

Ръководство на администратора

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

Последователност на настройките и управление на скенера.	10
Примерна мрежова среда.	11
Представяне на пример за настройка на връзката на скенера.	11
Подготовка за свързване към мрежата.	12
Събиране на информация в настройката за свързване.	12
Спецификации на скенера.	13
Използване на номер на порт.	13
Тип назначаване на IP адрес.	13
DNS сървър и прокси сървър.	13
Метод за настройка на мрежова връзка.	13

Свързване

Свързване към мрежата.	15
Свързване към мрежата от контролния панел.	15
Свързване към мрежата с използване на програмата за инсталиране.	19

Настройки на функции

Софтуер за настройка.	22
Web Config (уебстраница за устройството).	22
Използване на функции за сканиране.	24
Сканиране от компютър.	24
Сканиране с помощта на контролния панел.	26
Настройки на системата.	28

Настройки на системата от контролния панел.	28
Настройки на системата чрез Web Config.	30

Основни настройки за сигурност

Въведение в основни настройки за сигурност.	32
Конфигуриране на администраторска парола.	33
Конфигуриране на администраторска парола от контролния панел.	33
Конфигуриране на администраторска парола с Web Config.	33
Елементи, които да бъдат заключени с администраторска парола.	34
Управляващи протоколи.	35
Протоколи, които можете да разрешите или забраните.	36
Елементи за настройка на протоколи.	37

Настройки за работа и управление

Проверка на информация на устройството.	40
Управление на устройства (Epson Device Admin).	40
Получаване на имейл известия при възникване на събития.	41
Относно известията по имейл.	41
Конфигуриране на известията по имейл.	41
Конфигуриране на сървър за електронна поща.	42
Проверка на връзката с пощенския сървър.	44
Обновяване на фърмуер.	46
Обновяване на фърмуера чрез Web Config.	46
Обновяване на фърмуера чрез използване на Epson Firmware Updater.	46
Архивиране на настройките.	47
Експортиране на настройки.	47
Импортиране на настройки.	47

Отстраняване на проблеми

Съвети за отстраняване на проблеми.	49
Проверка на регистъра за сървър и мрежово устройство.	49
Инициализиране на мрежовите настройки.	49
Възстановяване на мрежовите настройки от контролния панел.	49

Съдържание

Проверка на комуникацията между устройства и компютри.	49	Свързване на скенера към мрежа IEEE802.1X. . .	85
Проверка на връзката чрез команда Ping — Windows.	49	Конфигуриране на мрежа IEEE802.1X.	85
Проверка на връзката чрез команда Ping — Mac OS.	51	Конфигуриране на сертификата за IEEE802.1X.	86
Проблеми при използване на мрежов софтуер. . .	52	Решаване на проблеми за повишена защита. . . .	87
Няма достъп до Web Config.	52	Възстановяване на настройките за сигурност.	87
Името на модела и/или IP адресът не се показват на EpsonNet Config.	53	Проблеми при използване на функциите за мрежова сигурност.	88
		Проблеми при използване на цифров сертификат.	90
Приложение			
Въведение в мрежов софтуер.	55		
Epson Device Admin.	55		
EpsonNet Config.	55		
EpsonNet SetupManager.	56		
Присвояване на IP адрес с EpsonNet Config. . . .	56		
Присвояване на IP с партидни настройки. . . .	56		
Задаване на IP адрес за всяко устройство. . . .	59		
Използване на порт за скенера.	60		
Разширени настройки за сигурност за корпорации			
Настройки за сигурност и предпазване от опасност.	62		
Настройки на функции за сигурност.	63		
SSL/TLS комуникация със скенера.	63		
Относно цифрово сертифициране.	63		
Получаване и импортиране на сертификат, подписан от сертифициращ орган.	64		
Изтриване на сертификат, подписан от сертифициращ орган.	68		
Актуализиране на самоподписан сертификат.	68		
Конфигурирайте CA Certificate.	69		
Криптирана комуникация с IPsec/IP филтриране.	71		
Относно IPsec/IP Filtering.	71		
Конфигуриране на Default Policy.	72		
Конфигуриране на Group Policy.	75		
Примери за конфигурация на IPsec/IP Filtering.	81		
Конфигуриране на сертификат за IPsec/IP Filtering.	82		
Използване на SNMPv3 протокол.	83		
Относно SNMPv3.	83		
Конфигуриране на SNMPv3.	83		

Авторско право

Никоя част от тази публикация не може да се възпроизвежда, съхранява в система за обработка или да се прехвърля под каквато и да е форма или с каквито и да е средства — електронни, механични, фотокопиране, записване или по друг начин — без предварителното писмено разрешение от 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 в настоящия документ е предназначена само за използване с този продукт на Epson. Epson не носи отговорност за използването на тази информация по отношение на други продукти.

Нито Seiko Epson Corporation, нито нейните свързани дружества носят отговорност към купувача на този продукт или към трети страни за щети, загуби или разходи, понесени от купувача или от трети страни, в резултат на инцидент, неправилна употреба или злоупотреба с този продукт, или неупълномощени модификации, ремонти или промени на този продукт, или (с изключение на САЩ) липса на стриктно спазване на инструкциите за експлоатация и поддръжка на Seiko Epson Corporation.

Seiko Epson Corporation и нейните филиали не носят отговорност за повреди 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 повреди, възникнали в резултат на електромагнитни смущения, които възникват от употребата на интерфейсни кабели, различни от обозначените като одобрени от Epson продукти от Seiko Epson Corporation.

©Seiko Epson Corporation 2016.

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

Търговски марки

- ❑ EPSON® е регистрирана търговска марка, а EPSON EXCEED YOUR VISION или EXCEED YOUR VISION е търговска марка на Seiko Epson Corporation.
- ❑ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❑ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❑ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❑ Обща бележка: Другите имена на продукти, които се използват тук, са само за информация и е възможно да са търговски марки на съответните собственици. Epson не разполага с никакви права над тези марки.

Относно това ръководство

Знаци и символи



Внимание:

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



Важно:

Инструкции, които трябва да се съблюдават, за да се избегнат повреди на оборудването.

Забележка:

Инструкции, които съдържат полезни съвети и ограничения за работата на скенера.

Още по темата

➔ Щракването върху тази икона ще ви отведе до съответната информация.

Описания, използвани в това ръководство

- Екранните снимки от екраните на драйвера на скенера и екраните Epson Scan 2 (драйвер на скенера) са от Windows 10 или OS X El Capitan. Съдържанието, показано на екраните, варира в зависимост от модела и ситуацията.
- Илюстрациите, използвани в това ръководство, са само примерни. Въпреки че може да има малки разлики в зависимост от модела, методът на работа е същият.
- Някои от елементите на менюто на LCD екрана се различават в зависимост от модела и настройките.

Справки за операционните системи

Windows

В настоящото ръководство термини като „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Vista“, „Windows XP“, Windows Server 2016, „Windows Server 2012 R2“, „Windows Server 2012“, „Windows Server 2008 R2“, „Windows Server 2008“, „Windows Server 2003 R2“ и „Windows Server 2003“ се отнасят до следните операционни системи. В допълнение, „Windows“ се отнася към всички версии.

- Операционна система Microsoft® Windows® 10
- Операционна система Microsoft® Windows® 8.1
- Операционна система Microsoft® Windows® 8
- Операционна система Microsoft® Windows® 7
- Операционна система Microsoft® Windows Vista®
- Операционна система Microsoft® Windows® XP

Относно това ръководство

- Операционна система Microsoft® Windows® XP Professional x64 Edition
- Операционна система Microsoft® Windows Server® 2016
- Операционна система Microsoft® Windows Server® 2012 R2
- Операционна система Microsoft® Windows Server® 2012
- Операционна система Microsoft® Windows Server® 2008 R2
- Операционна система Microsoft® Windows Server® 2008
- Операционна система Microsoft® Windows Server® 2003 R2
- Операционна система Microsoft® Windows Server® 2003

Mac OS

В настоящето ръководство „Mac OS“ се отнася към macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x и Mac OS X v10.6.8.

Въведение

Ръчен компонент

Това ръководство е за администратора на устройството, който отговаря за свързването на принтера или скенера към мрежата, и съдържа информация как да се направят настройките за използване на функциите.

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

Подготовка

Описва задачите на администратора, как да настроят устройствата и софтуера за управление.

Свързване

Описва как да се свърже устройството към мрежата или към телефонна линия. Описва също и мрежовата среда, като например използването на порт за устройството, информация за DNS и прокси сървър.

Настройки на функции

Разяснява настройките за всяка функция на устройството.

Основни настройки за сигурност

Описва настройките за всяка функция, например печат, сканиране и факсове.

Настройки за работа и управление

Описва задачите след започване на използването на устройството, например информационна проверка и поддръжка.

Разрешаване на проблеми

Описва инициализацията на настройките и отстраняването на неизправности в мрежата.

Разширени настройки за сигурност за корпорации

Описва начина за настройка с цел подобряване на сигурността на устройството, например използване на сертификат на сертифициращ орган, SSL/TLS комуникация и IPsec/IP филтриране.

В зависимост от модела някои функции в тази глава не се поддържат.

Дефиниции на термините, използвани в това ръководство

В това ръководство са използвани следните термини.

Въведение

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 и скенери.

Web Config (уебстраницата на устройството)

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

Инструмент

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

Сканиране по заявка

Общ термин за сканиране от контролния панел на устройството.

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 е използвано „ASCII“, това показва 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 „UTF-8“ е използвано в това ръководство, то показва кодиране на символи в UTF-8 формат.

Подготовка

Тази глава описва ролята на администратора и подготовката преди настройките.

Последователност на настройките и управление на скенера

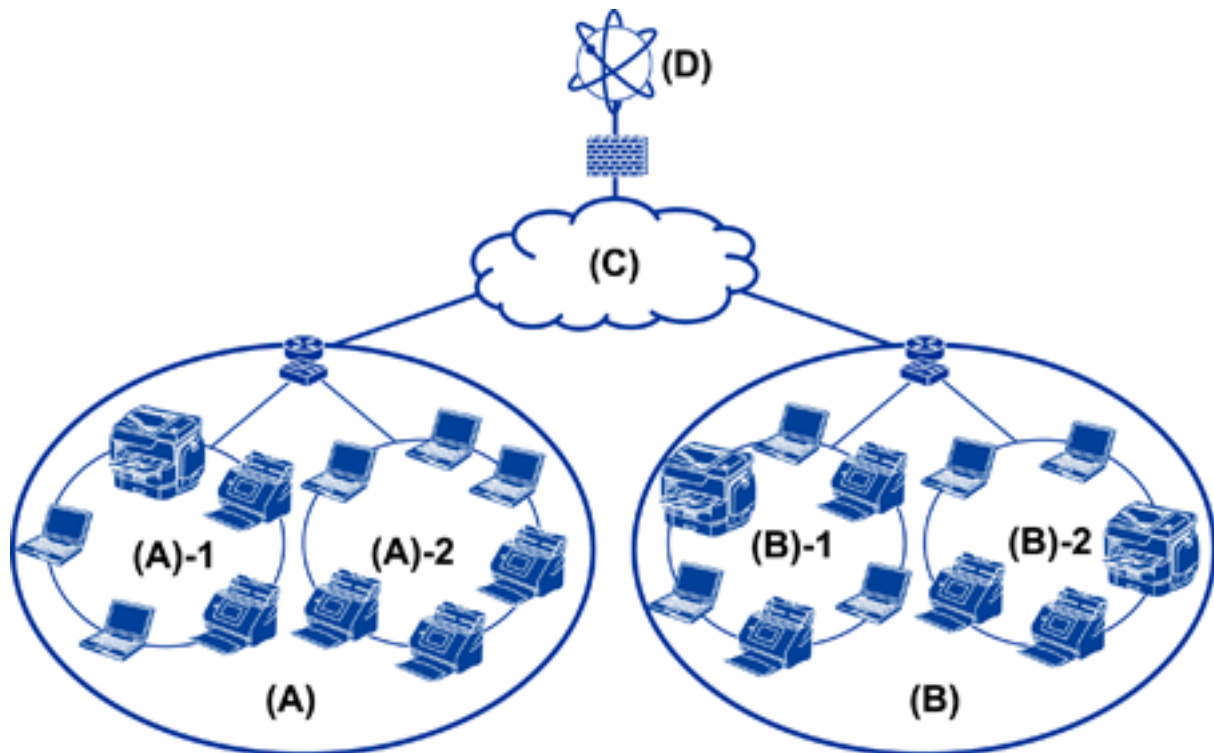
Администраторът прави настройките за мрежова връзка, първоначалната настройка и поддръжката на скенера, за да са достъпни за потребителите.

1. Подготовка
 - Събиране на информация за настройки на връзката
 - Решение за начин на свързване
2. Свързване
 - Мрежова връзка от контролния панел на скенера
3. Настройка на функциите
 - Настройка на драйвера на скенера
 - Други разширени настройки
4. Настройки за сигурност
 - Настройки на администратора
 - SSL/TLS
 - Управление на протоколи
 - Разширени настройки за сигурност (опция)
5. Работа и управление
 - Проверка на състоянието на устройството
 - Реакция при аварийни ситуации
 - Архивиране на настройките на устройството

Още по темата

- ➔ [“Подготовка” на страница 10](#)
- ➔ [“Свързване” на страница 15](#)
- ➔ [“Настройки на функции” на страница 22](#)
- ➔ [“Основни настройки за сигурност” на страница 32](#)
- ➔ [“Настройки за работа и управление” на страница 40](#)

Примерна мрежова среда



(A): офис 1

(A) – 1: LAN 1

(A) – 2: LAN 2

(B): офис 2

(B) – 1: LAN 1

(B) – 2: LAN 2

(C): WAN

(D): интернет

Представяне на пример за настройка на връзката на скенера

Основно има два типа връзки в зависимост от начина на използване на скенера. Свържете скенера към мрежата с компютъра чрез концентратора.

- Връзка сървър/клиент (скенер с помощта на сървър на Windows, управление на задания)
- Връзка тип „Peer to Peer“ (директна връзка чрез клиентски компютър)

Още по темата

- ➔ [“Връзка сървър/клиент” на страница 12](#)
- ➔ [“Връзка тип „Peer to Peer“” на страница 12](#)

Подготовка

Връзка сървър/клиент

Централизирано управление на скенер и задание с инсталиран Document Capture Pro Server на сървъра. Най-подходящо е за работа, която използва няколко скенера за сканиране на голям брой документи в конкретен формат.

Още по темата

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

Връзка тип „Peer to Peer“

Използвайте отделен скенер с драйвер за скенер като Epson Scan 2, инсталиран на клиентския компютър. Инсталирането на Document Capture Pro (Document Capture) на клиентския компютър ви позволява да извършвате задания на отделните клиентски компютри на скенера.

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.

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 за Ethernet връзка.
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 присвоявате автоматично чрез DHCP функцията и когато DNS сървърът не може да се зададе автоматично.
Информация за прокси сървър	<input type="checkbox"/> Име на прокси сървър <input type="checkbox"/> Номер на порт	Конфигурирайте, когато използвате прокси сървър за връзка с интернет и когато използвате услугата Epson Connect или функцията за автоматично обновяване на фърмуера.

Спецификации на скенера

Спецификациите, които скенерът поддържа стандартно или в режим на свързване, вижте *Ръководство на потребителя*.

Използване на номер на порт

Вижте „Приложение“ за номера на порта, който използва скенерът.

Още по темата

➔ [“Използване на порт за скенера” на страница 60](#)

Тип назначаване на IP адрес

Има два вида назначаване на IP адрес на скенера.

Статичен IP адрес:

Задаване на предварително определен уникален IP адрес на скенера.

IP адресът не се променя, дори при изключване на скенера или на маршрутизатора, затова можете да управлявате устройството по IP адрес.

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

Автоматично присвояване с DHCP функция:

Правилният IP адрес се присвоява автоматично, когато комуникацията между скенера 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.

DNS сървър и прокси сървър

Ако използвате услуга за интернет връзка, конфигурирайте DNS сървъра. Ако не го конфигурирате, трябва да укажете IP адрес за достъп, защото преобразуването на имена може да е неуспешно.

Прокси сървърът е поставен на шлюза между мрежата и интернет и комуникира с компютъра, скенера и интернет (срещуположен сървър) вместо всеки от тях. Срещуположният сървър комуникира само с прокси сървъра. Следователно, информацията за скенера, например IP адрес и номер на порт, не може да бъде прочетена и се очаква увеличена сигурност.

Можете да разрешите достъп до конкретен URL адрес, като използвате функцията за филтриране, защото прокси сървърът може да провери съдържанието на комуникацията.

Метод за настройка на мрежова връзка

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

Подготовка

Използване на контролния панел:

Конфигурирайте настройките за всеки скенер от контролния панел на скенера. Свържете към мрежата след конфигуриране на мрежовите настройки на скенера.

Използване на програма за инсталиране:

Ако се използва програма за инсталиране, мрежата на скенера и клиентският компютър се настройват автоматично. Настройката е възможна чрез следване на инструкциите на програмата за инсталиране дори ако нямате сериозни познания за мрежата.

Използване на инструмент:

Използвайте инструмент от компютъра на администратора. Можете да намерите скенера и после да го настроите или да създадете SYLK файл, за да направите партидни настройки на скенерите. Можете да настроите много скенери, но те трябва да са физически свързани с Ethernet кабел преди настройката. Затова се препоръчва да изградите Ethernet връзка за настройката.

Още по темата

- ➔ [“Свързване към мрежата от контролния панел” на страница 15](#)
- ➔ [“Свързване към мрежата с използване на програмата за инсталиране” на страница 19](#)
- ➔ [“Присвояване на IP адрес с EpsonNet Config” на страница 56](#)

Свързване

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

Свързване към мрежата

Свързване към мрежата от контролния панел

Свържете скенера към мрежа от контролния панел на скенера.

Относно контролния панел на скенера вижте *Ръководство на потребителя* за подробности.

Задаване на IP адрес

Настройка на основни елементи като IP адрес, Маска на подмрежата и Шлюз по подразбиране.

1. Включете скенера.
2. Плъзнете бързо наляво по екрана на контролния панел на скенера и докоснете **Настройки**.

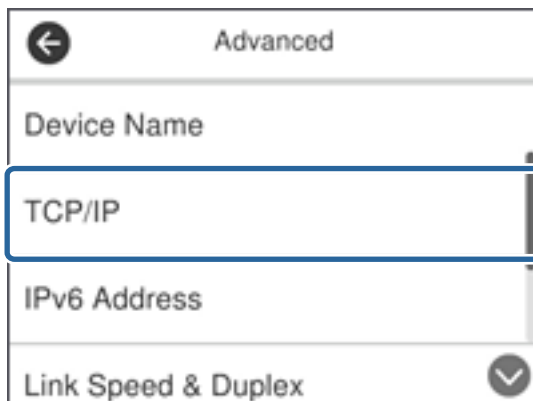


3. Докоснете **Настройки на мрежата > Промяна на настройки**.

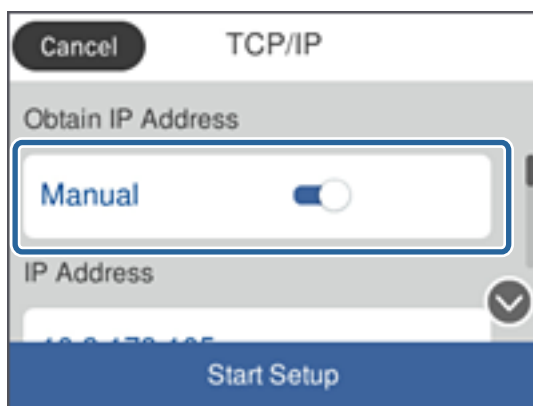
Ако елементът не се показва, плъзнете бързо по екрана нагоре, за да се покаже.

Свързване

4. Натиснете **TCP/IP**.



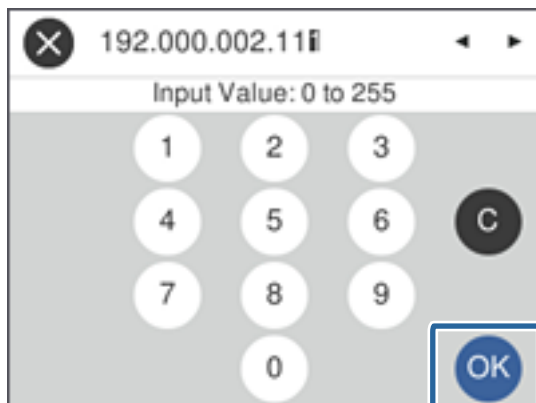
5. Изберете **Ръчно** за Получаване на IP адрес.



Забележка:

Когато зададете IP адреса автоматично чрез DHCP функцията на маршрутизатора, изберете **Автоматично**. В този случай IP адрес, Маска на подмрежата и Шлюз по подразбиране в стъпка 6 до 7 също се настройват автоматично, затова продължете към стъпка 8.

6. Докоснете полето **IP адрес**, въведете IP адреса, като използвате клавиатурата, показана на екрана, после докоснете **ОК**.



Потвърдете стойността от предишния екран.

Свързване

7. Настройте **Маска на подмрежата** и **Шлюз по подразбиране**.

Потвърдете стойността от предишния екран.

Забележка:

Ако комбинацията от IP адрес, Маска на подмрежата и Шлюз по подразбиране е неправилна, **Старт на настройката** не е активно и не можете да продължите с настройките. Проверете дали няма грешка при въвеждането.

8. Докоснете полето **Главен DNS за DNS сървър**, въведете IP адреса на първичния DNS сървър, като използвате клавиатурата, показана на екрана, после докоснете **ОК**.

Потвърдете стойността от предишния екран.

Забележка:

Когато изберете **Автоматично** за настройка за задаване на IP адрес, можете да изберете настройки на DNS сървъра от **Ръчно** или **Автоматично**. Ако не можете да получите адреса на DNS сървъра автоматично, изберете **Ръчно**, после въведете адреса на DNS сървъра. След това въведете директно адреса на вторичния DNS сървър. Ако изберете **Автоматично**, отидете на стъпка 10.

9. Докоснете полето **Вторичен DNS**, въведете IP адреса на вторичния DNS сървър, като използвате клавиатурата, показана на екрана, после докоснете **ОК**.

Потвърдете стойността от предишния екран.

10. Натиснете **Старт на настройката**.

