Ръководство за функциите за сигурност

Съдържание

Въведение

Дефиниции на бележките

В това ръководство за потребителя използваме следните символи и конвенции:

ВАЖНО	ВАЖНО показва потенциално опасна ситуация, която, ако не се избегне, може да доведе до повреда на собственост или загуба на функционалност на продукта.
ЗАБЕЛЕЖКА	ЗАБЕЛЕЖКА посочва работната среда, условията за монтаж или специални условия за употреба.
	Иконите за съвети предоставят полезни препоръки и допълнителна информация.
Получер шрифт	С получер шрифт са посочени бутоните на контролния панел на устройството или на екрана на компютъра.
Курсив	Italicized emphasizes върху важните моменти или представлява позоваване на сродна тема.

Свързана информация

- Въведение

Търговски марки

Adobe® и Reader® са или регистрирани търговски марки, или търговски марки на Adobe Systems Incorporated в САЩ и/или други държави.

Всяка фирма, заглавието на чийто софтуер е споменат в настоящото ръководство, притежава License споразумение за софтуер, специфично за собствените й програми.

Всички търговски имена и имена на продукти на компании, появяващи се в устройства на Brother, както и свързани документи и всякакви други материали, са търговски марки или регистрирани търговски марки на съответните компании.

Свързана информация

- Въведение

Авторски права

Свързана информация

- Въведение

Преди да се използват функциите за защита на мрежата

Устройството използва някои от най-новите налични днес протоколи за мрежова защита и шифроване. Тези мрежови функции могат да бъдат внедрени във вашия цялостен план за мрежова защита, за да помогнат за защитата на данните ви и за предотвратяване на unauthorized достъп до устройството.

Препоръчваме да деактивирате FTP и TFTP протоколите. Достъпът до устройството чрез тези протоколи не е безопасен.

Свързана информация

- Въведение
  - Деактивирайте ненужните протоколи

Деактивирайте ненужните протоколи

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

   Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.
4. Щракнете върху **Network (Мрежа)** > **Network (Мрежа)** > **Protocol (Протокол)** в лявата навигационна лента.

   Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.
5. Премахнете отметките от квадратчетата за ненужните протоколи, за да ги деактивирате.
6. Щракнете върху **Submit (Изпрати)**.
7. Рестартирайте устройството Brother, за да активирате конфигурацията.

Свързана информация

- Преди да се използват функциите за защита на мрежата

Защита на мрежата

Конфигуриране на сертификати за защита на устройството

Трябва да конфигурирате сертификат за безопасно управление на вашето мрежово устройство посредством SSL/TLS. Трябва да използвате уеб базирано управление за конфигуриране на сертификат.

- Преглед на функциите на сертификата за защита
- Как се създава и инсталира сертификат
- Създаване на самоподписан сертификат
- Създаване на искане за подписване на сертификат (CSR) и инсталиране на сертификат от сертифициращ орган (CO)
- Импортиране и експортиране на сертификата и персоналния ключ
- Импортиране и експортиране на CA сертификат

Преглед на функциите на сертификата за защита

Устройството поддържа използването на множество сертификати за защита, което позволява безопасно удостоверяване и комуникация с устройството. Следните функции на сертификата за защита могат да бъдат използвани с устройството:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

- SSL/TLS комуникация
- IEEE 802.1x удостоверяване
- IPsec

Вашето устройство поддържа следните:

- Предварително инсталиран сертификат

  Вашето устройство има предварително инсталиран самоподписан сертификат. Този сертификат ви позволява да използвате SSL/TLS комуникация без създаване или инсталиране на отделен сертификат.

Предварително инсталираният самостоятелно заверен сертификат защитава комуникацията ви до определено ниво. Ние препоръчваме използването на сертификат, издаден от доверена организация, за по-добра сигурност.

- Самоподписан сертификат

  Този сървър за печат издава свой сертификат. Чрез този сертификат можете лесно да използвате SSL/TLS комуникацията без създаване или инсталиране на отделен сертификат от сертифициращ орган.

- Сертификат от сертифициращ орган (CA)

  Има два начина за инсталиране на сертификат от CA. Ако вече имате издаден сертификат от CA или ако искате да използвате сертификат от външен доверен CA:

  - Когато използвате заявка за подписване на сертификат (CSR) от този сървър за печат.
  - Когато импортирате сертификат и частен ключ.

- Сертификат от сертифициращ орган (CA)

  За да използвате сертификат на CO, който идентифицира CO и притежава неговия персонален ключ, вие трябва да импортирате сертификат на CO от CO преди конфигурирането на функциите за защита на мрежата.

- Ако възнамерявате да използвате SSL/TLS комуникация, препоръчваме ви първо да се свържете със системния администратор.
- Когато нулирате фабричните настройки на сървъра за печат, сертификатът и личният ключ, които са инсталирани, ще бъдат изтрити. Ако искате да запазите същия сертификат и личен ключ след нулиране на сървъра за печат, експортирайте ги преди нулирането и след това ги преинсталирайте.

Свързана информация

- Конфигуриране на сертификати за защита на устройството

Свързани теми:

- Конфигуриране на удостоверяване с IEEE 802.1x за вашата мрежа с помощта на уеб базираното управление (уеб браузър)

Как се създава и инсталира сертификат

Има две опции при избирането на сертификат за защита: използване на самоподписан сертификат и използване на сертификат от сертифициращ орган (CO).

Опция 1

Самоподписан сертификат

1. Създаване на собственоръчно подписан сертификат с помощта на Уеб-базирано управление.
2. Инсталирайте самоподписания сертификат на вашия компютър.

Опция 2

Сертификат от CO

1. Създайте искане за подписване на сертификат (CSR), като използвате уеб-базираното управление.
2. Инсталирайте сертификата, издаден от CO за вашето устройство на Brother, като използвате уеб базираното управление.
3. Инсталирайте сертификата на вашия компютър.

Свързана информация

- Конфигуриране на сертификати за защита на устройството

Създаване на самоподписан сертификат

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **Certificate (Сертификат)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Щракнете върху **Create Self-Signed Certificate (Създаване на самоподписан сертификат)**.
6. Въведете **Common Name (Общо име)** и **Valid Date (Дата на валидност)**.
   - Дължината на **Common Name (Общо име)** е по-малко от 64 байта. Въведете идентификатор, например IP адрес, име на възел или име на домейн, които да използвате при осъществяване на достъп до това устройство чрез комуникация SSL/TLS. По подразбиране се изписва името на възела.
   - Ще се появи предупреждение, ако използвате протокол IPPS или HTTPS и въведете друго име в полето за URL адрес, различно от **Common Name (Общо име)**, което е използвано за собственоръчно подписания сертификат.
7. Изберете настройка от падащия списък **Public Key Algorithm (Алгоритъм на публичен ключ)**.
8. Изберете настройка от падащия списък **Digest Algorithm (Алгоритъм на извличане)**.
9. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Конфигуриране на сертификати за защита на устройството

Създаване на искане за подписване на сертификат (CSR) и инсталиране на сертификат от сертифициращ орган (CO)

Ако вече имате сертификат от външен доверен сертифициращ орган (CA), можете да запаметите сертификата и личния ключ в устройството и да ги управлявате чрез импортиране и експортиране. Ако нямате сертификат от външен доверен CO, създайте искане за подписване на сертификат (CSR), изпратете го на CO за удостоверяване и инсталирайте върнатия сертификат на устройството.

- Създаване на заявка за издаване на сертификат (CSR)
- Инсталиране на сертификат на вашето устройство

Създаване на заявка за издаване на сертификат (CSR)

Заявка за издаване на сертификат (CSR) е заявка, изпратена до CO за удостоверяване на идентификационните данни, съдържащи се в сертификата.

Препоръчваме главният сертификат от CO да се инсталира на вашия компютър, преди да се създаде CSR.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

   Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.
4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **Certificate (Сертификат)** в лявата навигационна лента.

   Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.
5. Щракнете върху **Create CSR (Създаване на CSR)**.
6. Въведете **Common Name (Общо име)** (задължително) и друга информация за вашия **Organization (Организация)** (по избор).

   - Необходими са данни за вашата компания, за да може CO да провери вашата самоличност и да я потвърди пред външните потребители.
   - Дължината на **Common Name (Общо име)** трябва да е по-малко от 64 байта. Въведете идентификатор, например IP адрес, име на възел или име на домейн, които да използвате при осъществяване на достъп до това устройство чрез комуникация SSL/TLS. По подразбиране се изписва името на възела. Необходимо е **Common Name (Общо име)**.
   - Ще се появи предупреждение, ако въведете друго име в полето за URL адрес, различно от общото име, което е използвано за сертификата.
   - Дължината на **Organization (Организация)**, **Organization Unit (Организационна единица)**, **City/Locality (Град/местност)** и **State/Province (Област)** трябва да е по-малка от 64 байта.
   - **Country/Region (Държава/регион)** трябва да е ISO 3166 код на държавата от два знака.
   - Ако конфигурирате продължение на сертификат X.509v3, изберете квадратчето за отметка **Configure extended partition (Конфигуриране на разширения раздел)**, а после изберете **Auto (Register IPv4) (Автоматично (регистриране на IPv4))** или **Manual (Ръчно)**.
7. Изберете настройка от падащия списък **Public Key Algorithm (Алгоритъм на публичен ключ)**.
8. Изберете настройка от падащия списък **Digest Algorithm (Алгоритъм на извличане)**.
9. Щракнете върху **Submit (Изпрати)**.

   CSR се появява на екрана ви. Запишете CSR като файл или я копирайте и поставете в онлайн формуляр за CSR, предоставен от CO.
10. Щракнете върху **Запиши**.

- Спазвайте правилата на вашия CO по отношение на начина на изпращане на CSR на вашия CO.
- Ако използвате Enterprise root CA на Windows Server, препоръчваме да използвате уеб сървъра за шаблона за сертификат, за да създадете защитено клиентския сертификат. Ако създавате Клиентски сертификат за среда IEEE 802.1x с удостоверяване EAP-TLS, препоръчваме да използвате Потребител за шаблон на сертификата.

Свързана информация

- Създаване на искане за подписване на сертификат (CSR) и инсталиране на сертификат от сертифициращ орган (CO)

Инсталиране на сертификат на вашето устройство

Когато получите сертификат от Сертифициращ орган (CA), следвайте стъпките по-долу, за да го инсталирате на сървъра за печат:

На устройството може да се инсталира само сертификат, издаден с искане за подписване на сертификат (CSR). Когато искате да създадете друго CSR, уверете се, че сертификатът е инсталиран, преди да създавате друго CSR. Създавайте друго CSR само след инсталирането на сертификата на устройствата, защото иначе CSR, създадено преди инсталирането на новото CSR, ще бъде невалидно.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

   Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.
4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **Certificate (Сертификат)** в лявата навигационна лента.

   Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.
5. Щракнете върху **Install Certificate (Инсталиране на сертификат)**.
6. Отидете до файла, който съдържа сертификата, издаден от CO, и след това щракнете върху **Submit (Изпрати)**.

