EPSON
EXCEED YOUR VISION

Водич за администратори

NPD5668-00 MK

Содржина

Содржина

Додаток

Напредни безбедносни поставки за претпријатија

Авторски права

Трговски марки

- ❏ EPSON® е регистрирана заштитена трговска марка, а EPSON EXCEED YOUR VISION или EXCEED YOUR VISION е заштитена трговска марка на корпорацијата Seiko Epson.
- ❏ 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.
- ❏ Општо известување: Останатите имиња на производи што се употребени овде се наменети само за идентификување и може да се трговски марки на нивните сопственици. Epson се одрекува од сите права на овие марки.

Во врска со овој прирачник

Ознаки и симболи

> ***Внимание:***
> *Упатства коишто мора да ги следите внимателно за да избегнете телесна повреда.*

> ***Важно:***
> *Упатства коишто мора да ги следите за да избегнете оштетување на опремата.*

Белешка:
Упатства коишто содржат корисни совети и ограничувања за функционирањето на скенерот.

Поврзани информации

➡ Со кликнување на оваа икона имате пристап до поврзаните информации.

Описи што се користат во прирачникот

❏ Кадрите на екранот од двигателот за скенерот и екраните за Epson Scan 2 (двигателот за скенерот) се од Windows 10 или OS X El Capitan. Содржината што е прикажана на екраните се разликува во зависност од моделот и ситуацијата.

❏ Илустрациите коишто се користат во прирачников се само примери. Иако може да има мали разлики, зависно од моделот, начинот на ракување е ист.

❏ Некои од ставките на менито на LCD-екранот се разликуваат, зависно од моделот и поставките.

Референци за оперативни системи

Windows

Во овој прирачник термините како на пример „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 однесуваат на следниве оперативни системи. Освен тоа, „Windows“ се користи како референца за сите верзии.

❏ Microsoft® Windows® 10 оперативен систем

❏ Microsoft® Windows® 8.1 оперативен систем

❏ Microsoft® Windows® 8 оперативен систем

❏ Microsoft® Windows® 7 оперативен систем

❏ Microsoft® Windows Vista® оперативен систем

Во врска со овој прирачник

- ❏ Microsoft® Windows® XP оперативен систем
- ❏ Microsoft® Windows® XP Professional x64 Edition оперативен систем
- ❏ Microsoft® Windows Server® 2016 оперативен систем
- ❏ Microsoft® Windows Server® 2012 R2 оперативен систем
- ❏ Microsoft® Windows Server® 2012 оперативен систем
- ❏ Microsoft® Windows Server® 2008 R2 оперативен систем
- ❏ Microsoft® Windows Server® 2008 оперативен систем
- ❏ Microsoft® Windows Server® 2003 R2 оперативен систем
- ❏ Microsoft® Windows Server® 2003 оперативен систем

Mac OS

Во овој прирачник, „Mac OS“ се однесува на 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.

Вовед

Manual Component

Овој прирачник е за администраторот на уредот којшто е задолжен за поврзување на печатачот или скенерот со мрежата и содржи информации за тоа како да правите поставки за да ги употребувате функциите.

Видете го *Упатство за корисникот* околу информации за искористеност на функцијата.

Подготовка

Се објаснуваат задачите на администраторот, како да ги поставува уредите и софтверот за управување.

Конекција

Се објаснува како да се поврзе уред со мрежа или телефонска линија. Исто така, се објаснува средината на мреќата како што е употребата на порти за уредот, информации за DNS и прокси серверот.

Поставки за функција

Се објаснуваат поставките за секоја функција на уредот.

Основни безбедносни поставки

Се објаснуваат поставките за секоја функција, како што е печатење, скенирање и праќање факс.

Поставки за работење и менаџирање

Се објаснуваат операциите откако ќе се започне со употреба на уреди, како што е проверката на информации и одржувањето.

Решавање на проблеми

Се објаснуваат поставките за иницијализацијата и решавањето проблеми за мрежата.

Напредни безбедносни поставки за претпријатија

Се објаснува методот на поставки за подобрување на безбедноста на уредот, како што е употреба на CA сертификат, SSL/TLS комуникација и IPsec/IP филтрирање.

Во зависност од моделот одредени функции во ова поглавје не се поддржани.

Дефиниции на термини користени во овој водич

Во овој водич се користат следниве термини.

Администратор

Лицето задолжено за инсталирање и поставување на уредот или мрежата во канцеларија или организација. Во случај на мали организации ова лице може да е задолжено за администрирање и со уредот и со мрежата. Во случај на големи организации администраторите имаат авторитет над мрежата или уредите во

групната единица составена од оддел или дивизија, а администраторите за мрежата се задолжени за поставките за комуникацијата пошироко од самата организација, како, на пример, интернетот.

Администратор за мрежа

Лицето задолжено за контрола на комуникацијата во мрежата. Лицето што го поставува рутерот, proxy серверот, DNS серверот и серверот за пошта за да се постигне контрола над комуникацијата на интернет или во мрежата.

Корисник

Лицето што ги користи уредите како печатачите или скенерите.

Web Config (веб-страница за уредот)

Веб-серверот што е направен во уредот. Се нарекува Web Config. На него може да го проверите и да го промените статусот на печатачот со помош на прелистувачот.

Алатка

Генерички термин за софтвер за поставување или менаџирање со уред, како што е Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, итн.

Push скенирање

Генерички термин за скенирање од контролниот панел на уредот.

ASCII (Американски стандарден код за размена на информации)

Еден од стандардните кодови за карактери. Дефинирани се 128 карактери, вклучувајќи карактери како азбучни букви (a–z, A–Z), арапски броеви (0–9), симболи, празни карактери и контролни карактери. Кога во овој водич се опишува „ASCII“, индицира 0x20–0x7E (хексадецимален број) именувано подолу и не вклучува контролни карактери.

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	{	|	}	~	

* Знак за празно место.

Unicode (UTF-8)

Интернационален стандарден код што ги опфаќа главните глобални јазици. Кога се опишува „UTF-8“ во овој водич, тој индицира карактери за кодирање во UTF-8 формат.

Подготовка

Ова поглавје ја објаснува улогата на администраторот и подготовката пред да се направат поставките.

Текот на поставките и менаџирањето со скенерот

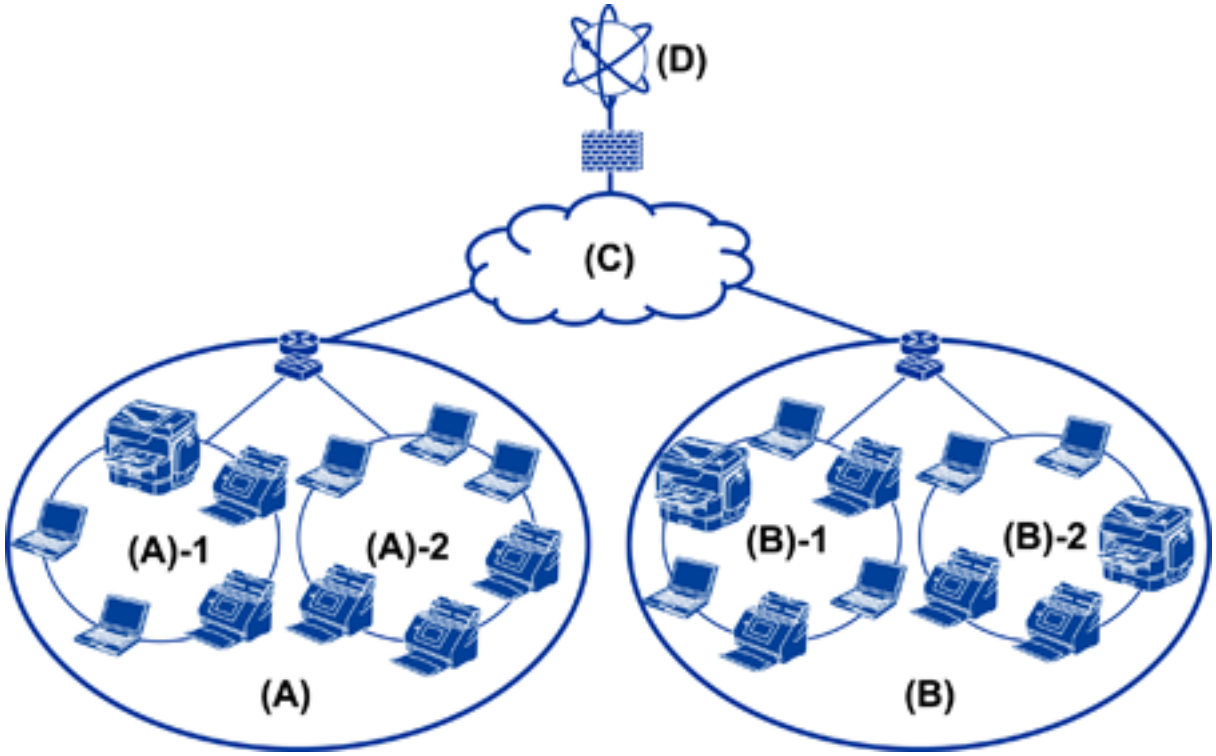
Администраторот ги прави поставките за мрежната конекција, иницијалното поставување и одржувањето за скенерот за да може да биде достапен на корисници.

1. Подготовка
   - ❏ Собирање информации за поставувањето на конекцијата
   - ❏ Одлучување околу методот на конекција
2. Поврзување
   - ❏ Мрежна конекција од контролниот панел на скенерот
3. Поставување на функциите
   - ❏ Поставки за скенерот на печатачот
   - ❏ Други напредни поставки
4. Безбедносни поставки
   - ❏ Администраторски поставки
   - ❏ SSL/TLS
   - ❏ Контрола на протокол
   - ❏ Напредни безбедносни поставки (опционално)
5. Работење и менаџирање
   - ❏ Проверување на состојбата на драјверот
   - ❏ Ракување при итни случаи
   - ❏ Резервна копија на поставките за уредот

Поврзани информации

➡ „Подготовка“ на страница 10
➡ „Конекција“ на страница 15
➡ „Поставки за функција“ на страница 22
➡ „Основни безбедносни поставки“ на страница 32
➡ „Поставки за работење и менаџирање“ на страница 40

Пример за средина на мрежата



(A): Канцеларија 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Канцеларија 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Интернет

Пример за поставка за воведување на конекција на скенер

Има два типа на конекција во зависност од тоа како го користите скенерот. И на двата начина може да го поврзете скенерот на мрежата со компјутер преку hub.

❏ Конекција со сервер/клиент (скенер со Windows сервер, управување со задачи)

❏ Peer to Peer конекција (директна конекција од компјутер на клиент)

Поврзани информации

➡ „Конекција со сервер/клиент“ на страница 12

➡ „Peer to Peer конекција“ на страница 12

Конекција со сервер/клиент

Централизирајте го скенерот и уредувањето на задачата со Document Capture Pro Server инсталиран на серверот. Најпогоден е за работи за коишто се употребуваат повеќе секнери за скенирање на голем број на документи во одреден формат.

Поврзани информации

➡ „Дефиниции на термини користени во овој водич“ на страница 8

Peer to Peer конекција

Користете поединечен скенер со двигател за скенер како на пример Epson Scan 2 инсталиран на компјутерот на клиент. Со инсталирање на Document Capture Pro (Document Capture) на компјутерот на клиент може да вршите задачи на поединечните компјутери на клиент на скенерот.

Поврзани информации

➡ „Дефиниции на термини користени во овој водич“ на страница 8

Подготовка на конекција за мрежа

Собирање информации за поставувањето на конекцијата

За мрежната конекција треба да имате IP адреса, адреса на капија итн. Проверете го следново однапред.

Поделби	Ставки	Забелешка
Метод на поврзување уред	❏ Ethernet	Користете кабел од категорија 5e или повисок STP (Shielded Twisted Pair) за Ethernet конекција.
Информации за LAN конекција	❏ IP адреса ❏ Подмрежна маска ❏ Стандардна капија	Ако автоматски ја поставите IP адресата со функцијата DHCP на рутерот, тогаш не е потребно.
Информации за DNS сервер	❏ IP адреса за примарен DNS ❏ IP адреса за секундарен DNS	Ако употребувате статична IP адреса, конфигурирајте го DNS серверот. Конфигурирајте кога назначувате автоматски со помош на функцијата DHCP и кога DNS серверот не може да биде назначен автоматски.
Информации за Proxy сервер	❏ Име на Proxy сервер ❏ Број на порта	Конфигурирајте кога употребувате proxy сервер за интернет конекција и кога ја употребувате услугата Epson Connect или функцијата за автоматско ажурирање на фирмверот.

Спецификации на скенерот

За спецификацијата дека скенерот поддржува стандарден режим или режим на конекција, видете *Упатство за корисникот*.

Употреба на број на порта

Види „Додаток“ за бројот на порта којашто ја употребува скенерот.

Поврзани информации

➡ „Употреба на порта за скенерот“ на страница 60

Назначување тип на IP адреса

Постојат два типа за назначување IP адреси за скенер.

Статична IP адреса:

Назначете ја претходно одредената уникатна IP адреса за скенерот.

IP адресата не е променета дури и кога се исклучуваат скенерот или рутерот за да може да управувате со уредот преку IP адреса.

Овој тип одговара за мрежа каде што се управува со голем број скенери како што е голема канцеларија или училиште.

Автоматско назначување преку DHCP функција:

Правилната IP адреса се назначува автоматски кога е успешна комуникацијата меѓу скенерот и рутерот којшто поддржува DHCP функција.

Ако е непригодно да се смени IP адреса за одреден уред, резервирајте ја IP адресата однапред и потоа назначете ја.

DNS сервер и Proxy сервер

Ако употребувате сервис за поврзување со интернетот, конфигурирајте го DNS серверот. Ако не го конфигурирате, треба да ја наведете IP адресата за пристапување бидејќи разрешувањето на името може да биде неуспешно.

Proxy серверот е поставен на преминот меѓу мрежата и интернетот и комуницира со компјутерот, скенерот, интернетот (спротивен сервер) во име на секое од нив. Спротивниот сервер комуницира само со proxy серверот. Според тоа, информациите за скенерот како што е IP адресата и бројот на порти не може да се прочита и се очекува зголемена безбедност.

Можете да забраните пристап до специфични URL со помош на функцијата за филтрирање, бидејќи proxy серверот може да ја провери содржината на комуникацијата.

Метод за поставување на мрежна конекција

Продолжете на следниов начин околу поставките за конекција за IP адреса на скенер, подмрежна маска и вообичаена капија.

Употреба на контролниот панел:

Конфигурирајте ги поставките за секој скенер со помош на контролниот панел. Поврзете се со мрежата по конфигурирањето на поставките за конекција на скенерот.

Подготовка

Употреба на датотеката за инсталација:

Ако е употребена датотеката за инсталација, мрежата на скенерот и компјутерот на клиентот се поставуваат автоматски. Поставката е достапна ако се следат инструкциите за датотеката за инсталација, дури и ако немате големи познавања од мрежата.

Употреба на алатка:

Употребете алатка од компјутерот на администраторот. Можете да откриете скенер и потоа да го поставите скенерот или да содадете SYLK датотека за да правите групни поставки за печатачи. Можете да поставите многу скенери, но треба да бидат физички поврзани со Ethernet кабел пред поставување. Според тоа, ова се препорачува ако можете да направите Ethernet за поставката.

Поврзани информации

- „Поврзување со мрежата преку контролниот панел“ на страница 15
- „Поврзување со мрежата со помош на датотеката за инсталација“ на страница 19
- „Назначува на IP адреса со EpsonNet Config“ на страница 56

Конекција

Ова поглавје ја објаснува средината или процедурата на поврзување на скенерот со мрежата.

Поврзување со мрежа

Поврзување со мрежата преку контролниот панел

Поврзете го скенерот преку контролниот панел на скенерот.

За повеќе детали околу контролниот панел на скенерот, погледнете во *Упатство за корисникот*.

Назначување на IP адресата

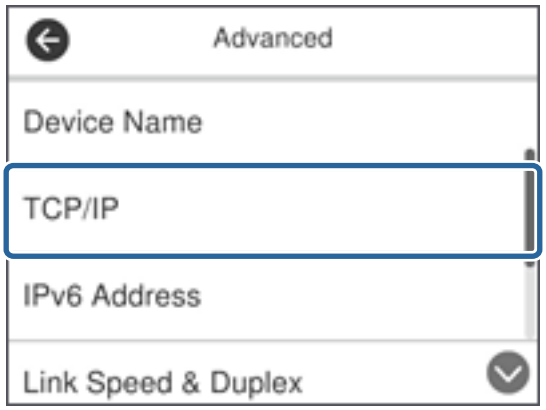
Поставете основни ставки како IP адреса, Маска на подмрежа, и Стандарден излез.

1. Вклучете го скенерот.
2. Придвижете го екранот кон десно на контролниот панел на скенерот и потоа допрете на **Поставки**.

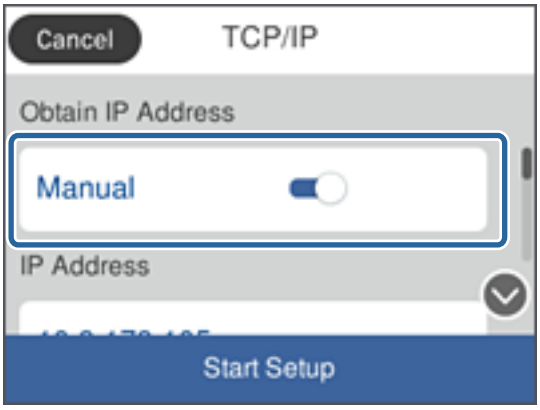
3. Допрете **Поставки за мрежа** > **Промени поставки**.

   Ако ставката не е прикажана, благо придвижете го нагоре екранот за да се прикаже.

4. Допрете **TCP/IP**.

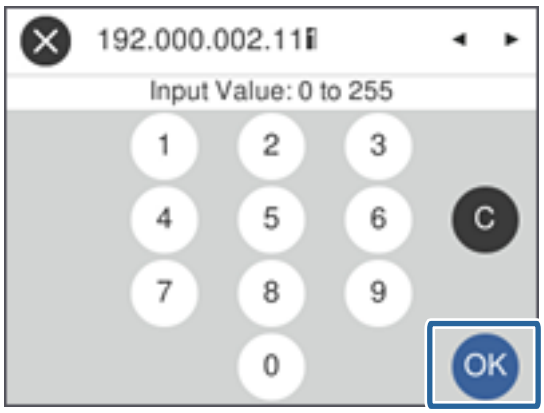


5. Одберете **Рачно** за **Добиј IP Адреса**.



Белешка:
Кога автоматски ја поставувате IP адресата со функцијата DHCP на рутерот, одберете ***Автоматски****. Во тој случај* ***IP адреса****,* ***Маска на подмрежа****, и* ***Стандарден излез*** *од чекорите 6 до 7 се исто така автоматски извршени, така што преминете на чекорот 8.*

6. Допрете на полето **IP адреса**, внесете ја IP адресата со помош на тастатурата прикажана на екранот и допрете на **Во ред**.



Потврдете ја вредноста прикажана на претходниот екран.

7. Поставете ги **Маска на подмрежа** и **Стандарден излез**.

   Потврдете ја вредноста прикажана на претходниот екран.

   Белешка:
   *Ако кобминацијата на IP адреса, Маска на подмрежа и Стандарден излез е неправилна, **Започни со поставување** е неактивно и не може да се продолжи со поставките. Потврдете дека нема грешка во внесеното.*

8. Допрете на полето **Примарен DNS** за **DNS Сервер**, внесете ја IP адресата за примарниот DNS сервер со помош на тастатурата прикажана на екранот и потоа допрете на **Во ред**.

   Потврдете ја вредноста прикажана на претходниот екран.

   Белешка:
   *Кога одбирате **Автоматски** за поставките за назначување на IP адреса, можете да ги одберете поставките за DNS сервер од **Рачно** или **Автоматски**. Ако не можете автоматски да добиете адреса за DNS сервер, одберете **Рачно** и внесете ја адресата за DNS серверот. Потоа директно внесете ја втората адреса за DNS сервер. Ако одберете **Автоматски**, одете на чекор 10.*

9. Допрете на полето **Секундарен DNS**, внесете ја IP адресата за секундарниот DNS сервер со помош на тастатурата прикажана на екранот и потоа допрете на **Во ред**.

   Потврдете ја вредноста прикажана на претходниот екран.

10. Допрете **Започни со поставување**.

11. Допрете на **Затвори** на екранот за потврда.

    Екранот автоматски се затвора по одреден временски период ако не допрете на **Затвори**.

Поврзување со Ethernet

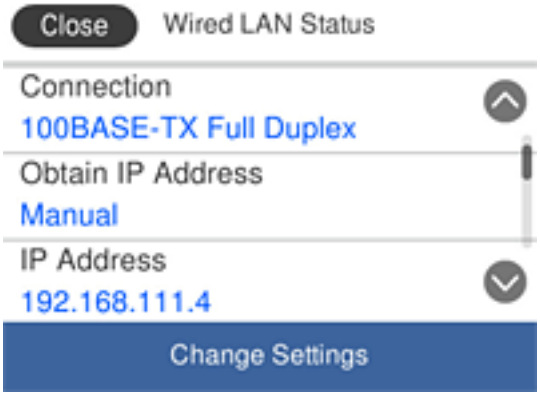
Поврзете го скенерот со мрежата со употреба на Ethernet кабел и проверете ја конекцијата.

1. Поврзете го скенерот и hub (прекинувач L2) преку Ethernet кабел.

   Иконата на почетниот екран се менува во  .

2. Допрете на  од почетниот екран.

3. Придвижете екранот нагоре и погрижете се дека статусот на конекцијата и IP адресата се точни.



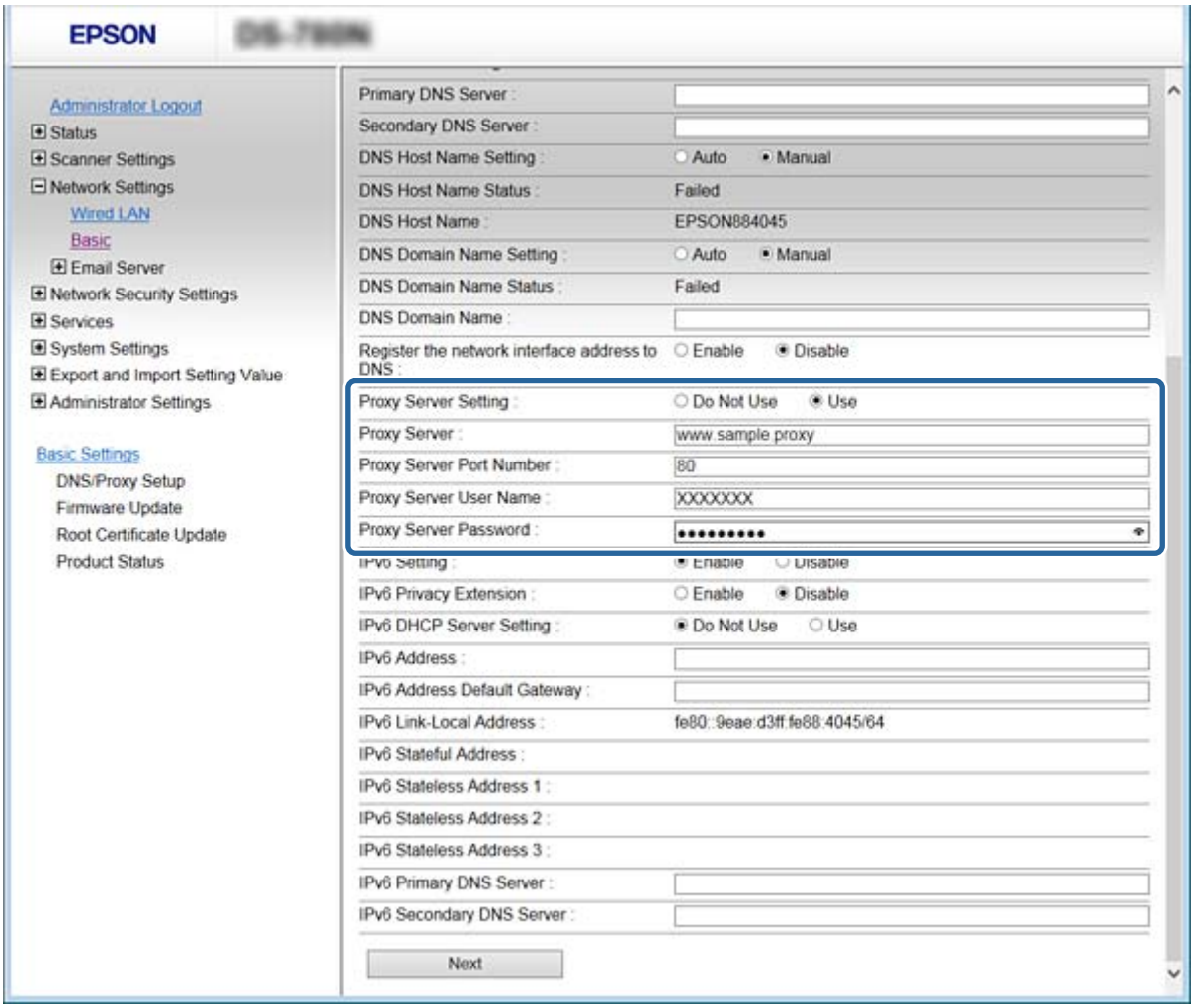
Поставување на proxy сервер

Не може да го поставите прокси серверот на таблата. Конфигурирајте го со користење на Web Config.

