EPSON
EXCEED YOUR VISION

Посібник адміністратора

NPD5668-00 UK

Зміст

Додаток

Розширені параметри безпеки для підприємства

Авторські права

Торгові марки

- ❏ EPSON® — зареєстрована торгова марка, а EPSON EXCEED YOUR VISION або EXCEED YOUR VISION — торгові марки корпорації 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.
- ❏ Загальне зауваження: інші назви продуктів, використані тут, призначені лише для ідентифікації і можуть бути торговими марками відповідних власників. Компанія Epson відмовляється від жодного та всіх прав на ці торгові марки.

Про цей посібник

Символи та позначення

> ***Застереження.***
> *Інструкції, яких необхідно дотримуватися, щоб уникнути травм.*

> ***Важливо***
> *Інструкції, яких необхідно дотримуватися, щоб уникнути пошкодження обладнання.*

Примітка.
Інструкції, що містять корисні поради та обмеження щодо експлуатації сканера.

Пов'язані відомості

➡ Натисніть цю піктограму, щоб отримати додаткову інформацію.

Описи, використані в цьому посібнику

❏ Знімки екранів драйвера сканера та Epson Scan 2 (драйвера сканера) наведені з Windows 10 або OS X El Capitan. Зміст, що відображається на екранах, може різнитись в залежності від моделі та ситуації.

❏ Ілюстрації, використані в цьому посібнику, наведені тільки для прикладу. Хоча в залежності від моделі можуть спостерігатися певні відмінності, спосіб експлуатації буде той самий.

❏ Деякі пункти меню на РК-екрані відрізняються в залежності від моделі й налаштувань.

Позначення операційної системи

Windows

У цьому посібнику «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» та «Windows Server 2003» позначають наведені нижче операційні системи. Крім того термін «Windows» використовується для позначення всіх версій.

❏ Операційні система Microsoft® Windows® 10

❏ Операційні система Microsoft® Windows® 8.1

❏ Операційні система Microsoft® Windows® 8

❏ Операційні система Microsoft® Windows® 7

❏ Операційні система Microsoft® Windows Vista®

❏ Операційні система Microsoft® Windows® XP

❏ Операційні система Microsoft® Windows® XP Professional x64 Edition

Про цей посібник

- ❏ Операційні система Microsoft® Windows Server® 2016
- ❏ Операційні система Microsoft® Windows Server® 2012 R2
- ❏ Операційні система Microsoft® Windows Server® 2012
- ❏ Операційні система Microsoft® Windows Server® 2008 R2
- ❏ Операційні система Microsoft® Windows Server® 2008
- ❏ Операційні система Microsoft® Windows Server® 2003 R2
- ❏ Операційні система Microsoft® Windows Server® 2003

Mac OS

У цьому посібнику термін «Mac OS» використовується для позначення «macOS Sierra», «OS X El Capitan», «OS X Yosemite», «OS X Mavericks», «OS X Mountain Lion», «Mac OS X v10.7.x» і «Mac OS X v10.6.8».

Вступ

Компонент посібника

Цей посібник створено для адміністратора, який відповідає за підключення принтера або сканера до мережі, і містить інформацію про те, як внести налаштування для використання цих функцій.

Див. *Посібник користувача* для інформації про використання функції.

Підготовка

Пояснюються завдання адміністратора, як налаштовувати пристрої та керування програмним забезпеченням.

Підключення

Пояснює, як підключати пристрій до мережі або телефонної лінії. Крім того, тут описано мережеве середовище, наприклад використання порту для пристрою, DNS, і надано інформацію про проксі-сервер.

Налаштування функції

Наведено опис налаштувань для кожної функції пристрою.

Базові налаштування безпеки

Описує налаштування для кожної функції, наприклад, друку, сканування та факсу.

Налаштування роботи та керування

Описує операції після початку користування пристроєм, такі як перевірка інформації та обслуговування.

Вирішення проблем

Описує ініціалізацію налаштувань та вирішення проблем із мережею.

Розширені параметри безпеки для підприємства

Пояснюється спосіб налаштування для покращення безпеки пристрою, наприклад використання сертифікату CA, зв'язок SSL/TLS та фільтрування за IPsec/IP.

У залежності від моделі деякі функції в цьому розділі можуть не підтримуватися.

Визначення термінів, що зустрічаються в цьому посібнику

У цьому посібнику використовуються вказані нижче терміни.

Адміністратор

Відповідальна особа за встановлення та налаштування пристрою або мережі в офісі або організації. У малих організаціях ця людина може також бути відповідальним адміністратором за пристрої та мережу. У

великих організаціях адміністратори повинні мати права керування мережею або пристроями у своїй робочій групі або підрозділі, тоді як адміністратори мережі відповідають за налаштування зв'язку за межами організації, наприклад в інтернеті.

Адміністратор мережі

Особа, відповідальна за керування підключенням до мережі. Працівник, який налаштовує маршрутизатор, проксі-сервер, сервер DNS та сервер електронної пошти для контролю зв'язку через інтернет або мережу.

Користувач

Особа, яка використовує пристрої, такі як принтери та сканери.

Web Config(веб-сторінка пристрою)

Веб-сервер, який вбудований у пристрій. Він називається Web Config. У ньому можна перевірити та змінити статус пристрою за допомогою браузера.

Інструмент

Загальний термін для програмного забезпечення, за допомогою якого можна встановлювати або керувати пристроєм, наприклад, Epson Device Admin, EpsonNet Config, EpsonNet SetupManager тощо.

Push scan

Загальний термін для сканування з панелі керування пристрою.

ASCII (стандартний американський код для обміну інформацією)

Один із стандартних кодів символів. Визначено 128 символів, зокрема літери алфавіту (a – z, A – Z), арабські цифри (0 – 9), символи, пробіли та контрольні символи. Коли в цьому посібнику зазначено «ASCII», то термін вказує на 0x20 – 0x7E (шістнадцяткове число), що вказане нижче і не включає контрольні символи.

SP*	!	"	#	$	%	&	‘	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* Символ пробілу.

Unicode (UTF-8)

Код міжнародного стандарту, що охоплює основні мови світу. Коли у цьому посібнику згадується термін «UTF-8», він означає символи кодування формату UTF-8.

Підготовка

У цьому розділі пояснено роль адміністратора та підготовку перед налаштуванням.

Послідовність дій налаштування сканера та керування ним

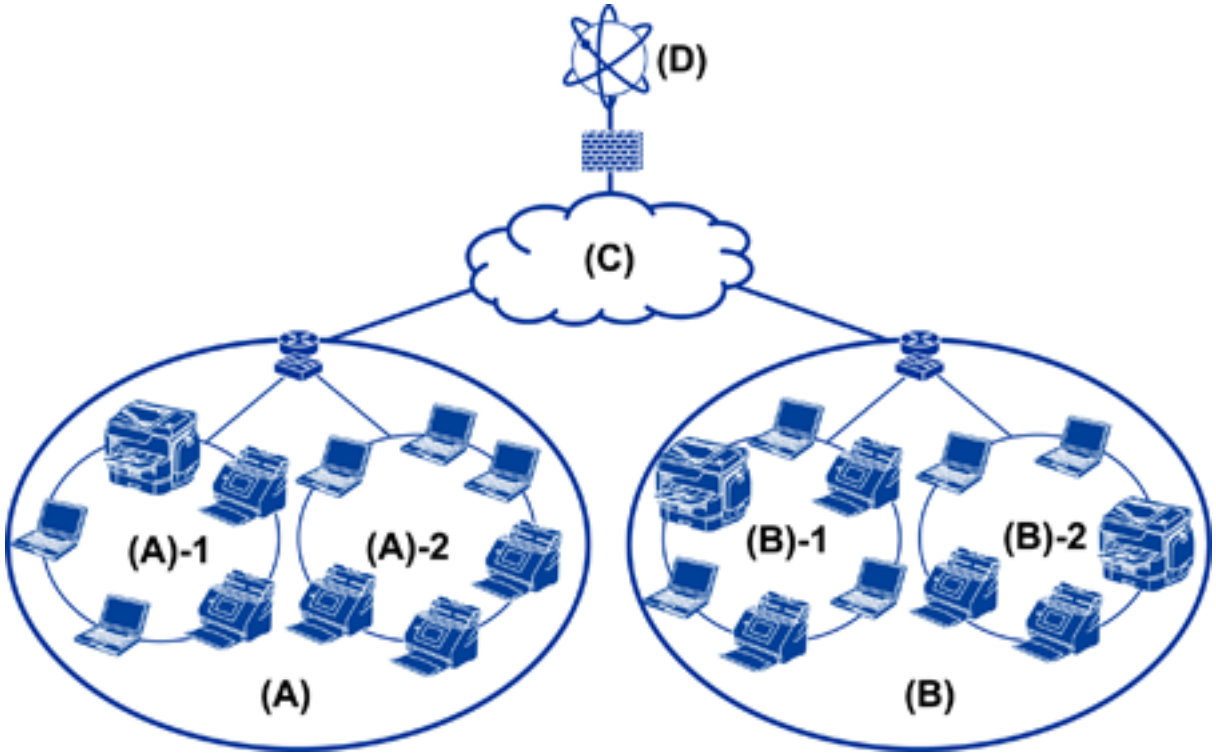
Адміністратор вносить параметри підключення до мережі, робить початкові налаштування та обслуговування сканера, щоб вони були доступними для користувачів.

1. Підготовка
   - ❏ Збір інформації про налаштування мережі
   - ❏ Рішення щодо способу підключення
2. Підключається
   - ❏ Підключення до мережі з панелі керування сканера
3. Налаштування функцій
   - ❏ Налаштування драйвера сканера
   - ❏ Інші розширені налаштування
4. Налаштування безпеки
   - ❏ Налаштування адміністратора
   - ❏ SSL/TLS
   - ❏ Керування протоколом
   - ❏ Розширені параметри безпеки (опція)
5. Робота й керування
   - ❏ Перевірка стану пристрою
   - ❏ Робота у разі виникнення подій
   - ❏ Резервне копіювання налаштувань пристрою

Пов'язані відомості

➡ «Підготовка» на сторінці 10
➡ «Підключення» на сторінці 15
➡ «Налаштування функції» на сторінці 22
➡ «Базові налаштування безпеки» на сторінці 32
➡ «Налаштування роботи та керування» на сторінці 40

Приклад мережевого середовища



(A): Office 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Office 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Представлення прикладу налаштування з'єднання для сканера

В основному є два типи з'єднання залежно від способу використання сканера. Обидва типи підключають сканер до мережі з комп'ютером через вузол.

❏ З'єднання сервер-клієнт (сканер, що використовує сервер Windows, керування завданнями)

❏ Одноранговe з'єднання (пряме підключення з комп'ютера клієнта)

Пов'язані відомості

➡ «З'єднання сервер/клієнт» на сторінці 12

➡ «Налаштування одноранговoго з'єднання» на сторінці 12

З'єднання сервер/клієнт

Централізуйте керування сканером і завданнями за допомогою програми Document Capture Pro Server, установленої на сервері. Вона найбільше підходить для роботи з використанням кількох сканерів для сканування великої кількості документів у певному форматі.

Пов'язані відомості

➡ «Визначення термінів, що зустрічаються в цьому посібнику» на сторінці 8

Налаштування одноранговогo з'єднання

Виконайте налаштування на окремому сканері з установленим на клієнтському комп'ютері драйвером сканера, наприклад Epson Scan 2. Установлення програми Document Capture Pro (Document Capture) на клієнтському комп'ютері дає змогу керувати завданнями на окремих клієнтських комп'ютерах, до яких підключено сканер.

Пов'язані відомості

➡ «Визначення термінів, що зустрічаються в цьому посібнику» на сторінці 8

Підготовка підключення до мережі

Збір інформації про налаштування підключення

Для підключення до мережі потрібно мати IP-адресу, адресу шлюзу тощо. Перевірте спочатку вказані нижче пункти.

Розділи	Налаштування	Примітка
Спосіб підключення пристрою	❏ Ethernet	Використовуйте кабель STP (екранована вита пара) категорії вище 5e для підключення до Ethernet.
Інформація про підключення до локальної мережі	❏ IP-адреса ❏ Маска підмережі ❏ Стандартний шлюз	Якщо ви автоматично налаштовуєте IP-адресу за допомогою функції DHCP маршрутизатора, то це непотрібно.
Інформація про сервер DNS	❏ IP-адреса для головного сервера DNS ❏ IP-адреса для допоміжного сервера DNS	Якщо використовувати статичну IP-адресу як IP-адресу, налаштуйте сервер DNS. Налаштуйте у разі автоматичного присвоєння за допомогою функції DHCP або коли сервер DNS не можна призначити автоматично.
Інформація про проксі-сервер	❏ Ім'я проксі-сервера ❏ Номер порту	Налаштуйте у разі використання проксі-сервера для з'єднання з інтернетом та в разі використання служби Epson Connect чи функції автоматичного оновлення мікропрограми.

Технічні характеристики сканера

Технічні характеристики зі стандартами та режимами підключення, які підтримує сканер, див у *Посібник користувача*.

Використання номера порту

Див. «Додаток», щоб дізнатися номер порту сканера.

Пов'язані відомості

➡ «Використання порту для сканера» на сторінці 60

Типи призначення IP-адреси

Існує два типи призначення IP-адрес сканерам.

Статична IP-адреса:

Призначте наперед визначену унікальну IP-адресу сканеру.

IP-адреса не змінюється, навіть якщо вимкнути сканер або маршрутизатор, тому можна керувати пристроєм за IP-адресою.

Цей тип підходить до мережі з багатьма сканерами, наприклад, у великому офісі або школі.

Автоматичне призначення функцією DHCP:

Правильна IP-адреса автоматично призначається, коли встановлюється з'єднання між сканером та маршрутизатором, який підтримує функцію DHCP.

Якщо змінювати IP-адресу для певного пристрою незручно, зарезервуйте IP-адресу заздалегідь та призначте її.

Сервер DNS та проксі-сервер

Якщо ви використовуєте службу підключення до інтернету, налаштуйте сервер DNS. Якщо його не налаштувати, потрібно буде вказувати IP-адресу для доступу, оскільки ідентифікація імені може бути невдалою.

Проксі-сервер розміщується на шлюзі між мережею та інтернетом та підключається до комп'ютера, сканера та інтернету (протилежний сервер) від імені кожного з них. Протилежний сервер підключається тільки до проксі-сервера. Тому така інформація про сканер, як IP-адреса та номер порту, не зчитується, оскільки очікується підвищений захист.

Цю функцію фільтрування неможливо використовувати для заборони доступу до певних URL-адрес, оскільки проксі-сервер здатен перевірити вміст зв'язку.

Спосіб налаштування мережевого з'єднання

Для налаштування з'єднання для IP-адреси сканера, маски підмережі та шлюзу за замовчуванням виконайте вказані нижче дії.

Підготовка

Використання панелі керування:

Налаштуйте параметри за допомогою панелі керування для кожного сканера. Підключіть до мережі після налаштування параметрів з'єднання сканера.

Використання інсталятора:

У разі використання інсталятора мережа сканера та клієнтського комп'ютера встановлюється автоматично. Це налаштування доступне через вказані нижче інструкції до інсталятора, навіть якщо у вас немає достатніх знань мережі.

Використання інструмента:

Використовуйте інструмент із комп'ютера адміністратора. Ви можете знайти сканер та встановити його або створити файл SYLK для пакетного налаштування сканерів. Ви можете встановити багато сканерів, але їх потрібно буде фізично підключити через кабель Ethernet перед встановленням. Тому рекомендується створити мережу Ethernet для встановлення.

Пов'язані відомості

➡ «Підключення до мережі з панелі керування» на сторінці 15

➡ «Підключення мережі за допомогою встановлювача» на сторінці 19

➡ «Призначення IP-адреси за допомогою EpsonNet Config» на сторінці 56

Підключення

У цьому розділі подано опис середовища або процедури для підключення сканера до мережі.

Підключення до мережі

Підключення до мережі з панелі керування

Підключіть сканер до мережі за допомогою панелі керування сканера.

Щоб отримати докладнішу інформацію про панель керування сканера, див. *Посібник користувача*.

Призначення IP-адреси

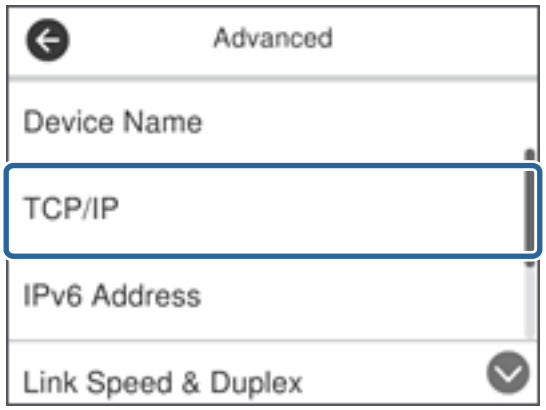
Налаштуйте основні елементи, зокрема IP-адреса, Маска підмережі та Шлюз за замовчанням.

1. Увімкніть сканер.
2. Прокрутіть екран вліво на панелі керування сканера, а тоді натисніть **Налаш.**.

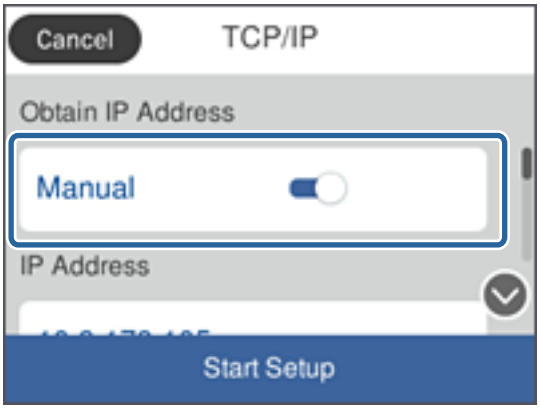
3. Натисніть **Налаштування мережі** > **Змінити налаштування**.

   Якщо елемент не відображається, прогорніть екран вгору, щоб побачити його.

4. Натисніть **TCP/IP**.

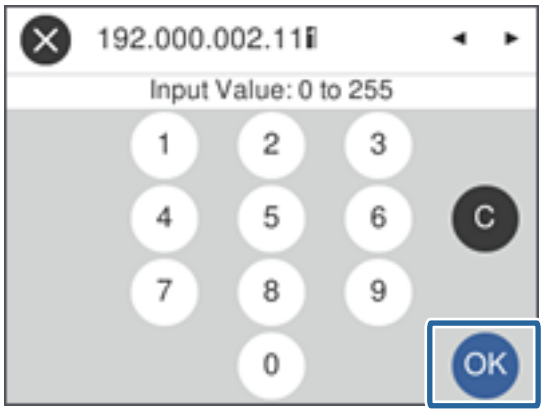


5. Виберіть **Вручну** для **Отримати IP-адресу**.



Примітка.
Коли ви автоматично налаштовуєте IP-адресу за допомогою функції DHCP маршрутизатора, виберіть ***Авто****. У такому разі* ***IP-адреса****,* ***Маска підмережі*** *та* ***Шлюз за замовчанням*** *у кроках 6 і 7 встановлюються автоматично, тому перейдіть до кроку 8.*

6. Натисніть поле **IP-адреса**, уведіть IP-адресу за допомогою клавіатури, що відобразиться на екрані, а тоді натисніть **OK**.



Підтвердьте значення, що вказане на екрані.

7. Налаштуйте **Маска підмережі** та **Шлюз за замовчанням**.

   Підтвердьте значення, що вказане на екрані.

   Примітка.
   *Якщо комбінація IP-адреса, Маска підмережі та Шлюз за замовчанням неправильна, то функція **Запуск налаштув.** неактивна і не може продовжити налаштування. Підтвердьте, що у внесеній інформації немає помилки.*

8. Натисніть поле **Первинний DNS** для **DNS-сервер**, уведіть IP-адресу для головного DNS-сервера за допомогою клавіатури, що відобразиться на екрані, а тоді натисніть **OK**.

   Підтвердьте значення, що вказане на екрані.

   Примітка.
   *Коли вибрати **Авто** для параметрів призначення IP-адреси, можна вибрати налаштування DNS-сервера з меню **Вручну** або **Авто**. Якщо ви не можете отримати адресу DNS-сервера автоматично, виберіть **Вручну** та уведіть адресу DNS-сервера. Тоді безпосередньо уведіть допоміжну адресу DNS-сервера. Якщо вибрано параметр **Авто**, перейдіть до кроку 10.*

9. Натисніть поле **Вторинний DNS-сервер**, уведіть IP-адресу для допоміжного DNS-сервера за допомогою клавіатури, що відобразиться на екрані, а тоді натисніть **OK**.

   Підтвердьте значення, що вказане на екрані.

10. Натисніть **Запуск налаштув.**.

11. Натисніть **Закрити** на екрані підтвердження.

    Екран автоматично закриється після певного часу, якщо ви не натискаєте **Закрити**.

Підключення до Ethernet

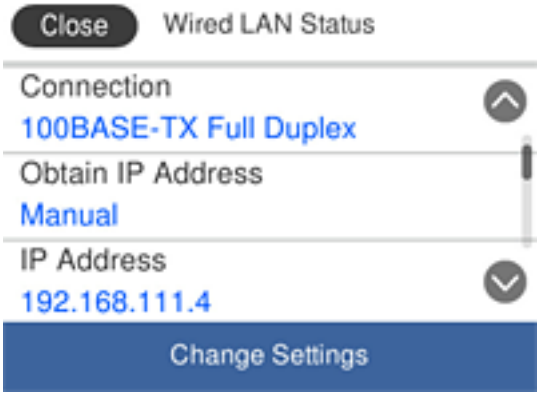
Підключіть сканер до мережі за допомогою кабелю Ethernet, а тоді перевірте з'єднання.

1. Підключіть сканер до вузла (перемикач L2) за допомогою кабелю Ethernet.

   Піктограма на головному екрані зміниться на  .

2. Натисніть  на головному екрані.

3. Прокрутіть екран угору, а тоді переконайтесь, що статус з'єднання та IP-адреса правильні.



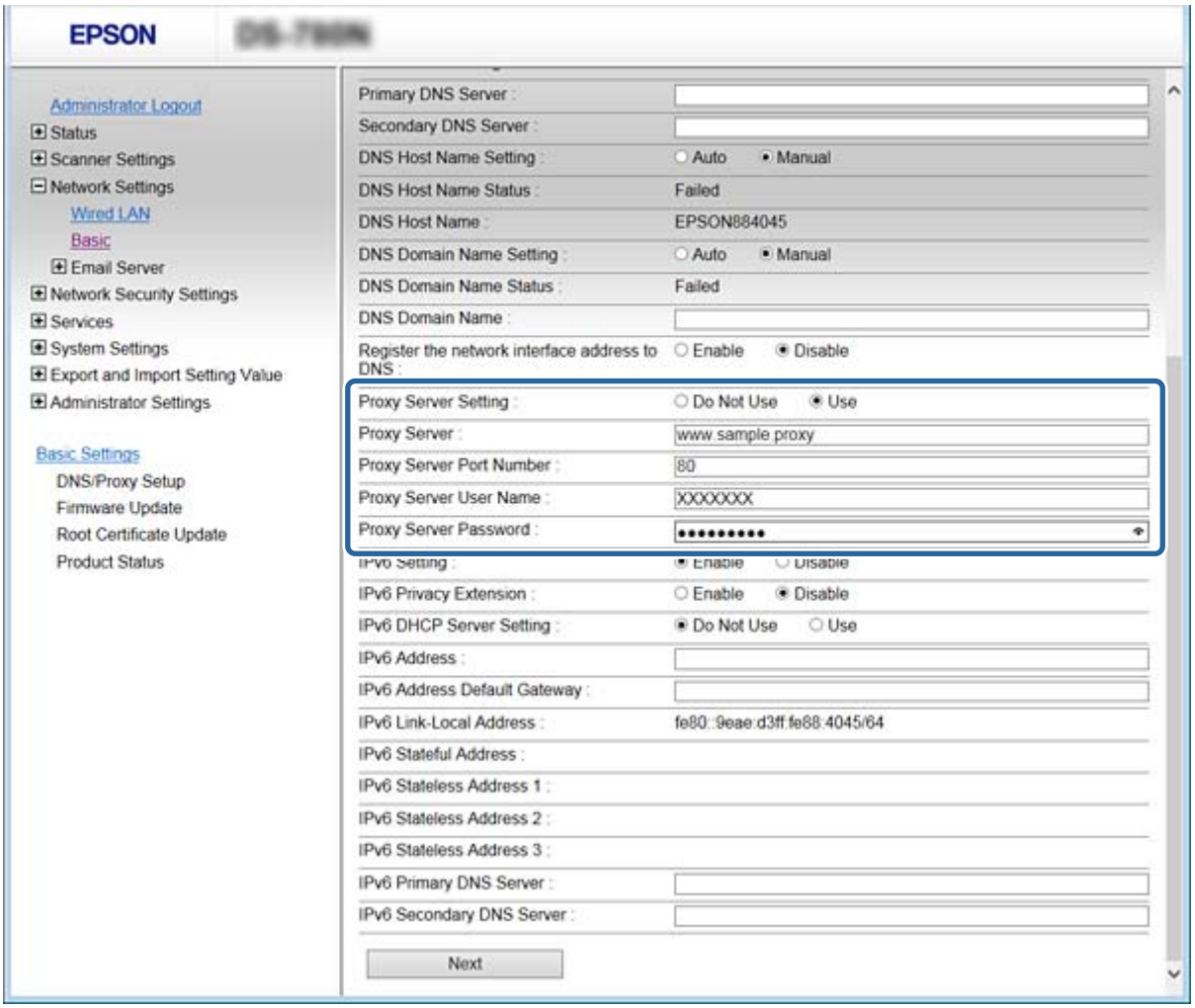
Налаштування проксі-сервера

Проксі-сервер не можна налаштувати за допомогою панелі. Виконайте налаштування за допомогою Web Config.