   Сертификатът е създаден и записан успешно в паметта на вашето устройство.

За да използвате SSL/TLS комуникация, главният сертификат от CO трябва да се инсталира на вашия компютър. Обърнете се към мрежовия администратор.

Свързана информация

- Създаване на искане за подписване на сертификат (CSR) и инсталиране на сертификат от сертифициращ орган (CO)

Импортиране и експортиране на сертификата и персоналния ключ

Съхранявайте сертификата и личния ключ на вашето устройство и ги управлявайте чрез импортиране и експортиране.

- Импортиране на сертификат и личен ключ
- Експортиране на сертификата и персоналния ключ

Импортиране на сертификат и личен ключ

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **Certificate (Сертификат)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Щракнете върху **Import Certificate and Private Key (Импортиране на сертификат и личен ключ)**.
6. Отидете до файла, който искате да импортирате, и го изберете.
7. Въведете паролата, ако файлът е шифрован, а след това щракнете върху **Submit (Изпрати)**.

Сертификатът и личният ключ се импортират на вашето устройство.

Свързана информация

- Импортиране и експортиране на сертификата и персоналния ключ

Експортиране на сертификата и персоналния ключ

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **Certificate (Сертификат)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Щракнете върху **Export (Експортиране)**, показан със **Certificate List (Списък със сертификати)**.
6. Въведете паролата, ако искате да шифровате файла.

   Ако се използва празна парола, резултатът не се шифрова.
7. Въведете паролата отново за потвърждение, а след това щракнете върху **Submit (Изпрати)**.
8. Щракнете върху **Запиши**.

Сертификатът и персоналният ключ се експортират към вашия компютър.

Можете също да импортирате сертификата в компютъра си.

Свързана информация

- Импортиране и експортиране на сертификата и персоналния ключ

Импортиране и експортиране на CA сертификат

Можете да импортирате, експортирате и съхранявате CA сертификати на устройството на Brother.

- Импортиране на CA сертификат
- Експортиране на CA сертификат

Импортиране на CA сертификат

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **CA Certificate (CA сертификат)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Щракнете върху **Import CA Certificate (Импортиране на CA сертификат)**.
6. Отидете на файла, който искате да импортирате.
7. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Импортиране и експортиране на CA сертификат

Експортиране на CA сертификат

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **CA Certificate (CA сертификат)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Изберете сертификата, който желаете да експортирате, и щракнете върху **Export (Експортиране)**.
6. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Импортиране и експортиране на CA сертификат

Използване на SSL/TLS

- Безопасно управление на мрежовото устройство чрез SSL/TLS
- Защитено отпечатване на документи с помощта на SSL/TLS
- Безопасно изпращане и получаване на имейл чрез SSL/TLS

Безопасно управление на мрежовото устройство чрез SSL/TLS

- Конфигуриране на сертификат за SSL/TLS и налични протоколи
- Достъп до Уеб базираното управление чрез SSL/TLS
- Инсталиране на самоподписания сертификат за потребители администратори на Windows
- Конфигуриране на сертификати за защита на устройството

Конфигуриране на сертификат за SSL/TLS и налични протоколи

Конфигурирайте на устройството сертификат, като използвате Уеб базирано управление, преди да използвате SSL/TLS комуникацията.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

> Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Network (Мрежа)** > **Protocol (Протокол)** в лявата навигационна лента.

> Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Щракнете върху **HTTP Server Settings (Настройки на HTTP сървъра)**.
6. Изберете сертификата, който искате да конфигурирате, от падащия списък **Select the Certificate (Изберете сертификат)**.
7. Щракнете върху **Submit (Изпрати)**.
8. Щракнете върху **Yes (Да)**, за да рестартирате вашия сървър за печат.

Свързана информация

- Безопасно управление на мрежовото устройство чрез SSL/TLS

Свързани теми:

- Защитено отпечатване на документи с помощта на SSL/TLS

Достъп до Уеб базираното управление чрез SSL/TLS

За защитено управление на мрежовото устройство трябва да използвате помощните програми за управление с протоколи за сигурност.

- За да използвате HTTPS протокол, на устройството ви трябва да е активиран HTTPS. Протоколът HTTPS е активиран по подразбиране.
- Можете да промените настройките на протокола HTTPS, като използвате екрана на уеб-базираното управление.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Сега имате достъп до устройството чрез HTTPS.

Свързана информация

- Безопасно управление на мрежовото устройство чрез SSL/TLS

Инсталиране на самоподписания сертификат за потребители администратори на Windows

- Стъпките по-долу са за Microsoft Edge. Ако използвате друг уеб браузър, вижте документацията или онлайн помощта на вашия уеб браузър за инструкции как да инсталирате сертификати.
- Непременно трябва да сте създали своя самоподписан сертификат с помощта на уеб базираното управление.

1. Щракнете с десния бутон върху иконата **Microsoft Edge**, а след това щракнете върху **Изпълнявай като администратор**.

   Ако се появи екранът **Управление на потребителските акаунти**, щракнете върху **Да**.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако връзката ви не е поверителна, щракнете върху бутона **Разширени** и след това продължете към уеб страницата.
4. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

   Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.
5. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **Certificate (Сертификат)** в лявата навигационна лента.

   Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.
6. Щракнете върху **Export (Експортиране)**.
7. За да шифровате изходния файл, въведете парола в полето **Enter password (Въведете парола)**. Ако полето **Enter password (Въведете парола)** е празно, изходният ви файл няма да е шифрован.
8. Въведете паролата отново в полето **Retype password (Въведете паролата отново)** и после щракнете върху **Submit (Изпрати)**.
9. Щракнете върху свалените файл, за да го отворите.
10. Когато се появи **Съветник за импортиране на сертификати**, щракнете върху **Напред**.
11. Щракнете върху **Напред**.
12. Ако е необходимо, въведете парола и след това щракнете върху **Напред**.
13. Изберете **Поставяй всички сертификати в следното хранилище**, а след това щракнете върху **Преглед...**.
14. Изберете **Надеждни главни сертифициращи органи** и след това щракнете върху **OK**.
15. Щракнете върху **Напред**.
16. Щракнете върху **Готово**.
17. Щракнете върху **Да**, ако отпечатъкът е правилен.
18. Щракнете върху **OK**.

Свързана информация

- Безопасно управление на мрежовото устройство чрез SSL/TLS

Защитено отпечатване на документи с помощта на SSL/TLS

- Отпечатване на документи с използване на IPPS
- Конфигуриране на сертификат за SSL/TLS и налични протоколи
- Конфигуриране на сертификати за защита на устройството

Отпечатване на документи с използване на IPPS

За защитен печат на документи с протокол IPP можете да използвате протокола IPPS.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Network (Мрежа)** > **Protocol (Протокол)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Уверете се, че квадратчето за отметка **IPP** е избрано.

Ако квадратчето за отметка **IPP** не е избрано, изберете квадратчето за отметка **IPP** и после щракнете върху **Submit (Изпрати)**.

Рестартирайте устройството за активиране на конфигурацията.

След като устройството се рестартира, се върнете на уеб страницата на устройството, въведете паролата, а след това щракнете върху **Network (Мрежа)** > **Network (Мрежа)** > **Protocol (Протокол)** в лявата навигационна лента.

6. Щракнете върху **HTTP Server Settings (Настройки на HTTP сървъра)**.
7. Изберете квадратчето за отметка **HTTPS(Порт 443)** в областта **IPP** и после щракнете върху **Submit (Изпрати)**.
8. Рестартирайте устройството за активиране на конфигурацията.

Комуникацията с помощта на IPPS не може да предотврати unauthorized достъп до сървъра за печат.

Свързана информация

- Защитено отпечатване на документи с помощта на SSL/TLS

Използване на SNMPv3

- Безопасно управление на вашето мрежово устройство чрез SNMPv3

Безопасно управление на вашето мрежово устройство чрез SNMPv3

Простият протокол за управление на мрежа версия 3 (SNMPv3) осигурява удостоверяване на потребителя и шифроване на данните за сигурно управление на мрежовите устройства.

1. Стартирайте уеб браузъра.
2. Напишете “https://Общо име” в адресната лента на браузъра (където “Общо име” е общото име, което сте присвоили на сертификата – това може да бъде вашият IP адрес, име на възел или име на домейн).
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Network (Мрежа)** > **Protocol (Протокол)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Уверете се, че настройката на **SNMP** е активирана, а след това щракнете върху **Advanced Settings (Разширени настройки)**.
6. Конфигурирайте настройките на режима SNMPv1/v2c.

Опция	Описание
SNMP v1/v2c read-write access (SNMP v1/v2c достъп за четене и записване)	Сървърът за печат използва версия 1 и версия 2c на протокола SNMP. В този режим можете да използвате всички приложения на устройството. Той обаче не е защитен, тъй като не удостоверява потребителя и данните не се шифроват.
SNMP v1/v2c read-only access (SNMP v1/v2c достъп само за четене)	Сървърът за печат използва достъпа само за четене на версия 1 и версия 2c на протокола SNMP.
Disabled (Деактивирано)	Деактивирайте версия 1 и версия 2c на протокола SNMP. Всички приложения, които използват SNMPv1/v2c, ще бъдат ограничени. За да разрешите използването на приложения SNMPv1/v2c, използвайте режима **SNMP v1/v2c read-only access (SNMP v1/v2c достъп само за четене)** или **SNMP v1/v2c read-write access (SNMP v1/v2c достъп за четене и записване)**.

7. Конфигурирайте настройките на режима SNMPv3.

Опция	Описание
Enabled (Разрешено)	Сървърът за печат използва версия 3 на протокола SNMP. За да управлявате сървъра за печат по защитен начин, използвайте режима SNMPv3.
Disabled (Деактивирано)	Деактивирайте версия 3 на протокола SNMP. Всички приложения, които използват SNMPv3, ще бъдат ограничени. За да разрешите използването на приложения под SNMPv3, използвайте режима SNMPv3.

8. Щракнете върху **Submit (Изпрати)**.

Ако устройството ви показва опции за настройка на протокол, изберете желаните опции.

9. Рестартирайте устройството за активиране на конфигурацията.

Свързана информация

- Използване на SNMPv3

Използване на IPsec

Въведение в IPsec

IPsec (Internet Protocol Security) е протокол за защита, който използва допълнителна функция на интернет протокола, за да предотврати манипулирането на данни и да гарантира поверителността на данните, предавани като IP пакети. IPsec шифрова данните, предавани по мрежата, като напр. данните за печат, изпратени от компютри към принтер. Тъй като данните са шифровани в мрежовия слой, приложенията, които използват протокол от по-високо ниво, използват IPsec дори потребителят да не е наясно за използването му.

