

# Мрежово ръководство

---

---

## Съдържание

**Съдържание****Авторско право****Търговски марки****Относно това ръководство**

Знаци и символи. . . . .	6
Описания, използвани в това ръководство. . . . .	6
Справки за операционните системи. . . . .	6

**Въведение**

Ръчен компонент. . . . .	8
Дефиниции на термините, използвани в това ръководство. . . . .	8

**Подготовка**

Поток на настройките на принтера. . . . .	10
Въведение в свързването на принтера. . . . .	10
Настройки на връзка сървър/клиент. . . . .	11
Настройки на връзка тип „Peer to Peer“. . . . .	11
Подготовка за свързване към мрежата. . . . .	11
Събиране на информация в настройката за свързване. . . . .	11
Спецификации на принтера. . . . .	12
Тип назначаване на IP адрес. . . . .	12
Метод за настройка на мрежова връзка. . . . .	12
Инсталиране на EpsonNet Config. . . . .	13
Изпълнение на EpsonNet Config. . . . .	13

**Свързване**

Свързване към мрежата. . . . .	14
Свързване към LAN. . . . .	14
Назначаване на IP адрес чрез EpsonNet Config. . . . .	14
Свързване към мрежата с използване на програмата за инсталиране. . . . .	18

**Настройки на функции**

Web Config (уеб страница за устройството). . . . .	20
Относно Web Config. . . . .	20

Достъп до Web Config. . . . .	20
Използване на функции за печат. . . . .	21
Изисквания за печат по мрежа. . . . .	21
Настройка на драйвер на принтер с използване на връзка клиент/сървър. . . . .	21
Настройки на драйвера на принтера за връзка тип „Peer to Peer“. . . . .	26

**Настройки за защита**

Настройки за защита и предпазване от опасност. . . . .	28
Настройки на функциите за защита. . . . .	29
Конфигуриране на администраторска парола . . . . .	29
Конфигуриране на администраторска парола чрез Web Config. . . . .	29
Управляващи протоколи и услуги. . . . .	30
Управляващи протоколи. . . . .	30
SSL/TLS комуникация с принтера. . . . .	34
Относно цифрово сертифициране. . . . .	35
Получаване и импортиране на сертификат, подписан от сертифициращ орган. . . . .	35
Изтриване на сертификат, подписан от сертифициращ орган. . . . .	39
Актуализиране на самоподписан сертификат. . . . .	39
Шифрована комуникация с IPsec/IP филтриране. . . . .	40
Относно IPsec/IP филтрирането. . . . .	40
Конфигуриране на правила по подразбиране. . . . .	41
Конфигуриране на групови правила. . . . .	43
Примери за конфигурация на IPsec/IP Filtering (IPsec/IP филтриране). . . . .	48
Използване на SNMPv3 протокол. . . . .	50
Относно SNMPv3. . . . .	50
Конфигуриране на SNMPv3. . . . .	50

**Разрешаване на проблеми**

Проверка на регистри за сървър и мрежово устройство. . . . .	53
Печат на лист за състоянието на мрежата. . . . .	53
Инициализиране на мрежовите настройки. . . . .	53
Възстановяване на мрежовите настройки от принтера. . . . .	53

**Съдържание**

Възстановяване на мрежови настройки с помощта на EpsonNet Config. . . . .	54
Проверка на комуникацията между устройства и компютри. . . . .	54
Проверка на връзката чрез команда Ping. . . . .	54
Проблеми при използване на мрежов софтуер . . . . .	55
Няма достъп до Web Config. . . . .	55
Името на модела и/или IP адресът не се показват на EpsonNet Config. . . . .	56
Решаване на проблеми за повишена защита. . . . .	56
Възстановяване на настройките за защита . . . . .	56
Забрана на функцията за защита от принтера. . . . .	56
Възстановяване на функциите за защита с Web Config. . . . .	57
Проблеми при използване на функциите за мрежова защита. . . . .	58
Проблеми при използване на цифров сертификат. . . . .	59

**Приложение**

Въведение в мрежов софтуер. . . . .	63
Epson Device Admin. . . . .	63
EpsonNet Print. . . . .	63
EpsonNet SetupManager. . . . .	63

**Авторско право**

---

**Авторско право**

Никоя част от тази публикация не може да бъде възпроизведена, съхранявана в система за извличане на информация или изпращана в каквато и да е форма или по какъвто и да е начин – електронен, механичен, чрез фотокопиране, записване или по друг начин, без предварителното разрешение на Seiko Epson Corporation. Не се поема никаква патентна отговорност по отношение на употребата на съдържащата се тук информация. Не се поема отговорност за повреди, дължащи се на използването на информацията тук. Информацията, предоставена в настоящия документ, е предназначена за използване само с този продукт на Epson. Epson не носи отговорност за каквато и да е употреба на тази информация по отношение на други принтери.

Seiko Epson Corporation и нейните филиали не носят отговорност пред купувача на този продукт или пред трети страни за щети, загуби, разноси или разходи, понесени от купувача или трети страни, в резултат на инцидент, неправилна употреба или злоупотреба с този продукт или в резултат на неоторизирани модификации, ремонти или изменения на този продукт или (с изключение на САЩ) ако не се спазват стриктно работните инструкции и инструкциите за техническа поддръжка на Seiko Epson Corporation.

Seiko Epson Corporation и нейните филиали не са отговорни за щети или проблеми, възникнали от употребата на каквато и да е опция или консумативи, различни от указаните като Оригинални продукти на Epson или Одобрени от Epson продукти от Seiko Epson Corporation.

Seiko Epson Corporation не носи отговорност за щети в резултат на електромагнитни смущения, които възникват от употребата на интерфейсни кабели, различни от обозначените като Одобрени от Epson продукти от Seiko Epson Corporation.

© 2017 Seiko Epson Corporation

Съдържанието на това ръководство и спецификациите на този продукт подлежат на промяна без предизвестие.

## Търговски марки

---

### **Търговски марки**

- ❑ EPSON® е регистрирана търговска марка и EPSON EXCEED YOUR VISION или EXCEED YOUR VISION е търговска марка на Seiko Epson Corporation.
- ❑ Софтуерът Epson Scan 2 е базиран частично на работата на Independent JPEG Group.
- ❑ Google Cloud Print™, Chrome™, Chrome OS™ и Android™ са търговски марки на Google Inc.
- ❑ Microsoft®, Windows®, Windows Server® и Windows Vista® са регистрирани търговски марки на Microsoft Corporation.
- ❑ IBM е регистрирана търговска марка на International Business Machines Corporation.
- ❑ Обща бележка: Другите имена на продукти, които се използват тук, са само за информация и е възможно да са търговски марки на съответните им собственици. Epson не разполага с никакви права над тези марки.

**Относно това ръководство****Относно това ръководство****Знаци и символи****Внимание:**

Инструкции, които трябва да се спазват внимателно, за да се избегнат наранявания.

**Важно:**

Инструкции, които трябва да се спазват, за да се избегне повреда на оборудването.

**Забележка:**

Инструкции, които съдържат полезни съвети и ограничения относно работата на продукта.

**Още по темата**

➔ Щракването върху тази икона ще Ви отведе до свързана с темата информация.

**Описания, използвани в това ръководство**

Илюстрациите на принтера, използвани в това ръководство, са само примерни. Въпреки че може да има малки разлики в зависимост от модела, методът на работа е същият.

**Справки за операционните системи****Windows**

Употребените в това ръководство термини, като например "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2", "Windows Server 2008", "Windows Server 2003 R2" и "Windows Server 2003" се отнасят до следните операционни системи. В допълнение "Windows" се отнася до всички версии.

- Microsoft® Операционна система Windows® 10
- Microsoft® Операционна система Windows® 8.1
- Microsoft® Операционна система Windows® 8
- Microsoft® Операционна система Windows® 7
- Microsoft® Операционна система Windows Vista®
- Microsoft® Операционна система Windows® XP
- Microsoft® Операционна система Windows® XP Professional x64 Edition
- Microsoft® Операционна система Windows Server® 2012 R2

**Относно това ръководство**

- Microsoft® Операционна система Windows Server® 2012
- Microsoft® Операционна система Windows Server® 2008 R2
- Microsoft® Операционна система Windows Server® 2008
- Microsoft® Операционна система Windows Server® 2003 R2
- Microsoft® Операционна система Windows Server® 2003

---

## Въведение

### Ръчен компонент

Това ръководство обяснява как да свържете принтера към мрежата и съдържа информация относно как се конфигурират настройките за използване на функциите.

Вижте *Ръководство на потребителя* за информация за използване на функциите.

#### Подготовка

Обяснява как да конфигурирате устройствата и софтуера, който се използва за управление.

#### Свързване

Обяснява как да свържете принтер към мрежата.

#### Настройки на функции

Обяснява настройките за печат.

#### Настройки за защита

Описва настройките за защита, например настройки на администраторска парола и управление на протоколи.

#### Разрешаване на проблеми

Описва инициализацията на настройките и отстраняването на неизправности в мрежата.

## Дефиниции на термините, използвани в това ръководство

Следните термини се използват в това ръководство.

#### Администратор

Лицето, което отговаря за инсталиране и настройка на устройството или мрежата в офиса или организацията. За малки организации това лице може да отговаря за администрирането на устройствата и на мрежата. За големи организации администраторите управляват мрежата или устройствата в група в отдела или подразделението, а мрежовите администратори отговарят за комуникационните настройки извън организацията, например интернет.

#### Мрежов администратор

Лицето, което отговаря за управление на мрежовите комуникации. Лицето, което настройва маршрутизатора, прокси сървър, DNS сървър и имейл сървър за управление на комуникациите с интернет или в мрежата.

#### Потребител

Лице, което използва устройствата, например принтери.

#### Връзка сървър/клиент (споделяне на принтера със сървър на Windows)

Връзка, която указва, че принтерът е свързан към Windows сървър по мрежата или чрез USB кабел, и опашката за печат, настроена на сървъра, може да бъде споделена. Комуникацията между принтера и компютъра минава през сървъра и принтерът се управлява от сървъра.



## Въведение

### Връзка „Peer to peer“ (директен печат)

Връзка, която указва, че принтерът и компютърът са свързани по мрежата чрез концентратор или точка за достъп, и заданието за печат може да бъде изпълнено директно от компютъра.

### Web Config (уеб страницата на устройството)

Уеб сървър, който е вграден в устройството. Нарича се Web Config. Можете да проверите и да промените състоянието на устройството през браузър.

### Опашка за печат

За Windows иконата за всеки порт е показана в **Devices and Printers (Устройства и принтери)**, например принтер. Две или повече икони се създават дори за едно устройство, ако то е свързано към мрежата чрез два или повече порта, например стандартен TCP/IP порт.

### Инструмент

Общ термин за обозначаване на софтуер за настройка или управление на устройство, например Epson Device Admin, EpsonNet Config, EpsonNet SetupManager и др.

### ASCII (американски стандартен код за обмен на информация)

Една от стандартните кодировки на символи. Дефинирани са 128 символа, включително букви (a-z, A-Z), арабски цифри (0-9), символи, празни символи и контролни символи. Когато в това ръководство се описва ASCII, това означава 0x20 – 0x7E (шестнадесетично число), описано по-долу, и не включва контролните символи.

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

\* Символ за интервал.

### Unicode (UTF-8)

Международна стандартна кодировка, която покрива главните световни езици. Когато в това ръководство се описва UTF-8, това означава кодиране на символи в UTF-8 формат.

---

# Подготовка

---

Тази глава обяснява какво трябва да подготвите, преди да конфигурирате настройки.

## Поток на настройките на принтера

Трябва да конфигурирате мрежовите настройки и да извършите първоначална настройка, така че принтерът да стане достъпен за потребителите.

**1**

Подготовка

- Събиране на информация за настройка на връзката
- Решение за начин на свързване

**2**

Свързване

- Конфигурирайте мрежова връзка с помощта на EpsonNet Config

**3**

Настройка за печат

- Настройка на драйвера на принтера

**4**

Настройки за защита

- Настройки на администратора
- SSL/TLS
- Управление на протоколи
- IPsec/IP филтриране

### Още по темата

- ➔ [“Свързване” на страница 14](#)
- ➔ [“Настройки на функции” на страница 20](#)
- ➔ [“Настройки за защита” на страница 28](#)

---

## Въведение в свързването на принтера

Следните два начина са налични за свързване на принтера към мрежата директно и чрез двата начина.

- Връзка сървър/клиент (споделяне на принтера с Windows сървър)
- Връзка „Peer to peer“ (директен печат)

### Още по темата

- ➔ [“Настройки на връзка сървър/клиент” на страница 11](#)
- ➔ [“Настройки на връзка тип „Peer to Peer“” на страница 11](#)

## Подготовка

---

### Настройки на връзка сървър/клиент

#### Начин на свързване:

Свържете принтера към мрежа с помощта на концентратор (L2 комутатор). Можете също да свържете принтера директно към сървъра с USB кабел.

#### Драйвер на принтера:

Инсталирайте драйвера на принтера на Windows сървър в зависимост от операционната система на клиентските компютри. Чрез достъп до Windows сървър и свързване на принтера драйверът на принтера се инсталира на клиентския компютър и може да се използва.

#### Функции:

- Управление на принтер и на драйвер на принтер в партида.
- В зависимост от спецификациите на сървъра може да отнеме време стартирането на заданието за печат, защото всички задания за печат минават през сървъра за печат.
- Не можете да печатате, когато Windows сървърът е изключен.

#### Още по темата

➔ [“Дефиниции на термините, използвани в това ръководство” на страница 8](#)

---

### Настройки на връзка тип „Peer to Peer“

#### Начин на свързване:

Свържете принтера към мрежа с помощта на концентратор (L2 комутатор).

#### Драйвер на принтера:

Инсталирайте драйвера на принтера на всеки клиентски компютър. Той може да се разположи като пакет чрез EpsonNet SetupManager или автоматично чрез груповите правила на сървъра на Windows.

#### Функции:

- Заданието за печат стартира незабавно, защото е изпратено директно към принтера.
- Можете да печатате, докато принтерът работи.

#### Още по темата

➔ [“Дефиниции на термините, използвани в това ръководство” на страница 8](#)

---

## Подготовка за свързване към мрежата

---

### Събиране на информация в настройката за свързване

Трябва да имате IP адрес, адрес на шлюз и др. за мрежова връзка. Проверете следните предварително.

## Подготовка

Раздели	Елементи	Забележка
Начин на свързване на устройство	<input type="checkbox"/> Ethernet	Използвайте STP кабел (с екранирана усукана двойка) от категория 5e или по-висока.
Информация за LAN връзка	<input type="checkbox"/> IP адрес <input type="checkbox"/> Подмрежова маска <input type="checkbox"/> Шлюз по подразбиране	Ако настроите автоматично IP адреса с DHCP функцията на маршрутизатора, това не се изисква.
Информация за DNS сървър	<input type="checkbox"/> IP адрес за първичен DNS <input type="checkbox"/> IP адрес за вторичен DNS	Ако използвате статичен IP адрес като IP адрес, конфигурирайте DNS сървъра.  Конфигурирайте, когато назначавате IP адреси автоматично чрез функцията DHCP и когато DNS сървърът не може да се назначи автоматично.

## Спецификации на принтера

За спецификациите, които принтерът поддържа стандартно или в режим на свързване, вижте *Ръководство на потребителя*.

## Тип назначаване на IP адрес

Има два вида назначаване на IP адрес на принтера.

### Статичен IP адрес:

Задаване на предварително определен уникален IP адрес на принтера.

IP адресът не се променя, дори при включване на принтера или изключване на маршрутизатора, така че да можете да управлявате устройството по IP адрес.

Този тип е подходящ за мрежи, в които се управляват много принтери, например големи офиси или училища.

### Автоматично присвояване с DHCP функция:

Правилният IP адрес се присвоява автоматично, когато комуникацията между принтера и маршрутизатора, който поддържа DHCP функция, е успешна.

Ако не е удобно да се сменя IP адресът за конкретно устройство, запазете IP адрес предварително и след това го присвоете.

#### **Забележка:**

*За порта за опашката за печат изберете протокол, който може автоматично да определи IP адреса, например EpsonNet Print Port.*

## Метод за настройка на мрежова връзка

За настройка на IP адреса на принтера, подмрежова маска и шлюз по подразбиране процедирайте както следва.