1. Відкрийте Web Config та виберіть **Network Settings** > **Basic**.
2. Виберіть **Use** на екрані **Proxy Server Setting**.
3. Укажіть проксі-сервер в адресі IPv4 або форматі FQDN на екрані **Проксі-сервер**, а тоді введіть номер порту в полі **Proxy Server Port Number**.

   Для проксі-серверів, які потребують автентифікації, введіть ім'я користувача та пароль для автентифікації на проксі-сервері.

4. Натисніть кнопку **Next**.



5. Підтвердіть налаштування та натисніть **Налаштування**.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Підключення мережі за допомогою встановлювача

Радимо використовувати встановлювач для підключення сканера до комп'ютера. Можна запустити встановлювач кількома способами, що вказані нижче.

❏ Налаштування через веб-сайт

Увійдіть на вказаний нижче веб-сайт, а тоді вкажіть номер пристрою. Перейдіть до **Установка**, а тоді запустіть налаштування.

http://epson.sn

❏ Налаштування за допомогою диску з програмним забезпеченням (тільки для моделей, що постачаються з диском з програмним забезпеченням, та користувачів, які мають комп'ютери з дисководами).

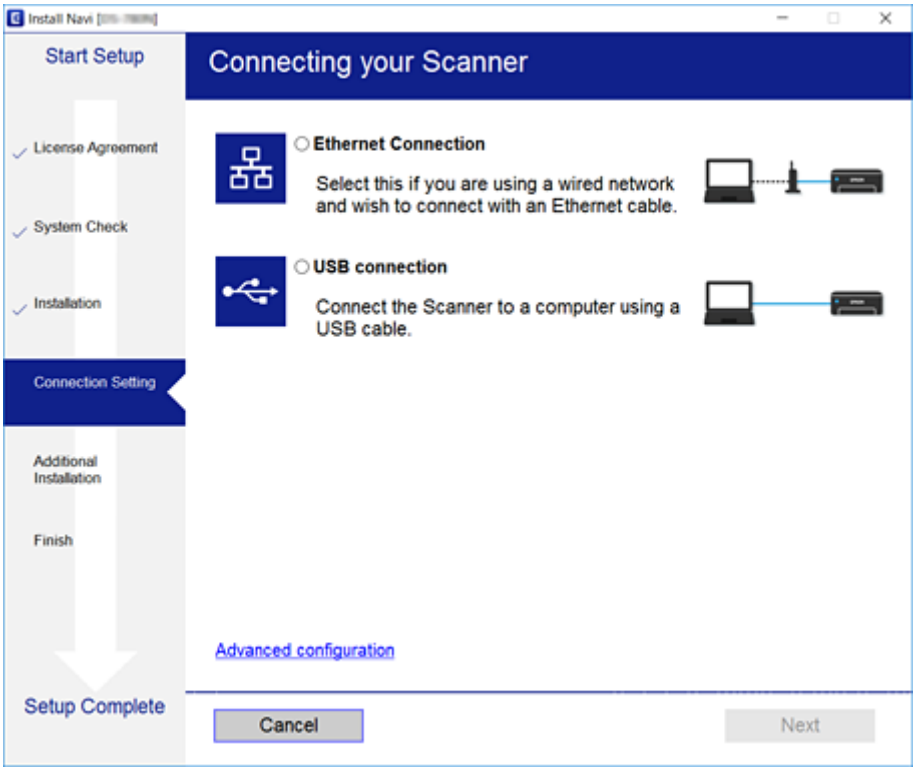
Вставте диск із програмним забезпеченням у комп'ютер, а тоді дотримуйтеся вказівок на екрані.

Вибір способу підключення

Дотримуйтеся вказівок на екрані, доки не з'явиться вказаний нижче екран, а тоді виберіть спосіб підключення сканера до комп'ютера.

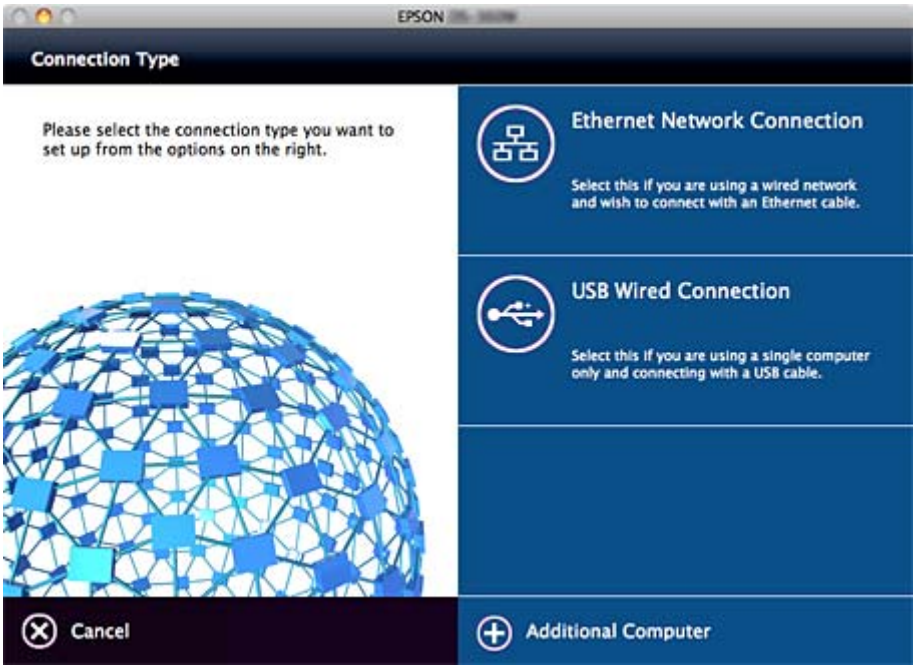
❏ Windows

Виберіть тип підключення, а потім клацніть **Далі**.



❏ Mac OS

Оберіть тип підключення.



Підключення

Дотримуйтеся вказівок на екрані. Необхідне програмне забезпечення встановлено.

Налаштування функції

У цьому розділі описано перші налаштування, які потрібно зробити для використання кожної функції пристрою.

Програмне забезпечення для налаштування

У цьому розділі описано процедуру налаштування з комп'ютера адміністратора за допомогою Web Config.

Web Config (Веб-сторінка для пристрою)

Про Web Config

Web Config — це браузерна програма для налаштування параметрів сканера.

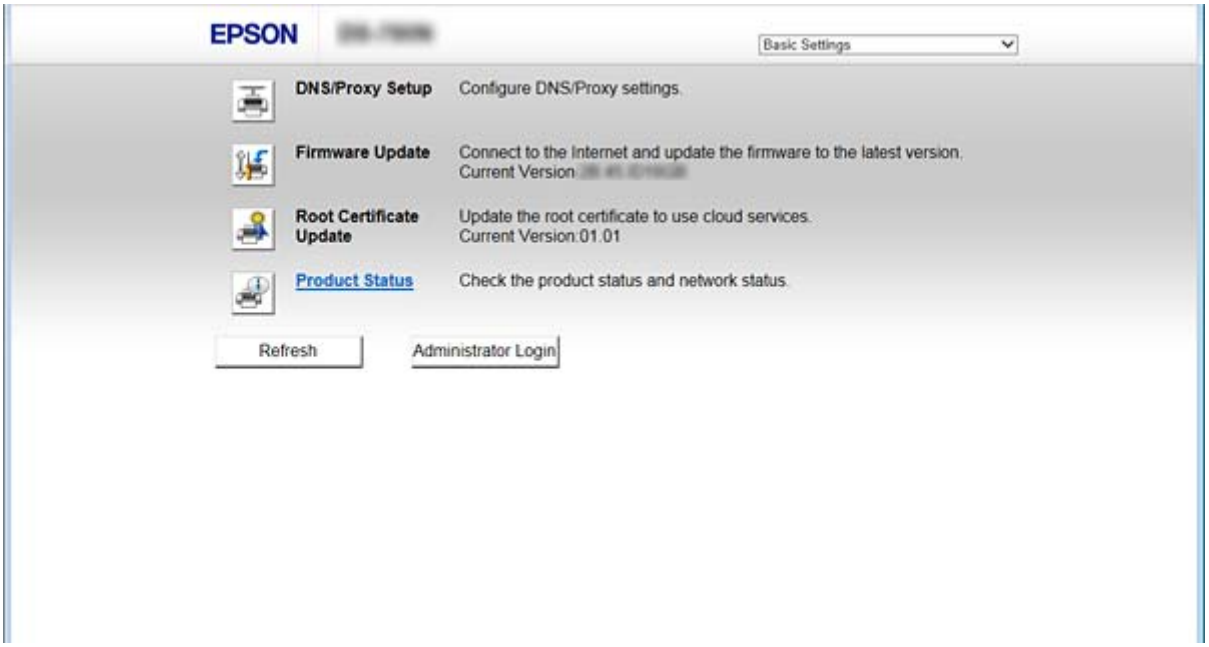
Для доступу до програми Web Config необхідно спочатку призначити сканеру IP-адресу.

Примітка.
Доступ до налаштувань можна заблокувати, встановивши для сканера пароль адміністратора.

Налаштування описані на двох сторінках, як зображено нижче.

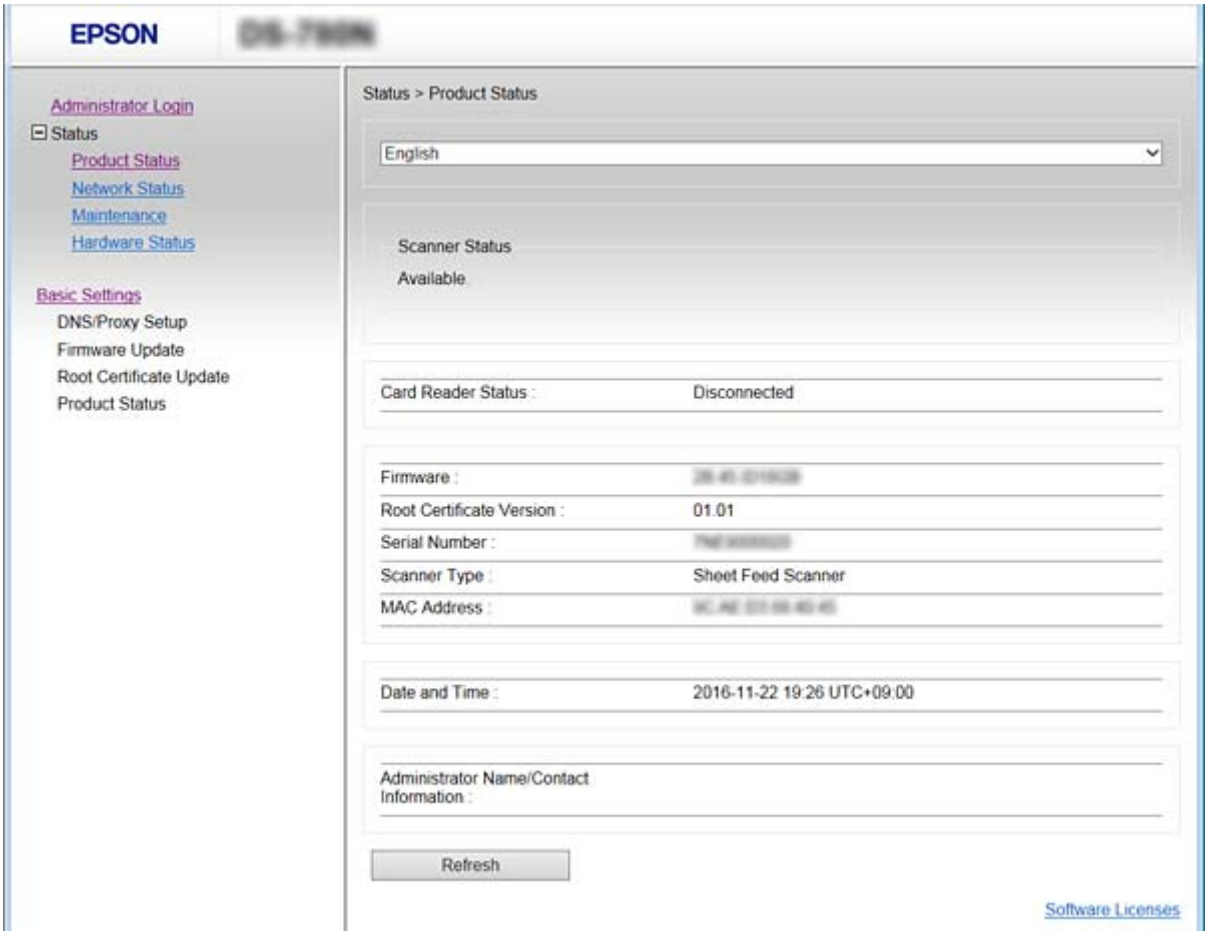
❏ **Basic Settings**

Налаштування основних параметрів сканера.



❏ **Advanced Settings**

Налаштування розширених параметрів сканера. Ця сторінка призначена в основному для адміністратора.



Доступ до налаштувань Web Config

Введіть IP-адресу сканера у веб-браузері. JavaScript має бути ввімкнено. У разі отримання доступу до налаштувань Web Config через HTTPS, у браузері з'явиться повідомлення з попередженням, оскільки використовуватиметься сертифікат із власним підписом, що зберігається у сканері.

❏ Доступ через HTTPS

IPv4: https://<IP-адреса сканера> (без < >)

IPv6: https://[IP-адреса сканера]/ (з [ ])

❏ Доступ через HTTP

IPv4: http://<IP-адреса сканера> (без < >)

IPv6: http://[IP-адреса сканера]/ (з [ ])

Примітка.

❏ *Приклади*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Якщо ім'я сканера зареєстровано на сервері DNS, можна використовувати це ім'я, а не IP-адресу сканера.*

Пов'язані відомості

➡ «Зв'язок SSL/TLS зі сканером» на сторінці 63

➡ «Про цифрову сертифікацію» на сторінці 63

Використання функцій сканування

Залежно від способу використання сканера встановіть зазначене нижче програмне забезпечення та за допомогою нього виконайте налаштування.

❏ **Сканування з комп'ютера**

❏ Підтвердіть чинність служби мережевого сканування за допомогою Web Config (служба чинна на момент заводської доставки).

❏ Установіть програму Epson Scan 2 на своєму комп'ютері та встановіть IP-адресу

❏ Під час сканування з використанням завдань установіть програму Document Capture Pro (Document Capture) та виконайте налаштування завдань.

❏ **Сканування з панелі керування**

❏ У разі використання програми Document Capture Pro або Document Capture Pro Server:

Установіть програму Document Capture Pro або Document Capture Pro Server

Налаштування DCP (режим сервера, режим клієнта).

❏ У разі використання протоколу WSD:

Підтвердіть чинність протоколу WSD у Web Config або на панелі керування (протокол чинний на момент заводської доставки).

Додаткові налаштування пристрою (комп'ютер Windows).

Сканування з комп'ютера

Установіть програмне забезпечення та переконайтесь, що службу мережевого сканування ввімкнено для сканування через мережу з комп'ютера.

Пов'язані відомості

➡ «Програмне забезпечення, яке необхідно встановити» на сторінці 25

➡ «Увімкнення мережевого сканування» на сторінці 25

Програмне забезпечення, яке необхідно встановити

❏ Epson Scan 2

Це драйвер сканера. Якщо потрібно використовувати пристрій із комп'ютера, встановіть драйвер на кожному клієнтському комп'ютері. Якщо встановлено Document Capture Pro/Document Capture можна здійснювати операції, що призначені кнопкам пристрою.

За допомогою EpsonNet SetupManager драйвери принтера також можуть розповсюджуватися разом у пакетах.

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

Установіть на клієнтському комп'ютері. За допомогою програми Document Capture Pro/Document Capture, встановленої в мережі з комп'ютера та пенлі керування сканера, можна викликати та виконувати завдання, зареєстровані на комп'ютері.

Також можна виконувати сканування з комп'ютера через мережу. Для сканування потрібен Epson Scan 2.

Пов'язані відомості

➡ «EpsonNet SetupManager» на сторінці 56

Установлення IP-адресою сканера Epson Scan 2

Укажіть IP-адресу сканера, щоб сканер можна було використовувати в мережі.

1. Запустіть службову програму **Epson Scan 2 Utility** в меню **Пуск** > **Усі програми** > **EPSON** > **Epson Scan 2**.

   Якщо вже зареєстровано інший сканер, перейдіть до кроку 2.

   Якщо сканер не зареєстровано. перейдтть до кроку 4.

2. Клацніт ▼ на екрані **Сканер**.
3. Клацніть **Настройки**.
4. Натисніть **Включити редагування**, а тоді **Додати**.
5. Виберіть назву моделі сканера на вкладці **Модель**.
6. Виберіть IP-адресу сканера, що використовуватиметься в полі **Адреса** на вкладці **Шукати мережу**.

   Клацніть  та  , щоб оновити список. Якщо не вдається знайти IP-адресу сканера, виберіть поле **Вв&ести адресу** та введіть IP-адресу.

7. Клацніть **Додати**.
8. Клацніть **OK**.

Увімкнення мережевого сканування

Можна налаштувати службу мережевого сканування, якщо ви скануєте з клієнтського комп'ютера через мережу. За замовчуванням ця функція увімкнена.

1. Відкрийте Web Config і виберіть **Services** > **Network Scan**.
2. Упевніться, що вибрано значення **Enable scanning** програми **EPSON Scan**.

   Якщо вибрано це значення, це завдання виконано. Закрийте Web Config.

   Якщо значення не вибрано, виберіть його та перейдіть до наступного кроку.
3. Клацніть **Next**.
4. Клацніть **OK**.

   Мережа повторно підключиться, і тоді параметри будуть увімкнені.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Сканування за допомогою панелі керування

Сканування зі збереженням у папці або в електронній пошті за допомогою панелі керування сканера, а також передавання результатів сканування електронною поштою, до папок тощо здійснюється за допомогою виконання завдання з комп'ютера.

Під час передавання результатів сканування налаштуйте завдання у програмі Document Capture Pro Server або Document Capture Pro.

Докладніше про параметри та налаштування завдань див у документації або довідці програми Document Capture Pro Server або Document Capture Pro.

Пов'язані відомості

➡ «Налаштування програми Document Capture Pro Server/Document Capture Pro» на сторінці 27

➡ «Налаштування для серверів і папок» на сторінці 27

Програмне забезпечення, яке необхідно встановити на комп'ютері

❏ **Document Capture Pro Server**

Це серверна версія програми Document Capture Pro. Установіть її на сервері Windows. Із сервера можна централізовано керувати кількома пристроями та завданнями. Завдання можуть виконуватися одночасно на кількох сканерах.

Використовуючи сертифіковану версію програми Document Capture Pro Server, можна керувати завданнями та історією сканування, які пов'язані з користувачами та групами.

Для отримання докладніших відомостей про програму Document Capture Pro Server зверніться до місцевого представництва компанії Epson.

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

Так само, як і сканування з комп'ютера, за допомогою панелі керування можна викликати завдання, зареєстровані на комп'ютері, і виконувати їх. Неможливо запустити завдання з комп'ютера одночасно на кількох сканерах.

Налаштування програми Document Capture Pro Server/Document Capture Pro

Виконайте налаштування для використання функції сканування з панелі керування сканера.

1. Відкрийте Web Config та виберіть **Services** > **Document Capture Pro**.
2. Виберіть **Режим роботи**.
   - ❏ Server Mode:

     Виберіть цей режим в разі використання програми Document Capture Pro Server або якщо програма Document Capture Pro використовується тільки для завдань, установлених для певного комп'ютера.
   - ❏ Client Mode:

     Установіть цей режим, якщо вибрано налаштування завдань програми Document Capture Pro (Document Capture), яку встановлено на кожному клієнтському комп'ютері в мережі, без указання комп'ютера.
3. Згідно з вибраним режимом налаштуйте зазначене нижче.
   - ❏ Server Mode:

     У полі **Server Address** укажіть сервер, на якому встановлено програму Document Capture Pro Server. Адреса може бути довжиною від 2 до 252 символів у форматі IPv4, IPv6, імені хосту або FQDN. У форматі FQDN можуть використовуватися символи стандарту US-ASCII, цифри, літери алфавіту та дефіси (крім дефісів попереду та позаду імені).
   - ❏ Client Mode:

     Укажіть значення **Group Settings** для використання групи сканерів, указаних у програмі Document Capture Pro (Document Capture).
4. Клацніть **Налаштування**.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Налаштування для серверів і папок

Програми Document Capture Pro та Document Capture Pro Server зберігають скановані дані на сервер або клієнтський комп'ютер один раз і використовують функцію передавання для виконання сканування до папки та сканування на електронну пошту.

Для передавання даних з комп'ютера, на якому встановлено Document Capture Pro, Document Capture Pro Server, на комп'ютер або у хмарну службу, необхідно мати дозвіл та відомості.

Підготуйте відомості про функцію, що використовуватиметься, спираючись на зазначене нижче.

Налаштування для цих функцій можна виконати за допомогою програми Document Capture Pro або Document Capture Pro Server. Докладніше про налаштування див у документації або довідці програми Document Capture Pro Server чи Document Capture Pro.

Налаштування функції

Ім'я	Налаштування	Вимоги
Сканування в мережеву папку (SMB)	Створення і налаштування спільного використання папки для зберігання	Обліковий запис адміністратора на комп'ютері, який створює папку для зберігання.
	Цільова папка для сканування в мережеву папку (SMB)	Ім'я та пароль користувача для входу в комп'ютер, який містить папку для зберігання, та права для оновлення папки для зберігання.
Сканування в мережеву папку (FTP)	Налаштування для входу на сервер FTP	Інформація для входу на сервер FTP та право новлення папки для зберігання.
Сканування в електронну пошту	Налаштування для сервера електронної пошти	Інформація про налаштування для сервера електронної пошти
Сканування у Document Capture Pro (у разі використання Document Capture Pro Server)	Виконання налаштувань для входу у хмарні служби	Середовище підключення до інтернету Реєстрація облікового запису для хмарних служб

Сканування за допомогою протоколу WSD (тільки для ОС Windows)

Якщо на комп'ютері використовується ОС Windows Vista або новішої версії, можна скористатися скануванням WSD.

Якщо протокол WSD можна використовувати, на панелі керування сканера відображатиметься меню **ПК (WSD)**.

1. Відкрийте Web Config та виберіть **Services** > **Protocol**.
2. Переконайтесь, що встановлено прапорець **Enable WSD** у налаштуваннях **WSD Settings**.

   Якщо прапорець установлено, завдання виконано та можна закрити Web Config.

   Якщо прапорець не встановлено, встановіть його та перейдіть до наступного кроку.
3. Натисніть кнопку **Next**.
4. Підтвердіть налаштування та натисніть **Налаштування**.

Налаштування системи

Виконання системних налаштувань з панелі керування

Налаштування яскравості екрана

Налаштуйте яскравість РК-екрана.

1. Натисніть **Налаш.** на головному екрані.

2. Натисніть **Звичайні налаштув.** > **Яскр. РК-дис.**.
3. Натисніть  або  для налаштування яскравості.

   Яскравість можна налаштувати в діапазоні від 1 до 9.
4. Натисніть **ОК**.

Налаштування звуку

Налаштуйте звуковий сигнал роботи панелі керування та звуковий сигнал помилки.

1. Натисніть **Налаш.** на головному екрані.
2. Натисніть **Звичайні налаштув.** > **Звук**.
3. Виконайте зазначені нижче налаштування у разі необхідності.
   - ❏ Звуковий сигнал

     Установіть гучність звукового сигналу панелі керування.
   - ❏ Звуковий сигнал помилки

     Установіть гучність звукового сигналу помилки.
4. Натисніть **ОК**.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Виявлення подвійної подачі оригіналу

Визначте налаштування функції, яка виявлятиме подвійну подачу документа для сканування та зупинятиме сканування в разі подачі кількох сторінок.

Для сканування оригіналів, які мають подаватися кількома сторінками, наприклад конвертів або паперу з наклейками, вимкніть функцію.

Примітка.
Функцію можна також налаштувати у Web Config або Epson Scan 2.

1. Натисніть **Налаш.** на головному екрані.
2. Натисніть **Додаткові Налаштування сканера** > **УЗ виявл. завантаж. кількох листів**.
3. Натисніть **УЗ виявл. завантаж. кількох листів** для ввімкнення або вимкнення функції.
4. Натисніть **Закрити**.

