EPSON

DS-900WN DS-800WN

راهنمای سرپرست

NPD7398-00 FA

حق نسخه‌برداری

علایم تجاری

- Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- Chrome, Chromebook and Android are trademarks of Google LLC.
- Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- اطلاعیه عمومی: همه علائم تجاری دیگر متعلق به مالکان مربوطه هستند و فقط برای اهداف شناسایی استفاده می‌شوند.

محتوا

تنظیمات امنیتی پیشرفته

استفاده از *Epson Open Platform*

نصب یک دستگاه احراز هویت

نگهداری

مقدمه

محتویات این سند

این سند اطلاعات زیر را برای سرپرستان اسکنر فراهم می‌آورد.

❏ تنظیمات شبکه

❏ آماده‌سازی عملکرد اسکن

❏ فعال‌سازی و مدیریت تنظیمات امنیتی

❏ اجرای سرویس و نگهداری روزانه

جهت اطلاع از روش‌های استاندارد استفاده از اسکنر، بخش راهنماي کاربر را ملاحظه کنید.

استفاده از این راهنما

علائم و نشان ها

> **!احتیاط:**
> دستورالعمل هایی که باید با دقت دنبال شود تا از آسیب بدنی جلوگیری شود.

> **مهم:**
> دستورالعمل هایی که باید مورد توجه قرار گیرد تا از آسیب به تجهیزات جلوگیری شود.

نکته:
اطلاعات تکمیلی و مرجع ارائه می دهد.

اطلاعات مرتبط
به بخش های مربوطه پیوند می دهد.

توضیحات مورد استفاده در این دفترچه راهنما

❏ تصاویر صفحه نمایش مربوط به برنامه‌ها از Windows 10 یا macOS High Sierra گرفته شده‌اند. محتوای نمایش داده شده بر روی صفحه نمایش بسته به مدل و موقعیت متفاوت است.

❏ تصاویر مورد استفاده در این دفترچه راهنما تنها به‌عنوان نمونه است. اگرچه ممکن است این موارد اندکی با محصول واقعی تفاوت داشته باشند، اما شیوه کار آنها یکسان است.

مراجع سیستم عامل

Windows

در این دفترچه راهنما، عباراتی نظیر "Windows 11", "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Server 2022", "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2", و "Windows Server 2008" به این سیستم عامل ها اشاره دارند. به علاوه "Windows" برای ارجاع به تمامی نسخه‌ها استفاده شده است.

- ❑ سیستم عامل Microsoft® Windows® 11
- ❑ سیستم عامل Microsoft® Windows® 10
- ❑ سیستم عامل Microsoft® Windows® 8.1
- ❑ سیستم عامل Microsoft® Windows® 8
- ❑ سیستم عامل Microsoft® Windows® 7
- ❑ سیستم عامل Microsoft® Windows Server® 2022
- ❑ سیستم عامل Microsoft® Windows Server® 2019
- ❑ سیستم عامل Microsoft® Windows Server® 2016
- ❑ سیستم عامل Microsoft® Windows Server® 2012 R2
- ❑ سیستم عامل Microsoft® Windows Server® 2012
- ❑ سیستم عامل Microsoft® Windows Server® 2008 R2
- ❑ سیستم عامل Microsoft® Windows Server® 2008

Mac OS

در این دفترچه راهنما، از "Mac OS" برای اشاره به Mac OS X 10.9 یا جدیدتر و همچنین macOS 11 یا نسخه جدیدتر استفاده می‌شود.

نکاتی در مورد رمز عبور سرپرست

نکاتی در مورد رمز عبور سرپرست

این دستگاه به شما امکان می‌دهد رمز عبور سرپرست را تنظیم کنید تا از دسترسی اشخاص ثالث غیرمجاز یا تغییر تنظیمات دستگاه یا تنظیمات شبکه ذخیره‌شده در دستگاه هنگام اتصال آن به شبکه جلوگیری کنید.

اگر رمز عبور سرپرست را تنظیم کنید، هنگام تغییر تنظیمات در نرم‌افزارهای پیکربندی مانند Web Config باید رمز عبور را وارد کنید.

رمز عبور سرپرست اولیه روی اسکنر تنظیم شده است، اما می‌توانید آن را به هر رمز عبوری تغییر دهید.