1. Пристапете до Web Config и одберете **Network Settings** > **Basic**.
2. Изберете **Use** во **Proxy Server Setting**.
3. Одредете го прокси серверот во IPv4 адресата или FQDN формат во **Прокси-сервер** и внесете го бројот на портата во **Proxy Server Port Number**.

   За прокси сервери за коишто е потребна автентикација, внесете го корисничкото име за автентикација на прокси сервер и лозинката за автентикација за проски сервер.

4. Кликнете на копчето **Next**.



5. Потврдете ги поставките и кликнете на **Поставки**.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Поврзување со мрежата со помош на датотеката за инсталација

Препорачуваме да ја употребувате датотеката за инсталација за да го поврзете скенерот со компјутер. Може да ја активирате датотеката за инсталација со користење на една од следниве методи.

❏ Поставување преку интернет страница

Посетете ја следната интернет страница и внесете го името на производот. Одете во **Поставување** и почнете со поставувањето.

http://epson.sn

❏ Поставување со помош на софтверски диск (само за моделите што доаѓаат со софтверски диск и корисници со компјутери со читачи за дискови).

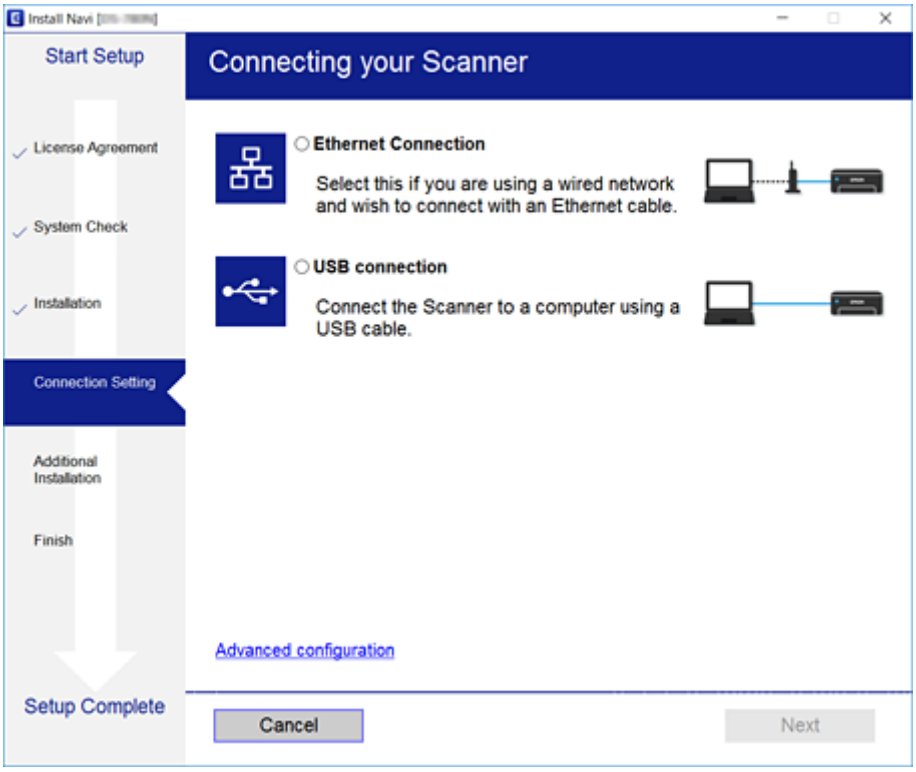
Внесете го дискот со софтвер во компјутерот и следете ги упатствата на екранот.

Избирање на методот на конекција

Следете ги упатствата на екранот додека не се прикаже следниот екран и потоа одберете го методот на поврзување на скенерот со компјутерот.

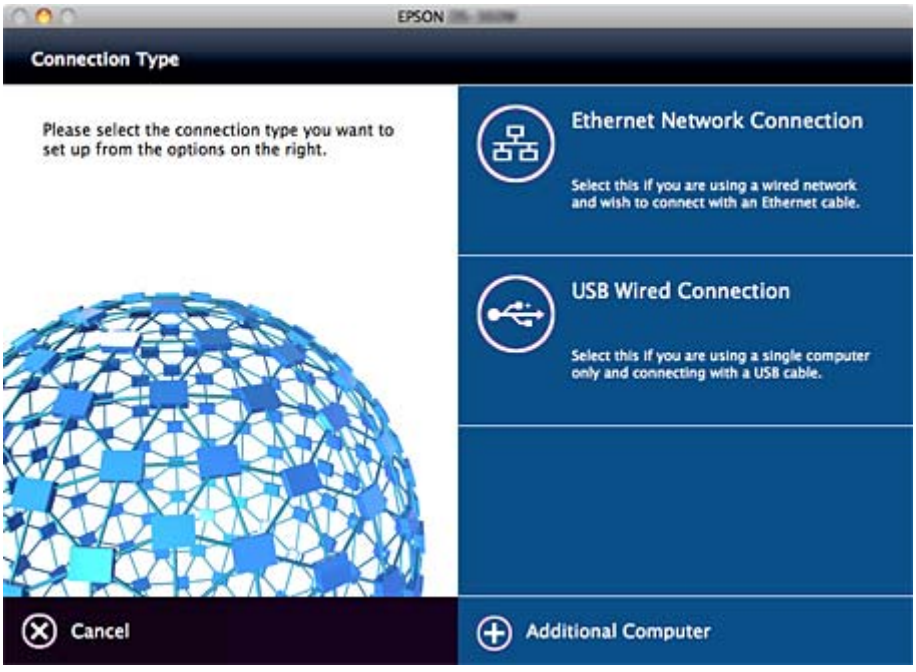
❏ Windows

Изберете го типот на конекција и потоа кликнете на **Следно**.



❏ Mac OS

Изберете го типот на конекција.



Конекција

Следете ги упатствата на екранот. Потребниот софтвер е инсталиран.

Поставки за функција

Ова поглавје ги објаснува првите поставки што се прават за да може да се употребува секоја функција на уредот.

Софтвер за поставување

Во оваа тема објаснета е процедурата за правење на поставки од компјутерот на администраторо со помош на Web Config.

Web Config (Web Page for Device)

Во врска со Web Config

Web Config е апликација заснована на пребарувач за конфигурација на поставките за скенерот.

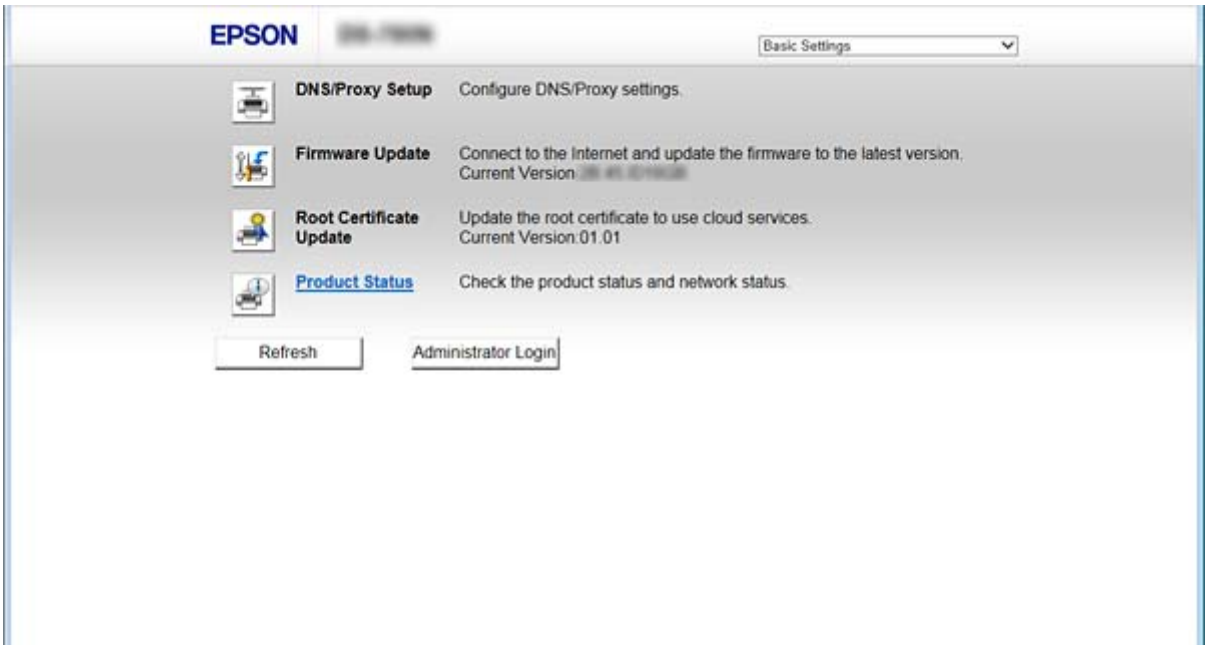
За да пристапите на Web Config, мора првин да назначите IP адреса на скенерот.

Белешка:
Може да ги заклучите поставките со конфигурирање на лозинката на администраторот за скенерот.

Има две страници за поставки како што е прикажано подолу.

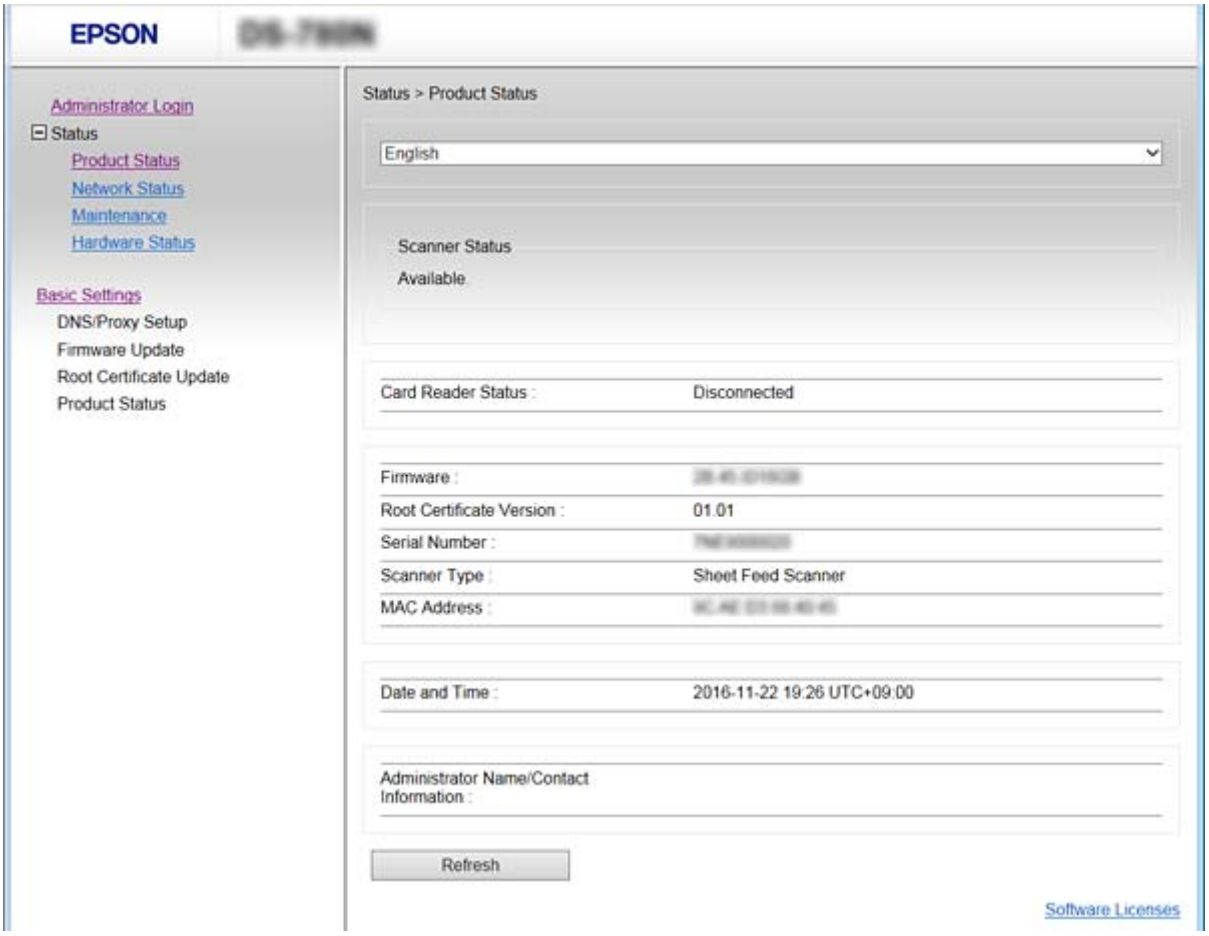
❏ **Basic Settings**

Може да ги конфигурирате основните поставки за скенерот.



❏ **Advanced Settings**

Може да ги конфигурирате напредните поставки за скенерот. Оваа страница е главно за администраторот.



Пристапување до Web Config

Внесете ја IP адресата на скенерот во интернет пребарувачот. JavaScript мора да биде овозможено. Кога пристапувате до Web Config преку HTTPS, се прикажува порака за предупредување во пребарувачот затоа што користите самопотпишан сертификат, зачуван во скенерот.

❏ Пристапување преку HTTPS

IPv4: https://<IP адреса на скенер> (без < >)

IPv6: https://[IP адреса на скенер]/ (со [ ])

❏ Пристапување преку HTTP

IPv4: http://<IP адреса на скенер> (без < >)

IPv6: http://[IP адреса на скенер]/ (со [ ])

Поставки за функција

Белешка:

❏ *Примери*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Ако го регистрирате името на скенерот со DNS серверот, може да го користите името на скенерот наместо IP адресата на скенерот.*

Поврзани информации

➡ „SSL/TLS комуникација со скенер“ на страница 63

➡ „Во врска со дигитална сертификација“ на страница 63

Употреба на функциите за скенирање

Во зависност од тоа како го користите скенерот, инсталирајте го следниов софтвер и направете ги поставките користејќи го.

❏ **Скенирање од компјутер**

❏ Потврдете ја валидноста на услугата за мрежно скенирање со Web Config (валидно со фабричка испорака).

❏ Инсталирајте Epson Scan 2 на компјутерот и поставете ја IP адресата

❏ Кога скенирате со користење на задачи, инсталирајте го Document Capture Pro (Document Capture) и поставете ги поставките за задача.

❏ **Скенирање од оперативна табла**

❏ Кога користите Document Capture Pro или Document Capture Pro Server:

Инсталирајте го Document Capture Pro или Document Capture Pro Server

DCP поставка (режим на сервер, режим на клиент).

❏ Кога го користите WSD протоколот:

Потврдете ја валидноста на WSD на Web Config или оперативна табла (валидна со фабричка испорака)

Дополнителни поставки за уред (Windows компјутер).

Скенирање од компјутер

Инсталирајте го софтверот и проверете дали сервисот за мрежно скенирање е овозможен за да скенирате преку мрежа од компјутерот.

Поврзани информации

➡ „Софтвер што треба да се инсталира“ на страница 25

➡ „Овозможување на скенирање на мрежата“ на страница 25

Софтвер што треба да се инсталира

❏ Epson Scan 2

Ова е драјвер за скенер. Ако го употребувате уредот од компјутер, инсталирајте го драјверот на секој компјутер на клиент. Ако е инсталирано Document Capture Pro/Document Capture може да извршувате операции назначени на копчињата на уредот.

Со EpsonNet SetupManager, двигателите за печатач може да бидат испорачани заедно во пакувањата.

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

Инсталирајте го на компјутерот на клиентот. Може да повикате и да извршите задачи регистрирани на компјутер со Document Capture Pro/Document Capture инсталирани на мрежата од оперативната табла на компјутерот и скенерот.

Може и да скенирате од компјутерот преку мрежата. Epson Scan 2 е потребно за скенирање.

Поврзани информации

➡ „EpsonNet SetupManager“ на страница 56

Поставете ја IP адресата на скенерот на Epson Scan 2

Одредете ја IP адресата на скенерот за да може да го користите скенерот на мрежата.

1. Започнете **Epson Scan 2 Utility** од **Започни** > **Сите програми** > **EPSON** > **Epson Scan 2**.

   Ако друг скенер е веќе регистриран, одете на чекор 2.

   Ако не е регистриран, одете на чекор 4.

2. Кликнете на ▼ на **Скенер**.
3. Кликнете **Поставки**.
4. Кликнете на **Овозможи уредување**, а потоа кликнете на **Додај**.
5. Изберете го името на моделот на скенерот од **Модел**.
6. Изберете ја IP адресата на скенерот којашто сакате да ја користите од **Адреса** во **Барај мрежа**.

   Кликнете на  и кликнете на  за да ја ажурирате листата. Ако не може да ја најдете IP адресата на скенерот, изберете **Внесете адреса** и внесете ја IP адресата.

7. Кликнете **Додај**.
8. Кликнете **Добро**.

Овозможување на скенирање на мрежата

Сервисот за скенирање на мрежата може да го поставите кога скенирате од компјутер на клиент кога сте во мрежата. Овозможена е вообичаената поставка.

1. Влезете во Web Config и одберете **Services** > **Network Scan**.

2. Осигурете се дека е избрано **Enable scanning** од **EPSON Scan**.

   Ако е избрано, задачата е комплетирана. Затворете ја Web Config.

   Ако е избришано, изберете го и одете на следниот чекор.

3. Кликнете **Next**.

4. Кликнете **OK**.

   Мрежата се поврзува повторно и потоа поставките се овозможени.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Скенирање преку контролната табла

Функцијата за скенирање во папка и функцијата скенирање во пошта со користење на контролната табла на скенерот, како и трансферот на скенирањето во пошта, папки итн. се извршуваат со иршување на задача од компјутерот.

Кога префрлате резултати од скенирање, поставете ја задачата со Document Capture Pro Server или Document Capture Pro.

За детали за скенирање и поставување на задача, погледнете ја документацијата или помош за Document Capture Pro Server или Document Capture Pro.

Поврзани информации

➡ „Поставки за Document Capture Pro Server/Document Capture Pro“ на страница 26

➡ „Поставки за сервери и папки“ на страница 27

Софтвер за инсталирање на компјутер

❏ **Document Capture Pro Server**

Ова е верзија на сервер на Document Capture Pro. Инсталирајте на Windows сервер. Може централно да уредувате повеќе уреди и задачи со серверот. Може истовремено да извршувате задачи од неколку скенери.

Со користење на сертифицирана верзија на Document Capture Pro Server, може да уредувате задачи и да историја на скенирање во врска со корисници и групи.

За детали за Document Capture Pro Server, контактирајте со локалната канцеларија на Epson.

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

Исто како и скенирање од компјутер, може да повикате задачи регистрирани на компјутерот од контролната табла и да ги извршите. Не може истовремено да извршувате задачи од неколку скенери.

Поставки за Document Capture Pro Server/Document Capture Pro

Направете поставки за користење на функцијата за скенирање од оперативниот панел на скенерот.

1. Пристапете до Web Config и одберете **Services** > **Document Capture Pro**.

2. Изберете **Режим на работа**.

   ❏ Server Mode:

   Изберете го ова кога го користите Document Capture Pro Server или кога го користите Document Capture Pro само за задачи коишто се поставени за одреден компјутер.

   ❏ Client Mode:

   Поставете го ова кога ќе ја изберете поставката за задача Document Capture Pro (Document Capture) инсталирана на секој компјутер на клиент на мрежата без одредување на компјутерот.

3. Поставете го следново според избраниот режим.

   ❏ Server Mode:

   Во **Server Address**, одредете го серверот на којшто Document Capture Pro Server е инсталиран. Може да биде помеѓу 2 и 252 знаци од IPv4, IPv6, име на хост или FQDN формат. Во FQDN формат, може да користите US-ASCII букви, броеви, азбучни букви, тире (освен почетниот и задниот).

   ❏ Client Mode:

   Одредете **Group Settings** за да користите група на скенер одредена од Document Capture Pro (Document Capture).

4. Кликнете **Поставки**.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Поставки за сервери и папки

Document Capture Pro и Document Capture Pro Server ги зачувуваат скенираните податоци на сервер или на компјутер на сервер еднаш и со функцијата за трансфер ги извршуваат функцијата за скенирањето во папка и функцијата за скенирање во пошта.

Потребна е авторизација и информации за трансфер од компјутерот на којшто Document Capture Pro, Document Capture Pro Server е инсталиран на компјутер или услуга на облак.

Подгответе ги информациите за функцијата којашто ќе ја користите коишто се однесуваат на следново.

Може да направите поставки за овие функции со користење на Document Capture Pro или Document Capture Pro Server. За детали за поставките, погледнете ја документацијата или помош за Document Capture Pro Server или Document Capture Pro.

Име	Поставки	Побарување
Scan to Network папка (SMB)	Создадете и поставете споделување на папката за зачувување	Административна корисничка сметка за компјутер којшто создава папки за зачувување.
	Дестинација за Scan to Network папка (SMB)	Корисничко име и лозинка за најава во компјутерот на којшто е папката за зачувување и привилегијата за ажурирање на папката.
Scan to Network папка (FTP)	Поставување за најава на FTP сервер	Информација за најавување за FTP сервер и привилегија за ажурирање на фолдер за зачувување.

Поставки за функција

Име	Поставки	Побарување
Scan to Email	Поставување за сервер за е-пошта	Поставување информации за сервер за е-пошта
Scan to Document Capture Pro (кога се употребува Document Capture Pro Server)	Поставување за најавување на услуги на облак	Средина за интернет конекција Регистрација на сметка за услуги на облак

Користете WSD скенирање (само за Windows)

Ако компјутерот користи Windows Vista или понова верзија, може да го користите WSD скенирањето.

Кога го користите WSD протоколот, **Компјутер(WSD)** менито ќе се прикаже на контролната табла на скенерот.

1. Пристапете до Web Config и одберете **Services** > **Protocol**.
2. Проверете дали **Enable WSD** е штиклирано во **WSD Settings**.

   Ако е штиклирано, задачата е комплетирана и може да ја затворите Web Config.

   Ако не е штиклирано, проверете го и продолжете со следниот чекор.
3. Кликнете на копчето **Next**.
4. Потврдете ги поставките и кликнете на **Поставки**.

Правење на системски поставки

Правење на системски поставки од контролната табла

Поставување на осветленост на екран

Поставете ја осветленоста на LCD екранот.

1. Допрете на **Поставки** на почетниот екран.
2. Допрете **Општи поставки** > **ЛЦД осветленост**.
3. Допрете на  или на  за да ја приспособите осветленоста.

   Може да приспособувате од 1 до 9.
4. Допрете **Во ред**.

Поставување на звук

Поставете ги звукот за работење на таблата и звукот за грешка.

1. Допрете на **Поставки** на почетниот екран.
2. Допрете **Општи поставки** > **Звук**.
3. Поставете ги следните ставки како што е потребно.
   - ❏ Звук за работење
     Поставете го волуменот на звукот за работење на оперативната табла.
   - ❏ Звук за грешка
     Поставете го волуменот на звукот за грешка.
4. Допрете **Во ред**.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Детекција на двојно внесување на оригинал

Одредете ја функцијата за да детектирате двојно внесување на документ којшто сакате да го скенирање и за да го запрете скенирањето кога ќе дојде до повеќе внесувања.

За да скенирате оригинали за коишто се смета дека се со повеќе внесувања, како на пример пликови или хартија со налепници, поставете ги на исклучено.

Белешка:
Може да ја поставите и од Web Config или Epson Scan 2.

1. Допрете на **Поставки** на почетниот екран.
2. Допрете **Надворешни Поставки за скенирање** > **Ултрасо. откр. на двојно ставање**.
3. Допрете на **Ултрасо. откр. на двојно ставање** за да ја вклучите и за да ја исклучите.
4. Допрете **Затвори**.