Налаштування режиму низької швидкості

Налаштуйте сканування на низькій швидкості, щоб уникнути випадків зминання паперу під час сканування тонких документів, наприклад бланків.

1. Натисніть **Налаш.** на головному екрані.
2. Натисніть **Додаткові Налаштування сканера** > **Повільна швидкість**.
3. Натисніть **Повільна швидкість** для ввімкнення або вимкнення функції.
4. Натисніть **Закрити**.

Виконання системних налаштувань за допомогою Web Config

Налаштування енергозбереження за період без використання

Виконайте налаштування енергозбереження для періоду неактивності сканера. Встановіть час у залежності від середовища використання.

Примітка.
Налаштування енергозбереження також можна виконати на панелі керування сканера.

1. Відкрийте Web Config та виберіть **System Settings** > **Power Saving**.
2. Уведіть час для **Sleep Timer**, щоб вмикати режим збереження енергії в разі невикористання.

   Можна встановити до 240 хвилин з кроком в одну хвилину.
3. Виберіть час вимикання для **Power Off Timer**.
4. Клацніть **OK**.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Налаштування панелі керування

Налаштування для панелі керування сканера. Можна внести перелічені нижче налаштування.

1. Відкрийте Web Config та виберіть **System Settings** > **Control Panel**.
2. Зробіть вказані нижче налаштування у разі необхідності.
   - ❏ Language

     Оберіть мову відображення на панелі керування.
   - ❏ Panel Lock

     Якщо вибрати **ON**, потрібен пароль адміністратора для виконання операції, яка вимагає прав адміністратора. Якщо пароль адміністратора не встановлено, блокування панелі вимкнено.

❏ Operation Timeout

Якщо вибрати **ON** та увійти як адміністратор, відбудеться автоматичний вихід і перехід на початковий екран, якщо певний час не здійснюється жодних операцій.

Можна встановити від 10 секунд до 240 хвилин з кроком в одну секунду.

3. Клацніть **OK**.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Налаштування обмеження для зовнішнього інтерфейсу

Можна обмежити USB-з'єднання з комп'ютера. Налаштуйте обмеження, щоб обмежити інше сканування, крім сканування через мережу.

1. Відкрийте Web Config та виберіть **System Settings** > **External Interface**.
2. Виберіть **Enable** або **Disable**.

   Щоб обмежити з'єднання, виберіть **Disable**.
3. Натисніть **OK**.

Синхронізація дати й часу із сервером часу

У разі використання сертифікату CA можна запобігти виникненню проблем із часом.

1. Відкрийте Web Config та виберіть **System Settings** > **Date and Time** > **Time Server**.
2. Виберіть **Use** для **Use Time Server**.
3. Уведіть адресу сервера часу **Time Server Address**.

   Можна використовувати формат IPv4, IPv6 або FQDN. Уведіть до 252 символів. Якщо це непотрібно вказувати, то залиште це місце пустим.
4. Введіть **Update Interval (min)**.

   Можна встановити до 10 800 хвилин з кроком в одну хвилину.
5. Клацніть **OK**.

   Примітка.
   Підтвердити стан з'єднання із сервером часу можна в ***Time Server Status****.*

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Базові налаштування безпеки

У цьому розділі описано базові налаштування безпеки, які не вимагають особливого середовища.

Вступ до базових функцій безпеки

Тут подано інформацію про базові функції безпеки пристроїв Epson.

Ім'я функції	Тип функції	Що налаштовувати	Чого уникати
Налаштуйте пароль адміністратора	Заблокуйте налаштування, пов'язані із системою, наприклад налаштування мережі та USB-з'єднання, щоб їх міг змінити тільки адміністратор.	Адміністратор встановлює пароль на пристрої. Конфігурація та оновлення доступні будь-де з програми Web Config, панелі керування, Epson Device Admin та EpsonNet Config.	Уникайте несанкціонованого зчитування або зміни інформації, що зберігається на пристрої, наприклад, ідентифікатор, пароль, мережеві налаштування та контакти. Крім того, слід зменшити ризики безпеки, наприклад, витікання інформації для мережевого середовища або політики безпеки.
Зв'язок за допомогою протоколів SSL/TLS	Під час отримання доступу до сервера Epson в Інтернеті з пристрою, зокрема під час установлення зв'язку з комп'ютером через браузер або оновлення мікропрограми, вміст зв'язку шифрується за допомогою протоколів SSL/TLS.	Отримайте сертифікат, підписаний ЦС, а тоді імпортуйте його на сканер.	Очищення ідентифікації пристрою за допомогою сертифікату, підписаному ЦС, запобігає маскуванню під законного користувача та несанкціонований доступ. Крім того, вміст зв'язку SSL/TLS захищений і запобігає просочуванню вмісту даних для дурку чи інформації про налаштування.
Керування протоколами	Керує протоколами, що використовуються для зв'язку між пристроями та комп'ютерами та вмикає й вимикає функції.	Протокол або служба застосовується до функцій, на які дається дозвіл або заборона окремо.	Зниження ризиків безпеки, що може статися через ненавмисне використання, шляхом обмеження користувачів від непотрібних для них функцій.

Пов'язані відомості

➡ «Про Web Config» на сторінці 22
➡ «EpsonNet Config» на сторінці 55
➡ «Epson Device Admin» на сторінці 55
➡ «Установлення пароля адміністратора» на сторінці 33
➡ «Керування протоколами» на сторінці 35

Установлення пароля адміністратора

Коли встановлено пароль адміністратора, користувачі, які не мають прав адміністратора, не зможуть змінити налаштування, що стосуються адміністрування системи. Можна встановити або змінити пароль адміністратора за допомогою Web Config, панелі керування сканера або програмного забезпечення (Epson Device Admin або EpsonNet Config). Під час використання програмного забезпечення див. документацію до нього.

Пов'язані відомості

➡ «Конфігурація паролю адміністратора з панелі керування» на сторінці 33
➡ «Конфігурація пароля адміністратора за допомогою Web Config» на сторінці 33
➡ «EpsonNet Config» на сторінці 55
➡ «Epson Device Admin» на сторінці 55

Конфігурація паролю адміністратора з панелі керування

Пароль адміністратора можна встановити на панелі керування сканера.

1. Натисніть **Налаш.** на головному екрані.
2. Натисніть **Сист. адміністрування** > **Налаштув. адміністратора**.

   Якщо елемент не відображається, прогорніть екран вгору, щоб побачити його.
3. Натисніть **Пароль адміністратора** > **Зареєструвати**.
4. Уведіть новий пароль, а тоді виберіть **ОК**.
5. Уведіть пароль ще раз, а тоді виберіть **ОК**.
6. Натисніть **ОК** на екрані підтвердження.

   Відобразиться екран з налаштуваннями адміністратора.
7. Натисніть **Налаштування блокування**, а тоді виберіть **ОК** на екрані підтвердження.

   Параметр Налаштування блокування матиме значення **Увімк**, тоді для роботи із заблокованими елементами меню, потрібно буде вводити пароль адміністратора.

Примітка.

❏ *Якщо для параметра **Налаш.** > **Звичайні налаштув.** > **Пауза в роботі** вибрано значення **Увімк**, сканер вийде з облікового запису після певного часу простою панелі керування.*

❏ *Ви можете змінити або видалити пароль адміністратора, якщо виберете **Змінити** або **Скинути** на екрані **Пароль адміністратора** та введете пароль адміністратора.*

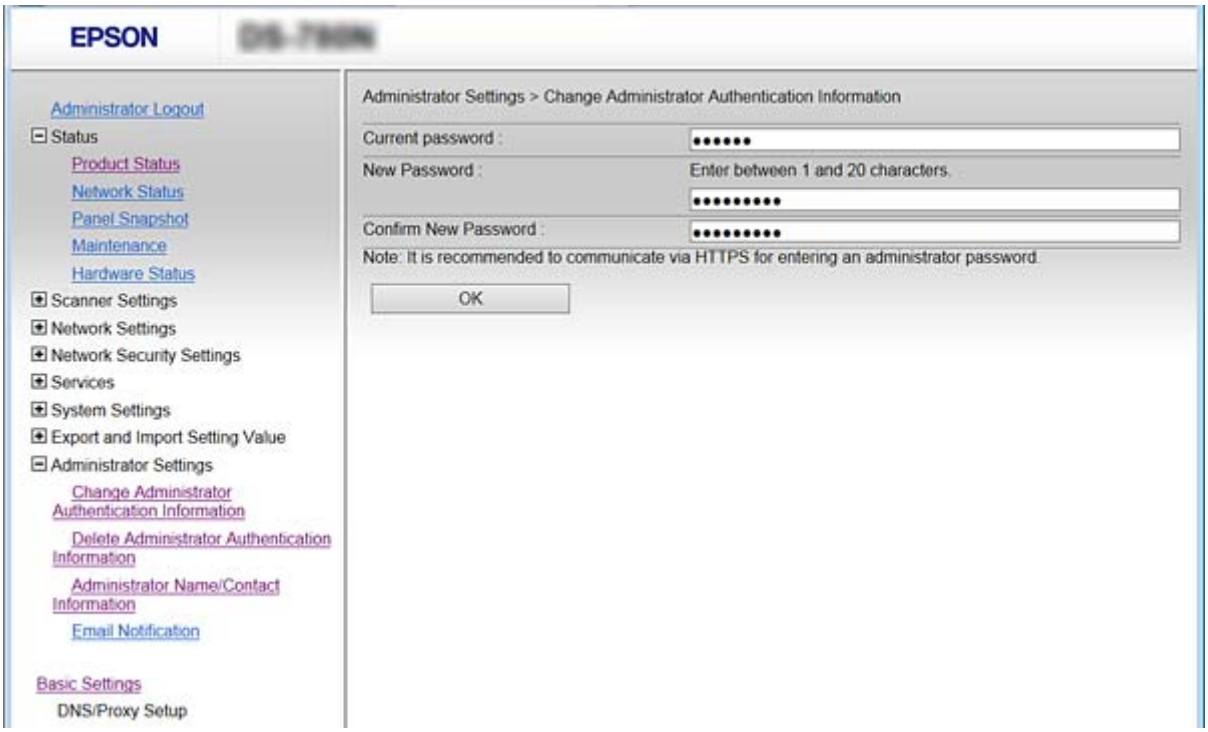
Конфігурація пароля адміністратора за допомогою Web Config

Пароль адміністратора можна встановити за допомогою Web Config.

1. Відкрийте Web Config та виберіть **Administrator Settings** > **Change Administrator Authentication Information**.

2. Введіть пароль у поля **New Password** і **Confirm New Password**. Уведіть ім'я користувача в разі необхідності.

   Якщо необхідно змінити пароль на новий, введіть поточний пароль.



3. Виберіть **OK**.

Примітка.

- ❏ *Щоб встановити або змінити заблоковані елементи меню, натисніть **Administrator Login**, а тоді введіть пароль адміністратора.*
- ❏ *Щоб видалити пароль адміністратора, натисніть **Administrator Settings** > **Delete Administrator Authentication Information**, а тоді введіть пароль адміністратора.*

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Елементи, які блокує адміністратор

Адміністратори мають право внесення налаштувань та змін для всіх функцій на пристрої.

Крім цього, якщо встановити пароль адміністратора на пристрої, його можа заблокувати, щоб не можна було змінити елементи, що стосуються керування пристроєм.

Нижче подані елементи, якими може керувати адміністратор.

Налаштування	Опис
Налаштування сканера	Налаштування виявлення подвійної подачі та режиму низької швидкості.
Налаштування з'єднання Ethernet	Зміна імен пристроїв та IP-адреси, налаштування сервера DNS або проксі-сервера, а також зміни налаштувань, що пов'язані з мережевими з'єднаннями.

Базові налаштування безпеки

Налаштування	Опис
Налаштування користувацьких служб	Налаштування для керування протоколами зв'язку, службами мережевого сканування та Document Capture Pro.
Налаштування електронної пошти	Встановлення сервера електронної пошти, з яким напряму зв'язуються пристрої.
Налаштування безпеки	Налаштування мережевої безпеки, наприклад, зв'язку SSL/TLS, фільтрування IPsec/IP та IEEE802.1X.
Оновлення кореневого сертифіката	Оновіть кореневі сертифікати, які необхідні для автентифікації Document Capture Pro Server та оновлення мікропрограм з Web Config.
Оновлення мікропрограм	Перевірка та оновлення мікропрограм пристроїв.
Налаштування часу і таймера	Час переходу в режим очікування, автоматичне вимкнення живлення, дата/час, таймер неактивності, інші налаштування, пов'язані з таймером.
Відновлення стандартних налаштувань	Налаштування сканера на відновлення заводських параметрів.
Налаштування адміністратора	Встановлення блокування адміністратора або паролю адміністратора.
Налаштування сертифікованого пристрою	Налаштування ідентифікатора пристрою автентифікації. Налаштуйте в разі використання сканера в системі автентифікації, що підтримує пристрої з автентифікацією.

Керування протоколами

Можна виконувати сканування з використанням цілої низки шляхів та протоколів. Також можна використовувати мережеве сканування з будь-якої кількості комп'ютерів у мережі. Наприклад, дозволяється сканування тільки за допомогою вказаних шляхів і протоколів. Можна знизити непередбачувані ризики для безпеки, обмеживши сканування з певних шляхів або керуючи доступними функціями.

Змініть конфігурацію налаштувань протоколу.

1. Відкрийте Web Config та виберіть **Services** > **Protocol**.
2. Налаштуйте конфігурацію кожного елемента.
3. Клацніть **Next**.
4. Клацніть **OK**.

   Ці налаштування будуть застосовані до сканера.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23
➡ «Протоколи, які можна увімкнути або вимкнути» на сторінці 36
➡ «Параметри протоколу» на сторінці 37

Протоколи, які можна увімкнути або вимкнути

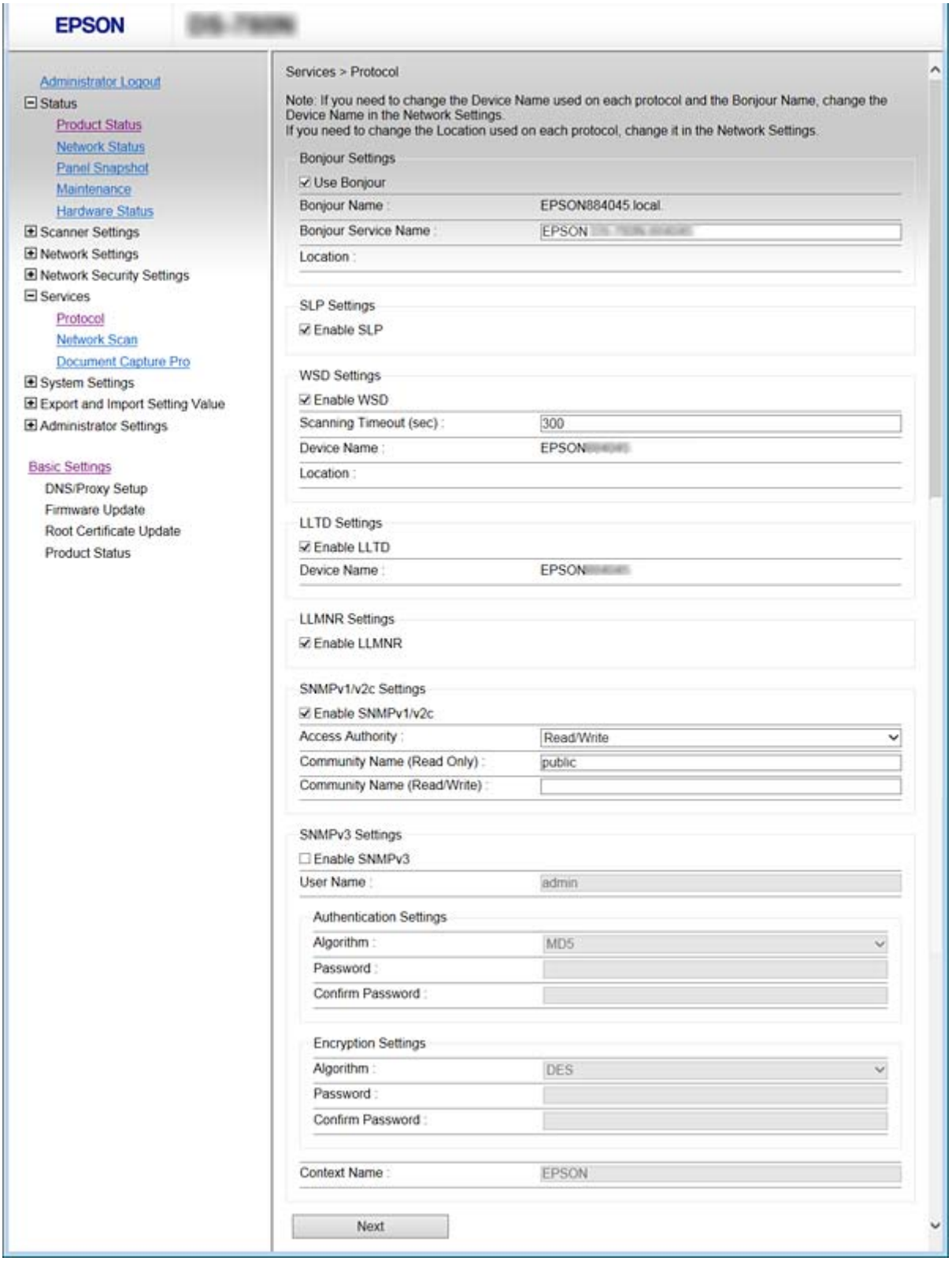
Протокол	Опис
Bonjour Settings	Можна вказати, чи потрібно використовувати Bonjour. Bonjour використовується для пошуку пристроїв, сканування тощо.
SLP Settings	Можна ввімкнути або вимкнути функцію SLP. Функція SLP використовується для програми Epson Scan 2 та мережевого пошуку в EpsonNet Config.
WSD Settings	Можна ввімкнути або вимкнути функцію WSD. Якщо її увімкнено, можна додавати пристрої WSD або сканувати через порт WSD.
LLTD Settings	Можна ввімкнути або вимкнути або функцію LLTD. Якщо її увімкнено, вона відображатиметься на мережевій мапі Windows.
LLMNR Settings	Можна ввімкнути або вимкнути або функцію LLMNR. Якщо її увімкнено, можна використовувати ідентифікацію імені без NetBIOS, навіть якщо ви не можете використовувати DNS.
SNMPv1/v2c Settings	Можна вказати, чи потрібно вмикати SNMPv1/v2c. Ця функція використовується для налаштування пристроїв, контролю і т.д.
SNMPv3 Settings	Можна вказати, чи потрібно вмикати SNMPv3. Ця функція використовується для налаштування шифрованих пристроїв.

Пов’язані відомості

➡ «Керування протоколами» на сторінці 35

➡ «Параметри протоколу» на сторінці 37

Параметри протоколу



Налаштування	Встановлення значення та опис
Bonjour Settings	

Базові налаштування безпеки

Налаштування	Встановлення значення та опис
Use Bonjour	Виберіть це для пошуку або використання пристроїв через Bonjour.
Bonjour Name	Відображення імені Bonjour.
Bonjour Service Name	Можна відобразити та вказати назву служби Bonjour.
Location	Відображення назви місця розташування Bonjour.
SLP Settings	
Enable SLP	Виберіть це, щоб увімкнути функцію SLP. Вона використовується для виявлення мережі у програмі Epson Scan 2 та EpsonNet Config.
WSD Settings	
Enable WSD	Виберіть це, щоб увімкнути додавання пристроїв за допомогою WSD, а тоді друкувати та сканувати через порт WSD.
Scanning Timeout (sec)	Введіть значення часу очікування зв'язку для сканування через WSD від 3 до 3600 секунд.
Device Name	Відображення назви пристрою WSD.
Location	Відображення назви місця розташування WSD.
LLTD Settings	
Enable LLTD	Виберіть це, щоб увімкнути LLTD. Сканер відобразиться на мережевій карті Windows.
Device Name	Відображення назви пристрою LLTD.
LLMNR Settings	
Enable LLMNR	Виберіть це, щоб увімкнути LLMNR. Можна використовувати ідентифікацію імені без NetBIOS, навіть якщо ви не можете використовувати DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Виберіть, щоб увімкнути SNMPv1/v2c. Відображатимуться тільки ті сканери, що підтримують SNMPv3.
Access Authority	Установіть права доступу За ввімкненого параметра SNMPv1/v2c. Виберіть **Read Only** або **Read/Write**.
Community Name (Read Only)	Введіть від 0 до 32 символів ASCII (від 0x20 до 0x7E).
Community Name (Read/Write)	Введіть від 0 до 32 символів ASCII (від 0x20 до 0x7E).
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 вмикається, коли встановлено прапорець.
User Name	Введіть від 1 до 32 символів, використовуючи 1-байтні символи.
Authentication Settings	

Базові налаштування безпеки

Налаштування	Встановлення значення та опис
Algorithm	Виберіть алгоритм для автентифікації до SNMPv3.
Password	Виберіть пароль для автентифікації до SNMPv3. Можна ввести від 8 до 32 символів формату ASCII (0x20 – 0x7E). Якщо це непотрібно вказувати, то залиште це місце пустим.
Confirm Password	Введіть установлений пароль для підтвердження.
Encryption Settings	
Algorithm	Виберіть алгоритм для шифрування для SNMPv3.
Password	Виберіть пароль для шифрування для SNMPv3. Можна ввести від 8 до 32 символів формату ASCII (0x20 – 0x7E). Якщо це непотрібно вказувати, то залиште це місце пустим.
Confirm Password	Введіть установлений пароль для підтвердження.
Context Name	Уведіть до 32 символів формату Unicode (UTF-8). Якщо це непотрібно вказувати, то залиште це місце пустим. Кількість символів, які можна ввести, змінюється в залежності від мови.

Пов'язані відомості

➡ «Керування протоколами» на сторінці 35

➡ «Протоколи, які можна увімкнути або вимкнути» на сторінці 36

Налаштування роботи та керування

У цьому розділі описано елементи, що пов'язані зі щоденними операціями та керуванням пристроєм.

Підтвердьте інформацію про пристрій

Подану нижче інформацію про робочий пристрій можна перевірити з меню **Status** за допомогою Web Config.

❏ Product Status

Перевірте мову, стан, номер продукту, адресу MAC тощо.

❏ Network Status

Перевірте інформацію про стан мережевого з'єднання, IP-адресу, сервер DNS тощо.

❏ Panel Snapshot

Відкрийте знімок екрану, який відображається на панелі керування пристрою.

❏ Maintenance

Перевірте дату початку, інформацію про сканування тощо.

❏ Hardware Status

Перевірте стан сканера.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Керування пристроями (Epson Device Admin)

Можна керувати і працювати з багатьма пристроями за допомогою Epson Device Admin. Epson Device Admin дає змогу керувати пристроями, розташованими в іншій мережі. Нижче описані основні функції керування.

Для детальнішої інформації про функції та використання програмного забезпечення, див. документацію або довідку Epson Device Admin.

❏ Знаходження пристроїв

Можна знайти пристрої у мережі, а тоді зареєструвати їх у списку. Якщо пристрої Epson, наприклад принтери або сканери, підключені до того самого сегменту мережі, що й комп'ютер адміністратора, їх можна знайти навіть якщо їм не було призначено IP-адресу.

Ви також можете знайти пристрої, які підключені до комп'ютерів у мережі через кабелі USB. Потрібно встановити на комп'ютері Epson Device USB Agent.

❏ Налаштування пристроїв

Можна зробити шаблон, який міститиме елементи налаштування, такі як мережевий інтерфейс та джерело паперу, та застосовувати їх для інших пристроїв як спільні налаштування. Якщо підключити його до мережі, то іншим пристроям, яким ще не призначено IP-адресу, можна призначити її.

❏ Контроль пристроїв

Ви можете систематично отримувати статус і детальну інформацію про пристрої в мережі. Крім того, ви можете контролювати пристрої, що підключені до комп'ютерів у мережі через кабелі USB, та пристрої від інших компаній, які були зареєстровані у списку пристроїв. Щоб контролювати пристрої, що підключені через кабелі USB, потрібно встановити Epson Device USB Agent.

❏ Керування сповіщеннями

Можна контролювати сповіщення про стан пристроїв та витратні матеріали. Система регулярно надсилає електронні повідомлення адміністратору на основі встановлених параметрів.

❏ Керування звітами

Ви можете створювати систематичні звіти, коли система назбирає дані про використання пристрою та витратні матеріали. Тоді ви можете зберегти ці звіти і надіслати їх електронною поштою.

Пов'язані відомості

➡ «Epson Device Admin» на сторінці 55

Отримання сповіщень електронної пошти щодо певних подій

Про сповіщення електронною поштою

Цю функцію можна використовувати для отримання попереджень електронною поштою в разі виникнення певних подій. Можна зареєструвати до 5 адрес електронної пошти та вибрати події, для яких необхідно отримувати сповіщення.

Сервер електронної пошти має бути налаштований для використання цієї функції.