## Подготовка

### Използване на EpsonNet Config:

Използвайте EpsonNet Config от компютъра на администратора. Можете да настроите много принтери, но те трябва да са физически свързани с Ethernet кабел преди настройката. Ако можете да създадете Ethernet връзката за настройката, зададете мрежови настройки за принтера, след което свържете принтера към обикновена мрежа, можете да сведете до минимум риска за защитата.

### Използване на програма за инсталиране:

Ако се използва програма за инсталиране, мрежата на принтера и клиентският компютър се настройват автоматично. Настройката е възможна чрез следване на инструкциите на програмата за инсталиране дори ако нямате сериозни познания за мрежата. Това се препоръчва при настройване на принтера и няколко клиентски компютъра чрез връзка сървър/клиент (споделяне на принтера чрез сървър на Windows).

### Още по темата

- ➔ [“Назначаване на IP адрес чрез EpsonNet Config” на страница 14](#)
- ➔ [“Свързване към мрежата с използване на програмата за инсталиране” на страница 18](#)

---

## Инсталиране на EpsonNet Config

Изтеглете EpsonNet Config от уеб сайта за поддръжка на Epson и след това го инсталирайте, като следвате инструкциите на екрана.

---

## Изпълнение на EpsonNet Config

Изберете **All Programs (Всички програми) > EpsonNet > EpsonNet Config SE > EpsonNet Config**.

**Забележка:**

Ако се появи предупреждение на защитната стена, разрешете достъпа за EpsonNet Config.

---

# Свързване

---

Тази глава описва средата или процедурата за свързване на принтера към мрежата.

## Свързване към мрежата

---

### Свързване към LAN

Свържете принтера към мрежата с помощта на Ethernet.



Още по темата

➔ [“Свързване към мрежата с използване на програмата за инсталиране” на страница 18](#)

---

### Назначаване на IP адрес чрез EpsonNet Config

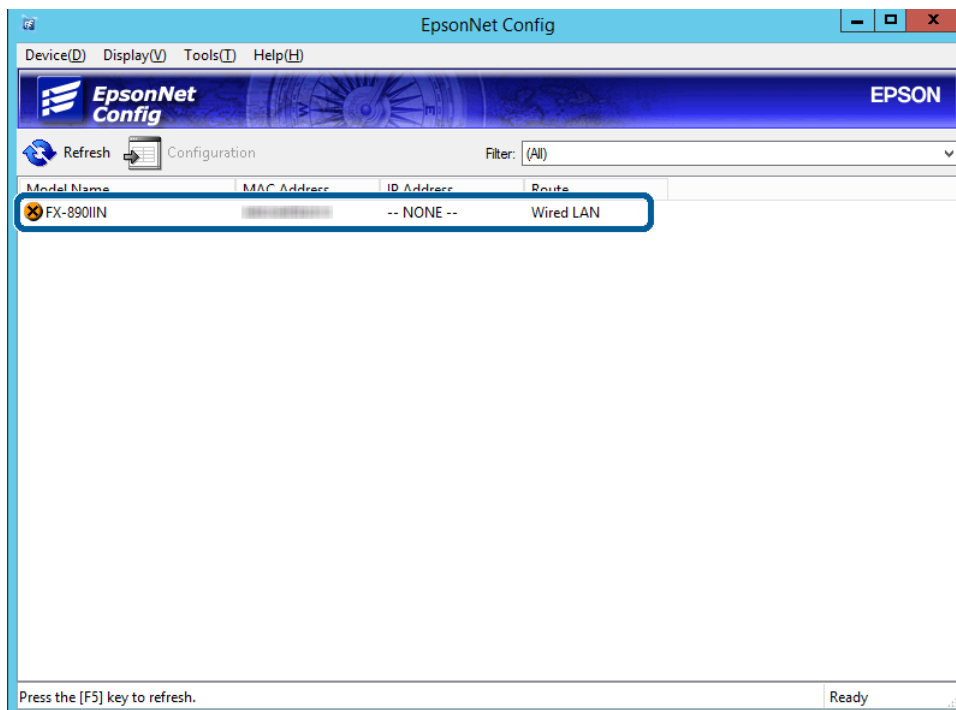
Назначаване на IP адрес за принтера чрез EpsonNet Config.

- 1 Включете принтера.
- 2 Свържете принтера към мрежата с помощта на Ethernet кабел.
- 3 Стартирайте EpsonNet Config.  
Показва се списък с принтери в мрежата. Може да отнеме известно време, преди да се покажат.
- 4 Щракнете двукратно върху  принтера, на който искате да назначавате.  
Ако свържете принтера към мрежа с налична функция DHCP, IP адресът е назначен с помощта на функцията DHCP, след което се показва .

**Забележка:**

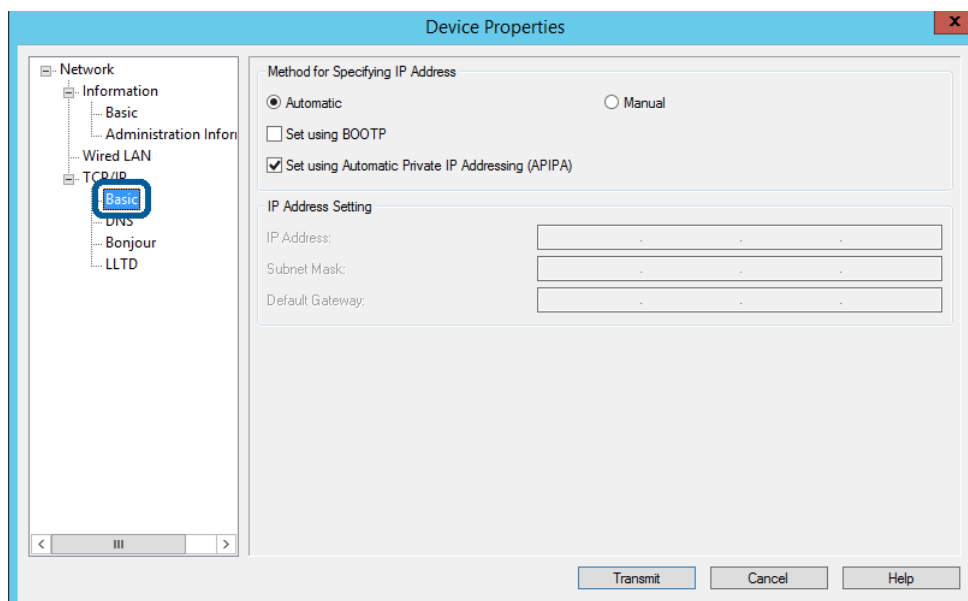
- Ако сте свързали няколко принтера от един и същ модел, можете да идентифицирате принтера по MAC адрес.
- След като принтерът е свързан към мрежата, можете да промените начина за назначаване на IP адреса.

## Свързване



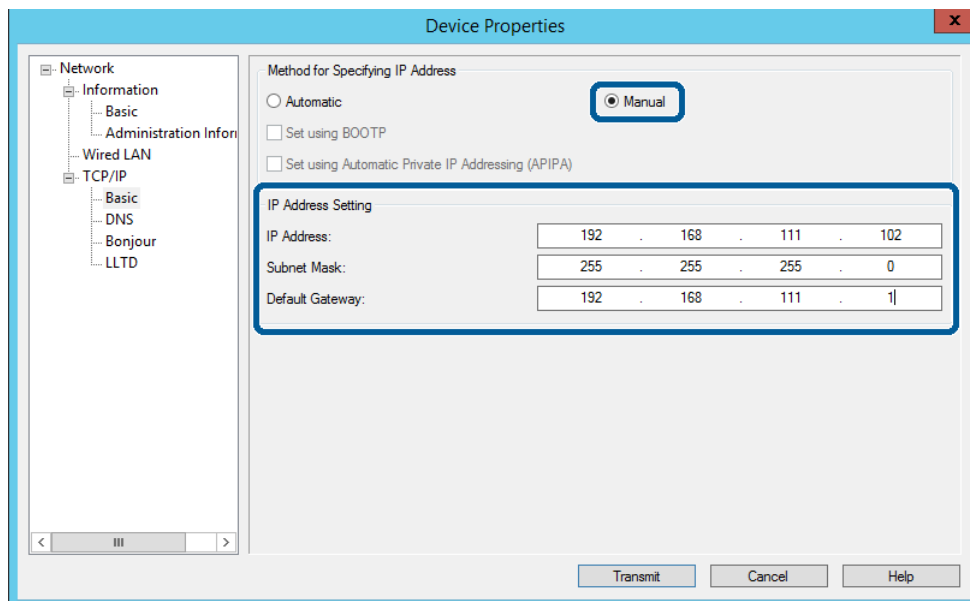
5

Изберете **Network (Мрежа) > TCP/IP > Basic (Основни)**.



## Свързване

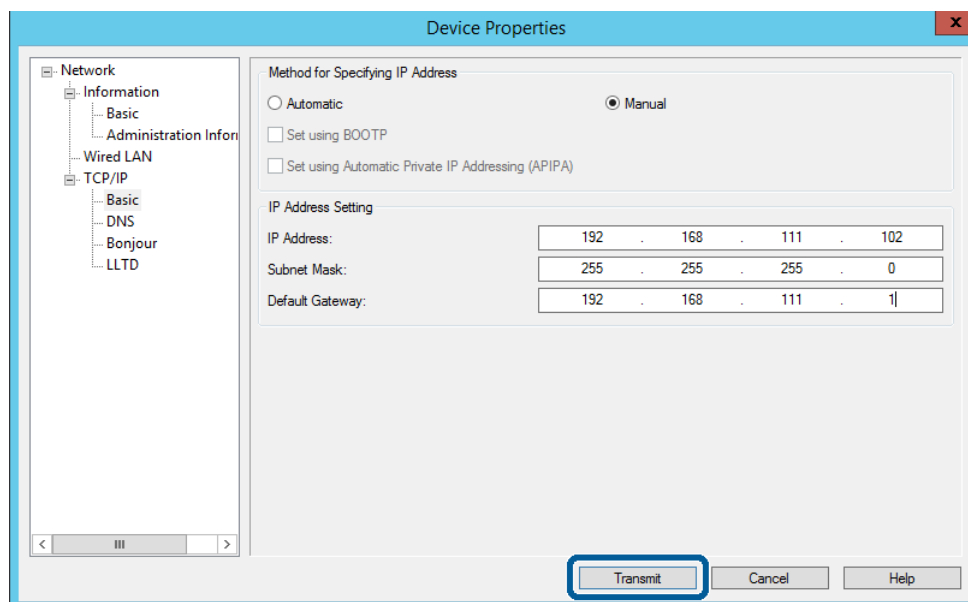
- 6** Въведете адреси за **IP Address (IP адрес)**, **Subnet Mask (Подмрежова маска)** и **Default Gateway (Шлюз по подразбиране)**.



**Забележка:**

- Въведете статичен адрес, когато свързвате принтера към защитена мрежа.
- В менюто **TCP/IP** можете да зададете настройките за **DNS** на екрана **DNS**.

- 7** Щракнете върху **Transmit (Предаване)**.

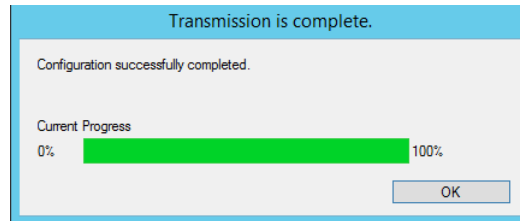


- 8** Щракнете върху **OK** на екрана за потвърждение.

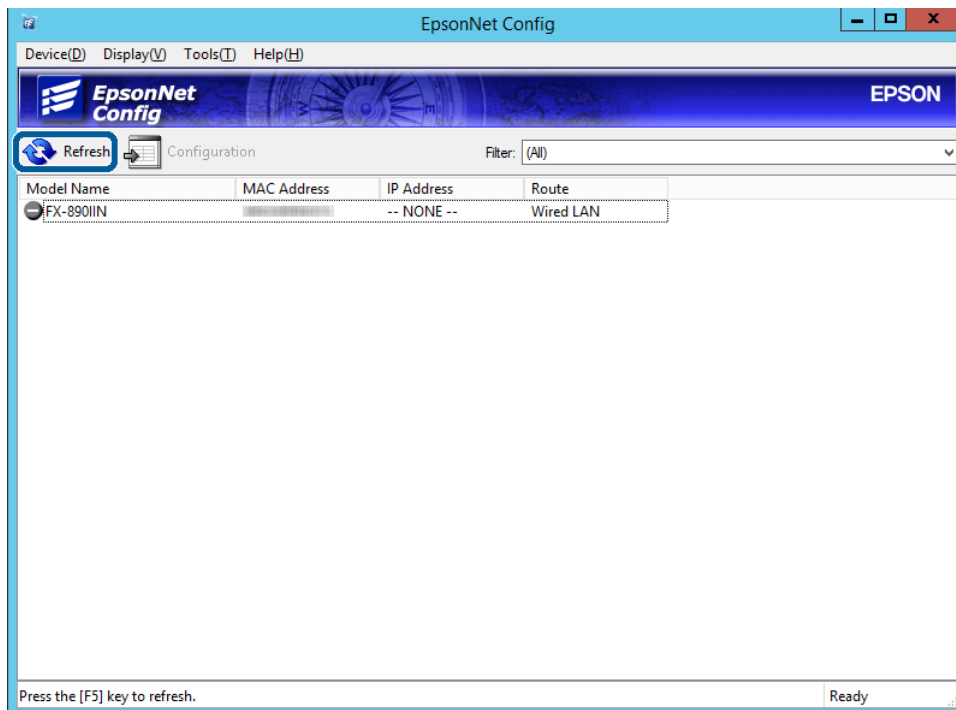


**Свързване**

**9** Щракнете върху **ОК**.

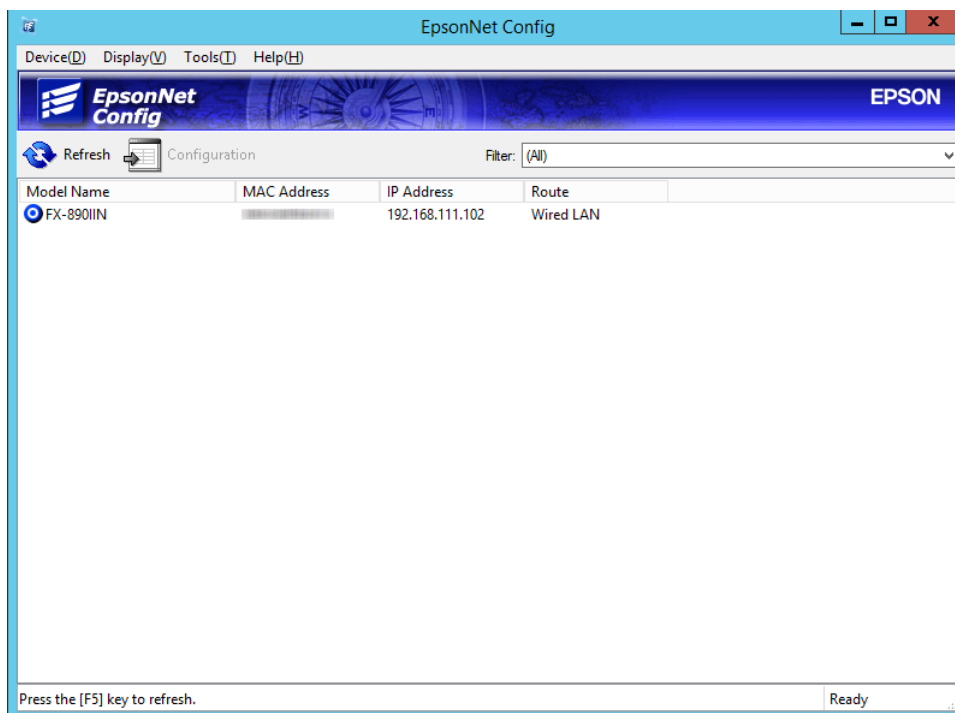


**10** Щракнете върху **Refresh (Обновяване)**.



## Свързване

Проверете дали е назначен IP адрес.