Поставување на режим на мала брзина

Поставете за да скенирате со мала брзина за да не дојде до заглавување на хартија при скенирање на тенки документи како на пример мали парчиња на хартија.

1. Допрете на **Поставки** на почетниот екран.
2. Допрете **Надворешни Поставки за скенирање** > **Бавно**.
3. Допрете на **Бавно** за да ја вклучите и за да ја исклучите.
4. Допрете **Затвори**.

Правење на системски поставки со користење на Web Config

Поставки за заштеда на струја за време на неактивност

Направете ги поставките за заштеда на струја кога скенерот има период на неактивност. Поставете го времето во зависност од искористеноста на средината.

Белешка:
Може да ги направите поставките за заштеда на струја на контролната табла на скенерот.

1. Пристапете до Web Config и одберете **System Settings** > **Power Saving**.
2. Внесете го времето за **Sleep Timer** за да се префрлие во режим на заштеда на струја кога има неактивност.

   Можете да поставите до 240 минути.
3. Одберете го времето на исклучување за **Power Off Timer**.
4. Кликнете **OK**.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Поставување на контролниот панел

Поставување за контролниот панел на скенерот. Може да поставувате на следниот начин.

1. Пристапете до Web Config и одберете **System Settings** > **Control Panel**.
2. Поставете ги следните ставки како што е потребно.

   ❏ Language

   Изберете го прикажаниот јазик на контролниот панел.

   ❏ Panel Lock

   Ако одберете **ON**, потребна е лозинката за администратор кога се изведува операција за којашто е потребно овластување на администратор. Ако лозинката за администратор не е поставена, оневозможено е заклучувањето на панелот.

   ❏ Operation Timeout

   Ако одберете **ON** кога се најавувате како администратор, автоматски се одјавувате и преминувате на иницијалниот екран ако нема активност за одреден период од време.

   Можете да поставите помеѓу 10 секунди и 240 минути.
3. Кликнете **OK**.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Поставување рестрикција за екстерниот интерфејс

Можете да ја ограничите USB конекцијата од компјутерот. Поставете ја за да го ограничите скенирањето различно од она преку мрежата.

1. Пристапете до Web Config и одберете **System Settings** > **External Interface**.
2. Изберете **Enable** или **Disable**.

   За да ја ограничите, изберете **Disable**.
3. Допрете **OK**.

Синхронизација на датумот и времето со времето на серверот

Ако употребувате CA сертификат, можете да спречите проблем со времето.

1. Пристапете до Web Config и одберете **System Settings** > **Date and Time** > **Time Server**.
2. Одберете **Use** за **Use Time Server**.
3. Внесете го времето за адресата на серверот **Time Server Address**.

   Може да користите IPv4, IPv6 или FQDN формат. Внесете 252 знаци или помалку. Во спротивно оставете го празно.
4. Внесете **Update Interval (min)**.

   Можете да поставите до 10.800 минути.
5. Кликнете **OK**.

   Белешка:
   *Можете да го потврдите статусот на конекцијата со времето на серверот на **Time Server Status**.*

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Основни безбедносни поставки

Ова поглавје ги објаснува основните безбедносни поставки за коишто не е потребна специјална средина.

Вовед во основните безбедносни карактеристики

Ви ги претставуваме основните безбедносни карактеристики за Epson уреди.

Име на карактеристика	Тип на карактеристика	Што да се постави	Што да се спречи
Поставување на лозинката за администратор	Заклучете ги поставките за системот, како на пример мрежни поставки и поставки за USB конекција за само администраторот да може да ги промени.	Администратор поставува лозинка за уредот. Конфигурирање или ажурирање е достапно од каде било од Web Config, контролниот панел, Epson Device Admin, и EpsonNet Config.	Спречување од нелегално отчитување и промена на информациите складирани на уредот како што е ID, лозинка, мрежни поставки и контакти. Исто така, се намалува голем опсег на безбедносни ризици како протекување на информации за мрежната средина или безбедносната политика.
SSL/TLS комуникација	Кога пристапувате на Epson сервер на интернет од уред, како на пример комуникација помеѓу компјутер преку пребарувач или ажурирање на фирмвер, содржината на конекцијата е шифрирана со помош на SSL/TLS комуникација.	Стекнете се со CA потпишан сертификат и потоа импортирајте го во скенерот.	Расчистување на идентификација на уредот преку CA потпишан сертификат спречува имитирање и неавторизиран пристап. Дополнително на тоа, комуникациските содржини на SSL/TLS се заштитени и се спречува протекување на содржина за податоци за печатење и информации за поставување.
Протоколи за контрола	Протоколи за контрола коишто се користат за комуникација помеѓу уреди и компјутери и функции за активирање/деактивирање.	Протокол или услуга што е примената на карактеристики се дозволува или забранува одделно.	Намалување на безбедносните ризици што може да се случат преку ненамерно користење преку спречување на корисниците од употреба на непотребни функции.

Поврзани информации

➡ „Во врска со Web Config“ на страница 22
➡ „EpsonNet Config“ на страница 55
➡ „Epson Device Admin“ на страница 55
➡ „Конфигурирање на лозинка за администратор“ на страница 33
➡ „Контролирање на протоколи“ на страница 35

Конфигурирање на лозинка за администратор

Кога ја поставувате лозинката за администратор, корисници што не се администратори нема да можат да ги менуваат поставките за администрирањето со системот. Лозинката за администратор можете да ја поставувате или менувате со Web Config, контролниот панел на скенерот, или софтверот (Epson Device Admin или EpsonNet Config). Кога го употребувате софтверот, видете ја документацијата за секој софтвер.

Поврзани информации

➡ „Конфигурирање на лозинката за администратор преку контролниот панел“ на страница 33

➡ „Конфигурирање на лозинка за администратор со Web Config“ на страница 33

➡ „EpsonNet Config“ на страница 55

➡ „Epson Device Admin“ на страница 55

Конфигурирање на лозинката за администратор преку контролниот панел

Лозинката за администратор може да ја поставите од контролниот панел на скенерот.

1. Допрете на **Поставки** на почетниот екран.
2. Допрете **Администрир. на систем** > **Администраторски поставки**.

   Ако ставката не е прикажана, благо придвижете екранот нагоре за да се прикаже.
3. Допрете **Лозинка на администраторот** > **Регистрирај**.
4. Внесете ја новата лозинка и допрете на **Во ред**.
5. Внесете ја новата лозинка повторно и допрете на **Во ред**.
6. Допрете на **Во ред** на екранот за потврда.

   Прикажан е екранот со администраторски поставки.
7. Допрете на **Поставка за заклучување**, и потоа допрете на **Во ред** на екранот за потврда.

   Поставка за заклучување е поставено на **Вкл.**, а лозинката за администратор се бара кога работите со заклучена ставка на мени.

Белешка:

❏ *Ако поставите **Поставки** > **Општи поставки** > **Изминато време на операцијата** до **Вкл.**, скенерот ќе ве одјави по период на неактивност во контролниот панел.*

❏ *Кога одбирате **Промени** или **Ресетирај** на екранот **Лозинка на администраторот** и ја внесувате лозинката за администратор, истата можете да ја промените или избришете.*

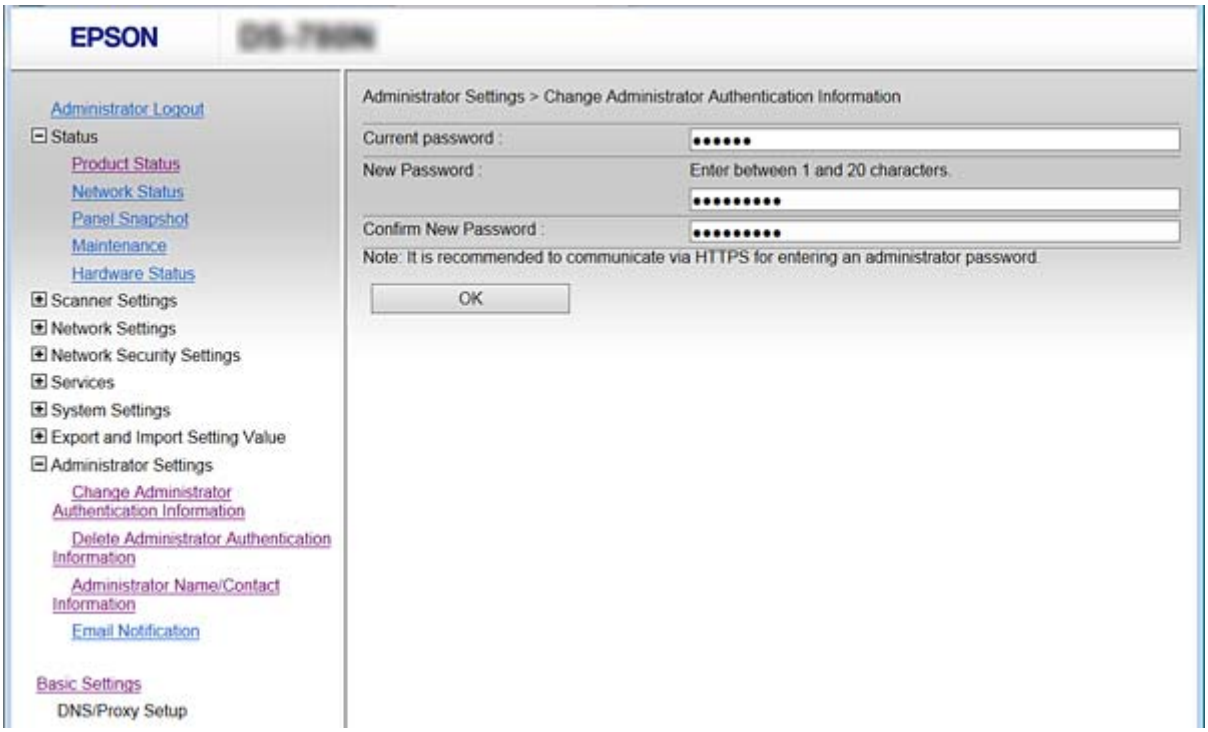
Конфигурирање на лозинка за администратор со Web Config

Можете да ја поставите лозинката за администратор со Web Config.

1. Пристапете до Web Config и одберете **Administrator Settings** > **Change Administrator Authentication Information**.

2. Внесете лозинка во **New Password** и **Confirm New Password**. Внесете го корисничкото име доколку е потребно.

   Ако сакате да внесете нова лозинка, внесете ја тековната лозинка.



3. Изберете **OK**.

   Белешка:

   ❏ *За да поставувате или менувате заклучени ставки, кликнете на **Administrator Login**, и потоа внесете ја лозинката за администратор.*

   ❏ *За да ја избришете лозинката за администратор, кликнете **Administrator Settings** > **Delete Administrator Authentication Information**, и потоа внесете ја лозинката за администратор.*

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Ставки што треба да се заклучат со лозинка за администратор

Администраторите имаат привилегии на поставување и промена на сите карактеристики за уреди.

Исто така, ако поставите лозинка за администратор на уредот, може да ја заклучите за да не може да ги менувате ставките во врска со уредување на уредот.

Следните се ставки коишто може да ги контролира администратор.

Ставка	Опис
Поставки за скенер	Поставка за детекција на двојно внесување и режим со мала брзина.

Основни безбедносни поставки

Ставка	Опис
Поставки Ethernet конекција	Промена на името на уреди и IP адреса, поставување на DNS сервер или Proxy сервер и промена на поставки поврзани со мрежните конекции.
Поставување на кориснички услуги	Поставување на контрола на комуникациски протоколи, мрежно скенирање и Document Capture Pro услуги.
Поставување на сервер за е-пошта	Поставување на сервер за е-пошта со којшто уредите комуницираат директно.
Безбедносни поставки	Поставки за мрежна безбедност како SSL/TLS комуникација, IPsec/IP филтрирање и IEEE802.1X.
Ажурирање на коренов сертификат	Ажурирање на коренови сертификати потребни за Document Capture Pro Server автентикација и ажурирање на фирмвер од Web Config.
Ажурирање фирмвер	Проверка и ажурирање на фирмвер на уреди.
Време, поставување тајмер	Време на транзиција за режим на спиење, автоматско исклучување, тајмер за неработење и други поставки поврзани со тајмер.
Враќање на вообичаени поставки	Поставки за скенерот да се врати во фабричка состојба.
Администраторски поставки	Поставување на администраторско заклучување или лозинка за администратор.
Поставување сертифициран уред	Поставување ID за автентикација на уред. Се поставува кога се употребува скерер на систем за автентикација којшто поддржува уреди за автентикација.

Контролирање на протоколи

Може да скенирате со користење на разни патеки и протоколи. Може да го користите и скенирањето на мрежата од неодреден број на компјутери на мрежата. На пример, дозволено е скенирање со користење на одредени патеки и протоколи. Може да ги намалите ненамерните безбедносни опасности со ограничување на скенирање од одредени патеки или со контролирање на достапните функции.

Конфигурирајте ги поставките за протоколи.

1. Пристапете до Web Config и одберете **Services** > **Protocol**.
2. Конфигурирајте ги сите ставки.
3. Кликнете **Next**.
4. Кликнете **OK**.

   Поставките се применети на скенерот.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23
➡ „Протоколи коишто може да ги активирате и да ги деактивирате“ на страница 36
➡ „Ставки за поставка на протокол“ на страница 37

Протоколи коишто може да ги активирате и да ги деактивирате

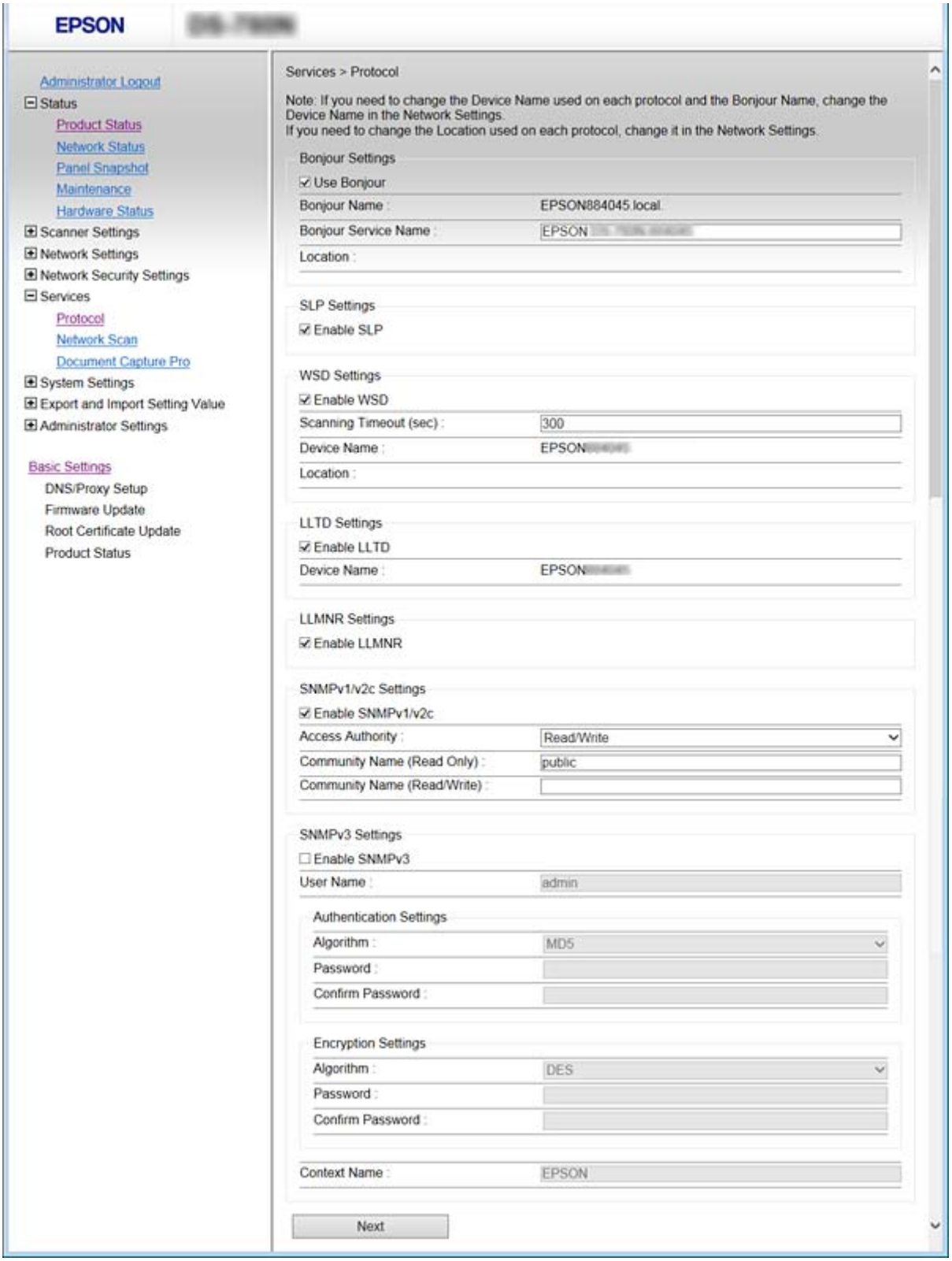
Протокол	Опис
Bonjour Settings	Може да назначите дали ќе користите Bonjour. Bonjour се користи за уреди, скенирање итн.
SLP Settings	Може да ја овозможите или да ја оневозможите функцијата SLP. SLP се користи за Epson Scan 2 и мрежно пребарување во EpsonNet Config.
WSD Settings	Може да ја овозможите или да ја оневозможите функцијата WSD. Кога е овозможено, може да додавате WSD уреди или да скенирате од WSD портата.
LLTD Settings	Може да ја овозможите или да ја оневозможите функцијата LLTD. Кога ова е активирано, се прикажува на Windows мапата на мрежата.
LLMNR Settings	Може да ја овозможите или да ја оневозможите функцијата LLMNR. Кога ова е активирано, може да користите резолуција на име без NetBIOS дури и ако не може да го користите DNS.
SNMPv1/v2c Settings	Може да назначите дали да го активирате или не SNMPv1/v2c. Ова се користи за поставување на уреди, следење итн.
SNMPv3 Settings	Може да назначите дали да го активирате или не SNMPv3. Ова се користи за поставување на шифрирани уреди, следење итн.

Поврзани информации

➡ „Контролирање на протоколи“ на страница 35

➡ „Ставки за поставка на протокол“ на страница 37

Ставки за поставка на протокол



Ставки	Вредност на поставка и опис
Bonjour Settings	

Основни безбедносни поставки

Ставки	Вредност на поставка и опис
Use Bonjour	Изберете го ова за да пребарувате или за да користите уреди со Bonjour.
Bonjour Name	Се прикажува името Bonjour.
Bonjour Service Name	Може да се прикаже и да го поставите името на услугата Bonjour.
Location	Се прикажува името на локацијата Bonjour.
SLP Settings	
Enable SLP	Изберете го ова за да ја активирате функцијата SLP. Се користи за мрежно откривање во Epson Scan 2 и EpsonNet Config.
WSD Settings	
Enable WSD	Изберете го ова за да може да додадете уреди со користење на WSD и печатете и скенирајте од WSD портот.
Scanning Timeout (sec)	Внесете вредност за прекин во комуникација за WSD скенирање од 3 до 3600 секунди.
Device Name	Се прикажува името на уредот WSD.
Location	Се прикажува името на локацијата WSD.
LLTD Settings	
Enable LLTD	Изберете го ова за да ја активирате LLTD. Скенерот е прикажан во Windows мапата на мрежа.
Device Name	Се прикажува името на уредот LLTD.
LLMNR Settings	
Enable LLMNR	Изберете го ова за да ја активирате LLMNR. Може да користите резолуција на име без NetBIOS дури и ако не може да го користите DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Изберете го ова за да ја активирате SNMPv1/v2c. Прикажани се само скенери коишто поддржуваат SNMPv3.
Access Authority	Поставете го овластувањето за пристап кога SNMPv1/v2c е активирано. Изберете **Read Only** или **Read/Write**.
Community Name (Read Only)	Внесете од 0 до 32 ASCII (од 0x20 до 0x7E) знаци.
Community Name (Read/Write)	Внесете од 0 до 32 ASCII (од 0x20 до 0x7E) знаци.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 е активирано ако е штиклирано квадратчето.
User Name	Внесете од 1 до 32 знаци со користење на знаци од 1 бајт.
Authentication Settings	

Основни безбедносни поставки

Ставки	Вредност на поставка и опис
Algorithm	Изберете алгоритам за автентикација за SNMPv3.
Password	Внесете лозинка за автентикација за SNMPv3. Внесете од 8 до 32 знаци во ASCII (0x20–0x7E). Во спротивно оставете го празно.
Confirm Password	Внесете ја лозинката којашто сте ја конфигурирале за потврда.
Encryption Settings	
Algorithm	Изберете алгоритам за шифрирање на SNMPv3.
Password	Внесете лозинка за шифрирање на SNMPv3. Внесете од 8 до 32 знаци во ASCII (0x20–0x7E). Во спротивно оставете го празно.
Confirm Password	Внесете ја лозинката којашто сте ја конфигурирале за потврда.
Context Name	Внесете до 32 знаци или помалку во Unicode (UTF-8). Во спротивно оставете го празно. Бројот на знаци што може да се внесе варира во зависност од јазикот.

Поврзани информации

➡ „Контролирање на протоколи“ на страница 35

➡ „Протоколи коишто може да ги активирате и да ги деактивирате“ на страница 36

Поставки за работење и менаџирање

Ова поглавје ги објаснува ставките поврзани со дневните операции и управувањето со уредотс.

Потврдување информации за уред

Следниве информации можете да ги проверите за уредот што работи преку **Status** со употреба на Web Config.

❏ Product Status

Проверете го јазикот, статусот, бројот на производ, MAC адресата итн.

❏ Network Status

Проверете ги информациите за статусот на мрежната конекција, IP адресата, DNS серверот итн.

❏ Panel Snapshot

Прикажете скриншот од екранот којшто е прикажан на контролниот панел за уредот.

❏ Maintenance

Проверете ги почетниот датум, информациите за скенирање итн.

❏ Hardware Status

Проверете го статусот на скенерот.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Управување со уреди (Epson Device Admin)

Можете да управувате и да работите со многу уред со помош на Epson Device Admin. Epson Device Admin ви дозволува да управувате со уреди лоцирани различна мрежа. Следното ги отцртува главните карактеристики за управување.

За повеќе информации околу функциите и употребата на софтверот видете ја документацијата или помошта за Epson Device Admin.

❏ Откривање уреди

Можете да откривате уреди на мрежата и потоа да ги регистрирате во листа. Ако уредите Epson како што се печатачите и скенерите се поврзани со истите мрежни сегменти како компјутерот за администратор, тогаш можете да ги пронајдете дури и ако не им е назначена IP адреса.

Исто така, можете да откривате уреди коишто се поврзани со компјутери на мрежата преку USB кабли. Треба да го инсталирате Epson Device USB Agent на компјутерот.

❏ Поставување уреди

Може да направите образец којшто ги содржи ставките како што се мрежниот интерфејс или изворот на хартија за поставки и да го примените на други уреди како заеднички поставки. Кога е поврзан со мреќата можете да назначувате IP адреса на уред на којшто не му била назначена IP адреса.

❏ Надгледување уреди

Можете редовно да добивате статус и детални информации за уреди на мрежата. Исто така, можете да надгледувате уреди коишто се поврзани со компјутери на мрежата преку USB кабли и уреди од другите компании коишто се регистрирани со листата на уреди. За да надгледувате уреди поврзани со USB кабли треба да инсталирате Epson Device USB Agent.

❏ Управување со тревоги

Можете да ги надгледувате тревогите за статусот на уредите и артиклите. Системот автоматски испраќа е-пошта со известувања до администраторот базирано на поставени услови.

❏ Управување со извештаи

Можете да создавате редовни извештаи како што системот акумулира податоци за искористеноста на уред и артикли. Потоа можете да ги зачувувате овие создадени извештаи и да ги испраќате по е-пошта.

Поврзани информации

➡ „Epson Device Admin“ на страница 55

Примање на известувања на е-пошта кога ќе има настани

Во врска со известувањата на е-пошта

Може да ја користите оваа функција за да примате предупредувања по електронска пошта кога ќе има настани. Може да регистрирате до 5 адреси на е-пошта и да изберете за кои настани сакате да примате известувања.

Серверот за пошта мора да биде конфигуриран за да ја употребува оваа функција.