IPsec поддържа следните функции:

- Предавания чрез IPsec

  Според условията на настройката за IPsec, свързаният към мрежата компютър изпраща данни към и получава данни от зададеното устройство чрез IPsec. Когато устройствата започнат да комуникират чрез IPsec, първо се обменят ключове посредством протокола Internet Key Exchange (IKE), а след това шифрованите данни се предават чрез ключовете.

  Освен това IPsec има два работни режима: транспортен режим и тунелен режим. Транспортният режим се използва предимно за комуникация между устройствата, а тунелният режим се използва за среда, като Виртуална частна мрежа (VPN).

За предавания чрез IPsec са необходими следните условия:

- Компютър, който може да комуникира чрез IPsec, да е свързан с мрежата.
- Вашето устройство е конфигурирано за IPsec комуникация.
- Компютърът, свързан към вашето устройство, е конфигуриран за IPsec комуникация.

- Настройки на IPsec

  Настройките, необходими за връзки чрез IPsec. Тези настройки могат да се конфигурират чрез Уеб-базирано управление.

За конфигуриране на настройките на IPsec трябва да използвате браузъра на компютър, който е свързан с мрежата.

Свързана информация

- Използване на IPsec

Конфигуриране на IPsec с помощта на Уеб-базирано управление

Условията за IPsec връзка включват два типа **Template (Шаблон)**: **Address (Адрес)** и **IPsec**. Можете да конфигурирате до 10 условия за връзка.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **IPsec** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Конфигурирайте настройките.

Опция	Описание
Status (Статус)	Активиране или деактивиране на IPsec.
Negotiation Mode (Режим за съгласуване)	Изберете **Negotiation Mode (Режим за съгласуване)** за IKE Phase 1. IKE е протокол, който се използва за обмен на ключове за шифроване за осъществяване на шифрована комуникация с помощта на IPsec. В режим **Main (Основен)** скоростта на обработване е ниска, но степента на сигурност е висока. В режим **Aggressive (Агресивен)** скоростта на обработване е по-висока от тази в режим **Main (Основен)**, но сигурността е по-малка.
All Non-IPsec Traffic (Целият трафик, който не е IPsec)	Изберете действието, което трябва да се извърши за пакети, които не са IPsec. Когато се използват Уеб услуги, трябва да изберете **Allow (Позволяване)** за **All Non-IPsec Traffic (Целият трафик, който не е IPsec)**. Ако изберете **Drop (Блокиране)**, Уеб услуги не могат да се използват.
Broadcast/Multicast Bypass (Излъчване/мултикаст заобикаляне)	Изберете **Enabled (Разрешено)** или **Disabled (Деактивирано)**.
Protocol Bypass (Заобикаляне на протокола)	Поставете отметка в квадратчето на опцията или опциите, които желаете.
Rules (Правила)	Поставете отметка в квадратчето **Enabled (Разрешено)**, за да активирате шаблона. Когато изберете няколко квадратчета за отметка, квадратчетата за отметка с по-малки номера имат приоритет, ако има конфликт между настройките за избраните квадратчета за отметка. Щракнете върху съответния падащ списък, за да изберете **Address Template (Шаблон за адрес)**, който се използва за условията за връзка на IPsec. За да добавите **Address Template (Шаблон за адрес)**, щракнете върху **Add Template (Добавяне на шаблон)**. Щракнете върху съответния падащ списък, за да изберете **IPsec Template (IPsec шаблон)**, който се използва за условията за

Опция	Описание
	връзка на IPsec. За да добавите **IPsec Template (IPsec шаблон)**, щракнете върху **Add Template (Добавяне на шаблон)**.

6. Щракнете върху **Submit (Изпрати)**.

   Ако устройството трябва да се рестартира за активиране на новите настройки, ще се появи екранът за потвърждение на рестартирането.

   Ако има празна позиция в шаблона, който активирахте в таблицата **Rules (Правила)**, се показва съобщение за грешка. Прегледайте това, което сте избрали, и щракнете отново върху **Submit (Изпрати)**.

Свързана информация

- Използване на IPsec

Свързани теми:

- Конфигуриране на сертификати за защита на устройството

Конфигуриране на шаблон за адрес на IPsec чрез Уеб-базирано управление

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **IPsec Address Template (Шаблон за IPsec адрес)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Щракнете върху бутона **Delete (Изтрий)**, за да изтриете **Address Template (Шаблон за адрес)**. По време на използване на **Address Template (Шаблон за адрес)**, той не може да се изтрие.
6. Щракнете върху **Address Template (Шаблон за адрес)**, който искате да създадете. Показва се **IPsec Address Template (Шаблон за IPsec адрес)**.
7. Конфигурирайте настройките.

Опция	Описание
Template Name (Име на шаблона)	Въведете име за шаблона (до 16 знака).
Local IP Address (Локален IP адрес)	• **IP Address (IP адрес)** Задайте IP адреса. Изберете **ALL IPv4 Address (ALL IPv4 адрес)**, **ALL IPv6 Address (ALL IPv6 адрес)**, **ALL Link Local IPv6** или **Custom (По избор)** от падащия списък. Ако изберете **Custom (По избор)** от падащия списък, напишете IP адреса (IPv4 или IPv6) в текстовото поле. • **IP Address Range (Обхват на IP адреса)** Въведете началния и крайния IP адреси за диапазона от IP адреси в текстовите полета. Ако началният и крайният IP адреси не са standardized спрямо IPv4 или IPv6 или крайният IP адрес е по-малък от началния адрес, ще възникне грешка. • **IP Address / Prefix (IP адрес/префикс)** Задайте IP адреса, като използвате обозначаване CIDR. Например: 192.168.1.1/24 Тъй като префиксът е посочен във формата на 24-битова маска на подмрежата (255.255.255.0) за 192.168.1.1, адресите 192.168.1.### са валидни.
Remote IP Address (Отдалечен IP адрес)	• **Any (Всякакъв)** Ако изберете **Any (Всякакъв)**, всички IP адреси се активират. • **IP Address (IP адрес)** Напишете посочения IP адрес (IPv4 или IPv6) в текстовото поле. • **IP Address Range (Обхват на IP адреса)** Въведете първия и последния IP адрес за диапазона от IP адреси. Ако първият и последният IP адрес не са standardized

Опция	Описание
	спрямо IPv4 или IPv6 или последният IP адрес е по-малък от първия адрес, ще възникне грешка. • **IP Address / Prefix (IP адрес/префикс)** Задайте IP адреса, като използвате обозначаване CIDR. Например: 192.168.1.1/24 Тъй като префиксът е посочен във формата на 24-битова маска на подмрежата (255.255.255.0) за 192.168.1.1, адресите 192.168.1.### са валидни.

8. Щракнете върху **Submit (Изпрати)**.

Когато промените настройките за шаблона, който се използва в момента, рестартирайте устройството си, за да активирате конфигурацията.

Свързана информация

- Използване на IPsec

Конфигуриране на шаблон на IPsec с помощта на Уеб-базирано управление

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Security (Защита)** > **IPsec Template (IPsec шаблон)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Щракнете върху бутона **Delete (Изтрий)**, за да изтриете **IPsec Template (IPsec шаблон)**. По време на използване на **IPsec Template (IPsec шаблон)**, той не може да се изтрие.
6. Щракнете върху **IPsec Template (IPsec шаблон)**, който искате да създадете. Показва се екранът **IPsec Template (IPsec шаблон)**. Полетата за конфигурация са различни в зависимост от настройките за **Use Prefixed Template (Използване на шаблон с префикс)** и **Internet Key Exchange (IKE) (Протокол IKE)**, които изберете.
7. В полето **Template Name (Име на шаблона)** напишете име на шаблона (до 16 знака).
8. Ако сте избрали **Custom (По избор)** в падащия списък **Use Prefixed Template (Използване на шаблон с префикс)**, изберете опциите **Internet Key Exchange (IKE) (Протокол IKE)** и после променете настройките, ако е необходимо.
9. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Използване на IPsec
  - Настройки на IKEv1 за шаблон на IPsec
  - Настройки на IKEv2 за шаблон на IPsec
  - Ръчни настройки за шаблон на IPsec

Настройки на IKEv1 за шаблон на IPsec

Опция	Описание
Template Name (Име на шаблона)	Въведете име за шаблона (до 16 знака).
Use Prefixed Template (Използване на шаблон с префикс)	Изберете **Custom (По избор)**, **IKEv1 High Security (IKEv1 висока защита)** или **IKEv1 Medium Security (IKEv1 средна защита)**. Елементите на настройките са различни в зависимост от избрания шаблон.
Internet Key Exchange (IKE) (Протокол IKE)	IKE е протокол за комуникация, който се използва за обмен на ключове за шифроване за осъществяване на шифрована комуникация с помощта на IPsec. За да се пренесат еднократно шифрованите данни, се определя алгоритъмът на шифроване, който е необходим за IPsec, и се споделят ключовете за шифроване. За IKE, ключовете за шифроване се обменят чрез метода Дифи-Хелман за обмен на ключове и се осъществява шифрована комуникация, която е ограничена само за IKE. Ако те избрали **Custom (По избор)** в **Use Prefixed Template (Използване на шаблон с префикс)**, изберете **IKEv1**.
Authentication Type (Тип удостоверяване)	• **Diffie-Hellman Group (Diffie-Hellman група)** Този метод за обмен на ключове позволява да се извършва защитен обмен на тайни ключове по незащитена мрежа. При метода на Дифи-Хелман за обмен на ключове се използва не тайният ключ, а абстрактна логаритмична задача за изпращане и получаване на открита информация, която се генерира с помощта на произволно число и тайния ключ. Изберете **Group1 (Група 1)**, **Group2 (Група 2)**, **Group5 (Група 5)** или **Group14 (Група 14)**. • **Encryption (Кодиране)** Изберете **DES**, **3DES**, **AES-CBC 128** или **AES-CBC 256**. • **Hash (Хеширане)** Изберете **MD5**, **SHA1**, **SHA256**, **SHA384** или **SHA512**. • **SA Lifetime (Продължителност на SA)** Задайте времето на живот на SA за IKE. Въведете времето (секунди) и броя килобайтове (килобайт).
Encapsulating Security (Включване на защита)	• **Protocol (Протокол)** Изберете **ESP**, **AH** или **AH+ESP**.