11. Докоснете **Затвори** на екрана за потвърждение.

Екранът се затваря автоматично след определен период от време, ако не натиснете **Затвори**.

Свързване към Ethernet

Свържете скенера към мрежата с Ethernet кабел и проверете връзката.

1. Свържете скенера и концентратора (L2 превключвател) с Ethernet кабел.

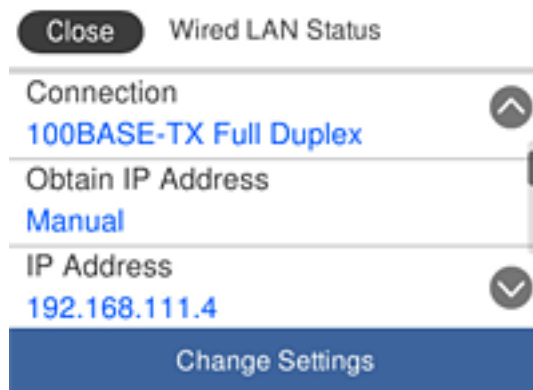
Иконата на началния екран се променя на .

2. Докоснете  от началния екран.



Свързване

- Плъзнете екрана нагоре и след това се уверете, че състоянието на връзката и IP адресът са правилни.



Настройка на прокси сървър

Прокси сървърът не може да бъде зададен на панела. Конфигурирайте чрез Web Config.

- Влезте в Web Config и изберете **Network Settings > Basic**.
- Изберете **Use** в **Proxy Server Setting**.
- Посочете прокси сървъра в IPv4 адрес или FQDN формат в **Прокси сървър**, след което въведете номера на порта в **Proxy Server Port Number**.

За прокси сървъри, които изискват удостоверяване, въведете потребителското име и паролата за удостоверяване на прокси сървър.

Свързване

4. Щракнете върху бутона **Next**.

The screenshot shows the EPSON Web Config interface for a printer. The left sidebar contains navigation options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Wired LAN', 'Basic', 'Email Server', 'Network Security Settings', 'Services', 'System Settings', 'Export and Import Setting Value', and 'Administrator Settings'. Under 'Basic Settings', 'DNS/Proxy Setup' is selected. The main content area displays various network configuration fields:

- Primary DNS Server : [text box]
- Secondary DNS Server : [text box]
- DNS Host Name Setting : Auto Manual
- DNS Host Name Status : Failed
- DNS Host Name : EPSON884045
- DNS Domain Name Setting : Auto Manual
- DNS Domain Name Status : Failed
- DNS Domain Name : [text box]
- Register the network interface address to DNS : Enable Disable
- Proxy Server Setting** : Do Not Use Use
- Proxy Server : www.sample.proxy
- Proxy Server Port Number : 80
- Proxy Server User Name : XXXXXXXX
- Proxy Server Password : [password field]
- IPv6 Setting : Enable Disable
- IPv6 Privacy Extension : Enable Disable
- IPv6 DHCP Server Setting : Do Not Use Use
- IPv6 Address : [text box]
- IPv6 Address Default Gateway : [text box]
- IPv6 Link-Local Address : fe80::9eae:d3ff:fe88:4045/64
- IPv6 Stateful Address : [text box]
- IPv6 Stateless Address 1 : [text box]
- IPv6 Stateless Address 2 : [text box]
- IPv6 Stateless Address 3 : [text box]
- IPv6 Primary DNS Server : [text box]
- IPv6 Secondary DNS Server : [text box]

A 'Next' button is located at the bottom of the configuration area.

5. Потвърдете настройките, след което щракнете върху **Настройки**.

Още по темата

- ➔ “Достъп до Web Config” на страница 23

Свързване към мрежата с използване на програмата за инсталиране

Препоръчваме ви да използвате програмата за инсталиране за свързване на скенера към компютър. Можете да стартирате програмата за инсталиране по един от следните методи.

- Инсталиране от уебсайта

Отидете на следния уебсайт и въведете името на продукта. Отидете на **Конфигуриране**, след което стартирайте инсталацията.

<http://epson.sn>

- Инсталиране от диска със софтуер (само за модели, които имат диск със софтуер и потребители с компютри с дискови устройства).

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

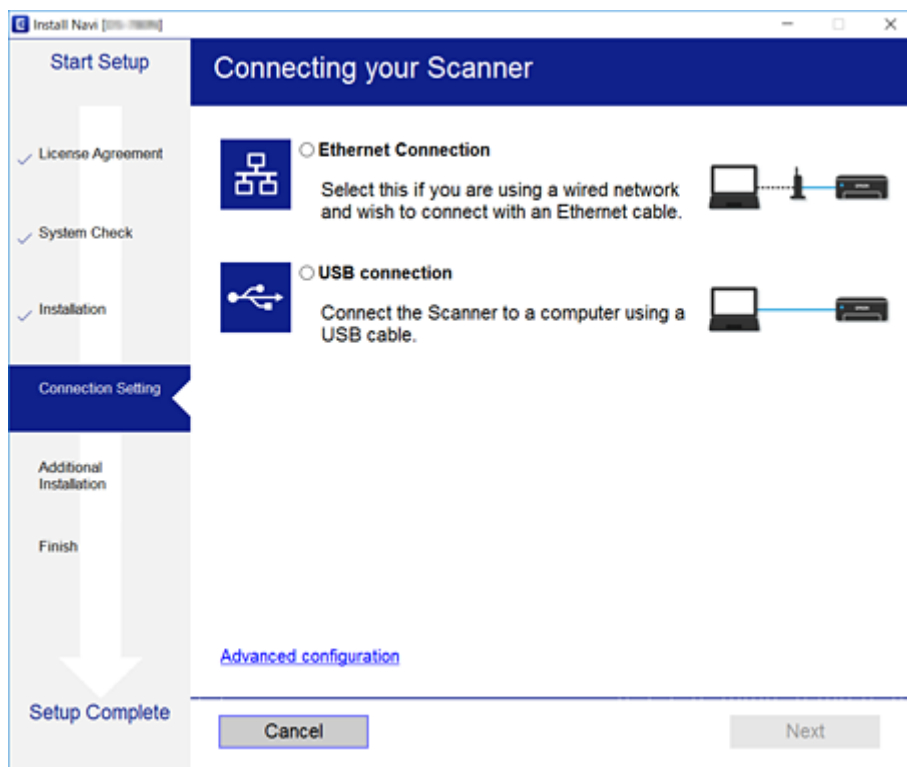
Свързване

Избор на начини за свързване

Следвайте инструкциите на екрана, докато се покаже следния екран, после изберете начина на свързване на скенера към компютър.

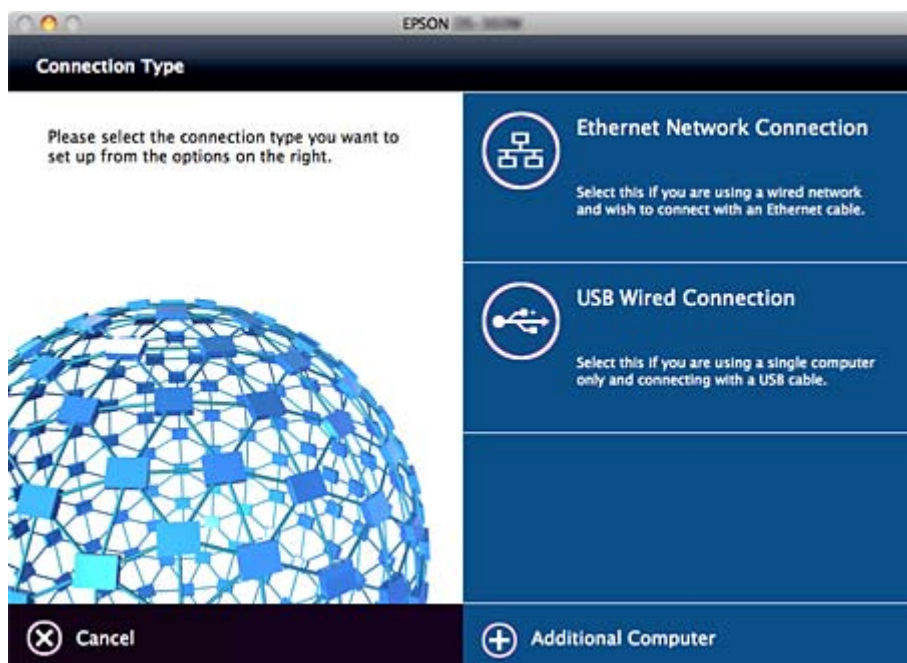
Windows

Изберете вида връзка, след което щракнете върху **Следващ**.



Mac OS

Изберете вида връзка.



Свързване

Следвайте инструкциите на екрана. Необходимият софтуер е инсталиран.

Настройки на функции

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

Софтуер за настройка

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

Web Config (уебстраница за устройството)

Относно Web Config

Web Config е браузър-базирано приложение за конфигуриране на настройките на скенера.

За достъп до Web Config трябва първо да имате присвоен IP адрес на скенера.

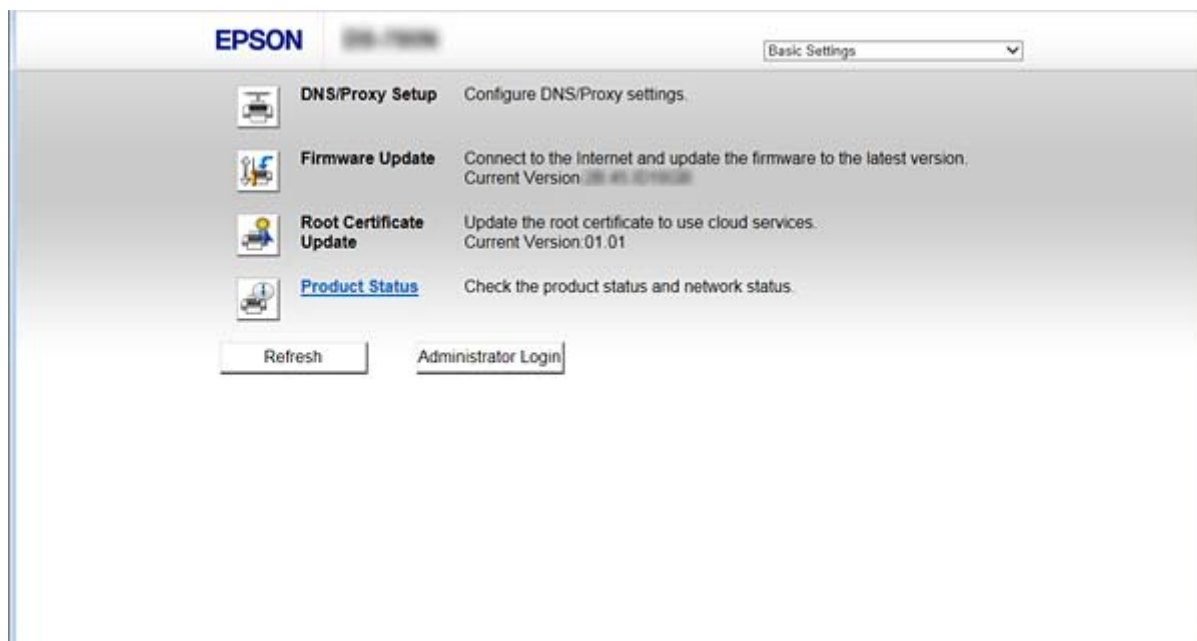
Забележка:

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

Има две страници за настройки като тези по-долу.

Basic Settings

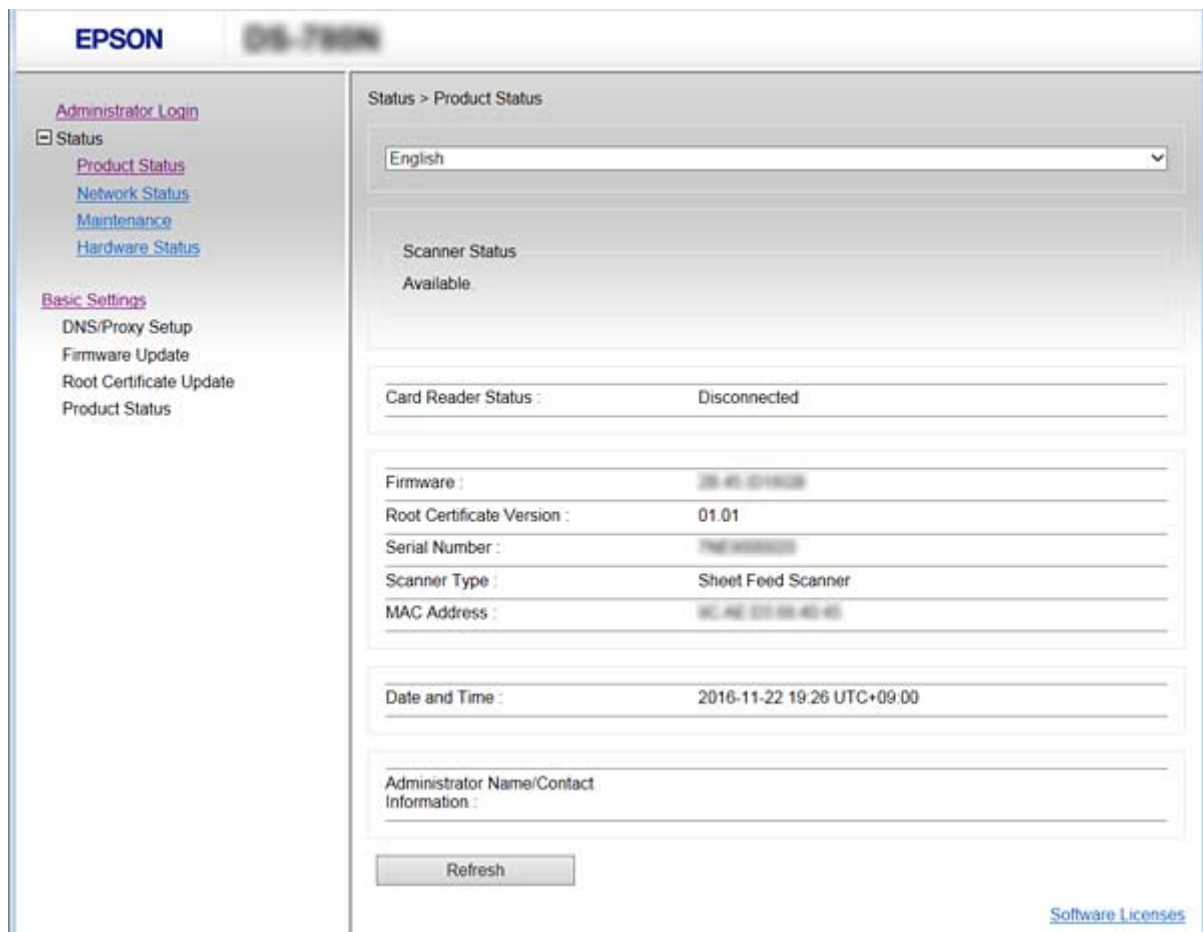
Можете да конфигурирате основните настройки за скенера.



Настройки на функции

❑ Advanced Settings

Можете да конфигурирате разширените настройки за скенера. Тази страница е основно за администратора.



Достъп до Web Config

Въведете IP адреса на скенера в уеббраузър. Трябва да е активиран JavaScript. При достъп до Web Config чрез HTTPS, в брауъра ще се появи предупредително съобщение, тъй като се използва самоподписан сертификат, запазен в скенера.

❑ Достъп чрез HTTPS

IPv4: <https://<IP адрес на скенера>> (без < >)

IPv6: [https://\[IP адрес на скенера\]/](https://[IP адрес на скенера]/) (с [])

❑ Достъп чрез HTTP

IPv4: <http://<IP адрес на скенера>> (без < >)

IPv6: [http://\[IP адрес на скенера\]/](http://[IP адрес на скенера]/) (с [])

Настройки на функции

Забележка:

Примери

IPv4:

<https://192.0.2.111/>

<http://192.0.2.111/>

IPv6:

[https://\[2001:db8::1000:1\]/](https://[2001:db8::1000:1]/)

[http://\[2001:db8::1000:1\]/](http://[2001:db8::1000:1]/)

- Ако името на скенера е регистрирано в DNS сървъра, можете да използвате името на скенера вместо IP адреса на скенера.

Още по темата

- ➔ [“SSL/TLS комуникация със скенера” на страница 63](#)
- ➔ [“Относно цифрово сертифициране” на страница 63](#)

Използване на функции за сканиране

В зависимост от начина на използване на скенера инсталирайте следния софтуер и извършете настройки с негова помощ.

Сканиране от компютър

- Потвърдете валидността на услугата за мрежово сканиране с Web Config (валидно при доставка от завода).
- Инсталирайте Epson Scan 2 на вашия компютър и задайте IP адреса
- При сканиране с помощта на задания инсталирайте Document Capture Pro (Document Capture) и задайте настройки на задания.

Сканиране от работния панел

- При използване на Document Capture Pro или Document Capture Pro Server:
Инсталирайте Document Capture Pro или Document Capture Pro Server
Настройка на DCP (режим на сървър, режим на клиента).
- При използване на WSD протокол:
Потвърдете валидността на WSD на Web Config или на работния панел (валидно при доставка от завода)
Допълнителни настройки на устройството (компютър с Windows).

Сканиране от компютър

Инсталирайте софтуера и проверете дали услугата за мрежово сканиране е активирана за сканиране чрез мрежа от компютъра.

Още по темата

- ➔ [“Софтуер за инсталиране” на страница 25](#)
- ➔ [“Разрешаване на мрежово сканиране” на страница 25](#)

Настройки на функции

Софтуер за инсталиране

Epson Scan 2

Това е драйвер на скенера. Ако използвате устройството от компютър, инсталирайте драйвера на всеки клиентски компютър. Ако е инсталиран Document Capture Pro/Document Capture, можете да изпълните операциите, присвоени на бутоните на устройството.

С EpsonNet SetupManager драйверите на принтера могат също да бъдат разпространени заедно в пакети.

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

Инсталирайте на клиентския компютър. Можете да извиквате и да изпълнявате задачи, регистрирани на компютър с инсталиран Document Capture Pro/Document Capture на мрежата, от работния панел на компютъра и скенера.

Можете също да сканирате от компютъра през мрежата. За сканиране се изисква Epson Scan 2.

Още по темата

➔ [“EpsonNet SetupManager” на страница 56](#)

Задаване на IP адреса на скенера на Epson Scan 2



Посочете IP адреса на скенера, така че скенерът да може да се използва на мрежата.

1. Стартирайте **Epson Scan 2 Utility** от **Старт > Всички програми > EPSON > Epson Scan 2**.

Ако вече има регистриран друг скенер, отидете на стъпка 2.

Ако не е регистриран, отидете на стъпка 4.

2. Щракнете върху ▼ на **Скенер**.
3. Щракнете върху **Настройки**.
4. Щракнете върху **Активиране на редакция**, след което щракнете върху **Добавяне**.
5. Изберете името на модела на скенера от **Модел**.
6. Изберете IP адреса на скенера, който ще използвате, от **Адрес в Търсене на мрежа**.

Щракнете върху  и щракнете върху , за да актуализирате списъка. Ако не можете да намерите IP адреса на скенера, изберете **Въведете адрес** и въведете IP адреса.

7. Щракнете върху **Добавяне**.
8. Щракнете върху **ОК**.

Разрешаване на мрежово сканиране

Можете да настроите услугата за мрежово сканиране, когато сканирате от клиентски компютър по мрежата. Настройката по подразбиране е разрешена.

1. Отворете Web Config и изберете **Services > Network Scan**.

Настройки на функции

- Уверете се, че сте избрали **Enable scanning** в **EPSON Scan**.
Ако е избрано, тази задача е завършена. Затворете Web Config.
Ако е изчистен, изберете го и преминете към следващата стъпка.
- Щракнете върху **Next**.
- Щракнете върху **OK**.
Мрежата се свързва отново, след което настройката се разрешава.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)

Сканиране с помощта на контролния панел

Функцията за сканиране в папка и функцията за сканиране към имейл чрез контролния панел на скенера, както и прехвърлянето на резултати от сканиране към имейл, папки и т.н., се извършват чрез изпълнение на задание от компютъра.

Когато прехвърляте резултати от сканиране, задайте заданието с Document Capture Pro Server или Document Capture Pro.

За подробности относно настройки и конфигуриране на заданието вижте документацията или помощта за Document Capture Pro Server или Document Capture Pro.

Още по темата

- ➔ [“Настройки на Document Capture Pro Server/Document Capture Pro” на страница 26](#)
- ➔ [“Настройка на сървъри и папки” на страница 27](#)

Софтуер за инсталиране на компютъра

Document Capture Pro Server

Това е версията на сървъра на Document Capture Pro. Инсталирайте го на сървъра на Windows. Множество устройства и задания могат да се управляват централно от сървъра. Заданията могат да се изпълняват едновременно от няколко скенера.

С помощта на сертифицирана версия на Document Capture Pro Server можете да управлявате хронологията на задания и сканиране, свързана към потребители и групи.

За подробности за Document Capture Pro Server се свържете с вашия местен офис на Epson.

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

Точно както при сканирането от компютър, можете да извиквате задания, регистрирани на компютъра от контролния панел, и да ги изпълнявате. Не е възможно да изпълнявате едновременно задания на компютър от няколко скенера.

Настройки на Document Capture Pro Server/Document Capture Pro

Извършете настройки с помощта на функцията за сканиране от работния панел на скенера.

- Влезте в Web Config и изберете **Services > Document Capture Pro**.

Настройки на функции

2. Изберете **Режим на работа**.

Server Mode:

Изберете това чрез Document Capture Pro Server или когато използвате Document Capture Pro само за задания, които са били конфигурирани за конкретен компютър.

Client Mode:

Задайте тази функция, когато изберете настройката за заданието на Document Capture Pro (Document Capture), инсталиран на всеки клиентски компютър в мрежата без посочване на компютъра.

3. Задайте следното в съответствие с избрания режим.

Server Mode:

В **Server Address** посочете сървъра, на който е инсталиран Document Capture Pro Server. Може да бъде между 2 и 252 знака във формат IPv4, IPv6, име на хост или FQDN. Във формат FQDN могат да се използват US-ASCII букви, цифри, букви и тирета (освен начални и крайни).

Client Mode:

Посочете **Group Settings**, за да използвате група от скенери, посочени от Document Capture Pro (Document Capture).