Поврзани информации

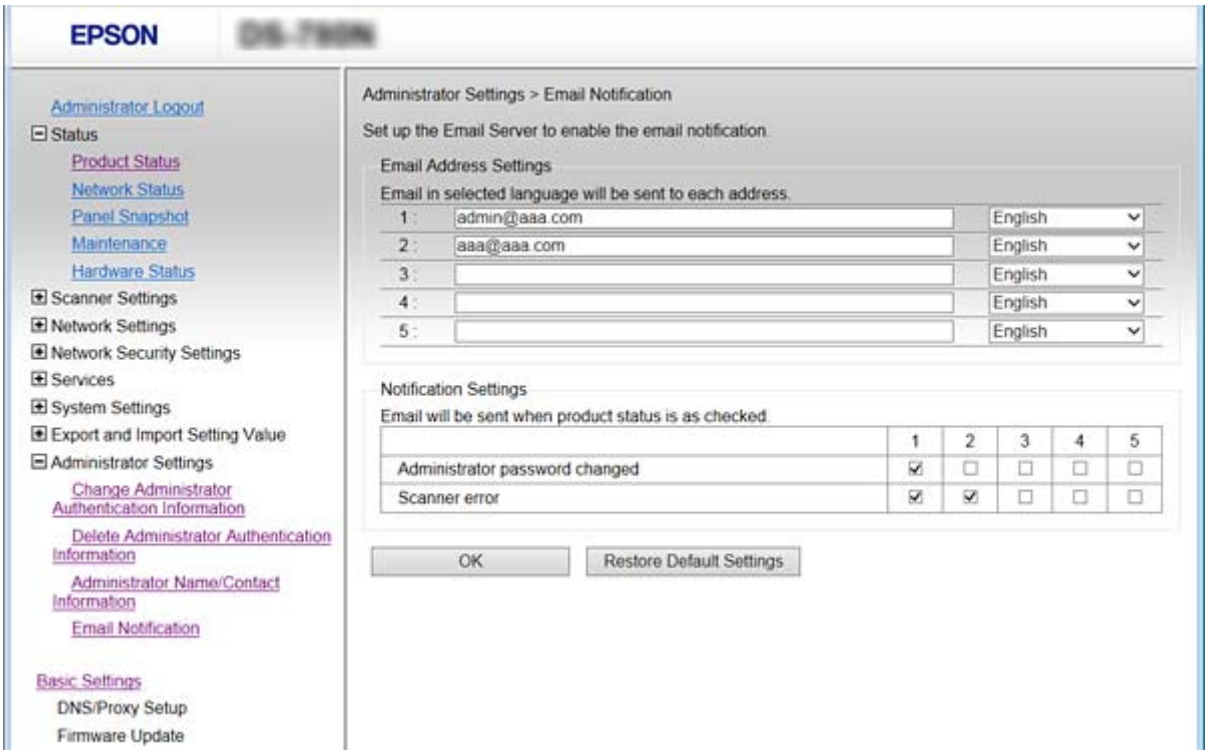
➡ „Конфигурирање на сервер за пошта“ на страница 42

Конфигурирање на известувања за е-пошта

За да ја користите оваа функција, потребно е да го конфигурирате серверот за пошта.

1. Пристапете до Web Config и изберете **Administrator Settings** > **Email Notification**.
2. Внесете ја адресата на е-пошта на којашто сакате да примате известувања за е-пошта.
3. Изберете го јазикот на известувањата за е-пошта.

4. Штиклирајте ги квадратчињата за известувањата коишто сакате да ги примате.



5. Кликнете на **OK**.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Конфигурирање на сервер за пошта“ на страница 42

Конфигурирање на сервер за пошта

Проверете го следново пред да конфигурирате.

❏ Скенерот е поврзан на мрежата.

❏ Информации за сервер за пошта на компјутерот.

1. Пристапете до Web Config и изберете **Network Settings** > **Email Server** > **Basic**.
2. Внесете вредност за секоја ставка.
3. Изберете **OK**.

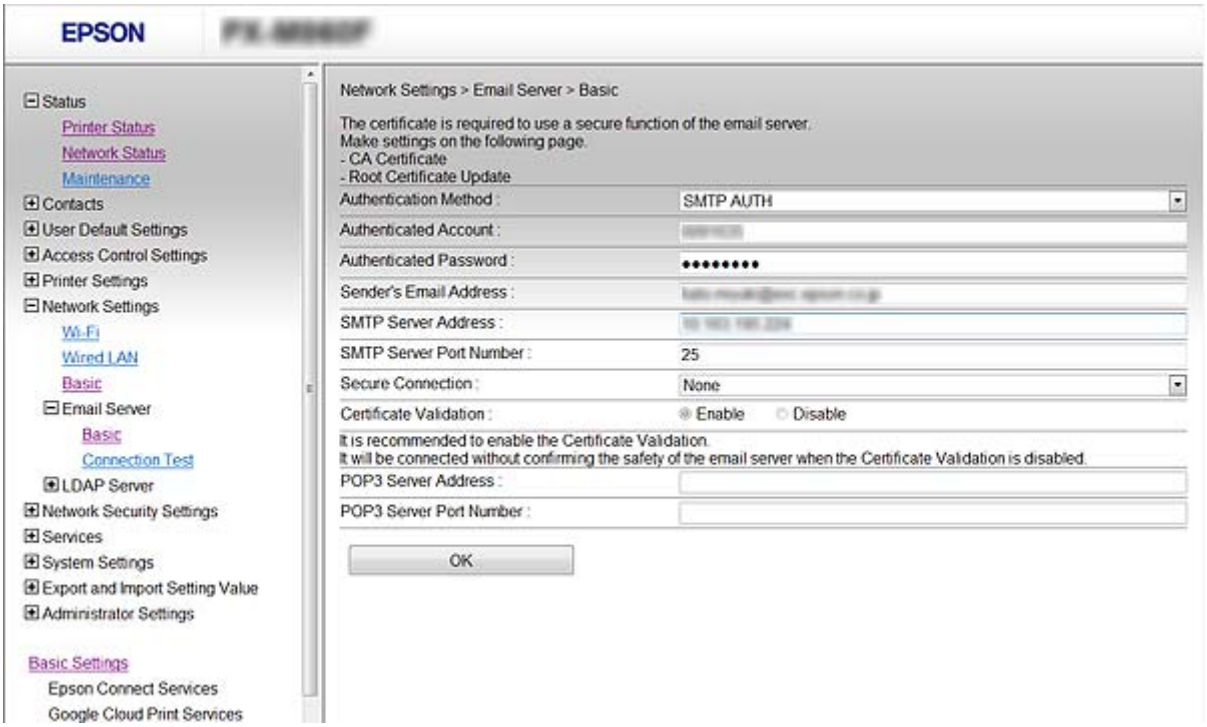
   Се прикажуваат поставките коишто сте ги избрале.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Ставки за поставка на сервер за пошта“ на страница 43

Ставки за поставка на сервер за пошта



Ставки	Поставки и објаснувања	
Authentication Method	Одредете го методот на автентикација за скенерот да пристапи на серверот за пошта.	
	Off	Автентикацијата е деактивирана при комуникација со серверот за пошта.
	SMTP AUTH	Потребно е серверот за пошта да ја поддржува SMTP автентикацијата.
	POP before SMTP	Конфигурирајте го POP3 серверот кога ќе го изберете овој метод.
Authenticated Account	Ако изберете **SMTP AUTH** или **POP before SMTP** како **Authentication Method**, внесете име на автентицирана сметка од 0 до 255 знаци во ASCII (0x20–0x7E).	
Authenticated Password	Ако изберете **SMTP AUTH** или **POP before SMTP** како **Authentication Method**, внесете име на автентицирана лозинка од 0 до 20 знаци со користење на A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Внесете ја адресата на е-пошта на испраќачот. Внесете од 0 до 255 знаци во ASCII (0x20–0x7E) освен : ( ) < > [ ] ; ¥. Точката „.“ не може да биде првиот знак.	
SMTP Server Address	Внесете од 0 до 255 знаци со користење на A–Z a–z 0–9. - . Може да користите IPv4 или FQDN формат.	
SMTP Server Port Number	Внесете број од 1 до 65535.	

Поставки за работење и менаџирање

Ставки	Поставки и објаснувања	
Secure Connection	Одредете метод на безбедна конекција за сервер на е-пошта.	
	None	Ако изберете **POP before SMTP** во **Authentication Method**, методот на конекција е поставен на **None**.
	SSL/TLS	Ова е достапно кога **Authentication Method** е поставено на **Off** или **SMTP AUTH**.
	STARTTLS	Ова е достапно кога **Authentication Method** е поставено на **Off** или **SMTP AUTH**.
Certificate Validation	Сертификатот е проверен кога ова е активирано. Препорачуваме ова да е поставено на **Enable**.	
POP3 Server Address	Ако изберете **POP before SMTP** како **Authentication Method**, внесете ја адресата на POP3 серверот од 0 до 255 знаци со користење на A–Z a–z 0–9. - . Може да користите IPv4 или FQDN формат.	
POP3 Server Port Number	Ако изберете **POP before SMTP** како **Authentication Method**, внесете број од 1 до 65535.	

Поврзани информации

➡ „Конфигурирање на сервер за пошта“ на страница 42

Проверување на конекција на сервер за пошта

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

   Пробната конекција за серверот за пошта е започната. По тестот се прикажува извештајот за проверка.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Пробни референции за конекција на серверот за пошта“ на страница 44

Пробни референции за конекција на серверот за пошта

Пораки	Објаснување
Connection test was successful.	Оваа порака се прикажува кога конекцијата со серверот е успешна.
SMTP server communication error. Check the following. - Network Settings	Оваа порака се прикажува кога ❏ Скенерот не е поврзан на мрежа ❏ SMTP серверот е исклучен ❏ Мрежната конекција е исклучена при комуницирање ❏ Примени некомплетни податоци

Поставки за работење и менаџирање

Пораки	Објаснување
POP3 server communication error. Check the following. - Network Settings	Оваа порака се прикажува кога ❏ Скенерот не е поврзан на мрежа ❏ POP3 серверот е исклучен ❏ Мрежната конекција е исклучена при комуницирање ❏ Примени некомплетни податоци
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Оваа порака се прикажува кога ❏ Поврзување на DNS серверот е неуспешно ❏ Име на резолуција за SMTP серверот е неуспешно
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Оваа порака се прикажува кога ❏ Поврзување на DNS серверот е неуспешно ❏ Име на резолуција за POP3 серверот е неуспешно
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Оваа порака се прикажува кога автентикацијата на SMTP серверот е неуспешна.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Оваа порака се прикажува кога автентикацијата на POP3 серверот е неуспешна.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Оваа порака се прикажува кога се обидувате да комуницирате со несоодветни протоколи.
Connection to SMTP server failed. Change Secure Connection to None.	Оваа порака се прикажува кога настанува SMTP несовпаѓање помеѓу серверот и клиентот или кога серверот не поддржува SMTP безбедна конекција (SSL конекција).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Оваа порака се прикажува кога настанува SMTP несовпаѓање помеѓу серверот и клиентот или кога серверот бара да користи SSL/TLS конекција за SMTP безбедна конекција.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Оваа порака се прикажува кога настанува SMTP несовпаѓање помеѓу серверот и клиентот или кога серверот бара да користи STARTTLS конекција за SMTP безбедна конекција.
The connection is untrusted. Check the following. - Date and Time	Оваа порака се прикажува кога поставката на датумот и времето на скенерот се неточни или кога сертификатот е застарен.
The connection is untrusted. Check the following. - CA Certificate	Оваа порака се прикажува кога скенерот нема коренов сертификат којшто одговара на серверот или CA Certificate не е увезен.
The connection is not secured.	Пораката се прикажува кога добиениот сертификат е оштетен.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Оваа порака се прикажува кога настанува несовпаѓање при методот на автентикација помеѓу серверот и клиентот. Серверот поддржува SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Оваа порака се прикажува кога настанува несовпаѓање при методот на автентикација помеѓу серверот и клиентот. Серверот не поддржува SMTP AUTH.

Пораки	Објаснување
Sender's Email Address is incorrect. Change to the email address for your email service.	Оваа порака се прикажува кога адресата на е-пошта на одредениот испраќач е погрешна.
Cannot access the product until processing is complete.	Пораката се прикажува кога скенерот е зафатен.

Поврзани информации

➡ „Проверување на конекција на сервер за пошта“ на страница 44

Ажурирање фирмвер

Ажурирање фирмвер со Web Config

Се ажурира фирмвер со Web Config. Уредот мора да биде поврзан со интернет.

1. Пристапете до Web Config и одберете **Basic Settings** > **Firmware Update**.
2. Кликнете **Start**.

   Започнува потврдувањето на фирмверот и прикажана е информацијата за фирмверот ако постои ажурираниот фирмвер.
3. Кликнете на **Start**, и следете ги упатствата на екранот.

Белешка:
Исто така, фирмверот можете да го ажурирате со Epson Device Admin. Можете визуелно да ја потврдите информацијата за фирмверот на листата со уреди. Корисна е кога сакате да ажурирате фирмвер на повеќе уреди. Погледнете во водичот или помошта за Epson Device Admin за повеќе информации.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23
➡ „Epson Device Admin“ на страница 55

Ажурирање фирмвер со Epson Firmware Updater

Можете да го преземете фирмверот за уредот од веб-страницата на Epson директно на компјутер и потоа да го поврзете уредот и компјутерот преку USB кабел за да го ажурирате фирмверот. Ако не можете да го ажурирате преку мрежата, обидете се со овој метод.

1. Влезете во веб-страницата на Epson и преземете го фирмверот.
2. Поврзете го компјутерот којшто го содржи преземениот фирмвер со уредот преку USB кабел.
3. Кликнете двапати на преземената .exe датотека.

   Започнува Epson Firmware Updater.

4. Следете ги упатствата на екранот.

Правење резервна копија на поставките

Со експортирање на поставките за ставките на Web Config, ставките можете да ги ископирате во други скенери.

Ивезување на поставки

Извезете ја секоја поставка за скенерот.

1. Пристапете до Web Config и изберете **Export and Import Setting Value** > **Export**.
2. Изберете ги поставките коишто сакате да ги извезете.

   Изберете ги поставките коишто сакате да ги извезете. Ако изберете слична категорија, избрани се и поткатегориите. Меѓутоа, не може да ги изберете поткатегориите коишто предизвикуваат грешки со удвојување во рамките на истата мрежа (како на пример IP адреса итн.).
3. Внесете лозинка за да ја шифрирате извезената датотека.

   Потребна ви е лозинка за да ја увезете датотеката. Оставете го ова празно ако не сакате да ја шифрирате датотеката.
4. Кликнете на **Export**.

> ***Важно:***
>
> *Ако сакате да ги извезете мрежните поставки за скенерот како на пример името на скенерот и IP адресата, изберете **Enable to select the individual settings of device** и изберете уште ставки. Користете ги избраните вредности само за скенерот за замена.*

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Увезување на поставки

Увезете ја изнесената датотека Web Config на скенерот.

> ***Важно:***
>
> *Кога ги увезувате вредностите коишто содржат поединечни информации како на пример име на скенер или IP адреса, погрижете се IP адресата да не постои на истата мрежа. Ако IP адресата се совпаѓа, скенерот нема да ја прикаже вредноста.*

1. Пристапете до Web Config и изберете **Export and Import Setting Value** > **Import**.
2. Изберете ја изнесената датотека и внесете ја шифрираната лозинка.
3. Кликнете на **Next**.

4. Изберете ги поставките коишто сакате да ги увезете и кликнете на **Next**.
5. Кликнете на **OK**.

Поставките се применети на скенерот.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Решавање на проблеми

Совети за решавање на проблеми

Може да најдете повеќе информации во следниве прирачници.

❏ Упатство за корисникот

Обезбедува упатства за користење на скенерот, одржувањето и решавањето на проблеми.

Проверка на дневниците за серверски и мрежен уред

Во случај со проблем со мрежната конекција, може да ја дознаете причината така што ќе го потврдите дневникот на серверот за е-пошта, LDAP серверот итн., ќе го проверите статусот со користење на мрежниот дневник на дневниците за системска опрема и команди, како на пример рутерите.

Иницијализација на поставките за мрежата

Обновување на мрежните поставки од контролниот панел на печатачот

Може да ги вратите сите мрежни поставки на нивните почетни вредности.

1. Допрете на **Поставки** на почетниот екран.
2. Допрете **Администрир. на систем** > **Врати стандардни поставки** > **Поставки за мрежа**.
3. Проверете ја пораката и потоа изберете **Да**.
4. Кога ќе се прикаже порака за завршување, допрете на **Затвори**.

   Екранот автоматски се затвора по одреден временски период ако не допрете на **Затвори**.

Проверување на комуникацијата помеѓу уреди и компјутери

Проверување на конекцијата со користење на команда Ping — Windows

Може да користите Ping команда за да се осигурате дека компјутерот е поврзан со скенерот. Следете ја постапката опишана подолу за да ја проверите конекцијата со помош на Ping команда.

1. Проверете ја IP адресата на скенерот за конекцијата којашто сакате да ја проверите.

   Ова може да го проверите со помош на Epson Scan 2.

2. Се прикажува екранот за брза команда на комјутерот.

   ❏ Windows 10

   Со десен клик притиснете го копчето за старт или притиснете го и држете го, а потоа изберете **Брза команда**.

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

   Се прикажува екранот за апликација и потоа изберете **Брза команда**.

   ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 или понова верзија

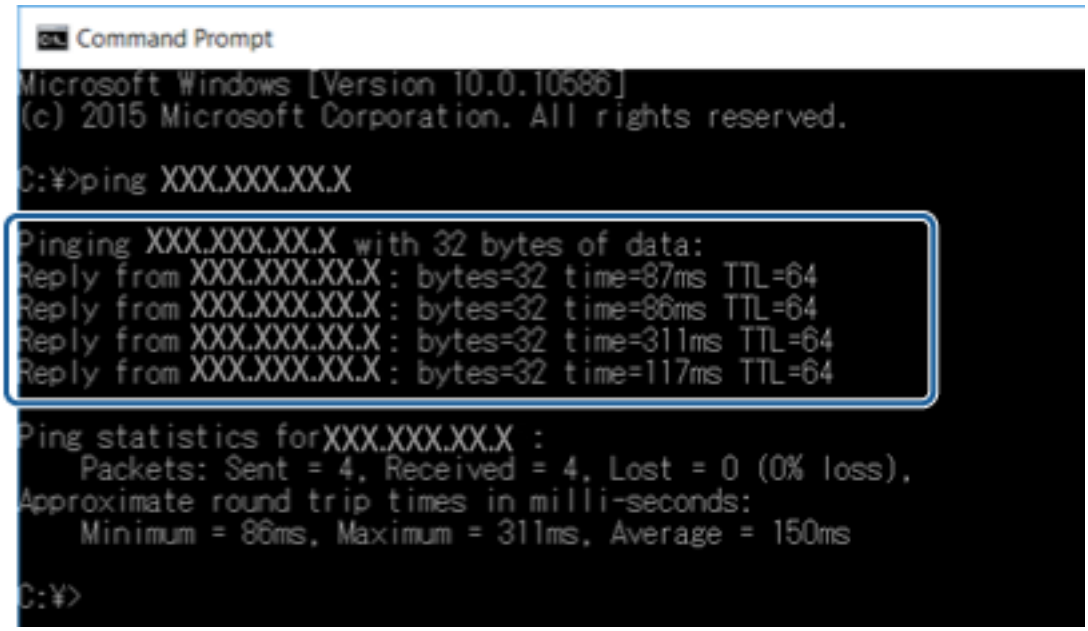
   Кликнете на почетното копче, изберете **Сите програми** или **Програми** > **Дополнителни делови** > **Брза команда**.

3. Внесете „ping xxx.xxx.xxx.xxx“ и притиснете на копчето Enter (Внеси).

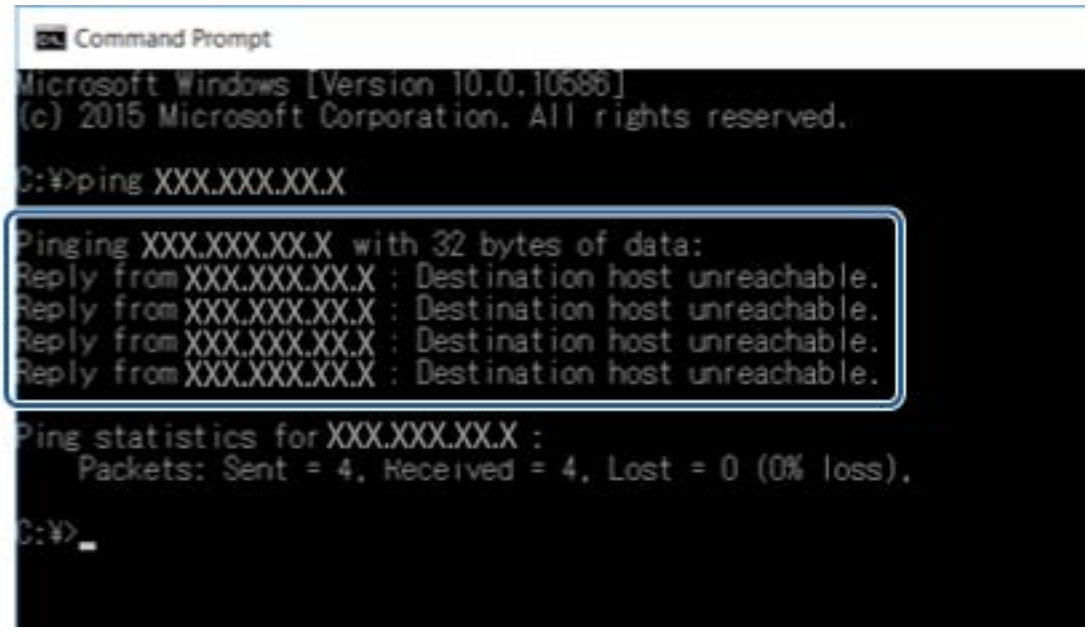
   Внесете ја IP адресата на скенерот за xxx.xxx.xxx.xxx.

4. Проверете го статусот на комуникација.

   Ако се воспостави комуникација помеѓу скенерот и компјутерот, се прикажува следнава порака.



Ако не се воспостави комуникација помеѓу скенерот и компјутерот, се прикажува следнава порака.



Проверување на конекцијата со користење на команда Ping — Mac OS

Може да користите Ping команда за да се осигурате дека компјутерот е поврзан со скенерот. Следете ја постапката опишана подолу за да ја проверите конекцијата со помош на Ping команда.

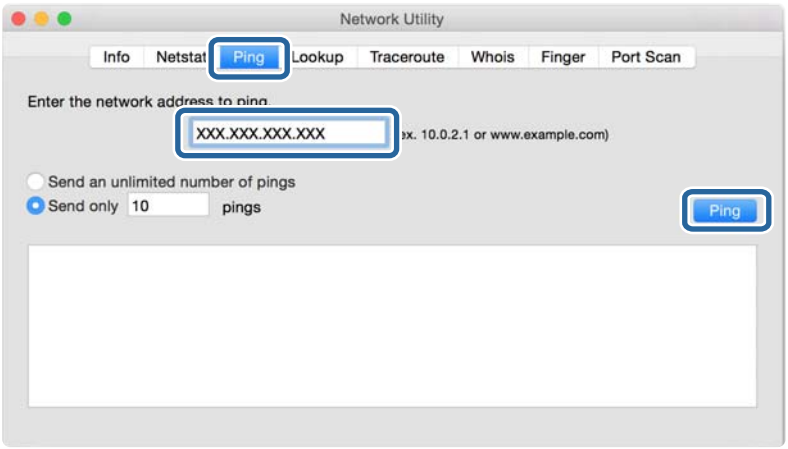
1. Проверете ја IP адресата на скенерот за конекцијата којашто сакате да ја проверите.

   Ова може да го проверите со помош на Epson Scan 2.

2. Активирајте ги алатките за мрежа.

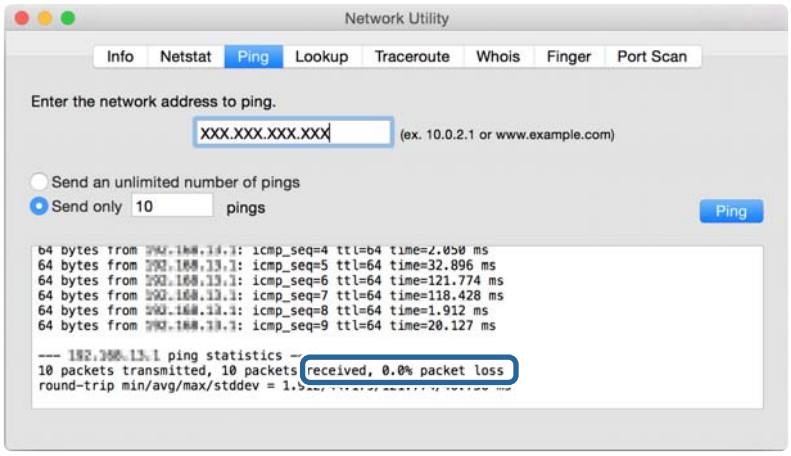
   Внесете „Алатки за мрежа“ во **Spotlight**.