---

## Свързване към мрежата с използване на програмата за инсталиране

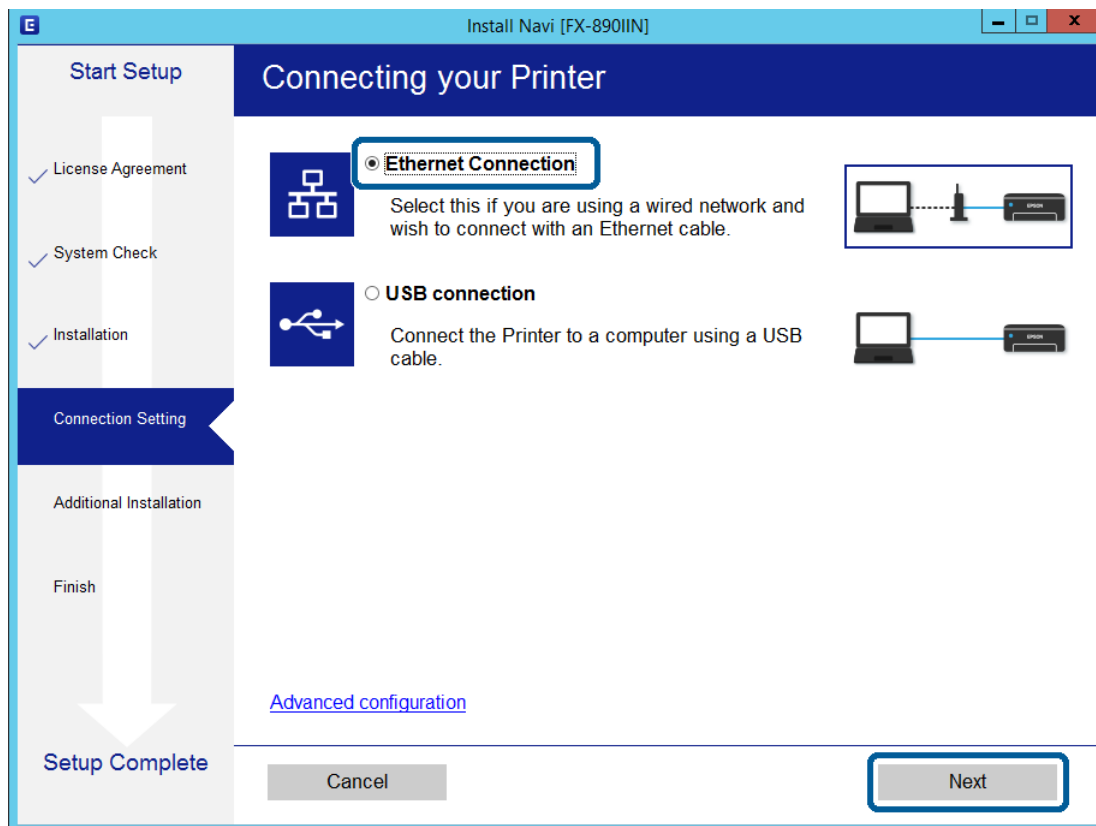
Препоръчваме Ви да използвате програмата за инсталиране за свързване на принтера към компютър.

1

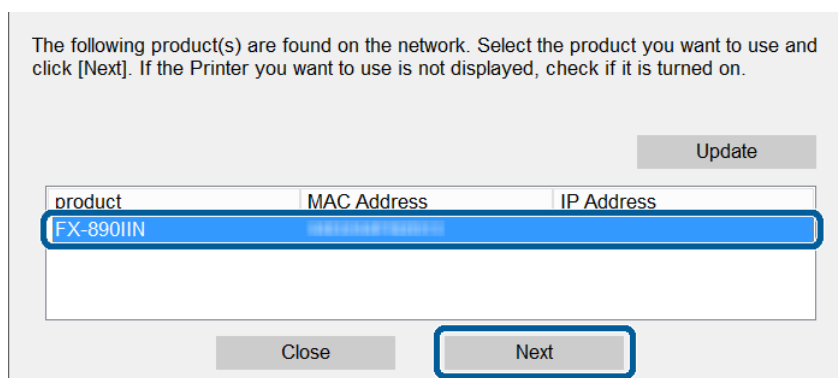
Поставете диска със софтуер в компютъра, след което следвайте инструкциите на екрана.

## Свързване

- 2** Следвайте инструкциите на екрана, докато не се покаже следният екран. Изберете **Ethernet Connection (Ethernet връзка)**, след което изберете **Next (Следващ)**.



Ако сте свързали принтера към мрежата с помощта на Ethernet кабел, ще бъде показан следният екран. Изберете принтера, след което щракнете върху **Next (Следващ)**.



- 3** Следвайте инструкциите на екрана.

---

# Настройки на функции

---

Тази глава описва как да направите първите настройки за използване на всяка функция в устройството.

В тази тема е обяснена процедурата за конфигуриране на настройки от компютъра на администратора чрез Web Config.

## Web Config (уеб страница за устройството)

---

### Относно Web Config

Web Config е базирано на браузър приложение за конфигуриране на настройките на принтера.

За достъп до Web Config трябва първо да имате назначен IP адрес на принтера.

**Забележка:**

Можете да заключите настройките чрез конфигуриране на администраторска парола за принтера.

---

### Достъп до Web Config

Има два начина за достъп до Web Config. JavaScript трябва да е разрешен в браузъра.

#### Въвеждане на IP адрес

Стартирайте EpsonNet Config, след което щракнете двукратно върху принтера в списъка.

Въведете IP адреса на принтера в уеб браузър. При достъп до Web Config чрез HTTPS в браузъра ще се появи предупредително съобщение, тъй като се използва самоподписан сертификат, запазен в принтера.

- Достъп чрез HTTPS  
IPv4: `https://<IP адрес на принтера> (без < >)`  
IPv6: `https://[IP адрес на принтера]/ (с [ ])`
- Достъп чрез HTTP  
IPv4: `http://<IP адрес на принтера> (без < >)`  
IPv6: `http://[IP адрес на принтера]/ (с [ ])`

## Настройки на функции

### Забележка:

- Примери*  
IPv4:  
*https://192.0.2.111/*  
*http://192.0.2.111/*  
IPv6:  
*https://[2001:db8::1000:1]/*  
*http://[2001:db8::1000:1]/*
- Ако името на принтера е регистрирано в DNS сървъра, можете да използвате името на принтера вместо IP адреса на принтера.*
- Не всички менюта се показват при достъп до Web Config чрез HTTP. За да видите всички менюта, влезте в Web Config чрез HTTPS.*

### Още по темата

- ➔ [“SSL/TLS комуникация с принтера” на страница 34](#)
- ➔ [“Относно цифрово сертифициране” на страница 35](#)

## Използване на функции за печат

Разрешаване на използване на функция за печат.

---

### Изисквания за печат по мрежа

За печат по мрежата се изисква следното. Можете да конфигурирате тези настройки, като използвате драйвера на принтера и функциите на операционната система.

- Инсталиране на драйвера на принтера
- Създаване на опашка за печат на компютър
- Настройка на порт за мрежа

---

### Настройка на драйвер на принтер с използване на връзка клиент/сървър

Настройте принтера да позволява печат от компютър, който преди това е бил настроен като сървър за печат, и споделете принтера. Инсталирайте драйвера на принтера за сървъра и за клиента на сървъра за печат. Ако се използва програма за инсталиране, настройката на мрежата на принтера или на компютъра, инсталацията на драйвера и опашката за печат се създават автоматично.

### Настройка на стандартни TCP/IP портове – Windows

Настройка на стандартен TCP/IP порт на сървъра за печат и създаване на опашка за печат за мрежов печат.

## Настройки на функции

1

Отворете екрана Devices and Printers (Устройства и принтери).

- Windows 10/Windows Server 2016  
Щракнете с десния бутон върху бутона Start (Старт) или го натиснете и задръжте, след което изберете **Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук) > Devices and Printers (Устройства и принтери)**.
- Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012  
**Desktop (Работен плот) > Settings (Настройки) > Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук)** или **Hardware (Хардуер) > Devices and Printers (Устройства и принтери)**.
- Windows 7/Windows Server 2008 R2  
Щракнете върху Start (Старт) > **Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук)** (или **Hardware (Хардуер)**) > **Devices and Printers (Устройства и принтери)**.
- Windows Vista/Windows Server 2008  
Щракнете върху Start (Старт) > **Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук) > Printers (Принтери)**.
- Windows XP/Windows Server 2003 R2/Windows Server 2003  
Щракнете върху Start (Старт) > **Control Panel (Контролен панел) > Printers and Other Hardware (Принтери и друг хардуер) > Printers and Faxes (Принтери и факсове)**.

2

Добавяне на принтер.

- Windows 10/Windows 8.1/Windows 8/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012  
Щракнете върху **Add printer (Добавяне на принтер)**, след това изберете **The printer that I want isn't listed (Гърсеният принтер не е в списъка)**.
- Windows 7/Windows Server 2008 R2  
Щракнете върху **Add printer (Добавяне на принтер)**.
- Windows Vista/Windows Server 2008  
Щракнете върху **Install Printer (Инсталиране на принтер)**.
- Windows XP/Windows Server 2003 R2/Windows Server 2003  
Щракнете върху **Install Printer (Инсталиране на принтер)**, след това щракнете върху **Next (Напред)**.

3

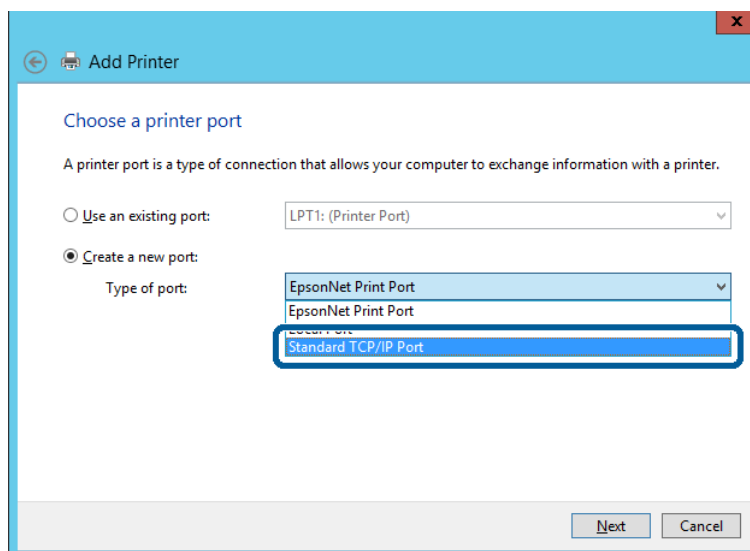
Добавяне на локален принтер.

- Windows 10/Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012  
Изберете **Add a local printer or network printer with manual settings (Добавяне на локален принтер или мрежов принтер с ръчни настройки)**, след това щракнете върху **Next (Напред)**.
- Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008  
Щракнете върху **Add a local printer (Добавяне на локален принтер)**.
- Windows XP/Windows Server 2003 R2/Windows Server 2003  
Изберете **Local printer attached to this computer (Свързан към този компютър локален принтер)**, след това щракнете върху **Next (Напред)**.

## Настройки на функции

- 4** Изберете **Create a new port (Създай нов порт)**, изберете **Standard TCP/IP Port (Стандартен TCP/IP порт)** като Port Type (Тип порт), след което щракнете върху **Next (Напред)**.

За Windows XP/Windows Server 2003 R2/Windows Server 2003 щракнете върху **Next (Напред)** на екрана **Add Standard TCP/IP Printer Port Wizard (Съветник за добавяне на стандартен TCP/IP порт за принтер)**.

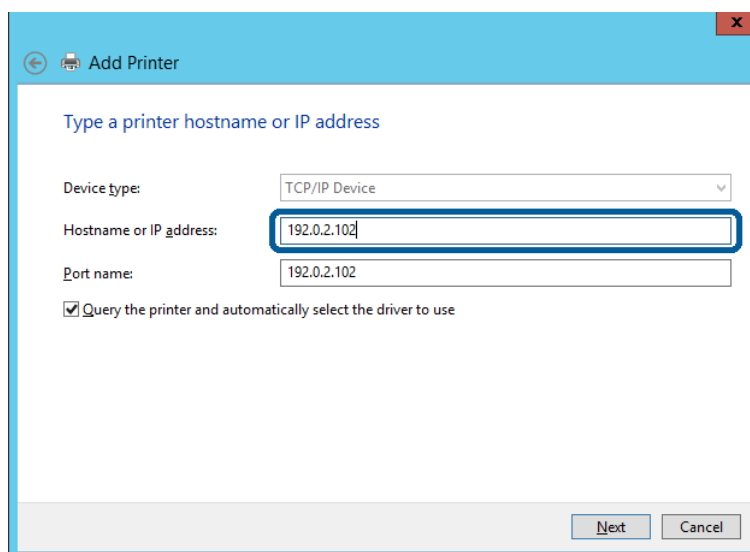


- 5** Въведете IP адреса на принтера или името на принтера в **Host Name or IP Address (Име на хост или IP адрес)** или **Printer Name or IP Address (Име или IP адрес на принтера)**, след това щракнете върху **Next (Напред)**.

Не променяйте **Port name (Име на порт)**.

Щракнете върху **Continue (Продължаване)**, когато се появи екранът **User Account Control (Управление на потребителските акаунти)**.

За Windows XP/Windows Server 2003 R2/Windows Server 2003 щракнете върху **Done (Готово)** на екрана **Standard TCP/IP Printer Port (Добавяне на стандартен TCP/IP порт за принтер)**.



## Настройки на функции

### Забележка:

Ако зададете името на принтера в мрежа, където има преобразуване на име, IP адресът се проследява дори ако IP адресът на принтера е променен от DHCP. Можете да проверите името на принтера от екрана за състоянието на мрежата в контролния панел на принтера или в листа за състоянието на мрежата.

6

Конфигурирайте драйвера за принтера.

- Ако драйверът за принтера вече е инсталиран:  
Изберете **Manufacturer (Производител)** и **Printers (Принтери)**. Щракнете върху **Next (Напред)**.
- Ако драйверът за принтера не е инсталиран:  
Щракнете върху **Have Disc (Наличен е диск)** и поставете доставения при покупката на принтера диск със софтуер. Щракнете върху **Browse (Преглед)**, след което изберете папката на диска, където се намира драйверът за принтера. Уверете се, че сте избрали правилната папка. Местоположението на папката може да е различно в зависимост от операционната система.  
32-битова версия на Windows: WINX86  
64-битова версия на Windows: WINX64

7

Следвайте инструкциите на екрана.

За Windows XP/Windows Server 2003 R2/Windows Server 2003 настройката завърши. За Windows Vista/Windows Server 2008 и по-нови версии проверете конфигурацията на порта.

Когато използвате принтера във връзка сървър/клиент (споделяне на принтера чрез Windows сървър), направете следните настройки за споделяне.

### Още по темата

➔ [“Споделяне на принтера” на страница 25](#)

## Проверка на конфигурацията на порта — Windows

Проверете дали е настроен правилният порт за опашката на за печат.

1

Отворете екрана Devices and Printers (Устройства и принтери).

- Windows 10/Windows Server 2016  
Щракнете с десния бутон върху бутона Start (Старт) или го натиснете и задръжте, след което изберете **Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук) > Devices and Printers (Устройства и принтери)**.
- Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012  
**Desktop (Работен плот) > Settings (Настройки) > Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук)** или **Hardware (Хардуер) > Devices and Printers (Устройства и принтери)**.
- Windows 7/Windows Server 2008 R2  
Щракнете върху Start (Старт) > **Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук)** (или **Hardware (Хардуер) > Devices and Printers (Устройства и принтери)**).
- Windows Vista/Windows Server 2008  
Щракнете върху Start (Старт) > **Control Panel (Контролен панел) > Hardware and Sound (Хардуер и звук) > Printers (Принтери)**.



## Настройки на функции

2

Отворете екрана със свойствата на принтера.

- Windows 10/Windows 8.1/Windows 8/Windows 7/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012/Windows Server 2008 R2

Щракнете с десния бутон на мишката върху иконата на принтера, след което щракнете върху **Printer properties (Свойства на принтера)**.

- Windows Vista  
Щракнете с десния бутон на мишката върху иконата на принтера, след което изберете **Run as administrator (Изпълнявай като администратор) > Properties (Свойства)**.

