EPSON
EXCEED YOUR VISION

DS-790WN

Посібник адміністратора

NPD6726-00 UK

Авторські права

Зміст цієї інструкції та характеристики цього продукту можуть бути змінені без попереднього повідомлення.

Торгові марки

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION і їхні логотипи є зареєстрованими товарними знаками або товарними знаками Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa та PaSoRi є зареєстрованими торговими марками корпорації Sony.
- ❏ MIFARE є зареєстрованою торговою маркою NXP Semiconductor Corporation.
- ❏ Загальне зауваження: інші назви продуктів, використані тут, призначені лише для ідентифікації та можуть бути товарними знаками відповідних власників. Компанія Epson відмовляється від усіх прав на ці товарні знаки.

Зміст

Базові налаштування безпеки

Розширені налаштування безпеки

Налаштування автентифікації

Обслуговування

Вступ

Зміст документу

Цей документ містить наступну інформацію для адміністраторів сканерів.

❏ Параметри мережі

❏ Підготовка функції сканування

❏ Увімкнення й керування налаштуваннями безпеки

❏ Увімкнення й керування Налаштування автентифікації

❏ Виконання щоденного технічного обслуговування

Стандартні методи використання сканера викладено у *Посібник користувача*.

Примітка.
У цьому документі пояснюються Налаштування автентифікації, які забезпечують незалежну автентифікацію без використання сервера аутентифікації. На додаток до Налаштування автентифікації, викладених у цьому посібнику, ви також можете створити систему автентифікації за допомогою сервера автентифікації. Для цього скористайтеся Document Capture Pro Server Authentication Edition (скорочена назва — Document Capture Pro Server AE).

Для отримання додаткової інформації зверніться до місцевого представництва Epson.

Використання цього керівництва

Позначки та символи

> ***Застереження.***
> *Вказівки, яких необхідно ретельно дотримуватись, щоб уникнути травмування.*

> ***Важливо***
> *Вказівки, яких необхідно дотримуватись, щоб уникнути пошкодження пристрою.*

Примітка.
Надає додаткову та довідкову інформацію.

Пов'язані відомості

➡ Посилання, що пов'язані з розділами.

Описи, що використовуються в цьому посібнику

❏ Подані тут знимки екранів зроблені у програмах на ОС Windows 10 або macOS High Sierra. Відображений на екрані вміст може відрізнятися в залежності від моделі пристрою та ситуації.

❏ Використані тут ілюстрації подаються тільки для довідки. Способи керування пристроєм однакові, хоча вони можуть злегка відрізнятися від фактичного функціонування продукту.

Довідка щодо операційної системи

Windows

У цьому посібнику терміни «Windows 10», «Windows 8.1», «Windows 8», «Windows 7», «Windows Server 2019», «Windows Server 2016», «Windows Server 2012 R2», «Windows Server 2012» та «Windows Server 2008 R2» відносяться до операційних систем, перелічених нижче. Крім цього, термін «Windows» використовується для позначення всіх версій, а термін «Windows Server» використовується для позначення «Windows Server 2019», «Windows Server 2016», «Windows Server 2012 R2», «Windows Server 2012» і «Windows Server 2008 R2».

- ❏ Операційна система Microsoft® Windows® 10
- ❏ Операційна система Microsoft® Windows® 8.1
- ❏ Операційна система Microsoft® Windows® 8
- ❏ Операційна система Microsoft® Windows® 7
- ❏ Операційна система Microsoft® Windows Server® 2019
- ❏ Операційна система Microsoft® Windows Server® 2016
- ❏ Операційна система Microsoft® Windows Server® 2012 R2
- ❏ Операційна система Microsoft® Windows Server® 2012
- ❏ Операційна система Microsoft® Windows Server® 2008 R2

Mac OS

У цьому посібнику термін «Mac OS» використовується для позначення macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan та OS X Yosemite.

Необхідні налаштування для ваших потреб

Необхідні налаштування для ваших потреб

Перегляньте наведені нижче параметри, аби виконати необхідні налаштування відповідно до ваших потреб.

Підключення сканера до мережі

Мета	Необхідні налаштування
Я хочу підключити сканер до мережі.	Налаштуйте сканер для мережевого сканування. «Підключення сканера до мережі» на сторінці 14
Я хочу підключити сканер до нового комп'ютера.	Налаштуйте на новому комп'ютері параметри мережі для вашого сканера. «Додавання або заміна комп'ютера або пристроїв» на сторінці 21

Налаштування для сканування

Мета	Необхідні налаштування
Я хочу надсилати скановані зображення електронною поштою. (Сканувати в ел. пошту)	1. Налаштуйте сервер електронної пошти, який ви бажаєте підключити. «Налаштування поштового сервера» на сторінці 43 2. Зареєструйте адресу електронної пошти одержувача в **Контакти** (необов'язково). Зареєструвавши адресу електронної пошти один раз, вам не потрібно вводити її щоразу, коли ви хочете щось надіслати, — ви можете просто вибрати її зі своїх Контактів. «Відкриття доступу до контактів» на сторінці 65
Я хочу зберігати відсканові зображення в папку у мережі. (Сканувати в мережеву папку/FTP)	1. Створіть у мережі папку, куди ви бажаєте зберігати зображення. «Налаштування спільної мережевої папки» на сторінці 46 2. Зареєструйте шлях до папки в **Контакти** (необов'язково). Зареєструвавши шлях до папки один раз, вам не потрібно вводити її щоразу, коли ви хочете щось надіслати, — ви можете просто вибрати її зі своїх Контактів. «Відкриття доступу до контактів» на сторінці 65
Я хочу зберігати відсканові зображення в хмарній службі. (Сканувати в «хмарний» сервіс)	Налаштуйте Epson Connect. Див. докладнішу інформацію про налаштування на порталі веб-сайту Epson Connect. Під час налаштування вам знадобиться обліковий запис користувача для служби онлайн-сховища, до якої ви бажаєте підключитися. https://www.epsonconnect.com/ http://www.epsonconnect.eu (тільки для Європи)

Настроювання відображення панелі керування

Мета	Необхідні налаштування
Я хочу змінити елементи, що відображаються на панелі керування сканера.	Встановіть **Налашт** або **Редагувати Головний екран**. Ви можете зареєструвати бажані налаштування сканування на панелі керування й редагувати відображувані елементи. «Настроювання відображення панелі керування» на сторінці 79

Налаштування основних функцій безпеки

Мета	Необхідні налаштування
Я хочу заборонити усім можливим користувачам (окрім адміністратора) змінювати налаштування сканера.	Встановіть для сканера пароль адміністратора. «Налаштування адміністратора» на сторінці 88
Я хочу вимкнути можливість використання сканерів з USB-з'єднаннями.	Вимкніть зовнішній інтерфейс. «Вимикання зовнішнього інтерфейсу» на сторінці 94

Налаштування розширених функцій безпеки

Мета	Необхідні налаштування
Я хочу контролювати, які протоколи використовуватимуться.	Увімкніть або вимкніть протоколи. «Керування протоколами використання» на сторінці 100
Я хочу зашифрувати шлях комунікації.	1. Налаштуйте свій цифровий сертифікат. «Використання цифрового сертифіката» на сторінці 103 2. Налаштуйте з'єднання за протоколом SSL/TLS. «Зв'язок SSL/TLS зі сканером» на сторінці 109
Я хочу використовувати зашифрований спосіб комунікації (IPsec). Я хочу мати можливість використовувати програмне забезпечення лише з певного комп'ютера (фільтрація за IP).	Налаштуйте політику фільтрації трафіку. «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 110
Я хочу використовувати сканер у мережі IEEE802.1X.	Налаштуйте IEEE802.1X для сканера. «Підключення сканера до мережі IEEE802.1X» на сторінці 122

Налаштування функцій для автентифікації за допомогою сканера

Мета	Необхідні налаштування
Я хочу увімкнути Налаштування автентифікації.	Подробиці про налаштування доступних Налаштування автентифікації та Метод ідентифікації див. нижче. «Про Налаштування автентифікації» на сторінці 132 «Про Метод ідентифікації» на сторінці 133

Використання системи автентифікації сервера

За допомогою Document Capture Pro Server Authentication Edition (скорочено — Document Capture Pro Server AE) ви можете створити систему автентифікації, яка використовує сервер для автентифікації.

Для отримання додаткової інформації зверніться до місцевого представництва Epson.

Налаштування мережі

Підключення сканера до мережі

У цьому розділі пояснено, як підключити сканер до мережі за допомогою панелі керування сканера.

Примітка.
Якщо ваш сканер і комп'ютер розміщені в одному сегменті, ви також можете виконати підключення за допомогою програми встановлення.

❏ *Налаштування з веб-сайту*

Відкрийте вказаний нижче веб-сайт і введіть назву продукту. Перейдіть до ***Установка*** *та почніть установлення.*

http://epson.sn

❏ *Установлення за допомогою диска із програмним забезпеченням (тільки для моделей, що постачаються в комплекті з диском із програмним забезпеченням і користувачів, чиї комп'ютери із Windows оснащено дисководами).*

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

До початку встановлення мережевого з'єднання

Щоб підключитись до мережі, перевірте заздалегідь спосіб з'єднання та дані налаштування з'єднання.

Збір інформації про налаштування підключення

Підготуйте необхідну інформацію про налаштування для підключення. Перевірте спочатку вказану нижче інформацію.

Розділи	Параметри	Примітка
Спосіб підключення пристрою	❏ Ethernet ❏ Wi-Fi	Вирішіть, як підключати сканер до мережі. Для проводової локальної мережі — підключається до перемикача локальної мережі. Для Wi-Fi — підключається до мережі (SSID) точки доступу.
Інформація про підключення до локальної мережі	❏ IP-адреса ❏ Маска підмережі ❏ Стандартний шлюз	Визначте IP-адресу, щоб призначити її сканеру. Якщо IP-адреса призначається статично, всі значення є обов'язковими. Якщо IP-адреса призначається динамічно за допомогою функції DHCP, ця інформація не є обов'язковою, оскільки вона встановлюється автоматично.
Інформація про підключення до мережі Wi-Fi	❏ SSID ❏ Пароль	Це — SSID (ім'я мережі) та пароль точки доступу, до якої підключається сканер. Якщо було встановлено фільтрування MAC-адрес, зареєструйте MAC-адресу сканера заздалегідь, щоб зареєструвати сканер. Нижче наведено підтримувані стандарти. «Технічні характеристики мережі» на сторінці 29

Розділи	Параметри	Примітка
Інформація про сервер DNS	❏ IP-адреса для головного сервера DNS ❏ IP-адреса для допоміжного сервера DNS	Ці дані необхідні для визначення DNS-серверів. Допоміжний DNS встановлюється, коли система має резервне розташування та є допоміжний сервер DNS. Якщо ви працюєте у маленькій організації і не встановлювали сервер DNS, встановіть IP-адресу маршрутизатора.
Інформація про проксі-сервер	❏ Ім'я проксі-сервера	Налаштуйте, якщо мережеве середовище використовує проксі-сервер для доступу до інтернету з інтранету, а ви використовуєте функцію, за якої сканер напряму отримує доступ до інтернету. Сканер підключається до інтернету напряму при використанні таких функцій. ❏ Служби Epson Connect ❏ Хмарні служби інших компаній ❏ Оновлення мікропрограм ❏ Надсилання сканованих зображень на SharePoint(WebDAV)
Інформація про номер порту	❏ Номер порту, який необхідно відкрити	Перевірте номер порту, який використовує сканер та комп'ютер, а тоді, за необхідності, відкрийте порт, заблокований брандмауером. Щодо номера порту, який використовує сканер, див. нижче. «Використання порту для сканера» на сторінці 31

Присвоєння IP-адреси

Це наступні типи присвоєння IP-адреси.

Статична IP-адреса:

Призначте попередньо визначену IP-адресу на сканер (хост) вручну.

Інформація для підключення до мережі (маска підмережі, шлюз за замовчуванням, сервер DNS тощо) потрібно встановити вручну.

IP-адреса не змінюється навіть тоді, коли пристрій вимкнено, тому це корисно, якщо ви хочете керувати пристроями із середовищем, де ви не можете змінити IP-адресу, або хочете керувати пристроями за допомогою IP-адреси. Ми рекомендуємо налаштування для сканера, сервера тощо, до якого матимуть доступ багато комп'ютерів. Крім того, при використанні функцій безпеки, таких як фільтрація IPsec/IP, призначте фіксовану IP-адресу, щоб IP-адреса не змінювалася.

Автоматичне призначення за допомогою функції DHCP (динамічна IP-адреса):

Призначте IP-адресу автоматично до сканера (хосту) за допомогою функції DHCP DHCP-сервера або роутера.

Інформація для підключення до мережі (маска підмережі, шлюз за замовчуванням, DNS-сервер тощо) встановлюється автоматично, тому ви можете легко підключити пристрій до мережі.

Якщо пристрій або роутер вимкнено, або залежно від налаштувань сервера DHCP, IP-адреса може змінюватися при повторному підключенні.

Ми рекомендуємо керувати іншими пристроями, окрім IP-адреси, і спілкуватися з протоколами, які можуть слідувати IP-адресою.

Примітка.
Якщо ви використовуєте функцію резервування IP-адреси DHCP, ви можете призначити таку ж IP-адресу пристроям у будь-який час.

Сервер DNS та проксі-сервер

Сервер DNS має ім'я хосту, ім'я домена адреси електронної пошти тощо разом з інформацією про IP-адресу.

Можна встановити зв'язок, якщо іншу сторону описано іменем хосту, іменем домену тощо, коли комп'ютер або сканер здійснює IP-зв'язок.

Запитує сервер DNS цю інформацію та отримує IP-адресу іншої сторони. Цей процес називається ідентифікація імені.

Тому такі пристрої, як комп'ютери та сканери можуть підключатись за допомогою IP-адреси.

Ідентифікація імені необхідна для того, щоб сканер підключився за допомогою функції електронної пошти або функції інтернет-підключення.

Необхідно виконати налаштування сервера DNS, якщо ви використовуєте ці функції.

Якщо ви призначаєте IP-адресу сканера за допомогою функції DHCP сервера DHCP чи маршрутизатора, то її буде налаштовано автоматично.

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.

При підключенні до інтернету через проксі-сервер налаштуйте проксі-сервер на сканері.

Підключення до мережі з панелі керування

Підключіть сканер до мережі за допомогою панелі керування сканера.

Призначення IP-адреси

Налаштуйте базові елементи, такі як адреса хоста, Маска підмережі, Шлюз за замовчанням.

Цей розділ надає роз'яснення щодо процедури налаштування статичної IP-адреси.

1. Увімкніть сканер.
2. На головному екрані панелі керування сканера виберіть **Налаш.**.
3. Виберіть **Налаштування мережі** > **Розширений** > **TCP/IP**.
4. Виберіть **Вручну** для **Отримати IP-адресу**.

   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 5 і 6 встановлюються автоматично, тому перейдіть до кроку 7.

5. Введіть IP-адресу.

   Фокус переміщується на передній чи задній сегмент, розділений крапкою, якщо ви вибираєте ◀ та ▶.

   Підтвердьте значення, що вказане на екрані.

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

   Підтвердьте значення, що вказане на екрані.

   > ***Важливо***
   >
   > *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.*

7. Введіть IP-адресу сервера DNS.

   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 ви вибрали **Авто**, перейдіть до кроку 9.*

8. Введіть IP-адресу другорядного сервера DNS.

   Підтвердьте значення, що вказане на екрані.

9. Торкніться **Запуск налаштув.**.

Налаштування проксі-сервера

Налаштуйте проксі-сервер, якщо обидва пункти є вірними.

❏ Проксі-сервер збудований для інтернет-з'єднання.

❏ При використанні функції прямого підключення сканера до інтернету, наприклад, служба Epson Connect або хмарні служби іншої компанії.

1. Виберіть **Налаш.** на головному екрані.

   У разі внесення налаштувань після IP-адреси, відобразиться екран **Розширений**. Перейдіть до пункту 3.

2. Виберіть **Налаштування мережі** > **Розширений**.

3. Виберіть **Проксі-сервер**.

4. Виберіть **Кори.** для **Налашт. проксі-серв.**.

5. Уведіть адресу проксі-сервера у форматі IPv4 або FQDN.

   Підтвердьте значення, що вказане на екрані.

6. Уведіть номер порту для проксі-сервера.

   Підтвердьте значення, що вказане на екрані.

7. Торкніться **Запуск налаштув.**.

Підключення до Ethernet

Підключіть сканер до мережі за допомогою кабелю LAN (локальної мережі), а тоді перевірте з'єднання.

1. Підключіть сканер до вузла (перемикач локальної мережі) за допомогою кабелю локальної мережі.
2. Виберіть на головному екрані.
3. Виберіть **Роутер**.
4. Перевірте, чи правильно задано параметри Підключення та IP-адреса.
5. Торкніться **Закрити**.

Підключення до бездротової локальної мережі (Wi-Fi)

Підключити сканер до безпровідної локальної мережі (Wi-Fi) можна в кілька способів. Виберіть спосіб підключення, який відповідає середовищу та умовам використання.

Якщо вам відома інформація, що стосується бездротового маршрутизатора, наприклад SSID і пароль, ви можете виконати налаштування вручну.

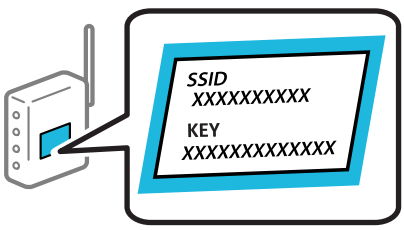
Якщо бездротовий маршрутизатор підтримує WPS, можна виконати налаштування шляхом встановлення кнопки запуску.

Підключивши сканер до мережі, встановіть з'єднання з ним із пристрою, який потрібно використовувати (комп'ютер, смарт-пристрій, планшет тощо.)

Налаштування Wi-Fi шляхом введення SSID і пароля

Налаштувати Wi-Fi-мережу можна за допомогою введення інформації, необхідної для підключення до безпровідного маршрутизатора з панелі керування сканера. Щоб налаштувати цей спосіб, вам потрібно мати SSID і пароль для безпровідного маршрутизатора.

Примітка.
Якщо використовується безпровідний маршрутизатор зі стандартними налаштуваннями, SSID і пароль вказано на етикетці. Якщо ви не знаєте SSID і пароль, зверніться до особи, яка встановлювала безпровідний маршрутизатор, або див. документацію до безпровідного маршрутизатора.



1. Торкніться  на головному екрані.
2. Виберіть **Роутер**.
3. Торкніться **Установки запуску**.

   Якщо мережеве з'єднання вже налаштовано, буде відображено докладні відомості про з'єднання. Торкніться елемента **Змінити на підключення Wi-Fi.** або **Змінити налаштування**, щоб змінити налаштування.
4. Виберіть **Майстер налаштування Wi-Fi**.
5. Щоб вибрати SSID, виконуйте вказівки на екрані, введіть пароль безпровідного маршрутизатора, і почніть налаштування.

   Якщо потрібно перевірити стан підключення сканера до мережі після завершення налаштування, див. докладніше, перейшовши за відповідним посиланням нижче.

   Примітка.
   - ❏ *Якщо SSID невідомо, перевірте, чи не вказано його на етикетці на безпровідному маршрутизаторі. Якщо використовується безпровідний маршрутизатор зі стандартними налаштуваннями, використовуйте SSID, який вказано на етикетці. Якщо жодної інформації знайти не вдається, див. документацію до безпровідного маршрутизатора.*
   - ❏ *Пароль чутливий до регістру літер.*
   - ❏ *Якщо пароль невідомо, перевірте, чи не вказано його на етикетці на безпровідному маршрутизаторі. На етикетці може бути вказано «Network Key», «Wireless Password» тощо. Якщо використовується безпровідний маршрутизатор зі стандартними налаштуваннями, використовуйте пароль, що вказаний на етикетці.*

Пов'язані відомості

➡ «Перевірка стану підключення до мережі» на сторінці 27

Налаштування Wi-Fi через налаштування кнопки пуску (WPS)

Налаштувати мережу Wi-Fi можна автоматично, натиснувши кнопку на безпровідному маршрутизаторі. Якщо дотримано вказані нижче умови, мережу можна налаштовувати в цей спосіб.

- ❏ Безпровідний маршрутизатор, сумісний з WPS (Wi-Fi Protected Setup).
- ❏ Поточне підключення до Wi-Fi було здійснено через натискання кнопки на безпровідному маршрутизаторі.

Примітка.
Якщо кнопку не вдалося знайти або підключення відбулося через програмне забезпечення, див. документацію до маршрутизатора.

1. Торкніться  на головному екрані.
2. Виберіть **Роутер**.

3. Торкніться **Установки запуску**.

   Якщо мережеве з'єднання вже налаштовано, буде відображено докладні відомості про з'єднання. Торкніться елемента **Змінити на підключення Wi-Fi.** або **Змінити налаштування**, щоб змінити налаштування.

4. Виберіть **Налашт. кнопки(WPS)**.

5. Виконайте інструкції на екрані.

   Якщо потрібно перевірити стан підключення сканера до мережі після завершення налаштування, див. докладніше, перейшовши за відповідним посиланням нижче.

   Примітка.
   Якщо з'єднання встановити не вдалося, перезапустіть безпровідний маршрутизатор, перемістіть його ближче до сканера, а тоді повторіть спробу.

Пов'язані відомості

➡ «Перевірка стану підключення до мережі» на сторінці 27

Налаштування Wi-Fi через встановлення PIN-коду (WPS)

Ви можете автоматично підключитися до безпровідного маршрутизатора за допомогою PIN-коду. Можна використовувати цей спосіб, якщо безпровідний маршрутизатор обладнано функцією WPS (безпечне налаштування Wi-Fi). За допомогою комп'ютера введіть PIN-код у бездротовий маршрутизатор.

1. Торкніться  на головному екрані.

2. Виберіть **Роутер**.

3. Торкніться **Установки запуску**.

   Якщо мережеве з'єднання вже налаштовано, буде відображено докладні відомості про з'єднання. Торкніться елемента **Змінити на підключення Wi-Fi.** або **Змінити налаштування**, щоб змінити налаштування.

4. Оберіть **Інші** > **Настр. PIN-коду (WPS)**

5. Виконайте інструкції на екрані.

   Якщо потрібно перевірити стан підключення сканера до мережі після завершення налаштування, див. докладніше, перейшовши за відповідним посиланням нижче.

   Примітка.
   Детальнішу інформацію про введення PIN-коду див. у документації до безпровідного маршрутизатора.

Пов'язані відомості

➡ «Перевірка стану підключення до мережі» на сторінці 27

Додавання або заміна комп'ютера або пристроїв

Підключення до сканера, підключеного до мережі

Якщо сканер вже підключено до мережі, здійснити підключення комп'ютера або смарт-пристрою до сканера можна по мережі.

Використання мережевого сканера з другого комп'ютера

Щоб підключити сканер до комп'ютера, радимо скористатися програмою встановлення. Запустити програму встановлення можна одним із вказаних нижче способів.

❏ Налаштування з веб-сайту

Відкрийте вказаний нижче веб-сайт і введіть назву продукту. Перейдіть до **Установка** та почніть установлення.

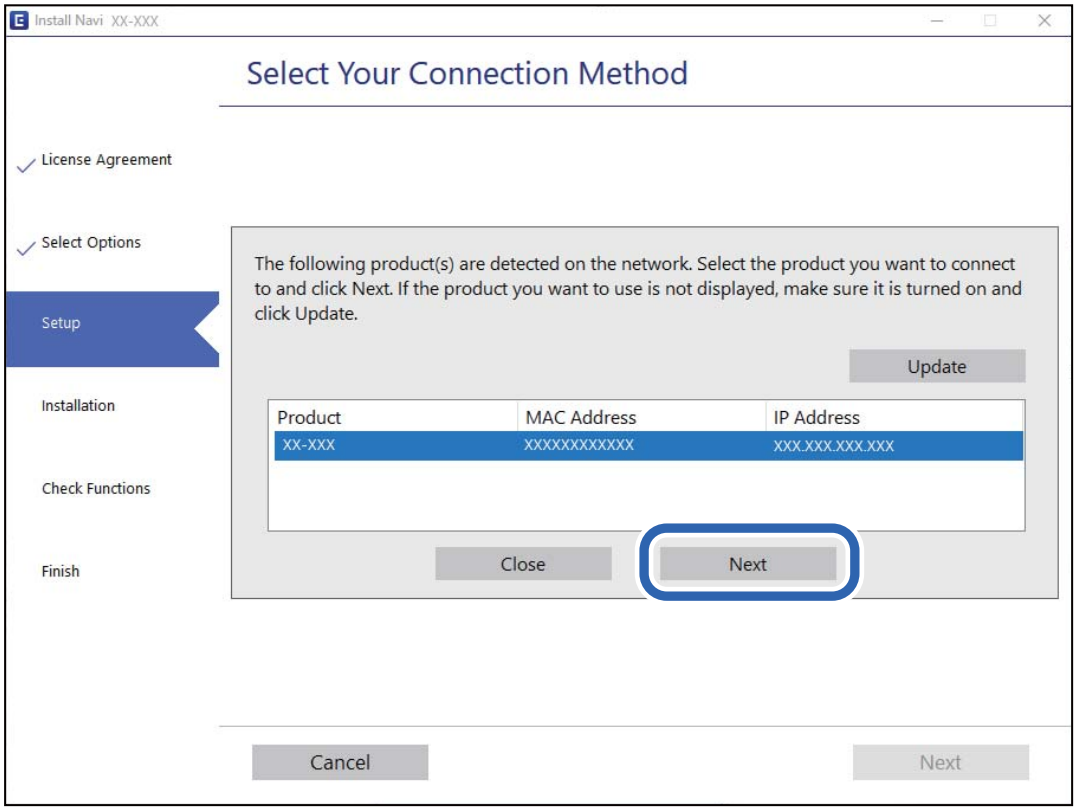
http://epson.sn

❏ Установлення за допомогою диска із програмним забезпеченням (тільки для моделей, що постачаються в комплекті з диском із програмним забезпеченням і користувачів, чиї комп'ютери під керуванням ОС Windows оснащено дисководами).

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

Вибір сканера

Виконуйте вказівки на екрані, доки не з'явиться наведений нижче екран, виберіть ім'я сканера, до якого потрібно підключитися, після чого клацніть **Далі**.



Виконайте інструкції на екрані.

Використання мережевого сканера зі смарт-пристрою

Ви можете підключити смарт-пристрій до сканер в один з кількох способів, зазначених нижче.

Підключення по безпровідному маршрутизатору

Підключіть смарт-пристрій до тієї самої мережі Wi-Fi (SSID), що й сканер.

Детальніше див.

«Налаштування підключення до смарт-пристрою» на сторінці 25

Підключення за допомогою Wi-Fi Direct

Підключіть смарт-пристрій безпосередньо до сканера без безпровідного маршрутизатора.

Детальніше див.

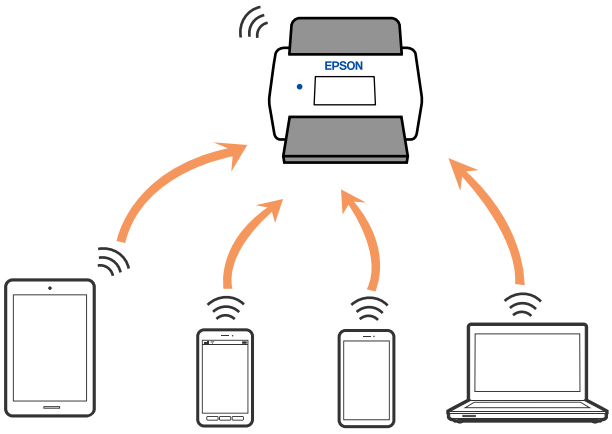
«Підключення смарт-пристрою до сканера напряму (Wi-Fi Direct)» на сторінці 22

Підключення смарт-пристрою до сканера напряму (Wi-Fi Direct)

Wi-Fi Direct (Простий режим AP) дає змогу підключити смарт-пристрій до сканера напряму без безпровідного маршрутизатора та здійснювати друк зі смарт-пристрою.

Про Wi-Fi Direct

Використовуйте цей спосіб підключення, коли не застосовуєте Wi-Fi вдома або в офісі, або коли потрібно напряму підключити сканер до смарт-пристрою. У цьому режимі сканер виконуватиме функцію безпровідного маршрутизатора, а ви зможете підключати до чотирьох пристроїв до сканера не використовуючи стандартний безпровідний маршрутизатор. Однак пристрої, підключені до сканера напряму, не можуть з'єднуватися один з одним через сканер.



Сканер можна одночасно підключити через Wi-Fi або Ethernet і режим Wi-Fi Direct (Простий режим AP). Однак, якщо з'єднання з мережею буде запущене у режимі Wi-Fi Direct (Простий режим AP), коли сканер підключено до Wi-Fi, з'єднання Wi-Fi буде тимчасово відключено.

Підключення до смарт-пристрою за допомогою Wi-Fi Direct

Цей спосіб дає змогу підключати сканер напряму до смарт-пристроїв без допомоги бездротового маршрутизатора.

1. Виберіть  на головному екрані.
2. Виберіть **Wi-Fi Direct**.
3. Виберіть **Установки запуску**.
4. Запустіть на смарт-пристрої програму Epson Smart Panel.
5. Щоб виконати підключення до сканера, виконайте вказівки, відображені на Epson Smart Panel.

   Після підключення смарт-пристрою до сканера перейдіть до наступного кроку.
6. На панелі керування сканера виберіть **Заверш.**.

Відключення Wi-Fi Direct (Простий режим AP)

Є два способи, доступні для відключення Wi-Fi Direct (Простий режим AP); всі з'єднання можна відключити за допомогою панелі керування сканера або на комп'ютері чи смарт-пристрої.

Якщо потрібно вимкнути всі з'єднання, виберіть  > **Wi-Fi Direct** > **Установки запуску** > **Змінити** > **Вимкнути Wi-Fi Direct**.

> ***Важливо***
>
> *Коли вимкнути з'єднання Wi-Fi Direct (Простий режим AP), усі комп'ютери і смарт-пристрої, підключені до сканера через Wi-Fi Direct (Простий режим AP), буде відключено.*

Примітка.
Якщо потрібно відключити тільки один пристрій, виконайте відключення з пристрою, а не зі сканера. Використовуйте один із наведених нижче способів відключення Wi-Fi Direct (Простий режим AP) на пристрої.

❏ *Від'єднайте Wi-Fi-підключення від імені мережі сканера (SSID).*

❏ *Підключення до іншої мережі (SSID).*

Змінення параметрів Wi-Fi Direct (Простий режим AP), як-от SSID

Якщо увімкнено підключення Wi-Fi Direct (Простий режим AP), змінити налаштування можна на вкладці  > **Wi-Fi Direct** > **Установки запуску** > **Змінити**, після чого буде відображено наведені нижче елементи.

Змінити назву мережі

Зміна імені мережі (SSID) Wi-Fi Direct (Простий режим AP), яке використовується для підключення до сканера, на довільне ім'я. Ви можете змінити ім'я мережі (SSID) за допомогою символів ASCII, відображених на програмній клавіатурі на панелі керування. Ви можете ввести до 22 символів.

Під час зміни імені мережі (SSID), усі підключені пристрої буде відключено. Використовуйте нове ім'я мережі (SSID), якщо потрібно підключити пристрій повторно.

Змінити пароль

Змініть пароль Wi-Fi Direct (Простий режим AP) для з'єднання сканера з вашим умовним значенням. Можна встановити пароль, використовуючи символи ASCII, відображені на віртуальній клавіатурі на панелі керування. Можна ввести від 8 до 22 символів.

Під час зміни пароля, усі підключені пристрої буде відключено. Використайте новий пароль, якщо потрібно підключити пристрій повторно.

Змінити діапазон частоти

Змініть діапазон частоти Wi-Fi Direct, яка використовується для підключення до сканера. Можна вибрати 2,4 ГГц або 5 ГГц.

Під час зміни діапазону частоти, усі підключені пристрої буде відключено. Підключіть пристрій знову.

Зауважте, що із пристроїв, які не підтримують діапазон частот у 5 ГГц, повторне підключення буде неможливим, якщо частоту змінено на 5 ГГц.

В залежності від регіону дані налаштування можуть не відображатися.

Вимкнути Wi-Fi Direct

Вимкніть налаштування сканера Wi-Fi Direct (Простий режим AP). Усі пристрої, які підключено до сканера за допомогою з'єднання Wi-Fi Direct (Простий режим AP), буде відключено.

Віднов. налашт. за зам.

Відновлення всіх налаштувань Wi-Fi Direct (Простий режим AP) до значень за замовчуванням.

Інформацію про підключення Wi-Fi Direct (Простий режим AP) смарт-пристрою, збережену на сканері, буде видалено.

Примітка.
Можна також зробити налаштування у вкладці ***Мережа*** *>* ***Wi-Fi Direct*** *у Web Config, але це стосується перелічених нижче параметрів.*

❏ *Увімкнення або вимкнення Wi-Fi Direct (Простий режим AP)*

❏ *Зміна мережевого імені (SSID)*

❏ *Зміна пароля*

❏ *Змінення діапазону частоти*

В залежності від регіону дані налаштування можуть не відображатися.

❏ *Відновлення налаштувань Wi-Fi Direct (Простий режим AP)*

Повторне налаштування підключення до мережі

У цьому розділі пояснюється, як налаштувати підключення до мережі та змінити спосіб підключення в разі заміни безпровідного маршрутизатора або комп'ютера.

У разі заміни безпровідного маршрутизатора

У разі заміни безпровідного маршрутизатора, виконайте налаштування підключення між комп'ютером або смарт-пристроєм і сканером.

Ці налаштування потрібно виконати в разі зміни Інтернет-провайдера тощо.

Налаштування підключення до комп'ютера

Щоб підключити сканер до комп'ютера, радимо скористатися програмою встановлення. Запустити програму встановлення можна одним із вказаних нижче способів.

❏ Налаштування з веб-сайту

Відкрийте вказаний нижче веб-сайт і введіть назву продукту. Перейдіть до **Установка** та почніть установлення.

http://epson.sn

❏ Установлення за допомогою диска із програмним забезпеченням (тільки для моделей, що постачаються в комплекті з диском із програмним забезпеченням і користувачів, чиї комп'ютери під керуванням ОС Windows оснащено дисководами).

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

Вибір способу підключення

Виконайте інструкції на екрані. На екрані **Виберіть операцію** виберіть **Налаштувати з'єднання для Принтера знову (для нового мережевого або для зміни USB на мережу тощо)**, після чого клацніть **Далі**.

Для завершення налаштування виконайте вказівки на екрані.

Якщо підключитися не вдається, див. нижче, щоб спробувати вирішити проблему.

«Не вдається підключитися до мережі» на сторінці 33

Налаштування підключення до смарт-пристрою

Якщо підключити сканер до тієї самої мережі Wi-Fi (SSID), що й смарт-пристрій, можна користуватися сканером просто зі смарт-пристрою. Для використання сканера зі смарт-пристрою відкрийте нижченаведений веб-сайт, після чого введіть ім'я продукту. Перейдіть до **Установка** та почніть установлення.

http://epson.sn

Відкрийте цей веб-сайт зі свого смарт-пристрою, який потрібно підключити до сканера.

У разі заміни комп'ютера

У разі заміни комп'ютера, виконайте налаштування підключення між комп'ютером і сканером.

Налаштування підключення до комп'ютера

Щоб підключити сканер до комп'ютера, радимо скористатися програмою встановлення. Запустити програму встановлення можна вказаним нижче способом.

❏ Налаштування з веб-сайту

Відкрийте вказаний нижче веб-сайт і введіть назву продукту. Перейдіть до **Установка** та почніть установлення.

http://epson.sn

❏ Установлення за допомогою диска із програмним забезпеченням (тільки для моделей, що постачаються в комплекті з диском із програмним забезпеченням і користувачів, чиї комп'ютери під керуванням ОС Windows оснащено дисководами).

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

Виконайте інструкції на екрані.

Змінення способу підключення до комп'ютера

У цьому розділі пояснюється, як змінити спосіб підключення, коли підключення між комп'ютером і сканером встановлено.

Змінення способу підключення до мережі із Ethernet на Wi-Fi

Змініть Ethernet-підключення на Wi-Fi-підключення з панелі керування сканера. Спосіб змінення підключення здебільшого такий самий, як налаштування підключення до Wi-Fi.

Пов'язані відомості

➡ «Підключення до бездротової локальної мережі (Wi-Fi)» на сторінці 18

Змінення способу підключення до мережі із Wi-Fi на Ethernet

Щоб змінити Wi-Fi-підключення на Ethernet-підключення, виконайте наведені нижче кроки.

1. Виберіть **Налаш.** на головному екрані.
2. Виберіть **Налаштування мережі** > **Налаштування дротової LAN**.
3. Виконайте інструкції на екрані.

Змінення підключення з USB на мережеве підключення

Використання встановлення та переналаштування з іншим способом підключення.

❏ Налаштування з веб-сайту

Відкрийте вказаний нижче веб-сайт і введіть назву продукту. Перейдіть до **Установка** та почніть установлення.

http://epson.sn

❏ Установлення за допомогою диска із програмним забезпеченням (тільки для моделей, що постачаються в комплекті з диском із програмним забезпеченням і користувачів, чиї комп'ютери під керуванням ОС Windows оснащено дисководами).

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

Як вибрати зміну способу підключення

Виконайте інструкції на екрані. На екрані **Виберіть операцію** виберіть **Налаштувати з'єднання для Принтера знову (для нового мережевого або для зміни USB на мережу тощо)**, після чого клацніть **Далі**.

Виберіть підключення до мережі, яке потрібно використовувати, **Підключити через бездротову мережу (Wi-Fi)** або **Підключення через дротову мережу LAN (Ethernet)**, після чого клацніть **Далі**.

Для завершення налаштування виконайте вказівки на екрані.

Перевірка стану підключення до мережі

Можна перевірити стан підключення до мережі зазначеним способом.

Перевірка стану підключення до мережі з панелі керування

Ви можете перевірити стан підключення до мережі за допомогою піктограми мережі або інформації про мережу на панелі керування сканера.

Перевірка стану підключення до мережі за допомогою піктограми мережі

Можна перевірити стан мережі та силу радіохвилі за допомогою піктограми мережі на головному екрані сканера.

	Відображає стан мережевого підключення. Торкніться піктограми, щоб перевірити та змінити поточні налаштування. Це ярлик для вказаного нижче меню. **Налаш.** > **Налаштування мережі** > **Настр. Wi-Fi**	
		Сканер не підключено до безпровідної мережі (Wi-Fi).
		Сканер шукає ідентифікатор SSID, не має налаштованої IP-адреси або має проблеми із безпровідною мережею (Wi-Fi).
		Сканер підключено до безпровідної мережі (Wi-Fi). Кількість стовпчиків позначає силу сигналу з'єднання. Чим більше стовпчиків, тим краще з'єднання.
		Сканер не підключено до безпровідної мережі (Wi-Fi) в режимі Wi-Fi Direct (Простому режимі AP).
		Сканер підключено до безпровідної мережі (Wi-Fi) в режимі Wi-Fi Direct (Простому режимі AP).
		Сканер не підключено до проводової мережі (Ethernet) або не налаштовано для використання в цій мережі.
		Сканер підключено до проводової мережі (Ethernet).

Відображення докладних відомостей про мережу з панелі керування

Коли сканер підключено до мережі, можна також переглянути іншу інформацію про мережу, вибравши відповідне меню мережі, яку потрібно перевірити.

1. Виберіть **Налаш.** на головному екрані.
2. Виберіть **Налаштування мережі** > **Стан мережі**.
3. Щоб перевірити інформацію, виберіть меню, які потрібно перевірити.
   - ❏ Стан підкл. до LAN/Wi-Fi

     Відображається інформація про мережу (назва пристрою, відомості про з'єднання, сила сигналу тощо) для з'єднання Ethernet або Wi-Fi.
   - ❏ Стан Wi-Fi Direct

     Відображається інформація про те, чи ввімкнено або вимкнено Wi-Fi Direct, про SSID, пароль тощо для з'єднання Wi-Fi Direct.
   - ❏ Стан серв. ел. пошти

     Відображається мережева інформація для поштового сервера.

Технічні характеристики мережі

Характеристики Wi-Fi

Щоб дізнатися технічні характеристики Wi-Fi, див. таблицю внизу.

Країни на регіони, крім нижчезазначених	Таблиця A
Австралія Нова Зеландія Тайвань Південна Корея	Таблиця B

Таблиця A

Стандарти	IEEE 802.11b/g/n*1
Діапазон частот	2,4 ГГц
Максимальна потужність передачі радіочастот	2400–2483,5 МГц: 20 дБм (EIRP)
Канали	1/2/3/4/5/6/7/8/9/10/11/12/13
Режими підключення	Інфраструктура, Wi-Fi Direct (Простий режим AP)*2*3
Протоколи безпеки*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Стандарт доступний тільки для HT20.

