следующее</i> : ►► стр. 28.
Как можно узнать сетевые параметры имеющегося аппарата Brother, например IP-адрес?	Напечатайте отчёт конфигурации сети. См. раздел <i>Печать страницы параметров принтера (для модели HL-5450DN(T))</i> ►► стр. 30 или раздел <i>Печать отчёта конфигурации сети (для других моделей)</i> ►► стр. 30.

Печать страницы параметров принтера (для модели HL-5450DN(T))



Примечание

Имя узла: имя узла отображается в отчете конфигурации сети. По умолчанию имя узла — “BRNxxxxxxxxxxxx”. (“xxxxxxxxxxxx” — это MAC-адрес / адрес Ethernet аппарата.)

Страница параметров принтера позволяет напечатать отчет, содержащий все текущие параметры принтера, в том числе параметры сетевого сервера печати.

Печать страницы параметров принтера можно выполнить с помощью кнопки **Go** на аппарате.

- 1 Убедитесь, что передняя крышка закрыта и кабель питания подключен.
- 2 Включите аппарат и дождитесь, пока он перейдет в режим готовности.
- 3 В течение 2 секунд три раза нажмите кнопку **Go**. Аппарат распечатает страницу текущих параметров принтера.

6

Печать отчёта конфигурации сети (для других моделей)



Примечание

Имя узла: имя узла отображается в отчете конфигурации сети. По умолчанию используется имя узла “BRNxxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxxx” — это MAC-адрес / адрес Ethernet аппарата.)

Отчет конфигурации сети позволяет напечатать отчет, содержащий все текущие параметры конфигурации сети, в том числе параметры сетевого сервера печати.

Для моделей HL-5470DW(T) и HL-6180DW(T)

- 1 С помощью ▲ или ▼ выберите **Инф. об уст-ве**.
Нажмите клавишу **OK**.
- 2 С помощью ▲ или ▼ выберите **Печать сет.настр.**.
Нажмите клавишу **OK**.

Для моделей DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW, MFC-8910DW

- 1 Нажмите клавишу **Меню**.
- 2 (Для моделей MFC) С помощью кнопок ▲ и ▼ выберите Печать отчетов.
(Для моделей DCP) С помощью кнопок ▲ и ▼ выберите Инф. об уст-ве.
Нажмите клавишу **ОК**.
- 3 С помощью ▲ или ▼ выберите Конфигур. сети.
Нажмите клавишу **ОК**.
- 4 Нажмите клавишу **Старт**.

Для моделей DCP-8250DN и MFC-8950DW(T)

- 1 Нажмите клавишу **Меню**.
- 2 С помощью кнопок ▲ и ▼ отобразите Печать отчетов, а затем нажмите Печать отчетов.
- 3 Нажмите клавишу Сетев. конфиг..
- 4 Нажмите клавишу **Старт**.



Примечание

Если для параметра **IP Address** в отчете конфигурации сети отображается **0.0.0.0**, подождите в течение минуты, затем повторите попытку.

Сетевые термины и понятия

Технический обзор SSL

Secure Socket Layer (SSL – уровень защищенных сокетов) - это способ защиты данных транспортного уровня, передаваемых по локальной или региональной сети с использованием протокола Internet Printing Protocol (IPP – протокол печати через Интернет), предотвращающий прочтение документов неавторизованными пользователями.

Это достигается за счёт использования протоколов аутентификации в виде одного из двух цифровых ключей:

- Открытый ключ, известный всем, кто осуществляет печать.
- Секретный ключ, известный только аппарату, производящему дешифровку пакетов и возврат к виду, читаемому аппаратом.

Открытый ключ использует шифрование 1024 бит или 2048 бит и хранится в цифровом сертификате. Эти сертификаты могут быть самозаверяющими или подтверждёнными Центром сертификации (ЦС).

Прежде всего, существует три вида ключей - секретные, открытые и общие.

Секретный ключ, известный только аппарату, привязан к открытому ключу, но не хранится в цифровом сертификате клиента (отправителя). Когда соединение устанавливается впервые, аппарат отправляет открытый ключ вместе с сертификатом. Клиентский ПК считает, что открытый ключ получен от аппарата с сертификатом. Клиент генерирует общий ключ и шифрует его с использованием открытого ключа, а затем отправляет на аппарат. Аппарат шифрует общий ключ вместе с секретным ключом. Теперь аппарат и клиент совместно используют общий защищённый ключ, и установлено безопасное соединение для передачи данных для печати.

Данные для печати шифруются и дешифруются с использованием общего ключа.

SSL не будет предотвращать доступ неавторизованных пользователей к пакетам, однако, они будут нечитаемыми без закрытого ключа, который не известен никому, кроме аппарата.

Его можно настроить как для проводных, так и для беспроводных сетей, и он совместим с другими методами защиты, например, ключами WPA и брандмауэрами при условии корректной настройки.

Сетевая терминология

■ Secure Socket Layer (SSL – уровень защищенных сокетов)

При использовании протокола безопасности соединений данные шифруются с целью предотвращения угрозы их безопасности.

■ Internet Printing Protocol (IPP – протокол печати через Интернет)

IPP - это стандартный протокол печати, используемый для управления и создания заданий печати. Он может использоваться как локально, так и глобально, поэтому печать на одном аппарате может осуществляться из любой точки мира.

■ IPPS

Версию протокола IPP (Internet Printing Protocol – протокол печати через Интернет) версии 1.0 использует SSL.

■ HTTPS

Версию протокола Интернета HTTP (Hyper Text Transfer Protocol – протокол передачи гипертекста) использует SSL.

■ ЦС (центр сертификации)

Центр сертификатов — организация, которая выдает цифровые сертификаты (особенно сертификаты X.509) и гарантирует взаимосвязь между всеми данными, содержащимися в сертификате.

■ CSR (Запрос о подписи сертификата)

Запрос на подпись сертификата (CSR) отправляется от лица-заявителя в центр сертификатов, чтобы имелась возможность применить подпись для выдачи сертификата. В запросе на подпись сертификата содержится информация, идентифицирующая заявителя, открытый ключ, сгенерированный заявителем и цифровая подпись заявителя.

■ Сертификат

Сертификат — это информация, которая объединяет открытый ключ и личность заявителя. Сертификат может использоваться для того, чтобы подтвердить принадлежность открытого ключа определенному лицу. Формат определяется по стандарту x.509.

■ Криптосистема с открытым ключом

Криптосистема с открытым ключом — это современная отрасль криптографии, в которой алгоритм задействует пару ключей (открытый ключ и секретный ключ) и использует компонент из каждой пары для различных шагов реализации алгоритма.

■ Криптосистема с общим ключом

Криптосистема с общим ключом — это отрасль криптографии, использующая алгоритмы, которые задействуют один и тот же ключ для реализации различных шагов алгоритма (таких как шифрование и расшифровка данных).