- Windows Server 2008  
Щракнете с десния бутон на мишката върху иконата на принтера, след което щракнете върху **Properties (Свойства)**.

3

Щракнете върху раздел **Ports (Портове)**, изберете **Standard TCP/IP Port (Стандартен TCP/IP порт)**, след това щракнете върху **Configure Port (Конфигуриране на порт)**.

4

Проверете конфигурацията на порта.

- За RAW

Проверете дали **Raw** е избрано в **Protocol (Протокол)**, след което щракнете върху **ОК**.

- За LPR

Проверете дали **LPR** е избрано в **Protocol (Протокол)**. Въведете "PASSTHRU" в **Queue name (Име на опашката)** от **LPR Settings (LPR настройки)**. Изберете **LPR Byte Counting Enabled (Разрешено броенето на байтове по LPR)**, след това щракнете върху **ОК**.

## Споделяне на принтера

Когато използвате принтера във връзка сървър/клиент (споделяне на принтера чрез Windows сървър), настройте споделянето на принтера от сървъра за печат.

1

Изберете **Control Panel (Контролен панел) > View devices and printers (Преглед на устройства и принтери)** на сървъра за печат.

2

Щракнете с десния бутон върху иконата на принтера (опашката за печат), с който искате да споделяте, след което щракнете върху **Printer Properties (Свойства на принтера) > раздел Sharing (Споделяне)**.

3

Изберете **Share this printer (Сподели този принтер)** и след това въведете в **Share name (Сподели име)**.

За Windows Server 2012 щракнете върху **Change Sharing Options (Промяна на опциите за споделяне)**, след което конфигурирайте настройките.

## Инсталиране на допълнителни драйвери

Ако версиите на Windows за сървър и клиент са различни, е препоръчително да инсталирате допълнителни драйвери на сървъра за печат.

1

Изберете **Control Panel (Контролен панел) > View devices and printers (Преглед на устройства и принтери)** на сървъра за печат.

## Настройки на функции

- 2 Щракнете с десния бутон върху иконата на принтера, който искате да споделите с клиентите, след което щракнете върху **Printer Properties (Свойства на принтера)** > раздел **Sharing (Споделяне)**.
- 3 Щракнете върху **Additional Drivers (Допълнителни драйвери)**.  
За Windows Server 2012 щракнете върху **Change Sharing Options (Промяна на опциите за споделяне)**, след което конфигурирайте настройките.
- 4 Изберете версии на Windows за клиентите и след това щракнете върху **ОК**.
- 5 Изберете информационен файл за драйвера на принтера (\*.inf) и инсталирайте драйвера.

### Още по темата

➔ [“Използване на споделения принтер” на страница 26](#)

## Използване на споделения принтер

Администраторът трябва да информира клиентите за името на компютъра, зададено на сървъра за печат, и как да го добавят към своите компютри. Ако все още няма конфигуриран(и) допълнителен(ни) драйвер(и), информирайте клиентите как да използват **Devices and Printers (Устройства и принтери)**, за да добавят споделения принтер.

Ако вече има конфигуриран(и) допълнителен(ни) драйвер(и) на сървъра за печат, следвайте тези стъпки:

- 1 Изберете името, зададено на сървъра за печат, в **Windows Explorer**.
- 2 Щракнете двукратно върху принтера, който искате да използвате.

### Още по темата

- ➔ [“Споделяне на принтера” на страница 25](#)
- ➔ [“Инсталиране на допълнителни драйвери” на страница 25](#)

---

## Настройки на драйвера на принтера за връзка тип „Peer to Peer“

За връзка тип „Peer to Peer“ (директен печат) драйверът на принтера трябва да е инсталиран на всеки клиентски компютър.

### Още по темата

➔ [“Настройка на драйвера на принтера” на страница 26](#)

## Настройка на драйвера на принтера

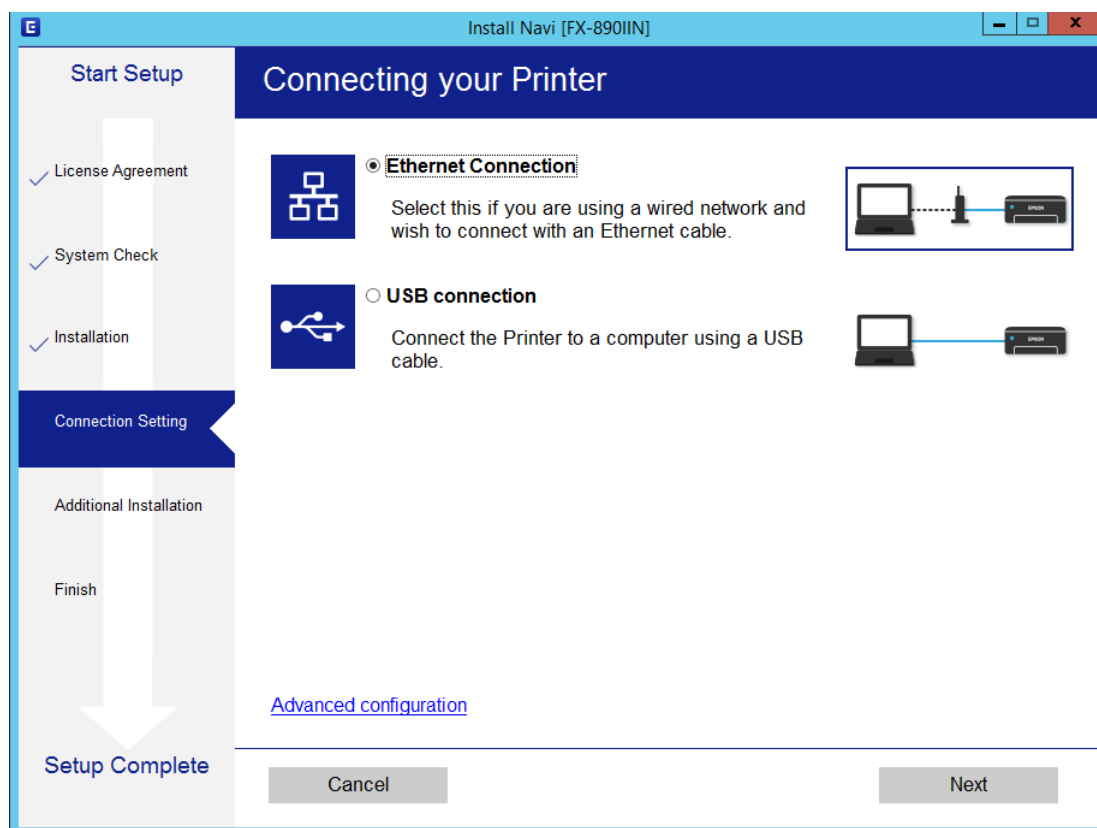
За малки организации препоръчваме инсталиране на драйвера на принтера на всеки клиентски компютър.

### **Забележка:**

Когато принтерът се използва от много клиентски компютри, като използвате *EpsonNet SetupManager* и разположите драйвера като пакет, времето за инсталиране може да се намали драстично.

## Настройки на функции

- 1 Стартирайте програмата за инсталиране.
- 2 Изберете начин на свързване за принтера и щракнете върху **Next (Следващ)**.



**Забележка:**

Ако е показан **Select Software Installation (Изберете софтуер за инсталиране)**, изберете **Change or re-set the connection method (Променете или възстановете метода на свързване)** и след това щракнете върху **Next (Следващ)**.

- 3 Следвайте инструкциите на екрана.

**Още по темата**

➔ [“EpsonNet SetupManager” на страница 63](#)

## Настройки за защита

# Настройки за защита

Тази глава обяснява настройките за защита.

## Настройки за защита и предпазване от опасност

Когато устройството е свързано към мрежата, имате достъп до него от отдалечено местоположение. Освен това, много хора могат да споделят устройството, което е удобно и подобрява оперативната ефективност. Но рисковете за неупълномощен достъп, използване и подправяне на данните се увеличават.

За да се избегне тази опасност, принтерите на Epson имат множество технологии за защита. Настройте устройството според необходимостта и условията на средата, която е изградена с информация за средата на клиента.

Име на функция	Тип функция	Какво да се настрои	Какво да се предотврати
Настройка на администраторска парола	Заклучва системните настройки, като например настройка за свързване за мрежа или USB.	Администраторът задава парола на устройството. Конфигурация или актуализация са налични навсякъде от Web Config и Epson Device Admin.	Предпазва от неупълномощено прочитане и промяна на информацията, записана в устройството, например ИД, парола, мрежови настройки и контакти. Освен това намалява много рискове за защитата, например изтичане на информация за мрежовата среда или правила за защита.
Протокол и управление на услугата	Управява протоколите и услугите, които ще се използват за комуникация между устройства и компютри, и разрешава и забранява функции, като например печат.	Протокол или услуга, която се прилага към функции, разрешени или забранени поотделно.	Намалява рисковете за сигурността, които могат да възникнат при инцидентно използване, като предпазва потребителите от използване на функции, които не са необходими.
SSL/TLS комуникации	Пътят на комуникацията между принтера и компютъра е криптиран с SSL/TLS комуникация. Съдържанието на комуникацията е защитено от настройки на принтера и печат с IPPS протокол през браузър.	Получаване на подписан от сертифициращ орган сертификат и импортиране на принтера.	Установяването на идентификацията на устройството с подписан от сертифициращ орган сертификат предотвратява подмяна на самоличност и неупълномощен достъп. Освен това, комуникационното съдържание на SSL/TLS е защитено и предпазва от изтичане на съдържанието на отпечатаните данни и информацията за настройката.

## Настройки за защита

Име на функция	Тип функция	Какво да се настрои	Какво да се предотврати
IPsec/IP филтриране	Можете да настроите разделяне и прекъсване на данните от определен клиент или от конкретен вид. Тъй като IPsec защитава данните по IP пакет (кодиране и удостоверяване), можете безопасно да споделяте необезопасен протокол за печат и сканиране.	Създаване на базова политика и индивидуална политика, за да настроите клиента или типа данни, които имат право на достъп до устройството.	Защита от неупълномощен достъп, подправяне и прехващане на комуникационните данни към устройството.
SNMPv3	Добавени са функции, например следене на свързаните устройства в мрежата, цялост на данните към SNMP протокола за управление, шифроване, удостоверяване на потребителите и др.	Разрешаване на SNMPv3, последвано от задаване на начин за удостоверяване и шифроване.	Осигуряване на промяна на настройките по мрежата и поверителност при следене на състоянието.

### Още по темата

- ➔ [“Конфигуриране на администраторска парола” на страница 29](#)
- ➔ [“Управляващи протоколи и услуги” на страница 30](#)
- ➔ [“SSL/TLS комуникация с принтера” на страница 34](#)

---

## Настройки на функциите за защита

Когато настройвате IPsec/IP филтриране, е препоръчително да отворите Web Config, като използвате SSL/TLS за споделяне на информацията за настройките, за да намалите опасността от подправяне или прихващане на данните.

## Конфигуриране на администраторска парола

Когато зададете администраторска парола, потребителите, които не са администратори, няма да могат да променят настройките за системно администриране. Можете да зададете и промените администраторската парола чрез Web Config.

### Още по темата

- ➔ [“Конфигуриране на администраторска парола чрез Web Config” на страница 29](#)

---

## Конфигуриране на администраторска парола чрез Web Config

Можете да зададете администраторската парола чрез Web Config.

- 1 Отворете Web Config и изберете **Administrator Settings (Администраторски настройки) > Change Administrator Password (Промяна на администраторската парола)**.

## Настройки за защита

- Въведете парола в **New Password (Нова парола)** и **Confirm New Password (Потвърждаване на нова парола)**.

Ако искате да смените паролата с нова, въведете текущата парола.

- Изберете **ОК**.

### Забележка:

- За да настроите или промените заключените елементи в менюто, щракнете върху **Administrator Login (Вход за администратори)**, след което въведете администраторската парола.
- За да изтриете администраторската парола, щракнете върху **Administrator Settings (Настройки на администратора) > Delete Administrator Authentication Information (Изтриване на информация за удостоверяване на администратор)** и след това въведете администраторската парола.

### Още по темата

➔ “Достъп до Web Config” на страница 20

## Управляващи протоколи и услуги

Можете да печатате като използвате разнообразни пътища и протоколи. Можете да намалите случайните рискове за сигурността като ограничите печата от определени пътища или чрез управление на достъпните функции.

### Управляващи протоколи

Конфигурирайте настройките на протоколите.

- Влезте в Web Config и изберете **Services (Услуги) > Protocol (Протокол)**.
- Конфигурирайте всеки елемент.
- Щракнете върху **Next (Напред)**.

## Настройки за защита

4

Щракнете върху **ОК**.

Настройките се прилагат за принтера.

### Още по темата

- ➔ [“Достъп до Web Config” на страница 20](#)
- ➔ [“Протоколи, които можете да разрешите или забраните” на страница 31](#)
- ➔ [“Елементи за настройка на протоколи” на страница 32](#)

## Протоколи, които можете да разрешите или забраните

Протокол	Описание
Bonjour Settings (Настройки на Bonjour)	Можете да посочите дали да се използва Bonjour. Bonjour се използва за търсене на устройства, печат (AirPrint) и др.
SLP Settings (SLP настройки)	Можете да разрешите или забраните функцията SLP. SLP се използва за търсене на мрежа в EpsonNet Config.
LLTD Settings (LLTD настройки)	Можете да разрешите или забраните функцията LLTD. Когато тя е разрешена, тя е видима в картата на мрежата Windows.
LLMNR Settings (LLMNR настройки)	Можете да разрешите или забраните функцията LLMNR. Когато функцията е разрешена, можете да използвате преобразуване на имена без NetBIOS, дори и да не можете да използвате DNS.
LPR Settings (LPR настройки)	Можете да посочите дали да е разрешен LPR печат. Когато функцията е разрешена, можете да печатате и сканирате от порта LPR.
RAW(Port9100) Settings (RAW (порт 9100)) настройки)	Можете да посочите дали да се разреши печат от порта RAW (порт 9100). Когато функцията е разрешена, можете да печатате и сканирате от порта RAW (порт 9100).
RAW(Custom Port) Settings (RAW(Custom Port) настройки)	Можете да посочите дали да се разреши печат от порта RAW (потребителски порт). Когато функцията е разрешена, можете да печатате и сканирате от порта RAW (потребителски порт).
IPP Settings (IPP настройки)	Можете да посочите дали да е разрешен печат от IPP. Когато функцията е разрешена, можете да печатате през интернет (включително AirPrint).
FTP Settings (FTP настройки)	Можете да посочите дали да е разрешен FTP печат. Когато функцията е разрешена, можете да печатате чрез FTP сървър.
SNMPv1/v2c Settings (SNMPv1/v2c настройки)	Можете да посочите дали да се разреши SNMPv1/v2c. Тази опция се използва за настройка на устройства, мониторинг и други.
SNMPv3 Settings (SNMPv3 настройки)	Можете да посочите дали да се разреши SNMPv3. Тази опция се използва за настройка на криптирани устройства, следене и други.

### Още по темата

- ➔ [“Управляващи протоколи” на страница 30](#)
- ➔ [“Елементи за настройка на протоколи” на страница 32](#)

## Настройки за защита

## Елементи за настройка на протоколи

**EPSON** **FX-890IIN**

Administrator Logout  
 Status  
[Product Status](#)  
[Network Status](#)  
 Network Settings  
 Network Security Settings  
 Services  
[Protocol](#)  
 Administrator Settings

Services > Protocol

Note: If you need to change the Device Name used on each protocol and the Bonjour Name, change the Device Name in the Network Settings.  
 If you need to change the Location used on each protocol, change it in the Network Settings.