Пов'язані відомості

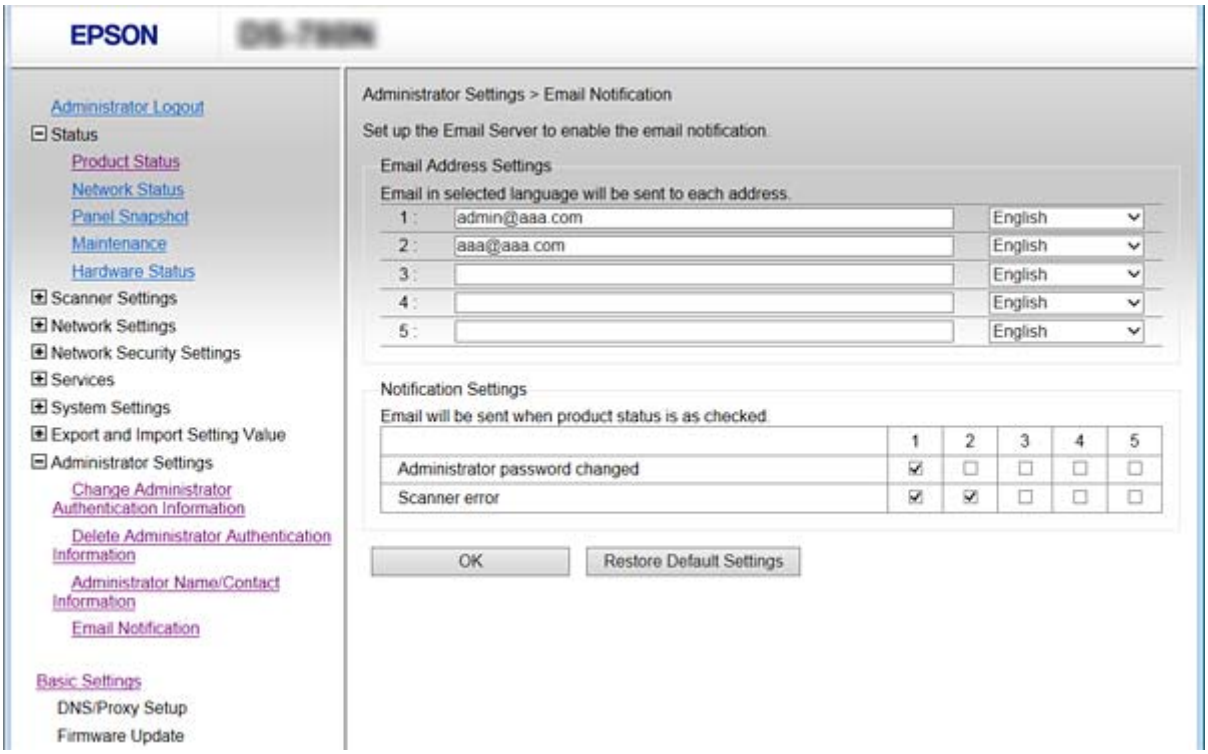
➡ «Налаштування поштового сервера» на сторінці 42

Налаштування отримання сповіщень електронною поштою

Для використання цієї функції необхідно налаштувати поштовий сервер.

1. Відкрийте Web Config і виберіть **Administrator Settings** > **Email Notification**.
2. Введіть адресу електронної пошти, на яку необхідно отримувати сповіщення.
3. Виберіть мову для сповіщень електронною поштою.

4. Установіть прапорці біля сповіщень, які необхідно отримувати.



5. Натисніть **OK**.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Налаштування поштового сервера» на сторінці 42

Налаштування поштового сервера

Перевірте інформацію нижче, перш ніж змінити конфігурацію.

❏ Сканер підключено до мережі.

❏ Інформація сервера електронної пошти на комп'ютері.

1. Відкрийте Web Config і виберіть **Network Settings** > **Email Server** > **Basic**.

2. Введіть значення для кожного елемента.

3. Виберіть **OK**.

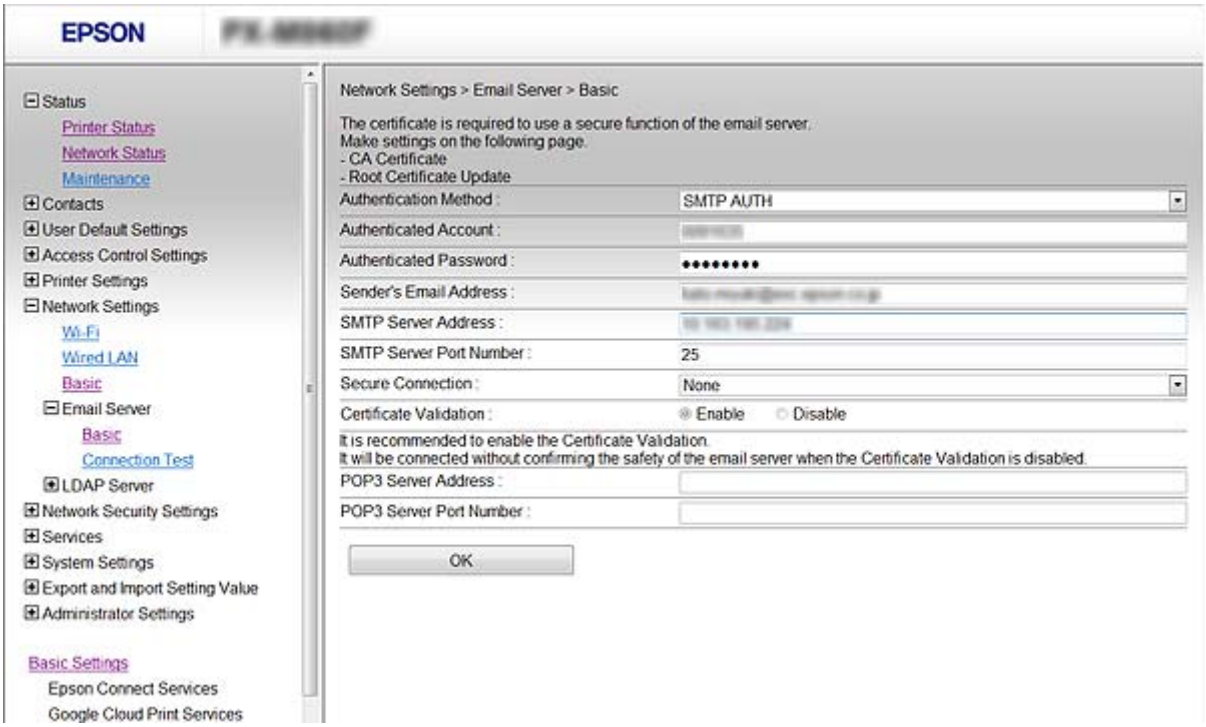
   Відобразяться вибрані параметри.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Параметри поштового сервера» на сторінці 43

Параметри поштового сервера



Елементи	Налаштування та пояснення	
Authentication Method	Виберіть метод автентифікації для доступу сканера до поштового сервера.	
	Off	Автентифікацію вимкнено під час зв'язку з поштовим сервером.
	SMTP AUTH	Потребує підтримки SMTP-автентифікації поштовим сервером.
	POP before SMTP	Налаштуйте сервер POP3 для вибору цього методу.
Authenticated Account	Якщо вибрати **SMTP AUTH** або **POP before SMTP** як значення для **Authentication Method**, введіть назву ідентифікованого облікового запису довжиною від 0 до 255 символів у ASCII (0x20–0x7E).	
Authenticated Password	Якщо вибрати **SMTP AUTH** або **POP before SMTP** як значення для **Authentication Method**, введіть пароль для автентифікації довжиною від 0 до 20 символів, використовуючи символи A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Введіть адресу електронної пошти відправника. Можна ввести від 0 до 255 символів формату ASCII (0x20–0x7E) за винятком символів : ( ) < > [ ] ; ¥. Крапка «.» не може бути першим символом.	
SMTP Server Address	Введіть від 0 до 255 символів, використовуючи символи A–Z a–z 0–9 . - . Можна використовувати формат IPv4 або FQDN.	
SMTP Server Port Number	Введіть число від 1 до 65535.	

Елементи	Налаштування та пояснення	
Secure Connection	Укажіть метод безпечного підключення для сервера електронної пошти.	
	None	Якщо вибрати **POP before SMTP** у **Authentication Method**, метод з'єднання перейде у значення **None**.
	SSL/TLS	Воно доступне, коли **Authentication Method** має значення **Off** або **SMTP AUTH**.
	STARTTLS	Воно доступне, коли **Authentication Method** має значення **Off** або **SMTP AUTH**.
Certificate Validation	Сертифікат перевіряється, коли увімкнена ця функція. Рекомендується встановити для неї значення **Enable**.	
POP3 Server Address	Якщо вибрати **POP before SMTP** для **Authentication Method**, введіть адресу POP3-сервера довжиною від 0 до 255 символів, використовуючи символи A–Z a–z 0–9 . - . Можна використовувати формат IPv4 або FQDN.	
POP3 Server Port Number	Щоб вибрати **POP before SMTP** для **Authentication Method**, введіть число від 1 до 65535.	

Пов'язані відомості

➡ «Налаштування поштового сервера» на сторінці 42

Перевірка з'єднання з поштовим сервером

1. Відкрийте Web Config і виберіть **Network Settings** > **Email Server** > **Connection Test**.
2. Виберіть **Start**.

   Розпочнеться перевірка підключення до сервера електронної пошти. Після завершення перевірки відображається звіт про її результати.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Повідомлення перевірки з'єднання з поштовим сервером» на сторінці 44

Повідомлення перевірки з'єднання з поштовим сервером

Повідомлення	Пояснення
Connection test was successful.	Це повідомлення з'являється, якщо з'єднання з сервером успішне.
SMTP server communication error. Check the following. - Network Settings	Це повідомлення відображається у перелічених нижче випадках ❏ Сканер не підключено до мережі ❏ Сервер SMTP не працює ❏ Пропало з'єднання з мережею під час підключення ❏ Отримано неповні дані

Налаштування роботи та керування

Повідомлення	Пояснення
POP3 server communication error. Check the following. - Network Settings	Це повідомлення відображається у перелічених нижче випадках ❏ Сканер не підключено до мережі ❏ Сервер POP3 не працює ❏ Пропало з'єднання з мережею під час підключення ❏ Отримано неповні дані
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Це повідомлення відображається у перелічених нижче випадках ❏ Не вдалося підключитися до сервера DNS ❏ Не вдалося ідентифікувати ім'я сервера SMTP
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Це повідомлення відображається у перелічених нижче випадках ❏ Не вдалося підключитися до сервера DNS ❏ Не вдалося ідентифікувати ім'я сервера POP3
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Це повідомлення відображається у разі невдалої автентифікації сервера SMTP.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Це повідомлення відображається у разі невдалої автентифікації сервера POP3.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Це повідомлення відображається у разі спроби підключитися до протоколів, що не підтримуються.
Connection to SMTP server failed. Change Secure Connection to None.	Це повідомлення відображається у разі виникнення розбіжності SMTP між сервером та клієнтом або якщо сервер не підтримує безпечне підключення SMTP (SSL-з'єднання).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Це повідомлення відображається у разі виникнення розбіжності SMTP між сервером та клієнтом або якщо сервер просить використовувати підключення SSL/TLS для безпечного SMTP-з'єднання.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Це повідомлення відображається у разі виникнення розбіжності SMTP між сервером та клієнтом або якщо сервер просить використовувати підключення STARTTLS для безпечного SMTP-з'єднання.
The connection is untrusted. Check the following. - Date and Time	Це повідомлення відображається, коли налаштування дати й часу сканера неправильні або термін дії сертифіката завершився.
The connection is untrusted. Check the following. - CA Certificate	Це повідомлення відображається, якщо сканер не має кореневого сертифіката, що відповідає серверу, або CA Certificate не імпортовано.
The connection is not secured.	Це повідомлення з'являється, коли отриманий сертифікат пошкоджений.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Це повідомлення з'являється, якщо не збігаються методи автентифікації між сервером та клієнтом. Сервер підтримує SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Це повідомлення з'являється, якщо не збігаються методи автентифікації між сервером та клієнтом. Сервер не підтримує SMTP AUTH.

Повідомлення	Пояснення
Sender's Email Address is incorrect. Change to the email address for your email service.	Це повідомлення з'являється, якщо вказано неправильну електронну адресу відправника.
Cannot access the product until processing is complete.	Це повідомлення з'являється, коли сканер зайнятий.

Пов'язані відомості

➡ «Перевірка з'єднання з поштовим сервером» на сторінці 44

Оновлення мікропрограми

Оновлення мікропрограми за допомогою Web Config

Виконується оновлення мікропрограми за допомогою Web Config. Пристрій має бути підключений до інтернету.

1. Відкрийте Web Config та виберіть **Basic Settings** > **Firmware Update**.
2. Клацніть **Start**.

   Запуститься підтвердження мікропрограми, а тоді з'явиться інформація про те, чи вже існує оновлення мікропрограми.
3. Клацніть **Start**, а тоді дотримуйтеся вказівок на екрані.

Примітка.
Ви також можете оновити мікропрограмне забезпечення за допомогою Epson Device Admin. Можна візуально перевірити інформацію про мікропрограмне забезпечення у списку пристроїв. Це корисно, коли вам потрібно оновити мікропрограми кількох пристроїв. Докладнішу інформацію див. у посібнику Epson Device Admin.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23
➡ «Epson Device Admin» на сторінці 55

Оновлення програмного забезпечення за допомогою Epson Firmware Updater

Можна завантажити програмне забезпечення із веб-сайту Epson на комп'ютер, а тоді підключити пристрій до комп'ютера через кабель USB, щоб оновити мікропрограму. Якщо не вдається оновити через мережу, спробуйте вказаний нижче спосіб.

1. Відкрийте веб-сайт Epson і завантажте мікропрограму.
2. Підключіть комп'ютер, на який завантажено мікропрограму, до пристрою за допомогою кабелю USB.

3. Двічі клацніть завантажений файл .exe.

   Запуститься Epson Firmware Updater.

4. Дотримуйтеся вказівок на екрані.

Резервне копіювання налаштувань

Шляхом експортування елементів налаштування у Web Config можна копіювати їх на інші сканери.

Експортування налаштувань

Експортуйте кожне налаштування для сканера.

1. Відкрийте Web Config, а тоді виберіть **Export and Import Setting Value** > **Export**.

2. Виберіть налаштування, які слід експортувати.

   Виберіть налаштування, які потрібно експортувати. Якщо ви вибрали основну категорію, то підкатегорії також будуть вибрані. Слід мати на увазі, що не можна вибирати підкатегорії, якщо вони дублюються в межах однієї мережі (наприклад, IP-адреси і т.д.).

3. Введіть пароль для кодування експортованого файлу.

   Для імпортування файлу потрібен пароль. Залиште це поле порожнім, якщо не бажаєте кодувати файл.

4. Натисніть **Export**.

> ***Важливо***
>
> *Якщо потрібно експортувати мережеві налаштування сканера, наприклад ім'я принтера та IP-адресу, виберіть* ***Enable to select the individual settings of device*** *та виберіть інші елементи. Використовуйте тільки вибрані значення для змінного сканера.*

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Імпортування налаштувань

Імпортування експортованого файлу Web Config на сканер.

> ***Важливо***
>
> *Перш ніж імпортувати значення, які містять окрему інформацію, наприклад, про ім'я сканера або IP-адресу, перевірте, чи немає такої самої IP-адреси у тій самій мережі. Якщо IP-адреси збігаються, сканер не відображатиме значення.*

1. Відкрийте Web Config, а тоді виберіть **Export and Import Setting Value** > **Import**.

2. Виберіть експортований файл, а тоді введіть закодований пароль.

3. Натисніть **Next**.
4. Виберіть обсяг, який потрібно додати, і натисніть **Next**.
5. Натисніть **OK**.

Ці налаштування будуть застосовані до сканера.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Усунення несправностей

Поради з усунення несправностей

Додаткову інформацію можна знайти в зазначеному нижче посібнику.

❏ Посібник користувача

Містить інструкції з експлуатації сканера, технічного обслуговування та усунення несправностей.

Перевірка журналу для сервера та мережевого пристрою

У разі появи проблем з мережевим з'єднанням можна визначити її причину, переглянувши журнал сервера електронної пошти, сервера LDAP тощо, перевіривши статус за допомогою мережевого журналу з журналів і команд системного обладнання, наприклад маршрутизаторів.

Ініціалізація налаштування мережі

Відновлення налаштувань мережі з панелі керування

Можна відновити параметри мережі до стандартних.

1. Натисніть **Налаш.** на головному екрані.
2. Натисніть **Сист. адміністрування** > **Віднов. налашт. за зам.** > **Налаштування мережі**.
3. Перевірте повідомлення та натисніть **Так**.
4. Коли з'явиться повідомлення про завершення, натисніть **Закрити**.

   Екран автоматично закриється після певного часу, якщо ви не натискаєте **Закрити**.

Перевірка з'єднання між пристроями та комп'ютерами

Перевірка підключення за допомогою команди Ping — Windows

Щоб переконатися, що комп'ютер підключено до сканера, можна використовувати команду Ping. Щоб перевірити підключення за допомогою команди Ping, виконайте зазначені нижче дії.

Усунення несправностей

1. Перевірте IP-адресу сканера для підключення, яке потрібно перевірити.

   Це можна зробити за допомогою програми Epson Scan 2.

2. Відкрийте командний рядок комп'ютера.

   ❏ Windows 10

   Натисніть правою кнопкою миші кнопку пуску або натисніть і утримуйте її, тоді виберіть **Командний рядок**.

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

   Відкрийте вікно програми, а тоді виберіть **Командний рядок**.

   ❏ Для Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 або старішої версії

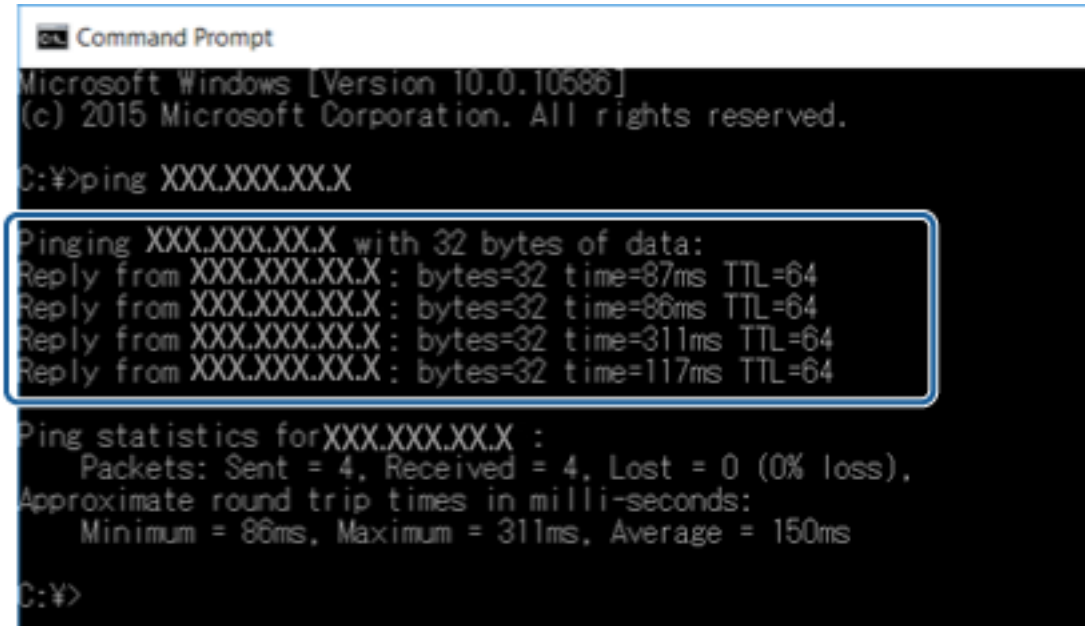
   Натисніть кнопку пуску, виберіть **Усі програми** або **Програми** > **Службові** > **Командний рядок**.

3. Уведіть «ping xxx.xxx.xxx.xxx», а тоді натисніть клавішу Enter.

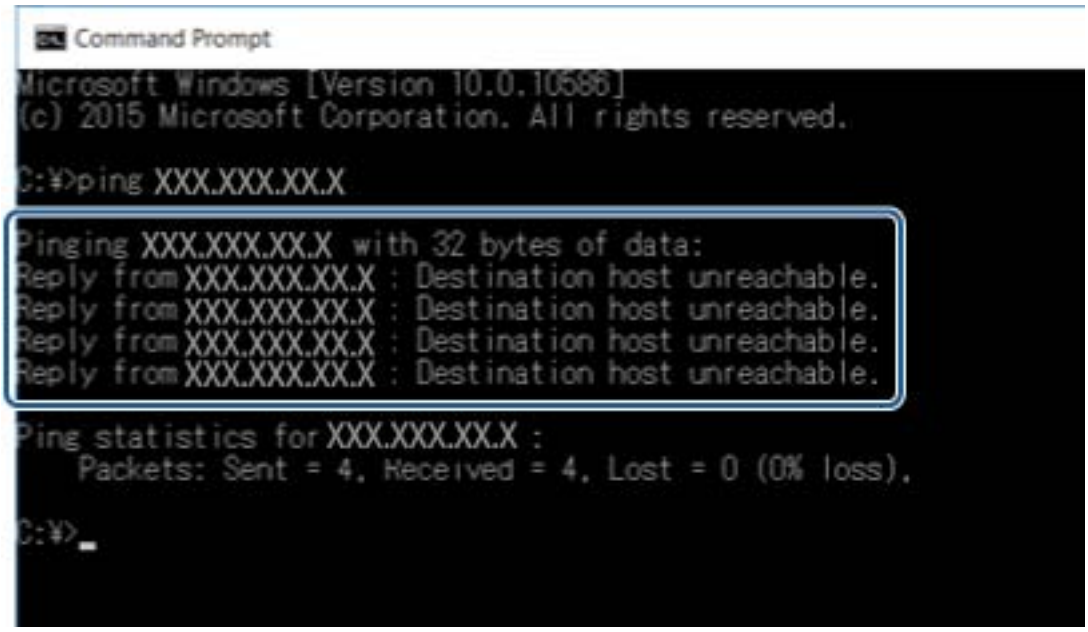
   Укажіть IP-адресу сканера для xxx.xxx.xxx.xxx.

4. Перевірте стан зв'язку.

   Якщо зв'язок між сканером і комп'ютером налагоджено, з'явиться вказане нижче повідомлення.



Якщо зв'язок між сканером і комп'ютером не налагоджено, з'явиться вказане нижче повідомлення.



Перевірка з'єднання за допомогою команди Ping — Mac OS

Щоб переконатися, що комп'ютер підключено до сканера, можна використовувати команду Ping. Щоб перевірити підключення за допомогою команди Ping, виконайте зазначені нижче дії.

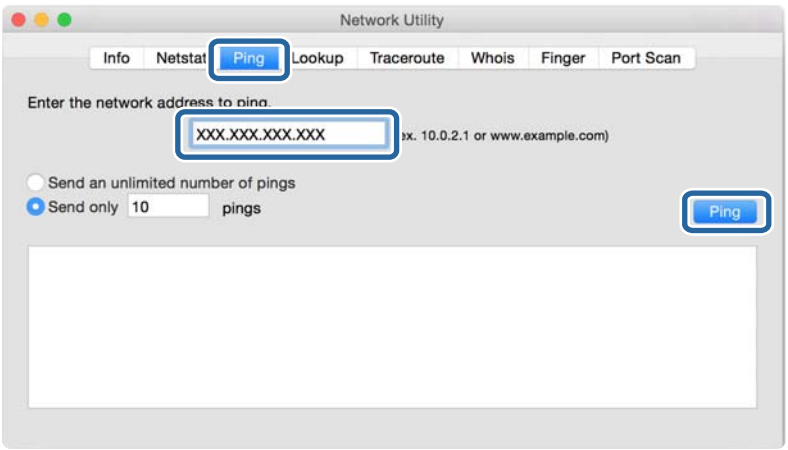
1. Перевірте IP-адресу сканера для підключення, яке потрібно перевірити.

   Це можна зробити за допомогою програми Epson Scan 2.

2. Запустіть сервісну програму мережі Network Utility.

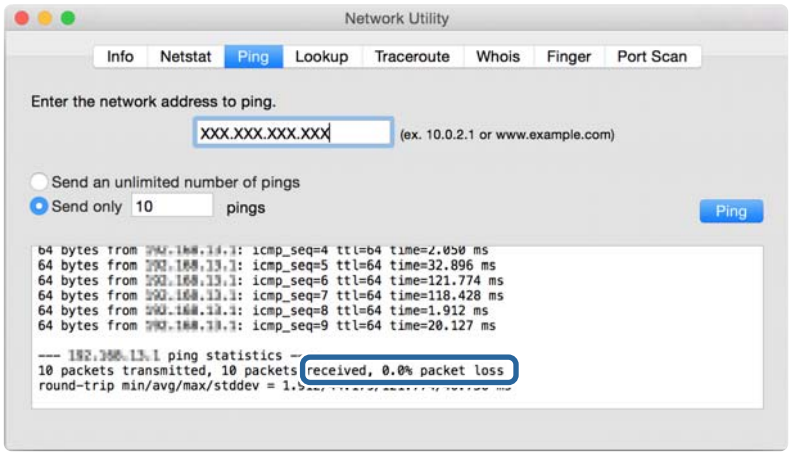
   Уведіть «Network Utility» у розділ **Spotlight**.