3. Кликнете на јазичето **Ping**, вметнете ја IP адресата којашто сте ја избрале во чекор 1 и кликнете на **Ping**.

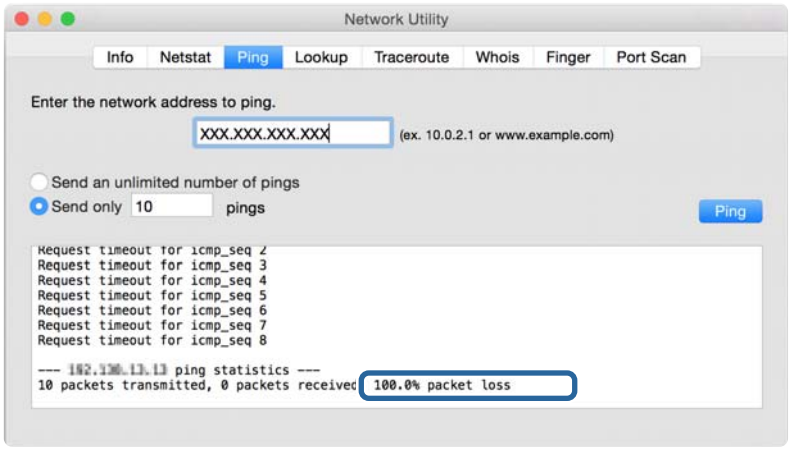


4. Проверете го статусот на комуникација.

   Ако се воспостави комуникација помеѓу скенерот и компјутерот, се прикажува следнава порака.



   Ако не се воспостави комуникација помеѓу скенерот и компјутерот, се прикажува следнава порака.



Проблеми со користење на мрежен софтвер

Не може да пристапите на Web Config

Дали IP адресата на скенерот е правилно конфигурирана?

Конфигурирајте ја IP адресата со користење на Epson Device Admin или EpsonNet Config.

Дали вашиот пребарувач ги поддржува групните енркипции за Encryption Strength за SSL/TLS?

Групните енкрипции за Encryption Strength за SSL/TLS се следниве. Со Web Config може да пристапите во пребарувач којшто ги поддржува следниве групни енкрипции. Проверете ја поддршката за енкрипција на пребарувачот.

❏ 80-битна: AES256/AES128/3DES

❏ 112-битна: AES256/AES128/3DES

❏ 128-битна: AES256/AES128

❏ 192-битна: AES256

❏ 256-битна: AES256

Пораката „Застарено“ се прикажува кога сакате да пристапите до Web Config со користење на SSL комуникација (https).

Ако сертификатот е застарен, повторно добијте го сертификатот. Ако се прикаже порака пред датумот на истекување, погрижете се датумот на скенерот да биде правилно конфигуриран.

Се прикажува пораката „Името на безбедносниот сертификат не се совпаѓа…“ кога сакате да пристапите до Web Config со користење на SSL комуникација (https).

IP адресата на скенерот внесена за **Common Name** за креирање на самопотпишан сертификат или CSR не се совпаѓа со адресата внесена во пребарувачот. Добијте го и повторно внесете го сертификатот или променете го името на скенерот.

На скенерот се пристапува преку прокси сервер.

Ако користите прокси сервер со скенерот, треба да ги конфигурирате поставките за прокси на пребарувачот.

❏ Windows:

Изберете **Контролна табла** > **Мрежа и интернет** > **Опции за интернет** > **Конекции** > **Поставки за LAN** > **Прокси сервер** и конфигурирајте да не го користите прокси серверот за локални адреси.

❏ Mac OS:

Изберете **Претпочитани вредности на систем** > **Мрежа** > **Напредно** > **Прокси** и регистрирајте ја локалната адреса за **Поставки за бајпас прокси за овие главни компјутери и домени**.

Пример:

192.168.1.*: Локална адреса 192.168.1.XXX, маска на подмрежа 255.255.255.0

192.168.*.*: Локална адреса 192.168.XXX.XXX, маска на подмрежа 255.255.0.0

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Назначување на IP адресата“ на страница 15

➡ „Назначува на IP адреса со EpsonNet Config“ на страница 56

Име на модел и/или IP адреса не се прикажани на EpsonNet Config

Дали сте избрале Блокирај, Откажи или Исклучи кога Windows е прикажан безбедносен екран или екран на заштитен ѕид?

Ако изберете **Блокирај**, **Откажи** или **Исклучи**, IP адресата и името на моделот нема да се прикаже на EpsonNet Config или EpsonNet Setup.

За да го поправите ова, регистрирајте го EpsonNet Config како исклучок со користење на Windows заштитен ѕид и комерцијален безбедносен софтвер. Ако користите антивирус или безбедносен програм, затворете го и обидете се да го користите EpsonNet Config.

Дали поставката за прекин на грешка во комуникација е премногу кратка?

Активирајте го EpsonNet Config и изберете **Tools** > **Options** > **Timeout** и зголемете ја должината на времето за поставката **Communication Error**. Имајте предвид дека ако го направите ова EpsonNet Config може да функционира побавно.

Поврзани информации

➡ „Активирање на EpsonNet Config — Windows“ на страница 56

➡ „Активирање на EpsonNet Config — Mac OS“ на страница 56

Додаток

Вовед во мрежен софтвер

Со следното се опишува софтверот со кој се конфигурира и менаџира со уреди.

Epson Device Admin

Epson Device Admin е апликација со којашто може да инсталирате уреди на мрежата и потоа да ги конфигурирате и да ги уредувате. Може да се стекнете со детални информации за уреди како што е статусот и артиклите, испраќање известувања за тревоги и создавање извештаи за употребата на уредот. Исто така, може да направите образец којшто ги содржи ставките за поставки и да го примените на други уреди како заеднички поставки. Може да го преземете Epson Device Admin од интернет страницата за поддршка на Epson. За повеќе информации погледнете ја документацијата или помошта на Epson Device Admin.

Активирање на Epson Device Admin (само за Windows)

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

Белешка:
Ако се прикаже предупредување за заштитен ѕид, дозволете пристап за Epson Device Admin.

EpsonNet Config

Со EpsonNet Config администраторот може да ги конфигурира мрежните поставки на скенерот, како одредување на IP адреса или менување на режимот за поврзување. Функцијата за поставка на група е поддржана на Windows. За повеќе информации погледнете ја документацијата или помошта на EpsonNet Config.

Активирање на EpsonNet Config — Windows

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

Белешка:
Ако се прикаже предупредување за заштитен ѕид, дозволете пристап за EpsonNet Config.

Активирање на EpsonNet Config — Mac OS

Изберете **Оди** > **Апликации** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager е софтвер за креирање на пакет за едноставна инсталација на скенерот, како на пример инсталирање и конфигурирање на драјверот на скенерот и инсталирање на Document Capture Pro. Со овој софтвер администраторот може да креира единствени пакети на софтвер и да ги дистрибуира на групи.

За повеќе информации посетете ја регионалната интернет страница на Epson.

Назначува на IP адреса со EpsonNet Config

Можете да назначите IP за скенерот со помош на EpsonNet Config. EpsonNet Config ви дозволува да назначувате IP адреса за скенер којшто нема по поврзувањето со Ethernet кабел.

Назначување IP адреса со поставки за група

Создавање на датотека за групни поставки

Можете да создавате нова SYLK датотека за да поставите IP адреса со помош на MAC адресата и името на моделот како клучеви.

1. Отворете апликација за пресметки (како Microsoft Excel) или едитор на текстови.

2. Внесете „Info_MACAddress“, „Info_ModelName“, и „TCPIP_IPAddress“ во првиот ред како имиња на ставките од поставувањето.

   Внесете ставки за поставувањето за следните текстуални низи. За да направите разлика меѓу големи/мали букви и карактери со двоен/единечен бајт, само ако еден карактер е различен, ставката нема да биде препознаена.

   Внесете го името на ставката од поставувањето како што е опишано подолу; инаку, EpsonNet Config не може да ги препознае ставките од поставувањето.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Внесете ја MAC адресата, името на моделот и IP адресата за секој мрежен интерфејс.

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. Внесете име и зачувајте како SYLK датотека (*.slk).

Правење на групни поставки со конфигурациска датотека

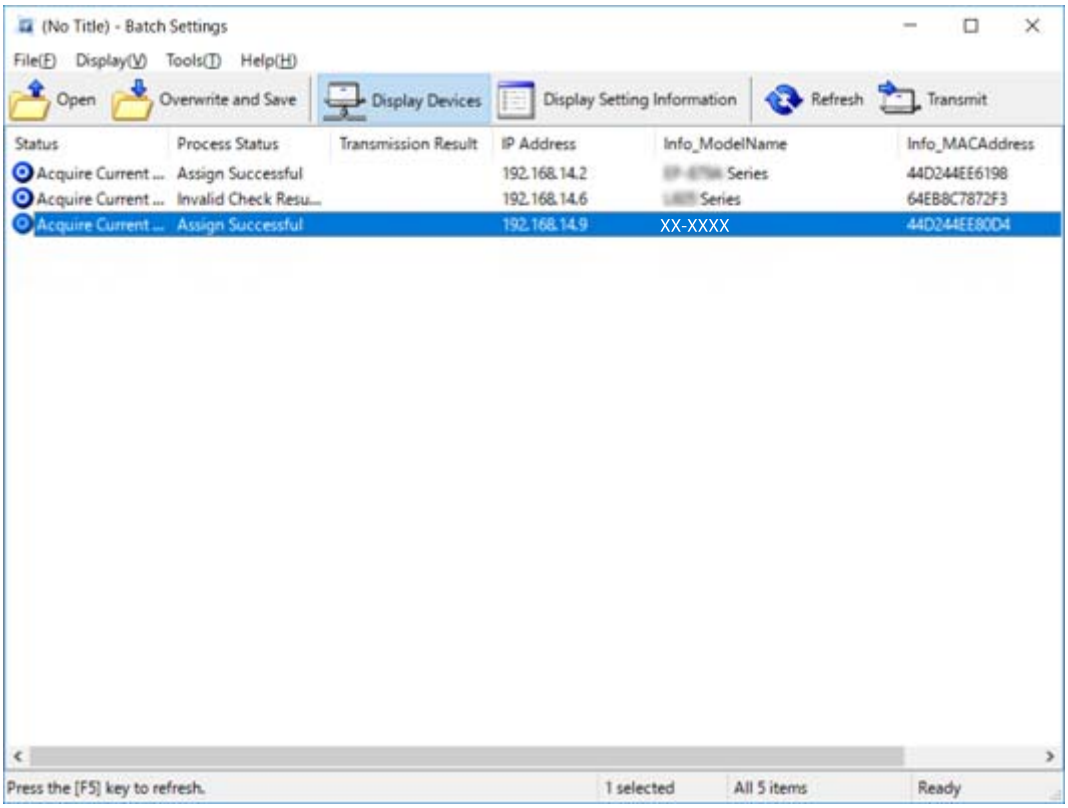
Назначувајте IP адреси во конфигурациската датотека (SYLK датотека) една по една. Треба да ја создадете конфигурациската датотека пред назначување.

1. Поврзете ги сите уреди со мрежата со Ethernet кабел.
2. Вклучете го скенерот.
3. Активирајте го EpsonNet Config.

   Ќе биде прикажана листа со скенери во мрежата. Може да биде потребно повеќе време додека се покажат.
4. Кликнете **Tools** > **Batch Settings**.
5. Кликнете **Open**.
6. Одберете ја SYLK датотеката (*.slk) на екранот за одбирање што ги содржи поставките и потоа кликнете на **Open**.

7. Одберете ги уредите за коишто сакате да извршувате групни поставки со колоната **Status** поставена на **Unassigned**, и **Process Status** поставено на **Assign Successful**.

   Кога избирате повеќекратно, притиснете Ctrl или Shift и кликнете или влечете со глувчето.



8. Кликнете **Transmit**.

9. Кога е пиркажан влезниот екран за лозинката, внесете ја и потоа кликнете на **OK**.

   Пренесете ги поставките.

   Белешка:
   Информациите се пренесуваат на мрежниот интерфејс сè додека мерачот за пренесувањето не се наполни. Не го исклучувајте уредот или безжичниот аптер и не испраќајте податоци до уредот.

10. На екранот **Transmitting Settings**, кликнете на **OK**.

11. Проверете го статусот на уредот што го поставувате.

    Проверете ја содржината на датотеката со поставки за уредите коишто прикажуваат  или  , или за уредот којшто се рестартирал нормално.

Икона	Status	Process Status	Објаснување
	Setup Complete	Setup Successful	Поставувањето е завршено нормално.
	Setup Complete	Rebooting	Кога информацијата е пренесена, секој уред треба да биде рестартиран за да се овозможат поставките. Се извршува проверка за да се одреди дали уредот може да биде поврзан по рестартирањето.
	Setup Complete	Reboot Failed	Не може да се потврди уредот по пренесувањето на поставките. Проверете дали уредот е вклучен или дали се рестартирал нормално.
	Setup Complete	Searching	Се пребарува уредот индициран во датотеката со поставки.*
	Setup Complete	Search Failed	Не може да се проверат уреди што веќе биле поставени. Проверете дали уредот е вклучен или дали се рестартирал нормално.*

    * Само кога се прикаќани информации за поставувањето.

Поврзани информации

➡ „Активирање на EpsonNet Config — Windows“ на страница 56

➡ „Активирање на EpsonNet Config — Mac OS“ на страница 56

Назначување IP адреса за секој уред

Назначете IP адреса за скенерот со EpsonNet Config.

1. Вклучете го скенерот.
2. Поврзете го скенерот на мрежата со Ethernet кабел.
3. Активирајте го EpsonNet Config.

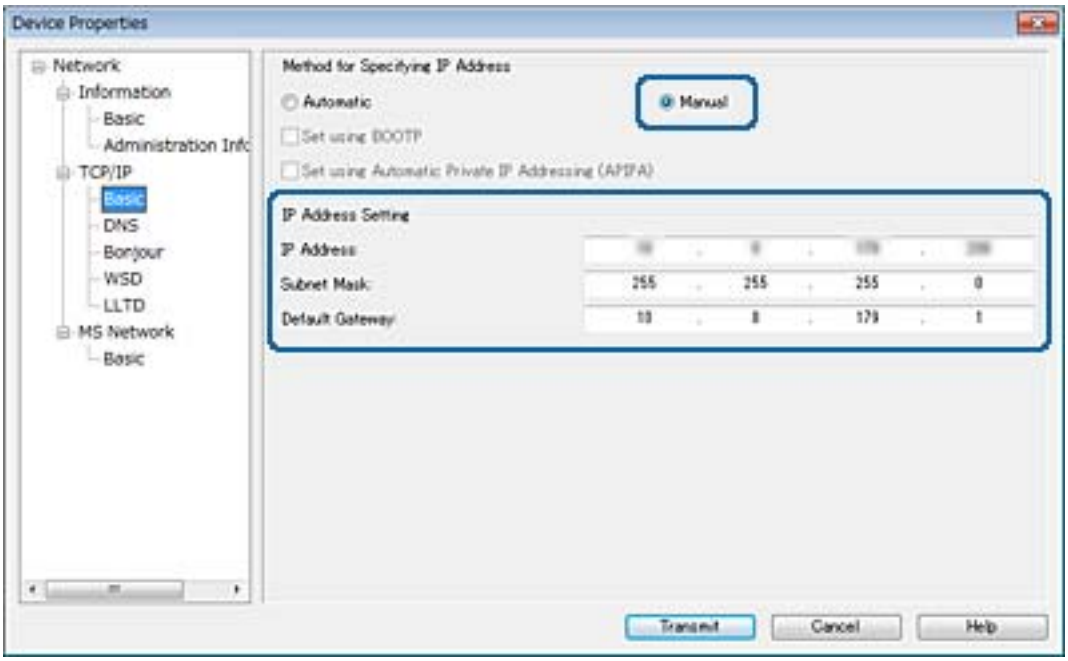
   Ќе биде прикажана листа со скенери во мрежата. Може да биде потребно повеќе време додека се покажат.

4. Кликнете двапати на скенерот којшто сакате да го назначите.

   Белешка:
   Ако сте поврзале повеќе скенери од истиот модел, можете да го идентификувате саканиот скенер со MAC адресата.

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

6. Внесете ги адресите за **IP Address**, **Subnet Mask**, и **Default Gateway**.



Белешка:
Внесете статична адреса кога го поврзувате скенерот на безбедна мрежа.

7. Кликнете **Transmit**.

   Се прикажува екран со којшто се потврдува преносот на информации.

8. Кликнете **OK**.

   Се прикажува екранот за комплетирање на преносот.

   Белешка:
   Информациите се пренесуваат до уредот и се прикажува пораката „Конфигурацијата е успешно компетирана“. Не го исклучувајте уредот и не испраќајте податоци до уредот.

9. Кликнете **OK**.

Поврзани информации

➡ „Активирање на EpsonNet Config — Windows“ на страница 56
➡ „Активирање на EpsonNet Config — Mac OS“ на страница 56

Употреба на порта за скенерот

Скенерот ја употребува следнава порта. Овие порти треба да се доволи да станат достапни од страна на администраторот на мрежата кога е потребно.

Додаток

Испраќач (клиент)	Употреба	Дестинација (сервер)	Протокол	Број на порта
Скенер	Испраќање на е-порака (Известување на е-пошта)	SMTP сервер	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP пред SMTP конекција (Известување на е-порака)	POP сервер	POP3 (TCP)	110
	Control WSD	Компјутер на клиент	WSD (TCP)	5357
	Пребарување на компјутер кога се врши скенирање со притискање од Document Capture Pro	Компјутер на клиент	Network Push Scan Discovery	2968
	Собирање информации за задача кога се скенира со притискање копче од Document Capture Pro	Компјутер на клиент	Network Push Scan	2968
Компјутер на клиент	Откријте го скенерот од апликација како што е EpsonNet Config, двигател за скенер.	Скенер	ENPC (UDP)	3289
	Соберете и поставете MIB информации од апликација како што е EpsonNet Config, двигател за скенер.	Скенер	SNMP (UDP)	161
	Пребарување WSD скенер	Скенер	WS-Discovery (UDP)	3702
	Препраќање податоци од скенирање од Document Capture Pro	Скенер	Network Scan (TCP)	1865

Напредни безбедносни поставки за претпријатија

Во ова поглавје објаснуваме напредни безбедносни поставки за претпријатија.

Безбедносни поставки и спречување на опасност

Кога уред е поврзан со мрежа, можете да му пристапите од далечна локација. Освен тоа, многу луѓе можат да ги споделуваат уредот што е корисно при подобрувањето на оперативната ефикасност и пригодност. Сепак, ризиците како што е нелегалниот пристап, нелегалната употреба и неодобреното чепкање на податоците се зголемени. Ако го употребувате уредот во средина каде што можете да добиете пристап до интернет, ризиците се уште поголеми.

За да се одбегне овој ризик, уредите на Epson употребуваат разни безбедносни технологии.

Поставете го уредот онака како што е потребно според условите на средината коишто се изградени со информациите на клиентот.

Име	Тип на карактеристика	Што да се постави	Што да се спречи
SSL/TLS комуникација	Патеката за комуникација на компјутерот и уредот е шифрирана со помош на SSL/TLS комуникација. Содржината на комуникацијата помеѓу пребарувачот е заштитена.	Поставете CA сертификат за серверот којшто е сертификат потпишан од CA (издавач на сертификати) за уредот.	Спречете протекување на информации за поставки и содржините на префрлените податоци на скенерот од компјутер. Пристапот до Epson серверот на интернет од уредот може да биде заштитен и со користење на ажурирана фирмвер верзија итн.
IPsec/IP филтрирање	Можете да поставите да се дозволи отсекување на податоци што се од одреден клиент или се од одреден тип. Бидејќи IPsec ги заштитува податоците преку IP пакет (енкрипција и автентикација), можете безбедно да комуницирате небезбеден протокол за скенирање.	Создадете основна и индивидуална политика за да го поставите клиентот или типот на податоци за коишто може да се пристапува на уредот.	Заштитете неавторизиран пристап, неодобрено чепкање и пресретнување на комуникациски податоци до уредот.
SNMPv3	Додадени се карактеристики како надгледување на поврзаните уреди во мрежата, интегритетот на податоци за SNMP протокол за контрола, енкрипција, корисничка автентикација итн.	Овозможете SNMPv3, потоа поставете го методот на автентикација и енкрипција.	Осигурете поставки за промена преку мрежата, доверливост во состојба на надгледување.

Име	Тип на карактеристика	Што да се постави	Што да се спречи
IEEE802.1X	Се дозволува само корисник кој е автентикуван за поврзување со Ethernet. Дозволува само одобрен корисник да го употребува уредот.	Поставка за автентикација за RADIUS сервер (сервер за автентикација).	Заштитува навторизиран пристап и употреба на уредот.
Отчитување на картичка за идентификација	Можете да го користите уредот со држење на картичка за идентификација над авентикуваниот уред што е поврзан. Можете да го ограничите стекнувањето со дневници за секој корисник или уред и да ја ограничите дозволената употреба на уредите и достапните карактеристики за секој корисник и група.	Поврзете го уредот за автентикација со уредот и потоа поставете ја информацијата за корисник во системот за автентикација.	Спречете неовластена употреба и фалсификување на уредот.

Поврзани информации

➡ „SSL/TLS комуникација со скенер“ на страница 63

➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 71

➡ „Користење на SNMPv3 протокол“ на страница 83

➡ „Поврзување на скенерот на IEEE802.1X мрежа“ на страница 85

Поставки за безбедносна карактеристика

Кога го поставувате IPsec/IP филтрирањето или IEEE802.1X, се препорачува да пристапите до Web Config со помош на SSL/TLS за да се искомуницираат информациите за поставките за да може да се намалат безбедносните ризици како што е неодобрено чепкање или пресретнување.

SSL/TLS комуникација со скенер

Кога сертификатот на серверот е поставен со SSL/TLS (Secure Sockets Layer/Transport Layer Security) комуникација со скенерот, можете да ја шифрирате патеката на комуникација меѓу компјутерите. Направете го ова ако сакате да спречите далечински и неавторизиран пристап.

Во врска со дигитална сертификација

❏ Сертификат потпишан од ИС

Сертификатот потпишан од ИС (Издавач на сертификати) може да го добиете од издавачот на сертификати. Може да обезбедите безбедни комуникации со користење на сертификат потпишан од ИС. Може да го користите сертификатот потпишан од ИС за сите безбедносни функции.

❏ ИС сертификат

ИС сертификатот означува дека трето лице го проверило идентитетот на серверот. Ова е клучна компонента од тип на проверена интернет страница. Треба да добиете ИС сертификат за автентикација на сервер од ИС којашто го издава.

❏ Самопотпишан сертификат

Самопотпишаниот сертификат е сертификат којшто скенерот го издава и го потпишува. Сертификатот е несигурен и не може да се избегне фалсификување. Ако го користите овој сертификат за SSL/TLS сертификат, може да се прикаже безбедносно предупредување на пребарувачот. Може да го користите овој сертификат само за SSL/TLS комуникација.

Поврзани информации

➡ „Добивање и внесување на ИС потпишан сертификат“ на страница 64

➡ „Бришење на ИС потпишан сертификат“ на страница 68

➡ „Ажурирање на самопотпишан сертификат“ на страница 68

Добивање и внесување на ИС потпишан сертификат

Добивање на ИС потпишан сертификат

За да добиете ИС потпишан сертификат, креирајте CSR (Барање за потпишување на сертификат) и применете го на издавачот на сертификати. Може да креирате CSR со користење на Web Config и компјутерот.

Следете ги чекорите за да креирате CSR и за да добиете ИС потпишан сертификат со користење на Web Config. Кога креирате CSR со користење на Web Config, сертификатот е во PEM/DER формат.

1. Пристапете до Web Config и изберете **Network Security Settings**. Следно, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.

2. Кликнете на **Generate** од **CSR**.

   Се отвора страница за креирање на CSR.

3. Внесете вредност за секоја ставка.

   Белешка:
   Достапните должина на клуч и кратенките се разликуваат во зависност од издавачот на сертификати. Креирајте барање во согласност со правилата на секој издавач на сертификати.

4. Кликнете на **OK**.

   Се прикажува порака за комплетирање.