Опция	Описание
	- ESP е протокол за осъществяване на шифрована комуникация чрез IPsec. ESP шифрова полезните данни (прехвърляното съдържание) и добавя допълнителна информация. IP пакетът се състои от горния колонтитул и шифрованата полезна информация, която следва след него. В допълнение към шифрованите данни IP пакетът включва и информация относно метода на шифроване, ключа за шифроване, данните за удостоверяване и т.н. - AH (Заглавката за удостоверяване) е част от IPsec протокола, която удостоверява подателя и предотвратява манипулирането на данните (гарантира целостта на данните). В IP пакета данните се вмъкват веднага след заглавката. Освен това пакетите съдържат стойности за хеширане, който се изчисляват чрез уравнение от прехвърляното съдържание, тайния ключ и т.н., за да се предотврати подправяне на подателя и манипулиране на данните. За разлика от ESP прехвърляното съдържание не е шифровано и данните се изпращат и получават като обикновен текст. • **Encryption (Кодиране) (Не е налично за опцията AH.)** Изберете **DES**, **3DES**, **AES-CBC 128** или **AES-CBC 256**. • **Hash (Хеширане)** Изберете **None (Няма)**, **MD5**, **SHA1**, **SHA256**, **SHA384** или **SHA512**. **None (Няма)** може да се избере, само когато е избрано **ESP** за **Protocol (Протокол)**. • **SA Lifetime (Продължителност на SA)** Посочете валидността на IKE SA. Напишете времето (секунди) и броя на килобайтовете (KByte). • **Encapsulation Mode (Включване на режим)** Изберете **Transport (Транспорт)** или **Tunnel (Тунел)**. • **Remote Router IP-Address (Отдалечен IP адрес на рутера)** Въведете IP адреса (IPv4 или IPv6) на отдалечения маршрутизатор. Въвеждайте тази информация само когато за режим е избрано **Tunnel (Тунел)**. SA (набор за сигурност) е метод за шифрована комуникация с помощта на IPsec или IPv6, който обменя и споделя информация, напр. метода за шифроване и ключа за шифроване, за да се установи защитен канал за комуникация, преди да започне комуникацията. SA може да се отнася и за виртуален защитен канал за комуникация, който е установен. SA, който се използва за IPsec, установява метода за шифроване, обменя ключовете и извършва взаимно удостоверяване съгласно стандартната процедура по IKE (протокол за обмен на ключове по Интернет). Освен това, SA се актуализира периодично.
Perfect Forward Secrecy (PFS) (Съвършена безопасност на информацията в бъдеще)	PFS не извлича ключове от предходни ключове, които са използвани за шифроване на съобщения. В допълнение, ако ключ, използван за шифроване на съобщение, е извлечен от родителски ключ, този родителски ключ не се използва за извличане на други ключове. Поради това, дори ако един ключ се компрометира, щетата ще се ограничи само до съобщенията, които са шифровани с този ключ. Изберете **Enabled (Разрешено)** или **Disabled (Деактивирано)**.

Опция	Описание
Authentication Method (Метод на удостоверяване)	Изберете метода на удостоверяване. Изберете **Pre-Shared Key (Предварително споделен ключ)** или **Certificates (Сертификати)**.
Pre-Shared Key (Предварително споделен ключ)	При шифроване на комуникация ключът за шифроване се обменя и споделя, преди да се използва друг канал. Ако сте избрали **Pre-Shared Key (Предварително споделен ключ)** за **Authentication Method (Метод на удостоверяване)**, напишете **Pre-Shared Key (Предварително споделен ключ)** (до 32 знака). • **Local/ID Type/ID (Локален/Тип ИД/ИД)** Изберете типа на идентификатора на подателя, а след това напишете идентификатора. Изберете **IPv4 Address (IPv4 адрес)**, **IPv6 Address (IPv6 адрес)**, **FQDN**, **E-mail Address (Имейл адрес)** или **Certificate (Сертификат)** за типа. Ако е изберете **Certificate (Сертификат)**, напишете общото наименование на сертификата в полето **ID (ИД)**. • **Remote/ID Type/ID (Отдалечен/Тип ИД/ИД)** Изберете типа на идентификатора на получателя, а след това напишете идентификатора. Изберете **IPv4 Address (IPv4 адрес)**, **IPv6 Address (IPv6 адрес)**, **FQDN**, **E-mail Address (Имейл адрес)** или **Certificate (Сертификат)** за типа. Ако е изберете **Certificate (Сертификат)**, напишете общото наименование на сертификата в полето **ID (ИД)**.
Certificate (Сертификат)	Ако сте избрали **Certificates (Сертификати)** за **Authentication Method (Метод на удостоверяване)**, изберете сертификата. Можете да изберете само сертификатите, които са създадени с помощта на страницата **Certificate (Сертификат)** на екрана за конфигурация на защитата в уеб базираното управление.

Свързана информация

- Конфигуриране на шаблон на IPsec с помощта на Уеб-базирано управление

Настройки на IKEv2 за шаблон на IPsec

Опция	Описание
Template Name (Име на шаблона)	Въведете име за шаблона (до 16 знака).
Use Prefixed Template (Използване на шаблон с префикс)	Изберете **Custom (По избор)**, **IKEv2 High Security (IKEv2 висока защита)** или **IKEv2 Medium Security (IKEv2 средна защита)**. Елементите на настройките са различни в зависимост от избрания шаблон.
Internet Key Exchange (IKE) (Протокол IKE)	IKE е протокол за комуникация, който се използва за обмен на ключове за шифроване за осъществяване на шифрована комуникация с помощта на IPsec. За да се пренесат еднократно шифрованите данни, се определя алгоритъмът на шифроване, който е необходим за IPsec, и се споделят ключовете за шифроване. За IKE, ключовете за шифроване се обменят чрез метода Дифи-Хелман за обмен на ключове и се осъществява шифрована комуникация, която е ограничена само за IKE. Ако те избрали **Custom (По избор)** в **Use Prefixed Template (Използване на шаблон с префикс)**, изберете **IKEv2**.
Authentication Type (Тип удостоверяване)	• **Diffie-Hellman Group (Diffie-Hellman група)** Този метод за обмен на ключове позволява да се извършва защитен обмен на тайни ключове по незащитена мрежа. При метода на Дифи-Хелман за обмен на ключове се използва не тайният ключ, а абстрактна логаритмична задача за изпращане и получаване на открита информация, която се генерира с помощта на произволно число и тайния ключ. Изберете **Group1 (Група 1)**, **Group2 (Група 2)**, **Group5 (Група 5)** или **Group14 (Група 14)**. • **Encryption (Кодиране)** Изберете **DES**, **3DES**, **AES-CBC 128** или **AES-CBC 256**. • **Hash (Хеширане)** Изберете **MD5**, **SHA1**, **SHA256**, **SHA384** или **SHA512**. • **SA Lifetime (Продължителност на SA)** Задайте времето на живот на SA за IKE. Въведете времето (секунди) и броя килобайтове (килобайт).
Encapsulating Security (Включване на защита)	• **Protocol (Протокол)** Изберете **ESP**. ESP е протокол за осъществяване на шифрована комуникация чрез IPsec. ESP шифрова полезните данни (прехвърляното съдържание) и добавя допълнителна информация. IP пакетът се състои от горния колонтитул и шифрованата полезна информация, която следва след него. В допълнение към шифрованите данни IP пакетът включва и информация относно метода на шифроване, ключа за шифроване, данните за удостоверяване и т.н. • **Encryption (Кодиране)** Изберете **DES**, **3DES**, **AES-CBC 128** или **AES-CBC 256**. • **Hash (Хеширане)** Изберете **MD5**, **SHA1**, **SHA256**, **SHA384** или **SHA512**. • **SA Lifetime (Продължителност на SA)** Посочете валидността на IKE SA. Напишете времето (секунди) и броя на килобайтовете (KByte).

Опция	Описание
	• **Encapsulation Mode (Включване на режим)** Изберете **Transport (Транспорт)** или **Tunnel (Тунел)**. • **Remote Router IP-Address (Отдалечен IP адрес на рутера)** Въведете IP адреса (IPv4 или IPv6) на отдалечения маршрутизатор. Въвеждайте тази информация само когато за режим е избрано **Tunnel (Тунел)**. SA (набор за сигурност) е метод за шифрована комуникация с помощта на IPsec или IPv6, който обменя и споделя информация, напр. метода за шифроване и ключа за шифроване, за да се установи защитен канал за комуникация, преди да започне комуникацията. SA може да се отнася и за виртуален защитен канал за комуникация, който е установен. SA, който се използва за IPsec, установява метода за шифроване, обменя ключовете и извършва взаимно удостоверяване съгласно стандартната процедура по IKE (протокол за обмен на ключове по Интернет). Освен това, SA се актуализира периодично.
Perfect Forward Secrecy (PFS) (Съвършена безопасност на информацията в бъдеще)	PFS не извлича ключове от предходни ключове, които са използвани за шифроване на съобщения. В допълнение, ако ключ, използван за шифроване на съобщение, е извлечен от родителски ключ, този родителски ключ не се използва за извличане на други ключове. Поради това, дори ако един ключ се компрометира, щетата ще се ограничи само до съобщенията, които са шифровани с този ключ. Изберете **Enabled (Разрешено)** или **Disabled (Деактивирано)**.
Authentication Method (Метод на удостоверяване)	Изберете метода на удостоверяване. Изберете **Pre-Shared Key (Предварително споделен ключ)**, **Certificates (Сертификати)**, **EAP - MD5** или **EAP - MS-CHAPv2**. EAP е протокол за удостоверяване, който е разширение на PPP. С помощта на EAP заедно с IEEE802.1x се използва различен ключ за удостоверяване на потребител по време на всяка сесия. Следните настройки са необходими, само когато е избран **EAP - MD5** или **EAP - MS-CHAPv2** в **Authentication Method (Метод на удостоверяване)**: • **Mode (Режим)** Изберете **Server-Mode (Сървърен режим)** или **Client-Mode (Клиентски режим)**. • **Certificate (Сертификат)** Изберете сертификата. • **User Name (Потребител. име)** Въведете потребителското име (до 32 знака). • **Password (Парола)** Въведете паролата (до 32 знака). Паролата трябва да бъде въведена два пъти за потвърждение.
Pre-Shared Key (Предварително споделен ключ)	При шифроване на комуникация ключът за шифроване се обменя и споделя, преди да се използва друг канал. Ако сте избрали **Pre-Shared Key (Предварително споделен ключ)** за **Authentication Method (Метод на удостоверяване)**, напишете **Pre-Shared Key (Предварително споделен ключ)** (до 32 знака). • **Local/ID Type/ID (Локален/Тип ИД/ИД)** Изберете типа на идентификатора на подателя, а след това напишете идентификатора.

Опция	Описание
	Изберете **IPv4 Address (IPv4 адрес)**, **IPv6 Address (IPv6 адрес)**, **FQDN**, **E-mail Address (Имейл адрес)** или **Certificate (Сертификат)** за типа. Ако е изберете **Certificate (Сертификат)**, напишете общото наименование на сертификата в полето **ID (ИД)**. • **Remote/ID Type/ID (Отдалечен/Тип ИД/ИД)** Изберете типа на идентификатора на получателя, а след това напишете идентификатора. Изберете **IPv4 Address (IPv4 адрес)**, **IPv6 Address (IPv6 адрес)**, **FQDN**, **E-mail Address (Имейл адрес)** или **Certificate (Сертификат)** за типа. Ако е изберете **Certificate (Сертификат)**, напишете общото наименование на сертификата в полето **ID (ИД)**.
Certificate (Сертификат)	Ако сте избрали **Certificates (Сертификати)** за **Authentication Method (Метод на удостоверяване)**, изберете сертификата. Можете да изберете само сертификатите, които са създадени с помощта на страницата **Certificate (Сертификат)** на екрана за конфигурация на защитата в уеб базираното управление.