3. Натисніть вкладку **Ping**, уведіть IP-адресу, яку ви перевірили у кроці 1, а тоді натисніть **Ping**.

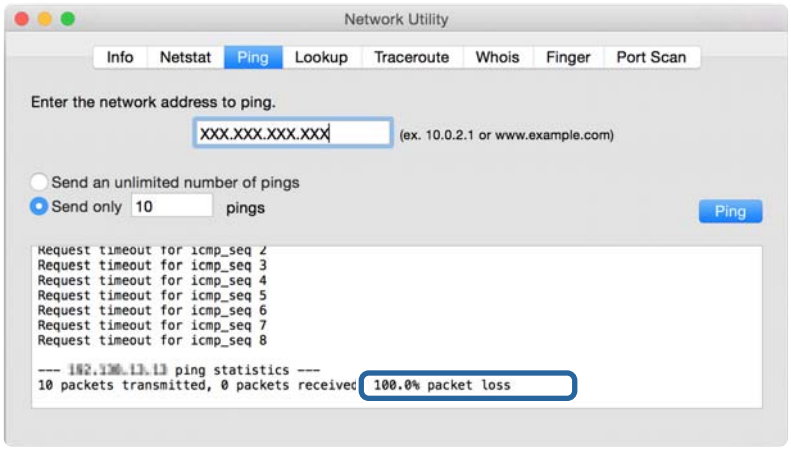


4. Перевірте стан підключення.

   Якщо зв'язок між сканером і комп'ютером налагоджено, з'явиться вказане нижче повідомлення.



   Якщо зв'язок між сканером і комп'ютером не налагоджено, з'явиться вказане нижче повідомлення.



Проблеми з використанням мережного програмного забезпечення

Якщо не вдається відкрити Web Config

Чи правильно налаштовано IP-адресу сканера?

Налаштуйте IP-адресу за допомогою Epson Device Admin або EpsonNet Config.

Чи підтримує ваш браузер групове шифрування для Encryption Strength для SSL/TLS?

Нидче наведено групові шифрування для Encryption Strength для SSL/TLS. Web Config можна відкрити тільки у браузері, який підтримує зазначені нижче групові шифрування. Перевірте, яке шифрування підтримує браузер.

❏ 80 біт: AES256/AES128/3DES

- ❏ 112 біт: AES256/AES128/3DES
- ❏ 128 біт: AES256/AES128
- ❏ 192 біти: AES256
- ❏ 256 біт: AES256

Повідомлення «Застарілі дані» з'являється під час доступу до Web Config з використанням з'єднання SSL (https).

Якщо сертифікат застарілий, отримайте його знову. Якщо таке повідомлення з'являється до завершення строку дії сертифіката, перевірте, чи правильно встановлено дату сканера.

Повідомлення «Ім'я сертифіката безпеки не відповідає…» з'являється під час доступу до Web Config з використанням з'єднання SSL (https).

IP-адреса сканера, введена в полі **Common Name** для створення власного сертифіката або ЗПС, не відповідає адресі, введеній у браузері. Отримайте та імпортуйте сертифікат знову або змініть ім'я сканера.

Доступ до сканера виконується через проксі-сервер.

Якщо зі сканером використовується проксі-сервер, необхідно налаштувати параметри проксі-сервера у браузері.

- ❏ Windows:

  Виберіть **Панель керування** > **Мережа й Інтернет** > **Властивості браузера** > **Підключення** > **Настройки локальної мережі** > **Проксі-сервер**, а потім укажіть не використовувати проксі-сервер для локальних адрес.

- ❏ Mac OS:

  Виберіть **Системні параметри** > **Мережа** > **Додаткові** > **Проксі**, а потім зареєструйте локальну адресу для параметра **Обхід проксі-сервера для цих хостів і доменів**.

  Приклад:

  192.168.1.*: локальна адреса 192.168.1.XXX, маска підмережі 255.255.255.0

  192.168.*.*: локальна адреса 192.168.XXX.XXX, маска підмережі 255.255.0.0

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Призначення IP-адреси» на сторінці 15

➡ «Призначення IP-адреси за допомогою EpsonNet Config» на сторінці 56

Назва моделі та/або IP-адреса не відображаються в EpsonNet Config

Чи вибирали ви Блокувати, Скасувати або Вимкнути, коли відобразився екран безпеки Windows або екран брандмауера?

Якщо було вибрано **Блокувати**, **Скасувати** або **Вимкнути**, IP-адреса не відображатиметься в EpsonNet Config або EpsonNet Setup.

Щоб виправити це, зареєструйте EpsonNet Config як виняток у брандмауері Windows і комерційних програмах для безпеки. якщо на комп'ютері інстальовано антивірус або програму безпеки, закрийте їх, а потім спробуйте скористатись EpsonNet Config.

Можливо, встановлено занадто короткий час очікування, перш ніж виникне помилка зв'язку?

Запустіть EpsonNet Config і виберіть **Tools** > **Options** > **Timeout**, а потім збільште тривалість очікування для параметра **Communication Error**. Зверніть увагу, що це може призвести до в вповільнення роботи EpsonNet Config.

Пов'язані відомості

➡ «Запуск EpsonNet Config — Windows» на сторінці 56

➡ «Запуск EpsonNet Config — Mac OS» на сторінці 56

Додаток

Вступ до мережевого програмного забезпечення

Нижче описано програмне забезпечення, яке задає конфігурацію та керує пристроями.

Epson Device Admin

Epson Device Admin — це програма, яка дає змогу встановлювати пристрої в мережі, а тоді задавати їхню конфігурацію та керувати. Ви можете отримувати детальну інформацію про пристрої, наприклад, стан та витратні матеріали, надсилати сповіщення про попередження системи і створювати звіти про використання пристрою. Можна також зробити шаблон, який міститиме елементи налаштування та застосовувати їх для інших пристроїв як спільні налаштування. Можна завантажити Epson Device Admin з веб-сайту підтримки Epson. Для отримання детальнішої інформації див. документацію або довідку Epson Device Admin.

Запуск Epson Device Admin (тільки для Windows)

Виберіть **Усі програми** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Примітка.
У разі виникнення сигналу тривоги брандмауера дозвольте доступ до програм Epson Device Admin.

EpsonNet Config

EpsonNet Config дозволяє адміністратору налаштувати конфігурацію мережі сканнера, зокрема призначити IP-адресу або змінити режим з'єднання. Функція налаштування пакетом підтримується в ОС Windows. Для отримання детальнішої інформації див. документацію або довідку EpsonNet Config.

Запуск EpsonNet Config — Windows

Виберіть меню **Усі програми** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Примітка.
У разі виникнення сигналу тривоги брандмауера дозвольте доступ до програм EpsonNet Config.

Запуск EpsonNet Config — Mac OS

Оберіть **Перейти** > **Застосунки** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager — це програмне забезпечення для створення пакета для простого встановлення компонентів сканера, наприклад установлення та налаштування драйвера або встановлення Document Capture Pro. Це програмне забезпечення дозволяє адміністратору створювати унікальні програмні пакети й розподіляти їх між групами.

Для отримання докладнішої інформації відвідайте веб-сайт Epson свого регіону.

Призначення IP-адреси за допомогою EpsonNet Config

Можна призначити IP-адресу сканеру за допомогою EpsonNet Config. EpsonNet Config дає змогу призначати IP-адресу сканеру, якому ще не була призначена така адреса після підключення через кабель Ethernet.

Призначення IP-адреси за допомогою пакетного налаштування

Створення файлу для пакетних налаштувань

За допомогою адреси MAC та моделі, використаних як ключі, можна створити файл SYLK для встановлення IP-адреси.

1. Відкрийте програму таблиці (наприклад, Microsoft Excel) або текстовий редактор.

2. Уведіть у першому рядку «Info_MACAddress», «Info_ModelName» та «TCPIP_IPAddress» як імена елементів налаштування.

   Уведіть елементи налаштування для вказаних нижче текстових рядків. Щоб розрізняти літери верхнього та нижнього регістрів та дво-/однобайтні символи, елемент не розпізнаватиметься, якщо хоча б один символ буде відрізнятися.

   Уведіть назву елемента налаштування, як це описано нижче, інакше EpsonNet Config не зможе розпізнати елементи налаштування.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Уведіть адресу MAC, назву моделі та IP-адресу для кожного мережевого пристрою.

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. Уведіть ім’я та збережіть як файл SYLK (*.slk).

Пакетне налаштування за допомогою файлу конфігурації

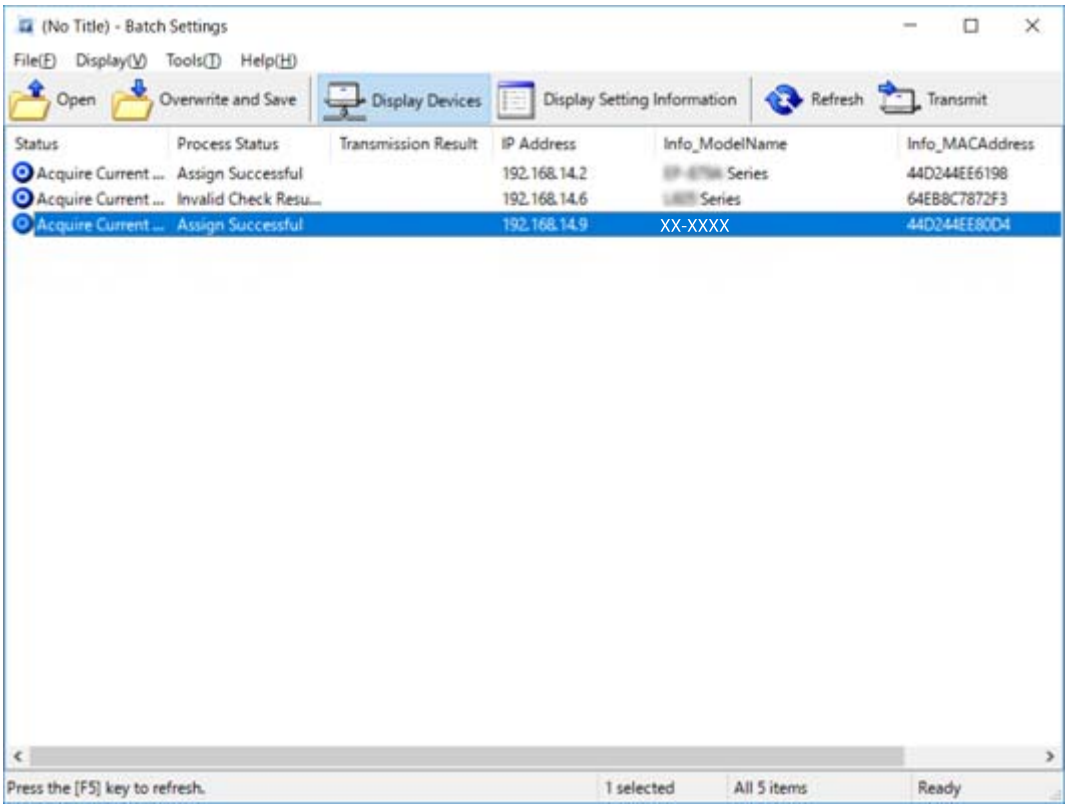
Миттєво призначайте IP-адреси у файлі конфігурації (файл SYLK file). Перед призначенням потрібно створити файл конфігурації.

1. Підключіть всі прситрої до мережі за допомогою кабелів Ethernet.
2. Увімкніть сканер.
3. Запустіть EpsonNet Config.

   Відобразиться список сканерів у мережі. Перш ніж вони з’являться на екрані, може пройти певний час.
4. Клацніть **Tools** > **Batch Settings**.
5. Клацніть **Open**.
6. На екрані вибору файлів, виберіть файл SYLK (*.slk), який містить налаштування, і натисніть **Open**.

7. Виберіть пристрої, для яких потрібно виконати пакетне налаштування, за допомогою стовпця **Status**, встановленого у значення **Unassigned**, та параметра **Process Status** зі значенням **Assign Successful**.

   Якщо потрібно вибрати кілька пристроїв, натисніть Ctrl або Shift і натисніть або перетягніть мишку.



8. Клацніть **Transmit**.

9. Коли з’явиться екран введення пароля, уведіть його, а тоді натисніть **OK**.

   Передача налаштувань.

   Примітка.
   Інформація передається через мережевий інтерфейс, доки індикатор перебігу не дійде до кінця. Не вимикайте пристрій або бездротовий адаптер, і не надсилайте жодних даних на пристрій.

10. На екрані **Transmitting Settings** оберіть **OK**.

11. Перевірте стан пристрою, який ви встановили.

    Для пристроїв, які показують  або  , перевірте вміст файлу налаштувань або що пристрій нормально перезавантажився.

Піктограма	Status	Process Status	Пояснення
	Setup Complete	Setup Successful	Встановлення пройшло успішно.
	Setup Complete	Rebooting	Після передачі інформації кожен пристрій потрібно перезавантажити, щоб увімкнулися налаштування. Перевірка виконується для визначення, чи може пристрій підключатися після перезавантаження.
	Setup Complete	Reboot Failed	Неможливо підтвердити пристрій після передачі налаштувань. Перевірте, чи пристрій увімкнено і чи нормально він перезавантажився.
	Setup Complete	Searching	Пошук пристрою, вказаного у файлі налаштувань.*
	Setup Complete	Search Failed	Неможливо перевірити пристрої, які вже встановлені. Перевірте, чи пристрій увімкнено і чи нормально він перезавантажився.*

    * Тільки в разі відображення інформації про налаштування.

Пов’язані відомості

➡ «Запуск EpsonNet Config — Windows» на сторінці 56

➡ «Запуск EpsonNet Config — Mac OS» на сторінці 56

Призначення IP-адреси кожному пристрою

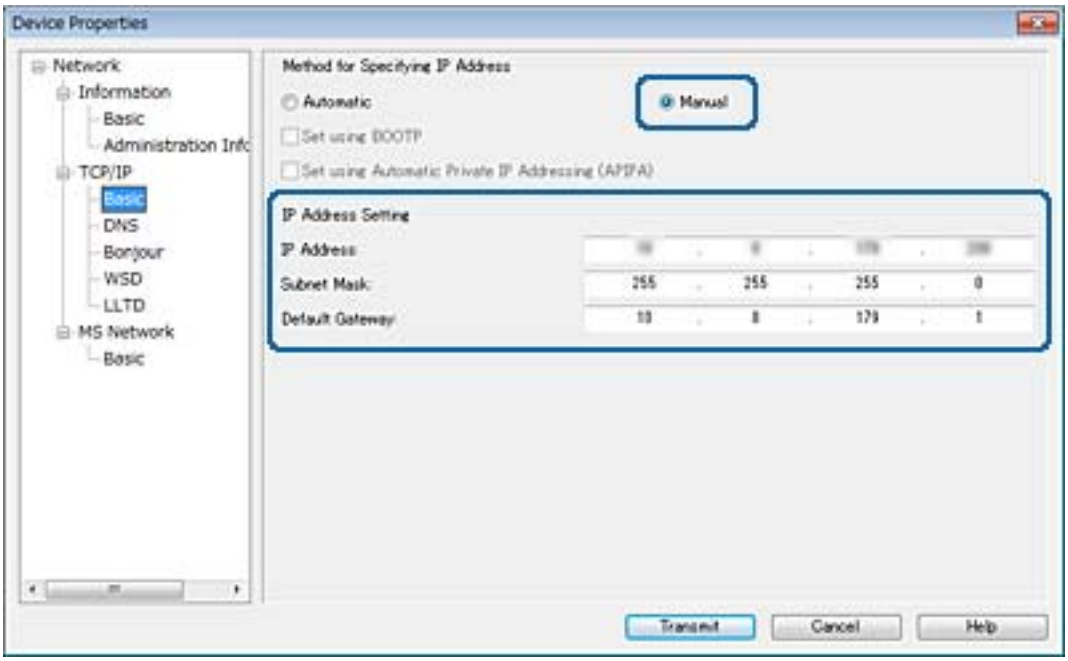
Призначте IP-адресу сканеру за допомогою EpsonNet Config.

1. Увімкніть сканер.
2. Підключіть сканер до мережі за допомогою кабелю Ethernet.
3. Запустіть EpsonNet Config.

   Відобразиться список сканерів у мережі. Перш ніж вони з’являться на екрані, може пройти певний час.
4. Двічі клацніть сканер, якому буде присвоєно значення.

   Примітка.
   Якщо ви підключили кілька сканерів однієї моделі, можна ідентифікувати їх за допомогою MAC-адреси.
5. Оберіть **Network** > **TCP/IP** > **Basic**.

6. Уведіть адреси для **IP Address**, **Subnet Mask** та **Default Gateway**.



Примітка.
Уведіть статичну адресу в разі підключення сканера до захищеної мережі.

7. Клацніть **Transmit**.

   Відобразиться екран підтвердження передавання інформації.

8. Клацніть **OK**.

   Відобразиться екран завершення передавання.

   Примітка.
   Інформацію буде передано на пристрій, після чого з'явиться повідомлення Configuration successfully completed (Налаштування успішно виконано). Не вимикайте пристрій і не надсилайте жодних даних до служби.

9. Клацніть **OK**.

Пов'язані відомості

➡ «Запуск EpsonNet Config — Windows» на сторінці 56

➡ «Запуск EpsonNet Config — Mac OS» на сторінці 56

Використання порту для сканера

Сканер використовує вказаний нижче порт. До цих портів потрібно надати відповідний доступ для адміністраторів мережі.

Додаток

Відправник (Клієнт)	Використання	Одержувач (Сервер)	Протокол	Номер порту
Сканер	Надсилання електронної пошти (сповіщення електронною поштою)	Сервер SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	Сервер POP перед SMTP-з'єднанням (сповіщення електронною поштою	Сервер POP	POP3 (TCP)	110
	Керування WSD	Клієнтський комп'ютер	WSD (TCP)	5357
	Пошук комп'ютера під час виконання функції «push-scan» у Document Capture Pro	Клієнтський комп'ютер	Пошук мережевої функції «push-scan»	2968
	Збір інформації про завдання під час виконання функції «push-scan» у Document Capture Pro	Клієнтський комп'ютер	Мережева функція «push-scan»	2968
Клієнтський комп'ютер	Знайдіть сканер через програму, наприклад EpsonNet Config, драйвер сканера.	Сканер	ENPC (UDP)	3289
	Зберіть та встановіть інформацію MIB через програму, таку як EpsonNet Config, драйвер сканера.	Сканер	SNMP (UDP)	161
	Пошук сканера WSD	Сканер	WS-Discovery (UDP)	3702
	Пересилання даних сканування Document Capture Pro	Сканер	Network Scan (TCP)	1865

Розширені параметри безпеки для підприємства

У цьому розділі описано розширені функції безпеки.

Налаштування безпеки та запобігання небезпеці

Коли пристрій підключений до мережі, його можна відкрити з віддаленого розташування. Крім того, багато людей можуть спільно використовувати пристрій, що значно підвищує ефективність і зручність роботи. Однак в такому разі збільшуються ризики несанкціонованого доступу, забороненого використання та зловмисне втручання в дані. Якщо ви використовуєте пристрій у середовищі, де можна зайти в інтернет, то ризики стають ще вищими.

Щоб уникнути цих ризиків, пристрої Epson містять низку технологій безпеки.

Встановіть пристрій відповідно до умов середовища, створеного за допомогою даних про середовище клієнта.

Ім'я	Тип функції	Що налаштовувати	Чого уникати
Зв'язок за допомогою протоколів SSL/TLS	Шлях з'єднання між комп'ютером і пристроєм шифрується за допомогою зв'язку SSL/TLS. Вміст з'єднання через браузер захищається.	Установіть сертифікат CA для сервера, який є сертифікатом, підписаним CA (Центром сертифікації) для пристрою.	Запобігайте витоку інформації про налаштування та вмісту даних, переданих з комп'ютера на сканер. Доступ на сервер Epson в інтернеті з пристрою також можна захистити за допомогою оновлення програмного забезпечення тощо.
Фільтрування за IPsec/IP	Можна встановити так, щоб обмежити або заблокувати дані від певного клієнта або певного типу. Оскільки IPsec захищає дані за допомогою пакетного блоку IP (шифрування та автентифікація), ви можете безпечно застосовувати незахищений протокол сканування.	Створіть базову політику та індивідуальну політику, щоб встановити тип клієнта або тип даних, які можуть отримувати доступ до пристрою.	Захистіть пристрій від несанкціонованого доступу, зловмисного втручання та перехоплювання даних зв'язку.
SNMPv3	Додаються функції, такі як моніторинг підключених пристроїв у мережі, інтегрування даних для протоколу SNMP, протокол для контролю, шифрування, автентифікації користувача тощо.	Увімкніть SNMPv3, тоді встановіть спосіб автентифікації та шифрування.	Забезпечте налаштування змін через мережу та конфіденційність у моніторингу стану.

Розширені параметри безпеки для підприємства

Ім'я	Тип функції	Що налаштовувати	Чого уникати
IEEE802.1X	Дозволяє підключатися користувачеві, який не авторизований в мережі Ethernet. Дозволяє використовувати пристрій тільки авторизованому користувачеві.	Налаштування автентифікації на сервері RADIUS (сервер автентифікації).	Захист від несанкціонованого доступу та використання пристрою.
Зчитування ідентифікаційної картки	Можна використовувати пристрій, підносячи ідентифікаційну картку до підключеного пристрою автентифікації. Можна обмежити отримання журналів для кожного користувача та пристрою, а також обмежити доступність пристроїв і функцій для використання користувачем або групою користувачів.	Підключіть пристрій автентифікації до пристрою, а тоді налаштуйте інформацію про користувача у системі автентифікації.	Запобігайте несанкціонованому використанню пристрою та імітації з'єднання з ним.

Пов'язані відомості

- «Зв'язок SSL/TLS зі сканером» на сторінці 63
- «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 71
- «Використання протоколу SNMPv3» на сторінці 83
- «Підключення сканера до мережі IEEE802.1X» на сторінці 85

Налаштування функцій безпеки

У разі налаштування фільтрації за IPsec/IP або IEEE802.1X, радимо відкрити Web Config за допомогою SSL/TLS, щоб донести інформацію про налаштування та зменшити ризики безпеки, наприклад, зловмисне втручання в систему чи перехоплення даних.

Зв'язок SSL/TLS зі сканером

Коли сертифікат сервера встановлено за допомогою зв'язку SSL/TLS (протокол захищених сокетів/протокол безпеки на транспортному рівні) зі сканером, шлях з'єднання між двома комп'ютерами можна шифрувати. Зробіть це, якщо ви бажаєте запобігти віддаленому та неавторизованому доступу.

Про цифрову сертифікацію

❏ Сертифікат, підписаний ЦС

Сертифікат, підписаний ЦС (Центром сертифікації), отримується в Центрі сертифікації. Безпечне з'єднання можна забезпечити шляхом використання сертифіката, підписаного ЦС. Сертифікат ЦС можна використовувати для кожної функції безпеки.

❏ Сертифікат ЦС

Сертифікат ЦС є показником того, що третя сторона перевірила дійсність сервера. Це є ключовим компонентом безпеки типу WOT. Сертифікат ЦС для автентифікації сервера необхідно отримати у ЦС, що їх видає.

❏ Сертифікат із власним підписом

Сертифікат із власним підписом видається та підписується сканером. Такий сертифікат є ненадійним і не може запобігти несанкціонованому доступу. Якщо використовувати цей сертифікат для сертифіката SSL/TLS, у браузері може відобразитися попередження служби безпеки. Цей сертифікат можна використовувати лише для зв'язку SSL/TLS.

Пов'язані відомості

➡ «Отримання та імпорт сертифіката, підписаного ЦС» на сторінці 64

➡ «Видалення сертифіката, підписаного ЦС» на сторінці 68

➡ «Оновлення сертифіката із власним підписом» на сторінці 68

Отримання та імпорт сертифіката, підписаного ЦС

Отримання сертифіката, підписаного ЦС

Щоб отримати сертифікат, підписаний ЦС, створіть ЗПС (запит на підписання сертифіката) і надішліть його до Центру сертифікації. Можна створити ЗПС за допомогою налаштувань Web Config та комп'ютера.

Виконайте наведені нижче дії, щоб створити ЗПС і отримати сертифікат, підписаний ЦС, за допомогою Web Config. У разі створення ЗПС за допомогою Web Config сертифікат матиме формат PEM/DER.

1. Відкрийте Web Config, а тоді виберіть **Network Security Settings**. Далі виберіть **SSL/TLS** > **Certificate** або **IPsec/IP Filtering** > **Client Certificate**, або **IEEE802.1X** > **Client Certificate**.

2. Клацніть **Generate** у **CSR**.

   Відкриється сторінка створення ЗПС.

3. Введіть значення для кожного елемента.

   Примітка.
   Доступні довжина ключа та скорочення залежать від Центру сертифікації. Створіть запит відповідно до правил Центру сертифікації.