4. Щракнете върху **Настройки**.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Настройка на сървъри и папки

Document Capture Pro и Document Capture Pro Server запазват веднъж сканираните данни към сървъра или клиентския компютър и използват функцията за прехвърляне за изпълнение на функцията за сканиране в папка и функцията за сканиране към имейл.

Имате нужда от оторизация и информация за прехвърляне от компютъра, на който е инсталирано Document Capture Pro, Document Capture Pro Server към компютъра или облачната услуга.

Подгответе информацията на функцията, която ще използвате, отнасяща се до следното.

Можете да извършвате настройки за тези функции чрез Document Capture Pro или Document Capture Pro Server. За подробности относно настройките вижте документацията или помощта за Document Capture Pro Server или Document Capture Pro.

Име	Настройки	Изискване
Папка за сканиране към мрежата (SMB)	Създайте и настройте споделянето на папката за запис	Административен потребителски акаунт на компютъра, който създава папки за запис.
	Местоназначение на папка за сканиране към мрежата (SMB)	Потребителско име и парола за влизане в компютъра, който има папка за запис и права за обновяване на папката за запис.
Папка за сканиране към мрежата (FTP)	Настройка за влизане в FTP сървър	Информация за вход в FTP сървъра и права за обновяване на папката за запис.

Настройки на функции

Име	Настройки	Изискване
Сканиране към имейл	Настройка на имейл сървър	Информация за настройка на имейл сървър
Сканиране към Document Capture Pro (при използване на Document Capture Pro Server)	Настройка за влизане в облачни услуги	Среда с интернет връзка Регистриране на акаунт за облачни услуги

Използване на сканиране с WSD (само за Windows)

Ако компютърът използва Windows Vista или по-нова версия, можете да използвате сканиране с WSD.

Когато WSD протоколът може да се използва, менюто **Компютър (WSD)** ще бъде изведено на контролния панел на скенера.



1. Влезте в Web Config и изберете **Services > Protocol**.
2. Потвърдете, че е поставена отметка на **Enable WSD** в **WSD Settings**.
Ако е поставена отметка, вашата задача е завършена и можете да затворите Web Config.
Ако не е поставена отметка, поставете я и продължете към следващата стъпка.
3. Щракнете върху бутона **Next**.
4. Потвърдете настройките, след което щракнете върху **Настройки**.

Настройки на системата

Настройки на системата от контролния панел

Настройка на яркостта на екрана

Задайте яркостта на LCD екрана.

1. Докоснете **Настройки** от началния екран.
2. Докоснете **Общи настройки > Яркост на LCD**.
3. Докоснете  или , за да регулирате яркостта.
Можете да регулирате от 1 до 9.
4. Натиснете **ОК**.

Настройка на звука

Задаване на звук на работата на панела и звук при грешка.

Настройки на функции

1. Докоснете **Настройки** от началния екран.
2. Докоснете **Общи настройки > Звук**.
3. Задайте следните елементи според необходимостта.
 - Звук по време на работа
Задайте силата на звука по време на работа на работния панел.
 - Звук при грешка
Задайте силата на звука при грешка.
4. Натиснете **ОК**.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Разпознаване на двойно подаване на оригинал

Определете функцията за разпознаване на двойно подаване на документа за сканиране и за спиране сканирането при възникването на подаване на много документи.

За сканиране на оригинали, които се считат за подаване на няколко листа като пликове или хартия със стикери, задайте ги на изключени.

Забележка:

Може да се зададе и от Web Config или Epson Scan 2.

1. Докоснете **Настройки** от началния екран.
2. Докоснете **Външни Настройки за сканиране > Откр. на двойно подав..**
3. Докоснете **Откр. на двойно подав.**, за да го включите или изключите.
4. Натиснете **Затвори**.

Настройка на режим на ниска скорост

Задайте сканиране на ниска скорост, така че да не възниква засядане на хартия при сканиране на тънки документи като пликове.

1. Докоснете **Настройки** от началния екран.
2. Докоснете **Външни Настройки за сканиране > Бавно**.
3. Докоснете **Бавно**, за да го включите или изключите.
4. Натиснете **Затвори**.

Настройки на системата чрез Web Config

Настройки за енергоспестяване при неактивност

Направете настройка за енергоспестяване при период на неактивност на скенера. Задайте времето в зависимост от средата на използване.

Забележка:

Можете също да извършите настройки за енергоспестяване на контролния панел на скенера.

1. Влезте в Web Config и изберете **System Settings > Power Saving**.
2. Въведете време за **Sleep Timer**, за да превключвате в режим на енергоспестяване в момент на неактивност.
Можете да зададете до 240 минути.
3. Изберете времето за изключване за **Power Off Timer**.
4. Щракнете върху **ОК**.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Настройка на контролен панел

Настройка на контролния панел на скенера. Можете да настроите както следва.

1. Влезте в Web Config и изберете **System Settings > Control Panel**.
2. Задайте следните елементи според необходимостта.
 - Language
Изберете показания език на контролния панел.
 - Panel Lock
Ако изберете **ON**, се изисква администраторска парола при изпълнение на операция, която изисква административни права. Ако не е настроена администраторска парола, заключването на панела е дезактивирано.
 - Operation Timeout
Ако изберете **ON**, когато влезете като администратор, сесията ви автоматично приключва и се връщате в началния екран, ако няма активност за определен период от време.
Можете да зададете между 10 секунди и 240 минути с точност до секунда.
3. Щракнете върху **ОК**.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Настройки на функции

Настройка на ограничения за външен интерфейс

Можете да ограничите USB връзката от компютъра. Задайте, за да ограничите сканирането, различно от това през мрежа.

1. Влезте в Web Config и изберете **System Settings > External Interface**.
2. Изберете **Enable** или **Disable**.
За ограничаване изберете **Disable**.
3. Натиснете **ОК**.

Синхронизиране на дата и час със сървър за време

Ако използвате сертификат на сертифициращ орган, можете да предотвратите проблеми с времето.

1. Влезте в Web Config и изберете **System Settings > Date and Time > Time Server**.
2. Изберете **Use** за **Use Time Server**.
3. Въведете адреса на сървъра за време в **Time Server Address**.
Можете да използвате формат IPv4, IPv6 или FQDN. Въведете 252 символа или по-малко. Ако не укажете това, го оставете празно.
4. Въведете **Update Interval (min)**.
Можете да зададете до 10 800 минути.
5. Щракнете върху **ОК**.
Забележка:
Можете да потвърдите състоянието на връзката със сървъра за време в **Time Server Status**.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Основни настройки за сигурност

Тази глава описва основни настройки за сигурност, които не изискват специална среда.

Въведение в основни настройки за сигурност

Представяме основните настройки за сигурност на устройствата Epson.

Име на функция	Тип функция	Какво да се настрои	Какво да се предотврати
Настройка на администраторска парола	Заклучете настройките, които се отнасят до системата, като например настройки на мрежа и USB връзка, така че да не могат да се променят, освен от администратора.	Администраторът задава парола на устройството. Конфигуриране или актуализация са налични навсякъде от Web Config, контролния панел, Epson Device Admin и EpsonNet Config.	Предпазва от неупълномощено прочитане и промяна на информацията, записана в устройството, например ИД, парола, мрежови настройки и контакти. Освен това, намалява много рисковете за сигурността, например изтичане на информация за мрежовата среда или политики за сигурност.
SSL/TLS комуникация	При достъп до сървър на Epson в интернет от устройство като комуникация с компютър чрез актуализация на браузър или фърмуер комуникационното съдържание се криптира чрез SSL/TLS комуникация.	Получаване на подписан от сертифициращ орган сертификат и импортиране на скенера.	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.
Протоколи за управление	Протоколи за управление, използвани за комуникация между устройства и компютри и активира/дезактивира функции.	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.

Още по темата

- ➔ [“Относно Web Config” на страница 22](#)
- ➔ [“EpsonNet Config” на страница 55](#)
- ➔ [“Epson Device Admin” на страница 55](#)
- ➔ [“Конфигуриране на администраторска парола” на страница 33](#)
- ➔ [“Управляващи протоколи” на страница 35](#)

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 да промените администраторската парола, като използвате Web Config, контролния панел на скенера или софтуера (Epson Device Admin или EpsonNet Config). Когато използвате софтуера, вижте документацията за всеки от тях.

Още по темата

- ➔ [“Конфигуриране на администраторска парола от контролния панел” на страница 33](#)
- ➔ [“Конфигуриране на администраторска парола с Web Config” на страница 33](#)
- ➔ [“EpsonNet Config” на страница 55](#)
- ➔ [“Epson Device Admin” на страница 55](#)

Конфигуриране на администраторска парола от контролния панел

Можете да настроите администраторската парола от контролния панел на скенера.

1. Докоснете **Настройки** от началния екран.
2. Докоснете **Системна администрация > Администраторски настройки**.
Ако елементът не се показва, плъзнете бързо по екрана нагоре, за да се покаже.
3. Докоснете **Администраторска парола > Регистрация**.
4. Въведете паролата, след което докоснете **ОК**.
5. Въведете паролата отново, след което докоснете **ОК**.
6. Докоснете **ОК** на екрана за потвърждение.
Показва се екранът с административни настройки.
7. Докоснете **Заклучване на настройка**, после докоснете **ОК** на екрана за потвърждение.
Заклучване на настройка е настроен на **Вкл.** и административната парола ще се изисква, когато работите с елемент от заключено меню.

Забележка:

- Ако настроите **Настройки > Общи настройки > Интервал за операцията** на **Вкл.**, скенерът ще прекрати сесията ви след период на неактивност на контролния панел.
- Можете да промените или да изтриете администраторската парола, когато изберете **Промяна** или **Нулиране** в екрана **Администраторска парола** и въведете администраторската парола.

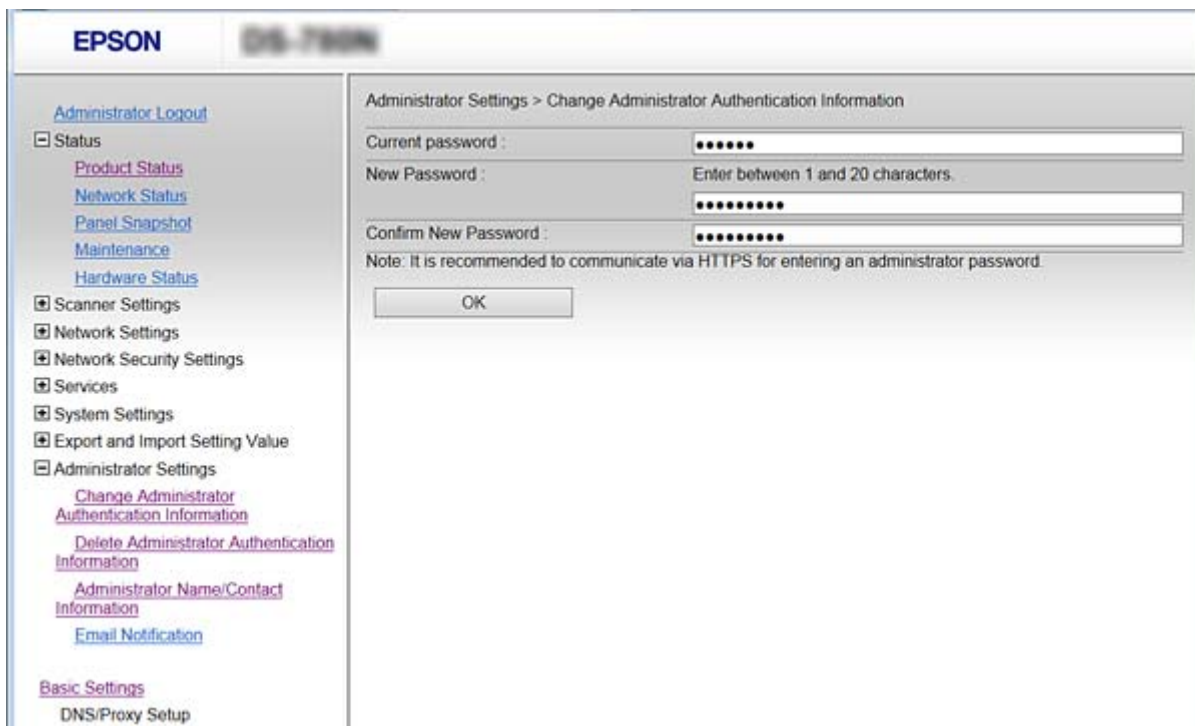
Конфигуриране на администраторска парола с Web Config

Можете да зададете администраторската парола от Web Config.

Основни настройки за сигурност

1. Влезте в Web Config и изберете **Administrator Settings > Change Administrator Authentication Information**.
2. Въведете парола в **New Password** и **Confirm New Password**. Въведете потребителско име, ако е необходимо.

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



3. Изберете **ОК**.

Забележка:

- За да настроите или промените заключените елементи в менюто, щракнете върху **Administrator Login**, после въведете администраторската парола.
- За да изтриете администраторската парола, щракнете върху **Administrator Settings > Delete Administrator Authentication Information** и след това въведете администраторската парола.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)

Елементи, които да бъдат заключени с администраторска парола

Администраторите имат права за настройка и промяна на всички функции в устройството.

Също така, ако зададете администраторската парола на устройството, можете да го заключите, за да не променят елементи, свързани с управлението на устройството.

Администраторът може да управлява следните елементи.

Основни настройки за сигурност

Елемент	Описание
Настройка на скенер	Задаване на разпознаване на двойно подаване и режим на ниска скорост.
Настройки за Ethernet връзка	Промяна на името на устройствата и IP адрес, настройка на DNS или прокси сървър и промяна на настройки, свързани с мрежови връзки.
Настройка на услуги за потребители	Настройка за управление на комуникационни протоколи, сканиране на мрежата и услуги Document Capture Pro.
Настройка на имейл сървър	Настройка на имейл сървър, с който устройствата комуникират директно.
Настройка за сигурност	Настройки за мрежова сигурност, например SSL/TLS комуникация, IPsec/IP филтриране и IEEE802.1X.
Актуализиране на основен сертификат	Актуализирането на основните сертификати е необходимо за удостоверяване на Document Capture Pro Server и за актуализиране на фърмуера от Web Config.
Актуализация на фърмуер	Проверка и актуализация на фърмуера на устройствата.
Таймер, настройка на таймер	Време за преминаване в режим на заспиване, автоматично изключване, дата/час, таймер за неактивност, други настройки на таймера.
Възстановяване на настройките по подразбиране	Настройка за връщане на фабричните настройки на скенера.
Настройка на администратора	Настройка на административно заключване или администраторска парола.
Настройка за сертифицирано устройство	ИД настройка на удостоверяващото устройство. Настройте, ако използвате скенера на система за удостоверяване, която поддържа удостоверяващи устройства.

Управляващи протоколи

Можете да сканирате, като използвате разнообразни пътища и протоколи. Можете също да използвате мрежово сканиране от неопределен брой компютри в мрежа. Например, позволено е сканиране с помощта само на определени пътища и протоколи. Можете да намалите случайните рискове за сигурността, като ограничите сканирането от определени пътища или чрез управление на достъпните функции.

Конфигурирайте настройките на протоколите.

1. Влезте в Web Config и изберете **Services > Protocol**.
2. Конфигурирайте всеки елемент.
3. Щракнете върху **Next**.
4. Щракнете върху **OK**.

Настройките се прилагат за скенера.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Основни настройки за сигурност

- ➔ [“Протоколи, които можете да разрешите или забраните”](#) на страница 36
- ➔ [“Елементи за настройка на протоколи”](#) на страница 37

Протоколи, които можете да разрешите или забраните

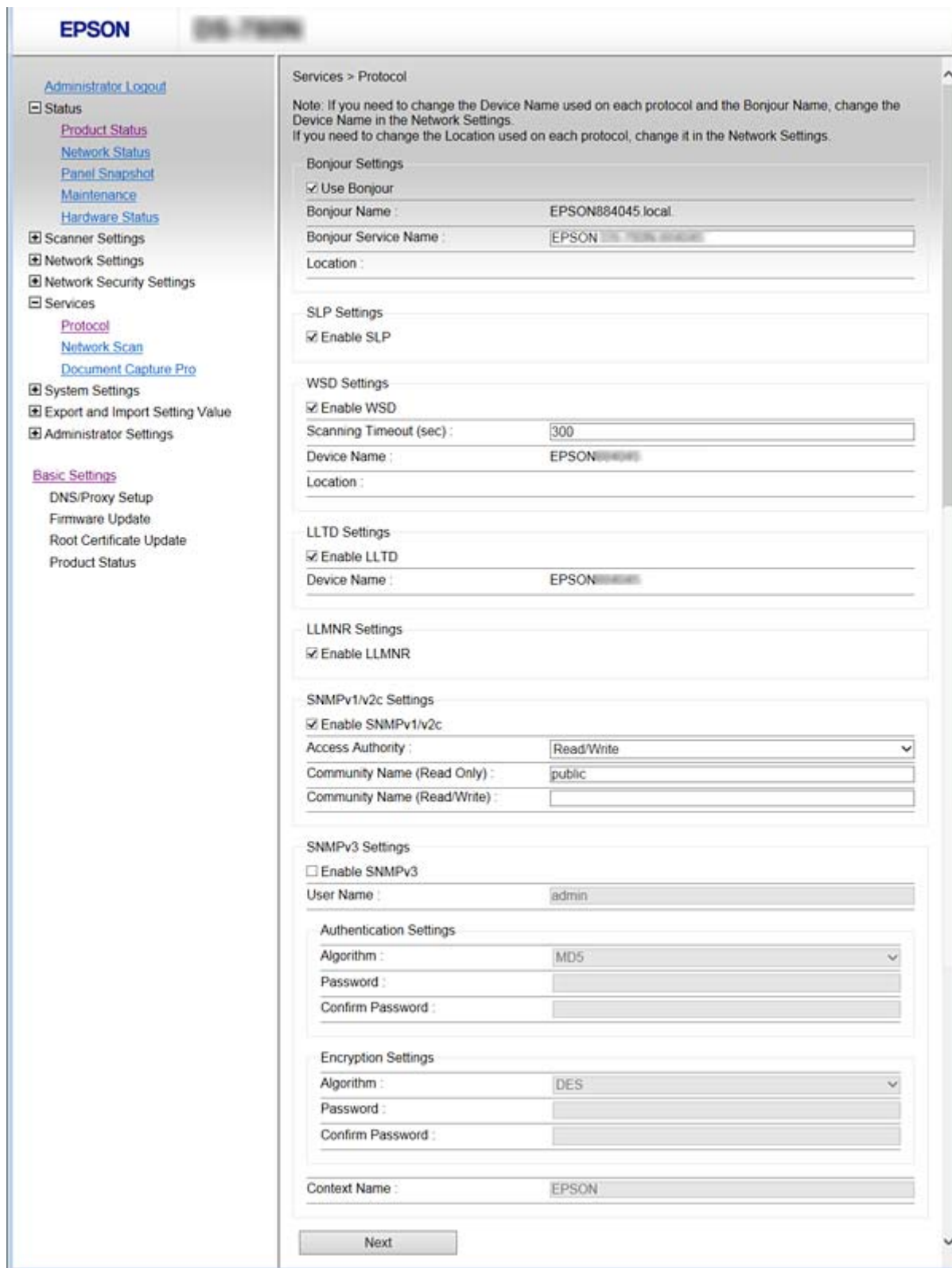
Протокол	Описание
Bonjour Settings	Можете да посочите дали да се използва Bonjour. Bonjour се използва за търсене на устройства, сканиране и др.
SLP Settings	Можете да разрешите или забраните функцията SLP. SLP се използва за Epson Scan 2 и мрежово търсене в EpsonNet Config.
WSD Settings	Можете да разрешите или забраните WSD функцията. Когато тя е разрешена, можете да добавите WSD устройства или да сканирате от порта WSD.
LLTD Settings	Можете да разрешите или забраните функцията LLTD. Когато тя е разрешена, тя е видима в картата на мрежата Windows.
LLMNR Settings	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.
SNMPv1/v2c Settings	Можете да посочите дали да активирате или не SNMPv1/v2c. Тази опция се използва за настройка на устройства, мониторинг и други.
SNMPv3 Settings	Можете да посочите дали да активирате или не SNMPv3. Тази опция се използва за настройка на криптирани устройства, следене и други.

Още по темата

- ➔ [“Управляващи протоколи”](#) на страница 35
- ➔ [“Елементи за настройка на протоколи”](#) на страница 37

Основни настройки за сигурност

Елементи за настройка на протоколи



Елементи	Стойност на настройка и описание
Bonjour Settings	

Основни настройки за сигурност

Елементи	Стойност на настройка и описание
Use Bonjour	Изберете тази опция за търсене на или използване на устройства чрез Bonjour.
Bonjour Name	Показва името Bonjour.
Bonjour Service Name	Можете да изведете и зададете името на услугата Bonjour.
Location	Показва името на местоположението Bonjour.
SLP Settings	
Enable SLP	Изберете тази опция, за да разрешите функция SLP. Използва се за откриване на мрежа в Epson Scan 2 и EpsonNet Config.
WSD Settings	
Enable WSD	Изберете тази опция, за да активирате добавяне на устройства чрез WSD и да печатате и сканирате от WSD порта.
Scanning Timeout (sec)	Въведете стойност за време за изчакване на комуникацията при WSD сканиране между 3 и 3600 секунди.
Device Name	Показва името на WSD устройството.
Location	Показва името на местоположението WSD.
LLTD Settings	
Enable LLTD	Изберете тази опция за разрешаване на LLTD. Скенерът е показан в Windows карта на мрежата.
Device Name	Показва името на LLTD устройството.
LLMNR Settings	
Enable LLMNR	Изберете тази опция за разрешаване на LLMNR. Можете да използвате преобразуване на имена без NetBIOS, дори и да не можете да използвате DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Изберете, за да разрешите SNMPv1/v2c. Показани са само скенери, които поддържат SNMPv3.
Access Authority	Задайте оторизация на достъпа, когато е разрешена опцията SNMPv1/v2c. Изберете Read Only или Read/Write .
Community Name (Read Only)	Въведете от 0 до 32 ASCII (0x20 до 0x7E) символа.
Community Name (Read/Write)	Въведете от 0 до 32 ASCII (0x20 до 0x7E) символа.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 е разрешен, когато е поставена отметката.
User Name	Въведете между 1 и 32 знака с помощта на 1-байтови символи.
Authentication Settings	

Основни настройки за сигурност

Елементи	Стойност на настройка и описание
Algorithm	Изберете алгоритъм за удостоверяване на SNMPv3.
Password	Въведете паролата за удостоверяване на SNMPv3. Въведете между 8 и 32 знака в ASCII (0x20 – 0x7E). Ако не укажете това, го оставете празно.
Confirm Password	Въведете паролата, която сте конфигурирали, за потвърждение.
Encryption Settings	
Algorithm	Изберете алгоритъм за криптиране на SNMPv3.
Password	Въведете паролата за криптиране на SNMPv3. Въведете между 8 и 32 знака в ASCII (0x20 – 0x7E). Ако не укажете това, го оставете празно.
Confirm Password	Въведете паролата, която сте конфигурирали, за потвърждение.
Context Name	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 35
- ➔ [“Протоколи, които можете да разрешите или забраните”](#) на страница 36

Настройки за работа и управление

Тази глава описва елементите, свързани с ежедневните операции и поддръжка на устройството.