Свързана информация

- Конфигуриране на шаблон на IPsec с помощта на Уеб-базирано управление

Ръчни настройки за шаблон на IPsec

Опция	Описание
Template Name (Име на шаблона)	Въведете име за шаблона (до 16 знака).
Use Prefixed Template (Използване на шаблон с префикс)	Изберете **Custom (По избор)**.
Internet Key Exchange (IKE) (Протокол IKE)	IKE е протокол за комуникация, който се използва за обмен на ключове за шифроване за осъществяване на шифрована комуникация с помощта на IPsec. За да се пренесат еднократно шифрованите данни, се определя алгоритъмът на шифроване, който е необходим за IPsec, и се споделят ключовете за шифроване. За IKE, ключовете за шифроване се обменят чрез метода Дифи-Хелман за обмен на ключове и се осъществява шифрована комуникация, която е ограничена само за IKE. Изберете **Manual (Ръчно)**.
Authentication Key (ESP, AH) (Ключ за удостоверяване (ESP, AH))	Напишете значенията на **In/Out (Вход/Изход)**. Тези настройки са необходими, когато е избрано **Custom (По избор)** за **Use Prefixed Template (Използване на шаблон с префикс)**, **Manual (Ръчно)** е избрано за **Internet Key Exchange (IKE) (Протокол IKE)** и е избрана настройка, различна от **None (Няма)**, за **Hash (Хеширане)** за раздел **Encapsulating Security (Включване на защита)**. Броят на знаците, които можете да зададете, е различен в зависимост от настройката, която сте избрали за **Hash (Хеширане)** в раздел **Encapsulating Security (Включване на защита)**. Ако дължината на зададения ключ за удостоверяване е различна от избрания алгоритъм за хеширане, ще възникне грешка. • **MD5**: 128 бита (16 байта) • **SHA1**: 160 бита (20 байта) • **SHA256**: 256 бита (32 байта) • **SHA384**: 384 бита (48 байта) • **SHA512**: 512 бита (64 байта) Когато зададете ключа в ASCII код, оградете знаците в двойни кавички (").
Code key (ESP) (Код на ключа (ESP))	Напишете значенията на **In/Out (Вход/Изход)**. Тези настройки са необходими, когато **Custom (По избор)** е избрано за **Use Prefixed Template (Използване на шаблон с префикс)**, **Manual (Ръчно)** е избрано за **Internet Key Exchange (IKE) (Протокол IKE)** и **ESP** е избрано за **Protocol (Протокол)** в **Encapsulating Security (Включване на защита)**.

Опция	Описание
	Броят на знаците, които можете да зададете, е различен в зависимост от настройката, която сте избрали за **Encryption (Кодиране)** в раздел **Encapsulating Security (Включване на защита)**. Ако дължината на зададения кодиращ ключ е различна от избрания алгоритъм за шифроване, ще възникне грешка. • **DES**: 64 бита (8 байта) • **3DES**: 192 бита (24 байта) • **AES-CBC 128**: 128 бита (16 байта) • **AES-CBC 256**: 256 бита (32 байта) Когато зададете ключа в ASCII код, оградете знаците в двойни кавички (").
SPI	Тези параметри се използват за идентифициране на информацията за сигурност. По принцип, един хост има няколко набора за сигурност (SA) за няколко типа IPsec комуникация. Ето защо е необходимо да се идентифицира приложимия SA, когато се получи IPsec пакет. Параметърът SPI, който идентифицира SA, е включен в Колонтитул за удостоверяване (AH) и в колонтитула Полезна информация за сигурност чрез капсулиране (ESP). Тези настройки са необходими, когато е избрано **Custom (По избор)** за **Use Prefixed Template (Използване на шаблон с префикс)**, а **Manual (Ръчно)** е избрано за **Internet Key Exchange (IKE) (Протокол IKE)**. Въведете значенията на **In/Out (Вход/Изход)**. (3-10 знака)
Encapsulating Security (Включване на защита)	• **Protocol (Протокол)** Изберете **ESP** или **AH**. - ESP е протокол за осъществяване на шифрована комуникация чрез IPsec. ESP шифрова полезните данни (прехвърляното съдържание) и добавя допълнителна информация. IP пакетът се състои от горния колонтитул и шифрованата полезна информация, която следва след него. В допълнение към шифрованите данни IP пакетът включва и информация относно метода на шифроване, ключа за шифроване, данните за удостоверяване и т.н. - AH е част от IPsec протокола, който удостоверява подателя и предотвратява манипулирането на данните (осигурява пълнотата на данните). В IP пакета данните се вмъкват непосредствено след колонтитула. Освен това, пакетите включват хеш стойности, които се изчисляват с помощта на уравнение от предаденото съдържание, тайния ключ и т.н., за да се предотврати фалшифициране на подателя и манипулиране на данните. За разлика от ESP, предаваното съдържание не се шифрова и данните се изпращат и получават като обикновен текст. • **Encryption (Кодиране) (Не е налично за опцията AH.)** Изберете **DES**, **3DES**, **AES-CBC 128** или **AES-CBC 256**. • **Hash (Хеширане)** Изберете **None (Няма)**, **MD5**, **SHA1**, **SHA256**, **SHA384** или **SHA512**. **None (Няма)** може да се избере, само когато е избрано **ESP** за **Protocol (Протокол)**. • **SA Lifetime (Продължителност на SA)** Посочете валидността на IKE SA. Напишете времето (секунди) и броя на килобайтовете (KByte).

Опция	Описание
	• **Encapsulation Mode (Включване на режим)** Изберете **Transport (Транспорт)** или **Tunnel (Тунел)**. • **Remote Router IP-Address (Отдалечен IP адрес на рутера)** Въведете IP адреса (IPv4 или IPv6) на отдалечения маршрутизатор. Въвеждайте тази информация само когато за режим е избрано **Tunnel (Тунел)**. SA (набор за сигурност) е метод за шифрована комуникация с помощта на IPsec или IPv6, който обменя и споделя информация, напр. метода за шифроване и ключа за шифроване, за да се установи защитен канал за комуникация, преди да започне комуникацията. SA може да се отнася и за виртуален защитен канал за комуникация, който е установен. SA, който се използва за IPsec, установява метода за шифроване, обменя ключовете и извършва взаимно удостоверяване съгласно стандартната процедура по IKE (протокол за обмен на ключове по Интернет). Освен това, SA се актуализира периодично.

Свързана информация

- Конфигуриране на шаблон на IPsec с помощта на Уеб-базирано управление

Използване на удостоверяване с IEEE 802.1x за вашата мрежа

Какво представлява удостоверяване с IEEE 802.1x?

IEEE 802.1x е стандарт на IEEE, който ограничава достъпа от unauthorized мрежови устройства. Вашето устройство на Brother изпраща заявка за удостоверяване до RADIUS сървър (сървър за удостоверяване) чрез вашата точка за достъп или концентратор. След като заявката ви бъде потвърдена от RADIUS сървъра, устройството ви може да получи достъп до мрежата.

Свързана информация

- Използване на удостоверяване с IEEE 802.1x за вашата мрежа

Конфигуриране на удостоверяване с IEEE 802.1x за вашата мрежа с помощта на уеб базираното управление (уеб браузър)

- Ако конфигурирате устройството си чрез EAP-TLS удостоверяване, трябва да инсталирате клиентския сертификат, издаден от сертифициращ орган, преди да започнете конфигурирането. Свържете се с мрежовия администратор във връзка с клиентския сертификат. Ако сте инсталирали повече от един сертификат, ви препоръчваме да си запишете името на този сертификат, който искате да използвате.
- Преди да проверите сертификата на сървъра, трябва да импортирате CA сертификата, издаден от CA, подписал сертификата на сървъра. Обърнете се към мрежовия администратор или доставчика на интернет услуги (ISP), за да проверите дали е необходимо импортиране на CA сертификат.

Можете също така да конфигурирате удостоверяване с IEEE 802.1x посредством помощника за безжична настройка от контролния панел (за безжична мрежа).

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Направете едно от следните неща:
   - За кабелната мрежа

     Щракнете върху **Wired (Кабелна)** > **Wired 802.1x Authentication (Удостоверяване на кабелна мрежа 802.1x)**.
   - За безжичната мрежа

     Щракнете върху **Wireless (Безжична)** > **Wireless (Enterprise) (Безжична (корпоратативно))**.
6. Конфигурирайте настройките за удостоверяване с IEEE 802.1x.

- Ако искате да активирате удостоверяване с IEEE 802.1x за кабелни мрежи, изберете **Enabled (Разрешено)** за **Wired 802.1x status (Кабелно 802.1x състояние)** на страница **Wired 802.1x Authentication (Удостоверяване на кабелна мрежа 802.1x)**.
- Ако използвате удостоверяване с **EAP-TLS**, трябва да изберете инсталирания клиентския сертификат (показан с име на сертификата) за проверка от падащия списък **Client Certificate (Сертификат на клиента)**.
- Ако изберете удостоверяване с **EAP-FAST**, **PEAP**, **EAP-TTLS**или **EAP-TLS**, изберете метода за проверка от падащия списък **Server Certificate Verification (Проверка на сертификата на сървъра)**. Проверете сертификата на сървъра с помощта на сертификата от CO, предварително импортиран в устройството, издаден от CO, подписал сертификата на сървъра.

Изберете един от следните методи за проверка от падащия списък **Server Certificate Verification (Проверка на сертификата на сървъра)**:

Опция	Описание
No Verification (Непотвърдено)	На сертификата на сървъра винаги може да се има доверие. Проверката не е извършена.
CA Cert. (CA сертификат)	Методът за проверка на надеждността на CO на сертификата на сървъра с помощта на сертификата на CO, издаден от CO, подписал сертификата на сървъра.
CA Cert. + ServerID (CA сертификат + ServerID)	Методът за проверка на общото име [1] на сертификата на сървъра, в допълнение към надеждността на сертифициращия орган на сертификата на сървъра.

7. Когато завършите конфигурирането, щракнете върху **Submit (Изпрати)**.

   За кабелни мрежи: след конфигурирането свържете устройството си с мрежата, поддържана от IEEE 802.1x. След няколко минути отпечатайте доклада за мрежова конфигурация, за да проверите състоянието на <**Wired IEEE 802.1x**>.

Опция	Описание
Success	Кабелната функция на IEEE 802.1x е активирана и удостоверяването беше успешно.
Failed	Кабелната функция на IEEE 802.1x е активирана, обаче удостоверяването беше неуспешно.
Off	Кабелната функция на IEEE 802.1x не е достъпна.