4. Натисніть **OK**.

   Відобразиться повідомлення про завершення.

5. Виберіть **Network Security Settings**. Далі виберіть **SSL/TLS** > **Certificate** або **IPsec/IP Filtering** > **Client Certificate**, або **IEEE802.1X** > **Client Certificate**.

6. У **CSR** клацніть одну з кнопок завантаження, щоб завантажити на комп'ютер ЗПС формату, зазначеного Центром сертифікації.

   Важливо
   Не потрібно ще раз генерувати ЗПС. Якщо ви це зробите, ви не зможете імпортувати виданий CA-signed Certificate.

7. Надішліть ЗПС до Центру сертифікації та отримайте сертифікат CA-signed Certificate.

   Дотримуйтеся правил щодо методу та форми надсилання запиту, встановлених Центром сертифікації.

8. Збережіть виданий CA-signed Certificate на комп'ютері, підключеному до сканера.

   Процес отримання CA-signed Certificate завершено, коли сертифікат збережено до папки призначення.

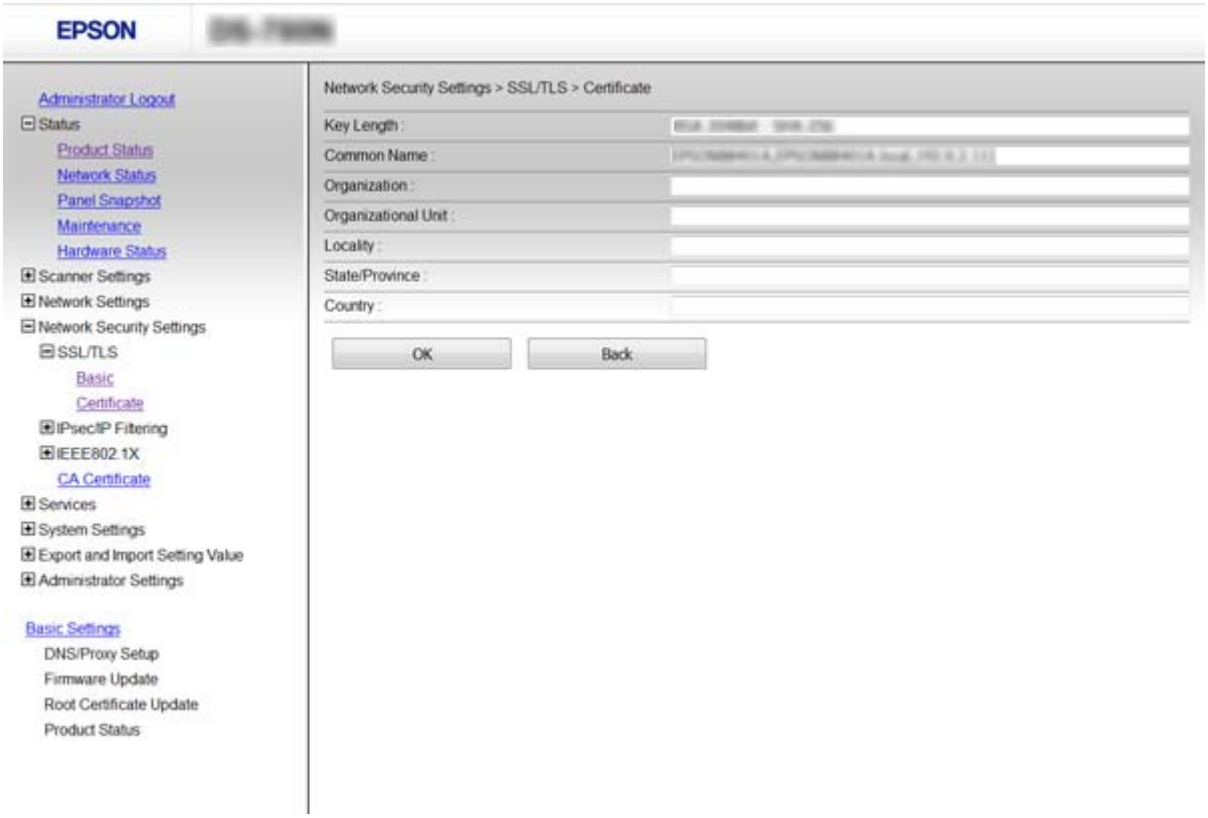
Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Параметри ЗПС» на сторінці 65

➡ «Імпортування сертифіката, підписаного ЦС» на сторінці 66

Параметри ЗПС



Налаштування	Налаштування та пояснення
Key Length	Виберіть довжину ключа для ЗПС.
Common Name	Можна ввести від 1 до 128 символів. Якщо це IP-адреса, вона має бути статичною. Приклад: Адреса URL для доступу до Web Config: https://10.152.12.225 Загальна назва: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Можна ввести від 0 до 64 символів формату ASCII (0x20 – 0x7E). Окремі імена можна розділяти комами.

Налаштування	Налаштування та пояснення
Country	Введіть двозначний код країни за стандартом ISO-3166.

Пов'язані відомості

➡ «Отримання сертифіката, підписаного ЦС» на сторінці 64

Імпортування сертифіката, підписаного ЦС

Важливо

❏ *Переконайтеся, що дата й час сканера встановлені правильно.*

❏ *У разі отримання сертифіката за ЗПС, створеним через Web Config, імпортувати сертифікат можна один раз.*

1. Відкрийте Web Config а тоді виберіт **Network Security Settings**. Далі виберіть **SSL/TLS** > **Certificate** або **IPsec/IP Filtering** > **Client Certificate**, або **IEEE802.1X** > **Client Certificate**.

2. Натисніть **Import**.

   Відкриється сторінка імпорту сертифіката.

3. Введіть значення для кожного елемента.

   Залежно від того, де створювався ЗПС та який формат файлу сертифіката, необхідні налаштування можуть різнитися. Введіть необхідні значення параметрів, дотримуючись наведених нижче умов.

   ❏ Сертифікат у форматі PEM/DER, отриманий з Web Config

   ❏ **Private Key**: не слід налаштовувати, тому що сканер має закритий ключ.

   ❏ **Password**: не налаштовувати.

   ❏ **CA Certificate 1**/**CA Certificate 2**: необов'язково

   ❏ Сертифікат у форматі PEM/DER, отриманий з комп'ютера

   ❏ **Private Key**: необхідно встановити.

   ❏ **Password**: не налаштовувати.

   ❏ **CA Certificate 1**/**CA Certificate 2**: необов'язково

   ❏ Сертифікат у форматі PKCS#12, отриманий з комп'ютера

   ❏ **Private Key**: не налаштовувати.

   ❏ **Password**: необов'язково

   ❏ **CA Certificate 1**/**CA Certificate 2**: не налаштовувати.

4. Натисніть **OK**.

   Відобразиться повідомлення про завершення.

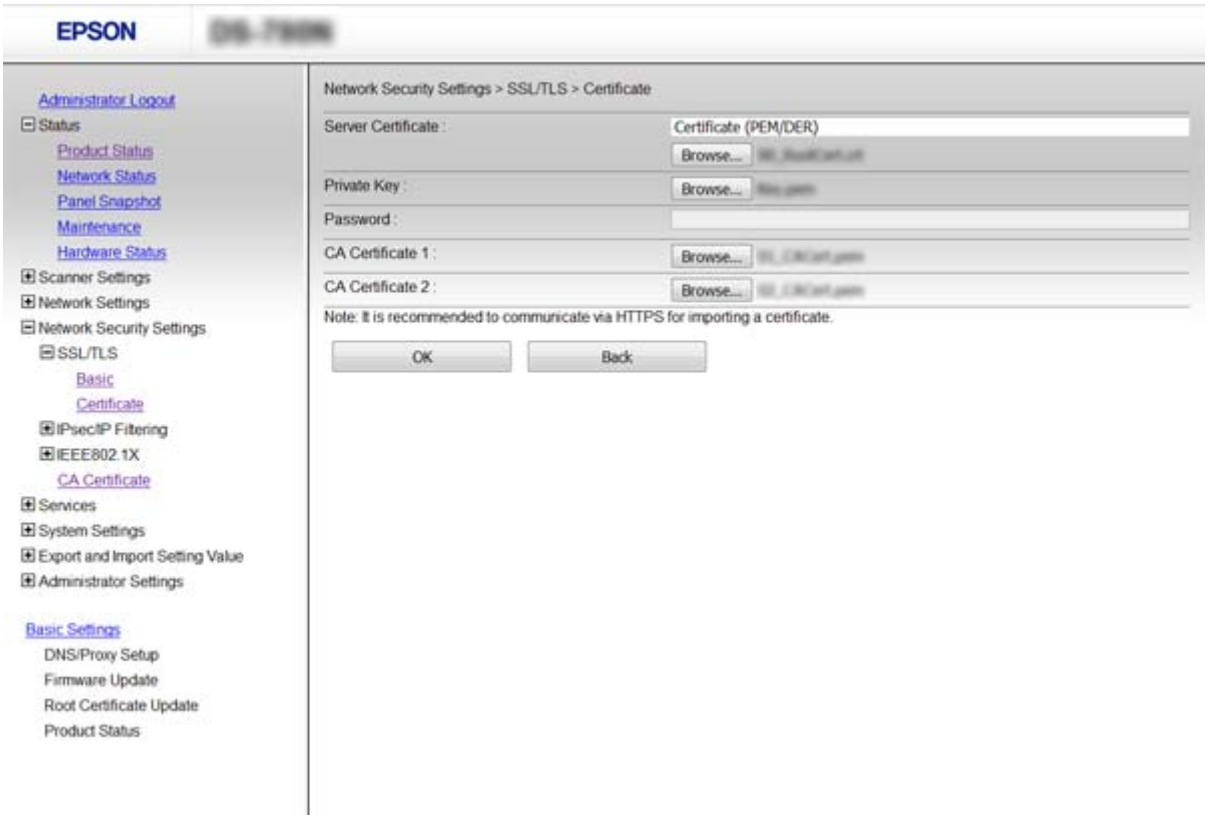
Примітка.
*Натисніть **Confirm**, щоб перевірити інформацію сертифіката.*

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Параметри імпорту сертифіката, підписаного ЦС» на сторінці 67

Параметри імпорту сертифіката, підписаного ЦС



Елементи	Налаштування та пояснення
Server Certificate або Client Certificate	Виберіть формат сертифіката.
Private Key	У разі отримання сертифіката у форматі PEM/DER за ЗПС, створеним на комп'ютері вкажіть файл закритого ключа, що відповідає сертифікату.
Password	Введіть пароль для шифрування закритого ключа.
CA Certificate 1	Якщо формат сертифіката **Certificate (PEM/DER)**, імпортуйте сертифікат із Центру сертифікації, що видав сертифікат сервера. Виберіть необхідний файл.
CA Certificate 2	Якщо формат сертифіката **Certificate (PEM/DER)**, імпортуйте сертифікат із Центру сертифікації, що видав **CA Certificate 1**. Виберіть необхідний файл.

Пов'язані відомості

➡ «Імпортування сертифіката, підписаного ЦС» на сторінці 66

Видалення сертифіката, підписаного ЦС

Імпортований сертифікат можна видалити, якщо строк його дії завершився або якщо шифрування з'єднання більше не потрібне.

> ***Важливо***
>
> *У разі отримання сертифіката за ЗПС, створеним через Web Config, імпортувати видалений сертифікат ще раз буде неможливо. У цьому випадку створіть ЗПС і отримайте сертифікат знову.*

1. Відкрийте Web Config, а тоді виберіть **Network Security Settings**. Далі виберіть **SSL/TLS** > **Certificate** або **IPsec/IP Filtering** > **Client Certificate**, або **IEEE802.1X** > **Client Certificate**.
2. Клацніть **Delete**.
3. Підтвердіть, що ви справді бажаєте видалити сертифікат, указаний у повідомленні.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Оновлення сертифіката із власним підписом

Якщо сканер підтримує функцію сервера HTTPS, сертифікат із власним підписом можна оновити. У разі доступу до Web Config з використанням сертифіката із власним підписом з'являється попередження.

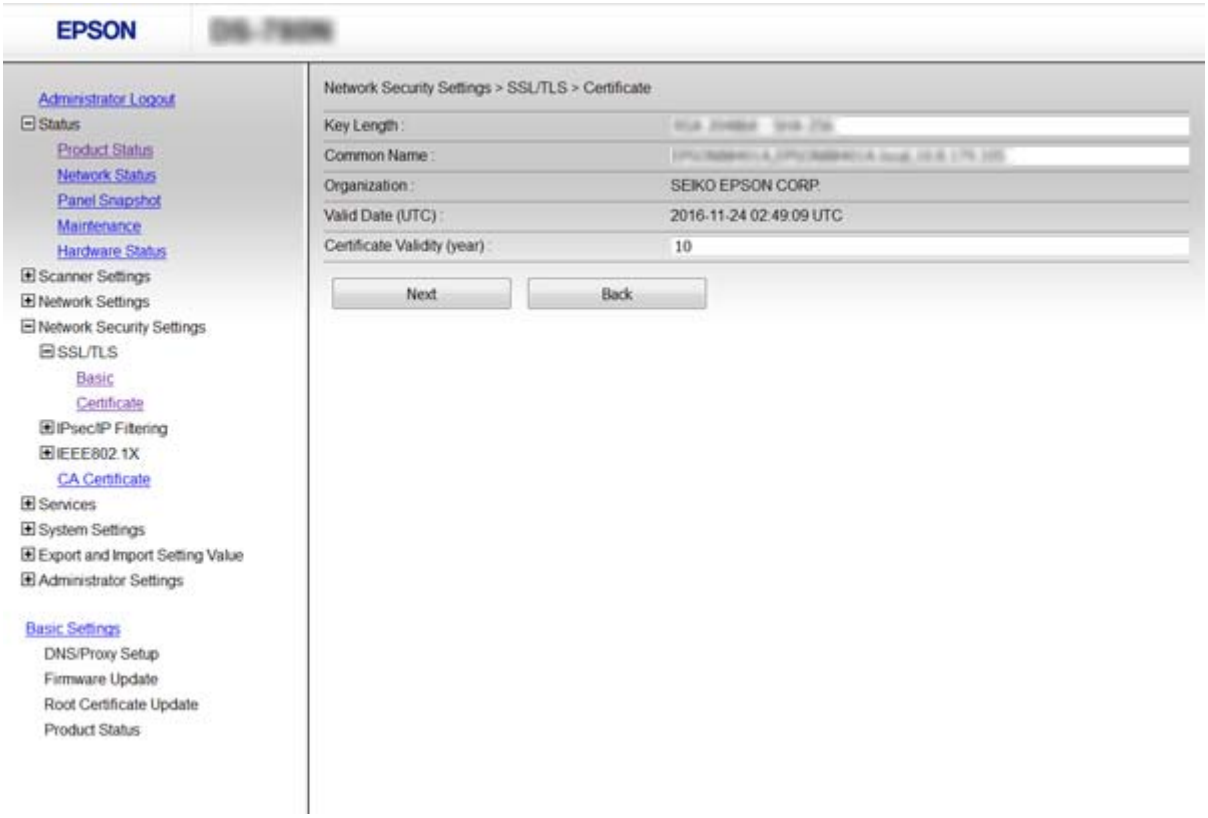
Сертифікат із власним підписом слід використовувати лише тимчасово, доки не буде отримано й імпортовано сертифікат, підписаний ЦС.

1. Відкрийте Web Config і виберіть **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Клацніть **Update**.
3. Введіть **Common Name**.

   Введіть IP-адресу або ідентифікатор, наприклад повне доменне ім'я сканера. Можна ввести від 1 до 128 символів.

   Примітка.
   Окремі імена (CN) можна розділяти комами.

4. Укажіть термін дії сертифіката.



5. Клацніть **Next**.

   Відобразиться повідомлення про підтвердження.

6. Клацніть **OK**.

   Сканер буде оновлено.

Примітка.
*Натисніть **Confirm**, щоб перевірити інформацію сертифіката.*

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Налаштування CA Certificate

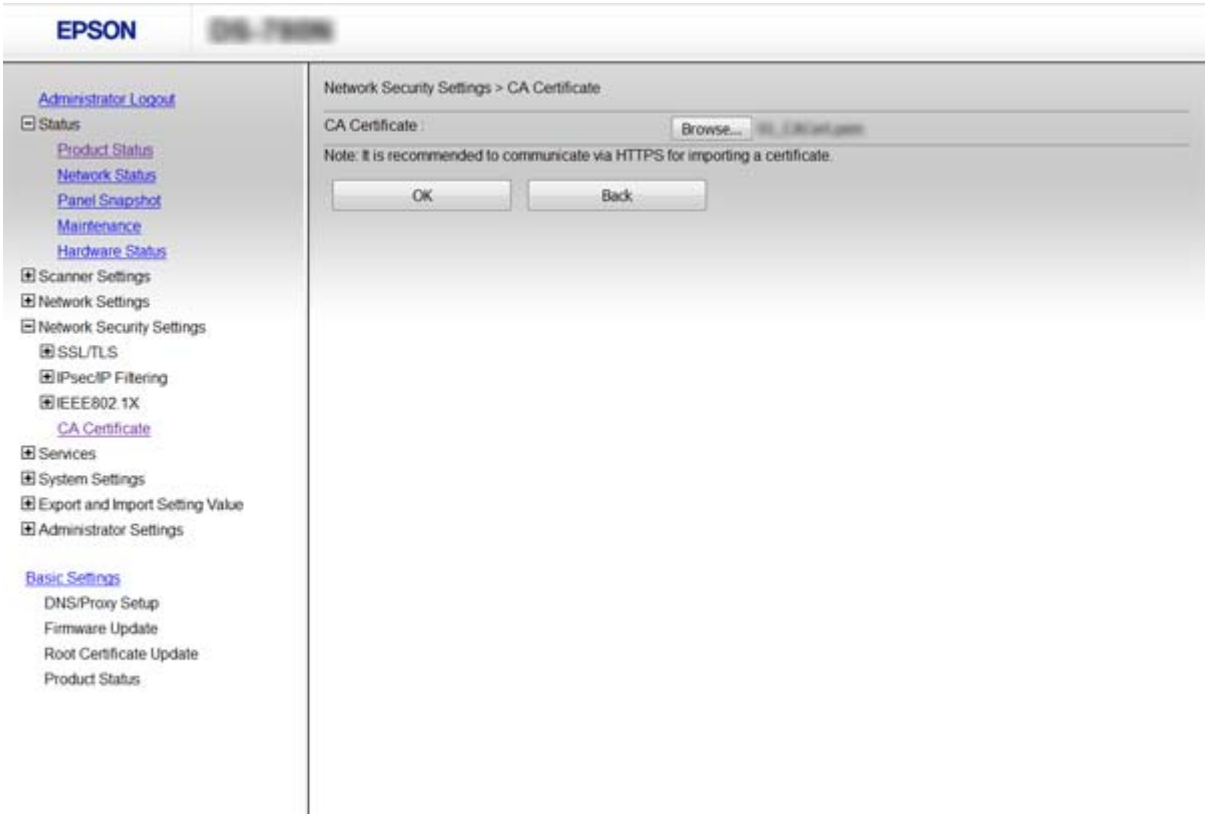
Можна імпортувати, відображати або видаляти CA Certificate.

Імпортування CA Certificate

1. Відкрийте Web Config, а тоді виберіть **Network Security Settings** > **CA Certificate**.

2. Натисніть **Import**.

3. Укажіть CA Certificate, який потрібно імпортувати.



4. Натисніть **OK**.

Після завершення імпортування ви повернетеся до екрану **CA Certificate**, де відображатиметься імпортований CA Certificate.

Пов'язані відомості

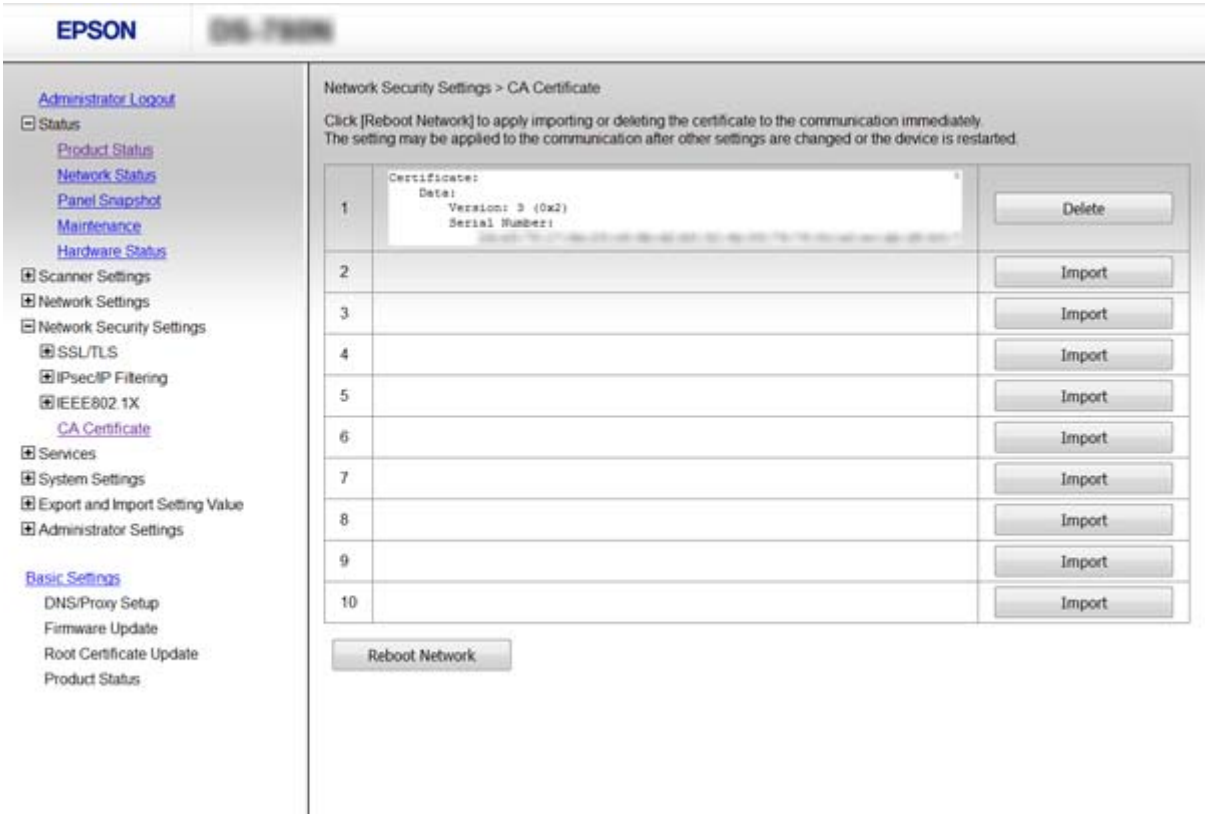
➡ «Доступ до налаштувань Web Config» на сторінці 23

Видалення CA Certificate

Можна видалити імпортований CA Certificate.

1. Відкрийте Web Config, а тоді виберіть **Network Security Settings** > **CA Certificate**.

2. Натисніть **Delete** поряд із CA Certificate, який потрібно видалити.



3. Підтвердіть, що ви справді бажаєте видалити сертифікат, указаний у повідомленні.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Шифрування зв'язку за допомогою фільтрації за IPsec/IP

Про IPsec/IP Filtering

Якщо сканер підтримує функцію IPsec/IP-фільтрування, можна налаштувати фільтрування трафіку за IP-адресами, послугами та портами. Поєднуючи фільтри, можна налаштувати сканер на приймання або блокування зазначених клієнтів і зазначених даних. Крім того, можна покращити рівень безпеки за допомогою IPsec.

Для фільтрації трафіку встановіть політику за замовчуванням. Політика за замовчуванням застосовується до кожного користувача або групи, що підключається до сканера. Для ефективнішого контролю над користувачами та групами користувачів установіть групову політику. Групова політика — це правило або ряд правил, що застосовуються до користувача або групи користувачів. Сканер керує пакетами IP, які відповідають налаштованим політикам. Пакети IP проходять перевірку групових політик в порядку з 1 по 10, а потім — політики за замовчуванням.

Примітка.
Комп'ютери під керуванням ОС Windows Vista та новіше або Windows Server 2008 і новіше підтримують функцію IPsec.

Налаштування Default Policy

1. Відкрийте Web Config і виберіть **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Введіть значення для кожного елемента.
3. Натисніть **Next**.