*2 Не підтримується для IEEE 802.11b.

*3 Інфраструктуру та режими Wi-Fi Direct або Ethernet-підключення можна використовувати одночасно.

*4 Wi-Fi Direct підтримує тільки протокол WPA2-PSK (AES).

*5 Сумісний з протоколом WPA2, підтримка протоколів WPA/WPA2 Personal.

Таблиця B

Стандарти	IEEE 802.11a/b/g/n*1/ac
Діапазони частот	IEEE 802.11b/g/n: 2,4 ГГц, IEEE 802.11a/n/ac: 5 ГГц

Канали	Wi-Fi	2,4 ГГц	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 ГГц*3	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 ГГц	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 ГГц*3	W52 (36/40/44/48) W58 (149/153/157/161/165)
Режими підключення	Інфраструктура, Wi-Fi Direct (Простий режим AP)*4, *5		
Протоколи безпеки*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Стандарт доступний тільки для HT20.

*2 Не доступно на Тайвані.

*3 Доступність цих каналів в використання продукту поза приміщенням на цих каналах залежить від регіону. Докладніше див. http://support.epson.net/wifi5ghz/

*4 Не підтримується для IEEE 802.11b.

*5 Інфраструктуру та режими Wi-Fi Direct або Ethernet-підключення можна використовувати одночасно.

*6 Wi-Fi Direct підтримує тільки WPA2-PSK (AES).

*7 Сумісний з протоколом WPA2, підтримка протоколів WPA/WPA2 Personal.

Технічні характеристики Ethernet

Стандарти	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Енергоефективний Ethernet)*2
Режим зв'язку	Авто, 10 Мбіт повний дуплекс, 10 Мбіт полудуплекс, 100 Мбіт повний дуплекс, 100 Мбіт полудуплекс
Сполучна лінія	RJ-45

*1 Використовуйте категорію 5e або вище STP (екранована кручена пара), щоб запобігти ризику радіоперешкод.

*2 Підключений пристрій повинен відповідати стандартам IEEE802.3az.

Функції мережі та IPv4/IPv6

Функції	**Підтримуються**
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Функції	Підтримуються
Document Capture Pro Server	IPv4, IPv6

Протокол безпеки

IEEE802.1X*	
IPsec/IP-фільтрація	
SSL/TLS	HTTPS сервер/клієнт
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Вам необхідно використовувати пристрій підключення, який відповідає IEEE802.1X.

Використання порту для сканера

Сканер використовує вказаний нижче порт. Адміністратор мережі, за необхідності, повинен мати дозвіл на відкриття на цих портах дозволу на доступність.

Якщо сканер є відправником (клієнтом)

Використання	Місце призначення (Сервер)	Протокол	Номер порту
Надсилання файлу (у разі використання на сканері функції сканування в мережеву папку)	Сервер FTP/FTPS	FTP/FTPS (TCP)	20
			21
	Файловий сервер	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	Сервер WebDAV	Протокол HTTP (TCP)	80
		Протокол HTTPS (TCP)	443
Надсилання електронного листа (у разі використання на сканері функції сканування на пошту)	Сервер SMTP	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
Підключення POP перед SMTP (у разі використання на сканері функції сканування на пошту)	Сервер POP	POP3 (TCP)	110

Використання	Місце призначення (Сервер)	Протокол	Номер порту
У разі використання Epson Connect	Сервер Epson Connect	HTTPS	443
		XMPP	5222
Збирання інформації про користувача (використання контактів на сканері)	Сервер LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Автентифікація користувача під час збирання інформації про користувача (у разі використання контактів на сканері) Автентифікація користувача у разі використання функції сканування у мережеву папку (SMB) на сканері	Сервер KDC	Kerberos	88
Керування WSD	Клієнтський комп'ютер	WSD (TCP)	5357
Пошук комп'ютера в разі пуш-сканування з програми	Клієнтський комп'ютер	Пошук пуш-сканування	2968

Якщо клієнтський комп'ютер є відправником (клієнтом)

Використання	Місце призначення (Сервер)	Протокол	Номер порту
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 з програми	Сканер	Network Scan (TCP)	1865
Збирання інформації про завдання в разі пуш-сканування програми	Сканер	Push-сканування	2968
Web Config	Сканер	HTTP (TCP)	80
		HTTPS (TCP)	443

Вирішення проблем

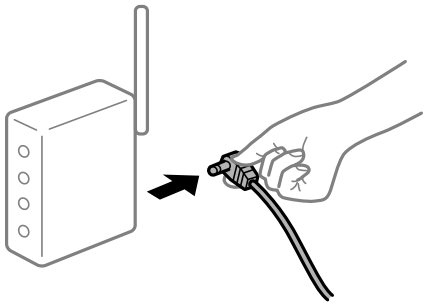
Не вдається підключитися до мережі

Проблема може виникнути через наведені нижче причини.

Виникли неполадки в роботі мережевих пристроїв при підключенні до Wi-Fi.

Solutions

Вимкніть пристрої, які потрібно підключити до мережі. Зачекайте 10 секунд, а тоді увімкніть пристрої у такій послідовності: бездротовий маршрутизатор, комп'ютер або смарт-пристрій, а тоді сканер. Перемістіть сканер та комп'ютер або смарт-пристрій ближче до бездротового маршрутизатора, щоб полегшити радіокомунікацію, а тоді спробуйте ще раз внести мережеві налаштування.



Пристрої не отримують сигнал від безпровідного маршрутизатора через велику відстань між ними.

Solutions

Перемістивши комп'ютер або смарт-пристрій і сканер ближче до безпровідного маршрутизатора, вимкніть безпровідний маршрутизатор, після чого знову ввімкніть його.

У разі заміни безпровідного маршрутизатора, налаштування не відповідають нового маршрутизатору.

Solutions

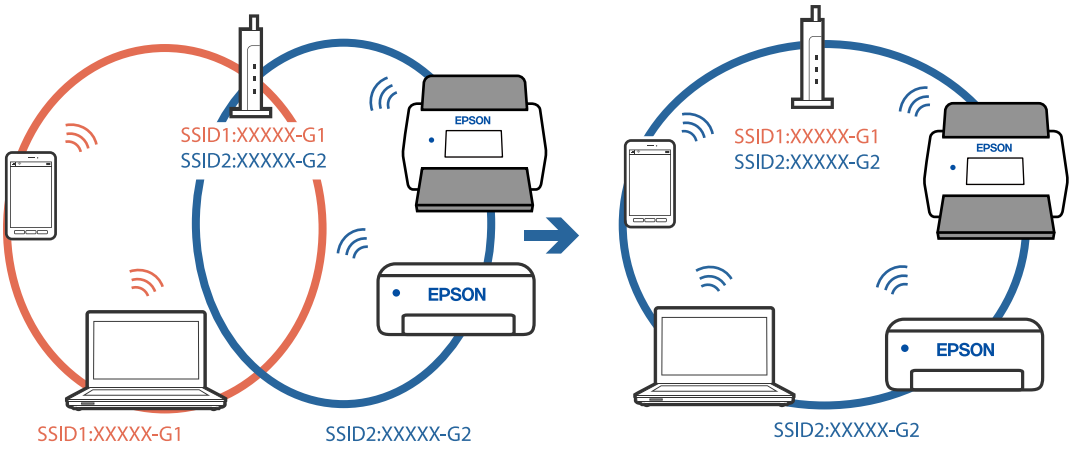
Виконайте налаштування підключення знову, щоб вони відповідали новому безпровідному маршрутизатору.

SSID, підключені з комп'ютера або смарт-пристрою та комп'ютера, різні.

Solutions

Якщо одночасно використовується кілька безпровідних маршрутизаторів, або якщо безпровідний маршрутизатор має кілька SSID, і пристрої підключено до різних SSID, вам не вдасться підключитися до безпровідного маршрутизатора.

Підключіть комп'ютер або смарт-пристрій до того самого ідентифікатора SSID, що й сканер.



На безпровідному маршрутизаторі доступна функція розмежування даних.

Solutions

Більшість безпровідних маршрутизаторів мають функцію розмежування даних, яка блокує з'єднання між підключеними пристроями. Якщо не вдається встановити з'єднання між сканером і комп'ютером або смарт-пристроєм, навіть якщо вони підключені до однієї мережі, вимкніть на бездротовому маршрутизаторі функцію розмежування даних. Для отримання детальнішої інформації див. посібник, який постачається разом із бездротовим маршрутизатором.

IP-адресу призначено неправильно.

Solutions

Якщо IP-адреса, призначена сканеру, — 169.254.XXX.XXX, а маска підмережі — 255.255.0.0, можливо IP-адресу призначено неправильно.

Виберіть на панелі керування сканера **Налаш.** > **Налаштування мережі** > **Розширений** > **Настройка TCP/IP**, після чого перевірте IP-адресу та маску підмережі, призначені сканеру.

Перезапустіть бездротовий маршрутизатор або переналаштуйте мережу для сканера.

Виникла проблема з налаштуваннями мережі на комп'ютері.

Solutions

Спробуйте відкрити будь-який веб-сайт із комп'ютера, щоб упевнитися, що налаштування мережі на комп'ютері правильні. Якщо жоден веб-сайт відкрити не вдається, проблема може бути на комп'ютері.

Перевірте мережеве з'єднання комп'ютера. Для детальнішої інформації див. документацію, що у комплекті з комп'ютером.

Сканер підключено через Ethernet за допомогою пристроїв, що підтримують IEEE 802.3az (технологія Ethernet з режимом енергозбереження).

Solutions

Під час підключення сканера до мережі Ethernet за допомогою пристроїв, що підтримують стандарт IEEE 802.3az (технологія Ethernet з режимом енергозбереження), залежно від використання концентратора або маршрутизатора можуть виникати перелічені далі проблеми.

❏ Підключення стає нестабільним, сканер підключається та відключається знову й знову.

❏ Неможливо підключитися до сканера.

❏ Швидкість зв'язку стає повільною.

Виконайте наведені нижче дії, щоб вимкнути стандарт IEEE 802.3az для сканера, а потім підключити.

1. Відключіть кабель Ethernet, підключений до комп'ютера та сканера.
2. Якщо стандарт IEEE 802.3az для комп'ютера увімкнено, вимкніть його.

   Докладніше див. документацію, що входить до комплекту постачання комп'ютера.
3. Під'єднайте комп'ютер і сканер до Ethernet-кабелю.
4. Перевірте на сканері налаштування мережі.

   Виберіть **Налаш.** > **Налаштування мережі** > **Стан мережі** > **Стан підкл. до LAN/Wi-Fi**.
5. Перевірте IP-адресу сканера.
6. Відкрийте на комп'ютері Web Config.

   Відкрийте веб-браузер і введіть IP-адресу сканера.

   «Запуск конфігурації мережі у веб-браузері» на сторінці 37
7. Виберіть вкладку **Мережа** > **Дротова LAN**.
8. Виберіть **Вимкнути** для **IEEE 802.3az**.
9. Клацніть **Далі**.
10. Клацніть **OK**.
11. Відключіть кабель Ethernet, підключений до комп'ютера та сканера.
12. Якщо на кроці 2 для комп'ютера був відключений стандарт IEEE 802.3az, увімкніть його.
13. Підключіть кабелі Ethernet до комп'ютера та сканера, які були відключені на кроці 1.

Якщо проблема все ще існує, її можуть спричиняти інші пристрої, а не сканер.

Сканер вимкнено.

Solutions

Переконайтеся, що сканер увімкнено.

Крім того, зачекайте, поки індикатор стану припинить блимати: це свідчитиме про готовність сканера до роботи.

Програмне забезпечення для налаштування сканера

Web Config

Web Config — це програма, яка працює у веб-браузерах, як-от Internet Explorer та Safari, встановлених на комп'ютері. Можна підтвердити стан сканера або змінити мережеву службу та налаштування сканера. Оскільки доступ до сканерів і керування ними здійснюється безпосередньо з мережі, то він підходить для налаштування одного сканера за раз. Для використання Web Config, підключіть свій комп'ютер до тієї ж мережі, що й сканер.

Підтримуються вказані нижче веб-браузери.

Microsoft Edge, Windows Internet Explorer 8 або новішої версії, Firefox*, Chrome*, Safari*

* Використовуйте найновішу версію.

Запуск конфігурації мережі у веб-браузері

1. Перевірте IP-адресу сканера.

   На панелі керування сканера виберіть **Налаш.** > **Налаштування мережі** > **Стан мережі**. Далі виберіть активний стан способу підключення (**Стан підкл. до LAN/Wi-Fi** або **Стан Wi-Fi Direct**) для підтвердження IP-адреси сканера.

2. Запустіть веб-браузер із комп'ютера або смарт-пристрою, а тоді введіть IP-адресу сканера.

   Формат:

   IPv4: http://IP-адреса сканера/

   IPv6: http://[IP-адреса сканера]/

   Приклади:

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   Примітка.
   Оскільки у сканері під час доступу до HTTPS використовується цифровий сертифікат із власним підписом, під час запуску Web Config у браузері з'являється повідомлення; повідомлення не свідчить про проблему, тому його можна сміливо ігнорувати.

3. Для зміни налаштувань сканера увійдіть як адміністратор.

   Клацніть **Вхід в систему адміністратора** у правій верхній частині екрана. Введіть **Ім'я користувача** і **Поточний пароль**, після чого клацніть **OK**.

   Примітка.
   - ❏ *Нижче наведено початкові значення для інформації адміністратора Web Config.*

     Ім'я користувача: немає (пусто)

     Пароль: серійний номер сканера

     Серійний номер зазначено на етикетці на задній панелі сканера.
   - ❏ *Якщо у верхній правій частині екрана відображено **Вихід із системи адміністратора**, це значить, що ви вже увійшли як адміністратор.*

Запуск Web Config у Windows

Під час підключення комп'ютера до сканера за допомогою WSD, дотримуйтеся перелічених нижче вказівок щоб запустити Web Config.

1. Відкрийте список сканерів на комп'ютері.
   - ❏ Windows 10

     Натисніть кнопку «Пуск» та виберіть **Система Windows** > **Панель керування** > **Переглянути принтери та пристрої** у меню **Устаткування та звук**.
   - ❏ Windows 8.1/Windows 8

     Виберіть **Робочий стіл** > **Налаштування** > **Панель керування** > **Перегляд пристроїв та принтерів** у меню **Устаткування та звук** (або **Устаткування**).
   - ❏ Windows 7

     Натисніть кнопку «Пуск» та оберіть **Панель керування** > **Перегляд пристроїв та принтерів** у меню **Устаткування та звук**.
2. Правою кнопкою миші клацніть на сканері та виберіть **Властивості**.
3. Виберіть вкладку **Веб-служба** і натисніть URL-адресу.

   Оскільки у сканері під час доступу до HTTPS використовується цифровий сертифікат із власним підписом, під час запуску Web Config у браузері з'являється повідомлення; повідомлення не свідчить про проблему, тому його можна сміливо ігнорувати.

   Примітка.
   - ❏ *Нижче наведено початкові значення для інформації адміністратора Web Config.*

     Ім'я користувача: немає (пусто)

     Пароль: серійний номер сканера

     Серійний номер зазначено на етикетці на задній панелі сканера.
   - ❏ *Якщо у верхній правій частині екрана відображено **Вихід із системи адміністратора**, це значить, що ви вже увійшли як адміністратор.*

Epson Device Admin

Epson Device Admin — це багатофункціональна програма, яка дозволяє керувати пристроями в мережі.

За допомогою шаблонів конфігурації ви можете застосувати уніфіковані налаштування до кількох сканерів у мережі. Це зробить мережу придатною для встановлення й керування кількома сканерами.

Epson Device Admin можна завантажити з веб-сайту служби підтримки компанії Epson. Ви можете дізнатися більше про використання цієї програми у відповідній документації або за довідкою щодо Epson Device Admin.

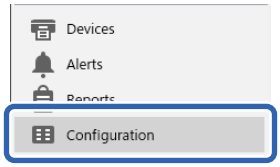
Шаблон конфігурації

Створення шаблону конфігурації

Створіть новий шаблон конфігурації.

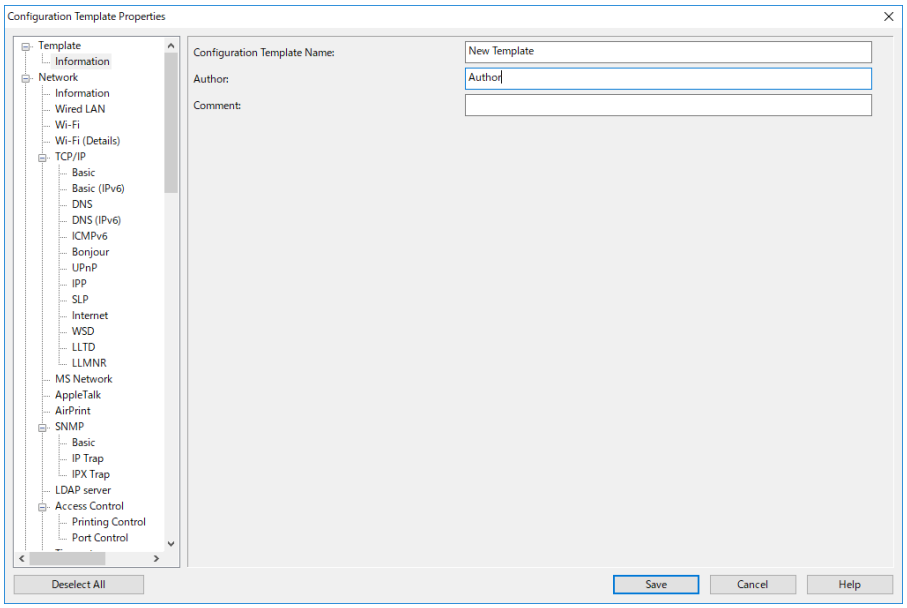
1. Запустіть Epson Device Admin.

2. Виберіть **Configuration** на бічній панелі меню завдань.



3. Виберіть **New** на стрічці меню.

4. Налаштуйте кожний елемент.



Елемент	Пояснення
Configuration Template Name	Ім’я шаблону конфігурації. Можна ввести до 1024 символів формату Юнікод (UTF-8).
Author	Інформація про автора шаблону. Можна ввести до 1024 символів формату Юнікод (UTF-8).
Comment	Можна ввести довільну інформацію. Можна ввести до 1024 символів формату Юнікод (UTF-8).

5. Виберіть ліворуч ті елементи, які потрібно налаштувати.

   Примітка.
   Щоб перейти до відповідного екрану, клацніть елементи меню ліворуч. Налаштоване значення зберігається, якщо перемикнути екран, але не зберігається, якщо скасувати екран. Після завершення налаштування клацніть ***Save****.*

Застосування шаблону конфігурації

Застосуйте збережений шаблон конфігурації до сканера. Буде застосовано елементи, вибрані в шаблоні. Якщо цільовий сканер не має відповідної функції, її не буде застосовано.

Примітка.
У разі встановлення для сканера пароля адміністратора, налаштуйте пароль заздалегідь.

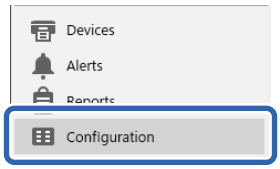
1. У меню стрічки на екрані Списку пристроїв виберіть ***Options*** *>* ***Password manager****.*

2. Виберіть ***Enable automatic password management****, а тоді клацніть* ***Password manager****.*

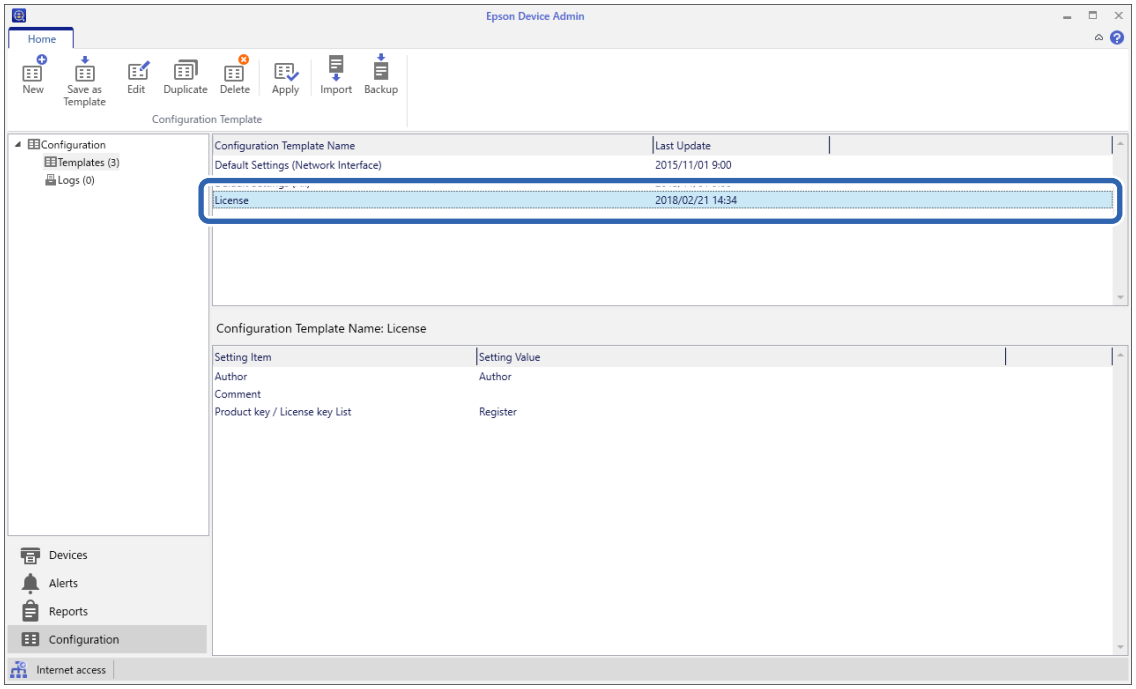
3. Виберіть відповідний сканер і натисніть опцію ***Edit****.*

4. Налаштуйте пароль, а тоді клацніть ***OK****.*

1. Виберіть **Configuration** на бічній панелі меню завдань.



2. Виберіть шаблон конфігурації, який потрібно застосувати, в розділі **Configuration Template Name**.



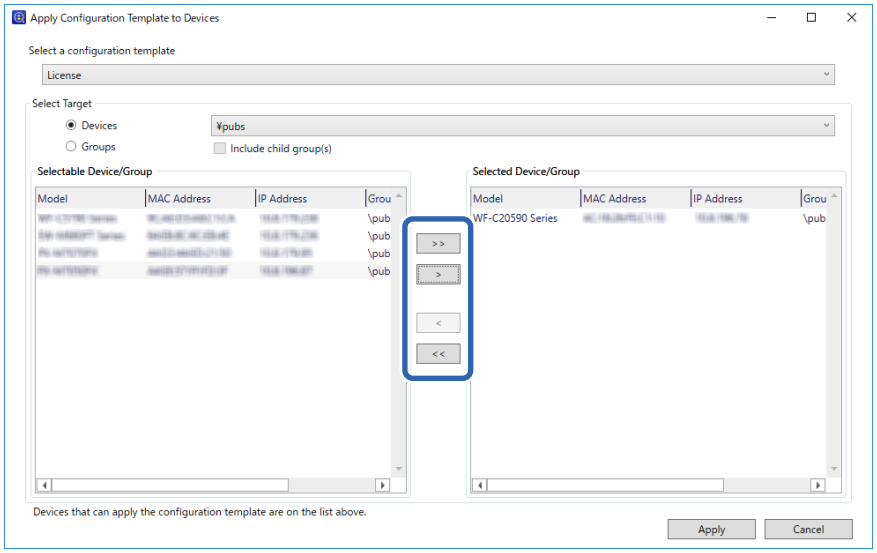
3. Натисніть кнопку **Apply** на стрічці меню.

   Буде відображено екран вибору пристроїв.

4. Виберіть шаблон конфігурації, який потрібно застосувати.

   Примітка.
   - ❏ *Під час вибирання **Devices** і груп, що містять пристрої з розкривного меню, буде відображено кожен пристрій.*
   - ❏ *Групи буде відображено під час вибирання **Groups**. Виберіть **Include child group(s)**, щоб автоматично вибирати групи в межах вибраних груп.*

5. Перемістіть сканер або групи, до яких потрібно застосувати шаблон, до **Selected Device/Group**.



6. Клацніть **Apply**.

   Буде відображено екран підтвердження для шаблону конфігурації.

7. Для застосування шаблону конфігурації натисніть **OK**.

8. Коли з'явиться повідомлення про завершення процедури, натисніть **OK**.

9. Клацніть **Details** і перевірте інформацію.

   Коли на елементах, до яких ви застосовували шаблон, буде відображено , це значить, що застосування шаблону відбулося успішно.

10. Клацніть **Close**.

Необхідні налаштування для сканування

Налаштування поштового сервера

Налаштуйте поштовий сервер через Web Config.

Якщо сканер може надсилати електронні листи за допомогою налаштування поштового сервера, можливі нижче наведені ситуації.

❏ Передає результати сканування за допомогою електронної пошти

❏ Отримує сповіщення електронною поштою зі сканера

Перевірте зазначене нижче до початку налаштування.

❏ Сканер підключено до мережі, яка має доступ до поштового сервера.

❏ Інформація щодо налаштування електронної пошти комп'ютера, який використовує той самий поштовий сервер, що й сканер.

Примітка.

❏ *Якщо ви використовуєте поштовий сервер в інтернеті, перевірте інформацію налаштування у провайдера чи на веб-сайті.*

❏ *Поштовий сервер також можна налаштувати з панелі керування сканера. Виконайте дії, як зазначено нижче.*

Налаш. > ***Налаштування мережі*** > ***Розширений*** > ***Сервер ел. пошти*** > ***Налаштування сервера***

1. Відкрийте Web Config і виберіть вкладку **Мережа** > **Сервер ел. пошти** > **Основні**.
2. Введіть значення для кожного елемента.
3. Виберіть **OK**.

   Відобразяться вибрані параметри.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Параметри поштового сервера

Параметри	Налаштування та пояснення	
Метод ідентифікації	Виберіть метод автентифікації для доступу сканера до поштового сервера.	
	Вимкнути	Автентифікацію вимкнено під час зв'язку з поштовим сервером.
	аутентифікація SMTP	Потребує підтримки SMTP-автентифікації поштовим сервером.
	POP перед SMTP	Налаштуйте сервер POP3 для вибору цього методу.
Ідентифіков. обл. Запис	Якщо вибрати **аутентифікація SMTP** або **POP перед SMTP** як значення для **Метод ідентифікації**, введіть назву ідентифікованого облікового запису довжиною від 0 до 255 символів у ASCII (0x20–0x7E).	

Параметри	Налаштування та пояснення	
Ідентифікований пароль	Якщо вибрати **аутентифікація SMTP** або **POP перед SMTP** як значення для **Метод ідентифікації**, введіть автентифікований пароль довжиною від 0 до 20 символів у ASCII (0x20–0x7E).	
Ел. адреса відправника	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.	
Адреса сервера SMTP	Введіть від 0 до 255 символів, використовуючи символи A–Z a–z 0–9 . -. Можна використовувати формат IPv4 або FQDN.	
Номер порту сервера SMTP	Введіть число від 1 до 65535.	
Надійне підключення	Укажіть метод безпечного підключення для сервера електронної пошти.	
	Немає	Якщо вибрати **POP перед SMTP** у **Метод ідентифікації**, метод з'єднання перейде у значення **Немає**.
	SSL/TLS	Воно доступне, коли **Метод ідентифікації** має значення **Вимкнути** або **аутентифікація SMTP**.
	STARTTLS	Воно доступне, коли **Метод ідентифікації** має значення **Вимкнути** або **аутентифікація SMTP**.
Перевірка сертифікату	Сертифікат перевіряється, коли увімкнена ця функція. Рекомендується встановити для неї значення **Увімкн.**.	
Адреса сервера POP3	Якщо вибрати **POP перед SMTP** для **Метод ідентифікації**, введіть адресу POP3-сервера довжиною від 0 до 255 символів, використовуючи символи A–Z a–z 0–9 . -. Можна використовувати формат IPv4 або FQDN.	
Номер порту сервера POP3	Щоб вибрати **POP перед SMTP** для **Метод ідентифікації**, введіть число від 1 до 65535.	

Перевірка з'єднання з поштовим сервером

Можна перевірити з'єднання з поштовим сервером, виконавши перевірку з'єднання.

1. Відкрийте Web Config і виберіть вкладку **Мережа** > **Сервер ел. пошти** > **Перевірка підключення**.

2. Виберіть **Пуск**.

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

   Примітка.
   Перевірку з'єднання з поштовим сервером також можна виконати з панелі керування сканера. Виконайте дії, як зазначено нижче.

   Налаш.* > *Налаштування мережі* > *Розширений* > *Сервер ел. пошти* > *Перевірка підключення

Повідомлення перевірки з'єднання з поштовим сервером

Повідомлення	Причина
Перевірка підключення пройшла успішно.	Це повідомлення відображається тоді, коли відбулося успішне з'єднання з сервером.
Помилка зв'язку серверу SMTP. Перевірте наступне. - Налаштування мережі	Це повідомлення відображається, коли ❏ Сканер не підключено до мережі ❏ Сервер SMTP не працює ❏ Мережеве з'єднання припинилося під час підключення ❏ Отримано неповні дані
Помилка зв'язку серверу POP3. Перевірте наступне. - Налаштування мережі	Це повідомлення відображається, коли ❏ Сканер не підключено до мережі ❏ Сервер POP3 не працює ❏ Мережеве з'єднання припинилося під час підключення ❏ Отримано неповні дані
Виникла помилка під час підключення до серверу SMTP. Перевірте наступне. - Адреса сервераSMTP - Сервер DNS	Це повідомлення відображається, коли ❏ Не вдалося підключитися до сервера DNS ❏ Не вдалося розібрати ім'я для сервера SMTP
Виникла помилка під час підключення до серверу POP3. Перевірте наступне. - Адреса сервераPOP3 - Сервер DNS	Це повідомлення відображається, коли ❏ Не вдалося підключитися до сервера DNS ❏ Помилка розпізнавання імені сервера POP3
Помилка автентифікації сервера SMTP. Перевірте наступне. -Метод автентифікації - Автентифікований обліковий запис - Автентифікований пароль	Це повідомлення відображається, коли не вдалося пройти автентифікацію на сервері SMTP.
Помилка автентифікації сервера POP3. Перевірте наступне. - Метод автентифікації - Автентифікований обліковий запис - Автентифікований пароль	Це повідомлення відображається, коли не вдалося пройти автентифікацію на сервері POP3.
Метод зв'язку, що не підтримується. Перевірте наступне. - Адреса сервера SMTP - Номер порту сервера SMTP	Це повідомлення відображається, коли робиться спроба підключитися за допомогою протоколів, які не підтримуються.
Невдале підключення до серверу SMTP. Змініть Надійне підключення на Немає.	Це повідомлення відображається, коли сервер та клієнт не збігаються на сервері SMTP або коли сервер не підтримує безпечне підключення SMTP (SSL-підключення).
Невдале підключення до серверу SMTP. Змініть Надійне підключення на SSL/TLS.	Це повідомлення відображається, коли сервер та клієнт не збігаються на сервері SMTP або коли сервер подає запит на використання з'єднання SSL/TLS для безпечного підключення SMTP.
Невдале підключення до серверу SMTP. Змініть Надійне підключення на STARTTLS.	Це повідомлення відображається, коли сервер та клієнт не збігаються на сервері SMTP або коли сервер подає запит на використання з'єднання STARTTLS для безпечного підключення SMTP.

Повідомлення	Причина
Підключення ненадійне. Перевірте наступне. - Дата і час	Це повідомлення відображається, коли неправильно вказано дату і час на сканері або термін дії сертифіката завершився.
Підключення ненадійне. Перевірте наступне. - Сертифікат CA	Це повідомлення відображається, коли сканер не має кореневого сертифіката, що відповідає серверу, або Сертифікат CA не імпортовано.
Підключення незахищене.	Це повідомлення відображається, коли пошкоджено отриманий сертифікат.
Невдала автентифікація сервера SMTP. Змініть метод автентифікації на SMTP-AUTH.	Це повідомлення відображається, коли спосіб автентифікації не збігається між сервером і клієнтом. Сервер підтримує аутентифікація SMTP.
Невдала автентифікація сервера SMTP. Змініть метод автентифікації на POP перед SMTP.	Це повідомлення відображається, коли спосіб автентифікації не збігається між сервером і клієнтом. Сервер не підтримує аутентифікація SMTP.
Адреса ел. пошти відправника неправильна. Змініть на адресу вашої ел. пошти.	Це повідомлення відображається, коли неправильно вказано адресу електронної пошти відправника.
Немає доступу до продукту, доки обробку не буде завершено.	Це повідомлення відображається, коли сканер зайнятий.

Налаштування спільної мережевої папки

Налаштуйте спільну мережеву папку, щоб зберегти скановане зображення.

У разі зберігання файлу в папку, сканер здійснює вхід як користувач комп'ютера, на якому було створено папку.

Створення спільної папки

Пов'язані відомості

- «До початку створення спільної папки» на сторінці 46
- «Перевірка профілю мережі» на сторінці 47
- «Місце створення спільної папки та приклад безпеки» на сторінці 47
- «Додавання групи або користувача для надання доступу» на сторінці 61

До початку створення спільної папки

Перед створенням спільної папки перевірте таке.

❏ Сканер під'єднано до мережі, в якій він має доступ до комп'ютера, на якому буде створено спільну папку.

❏ Ім'я комп'ютера, на якому буде створено спільну папка, не містить багатобайтових символів.

Важливо

Якщо до імені комп'ютера входять багатобайтові символи, то може виникнути помилка збереження файлу у спільній папці.

У такому випадку, замініть на комп'ютер, в імені якого немає багатобайтових символів, або змініть ім'я комп'ютера.

Погодьте заздалегідь з адміністратором зміну імені комп'ютера, оскільки це може вплинути на деякі налаштування, такі як керування комп'ютером, доступ до ресурсу і т.д.

Перевірка профілю мережі

Перевірте можливість надання спільного доступу до папки на комп'ютері, де буде створена спільна папка.

1. Увійдіть до комп'ютера, де буде створено спільну папку, за допомогою облікового запису адміністратора.

2. Виберіть **Панель керування** > **Мережа й Інтернет** > **Центр мереж і спільного доступу**.

3. Натисніть **Змінити додаткові настройки спільного доступу**, а потім натисніть , щоб вибрати профіль з **(поточний профіль)** серед відображених мережевих профілів.

4. Перевірте, чи установлено прапорець на **Ввімкнути спільний доступ для файлів та принтера** у **Спільний доступ для фалів та принтера**.

   Якщо його вже вибрано, натисніть **Скасувати** і закрийте вікно.

   Щоб змінити налаштування, натисніть **Зберегти зміни** і закрийте вікно.

Місце створення спільної папки та приклад безпеки

Безпека та зручність можуть бути різними в залежності від місця створення спільної папки.

Щоб керувати спільною папкою зі сканерів або інших комп'ютерів, необхідно надати такі дозволи читання та зміни для папки.

❏ Вкладка **Спільний доступ** > **Додаткові настройки спільного доступу** > **Дозволи**

Керує дозволами мережевого доступу для спільної папки.

❏ Дозволи доступу вкладки **Безпека**

Керує дозволами доступу до мережі та локальним доступом для спільної папки.

Якщо встановити **Всі** для спільної папки, що створена на робочому столі, як приклад створення спільної папки, всі користувачі, які мають доступ до комп'ютера, будуть мати дозвіл доступу.

Однак, користувач, у якого нема прав, не може відкрити їх, оскільки робочий стіл (папка) знаходиться під контролем папки користувача, а тому налаштування безпеки папки користувача передаються їй. Користувач, якому надано дозвіл доступу у вкладці **Безпека** (користувач, який увійшов, та адміністратор у такому випадку) може керувати папкою.

Див. нижче, щоб створити правильне місце розташування.

Це приклад створення папки «scan_folder».

Пов'язані відомості

➡ «Приклад конфігурації для файлових серверів» на сторінці 48

➡ «Приклад конфігурації для персонального комп'ютера» на сторінці 55

Приклад конфігурації для файлових серверів

Це пояснення є прикладом створення спільної папки у кореневому каталозі драйвера на загальному комп'ютері, як от файловий сервер, за таких умов.

Увійдіть до контрольованих користувачів, як от до когось, хто має однаковий домен комп'ютера для створення спільної папки, мають доступ до спільної папки.

Встановіть цю конфігурацію, якщо ви дозволяєте будь-якому користувачу читання та запис у спільній папці у комп'ютері, як от файловий сервер та загальний комп'ютер.

❏ Місце створення спільної папки: кореневий каталог драйвера

❏ Шлях до папки: C:\scan_folder

❏ Дозвіл доступу через мережу (Дозволи для спільного ресурсу): всі

❏ Дозвіл доступу до системних файлів (Безпека): автентифіковані користувачі

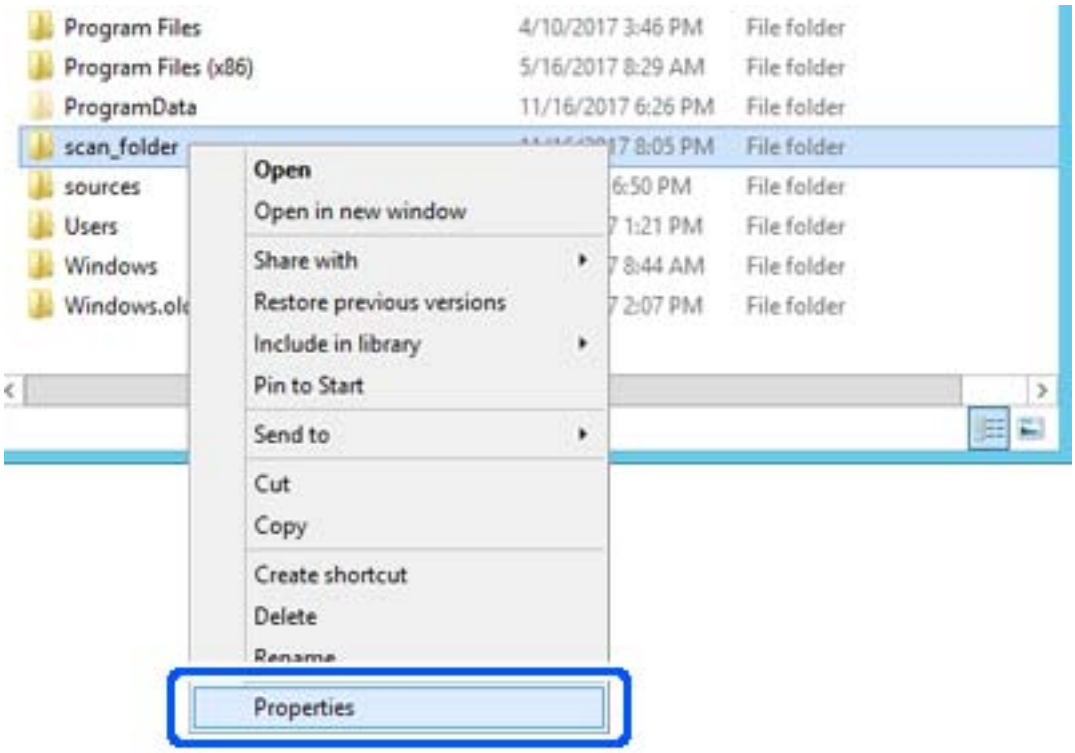
1. Увійдіть до комп'ютера, де буде створено спільну папку, за допомогою облікового запису адміністратора.

2. Запустіть переглядач.