Свързана информация

- Използване на удостоверяване с IEEE 802.1x за вашата мрежа

Свързани теми:

- Преглед на функциите на сертификата за защита
- Конфигуриране на сертификати за защита на устройството

1 Проверката на общото име сравнява общото наименование на сертификата на сървъра със символния низ, конфигуриран за **Server ID (ИД на сървъра)**. Преди да използвате този метод, обърнете се към вашия системен администратор във връзка с общото наименование на сертификата на сървъра, а след това конфигурирайте величината **Server ID (ИД на сървъра)**.

Методи за удостоверяване с IEEE 802.1x

EAP-FAST

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunnel) е разработен от Cisco Systems, Inc. и използва потребителски ИД и парола за удостоверяване, както и алгоритми за симетричен ключ, за осъществяване на tunneled процес на удостоверяване.

Устройството ви на Brother поддържа следните вътрешни методи на удостоверяване:

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (кабелна мрежа)

Разширяем протокол за удостоверяване–алгоритъм за представяне на съобщение в кратка форма 5 (EAP-MD5) използва ИД и парола на потребител за удостоверяване по метода заявка-отговор.

PEAP

Защитен разширяем протокол за удостоверяване (PEAP) е версия на EAP метода, разработен от Cisco Systems, Inc., Microsoft Corporation и RSA Security. PEAP създава шифрован Слой на защитен сокет (SSL)/Защита на транспортни слоеве (TLS) между клиент и сървър за удостоверяване, за да се изпратят потребителски идентификатор и парола. PEAP предоставя взаимно удостоверяване между сървъра и клиента.

Устройството ви на Brother поддържа следните вътрешни методи на удостоверяване:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Разширяем протокол за удостоверяване с тунелирана защита на транспортни слоеве (EAP-TTLS) е разработен от Funk Software и Certicom. EAP-TTLS създава подобен шифрован SSL тунел към PEAP, между клиент и сървър за удостоверяване, за да се изпратят потребителски идентификатор и парола. EAP-TTLS предоставя взаимно удостоверяване между сървъра и клиента.

Устройството ви на Brother поддържа следните вътрешни методи на удостоверяване:

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

Разширяем протокол за удостоверяване със защита на транспортни слоеве (EAP-TLS) изисква удостоверяване с цифров сертификат както от клиента, така и от сървъра за удостоверяване.

Свързана информация

- Използване на удостоверяване с IEEE 802.1x за вашата мрежа

Удостоверяване на потребител

Използване на удостоверяване чрез Active Directory

- Въведение в Удостоверяване въз основа на Active Directory
- Конфигуриране на удостоверяването въз основа на Active Directory чрез уеб-базирано управление
- Влезте в системата, за да промените настройките на устройството чрез контролния панел (Удостоверяванечрез Active Directory)

Въведение в Удостоверяване въз основа на Active Directory

Удостоверяването чрез Active Directory ограничава използването на устройството. Ако удостоверяването чрез Active Directory е активирано, контролният панел на устройството ще бъде заключен. Не можете да промените настройките на устройството, докато не въведете потребителски ИД и парола.

Удостоверяване чрез Active Directory предлага следните функции:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

- Съхранява входящите данни за печат
- Съхранява входящите данни за факс
- Получава имейл адрес от сървъра Active Directory въз основа на вашия потребителски идентификатор при изпращане на сканирани данни към имейл сървър.

  За да използвате тази функция, изберете опцията **On (Вкл.)** за настройката **Get Mail Address (Получаване на пощенски адрес)** и **LDAP + kerberos** или метода на удостоверяване **LDAP + NTLMv2**. Вашият имейл адрес ще бъде зададен като подател, когато устройството изпраща сканирани данни към имейл сървър, или като получател, ако искате да изпратите сканираните данни към вашия имейл адрес.

Когато е разрешено Удостоверяване въз основа на Active Directory, вашето устройство съхранява всички данни за входящите факсове. След като влезете в системата, устройството отпечатва съхранените факс данни.

Можете да промените настройките на удостоверяване въз основа на Active Directory с помощта на уеб базираното управление.

Свързана информация

- Използване на удостоверяване чрез Active Directory

Конфигуриране на удостоверяването въз основа на Active Directory чрез уеб-базирано управление

Удостоверяване въз основа на Active Directory поддържа удостоверяване Kerberos и удостоверяване NTLMv2. Трябва да конфигурирате SNTP протокола (сървър за мрежово време) и конфигурацията на DNS сървъра за удостоверяване.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **User Restriction Function (Функция за потреб. огранич.)** или **Restriction Management (Управл. на ограниченията)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Изберете **Active Directory Authentication (Active Directory удостоверяване)**.
6. Щракнете върху **Submit (Изпрати)**.
7. Щракнете върху **Active Directory Authentication (Active Directory удостоверяване)**.
8. Конфигурирайте следните настройки:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

Опция	Описание
Storage Fax RX Data (Съхранени факс RX данни)	Изберете тази опция за съхранение на входящи факс данни. Можете да отпечатвате всички входящи факс данни, след като влезете в системата на устройството.
Remember User ID (Запомняне на потребителския ИД)	Изберете тази опция, за да запишете вашия потребителски ИД.
Active Directory Server Address (Адрес на сървъра за Active Directory)	Напишете IP адреса или името на сървъра (например: ad.example.com) на Active Directory.
Active Directory Domain Name (Име на домейна за Active Directory)	Въведете името на домейн на Active Directory.
Protocol & Authentication Method (Протокол и метод за удостоверяване)	Изберете протокола и метода на удостоверяване.
SSL/TLS	Изберете опцията **SSL/TLS**.

Опция	Описание
LDAP Server Port (LDAP сървърен порт)	Въведете номера на порта, за да се свържете със сървъра на Active Directory през LDAP (може да се използва само за метод на удостоверяване **LDAP + kerberos** или **LDAP + NTLMv2**).
LDAP Search Root (LDAP маршрут за търсене)	Напишете корена на търсенето с LDAP (достъпно само за метод на удостоверяване **LDAP + kerberos** или **LDAP + NTLMv2**).
Get Mail Address (Получаване на пощенски адрес)	Изберете тази опция, за да получите имейл адреса на влезлия потребител от сървъра Active Directory. (Достъпно само за метод на удостоверяване **LDAP + kerberos** или **LDAP + NTLMv2**)
Get User's Home Directory (Получаване на началната директория на потребителя)	Изберете тази опция, за да получите вашата начална директория и да я зададете като местоназначение за функцията “Сканиране към мрежа”. (Достъпно само за метод на удостоверяване **LDAP + kerberos** или **LDAP + NTLMv2**)

9. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Използване на удостоверяване чрез Active Directory

Влезте в системата, за да промените настройките на устройството чрез контролния панел (Удостоверяванечрез Active Directory)

Когато е активирано удостоверяване чрез Active Directory, контролният панел на устройството ще бъде заключен, докато не въведете вашия потребителски ИД и парола от контролния панел на устройството.

1. На контролния панел на устройството въведете вашия потребителски ИД и парола, за да влезете в системата.
2. Когато удостоверяването е успешно, контролният панел на устройството се отключва.

Свързана информация

- Използване на удостоверяване чрез Active Directory

Използване на удостоверяване чрез LDAP

- Въведение в удостоверяването чрез LDAP
- Конфигуриране на удостоверяване чрез LDAP с помощта на уеб-базираното управление
- Влизане за промяна на настройките на устройството от контролния му панел (удостоверяване чрез LDAP)

Въведение в удостоверяването чрез LDAP

Удостоверяването чрез LDAP ограничава използването на устройството. Ако е активирано удостоверяване чрез LDAP, контролният панел на устройството ще бъде заключен.Не можете да промените настройките на устройството, докато не въведете потребителски ИД и парола.

Удостоверяване чрез LDAP предлага следните функции:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

- Съхранява входящите данни за печат
- Съхранява входящите данни за факс
- Получава имейл адрес от LDAP сървъра въз основа на вашия потребителски ИД при изпращане на сканирани данни към имейл сървър.

  За да използвате тази функция, изберете опцията **On (Вкл.)** за настройката **Get Mail Address (Получаване на пощенски адрес)**. Вашият имейл адрес ще бъде зададен като подател, когато устройството изпраща сканирани данни към имейл сървър, или като получател, ако искате да изпратите сканираните данни към вашия имейл адрес.

Когато е разрешено Удостоверяване чрез LDAP, вашето устройство съхранява всички данни за входящите факсове. След като влезете в системата, устройството отпечатва съхранените факс данни.

Можете да промените настройките на удостоверяване въз основа на LDAP с помощта на уеб базираното управление.

Свързана информация

- Използване на удостоверяване чрез LDAP

Конфигуриране на удостоверяване чрез LDAP с помощта на уеб-базираното управление

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **User Restriction Function (Функция за потреб. огранич.)** или **Restriction Management (Управл. на ограниченията)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Изберете **LDAP Authentication (LDAP удостоверяване)**.
6. Щракнете върху **Submit (Изпрати)**.
7. Щракнете върху менюто **LDAP Authentication (LDAP удостоверяване)**.
8. Конфигурирайте следните настройки:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

Опция	Описание
Storage Fax RX Data (Съхранени факс RX данни)	Изберете тази опция за съхранение на входящи факс данни. Можете да отпечатвате всички входящи факс данни, след като влезете в системата на устройството.
Remember User ID (Запомняне на потребителския ИД)	Изберете тази опция, за да запишете вашия потребителски ИД.
LDAP Server Address (Адрес на LDAP сървър)	Въведете IP адреса или името на сървъра (напр. ldap.example.com) на LDAP сървъра.
SSL/TLS	Изберете опцията **SSL/TLS**, за да използвате LDAP по SSL/TLS.
LDAP Server Port (LDAP сървърен порт)	Въведете номера на порта на LDAP сървъра.
LDAP Search Root (LDAP маршрут за търсене)	Въведете главната папка за LDAP търсене.
Attribute of Name (Search Key) (Атрибут към името (Ключ за търсене))	Въведете атрибута, който искате да използвате като ключ за търсене.
Get Mail Address (Получаване на пощенски адрес)	Изберете тази опция, за да получите имейл адреса на влезлия потребител от LDAP сървъра.

Опция	Описание
Get User's Home Directory (Получаване на началната директория на потребителя)	Изберете тази опция, за да получите вашата начална директория и да я зададете като местоназначение за функцията “Сканиране към мрежа”.

9. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Използване на удостоверяване чрез LDAP

Влизане за промяна на настройките на устройството от контролния му панел (удостоверяване чрез LDAP)

Когато е активирано удостоверяване чрез LDAP, контролният панел на устройството ще бъде заключен, докато не въведете вашия потребителски ИД и парола от контролния панел на устройството.

1. На контролния панел на устройството въведете вашия потребителски ИД и парола, за да влезете в системата.
2. Когато удостоверяването е успешно, контролният панел на устройството се отключва.

Свързана информация

- Използване на удостоверяване чрез LDAP

Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Secure Function Lock (заключваща функция за безопасност) 3.0 повишава сигурността чрез ограничаване на функциите, налични на устройството.