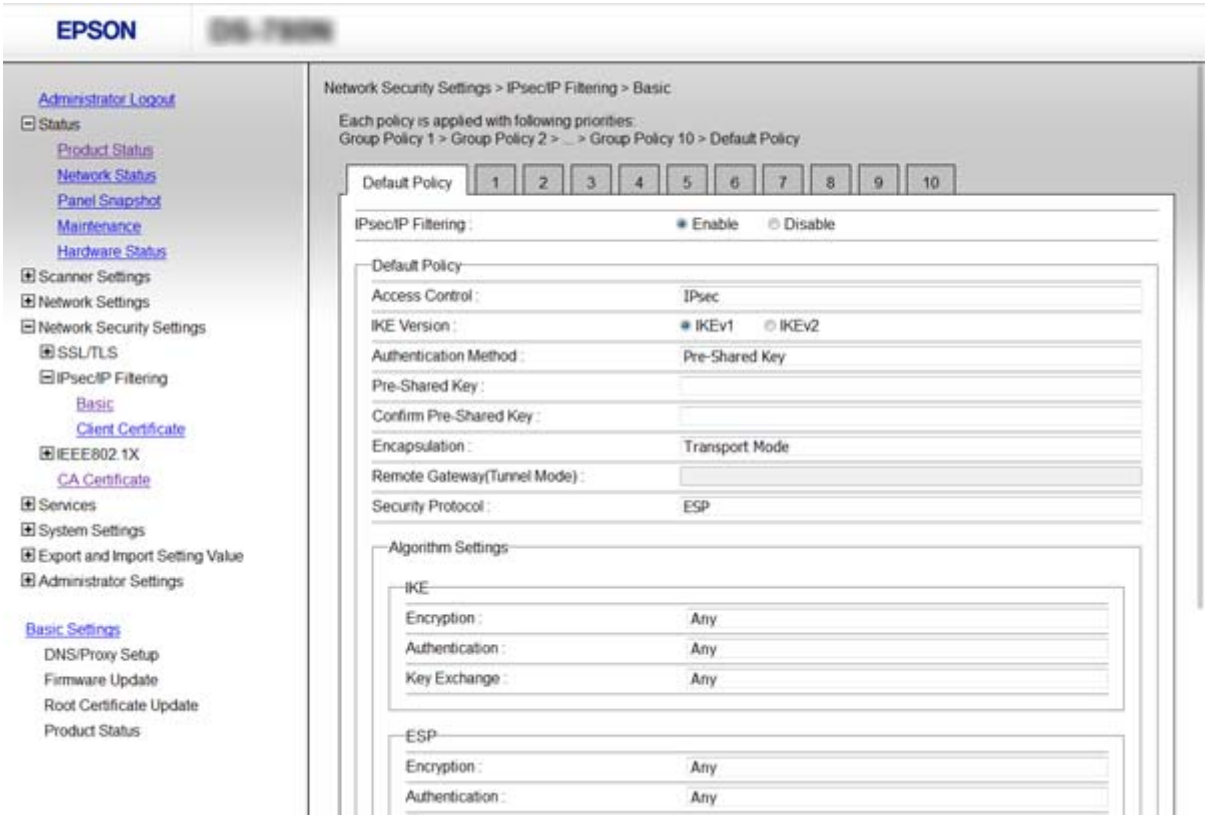
   Відобразиться повідомлення про підтвердження.
4. Натисніть **OK**.

   Сканер буде оновлено.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23
➡ «Параметри Default Policy» на сторінці 72

Параметри Default Policy



Розширені параметри безпеки для підприємства

Налаштування	Налаштування та пояснення	
IPsec/IP Filtering	Функцію мережі IPsec/IP-фільтрування можна ввімкнути або вимкнути.	
Access Control	Налаштуйте спосіб керування для трафіку або пакетів IP.	
	Permit Access	Виберіть це, щоб дозволити проходження налаштованих пакетів IP.
	Refuse Access	Виберіть це, щоб заборонити проходження налаштованих пакетів IP.
	IPsec	Виберіть це, щоб дозволити проходження налаштованих пакетів IPsec.
IKE Version	Виберіть IKEv1 або IKEv2 для версії IKE. Виберіть одне зі значень відповідно до пристрою, до якого підключено сканер.	
IKEv1	Вказані нижче елементи відображаються, якщо вибрати **IKEv1** для **IKE Version**.	
	Authentication Method	Щоб вибрати **Certificate**, необхідно заздалегідь отримати та імпортувати сертифікат, підписаний ЦС.
	Pre-Shared Key	Щоб вибрати **Pre-Shared Key** для **Authentication Method**, введіть спільний ключ довжиною від 1 до 127 символів.
	Confirm Pre-Shared Key	Введіть установлений ключ для підтвердження.
IKEv2	Вказані нижче елементи відображаються, якщо вибрати **IKEv2** для **IKE Version**.	
Local	Authentication Method	Щоб вибрати **Certificate**, необхідно заздалегідь отримати та імпортувати сертифікат, підписаний ЦС.
	ID Type	Виберіть тип ідентифікатора для сканера.
	ID	Введіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Distinguished Name**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «=». **IP Address**: Введіть формат IPv4 або IPv6. **FQDN**: Введіть комбінацію від 1 до 255 символів, використовуючи символи A – Z, a – z, 0 – 9, «-» та крапку (.). **Email Address**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «@». **Key ID**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E).
	Pre-Shared Key	Щоб вибрати **Pre-Shared Key** для **Authentication Method**, введіть спільний ключ довжиною від 1 до 127 символів.
	Confirm Pre-Shared Key	Введіть установлений ключ для підтвердження.

Розширені параметри безпеки для підприємства

Налаштування	Налаштування та пояснення	
Remote	Authentication Method	Щоб вибрати **Certificate**, необхідно заздалегідь отримати та імпортувати сертифікат, підписаний ЦС.
	ID Type	Виберіть тип ідентифікатора для пристрою, який ви бажаєте автентифікувати.
	ID	Введіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Distinguished Name**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «=». **IP Address**: Введіть формат IPv4 або IPv6. **FQDN**: Введіть комбінацію від 1 до 255 символів, використовуючи символи A – Z, a – z, 0 – 9, «-» та крапку (.). **Email Address**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «@». **Key ID**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E).
	Pre-Shared Key	Щоб вибрати **Pre-Shared Key** для **Authentication Method**, введіть спільний ключ довжиною від 1 до 127 символів.
	Confirm Pre-Shared Key	Введіть установлений ключ для підтвердження.
Encapsulation	Щоб вибрати **IPsec** для **Access Control**, необхідно налаштувати режим інкапсуляції.	
	Transport Mode	Виберіть це, якщо сканер використовується в одній локальній мережі. Шифруватимуться пакети IP рівня 4 або вище.
	Tunnel Mode	Виберіть цей параметр, якщо сканер використовується в мережі з можливістю підключення до Інтернету, наприклад IPsec-VPN. Шифруватимуться заголовки та дані пакетів IP.
Remote Gateway(Tunnel Mode)	Щоб вибрати **Tunnel Mode** для **Encapsulation**, введіть адресу шлюзу довжиною від 1 до 39 символів.	
Security Protocol	**IPsec** для **Access Control**, виберіть параметр.	
	ESP	Виберіть цей варіант для забезпечення цілісності автентифікації та даних, а також для шифрування даних.
	AH	Виберіть цей варіант для забезпечення цілісності автентифікації та даних. IPsec можна використовувати навіть у разі забороненого шифрування даних.
Algorithm Settings		

Розширені параметри безпеки для підприємства

Налаштування	Налаштування та пояснення	
IKE	Encryption	Виберіть алгоритм шифрування для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
	Authentication	Виберіть алгоритм автентифікації для IKE.
	Key Exchange	Виберіть алгоритм обміну ключами для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
ESP	Encryption	Виберіть алгоритм шифрування для ESP. Воно доступне, коли **ESP** вибрано для **Security Protocol**.
	Authentication	Виберіть алгоритм автентифікації для ESP. Воно доступне, коли **ESP** вибрано для **Security Protocol**.
AH	Authentication	Виберіть алгоритм шифрування для AH. Воно доступне, коли **AH** вибрано для **Security Protocol**.

Пов'язані відомості

➡ «Налаштування Default Policy» на сторінці 72

Налаштування Group Policy

1. Відкрийте Web Config і виберіть **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Натисніть вкладку з номером, у якій необхідно виконати налаштування.
3. Введіть значення для кожного елемента.
4. Натисніть **Next**.

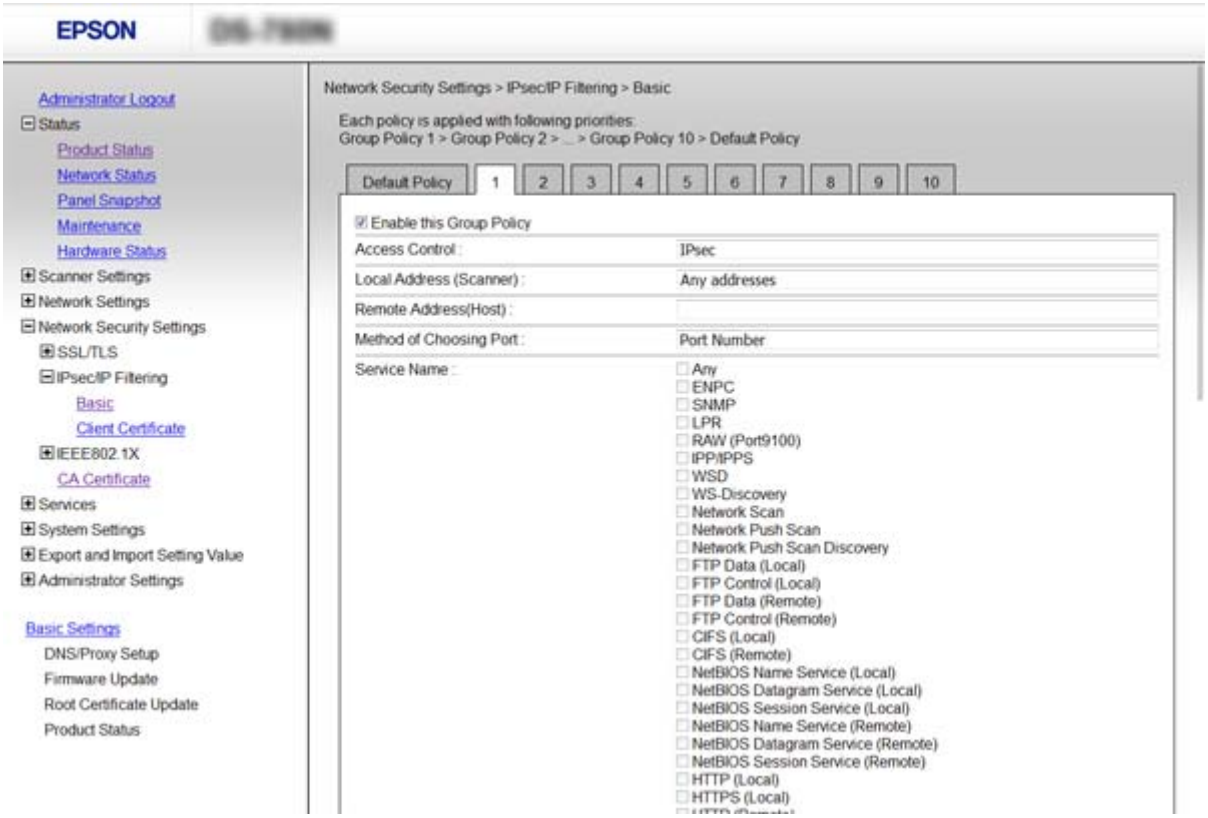
   Відобразиться повідомлення про підтвердження.
5. Натисніть **OK**.

   Сканер буде оновлено.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23
➡ «Параметри Group Policy» на сторінці 76

Параметри Group Policy



Налаштування	Налаштування та пояснення	
Enable this Group Policy	Групову політику можна ввімкнути або вимкнути.	
Access Control	Налаштуйте спосіб керування для трафіку або пакетів IP.	
	Permit Access	Виберіть це, щоб дозволити проходження налаштованих пакетів IP.
	Refuse Access	Виберіть це, щоб заборонити проходження налаштованих пакетів IP.
	IPsec	Виберіть це, щоб дозволити проходження налаштованих пакетів IPsec.
Local Address (Scanner)	Виберіть адресу IPv4 або IPv6, яка відповідає мережевому середовищу. Якщо IP-адреса призначається автоматично, можна вибрати параметр **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Введіть IP-адресу пристрою для керування доступом до нього. Довжина IP-адреси має складати до 43 символів. Якщо не ввести IP-адресу, контролюватимуться всі адреси. ***Примітка.*** *Якщо IP-адреса призначається автоматично (наприклад, протоколом DHCP), зв'язок може бути відсутнім. Установіть статичну IP-адресу.*	
Method of Choosing Port	Виберіть метод указання портів.	
Service Name	Щоб вибрати **Service Name** для **Method of Choosing Port**, виберіть один з варіантів.	

Розширені параметри безпеки для підприємства

Налаштування	Налаштування та пояснення	
Transport Protocol	Щоб вибрати **Port Number** для **Method of Choosing Port**, необхідно налаштувати режим інкапсуляції.	
	Any Protocol	Виберіть це, щоб контролювати всі типи протоколів.
	TCP	Виберіть це, щоб контролювати дані одноадресних передавань.
	UDP	Виберіть це, щоб контролювати дані широкомовних і багатоадресних передавань.
	ICMPv4	Виберіть це, щоб контролювати команду перекидання.
Local Port	Якщо вибрати значення **Port Number** для параметра **Method of Choosing Port** та якщо вибрати протокол **TCP** або **UDP** для параметра **Transport Protocol**, необхідно ввести номери портів для керування отриманням пакетів, відокремлюючи їх комами. Можна вказати до 10 номерів портів. Наприклад, 20,80,119,5220 Якщо не ввести номери портів, усі порти контролюватимуться.	
Remote Port	Якщо вибрати значення **Port Number** для параметра **Method of Choosing Port** та якщо вибрати протокол **TCP** або **UDP** для параметра **Transport Protocol**, необхідно ввести номери портів для керування надсиланням пакетів, відокремлюючи їх комами. Можна вказати до 10 номерів портів. Наприклад, 25,80,143,5220 Якщо не ввести номери портів, усі порти контролюватимуться.	
IKE Version	Виберіть IKEv1 або IKEv2 для версії IKE. Виберіть одне зі значень відповідно до пристрою, до якого підключено сканер.	
IKEv1	Вказані нижче елементи відображаються, якщо вибрати **IKEv1** для **IKE Version**.	
	Authentication Method	Щоб вибрати **IPsec** для **Access Control**, виберіть один з варіантів. Сертифікат, що використовується, має однакові параметри із сертифікатом політики за замовчуванням.
	Pre-Shared Key	Щоб вибрати **Pre-Shared Key** для **Authentication Method**, введіть спільний ключ довжиною від 1 до 127 символів.
	Confirm Pre-Shared Key	Введіть установлений ключ для підтвердження.
IKEv2	Вказані нижче елементи відображаються, якщо вибрати **IKEv2** для **IKE Version**.	

Розширені параметри безпеки для підприємства

Налаштування	Налаштування та пояснення	
Local	Authentication Method	Щоб вибрати **IPsec** для **Access Control**, виберіть один з варіантів. Сертифікат, що використовується, має однакові параметри із сертифікатом політики за замовчуванням.
	ID Type	Виберіть тип ідентифікатора для сканера.
	ID	Введіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Distinguished Name**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «=». **IP Address**: Введіть формат IPv4 або IPv6. **FQDN**: Введіть комбінацію від 1 до 255 символів, використовуючи символи A – Z, a – z, 0 – 9, «-» та крапку (.). **Email Address**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «@». **Key ID**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E).
	Pre-Shared Key	Щоб вибрати **Pre-Shared Key** для **Authentication Method**, введіть спільний ключ довжиною від 1 до 127 символів.
	Confirm Pre-Shared Key	Введіть установлений ключ для підтвердження.
Remote	Authentication Method	Щоб вибрати **IPsec** для **Access Control**, виберіть один з варіантів. Сертифікат, що використовується, має однакові параметри із сертифікатом політики за замовчуванням.
	ID Type	Виберіть тип ідентифікатора для пристрою, який ви бажаєте автентифікувати.
	ID	Введіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Distinguished Name**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «=». **IP Address**: Введіть формат IPv4 або IPv6. **FQDN**: Введіть комбінацію від 1 до 255 символів, використовуючи символи A – Z, a – z, 0 – 9, «-» та крапку (.). **Email Address**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E). Потрібно включити «@». **Key ID**: Введіть від 1 до 128 1-байтних символів ASCII (0x20 – 0x7E).
	Pre-Shared Key	Щоб вибрати **Pre-Shared Key** для **Authentication Method**, введіть спільний ключ довжиною від 1 до 127 символів.
	Confirm Pre-Shared Key	Введіть установлений ключ для підтвердження.

Розширені параметри безпеки для підприємства

Налаштування	Налаштування та пояснення	
Encapsulation	Щоб вибрати **IPsec** для **Access Control**, необхідно налаштувати режим інкапсуляції.	
	Transport Mode	Виберіть це, якщо сканер використовується в одній локальній мережі. Шифруватимуться пакети IP рівня 4 або вище.
	Tunnel Mode	Виберіть цей параметр, якщо сканер використовується в мережі з можливістю підключення до Інтернету, наприклад IPsec-VPN. Шифруватимуться заголовки та дані пакетів IP.
Remote Gateway(Tunnel Mode)	Щоб вибрати **Tunnel Mode** для **Encapsulation**, введіть адресу шлюзу довжиною від 1 до 39 символів.	
Security Protocol	Щоб вибрати **IPsec** для **Access Control**, виберіть один з варіантів.	
	ESP	Виберіть цей варіант для забезпечення цілісності автентифікації та даних, а також для шифрування даних.
	AH	Виберіть цей варіант для забезпечення цілісності автентифікації та даних. IPsec можна використовувати навіть у разі забороненого шифрування даних.
Algorithm Settings		
IKE	Encryption	Виберіть алгоритм шифрування для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
	Authentication	Виберіть алгоритм автентифікації для IKE.
	Key Exchange	Виберіть алгоритм обміну ключами для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
ESP	Encryption	Виберіть алгоритм шифрування для ESP. Воно доступне, коли **ESP** вибрано для **Security Protocol**.
	Authentication	Виберіть алгоритм автентифікації для ESP. Воно доступне, коли **ESP** вибрано для **Security Protocol**.
AH	Authentication	Виберіть алгоритм автентифікації для AH. Воно доступне, коли **AH** вибрано для **Security Protocol**.

Пов'язані відомості

➡ «Налаштування Group Policy» на сторінці 75

➡ «Поєднання адрес Local Address (Scanner) та Remote Address(Host) у поілтиці Group Policy» на сторінці 80

➡ «Довідник назви служби відповідно до групової політики» на сторінці 80

Поєднання адрес Local Address (Scanner) та Remote Address(Host) у поілтиці Group Policy

		Налаштування параметра Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Налаштування параметра Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Пуста	✓	✓	✓

*1 Якщо вибрано **IPsec** для параметра **Access Control**, не можна вказати довжину префікса.

*2 Якщо вибрано функцію **IPsec** для параметра **Access Control**, можна вибрати адресу локального зв'язку (fe80::), але групову політику буде вимкнено.

*3 Крім адрес локального зв'язку IPv6.

Довідник назви служби відповідно до групової політики

Примітка.
Недоступні служби відображаються, але їх не можна вибрати.

Назва служби	Тип протоколу	Номер локального порту	Номер віддаленого порту	Доступні функції
Any	–	–	–	Усі служби
ENPC	UDP	3289	Будь-який порт	Пошук сканера з таких програм як EpsonNet Config, драйвера принтера та драйвера сканера
SNMP	UDP	161	Будь-який порт	Отримання та конфігурація MIB-об'єкта з таких програм як EpsonNet Config і драйвера сканера Epson
WSD	TCP	Будь-який порт	5357	Керування WSD
WS-Discovery	UDP	3702	Будь-який порт	Пошук сканера через порт WSD
Network Scan	TCP	1865	Будь-який порт	Пересилання даних сканування з Document Capture Pro
Network Push Scan Discovery	UDP	2968	Будь-який порт	Пошук комп'ютера зі сканера.
Network Push Scan	TCP	Будь-який порт	2968	Отримання відомостей про завдання з програми Document Capture Pro або Document Capture
HTTP (Local)	TCP	80	Будь-який порт	Сервер HTTP(S) (пересилання даних Web Config та WSD)
HTTPS (Local)	TCP	443	Будь-який порт	

Назва служби	Тип протоколу	Номер локального порту	Номер віддаленого порту	Доступні функції
HTTP (Remote)	TCP	Будь-який порт	80	Клієнт HTTP(S) (зв'язок між оновленням мікропрограм і оновленням кореневого сертифікату)
HTTPS (Remote)	TCP	Будь-який порт	443	

Приклади налаштування функції IPsec/IP Filtering

Отримання лише пакетів IPsec

Цей приклад демонструє налаштування лише політики за замовчуванням.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: введіть до 127 символів.

Group Policy:

Не налаштовувати.

Приймання сканування за допомогою Epson Scan 2 та налаштувань сканера

Цей приклад демонструє зв'язок між даними сканування та конфігурацією сканера з указаних пристроїв.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: установіть прапорець.

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

❏ **Remote Address(Host)**: IP-адреса клієнта

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

❏ **Service Name**: установіть прапорець **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** та **HTTPS (Local)**.

Отримання дозволу на доступ лише з указаної IP-адреси

У цьому прикладі демонструється дозвіл доступу до сканера із зазначеної IP-адреси.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: установіть прапорець.

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

❏ **Remote Address(Host)**: IP-адреса клієнта адміністратора

Примітка.
Незалежно від параметрів політики клієнт матиме можливість доступу до сканера та його налаштувань.

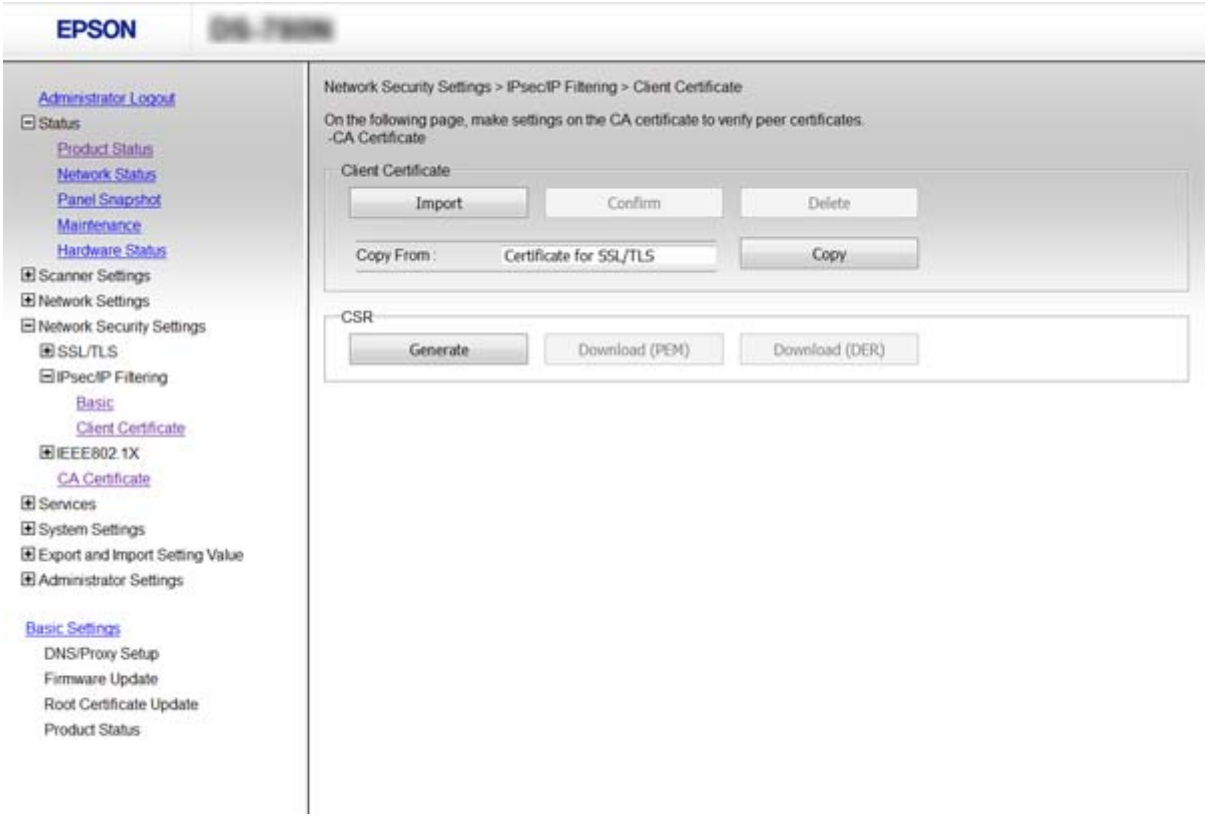
Налаштування сертифіката для IPsec/IP Filtering

Змініть конфігурацію сертифіката клієнта для IPsec/IP-фільтрування. Якщо потрібно змінити конфігурацію центру сертифікації, перейдіть до **CA Certificate**.

1. Відкрийте Web Config і виберіть **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Імпортуйте сертифікат у **Client Certificate**.

   Якщо ви вже імпортували сертифікат, опублікований Центром сертифікації, у IEEE802.1X або SSL/TLS, можна скопіювати його та використовувати для IPsec/IP-фільтрування. Щоб скопіювати, виберіть сертифікат із **Copy From**, а тоді натисніть **Copy**.



Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Отримання та імпорт сертифіката, підписаного ЦС» на сторінці 64

Використання протоколу SNMPv3

Про SNMPv3

SNMP — це протокол, який виконує моніторинг та контроль для збору інформації про пристрої, які підключені до мережі. SNMPv3 — це удосконалена версія функції безпеки.

У разі використання SNMPv3 моніторинг стану та налаштування змін до (пакету) з'єднання SNMP може відбуватися за умови автентифікації та шифрування для захисту (пакету) з'єднання SNMP від ризиків мережі, таких як підслуховування телефонних розмов, маскування під законного користувача або зловмисне втручання в систему.

Налаштування протоколу SNMPv3

Якщо принтер підтримує протокол SNMPv3, можна відстежувати доступи до сканера й керувати ними.

1. Відкрийте Web Config і виберіть **Services** > **Protocol**.
2. Введіть значення для кожного елемента налаштувань **SNMPv3 Settings**.
3. Натисніть **Next**.

   Відобразиться повідомлення про підтвердження.
4. Натисніть **OK**.

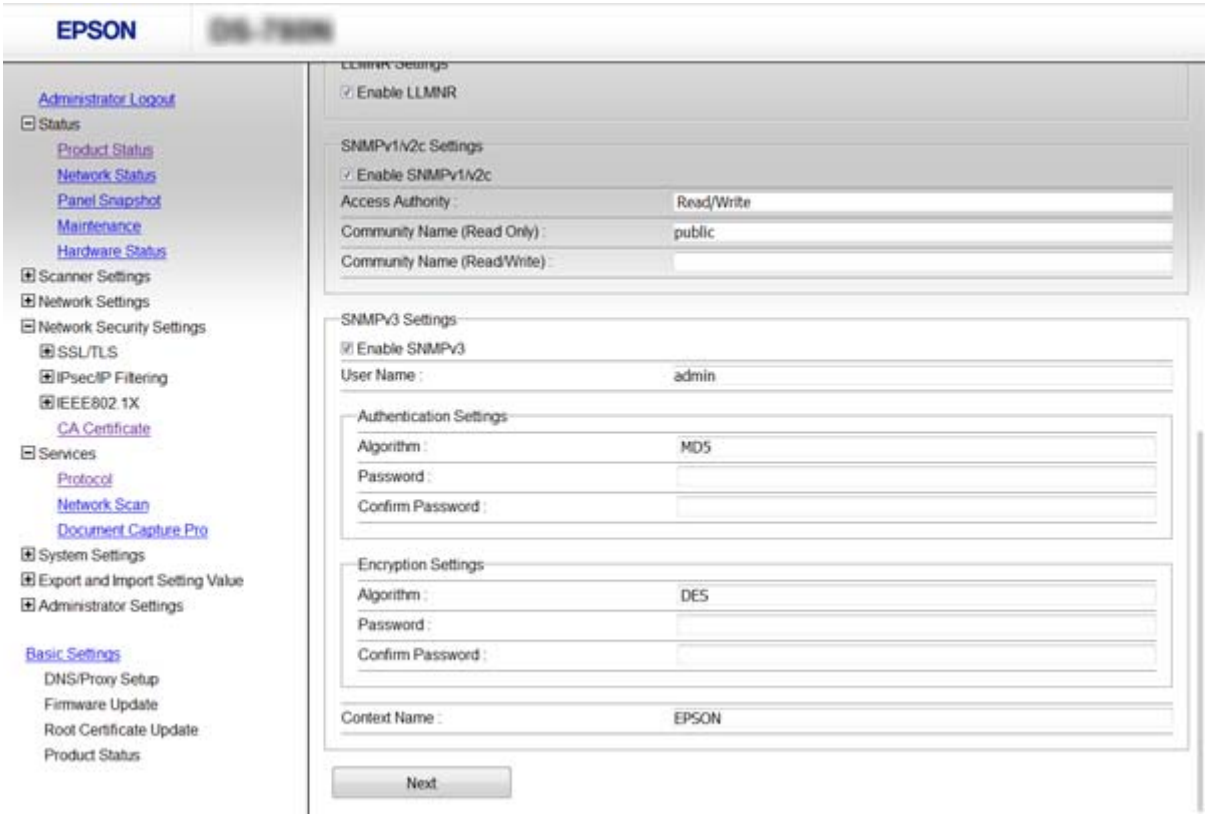
   Сканер буде оновлено.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Елементи налаштування SNMPv3» на сторінці 84

Елементи налаштування SNMPv3



Елементи	Налаштування та пояснення
Enable SNMPv3	SNMPv3 увімкнено, якщо встановлено прапорець.
User Name	Введіть від 1 до 32 символів, використовуючи 1-байтові символи.
Authentication Settings	
Algorithm	Виберіть алгоритм для здійснення автентифікації.
Password	Введіть від 8 до 32 символів формату ASCII (0x20-0x7E).
Confirm Password	Введіть пароль, налаштований для підтвердження.
Encryption Settings	
Algorithm	Виберіть алгоритм для здійснення шифрування.
Password	Введіть від 8 до 32 символів формату ASCII (0x20-0x7E).
Confirm Password	Введіть пароль, налаштований для підтвердження.
Context Name	Введіть від 1 до 32 символів, використовуючи 1-байтові символи.

Пов’язані відомості

➡ «Налаштування протоколу SNMPv3» на сторінці 83

Підключення сканера до мережі IEEE802.1X

Налаштування мережі IEEE802.1X

Якщо сканер підтримує стандарт IEEE802.1X, його можна використовувати в мережі з автентифікацією, підключеній до RADIUS-сервера з концентратором, що виконує роль автентифікатора.

1. Відкрийте Web Config і виберіть **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Введіть значення для кожного елемента.
3. Клацніть **Next**.

   Відобразиться повідомлення про підтвердження.
4. Клацніть **OK**.

   Сканер буде оновлено.

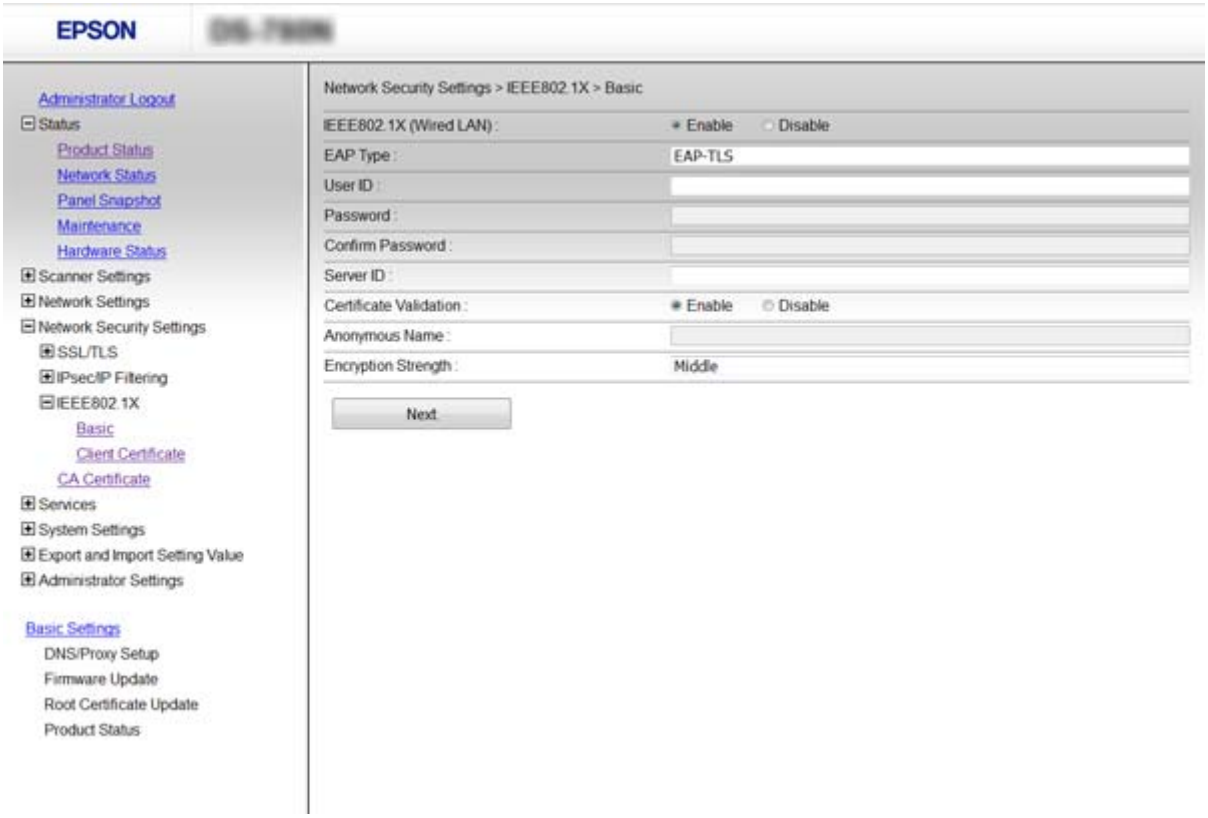
Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Параметри мережі IEEE802.1X» на сторінці 86

➡ «Якщо не вдається отримати доступ до принтера або сканера після налаштування IEEE802.1X» на сторінці 91

Параметри мережі IEEE802.1X



Налаштування	Налаштування та пояснення	
IEEE802.1X (Wired LAN)	Можна ввімкнути або вимкнути налаштування сторінки (**IEEE802.1X** > **Basic**) для IEEE802.1X (дротова мережа LAN).	
EAP Type	Виберіть спосіб автентифікації між сканером і сервером RADIUS.	
	EAP-TLS	Отримайте та імпортуйте сертифікат, підписаний ЦС.
	PEAP-TLS	
	PEAP/MSCHAPv2	Установіть пароль.
User ID	Налаштуйте ідентифікатор, який використовуватиметься для автентифікації сервера RADIUS. Введіть від 1 до 128 1-байтних символів ASCII (від 0x20 до 0x7E).	
Password	Установіть пароль для автентифікації сканера. Введіть від 1 до 128 1-байтних символів ASCII (від 0x20 до 0x7E). У разі використання сервера Windows як RADIUS-сервера можна ввести до 127 символів.	
Confirm Password	Введіть установлений пароль для підтвердження.	
Server ID	Можна налаштувати ідентифікатор сервера для автентифікації на зазначеному сервері RADIUS. Автентифікатор перевіряє, чи міститься ідентифікатор сервера в полі subject/subjectAltName сертифіката сервера, який надсилається з RADIUS-сервера. Введіть від 0 до 128 1-байтних символів ASCII (від 0x20 до 0x7E).	

Розширені параметри безпеки для підприємства

Налаштування	Налаштування та пояснення	
Certificate Validation	Незалежно від методу автентифікації можна встановити перевірку сертифіката. Імпортуйте сертифікат у **CA Certificate**.	
Anonymous Name	Якщо вибрати **PEAP-TLS** або **PEAP/MSCHAPv2** для **Authentication Method**, ідентифікатор користувача для 1 фази PEAP-автентифікації можна залишити невизначеним. Введіть від 0 до 128 1-байтних символів ASCII (від 0x20 до 0x7E).	
Encryption Strength	Можна вибрати одне з наступних значень.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Пов'язані відомості

➡ «Налаштування мережі IEEE802.1X» на сторінці 85

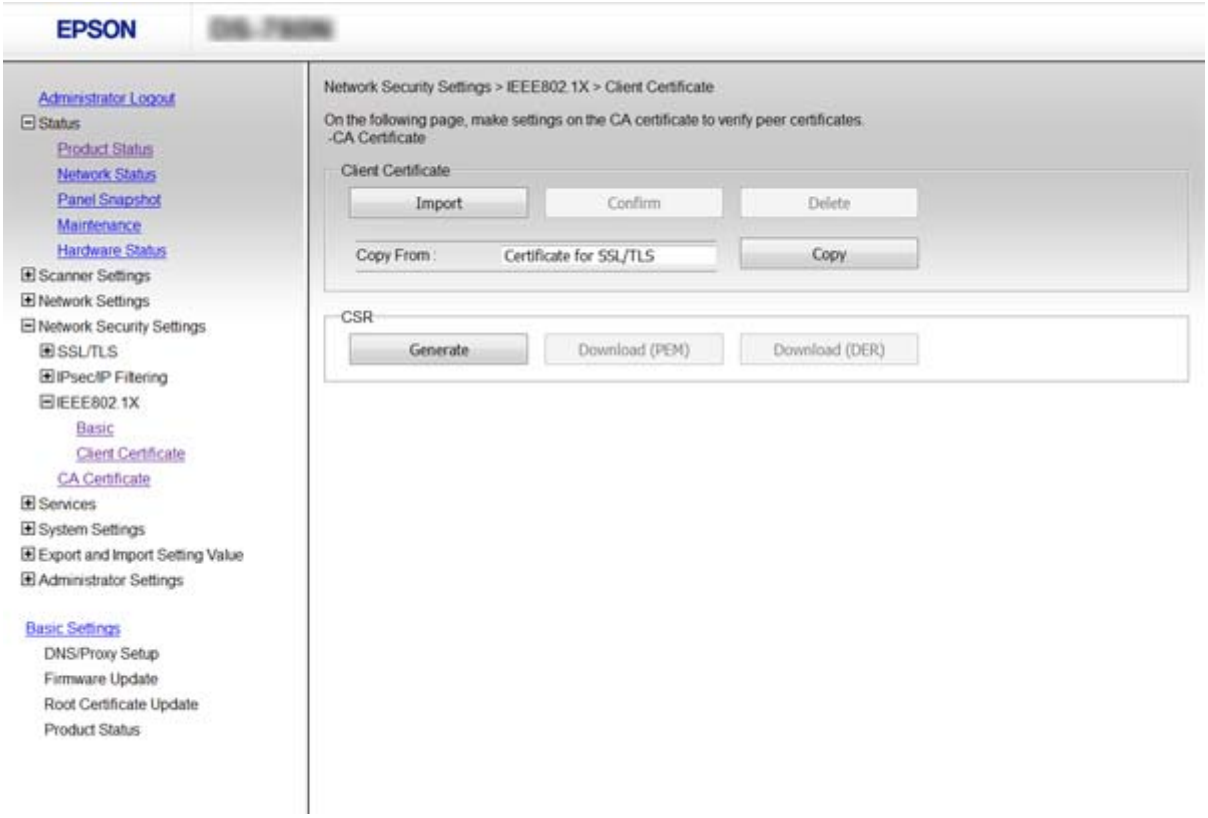
Налаштування сертифіката для IEEE802.1X

Змініть конфігурацію сертифікату клієнта для IEEE802.1X. Якщо потрібно змінити конфігурацію сертифіката від центру сертифікації, перейдіть до **CA Certificate**.

1. Відкрийте Web Config і виберіть **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. Введіть сертифікат у **Client Certificate**.

   Можна скопіювати сертифікат, якщо його опубліковано Центром сертифікації. Щоб скопіювати, виберіть сертифікат із **Copy From**, а тоді натисніть **Copy**.



Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Отримання та імпорт сертифіката, підписаного ЦС» на сторінці 64

Вирішення проблем розширеного захисту

Відновлення функцій безпеки

У разі встановлення середовища з високим рівнем захисту, наприклад із фільтруванням за IPsec/IP або IEEE802.1X, можуть виникнути труднощі зі зв'язком з іншими пристроями через неправильні налаштування або проблеми на пристрої чи сервері. У такому випадку відновіть налаштування безпеки, щоб внести нові або щоб тимчасово скористатися пристроєм.

Вимкнення функції безпеки за допомогою панелі керування

Вимкнути фільтрацію за IPsec/IP або IEEE802.1X можна на панелі керування сканера.

1. Натисніть **Налаш.** > **Налаштування мережі**.

2. Натисніть **Змінити налаштування**.
3. Виберіть елементи, які потрібно вимкнути.
   - ❏ **IPsec/фільтрування IP**
   - ❏ **IEEE802.1X**
4. Коли з'явиться повідомлення про завершення, натисніть **Продовж.**.

Відновлення функції безпеки за допомогою Web Config

Для стандарту IEEE802.1X, пристрої можуть не розпізнаватися в мережі. У такому разі вимкніть функцію на панелі керування сканера.

Для фільтрування за IPsec/IP можна вимкнути функцію, якщо ви можете відкрити пристрій з комп'ютера.

Вимкнення фільтрування IPsec/IP за допомогою Web Config

1. Відкрийте Web Config та виберіть **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Виберіть **Disable** для **IPsec/IP Filtering** у **Default Policy**.
3. Клацніть **Next**, а тоді зніміть прапорець **Enable this Group Policy** для всіх правил групи.
4. Клацніть **OK**.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Проблеми з використанням функцій безпеки мережі

Якщо ви забули спільний ключ

Знову налаштуйте ключ за допомогою Web Config.

Щоб змінити ключ, відкрийте Web Config і виберіть **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** або **Group Policy**.

Після зміни спільного ключа налаштуйте його для комп'ютерів.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

Не вдається встановити зв'язок IPsec

Можливо, використовується непідтримуваний алгоритм налаштувань комп'ютера?

Сканер підтримує такі алгоритми.

Методи безпеки	Алгоритми
Алгоритм шифрування IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Алгоритм автентифікації IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Алгоритм обміну ключами IKE	група DH 1, група DH 2, група DH 5, група DH 14, група DH 15, група DH 16, група DH 17, група DH 18, група DH 19, група DH 20, група DH 21, група DH 22, група DH 23, група DH 24, група DH 25, група DH 26, група DH 27*, група DH 28*, група DH 29*, група DH 30*
Алгоритм шифрування ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Алгоритм автентифікації ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Алгоритм автентифікації AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* доступно тільки для IKEv2

Пов'язані відомості

➡ «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 71

Раптове переривання зв'язку

Можливо, IP-адреса сканера недійсна або змінилася?

Вимкніть IPsec за допомогою панелі керування сканера.

Якщо термін DHCP зійшов, термін перезавантаження або адреси IPv6 минув чи не був отриманий, то IP-адресу, зареєстровану для Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) сканера, може бути неможливо знайти.

Використовуйте статичну IP-адресу.

Можливо, IP-адреса комп'ютера недійсна або змінилася?

Вимкніть IPsec за допомогою панелі керування сканера.

Якщо термін DHCP зійшов, термін перезавантаження або адреси IPv6 минув чи не був отриманий, то IP-адресу, зареєстровану для Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) сканера, може бути неможливо знайти.

Використовуйте статичну IP-адресу.

Пов'язані відомості

➡ «Доступ до налаштувань Web Config» на сторінці 23

➡ «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 71

Не вдається підключитися після зміни конфігурації IPsec/IP-фільтрування

Встановлене значення може бути неправильним.

Вимкніть IPsec/фільтрацію за IP на панелі керування сканера. Підключіть сканер до комп'ютера та повторно налаштуйте IPsec/фільтрацію за IP.

Пов'язані відомості

➡ «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 71

Якщо не вдається отримати доступ до принтера або сканера після налаштування IEEE802.1X

Налаштування можуть бути неправильними.

Вимкніть IEEE802.1X на панелі керування сканера. Підключіть сканер до комп'ютера та повторно налаштуйте з'єднання IEEE802.1X.

Пов'язані відомості

➡ «Налаштування мережі IEEE802.1X» на сторінці 85

Проблеми з використанням цифрового сертифіката

Не вдається імпортувати сертифікат, підписаний ЦС

Чи відповідає сертифікат ЦС даним у ЗПС?

Якщо сертифікат, підписаний ЦС, і ЗПС містять різні дані, ЗПС не можна буде імпортувати. Перевірте наступне:

❏ Можливо, ви намагаєтесь імпортувати сертифікат на пристрій, дані якого відрізняються?

Перевірте дані, зазначені у ЗПС, а потім імпортуйте сертифікат на пристрій з тими самими даними.

❏ Можливо, ЗПС, збережений на сканері, було перезаписано після відправлення ЗПС до ЦС?

Використайте ЗПС для отримання нового сертифіката, підписаного ЦС.

Чи не перевищує розмір сертифіката, підписаного ЦС, 5 КБ?

Неможливо імпортувати сертифікат ЦС, розмір якого перевищує 5 КБ.

Чи правильний пароль вказано для імпорту сертифіката?

Неможливо імпортувати сертифікат без пароля.

Пов'язані відомості

➡ «Імпортування сертифіката, підписаного ЦС» на сторінці 66

Не вдається оновити сертифікат із власним підписом

Чи було введено Common Name?

Common Name має бути введено.

Чи містить Common Name непідтримувані символи? Наприклад, японські символи не підтримуються.

Введіть від 1 до 128 символів формату IPv4, IPv6, FQDN або імені хосту в кодуванні ASCII (0x20-0x7E).

Чи містить Common Name коми або пробіли?

Кома розділяє **Common Name** на частини. Якщо перед комою або після неї є пробіл, виникне помилка.

Пов'язані відомості

➡ «Оновлення сертифіката із власним підписом» на сторінці 68

Не вдається створити ЗПС

Чи було введено Common Name?

Common Name має бути введено.

Чи містить Common Name, Organization, Organizational Unit, Locality, State/Province непідтримувані символи? Наприклад, японські символи не підтримуються.

Введіть символи формату IPv4, IPv6, FQDN кодування ASCII (0x20-0x7E) або імені хосту.

Чи містить Common Name коми або пробіли?

Кома розділяє **Common Name** на частини. Якщо перед комою або після неї є пробіл, виникне помилка.

Пов'язані відомості

➡ «Отримання сертифіката, підписаного ЦС» на сторінці 64

Дії в разі появи попередження стосовно цифрового сертифіката

Повідомлення	Причини/Дії
Enter a Server Certificate.	**Причина:** Не вибрано файл для імпорту. **Дія:** Виберіть файл і натисніть **Import**.
CA Certificate 1 is not entered.	**Причина:** 1-ий сертифікат ЦС не введено, введено лише 2-ий сертифікат ЦС. **Дія:** Спочатку імпортуйте 1-ий сертифікат ЦС.

Розширені параметри безпеки для підприємства

Повідомлення	Причини/Дії
Invalid value below.	**Причина:** Шлях до файлу та/або пароль містить непідтримувані символи. **Дія:** Переконайтесь, що введено правильні символи.
Invalid date and time.	**Причина:** Дата й час сканера не встановлені. **Дія:** Установіть дату та час за допомогою налаштувань Web Config або EpsonNet Config.
Invalid password.	**Причина:** Пароль, встановлений для сертифіката ЦС, і введений пароль відрізняються. **Дія:** Введіть правильний пароль.
Invalid file.	**Причина:** Файл імпортується не у форматі X509. **Дія:** Переконайтеся, що обираєте правильний сертифікат, надісланий довіреним Центром сертифікації.
	Причина: Імпортований файл має завеликий розмір. Максимальний розмір файлу — 5 КБ. **Дія:** Якщо вибрано правильний файл, сертифікат може бути пошкодженим або сфабрикованим.
	Причина: Ланцюжок, що міститься в сертифікаті, недійсний. **Дія:** Щоб отримати більше інформації про сертифікат, завітайте на веб-сайт Центру сертифікації.
Cannot use the Server Certificates that include more than three CA certificates.	**Причина:** Файл сертифіката формату PKCS#12 містить більше 3 сертифікатів ЦС. **Дія:** Імпортуйте кожний сертифікат через конвертацію формату PKCS#12 у формат PEM або імпортуйте файл сертифіката у форматі PKCS#12, що містить до 2 сертифікатів ЦС.

Повідомлення	Причини/Дії
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Причина:** Сертифікат застарілий. **Дія:** ❏ Якщо сертифікат застарілий, отримайте та імпортуйте новий сертифікат. ❏ Якщо строк дії сертифіката насправді не вичерпано, перевірте, чи правильно встановлені дата й час сканера.
Private key is required.	**Причина:** Сертифікат не має парного закритого ключа. **Дія:** ❏ Якщо сертифікат має формат PEM/DER, а отримано його через подання ЗПС із комп'ютера, укажіть файл закритого ключа. ❏ Якщо сертифікат має формат PKCS#12, а отримано його через подання ЗПС із комп'ютера, створіть файл, що містить закритий ключ.
	Причина: Сертифікат формату PEM/DER, отриманий через подання ЗПС із налаштувань Web Config, повторно імпортовано. **Дія:** Якщо сертифікат має формат PEM/DER, а отримано його через подання ЗПС із налаштувань Web Config, імпортувати його можна лише раз.
Setup failed.	**Причина:** Налаштування не може бути завершено через помилку зв'язку між сканером і комп'ютером або помилку читання файлу. **Дія:** Після перевірки файлу та зв'язку спробуйте здійснити імпорт ще раз.

Пов'язані відомості

➡ «Про цифрову сертифікацію» на сторінці 63

Сертифікат, підписаний ЦС, було помилково видалено

Чи маєте ви резервний файл для сертифіката?

Якщо у вас є резервний файл, імпортуйте сертифікат іще раз.

У разі отримання сертифіката за ЗПС, створеним через Web Config, імпортувати видалений сертифікат ще раз буде неможливо. Створіть ЗПС та отримайте новий сертифікат.

Пов'язані відомості

➡ «Видалення сертифіката, підписаного ЦС» на сторінці 68

➡ «Імпортування сертифіката, підписаного ЦС» на сторінці 66