5. Изберете **Network Security Settings**. Следно, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.

6. Кликнете на едно од копчињата за преземање на **CSR** според одредениот формат од секој издавач на сертификати за да го преземете CSR на компјутер.

> ***Важно:***
>
> *Не генерирајте го CSR повторно. Ако го направите тоа, можно е да не може да го увезете издадениот CA-signed Certificate.*

7. Испратете го CSR на издавач на сертификати и добијте CA-signed Certificate.

   Следете ги правилата на секој издавач на сертификати за методот и формата на испраќање.

8. Зачувајте го издадениот CA-signed Certificate на компјутер поврзан на скенер.

   Добивањето на CA-signed Certificate е комплетирано кога ќе го зачувате сертификатот во дестинација.

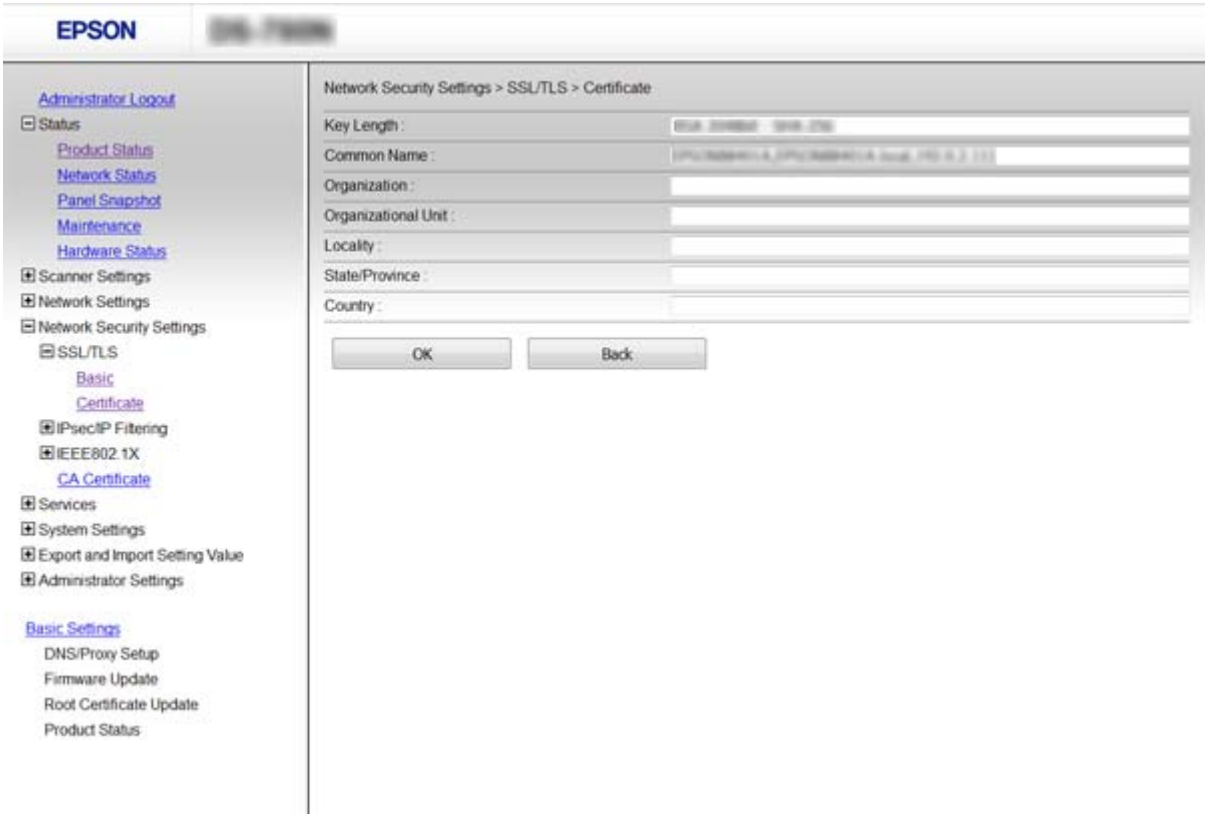
Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Ставки за поставки за CSR“ на страница 65

➡ „Увезување на ИС потпишан сертификат“ на страница 66

Ставки за поставки за CSR



Ставки	Поставки и објаснувања
Key Length	Изберете должина на клуч за CSR.

Ставки	Поставки и објаснувања
Common Name	Може да внесете од 1 до 128 знаци. Ако е IP адреса, треба да биде статична IP адреса. Пример: URL за пристапување Web Config: https://10.152.12.225 Заедничко име: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Може да внесете од 0 до 64 знаци во ASCII (0x20–0x7E). Може да ги одвоите одредените имиња со запирки.
Country	Внесете код за земја со двоцифрен број назначен со ISO-3166.

Поврзани информации

➡ „Добивање на ИС потпишан сертификат“ на страница 64

Увезување на ИС потпишан сертификат

Важно:

❏ *Погрижете се дека датумот и времето на скенерот се точно поставени.*

❏ *Ако добиете сертификат со користење на CSR креиран од Web Config, може еднаш да го увезете сертификатот.*

1. Пристапете до Web Config и изберете **Network Security Settings**. Следно, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.

2. Кликнете на **Import**.

   Се отвора страница за увезување на сертификат.

3. Внесете вредност за секоја ставка.

   Во зависност од тоа каде го креирате CSR и форматот на датотеката на сертификатот, бараните поставки може да се разликуваат. Внесете ги вредностите за бараните ставки во согласност со следново.

   ❏ Сертификат со PEM/DER формат добиен од Web Config

      ❏ **Private Key**: Не конфигурирајте затоа што скенерот содржи приватен клуч.

      ❏ **Password**: Не конфигурирајте.

      ❏ **CA Certificate 1**/**CA Certificate 2**: Опционално

   ❏ Сертификат со PEM/DER формат добиен од компјутер

      ❏ **Private Key**: Треба да го поставите.

      ❏ **Password**: Не конфигурирајте.

      ❏ **CA Certificate 1**/**CA Certificate 2**: Опционално

❏ Сертификат со PKCS#12 формат добиен од компјутер

❏ **Private Key**: Не конфигурирајте.

❏ **Password**: Опционално

❏ **CA Certificate 1/CA Certificate 2**: Не конфигурирајте.

4. Кликнете на **OK**.

Се прикажува порака за комплетирање.

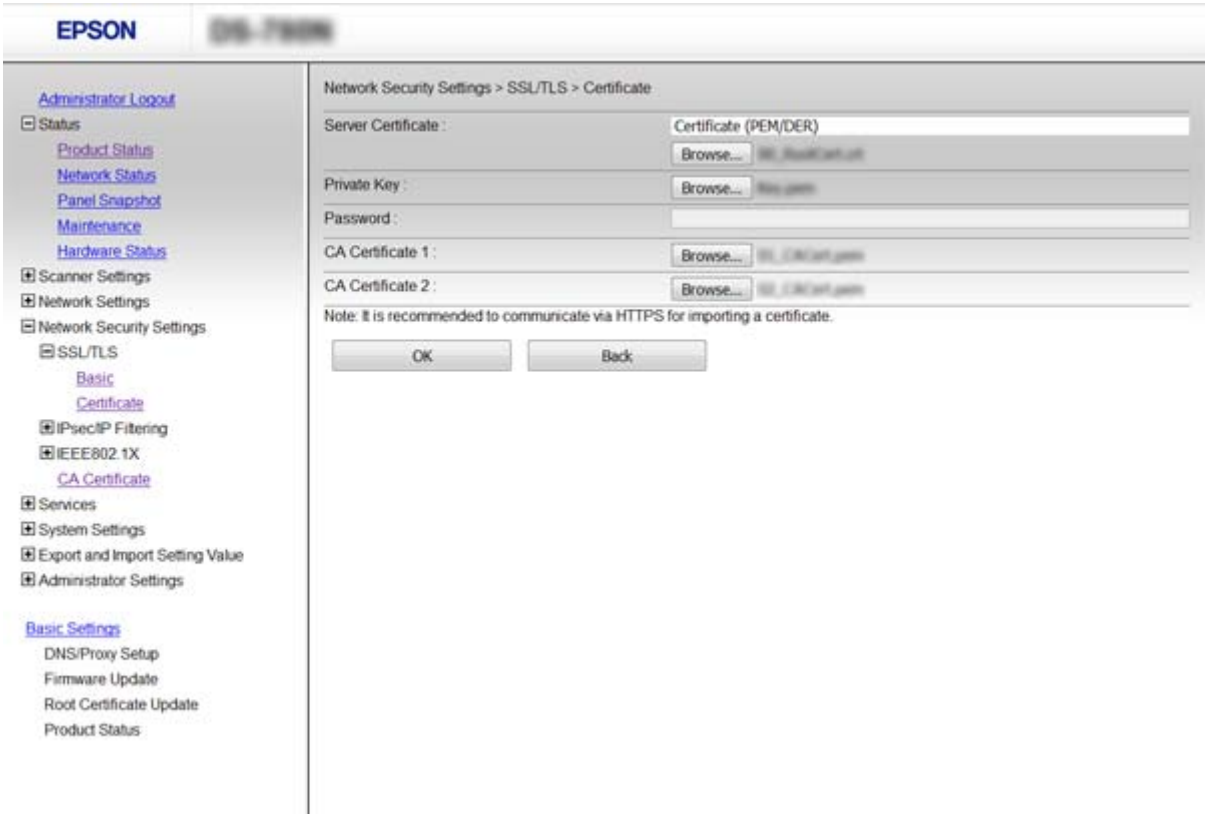
Белешка:
*Кликнете на **Confirm** за да ги проверите информациите за сертификатот.*

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Ставки за поставка на ИС потпишан сертификат“ на страница 67

Ставки за поставка на ИС потпишан сертификат



Ставки	Поставки и објаснувања
Server Certificate или Client Certificate	Изберете го форматот на сертификатот.
Private Key	Ако добиете сертификат со PEM/DER формат со користење на CSR креиран од компјутер, назначете датотека за приватен клуч којашто одговара на сертификатот.
Password	Внесете лозинка за да го шифрирате приватниот клуч.

Ставки	Поставки и објаснувања
CA Certificate 1	Ако форматот на сертификатот е **Certificate (PEM/DER)**, внесете го сертификатот на издавачот на сертификати којшто го издава сертификатот за серверот. Назначете датотека ако е потребно.
CA Certificate 2	Ако форматот на сертификатот е **Certificate (PEM/DER)**, внесете го сертификатот на издавачите на сертификати коишто го издаваат **CA Certificate 1**. Назначете датотека ако е потребно.

Поврзани информации

➡ „Увезување на ИС потпишан сертификат“ на страница 66

Бришење на ИС потпишан сертификат

Може да избришете внесен сертификат ако сертификатот е застарен или кога шифрираната конекција повеќе не е потребна.

Важно:

Ако добиете сертификат со користење на CSR креиран од Web Config, не може повторно да го внесете избришаниот сертификат. Во овој случај, креирајте CSR и повторно добијте го сертификатот.

1. Пристапете до Web Config, и потоа изберете **Network Security Settings**. Следно, изберете **SSL/TLS** > **Certificate** или **IPsec/IP Filtering** > **Client Certificate** или **IEEE802.1X** > **Client Certificate**.
2. Кликнете **Delete**.
3. Потврдете дека сакате да го избришете сертификатот во прикажаната порака.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Ажурирање на самопотпишан сертификат

Ако скенерот ја поддржува функцијата за HTTPS сервер, може да го ажурирате самопотпишаниот сертификат. Кога пристапувате на Web Config со користење на самопотпишан сертификат, се прикажува порака за предупредување.

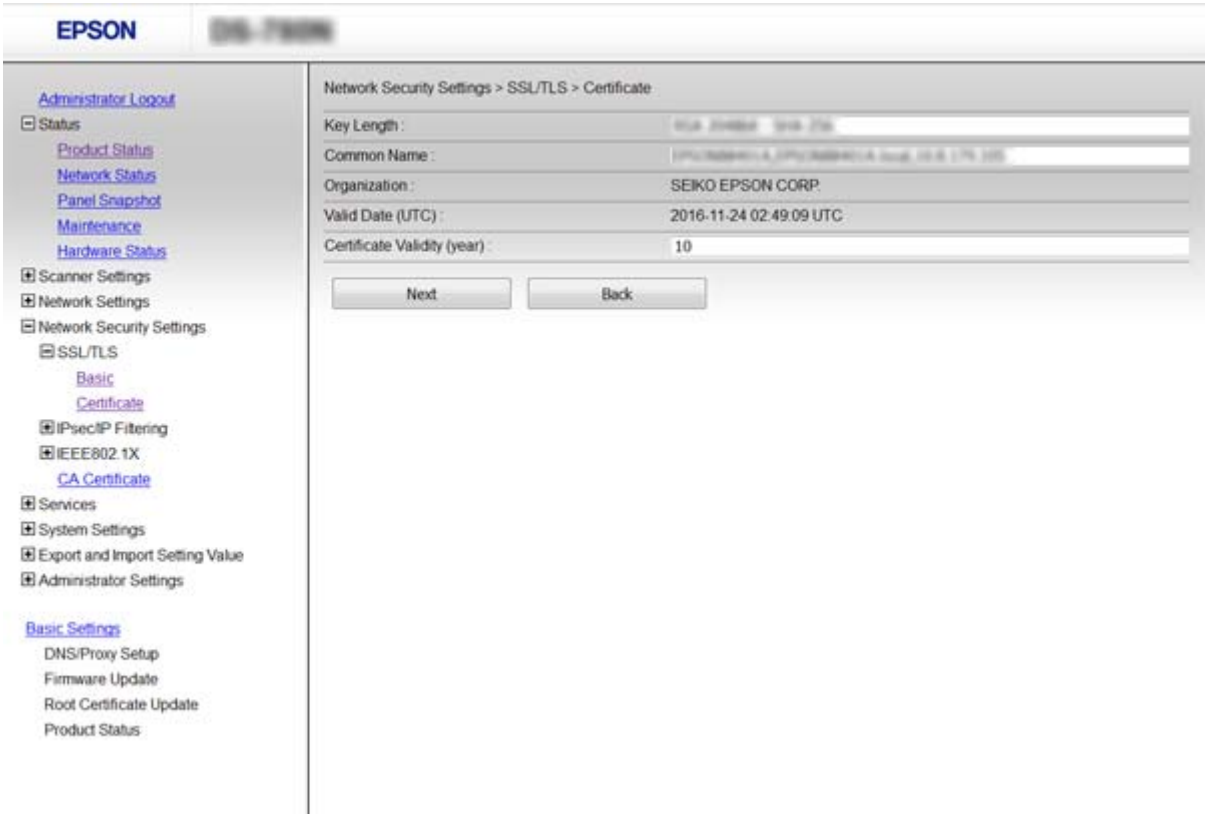
Користете го самопотпишаниот сертификат привремено додека не го добиете и увезете ИС потпишаниот сертификат.

1. Пристапете до Web Config и изберете **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Кликнете **Update**.
3. Внесете **Common Name**.

   Внесете IP адреса или идентификатор како на пример FQDN име за скенерот. Може да внесете од 1 до 128 знаци.

Белешка:
Може да го одвоите одредената име (CN) со запирки.

4. Назначете период на важност за сертификатот.



5. Кликнете **Next**.

   Се прикажува порака за потврда.

6. Кликнете **OK**.

   Скенерот е ажуриран.

Белешка:
*Кликнете на **Confirm** за да ги проверите информациите за сертификатот.*

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Конфигурирање на CA Certificate

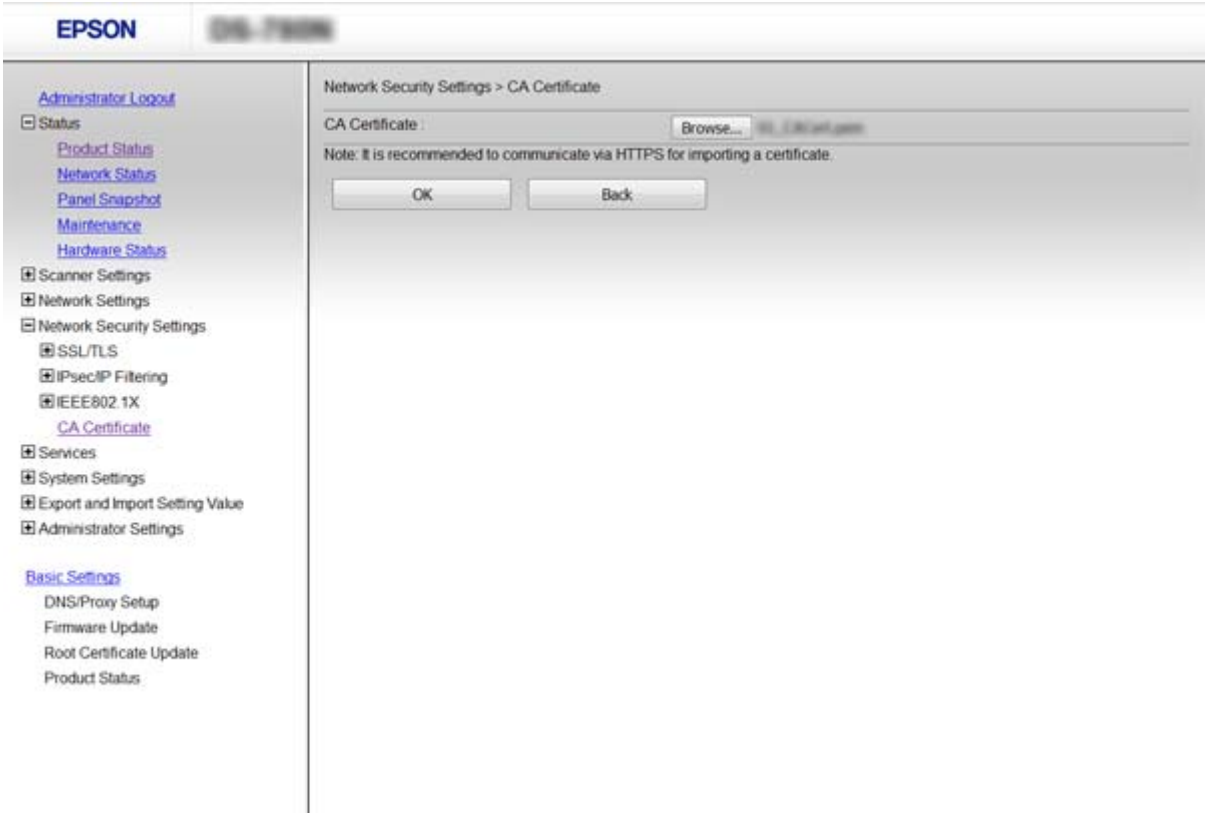
Може да го увезете, да го прикажете и да го избришете CA Certificate.

Увезување на CA Certificate

1. Пристапете до Web Config и изберете **Network Security Settings** > **CA Certificate**.

2. Кликнете на **Import**.

3. Одредете го CA Certificate којшто сакате да го увезете.



4. Кликнете на **OK**.

Кога увезувањето ќе заврши, се враќате на екранот **CA Certificate** и се прикажува увезениот CA Certificate.

Поврзани информации

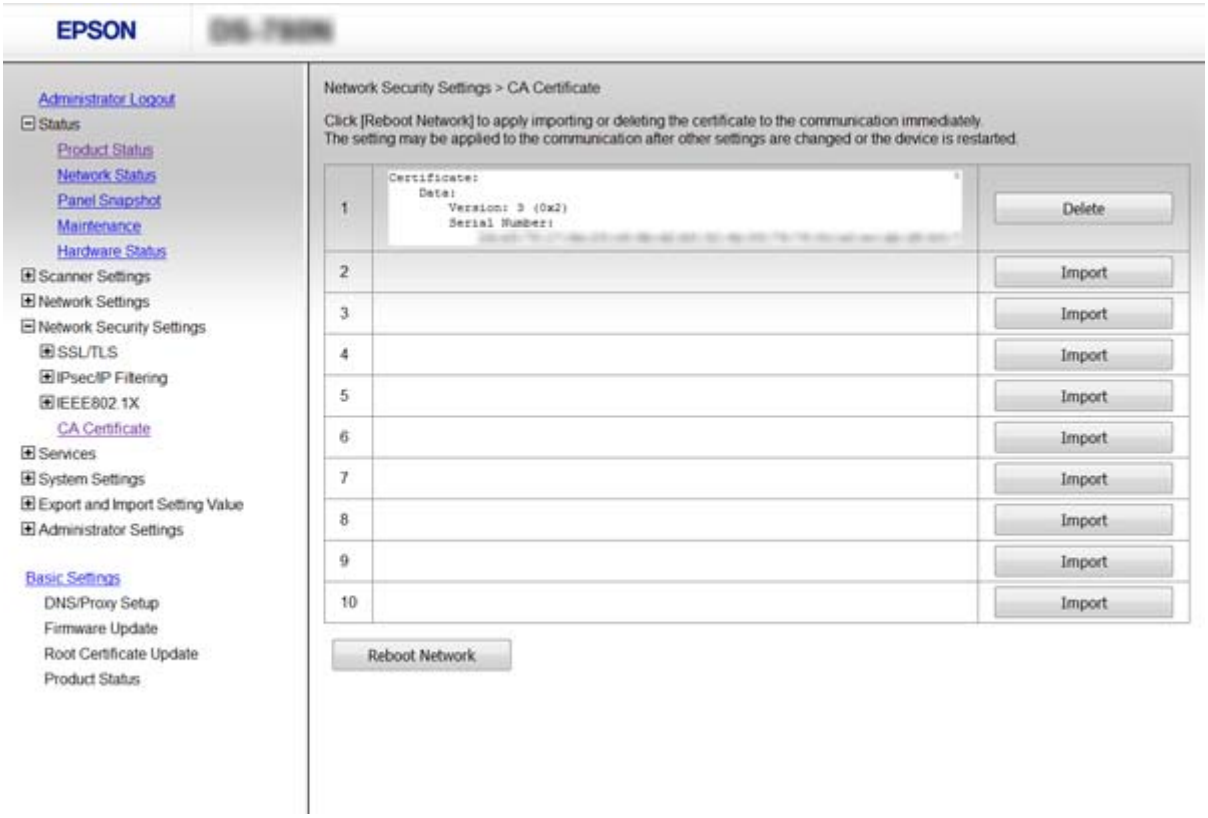
➡ „Пристапување до Web Config“ на страница 23

Бришење на CA Certificate

Може да го избришете внесениот CA Certificate.

1. Пристапете до Web Config и изберете **Network Security Settings** > **CA Certificate**.

2. Кликнете на **Delete** веднаш до CA Certificate којшто сакате да го избришете.



3. Потврдете дека сакате да го избришете сертификатот во прикажаната порака.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Комуникација со енкрипција со помош на IPsec/IP филтрирање

Во врска со IPsec/IP Filtering

Ако скенерот поддржува IPsec/IP филтрирање, може да го филтрирате сообраќајот врз основа на IP адресите, услугите или портите. Со комбинирање на филтрирањето може да го конфигурирате скенерот за да ги прифатите или да ги блокирате одредените клиенти или одредените податоци. Покрај тоа, може да го подобрите нивото на безбедност со користење на IPsec.

За да филтрирате сообраќај, конфигурирајте ја стандардната политика. Стандардната политика се применува на секој корисник или група поврзана на скенерот. За подетална контрола над корисниците или групите на корисници конфигурирајте ги политиките на групата. Политика на групата претставува едно или повеќе правила коишто се применуваат на корисник или на група на корисници. Скенерот ги контролира IP пакетите коишто се совпаѓаат со конфигурираните политики. IP пакетите се автентицираат според редоследот на политиката на групата од 1 до 10, а потоа според стандардната политика.

Белешка:
Компјутерите кошшто имаат Windows Vista или понова верзија или Windows Server 2008 или понова верзија на поддршка за IPsec.

Конфигурирање на Default Policy

1. Пристапете до Web Config и изберете **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Внесете вредност за секоја ставка.
3. Кликнете на **Next**.