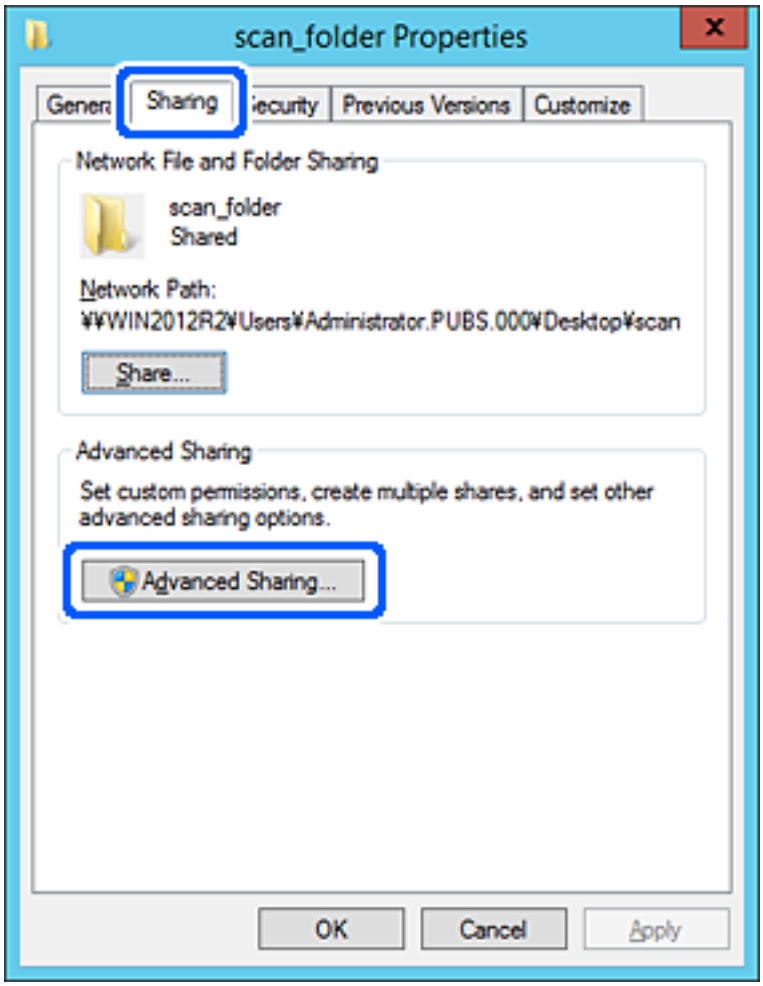
3. Створіть папку в кореневому каталозі драйвера, а тоді назвіть її «scan_folder».

   Введіть від 1 до 12 алфавітно-цифрових символів для імені папки. Якщо перевищено ліміт кількості символів для імені папки, різноманітне середовище, можливо, не матиме адекватного доступу до неї.

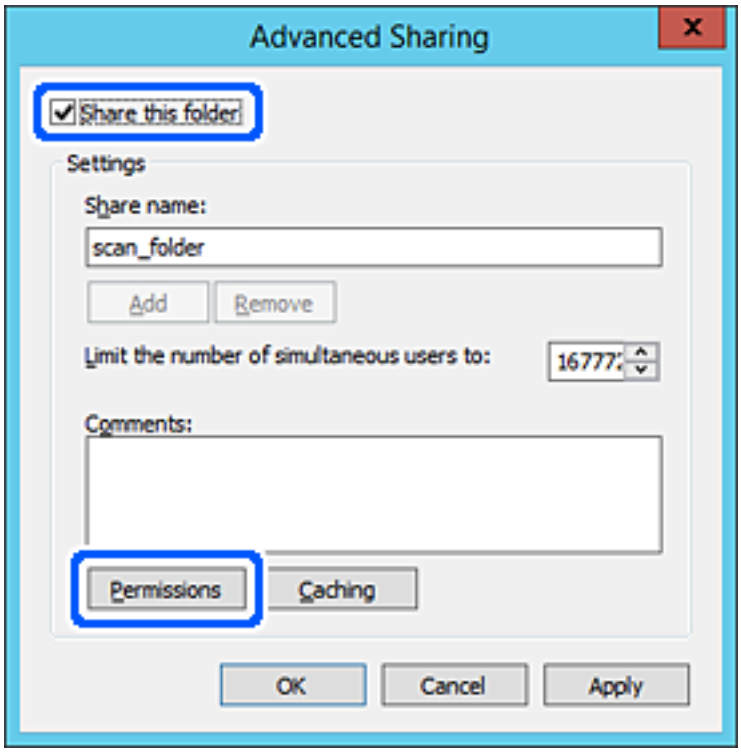
4. Клацніть правою клавішею миші на папці, а тоді виберіть **Властивості**.



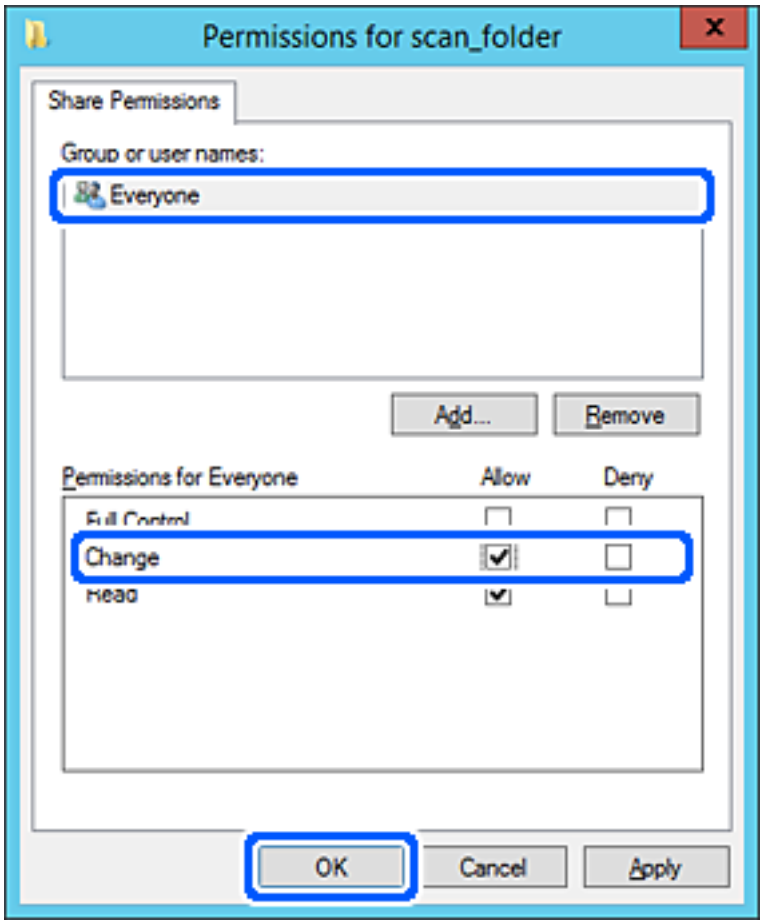
5. Клацніть **Додаткові настройки спільного доступу** у вкладці **Спільний доступ**.



6. Виберіть **Надати спільний доступ до цієї папки**, а тоді клацніть **Дозвіл**.

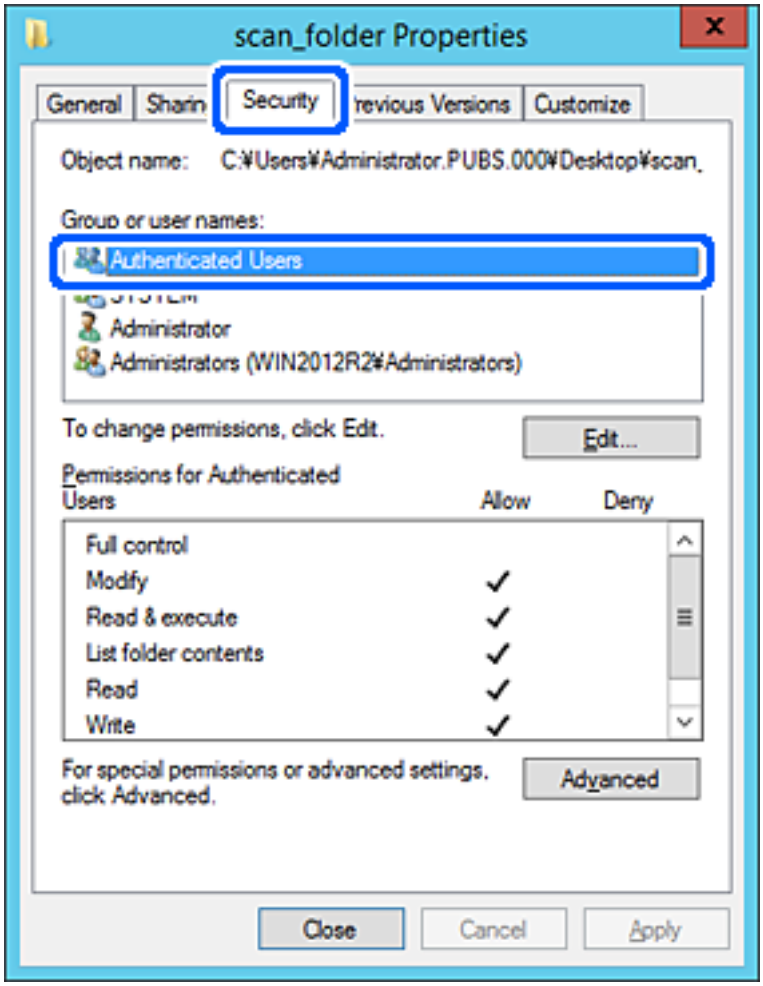


7. Виберіть групу **Всі** в розділі **Ім'я групи або користувача**, виберіть **Дозволити** у **Змінити**, а тоді клацніть **OK**.



8. Клацніть **OK**.

9. Виберіть вкладку **Безпека**, а тоді виберіть **Автентифіковані користувачі** у **Ім’я групи або користувача**.

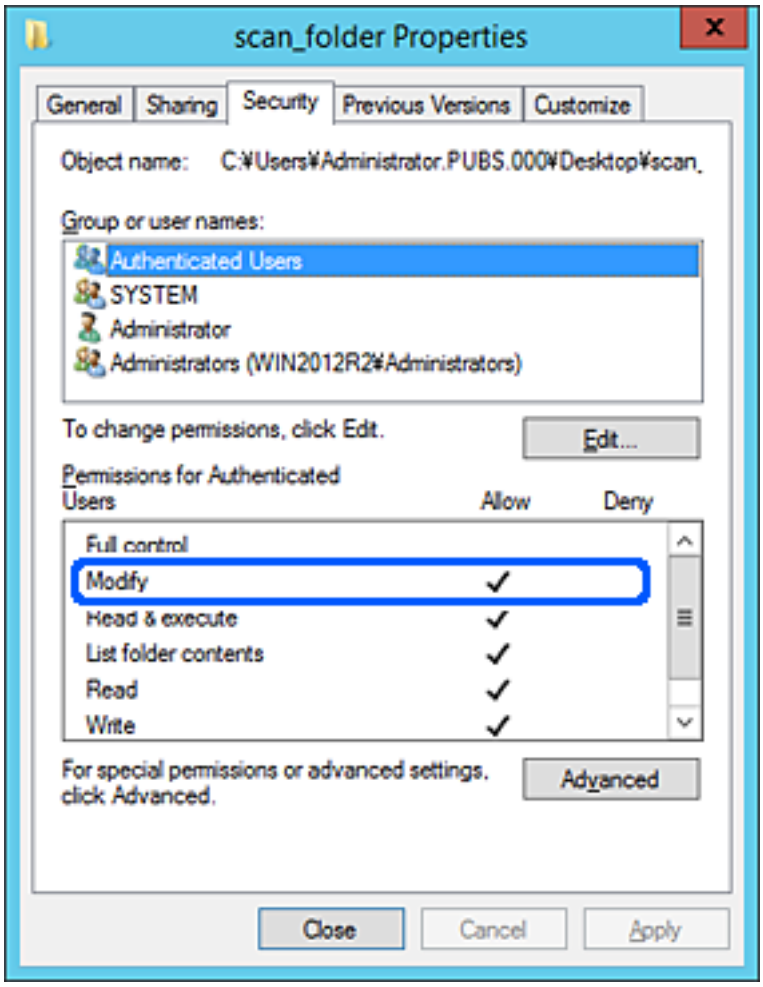


«Автентифіковані користувачі» — це спеціальна група, яка включає всіх користувачів, які можуть входити на домен або у комп’ютер. Ця група відображається тільки, якщо папка створена прямо під кореневою папкою.

Якщо вона не відображається, її можна додати, клацнувши **Редагувати**. Докладнішу інформацію див. у розділі «Пов’язані відомості».

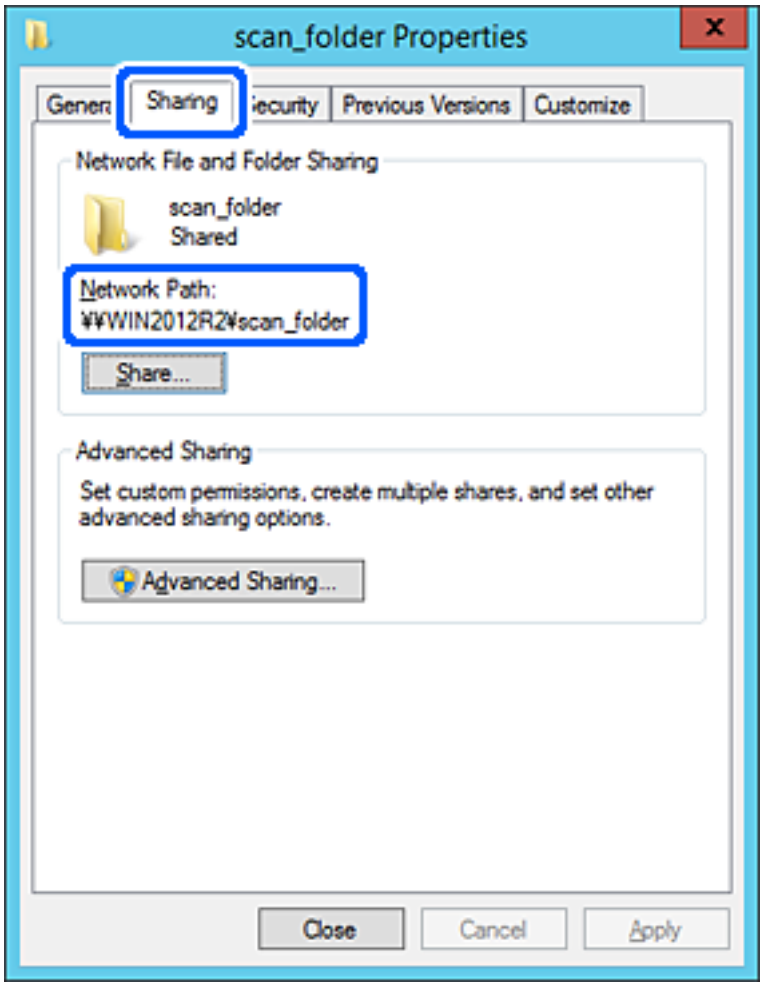
10. Перевірте, щоб **Дозволити** на **Змінити** було вибрано у **Дозволи для автентифікованих користувачів**.

    Якщо не вибрано, виберіть **Автентифіковані користувачі**, клацніть **Редагувати**, виберіть **Дозволити** на **Змінити** у **Дозволи для автентифікованих користувачів**, а тоді клацніть **OK**.



11. Виберіть вкладку **Спільний доступ**.

    Відображено мережевий шлях до спільної папки. Він використовується, якщо здійснюється реєстрація до контактів сканера. Запишіть його.



12. Клацніть **OK** або **Закрити**, щоб закрити екран.

    Перевірте, чи можна записати або прочитати файл у спільній папці з комп'ютерів одного домену.

Пов'язані відомості

➡ «Додавання групи або користувача для надання доступу» на сторінці 61

➡ «Реєстрація напряму до контактів з використанням Web Config» на сторінці 66

Приклад конфігурації для персонального комп'ютера

Це пояснення є прикладом створення спільної папки на робочому столі користувача, який зараз увійшов у комп'ютер.

Користувач, який увійшов у комп'ютер та має права адміністратора, має доступ до папки робочого стола та папки документів, що знаходиться під папкою користувача.

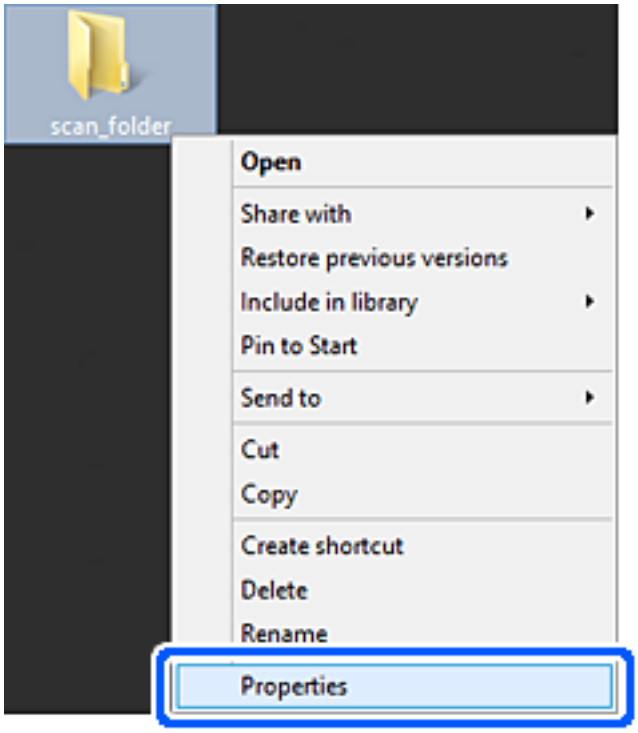
Встановіть цю конфігурацію, якщо ви НЕ ДОЗВОЛЯЄТЕ читання та запис спільної папки іншому користувачу на персональному комп'ютері.

❏ Місце створення спільної папки: робочий стіл

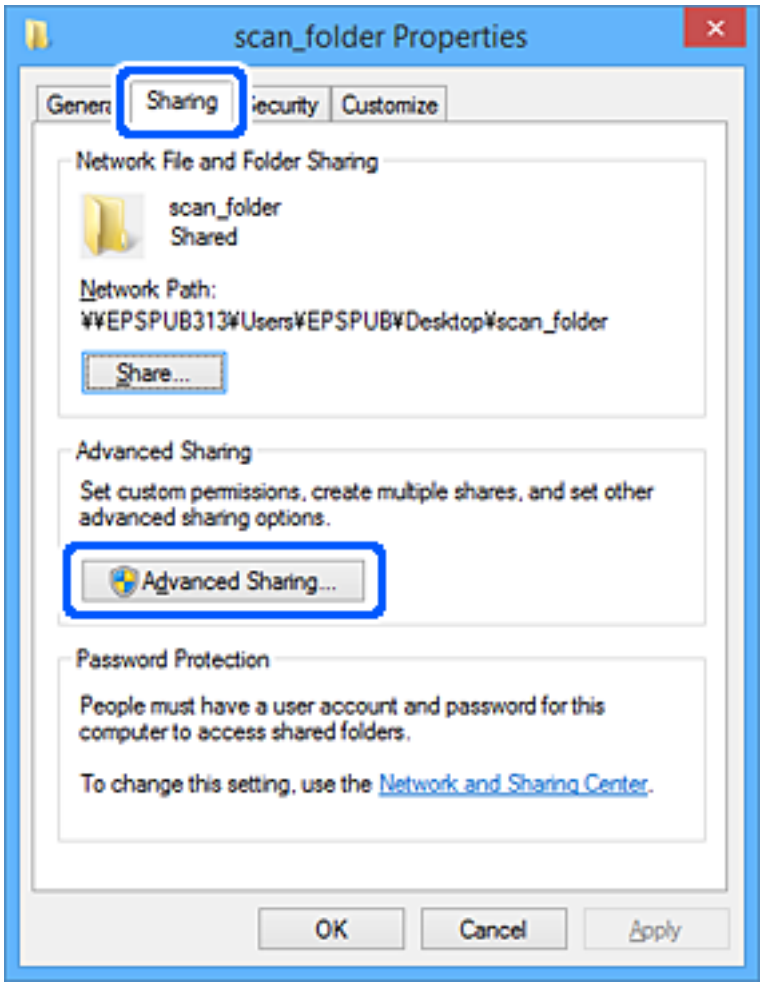
- ❏ Шлях до папки: C:\Users\xxxx\Desktop\scan_folder
- ❏ Дозвіл доступу через мережу (Дозволи для спільного ресурсу): всі
- ❏ Дозвіл доступу до файлової системи (Безпека): не додавати, або додати ім'я користувача/групи, якому/якій дозволити доступ

1. Увійдіть до комп'ютера, де буде створено спільну папку, за допомогою облікового запису адміністратора.
2. Запустіть переглядач.
3. Створіть папку на робочому столі, а тоді назвіть її «scan_folder».

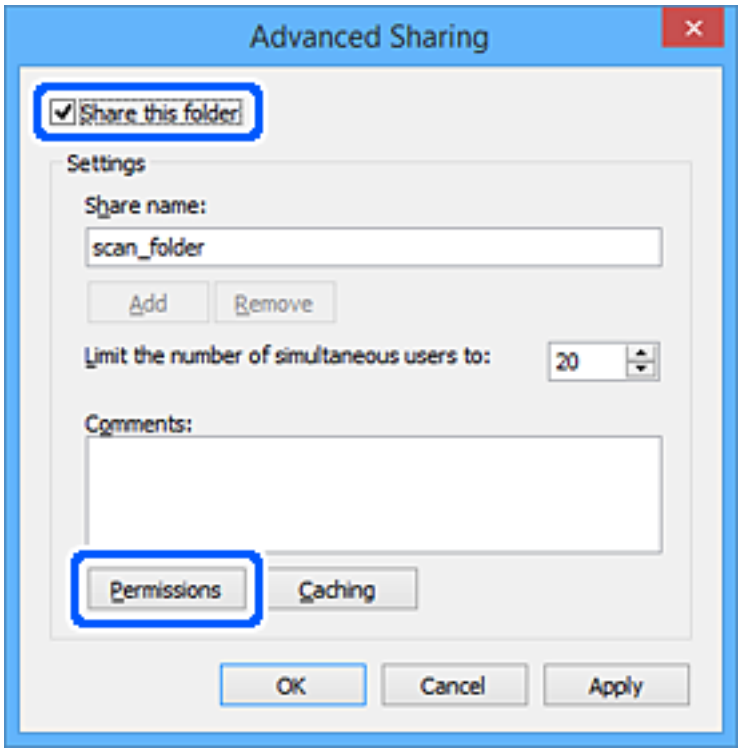
   Введіть від 1 до 12 алфавітно-цифрових символів для імені папки. Якщо перевищено ліміт кількості символів для імені папки, різноманітне середовище, можливо, не матиме адекватного доступу до неї.
4. Клацніть правою клавішею миші на папці, а тоді виберіть **Властивості**.



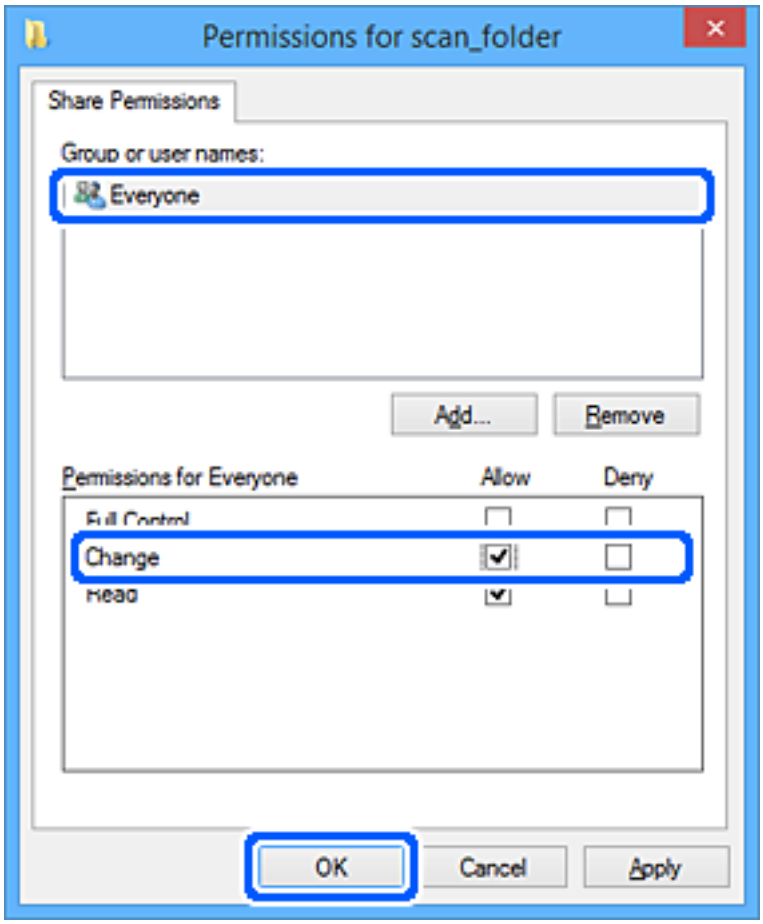
5. Клацніть **Додаткові настройки спільного доступу** у вкладці **Спільний доступ**.



6. Виберіть **Надати спільний доступ до цієї папки**, а тоді клацніть **Дозвіл**.



7. Виберіть групу **Всі** в розділі **Ім'я групи або користувача**, виберіть **Дозволити** у **Змінити**, а тоді клацніть **OK**.



8. Клацніть **OK**.

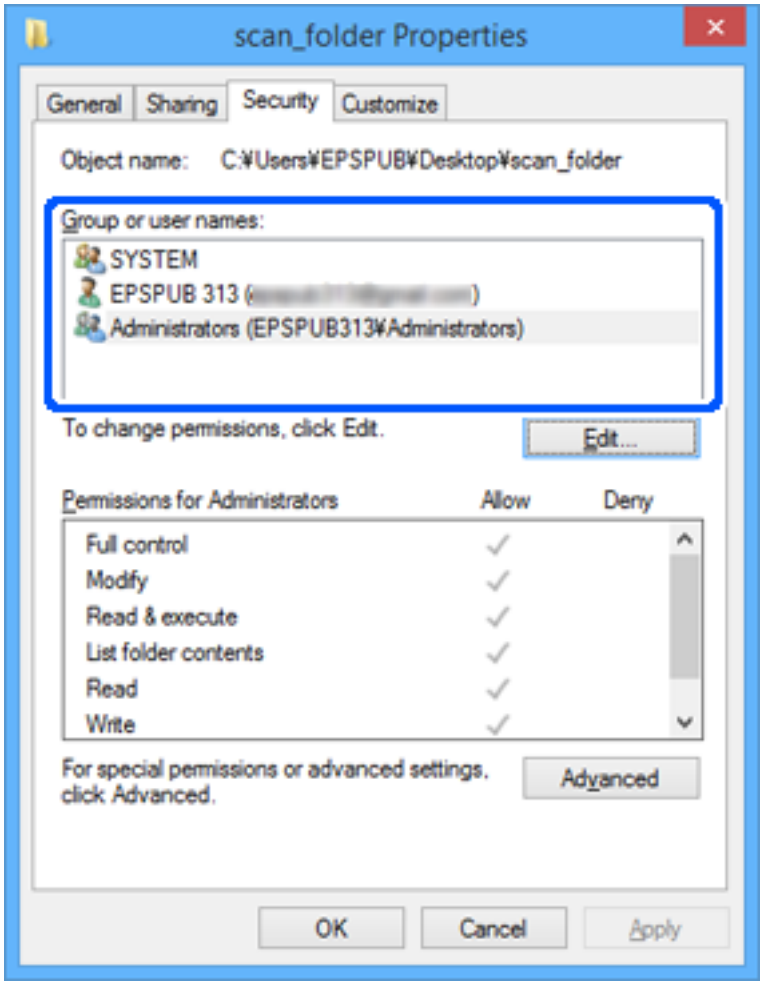
9. Виберіть вкладку **Безпека**.

10. Перевірте групу або користувача у розділі **Імена груп або користувачів**.

    Група або користувач, які тут відображаються, мають доступ до спільної папки.

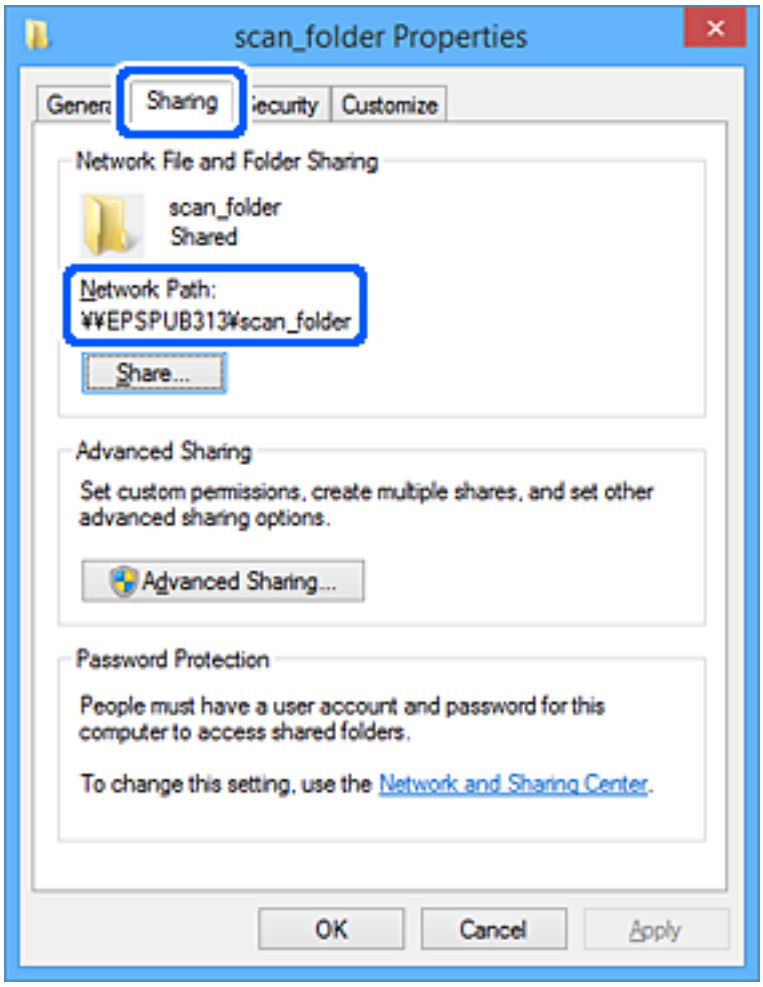
    У такому разі користувач, який входить у цей комп'ютер, та адміністратор мають доступ до спільної папки.

Додайте дозвіл доступу у разі потреби. Його можна додати, клацнувши **Редагувати**. Докладнішу інформацію див. у розділі «Пов'язані відомості».



11. Виберіть вкладку **Спільний доступ**.

    Відображено мережевий шлях до спільної папки. Він використовується, якщо здійснюється реєстрація до контактів сканера. Запишіть його.



12. Клацніть **OK** або **Закрити**, щоб закрити екран.

    Перевірте, чи можна записати або прочитати файл у спільній папці з комп'ютерів користувачів або груп, які мають дозвіл доступу.

Пов'язані відомості

➡ «Додавання групи або користувача для надання доступу» на сторінці 61

➡ «Реєстрація напряму до контактів з використанням Web Config» на сторінці 66

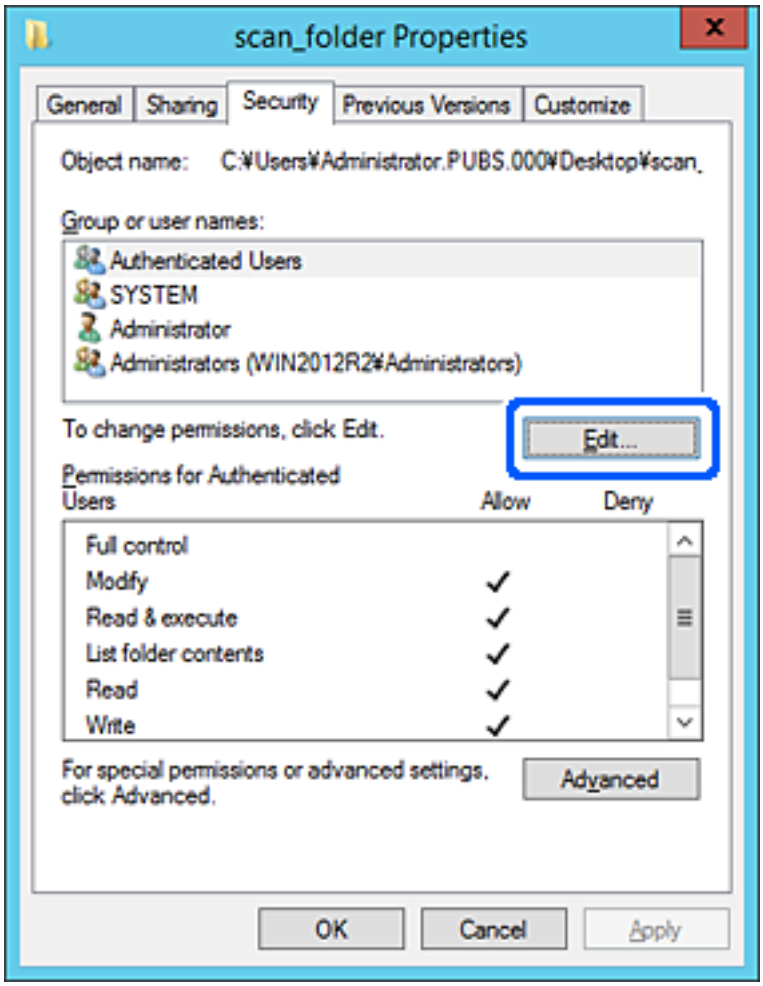
Додавання групи або користувача для надання доступу

Можна додати групу або користувача для надання доступу.

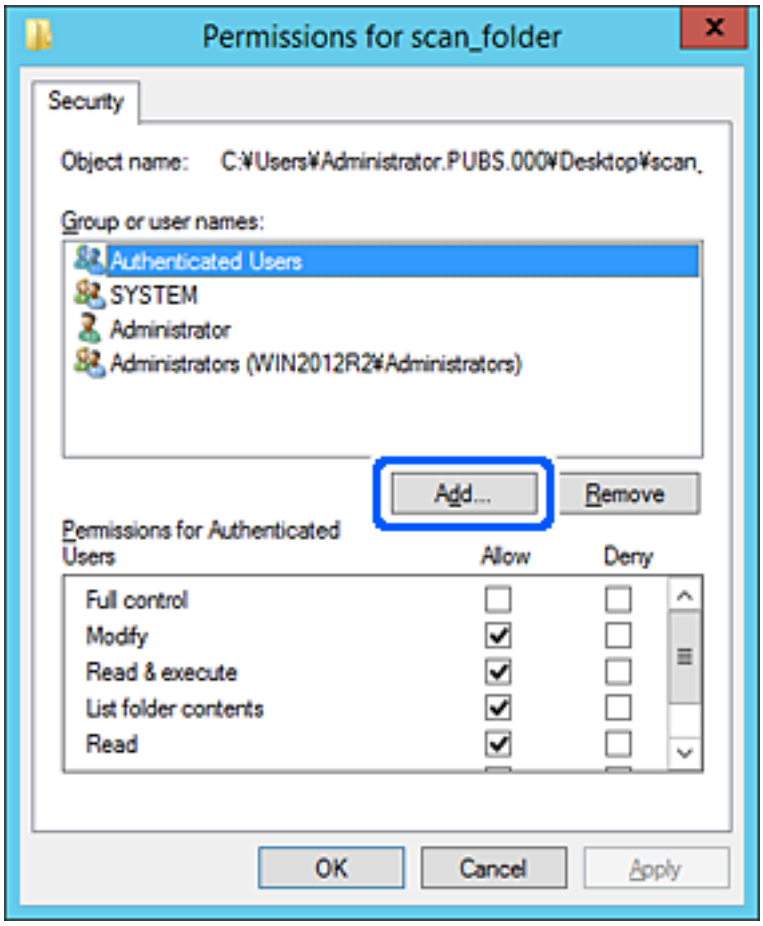
1. Клацніть правою клавішею миші на папці, а тоді натисніть **Властивості**.

2. Виберіть вкладку **Безпека**.

3. Клацніть **Редагувати**.



4. Клацніть **Додати** під списком **Імена груп або користувачів**.

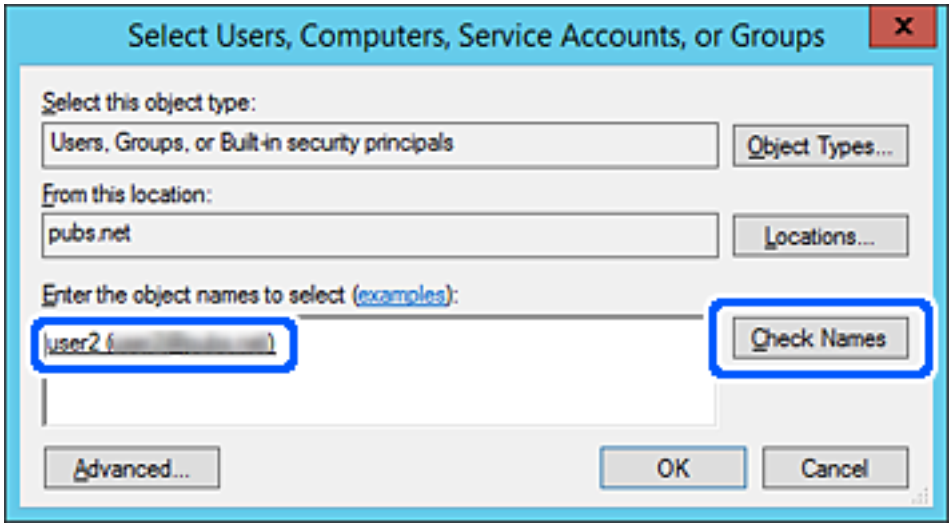


5. Введіть ім’я групи або користувача, якому ви хочете надати доступ, а потім клацніть **Перевірити імена**.

   Додано підкреслення імені.

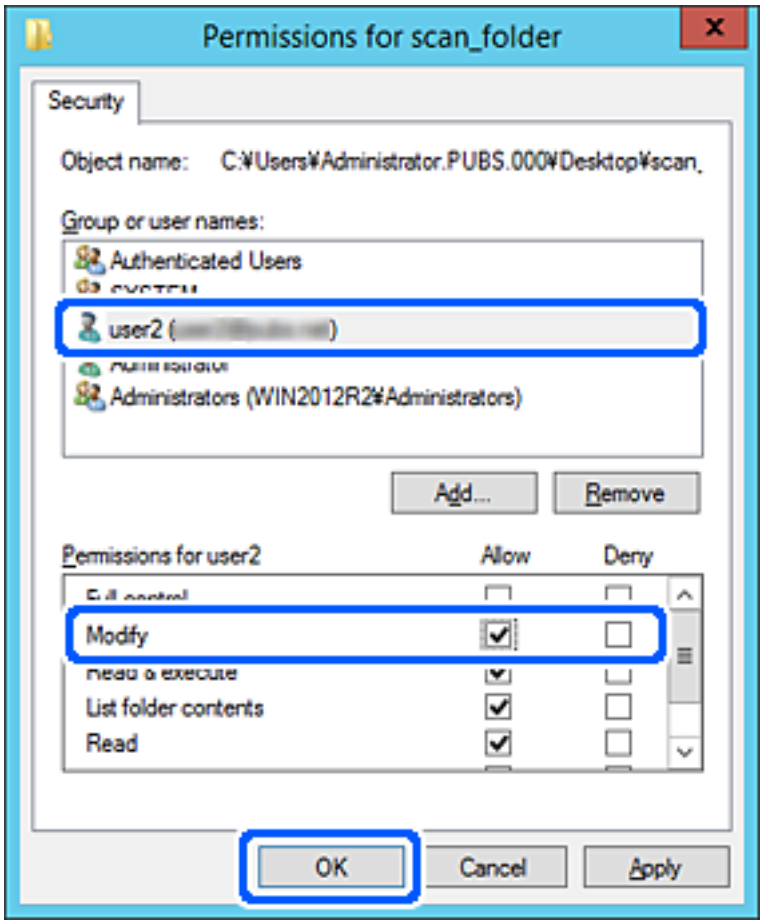
Примітка.
Якщо ви не знаєте повне ім'я групи чи користувача, введіть частину імені, а потім натисніть ***Перевірити імена****. Коли відобразиться список імен груп або користувачів, що відповідають частині імені, можна вибрати повне ім'я зі списку.*

Якщо відповідає тільки одне ім'я, повне ім'я з підкресленням відобразиться у рядку ***Введіть ім'я об'єкта, щоб зробити вибір****.*



6. Клацніть **OK**.

7. На екрані Дозволів виберіть ім’я користувача, що додане до списку **Імена груп або користувачів**, виберіть дозвіл доступу у вкладці **Змінити**, а тоді клацніть **OK**.



8. Клацніть **OK** або **Закрити**, щоб закрити екран.

   Перевірте, чи можна записати або прочитати файл у спільній папці з комп’ютерів користувачів або груп, які мають дозвіл доступу.

Відкриття доступу до контактів

Реєстрація місць призначення у списку контактів сканера дасть змогу легко вводити місце призначення під час сканування.

У списку контактів можна зареєструвати такі типи місць призначення. Ви можете зберегти максимум 300.

Примітка.
Для введення місця призначення можна також використовувати сервер LDAP (пошук LDAP).