Проверка на информация на устройството

Можете да проверите следната информация на работещо устройство от **Status**, като използвате Web Config.

Product Status

Проверете езика, състоянието, номера на продукта, MAC адреса и др.

Network Status

Проверете информацията за състоянието на мрежовата връзка, IP адрес, DNS сървър и др.

Panel Snapshot

Показване на снимка на екрана, показан на контролния панел на устройството.

Maintenance

Проверете началната дата, информацията за сканиране и т.н.

Hardware Status

Проверете състоянието на скенера.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Управление на устройства (Epson Device Admin)

Можете да управлявате и да работите с множество устройства от Epson Device Admin. Epson Device Admin ви позволява да управлявате устройства, разположени в различни мрежи. Следното описва основните функции за управление.

За повече информация за функциите и използването на софтуера вижте документацията или помощта на Epson Device Admin.

Откриване на устройства

Можете да откривате устройства в мрежата и после да ги регистрирате в списък. Ако Epson устройства, например принтери и скенери, са свързани към същия мрежов сегмент като компютъра на администратора, можете да ги намерите дори ако нямат присвоен IP адрес.

Можете също да откриете устройства, които са свързани към компютри в мрежата с USB кабели. Трябва да инсталирате Epson Device USB Agent на компютъра.

Настройка на устройства

Можете да направите шаблон, съдържащ елементи с настройки, например мрежов интерфейс и източник на хартия и да го приложите за други устройства като споделени настройки. Когато е свързан към мрежата, можете да присвоите IP адрес на устройство, което няма такъв.

Настройки за работа и управление

Следене на устройства

Можете редовно да извличате състоянието и подробна информация за устройствата в мрежата. Можете да следите устройства, които са свързани към компютри в мрежата с USB кабели, и устройства от други производители, които са регистрирани в списъка с устройства. За да наблюдавате устройства, свързани с USB кабели, трябва да инсталирате Epson Device USB Agent.

Управление на предупреждения

Можете да следите предупрежденията за състоянието на устройствата и консумативите. Системата автоматично изпраща известия по имейл на администратора според настроените условия.

Управление на отчети

Можете да създавате редовни отчети с натрупването на данни в системата за използването на устройството и консумативите. След това можете да запишете тези създадени отчети и да ги изпратите по имейл.

Още по темата

➔ [“Epson Device Admin” на страница 55](#)

Получаване на имейл известия при възникване на събития

Относно известяванията по имейл

Можете да използвате тази функция, за да получавате предупреждения по имейл, когато се случи дадено събитие. Можете да регистрирате до 5 имейл адреса и да изберете за кои събития искате да получавате известявания.

Имейл сървърът трябва да е конфигуриран за използване на тази функция.

Още по темата

➔ [“Конфигуриране на сървър за електронна поща” на страница 42](#)

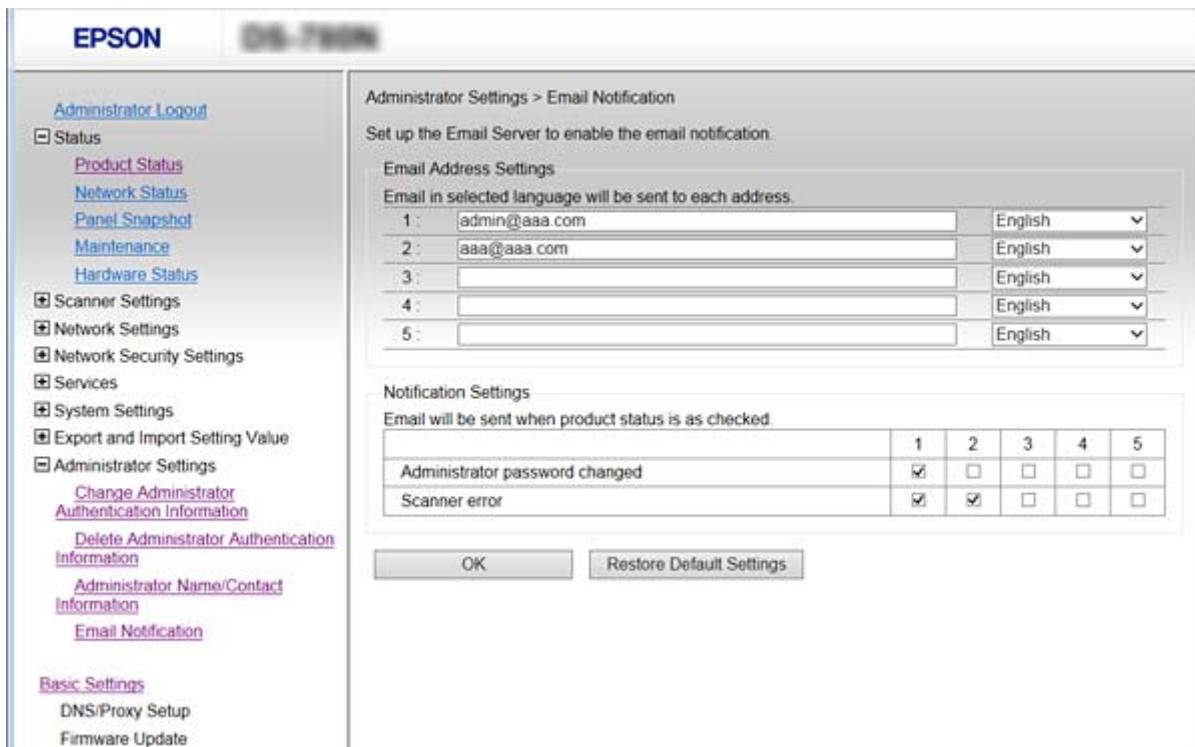
Конфигуриране на известяванията по имейл

За да използвате функцията, трябва да конфигурирате сървър за електронна поща.

1. Влезте в Web Config и изберете **Administrator Settings > Email Notification**.
2. Въведете имейл адреса, на който искате да получавате известявания по имейл.
3. Изберете езика за известявания по имейл.

Настройки за работа и управление

4. Поставете отметка в квадратчетата за известията, които искате да получавате.



5. Щракнете върху **ОК**.

Още по темата

- ➔ “Достъп до Web Config” на страница 23
- ➔ “Конфигуриране на сървър за електронна поща” на страница 42

Конфигуриране на сървър за електронна поща

Проверете следното преди конфигуриране.

- Скенерът е свързан към мрежа.
- Информация за имейл сървъра на компютъра.

1. Влезте в Web Config и изберете **Network Settings > Email Server > Basic**.
2. Въведете стойност за всеки елемент.
3. Изберете **ОК**.

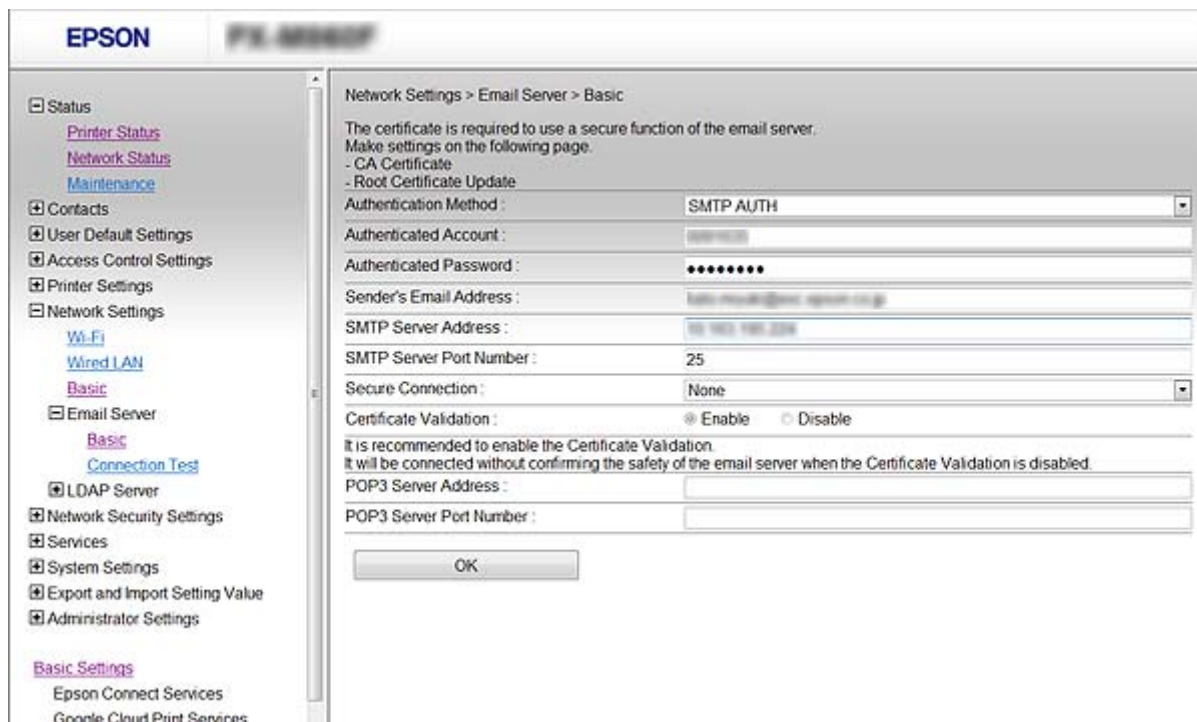
Показват се настройките, които сте избрали.

Още по темата

- ➔ “Достъп до Web Config” на страница 23
- ➔ “Елементи за настройка на сървъра за електронна поща” на страница 43

Настройки за работа и управление

Елементи за настройка на сървъра за електронна поща



Елементи	Настройки и обяснение	
Authentication Method	Посочете метода на удостоверяване за скенера за достъп до сървъра за електронна поща.	
	Off	Удостоверяването е изключено, когато тече комуникация със сървъра за електронна поща.
	SMTP AUTH	Изисква се сървърът за електронна поща да поддържа SMTP удостоверяване.
	POP before SMTP	Конфигурирайте POP3 сървъра, когато изберете този метод.
Authenticated Account	Ако изберете SMTP AUTH или POP before SMTP като Authentication Method , въведете име на акаунта за удостоверяване между 0 и 255 символа в ASCII (0x20–0x7E).	
Authenticated Password	Ако изберете SMTP AUTH или POP before SMTP като Authentication Method , въведете удостоверена парола между 0 и 20 знака, като използвате A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.	
Sender's Email Address	Въведете имейл адреса на подателя. Въведете между 0 и 255 знака в ASCII (0x20–0x7E), с изключение на: () < > [] ; ¥. Първият знак не може да бъде точка „.“.	
SMTP Server Address	Въведете между 0 и 255 знака с помощта на A–Z a–z 0–9 . - . Можете да използвате формат IPv4 или FQDN.	
SMTP Server Port Number	Въведете число между 1 и 65535.	

Настройки за работа и управление

Елементи	Настройки и обяснение	
Secure Connection	Посочете защитен метод за свързване за имейл сървъра.	
	None	Ако изберете POP before SMTP в Authentication Method , методът за свързване е зададен да бъде None .
	SSL/TLS	Тази опция е достъпна, когато Authentication Method е Off или SMTP AUTH .
	STARTTLS	Тази опция е достъпна, когато Authentication Method е Off или SMTP AUTH .
Certificate Validation	Сертификатът е проверен при разрешаването му. Препоръчваме задаване на Enable .	
POP3 Server Address	Ако изберете POP before SMTP като Authentication Method , въведете POP3 адреса на сървъра между 0 и 255 знака, като ползвате A–Z a–z 0–9. - . Можете да използвате формат IPv4 или FQDN.	
POP3 Server Port Number	Ако изберете POP before SMTP за Authentication Method , въведете число между 1 и 65535.	

Още по темата

➔ [“Конфигуриране на сървър за електронна поща” на страница 42](#)

Проверка на връзката с пощенския сървър

1. Влезте в Web Config и изберете **Network Settings > Email Server > Connection Test**.
2. Изберете **Start**.

Тестът за свързване към имейл сървъра е стартиран. След диагностиката се показва доклад от проверката.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

➔ [“Позовавания при диагностика на връзката с имейл сървъра” на страница 44](#)

Позовавания при диагностика на връзката с имейл сървъра

Съобщения	Обяснение
Connection test was successful.	Това съобщение се появява, когато връзката със сървъра е успешна.
SMTP server communication error. Check the following. - Network Settings	Това съобщение се появява, когато <ul style="list-style-type: none"> <input type="checkbox"/> Скенерът не е свързан към мрежа <input type="checkbox"/> SMTP сървърът не работи <input type="checkbox"/> Мрежовата връзка е прекъсната по време на комуникация <input type="checkbox"/> Получени са непълни данни

Настройки за работа и управление

Съобщения	Обяснение
POP3 server communication error. Check the following. - Network Settings	Това съобщение се появява, когато <ul style="list-style-type: none"> <input type="checkbox"/> Скенерът не е свързан към мрежа <input type="checkbox"/> POP3 сървърът не работи <input type="checkbox"/> Мрежовата връзка е прекъсната по време на комуникация <input type="checkbox"/> Получени са непълни данни
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Това съобщение се появява, когато <ul style="list-style-type: none"> <input type="checkbox"/> Неуспешно свързване към DNS сървър <input type="checkbox"/> Неуспешно преобразуване на имена за SMTP сървър
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Това съобщение се появява, когато <ul style="list-style-type: none"> <input type="checkbox"/> Неуспешно свързване към DNS сървър <input type="checkbox"/> Неуспешно преобразуване на имена за POP3 сървър
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Това съобщение се появява, когато удостоверяването на SMTP сървъра е неуспешно.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Това съобщение се появява, когато удостоверяването на POP3 сървъра е неуспешно.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Това съобщение се появява, когато се опитвате да комуникирате с неподдържани протоколи.
Connection to SMTP server failed. Change Secure Connection to None.	Това съобщение се появява при SMTP несъответствие между сървър и клиент или когато сървърът не поддържа защитена SMTP връзка (SSL връзка).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Това съобщение се появява при SMTP несъответствие между сървър и клиент или когато сървърът изпраща заявка за използване на SSL/TLS свързване за защитена SMTP връзка.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Това съобщение се появява при SMTP несъответствие между сървър и клиент или когато сървърът изпраща заявка за използване на STARTTLS свързване за защитена SMTP връзка.
The connection is untrusted. Check the following. - Date and Time	Това съобщение се появява, когато настройката за датата и часа на скенера е грешна или сертификатът е изтекъл.
The connection is untrusted. Check the following. - CA Certificate	Това съобщение се появява, когато скенерът няма основен сертификат, съответстващ на сървъра, или когато CA Certificate не е импортиран.
The connection is not secured.	Това съобщение се появява, когато полученият сертификат е повреден.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Това съобщение се появява, когато методът на удостоверяване на сървъра и клиента не съвпадат. Сървърът поддържа SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Това съобщение се появява, когато методът на удостоверяване на сървъра и клиента не съвпадат. Сървърът не поддържа SMTP AUTH.

Настройки за работа и управление

Съобщения	Обяснение
Sender's Email Address is incorrect. Change to the email address for your email service.	Това съобщение се появява, когато посоченият имейл на изпращача е грешен.
Cannot access the product until processing is complete.	Това съобщение се появява, когато скенерът е зает.

Още по темата

➔ [“Проверка на връзката с пощенския сървър” на страница 44](#)

Обновяване на фърмуер

Обновяване на фърмуера чрез Web Config

Обновява фърмуера чрез използване на Web Config. Устройството трябва да е свързано към интернет.

1. Влезте в Web Config и изберете **Basic Settings > Firmware Update**.
2. Щракнете върху **Start**.
Започва проверка на фърмуера и ако съществува обновен фърмуер, се показва информация.
3. Щракнете върху **Start** и следвайте инструкциите на екрана.

Забележка:

Можете да актуализирате фърмуера и от *Epson Device Admin*. Можете да проверите информацията за фърмуера визуално в списъка с устройства. Полезно е, когато искате да обновите фърмуера на няколко устройства. За повече подробности вижте помощта или *Epson Device Admin*.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

➔ [“Epson Device Admin” на страница 55](#)

Обновяване на фърмуера чрез използване на Epson Firmware Updater

Можете да изтеглите фърмуера на устройството от уебсайта на Epson на компютър, след което да свържете устройството и компютъра чрез USB кабел, за да обновите фърмуера. Ако не можете да обновите по мрежата, опитайте този начин.

1. Отворете уебсайта на Epson и изтеглете фърмуера.
2. Свържете компютъра, който съдържа изтегления фърмуер, към устройството чрез USB кабел.
3. Щракнете двукратно върху изтегления .exe файл.
Epson Firmware Updater се стартира.

4. Следвайте инструкциите на екрана.

Архивиране на настройките

Чрез експортиране на елементите от настройките в Web Config можете да ги копирате на други скенери.

Експортиране на настройки

Експортирайте всяка настройка на скенера.

1. Влезте в Web Config и след това изберете **Export and Import Setting Value > Export**.

2. Изберете настройките, които искате да експортирате.

Изберете настройките, които искате да експортирате. Ако изберете основна категория, подкатегиите също ще бъдат избрани. Обаче, подкатегиите, които водят до грешки чрез дублиране в рамките на една и съща мрежа (като IP адрес и др.) не могат да бъдат избрани.

3. Въведете парола за шифроване на експортирания файл.

Нужна Ви е парола за импортиране на файла. Оставете полето празно, ако не искате да шифровате файла.

4. Щракнете върху **Export**.



Важно:

Ако искате да експортирате мрежовите настройки на скенера като име на скенера и IP адрес, изберете **Enable to select the individual settings of device** и изберете още елементи. Използвайте само избраните стойности на новия скенер.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)

Импортиране на настройките

Импортирайте експортирания Web Config файл в скенера.



Важно:

Когато импортирате стойности, които включват индивидуална информация като име на скенера или IP адрес, се уверете, че същият IP адрес не съществува в същата мрежа. Ако IP адресът се застъпва, скенерът не отразява стойността.

1. Влезте в Web Config и след това изберете **Export and Import Setting Value > Import**.

2. Изберете експортирания файл и въведете паролата за криптиране.

3. Щракнете върху **Next**.

Настройки за работа и управление

4. Изберете настройките, които искате да импортирате и щракнете върху **Next**.
5. Щракнете върху **OK**.

Настройките се прилагат за скенера.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Отстраняване на проблеми

Съвети за отстраняване на проблеми

Можете да намерите повече информация в следното ръководство.

- Ръководство на потребителя

Предлага указания за използване на скенера, поддръжка и отстраняване на проблеми.

Проверка на регистъра за сървър и мрежово устройство

В случай на проблем с мрежовата връзка можете да идентифицирате причината, като потвърдите регистъра на сървъра на електронната поща, LDAP сървър и т.н., да проверите състоянието с помощта на мрежовия регистър на регистрите и командите на системното оборудване като рутери.

Инициализиране на мрежовите настройки

Възстановяване на мрежовите настройки от контролния панел

Можете да възстановите всички мрежови настройки до първоначалните им стойности.

1. Докоснете **Настройки** от началния екран.
 2. Докоснете **Системна администрация > Възстановяване на настройки по подразбиране > Настройки на мрежата**.
 3. Прочетете съобщението, след това изберете **Да**.
 4. Когато се появи съобщение, указващо завършване, докоснете **Затвори**.
Екранът се затваря автоматично след определен период от време, ако не натиснете **Затвори**.
-

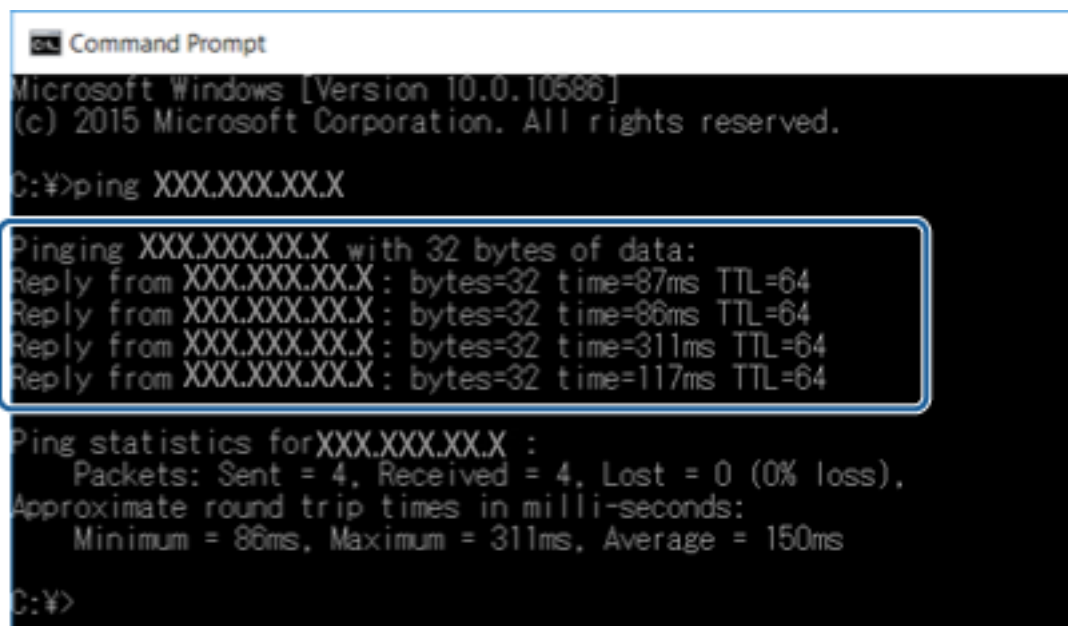
Проверка на комуникацията между устройства и компютри

Проверка на връзката чрез команда Ping — Windows

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

Отстраняване на проблеми

1. Вижте IP адреса на скенера за връзката, която искате да проверите.
Можете да проверите това от Epson Scan 2.
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 **Команден прозорец**.
 - ❑ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Изведете екрана на приложението, след което изберете **Команден прозорец**.
 - ❑ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 или по-стари
Щракнете върху стартовия бутон, изберете **Всички програми** или **Програми > Принадлежности > Команден прозорец**.
3. Въведете 'ping xxx.xxx.xxx.xxx', след това натиснете клавиша Enter.
Въведете IP адреса на скенера на мястото на xxx.xxx.xxx.xxx.
4. Проверете статуса на комуникацията.
Ако скенерът и компютърът комуникират, ще се покаже следното съобщение.