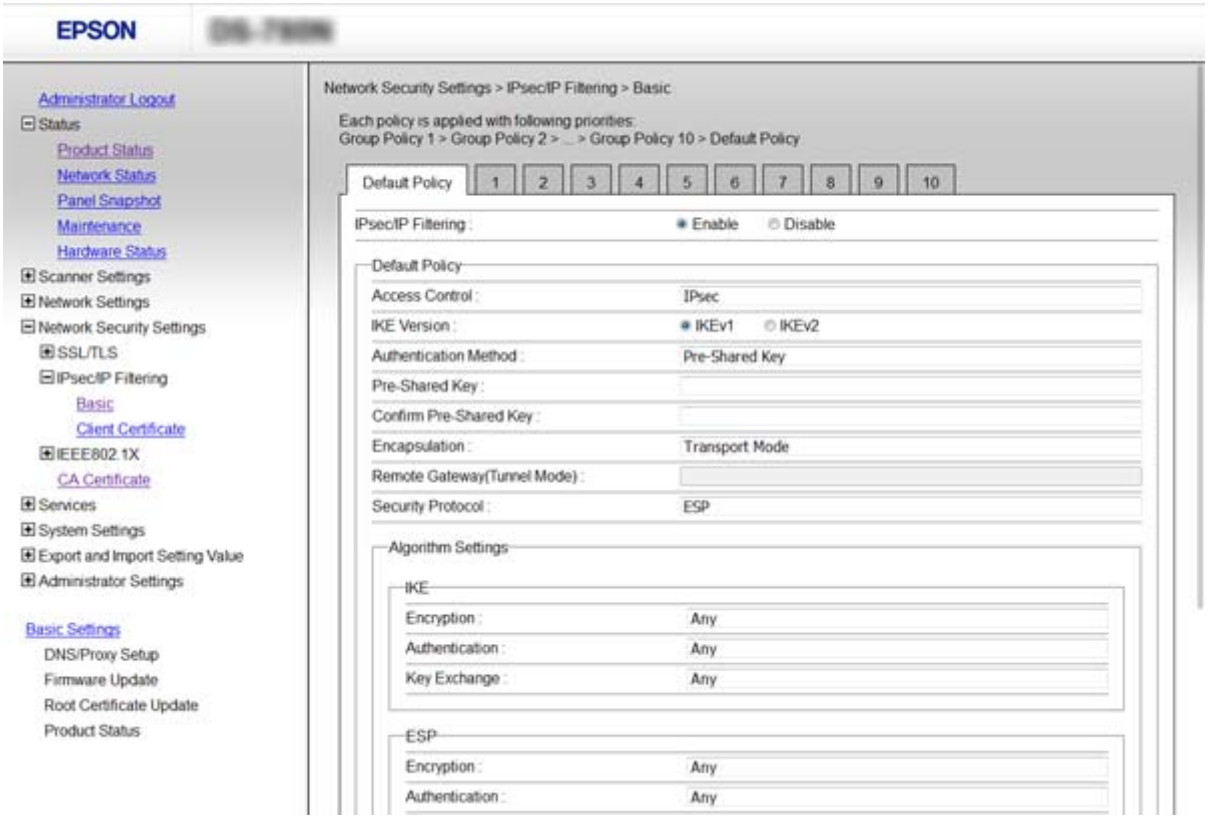
   Се прикажува порака за потврда.
4. Кликнете на **OK**.

   Скенерот е ажуриран.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23
➡ „Ставки за поставки за Default Policy“ на страница 72

Ставки за поставки за Default Policy



Напредни безбедносни поставки за претпријатија

Ставки	Поставки и објаснувања	
IPsec/IP Filtering	Може да ја активирате или да ја деактивирате функцијата IPsec/IP филтрирање.	
Access Control	Конфигурирајте го методот на контрола за сообраќајот на IP пакети.	
	Permit Access	Изберете го ова за да дозволите конфигурираните IP пакети да поминат.
	Refuse Access	Изберете го ова за да одбиете конфигурираните IP пакети да поминат.
	IPsec	Изберете го ова за да дозволите конфигурираните IPsec пакети да поминат.
IKE Version	Одберете IKEv1 или IKEv2 за верзија IKE. Одберете едно од тие според уредот со којшто е поврзан скенерот.	
IKEv1	Прикажани се следните ставки кога одбирате **IKEv1** за **IKE Version**.	
	Authentication Method	За да изберете **Certificate**, мора да го добиете и да го внесете ИС потпишаниот сертификат однапред.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете го претходно споделениот клуч од 1 до 127 знаци.
	Confirm Pre-Shared Key	Внесете го клучот којшто сте го конфигурирале за потврда.
IKEv2	Прикажани се следните ставки кога одбирате **IKEv2** за **IKE Version**.	
Local	Authentication Method	За да изберете **Certificate**, мора да го добиете и да го внесете ИС потпишаниот сертификат однапред.
	ID Type	Одберете го типот на ID за скенерот.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не можете да употребувате „@“, „#“, и „=“ за првиот карактер. **Distinguished Name**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „=“. **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 и 255 карактери со помош на A–Z, a–z, 0–9, „-“ и точка, и (.). **Email Address**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „@“. **Key ID**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете го претходно споделениот клуч од 1 до 127 знаци.
	Confirm Pre-Shared Key	Внесете го клучот којшто сте го конфигурирале за потврда.

Напредни безбедносни поставки за претпријатија

Ставки	Поставки и објаснувања	
Remote	Authentication Method	За да изберете **Certificate**, мора да го добиете и да го внесете ИС потпишаниот сертификат однапред.
	ID Type	Изберете го типот на ID за уредот што сакате да извршите автентикација.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не можете да употребувате „@“, „#“, и „=“ за првиот карактер. **Distinguished Name**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „=“. **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 и 255 карактери со помош на A–Z, a–z, 0–9, „-“ и точка, и (.). **Email Address**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „@“. **Key ID**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете го претходно споделениот клуч од 1 до 127 знаци.
	Confirm Pre-Shared Key	Внесете го клучот којшто сте го конфигурирале за потврда.
Encapsulation	Ако изберете **IPsec** за **Access Control**, треба да го конфигурирате режимот за енкапсулација.	
	Transport Mode	Ако го користите само скенерот на истата LAN, изберете го ова. IP пакетите од ниво 4 или понови се шифрирани.
	Tunnel Mode	Ако користите скенер на мрежа на интернет како на пример IPsec-VPN, изберете ја оваа опција. Насловот и податоците на IP пакетите се шифрирани.
Remote Gateway(Tunnel Mode)	Ако изберете **Tunnel Mode** за **Encapsulation**, внесете ја адресата на излезот од 1 до 39 знаци.	
Security Protocol	**IPsec** за **Access Control**, одберете опција.	
	ESP	Изберете го ова да за обезбедите интегритет на автентикацијата и на податоците и да ги шифрирате податоците.
	AH	Изберете го ова да за обезбедите интегритет на автентикацијата и на податоците. Дури и кога податоците за енркипција се забранети, може да го користите IPsec.
Algorithm Settings		

Ставки	Поставки и објаснувања	
IKE	Encryption	Одберете го алгоритамот на енкрипција за IKE. Ставките варираат во зависност од верзијата на IKE.
	Authentication	Одберете го алгоритамот на автентикација за IKE.
	Key Exchange	Одберете го алгоритамот на размена за IKE. Ставките варираат во зависност од верзијата на IKE.
ESP	Encryption	Одберете го алгоритамот на енкрипција за ESP. Ова е достапно кога **ESP** е одбрано за **Security Protocol**.
	Authentication	Одберете го алгоритамот на автентикација за ESP. Ова е достапно кога **ESP** е одбрано за **Security Protocol**.
AH	Authentication	Одберете го алгоритамот на енкрипција за AH. Ова е достапно кога **AH** е одбрано за **Security Protocol**.

Поврзани информации

➡ „Конфигурирање на Default Policy“ на страница 72

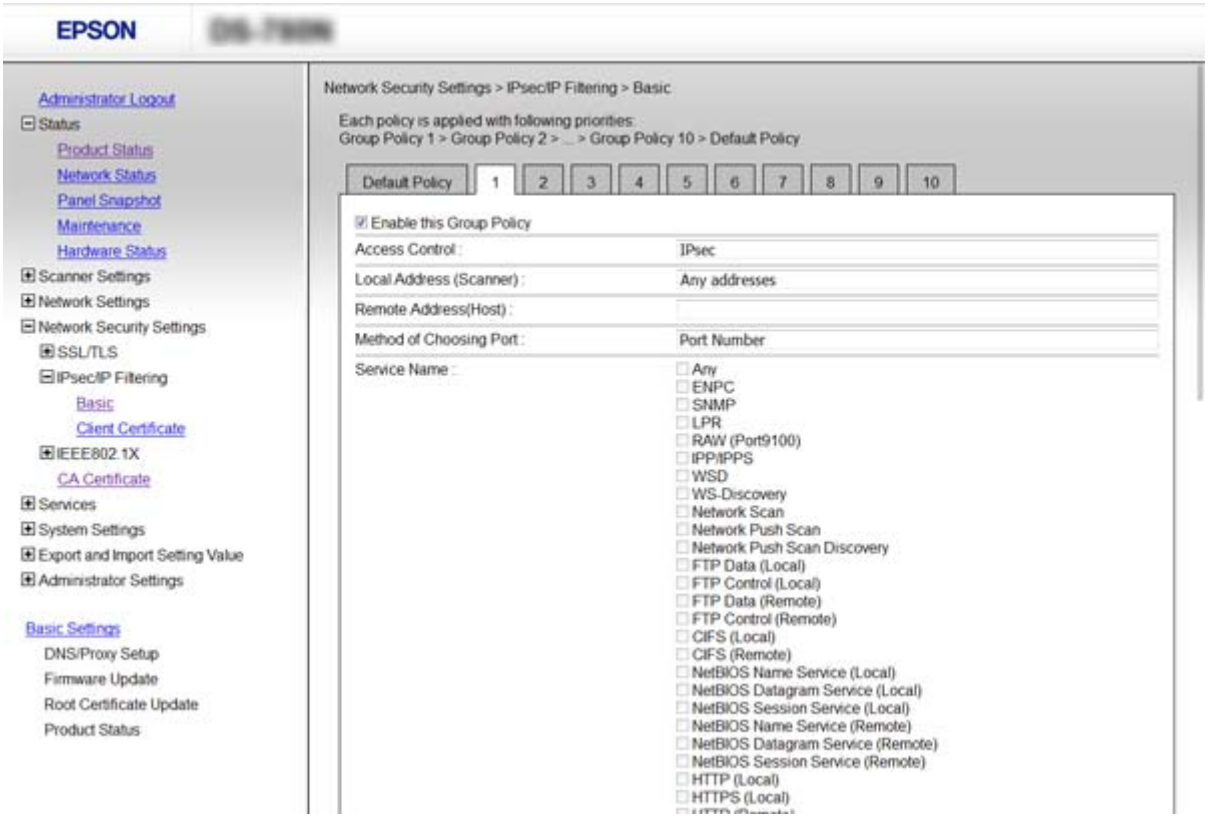
Конфигурирање на Group Policy

1. Пристапете до Web Config и изберете **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Кликнете на нумерираното јазиче коешто сакате да го конфигурирате.
3. Внесете вредност за секоја ставка.
4. Кликнете на **Next**.
   Се прикажува порака за потврда.
5. Кликнете на **OK**.
   Скенерот е ажуриран.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23
➡ „Ставки за поставки за Group Policy“ на страница 76

Ставки за поставки за Group Policy



Ставки	Поставки и објаснувања	
Enable this Group Policy	Може да ја овозможите или да ја оневозможите политиката на групата.	
Access Control	Конфигурирајте го методот на контрола за сообраќајот на IP пакети.	
	Permit Access	Изберете го ова за да дозволите конфигурираните IP пакети да поминат.
	Refuse Access	Изберете го ова за да одбиете конфигурираните IP пакети да поминат.
	IPsec	Изберете го ова за да дозволите конфигурираните IPsec пакети да поминат.
Local Address (Scanner)	Изберете IPv4 адреса или IPv6 адреса којашто одговара на вашата мрежна околина. Ако IP адресата ја назначувате автоматски, може да изберете **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Внесете ја IP адресата за да го контролирате пристапот. IP адресата мора да има 43 знаци или помалку. Ако не внесете IP адреса, сите адреси се контролирани. ***Белешка:*** *Ако IP адресата се назначува автоматски (на пр. назначена со DHCP), конекцијата може да не биде достапна. Конфигурирајте статична IP адреса.*	
Method of Choosing Port	Изберете метод за специфицирање на порти.	
Service Name	Ако изберете **Service Name** за **Method of Choosing Port**, изберете опција.	

Напредни безбедносни поставки за претпријатија

Ставки	Поставки и објаснувања	
Transport Protocol	Ако изберете **Port Number** за **Method of Choosing Port**, треба да го конфигурирате режимот за енкапсулација.	
	Any Protocol	Изберете го ова за да ги контролирате сите типови на протоколи.
	TCP	Изберете го ова за да ги контролирате податоците за unicast.
	UDP	Изберете го ова за да ги контролирате податоците за емитирање и multicast.
	ICMPv4	Изберете го ова за да ја контролирате командата ping.
Local Port	Ако изберете **Port Number** за **Method of Choosing Port** и ако изберете **TCP** или **UDP** за **Transport Protocol**, внесете ги броевите на портата за да го контролирате примањето на пакети, одделувајќи ги со запирки. Може да внесете броеви на најмногу 10 порти. Пример: 20,80,119,5220 Ако не внесете број на порта, сите порти се контролирани.	
Remote Port	Ако изберете **Port Number** за **Method of Choosing Port** и ако изберете **TCP** или **UDP** за **Transport Protocol**, внесете ги броевите на портата за да го контролирате испраќањето на пакети, одделувајќи ги со запирки. Може да внесете броеви на најмногу 10 порти. Пример: 25,80,143,5220 Ако не внесете број на порта, сите порти се контролирани.	
IKE Version	Одберете IKEv1 или IKEv2 за верзија IKE. Одберете едно од тие според уредот со којшто е поврзан скенерот.	
IKEv1	Прикажани се следните ставки кога одбирате **IKEv1** за **IKE Version**.	
	Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опција. Употребениот сертификат е заеднички со стандардна политика.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете го претходно споделениот клуч од 1 до 127 знаци.
	Confirm Pre-Shared Key	Внесете го клучот којшто сте го конфигурирале за потврда.
IKEv2	Прикажани се следните ставки кога одбирате **IKEv2** за **IKE Version**.	

Напредни безбедносни поставки за претпријатија

Ставки	Поставки и објаснувања	
Local	Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опција. Употребениот сертификат е заеднички со стандардна политика.
	ID Type	Одберете го типот на ID за скенерот.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не можете да употребувате „@“, „#“, и „=“ за првиот карактер. **Distinguished Name**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „=“. **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 и 255 карактери со помош на A–Z, a–z, 0–9, „-“ и точка, и (.). **Email Address**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „@“. **Key ID**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете го претходно споделениот клуч од 1 до 127 знаци.
	Confirm Pre-Shared Key	Внесете го клучот којшто сте го конфигурирале за потврда.
Remote	Authentication Method	Ако изберете **IPsec** за **Access Control**, изберете опција. Употребениот сертификат е заеднички со стандардна политика.
	ID Type	Изберете го типот на ID за уредот што сакате да извршите автентикација.
	ID	Внесете го ID на скенерот, којшто се совпаѓа со типот на ID. Не можете да употребувате „@“, „#“, и „=“ за првиот карактер. **Distinguished Name**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „=“. **IP Address**: Внесете IPv4 или IPv6 формат. **FQDN**: Внесете комбинација од 1 и 255 карактери со помош на A–Z, a–z, 0–9, „-“ и точка, и (.). **Email Address**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци. Треба да вклучите и „@“. **Key ID**: Внесете од 1 до 128 1-бајтни ASCII (од 0x20 до 0x7E) знаци.
	Pre-Shared Key	Ако изберете **Pre-Shared Key** за **Authentication Method**, внесете го претходно споделениот клуч од 1 до 127 знаци.
	Confirm Pre-Shared Key	Внесете го клучот којшто сте го конфигурирале за потврда.

Напредни безбедносни поставки за претпријатија

Ставки	Поставки и објаснувања	
Encapsulation	Ако изберете **IPsec** за **Access Control**, треба да го конфигурирате режимот за енкапсулација.	
	Transport Mode	Ако го користите само скенерот на истата LAN, изберете го ова. IP пакетите од ниво 4 или понови се шифрирани.
	Tunnel Mode	Ако користите скенер на мрежа на интернет како на пример IPsec-VPN, изберете ја оваа опција. Насловот и податоците на IP пакетите се шифрирани.
Remote Gateway(Tunnel Mode)	Ако изберете **Tunnel Mode** за **Encapsulation**, внесете ја адресата на излезот од 1 до 39 знаци.	
Security Protocol	Ако изберете **IPsec** за **Access Control**, изберете опција.	
	ESP	Изберете го ова да за обезбедите интегритет на автентикацијата и на податоците и да ги шифрирате податоците.
	AH	Изберете го ова да за обезбедите интегритет на автентикацијата и на податоците. Дури и кога податоците за енркипција се забранети, може да го користите IPsec.
Algorithm Settings		
IKE	Encryption	Одберете го алгоритамот на енкрипција за IKE. Ставките вариpаат во зависност од верзијата на IKE.
	Authentication	Одберете го алгоритамот на автентикација за IKE.
	Key Exchange	Одберете го алгоритамот на размена за IKE. Ставките вариpаат во зависност од верзијата на IKE.
ESP	Encryption	Одберете го алгоритамот на енкрипција за ESP. Ова е достапно кога **ESP** е одбрано за **Security Protocol**.
	Authentication	Одберете го алгоритамот на автентикација за ESP. Ова е достапно кога **ESP** е одбрано за **Security Protocol**.
AH	Authentication	Одберете го алгоритамот на автентикација за AH. Ова е достапно кога **AH** е одбрано за **Security Protocol**.

Поврзани информации

➡ „Конфигурирање на Group Policy“ на страница 75

➡ „Комбинација на Local Address (Scanner) и Remote Address(Host) на Group Policy“ на страница 80

➡ „Референции за име на услуга на политика на група“ на страница 80

Комбинација на Local Address (Scanner) и Remote Address(Host) на Group Policy

		Поставување на Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Поставување на Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Празно место	✓	✓	✓

*1 Ако е избрано **IPsec** за **Access Control**, не може да одредите во должина на префикс.

*2 Ако е избрано **IPsec** за **Access Control**, може да изберете линк-локална адреса (fe80::), но политиката на групата ќе биде оневозможена.

*3 Освен IPv6 линк локални адреси.

Референции за име на услуга на политика на група

Белешка:
Прикажани се недостапните услуги, но не може да ги изберете.

Име на услуга	Тип на протокол	Број на локална порта	Број на далечинска порта	Контролирани функции
Any	–	–	–	Сите услуги
ENPC	UDP	3289	Која било порта	Пребарување на скенер од апликации како на пример EpsonNet Config и драјвер за скенер
SNMP	UDP	161	Која било порта	Добивање и конфигурирање на MIB од апликации како на пример EpsonNet Config и Epson драјвер за скенер
WSD	TCP	Која било порта	5357	Контролирање на WSD
WS-Discovery	UDP	3702	Која било порта	Пребарување на скенери од WSD
Network Scan	TCP	1865	Која било порта	Препраќање на податоци од скенирање од Document Capture Pro
Network Push Scan Discovery	UDP	2968	Која било порта	Барање на компјутери од скенерот.
Network Push Scan	TCP	Која било порта	2968	Добивање на информации за работа од скенирање со притискање од Document Capture Pro или Document Capture
HTTP (Local)	TCP	80	Која било порта	HTTP(S) сервер (препраќање на податоци за Web Config и WSD)
HTTPS (Local)	TCP	443	Која било порта	

Име на услуга	Тип на протокол	Број на локална порта	Број на далечинска порта	Контролирани функции
HTTP (Remote)	TCP	Која било порта	80	HTTP(S) клиент (комуникација помеѓу ажурирање на фирмвер и ажурирање на коренов сертификат)
HTTPS (Remote)	TCP	Која било порта	443	

Примери на конфигурација на IPsec/IP Filtering

Примање само на IPsec пакети

Овој пример служи само за конфигурација на стандардна политика.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: Внесете до 127 знаци.

Group Policy:

Не конфигурирајте.

Прифаќање на скенирање со користење на Epson Scan 2 и поставки за скенер

Со овој пример може да комуницирате со податоците за скенирање и конфигурацијата на скенерот од одредени услуги.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Проверете го квадратчето.

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

❏ **Remote Address(Host)**: IP адреса на клиент

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

❏ **Service Name**: Проверете го квадратчето на **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** и **HTTPS (Local)**.

Добивање пристап само од одредена IP адреса

Овој пример овозможува со одредена IP адреса да пристапите до скенерот.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Проверете го квадратчето.

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

❏ **Remote Address(Host)**: IP адреса на клиентот на администраторот

Белешка:
Без разлика на конфигурацијата на политиката, клиентот може да пристапи до и да го конфигурира скенерот.

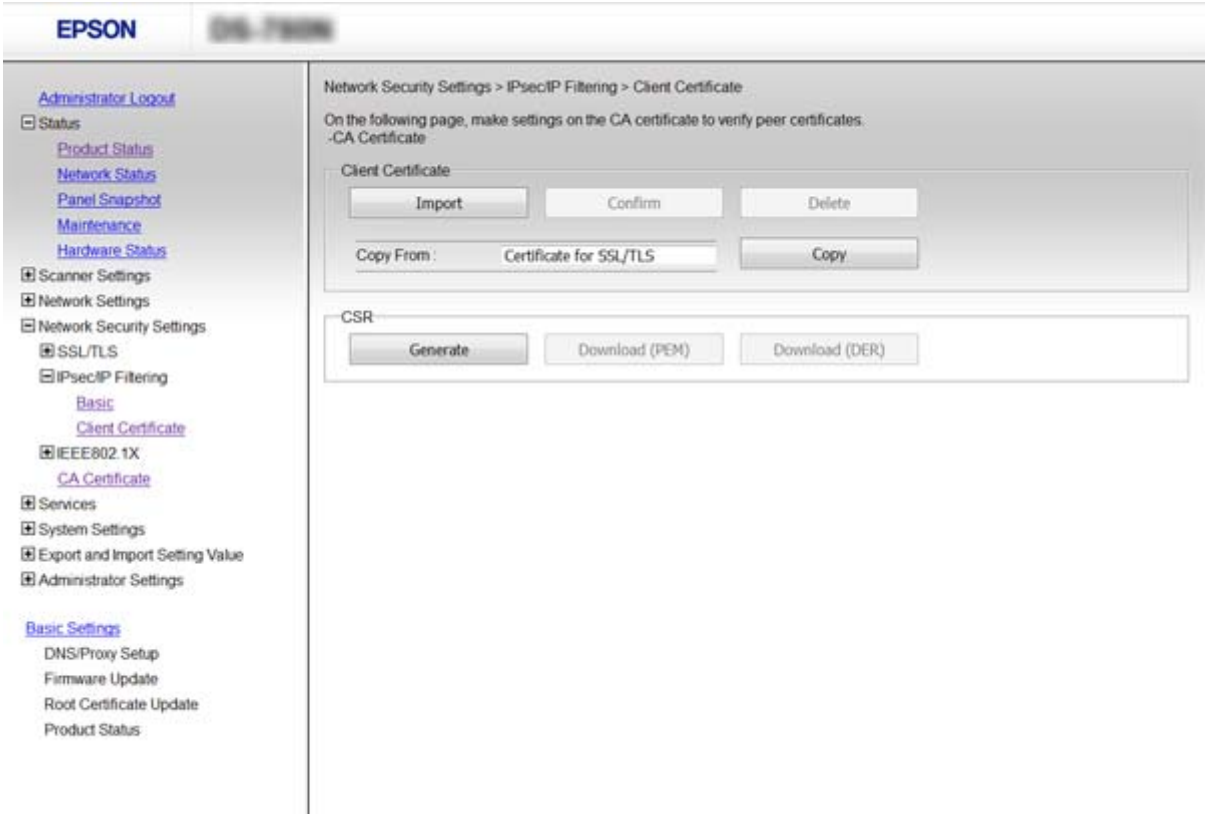
Конфигурирање на сертификат за IPsec/IP Filtering

Конфигурирајте го сертификатот на клиентот за IPsec/IP филтрирање. Ако сакате да го конфигурирате издавачот на сертификати, одете на **CA Certificate**.

1. Пристапете до Web Config и изберете **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Внесете го сертификатот во **Client Certificate**.

   Ако веќе сте го внеле сертификатот објавен од издавачот на сертификати во IEEE802.1X или SSL/TLS, може да го копирате сертификатот и употребете го за IPsec/IP филтрирање. За да го копирате, изберете го сертификатот од **Copy From** и кликнете на **Copy**.



Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Добивање и внесување на ИС потпишан сертификат“ на страница 64

Користење на SNMPv3 протокол

За SNMPv3

SNMP е протокол којшто изведува надгледување и контрола за да собира информации од уредите поврзани со мрежата. SNMPv3 е верзијата на функција за менаџирање со безбедноста, којашто е подобрена.