Адреса ел. пошти	Місце призначення для електронної пошти. Необхідно заздалегідь налаштувати сервер електронної пошти.
Мережева папка	Папка для даних сканування. Мережеву папку слід підготувати заздалегідь.

Пов'язані відомості

➡ «Взаємодія між сервером LDAP та користувачами» на сторінці 72

Порівняння налаштувань контактів

Налаштування контактів сканера виконується за допомогою трьох інструментів: Web Config, Epson Device Admin і панель керування сканера. Відмінності між цими трьома інструментами наведені в таблиці нижче.

Функціональні можливості	Web Config*	Epson Device Admin	Панель керування сканера
Реєстрація призначення	✓	✓	✓
Редагування призначення	✓	✓	✓
Додавання групи	✓	✓	✓
Редагування групи	✓	✓	✓
Видалення призначень і груп	✓	✓	✓
Видалення всіх призначень	✓	✓	–
Імпорт файлів	✓	✓	–
Експорт файлів	✓	✓	–

* Для налаштування увійдіть із правами адміністратора.

Реєстрація напряму до контактів з використанням Web Config

Примітка.
Реєстрацію контактів також можна виконати на панелі керування сканера.

1. Відкрийте Web Config і виберіть вкладку **Скан.** > **Контакти**.
2. Виберіть номер, який потрібно зареєструвати, після чого натисніть **Редагувати**.
3. Введіть **Назва** та **Індексне слово**.
4. Виберіть тип призначення в полі **Тип**.

   Примітка.
   *Змінити вибір значення **Тип** після реєстрації не можна. Якщо необхідно змінити тип на інший, видаліть призначення та виконайте реєстрацію ще раз.*
5. Введіть значення для кожного елемента, а потім натисніть **Застосувати**.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Елементи налаштування місця призначення

Параметри	Налаштування та пояснення
Загальні параметри	
Назва	Уведіть ім'я, що відображається у контактах розміром до 30 символів у форматі Unicode (UTF-8). Якщо дані вводити непотрібно, лишіть поле пустим.
Індексне слово	Уведіть ім'я, використавши до 30 символів у форматі Unicode (UTF-8), для пошуку контаків у панелі керування сканера. Якщо дані вводити непотрібно, лишіть поле пустим.
Тип	Виберіть тип адреси, який потрібно зареєструвати.
Призначити для частого використ.	Виберіть, щоб налаштувати зареєстровану адресу як таку, що часто використовується. У разі налаштування адреси, як такої, що часто використовується, її буде відображено на верхньому екрані сканованого зображення, і ви зможете указати адресата, не відкриваючи контакти.
Ел. адреса	
Ел. адреса	Введіть від 1 до 255 символів, використовуючи символи A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Мережева папка (SMB)	
Зберегти в	\\«Шлях до папки» Уведіть місце розташування цільової папки, використовуючи від 1 до 253 символів формату Unicode (UTF-8), упускаючи «\\». Уведіть мережевий шлях, відображений на екрані властивостей папки. Докладніше про налаштування мережевого шляху див. нижче. «Приклад конфігурації для персонального комп'ютера» на сторінці 55
Ім'я користувача	Уведіть ім'я користувача для доступу до мережевої папки, використавши до 30 символів у форматі Unicode (UTF-8). Слід уникати використання символів керування (від 0x00 до 0x1F, 0x7F).
Пароль	Уведіть пароль для доступу до мережевої папки, використавши до 20 символів у форматі Unicode (UTF-8). Слід уникати використання символів керування (від 0x00 до 0x1F, 0x7F).
FTP	
Надійне підключення	Виберіть FTP або FTPS згідно з протоколом передачі файлів, який підтримує FTP-сервер. Виберіть **FTPS**, щоб дозволити сканеру здійснювати зв'язок із використанням заходів безпеки.
Зберегти в	Введіть ім'я сервера, використовуючи від 1 до 253 символів у кодуванні ASCII (0x20–0x7E), пропускаючи «ftp://» або «ftps://».
Ім'я користувача	Уведіть ім'я користувача для доступу до сервера FTP, використавши до 30 символів у форматі Unicode (UTF-8). Слід уникати використання символів керування (від 0x00 до 0x1F, 0x7F). Якщо на сервері допускається анонімний вхід, уведіть ім'я користувача, наприклад, «Анонім», та вкажіть FTP. Якщо дані вводити непотрібно, лишіть поле пустим.
Пароль	Уведіть пароль для доступу до сервера FTP, використавши до 20 символів у форматі Unicode (UTF-8). Слід уникати використання символів керування (від 0x00 до 0x1F, 0x7F). Якщо дані вводити непотрібно, лишіть поле пустим.

Параметри	Налаштування та пояснення
Режим підключення	Виберіть режим підключення з меню. Якщо між сканером і FTP-сервером установлено брандмауер, виберіть **Пасивний режим**.
Номер порту	Уведіть номер порту сервера FTP за допомогою чисел від 1 до 65535.
Перевірка сертифікату	Після підключення буде перевірено сертифікат FTP-сервера. Воно доступне, коли **FTPS** вибрано для **Надійне підключення**. Для налаштування необхідно імпортувати Сертифікат CA на сканер.
SharePoint(WebDAV)	
Надійне підключення	Виберіть HTTP або HTTPS згідно з протоколом передачі файлів, який підтримує сервер. Виберіть **HTTPS**, щоб дозволити сканеру здійснювати зв'язок із використанням заходів безпеки.
Зберегти в	Введіть ім'я сервера, використовуючи від 1 до 253 символів у кодуванні ASCII (0x20–0x7E), пропускаючи «http://» або «https://».
Ім'я користувача	Уведіть ім'я користувача для доступу до сервера, використавши до 30 символів у форматі Unicode (UTF-8). Слід уникати використання символів керування (від 0x00 до 0x1F, 0x7F). Якщо дані вводити непотрібно, лишіть поле пустим.
Пароль	Уведіть пароль для доступу до сервера, використавши до 20 символів у форматі Unicode (UTF-8). Слід уникати використання символів керування (від 0x00 до 0x1F, 0x7F). Якщо дані вводити непотрібно, лишіть поле пустим.
Перевірка сертифікату	Після підключення буде перевірено сертифікат сервера. Воно доступне, коли **HTTPS** вибрано для **Надійне підключення**. Для налаштування необхідно імпортувати Сертифікат CA на сканер.
Проксі-сервер	Виберіть, чи потрібно використовувати проксі-сервер.

Реєстрація місць призначення як групи за допомогою Web Config

Якщо типом призначення вибрано **Ел. адреса**, ви можете зареєструвати місця призначення як групу.

1. Відкрийте Web Config і виберіть вкладку **Скан.** > **Контакти**.
2. Виберіть номер, який потрібно зареєструвати, після чого натисніть **Редагувати**.
3. Виберіть групу з **Тип**.
4. Клацніть **Вибрати** для **Контакти для групи**.
   Буде відображено доступне місця призначення.
5. Виберіть місце призначення, яке потрібно зареєструвати у групу, після чого клацніть **Вибрати**.
6. Введіть **Назва** та **Індексне слово**.

7. Виберіть, чи потрібно внести зареєстровану групу до тих, що часто використовуються.

   Примітка.
   Місця призначення можна реєструвати в кілька груп.

8. Клацніть **Застосувати**.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Резервне копіювання та імпортування контактів

За допомогою Web Config або інших інструментів можна зробити резервну копію або імпортувати контакти.

Для Web Config: можна зробити резервну копію контактів за допомогою експортування налаштувань сканера, що містять контакти. Експортований файл не можна редагувати, оскільки його експортовано як бінарний файл.

Під час імпортування на сканер налаштувань сканера, контакти перезаписуються.

Для Epson Device Admin: з екрана властивостей пристрою можна експортувати тільки контакти. Також, якщо ви не експортуєте елементи, пов'язані з безпекою, то можна редагувати експортовані контакти та імпортувати їх, оскільки їх можна зберегти як файли у форматі SYLK або CSV.

Імпортування контактів за допомогою Web Config

Якщо у вас є сканер, який дозволяє створювати резервні копії контактів і сумісний з цим сканером, ви можете легко зареєструвати контакти, імпортувавши їх із файлу резервної копії.

Примітка.
Див. вказівки щодо створення резервної копії контактів у посібнику до сканера.

Щоб імпортувати контакти на цей сканер, виконайте наведені нижче кроки.

1. Відкрийте Web Config, виберіть вкладку **Керування пристроєм** > **Експортувати та імпортувати значення налаштування** > **Імпорт**.

2. Виберіть файл резервної копії, створеної в **Файл**, введіть пароль, після чого клацніть **Далі**.

3. Установіть прапорець **Контакти**, після чого клацніть **Далі**.

Резервне копіювання контактів за допомогою Web Config

Контактні дані можуть бути втрачені через несправність сканера. Ми рекомендуємо робити копії даних під час кожного оновлення даних. Компанія Epson не несе відповідальності за втрату будь-яких даних, а також не зобов'язана виконувати резервне копіювання чи відновлення даних і настройок навіть під час гарантійного строку.

Крім того, за допомогою Web Config можна створити на комп'ютері резервну копію контактних даних, що зберігаються на сканері.

1. Відкрийте Web Config, а тоді виберіть вкладку **Керування пристроєм** > **Експортувати та імпортувати значення налаштування** > **Експорт**.
2. Установіть прапорець **Контакти** у категорії **Скан.**.
3. Введіть пароль для кодування експортованого файлу.

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

Експортування та групова реєстрація контактів за допомогою інструменту

Якщо ви використовуєте Epson Device Admin, можна створити резервну копію лише контактів та редагувати експортовані файли, а потім всі їх зареєструвати.

Це корисно, коли потрібно створити резервну копію тільки контактів, або потрібно замінити сканер і перенести контакти зі старого сканера на новий.

Експортування контактів

Збережіть дані контактів у файл.

Можна редагувати файли, що збережені у форматі SYLK або csv за допомогою табличного додатку або текстового редактора. Можна зареєструвати всі контакти разом після видалення або додавання інформації.

Інформацію, яка включає елементи безпеки, такі як пароль або персональні дані, можна зберегти у бінарному форматі з паролем. Файл не можна редагувати. Він може бути використаний як резервна копія інформації, що включає елементи безпеки.

1. Запустіть Epson Device Admin.
2. Виберіть **Devices** на бічній панелі меню завдань.
3. Виберіть пристрій, який необхідно налаштувати, зі списку пристроїв.
4. Клацніть **Device Configuration** у вкладці **Home** у стрічковому меню.

   Коли встановлено пароль адміністратора, введіть пароль і клацніть **OK**.
5. Клацніть **Common** > **Contacts**.
6. Виберіть формат експортування у **Export** > **Export items**.

   ❏ All Items

   Експортуйте зашифрований бінарний файл. Виберіть, коли необхідно включити елементи безпеки, такі як пароль та персональні дані. Файл не можна редагувати. Якщо ви виберете його, то необхідно встановити пароль. Клацніть **Configuration** та встановіть пароль довжиною від 8 до 63 символів формату ASCII. Цей пароль потрібен під час імпортування бінарного файлу.

❏ Items except Security Information

Експортуйте файли у форматі SYLK або csv. Виберіть, коли потрібно редагувати дані експортованого файлу.

7. Клацніть **Export**.

8. Вкажіть місце збереження файлу, виберіть тип файлу, а тоді клацніть **Save**.

Відобразиться повідомлення про завершення.

9. Клацніть **OK**.

Перевірте, чи зберігся файл у вказаному місці.

Імпортування контактів

Імпортуйте дані контактів з файлу.

Можна імпортувати файли, що збережені у форматі SYLK або csv, або резервний бінарний файл, який має елементи безпеки.

1. Запустіть Epson Device Admin.

2. Виберіть **Devices** на бічній панелі меню завдань.

3. Виберіть пристрій, який необхідно налаштувати, зі списку пристроїв.

4. Клацніть **Device Configuration** у вкладці **Home** у стрічковому меню.

Коли встановлено пароль адміністратора, введіть пароль і клацніть **OK**.

5. Клацніть **Common** > **Contacts**.

6. Клацніть **Browse** у **Import**.

7. Виберіть файл, який потрібно імпортувати, а тоді клацніть **Open**.

Коли ви вибрали бінарний файл, у **Password** введіть пароль, що було встановлено при експортуванні файлу.

8. Клацніть **Import**.

Відобразиться екран підтвердження.

9. Клацніть **OK**.

Відобразиться результат перевірки.

❏ Edit the information read

Клацніть, коли потрібно індивідуально редагувати інформацію.

❏ Read more file

Клацніть, коли потрібно імпортувати кілька файлів.

10. Клацніть **Import**, а тоді натисніть **OK** на екрані завершення імпортування.

    Поверніться до екрану властивостей пристрою.

11. Клацніть **Transmit**.

12. Клацніть **OK** на повідомлення підтвердження.

    Налаштування відправлено на сканер.

13. На екрані завершення відправлення клацніть **OK**.

    Інформацію про сканер оновлено.

    Відкрийте контакти з Web Config або панелі керування сканера, а тоді перевірте, щоб контакти було оновлено.

Взаємодія між сервером LDAP та користувачами

Під час взаємодії з сервером LDAP можна використовувати інформацію про адресу, що зареєстрована на сервері LDAP, як місце призначення електронної пошти.

Налаштування сервера LDAP

Щоб використовувати інформацію сервера LDAP, зареєструйте її на сканері.

1. Відкрийте Web Config і виберіть вкладку **Мережа** > **Сервер LDAP** > **Основні**.

2. Введіть значення для кожного елемента.

3. Виберіть **OK**.

   Відобразяться вибрані параметри.

Параметри сервера LDAP

Параметри	Налаштування та пояснення
Застосувати Сервер LDAP	Виберіть **Викор.** або **Не використ.**.
LDAP Адреса сервера	Введіть адресу сервера LDAP. Введіть від 1 до 255 символів формату IPv4, IPv6 або FQDN. Для формату FQDN можна використовувати букви або цифри кодування ASCII (0x20–0x7E) і символ «-», за винятком початку і кінця адреси.
LDAP Номер порту сервера	Уведіть номер порту сервера LDAP за допомогою чисел від 1 до 65535.
Надійне підключення	Виберіть спосіб автентифікації для доступу сканера до сервера LDAP.
Перевірка сертифікату	Сертифікат сервера LDAP перевіряється, коли увімкнено цю функція. Рекомендується встановити для неї значення **Увімкн.**. Для налаштування потрібно, щоб **Сертифікат CA** було імпортовано на сканер.
Перерва пошуку (сек)	Установіть ліміт часу пошуку, використовуючи від 5 до 300 символів.

Параметри	Налаштування та пояснення
Метод ідентифікації	Виберіть один із методів. Якщо вибрали **Kerberos Автентифікація**, виберіть **Налаштування Kerberos** для внесення налаштувань для Kerberos. Щоб виконати Kerberos Автентифікація, нижченаведене середовище є обов'язковим. ❏ Сканер та сервер DNS можна з'єднати. ❏ Час, необхідний сканеру, серверу KDC та серверу для автентифікації (сервер LDAP, сервер SMTP, файловий сервер), синхронізується. ❏ Якщо сервер послуг призначено як IP-адресу, то FQDN сервера послуги буде зареєстровано у зворотній зоні пошуку сервера DNS.
Kerberos Область для використання	Якщо вибрали **Kerberos Автентифікація** для **Метод ідентифікації**, то слід вказати область Kerberos, яку потрібно використовувати.
Унікальне ім'я адміністратора / Ім'я користувача	Уведіть ім'я користувача для сервера LDAP, використавши до 128 символів у форматі Unicode (UTF-8). Не можна використовувати керівні символи, такі як 0x00–0x1F та 0x7F. Це значення не потрібне, якщо вибрано **Анонімна автентифікація** для параметра **Метод ідентифікації**. Якщо дані вводити непотрібно, лишіть поле пустим.
Пароль	Уведіть пароль для автентифікації на сервері LDAP, використавши до 128 символів у форматі Unicode (UTF-8). Не можна використовувати керівні символи, такі як 0x00–0x1F та 0x7F. Це значення не потрібне, якщо вибрано **Анонімна автентифікація** для параметра **Метод ідентифікації**. Якщо дані вводити непотрібно, лишіть поле пустим.

Налаштування Kerberos

Якщо вибрати **Kerberos Автентифікація** для **Метод ідентифікації** у **Сервер LDAP** > **Основні**, внесіть вказані нижче налаштування Kerberos у вкладці **Мережа** > **Налаштування Kerberos**. Для налаштування Kerberos можна внести до 10 параметрів.

Параметри	Налаштування та пояснення
Область (домен)	Введіть в області автентифікації Kerberos до 255 символів формату ASCII (0x20–0x7E). Якщо дані вводити непотрібно, залиште поле пустим.
KDC Адреса	Введіть адресу сервера автентифікації Kerberos. Введіть до 255 символів у форматі IPv4, IPv6 або FQDN. Якщо дані вводити непотрібно, залиште поле пустим.
Номер порту (Kerberos)	Уведіть номер порту сервера Kerberos за допомогою чисел від 1 до 65535.

Налаштування параметрів пошуку сервера LDAP

Після налаштування параметрів пошуку, ви зможете використовувати адресу електронної пошти, зареєстровану на сервері LDAP.

1. Відкрийте Web Config і виберіть вкладку **Мережа** > **Сервер LDAP** > **Налаштування пошуку**.

2. Введіть значення для кожного елемента.

3. Клацніть **OK** для відображення результатів налаштування.

   Відобразяться вибрані параметри.

Параметри пошуку сервера LDAP

Параметри	Налаштування та пояснення
Пошук бази (унікальне ім'я)	Щоб знайти довільний домен, укажіть доменне ім'я сервера LDAP. Введіть від 0 до 128 символів формату Юнікод (UTF-8). Якщо шукати довільний атрибут не треба, залиште це поле порожнім. Приклад каталогу локального сервера: dc=сервер,dc=локальний
Кількість пошукових записів	Укажіть кількість пошукових записів від 5 до 500. Зазначена кількість записів пошуку зберігається й тимчасово відображається. Навіть якщо кількість пошукових записів перевищує зазначену кількість і з'являється повідомлення про помилку, пошук може бути завершений.
Ім'я користувача Атрибут	Укажіть ім'я атрибута для відображення під час пошуку імен користувачів. Введіть від 1 до 255 символів формату Юнікод (UTF-8). Першим має бути один із символів a–z або A–Z. Наприклад: cn, uid
Ім'я користувача Показати атрибут	Укажіть ім'я атрибута для відображення як імені користувача. Введіть від 0 до 255 символів формату Юнікод (UTF-8). Першим має бути один із символів a–z або A–Z. Наприклад: cn, sn
Адреса ел. пошти атрибут	Укажіть ім'я атрибута для відображення під час пошуку адрес електронної пошти. Введіть комбінацію від 1 до 255 символів, використовуючи символи A–Z a–z 0–9 та -. Першим має бути один із символів a–z або A–Z. Наприклад: пошта
Довільний атрибут 1 - Довільний атрибут 4	Можна також указати інші довільні атрибути для пошуку. Введіть від 0 до 255 символів формату Юнікод (UTF-8). Першим має бути один із символів a–z або A–Z. Якщо шукати довільний атрибут не треба, залиште це поле порожнім. Наприклад: o, ou

Перевірка з'єднання з сервером LDAP

Виконує перевірку з'єднання з сервером LDAP за допомогою параметра, встановленого в **Сервер LDAP** > **Налаштування пошуку**.

1. Відкрийте Web Config і виберіть вкладку **Мережа** > **Сервер LDAP** > **Перевірка підключення**.

2. Виберіть **Пуск**.

   Почнеться перевірка з'єднання. Після завершення перевірки відображається звіт про її результати.

Повідомлення перевірки з'єднання з сервером LDAP

Повідомлення	Пояснення
Перевірка підключення пройшла успішно.	Це повідомлення відображається тоді, коли відбулося успішне з'єднання з сервером.
Помилка перевірки підключення. Перевірте налаштування.	Це повідомлення з'являється з однієї з нижчезазначених причин: ❏ Адресу сервера LDAP або номер порту вказано невірно. ❏ Минув час очікування. ❏ **Не використ.** вибрано для **Застосувати Сервер LDAP**. ❏ Якщо значення **Kerberos Автентифікація** вибрано для **Метод ідентифікації**, такі налаштування як **Область (домен)**, **KDC Адреса** та **Номер порту (Kerberos)** будуть неправильні.
Помилка перевірки підключення. Перевірте дату й час на виробі чи сервері.	Це повідомлення з'являється в разі виникнення помилки з'єднання, коли налаштування часу сканера та сервера LDAP не збігаються.
Помилка автентифікації. Перевірте налаштування.	Це повідомлення з'являється з однієї з нижчезазначених причин: ❏ Невірно вказано **Ім'я користувача** та/або **Пароль**. ❏ Якщо вибрано **Kerberos Автентифікація** як **Метод ідентифікації**, дату/час, можливо, не вдасться налаштувати.
Немає доступу до продукту, доки обробку не буде завершено.	Це повідомлення відображається, коли сканер зайнято.

Використання Document Capture Pro Server

За допомогою Document Capture Pro Server можна керувати способом сортування, форматом зберігання та одержувачами для пересилання результатів сканування, отриманих за допомогою панелі керування сканера. Можна викликати й виконати попередньо зареєстроване завдання на сервері з панелі керування сканера.

Установіть її на комп'ютері сервера.

Щоб отримати докладнішу інформацію про Document Capture Pro Server, зверніться до місцевого представництва компанії Epson.

Налаштування режиму сервера

Для використання Document Capture Pro Server зробіть налаштування, як це показано нижче.

1. Відкрийте Web Config і виберіть вкладку **Скан.** > **Document Capture Pro**.
2. Виберіть **Режим сервера** для **Режим**.
3. Уведіть адресу сервера зі встановленим Document Capture Pro Server для **Адреса сервера**.

   Введіть від 2 до 255 символів у форматі IPv4, IPv6, імені хосту або FQDN. Для формату FQDN можна використовувати букви або цифри кодування ASCII (0x20–0x7E) і символ «-», за винятком початку і кінця адреси.

4. Клацніть **OK**.

   Мережа повторно підключиться, після чого параметри буде увімкнено.

Налаштування AirPrint

Виберіть вкладку Web Config, тоді виберіть вкладку **Мережа**, після чого виберіть **Настроювання AirPrint**.

Параметри	Пояснення
Службове ім'я Bonjour	Введіть назву служби Bonjour, використовуючи текст ASCII (0x20-0x7E), — до 41 символу.
Розташування Bonjour	Введіть опис розташування сканера, використовуючи текст Unicode (UTF-8) і розмір до 127 байт.
Wide-Area Bonjour	Встановіть, чи потрібно використовувати Wide-Area Bonjour. Якщо ви його використовуєте, сканер має бути зареєстровано на сервері DNS, аби мати можливість шукати сканер через сегмент.
Увімк. AirPrint	Bonjour та AirPrint (служба сканування) увімкнено.

Проблеми з підготування сканування по мережі

Поради щодо вирішення проблем

❏ Перевірка повідомлення про помилку

У разі помилки, спочатку перевірте чи є якісь повідомлення на панелі керування сканера або екрані драйвера. Якщо у вас встановлено сповіщення електронною поштою у разі виникнення помилки, ви можете відразу дізнатись про стан.

❏ Перевірка стану підключення

Перевірте стан підключення сервера комп'ютера або клієнтського комп'ютера за допомогою таких команд, як ping та ipconfig.

❏ Перевірка підключення

Щоб перевірити з'єднання між сканером та поштовим сервером, виконайте перевірку підключення зі сканера. Також перевірте підключення з клієнтського комп'ютера до сервера, щоб перевірити стан підключення.

❏ Ініціалізація налаштувань

Якщо з боку налаштувань та стану підключення не виявлено помилок, проблему можна вирішити, відключивши або ініціалізувавши налаштування мережі сканера, після чого встановити їх знову.

Не вдається відкрити Web Config

Не призначено IP-адресу для сканера.

Solutions

Чинну IP-адресу не можна призначити сканеру. Налаштуйте IP-адресу за допомогою панелі керування сканера. Перевірити правильність поточного налаштування можна з панелі керування сканера.

Веб-браузер не підтримує стійкість шифрування для SSL/TLS.

Solutions

SSL/TLS має Стійкість шифрування. Ви можете відкрити Web Config за допомогою веб-браузера, який підтримує групове шифрування, як показано нижче. Переконайтеся, що ви використовуєте підтримуваний браузер.

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

Термін дії CA-підписаний Сертифікат минув.

Solutions

Якщо виникла проблема з датою спливання терміну дії сертифіката, при підключенні до Web Config за допомогою зв'язку SSL/TLS (https) буде відображено повідомлення «Термін дії сертифікату минув». Якщо це повідомлення з'являється до дати спливання терміну дії, переконайтеся, що дату на сканері налаштовано правильно.

Загальна назва сертифіката та сканера не збігаються.

Solutions

Якщо загальна назва сертифіката та сканера не збігаються, з'являється повідомлення «Назва сертифіката безпеки не збігається···» під час доступу до Web Config за допомогою зв'язку SSL/TLS (https). Це відбувається через те, що нижченаведені IP-адреси не збігаються.

- ❏ IP-адреса сканера, що введена до загальної назви для створення Сертифікат із власним підписом або CSR
- ❏ IP-адреса, що введена у веб-браузер під час запуску Web Config

Якщо це Сертифікат із власним підписом, оновіть сертифікат.

Для CA-підписаний Сертифікат знов візьміть сертифікат для сканера.

Для веб-браузера не налаштовано параметр проксі-сервера локальної адреси.

Solutions

Якщо сканер налаштовано на використання проксі-сервера, налаштуйте веб-браузер так, щоб він не підключався до локальної адреси через проксі-сервер.

❏ Windows:

Виберіть **Панель керування** > **Мережа й Інтернет** > **Властивості браузера** > **Підключення** > **Настройки локальної мережі** > **Проксі-сервер**, після чого налаштуйте на невикористання проксі-сервера для локальної мережі (локальних адрес).

❏ Mac OS:

Виберіть **Системні параметри** > **Мережа** > **Додатково** > **Проксі**, після чого зареєструйте локальну адресу для **Не використовувати налаштування проксі для таких 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

У налаштуваннях комп'ютера вимкнено DHCP.

Solutions

Якщо на комп'ютерів вимкнено службу DHCP, призначену для автоматичного отримання IP-адреси, відкрити Web Config не вдасться. Увімкніть DHCP.

Приклад для Windows 10:

Відкрийте панель керування, а потім натисніть **Мережа та інтернет** > **Центр мережевих підключень і спільного доступу** > **Змінити налаштування адаптера**. Відкрийте екран властивостей підключення, яке використовується, а потім екран властивостей для **Протоколу Інтернету версії 4 (TCP/IPv4)** або **Протоколу Інтернету версії 6 (TCP/IPv6)**. Перевірте, чи вибрано у відображеному вікні параметр **Отримати IP-адресу автоматично**.

Настроювання відображення панелі керування

Реєстрація Налашт

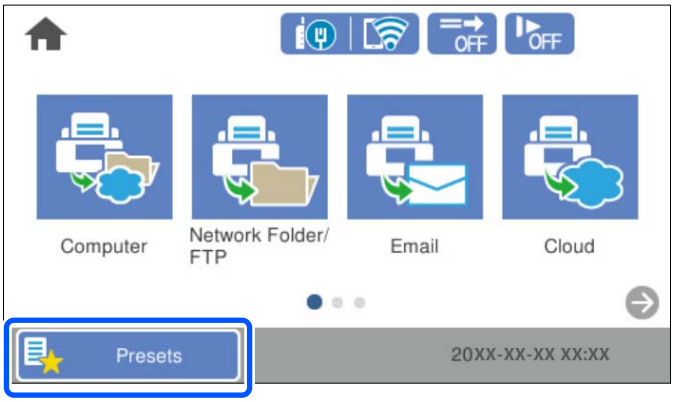
Часто використовувані налаштування сканування можна зареєструвати як **Налашт**. Зареєструвати можна до 48 попередніх налаштувань.

Примітка.

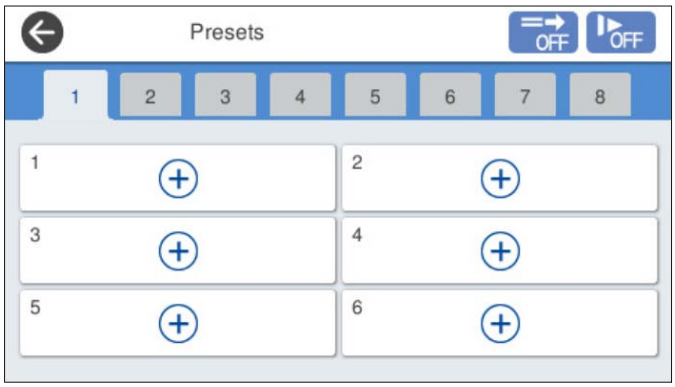
- *Ви можете зареєструвати поточні налаштування, вибравши* ☆ *на екрані початку сканування.*
- *Ви також можете зареєструвати* ***Налашт*** *у Web Config.*

  Виберіть вкладку ***Скан.*** *>* ***Налашт****.*
- *Якщо під час реєстрації вибрати* ***Сканувати до ПК****, можна зареєструвати створене у Document Capture Pro завдання як* ***Налашт****. Це доступно тільки для комп'ютерів, підключених через мережу. Реєструйте завдання у Document Capture Pro заздалегідь.*
- *Якщо функцію автентифікації ввімкнено, зареєструвати* ***Налашт*** *може тільки адміністратор.*

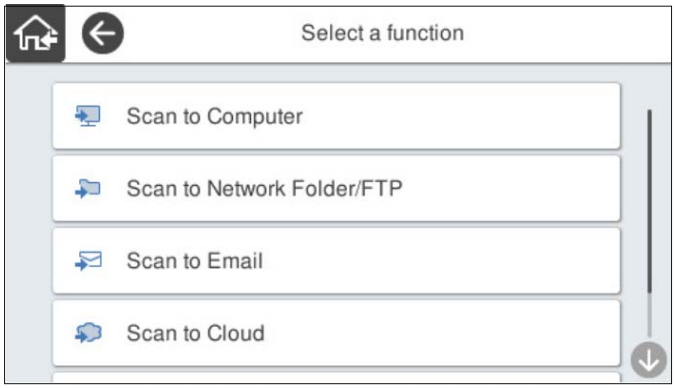
1. На головному екрані панелі керування сканера виберіть **Налашт**.



2. Виберіть ⊕.



3. Виберіть меню, яке потрібно використати для реєстрації попередніх налаштувань.



4. Установіть кожний елемент і виберіть ☆+.

Примітка.
*Якщо вибрати **Сканувати до ПК**, потрібно вибрати комп'ютер, на який встановлено Document Capture Pro, а потім вибрати зареєстроване завдання. Це доступно тільки для комп'ютерів, підключених через мережу.*

5. Виконайте попередні налаштування.
   - ❏ **Ім'я**: укажіть ім'я.
   - ❏ **Указаний Значок**: налаштуйте зображення та колір піктограми для відображення.
   - ❏ **Налаштування Швидкого надсилання**: негайний запуск сканування без підтвердження в разі вибору попереднього налаштування.

     У разі використання Document Capture Pro Server, навіть якщо програмне забезпечення налаштовано на підтвердження вмісту завдання перед скануванням, **Налаштування Швидкого надсилання** у попередніх налаштуваннях сканера має перевагу над програмним забезпеченням.
   - ❏ **Вміст**: перевірте налаштування сканування.

6. Виберіть **OK**.

Параметри меню Налашт

Ви можете змінити параметри попередніх налаштувань, вибравши › у кожному попередньому налаштуванні.

Змінити Ім'я:

Зміна параметрів попередніх налаштувань.

Змінити Значок:

Зміна зображення піктограми й кольору попередніх налаштувань.

Налаштування Швидкого надсилання:

Негайний запуск сканування без підтвердження в разі вибору попереднього налаштування.

Змінити позицію:

Зміна порядку відображення попередніх налаштувань.

Видалити:

Видалення попередніх налаштувань.

Додати або видалити Значок на Верхньому екрані:

Додавання або видалення піктограми попередніх налаштувань із головного екрана.

Підтвердіть Подробиці:

Перегляд параметрів попередніх налаштувань. Завантажити попередні налаштування можна, вибравши **Застосуйте налаштув.**.

Редагування головного екрана панелі керування

Налаштувати головний екран можна, вибравши на панелі керування **Налаш.** > **Редагувати Головний екран**.

- Макет: зміна способу відображення піктограм меню.

  «Зміна Макет головного екрана» на сторінці 82

- Додати піктограму: додавання піктограм до виконаних вами налаштувань **Налашт** або відновлення піктограм, видалених із екрана.

  «Додати піктограму» на сторінці 83

- Видалити піктограму: видалення піктограм з головного екрана.

  «Видалити піктограму» на сторінці 84

- Перемістити піктограму: зміна порядку відображення піктограм.

  «Перемістити піктограму» на сторінці 85

- Відновити відобр. пікт. за промовч.: відновлення налаштувань відображення за замовчуванням на головному екрані.

- Фон: змінення кольору шпалер РК-екрана.

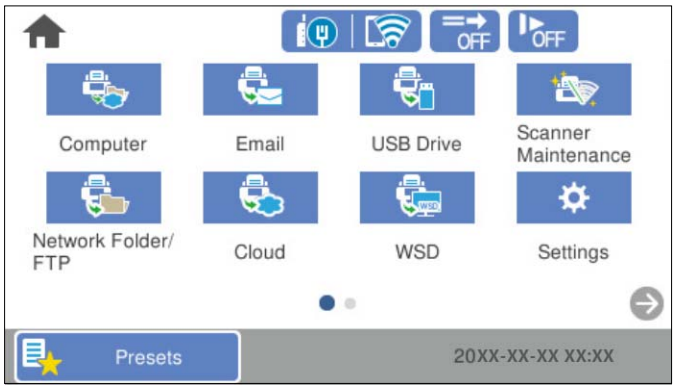
Зміна Макет головного екрана

1. На панелі керування сканера виберіть **Налаш.** > **Редагувати Головний екран** > **Макет**.

2. Виберіть **Лінія** або **Матриця**.

   Лінія:

   Матриця:



3. Виберіть , щоб повернутися та переглянути головний екран.

Додати піктограму

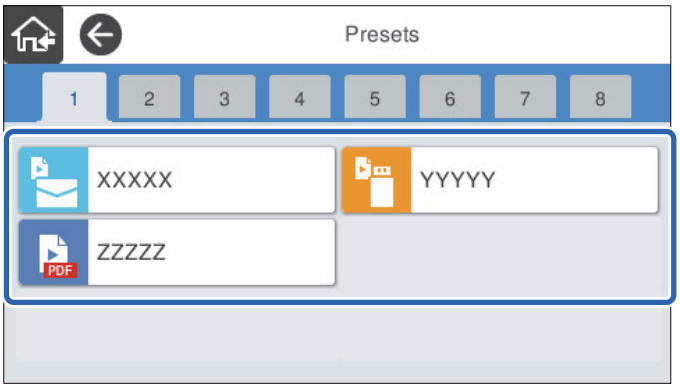
1. На панелі керування сканера виберіть **Налаш.** > **Редагувати Головний екран** > **Додати піктограму**.

2. Виберіть **Функція** або **Налашт**.

   ❏ Функція: відображення на головному екрані функцій за замовчуванням.

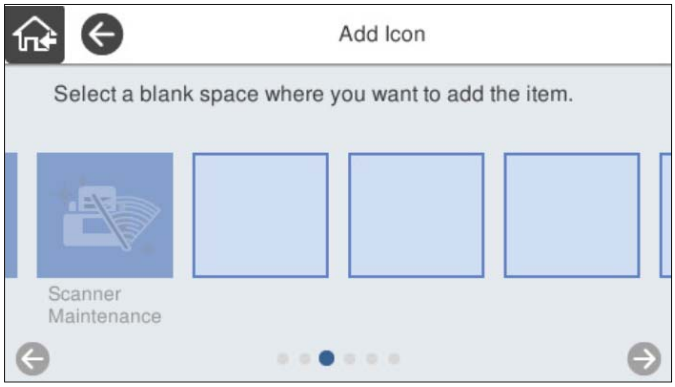
❏ Налашт: відображення зареєстрованих попередніх налаштувань.

3. Виберіть елемент, який потрібно додати до головного екрана.



4. Виберіть порожнє місце, куди потрібно додати елемент.

   Якщо потрібно додати кілька піктограм, повторіть пункти 3–4.

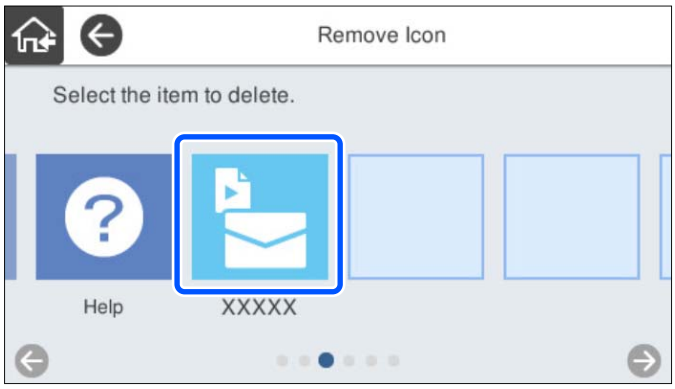


5. Виберіть  , щоб повернутися та переглянути головний екран.

Видалити піктограму

1. На панелі керування сканера виберіть **Налаш.** > **Редагувати Головний екран** > **Видалити піктограму**.

2. Виберіть піктограму, яку потрібно видалити.



3. Виберіть **Так** для завершення.

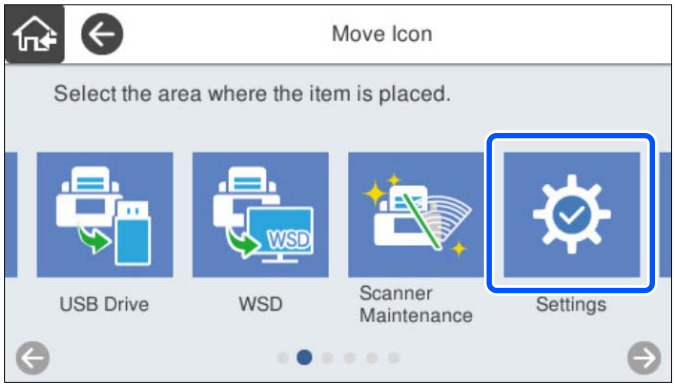
   Якщо потрібно видалити кілька піктограм, повторіть пункти 2–3.

4. Виберіть , щоб повернутися та переглянути головний екран.

Перемістити піктограму

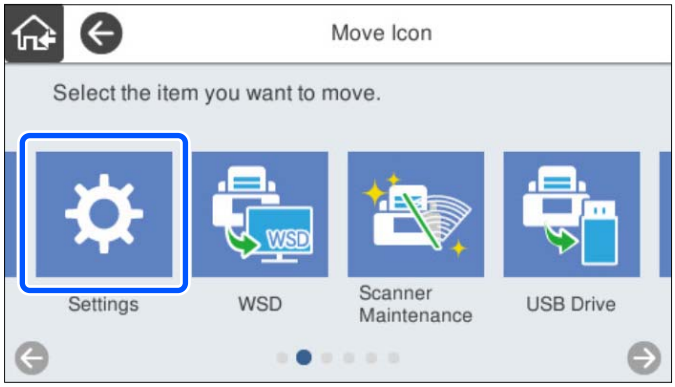
1. На панелі керування сканера виберіть **Налаш.** > **Редагувати Головний екран** > **Перемістити піктограму**.

2. Виберіть піктограму, яку потрібно перемістити.



3. Виберіть рамку місця призначення.

   Якщо в рамці місця призначення вже налаштовано іншу піктограму, її буде замінено.



4. Виберіть , щоб повернутися та переглянути головний екран.

Базові налаштування безпеки

Вступ до функцій безпеки виробу

У цьому розділі описано функції безпеки пристроїв Epson.

Назва функції	Тип функції	Що налаштовує	Чому запобігає
Налаштування пароля адміністратора	Заблоковує налаштування системи, такі як параметри з'єднання для мережі або інформацію про USB.	Пароль до пристрою встановлює адміністратор. Можна встановити або змінити і Web Config, і панель керування сканера.	Уникайте несанкціонованого зчитування або зміни інформації, що зберігається на пристрої, наприклад, ідентифікатор, пароль, мережеві налаштування тощо. А також зменшення широкого діапазону ризиків безпеки, як-от, витоку інформації про мережеве середовище або політики безпеки.
Налаштування зовнішнього інтерфейсу	Керування інтерфейсом, через який здійснюється підключення до пристрою.	Увімкнення або вимкнення USB-підключення до комп'ютера.	USB-з'єднання з комп'ютером: запобігає несанкціонованому використанню пристрою, забороняючи сканування без підключення через мережу.