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

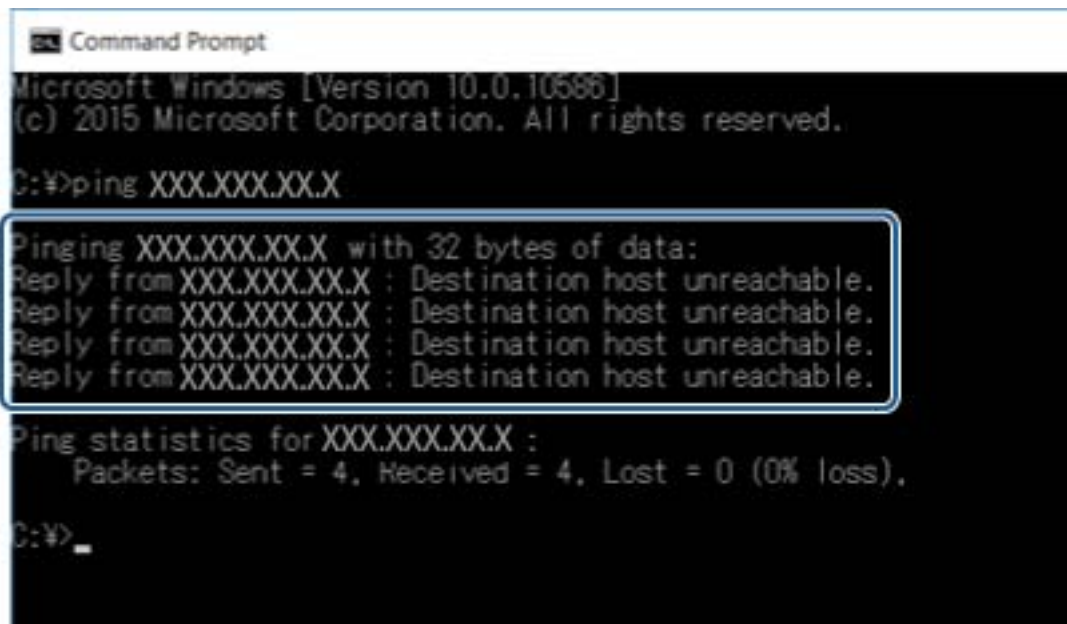
Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : bytes=32 time=87ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=86ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=311ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=117ms TTL=64

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 86ms, Maximum = 311ms, Average = 150ms