Преди да се използва Secure Function Lock 3.0

Използвайте Secure Function Lock (заключваща функция за безопасност), за да конфигурирате пароли, да определяте ограничения за страници за определен потребител и да предоставяте достъп до някои или всички функции, изброени тук.

Можете да конфигурирате и промените следните настройки на Secure Function Lock (заключваща функция за безопасност) 3.0 чрез уеб базираното управление:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

- **Print (Печат)**
- **Copy (Копиране)**
- **Scan (Сканиране)**
- **Факс**
- **Носител**
- **Web Connect (Уеб свързване)**
- **Apps (Приложения)**
- **Page Limits (Ограничение за страниците)**
- **Page Counters (Броячи за страници)**
- **Card ID (NFC ID) (ИД на карта (NFC ИД))**

Модели със сензорен LCD дисплей:

Когато функцията Secure Function Lock е активирана, устройството автоматично влиза в публичен режим и някои от функциите на устройството стават ограничени само за authorized потребители. За достъп до ограничените функции на устройството натиснете , изберете вашето потребителско име и въведете паролата си.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Конфигуриране на Secure Function Lock 3.0 с помощта на Уеб-базирано управление

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **User Restriction Function (Функция за потреб. огранич.)** или **Restriction Management (Управл. на ограниченията)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Изберете **Secure Function Lock (Защитно закл. функция)**.
6. Щракнете върху **Submit (Изпрати)**.
7. Щракнете върху менюто **Restricted Functions (Ограничени функции)**.
8. Конфигурирайте настройките, за да управлявате ограниченията по потребител или група.
9. Щракнете върху **Submit (Изпрати)**.
10. Щракнете върху менюто **User List (Списък с потребители)**.
11. Конфигурирайте списъка с потребители.
12. Щракнете върху **Submit (Изпрати)**.

Можете също така да промените настройките за блокиране за списъка с потребители в меню **Secure Function Lock (Защитно закл. функция)**.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Сканиране чрез Secure Function Lock 3.0

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

Настройка на ограниченията за сканиране (за администратори)

Secure Function Lock (заключваща функция за безопасност) 3.0 позволява на администратора да определи кои потребители имат право да сканират. Когато функцията за сканиране е зададена на Изкл. за настройката за публичен потребител, само потребители, за които е отметнато **Scan (Сканиране)**, ще могат да сканират.

Използване на функцията Сканиране (за потребители с ограничен достъп)

- За сканиране с помощта на контролния панел на устройството:

  Ограничените потребители трябва да въведат своите пароли на контролния панел на устройството, за да получат достъп до режим Сканиране.
- За сканиране от компютър:

  Ограничените потребители трябва да въведат своите пароли на контролния панел на устройството, преди да сканират от компютрите си. Ако не се въведе паролата на контролния панел на устройството, на компютъра на потребителя ще се покаже съобщение за грешка.

Ако устройството поддържа удостоверяване с IC карта, ограничени потребители също могат да получат достъп до режима на сканиране чрез докосване на символа NFC на контролния панел на устройството с регистрираните си IC карти.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Конфигуриране на Public Mode (Публичен режим) за Secure Function Lock 3.0

Използвайте екрана на Secure Function Lock (Заключваща функция за безопасност), за да конфигурирате публичен режим, който ограничава функциите, достъпни за потребители с публичен достъп. Няма да е необходимо потребителите с публичен достъп да въвеждат парола за достъп до функциите, достъпни чрез настройките на публичния режим.

Публичният режим включва заявки за печат, изпратени чрез Brother iPrint&Scan и Brother Mobile Connect.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **User Restriction Function (Функция за потреб. огранич.)** или **Restriction Management (Управл. на ограниченията)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Изберете **Secure Function Lock (Защитно закл. функция)**.
6. Щракнете върху **Submit (Изпрати)**.
7. Щракнете върху менюто **Restricted Functions (Ограничени функции)**.
8. В реда **Public Mode (Публичен режим)** поставете отметка в квадратчето, за да разрешите съответната функция, или премахнете отметка, за да я забраните.
9. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Конфигуриране на лични настройки на началните екрани с помощта на уеб базираното управление

Като администратор, можете да зададете кои раздели потребителите могат да виждат на личните си начални екрани. Тези раздели осигуряват бърз достъп до favorite преки пътища на потребителите, които те могат да присвоят на разделите на личните си начални екрани от контролния панел на устройството.

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **User Restriction Function (Функция за потреб. огранич.)** или **Restriction Management (Управл. на ограниченията)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Изберете **Secure Function Lock (Защитно закл. функция)**.
6. В полето **Tab Settings (Настройки за раздел)** изберете **Personal (Лично)** за имената на разделите, които искате да използвате като свой личен начален екран.
7. Щракнете върху **Submit (Изпрати)**.
8. Щракнете върху менюто **Restricted Functions (Ограничени функции)**.
9. Конфигурирайте настройките, за да управлявате ограниченията по потребител или група.
10. Щракнете върху **Submit (Изпрати)**.
11. Щракнете върху менюто **User List (Списък с потребители)**.
12. Конфигурирайте списъка с потребители.
13. Изберете **User List / Restricted Functions (Потребителски списък/Ограничени функции)** от падащия списък за всеки потребител.
14. Изберете името на раздела от падащия списък **Home Screen (Начален екран)** за всеки потребител.
15. Щракнете върху **Submit (Изпрати)**.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Допълнителни функции на Secure Function Lock 3.0

Конфигурирайте следните функции на екрана Secure Function Lock (заключваща функция за безопасност):

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

All Counter Reset (Нулиране на всички броячи)

Щракнете върху **All Counter Reset (Нулиране на всички броячи)** в колоната **Page Counters (Броячи за страници)**, за да нулирате брояча на страници.

Export to CSV file (Експортиране в CSV файл)

Щракнете върху **Export to CSV file (Експортиране в CSV файл)**, за да експортирате текущия и последния брояч на страници, включително информация за **User List / Restricted Functions (Потребителски списък/Ограничени функции)**, като CSV файл.

Card ID (NFC ID) (ИД на карта (NFC ИД))

Щракнете върху менюто **User List (Списък с потребители)**, а след това напишете идентификационния номер на картата на потребителя в полето **Card ID (NFC ID) (ИД на карта (NFC ИД))**. Можете да използвате IC картата си за удостоверяване.

Output (Изход)

Когато специализираната изходяща тава е поставена на устройството ви, изберете изходящата тава за всеки потребител от падащия списък.

Last Counter Record (Последен запис от брояча)

Щракнете върху **Last Counter Record (Последен запис от брояча)**, ако искате устройството да запази броя страници след нулирането на брояча.

Counter Auto Reset (Автоматично нулиране на брояча)

Щракнете върху **Counter Auto Reset (Автоматично нулиране на брояча)**, за да конфигурирате желания интервал от време между нулиранията на брояча на страници. Изберете ежедневен, ежеседмичен или ежемесечен интервал.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Регистриране на нова IC карта от контролния панел на устройството

Можете да регистрирате карти с интегрални схеми (карти с ИС) на своето устройство.

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

1. Допрете символа за комуникация в близко поле (NFC) на контролния панел на устройството с регистрирана микропроцесорна карта (IC карта).
2. Натиснете вашия потребителски ИД на LCD дисплея.
3. Натиснете бутона Register Card (Регистриране на карта).
4. Докоснете нова IC карта до символа NFC.

   След това номерът на новата IC карта се регистрира в устройството.
5. Натиснете бутона OK.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Регистриране на външен четец на IC карти

Когато свържете външен четец на IC карти (микропроцесорни карти), използвайте уеб базирано управление, за да го регистрирате. Вашето устройство поддържа външни четци на IC карти, поддържани от драйвери от HID клас.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **External Card Reader (Външен четец на карти)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. Въведете необходимата информация и след това щракнете върху **Submit (Изпрати)**.
6. Рестартирайте устройството Brother, за да активирате конфигурацията.
7. Свържете карточетеца към устройството си.
8. Допрете картата до четеца на карти, когато използвате удостоверяване на картата.

Свързана информация

- Използване на Secure Function Lock (заключваща функция за безопасност) 3.0

Безопасно изпращане и получаване на имейл

- Конфигуриране на изпращане и получаване на имейл чрез уеб базираното управление
- Изпращане на имейл с удостоверяване на потребителя
- Безопасно изпращане и получаване на имейл чрез SSL/TLS

Конфигуриране на изпращане и получаване на имейл чрез уеб базираното управление

- Получаване на имейл се предлага само за някои модели.
- Препоръчваме ви да използвате уеб базирано управление, за да конфигурирате безопасно изпращане на имейл с удостоверяване на потребителя или изпращане и получаване на имейл с помощта на SSL/TLS (само поддържаните модели).

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Network (Мрежа)** > **Network (Мрежа)** > **Protocol (Протокол)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. В полето **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP клиент)** щракнете върху **Advanced Settings (Разширени настройки)** и се уверете, че състоянието на **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP клиент)** е **Enabled (Разрешено)**.

- Наличните протоколи може да се различават в зависимост от вашето устройство.
- Ако се появи екранът за избор **Authentication Method (Метод на удостоверяване)**, изберете вашия метод на удостоверяване, след което следвайте инструкциите на екрана.

6. Конфигурирайте настройките на **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP клиент)**.
   - Проверете дали имейл настройките са правилни след конфигурирането им чрез изпращане на тестов имейл.
   - Ако не знаете настройките на POP3/IMAP4/SMTP сървъра, свържете се с вашия мрежов администратор или доставчика на интернет услуги (ISP).
7. Когато приключите, щракнете върху **Submit (Изпрати)**.

   Показва се диалоговият прозорец **Test Send/Receive E-mail Configuration (Тестване на конфигурацията за изпращане/получаване на имейли)**.
8. Следвайте инструкциите в диалоговия прозорец за проверка на текущите настройки.

Свързана информация

- Безопасно изпращане и получаване на имейл

Свързани теми:

- Безопасно изпращане и получаване на имейл чрез SSL/TLS

Изпращане на имейл с удостоверяване на потребителя

Вашето устройство изпраща имейли чрез имейл сървър, който изисква удостоверяване на потребителите. Този метод не позволява на unauthorized потребители да осъществяват достъп до имейл сървъра.

Можете да изпращате уведомление по имейл, имейл отчети и I-Fax (достъпно само за определени модели), като използвате удостоверяване на потребителя.

- Наличните протоколи може да се различават в зависимост от вашето устройство.
- Препоръчваме ви да използвате уеб базирано управление, за да конфигурирате SMTP удостоверяването.

Настройки на имейл сървър

Трябва да конфигурирате метода на удостоверяване на SMTP на вашето устройство така, че да съвпада с метода, използван от вашия имейл сървър. За подробности относно настройките на имейл сървъра се обърнете към мрежовия администратор или доставчика на интернет (ISP).