Bonjour Settings

Use Bonjour

Bonjour Name : EPSON [REDACTED].local

Bonjour Service Name : EPSON FX-890IIN

Location :

Top Priority Protocol : IPP

SLP Settings

Enable SLP

LLTD Settings

Enable LLTD

Device Name : EPSON [REDACTED]

LLMNR Settings

Enable LLMNR

LPR Settings

Allow LPR Port Printing

Printing Timeout (sec) : 300

RAW(Port9100) Settings

Елементи	Стойност на настройка и описание
Bonjour Settings (Настройки на Bonjour)	
Use Bonjour (Използване на Bonjour)	Изберете тази опция за търсене или използване на устройства чрез Bonjour. Не можете да използвате AirPrint, ако опцията не е маркирана.
Bonjour Name (Име в Bonjour)	Показва името в Bonjour.
Bonjour Service Name (Име на услуга в Bonjour)	Показва името на услугата в Bonjour.
Location (Местоположение)	Показва името на местоположението в Bonjour.
Top Priority Protocol (Протокол с най-висок приоритет)	Изберете протокола с най-висок приоритет за печат чрез Bonjour.
SLP Settings (SLP настройки)	
Enable SLP (Разрешаване на SLP)	Изберете тази опция, за да разрешите функцията SLP. Тази функция се използва за търсене на мрежа в EpsonNet Config.
LLTD Settings (LLTD настройки)	
Enable LLTD (Разрешаване на LLTD)	Изберете тази опция за разрешаване на LLTD. Принтерът е показан в Windows карта на мрежата.
Device Name (Име на устройството)	Показва името на LLTD устройството.



## Настройки за защита

Елементи	Стойност на настройка и описание
LLMNR Settings (LLMNR настройки)	
Enable LLMNR (Разрешаване на LLMNR)	Изберете тази опция за разрешаване на LLMNR. Можете да използвате преобразуване на имена без NetBIOS, дори и да не можете да използвате DNS.
LPR Settings (LPR настройки)	
Allow LPR Port Printing (Разрешаване на печат от LPR порт)	Изберете, за да разрешите печат от LPR порта.
Printing Timeout (sec) (Време на изчакване за печат (в сек))	Въведете стойност за време на изчакване при LPR печат между 0 и 3600 секунди. Ако не желаете време за изчакване, въведете 0.
RAW(Port9100) Settings (RAW (порт 9100)) настройки	
Allow RAW(Port9100) Printing (Разрешаване на RAW (порт 9100) печат)	Изберете, за да разрешите печат от RAW порта (порт 9100).
Printing Timeout (sec) (Време на изчакване за печат (в сек))	Въведете стойност за изчакване за RAW (порт 9100) при печат между 0 и 3600 секунди. Ако не желаете време за изчакване, въведете 0.
RAW(Custom Port) Settings (RAW(Custom Port) настройки)	
Allow RAW(Custom Port) Printing (Разрешаване на RAW(Custom Port) печат)	Изберете, за да разрешите печат от RAW порта (потребителски порт).
Port Number (Номер на порт)	Въведете номера на порта за RAW (потребителски порт) печат между 1024 и 65535, с изключение на 9100, 1865 и 2968.
Printing Timeout (sec) (Време на изчакване за печат (в сек))	Въведете стойност за време на изчакване за RAW (потребителски порт) при печат между 0 и 3600 секунди. Ако не желаете време за изчакване, въведете 0.
IPP Settings (IPP настройки)	
Enable IPP (Разрешаване на IPP)	Изберете, за да разрешите IPP комуникацията. Показани са само принтери, които поддържат IPP. Не можете да използвате AirPrint, ако опцията е забранена.
Allow Non-secure Communication (Разрешаване на незащитена комуникация)	Изберете, за да разрешите на принтера да комуникира без мерки за защита (IPP).
Communication Timeout (sec) (Време на изчакване за комуникацията (в сек))	Въведете стойност за време на изчакване при IPP печат между 0 и 3600 секунди.
URL(Network (Мрежа))	Показва IPP URL адреси (http и https), когато принтерът е свързан чрез кабелна LAN мрежа. URL адресът е стойност, която представлява комбинация от IP адреса на принтера, номера на порта и IPP името на принтера.
Printer Name (Име на принтера)	Показва името на IPP принтера.
Location (Местоположение)	Показва IPP местоположението.
FTP Settings (FTP настройки)	
Enable FTP Server (Разрешаване на FTP сървър)	Изберете, за да разрешите FTP печат. Показани са само принтери, които поддържат FTP печат.
Communication Timeout (sec) (Време на изчакване за комуникацията (в сек))	Въведете стойност за време на изчакване при FTP комуникация между 0 и 3600 секунди. Ако не желаете време за изчакване, въведете 0.
SNMPv1/v2c Settings (SNMPv1/v2c настройки)	

## Настройки за защита

Елементи	Стойност на настройка и описание
Enable SNMPv1/v2c (Разрешаване на SNMPv1/v2c)	Изберете, за да разрешите SNMPv1/v2c. Показани са само принтери, които поддържат SNMPv3.
Access Authority (Контролен орган на достъпа)	Задайте контролен орган на достъпа, когато е разрешена опцията SNMPv1/v2c. Изберете <b>Read Only (Само за четене)</b> или <b>Read/Write (Четене/Писане)</b> .
Community Name (Read Only) (Име на общност (само за четене))	Въведете от 0 до 32 ASCII (0x20 до 0x7E) символа.
Community Name (Read/Write) (Име на общност (четене/писане))	Въведете от 0 до 32 ASCII (0x20 до 0x7E) символа.
SNMPv3 Settings (SNMPv3 настройки)	
Enable SNMPv3 (Разрешаване на SNMPv3)	SNMPv3 е разрешен, когато е поставена отметката.
User Name (Потребителско име)	Въведете между 1 и 32 знака с помощта на 1-байтови символи.
Authentication Settings (Настройки за удостоверяване)	
Algorithm (Алгоритъм)	Изберете алгоритъм за удостоверяване на SNMPv3.
Password (Парола)	Въведете парола за удостоверяване на SNMPv3. Въведете между 8 и 32 знака в ASCII (0x20–0x7E). Ако не укажете това, го оставете празно.
Confirm Password (Потвърждаване на паролата)	Въведете паролата, която сте конфигурирали, за потвърждение.
Encryption Settings (Настройки за шифроване)	
Algorithm (Алгоритъм)	Изберете алгоритъм за шифроване за SNMPv3.
Password (Парола)	Въведете паролата за шифроване за SNMPv3. Въведете между 8 и 32 знака в ASCII (0x20–0x7E). Ако не укажете това, го оставете празно.
Confirm Password (Потвърждаване на паролата)	Въведете паролата, която сте конфигурирали, за потвърждение.
Context Name (Име на контекста)	Въведете 32 символа или по-малко в Unicode (UTF-8). Ако не укажете това, го оставете празно. Броят на символите, които могат да бъдат въведени, зависи от езика.

### Още по темата

- ➔ [“Управляващи протоколи” на страница 30](#)
- ➔ [“Протоколи, които можете да разрешите или забраните” на страница 31](#)

## SSL/TLS комуникация с принтера

Когато се настрои сертификат на сървъра чрез SSL/TLS (Secure Sockets Layer/Transport Layer Security) (Слой със защитени сокети/Защита на транспортния слой) комуникация към принтера, можете да шифровате пътя на комуникация между компютрите. Направете това, ако искате да предотвратите дистанционен и неупълномощен достъп.

## Настройки за защита

---

### Относно цифрово сертифициране

- ❑ Сертификат, подписан от сертифициращ орган  
Сертификат, подписан от сертифициращ орган (CA), трябва да се получи от сертифициращ орган. Можете да осигурите сигурни комуникации с помощта на сертификат, подписан от сертифициращ орган. Можете да използвате сертификата, подписан от сертифициращ орган, за всяка функция за защита.
- ❑ Сертификат на сертифициращ орган  
Сертификатът на сертифициращ орган показва, че трета страна е проверила самоличността на сървъра. Това е ключов компонент в стила на защита „мрежа на доверие“. Трябва да получите сертификата на сертифициращ орган за удостоверяване на сървъра от сертифициращия орган, който го издава.
- ❑ Самоподписан сертификат  
Самоподписаният сертификат е сертификат, който принтерът издава и подписва сам. Този сертификат е ненадежден и не може да се избегне неправомерна смяна на самоличността. Ако използвате този сертификат за SSL/TLS сертификат, на брауъра може да се покаже предупреждение за защита. Можете да използвате този сертификат само за SSL/TLS комуникация.

#### Още по темата

- ➔ [“Получаване и импортиране на сертификат, подписан от сертифициращ орган” на страница 35](#)
- ➔ [“Изтриване на сертификат, подписан от сертифициращ орган” на страница 39](#)
- ➔ [“Актуализиране на самоподписан сертификат” на страница 39](#)

---

### Получаване и импортиране на сертификат, подписан от сертифициращ орган

#### Получаване на сертификат, подписан от сертифициращ орган

За да получите сертификат, подписан от сертифициращ орган, създайте CSR (заявка за подписване на сертификат) и я приложете по отношение на сертифициращия орган. Можете да създадете CSR с помощта на Web Config и компютър.

Следвайте стъпките, за да създадете CSR и да получите сертификат, подписан от сертифициращ орган, с помощта на Web Config. Когато създавате CSR с помощта на Web Config, сертификатът е във формат PEM/DER.

- 1** Влезте в Web Config и след това изберете **Network Security Settings (Настройки за мрежова защита)**. След това изберете **SSL/TLS > Certificate (Сертификат)**.
- 2** Щракнете върху **Generate (Генериране)** на CSR.  
Отваря се страница за създаване на CSR.
- 3** Въведете стойност за всеки елемент.

**Забележка:**

Наличната дължина на ключа и съкращенията варират според сертифициращия орган. Създайте заявка съгласно правилата на всеки сертифициращ орган.

## Настройки за защита

- 4 Щракнете върху **ОК**.  
Показва се съобщение за завършване.
- 5 Изберете **Network Security Settings (Настройки за мрежова защита)**. След това изберете **SSL/TLS > Certificate (Сертификат)**.
- 6 Щракнете върху един от бутоните за изтегляне на **CSR** в съответствие с определения формат от всеки сертифициращ орган, за да изтеглите CSR на компютър.



**Важно:**

Не генерирайте CSR отново. Ако направите това, възможно е да не можете да импортирате издаден сертификат, подписан от сертифициращ орган.

- 7 Изпратете CSR на сертифициращ орган и получите сертификат, подписан от сертифициращ орган.  
Следвайте правилата на всеки сертифициращ орган относно метода и формата на изпращане.
- 8 Запазете издадения сертификат, подписан от сертифициращ орган, на компютър, свързан към принтера.

Получаването на сертификат, подписан от сертифициращ орган, е завършено, когато запазите сертификата в определена дестинация.

### Още по темата

- ➔ [“Достъп до Web Config” на страница 20](#)
- ➔ [“Елементи за настройка на CSR” на страница 36](#)
- ➔ [“Импортиране на сертификат, подписан от сертифициращ орган” на страница 37](#)

### Елементи за настройка на CSR

EPSON	FX-890IIN
<a href="#">Administrator Logout</a> <input type="checkbox"/> Status <a href="#">Product Status</a> <a href="#">Network Status</a> <input checked="" type="checkbox"/> Network Settings <input checked="" type="checkbox"/> Network Security Settings <input checked="" type="checkbox"/> SSL/TLS <a href="#">Basic</a> <a href="#">Certificate</a> <input checked="" type="checkbox"/> IPsec/IP Filtering <input checked="" type="checkbox"/> Services <input checked="" type="checkbox"/> Administrator Settings	Network Security Settings > SSL/TLS > Certificate Key Length : RSA 2048bit - SHA-256 Common Name : EPSONXXXXXX,EPSONXXXXXX.local,192.0.2.102 Organization : Organizational Unit : Locality : State/Province : Country : <div style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Back"/> </div>

Елементи	Настройки и обяснение
Key Length (Дължина на ключ)	Изберете дължина на ключа за CSR.

## Настройки за защита

Елементи	Настройки и обяснение
Common Name (Използвано име)	Може да въведете между 1 и 128 знака. Ако това е IP адрес, той трябва да бъде статичен IP адрес.  Пример: URL адрес за достъп до Web Config: https://10.152.12.225  Използвано име: 10.152.12.225
Organization (Организация)/ Organizational Unit (Организационна единица)/Locality (Населено място)/ State/Province (Щат/провинция)	Можете да въведете между 0 и 64 знака в ASCII (0x20-0x7E). Можете да отделите индивидуални имена със запетаи.
Country (Държава)	Въведете кода на страната с двуцифрен номер, определен от ISO-3166.

### Още по темата

➔ [“Получаване на сертификат, подписан от сертифициращ орган” на страница 35](#)

## Импортиране на сертификат, подписан от сертифициращ орган



### Важно:

- Уверете се, че датата и часът на принтера са настроени правилно.
- Ако получите сертификат с помощта на CSR, създадена от Web Config, можете да импортирате сертификата веднъж.

1

Отворете Web Config и след това изберете **Network Security Settings (Настройки за мрежова защита)**. След това изберете **SSL/TLS > Certificate (Сертификат)**.

2

Щракнете върху **Import (Импортиране)**.

Отваря се страница за импортиране на сертификат.

3

Въведете стойност за всеки елемент.

В зависимост от това къде създавате CSR и файловия формат на сертификата, необходимите настройки могат да се различават. Въведете стойности на изискваните елементи според следното.

- Сертификат във формат PEM/DER, получен от Web Config
  - **Private Key (Личен ключ)**: Не конфигурирайте, защото принтерът съдържа личен ключ.
  - **Password (Парола)**: Не конфигурирайте.
  - **CA Certificate 1 (Сертификат на сертифициращ орган 1)/CA Certificate 2 (Сертификат на сертифициращ орган 2)**: по желание
- Сертификат във формат PEM/DER, получен от компютър
  - **Private Key (Личен ключ)**: Трябва да зададете.
  - **Password (Парола)**: Не конфигурирайте.
  - **CA Certificate 1 (Сертификат на сертифициращ орган 1)/CA Certificate 2 (Сертификат на сертифициращ орган 2)**: по желание

## Настройки за защита

- Сертификат във формат PKCS#12, получен от компютър
  - **Private Key (Личен ключ):** Не конфигурирайте.
  - **Password (Парола):** по желание
  - **CA Certificate 1 (Сертификат на сертифициращ орган 1)/CA Certificate 2 (Сертификат на сертифициращ орган 2):** Не конфигурирайте.

**4**

Щракнете върху **ОК**.

Показва се съобщение за завършване.

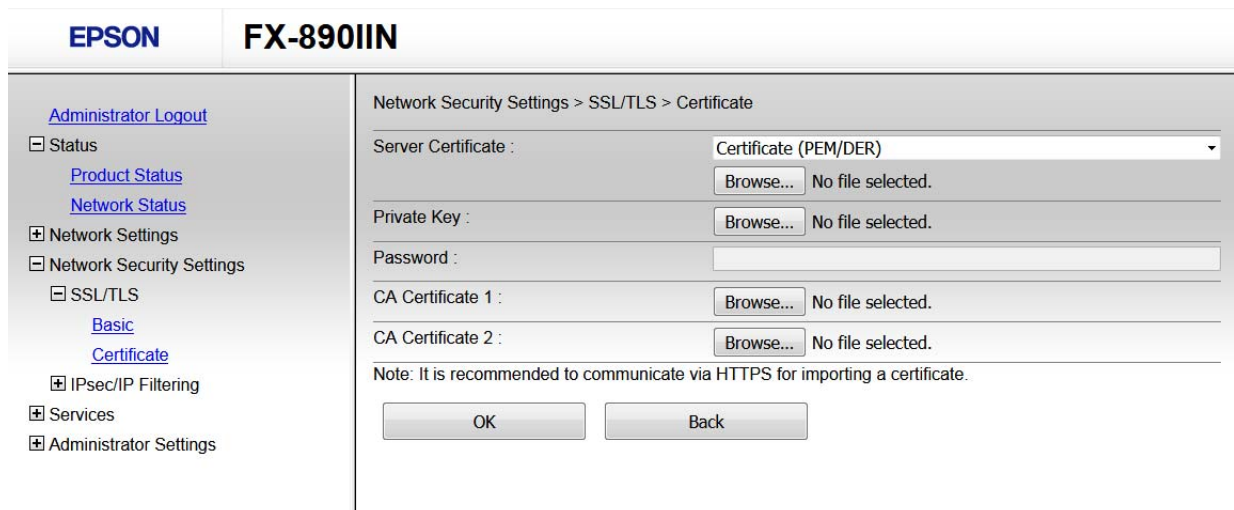
**Забележка:**

Щракнете върху *Confirm (Потвърди)*, за да проверите информацията за сертификата.