C:\>
```

Отстраняване на проблеми

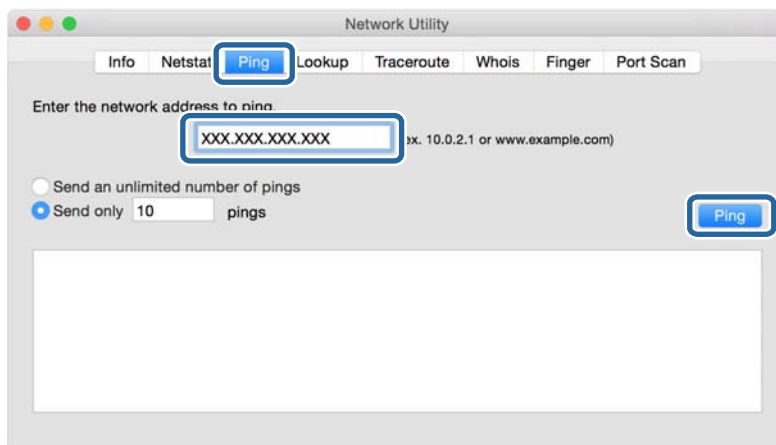
Ако скенерът и компютърът не комуникират, ще се покаже следното съобщение.



Проверка на връзката чрез команда Ping — Mac OS

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

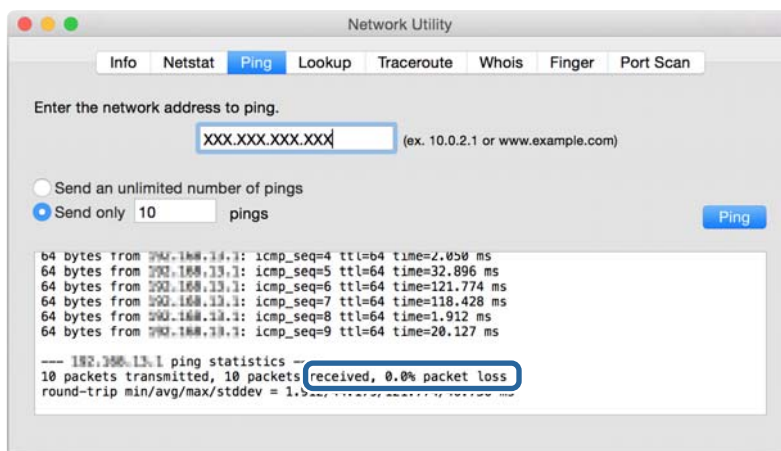
1. Вижте IP адреса на скенера за връзката, която искате да проверите.
Можете да проверите това от Epson Scan 2.
2. Стартирайте Network Utility.
Напишете „Network Utility“ в **Spotlight**.
3. Щракнете върху раздел **Ping**, въведете IP адреса, който сте проверили в стъпка 1, след което щракнете върху **Ping**.



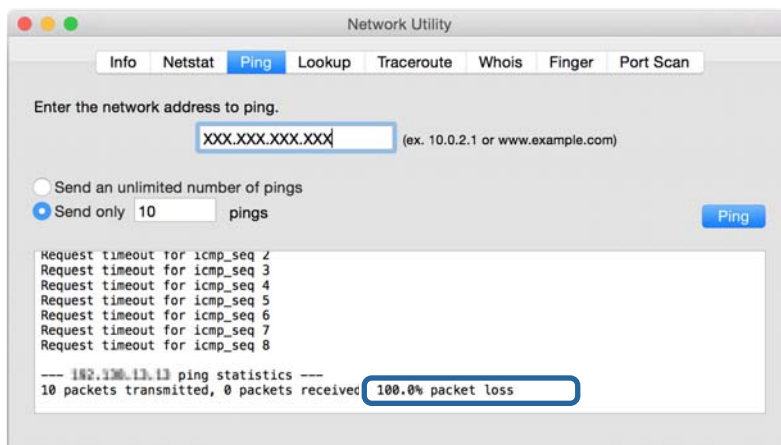
Отстраняване на проблеми

4. Проверете статуса на комуникацията.

Ако скенерът и компютърът комуникират, ще се покаже следното съобщение.



Ако скенерът и компютърът не комуникират, ще се покаже следното съобщение.



Проблеми при използване на мрежов софтуер

Няма достъп до Web Config

Конфигуриран ли е правилно IP адресът на скенера?

Конфигурирайте IP адреса с Epson Device Admin или EpsonNet Config.

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 е достъпна само в браузър, поддържащ шифроване в голям обем. Проверете поддръжката за криптиране на вашия браузър.

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

Отстраняване на проблеми

- 192 бита: AES256
- 256 бита: AES256

Появява се съобщение „Изтекла“ при достъп до Web Config чрез SSL комуникация (https).

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

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

IP адресът на скенера, въведен за **Common Name** за създаване на самоподписан сертификат или CSR, не съвпада с адреса, въведен в брауъра. Получете и импортирайте сертификата отново или сменете името на скенера.

Осъществява се достъп до скенера през прокси сървър.

Ако използвате прокси сървър с вашия скенер, трябва да конфигурирате настройките за прокси на вашия брауър.

Windows:

Изберете **Контролен панел > Мрежа и интернет > Опции за интернет > Връзки > LAN настройки > Прокси сървър** и след това изберете да не се използва прокси сървър за локални адреси.

Mac OS:

Изберете **Системни предпочитания > Мрежа > Разширени > Прокси сървъри** и след това регистрирайте локалния адрес за **Настройки за заобикаляне на прокси сървъра за тези хостове & домейни**.

Пример:

192.168.1.*: Локален адрес 192.168.1.XXX, маска на подмрежа 255.255.255.0

192.168.*.*: Локален адрес 192.168.XXX.XXX, маска на подмрежа 255.255.0.0

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)
- ➔ [“Задаване на IP адрес” на страница 15](#)
- ➔ [“Присвояване на IP адрес с EpsonNet Config” на страница 56](#)

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

Избрахте ли **Блокирай**, **Отказ** или **Изключване**, когато се появи екранът за защитата на Windows или защитната стена?

Ако изберете **Блокирай**, **Отказ** или **Изключване**, IP адресът и името на модела няма да се показват на EpsonNet Config или EpsonNet Setup.

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

Отстраняване на проблеми

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

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

Още по темата

- ➔ [“Изпълнение на EpsonNet Config — Windows” на страница 56](#)
- ➔ [“Изпълнение на EpsonNet Config — Mac OS” на страница 56](#)

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 уебсайта за поддръжка на Epson. За повече информация вижте документацията или помощта на Epson Device Admin.

Стартиране на Epson Device Admin (само за Windows)

Изберете **Всички програми > EPSON > Epson Device Admin > Epson Device Admin**.

Забележка:

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

EpsonNet Config

EpsonNet Config позволява на администратора да конфигурира мрежовите настройки на скенера като задаване на IP адрес и промяна на режима на свързване. Функцията за партидна настройка се поддържа на Windows. За повече информация вижте документацията или помощта на EpsonNet Config.



Приложение

Изпълнение на EpsonNet Config — Windows

Изберете **Всички програми > EpsonNet > EpsonNet Config SE > EpsonNet Config**.

Забележка:

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

Изпълнение на EpsonNet Config — Mac OS

Изберете **Отиди > Приложения > Epson Software > EpsonNet > EpsonNet Config SE > EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager е софтуер за създаване на пакет за лесна инсталация на скенера като инсталиране на драйвера на скенера, инсталиране на Document Capture Pro. Този софтуер позволява на администратора да създава уникални софтуерни пакети и да ги разпределя между различни групи.

За повече информация посетете регионалния уебсайт на Epson.

Присвояване на IP адрес с EpsonNet Config

Можете да присвоите IP адрес на скенера от EpsonNet Config. EpsonNet Config ви позволява да присвоите IP адрес на скенер, който няма такъв след свързване с Ethernet кабел.

Присвояване на IP с партидни настройки**Създаване на файл за партидни настройки**

Като използвате MAC адреса и името на модела като ключове, можете да създадете нов SYLK файл за задаване на IP адрес.

1. Отворете приложение за работна таблица (например Microsoft Excel) или текстов редактор.
2. Въведете „Info_MACAddress“, „Info_ModelName“ и „TCPIP_IPAddress“ в първия ред като имена на елементите в настройката.

Въведете елементите от настройката за следните текстови низове. Правете разлика между главни и малки букви и двубайтови/еднобайтови символи; ако се различава само един символ, елементът няма да бъде разпознат.

Въведете име на елемента от настройката, както е описано по-долу; в противен случай EpsonNet Config няма да разпознае елементите.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

Приложение

3. Въведете MAC адреса, името на модела и IP адрес за всеки мрежов интерфейс.

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

4. Въведете име и запишете като SYLK файл (*.slk).

Партидни настройки от конфигурационен файл

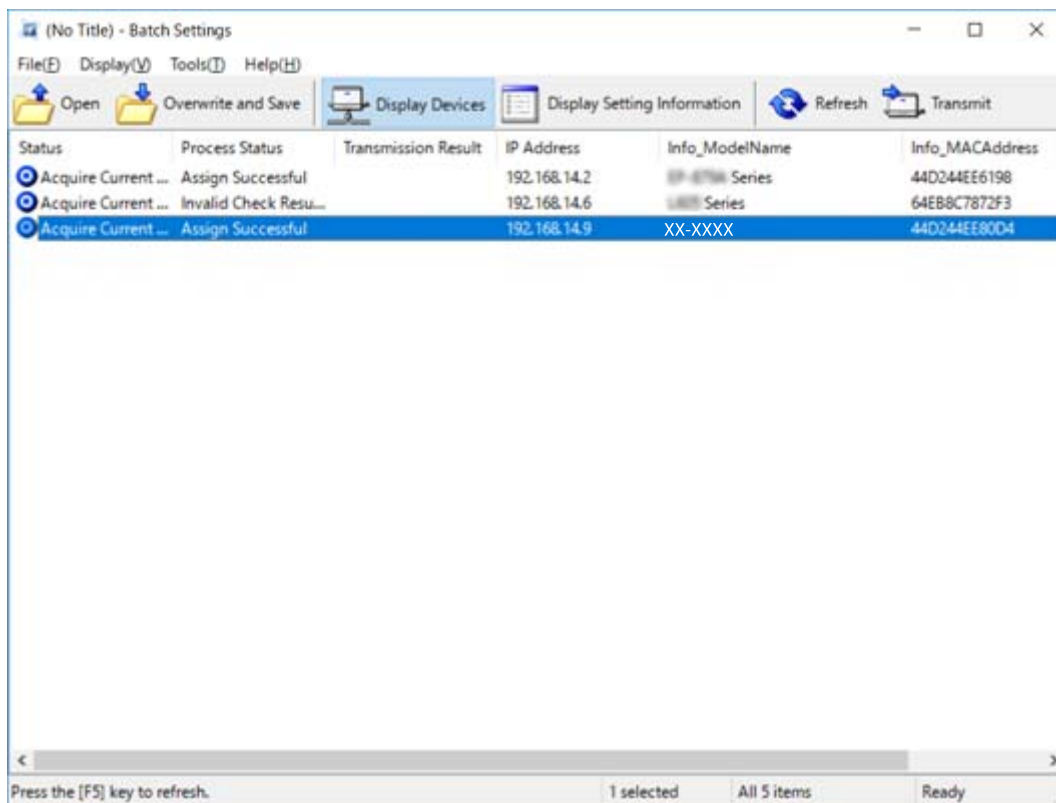
Присвояване на IP адрес в конфигурационния файл (SYLK файл) едновременно. Трябва да създадете конфигурационния файл преди присвояването.

1. Свържете всички устройства към мрежа с помощта на Ethernet кабели.
2. Включете скенера.
3. Стартирайте EpsonNet Config.
Показва се списък със скенери в мрежата. Може да отнеме известно време, преди да се покажат.
4. Щракнете върху **Tools > Batch Settings**.
5. Щракнете върху **Open**.
6. В екрана за избор изберете SYLK файл (*.slk) който съдържа настройките, после щракнете върху **Open**.

Приложение

- Изберете устройства, за които искате да направите партидни настройки с колоната **Status**, настроена на **Unassigned** и **Process Status**, настроен на **Assign Successful**.

Когато правите множество избори, натиснете Ctrl или Shift и щракнете или плъзнете с мишката.



- Щракнете върху **Transmit**.
- Когато се покаже екранът за въвеждане на парола, въведете паролата и щракнете върху **OK**.
Предаване на настройки.

Забележка:

Информацията се предава към мрежовия интерфейс до приключване на индикатора за напредък. Не изключвайте устройството или безжичния адаптер и не изпращайте данни към устройството.






- В екран **Transmitting Settings** щракнете върху **OK**.



Приложение

11. Проверете състоянието на устройството, което сте настроили.

За устройства, които показват  или , проверете съдържанието на файла с настройки или дали устройството е рестартирано нормално.

Икона	Status	Process Status	Обяснение
	Setup Complete	Setup Successful	Настройката е приключена нормално.
	Setup Complete	Rebooting	Когато се предава информацията, всяко устройство трябва да се рестартира, за да се разреши настройката. Изпълнява се проверка, за да се определи дали устройството може да се свърже след рестартирането.
	Setup Complete	Reboot Failed	Не може да се провери устройството след предаване на настройките. Проверете дали устройството е включено или дали се е рестартирало нормално.
	Setup Complete	Searching	Търсене на устройството, указано във файла с настройки.*
	Setup Complete	Search Failed	Не могат да се проверят устройства, които вече са настроени. Проверете дали устройството е включено или дали се е рестартирало нормално.*

* Само когато се показва информация за настройката.

Още по темата

- ➔ [“Изпълнение на EpsonNet Config — Windows” на страница 56](#)
- ➔ [“Изпълнение на EpsonNet Config — Mac OS” на страница 56](#)

Задаване на IP адрес за всяко устройство

Задайте IP адрес на скенера от EpsonNet Config.

1. Включете скенера.
2. Свържете скенера към мрежата с помощта на Ethernet кабел.
3. Стартирайте EpsonNet Config.
Показва се списък със скенери в мрежата. Може да отнеме известно време, преди да се покажат.
4. Щракнете двукратно върху скенера, който искате да използвате.

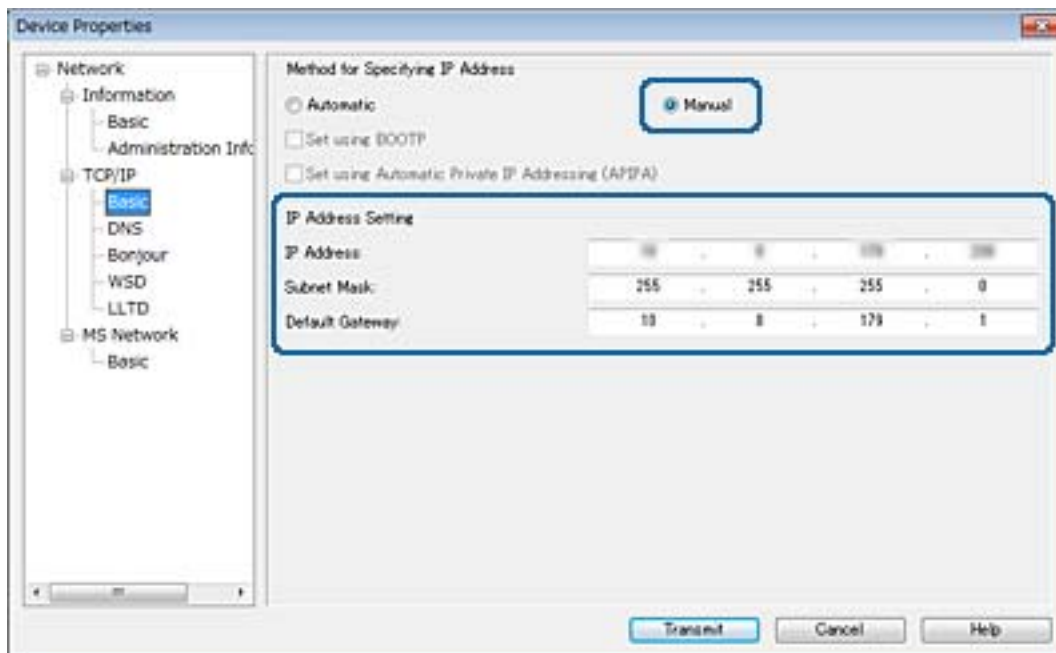
Забележка:

Ако сте свързали няколко скенера от един и същ модел, можете да идентифицирате скенера по MAC адрес.

5. Изберете **Network > TCP/IP > Basic**.

Приложение

6. Въведете адреси за **IP Address**, **Subnet Mask** и **Default Gateway**.

**Забележка:**

Въведете статичен адрес, когато свързвате скенера към защитена мрежа.

7. Щракнете върху **Transmit**.

Извежда се потвърждение за предаване на информацията на екрана.

8. Щракнете върху **OK**.

Показва се екранът за потвърждение на предаването.

Забележка:

Информацията се предава към устройството и след това се извежда съобщението „Конфигурацията е успешно завършена“. Не изключвайте устройството и не изпращайте данни към услугата.

9. Щракнете върху **OK**.

Още по темата

- ➔ [“Изпълнение на EpsonNet Config — Windows” на страница 56](#)
- ➔ [“Изпълнение на EpsonNet Config — Mac OS” на страница 56](#)

Използване на порт за скенера

Скенера използва следния порт. Тези портове трябва да са разрешени, за да са свободни за мрежовия администратор, ако е необходимо.

Приложение

Подател (клиент)	Употреба	Местоназначение (сървър)	Протокол	Номер на порт
Скенер	Изпращане на имейл (Известяване по имейл)	SMTP сървър	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP преди SMTP връзка (Известяване по имейл)	POP сървър	POP3 (TCP)	110
	Control WSD	Клиентски компютър	WSD (TCP)	5357
	Търсене на компютър при сканиране по заявка от Document Capture Pro	Клиентски компютър	Network Push Scan Discovery	2968
Събиране на информация за заданието при Push сканиране от Document Capture Pro	Клиентски компютър	Мрежово Push сканиране	2968	
Клиентски компютър	Откриване на скенера от приложение като EpsonNet Config и драйвер на скенера.	Скенер	ENPC (UDP)	3289
	Събиране и настройка на MIB информация от приложения като EpsonNet Config и драйвера на скенера.	Скенер	SNMP (UDP)	161
	Търсене на WSD скенер	Скенер	WS-Discovery (UDP)	3702
	Пренасочване на данни от сканиране от Document Capture Pro	Скенер	Мрежово сканиране (TCP)	1865

Разширени настройки за сигурност за корпорации

В тази глава описваме разширени функции за сигурност.

Настройки за сигурност 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. Ако използвате устройството в среда с достъп до интернет, рисковете са още по-големи.

За да се избегне тази опасност, устройствата на Epson имат множество технологии за сигурност.

Настройте устройството според необходимостта и условията на средата, която е изградена с информация за средата на клиента.

Име	Тип функция	Какво да се настрои	Какво да се предотврати
SSL/TLS комуникация	Пътят на комуникацията между компютъра и устройството е криптиран с SSL/TLS комуникация. Съдържанието на комуникацията чрез браузър е защитено.	Задаване на сертификат на сертифициращ орган за сървъра, който е сертификат, подписан от CA (сертифициращ орган) на устройството.	Предотвратяване на изтичане на информация за настройките и съдържанието на прехвърлените данни към скенера от компютъра. Достъпът до сървъра на Epson в интернет от устройството може също да бъде защитен с помощта на актуализация на фърмуера и др.
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 (кодирание и удостоверяване), можете безопасно да споделяте незащитен протокол за 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 по мрежата, интегритет на данните към SNMP протокола за управление, криптиране, удостоверяване на потребителите и др.	Разрешаване на SNMPv3, последвано от задаване на начин за удостоверяване и криптиране.	Осигуряване на промяна на настройките по мрежата и поверителност при следене на състоянието.

Разширени настройки за сигурност за корпорации

Име	Тип функция	Какво да се настрои	Какво да се предотврати
IEEE802.1X	Позволява свързване само на потребител, който е удостоверяван за свързване по Ethernet. Позволява само на потребители, които имат разрешение, да използват устройството.	Настройка на удостоверяване към RADIUS сървър (сървър за удостоверяване).	Защита от неупълномощен достъп и използване на устройството.
Прочитане на карта за самоличност	Можете да използвате устройството, като задържите карта за самоличност над свързаното упълномощено устройство. Можете да ограничите придобиването на регистри за всеки потребител и устройство и да ограничите наличните устройства и функции за всеки потребител и група.	Свържете устройството за удостоверяване към устройството, после настройте информацията за потребител в системата за удостоверяване.	Предотвратяване на неупълномощено използване и неправомерна смяна на самоличността на устройството.

Още по темата

- ➔ [“SSL/TLS комуникация със скенера” на страница 63](#)
- ➔ [“Криптирана комуникация с IPsec/IP филтриране” на страница 71](#)
- ➔ [“Използване на SNMPv3 протокол” на страница 83](#)
- ➔ [“Свързване на скенера към мрежа IEEE802.1X” на страница 85](#)

Настройки на функции за сигурност

Когато настройвате IPsec/IP филтриране или IEEE802.1X, 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.

SSL/TLS комуникация със скенера

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

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 сертификата, подписан от сертифициращ орган. Можете да използвате сертификата, подписан от сертифициращ орган, за всяка функция за сигурност.

Разширени настройки за сигурност за корпорации

Сертификат на сертифициращ орган

Сертификатът на сертифициращ орган показва, че трета страна е проверила самоличността на сървъра. Това е ключов компонент в стила на сигурност „мрежа на доверие“. Трябва да получите сертификат на сертифициращ орган за удостоверяване на сървъра от сертифициращия орган, който го издава.

Самоподписан сертификат

Самоподписаният сертификат е сертификат, който скенерът 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 браузъра може да се покаже предупреждение за сигурност. Можете да използвате този сертификат само за SSL/TLS комуникация.

Още по темата

- ➔ [“Получаване и импортиране на сертификат, подписан от сертифициращ орган”](#) на страница 64
- ➔ [“Изтриване на сертификат, подписан от сертифициращ орган”](#) на страница 68
- ➔ [“Актуализиране на самоподписан сертификат”](#) на страница 68

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**. След това изберете **SSL/TLS > Certificate** или **IPsec/IP Filtering > Client Certificate** или **IEEE802.1X > Client Certificate**.
2. Щракнете върху **Generate** 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.
4. Щракнете върху **OK**.
Показва се съобщение за завършване.
5. Изберете **Network Security Settings**. След това изберете **SSL/TLS > Certificate** или **IPsec/IP Filtering > Client Certificate** или **IEEE802.1X > Client Certificate**.

Разширени настройки за сигурност за корпорации

- 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 CA-signed Certificate.

- Изпратете CSR до сертифициращ орган и получите CA-signed Certificate.
Следвайте правилата на всеки сертифициращ орган относно метода и формата на изпращане.
- Запазете издадения CA-signed Certificate на компютър, свързан към скенера.
Получаването на CA-signed Certificate е завършено, когато запазите сертификата в определена дестинация.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)
- ➔ [“Елементи за настройка на CSR” на страница 65](#)
- ➔ [“Импортиране на сертификат, подписан от сертифициращ орган” на страница 66](#)

Елементи за настройка на CSR

The screenshot shows the 'Certificate' configuration page in the Epson Web Config interface. The breadcrumb path is 'Network Security Settings > SSL/TLS > Certificate'. The page contains several input fields for certificate details:

- Key Length: [Input field with a dropdown menu]
- Common Name: [Input field]
- Organization: [Input field]
- Organizational Unit: [Input field]
- Locality: [Input field]
- State/Province: [Input field]
- Country: [Input field]

At the bottom of the form are two buttons: 'OK' and 'Back'. On the left side of the interface, there is a navigation menu with various settings categories, including 'Network Security Settings' which is expanded to show 'SSL/TLS' and 'Certificate'.

Елементи	Настройки и обяснение
Key Length	Изберете дължина на ключа за CSR.

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение
Common Name	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/ Organizational Unit/ Locality/ State/Province	Можете да въведете между 0 и 64 знака в ASCII (0x20 – 0x7E). Можете да отделите идентификационно име със запетаи.
Country	Въведете кода на страната с двуцифрен номер, определен от ISO-3166.

Още по темата

➔ [“Получаване на сертификат, подписан от сертифициращ орган”](#) на страница 64

Импортиране на сертификат, подписан от сертифициращ орган

**Важно:**

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