За да активирате удостоверяване на SMTP сървър с помощта на уеб базирано управление, изберете вашия метод на удостоверяване под **Server Authentication Method (Метод на удостоверяване на сървъра)** на екрана **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP клиент)**.

Свързана информация

- Безопасно изпращане и получаване на имейл

Безопасно изпращане и получаване на имейл чрез SSL/TLS

Вашето устройство поддържа SSL/TLS методи за комуникация. За да използвате имейл сървър, който използва SSL/TLS комуникация, трябва да конфигурирате следните настройки.

- Получаване на имейл се предлага само за някои модели.
- Препоръчваме ви да използвате уеб базирано управление за конфигуриране на SSL/TLS.

Проверка на сертификата на сървъра

Ако в **SSL/TLS** изберете **SSL** или **TLS**, квадратчето за отметка **Verify Server Certificate (Проверка на сертификата на сървъра)** ще бъде отметнато автоматично.

- Преди да проверите сертификата на сървъра, трябва да импортирате сертификата, издаден от CO, подписал сертификата на сървъра. Обърнете се към мрежовия администратор или доставчика на Интернет услуги (ISP), за да проверите дали е необходимо импортиране на сертификат от CO.
- Ако не е необходимо да проверявате сертификата на сървъра, отстранете отметката от квадратчето за отметка **Verify Server Certificate (Проверка на сертификата на сървъра)**.

Номер на порт

Ако изберете **SSL** или **TLS**, стойността на **Port (Порт)** ще бъде променена така, че да съвпада с протокола. За да промените номера на порта ръчно, въведете го, след като сте избрали настройките на **SSL/TLS**.

Трябва да конфигурирате метода за комуникация на вашето устройство, така че да съвпада с метода, използван от вашия имейл сървър. За подробности относно настройките на имейл сървъра се обърнете към мрежовия администратор или доставчика на интернет услуги.

В повечето случаи защитените услуги за уеб имейл изискват следните настройки:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

SMTP	**Port (Порт)**	587
	Server Authentication Method (Метод на удостоверяване на сървъра)	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port (Порт)**	995
	SSL/TLS	**SSL**
IMAP4	**Port (Порт)**	993
	SSL/TLS	**SSL**

Свързана информация

- Безопасно изпращане и получаване на имейл

Свързани теми:

- Конфигуриране на изпращане и получаване на имейл чрез уеб базираното управление
- Конфигуриране на сертификати за защита на устройството

Запаметяване на дневника за печат в мрежата

Общ преглед на функцията за съхранение на дневника за печат в мрежата

Функцията Запаметяване на дневника за печат в мрежата ви позволява да запазите файл с дневника за печат от вашето устройство в мрежов сървър с помощта на протокола Обща Интернет файлова система (CIFS). Можете да запишете идентификатора, типа заявка за печат, името на задачата, потребителското име, датата, часа и броя на отпечатаните страници за всяка заявка за печат. CIFS е протокол, който работи по TCP/IP, и позволява на компютрите в една мрежа да споделят файлове по интранет или Интернет.

В дневника за печат се записват следните функции за печат:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

- Заявките за печат от вашия компютър
- Директен печат през USB
- Копиране
- Получен факс
- Печат чрез Web Connect

- Функцията “Запаметяване на дневника за печат в мрежата” поддържа удостоверяване Kerberos и удостоверяване NTLMv2. Трябва да конфигурирате протокола SNTP (сървър за време на мрежата) или трябва да настроите правилно датата, часа и часовата зона от контролния панел за удостоверяване.
- Можете да настроите типа файл на TXT или CSV, когато запаметявате файл в сървъра.

Свързана информация

- Запаметяване на дневника за печат в мрежата

Конфигуриране на настройките на запаметяване на дневника за печат в мрежата чрез Уеб-базирано управление

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **Store Print Log to Network (Съхраняване на регистъра за печат в мрежата)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. В полето **Print Log (Регистър за печат)** щракнете върху **On (Вкл.)**.
6. Конфигурирайте следните настройки:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

Опция	Описание
Network Folder Path (Път до папка в мрежата)	Въведете папката местоназначение, където ще се съхранява вашият дневник за печат на CIFS сървъра (например: \\ComputerName \SharedFolder).
File Name (Име на файл)	Напишете името на файла, който искате да използвате за дневника за печат (до 32 знака).
File Type (Вид на файл)	Изберете опцията **TXT** или **CSV** за тип на файла на дневника за печат.
Time Source for Log (Времеви източник за регистъра)	Изберете източника на време за дневника за печат.
Auth. Method (Метод на удостоверяване)	Изберете метода на удостоверяване, необходим за достъп до CIFS сървъра: **Auto (Авто)**, **Kerberos** или **NTLMv2**. Kerberos е протокол за удостоверяване, който позволява на устройства или хора безопасно да докажат своята самоличност на мрежови сървъри чрез еднократно въвеждане на парола. NTLMv2 е методът за удостоверяване, който Windows използва за влизане в сървъри. • **Auto (Авто)**: Ако изберете **Auto (Авто)**, NTLMv2 ще се използва за метод на удостоверяване. • **Kerberos**: Изберете опцията **Kerberos**, за да използвате само удостоверяване Kerberos. • **NTLMv2**: Изберете опцията **NTLMv2**, за да използвате само удостоверяване NTLMv2.

Опция	Описание
	• За удостоверяване **Kerberos** и **NTLMv2** трябва да конфигурирате и настройките за **Date&Time (Дата и час)** или протокола SNTP (мрежов сървър за време) и DNS сървъра. • Можете също да конфигурирате настройките за датата и часа от контролния панел на устройството.
Username (Потребителско име)	Напишете потребителското име за удостоверяване (до 96 знака). Ако потребителското име е част от домейн, въведете потребителското име, като използвате един от следните стилове: user@domain или domain\user.
Password (Парола)	Напишете паролата за удостоверяване (до 32 знака).
Kerberos Server Address (Адрес на сървър Kerberos) (при необходимост)	Напишете адреса на хоста на центъра за разпространение на ключове (KDC) (например: kerberos.example.com; до 64 знака) или IP адреса (например: 192.168.56.189).
Error Detection Setting (Настройка за откриване на грешки)	Изберете какво да се предприеме, когато дневникът за печат не може да се запамети в сървъра поради грешка в мрежата.

7. В полето **Connection Status (Състояние на връзката)** проверете последното състояние в регистрационния файл.

Можете също да проверите състоянието на грешката на LCD дисплея на устройството.

8. Щракнете върху **Submit (Изпрати)**, за да се отвори страница **Test Print Log to Network (Тест на регистъра за печат в мрежата)**.

   За да проверите настройките, щракнете върху **Yes (Да)** и преминете на следващата стъпка.

   За да пропуснете проверката, щракнете върху **No (Не)**. Настройките ще бъдат изпратени автоматично.
9. Устройството ще провери вашите настройки.
10. Ако настройките бъдат приети, на екрана се показва **Test OK (Тестът е успешен)**.

    Ако се появи **Test Error (Грешка в тест)**, проверете всички настройки, а след това щракнете върху **Submit (Изпрати)**, за да се отвори отново тестовата страница.

Свързана информация

- Запаметяване на дневника за печат в мрежата

Използване на настройката Откриване на грешки на Запаметяване на дневника за печат в мрежата

Използвайте настройките за откриване на грешки, за да определите действието, което трябва да се предприеме, когато дневникът за печат не може да се запамети в сървъра поради грешка в мрежата.

1. Стартирайте уеб браузъра.
2. Въведете “https://IP адрес на устройството” в адресната лента на браузъра (където “IP адрес на устройството” е IP адресът на вашето устройство).

   Например:

   https://192.168.1.2

   IP адреса на вашето устройство можете да намерите в отчета за мрежовата конфигурация.
3. Ако се изисква, въведете паролата в полето **Login (Вход)**, след което щракнете върху **Login (Вход)**.

Паролата по подразбиране за управление на настройките на това устройство се намира на гърба или на основата на устройството и е отбелязана с “**Pwd**”. Сменете паролата по подразбиране, като следвате инструкциите на екрана, когато влезете в системата за първи път.

4. Щракнете върху **Administrator (Администратор)** > **Store Print Log to Network (Съхраняване на регистъра за печат в мрежата)** в лявата навигационна лента.

Ако лявата навигационна лента не се вижда, започнете навигацията от ☰.

5. В раздел **Error Detection Setting (Настройка за откриване на грешки)** изберете опцията **Cancel Print (Отказ на печата)** или **Ignore Log & Print (Игнорирай регистъра и отпечатай)**.

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

Опция	Описание
Cancel Print (Отказ на печата)	Ако изберете опцията **Cancel Print (Отказ на печата)** заявките за печат се canceled, когато дневникът за печат не може да се запамети в сървъра. Дори ако изберете опцията **Cancel Print (Отказ на печата)**, устройството ще отпечата получен факс.

Ignore Log & Print (Игнорирай регистъра и отпечатай)	Ако изберете опцията **Ignore Log & Print (Игнорирай регистъра и отпечатай)**, устройството ще отпечата документите, дори ако дневникът за печат не може да се запамети в сървъра.
	
	Когато функцията за запаметяване на дневника за печат се възстанови, дневникът за печат се записва, както следва:
	
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	
	a. Ако дневникът за печат не може да се съхрани в края на печатането, броят на отпечатаните страници няма да се запише.
	b. Ако дневникът за печат не може да се запамети в началото и в края на печатането, дневникът за печат на заявката няма да се запише. Когато функцията се възстанови, грешката се отразява в дневника за печат.

6. Щракнете върху **Submit (Изпрати)**, за да се отвори страница **Test Print Log to Network (Тест на регистъра за печат в мрежата)**.

   За да проверите настройките, щракнете върху **Yes (Да)** и преминете на следващата стъпка.

   За да пропуснете проверката, щракнете върху **No (Не)**. Настройките ще бъдат изпратени автоматично.
7. Устройството ще провери вашите настройки.
8. Ако настройките бъдат приети, на екрана се показва **Test OK (Тестът е успешен)**.

   Ако се появи **Test Error (Грешка в тест)**, проверете всички настройки, а след това щракнете върху **Submit (Изпрати)**, за да се отвори отново тестовата страница.

Свързана информация

- Запаметяване на дневника за печат в мрежата

Използване на Запаметяване на дневника за печат в мрежата със Secure Function Lock 3.0

Когато Secure Function Lock 3.0 Secure Function Lock (заключваща функция за безопасност) е активна, имената на регистрираните потребители за копиране, Fax RX, печат чрез Web Connect Print и Директен печат от USB се записват в справката “Запаметяване на дневника за печат в мрежата”. Когато е активирано удостоверяване чрез Active Directory, потребителското име се записва в отчета “Съхраняване на дневника за печат в мрежата”:

Поддържаните функции, опции и настройки може да се различават в зависимост от вашия модел.

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

Свързана информация

- Запаметяване на дневника за печат в мрежата

brother

Brother Earth

www.brotherearth.com

BUL
Вариант 0