**Още по темата**

- ➔ [“Достъп до Web Config” на страница 20](#)
- ➔ [“Елементи за настройка на импортиране на сертификат, подписан от сертифициращ орган” на страница 38](#)

**Елементи за настройка на импортиране на сертификат, подписан от сертифициращ орган**



Елементи	Настройки и обяснение
Server Certificate (Сертификат на сървър) или Client Certificate (Сертификат на клиент)	Изберете формат на сертификата.
Private Key (Личен ключ)	Ако получите сертификат във формат PEM/DER с помощта на CSR, създадена от компютър, укажете файла с личен ключ, който съответства на сертификата.
Password (Парола)	Въведете парола за криптиране на личен ключ.
CA Certificate 1 (Сертификат на сертифициращ орган 1)	Ако форматът на Вашия сертификат е <b>Certificate (PEM/DER) (Сертификат (PEM/DER))</b> , импортирайте сертификат на сертифициращ орган, който издава сертификат на сървъра. Посочете файл, ако има нужда.

## Настройки за защита

Елементи	Настройки и обяснение
CA Certificate 2 (Сертификат на сертифициращ орган 2)	Ако форматът на Вашия сертификат е <b>Certificate (PEM/DER) (Сертификат (PEM/DER))</b> , импортирайте сертификат на сертифициращ орган, който издава <b>CA Certificate 1 (Сертификат на сертифициращ орган 1)</b> . Посочете файл, ако има нужда.

### Още по темата

➔ [“Импортиране на сертификат, подписан от сертифициращ орган”](#) на страница 37

## Изтриване на сертификат, подписан от сертифициращ орган

Можете да изтриете импортиран сертификат, когато сертификатът е изтекъл или когато вече не е необходима криптирана връзка.



### Важно:

Ако получавате сертификата с помощта на CSR, създадена от Web Config, не можете да импортирате отново изтрит сертификат. В този случай създайте CSR и получите сертификата отново.

- 1 Влезте в Web Config и след това изберете **Network Security Settings (Настройки за мрежова защита)**. След това изберете **SSL/TLS > Certificate (Сертификат)**.
- 2 Щракнете върху **Delete (Изтриване)**.
- 3 Потвърдете, че искате да изтриете сертификата в показаното съобщение.

### Още по темата

➔ [“Достъп до Web Config”](#) на страница 20

## Актуализиране на самоподписан сертификат

Ако принтерът поддържа функция за HTTPS сървър, можете да актуализирате самоподписан сертификат. При достъп до Web Config с помощта на самоподписан сертификат се появява предупредително съобщение.

Използвайте самоподписания сертификат временно, докато получите и импортирате сертификат, подписан от сертифициращ орган.

- 1 Влезте в Web Config и изберете **Network Security Settings (Настройки за мрежова защита) > SSL/TLS > Certificate (Сертификат)**.
- 2 Щракнете върху **Update (Актуализация)**.
- 3 Въведете **Common Name (Използвано име)**.  
Въведете IP адрес или идентификатор, например FQDN име за принтера. Може да въведете между 1 и 128 знака.

## Настройки за защита

**Забележка:**

Можете да отделите идентификационно име (CN) със запетайи.

- 4** Посочете срок на валидност на сертификата.

The screenshot shows the Epson Web Config interface for the FX-890IIN printer. The left sidebar contains a navigation menu with the following items: Administrator Logout, Status (with sub-links for Product Status and Network Status), Network Settings, Network Security Settings (expanded), SSL/TLS (expanded), Basic, Certificate, IPsec/IP Filtering, Services, and Administrator Settings. The main content area is titled 'Network Security Settings > SSL/TLS > Certificate'. It contains the following configuration fields:

Key Length :	RSA 2048bit - SHA-256
Common Name :	EPSONXXXXXX,EPSONXXXXXX.local,192.0.2.102
Organization :	SEIKO EPSON CORP.
Valid Date (UTC) :	2017-04-11 06:22:56 UTC
Certificate Validity (year) :	10

At the bottom of the configuration area, there are two buttons: 'Next' and 'Back'.

- 5** Щракнете върху **Next (Напред)**.

Показва се съобщение за потвърждение.

- 6** Щракнете върху **ОК**.

Принтерът се актуализира.

**Забележка:**

Щракнете върху *Confirm (Потвърди)*, за да проверите информацията за сертификата.

**Още по темата**

➔ [“Достъп до Web Config” на страница 20](#)

## Шифрована комуникация с IPsec/IP филтриране

### Относно IPsec/IP филтрирането

Ако принтерът поддържа IPsec/IP филтриране, можете да филтрирате трафика по IP адреси, услуги и порт. Чрез комбиниране на филтрирането, можете да конфигурирате принтера да приема или да блокира определени клиенти и определени данни. Освен това можете да подобрите нивото на защита, като използвате IPsec.



## Настройки за защита

За да филтрирате трафика, конфигурирайте правилата по подразбиране. Правилата по подразбиране се прилагат за всеки потребител или група, която се свързва към принтера. За по-фин контрол върху потребители и групи от потребители конфигурирайте групови правила. Групова политика представлява едно или повече правила, приложени към потребител или група потребители. Принтерът контролира IP пакети, които съответстват на конфигурирани политики. IP пакетите се удостоверяват по реда на групови правила от 1 до 10, след това – с правила по подразбиране.

**Забележка:**

Компютри, които работят под Windows Vista или по-нова версия или под Windows Server 2008 или по-нова версия, поддържат IPsec.

---

## Конфигуриране на правила по подразбиране

- 1 Влезте в Web Config и изберете **Network Security Settings (Настройки за мрежова защита) > IPsec/IP Filtering (IPsec/IP филтриране) > Basic (Основни)**.
- 2 Въведете стойност за всеки елемент.
- 3 Щракнете върху **Next (Напред)**.  
Показва се съобщение за потвърждение.
- 4 Щракнете върху **OK**.  
Принтерът се актуализира.

**Още по темата**

- ➔ [“Достъп до Web Config” на страница 20](#)
- ➔ [“Елементи за настройка на правила по подразбиране” на страница 42](#)

## Настройки за защита

### Елементи за настройка на правила по подразбиране

**EPSON** **FX-890IIN**

Administrator Logout

- [-] Status
  - [Product Status](#)
  - [Network Status](#)
- [+] Network Settings
  - [-] Network Security Settings
    - [-] SSL/TLS
    - [-] IPsec/IP Filtering
      - [Basic](#)
  - [-] Services
  - [-] Administrator Settings

Network Security Settings > IPsec/IP Filtering > Basic

Each policy is applied with following priorities:  
Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy

Default Policy 1 2 3 4 5 6 7 8 9 10

IPsec/IP Filtering :  Enable  Disable

Default Policy

Access Control : IPsec

Authentication Method : Pre-Shared Key

Pre-Shared Key : ●●●●●●

Confirm Pre-Shared Key : ●●●●●●

Encapsulation : Transport Mode

Remote Gateway(Tunnel Mode) :

Security Protocol : ESP

Next

Елементи	Настройки и обяснение	
IPsec/IP Filtering (IPsec/IP филтриране)	Можете да разрешите или забраните функцията за IPsec/IP филтриране.	
Access Control (Контрол на достъпа)	Permit Access (Разреша достъп)	Изберете тази опция, за да разрешите преминаване на конфигурирани IP пакети.
	Refuse Access (Откажи достъп)	Изберете тази опция, за да забраните преминаване на конфигурирани IP пакети.
	IPsec	Изберете тази опция, за да разрешите преминаване на конфигурирани IPsec пакети.
Authentication Method (Начин на удостоверяване)	Показва съвместими начини на удостоверяване.	
Pre-Shared Key (Предварително споделен ключ)	Въведете предварително споделен ключ между 1 и 127 символа.	
Confirm Pre-Shared Key (Потвърждаване на предварително споделен ключ)	Въведете ключа, който сте конфигурирали за потвърждение.	
Encapsulation (Капсулиране)	Ако изберете <b>IPsec</b> за <b>Access Control (Контрол на достъпа)</b> , трябва да конфигурирате режим на капсулиране.	
	Transport Mode (Транспортен режим)	Изберете тази опция, ако използвате принтера само на една и съща LAN мрежа. Шифроват се IP пакети от слой 4 или по-нов.
	Tunnel Mode (Тунелен режим)	Ако използвате принтера в мрежа с възможност за интернет, като например IPsec-VPN, изберете тази опция. Шифроват се заглавната част и данните на IP пакетите.

## Настройки за защита

Елементи	Настройки и обяснение			
Remote Gateway(Tunnel Mode) (Отдалечен шлюз (тунелен режим))	Ако изберете <b>Tunnel Mode (Тунелен режим)</b> за <b>Encapsulation (Капсулиране)</b> , въведете адрес на шлюз между 1 и 39 знака.			
Security Protocol (Протокол за защита)	Ако изберете <b>IPsec</b> за <b>Access Control (Контрол на достъпа)</b> , изберете опция.			
	<table border="1"> <tbody> <tr> <td>ESP</td> <td>Изберете тази опция, за да гарантирате целостта на удостоверяването и данните, както и за шифроване на данните.</td> </tr> <tr> <td>АН</td> <td>Изберете тази опция, за да гарантирате целостта на удостоверяването и данните. Дори ако шифроване на данни е забранено, можете да използвате IPsec.</td> </tr> </tbody> </table>	ESP	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните, както и за шифроване на данните.	АН
ESP	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните, както и за шифроване на данните.			
АН	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните. Дори ако шифроване на данни е забранено, можете да използвате IPsec.			

### Още по темата

➔ [“Конфигуриране на правила по подразбиране” на страница 41](#)

## Конфигуриране на групови правила

- 1 Отворете Web Config на принтера и изберете **Network Security Settings (Настройки за мрежова защита) > IPsec/IP Filtering (IPsec/IP филтриране) > Basic (Основни)**.
- 2 Щракнете върху номериран раздел, който искате да конфигурирате.
- 3 Въведете стойност за всеки елемент.
- 4 Щракнете върху **Next (Напред)**.  
Показва се съобщение за потвърждение.
- 5 Щракнете върху **ОК**.  
Принтерът се актуализира.

### Още по темата

➔ [“Достъп до Web Config” на страница 20](#)

➔ [“Елементи за настройка на групови правила” на страница 44](#)

## Настройки за защита

### Елементи за настройка на групови правила

**EPSON**
**FX-890IIN**

[Administrator Logout](#)

Status

[Product Status](#)

[Network Status](#)

Network Settings

Network Security Settings

SSL/TLS

IPsec/IP Filtering

[Basic](#)

Services

Administrator Settings

Network Security Settings > IPsec/IP Filtering > Basic

Each policy is applied with following priorities:  
Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy

Default Policy
1
2
3
4
5
6
7
8
9
10

Enable this Group Policy

Access Control : IPsec

Local Address(Printer) : Any addresses

Remote Address(Host) :

Method of Choosing Port : Port Number

Service Name :

- Any
- ENPC
- SNMP
- LPR
- RAW (Port9100)
- RAW (Custom Port)
- IPP/IPPS
- WSD
- WS-Discovery
- Network Scan
- Network Push Scan
- Network Push Scan Discovery
- FTP Data (Local)
- FTP Control (Local)
- FTP Data (Remote)
- FTP Control (Remote)
- CIFS (Local)
- CIFS (Remote)
- HTTP (Local)
- HTTPS (Local)
- HTTP (Remote)
- HTTPS (Remote)

Transport Protocol : Any Protocol

Елементи	Настройки и обяснение	
Enable this Group Policy (Разреши тези групови правила)	Можете да разрешите или забраните групови правила.	
Access Control (Контрол на достъпа)	Конфигурирайте контролен метод за трафик на IP пакети.	
	Permit Access (Разреши достъп)	Изберете тази опция, за да разрешите преминаване на конфигурирани IP пакети.
	Refuse Access (Откажи достъп)	Изберете тази опция, за да забраните преминаване на конфигурирани IP пакети.
IPsec	Изберете тази опция, за да разрешите преминаване на конфигурирани IPsec пакети.	
Local Address(Printer) (Локален адрес (принтер))	Изберете IPv4 адрес или IPv6 адрес, който съответства на средата на Вашата мрежа. Ако IP адресът се назначава автоматично, можете да изберете <b>Use auto-obtained IPv4 address (Да се използва автоматично получен IPv4 адрес)</b> .	
Remote Address (Host) (Отдалечен достъп (хост))	<p>Въведете IP адреса на устройството за контрол на достъпа. IP адресът трябва да бъде между 0 и 43 знака. Ако не въведете IP адрес, се контролират всички адреси.</p> <p>Забележка: Ако IP адресът се задава автоматично (например е назначен от DHCP), връзката може да не е налична. Конфигурирайте статичен IP адрес.</p>	

## Настройки за защита

Елементи	Настройки и обяснение	
Method of Choosing Port (Начин за избор на порт)	Изберете метод за определяне на портовете.	
Service Name (Име на услуга)	Ако изберете <b>Service Name (Име на услугата)</b> за <b>Method of Choosing Port (Начин за избор на порт)</b> , изберете опция.	
Transport Protocol (Транспортен протокол)	Ако изберете <b>Port Number (Номер на порт)</b> за <b>Method of Choosing Port (Начин за избор на порт)</b> , трябва да конфигурирате режим на капсулиране.	
	Any Protocol (Произволен протокол)	Изберете тази опция, за да контролирате всички типове протоколи.
	TCP	Изберете тази опция, за да контролирате данните за уникаст.
	UDP	Изберете тази опция, за да контролирате данните за излъчване и мултикаст.
	ICMPv4	Изберете тази опция, за да контролирате командата ping.
Local Port (Локален порт)	Ако изберете <b>Port Number (Номер на порт)</b> за <b>Method of Choosing Port (Начин за избор на порт)</b> и ако изберете <b>TCP</b> или <b>UDP</b> за <b>Transport Protocol (Транспортен протокол)</b> , въведете номера на портове, за да контролирате приемането на пакети, като ги отделяте със запетаи. Можете да въведете до 10 номера на портове. Пример: 20,80,119,5220 Ако не въведете номер на порт, се контролират всички портове.	
Remote Port (Отдалечен порт)	Ако изберете <b>Port Number (Номер на порт)</b> за <b>Method of Choosing Port (Начин за избор на порт)</b> и ако изберете <b>TCP</b> или <b>UDP</b> за <b>Transport Protocol (Транспортен протокол)</b> , въведете номера на портове, за да контролирате изпращането на пакети, като ги отделяте със запетаи. Можете да въведете до 10 номера на портове. Пример: 25,80,143,5220 Ако не въведете номер на порт, се контролират всички портове.	
Authentication Method (Начин на удостоверяване)	Ако изберете <b>IPsec</b> за <b>Access Control (Контрол на достъпа)</b> , изберете опция.	
Pre-Shared Key (Предварително споделян ключ)	Въведете предварително споделян ключ между 1 и 127 символа.	
Confirm Pre-Shared Key (Потвърждаване на предварително споделян ключ)	Въведете ключа, който сте конфигурирали за потвърждение.	
Encapsulation (Капсулиране)	Ако изберете <b>IPsec</b> за <b>Access Control (Контрол на достъпа)</b> , трябва да конфигурирате режим на капсулиране.	
	Transport Mode (Транспортен режим)	Изберете тази опция, ако използвате принтера само на една и съща LAN мрежа. Шифроват се IP пакети от слой 4 или по-нов.
	Tunnel Mode (Тунелен режим)	Ако използвате принтера в мрежа с възможност за интернет, като например IPsec-VPN, изберете тази опция. Шифроват се заглавната част и данните на IP пакетите.

## Настройки за защита

Елементи	Настройки и обяснение	
Remote Gateway(Tunnel Mode) (Отдалечен шлюз (тунелен режим))	Ако изберете <b>Tunnel Mode (Тунелен режим)</b> за <b>Encapsulation (Капсулиране)</b> , въведете адрес на шлюз между 1 и 39 знака.	
Security Protocol (Протокол за защита)	Ако изберете <b>IPsec</b> за <b>Access Control (Контрол на достъпа)</b> , изберете опция.	
	ESP	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните, както и за шифроване на данните.
	AH	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните. Дори ако шифроване на данни е забранено, можете да използвате IPsec.