1. Влезте в Web Config и след това изберете **Network Security Settings**. След това изберете **SSL/TLS > Certificate** или **IPsec/IP Filtering > Client Certificate** или **IEEE802.1X > Client Certificate**.

2. Щракнете върху **Import**.

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:** Не конфигурирайте, защото скенерът съдържа личен ключ.
 - Password:** Не конфигурирайте.
 - CA Certificate 1/CA Certificate 2:** По желание
- Сертификат във формат PEM/DER, получен от компютър
 - Private Key:** Трябва да зададете.
 - Password:** Не конфигурирайте.
 - CA Certificate 1/CA Certificate 2:** По желание

Разширени настройки за сигурност за корпорации

- Сертификат във формат PKCS#12, получен от компютър
 - Private Key:** Не конфигурирайте.
 - Password:** По желание
 - CA Certificate 1/CA Certificate 2:** Не конфигурирайте.

4. Щракнете върху ОК.

Показва се съобщение за завършване.

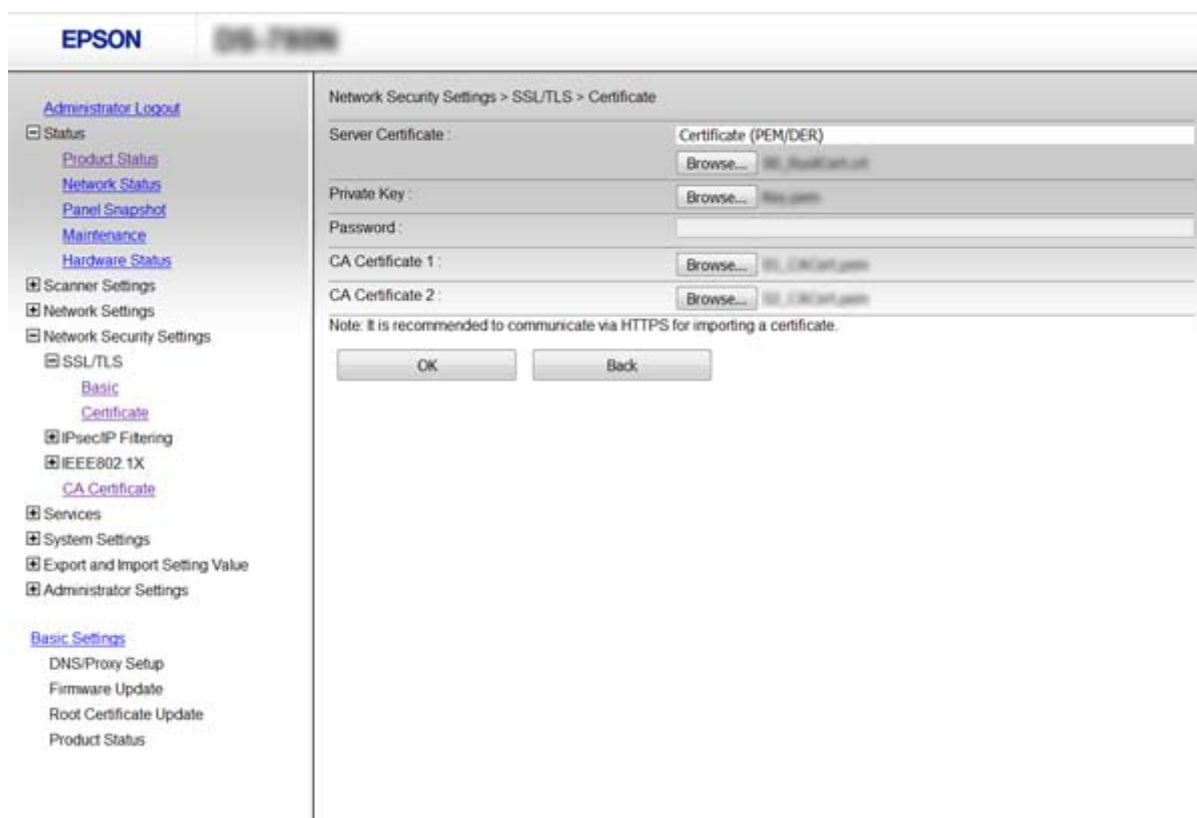
Забележка:

Щракнете върху *Confirm*, за да проверите информацията за сертификата.

Още по темата

- ➔ “Достъп до Web Config” на страница 23
- ➔ “Елементи за настройка на импортиране на сертификат, подписан от сертифициращ орган” на страница 67

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



Елементи	Настройки и обяснение
Server Certificate или Client Certificate	Изберете формат на сертификата.
Private Key	Ако получите сертификат във формат PEM/DER с помощта на CSR, създадена от компютър, укажете файла с личен ключ, който съответства на сертификата.

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение
Password	Въведете парола за криптиране на личен ключ.
CA Certificate 1	Ако форматът на вашия сертификат е Certificate (PEM/DER) , импортирайте сертификата на сертифициращ орган, който издава сертификата на сървъра. Посочете файл, ако има нужда.
CA Certificate 2	Ако форматът на вашия сертификат е Certificate (PEM/DER) , импортирайте сертификата на сертифициращ орган, който издава CA Certificate 1 . Посочете файл, ако има нужда.

Още по темата

➔ [“Импортиране на сертификат, подписан от сертифициращ орган”](#) на страница 66

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

1. Влезте в Web Config и след това изберете **Network Security Settings**. След това изберете **SSL/TLS > Certificate** или **IPsec/IP Filtering > Client Certificate** или **IEEE802.1X > Client Certificate**.
2. Щракнете върху **Delete**.
3. Потвърдете, че искате да изтриете сертификата в показаното съобщение.

Още по темата

➔ [“Достъп до Web Config”](#) на страница 23

Актуализиране на самоподписан сертификат

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

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

1. Влезте в Web Config и изберете **Network Security Settings > SSL/TLS > Certificate**.
2. Щракнете върху **Update**.
3. Въведете **Common Name**.

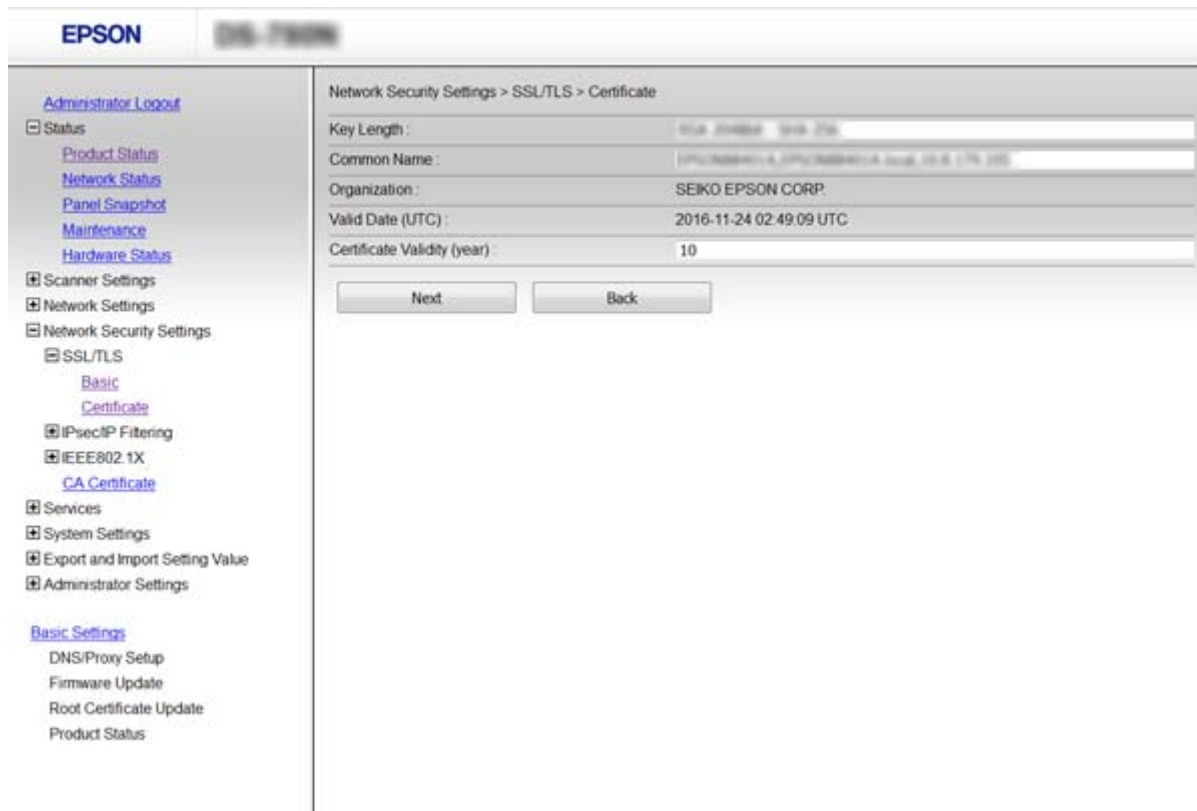
Въведете IP адрес или идентификатор, например FQDN име за скенера. Може да въведете между 1 и 128 знака.

Разширени настройки за сигурност за корпорации

Забележка:

Можете да отделите идентификационно име (CN) със запетайи.

- Посочете срок на валидност на сертификата.



- Щракнете върху **Next**.
Показва се съобщение за потвърждение.

- Щракнете върху **OK**.
Скенерът се актуализира.

Забележка:

Щракнете върху **Confirm**, за да проверите информацията за сертификата.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Конфигурирайте CA Certificate

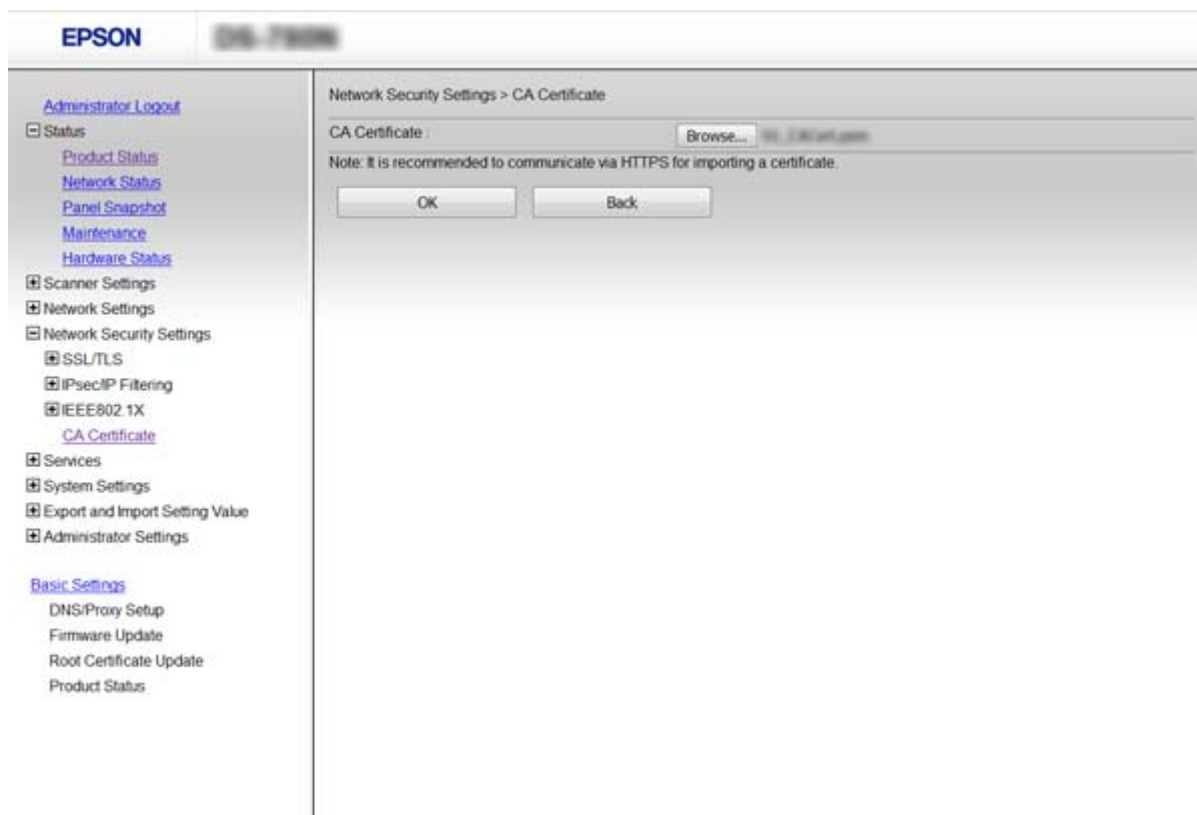
Можете да импортирате, покажете и изтриете CA Certificate.

Импортиране на CA Certificate

- Влезте в Web Config и след това изберете **Network Security Settings > CA Certificate**.

Разширени настройки за сигурност за корпорации

- Щракнете върху **Import**.
- Посочете CA Certificate, който искате да импортирате.



- Щракнете върху **OK**.

Когато импортирането завърши, ще се върнете на екрана **CA Certificate** и импортираният CA Certificate ще бъде показан.

Още по темата

➔ [“Достъп до Web Config”](#) на страница 23

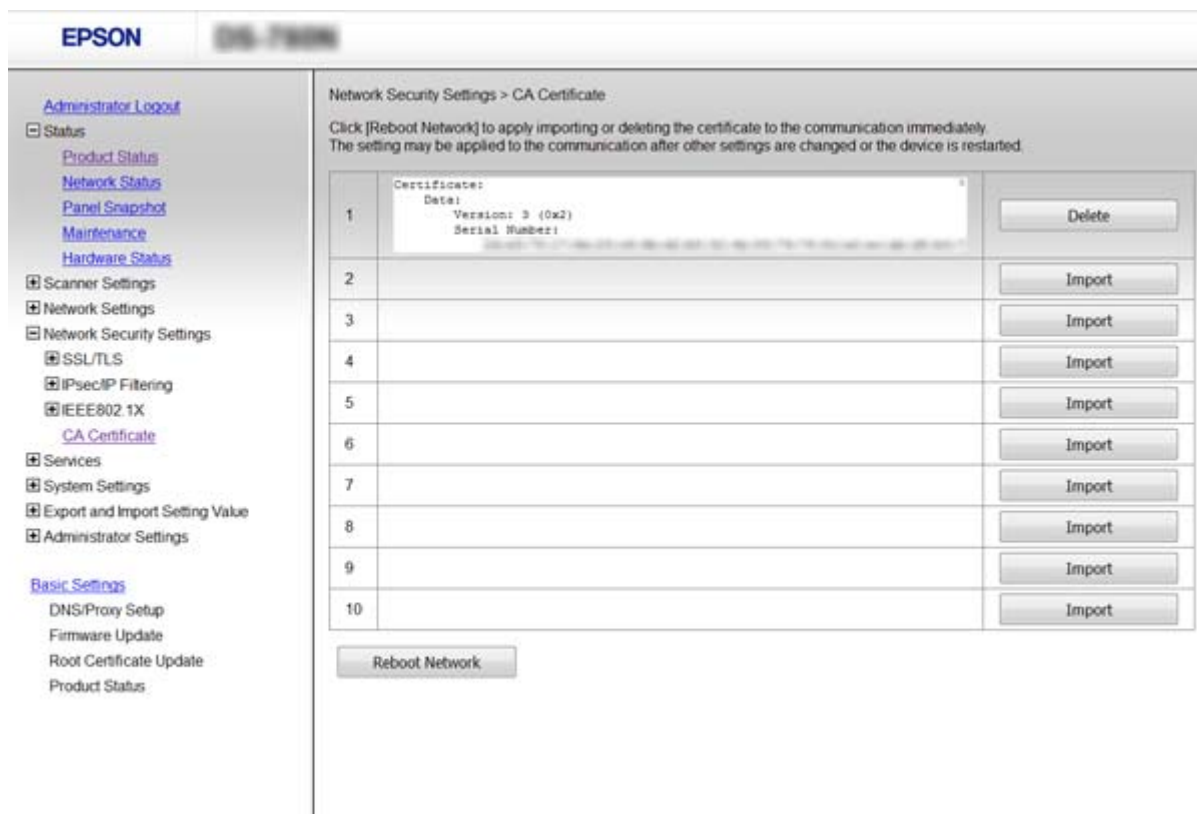
Изтриване на CA Certificate

Можете да изтриете импортиран CA Certificate.

- Влезте в Web Config и след това изберете **Network Security Settings > CA Certificate**.

Разширени настройки за сигурност за корпорации

- Щракнете върху **Delete** до CA Certificate, който искате да изтриете.



- Потвърдете, че искате да изтриете сертификата в показаното съобщение.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)

Криптирана комуникация с IPsec/IP филтриране

Относно IPsec/IP Filtering

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

За да филтрирате трафика, конфигурирайте политиката по подразбиране. Политиката по подразбиране се прилага за всеки потребител или група, които се свързват към скенера. За по-фин контрол върху потребители и групи от потребители конфигурирайте групови политики. Групова политика представлява едно или повече правила, приложени към потребител или група потребители. Скенерът контролира IP пакетите, които съответстват на конфигурирани политики. IP пакетите се удостоверяват по реда на групова политика 1 до 10, след това политика по подразбиране.

Забележка:

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

Разширени настройки за сигурност за корпорации

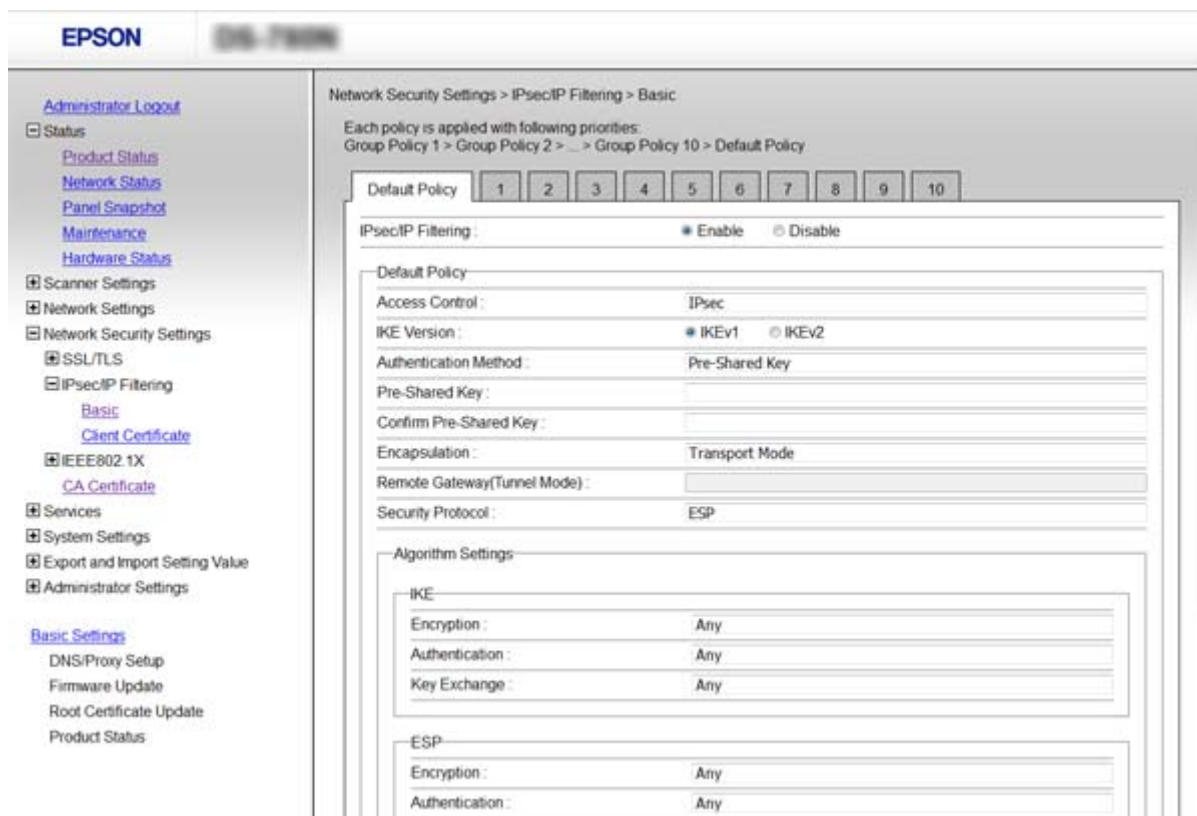
Конфигуриране на Default Policy

1. Влезте в Web Config и изберете **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Въведете стойност за всеки елемент.
3. Щракнете върху **Next**.
Показва се съобщение за потвърждение.
4. Щракнете върху **OK**.
Скенераът се актуализира.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)
- ➔ [“Елементи за настройка на Default Policy” на страница 72](#)

Елементи за настройка на Default Policy



Елементи	Настройки и обяснение
IPsec/IP Filtering	Можете да активирате или дезактивирате функцията за IPsec/IP Filtering филтриране.

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение	
Access Control	Конфигурирайте контролен метод за трафик на IP пакети.	
	Permit Access	Изберете тази опция, за да разрешите преминаване на конфигурирани IP пакети.
	Refuse Access	Изберете тази опция, за да забраните преминаване на конфигурирани IP пакети.
	IPsec	Изберете тази опция, за да разрешите преминаване на конфигурирани IPsec пакети.
IKE Version	Изберете IKEv1 или IKEv2 за версия на IKE. Изберете един от елементите според устройството, към което е свързан скенерът.	
IKEv1	Когато изберете IKEv1 за IKE Version , се показват следните елементи.	
	Authentication Method	За да изберете Certificate , трябва да получите и да импортирате предварително сертификат, подписан от сертифициращ орган.
	Pre-Shared Key	Ако изберете Pre-Shared Key за Authentication Method , въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете ключа, който сте конфигурирали за потвърждение.
IKEv2	Когато изберете IKEv2 за IKE Version , се показват следните елементи.	
Local	Authentication Method	За да изберете Certificate , трябва да получите и да импортирате предварително сертификат, подписан от сертифициращ орган.
	ID Type	Изберете вида на ИД на скенера.
	ID	Въведете ИД на скенера, което отговаря на вида на ИД. Не можете да използвате „@“, „#“ и „=“ за първия символ. Distinguished Name: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „=“. IP Address: въведете IPv4 или IPv6 формат. FQDN: въведете комбинация между 1 и 255 символа, като използвате A – Z, a – z, 0 – 9, „-“ и точка (.). Email Address: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „@“. Key ID: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа.
	Pre-Shared Key	Ако изберете Pre-Shared Key за Authentication Method , въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете ключа, който сте конфигурирали за потвърждение.

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение	
Remote	Authentication Method	За да изберете Certificate , трябва да получите и да импортирате предварително сертификат, подписан от сертифициращ орган.
	ID Type	Изберете типа на ИД на устройството, което искате да удостоверите.
	ID	<p>Въведете ИД на скенера, което отговаря на вида на ИД.</p> <p>Не можете да използвате „@“, „#“ и „=“ за първия символ.</p> <p>Distinguished Name: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „=“.</p> <p>IP Address: въведете IPv4 или IPv6 формат.</p> <p>FQDN: въведете комбинация между 1 и 255 символа, като използвате A – Z, a – z, 0 – 9, „-“ и точка (.).</p> <p>Email Address: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „@“.</p> <p>Key ID: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа.</p>
	Pre-Shared Key	Ако изберете Pre-Shared Key за Authentication Method , въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете ключа, който сте конфигурирали за потвърждение.
Encapsulation	Ако изберете IPsec за Access Control , трябва да конфигурирате режим на капсулиране.	
	Transport Mode	Ако използвате скенера само на една и съща LAN мрежа, изберете това. Криптират се IP пакети от слой 4 или по-нов.
	Tunnel Mode	Ако използвате скенера в мрежа с възможности за интернет като IPsec-VPN, изберете тази опция. Криптират се заглавната част и данните на IP пакетите.
Remote Gateway(Tunnel Mode)	Ако изберете Tunnel Mode за Encapsulation , въведете адрес на шлюз между 1 и 39 знака.	
Security Protocol	IPsec за Access Control , изберете опция.	
	ESP	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните, както и криптирането на данните.
	AH	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните. Дори ако криптирането на данни е забранено, можете да използвате IPsec.
Algorithm Settings		

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение	
IKE	Encryption	Изберете алгоритъма за криптиране на IKE. Елементите са различни в зависимост от версията на IKE.
	Authentication	Изберете алгоритъма за удостоверяване на IKE.
	Key Exchange	Изберете алгоритъма за размяна на ключове за IKE. Елементите са различни в зависимост от версията на IKE.
ESP	Encryption	Изберете алгоритъма за криптиране на ESP. Тази опция е достъпна, когато ESP е избран за Security Protocol .
	Authentication	Изберете алгоритъма за удостоверяване на ESP. Тази опция е достъпна, когато ESP е избран за Security Protocol .
AH	Authentication	Изберете алгоритъма за криптиране на AH. Тази опция е достъпна, когато AH е избран за Security Protocol .

Още по темата

➔ [“Конфигуриране на Default Policy” на страница 72](#)

Конфигуриране на Group Policy

1. Влезте в Web Config и изберете **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Щракнете върху номериран раздел, който искате да конфигурирате.
3. Въведете стойност за всеки елемент.
4. Щракнете върху **Next**.
Показва се съобщение за потвърждение.
5. Щракнете върху **OK**.
Скенера се актуализира.

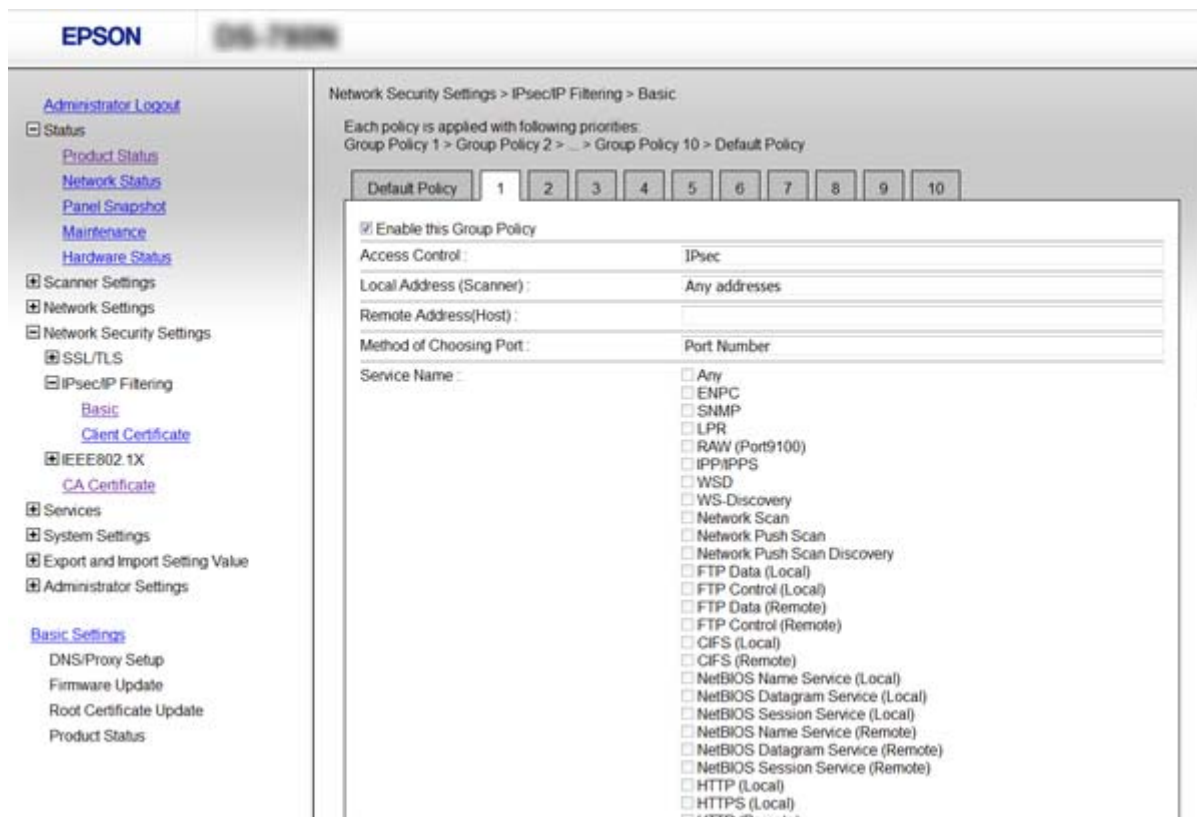
Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

➔ [“Елементи за настройка на Group Policy” на страница 76](#)

Разширени настройки за сигурност за корпорации

Елементи за настройка на Group Policy



Елементи	Настройки и обяснение	
Enable this Group Policy	Можете да активирате или дезактивирате групова политика.	
Access Control	Конфигурирайте контролен метод за трафик на IP пакети.	
	Permit Access	Изберете тази опция, за да разрешите преминаване на конфигурирани IP пакети.
	Refuse Access	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 (Scanner)	Изберете IPv4 адрес или IPv6 адрес, който съответства на средата на вашата мрежа. Ако IP адресът се задава автоматично, можете да изберете Use auto-obtained IPv4 address .	
Remote Address(Host)	Въведете IP адреса на устройството за контрол на достъпа. IP адресът трябва да бъде 43 знака или по-малко. Ако не въведете IP адрес, се контролират всички адреси. Забележка: Ако IP адресът се задава автоматично (например определен от DHCP), връзката може да не е налична. Конфигурирайте статичен IP адрес.	
Method of Choosing Port	Изберете метод за определяне на портовете.	
Service Name	Ако изберете Service Name за Method of Choosing Port , изберете опция.	

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение	
Transport Protocol	Ако изберете Port Number за Method of Choosing Port , трябва да конфигурирате режим на капсулиране.	
	Any Protocol	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	Ако изберете Port Number за Method of Choosing Port и ако изберете TCP или UDP за Transport Protocol , въведете номера на портове, за да контролирате приемането на пакети, като ги отделяте със запетаи. Можете да въведете максимално 10 номера на портове. Пример: 20,80,119,5220 Ако не въведете номер на порт, се контролират всички портове.	
Remote Port	Ако изберете Port Number за Method of Choosing Port и ако изберете TCP или UDP за Transport Protocol , въведете номера на портове, за да контролирате изпращането на пакети, като ги отделяте със запетаи. Можете да въведете максимално 10 номера на портове. Пример: 25,80,143,5220 Ако не въведете номер на порт, се контролират всички портове.	
IKE Version	Изберете IKEv1 или IKEv2 за версия на IKE. Изберете един от елементите според устройството, към което е свързан скенерът.	
IKEv1	Когато изберете IKEv1 за IKE Version , се показват следните елементи.	
	Authentication Method	Ако изберете IPsec за Access Control , изберете опция. Използваният сертификат се среща често с политика по подразбиране.
	Pre-Shared Key	Ако изберете Pre-Shared Key за Authentication Method , въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете ключа, който сте конфигурирали за потвърждение.
IKEv2	Когато изберете IKEv2 за IKE Version , се показват следните елементи.	

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение	
Local	Authentication Method	Ако изберете IPsec за Access Control , изберете опция. Използваният сертификат се среща често с политика по подразбиране.
	ID Type	Изберете вида на ИД на скенера.
	ID	<p>Въведете ИД на скенера, което отговаря на вида на ИД.</p> <p>Не можете да използвате „@“, „#“ и „=“ за първия символ.</p> <p>Distinguished Name: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „=“.</p> <p>IP Address: въведете IPv4 или IPv6 формат.</p> <p>FQDN: въведете комбинация между 1 и 255 символа, като използвате A – Z, a – z, 0 – 9, „-“ и точка (.).</p> <p>Email Address: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „@“.</p> <p>Key ID: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа.</p>
	Pre-Shared Key	Ако изберете Pre-Shared Key за Authentication Method , въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете ключа, който сте конфигурирали за потвърждение.
Remote	Authentication Method	Ако изберете IPsec за Access Control , изберете опция. Използваният сертификат се среща често с политика по подразбиране.
	ID Type	Изберете типа на ИД на устройството, което искате да удостоверите.
	ID	<p>Въведете ИД на скенера, което отговаря на вида на ИД.</p> <p>Не можете да използвате „@“, „#“ и „=“ за първия символ.</p> <p>Distinguished Name: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „=“.</p> <p>IP Address: въведете IPv4 или IPv6 формат.</p> <p>FQDN: въведете комбинация между 1 и 255 символа, като използвате A – Z, a – z, 0 – 9, „-“ и точка (.).</p> <p>Email Address: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Трябва да включите „@“.</p> <p>Key ID: въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа.</p>
	Pre-Shared Key	Ако изберете Pre-Shared Key за Authentication Method , въведете предварително споделен ключ между 1 и 127 знака.
	Confirm Pre-Shared Key	Въведете ключа, който сте конфигурирали за потвърждение.

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение	
Encapsulation	Ако изберете IPsec за Access Control , трябва да конфигурирате режим на капсулиране.	
	Transport Mode	Ако използвате скенера само на една и съща LAN мрежа, изберете това. Криптират се IP пакети от слой 4 или по-нов.
	Tunnel Mode	Ако използвате скенера в мрежа с възможности за интернет като IPsec-VPN, изберете тази опция. Криптират се заглавната част и данните на IP пакетите.
Remote Gateway(Tunnel Mode)	Ако изберете Tunnel Mode за Encapsulation , въведете адрес на шлюз между 1 и 39 знака.	
Security Protocol	Ако изберете IPsec за Access Control , изберете опция.	
	ESP	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните, както и криптирането на данните.
	AH	Изберете тази опция, за да гарантирате целостта на удостоверяването и данните. Дори ако криптирането на данни е забранено, можете да използвате IPsec.
Algorithm Settings		
IKE	Encryption	Изберете алгоритъма за криптиране на IKE. Елементите са различни в зависимост от версията на IKE.
	Authentication	Изберете алгоритъма за удостоверяване на IKE.
	Key Exchange	Изберете алгоритъма за размяна на ключове за IKE. Елементите са различни в зависимост от версията на IKE.
ESP	Encryption	Изберете алгоритъма за криптиране на ESP. Тази опция е достъпна, когато ESP е избран за Security Protocol .
	Authentication	Изберете алгоритъма за удостоверяване на ESP. Тази опция е достъпна, когато ESP е избран за Security Protocol .
AH	Authentication	Изберете алгоритъма за удостоверяване за AH. Тази опция е достъпна, когато AH е избран за Security Protocol .

Още по темата

- ➔ [“Конфигуриране на Group Policy” на страница 75](#)
- ➔ [“Комбинация от Local Address \(Scanner\) и Remote Address\(Host\) на Group Policy” на страница 80](#)
- ➔ [“Позовавания на име на услуга в груповата политика” на страница 80](#)

Разширени настройки за сигурност за корпорации

Комбинация от Local Address (Scanner) и Remote Address(Host) на Group Policy

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

*1 Ако IPsec е избрано за **Access Control**, не можете да определяте в дължината на префикса.

*2 Ако IPsec е избрано за **Access Control**, можете да изберете локален адрес за връзката (fe80::), но груповата политика ще бъде деактивирана.