Пов'язані відомості

➡ «Установлення пароля адміністратора» на сторінці 88

➡ «Вимикання зовнішнього інтерфейсу» на сторінці 94

Налаштування адміністратора

Установлення пароля адміністратора

Встановлення пароля адміністратора може запобігти зміні налаштувань керуванням системою користувачами. У момент покупки встановлюються значення за замовчуванням. У міру необхідності їх можна змінити.

Примітка.
Нижче наведено значення за замовчуванням для інформації адміністратора.

❏ *Ім'я користувача (використовується лише для Web Config): немає (пусто)*

❏ *Пароль: серійний номер сканера*

Серійний номер зазначено на етикетці на задній панелі сканера.

Змінити пароль адміністратора можна за допомогою Web Config, панелі керування сканера або Epson Device Admin. У разі використання Epson Device Admin, див. посібник або довідку Epson Device Admin.

Зміна пароля адміністратора за допомогою Web Config

Змініть пароль адміністратора у Web Config.

1. Відкрийте Web Config і виберіть вкладку **Безпека продукту** > **Змінити Пароль адміністратора**.

2. Введіть необхідну інформацію у **Поточний пароль**, **Ім'я користувача**, **Новий пароль**, та **Підтвердіть новий пароль**.

   Введіть принаймні один символ для встановлення нового пароля.

   Примітка.
   Нижче наведено значення за замовчуванням для інформації адміністратора.

   ❏ *Ім'я користувача: немає (пусто)*

   ❏ *Пароль: серійний номер сканера*

   Серійний номер зазначено на етикетці на задній панелі сканера.

   > ***Важливо***
   > *Обов'язково запам'ятайте встановлений вами пароль адміністратора. Якщо ви забудете свій пароль, то не зможете його скинути, і вам потрібно буде звернутися по допомогу до персоналу обслуговування.*

3. Виберіть **OK**.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Зміна паролю адміністратора з панелі керування

Пароль адміністратора можна змінити на панелі керування сканера.

1. На панелі керування сканера виберіть **Налаш.**.

2. Виберіть **Сист. адміністрування** > **Налаштув. адміністратора**.

3. Виберіть **Пароль адміністратора** > **Змінити**.

4. Введіть поточний пароль.

   Примітка.
   На момент придбання в якості пароль адміністратора встановлено серійний номер сканера (значення за замовчуванням).

   Серійний номер зазначено на етикетці на задній панелі сканера.

5. Введіть новий пароль.

   Введіть принаймні один символ.

> ***Важливо***
>
> *Обов'язково запам'ятайте встановлений вами пароль адміністратора. Якщо ви забудете свій пароль, то не зможете його скинути, і вам потрібно буде звернутися по допомогу до персоналу обслуговування.*

6. Знову введіть новий пароль для підтвердження.

Відобразиться повідомлення про завершення.

Використання Налаштування блокування для панелі керування

Ви можете скористатися Налаштування блокування, щоб заблокувати панель керування, аби користувачі не могли змінювати елементи, пов'язані з налаштуваннями системи.

Примітка.
Якщо увімкнути на сканері Налаштування автентифікації, то для панелі керування також увімкнеться Налаштування блокування. Панель керування не можна розблокувати, якщо увімкнено Налаштування автентифікації.

Навіть якщо ви вимкнете Налаштування автентифікації, то Налаштування блокування залишиться увімкненим. Якщо ви бажаєте вимкнути його, ви можете виконати налаштування на панелі керування або у Web Config.

Налаштування Налаштування блокування за допомогою панелі керування

1. Якщо ви хочете скасувати **Налаштування блокування** після його ввімкнення, торкніться  у верхньому правому куті головного екрана, аби увійти як адміністратор.

    не відображається, коли **Налаштування блокування** вимкнено. Якщо ви бажаєте ввімкнути цей параметр, перейдіть до наступного кроку.

2. Виберіть **Налаш.**.

3. Виберіть **Сист. адміністрування** > **Налаштув. адміністратора**.

4. Виберіть **Увімк** або **Вим.** як **Налаштування блокування**.

Налаштування Налаштування блокування з Web Config

1. Виберіть вкладку **Керування пристроєм** > **Контрольна панель**.

2. Виберіть **Увімкнути** або **Вимкнути** для **Блокування панелі**.

3. Клацніть **OK**.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Елементи Налаштування блокування у меню Налаш.

Нижче наведено список елементів, заблокованих у меню **Налаш.** на панелі керування за допомогою Налаштування блокування.

✓: заблокувати.

- : не блокувати.

Меню Налаш.		Налаштування блокування
Основні налашт.		-
	Яскр. РК-дис.	-
	Звуки	-
	Тайм. очікув.	✓
	Вимкнути таймер	✓
	Налаштув. дати/часу	✓
	Мова/Language	✓/-*
	Клавіатура (У деяких регіонах ця функція недоступна.)	-
	Час очікування операції	✓
	Підкл. ПК по USB	✓
	Автоматичне увімкнення	✓
Налашт. сканера		-
	Повільна швидкість	-
	Час зупинки подвійної подачі	✓
	Функція DFDS	-
	Захист паперу	✓
	Виявлення бруду на склі	✓
	УЗ виявл. завантаж. кількох листів	✓
	Час очікування Режиму автоматичної подачі	✓
	Підтвердіть одержувача	✓
Редагувати Головний екран		✓

Меню Налаш.		**Налаштування блокування**
	Макет	✓
	Додати піктограму	✓
	Видалити піктограму	✓
	Перемістити піктограму	✓
	Відновити відобр. пікт. за промовч.	✓
	Фон	✓
Параметри користувача		✓
	Мереж. пап./FTP	✓
	Ел. адреса	✓
	Cloud	✓
	USB-накопичувач	✓
Налаштування мережі		✓
	Настр. Wi-Fi	✓
	Налаштування дротової LAN	✓
	Стан мережі	✓
	Розширений	✓
Налаштування веб-служби		✓
	Послуги Epson Connect	✓
Document Capture Pro		-
	Змінити налаштування	✓
Конт. менеджер		-
	Зареєструвати/Видалити	✓/-*
	Частий	-
	Переглянути параметри	-
	Варіанти пошуку	-
Сист. адміністрування		✓

Меню Налаш.			**Налаштування блокування**
	Конт. менеджер		✓
	Налаштув. адміністратора		✓
	Обмеження		✓
	Шифрування пароля		✓
	Вивчення клієнтських вимог		✓
	WSD Налаштування		✓
	Віднов. налашт. за зам.		✓
	Оновлення мікропрограмного забезпечення		✓
Інформація про пристрій			-
	Серійний номер		-
	Поточна версія		-
	Загальна к-ть сканувань		-
	Кількість 1-стор. сканувань		-
	Кількість 2-стор. сканувань		-
	К-ть скан. за доп. Конв. для Скан.		-
	К-сть скан. після заміни		-
	К-сть скан. після очищ.		-
	Скинути кількість сканувань		✓
Обслуговув. та ремонт сканера			-
	Чистка роликів		-
	Заміна роликів		-
		Скинути кількість сканувань	✓
		Як замінити	-
	Рег. очищення		-
		Скинути кількість сканувань	✓
		Як чистити	-
	Очищення скла		-
Параметри сповіщення про заміну ролика			✓
	Налашт. сповіщень		✓
Налаштування сповіщення про регулярне очищення			✓

Меню Налаш.		**Налаштування блокування**
	Налаштування застережень	✓
	Налашт. сповіщень	✓

* Ви можете вказати, чи дозволяти зміни в **Сист. адміністрування** > **Обмеження**.

Вхід в якості адміністратора з панелі керування

Для входу в систему в якості адміністратора з панелі керування сканера ви можете використовувати будь-який з наведених нижче методів.

1. Торкніться елемента  у верхньому правому куті екрана.
   - ❏ Якщо Налаштування автентифікації ввімкнено, піктограма відображається на екрані **Ласкаво просимо** (екран очікування автентифікації).
   - ❏ Якщо Налаштування автентифікації вимкнено, на головному екрані відображається піктограма.
2. Коли відобразиться екран підтвердження, натисніть **Так**.
3. Введіть пароль адміністратора.

   Відобразиться повідомлення про успішне виконання входу, після чого ви побачите головний екран на панелі керування.

Для виходу торкніться елемента  у верхньому правому куті головного екрана.

Вимикання зовнішнього інтерфейсу

Зовнішній інтерфейс, який використовується для підключення пристрою до сканера, можна вимкнути. Виконайте обмежувальні налаштування, щоб сканування можна було здійснювати лише через мережу.

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

*Підкл. ПК по USB: **Налаш.** > **Основні налашт.** > **Підкл. ПК по USB***

1. Відкрийте Web Config і виберіть вкладку **Безпека продукту** > **Зовнішній інтерфейс**.
2. Виберіть **Вимкн.** на функціях, які потрібно налаштувати.

   Виберіть **Увімкн.**, якщо керування потрібно скасувати.

   Підкл. ПК по USB

   Можна обмежити використання підключення USB з комп'ютера. Якщо потрібно ввести це обмеження, виберіть **Вимкн.**.
3. Клацніть **OK**.

4. Перевірте, що вимкнений порт не можна використовувати.

   Підкл. ПК по USB

   Якщо на комп'ютері було встановлено драйвер принтера

   Під'єднайте сканер до комп'ютера за допомогою USB-кабелю, а потім переконайтеся, що сканер не сканує.

   Якщо на комп'ютері не було встановлено драйвер принтера

   Windows:

   Відкрийте диспетчер пристроїв і збережіть його, підключіть сканер до комп'ютера за допомогою USB-кабелю та переконайтеся, що вміст дисплею диспетчера пристрою залишається незмінним.

   Mac OS:

   Під'єднайте сканер до комп'ютера за допомогою USB-кабелю, а потім переконайтеся, що із **Принтери та сканери** сканер додати не вдається.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Моніторинг віддаленого сканера

Перевірка інформації віддаленого сканера

Наведену нижче інформацію про сканер, що працює, можна перевірити у **Статус** за допомогою Web Config.

❏ Стан продукту

Перевірте стан, хмарну службу, номер продукту, MAC-адресу тощо.

❏ Стан мережі

Перевірте інформацію про стан підключення до мережі, IP-адресу, сервер DNS тощо.

❏ Статус використання

Перевірте перший день сканування, лічильник сканування тощо.

❏ Статус обладнання

Перевірте стан кожної функції сканера.

❏ Знімок панелі

Відображення знімка екрана, відображеного на панелі керування сканера.

Отримання сповіщень електронної пошти щодо певних подій

Про сповіщення електронною поштою

Це функція сповіщення для відправлення електронного листа на вказану адресу, коли зупинено сканування та виникла помилка сканера.

Можна зареєструвати до п'яти одержувачів та встановити налаштування сповіщення для кожного одержувача.

Щоб використовувати цю функцію, потрібно налаштувати сервер електронної пошти до налаштування сповіщень електронною поштою.

Пов'язані відомості

➡ «Налаштування поштового сервера» на сторінці 43

Налаштування отримання сповіщень електронною поштою

Налаштуйте отримання сповіщень електронною поштою за допомогою Web Config.

1. Відкрийте Web Config і виберіть вкладку **Керування пристроєм** > **Повідомлення електронною поштою**.

2. Встановіть тему сповіщень електронною поштою.

   Виберіть вміст, відображений у темі, з двох спадних меню.

   ❏ Вибраний вміст відображаються поряд з **Тема**.

   ❏ Один і той самий вміст не можна встановити і справа, і зліва.

   ❏ Якщо кількість символів у **Місце** більше 32 байтів, то символи, що перевищують 32 байти, упускаються.

3. Введіть адресу електронної пошти, щоб надіслати сповіщення.

   Використайте A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @, і введіть від 1 до 255 символів.

4. Виберіть мову для сповіщень електронною поштою.

5. Встановіть прапорець біля події, щодо якої ви бажаєте отримати сповіщення.

   Номер **Налаштування сповіщень** пов'язаний із номером призначення у **Налаштування адреси ел. пошти**.

   Наприклад:

   Якщо потрібно відправити сповіщення на адресу електронної пошти, налаштованої під номером 1 у **Налаштування адреси ел. пошти** при зміні пароля адміністратора, установіть прапорець стовпця **1** у рядку **Пароль адміністратора змінено**.

6. Клацніть **OK**.

   Перевірте, що сповіщення електронною поштою відправляється за наявності випадку, що призводить до цього.

   Наприклад: пароль адміністратора змінено.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Налаштування сповіщення електронною поштою

Параметри	Налаштування та пояснення
Пароль адміністратора змінено	Сповіщення в разі зміни пароля адміністратора.
Помилка сканера	Сповіщення в разі виникнення помилки сканера.
Неполадка Wi-Fi	Повідомлення про виникнення помилки інтерфейсу безпровідної локальної мережі.

Вирішення проблем

Забули свій пароль адміністратора

Вам потрібна допомога персоналу з обслуговування. Зверніться до місцевого постачальника.

Примітка.
Нижче наведено початкові значення для адміністратора Web Config.

❏ *Ім'я користувача: немає (пусто)*

❏ *Пароль: серійний номер сканера*

Серійний номер зазначено на етикетці на задній панелі сканера. У разі відновлення налаштувань за замовчуванням для паролю адміністратора вони скидаються до початкових значень.

Розширені налаштування безпеки

Налаштування безпеки та запобігання небезпеки

Якщо сканер підключено до мережі, ви можете мати доступ до нього з віддаленого розташування. Крім того, багато людей можуть спільно використовувати сканер, що значно підвищує ефективність і зручність роботи. Однак в такому разі збільшуються ризики несанкціонованого доступу, забороненого використання та зловмисного втручання в дані. Якщо ви використовуєте сканер у середовищі, де є доступ до інтернету, то ризики стають ще вищими.

Для сканерів, які не мають захисту від зовнішнього доступу, є ризики зчитування контактів, які зберігаються на сканер з інтернету.

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

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

Назва	Тип функції	Що налаштовує	Чому запобігає
Керування протоколом	Контроль протоколів і служб, що мають використовуватися для зв'язку між сканерами та комп'ютерами, а також увімкнення чи вимкнення функцій.	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.
Зв'язок за допомогою протоколів SSL/TLS	Вміст зв'язку шифрується за допомогою зв'язку SSL/TLS під час входу на сервер Epson через інтернет зі сканера, наприклад під час з'єднання з комп'ютером через веб-браузер за допомогою Epson Connect та оновлення мікропрограм.	Отримайте сертифікат, підписаний ЦС, а тоді імпортуйте його на сканер.	Очищення ідентифікації сканера за допомогою сертифікату, підписаного ЦС, запобігає видаванню себе за іншу особу та несанкціонованому доступу. Крім того, вміст зв'язку SSL/TLS захищений і запобігає просочуванню вмісту даних для сканування чи інформації про налаштування.
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.	Створіть базову та індивідуальну політику, щоб встановити тип клієнта або тип даних, які можуть отримувати доступ до сканера.	Захистіть сканер від несанкціонованого доступу, зловмисного втручання та перехоплювання даних зв'язку.
IEEE 802.1X	Дозвіл на підключення до мережі надається тільки автентифікованим користувачам. Дозволяє використовувати сканер тільки авторизованому користувачеві.	Налаштування автентифікації на сервері RADIUS (сервер автентифікації).	Захист від несанкціонованого доступу та використання сканера.

Пов'язані відомості

- «Керування протоколами використання» на сторінці 100
- «Зв'язок SSL/TLS зі сканером» на сторінці 109
- «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 110
- «Підключення сканера до мережі IEEE802.1X» на сторінці 122

Налаштування функції безпеки

Під час налаштування фільтрування IPsec/IP або IEEE 802.1X, рекомендується відкритиWeb Config за допомогою SSL/TLS, щоб знизити ризики безпеки, як-от втручання або перехоплення.

Перш ніж налаштовувати фільтрування IPsec/IP або IEEE 802.1X, обов'язково встановіть пароль адміністратора.

Керування протоколами використання

Можна виконувати сканування з використанням цілої низки шляхів та протоколів. Також можна використовувати мережеве сканування з будь-якої кількості комп'ютерів у мережі.

Можна знизити непередбачувані ризики для безпеки, обмеживши сканування з певних шляхів або керуючи доступними функціями.

Керування протоколами

Налаштуйте налаштувань протоколу, підтримуваного сканером.

1. Відкрийте Web Config, а тоді виберіть вкладку **Мережева безпека** tab > **Протокол**.
2. Налаштуйте конфігурацію кожного елемента.
3. Клацніть **Далі**.
4. Клацніть **OK**.

   Ці налаштування будуть застосовані до сканера.

Пов'язані відомості

- «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Протоколи, які можна увімкнути або вимкнути

Протокол	Опис
Налаштування Bonjour	Можна вказати, чи потрібно використовувати Bonjour. Bonjour використовується для пошуку пристроїв, сканування і т.д.

Протокол	Опис
Налаштування SLP	Можна ввімкнути або вимкнути функцію SLP. SLP використовується для функцій «push-scan» та пошуку в мережі у програмі EpsonNet Config.
Налаштування WSD	Можна ввімкнути або вимкнути функцію WSD. Якщо її увімкнено, ви зможете додавати пристрої WSD або виконувати сканування через порт WSD.
Налаштування LLTD	Можна ввімкнути або вимкнути функцію LLTD. Якщо її увімкнено, вона відображатиметься на мережевій мапі Windows.
Налаштування LLMNR	Можна ввімкнути або вимкнути функцію LLMNR. Якщо її увімкнено, можна використовувати ідентифікацію імені без NetBIOS, навіть якщо ви не можете використовувати DNS.
Налаштування SNMPv1/v2c	Можна вказати, чи потрібно вмикати SNMPv1/v2c. Ця функція використовується для налаштування пристроїв, контролю і т.д.
Налаштування SNMPv3	Можна вказати, чи потрібно вмикати SNMPv3. Ця функція використовується для налаштування шифрованих пристроїв.

Параметри протоколу

Налаштування Bonjour

Параметри	Налаштування значення та опис
Застосувати Bonjour	Виберіть це для пошуку або використання пристроїв через Bonjour.
Ім'я Bonjour	Відображення імені Bonjour.
Службове ім'я Bonjour	Відображення назви служби Bonjour.
Місце	Відображення назви місця розташування Bonjour.
Wide-Area Bonjour	Встановіть, чи використовувати Wide-Area Bonjour.

Налаштування SLP

Параметри	Налаштування значення та опис
Увімкнути SLP	Виберіть це, щоб увімкнути функцію SLP. Це використовується для мережевого пошуку в EpsonNet Config.

Налаштування WSD

Параметри	Налаштування значення та опис
Увімкнути WSD	Виберіть, щоб увімкнути додавання пристроїв за допомогою WSD, а тоді виконувати сканування через порт WSD.
Перерва сканування (сек)	Введіть значення часу очікування зв'язку для сканування через WSD від 3 до 3600 секунд.
Ім'я пристрою	Відображення назви пристрою WSD.

Параметри	Налаштування значення та опис
Місце	Відображення назви місця розташування WSD.

Налаштування LLTD

Параметри	Налаштування значення та опис
Увімкнути LLTD	Виберіть це, щоб увімкнути LLTD. Сканер відобразиться на мережевій карті Windows.
Ім'я пристрою	Відображення назви пристрою LLTD.

Налаштування LLMNR

Параметри	Налаштування значення та опис
Увімкнути LLMNR	Виберіть це, щоб увімкнути LLMNR. Можна використовувати ідентифікацію імені без NetBIOS, навіть якщо ви не можете використовувати DNS.

Налаштування SNMPv1/v2c

Параметри	Налаштування значення та опис
Увімкнути SNMPv1/v2c	Виберіть, щоб увімкнути SNMPv1/v2c.
Дозвіл доступу	Установіть права доступу За ввімкненого параметра SNMPv1/v2c. Виберіть **Тільки чит.** або **Читання/Запис**.
Ім'я спільноти (тільки для читання)	Введіть від 0 до 32 символів ASCII (від 0x20 до 0x7E).
Ім'я спільноти (читання/запис)	Введіть від 0 до 32 символів ASCII (від 0x20 до 0x7E).

Налаштування SNMPv3

Параметри		Налаштування значення та опис
Увімкнути SNMPv3		SNMPv3 вмикається, коли поставлено прапорець навпроти опції.
Ім'я користувача		Введіть від 1 до 32 символів, використовуючи 1-байтні символи.
Налаштування автентифікації		
	Алгоритм	Виберіть алгоритм для автентифікації до SNMPv3.
	Пароль	Виберіть пароль для автентифікації до SNMPv3. Можна ввести від 8 до 32 символів формату ASCII (0x20–0x7E). Якщо дані вводити непотрібно, лишіть поле пустим.
	Пароль підтвердження	Введіть установлений пароль для підтвердження.
Налаштування кодування		

Параметри		Налаштування значення та опис
	Алгоритм	Виберіть алгоритм для шифрування для SNMPv3.
	Пароль	Виберіть пароль для шифрування для SNMPv3. Можна ввести від 8 до 32 символів формату ASCII (0x20–0x7E). Якщо дані вводити непотрібно, лишіть поле пустим.
	Пароль підтвердження	Введіть установлений пароль для підтвердження.
Контекстне ім'я		Уведіть до 32 символів формату Unicode (UTF-8). Якщо дані вводити непотрібно, лишіть поле пустим. Кількість символів, які можна ввести, змінюється в залежності від мови.

Використання цифрового сертифіката

Про цифрову сертифікацію

❏ CA-підписаний Сертифікат

Це сертифікат, підписаний ЦС (Центр сертифікації). Можна отримати його, щоб надіслати до Центру сертифікації. Сертифікат підтверджує існування сканера та використання його для зв'язку за допомогою протоколів SSL/TLS, щоб гарантувати безпеку передачі даних.

Коли він використовується для зв'язку за допомогою протоколів SSL/TLS, він використовується як сертифікат сервера.

Коли він встановлений на зв'язок фільтрування за IPsec/IP або IEEE 802.1X, він використовується як сертифікат клієнта.

❏ Сертифікат ЦС

Це сертифікат, що знаходиться в ланцюжку CA-підписаний Сертифікат, що також називається проміжним сертифікатом ЦС. Він використовується веб-браузером для підтвердження шляху сертифіката сканера під час входу на сервер іншої сторони чи Web Config.

Для сертифіката ЦС: налаштуйте, коли підтверджувати шлях сертифіката сервера під час входу зі сканера. Для сканера: налаштуйте підтвердження шляху CA-підписаний Сертифікат для зв'язку за допомогою протоколів SSL/TLS.

Можна отримати сертифікат ЦС сканера від Центру сертифікації, де видається сертифікат ЦС.

Також можна отримати сертифікат ЦС для підтвердження сервера іншої сторони від Центру сертифікації, який видав CA-підписаний Сертифікат сервера.

❏ Сертифікат із власним підписом

Це сертифікат, який сканер підписує та видає сам. Він також називається кореневим сертифікатом. Оскільки видавець самостійно підтверджує себе, він не є надійним і не може запобігти маскуванню під законного користувача.

Використовуйте його для здійснення налаштування безпеки та простого зв'язку за допомогою протоколів SSL/TLS без CA-підписаний Сертифікат.

Якщо використовувати цей сертифікат для зв'язку SSL/TLS, у веб-браузері може відобразитися попередження служби безпеки, оскільки сертифікат не зареєстровано на веб-браузері. Сертифікат із власним підписом можна використовувати лише для зв'язку SSL/TLS.

Пов'язані відомості

- «Налаштування CA-підписаний Сертифікат» на сторінці 104
- «Оновлення сертифіката із власним підписом» на сторінці 107
- «Налаштування Сертифікат CA» на сторінці 108

Налаштування CA-підписаний Сертифікат

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 вкладку **Мережева безпека**. Далі виберіть **SSL/TLS** > **Сертифікат** або **IPsec/фільтрування IP** > **Сертифікат клієнта**, або **IEEE802.1X** > **Сертифікат клієнта**.

   Що б ви не вибрали, ви можете отримати той самий сертифікат і використовувати його спільно.

2. Клацніть **Створити** 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. Клацніть **OK**.

   Відобразиться повідомлення про завершення.

5. Оберіть вкладку **Мережева безпека**. Далі виберіть **SSL/TLS** > **Сертифікат** або **IPsec/фільтрування IP** > **Сертифікат клієнта**, або **IEEE802.1X** > **Сертифікат клієнта**.

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-підписаний Сертифікат.*

7. Надішліть ЗПС до Центру сертифікації та отримайте сертифікат CA-підписаний Сертифікат.

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

8. Збережіть виданий CA-підписаний Сертифікат на комп'ютері, підключеному до сканера.

   Процес отримання CA-підписаний Сертифікат завершено, коли сертифікат збережено до папки призначення.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Параметри ЗПС

Параметри	Налаштування та пояснення
Довжина ключа	Виберіть довжину ключа для ЗПС.
Загальна назва	Можна ввести від 1 до 128 символів. Якщо це IP-адреса, вона має бути статичною. Можна ввести від 1 до 5 адрес IPv4, IPv6, імен хосту, FQDNs, розділяючи їх комою. Перший елемент зберігається у загальній назві, а інші елементи зберігаються у полі псевдонім сертифіката суб'єкта. Наприклад: IP-адреса сканера: 192.0.2.123, Ім'я сканера: EPSONA1B2C3 Загальна назва: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Організація/ Організаційна одиниця/ Місце розташування/ Країна/ Область	Можна ввести від 0 до 64 символів формату ASCII (0x20–0x7E). Окремі імена можна розділяти комами.
Країна	Введіть двозначний код країни за стандартом ISO-3166.
Ел. адреса відправника	Можна ввести адресу електронної пошти відправника для налаштування поштового сервера. Введіть ту саму адресу електронної пошти, що й **Ел. адреса відправника**, для вкладки **Мережа** > **Сервер ел. пошти** > **Основні**.

Імпортування сертифіката, підписаного ЦС

Імпортуйте отриманий CA-підписаний Сертифікат на сканер.

Важливо

- ❏ *Переконайтеся, що дата й час сканера встановлені правильно. Сертифікат може бути недійсний.*
- ❏ *У разі отримання сертифіката за ЗПС, створеним через Web Config, імпортувати сертифікат можна один раз.*

1. Відкрийте Web Config, а тоді виберіть вкладку **Мережева безпека**. Далі виберіть **SSL/TLS** > **Сертифікат** або **IPsec/фільтрування IP** > **Сертифікат клієнта**, або **IEEE802.1X** > **Сертифікат клієнта**.

2. Клацніть **Імпорт**

   Відкриється сторінка імпорту сертифіката.

3. Введіть значення для кожного елемента. Встановіть **Сертифікат CA 1** та **Сертифікат CA 2** під час перевірки шляху сертифіката у веб-браузері, який отримує доступ до сканера.

   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

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

❏ **Пароль**: не налаштовувати.

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

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

❏ **Особистий ключ**: необхідно встановити.

❏ **Пароль**: не налаштовувати.

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

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

❏ **Особистий ключ**: не налаштовувати.

❏ **Пароль**: необов'язково

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

4. Клацніть **OK**.

Відобразиться повідомлення про завершення.

Примітка.
*Клацніть **Підтвердити**, щоб перевірити інформацію сертифіката.*

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Елементи налаштування імпорту сертифіката з підписом ЦС

Елементи	Налаштування та пояснення
Сервер сертифікату або Сертифікат клієнта	Виберіть формат сертифіката. У разі підключення SSL/TLS, буде відображено Сервер сертифікату. У разі фільтрування IPsec/IP або IEEE 802.1X, буде відображено Сертифікат клієнта.
Особистий ключ	Якщо ви отримуєте сертифікат формату PEM/DER, використовуючи CSR, створену на комп'ютері, укажіть файл із приватним ключем, що відповідає сертифікату.
Пароль	Якщо формат файлу **Сертифікат з Особистим ключем (PKCS#12)**, введіть пароль шифрування приватного ключа, установлений під час отримання сертифіката.
Сертифікат CA 1	Якщо формат вашого сертифіката **Сертифікат (PEM/DER)**, імпортуйте сертифікат, виданий центром сертифікації, що видає CA-підписаний Сертифікат, який використовується в якості сертифіката сервера. Укажіть потрібний файл.
Сертифікат CA 2	Якщо формат вашого сертифіката **Сертифікат (PEM/DER)**, імпортуйте сертифікат, виданий центром сертифікації, що видає Сертифікат CA 1. Укажіть потрібний файл.

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 вкладку **Мережева безпека**. Далі виберіть **SSL/TLS** > **Сертифікат** або **IPsec/фільтрування IP** > **Сертифікат клієнта**, або **IEEE802.1X** > **Сертифікат клієнта**.
2. Клацніть **Видалити**.
3. Підтвердіть, що ви справді бажаєте видалити сертифікат, указаний у повідомленні.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Оновлення сертифіката із власним підписом

Оскільки Сертифікат із власним підписом видається сканером, його можна оновити, коли його термін дії закінчився, або коли опис буде змінено.

1. Відкрийте Web Config і виберіть вкладку **Мережева безпека** tab > **SSL/TLS** > **Сертифікат**.
2. Клацніть **Оновлення**.
3. Введіть **Загальна назва**.

   Ви можете ввести до 5 адрес IPv4, IPv6-адрес, імена хостів, FQDN від 1 до 128 символів і розділити їх комами. Перший параметр зберігається до загальної назви, а інші зберігаються у полі псевдоніма для об'єкта сертифіката.

   Приклад:

   IP-адреса сканера: 192.0.2.123, Назва сканера: EPSONA1B2C3

   Загальна назва: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Укажіть термін дії сертифіката.
5. Клацніть **Далі**.

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

   Сканер буде оновлено.

Примітка.
Ви можете перевірити інформацію про сертифікат із ***Мережева безпека*** *>* ***SSL/TLS*** *>* ***Сертифікат*** *>* ***Сертифікат із власним підписом*** *та натиснути на кнопку* ***Підтвердити****.*

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Налаштування Сертифікат CA

Виконуючи налаштування Сертифікат CA, можна затвердити маршрут до сертифіката ЦС сервера, до якого отримує доступ сканер. Так можна запобігти видаванню себе за іншу особу.

Можна отримати Сертифікат CA у Центрі сертифікації, де видається CA-підписаний Сертифікат.

Імпортування Сертифікат CA

Імпортуйте Сертифікат CA на сканер.

1. Відкрийте Web Config, а тоді виберіть вкладку **Мережева безпека** > **Сертифікат CA**.
2. Клацніть **Імпорт**.
3. Укажіть Сертифікат CA, який потрібно імпортувати.
4. Клацніть **OK**.

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

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Видалення Сертифікат CA

Ви можете видалити Сертифікат CA.

1. Відкрийте Web Config, після чого виберіть **Мережева безпека** вкладку > **Сертифікат CA**.
2. Клацніть **Видалити** поруч із Сертифікат CA, який потрібно видалити.
3. Підтвердьте, що ви бажаєте видалити сертифікат, зазначений у відображеному повідомленні.
4. Клацніть **Перезавантаження мережі**, після чого перевірте, що видалений сертифікат ЦС відсутній у списку на оновленому екрані.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

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.

Виконання базових налаштувань SSL/TLS

Якщо сканер підтримує функцію сервера HTTPS, ви можете використовувати зв'язок SSL/TLS для шифрування комунікацій. Налаштувати сканер і керувати ним можна за допомогою Web Config, водночас дбаючи про безпеку.

Налаштуйте стійкість шифрування та функцію перенаправлення.

1. Відкрийте Web Config і виберіть вкладку **Мережева безпека** > **SSL/TLS** > **Основні**.
2. Виберіть значення для кожного елемента.
   - ❏ Стійкість шифрування
     Виберіть рівень стійкості шифрування.
   - ❏ Переадресувати HTTP на HTTPS
     Виконайте перенаправлення на HTTPS, якщо здійснено підключення до HTTP.
3. Клацніть **Далі**.
   Буде відображено підтвердження.
4. Клацніть **OK**.
   Сканер оновлено.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Налаштування сертифіката сервера для сканера

1. Відкрийте Web Config і виберіть вкладку **Мережева безпека** > **SSL/TLS** > **Сертифікат**.
2. Виберіть необхідний сертифікат у меню **Сервер сертифікату**.
   - ❏ Сертифікат із власним підписом
     Сертифікат із власним підписом генерується сканером. Виберіть це, якщо не маєте сертифіката, підписаного ЦС.
   - ❏ CA-підписаний Сертифікат
     Можете вибрати це, якщо ви заздалегідь отримали та імпортували сертифікат, підписаний ЦС.
3. Клацніть **Далі**.
   Відобразиться повідомлення про підтвердження.

4. Клацніть **OK**.

   Сканер буде оновлено.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37
➡ «Налаштування CA-підписаний Сертифікат» на сторінці 104
➡ «Налаштування Сертифікат CA» на сторінці 108

Шифрування зв'язку за допомогою фільтрації за IPsec/IP

Про IPsec/фільтрування IP

Можна фільтрувати трафік на основі IP-адрес, служб та портів за допомогою функції фільтрації за IPsec/IP. Поєднуючи фільтри, можна налаштувати сканер на приймання або блокування зазначених клієнтів і зазначених даних. Крім того, можна покращити рівень безпеки за допомогою IPsec.

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

Налаштування політики за замовчуванням

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.

1. Відкрийте Web Config, а тоді виберіть вкладку **Мережева безпека** > **IPsec/фільтрування IP** > **Основні**.

2. Введіть значення для кожного елемента.

3. Клацніть **Далі**.

   Відобразиться повідомлення про підтвердження.

4. Клацніть **OK**.

   Сканер буде оновлено.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Політика за промовчанням Параметри

Політика за промовчанням

Параметри	Налаштування та пояснення
IPsec/фільтрування IP	Функцію мережі IPsec/IP-фільтрування можна ввімкнути або вимкнути.

❏ Контроль доступу

Налаштуйте спосіб керування для трафіку або пакетів IP.

Параметри	Налаштування та пояснення
Дозволити доступ	Виберіть, щоб дозволити проходження налаштованих пакетів IP.
Відмовити в доступі	Виберіть це, щоб заборонити проходження налаштованих пакетів IP.
IPsec	Виберіть це, щоб дозволити проходження налаштованих пакетів IPsec.

❏ **Версія IKE**

Виберіть **IKEv1** або **IKEv2** для **Версія IKE**. Виберіть одне зі значень відповідно до пристрою, до якого підключено сканер.

❏ IKEv1

Вказані нижче елементи відображаються, якщо вибрати **IKEv1** для **Версія IKE**.

Параметри	Налаштування та пояснення
Метод ідентифікації	Щоб вибрати **Сертифікат**, необхідно заздалегідь отримати та імпортувати сертифікат, підписаний ЦС.
Попередньо виданий ключ	Щоб вибрати **Попередньо виданий ключ** для **Метод ідентифікації**, введіть спільний ключ довжиною від 1 до 127 символів.
Підтвердити Попередньо виданий ключ	Введіть установлений ключ для підтвердження.

❏ IKEv2

Вказані нижче елементи відображаються, якщо вибрати **IKEv2** для **Версія IKE**.

Параметри		Налаштування та пояснення
Локально	Метод ідентифікації	Щоб вибрати **Сертифікат**, необхідно заздалегідь отримати та імпортувати сертифікат, підписаний ЦС.
	Тип ідентифікатора	Якщо вибрати **Попередньо виданий ключ** для параметра **Метод ідентифікації**, виберіть тип ідентифікатора для сканера.
	Ідентифікатор	Уведіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Відоме ім'я**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «=». **IP-адреса**: введіть формат IPv4 або IPv6. **FQDN**: введіть комбінацію від 1 до 255 символів, використовуючи символи A–Z, a–z, 0–9, «-» та крапку (.). **Ел. адреса**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «@». **Ідентифікатор ключа**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E).
	Попередньо виданий ключ	Щоб вибрати **Попередньо виданий ключ** для **Метод ідентифікації**, введіть спільний ключ довжиною від 1 до 127 символів.
	Підтвердити Попередньо виданий ключ	Введіть установлений ключ для підтвердження.

Параметри		Налаштування та пояснення
Віддалено	Метод ідентифікації	Щоб вибрати **Сертифікат**, необхідно заздалегідь отримати та імпортувати сертифікат, підписаний ЦС.
	Тип ідентифікатора	Якщо вибрано значення **Попередньо виданий ключ** для **Метод ідентифікації**, виберіть тип ідентифікатора для пристрою, який ви бажаєте автентифікувати.
	Ідентифікатор	Введіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Відоме ім'я**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «=». **IP-адреса**: введіть формат IPv4 або IPv6. **FQDN**: введіть комбінацію від 1 до 255 символів, використовуючи символи A–Z, a–z, 0–9, «-» та крапку (.). **Ел. адреса**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «@». **Ідентифікатор ключа**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E).
	Попередньо виданий ключ	Щоб вибрати **Попередньо виданий ключ** для **Метод ідентифікації**, введіть спільний ключ довжиною від 1 до 127 символів.
	Підтвердити Попередньо виданий ключ	Введіть установлений ключ для підтвердження.

❏ Інкапсуляція

Щоб вибрати **IPsec** для **Контроль доступу**, необхідно налаштувати режим інкапсуляції.

Параметри	Налаштування та пояснення
Транспортний режим	Виберіть, якщо сканер використовується в одній локальній мережі. Шифруватимуться пакети IP рівня 4 або вище.
Тунельний режим	Виберіть цей параметр, якщо сканер використовується в мережі з можливістю підключення до Інтернету, наприклад IPsec-VPN. Шифруватимуться заголовки та дані пакетів IP. **Віддалений шлюз (Тунельний режим)**: щоб вибрати **Тунельний режим** для **Інкапсуляція**, введіть адресу шлюзу довжиною від 1 до 39 символів.

❏ Протокол безпеки

Щоб вибрати **IPsec** для **Контроль доступу**, виберіть один з варіантів.

Параметри	Налаштування та пояснення
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.

❏ **Налаштування алгоритму**

Рекомендується вибирати **Будь-який** для всіх параметрів або вибирати для кожного параметра будь-яке значення, окрім **Будь-який**. Якщо для деяких параметрів вибрати **Будь-який** та вибрати інший елемент замість **Будь-який** для всіх інших параметрів, пристрій може не підключатися в залежності від іншого пристрою, який потрібно автентифікувати.

Параметри		Налаштування та пояснення
IKE	Шифрування	Виберіть алгоритм шифрування для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
	Автентифікація	Виберіть алгоритм автентифікації для IKE.
	Обмін ключами	Виберіть алгоритм обміну ключами для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
ESP	Шифрування	Виберіть алгоритм шифрування для ESP. Воно доступне, коли **ESP** вибрано для **Протокол безпеки**.
	Автентифікація	Виберіть алгоритм автентифікації для ESP. Воно доступне, коли **ESP** вибрано для **Протокол безпеки**.
AH	Автентифікація	Виберіть алгоритм шифрування для AH. Воно доступне, коли **AH** вибрано для **Протокол безпеки**.

Налаштування політики групи

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.

1. Відкрийте Web Config, а тоді виберіть вкладку **Мережева безпека** > **IPsec/фільтрування IP** > **Основні**.
2. Натисніть вкладку з номером, у якій необхідно виконати налаштування.
3. Введіть значення для кожного елемента.
4. Клацніть **Далі**.

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

   Сканер буде оновлено.

Групова політика Параметри

Параметри	Налаштування та пояснення
Увімкнути цю Групову політику	Групову політику можна ввімкнути або вимкнути.

Контроль доступу

Налаштуйте спосіб керування для трафіку або пакетів IP.

Параметри	Налаштування та пояснення
Дозволити доступ	Виберіть, щоб дозволити проходження налаштованих пакетів IP.
Відмовити в доступі	Виберіть це, щоб заборонити проходження налаштованих пакетів IP.
IPsec	Виберіть це, щоб дозволити проходження налаштованих пакетів IPsec.

Локальна адреса (Сканер)

Виберіть адресу IPv4 або IPv6, яка відповідає мережевому середовищу. Якщо IP-адреса призначається автоматично, можна вибрати параметр **Використовуйте автоматично отриману адресу IPv4**.

Примітка.
Якщо IPv6-адреса призначається автоматично, зв'язок може бути відсутнім. Установіть статичну IPv6-адресу.

Віддалена адреса (хост)

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.

Метод вибору порту

Виберіть метод указання портів.

❏ Ім'я служби

Щоб вибрати **Ім'я служби** для **Метод вибору порту**, виберіть один з варіантів.

❏ Транспортний протокол

Щоб вибрати **Номер порту** для **Метод вибору порту**, необхідно налаштувати режим інкапсуляції.