### Още по темата

- ➔ “Конфигуриране на групови правила” на страница 43
- ➔ “Комбинация от Local Address (Printer) (Локален адрес (принтер)) и Remote Address (Host) (Отдалечен достъп (хост)) в Group Policy (Групови правила)” на страница 46
- ➔ “Позовавания на име на услуга в груповата политика” на страница 46

## Комбинация от Local Address (Printer) (Локален адрес (принтер)) и Remote Address (Host) (Отдалечен достъп (хост)) в Group Policy (Групови правила)

		Настройка на Local Address(Printer) (Локален адрес (принтер))		
		IPv4	IPv6*2	Произволни адреси*3
Задаване на Remote Address (Host) (Отдалечен достъп (хост))	IPv4*1	✓	-	✓
	IPv6*1*2	-	✓	✓
	Празен	✓	✓	✓

\*1: Ако изберете **IPsec** за **Access Control (Контрол на достъпа)**, не можете да посочите дължина на префикса.

\*2: Ако изберете **IPsec** за **Access Control (Контрол на достъпа)**, можете да изберете локален адрес за връзката (fe80::), но правилата за групите ще бъдат забранени.

\*3 С изключение на локални за връзката IPv6 адреси.

## Позовавания на име на услуга в груповата политика

### Забележка:

Неналичните услуги се показват, но не могат да бъдат избирани.

Име на услуга	Тип на протокола	Номер на локален порт	Номер на отдалечен порт	Управлявани функции
Any (Произволни)	-	-	-	Всички услуги
ENPC	UDP	3289	Всеки порт	Търсене на принтер от приложения като EpsonNet Config, драйвер за принтер и драйвер за скенер

## Настройки за защита

Име на услуга	Тип на протокола	Номер на локален порт	Номер на отдалечен порт	Управлявани функции
SNMP	UDP	161	Всеки порт	Получаване и конфигуриране на MIB от приложения, като например EpsonNet Config, драйвера за принтер на Epson и драйвера за скенер на Epson
LPR	TCP	515	Всеки порт	Пренасочване на LPR данни
RAW (Port9100) (RAW (порт 9100))	TCP	9100	Всеки порт	Пренасочване на RAW данни
RAW (Custom Port) (RAW (потребителски порт))	TCP	2501 (по подразбиране)	Всеки порт	Пренасочване на RAW данни
IPP/IPPS	TCP	631	Всеки порт	Пренасочване на данни за AirPrint (IPP/IPPS печат)
WSD	TCP	Всеки порт	5357	Управление на WSD
WS-Discovery	UDP	3702	Всеки порт	Търсене на принтер от WSD
Network Scan (Мрежово сканиране)	TCP	1865	Всеки порт	Пренасочване на сканирани данни от Document Capture Pro
Network Push Scan (Мрежово Push сканиране)	TCP	Всеки порт	2968	Извличане на информация за заданието от насочено сканиране от Document Capture Pro
Network Push Scan Discovery	UDP	2968	Всеки порт	Извършва се търсене на компютър при насочено сканиране от Document Capture Pro
FTP Data (Local) (FTP данни (локални))	TCP	20	Всеки порт	FTP сървър (пренасочване на данни от FTP печат)
FTP Control (Local) (FTP контрол (локален))	TCP	21	Всеки порт	FTP сървър (управление на FTP печат)

## Настройки за защита

Име на услуга	Тип на протокола	Номер на локален порт	Номер на отдалечен порт	Управлявани функции
FTP Data (Remote) (FTP данни (отдалечени))	TCP	Всеки порт	20	FTP клиент (пренасочване на данни от сканиране и получени данни от факс)  Това обаче може да управлява само FTP сървър, който използва номер на отдалечен порт 20.
FTP Control (Remote) (FTP контрол (отдалечен))	TCP	Всеки порт	21	FTP клиент (управление за пренасочване на данни от сканиране и получени данни от факс)
CIFS (Local) (CIFS (локален))	TCP	445	Всеки порт	CIFS сървър (споделящ мрежова папка)
CIFS (Remote) (CIFS (отдалечен))	TCP	Всеки порт	445	CIFS клиент (пренасочване на данни от сканиране и получени данни от факс към папка)
HTTP (Local) (HTTP (локален))	TCP	80	Всеки порт	HTTP(S) сървър (пренасочване на данни на Web Config и WSD)
HTTPS (Local) (HTTPS (локален))	TCP	443	Всеки порт	
HTTP (Remote) (HTTP (отдалечен))	TCP	Всеки порт	80	HTTP(S) клиент (комуникация между Epson Connect или Google Cloud Print, актуализация на фърмуер и актуализация на основен сертификат)
HTTPS (Remote) (HTTPS (отдалечен))	TCP	Всеки порт	443	

## Примери за конфигурация на IPsec/IP Filtering (IPsec/IP филтриране)

### Приемане само на IPsec пакети

Този пример е за конфигуриране само на правила по подразбиране.

#### Default Policy (Правила по подразбиране):

- IPsec/IP Filtering (IPsec/IP филтриране): Enable (Разреша)
- Access Control (Контрол на достъпа): IPsec
- Authentication Method (Начин на удостоверяване): Pre-Shared Key (Предварително споделян ключ)
- Pre-Shared Key (Предварително споделян ключ): Въведете до 127 знака.



## Настройки за защита

### Group Policy (Групови правила):

Не конфигурирайте.

### Получаване на данни за печат и настройки на принтера

Този пример позволява комуникацията на данните за печат и конфигурацията на принтера от посочени услуги.

### Default Policy (Правила по подразбиране):

- IPsec/IP Filtering (IPsec/IP филтриране): Enable (Разреши)
- Access Control (Контрол на достъпа): Refuse Access (Откажи достъп)

### Group Policy (Групови правила):

- Enable this Group Policy (Разреши тези групови правила): Поставете отметка в квадратчето.
- Access Control (Контрол на достъпа): Permit Access (Разреши достъп)
- Remote Address (Host) (Отдалечен достъп (хост)): IP адрес на клиент
- Method of Choosing Port (Начин за избор на порт): Service Name (Име на услугата)
- Service Name (Име на услугата): Поставете отметка в ENPC, SNMP, HTTP (Local) (HTTP (Локален)), HTTPS (Local) (HTTPS (Локален)) и RAW (Port9100) (RAW (порт 9100)).

### Получаване на достъп само от определен IP адрес

Този пример позволява на посочен IP адрес да получи достъп до принтера.

### Default Policy (Правила по подразбиране):

- IPsec/IP Filtering (IPsec/IP филтриране): Enable (Разреши)
- Access Control (Контрол на достъпа): Refuse Access (Откажи достъп)

### Group Policy (Групови правила):

- Enable this Group Policy (Разреши тези групови правила): Поставете отметка в квадратчето.
- Access Control (Контрол на достъпа): Permit Access (Разреши достъп)
- Remote Address (Host) (Отдалечен достъп (хост)): IP адрес на клиент на администратора

#### **Забележка:**

Независимо от конфигурацията на политиката, клиентът ще има възможност за достъп и конфигуриране на принтера.

## Използване на SNMPv3 протокол

---

### Относно SNMPv3

SNMP е протокол, който изпълнява мониторинг и контрол за събиране на информация за устройствата, свързани в мрежата. SNMPv3 е подобрена версия на функцията за управление на защитата.

Когато използвате SNMPv3, мониторингът на състоянието и промените на настройките на SNMP комуникацията (пакет) може да се удостовери и криптира с цел да се защити SNMP комуникацията (пакета) от мрежови рискове, например подправяне, промяна на самоличността и прехващане.

---

### Конфигуриране на SNMPv3

Ако принтерът поддържа протокола SNMPv3, можете да наблюдавате и контролирате достъпа до принтера.

- 1 Влезте в Web Config и изберете **Services (Услуги) > Protocol (Протокол)**.
- 2 Въведете стойност за всеки елемент от **SNMPv3 Settings (SNMPv3 настройки)**.
- 3 Щракнете върху **Next (Напред)**.  
Показва се съобщение за потвърждение.
- 4 Щракнете върху **OK**.  
Принтерът се актуализира.

#### Още по темата

- ➔ [“Достъп до Web Config” на страница 20](#)
- ➔ [“Елементи за SNMPv3 настройка” на страница 51](#)

**Настройки за защита**

**Елементи за SNMPv3 настройка**

**EPSON**
**FX-890IIN**

[Administrator Logout](#)

Status

[Product Status](#)

[Network Status](#)

Network Settings

Network Security Settings

Services

[Protocol](#)

Administrator Settings

Communication Timeout (sec) :

SNMPv1/v2c Settings
 

Enable SNMPv1/v2c
 

Access Authority :

Community Name (Read Only) :

Community Name (Read/Write) :

SNMPv3 Settings
 

Enable SNMPv3
 

User Name :

Authentication Settings
 

Algorithm :

Password :

Confirm Password :

Encryption Settings
 

Algorithm :

Password :

Confirm Password :

Context Name :

Елементи	Настройки и обяснение
Enable SNMPv3 (Разрешаване на SNMPv3)	SNMPv3 е разрешен, когато е поставена отметката.
User Name (Потребителско име)	Въведете между 1 и 32 знака с помощта на 1-байтови символи.
Authentication Settings (Настройки за удостоверяване)	
Algorithm (Алгоритъм)	Изберете алгоритъм за удостоверяване.
Password (Парола)	Въведете между 8 и 32 знака в ASCII (0x20–0x7E).
Confirm Password (Потвърждаване на паролата)	Въведете паролата, която сте конфигурирали, за потвърждение.
Encryption Settings (Настройки за шифроване)	
Algorithm (Алгоритъм)	Изберете алгоритъм за шифроване.
Password (Парола)	Въведете между 8 и 32 знака в ASCII (0x20–0x7E).
Confirm Password (Потвърждаване на паролата)	Въведете паролата, която сте конфигурирали, за потвърждение.
Context Name (Име на контекста)	Въведете между 1 и 32 знака с помощта на 1-байтови символи.

## Настройки за защита

### Още по темата

- ➔ [“Конфигуриране на SNMPv3” на страница 50](#)

---

## Разрешаване на проблеми

---

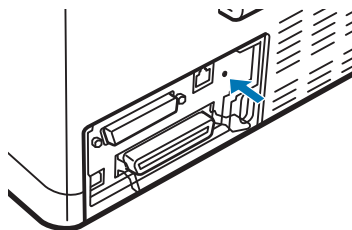
### Проверка на регистри за сървър и мрежово устройство

Ако възникне проблем с мрежовата връзка, е възможно да идентифицирате причината, като проверите регистъра за състоянието на имейл сървъра или на LDAP сървъра, като използвате системния регистър за мрежово устройство, например маршрутизатор или команди.

### Печат на лист за състоянието на мрежата

Може да отпечатате и да проверите подробна информация за мрежата.

- 1 Заредете хартия.
- 2 Задръжте бутона за листа за състоянието за около три секунди.  
Ще се отпечатаат листове за състоянието на мрежата.



### Инициализиране на мрежовите настройки

---

#### Възстановяване на мрежовите настройки от принтера

Можете да възстановите мрежови настройки до стойностите им по подразбиране.

- 1 Изключете принтера.
- 2 Задръжте бутона за лист за състоянието, докато включвате принтера.

## Разрешаване на проблеми

---

## Възстановяване на мрежови настройки с помощта на EpsonNet Config

Можете да възстановите мрежови настройки до стойностите по подразбиране, като използвате EpsonNet Config.

- 1 Стартирайте EpsonNet Config.
- 2 Изберете принтера, за който искате да възстановите мрежовите настройки.
- 3 Щракнете с десния бутон на мишката върху името на принтера и изберете **Default Settings (Настройки по подразбиране) > Network Interface (Мрежов интерфейс)**.
- 4 Щракнете върху **ОК** на екрана за потвърждение.
- 5 Щракнете върху **ОК**.

---

## Проверка на комуникацията между устройства и компютри

---

### Проверка на връзката чрез команда Ping

Можете да използвате командата Ping, за да се уверите, че компютърът е свързан към принтера. Следвайте стъпките по-долу, за да проверите връзката с командата Ping.

- 1 Вижте IP адреса на принтера за връзката, която искате да проверите.  
Можете да го проверите в колоната **IP Address (IP адрес)** от листа за състоянието на мрежата.
- 2 Изведете екрана на командната среда на компютъра.
  - Windows 10  
Щракнете върху стартовия бутон с десния бутон на мишката или го натиснете и задръжте, после изберете **Command Prompt (Команден прозорец)**.
  - Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012  
Изведете екрана на приложението, след което изберете **Command Prompt (Команден прозорец)**.
  - Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 или по-стари версии  
Щракнете върху стартовия бутон, изберете **All Programs (Всички програми)** или **Programs (Програми) > Accessories (Принадлежности) > Command Prompt (Команден прозорец)**.
- 3 Въведете следното в командния ред, след което натиснете Enter.  
ping 192.0.2.111 (ако IP адресът на компютъра, който искате да проверите, е 192.0.2.111)

## Разрешаване на проблеми

**4**

Ако се появи следното, потвърждението е завършено. Затворете **Command Prompt (Команден прозорец)**.

Статистика за ping за 192.0.2.111:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Round-trip time: (ms):

Minimum = 0ms, Maximum = 0ms, Average = 0ms

## Проблеми при използване на мрежов софтуер

---

### Няма достъп до Web Config

**Конфигуриран ли е правилно IP адресът на принтера?**

Конфигурирайте IP адреса с помощта на EpsonNet Config или контролния панел на принтера. Можете да потвърдите текущата информация за настройка с лист за състоянието на мрежата или от контролния панел на принтера.

**Вашият браузър поддържа ли шифроване в голям обем за Encryption Strength за SSL/TLS?**

Шифроването в голям обем за Encryption Strength за SSL/TLS е, както следва. Web Config може да се получи достъп в браузър, който поддържа следното шифроване в голям обем. Проверете какво шифроване поддържа Вашият браузър.

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

**Появява се съобщението „Изтекъл“ при достъп до Web Config чрез SSL комуникация (https).**

Ако сертификата е изтекъл, получите сертификата отново. Ако съобщението се появява преди датата на неговото изтичане, се уверете, че датата на принтера е конфигурирана правилно.

**Появява се съобщението „Името на сертификата за защита не съвпада“ при достъп до Web Config чрез SSL комуникация (https).**

IP адресът на принтера, въведен за Common Name (Използвано име) за създаване на самоподписан сертификат или CSR, не съвпада с адреса, вписан в браузъра. Получете и импортирайте сертификата отново или сменете името на принтера.

**Осъществява се достъп до принтера през прокси сървър.**

Ако използвате прокси сървър с Вашия принтер, трябва да конфигурирате настройките за прокси на Вашия браузър.

## Разрешаване на проблеми

Изберете **Control Panel (Контролен панел) > Network and Internet (Мрежа и интернет) > Internet Options (Интернет опции) > Connections (Връзки) > LAN settings (LAN настройки) > Proxy server (Прокси сървър)**, след което конфигурирайте да не се използва прокси сървър за локални адреси.

Пример:

192.168.1.\*: Локален адрес 192.168.1.XXX, подмрежова маска 255.255.255.0

192.168.\*.\*: Локален адрес 192.168.XXX.XXX, подмрежова маска 255.255.0.0

Още по темата

➔ “Достъп до Web Config” на страница 20

➔ “Назначаване на IP адрес чрез EpsonNet Config” на страница 14

---

## Името на модела и/или IP адресът не се показват на EpsonNet Config

Избрахте ли **Block (Блокиране)**, **Cancel (Отказ)** или **Shut down (Изключване)**, когато е показан екранът за защита на Windows или екранът на защитната стена?

Ако изберете **Block (Блокиране)**, **Cancel (Отказ)** или **Shut down (Изключване)**, IP адресът и името на модела няма да бъдат показани в EpsonNet Config или EpsonNet Setup.

За да коригирате това, регистрирайте EpsonNet Config като изключение с помощта на защитната стена на Windows и наличен в търговската мрежа софтуер за защита. Ако използвате антивирусна програма или програма за защита, затворете я и след това се опитайте да използвате EpsonNet Config.

Дали зададеното време на изчакване за грешка в комуникацията е твърде кратко?

Изпълнете EpsonNet Config и изберете **Tools (Инструменти) > Options (Опции) > Timeout (Време за изчакване)**, а след това увеличете продължителността на времето за настройката **Communication Error (Комуникационна грешка)**. Имайте предвид, че това може да накара EpsonNet Config да работи по-бавно.