*3 Освен 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	–	–	–	Всички услуги
ENPC	UDP	3289	Всеки порт	Търсене на скенер от приложения като EpsonNet Config и драйвера за скенер
SNMP	UDP	161	Всеки порт	Получаване и конфигуриране на MIB от приложения като EpsonNet Config и драйвера за скенер на Epson
WSD	TCP	Всеки порт	5357	Управление на WSD
WS-Discovery	UDP	3702	Всеки порт	Търсене на скенер от WSD
Network Scan	TCP	1865	Всеки порт	Пренасочване на данни от сканиране от Document Capture Pro
Network Push Scan Discovery	UDP	2968	Всеки порт	Търсене на компютър от скенера.
Network Push Scan	TCP	Всеки порт	2968	Получаване на информация за задание от push сканиране от Document Capture Pro или Document Capture
HTTP (Local)	TCP	80	Всеки порт	HTTP(S) сървър (пренасочване на данни на Web Config и WSD)
HTTPS (Local)	TCP	443	Всеки порт	

Разширени настройки за сигурност за корпорации

Име на услуга	Тип на протокола	Номер на локален порт	Номер на отдалечен порт	Управлявани функции
HTTP (Remote)	TCP	Всеки порт	80	HTTP(S) клиент (комуникация между надстройка на фърмуер и надстройка на основен сертификат)
HTTPS (Remote)	TCP	Всеки порт	443	

Примери за конфигурация на IPsec/IP Filtering

Приемане само на IPsec пакети

Този пример е за конфигуриране само на политика по подразбиране.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: IPsec
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: Въведете до 127 знака.

Group Policy:

Не конфигурирайте.

Приемане на сканиране с помощта на Epson Scan 2 и настройки на скенера

Този пример позволява комуникацията на данните за сканиране и конфигурацията на скенера от посочени услуги.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Поставете отметка в квадратчето.
- Access Control: Permit Access
- Remote Address(Host): IP адрес на клиент
- Method of Choosing Port: Service Name
- Service Name: Поставете отметка в квадратчето ENPC, SNMP, Network Scan, HTTP (Local) и HTTPS (Local).

Получаване на достъп само от определен IP адрес

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

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Поставете отметка в квадратчето.

Разширени настройки за сигурност за корпорации

- Access Control: Permit Access**
- Remote Address(Host):** IP адрес на клиент на администратора

Забележка:

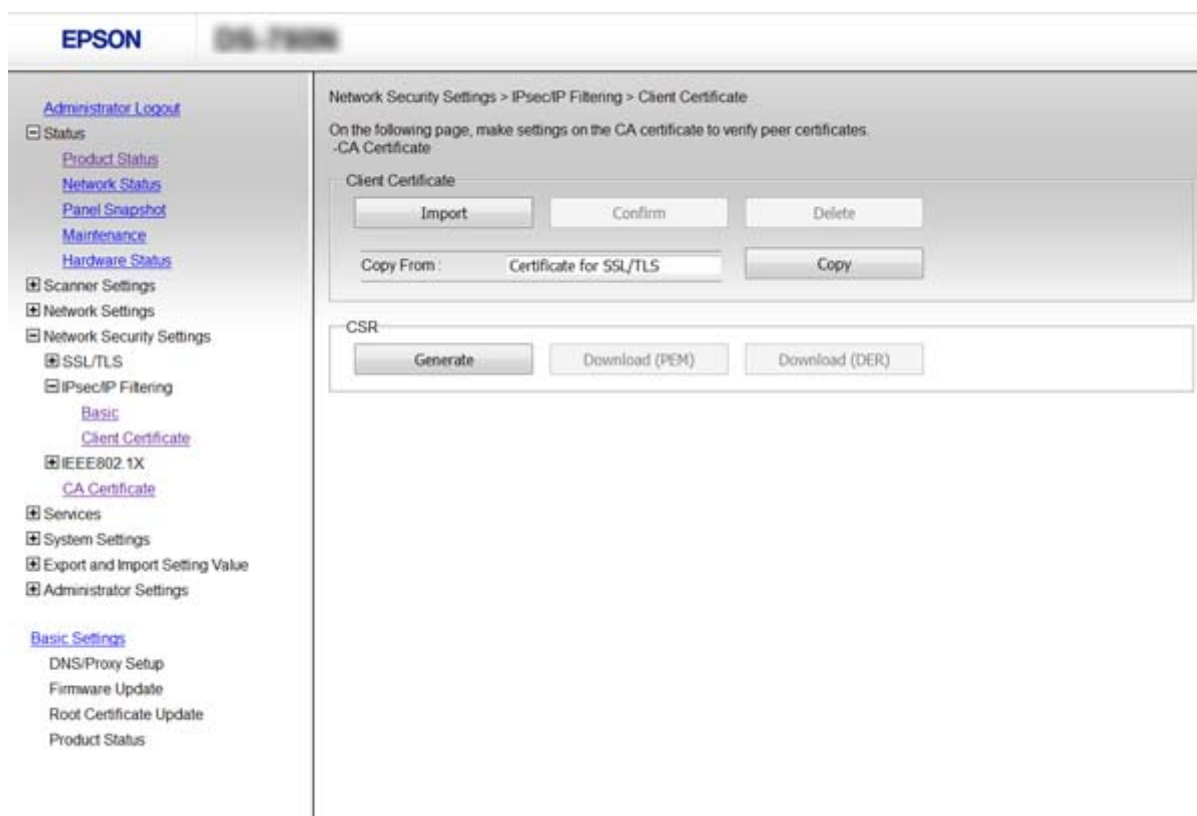
Независимо от конфигурацията на политиката клиентът ще има възможност за достъп и конфигуриране на скенера.

Конфигуриране на сертификат за IPsec/IP Filtering

Конфигурирайте сертификата на клиента за IPsec/IP филтриране. Ако искате да конфигурирате сертифициращ орган, отидете на **CA Certificate**.

1. Влезте в Web Config и изберете **Network Security Settings > IPsec/IP Filtering > Client Certificate**.
2. Импортирайте сертификата в **Client Certificate**.

Ако вече сте импортирали сертификат, публикуван от сертифициращ орган в IEEE802.1X или SSL/TLS, можете да копирате сертификата и да го използвате при IPsec/IP филтриране. За да копирате, изберете сертификата от **Copy From**, след което щракнете върху **Copy**.



Още по темата

- ➔ “Достъп до Web Config” на страница 23
- ➔ “Получаване и импортиране на сертификат, подписан от сертифициращ орган” на страница 64

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 сигурността.

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 скенерът поддържа протокола SNMPv3, можете да наблюдавате и контролирате достъпа до скенера.

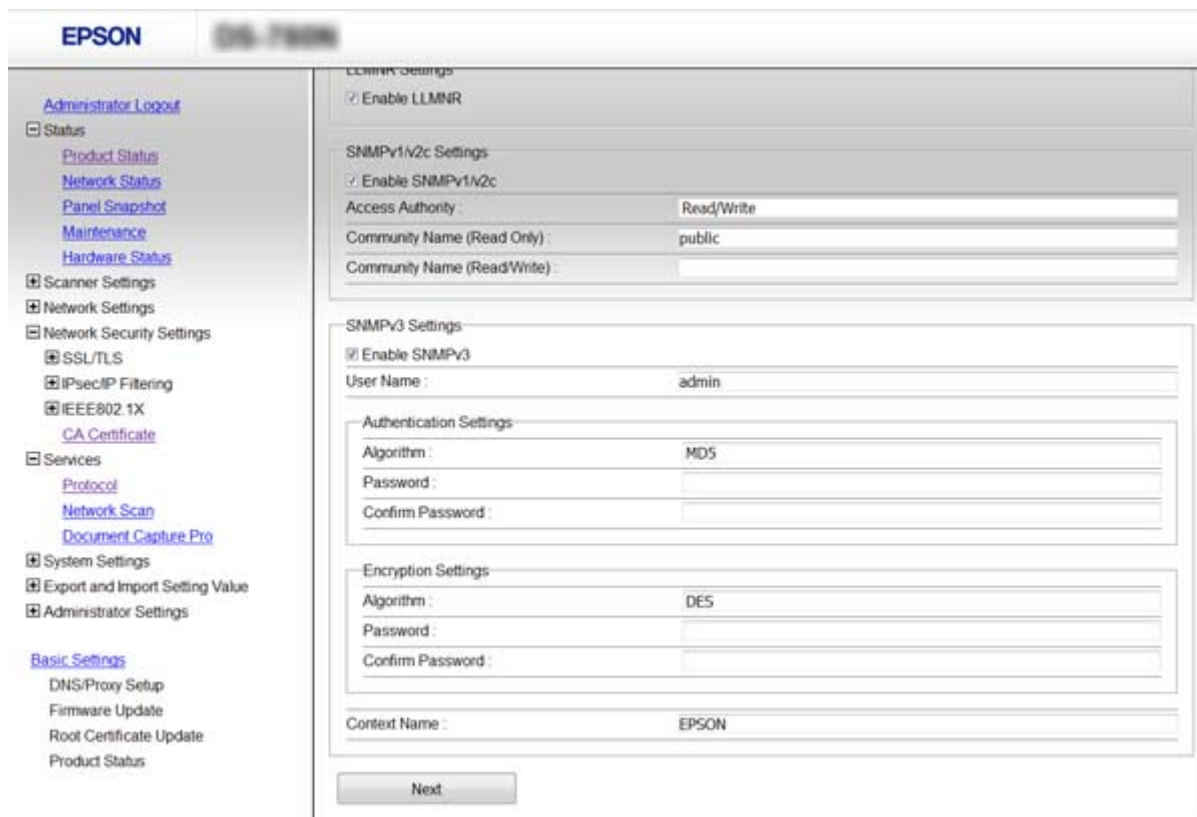
1. Влезте в Web Config и изберете **Services > Protocol**.
2. Въведете стойност за всеки елемент **SNMPv3 Settings**.
3. Щракнете върху **Next**.
Показва се съобщение за потвърждение.
4. Щракнете върху **OK**.
Скенерът се актуализира.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)
- ➔ [“Елементи за настройка на SNMPv3” на страница 84](#)

Разширени настройки за сигурност за корпорации

Елементи за настройка на SNMPv3



Елементи	Настройки и обяснение
Enable SNMPv3	SNMPv3 е активиран, когато има отметка в квадратчето.
User Name	Въведете между 1 и 32 знака с помощта на символи от 1 байт.
Authentication Settings	
Algorithm	Изберете алгоритъм за удостоверяване.
Password	Въведете между 8 и 32 знака в ASCII (0x20-0x7E).
Confirm Password	Въведете паролата, която сте конфигурирали, за потвърждение.
Encryption Settings	
Algorithm	Изберете алгоритъм за криптиране.
Password	Въведете между 8 и 32 знака в ASCII (0x20-0x7E).
Confirm Password	Въведете паролата, която сте конфигурирали, за потвърждение.
Context Name	Въведете между 1 и 32 знака с помощта на символи от 1 байт.

Още по темата

➔ [“Конфигуриране на SNMPv3” на страница 83](#)

Свързване на скенера към мрежа IEEE802.1X

Конфигуриране на мрежа IEEE802.1X

Ако скенерът поддържа IEEE802.1X, можете да използвате скенера в мрежа с удостоверяване, която е свързана към RADIUS сървър и концентратор като удостоверявател.

1. Влезте в Web Config и изберете **Network Security Settings > IEEE802.1X > Basic**.
2. Въведете стойност за всеки елемент.
3. Щракнете върху **Next**.
Показва се съобщение за потвърждение.
4. Щракнете върху **OK**.
Скенерът се актуализира.

Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)
- ➔ [“Елементи за настройка на мрежа IEEE802.1X” на страница 85](#)
- ➔ [“Няма достъп до принтера или скенера след конфигуриране на IEEE802.1X” на страница 90](#)

Елементи за настройка на мрежа IEEE802.1X

The screenshot displays the Epson Web Config interface for configuring IEEE802.1X. The left sidebar shows a navigation menu with categories like Status, Scanner Settings, Network Settings, and Network Security Settings. The main content area is titled 'Network Security Settings > IEEE802.1X > Basic' and contains the following configuration options:

- IEEE802.1X (Wired LAN): Enable Disable
- EAP Type: EAP-TLS
- User ID: [Text input field]
- Password: [Text input field]
- Confirm Password: [Text input field]
- Server ID: [Text input field]
- Certificate Validation: Enable Disable
- Anonymous Name: [Text input field]
- Encryption Strength: Middle

A 'Next' button is located at the bottom of the configuration area.

Разширени настройки за сигурност за корпорации

Елементи	Настройки и обяснение	
IEEE802.1X (Wired LAN)	Можете да разрешите или забраните настройки на страницата (IEEE802.1X > Basic) за IEEE802.1X (кабелна LAN).	
EAP Type	Изберете опция за метод на удостоверяване между скенера и RADIUS сървъра.	
	EAP-TLS	Трябва да получите и да импортирате сертификат, подписан от сертифициращ орган.
	PEAP-TLS	
	PEAP/MSCHAPv2	Трябва да конфигурирате парола.
User ID	Конфигурирайте ИД, което да се използва за удостоверяване на RADIUS сървъра. Въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа.	
Password	Конфигурирайте парола за удостоверяване на скенера. Въведете от 1 до 128 1-байтови ASCII (0x20 до 0x7E) символа. Ако използвате Windows сървър като RADIUS сървър, можете да въведете до 127 символа.	
Confirm Password	Въведете паролата, която сте конфигурирали, за потвърждение.	
Server ID	Можете да конфигурирате ИД на сървър за удостоверяване с посочения RADIUS сървър. Удостоверителят проверява дали ИД на сървъра се съдържа в полето subject/subjectAltName на сертификата на сървъра, който е изпратен от RADIUS сървър. Въведете от 0 до 128 1-байтови ASCII (0x20 до 0x7E) символа.	
Certificate Validation	Можете да зададете проверка на сертификата без оглед на метода на удостоверяване. Импортирайте сертификата в CA Certificate .	
Anonymous Name	Ако изберете PEAP-TLS или PEAP/MSCHAPv2 за Authentication Method , можете да конфигурирате анонимно име вместо ИД на потребител за фаза 1 на PEAP удостоверяване. Въведете от 0 до 128 1-байтови ASCII (0x20 до 0x7E) символа.	
Encryption Strength	Можете да изберете едно от следните.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Още по темата

➔ [“Конфигуриране на мрежа IEEE802.1X” на страница 85](#)

Конфигуриране на сертификат за IEEE802.1X

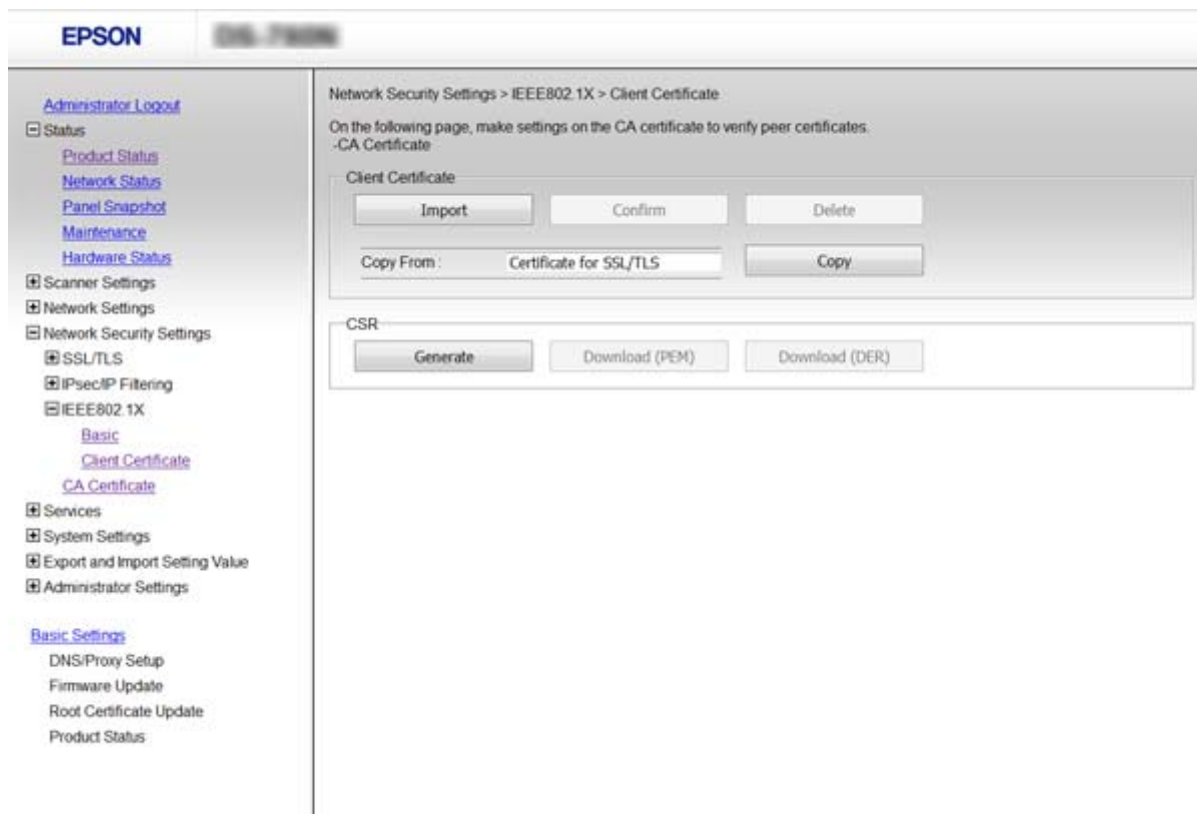
Конфигуриране на клиентски сертификат за IEEE802.1X. Ако искате да конфигурирате сертификата на сертифициращия орган, отидете на **CA Certificate**.

1. Влезте в Web Config и изберете **Network Security Settings > IEEE802.1X > Client Certificate**.

Разширени настройки за сигурност за корпорации

2. Въведете сертификата в Client Certificate.

Можете да копирате сертификата, ако е публикуван от сертифициращ орган. За да копирате, изберете сертификата от **Copy From**, след което щракнете върху **Copy**.



Още по темата

- ➔ [“Достъп до Web Config” на страница 23](#)
- ➔ [“Получаване и импортиране на сертификат, подписан от сертифициращ орган” на страница 64](#)

Решаване на проблеми за повишена защита

Възстановяване на настройките за сигурност

Когато установите силно защитена среда, например IPsec/IP филтриране или IEEE802.1X, е възможно да не можете да комуникирате с устройствата поради неправилни настройки или проблеми с устройството или сървъра. В този случай възстановете настройките за сигурност на устройството, за да направите отново настройките или за да получите временен достъп.

Забраняване на използване на функцията за сигурност от контролен панел

Можете да забраните IPsec/IP филтриране или IEEE802.1X от контролния панел на скенера.

1. Докоснете **Настройки > Настройки на мрежата**.

Разширени настройки за сигурност за корпорации

2. Натиснете **Промяна на настройки**.
3. Докоснете елементите, които искате да забраните.
 - IPsec/IP филтриране
 - IEEE802.1X
4. Когато се появи съобщение, указващо завършване, докоснете **Продължи**.

Възстановяване на функциите за сигурност с Web Config

При IEEE802.1X устройствата в мрежата може да не бъдат разпознати. В този случай забранете функцията от контролния панел на скенера.

При IPsec/IP филтриране можете да забраните функцията, ако имате достъп до устройството от компютъра.

Забраняване на IPsec/IP филтриране от Web Config

1. Влезте в Web Config и изберете **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Изберете **Disable** за **IPsec/IP Filtering** в **Default Policy**.
3. Щракнете върху **Next**, после изчистете **Enable this Group Policy** за всички групови политики.
4. Щракнете върху **OK**.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Проблеми при използване на функциите за мрежова сигурност

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 > IPsec/IP Filtering > Basic > Default Policy** или **Group Policy**.

Когато промените предварително споделения ключ, конфигурирайте го за компютри.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

Разширени настройки за сигурност за корпорации

Не може да комуникира с IPsec комуникация

Използвате ли неподдържан алгоритъм за настройките на компютъра?

Скенераът поддържа следните алгоритми.

Методи за защита	Алгоритми
IKE алгоритъм за криптиране	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE алгоритъм за удостоверяване	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE алгоритъм за размяна на ключове	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP алгоритъм за криптиране	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP алгоритъм за удостоверяване	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH алгоритъм за удостоверяване	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Възможно само за IKEv2

Още по темата

➔ [“Криптирана комуникация с IPsec/IP филтриране” на страница 71](#)

Не може да комуникира внезапно

Невалиден ли е IP адресът на скенера или е променен?

Забранете IPsec от контролния панел на скенера.

Ако DHCP е остарял, рестартирането или IPv6 адресът е остарял или не е получен, регистрираният за скенера IP адрес за Web Config (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Local Address (Scanner)**) може да не бъде намерен.

Използвайте статичен IP адрес.

Невалиден ли е IP адресът на компютъра или е променен?

Забранете IPsec от контролния панел на скенера.

Ако DHCP е остарял, рестартирането или IPv6 адресът е остарял или не е получен, регистрираният за скенера IP адрес за Web Config (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Remote Address(Host)**) може да не бъде намерен.

Използвайте статичен IP адрес.

Още по темата

➔ [“Достъп до Web Config” на страница 23](#)

➔ [“Криптирана комуникация с IPsec/IP филтриране” на страница 71](#)

Разширени настройки за сигурност за корпорации

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 скенера. Свържете скенера и компютъра и отново конфигурирайте настройките за IPsec/IP филтриране.

Още по темата

➔ [“Криптирана комуникация с IPsec/IP филтриране” на страница 71](#)

Няма достъп до принтера или скенера след конфигуриране на IEEE802.1X

Възможно е настройките да са грешни.

Деактивирайте IEEE802.1X от контролния панел на скенера. Свържете скенера и компютъра и след това конфигурирайте отново IEEE802.1X.

Още по темата

➔ [“Конфигуриране на мрежа IEEE802.1X” на страница 85](#)

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 скенера CSR след изпращането ѝ на сертифициращ орган?
Получете сертификата, подписан от сертифициращ орган, отново с CSR.

Дали сертификатът, подписан от сертифициращ орган, е по-голям 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?

Ако забравите паролата си, не можете да импортирате сертификата.

Още по темата

➔ [“Импортиране на сертификат, подписан от сертифициращ орган” на страница 66](#)

Разширени настройки за сигурност за корпорации

Не може да се актуализира самоподписан сертификат

Въведено ли е Common Name?

Трябва да е въведено Common Name.

Въведени ли са неподдържани знаци за Common Name? Например, не се поддържа японски език.

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?

Ако е въведена запетая, Common Name 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 68](#)

Не може да се създаде CSR

Въведено ли е Common Name?

Трябва да е въведено Common Name.

Въведени ли са неподдържани знаци за Common Name, Organization, Organizational Unit, Locality, State/Province? Например, не се поддържа японски език.

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

Включени ли са запетая или интервал в Common Name?

Ако е въведена запетая, Common Name 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 64](#)

Появява се предупреждение за цифров сертификат

Съобщения	Причина/Какво да се направи
Enter a Server Certificate.	Причина: Не сте избрали файл за импортиране. Какво да се направи: Изберете файл и щракнете върху Import .

Разширени настройки за сигурност за корпорации

Съобщения	Причина/Какво да се направи
CA Certificate 1 is not entered.	<p>Причина: Сертификат на сертифициращ орган 1 не е въведен, а е въведен само сертификат на сертифициращ орган 2.</p> <p>Какво да се направи: Импортирайте първо сертификат на сертифициращ орган 1.</p>
Invalid value below.	<p>Причина: Неподдържани знаци се съдържат в пътя до файла и/или паролата.</p> <p>Какво да се направи: Уверете се, че знаците за елемента са въведени правилно.</p>
Invalid date and time.	<p>Причина: Не са зададени дата и час на скенера.</p> <p>Какво да се направи: Задайте дата и час с помощта на Web Config или EpsonNet Config.</p>
Invalid password.	<p>Причина: Зададената за сертификат на сертифициращ орган парола и въведената парола не съвпадат.</p> <p>Какво да се направи: Въведете правилната парола.</p>
Invalid file.	<p>Причина: Не импортирате файл със сертификат в X509 формат.</p> <p>Какво да се направи: Уверете се, че сте избрали правилния сертификат, изпратен от надежден сертифициращ орган.</p>
	<p>Причина: Импортираният файл е твърде голям. Максималният размер на файла е 5 KB.</p> <p>Какво да се направи: Ако сте избрали правилния файл, сертификатът може да е повреден или подправен.</p>
	<p>Причина: Веригата, съдържаща се в сертификата, е невалидна.</p> <p>Какво да се направи: За повече информация относно сертификата вижте уеб сайта на сертифициращия орган.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p>Причина: Файлът на сертификата в PKCS#12 формат съдържа повече от 3 сертификата на сертифициращ орган.</p> <p>Какво да се направи: 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>

Разширени настройки за сигурност за корпорации

Съобщения	Причина/Какво да се направи
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p>Причина: Сертификатът е изтекъл.</p> <p>Какво да се направи:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ако сертификатът е изтекъл, получите и импортирайте нов сертификат. <input type="checkbox"/> Ако сертификатът не е изтекъл, се уверете, че датата и часът на скенера са настроени правилно.
Private key is required.	<p>Причина: Няма сдвоен личен ключ със сертификата.</p> <p>Какво да се направи:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ако сертификатът е в PEM/DER формат и е получен от CSR с помощта на компютър, посочете файла с личен ключ. <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.
	<p>Причина: Импортирали сте повторно PEM/DER сертификата, получен от CSR с помощта на Web Config.</p> <p>Какво да се направи: 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.	<p>Причина: Конфигурацията не може да се завърши, тъй като комуникацията между скенера и компютъра е неуспешна или файлът не може да се прочете поради някакви грешки.</p> <p>Какво да се направи: След проверка на дадения файл и комуникацията, импортирайте файла отново.</p>

Още по темата

➔ [“Относно цифрово сертифициране” на страница 63](#)

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 изтрит сертификат отново. Създайте CSR и получите нов сертификат.

Още по темата

➔ [“Изтриване на сертификат, подписан от сертифициращ орган” на страница 68](#)

➔ [“Импортиране на сертификат, подписан от сертифициращ орган” на страница 66](#)