Кога употребувате SNMPv3, може да биде докажана автентичноста и енкрипцијата на надгледувањето на состојбата и промените на поставките во SNMP комуникацијата (пакетот) за да може да се заштити SNMP комуникацијата (пакетот) од ризици по мрежата како што се прислушување, имитирање и менување.

Конфигурирање на SNMPv3

Ако скенерот го поддржува SNMPv3 протоколот, може да ги следите и да ги контролирате пристапите до скенерот.

1. Пристапете до Web Config и изберете **Services** > **Protocol**.
2. Внесете вредност за секоја ставка од **SNMPv3 Settings**.
3. Кликнете на **Next**.

   Се прикажува порака за потврда.
4. Кликнете на **OK**.

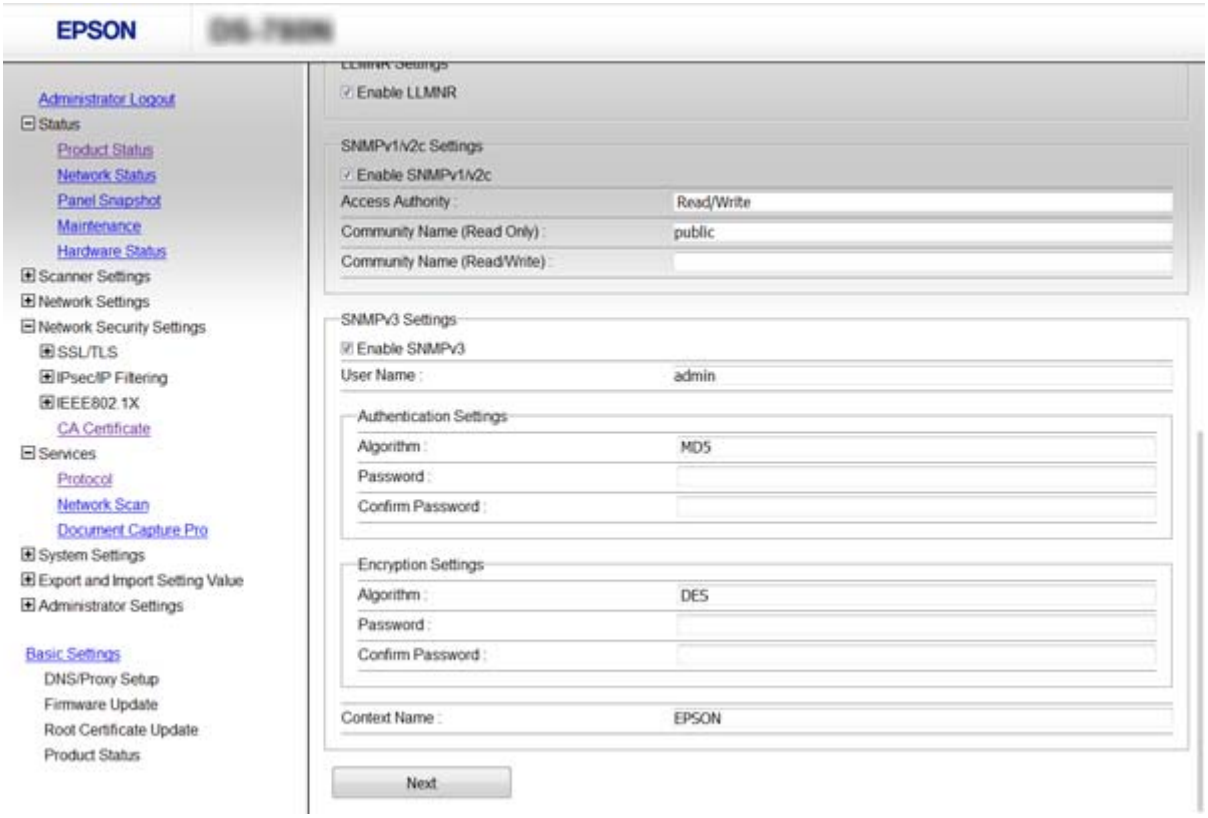
   Скенерот е ажуриран.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Ставки за поставка на SNMPv3“ на страница 84

Ставки за поставка на SNMPv3



Ставки	Поставки и објаснувања
Enable SNMPv3	SNMPv3 е активирано ако е штиклирано квадратчето.
User Name	Внесете од 1 до 32 знаци со користење на знаци од 1 бајт.
Authentication Settings	
Algorithm	Изберете алгоритам за автентикација.
Password	Внесете од 8 до 32 знаци во ASCII (0x20–0x7E).
Confirm Password	Внесете ја лозинката којашто сте ја конфигурирале за потврда.
Encryption Settings	
Algorithm	Изберете алгоритам за енкрипција.
Password	Внесете од 8 до 32 знаци во ASCII (0x20–0x7E).
Confirm Password	Внесете ја лозинката којашто сте ја конфигурирале за потврда.
Context Name	Внесете од 1 до 32 знаци со користење на знаци од 1 бајт.

Поврзани информации

➡ „Конфигурирање на SNMPv3“ на страница 83

Поврзување на скенерот на IEEE802.1X мрежа

Конфигурирање на IEEE802.1X мрежа

Ако скенерот поддржува IEEE802.1X, може да го користите скенерот на мрежа со автентикација којшто е поврзан на RADIUS сервер и мрежен разводник како автентикатор.

1. Пристапете до Web Config и изберете **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Внесете вредност за секоја ставка.
3. Кликнете **Next**.

   Се прикажува порака за потврда.
4. Кликнете **OK**.

   Скенерот е ажуриран.

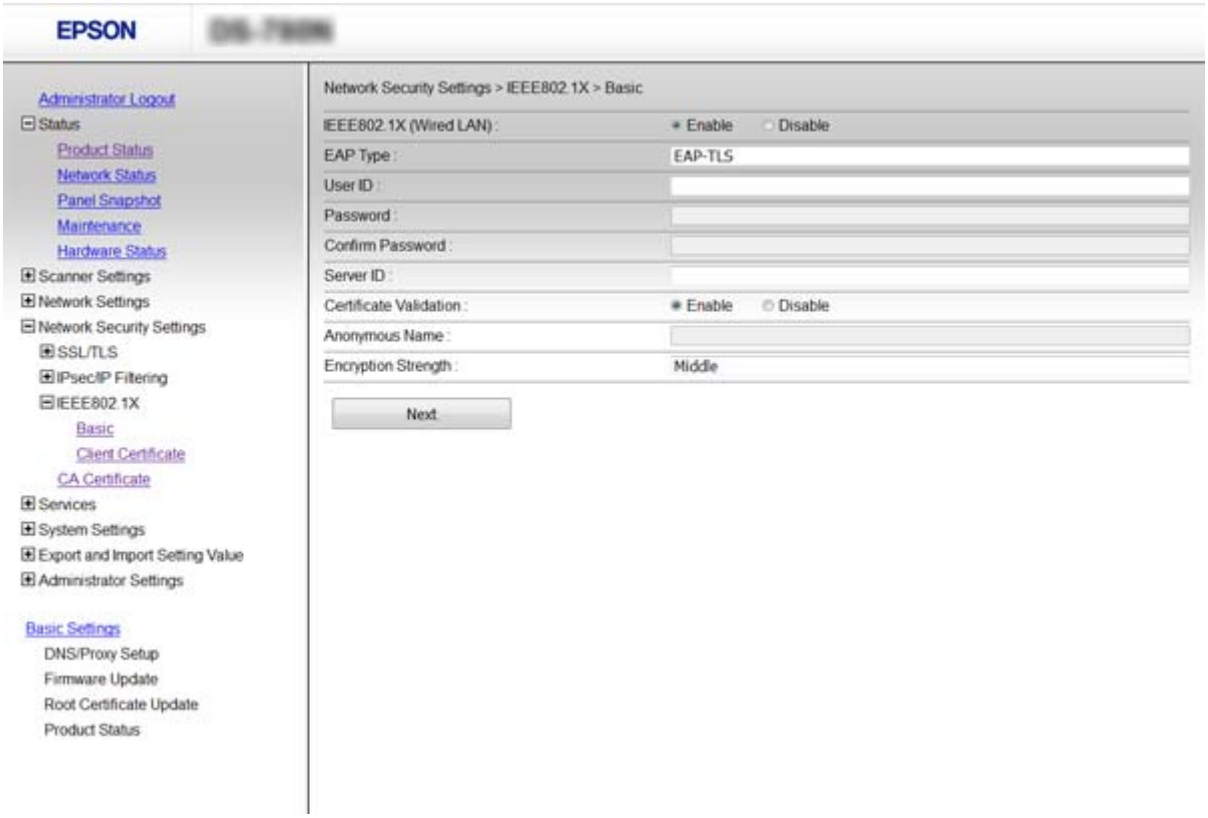
Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Ставки за поставки на IEEE802.1X мрежа“ на страница 86

➡ „Не може да ги конфигурирате печатачот или скенерот по конфигурирање на IEEE802.1X“ на страница 90

Ставки за поставки на IEEE802.1X мрежа



Ставки	Поставки и објаснувања	
IEEE802.1X (Wired LAN)	Може да ги активирате и да ги деактивирате поставките на страницата (**IEEE802.1X** > **Basic**) за IEEE802.1X (Жичен LAN).	
EAP Type	Изберете опција за метод на автентикација помеѓу скенерот и RADIUS серверот.	
	EAP-TLS	Треба да го добиете и да го внесете ИС потпишаниот сертификат.
	PEAP-TLS	
	PEAP/MSCHAPv2	Треба да конфигурирате лозинка.
User ID	Конфигурирајте ID за да го користите за автентикација на RADIUS сервер. Внесете од 1 до 128 1-битен ASCII (од 0x20 до 0x7E) знаци.	
Password	Конфигурирајте лозинка за автентикација на скенерот. Внесете од 1 до 128 1-битен ASCII (од 0x20 до 0x7E) знаци. Ако користите Windows сервер како RADIUS сервер, може да внесете до 127 знаци.	
Confirm Password	Внесете ја лозинката којашто сте ја конфигурирале за потврда.	
Server ID	Може да конфигурирате ID за сервер за да го автентицирате со одреден RADIUS сервер. Автентикаторот проверува дали ID за серверот се содржи во полето предмет/subjectAltName на сертификат за сервер којшто е испратен од RADIUS сервер или не. Внесете од 0 до 128 1-битен ASCII (од 0x20 до 0x7E) знаци.	
Certificate Validation	Може да поставите валидација на сертификат без разлика на методот на автентикација. Внесете го сертификатот во **CA Certificate**.	

Ставки	Поставки и објаснувања	
Anonymous Name	Ако изберете **PEAP-TLS** или **PEAP/MSCHAPv2** за **Authentication Method**, може да конфигурирате анонимно име наместо ID на корисник за фаза 1 од информациите за PEAP. Внесете од 0 до 128 1-битен ASCII (од 0x20 до 0x7E) знаци.	
Encryption Strength	Може да изберете една од следниве.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Поврзани информации

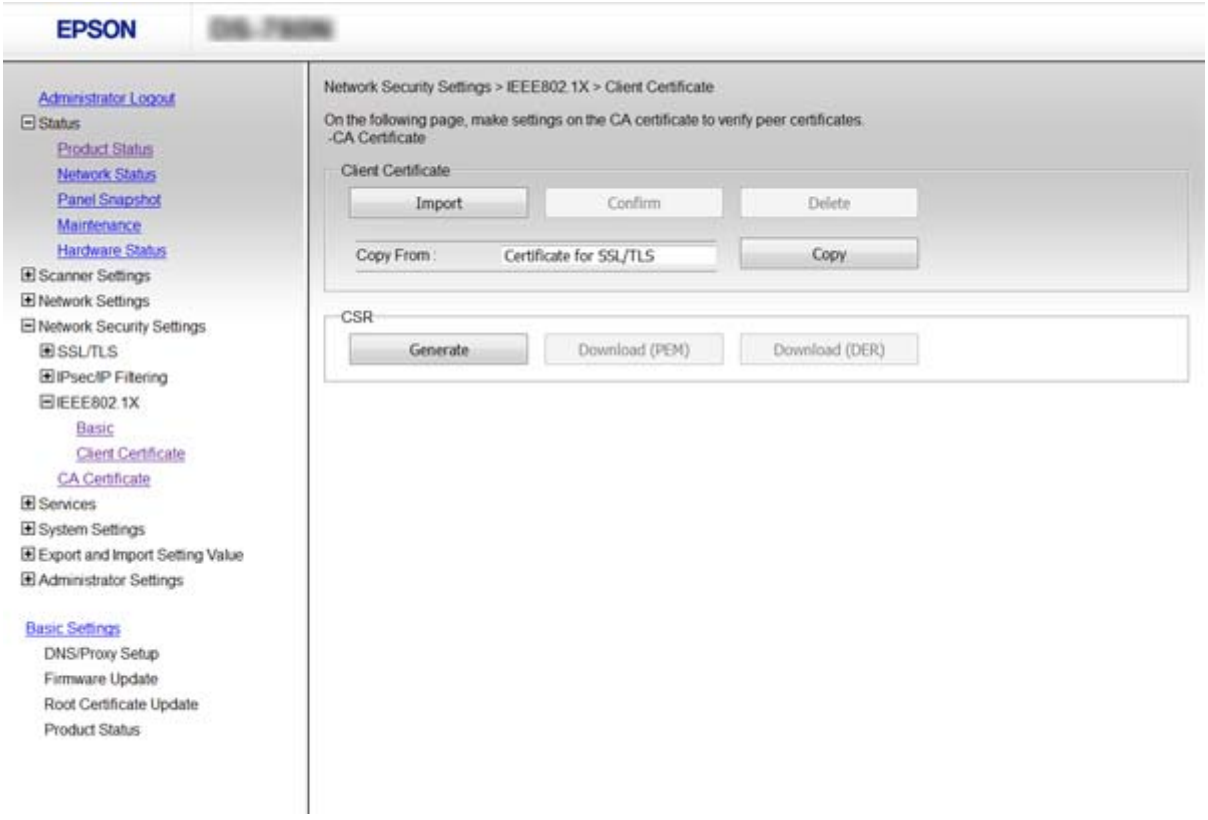
➡ „Конфигурирање на IEEE802.1X мрежа“ на страница 85

Конфигурирање на сертификат за IEEE802.1X

Конфигурирајте го сертификатот на клиентот за IEEE802.1X. Ако сакате да го конфигурирате сертификатот на издавачот на сертификати, одете на **CA Certificate**.

1. Пристапете до Web Config и изберете **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Внесете сертификат во **Client Certificate**.

   Може да го копирате сертификатот ако е објавен од издавачот на сертификати. За да го копирате, изберете го сертификатот од **Copy From** и кликнете на **Copy**.



Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Добивање и внесување на ИС потпишан сертификат“ на страница 64

Решавање проблеми за напредна безбедност

Враќање на безбедносните поставки

Кога утврдувате безбедна средина како IPsec/IP филтрирање или IEEE802.1X, може да не бидете во можност да комуницирате со уредите поради неправилни поставки или проблеми со уредот или серверот. Во тој случај, вратете ги безбедносните поставки за повторно да ги направите поставките за уредот или за да ви се дозволи времена употреба.

Оневозможување на безбедносната функција со помош на контролниот панел

Можете да го оневозможите IPsec/IP филтрирањето или IEEE802.1X со помош на контролниот панел на скенерот.

1. Допрете **Поставки** > **Поставки за мрежа**.
2. Допрете **Промени поставки**.
3. Допрете ги ставките коишто сакате да оневозможите.
   - ❏ **IPsec/IP филтрирање**
   - ❏ **IEEE802.1X**
4. Кога ќе се прикаже порака за завршување, допрете на **Продолжи**.

Враќање на безбедносната функција со Web Config

Уредите може да не се препознаени во мрежата за IEEE802.1X. Во тој случај, оневозможете ја функцијата преку контролниот панел на скенерот.

За IPsec/IP филтрирање можете да ја оневозможите функцијата ако можете да пристапите на уредите од компјутер.

Оневозможување на IPsec/IP филтрирање со помош на Web Config

1. Пристапете до Web Config и одберете **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Изберете **Disable** за **IPsec/IP Filtering** во **Default Policy**.
3. Кликнете на **Next**, и потоа отстранете го **Enable this Group Policy** за сите политики за групи.
4. Кликнете **OK**.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Проблеми со користење на функциите за безбедност на мрежа

Сте го заборавиле претходно споделениот клуч

Повторно конфигурирајте го клучот со користење на Web Config.

За да го промените клучот, пристапете до Web Config и изберете **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** или **Group Policy**.

Кога го менувате споделениот клуч, конфигурирајте го споделениот клуч за компјутери.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

Не може да комуницирате со IPsec комуникација

Дали користите несоодветен алгоритам за поставките за компјутерот?

Скенерот ги поддржува следниве алгоритми.

Безбедносни методи	Алгоритми
IKE алгоритам за енкрипција	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE алгоритам за автентикација	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE алгоритам за размена на клучеви	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 алгоритам за енкрипција	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP алгоритам за автентикација	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH алгоритам за автентикација	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* достапно само за IKEv2

Поврзани информации

➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 71

Одненадеж не може да комуницирате

Дали IP адресата на скенерот е неважечка или е променета?

Оневозможете го IPsec од контролната табла на скенерот.

Ако DHCP е застарен, рестартирањето или IPv6 адресата е застарена или не е добиена, тогаш IP адресата регистрирана за скенерот Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) може да не биде пронајдена.

Користете статична IP адреса.

Дали IP адресата на компјутерот е неважечка или е променета?

Оневозможете го IPsec од контролната табла на скенерот.

Ако DHCP е застарен, рестартирањето или IPv6 адресата е застарена или не е добиена, тогаш IP адресата регистрирана за скенерот Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) може да не биде пронајдена.

Користете статична IP адреса.

Поврзани информации

➡ „Пристапување до Web Config“ на страница 23

➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 71

Не може да се поврзете откако ќе го конфигурирате IPsec/IP филтрирањето

Поставената вредност може да не е точна.

Оневозможете го IPsec/IP филтрирањето од контролната табла на скенерот. Поврзете ги скенерот и компјутерот и повторно направете ги поставките за IPsec/IP филтрирање.

Поврзани информации

➡ „Комуникација со енкрипција со помош на IPsec/IP филтрирање“ на страница 71

Не може да ги конфигурирате печатачот или скенерот по конфигурирање на IEEE802.1X

Поставките може да не се точни.

Оневозможете ги IEEE802.1X од контролната табла на скенерот. Поврзете ги скенерот и компјутерот и повторно конфигурирајте ја IEEE802.1X.

Поврзани информации

➡ „Конфигурирање на IEEE802.1X мрежа“ на страница 85

Проблеми со користење на дигитален сертификат

Не може да го увезете потпишаниот ИС сертификат

Дали потпишаниот ИС сертификат и информациите на CSR се совпаѓаат?

Ако потпишаниот ИС сертификат и CSR не ги споделуваат истите информации, не може да го увезете CSR. Проверете го следново:

- ❏ Дали се обидувате да увезете сертификат на уред којшто ги нема истите информации?

  Проверете ги информациите на CSR па потоа увезете го сертификатот на уредот којшто ги има истите информации.

- ❏ Дали сте го презапишале CSR зачуван во скенерот откако сте го испратиле CSR на издавачите на сертификати?

  Повторно добијте потпишан ИС сертификат со CSR.

Дали потпишаниот ИС сертификат е поголем од 5 KB?

Не може да увезете потпишан ИС сертификат поголем од 5 KB.

Дали лозинката за увезување на сертификатот е точна?

Ако сте ја заборавиле лозинката, не може да го увезете сертификатот.

Поврзани информации

➡ „Увезување на ИС потпишан сертификат“ на страница 66

Не може да го ажурирате самопотпишаниот сертификат

Дали сте го внеле Common Name?

Мора да го внесете **Common Name**.

Дали сте внеле несоодветни знаци во Common Name? На пример, јапонскиот не е поддржан.

Внесете од 1 до 128 знака од IPv4, IPv6, име на главен компјутер или FQDN формат во ASCII (0x20–0x7E).

Дали има запирка или празно место во Common Name?

Ако има запирка, **Common Name** е одделено од таа точка. Ако има само празно место пред или по запирката, настанува грешка.

Поврзани информации

➡ „Ажурирање на самопотпишан сертификат“ на страница 68

Не може да креирате CSR

Дали сте го внеле Common Name?

Мора да го внесете **Common Name**.

Дали сте внеле несоодветни знаци во Common Name, Organization, Organizational Unit, Locality, State/Province? На пример, јапонскиот не е поддржан.

Внесете знаци од IPv4, IPv6, име на главен компјутер или FQDN формат во ASCII (0x20–0x7E).

Дали има запирка или празно место во Common Name?

Ако има запирка, **Common Name** е одделено од таа точка. Ако има само празно место пред или по запирката, настанува грешка.

Поврзани информации

➡ „Добивање на ИС потпишан сертификат“ на страница 64

Се прикажува предупредување во врска со дигитален сертификат

Пораки	Причина/Што да направите
Enter a Server Certificate.	**Причина:** Не сте избрале датотека за увезување. **Што да направите:** Изберете датотека и кликнете на **Import**.
CA Certificate 1 is not entered.	**Причина:** ИС сертификат 1 не е внесен и внесен е само ИС сертификат 2. **Што да направите:** Првин внесете го ИС сертификат 1.
Invalid value below.	**Причина:** Има несоодветни знаци во патеката на датотеката и/или лозинката. **Што да направите:** Погрижете се знаците да бидат внесени правилно за ставката.
Invalid date and time.	**Причина:** Датумот и времето на скенерот не се поставени. **Што да направите:** Поставете ги датумот и времето со користење на Web Config или EpsonNet Config.
Invalid password.	**Причина:** Одредената лозинка за ИС сертификатот и внесената лозинка не се совпаѓаат. **Што да направите:** Внесете ја точната лозинка.

Напредни безбедносни поставки за претпријатија

Пораки	Причина/Што да направите
Invalid file.	**Причина:** Не внесувате датотека за сертификат во X509 формат. **Што да направите:** Осигурете се дека сте го избрале точниот сертификат од проверен издавач на сертификати.
	Причина: Датотеката којашто сте ја внеле е премногу долга. Максималната големина на датотеката е 5 KB. **Што да направите:** Ако ја изберете точната датотека, сертификатот може да биде корумпиран или произведен.
	Причина: Синџирот којшто се содржи во сертификатот е неважечки. **Што да направите:** За повеќе информации за сертификатот, погледнете ја интернет страницата за издавачот на сертификати.
Cannot use the Server Certificates that include more than three CA certificates.	**Причина:** Датотеката на сертификатот во PKCS#12 формат содржи повеќе од 3 ИС сертификати. **Што да направите:** Увезете ги сите сертификати конвертирајќи ги од PKCS#12 формат во PEM формат или увезете ја датотеката на сертификатот во PKCS#12 формат којашто содржи до 2 ИС сертификати.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Причина:** ИС сертификатот е застерен. **Што да направите:** ❏ Ако сертификатот е застарен, добијте го и увезете го новиот сертификат. ❏ Ако сертификатот е застарен, погрижете се датумот и времето на скенерот да бидат поставени правилно.
Private key is required.	**Причина:** Нема спарен приватен клуч со сертификат. **Што да направите:** ❏ Ако сертификатот е во PEM/DER формат и е добиен од CSR со користење на компјутер, назначете ја датотеката за приватен клуч. ❏ Ако сертификатот е во PKCS#12 формат и е добиен од CSR со користење на компјутер, креирајте датотека којашто содржи приватен клуч.
	Причина: Повторно сте го увезле PEM/DER сертификатот добиен од CSR со користење на Web Config. **Што да направите:** Ако сертификатот е во PEM/DER формат и е добиен од CSR со користење на Web Config, може да го увезете само еднаш.

Пораки	Причина/Што да направите
Setup failed.	**Причина:** Не може да ја завршите конфигурацијата затоа што комуникацијата помеѓу скенерот и компјутерот е неуспешна или датотеката не може да биде прочитани поради одредени грешки. **Што да направите:** Откако ќе ја проверите одредената датотека и комуникацијата, повторно увезете ја датотеката.

Поврзани информации

➡ „Во врска со дигитална сертификација“ на страница 63

Сте го избришале ИС потпишаниот сертификат по грешка

Има ли резервна датотека за сертификатот?

Ако имате резервна датотека, повторно внесете го сертификатот.

Ако добиете сертификат со користење на CSR креиран од Web Config, не може повторно да го внесете избришаниот сертификат. Креирајте CSR и добијте нов сертификат.

Поврзани информации

➡ „Бришење на ИС потпишан сертификат“ на страница 68

➡ „Увезување на ИС потпишан сертификат“ на страница 66