## Решаване на проблеми за повишена защита

---

### Възстановяване на настройките за защита

Когато установите силно защитена среда, например IPsec/IP филтриране, е възможно да не можете да комуникирате с устройствата поради неправилни настройки или проблеми с устройството или сървъра. В този случай възстановете настройките за защита на устройството, за да конфигурирате отново настройките или за да получите временен достъп.

---

### Забрана на функцията за защита от принтера

Можете да забраните IPsec/IP Filtering (IPsec/IP филтриране) от принтера.

1

Уверете се, че има заредена хартия.



## Разрешаване на проблеми

- 2 Натиснете бутоните **Menu (Pitch и Tear Off/Bin)**, докато принтерът издаде звуков сигнал и индикаторите **Menu** (и двата индикатора **Tear Off/Bin**) светнат.  
  
Принтерът влиза в режим за настройка по подразбиране и отпечатва съобщение, което Ви подканва да изберете език за менюто за настройка по подразбиране. Подчертаният език показва текущата настройка.
- 3 Ако желаният от Вас език не е избран, натискайте бутона **Item↓ (Font)**, докато разпечатката не покаже желанния език.
- 4 Натиснете бутона **Set (Tear Off/Bin)**, за да изберете желанния език.
- 5 Ако искате да отпечатате текущите настройки, натиснете бутона **Set**. Ако искате да заобиколите печат на текущите настройки, натиснете бутона **Item↓** или бутона **Item↑**.  
  
Принтерът отпечатва първото меню и текущата стойност на менюто.
- 6 Натиснете бутона **Item↓** или бутона **Item↑**, за да изберете параметрите на менюто от **IPsec/IP Filtering**. Натиснете бутона **Set**, за да превъртите стойностите на избрания параметър докато не откриете **Off**.
- 7 След като приключите с настройките, натиснете бутоните **Menu (Pitch и Tear Off/Bin)**.  
  
Индикаторите **Menu** (и двата индикатора **Tear Off/Bin**) се изключват и принтерът излиза от режима за настройка по подразбиране.  
Настройките, които сте конфигурирали, са запазени като нова стойност.

**Забележка:**

Ако изключите принтера, преди да излезете от режима за настройка по подразбиране, евентуалните промени, които сте направили, ще бъдат отменени и няма да бъдат запазени.

---

## Възстановяване на функциите за защита с Web Config

Можете да забраните функцията, ако имате достъп до устройството от компютъра.

### Забрана на IPsec/IP Filtering (IPsec/IP филтриране) с Web Config

- 1 Влезте в Web Config и изберете **Network Security Settings (Настройки за мрежова защита) > IPsec/IP Filtering (IPsec/IP филтриране) > Basic (Основни)**.
- 2 Изберете **Disable (Забрани)** за **IPsec/IP Filtering (IPsec/IP филтриране)** в **Default Policy (Правила по подразбиране)**.
- 3 Щракнете върху **Next (Напред)**, после изчистете **Enable this Group Policy (Разреша тези групови правила)** за всички групови правила.
- 4 Щракнете върху **ОК**.

Още по темата

➔ [“Достъп до Web Config” на страница 20](#)

## Разрешаване на проблеми

## Проблеми при използване на функциите за мрежова защита

### Забравен предварително споделен ключ

Конфигурирайте ключа отново с помощта на Web Config.

За да промените ключа, влезте в Web Config и изберете **Network Security Settings (Настройки за мрежова защита) > IPsec/IP Filtering (IPsec/IP филтриране) > Basic (Основни) > Default Policy (Правила по подразбиране)** или **Group Policy (Групови правила)**.

Още по темата

➔ [“Достъп до Web Config” на страница 20](#)

### Не може да комуникира с IPsec комуникация

Използвате ли неподдържан алгоритъм за настройките на компютъра?

Принтерът поддържа следните алгоритми.

Методи за защита	Алгоритми
Алгоритъм за шифроване	AES-CBC 128,AES-CBC 192,AES-CBC 256,3DES-CBC,DES-CBC
Алгоритъм на хеширане	SHA-1,SHA2-256,SHA2-384,SHA2-512,MD5
Алгоритъм за обмен на ключове	Diffi e-Hellman Group2,Diffi e-Hellman Group1*,Diffi e-Hellman Group14* Elliptic Curve Diffi e- Hellman P-256*,Elliptic Curve Diffi e-Hellman P-384*

\* Наличният начин може да се различава според модела.

Още по темата

➔ [“Шифрована комуникация с IPsec/IP филтриране” на страница 40](#)

### Не може да комуникира внезапно

Дали IP адресът на принтера е невалиден или е променен?

Забранете IPsec от контролния панел на принтера.

Ако DHCP е остарял, рестартирането или IPv6 адресът е остарял или не е получен, регистрираният за принтера IP адрес за Web Config (**Network Security Settings (Настройки за мрежова защита) > IPsec/IP Filtering (IPsec/IP филтриране) > Basic (Основни) > Group Policy (Групови правила) > Local Address (Printer) (Локален адрес (принтер))**)) може да не е открит. Използвайте статичен IP адрес.

Дали IP адресът на компютъра е невалиден или е променен?

Забранете IPsec от контролния панел на принтера.

Ако DHCP е остарял, рестартирането или IPv6 адресът е остарял или не е получен, регистрираният за принтера IP адрес за Web Config (**Network Security Settings (Настройки за мрежова защита) > IPsec/IP Filtering (IPsec/IP филтриране) > Basic (Основни) > Group Policy (Групови правила) > Remote Address (Host) (Отдалечен адрес (хост))**)) може да не бъде открит. Използвайте статичен IP адрес.

## Разрешаване на проблеми

### Още по темата

- ➔ [“Достъп до Web Config” на страница 20](#)
- ➔ [“Шифрована комуникация с IPsec/IP филтриране” на страница 40](#)

## Не може да се създаде сигурен IPP порт за печат

### Посочен ли е правилният сертификат като сертификат на сървъра за SSL/TLS комуникация?

Ако посоченият сертификат не е правилен, създаването на порт може да е неуспешно. Уверете се, че използвате правилния сертификат.

### Импортиран ли е сертификат на сертифициращ орган на компютъра за достъп до принтера?

Ако не е импортиран сертификат на сертифициращ орган на компютъра, създаването на порт може да е неуспешно. Уверете се, че е импортиран сертификат на сертифициращ орган.

### Още по темата

- ➔ [“Достъп до Web Config” на страница 20](#)

## Не може да се установи връзка след конфигуриране на IPsec/IP филтриране

Възможно е зададената стойност да е грешна.

Забранете IPsec/IP филтриране от контролния панел на принтера. Свържете принтера и компютъра и отново конфигурирайте настройките за IPsec/IP филтриране.

### Още по темата

- ➔ [“Шифрована комуникация с IPsec/IP филтриране” на страница 40](#)

## Проблеми при използване на цифров сертификат

### Не може да се импортира сертификат, подписан от сертифициращ орган

#### Съвпада ли информацията на сертификата, подписан от сертифициращ орган, и на CSR?

Ако на сертификата, подписан от сертифициращ орган, и на CSR няма еднаква информация, CSR не може да се импортира. Проверете следното:

- Опитвате ли се да импортирате сертификата към устройство, което няма същата информация?

Проверете информацията на CSR и след това импортирайте сертификата към устройство, което има същата информация.

- Презаписахте ли запазената в принтера CSR след изпращането ѝ на сертифициращ орган?

Получете сертификата, подписан от сертифициращ орган, отново с CSR.

#### Сертификатът, подписан от сертифициращ орган, по-голям ли е от 5 KB?

Не можете да импортирате сертификат, подписан от сертифициращ орган, който е по-голям от 5 KB.

#### Правилна ли е паролата за импортиране на сертификата?

## Разрешаване на проблеми

Ако забравите паролата си, не можете да импортирате сертификата.

Още по темата

➔ [“Импортиране на сертификат, подписан от сертифициращ орган” на страница 37](#)

### Не може да се актуализира самоподписан сертификат

Въведено ли е Common Name (Използвано име)?

Трябва да е въведено Common Name (Използвано име).

Въведени ли са неподдържани символи в Common Name (Използвано име)? Например японският език не се поддържа.

Въведете между 1 и 128 знака във формат IPv4, IPv6, име на хост или FQDN в ASCII (0x20-0x7E).

Включени ли са запетая или интервал в Common Name (Използвано име)?

Ако е въведена запетая, Common Name (Използвано име) се разделя в тази точка. Ако е въведен само интервал преди или след запетая, възниква грешка.

Още по темата

➔ [“Актуализиране на самоподписан сертификат” на страница 39](#)

### Не може да се създаде CSR

Въведено ли е Common Name (Използвано име)?

Трябва да е въведено Common Name (Използвано име).

Въведени ли са неподдържани символи в Common Name (Използвано име), Organization (Организация), Organizational Unit (Подразделение на организация), Locality (Населено място), State/Province (Щат/провинция)? Например японският език не се поддържа.

Въведете знаци във формат IPv4, IPv6, име на хост или FQDN в ASCII (0x20-0x7E).

Включени ли са запетая или интервал в Common Name (Използвано име)?

Ако е въведена запетая, Common Name (Използвано име) се разделя в тази точка. Ако е въведен само интервал преди или след запетая, възниква грешка.

Още по темата

➔ [“Получаване на сертификат, подписан от сертифициращ орган” на страница 35](#)

### Появява се предупреждение за цифров сертификат

Съобщения	Причина/Какво да се направи
Enter a Server Certificate. (Въведете сертификат на сървър.)	<p><b>Причина:</b> Не сте избрали файл за импортиране.</p> <p><b>Какво да се направи:</b> Изберете файл и щракнете върху Import (Импортиране).</p>

## Разрешаване на проблеми

Съобщения	Причина/Какво да се направи
CA Certificate 1 is not entered. (Сертификат на сертифициращ орган 1 не е въведен.)	<p><b>Причина:</b> Сертификат на сертифициращ орган 1 не е въведен, а е въведен само сертификат на сертифициращ орган 2.</p> <p><b>Какво да се направи:</b> Импортирайте първо сертификат на сертифициращ орган 1.</p>
Invalid value below. (Невалидна стойност по-долу.)	<p><b>Причина:</b> Неподдържани знаци се съдържат в пътя до файла и/или паролата.</p> <p><b>Какво да се направи:</b> Уверете се, че знаците за елемента са въведени правилно.</p>
Invalid date and time. (Невалидна дата и час.)	<p><b>Причина:</b> Не са зададени дата и час на принтера.</p> <p><b>Какво да се направи:</b> Задайте дата и час с помощта на Web Config или Epson Device Admin.</p>
Invalid password. (Невалидна парола.)	<p><b>Причина:</b> Зададената за сертификата на сертифициращ орган парола и въведената парола не съвпадат.</p> <p><b>Какво да се направи:</b> Въведете правилната парола.</p>
Invalid file. (Невалиден файл.)	<p><b>Причина:</b> Не импортирате файл със сертификата в X509 формат.</p> <p><b>Какво да се направи:</b> За повече информация относно сертификата вижте уеб сайта на сертифициращия орган.</p>
	<p><b>Причина:</b> Импортираният файл е твърде голям. Максималният размер на файла е 5 KB.</p> <p><b>Какво да се направи:</b> Ако сте избрали правилния файл, сертификатът може да е повреден или подправен.</p>
	<p><b>Причина:</b> Веригата, съдържаща се в сертификата, е невалидна.</p> <p><b>Какво да се направи:</b> За повече информация относно сертификата вижте уеб сайта на сертифициращия орган.</p>
Cannot use the Server Certificates that include more than three CA certificates. (Сертификати на сървъри, които включват повече от три сертификата на сертифициращ орган, не могат да се използват.)	<p><b>Причина:</b> Файлът на сертификата в PKCS#12 формат съдържа повече от 3 сертификата на сертифициращ орган.</p> <p><b>Какво да се направи:</b> Импортирайте всеки сертификат, като го конвертирате от PKCS#12 формат в PEM формат, или импортирайте файла със сертификата в PKCS#12 формат, който съдържа до 2 сертификата на сертифициращ орган.</p>

## Разрешаване на проблеми

Съобщения	Причина/Какво да се направи
The certificate has expired. Check if the certificate is valid, or check the date and time on your printer. (Сертификатът е изтекъл. Проверете дали сертификатът е валиден или проверете датата и часа на Вашия принтер.)	<p><b>Причина:</b> Сертификатът е изтекъл.</p> <p><b>Какво да се направи:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Ако сертификатът е изтекъл, получите и импортирайте нов сертификат.</li> <li><input type="checkbox"/> Ако сертификатът не е изтекъл, проверете дали датата и часът на принтера са настроени правилно.</li> </ul>
Private key is required. (Изисква се личен ключ.)	<p><b>Причина:</b> Няма сдвоен личен ключ със сертификата.</p> <p><b>Какво да се направи:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Ако сертификатът е в PEM/DER формат и е получен от CSR с помощта на компютър, посочете файла с личен ключ.</li> <li><input type="checkbox"/> Ако сертификатът е в PKCS#12 формат и е получен от CSR с помощта на компютър, създайте файл, който съдържа личния ключ.</li> </ul>
	<p><b>Причина:</b> Импортирали сте повторно PEM/DER сертификата, получен от CSR с помощта на Web Config.</p> <p><b>Какво да се направи:</b> Ако сертификатът е в PEM/DER формат и е получен от CSR с помощта на Web Config, можете да го импортирате само веднъж.</p>
Setup failed. (Неуспешна настройка)	<p><b>Причина:</b> Не може да се завърши конфигурацията, тъй като комуникацията между принтера и компютъра е неуспешна или файлът не може да се прочете поради някакви грешки.</p> <p><b>Какво да се направи:</b> След проверка на дадения файл и комуникацията, импортирайте файла отново.</p>

## Още по темата

➔ [“Относно цифрово сертифициране” на страница 35](#)

## Изтриване на сертификат, подписан от сертифициращ орган, по грешка

## Има ли файл с резервно копие на сертификата?

Ако имате резервно копие на файла, импортирайте сертификата отново.

Ако получавате сертификат с помощта на CSR, създадена от Web Config, не можете да импортирате отново изтрит сертификат. Създайте CSR и получите нов сертификат.

## Още по темата

➔ [“Изтриване на сертификат, подписан от сертифициращ орган” на страница 39](#)

➔ [“Импортиране на сертификат, подписан от сертифициращ орган” на страница 37](#)

---

## Приложение

# Въведение в мрежов софтуер

Следното описва софтуера, който конфигурира и управлява устройствата.

---

## Epson Device Admin

Epson Device Admin е приложение, което ви позволява да инсталирате устройства в мрежата и да конфигурирате и управлявате устройствата. Можете да получите подробна информация за устройствата, например състояние и консумативи, да изпращате известия за предупреждения и да създавате отчет за използването на устройството. Можете също да направите шаблон, съдържащ елементи с настройки, и да го приложите за други устройства като споделени настройки. Можете да изтеглите Epson Device Admin от уеб сайта за поддръжка на Epson. За повече информация вижте документацията или помощта на Epson Device Admin.

### Изпълнение на Epson Device Admin (само за Windows)

Изберете **All Programs (Всички програми) > EPSON > Epson Device Admin > Epson Device Admin**.

**Забележка:**

Ако се появи предупреждение на защитната стена, разрешете достъпа за Epson Device Admin.

---

## EpsonNet Print

EpsonNet Print е софтуер за печат в TCP/IP мрежа. Възможностите и ограниченията са изброени по-долу.

- Състоянието на принтера се показва на екрана на спулера
- Ако IP адресът на принтера е променен от DHCP, принтерът все още се открива.
- Можете да използвате принтер, разположен на друг сегмент на мрежата.
- Можете да печатате, като използвате един от протоколите.
- IPv6 адрес не се поддържа.

---

## EpsonNet SetupManager

EpsonNet SetupManager е софтуер за създаване на пакет за лесна инсталация на принтера, като например инсталиране на драйвера на принтера, инсталиране на EPSON Status Monitor и създаване на порт за принтера. Този софтуер позволява на администратора да създава уникални софтуерни пакети и да ги разпределя между различни групи.

За повече информация посетете регионалния уеб сайт на Epson.