Параметри	Налаштування та пояснення
Будь-який протокол	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.

❏ Локальний порт

Якщо вибрати значення **Номер порту** для параметра **Метод вибору порту** та якщо вибрати протокол **TCP** або **UDP** для параметра **Транспортний протокол**, 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.

❏ Віддалений порт

Якщо вибрати значення **Номер порту** для параметра **Метод вибору порту** та якщо вибрати протокол **TCP** або **UDP** для параметра **Транспортний протокол**, 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.

Версія IKE

Виберіть **IKEv1** або **IKEv2** для **Версія IKE**. Виберіть одне зі значень відповідно до пристрою, до якого підключено сканер.

❏ IKEv1

Вказані нижче елементи відображаються, якщо вибрати **IKEv1** для **Версія IKE**.

Параметри	Налаштування та пояснення
Метод ідентифікації	Щоб вибрати **IPsec** для **Контроль доступу**, виберіть один з варіантів. Сертифікат, що використовується, має однакові параметри із сертифікатом політики за замовчуванням.
Попередньо виданий ключ	Щоб вибрати **Попередньо виданий ключ** для **Метод ідентифікації**, введіть спільний ключ довжиною від 1 до 127 символів.
Підтвердити Попередньо виданий ключ	Введіть установлений ключ для підтвердження.

❏ IKEv2

Вказані нижче елементи відображаються, якщо вибрати **IKEv2** для **Версія IKE**.

Параметри		**Налаштування та пояснення**
Локально	Метод ідентифікації	Щоб вибрати **IPsec** для **Контроль доступу**, виберіть один з варіантів. Сертифікат, що використовується, має однакові параметри із сертифікатом політики за замовчуванням.
	Тип ідентифікатора	Якщо вибрати **Попередньо виданий ключ** для параметра **Метод ідентифікації**, виберіть тип ідентифікатора для сканера.
	Ідентифікатор	Уведіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Відоме ім'я**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «=». **IP-адреса**: введіть формат IPv4 або IPv6. **FQDN**: введіть комбінацію від 1 до 255 символів, використовуючи символи A–Z, a–z, 0–9, «-» та крапку (.). **Ел. адреса**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «@». **Ідентифікатор ключа**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E).
	Попередньо виданий ключ	Щоб вибрати **Попередньо виданий ключ** для **Метод ідентифікації**, введіть спільний ключ довжиною від 1 до 127 символів.
	Підтвердити Попередньо виданий ключ	Введіть установлений ключ для підтвердження.

Параметри		Налаштування та пояснення
Віддалено	Метод ідентифікації	Щоб вибрати **IPsec** для **Контроль доступу**, виберіть один з варіантів. Сертифікат, що використовується, має однакові параметри із сертифікатом політики за замовчуванням.
	Тип ідентифікатора	Якщо вибрано значення **Попередньо виданий ключ** для **Метод ідентифікації**, виберіть тип ідентифікатора для пристрою, який ви бажаєте автентифікувати.
	Ідентифікатор	Введіть ідентифікатор сканера, який відповідає типу ідентифікатора. Неможливо як перший символ використовувати «@», «#» та «=». **Відоме ім'я**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «=». **IP-адреса**: введіть формат IPv4 або IPv6. **FQDN**: введіть комбінацію від 1 до 255 символів, використовуючи символи A–Z, a–z, 0–9, «-» та крапку (.). **Ел. адреса**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E). Потрібно включити «@». **Ідентифікатор ключа**: введіть від 1 до 255 1-байтних символів ASCII (0x20–0x7E).
	Попередньо виданий ключ	Щоб вибрати **Попередньо виданий ключ** для **Метод ідентифікації**, введіть спільний ключ довжиною від 1 до 127 символів.
	Підтвердити Попередньо виданий ключ	Введіть установлений ключ для підтвердження.

Інкапсуляція

Щоб вибрати **IPsec** для **Контроль доступу**, необхідно налаштувати режим інкапсуляції.

Параметри	Налаштування та пояснення
Транспортний режим	Виберіть, якщо сканер використовується в одній локальній мережі. Шифруватимуться пакети IP рівня 4 або вище.
Тунельний режим	Виберіть цей параметр, якщо сканер використовується в мережі з можливістю підключення до Інтернету, наприклад IPsec-VPN. Шифруватимуться заголовки та дані пакетів IP. **Віддалений шлюз (Тунельний режим)**: щоб вибрати **Тунельний режим** для **Інкапсуляція**, введіть адресу шлюзу довжиною від 1 до 39 символів.

Протокол безпеки

Щоб вибрати **IPsec** для **Контроль доступу**, виберіть один з варіантів.

Параметри	Налаштування та пояснення
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.

Налаштування алгоритму

Рекомендується вибирати **Будь-який** для всіх параметрів або вибирати для кожного параметра будь-яке значення, окрім **Будь-який**. Якщо для деяких параметрів вибрати **Будь-який** та вибрати інший елемент замість **Будь-який** для всіх інших параметрів, пристрій може не підключатися в залежності від іншого пристрою, який потрібно автентифікувати.

Параметри		Налаштування та пояснення
IKE	Шифрування	Виберіть алгоритм шифрування для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
	Автентифікація	Виберіть алгоритм автентифікації для IKE.
	Обмін ключами	Виберіть алгоритм обміну ключами для IKE. Ці елементи можуть відрізнятися в залежності від версії IKE.
ESP	Шифрування	Виберіть алгоритм шифрування для ESP. Воно доступне, коли **ESP** вибрано для **Протокол безпеки**.
	Автентифікація	Виберіть алгоритм автентифікації для ESP. Воно доступне, коли **ESP** вибрано для **Протокол безпеки**.
AH	Автентифікація	Виберіть алгоритм шифрування для AH. Воно доступне, коли **AH** вибрано для **Протокол безпеки**.

Поєднання адрес Локальна адреса (Сканер) та Віддалена адреса (хост) у поілтиці Групова політика

		Налаштування параметра Локальна адреса (Сканер)		
		IPv4	IPv6*2	Будь-які адреси*3
Налаштування параметра Віддалена адреса (хост)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Пуста	✓	✓	✓

*1 Якщо вибрано **IPsec** для параметра **Контроль доступу**, не можна вказати довжину префікса.

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

*3 Крім адрес локального зв'язку IPv6.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

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
Будь-який	–	–	–	Усі служби
ENPC	UDP	3289	Будь-який порт	Пошук сканера з таких програм як Epson Device Admin та драйвера сканера
SNMP	UDP	161	Будь-який порт	Отримання та конфігурація MIB-об'єкта з таких програм як Epson Device Admin і драйвера сканера Epson
WSD	TCP	Будь-який порт	5357	Керування WSD
WS-Discovery	UDP	3702	Будь-який порт	Пошук сканерів WSD
Network Scan	TCP	1865	Будь-який порт	Пересилання відсканованих даних з Document Capture Pro
Network Push Scan	TCP	Будь-який порт	2968	Отримання даних завдання для функції «push-scan» у Document Capture Pro
Network Push Scan Discovery	UDP	2968	Будь-який порт	Пошук комп'ютера зі сканера
FTP Дані (віддалена)	TCP	Будь-який порт	20	FTP-клієнт (пересилання відсканованих даних) Однак це дає змогу керувати тільки тим сервером FTP, який використовує віддалений порт 20.
FTP Контроль (віддалена)	TCP	Будь-який порт	21	FTP-клієнт (управління пересланими відсканованими даними)
CIFS (Віддалена)	TCP	Будь-який порт	445	CIFS-клієнт (пересилання відсканованих даних у папку)
NetBIOS Name Service (віддалена)	UDP	Будь-який порт	137	CIFS-клієнт (пересилання відсканованих даних у папку)
NetBIOS Datagram Service (віддалена)	UDP	Будь-який порт	138	
NetBIOS Session Service (віддалена)	TCP	Будь-який порт	139	
HTTP (Локальна)	TCP	80	Будь-який порт	Сервер HTTP(S) (пересилання даних Web Config та WSD)
HTTPS (Локальна)	TCP	443	Будь-який порт	

Назва служби	Тип протоколу	Номер локального порту	Номер віддаленого порту	Доступні функції
HTTP (Віддалена)	TCP	Будь-який порт	80	HTTP(S)-клієнт (оновлення мікропрограми й кореневого сертифіката)
HTTPS (Віддалена)	TCP	Будь-який порт	443	

Приклади налаштування функції IPsec/фільтрування IP

Отримання лише пакетів IPsec

Цей приклад демонструє налаштування лише політики за замовчуванням.

Політика за промовчанням:

❏ **IPsec/фільтрування IP**: **Увімкн.**

❏ **Контроль доступу**: **IPsec**

❏ **Метод ідентифікації**: **Попередньо виданий ключ**

❏ **Попередньо виданий ключ**: введіть до 127 символів.

Групова політика: не налаштовувати.

Отримання даних сканування та налаштувань сканера

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

Політика за промовчанням:

❏ **IPsec/фільтрування IP**: **Увімкн.**

❏ **Контроль доступу**: **Відмовити в доступі**

Групова політика:

❏ **Увімкнути цю Групову політику**: установіть прапорець.

❏ **Контроль доступу**: **Дозволити доступ**

❏ **Віддалена адреса (хост)**: IP-адреса клієнта

❏ **Метод вибору порту**: **Ім'я служби**

❏ **Ім'я служби**: установіть прапорець **ENPC**, **SNMP**, **HTTP (Локальна)**, **HTTPS (Локальна)** та **Network Scan**.

Отримання дозволу на доступ лише з указаної IP-адреси

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

Політика за промовчанням:

❏ **IPsec/фільтрування IP**: **Увімкн.**

❏ **Контроль доступу**:**Відмовити в доступі**

Групова політика:

❏ **Увімкнути цю Групову політику**: установіть прапорець.

❏ **Контроль доступу**: **Дозволити доступ**

❏ **Віддалена адреса (хост)**: IP-адреса клієнта адміністратора

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

Налаштування сертифіката для фільтрування IPsec/IP

Налаштуйте сертифікат клієнта для фільтрування IPsec/IP. При цьому ви можете використовувати сертифікат як спосіб автентифікації для фільтрування IPsec/IP. Якщо потрібно налаштувати центр сертифікації, перейдіть до **Сертифікат CA**.

1. Відкрийте Web Config, після чого виберіть вкладку **Мережева безпека** > **IPsec/фільтрування IP** > **Сертифікат клієнта**.

2. Імпортуйте сертифікат у **Сертифікат клієнта**.

   Якщо ви вже імпортували сертифікат, опублікований центром сертифікації, можна скопіювати сертифікат і використовувати його у фільтруванні IPsec/IP. Для копіювання виберіть сертифікат із **Копіювати з**, після чого клацніть **Копія**.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

➡ «Налаштування CA-підписаний Сертифікат» на сторінці 104

➡ «Налаштування Сертифікат CA» на сторінці 108

Підключення сканера до мережі IEEE802.1X

Налаштування мережі IEEE 802.1X

Коли ви налаштуєте мережу IEEE 802.1X на сканері, її можна використовувати в мережі, що підключена до сервера RADIUS, для перемикача локальної мережі з функцією автентифікації, або для точки доступу.

1. Відкрийте Web Config, а тоді виберіть вкладку **Мережева безпека** > **IEEE802.1X** > **Основні**.

2. Введіть значення для кожного елемента.

   Якщо необхідно використовувати сканер у мережі Wi-Fi, натисніть налаштування **Налаштування Wi-Fi** і виберіть або введіть ідентифікатор SSID.

   Примітка.
   До налаштувань можна надати спільний доступ у мережах Ethernet і Wi-Fi.

3. Клацніть **Далі**.

   Відобразиться повідомлення про підтвердження.

4. Клацніть **OK**.

   Сканер буде оновлено.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Параметри мережі IEEE 802.1X

Параметри	Налаштування та пояснення	
IEEE802.1X (Дротова LAN)	Можна ввімкнути або вимкнути налаштування сторінки (**IEEE802.1X** > **Основні**) для IEEE802.1X (дротова мережа LAN).	
IEEE802.1X (Wi-Fi)	Відображається стан з'єднання IEEE802.1X (Wi-Fi).	
Метод Підключення	Відображається спосіб підключення до поточної мережі.	
EAP Тип	Виберіть спосіб автентифікації між сканером і сервером RADIUS.	
	EAP-TLS	Отримайте та імпортуйте сертифікат, підписаний ЦС.
	PEAP-TLS	
	PEAP/MSCHAPv2	Установіть пароль.
	EAP-TTLS	
Ідентифікатор користувача	Налаштуйте ідентифікатор, який використовуватиметься для автентифікації сервера RADIUS. Введіть від 1 до 128 1-байтних символів ASCII (0x20–0x7E).	
Пароль	Установіть пароль для автентифікації сканера. Введіть від 1 до 128 1-байтних символів ASCII (0x20–0x7E). У разі використання сервера Windows як RADIUS-сервера можна ввести до 127 символів.	
Пароль підтвердження	Введіть установлений пароль для підтвердження.	
Ідентифікатор сервера	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 (0x20–0x7E).	
Перевірка сертифікату	Незалежно від методу автентифікації можна встановити перевірку сертифіката. Імпортуйте сертифікат у **Сертифікат CA**.	
Анонімне ім'я	Якщо вибрати **PEAP-TLS** або **PEAP/MSCHAPv2** для **EAP Тип**, ідентифікатор користувача для 1 фази PEAP-автентифікації можна залишити невизначеним. Введіть від 0 до 128 1-байтних символів ASCII (0x20–0x7E).	
Стійкість шифрування	Можна вибрати одне з нижченаведених значень.	
	Високий	AES256/3DES
	Середній	AES256/3DES/AES128/RC4

Налаштування сертифіката для IEEE 802.1X

Налаштування сертифіката клієнта для IEEE802.1X. Під час налаштування, можна використовувати **EAP-TLS** і **PEAP-TLS** як спосіб автентифікації IEEE 802.1X. Якщо потрібно налаштувати сертифікати, виданий центром сертифікації, перейдіть до **Сертифікат CA**.

1. Відкрийте Web Config, після чого виберіть вкладку **Мережева безпека** > **IEEE802.1X** > **Сертифікат клієнта**.

2. Введіть сертифікат у **Сертифікат клієнта**.

   Якщо ви вже імпортували сертифікат, опублікований центром сертифікації, можна скопіювати сертифікат і використовувати його в IEEE802.1X. Для копіювання виберіть сертифікат із **Копіювати з**, після чого клацніть **Копія**.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Вирішення проблем розширеного захисту

Відновлення функцій безпеки

У разі встановлення середовища з високим рівнем захисту, наприклад із фільтруванням за IPsec/IP 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 тимчасово скористатися пристроєм.

Відключення функції безпеки за допомогою Web Config

IPsec/фільтрування IP можна вимкнути за допомогою Web Config.

1. Відкрийте Web Config і виберіть вкладку **Мережева безпека** > **IPsec/фільтрування IP** > **Основні**.

2. Вимкніть **IPsec/фільтрування IP**.

Проблеми з використанням функцій безпеки мережі

Якщо ви забули спільний ключ

Налаштуйте знову спільний ключ.

Щоб змінити ключ, відкрийте Web Config та виберіть вкладку **Мережева безпека** > **IPsec/фільтрування IP** > **Основні** > **Політика за промовчанням** або **Групова політика**.

Після зміни спільного ключа налаштуйте його для комп'ютерів.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37
➡ «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 110

Не вдається встановити зв'язок IPsec

Зазначте алгоритм, який не підтримує сканер або комп'ютер.

Сканер підтримує такі алгоритми. Перевірте налаштування комп'ютера.

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	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
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 110

Раптове переривання зв'язку

IP-адресу сканера змінено або неможливо використати.

Якщо IP-адресу, зареєстровану до локальної адреси в Групова політика, було змінено або неможливо використати, то зв'язок IPsec не можна встановити. 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 (вкладка **Мережева безпека** > **IPsec/фільтрування IP** > **Основні** > **Групова політика** > **Локальна адреса (Сканер)**) сканера, може бути неможливо знайти.

Використовуйте статичну IP-адресу.

IP-адресу комп'ютера змінено або неможливо використати.

Якщо IP-адресу, зареєстровану до віддаленої адреси в Групова політика, було змінено або неможливо використати, то зв'язок IPsec не можна встановити.

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 (вкладка **Мережева безпека** > **IPsec/фільтрування IP** > **Основні** > **Групова політика** > **Віддалена адреса (хост)**) сканера, може бути неможливо знайти.

Використовуйте статичну IP-адресу.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

➡ «Шифрування зв'язку за допомогою фільтрації за IPsec/IP» на сторінці 110

Не вдається підключитися після зміни конфігурації IPsec/IP-фільтрування

Налаштування IPsec/IP-фільтрування неправильні.

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 110

Якщо не вдається отримати доступ до сканера після налаштування IEEE 802.1X

Налаштування IEEE 802.1X неправильні.

Вимкніть IEEE 802.1X та Wi-Fi на панелі керування сканера. Підключіть сканер до комп'ютера та повторно налаштуйте з'єднання IEEE 802.1X.

Підключіть сканер до комп'ютера та повторно налаштуйте з'єднання IEEE 802.1X.

Пов'язані відомості

➡ «Налаштування мережі IEEE 802.1X» на сторінці 122

Проблеми з використанням цифрового сертифіката

Не вдається імпортувати CA-підписаний Сертифікат

CA-підписаний Сертифікат та дані в ЗПС не збігаються.

Якщо CA-підписаний Сертифікат та ЗПС містять різні дані, ЗПС неможливо 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.

Розмір CA-підписаний Сертифікат більше 5 КБ.

Неможливо імпортувати CA-підписаний Сертифікат, розмір якого перевищує 5 КБ.

Невірний пароль для імпортування сертифіката.

Уведіть правильний пароль. Неможливо імпортувати сертифікат без пароля. Повторно отримайте CA-підписаний Сертифікат.

Пов'язані відомості

➡ «Імпортування сертифіката, підписаного ЦС» на сторінці 105

Не вдається оновити сертифікат із власним підписом

Не введено Загальна назва.

Загальна назва має бути введено.

Символи, що не підтримуються, введені у Загальна назва.

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

Загальна назва містить кому чи пробіл.

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

Пов'язані відомості

➡ «Оновлення сертифіката із власним підписом» на сторінці 107

Не вдається створити ЗПС

Не введено Загальна назва.

Загальна назва має бути введено.

Символи, що не підтримуються, введені до Загальна назва, Організація, Організаційна одиниця, Місце розташування, та Країна/Область.

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

Міститься кома чи пробіл у Загальна назва.

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

Пов'язані відомості

➡ «Отримання сертифіката, підписаного ЦС» на сторінці 104

Дії в разі появи попередження стосовно цифрового сертифіката

Повідомлення	Причини/Дії
Введіть Сертифікат сервера.	**Причина:** Не вибрано файл для імпорту. **Дія:** Виберіть файл і натисніть **Імпорт**.
Сертифікат CA 1 не введено.	**Причина:** 1-ий сертифікат ЦС не введено, введено лише 2-ий сертифікат ЦС. **Дія:** Спочатку імпортуйте 1-ий сертифікат ЦС.
Наведене нижче значення недійсне.	**Причина:** Шлях до файлу та/або пароль містить непідтримувані символи. **Дія:** Переконайтесь, що введено правильні символи.
Недійсні дата і час.	**Причина:** Дата й час сканера не встановлені. **Дія:** Установіть дату та час за допомогою налаштувань Web Config або EpsonNet Config.
Недійсний пароль.	**Причина:** Пароль, встановлений для сертифіката ЦС, і введений пароль відрізняються. **Дія:** Введіть правильний пароль.
Недійсний файл.	**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.

Повідомлення	Причини/Дії
Неможливо застосувати Сертифікати сервера які містять більше трьох Сертифікатів CA.	**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.
Термін дії сертифікату закінчився. Перевірте, чи сертифікат дійсний, або перевірте дату і час продукту.	**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.
Потрібний Особистий ключ.	**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.
Не вдалося настроїти.	**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 103

Сертифікат, підписаний ЦС, було помилково видалено

Нема резервного файлу для сертифіката, підписаного ЦС.

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

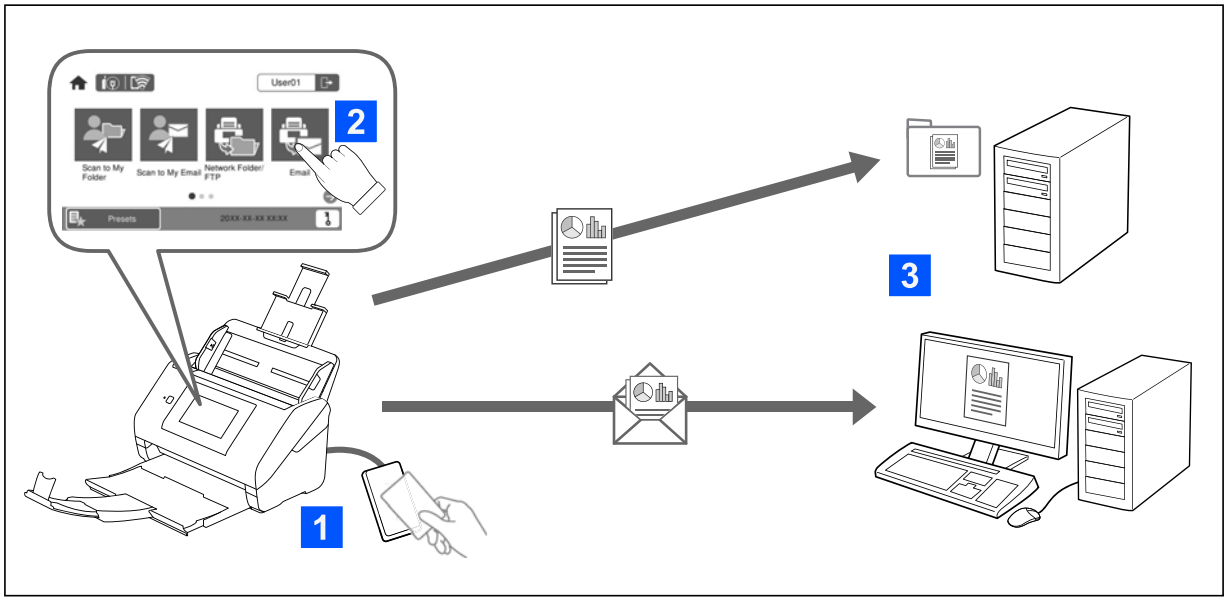
У разі отримання сертифіката за ЗПС, створеним через Web Config, імпортувати видалений сертифікат ще раз буде неможливо. Створіть ЗПС та отримайте новий сертифікат.

Пов'язані відомості

➡ «Імпортування сертифіката, підписаного ЦС» на сторінці 105
➡ «Видалення сертифіката, підписаного ЦС» на сторінці 107

Налаштування автентифікації

Про Налаштування автентифікації



Якщо Налаштування автентифікації ввімкнено, то для початку сканування буде потрібна автентифікація користувача. Ви можете налаштувати методи сканування, які може використовувати кожний окремий користувач, і запобігти випадковим операціям зі сканером.

Ви можете вказати адресу електронної пошти автентифікованого користувача як місце призначення сканування (Ск. в "Моя ел.пошта") або зберегти дані кожного користувача в особисту папку (Скан. в "Моя папка"). Ви також можете вказати інші методи сканування.

Примітка.

- ❏ *Ви не зможете виконувати сканування з комп'ютера або смарт-пристрою, якщо ввімкнено Налаштування автентифікації.*
- ❏ *На додаток до Налаштування автентифікації, викладених у цьому посібнику, ви також можете створити систему автентифікації за допомогою сервера автентифікації. Для цього скористайтеся Document Capture Pro Server Authentication Edition (скорочена назва — Document Capture Pro Server AE). Для отримання додаткової інформації зверніться до місцевого представництва Epson.*

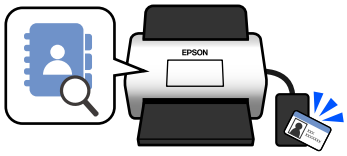
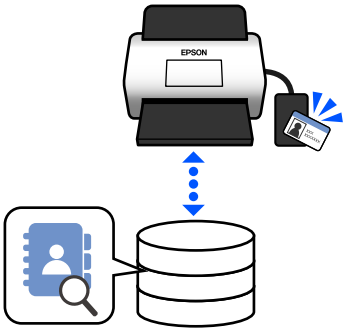
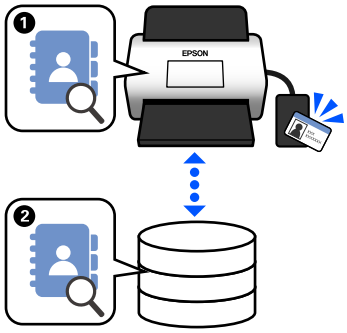
Доступні функції Налаштування автентифікації

Функція сканування на панелі керування	Налаштування автентифікації	
	Якщо увімкнено	Якщо вимкнено
Скан. в «Моя папка» Зберігає зображення до папки, призначеної для автентифікованого користувача.	✓	-
Скан. в «Моя ел.пошта» Надсилає зображення на електронну адресу автентифікованого користувача.	✓	-
Скан. до мереж. папки/FTP Зберігає зображення в папці в мережі.	✓	✓

Функція сканування на панелі керування	Налаштування автентифікації	
	Якщо увімкнено	Якщо вимкнено
Сканувати до ПК Зберігає зображення на підключеному комп'ютері за допомогою завдань, створених у Document Capture Pro (Windows)/Document Capture (Mac OS). * Якщо Налаштування автентифікації увімкнено, ви можете використовувати лише завдання, зареєстровані у **Налашт**.	✓*	✓
Сканувати до ел. пошти Надсилає зображення на вказану вами адресу електронної пошти.	✓	✓
Сканувати до Cloud Надсилає зображення до встановленої вами хмарної служби.	✓	✓
Скан. на USB-накопичувач Зберігає зображення на USB-накопичувач, підключений до сканера. Це доступно тільки, коли до сканера не підключено жодного пристрою автентифікації.	✓	✓
Сканувати у WSD Зберігає зображення на підключеному комп'ютері за допомогою функції WSD.	-	✓
Налашт Ви можете зареєструвати до 48 попередніх налаштувань функцій сканування. Користувачам, зареєстрованим у Локальний DB, можна призначити до п'яти Налашт. Призначені Налашт доступні лише для цього користувача. Налашт, які не було призначено жодному користувачеві, можуть використовуватися всіма користувачами.	✓	✓

Про Метод ідентифікації

Цей сканер може забезпечити автентифікацію за допомогою наступних методів без створення сервера аутентифікації.

	Локальний DB	**LDAP**	**Локальний DB та LDAP**
Розташування інформації про користувача	**Пам'ять сканера** Цей метод аутентифікації перевіряє інформацію про користувача, зареєстровану на сканері, і порівнює її з користувачем, який використовує функцію сканування.	**Сервер LDAP*** За допомогою цього методу автентифікації перевіряється інформація користувача на сервері LDAP, синхронізованому зі сканером. Оскільки до 300 елементів інформації про користувача із сервера LDAP можуть тимчасово зберігатися в сканері в якості кешу, то, якщо сервер LDAP вийде з ладу, автентифікацію можна виконати за допомогою кешу. * Сервер, що постачає службу каталогів, яка може зв'язуватися з LDAP.	**Пам'ять сканера й сервер LDAP** Спочатку перевірте інформацію користувача, зареєстровану в сканері (❶), і якщо збігу немає, перевірте інформацію користувача на сервері LDAP (❷).
			
Кількість зареєстрованих користувачів	50 (пам'ять сканера)	Необмежено (сервер LDAP)	50 (пам'ять сканера) Необмежено (сервер LDAP)
Кеш пам'яті сканера	-	300	Максимум 300 (50 слотів кешу використовуються спільно з Налаштування користувача у Локальний DB)
Методи входу в систему	Можна використовувати будь-який з наведених нижче способів. ❏ Підніміть картку автентифікації або введіть **Ідентифікатор користувача** та **Пароль** ❏ Підніміть картку автентифікації або введіть **Номер посвідчення** ❏ Введіть **Ідентифікатор користувача** та **Пароль** ❏ Введіть **Ідентифікатор користувача** ❏ Введіть **Номер посвідчення**		
Обмеження функції «Сканувати до»	Встановлюється індивідуально для кожного користувача	Однакові налаштування для всіх користувачів LDAP	Користувачі Локальний DB: встановлюється індивідуально Користувачі LDAP: однакові налаштування для всіх користувачів

	Локальний DB	LDAP	Локальний DB та LDAP
Розподіл Налашт для користувачів	До 5 на користувача	- (Не можна налаштувати окремо)	Користувачі Локальний DB: до 5 на користувача Користувачі LDAP: -

Програмне забезпечення для налаштування

Виконайте налаштування за допомогою Web Config або Epson Device Admin.

❏ У разі використання сторінки Web Config сканер можна налаштовувати тільки за допомогою веб-браузера.

«Web Config» на сторінці 37

❏ У разі використання сторінки Epson Device Admin ви можете налаштувати кілька сканерів одночасно за допомогою шаблону конфігурації.

«Epson Device Admin» на сторінці 38

Оновлення мікропрограми сканера

Перш ніж увімкнути Налаштування автентифікації, оновіть мікропрограму сканера до останньої версії. Заздалегідь підключіть сканер до Інтернету.

Важливо

Не вимикайте сканер або комп'ютер під час оновлення.

При налаштуванні з Web Config:

Виберіть вкладку **Керування пристроєм** > **Оновлення мікропрограми**, а потім дотримуйтесь інструкцій на екрані, аби оновити мікропрограму.

При налаштуванні з Epson Device Admin:

Виберіть на екрані списку пристроїв **Home** > **Firmware** > **Update**, а потім дотримуйтесь інструкцій на екрані, аби оновити мікропрограму.

Примітка.
Якщо найновішу версію мікропрограми вже встановлено, оновлення не потрібне.

Підключення й налаштування пристрою автентифікації

Якщо ви хочете підключити й використовувати такий пристрій автентифікації, як-от пристрій для зчитування IC-карт, спочатку потрібно налаштувати пристрій. Це необов'язково, якщо пристрій автентифікації не використовується.

Пов'язані відомості

➡ «Підключення пристрою автентифікації» на сторінці 138

➡ «Налаштування пристрою автентифікації» на сторінці 139

Список сумісності з пристроєм для зчитування карт

Цей список не гарантує успішного виконання операцій пристроями для зчитування карт, викладених у списку.

Так: підтримується (інформацію щодо ідентифікатора можна прочитати за допомогою стандартних налаштувань пристрою для зчитування карт)

Ні: несумісне

Виробник	Модель	Номер моделі	Картка автентифікації							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Так	Так*1	Так*1	Так*1	Ні	Ні	Ні	Клавіатура
RF IDEAS	pcProx	RDR-7081BKU	Так*1	Ні	Так	Так	Ні	Ні	Ні	Клавіатура
RF IDEAS	pcProx	RDR-7581AKU	Так	Ні	Так*1	Так*1	Ні	Ні	Ні	Клавіатура
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Ні	Ні	Так	Так	Ні	Ні	Ні	Клавіатура
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Так	Ні	Так	Так	Так	Так	Так	Клавіатура
ELATEC	TWN4 MULTITECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Так	Так	Так	Так	Так	Так	Так	Клавіатура

Виробник	Модель	Номер моделі	Картка автентифікації							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ELATEC	TWN4 MultiTech 2 BLE-PI	T4LK-FB4BLZ-PI	Так	Так	Так	Так	Так	Так	Так	Клавіатура
ELATEC	TWN4 Slim	T4QC-FC3B7	Так	Так	Так	Так	Так	Так	Так	Клавіатура
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Так	Так	Так	Так	Так	Hi	Так	Клавіатура[*1]
ACS	ACR122U	ACR122U	Hi	Hi	Так[*2]	Так[*2]	Так	Hi	Так[*2]	PC/SC
ACS	ACR1252	ACR1252	Hi	Hi	Так[*2]	Так[*2]	Так	Так	Так[*2]	PC/SC
Sony	PaSoRi	RC-S330/S	Hi	Hi	Так[*2]	Так[*2]	Так[*2]	Так[*2]	Так[*2]	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Hi	Hi	Так[*2]	Так[*2]	Так[*2]	Так[*2]	Так[*2]	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Так	Так	Так	Так	Так	Так	Так	Клавіатура
DMZ	Leitor RFID Multi-125	DMZ087	Hi	Так	Hi	Hi	Hi	Hi	Hi	Клавіатура
DMZ	Leitor RFID Mifare	DMZ088	Hi	Hi	Так	Так	Hi	Hi	Hi	Клавіатура
DMZ	Biometric & RFID Reader	DMZ073	Hi	Так	Hi	Hi	Hi	Hi	Hi	Клавіатура

Виробник	Модель	Номер моделі	Картка автентифікації							Режим
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
inepro	SCR708	SCR708	Так*1	Так*1	Так*1	Так*1	Так*1	Так*1	Так*1	Клавіатура
Y Soft	YU03088 001	MU0388	Так	Так	Так	Так	Так	Так	Так	Клавіатура
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Hi	Hi	Так	Так	Hi	Hi	Так	Клавіатура
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Hi	Hi	Так	Так	Hi	Hi	Так	Клавіатура
NT-ware	MiCard MultiTech4-PI	T4DT-FB4WUF-PI	Так	Так	Так	Так	Так	Так	Так	Клавіатура
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Так*1	Так*1	Так*1	Так*1	Hi	Hi	Hi	Клавіатура
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Так	Так	Так	Так	Так	Так	Hi	Клавіатура

*1 Вам потрібно змінити налаштування пристрою для зчитування карт за допомогою фірмового програмного забезпечення, наданого виробником пристрою для зчитування карт.

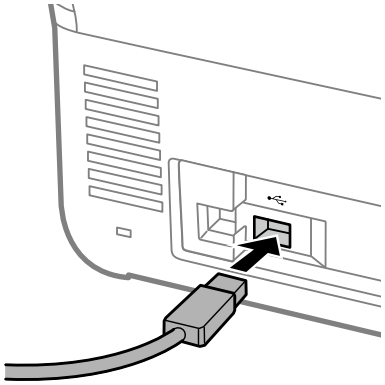
*2 Якщо вам потрібно використовувати дані в певній області на картці, крім стандартного ідентифікатора картки, в якості ідентифікатора автентифікації, налаштувавши параметри продукту, зверніться до свого партнера Epson або місцевого представника компанії для отримання додаткової інформації про спосіб налаштування продукту.

Підключення пристрою автентифікації

Важливо

Коли ви підключаєте пристрій аутентифікації до кількох сканерів, використовуйте продукт з тим самим номером моделі.

Під'єднайте USB-кабель пристрою для зчитування карт до порту зовнішнього інтерфейсу пристрою USB сканера.



Перевірка роботи пристрою автентифікації

Ви можете перевірити стан підключення й розпізнавання картки автентифікації для пристрою автентифікації на панелі керування сканера.

Інформація відображається, якщо вибрати **Налаш.** > **Інформація про пристрій** > **Аутентифікація статусу пристрою**.

Налаштування пристрою автентифікації

Встановіть формат зчитування інформації про автентифікацію, отриману з картки автентифікації.

На пристрої автентифікації можна налаштувати наведений нижче спосіб зчитування.

❏ Зчитування певної ділянки на картці автентифікації, як-от особистий номер або номер посвідчення працівника.

❏ Використання інформації картки автентифікації, окрім як для ідентифікатора користувача (інформація картки автентифікації, як-от серійний номер).

Ви можете використовувати інструмент для створення робочих параметрів. За докладнішою інформацією зверніться до дилера.

Примітка.
Використання карток автентифікації від різних виробників.

Під час використання даних картки ідентифікатора користувача (інформація ідентифікатора картки, як-от серійний номер) можна застосовувати набір різних типів карток автентифікації. При використанні іншої інформації картки цього робити не можна.

При налаштуванні з Web Config:

Виберіть вкладку **Керування пристроєм** > **Кард-рідер**.

При налаштуванні з Epson Device Admin:

Виберіть **Administrator Settings** > **Authentication Settings** > **Card Reader** із шаблону конфігурації.

Елемент	Пояснення
Vendor ID	Установіть ідентифікатор постачальника пристрою автентифікації, яким можна обмежити використання за допомогою 4 алфавітно-цифровими символів від 0000 до FFFF. Якщо обмеження не потрібно, введіть значення 0000.
Product ID	Установіть ідентифікатор виробу пристрою автентифікації, яким можна обмежити використання за допомогою 4 алфавітно-цифровими символів від 0000 до FFFF. Якщо обмеження не потрібно, введіть значення 0000.
Робочі параметри	Установіть параметр роботи пристрою автентифікації: 0–8192 символи. Доступні символи: A–Z, a–z, 0–9, +, /, =, пробіл і символ переміщення рядка.
Кард-рідер	Виберіть формат конвертації для пристрою автентифікації. Ви можете переглянути подробиці щодо формату. Перегляньте посилання в описі елемента.
Формат збереження ідентифікатора картки автентифікації	Виберіть формат конвертації для інформації автентифікації посвідчення. Ви можете переглянути подробиці щодо формату. Перегляньте посилання в описі елемента.
Встановити діапазон ідентифікатора картки	Увімкніть специфікацію положення зчитування.
Початкове положення тексту	Вкажіть початкову позицію тексту для читання в інформації щодо ідентифікатора. Можна вказати від 1 до 4096 символів.
Кількість символів	Вкажіть кількість символів, які потрібно зчитати з початкової позиції інформації щодо ідентифікатора. Можна вказати від 1 до 4096 символів.

Інформація про реєстрацію й налаштування

Налаштування

Виконайте необхідні налаштування залежно від Метод ідентифікації та методу сканування, який ви використовуєте.

Важливо

Перш ніж розпочати налаштування, переконайтеся, що налаштування часу сканера є правильним.

Якщо налаштування часу неправильне, буде відображено повідомлення помилки «Сплив термін дії ліцензії», що може призвести до неможливості налаштування сканера. Крім того, щоб використовувати функції безпеки, наприклад зв'язок через SSL/TLS або IPsec, потрібно правильно налаштувати час. Час можна налаштувати у спосіб, зазначений нижче.

❏ *Вкладка Web Config:* ***Керування пристроєм*** > ***Дата і час*** > ***Дата і час****.*

❏ *Панель керування сканера:* ***Налаш.*** > ***Основні налашт.*** > ***Налаштув. дати/часу****.*

Налаштування	Локальний DB	LDAP	Локальний DB та LDAP
Увімкнення автентифікації Перед встановленням параметрів автентифікації необхідно ввімкнути автентифікацію. «Увімкнення автентифікації» на сторінці 141	✓	✓	✓
Налаштування автентифікації Встановлення Метод ідентифікації та способів автентифікації користувача. «Налаштування автентифікації» на сторінці 142	✓	✓	✓
Реєстрація Налаштування користувача Зареєструйте налаштування для кожного користувача. За допомогою файлу CSV також можна реєструвати групу користувачів. «Реєстрація Налаштування користувача» на сторінці 143	✓	–	✓
Синхронізація з Сервер LDAP Створіть параметри синхронізації сервера LDAP. «Синхронізація зСервер LDAP» на сторінці 150	–	✓	✓
Налаштування Сервер ел. пошти Встановіть поточні налаштування сервера електронної пошти. Налаштуйте це під час використання функцій, для яких потрібні налаштування сервера електронної пошти, наприклад Ск. в "Моя ел.пошта". «Налаштування сервера електронної пошти» на сторінці 154	✓	✓	✓
Налаштування Скан. в "Моя папка" Укажіть папки місце призначення. Налаштуйте це під час використання функції Скан. в "Моя папка". «Налаштування Скан. в "Моя папка"» на сторінці 155	✓	✓	✓
Налаштувати функції одного дотику Встановіть ці параметри під час зміни елементів, що відображаються на панелі керування сканера. На панелі керування можна відобразити лише необхідні вам піктограми або ж змінити їх порядок. «Налаштувати функції одного дотику» на сторінці 157	✓	✓	✓

Увімкнення автентифікації

Перед встановленням параметрів автентифікації необхідно ввімкнути автентифікацію.

При налаштуванні з Web Config:

Виберіть **Увімкн. (пристрій/Сервер LDAP)** з вкладки **Безпека продукту** > **Основні** > **Автентифікація**.

При налаштуванні з Epson Device Admin:

Виберіть у шаблоні конфігурації **Увімкн. (пристрій/Сервер LDAP)** з **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Примітка.
Якщо увімкнути на сканері Налаштування автентифікації, то для панелі керування також увімкнеться Налаштування блокування. Панель керування не можна розблокувати, якщо увімкнено Налаштування автентифікації.

Навіть якщо ви вимкнете Налаштування автентифікації, то Налаштування блокування залишиться увімкненим. Якщо ви бажаєте вимкнути його, ви можете виконати налаштування на панелі керування або у Web Config.

Пов'язані відомості

➡ «Налаштування Налаштування блокування за допомогою панелі керування» на сторінці 90

➡ «Налаштування Налаштування блокування з Web Config» на сторінці 90

Налаштування автентифікації

Встановлення Метод ідентифікації та способів автентифікації користувача.

При налаштуванні з Web Config:

Виберіть вкладку **Безпека продукту** > **Налаштування автентифікації**.

При налаштуванні з Epson Device Admin:

Виберіть **Administrator Settings** > **Authentication Settings** > **Authentication Settings** із шаблону конфігурації.

Елемент	Пояснення
Метод ідентифікації	Виберіть Метод ідентифікації. ❏ Локальний DB Пройдіть автентифікацію за допомогою Налаштування користувача, зареєстрованих на сканері. Необхідно зареєструвати користувача на сканері. ❏ LDAP Автентифікація за допомогою інформації користувача сервера LDAP, синхронізованого зі сканером. Необхідно заздалегідь налаштувати сервер LDAP. ❏ Локальний DB та LDAP Автентифікація за допомогою інформації користувача, зареєстрованої для сканера або сервера LDAP, синхронізованого зі сканером. Вам потрібно зареєструвати користувача на сканері й налаштувати сервер LDAP.

Елемент	Пояснення
Як виконати автентифікацію користувача	Вибір способу автентифікації користувача. ❏ Картка чи ідентифікатор користувача та пароль Використовуйте картку автентифікації для автентифікації користувачів. Для автентифікації можна також використовувати ідентифікатор користувача та пароль. ❏ Код користувача та пароль Використання ідентифікатора користувача та пароля для автентифікації користувача. Якщо вибрати цю функцію, ви не зможете використовувати картку автентифікації для автентифікації користувача. ❏ Ідентифікатор користувача Використання лише ідентифікатора користувача для його автентифікації. Пароль встановлювати не потрібно. ❏ Картка чи номер ідентифікатора Використовуйте картку автентифікації для автентифікації користувачів. Також можна використовувати Номер посвідчення. ❏ Номер посвідчення Використання тільки посвідчень для автентифікації користувачів.
Дозволити користувачам реєструвати картки автентифікації	Вмикається, якщо потрібно дозволити користувачу зареєструвати карту автентифікації в системі. Якщо вибрати **LDAP** для **Метод ідентифікації**, ви не зможете встановити його. Додаткову інформацію про те, як користувачі можуть зареєструвати свої картки автентифікації, викладено в розділі «Реєстрація картки аутентифікації» у *Посібник користувача*.
Мінімальна кількість цифр в номер посвідчення	Виберіть для номера посвідчення мінімальну кількість цифр.
Кешування для користувачів, що пройшли аутентифікацію на сервері LDAP	Якщо користуватися сервер автентифікації LDAP, можна вибрати, чи використовувати кешування відомостей про користувача.
Використовувати дані користувача для автентифікації SMTP	Якщо користуватися ідентифікатором і паролем користувача для автентифікації, можна вибрати, чи використовувати відомості про користувача для автентифікації SMTP. Система використовує останній ідентифікатор і пароль користувача, з якими було здійснено вхід.
Обмеження для автентифцікованих користувачів LDAP	Якщо ви використовуєте LDAP, ви можете налаштувати функції, доступні для користувача.

Реєстрація Налаштування користувача

Зареєструйте Налаштування користувача, які використовуються для автентифікації користувача. Реєстрацію можна виконати будь-яким з наведених нижче способів.

❏ Реєстрація Налаштування користувача один за одним (Web Config)

❏ Реєстрація кількохНалаштування користувача в якості пакету за допомогою файлу CSV (Web Config)

❏ Реєстрація User Settings для кількох сканерів в якості пакету за допомогою шаблону конфігурації (Epson Device Admin)

Пов'язані відомості

- «Реєстрація Налаштування користувача окремо (Web Config)» на сторінці 144
- «Реєстрація кількохНалаштування користувача за допомогою файлу CSV (Web Config)» на сторінці 145
- «Реєстрація User Settings для кількох сканерів в якості пакету (Epson Device Admin)» на сторінці 148

Реєстрація Налаштування користувача окремо (Web Config)

Виберіть Web Config, а тоді виберіть вкладку **Безпека продукту** > **Налаштування користувача** > **Додати**, після чого введіть Налаштування користувача.

Елемент	Пояснення
Ідентифікатор користувача	Введіть ідентифікатор користувача, який ви хочете використовувати для автентифікації, в діапазоні від 1 до 83 байт, що може виражатися у форматі Unicode (UTF-8). Оскільки ідентифікатор користувача не чутливий до регістру, ви можете вводити дані великими або малими літерами.
Відображення ім'я користувача	Введіть ім'я користувача, що відображається на панелі керування сканера: 32 символи, які можуть бути виражені у форматі Unicode (UTF-16). Поле можна залишити порожнім.
Пароль	Введіть потрібний пароль для використання з метою автентифікації: не більше 32 символів у форматі ASCII. Пароль чутливий до регістру літер. Залиште порожнім, якщо використовується **Ідентифікатор користувача** для **Як виконати автентифікацію користувача**.
Ідентифікатор картки автентифікації	Введіть ідентифікатор картки аутентифікації: не більше 116 символів у форматі ASCII. Поле можна залишити порожнім. Якщо дозволити **Дозволити користувачам реєструвати картки автентифікації** для **Налаштування автентифікації**, буде відображено результати, зареєстровані користувачами.
Номер посвідчення	Цей елемент відображається, коли **Картка чи номер ідентифікатора** або **Номер посвідчення** вибрано у **Налаштування автентифікації** > **Як виконати автентифікацію користувача**. Введіть число, яке стоїть між числом, встановленим у **Налаштування автентифікації** > **Мінімальна кількість цифр в номер посвідчення**, і містить до 8 цифр.
Згенерувати автоматично	Цей елемент відображається, коли **Картка чи номер ідентифікатора** або **Номер посвідчення** вибрано у **Налаштування автентифікації** > **Як виконати автентифікацію користувача**. Натисніть сюди, аби автоматично згенерувати ідентифікаційний номер з такою ж кількістю цифр, яку ви вибрали в параметрі **Мінімальна кількість цифр в номер посвідчення**.
Відділ	Введіть назву відділу тощо, що ідентифікує користувача, — в межах 40 символів, які можуть бути виражені у форматі Unicode (UTF-16). Поле можна залишити порожнім.
Ел. адреса	Введіть адресу електронної пошти користувача: не більше 200 символів у форматі ASCII. Використовується як адреса для **Ск. в "Моя ел.пошта"**. Поле можна залишити порожнім.

Елемент	Пояснення
Скан. в "Моя папка"	Встановіть окремі місця призначення для збереження після вибору **Індивідуальні** у **Скан. в "Моя папка"** > **Тип налаштувань**. Подробиці про налаштування елементів див. нижче. «Налаштування Скан. в "Моя папка"» на сторінці 155
Обмеження	Функції можна обмежити для кожного користувача. Виберіть функцію, яку ви дозволяєте використати.
Налашт	Можна налаштувати до 5 параметрів, доступних лише вибраним користувачам у меню Налашт на сканері. ❏ Налашт, які було призначено користувачеві, може використовувати лише цей користувач. Налашт, які не було призначено жодному користувачеві, можуть використовуватися всіма користувачами. ❏ Якщо користувач має лише одне доступне Налашт, воно автоматично завантажується після автентифікації. Якщо доступно кілька Налашт, то після автентифікації відображатиметься список Налашт. ❏ Ви не можете створювати або відображати Налашт, що використовують функції, які було обмежено в **Обмеження**.

Реєстрація кількохНалаштування користувача за допомогою файлу CSV (Web Config)

Введіть налаштування для кожного користувача у файлі CSV та зареєструйте їх як пакет.

Створення файлу CSV

Створення файлу CSV для імпорту Налаштування користувача.

Примітка.
Якщо ви зареєструєте одне або кілька Налаштування користувача заздалегідь, а потім експортуєте відформатований файл (файл CSV), то зможете використовувати зареєстроване налаштування в якості посилання для введення елементів налаштувань.

1. Відкрийте Web Config і виберіть вкладку **Безпека продукту** > **Налаштування користувача**.
2. Клацніть **Експорт**.
3. Виберіть формат файлу для **Формат файлу**.

   Під час вибору користуйтеся наведеними нижче відомостями.

Елемент	Пояснення
CSV UTF-16 (розділений табуляцією)	Для редагування файлу за допомогою Microsoft Excel. Кожен параметр береться в «[ ]» (дужки). Введіть параметри в «[ ]». У разі оновлення файлу рекомендуємо замінити його. У разі збереження нового файлу, виберіть Unicode text (*.txt), як формат файлу.

Елемент	Пояснення
CSV UTF-8 (розділений комами)	Для редагування файлу за допомогою текстового редактора або макроса без використання Microsoft Excel.
CSV UTF-8 (розділений двокрапкою)	

4. Клацніть **Експорт**.

5. Редагуйте та зберігайте цей файл CSV в табличному редакторі, наприклад Microsoft Excel, або текстовому редакторі.

> ***Важливо***
>
> *Під час редагування файлу не змінюйте кодування та інформацію заголовка.*

Налаштування файлу CSV

Елемент	Налаштування та пояснення
UserID	Введення ідентифікатора користувача для використання автентифікації: 1–83 байтів у форматі Unicode.
UserName	Введення імені користувача, що відображається на панелі керування сканера: 32 символи у форматі Unicode. Поле можна залишити порожнім.
Password	Введення паролю для використання з метою автентифікації: не більше 32 символів у форматі ASCII. Під час імпорту це використовується як пароль замість [**EncPassword**]. Залиште порожнім, якщо використовується **Ідентифікатор користувача** для **Як виконати автентифікацію користувача**. Під час експорту цей параметр завжди порожній.
AuthenticationCardID	Встановлення результату зчитування картки автентифікації. Якщо дозволити **Дозволити користувачам реєструвати картки автентифікації** у **Налаштування автентифікації**, буде відображено результати, зареєстровані користувачами. Введіть до 116 символів у форматі ASCII. Поле можна залишити порожнім.
IDNumber	Цей елемент відображається, коли **Картка чи номер ідентифікатора** або **Номер посвідчення** вибрано у **Налаштування автентифікації** > **Як виконати автентифікацію користувача**. Введіть число, яке стоїть між числом, встановленим у **Налаштування автентифікації** > **Мінімальна кількість цифр в номер посвідчення**, і містить до 8 цифр. Номер посвідчення не можна дублювати. Якщо номер продубльовано, вам надійде оповіщення про помилку під час імпортування файлу. Якщо його не вказати, номер призначається автоматично.
Department	Введення довільного імені відділу з метою розрізнення користувачів. Введіть до 40 символів у Unicode. Поле можна залишити порожнім.

Елемент	Налаштування та пояснення
MailAddress	Встановлення адреси електронної пошти користувача. Використовується як адреса для **Ск. в "Моя ел.пошта"**. Можна використовувати: A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Уведіть до 200 символів. Неможливо як перший символ використовувати «,» (кому). Поле можна залишити порожнім.
FolderProtocol	Установлює тип функції Скан. в "Моя папка". Мережева папка/FTP (SMB): 0, FTP: 1
FolderPath	Указує місце збереження для функції Скан. в "Моя папка".
FolderUserName	Указує ім'я користувача для функції Скан. в "Моя папка".
FolderPassword	Указує пароль для автентифікації цільової папки для функції Скан. в "Моя папка", використовуючи до 32 символів ASCII. Під час імпорту це використовується як пароль замість [**EncPassword**]. Під час експорту цей параметр завжди порожній.
FtpPassive	Указує режим підключення для сервера FTP, коли параметр **FTP** вибрано як **Тип** для функції Скан. в "Моя папка". Активний режим: 0, пасивний режим: 1
FtpPort	Указує номер порту (від 0 до 65535) для надсилання сканованих даних на сервер FTP, коли параметр **FTP** вибрано як **Тип** для функції Скан. в "Моя папка".
ScanToMemory	Встановіть обмеження для Скан. на USB-накопичувач. Не дозволено: 0, дозволено: 1
ScanToMail	Встановіть обмеження для Сканувати в ел. пошту. Параметр **Скан. в «Моя ел.пошта»** можна встановити, тільки якщо ввімкнено функцію **Сканувати в ел. пошту**. Не дозволено: 0, дозволено: 1
ScanToFolder	Встановіть обмеження для Сканувати в мережеву папку/FTP. Параметр **Скан. в «Моя папка»** можна встановити, тільки якщо ввімкнено функцію **Сканувати в мережеву папку/FTP**. Не дозволено: 0, дозволено: 1
ScanToCloud	Встановіть обмеження для Сканувати в «хмарний» сервіс. Не дозволено: 0, дозволено: 1
ScanToComputer	Встановіть обмеження для Сканувати до ПК. Не дозволено: 0, дозволено: 1
PresetIndex	Встановіть Налашт, які ви хочете пов'язати з користувачем. Можна встановити до п'яти реєстраційних номерів для Налашт, розділених комами.
EncPassword	Під час експортування налаштувань користувача, параметр установлений для **Password** шифрується, після чого значення кодується за допомогою BASE64 і виводиться. Під час імпортування з новим паролем для **Password** це значення ігнорується. Якщо поле **Password** порожнє, це значення використовується, а пароль залишається таким, яким був до експортування.

Елемент	Налаштування та пояснення
EncFolderPassword	Під час експорту параметр установлений для **FolderPassword** шифрується, після чого значення кодується за допомогою BASE64 і виводиться. Під час імпортування з новим паролем для **FolderPassword** це значення ігнорується. Якщо поле **FolderPassword** порожнє, це значення використовується, а пароль залишається таким, яким був до експортування.

Імпорт файлу CSV

1. Відкрийте Web Config і виберіть вкладку **Безпека продукту** > **Налаштування користувача**.
2. Клацніть **Імпорт**.
3. Виберіть файл, який потрібно імпортувати.
4. Клацніть **Імпорт**.
5. Перегляньте відображену інформацію та клацніть **ОК**.

Реєстрація User Settings для кількох сканерів в якості пакету (Epson Device Admin)

Ви можете зареєструвати User Settings, що використовуються в Локальний DB, в якості пакету за допомогою сервера LDAP або файлу CSV/ENE.

Примітка.
*Файл ENE — це двійковий файл від Epson, який шифрує та зберігає інформацію щодо **Contacts**, наприклад, особисту інформацію та Налаштування користувача. Його можна експортувати з Epson Device Admin та встановити пароль. Він стане в нагоді, коли потрібно буде імпортувати Налаштування користувача з файлу резервної копії.*

Імпортування з файлу CSV/ENE

1. Виберіть **Administrator Settings** > **Authentication Settings** > **User Settings** із шаблону конфігурації.
2. Клацніть **Import**.
3. Виберіть значення **CSV or ENE File** у параметрі **Import Source**.
4. Клацніть **Browse**.

   Буде відображено екран вибору файлів.
5. Виберіть файл, який потрібно імпортувати, аби відкрити його.

6. Виберіть спосіб імпортування.

   ❏ Overwrite and Add: перезаписує, якщо існує той самий ідентифікатор користувача; додає новий ідентифікатор, якщо його не існує.

   ❏ Replace All: замінює всі елементи налаштуваннями користувача, які потрібно імпортувати.

7. Клацніть **Import**.

   Відобразиться екран підтвердження налаштування.

8. Клацніть **OK**.

   Відобразиться результат перевірки.

   Примітка.
   ❏ *Якщо кількість імпортованих налаштувань користувача перевищує кількість, яку можна імпортувати, з'явиться повідомлення з пропозицією видалити деякі налаштування користувача. Видаліть зайві налаштування користувача перед імпортом.*

   ❏ *Виберіть налаштування користувача, які потрібно видалити перед імпортом, а потім клацніть* ***Delete****.*

9. Клацніть **Import**.

   Налаштування користувача буде імпортовано до шаблону конфігурації.

Імпортування з сервера LDAP

1. Виберіть **Administrator Settings** > **Authentication Settings** > **User Settings** із шаблону конфігурації.

2. Клацніть **Import**.

3. Виберіть значення **LDAP** у параметрі **Import Source**.

4. Клацніть **Settings**.

   Відобразяться налаштування **LDAP Server**.

   Примітка.
   Це налаштування сервера LDAP призначене для імпорту налаштувань користувача з сервера LDAP. Імпортовані (скопійовані) налаштування користувача використовуються для автентифікації користувачів за допомогою самого сканера.

   З іншого боку, коли ви вибираєте ***LDAP*** *або* ***Local DB and LDAP*** *як метод автентифікації, користувачі автентифікуються шляхом комунікації з сервером LDAP.*

5. Налаштуйте кожен елемент.

   Під час імпорту налаштувань користувача з сервера LDAP, окрім параметрів LDAP, можна також налаштувати наступні параметри.

   Щоб дізнатися про інші елементи, перегляньте розділ «Пов'язані відомості».

Елемент		Пояснення
LDAP Server Settings	LDAP Server Type	Дозволяє виберат тип сервера LDAP.

Елемент			Пояснення
Search Settings	Search Filter		Ви можете встановити текст, який використовується для фільтра пошуку LDAP. Аби відредагувати текст пошуку, виберіть **Custom**.
	Options	Type	Ви можете встановити тип місця збереження для параметра **Scan To My Folder**.
		Connection Mode	Якщо **Type** встановлено як **FTP**, ви можете встановити режим підключення до FTP.
		Port Number	Якщо **Type** встановлено як **FTP**, ви можете встановити номер порту, який ви бажаєте використовувати.

6. Якщо потрібно, виконайте тест на зв'язок, клацнувши **Connection Test**.

   Отримує та відображає 10 налаштувань користувача з сервера LDAP.

7. Клацніть **OK**.

8. Виберіть спосіб імпортування.

   ❏ Overwrite and Add: перезаписує, якщо існує той самий ідентифікатор користувача; додає новий ідентифікатор, якщо його не існує.

   ❏ Replace All: замінює всі елементи налаштуваннями користувача, які потрібно імпортувати.

9. Клацніть **Import**.

   Відобразиться екран підтвердження налаштування.

10. Клацніть **OK**.

    Відобразиться результат перевірки.

11. Клацніть **Import**.

    Налаштування користувача буде імпортовано до шаблону конфігурації.

Пов'язані відомості

➡ «Налаштування сервера LDAP» на сторінці 151

➡ «Налаштування параметрів пошуку сервера LDAP» на сторінці 152

Синхронізація зСервер LDAP

Виконайте налаштування Сервер LDAP для сканера.

За потреби налаштуйте і первинний, і вторинний сервери.

Примітка.
*Налаштування **Сервер LDAP** повідомлено **Контакти**.*

Доступні служби

Підтримуються такі служби каталогів.

Назва служби	Версія
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Налаштування сервера LDAP

Для використання сервера LDAP, спочатку потрібно налаштувати сервер LDAP.

При налаштуванні з Web Config:

Виберіть вкладку **Мережа** > **Сервер LDAP** > **Основні (Головний сервер)** або **Основні (Резервний сервер)**.

Якщо ви вибрали **Kerberos Автентифікація** в якості **Метод ідентифікації**, виберіть **Мережа** > **Налаштування Kerberos** для внесення налаштувань для Kerberos.

При налаштуванні з Epson Device Admin:

Виберіть **Network** > **LDAP server** > **Server Settings (Primary Server)** або **Server Settings (Secondary Server)** із шаблону конфігурації.

Якщо ви вибрали **Kerberos Автентифікація** в якості **Метод ідентифікації**, виберіть **Network — Security** > **Налаштування Kerberos** для внесення налаштувань для Kerberos.

Елемент	Налаштування та пояснення
Застосувати Сервер LDAP	Виберіть **Викор.** або **Не використ.**.
LDAP Адреса сервера	Введіть адресу сервера LDAP. Введіть від 1 до 255 символів формату IPv4, IPv6 або FQDN. Для формату FQDN можна використовувати букви або цифри кодування ASCII (0x20–0x7E) і символ дефісу, за винятком початку та кінця адреси.
LDAP Номер порту сервера (Port number)	Уведіть номер порту сервера LDAP за допомогою чисел від 1 до 65535.
Надійне підключення	Виберіть метод автентифікації для доступу сканера до сервера LDAP.
Перевірка сертифікату	Після підключення буде автентифіковано сертифікат сервера LDAP. Ми рекомендуємо встановити для цього значення **Увімкн.**. Для налаштування потрібно, щоб **Сертифікат CA** було імпортовано на сканер.
Перерва пошуку (сек)	Установіть ліміт часу пошуку від 5 до 300 секунд.

Елемент	Налаштування та пояснення
Метод ідентифікації	Оберіть метод аутентифікації. Якщо ви вибрали **Kerberos Автентифікація**, заздалегідь встановіть налаштування для Kerberos. Щоб виконати Kerberos Автентифікація, нижченаведене середовище є обов'язковим. ❏ Сканер та сервер DNS можна з'єднати. ❏ Час, необхідний сканеру, серверу KDC та серверу для автентифікації (сервер LDAP, сервер SMTP, файловий сервер), синхронізується. ❏ Якщо сервер послуг призначено як IP-адресу, то FQDN для сервера служби буде зареєстровано у зворотній зоні пошуку сервера DNS.
Kerberos Область для використання	Якщо вибрали **Kerberos Автентифікація** для **Метод ідентифікації**, то слід вказати область Kerberos, яку потрібно використовувати.
Унікальне ім'я адміністратора / Ім'я користувача	Уведіть ім'я користувача для сервера LDAP, використавши до 128 символів у форматі Unicode (UTF-8). Не можна використовувати керівні символи, як-от від 0x00 до 0x1F та 0x7F. Це значення не потрібне, якщо вибрано **Анонімна автентифікація** для параметра **Метод ідентифікації**. Якщо ви не бажаєте вказувати дані, залиште поле пустим.
Пароль	Уведіть пароль для автентифікації на сервері LDAP, використавши до 128 символів у форматі Unicode (UTF-8). Не можна використовувати керівні символи, як-от від 0x00 до 0x1F та 0x7F. Це значення не потрібне, якщо вибрано **Анонімна автентифікація** для параметра **Метод ідентифікації**. Якщо ви не бажаєте вказувати дані, залиште поле пустим.

Налаштування Kerberos

Якщо ви вибрали **Kerberos Автентифікація** як значення для параметра **Метод ідентифікації**, вам потрібно виконати налаштування Kerberos. Зареєструвати можна до 10 параметрів Kerberos.

При налаштуванні з Web Config:

Виберіть вкладку **Мережа** > **Налаштування Kerberos**.

При налаштуванні з Epson Device Admin:

Виберіть **Network** > **Security** > **Налаштування Kerberos** із шаблону конфігурації.

Елемент	Налаштування та пояснення
Область (домен)	Введіть в області автентифікації Kerberos до 255 символів формату ASCII (0x20–0x7E). Якщо ви не бажаєте вводити дані, залиште поле пустим.
KDC Адреса	Введіть адресу сервера автентифікації Kerberos. Введіть до 255 символів у форматі IPv4, IPv6 або FQDN. Якщо ви не бажаєте вводити дані, залиште поле пустим.
Номер порту (Kerberos)	Уведіть номер порту сервера Kerberos за допомогою чисел від 1 до 65535.

Налаштування параметрів пошуку сервера LDAP

Встановлює атрибути пошуку для налаштувань користувача.

При налаштуванні з Web Config:

Виберіть вкладку **Мережа** > **Сервер LDAP** > **Параметри пошуку (автентифкація)**.

При налаштуванні з Epson Device Admin:

Виберіть **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** із шаблону конфігурації.

Елемент	Налаштування та пояснення
Search Base (Distinguished Name)	Укажіть початкову позицію для пошуку інформації користувача з сервера LDAP. Введіть від 0 до 128 символів формату Юнікод (UTF-8). Якщо шукати довільний атрибут не треба, залиште це поле порожнім. Приклад каталогу локального сервера: dc=server,dc=local
User ID Attribute	Укажіть ім'я атрибута для відображення під час пошуку номера посвідчення. Вводьте від 1 до 255 символів формату ASCII. Першим має бути один із символів a–z або A–Z. Наприклад: cn, uid
User name Display Attribute	Укажіть ім'я атрибута для відображення як імені користувача. Вводьте від 0 до 255 символів формату ASCII. Першим має бути один із символів a–z або A–Z. Поле можна залишити порожнім. Наприклад: cn, name
Authentication Card ID Attribute	Укажіть ім'я атрибута для відображення як ідентифікатора картки автентифікації. Вводьте від 0 до 255 символів формату ASCII. Першим має бути один із символів a–z або A–Z. Поле можна залишити порожнім. Наприклад: cn, sn
ID Number Attribute	Укажіть ім'я атрибута для відображення під час пошуку номера посвідчення. Вводьте від 1 до 255 символів формату ASCII. Першим має бути один із символів a–z або A–Z. Наприклад: cn, id
Department Attribute	Укажіть ім'я атрибута для відображення як імені відділу. Вводьте від 0 до 255 символів формату ASCII. Першим має бути один із символів a–z або A–Z. Поле можна залишити порожнім. Наприклад: ou, ou
Email Address Attribute	Укажіть ім'я атрибута для відображення під час пошуку адрес електронної пошти. Вводьте від 1 до 255 символів формату ASCII. Першим має бути один із символів a–z або A–Z. Наприклад: mail
Save To Attribute	Указує назву атрибута, який вказує місце для функції Scan To My Folder. Вводьте від 0 до 255 символів формату ASCII. Наприклад: homeDirectory

Перевірка з'єднання з сервером LDAP

Виконує перевірку з'єднання з сервером LDAP за допомогою параметра, встановленого в **Сервер LDAP** > **Налаштування пошуку**.

1. Відкрийте Web Config і виберіть вкладку **Мережа** > **Сервер LDAP** > **Перевірка підключення**.

2. Виберіть **Пуск**.

   Почнеться перевірка з'єднання. Після завершення перевірки відображається звіт про її результати.

Повідомлення перевірки з'єднання з сервером LDAP

Повідомлення	Пояснення
Перевірка підключення пройшла успішно.	Це повідомлення відображається тоді, коли відбулося успішне з'єднання з сервером.
Помилка перевірки підключення. Перевірте налаштування.	Це повідомлення з'являється з однієї з нижчезазначених причин: ❏ Адресу сервера LDAP або номер порту вказано невірно. ❏ Минув час очікування. ❏ **Не використ.** вибрано для **Застосувати Сервер LDAP**. ❏ Якщо значення **Kerberos Автентифікація** вибрано для **Метод ідентифікації**, такі налаштування як **Область (домен)**, **KDC Адреса** та **Номер порту (Kerberos)** будуть неправильні.
Помилка перевірки підключення. Перевірте дату й час на виробі чи сервері.	Це повідомлення з'являється в разі виникнення помилки з'єднання, коли налаштування часу сканера та сервера LDAP не збігаються.
Помилка автентифікації. Перевірте налаштування.	Це повідомлення з'являється з однієї з нижчезазначених причин: ❏ Невірно вказано **Ім'я користувача** та/або **Пароль**. ❏ Якщо вибрано **Kerberos Автентифікація** як **Метод ідентифікації**, дату/час, можливо, не вдасться налаштувати.
Немає доступу до продукту, доки обробку не буде завершено.	Це повідомлення відображається, коли сканер зайнято.

Налаштування сервера електронної пошти

При використанні **Ск. в "Моя ел.пошта"** встановіть параметр Серверу електронної пошти.

Примітка.
*Параметр **Ск. в "Моя ел.пошта"** можна встановити, тільки якщо ввімкнено функцію **Сканувати в ел. пошту**.*

При налаштуванні з Web Config:

Виберіть вкладку **Мережа** > **Сервер ел. пошти** > **Основні**.

При налаштуванні з Epson Device Admin:

Виберіть **Common** > **Email Server** > **Mail Server Settings** із шаблону конфігурації.

Елемент	Налаштування та пояснення	
Метод ідентифікації	Виберіть метод автентифікації для доступу сканера до поштового сервера.	
	Вимкнути	Автентифікацію вимкнено під час зв'язку з поштовим сервером.
	аутентифікація SMTP	Необхідно, щоб поштовий сервер підтримував автентифікацію SMTP.
	POP перед SMTP	Якщо ви вибрали цей елемент, налаштуйте сервер POP3.
Ідентифіков. обл. Запис	Якщо ви вибрали **аутентифікація SMTP** або **POP перед SMTP** в якості **Метод ідентифікації**, введіть ім'я автентифікованого облікового запису. Можна ввести від 0 до 255 символів формату ASCII (0x20–0x7E).	
Ідентифікований пароль	Якщо ви вибрали **аутентифікація SMTP** або **POP перед SMTP** в якості **Метод ідентифікації**, введіть автентифікований пароль. Можна ввести від 0 до 20 символів формату ASCII (0x20–0x7E).	
Ел. адреса відправника	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.	
Адреса сервера SMTP	Введіть від 0 до 255 символів, використовуючи символи A–Z a–z 0–9 . -. Можна використовувати формат IPv4 або FQDN.	
Номер порту сервера SMTP	Введіть число від 1 до 65535.	
Надійне підключення	Укажіть метод безпечного підключення для сервера електронної пошти.	
	Немає	Якщо вибрати **POP перед SMTP** у **Метод ідентифікації**, метод з'єднання перейде у значення **Немає**.
	SSL/TLS	Воно доступне, коли **Метод ідентифікації** має значення **Вимкнути** або **аутентифікація SMTP**.
	STARTTLS	Воно доступне, коли **Метод ідентифікації** має значення **Вимкнути** або **аутентифікація SMTP**.
Перевірка сертифікату	Сертифікат автентифікується, якщо увімкнено цю функцію. Ми рекомендуємо встановити для цього значення **Увімкн.**.	
Адреса сервера POP3	Якщо ви вибрали **POP перед SMTP** в якості **Метод ідентифікації**, введіть адресу сервера POP3. Можна ввести від 0 до 255 символів, використовуючи символи A–Z a–z 0–9. Можна використовувати формат IPv4 або FQDN.	
Номер порту сервера POP3	Якщо ви вибрали **POP перед SMTP** в якості **Метод ідентифікації**, вкажіть номер порту. Введіть число від 1 до 65535.	

Налаштування Скан. в "Моя папка"

Зберігає скановане зображення в папку, призначену кожному користувачеві. Варіанти встановлення спеціальної папки наведено нижче.

Примітка.
*Параметр **Scan To My Folder** можна встановити, тільки якщо ввімкнено функцію **Сканувати в мережеву папку/FTP**.*

Збереження в налаштуваннях	Метод ідентифікації	Розташування параметрів шляху до папки
Вкажіть одну мережеву папку для всіх Налаштування автентифікації, аби автоматично створити особисту папку під вказаною папкою, використовуючи ім'я ідентифікатора користувача.	❏ Локальний DB ❏ LDAP ❏ Локальний DB та LDAP	Сканер (налаштування Скан. в "Моя папка")
Створити окремі мережеві папки для кожного користувача.	Локальний DB	Сканер (Налаштування користувача)
	LDAP	Атрибути LDAP
	Локальний DB та LDAP	Сканер (Налаштування користувача) або атрибути LDAP

При налаштуванні з Web Config:

Виберіть вкладку **Безпека продукту** > **Сканувати в мережеву папку/FTP**.

При налаштуванні з Epson Device Admin:

Виберіть **Administrator Settings** > **Authentication Settings** > **Сканувати в мережеву папку/FTP** > **Scan to My Folder** із шаблону конфігурації.

Елемент		Пояснення
Зберегти в налаштування	Тип налаштувань	❏ **Спільні**: Автоматично створює папку, назва якої складається з ідентифікатора користувача, за шляхом до папки або URL-адресою, указаною в опції **Зберегти в**, і зберігає туди відскановані зображення. ❏ **Індивідуальні**: Установлює місце збереження результатів сканування для кожного користувача. Користувачів Локальний DB можна встановити в налаштуваннях користувачів. Користувачі LDAP застосовують місце зберігання, отримане з атрибутів пошуку сервера LDAP.
	Тип	Виберіть протокол передачі відповідно до місця призначення сканування. Для мережевої папки: **Мережева папка (SMB)** Для сервера FTP: **FTP**
	Зберегти в	Вкажіть шлях або URL шляху виводу. Введіть до 160 символів у Unicode (UTF-16).
	Режим підключення	Установлюється, якщо ви вибрали параметр **FTP** у налаштуваннях **Тип**. Виберіть режим підключення до сервера FTP.
	Номер порту	Установлюється, якщо ви вибрали параметр **FTP** у налаштуваннях **Тип**. Введіть номер порту для надсилання сканованих даних до серверу FTP — від 0 до 65535.

Елемент		Пояснення
Налаштування автентифікації	Тип налаштувань	Установлюється, якщо ви вибрали параметр **Індивідуальні** в якості **Тип налаштувань** у **Зберегти в налаштування**. Для отримання доступу в папку налаштуйте «Ім'я користувача» та «Пароль». ❏ **Спільні**: Використовуйте загальні **Ім'я користувача** та **Пароль** для всіх користувачів. ❏ **Індивідуальні**: Для користувачів Локальний DB встановіть **Ім'я користувача** та **Пароль** окремо в **Параметри користувача**. Для користувачів LDAP неможливо задати налаштування окремо. **Ім'я користувача** та **Пароль**, встановлені за допомогою цього елемента, використовуються як пакет.
	Ім'я користувача	Введіть ім'я користувача для доступу до папки виводу сканувань. Введіть до 30 символів у Unicode (UTF-16). Встановіть цей параметр, якщо ви використовуєте **Спільні** сервер або сервер LDAP.
	Пароль	Введіть пароль, відповідний до **Ім'я користувача**. Введіть до 20 символів у Unicode (UTF-16). Встановіть цей параметр, якщо ви використовуєте **Спільні** сервер або сервер LDAP.

Заборона зміни місця призначення для Сканувати в мережеву папку/FTP

Елемент	Пояснення
Заборонити введення призначення вручну	Коли цей параметр увімкнено, користувач не зможе змінювати місце призначення за замовчуванням.

Налаштувати функції одного дотику

Можна відображати лише необхідні значки, змінивши макет, який відображається на головному екрані для панелі керування.

При налаштуванні з Web Config:

Виберіть вкладку **Безпека продукту** > **Налаштувати функції одного дотику**.

При налаштуванні з Epson Device Admin:

Виберіть **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** із шаблону конфігурації.

Примітка.
У наступних випадках значки вказаних функцій не відображаються на головному екрані.

❏ *Якщо вибирати функції, заборонені через **Обмеження**.*

❏ *Якщо електронна адреса користувача, який виконав вхід, не зареєстрована. (Ск. в "Моя ел.пошта")*

❏ *Якщо не вибрано папку призначення. (Скан. в "Моя папка")*

Елемент	Пояснення
Максимальна кількість функцій у вікні	Виберіть макет значків, що відображаються на панелі керування. Зображення змінюється відповідно до вибраного макета.
Вікно(-а)	Виберіть кількість сторінок.
Номер	Виберіть функції, які потрібно відображати для кожної пронумерованої позиції.

Звіти Job History за допомогою Epson Device Admin

Ви можете створити звіт Job History для кожної групи та кожного користувача за допомогою Epson Device Admin. Ви можете зберегти на сканері до 3000 екземплярів історії використання. Звіт можна створити, вказавши період або звичайний розклад.

Аби вивести Job History у вигляді звіту, виберіть **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** у стрічці меню на екрані «Список пристроїв».

Ви можете дізнатися більше про те, як створити звіт користувача, у відповідній документації щодо Epson Device Admin.

Елементи, які може бути включено до звіту

У звіт користувача можна вивести наступні елементи.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Вхід в якості адміністратора з панелі керування

Для входу в систему в якості адміністратора з панелі керування сканера ви можете використовувати будь-який з наведених нижче методів.

1. Торкніться елемента  у верхньому правому куті екрана.
   - ❏ Якщо Налаштування автентифікації ввімкнено, піктограма відображається на екрані **Ласкаво просимо** (екран очікування автентифікації).
   - ❏ Якщо Налаштування автентифікації вимкнено, на головному екрані відображається піктограма.
2. Коли відобразиться екран підтвердження, натисніть **Так**.
3. Введіть пароль адміністратора.

   Відобразиться повідомлення про успішне виконання входу, після чого ви побачите головний екран на панелі керування.

Для виходу торкніться елемента  у верхньому правому куті головного екрана.

Вимикання Налаштування автентифікації

Налаштування автентифікації можна вимкнути за допомогою Web Config.

Примітка.
Налаштування користувача, зареєстровані на сканері, буде збережено, навіть якщо Налаштування автентифікації вимкнено. Ви можете видалити їх, відновивши налаштування сканера за замовчуванням.

1. Відкрийте Web Config.
2. Виберіть вкладку **Безпека продукту** > **Основні** > **Автентифікація**.
3. Виберіть **Вимкнути**.
4. Клацніть **Далі**.
5. Клацніть **OK**.

Примітка.
Навіть якщо ви вимкнете Налаштування автентифікації, то Налаштування блокування залишиться увімкненим. Якщо ви бажаєте вимкнути його, ви можете виконати налаштування на панелі керування або у Web Config.

Пов'язані відомості

➡ «Налаштування Налаштування блокування за допомогою панелі керування» на сторінці 90
➡ «Налаштування Налаштування блокування з Web Config» на сторінці 90

Видалення даних Налаштування автентифікації (Віднов. налашт. за зам.)

Щоб видалити всю інформацію щодоНалаштування автентифікації (Кард-рідер, Метод ідентифікації, Налаштування користувача тощо), відновіть усі налаштування сканера до налаштувань за замовчуванням, наявних на момент покупки.

Виберіть на панелі керування **Налаш.** > **Сист. адміністрування** > **Віднов. налашт. за зам.** > **Всі налаштування**.

> ***Важливо***
> *Усі контакти та інші налаштування мережі також буде видалено. Видалені налаштування відновити не можна.*

Вирішення проблем

Картка автентифікації не зчитується

Перевірте зазначену нижче інформацію.

❏ Перевірте, чи пристрій автентифікації правильно підключено до сканера.

Підключіть пристрій автентифікації до порту зовнішнього інтерфейсу пристрою USB на задній панелі сканера.

❏ Переконайтеся в тому, що пристрій та картка автентифікації підтримуються.

Обслуговування

Очищення зовнішніх компонентів сканера

Витріть будь-які плями на корпусі сухою або зволоженою у м'якому очиснику або воді тканиною.

Важливо

- ❏ *Не застосовуйте для очищення сканера спирт, розріджувач або будь-який розчинник. Це може призвести до деформації або втрати кольору.*
- ❏ *Стежте, щоб всередину продукту не потрапила вода. Це може призвести до несправності.*
- ❏ *Не відкривайте корпус сканера.*

1. Натисніть на сканері кнопку ⏻, щоб вимкнути його.
2. Відключіть адаптер змінного струму від сканера.
3. Очистіть зовнішню сторону корпусу тканиною, змоченою у м'якому миючому засобі.

   Примітка.
   Протріть сенсорний екран за допомогою м'якої сухої тканини.

Очищення внутрішніх компонентів сканера

Після певного часу використання сканера на внутрішньому ролику або на склі всередині сканера може збиратися кімнатний або паперовий пил, що призводить до проблем із подаванням паперу або до погіршення якості зображення. Очищуйте сканер зсередини після кожних 5,000 циклів сканування.

Кількість сканувань можна побачити на панелі керування або в Epson Scan 2 Utility.

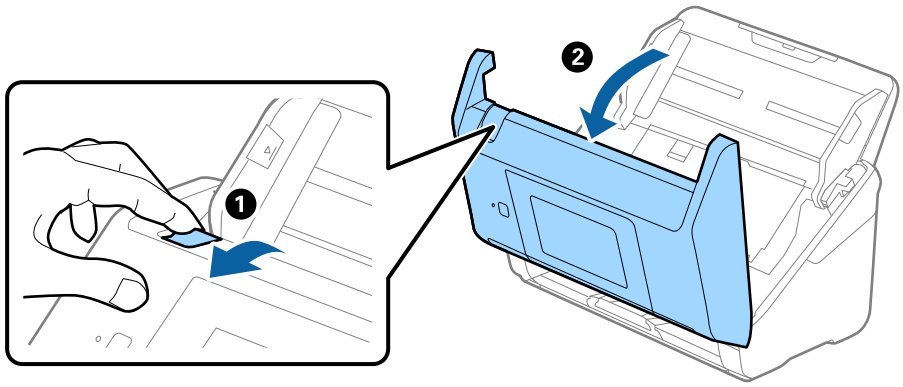
Якщо поверхня забруднена речовиною, яку важко видалити, використовуйте оригінальний набір для чищення Epson, щоб видалити плями. Щоб видалити плями, нанесіть трохи очисника на тканину.

Важливо

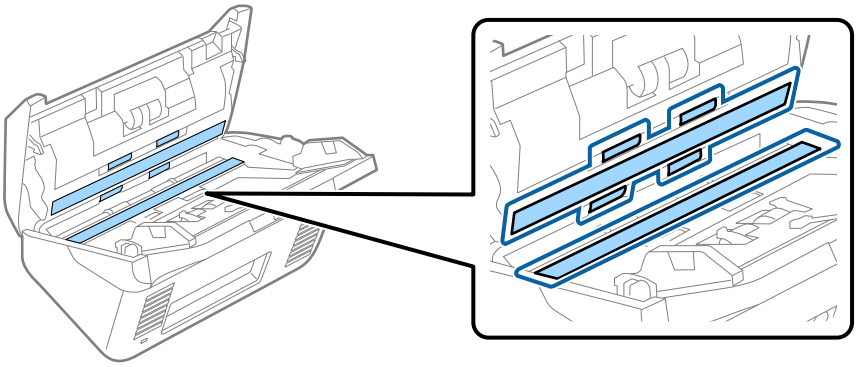
- ❏ *Не застосовуйте для очищення сканера спирт, розріджувач або будь-який розчинник. Це може призвести до деформації або втрати кольору.*
- ❏ *Ніколи не розпилюйте будь-яку рідину чи мастило на сканер. Пошкодження обладнання або коротке замикання можуть призвести до несправної роботи.*
- ❏ *Не відкривайте корпус сканера.*

1. Натисніть на сканері кнопку ⏻, щоб вимкнути його.
2. Відключіть адаптер змінного струму від сканера.

3. Потягніть важіль і відкрийте кришку сканера.

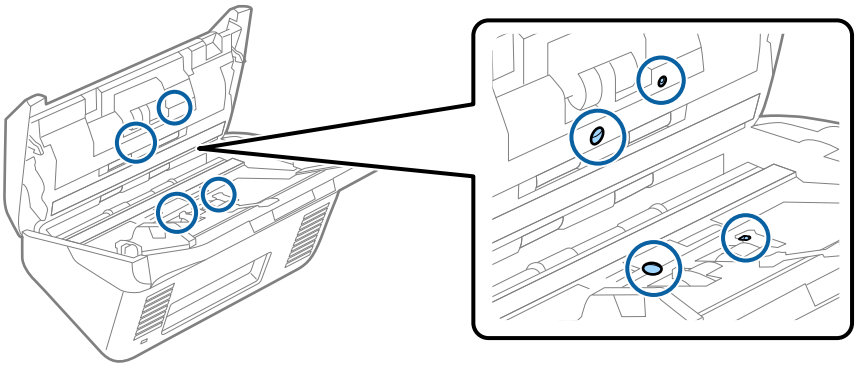


4. Витріть будь-які плями на пластиковому ролику та на поверхні скла під кришкою сканера, використовуючи м’яку тканину або оригінальний набір для чищення Epson.



> ***Важливо***
>
> ❏ *Не тисніть силою на поверхню скла.*
>
> ❏ *Не використовуйте щітку або твердий предмет. Будь-які подряпини на склі можуть призвести до погіршення якості сканування.*
>
> ❏ *Не розбризкуйте рідину для очищення безпосередньо на скляну поверхню.*

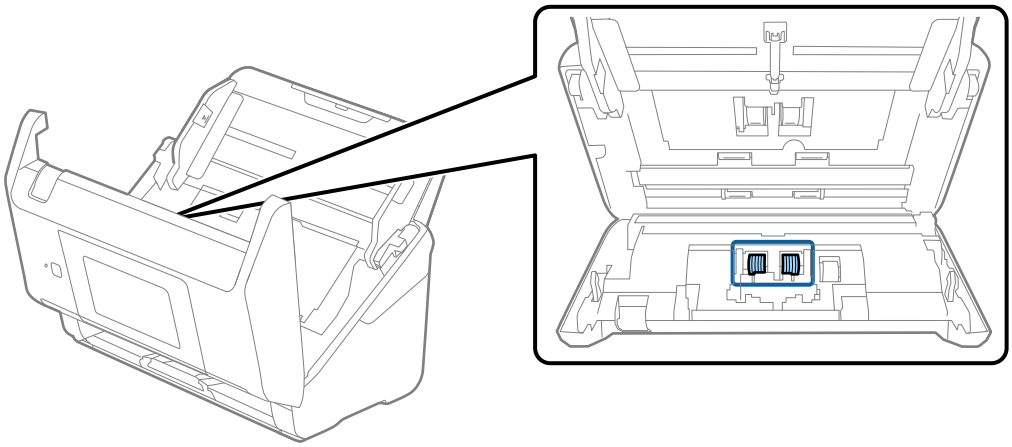
5. Зітріть будь-які плями на датчиках за допомогою ватного тампона.



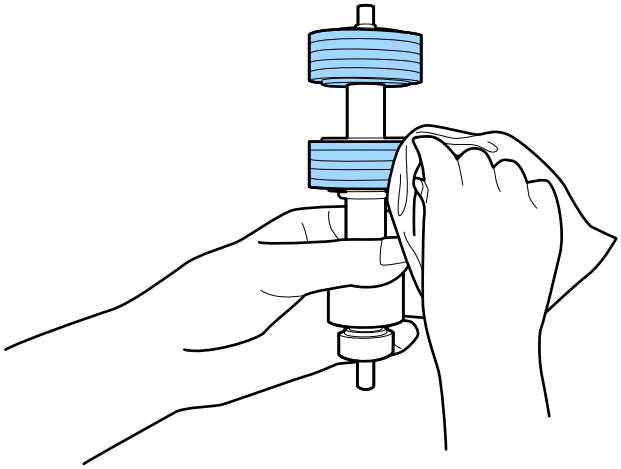
> ***Важливо***
>
> *Не потрібно наносити рідину, наприклад, очищувач, на ватний тампон.*

6. Відкрийте кришку та витягніть ролик розділення.

   Для детальнішої інформації див. «Заміна вузла подачі паперу».



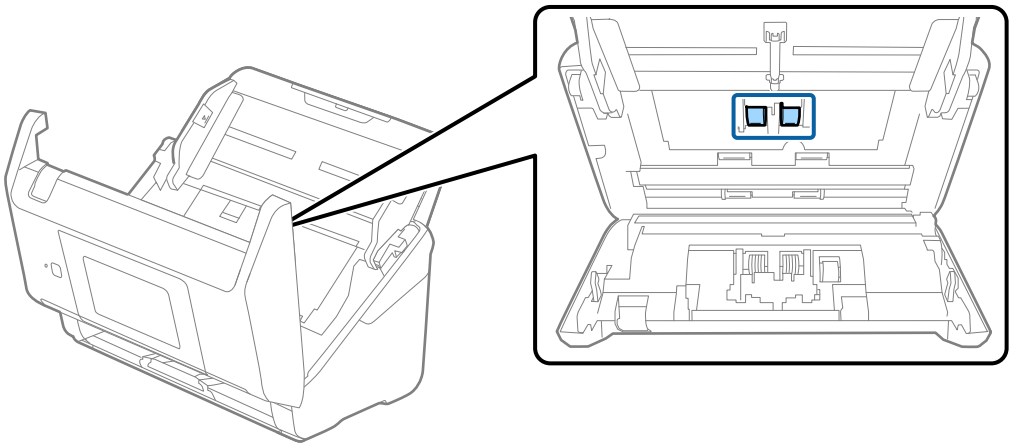
7. Зітріть пил або бруд з ролика розділення за допомогою оригінального набору для чищення Epson або м'якою вологою тканиною.



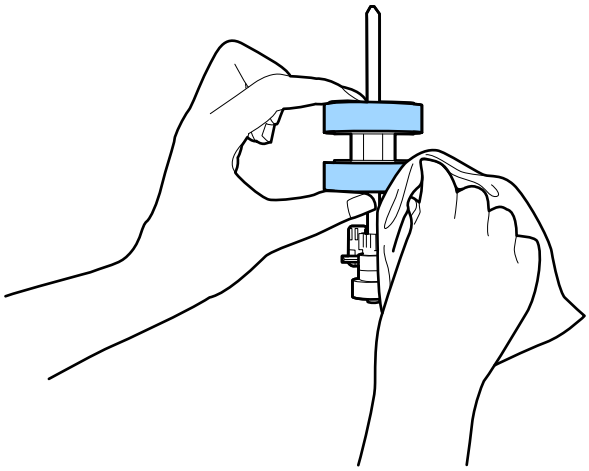
> ***Важливо***
>
> *Використовуйте лише оригінальний набір для чищення Epson або м'яку вологу тканину. Використання сухої тканини може призвести до пошкодження поверхні ролика.*

8. Відкрийте кришку та витягніть ролик подачі паперу.

   Для детальнішої інформації див. «Заміна вузла подачі паперу».



9. Зітріть пил або бруд з ролика подачі паперу за допомогою оригінального набору для чищення Epson або м'якою вологою тканиною.



> ***Важливо***
>
> *Використовуйте лише оригінальний набір для чищення Epson або м'яку вологу тканину. Використання сухої тканини може призвести до пошкодження поверхні ролика.*

10. Закрийте кришку сканера.

11. Вставте в розетку адаптер змінного струму та ввімкніть сканер.

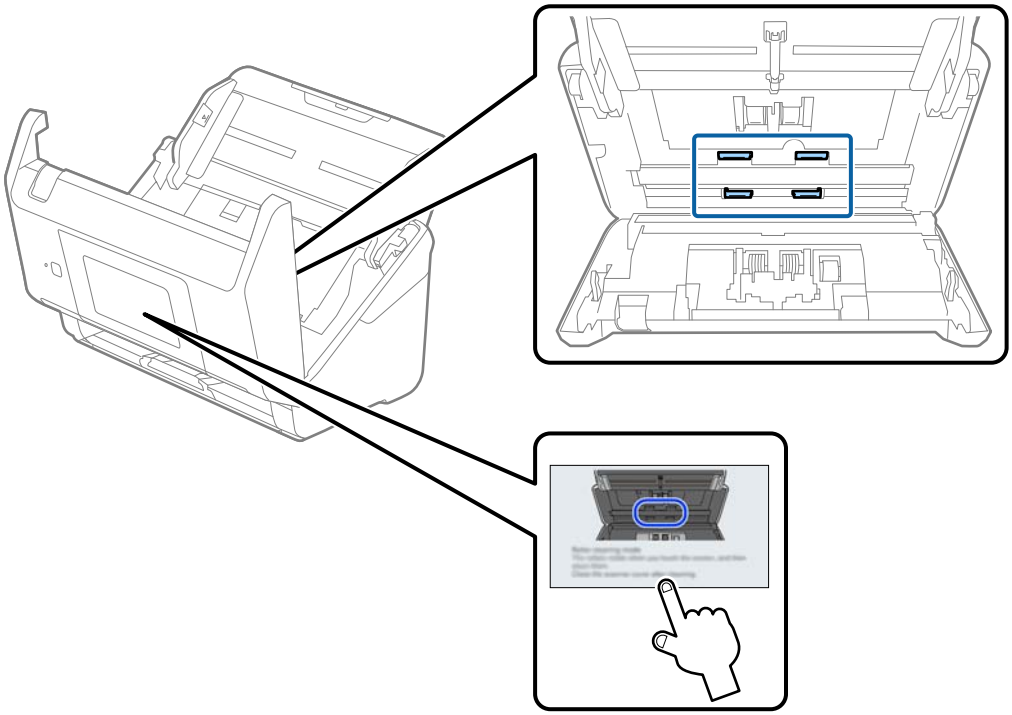
12. Виберіть **Обслуговув. та ремонт сканера** з головного екрану.

13. На екрані **Обслуговув. та ремонт сканера**, виберіть **Чистка роликів**.

14. Потягніть важіль, щоб відкрити кришку сканера.

    Сканер увійде в режим очищення.

15. Повільно обертайте ролики в нижній частині, натиснувши в будь-якому місці на РК-екрані. Протріть поверхню роликів використовуючи оригінальний набір для чищення Epson або м'якою тканиною, змоченою у воді. Повторіть це, поки ролики не стануть чистими.



> ***Застереження.***
>
> *Будьте обережні, щоб пальці або волосся не потрапили у механізм під час обертання роликів. Це може призвести до травми.*

16. Закрийте кришку сканера.

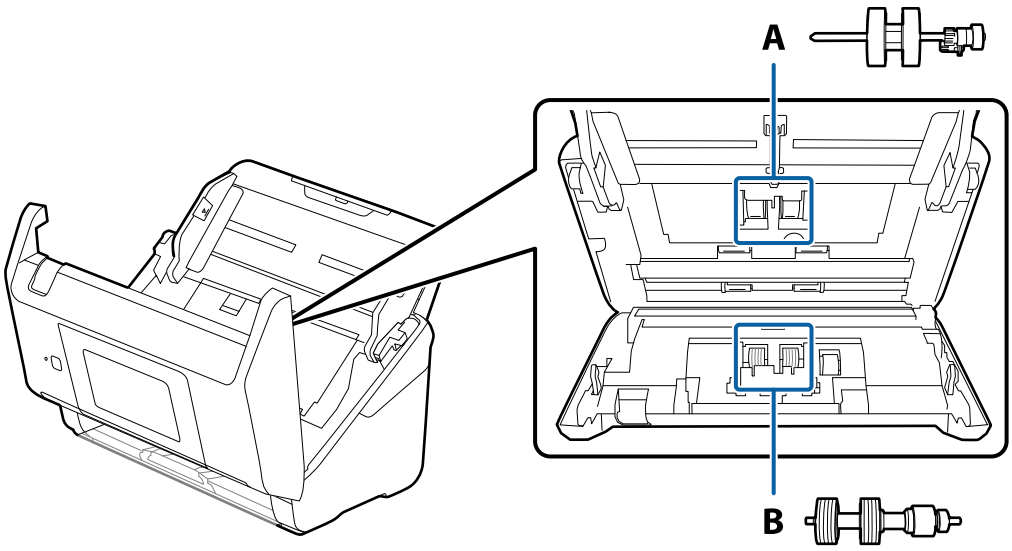
    Сканер вийде з режиму очищення.

Пов'язані відомості

➡ «Заміна вузла подачі паперу» на сторінці 167

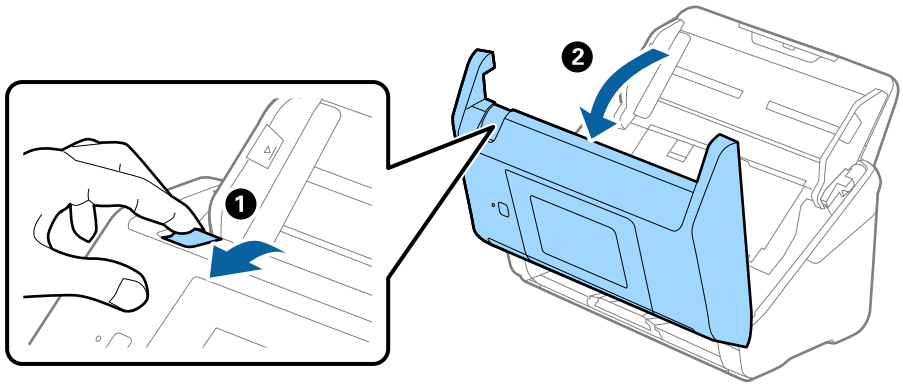
Заміна вузла подачі паперу

Вузол подачі (ролик захоплення і ролик розділення аркушів паперу) потребує заміни, коли кількість сканувань перевищує ресурс роликів. Коли на панелі керування або комп'ютері з'являється повідомлення про потребу заміни, дотримуйтеся вказівок нижче, щоб зробити її.

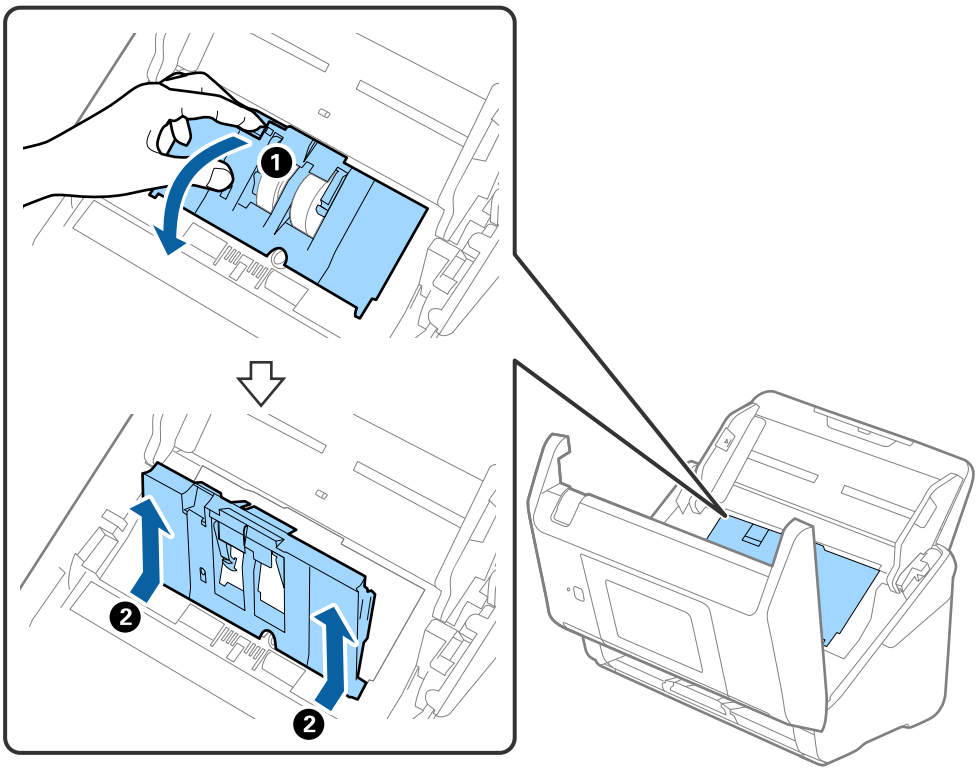


A: ролик захоплення, B: ролик розділення аркушів паперу

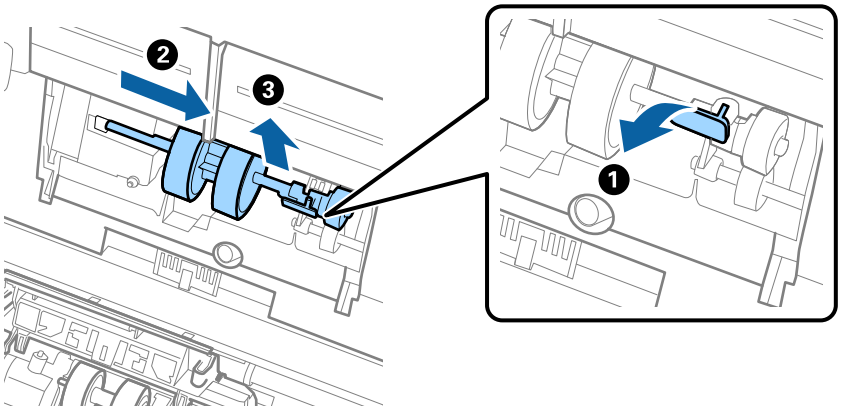
1. Натисніть на сканері кнопку ⏻, щоб вимкнути його.
2. Відключіть адаптер змінного струму від сканера.
3. Потягніть важіль і відкрийте кришку сканера.



4. Відкрийте кришку ролика подачі, а тоді зсуньте і витягніть його.

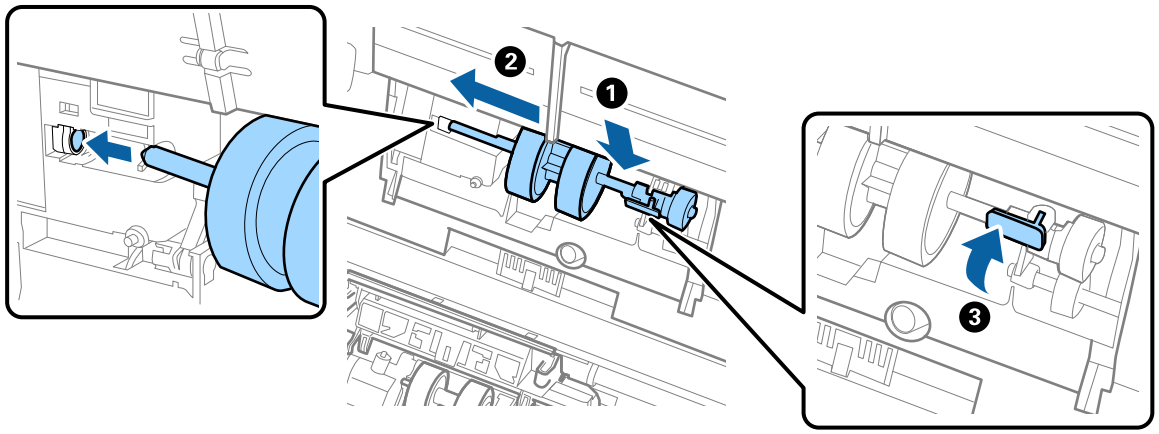


5. Опустіть фіксатор вісі ролика, а тоді зсуньте і витягніть встановлені ролики подачі.

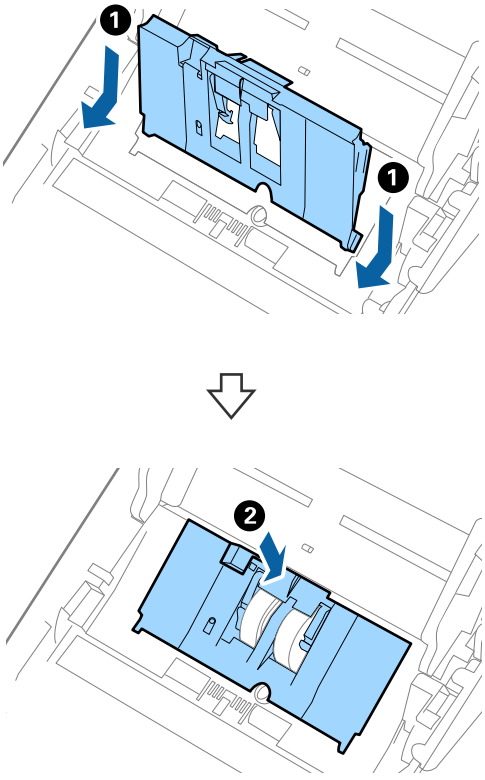


> ***Важливо***
>
> *Не намагайтеся витягнути ролик подачі силою. Це може пошкодити внутрішню частину сканера.*

6. Утримуючи фіксатор у положенні донизу, зсуньте новий ролик подачі вліво та вставте його в отвір в сканері. Притисніть фіксатор, щоб закріпити його.

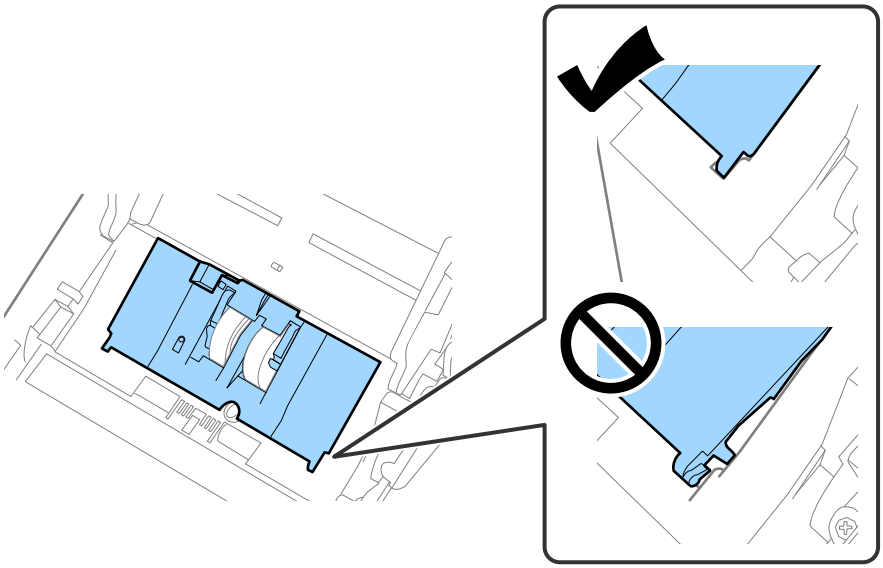


7. Поставте край кришки ролика подачі у паз та зсуньте її. Міцно закрийте кришку.

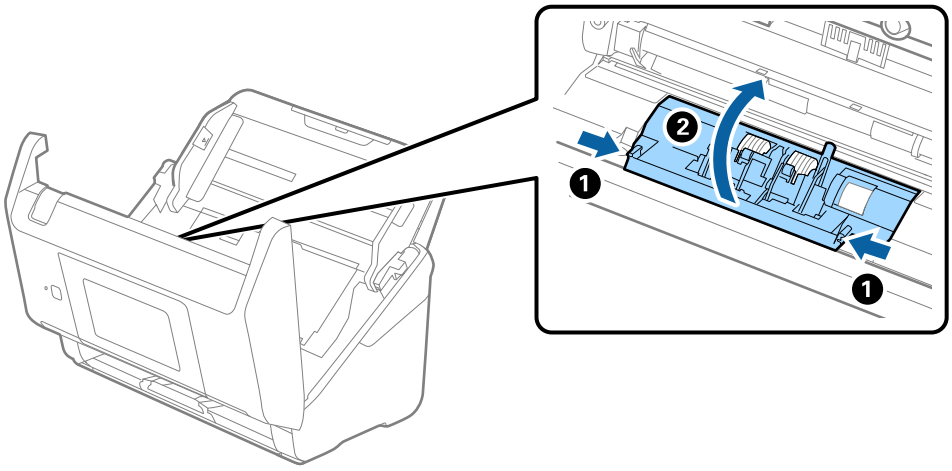


Важливо

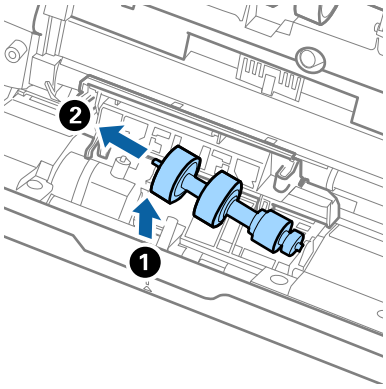
- ❏ *Перевірте, чи правильно закрита кришка.*
- ❏ *Якщо кришка важко закривається, перевірте, чи правильно встановлені ролики захоплення паперу.*
- ❏ *Не вставляйте кришку, доки вона піднята.*



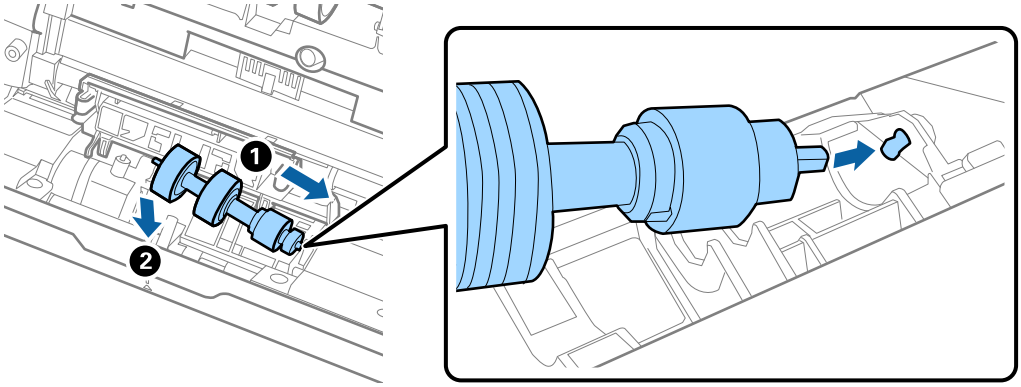
8. Притисніть гачки з обох боків кришки ролика подачі, щоб відкрити її.



9. Підніміть ліву сторону ролика розділення, а тоді зсуньте і витягніть встановлені ролики розділення.



10. Вставте вісь нового ролика розділення в отвір праворуч, а тоді опустіть ролик.



11. Закрийте кришку ролика розділення.

> ***Важливо***
>
> *Якщо кришка важко закривається, перевірте, чи правильно встановлені ролики розділення.*

12. Закрийте кришку сканера.

13. Вставте в розетку адаптер змінного струму та ввімкніть сканер.

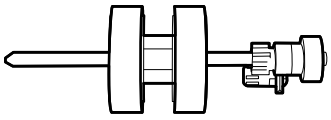
14. Скиньте номер сканування на панелі керування.

Примітка.
Утилізуйте ролики подачі і розділення відповідно до правил та норм у вашому законодавстві. Не розбирайте їх.

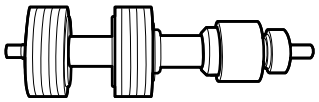
Коди вузла ролика подачі паперу

Частини (ролик захоплення та ролик розділення аркушів паперу) повинні бути замінені, коли кількість сканувань перевищить допустимий ресурс. Кількість сканувань можна побачити на панелі керування або в службовій програмі Epson Scan 2.

A



B



A: ролик захоплення, B: ролик розділення аркушів паперу

Назва частини	Коди	Ресурс
Ролики подачі паперу	B12B819671 B12B819681 (тільки для Індії)	200,000*

* Ця кількість була визначена послідовним скануванням за допомогою оригінального паперу Epson і є рекомендованою для циклу заміни. Цикл заміни може відрізнятися в залежності від різних типів паперу, таких як папір, що створює багато пилу або папір з жорсткою поверхнею, що може скоротити ресурс обладнання.

Скидання кількості сканувань

Скиньте кількість сканувань після заміни вузла подачі паперу.

1. Виберіть на головному екрані **Налаш.** > **Інформація про пристрій** > **Скинути кількість сканувань** > **К-сть скан. після заміни**.

2. Торкніться **Так**.

Пов'язані відомості

➡ «Заміна вузла подачі паперу» на сторінці 167

Енергоощадність

Можна заощаджувати енергію за допомогою режиму сну або режиму автоматичного вимкнення живлення, коли сканер не здійснює жодних операцій. Можна налаштувати час, після якого сканер переходить у режим сну й автоматично вимикається. Збільшення призводить до підвищення енергоспоживання. Перш ніж вносити будь-які зміни, подумайте про довкілля.

1. Виберіть **Налаш.** на головному екрані.

2. Виберіть **Основні налашт.**.

3. Натисніть **Налашт. вимк. живл** та виконайте налаштування.

   Примітка.
   Доступні функції залежать від місця придбання виробу.

Транспортування сканера

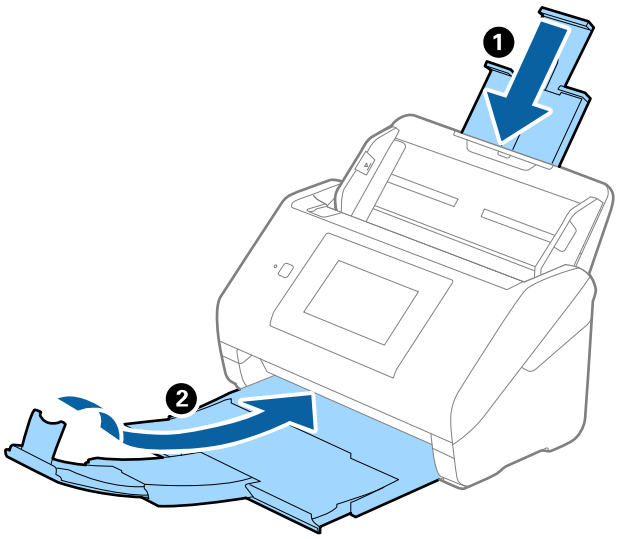
Якщо сканер потрібно перевезти, наприклад, для ремонту, дотримуйтеся вказівок нижче, щоб упакувати його.

1. Натисніть на сканері кнопку ⏻, щоб вимкнути його.

2. Від'єднайте адаптер змінного струму.

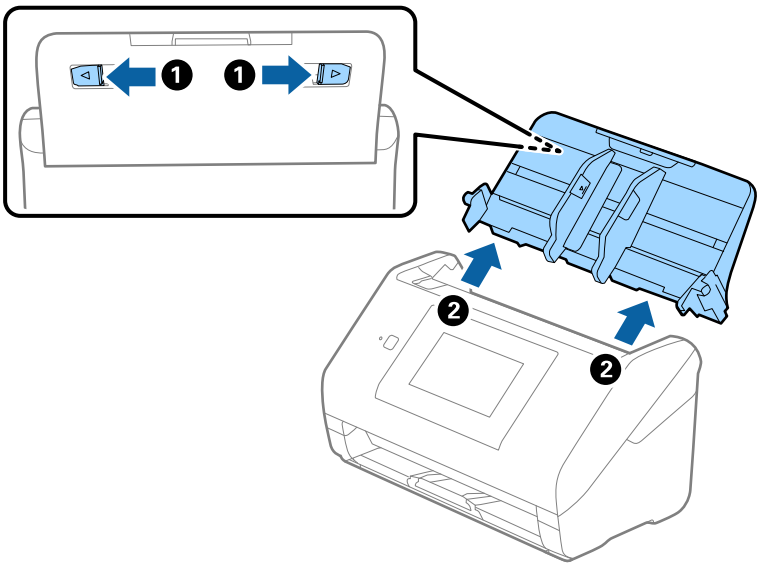
3. Видаліть кабелі і пристрої.

4. Закрийте розширення вхідного лотка і вихідний лоток.



> ***Важливо***
>
> *Перевірте, чи надійно закритий вихідний лоток; інакше його можна пошкодити під час транспортування.*

5. Вийміть вхідний лоток.



6. Загорніть сканер у пакувальні матеріали, з якими він продавався, а тоді запакуйте сканер в оригінальну або іншу міцну коробку.

Резервне копіювання налаштувань

Можна експортувати значення налаштування, встановлене з Web Config до файлу. Його можна використати для резервного копіювання контактів, значень налаштувань, заміни сканера і т.д.

Експортований файл не можна редагувати, оскільки він експортований як бінарний файл.

Експортування налаштувань

Експортуйте налаштування для сканера.

1. Відкрийте Web Config, а тоді виберіть вкладку **Керування пристроєм** > **Експортувати та імпортувати значення налаштування** > **Експорт**.

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. Клацніть **Експорт**.

> ***Важливо***
>
> *Якщо потрібно експортувати мережеві налаштування сканера, наприклад ім'я пристрою та адресу IPv6, виберіть **Увімкніть вибір індивідуальних налаштувань пристрою** та виберіть інші елементи. Використовуйте тільки вибрані значення для змінного сканера.*

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Імпортування налаштувань

Імпортуйте експортований файл Web Config на сканер.

> ***Важливо***
>
> *При імпортуванні значень, що включають окремі відомості, як-от ім'я сканера або IP-адресу, переконайтеся, що в цій мережі немає такої самої IP-адреси.*

1. Відкрийте Web Config, після чого виберіть вкладку **Керування пристроєм** > **Експортувати та імпортувати значення налаштування** > **Імпорт**.
2. Виберіть експортований файл, після чого введіть зашифрований пароль.
3. Клацніть **Далі**.
4. Виберіть налаштування, який потрібно імпортувати, після чого клацніть **Далі**.
5. Клацніть **OK**.

Налаштування застосовуються до сканера.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Віднов. налашт. за зам.

На панелі керування виберіть **Налаш.** > **Сист. адміністрування** > **Віднов. налашт. за зам.**, а потім виберіть елементи, для яких потрібно відновити значення за замовчуванням.

- ❏ Налаштування мережі: відновлення налаштувань мережі, до їх первісного стану.
- ❏ Всі, за винятком Налаштувань Мережі: відновлення інших налаштувань до їх первісного стану, окрім налаштувань, пов'язаних з мережею.
- ❏ Всі налаштування: відновлення всіх налаштувань в їх початковий стан при покупці.

Важливо

*Якщо вибрати і запустити **Всі налаштування**, усі дані налаштувань, зареєстровані для сканера, зокрема контакти та налаштування автентифікації користувача, буде видалено. Видалені налаштування відновити не можна.*

Оновлення програм і мікропрограми

Оновивши програми та мікропрограму, ви можете вирішити певні проблеми та покращити чи додати функції. Перевірте, чи ви використовуєте найновіше програмне забезпечення та мікропрограми.

Важливо

❏ *Не вимикайте сканер або комп'ютер під час оновлення.*

Примітка.
*Якщо сканер підключено до інтернету, його мікропрограму можна оновити за допомогою Web Config. Виберіть вкладку **Керування пристроєм** > **Оновлення мікропрограми**, перевірте відображене повідомлення, після чого клацніть **Пуск**.*

1. Перевірте, чи підключено сканер до комп'ютера, та чи підключено комп'ютер до інтернету.

2. Запустіть програму EPSON Software Updater та оновіть програмне забезпечення або мікропрограму.

   Примітка.
   Операційна система Windows Server не підтримується.

   ❏ Windows 10

   Натисніть кнопку «Пуск», а тоді виберіть **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Введіть назву програми в пошуковий рядок і виберіть відображену піктограму.

   ❏ Windows 7

   Натисніть кнопку «Пуск», а тоді виберіть **Усі програми** або **Програми** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Виберіть **Система пошуку** > **Перейти** > **Програми** > **Epson Software** > **EPSON Software Updater**.

Примітка.
Якщо ви не можете знайти в списку застосунок, який потрібно оновити, ви не зможете оновити його, використовуючи EPSON Software Updater. Перевірте останні версії програм на локальному веб-сайті Epson.

http://www.epson.com

Оновлення мікропрограми сканера з панелі керування

Якщо сканер може бути підключено до мережі Інтернет, ви можете оновити його мікропрограму з панелі керування. Ви можете також налаштувати сканер на систематичну перевірку наявності оновлень і сповіщення, якщо такі оновлення стануть доступні.

1. Виберіть **Налаш.** на головному екрані.

2. Виберіть **Сист. адміністрування** > **Оновлення мікропрограмного забезпечення** > **Оновити**.

   Примітка.
   *Виберіть **Повідомлення** > **Увімк**, щоб налаштувати сканер на систематичну перевірку оновлень для мікропрограм.*

3. Перегляньте повідомлення на екрані та почніть пошук доступних оновлень.

4. Якщо повідомлення відобразиться на РК-екрані і міститиме інформацію про доступне оновлення мікропрограми, дотримуйтеся вказівок на екрані, щоб запустити оновлення.

   Важливо

   - *Не вимикайте і не витягуйте з розетки штепсель сканера, доки не завершиться оновлення. Інакше сканер може вийти з ладу.*
   - *Якщо оновлення мікропрограм не завершилося або відбулося невдало, сканер не запуститься у звичному режимі, а на РК-екрані при наступному увімкненні сканера з'явиться повідомлення «Recovery Mode». У такому разі доведеться оновлювати програму ще раз за допомогою комп'ютера. Підключіть сканер до комп'ютера за допомогою кабелю USB. Доки на сканері відображається «Recovery Mode», ви не зможете оновити мікропрограму через мережу. Відкрийте на комп'ютері відкрийте веб-сайт Epson для вашого регіону, а тоді завантажте останню версію мікропрограми сканера. Див. подальші вказівки на веб-сайті.*

Оновлення мікропрограми за допомогою Web Config

Якщо сканер підключено до інтернету, його мікропрограму можна оновити за допомогою Web Config.

1. Відкрийте Web Config і виберіть вкладку **Керування пристроєм** > **Оновлення мікропрограми**.

2. Клацніть **Пуск**, а тоді виконайте вказівки на екрані.

   Запуститься підтвердження мікропрограми, а тоді з'явиться інформація про те, чи вже існує оновлення мікропрограми.

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 багатьох пристроїв. Докладнішу інформацію див. у посібнику Epson Device Admin.

Пов'язані відомості

➡ «Запуск конфігурації мережі у веб-браузері» на сторінці 37

Оновлення мікропрограми без підключення до Інтернету

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.

Примітка.
Перед оновленням переконайтеся, що на комп'ютері встановлено драйвер сканера Epson Scan 2. Якщо Epson Scan 2 не встановлено, установіть її знову.

1. Про випуск оновлень мікропрограмного забезпечення можна дізнаватись на веб-сайті Epson.

   http://www.epson.com

   ❏ Якщо для вашого сканера є мікропрограма, завантажте її та переходьте до наступного кроку.

   ❏ Якщо на веб-сайті немає інформації про мікропрограмне забезпечення, це значить, що ви використовуєте найновіше.

2. Підключіть комп'ютер, на який завантажено мікропрограму, до сканера за допомогою кабелю USB.

3. Двічі клацніть завантажений файл .exe.

   Запуститься Epson Firmware Updater.

4. Виконайте вказівки на екрані.