رمز عبور سرپرست اولیه

رمز عبور سرپرست اولیه بسته به برچسب چسبانده‌شده به محصول متفاوت است. اگر برچسب «PASSWORD» به پشت چسبانده شده است، عدد 8 رقمی درج‌شده روی برچسب را وارد کنید. اگر برچسب «PASSWORD» چسبانده نشده است، شماره سریال روی برچسب چسبانده‌شده به پشت محصول را برای رمز عبور سرپرست اولیه وارد کنید.

توصیه می‌کنیم رمز عبور اولیه سرپرست را از تنظیمات پیش‌فرض تغییر دهید.

نکته:
هیچ نام کاربری به‌عنوان پیش‌فرض تنظیم نشده است.

عملیاتی که به رمز عبور سرپرست نیاز دارند

اگر در طی عملیات زیر در پیام‌واره‌ای از شما خواسته شد رمز عبور سرپرست را وارد کنید، رمز عبور سرپرست تنظیم‌شده روی محصول را وارد کنید.

- ❑ هنگام ورود به تنظیمات پیشرفته Web Config
- ❑ هنگام کار کردن با منویی در پانل کنترل که سرپرست قفل کرده است
- ❑ هنگام تغییر تنظیمات دستگاه در برنامه
- ❑ هنگام به‌روزرسانی ثابت‌افزار دستگاه
- ❑ هنگام تغییر دادن یا بازنشانی رمز عبور سرپرست

تغییر رمز عبور سرپرست

می‌توانید از پانل کنترل محصول یا در Web Config تغییر دهید.

هنگام تغییر رمز عبور، رمز عبور جدید باید 8 تا 20 نویسه داشته باشد و فقط شامل نویسه‌ها و نمادهای الفبایی-عددی تک‌بایتی باشد.

بازنشانی رمز عبور سرپرست

می‌توانید رمز عبور سرپرست را از پانل کنترل محصول یا در Web Config به تنظیمات اولیه بازنشانی کنید.

اگر رمز عبور را فراموش کرده‌اید و نمی‌توانید آن را به تنظیمات پیش‌فرض بازنشانی کنید، محصول باید تعمیر شود. با فروشنده محلی تماس بگیرید.

تنظیمات مورد نیاز برای مطابقت با نیازهای شما

تنظیمات موردنیاز برای مطابقت با نیازهای شما

برای اعمال تنظیمات لازم جهت مطابقت با نیازهای خود بخش زیر را ببینید.

اتصال اسکنر به شبکه

هدف	تنظیمات لازم
من می‌خواهم اسکنر را به شبکه وصل کنم.	اسکنر خود را برای اسکن شبکه‌ای تنظیم کنید. "اتصال اسکنر به شبکه" در صفحه 15
من می‌خواهم اسکنر را به یک کامپیوتر جدید وصل کنم.	تنظیمات شبکه برای اسکنر خود را در کامپیوتر جدید تنظیم کنید. "افزودن یا تعویض رایانه یا دستگاه‌ها" در صفحه 21

تنظیمات برای اسکن‌کردن

هدف	تنظیمات لازم
من می‌خواهم تصاویر اسکن‌شده را با ایمیل ارسال کنم. (Scan to Email)	1. سرور ایمیل موردنظر برای پیونددادن را تنظیم کنید. "ثبت دوباره یک سرور ایمیل" در صفحه 43 2. آدرس ایمیل گیرنده را در قسمت **Contacts** ثبت کنید (اختیاری). با ثبت‌کردن آدرس ایمیل، نیاز نخواهید داشت هر بار که قصد ارسال چیزی را دارید آن را مجدداً وارد نمایید، کافی است در دفعات بعد آن را از مخاطبین خود انتخاب نمایید. "در دسترس قرار دادن مخاطبین" در صفحه 53
من می‌خواهم تصاویر اسکن‌شده را در یک پوشه در شبکه ذخیره کنم. (Scan to Network Folder/FTP)	1. یک پوشه در شبکه و محل موردنظر خود برای ذخیره تصاویر ایجاد کنید. "ایجاد یک پوشه اشتراک‌گذاری" در صفحه 45 2. مسیر پوشه را در قسمت **Contacts** ثبت کنید (اختیاری). با ثبت‌کردن مسیر پوشه، نیاز نخواهید داشت هر بار که قصد ارسال چیزی را دارید آن را مجدداً وارد نمایید، کافی است در دفعات بعد آن را از مخاطبین خود انتخاب نمایید. "در دسترس قرار دادن مخاطبین" در صفحه 53
من می‌خواهم تصاویر اسکن شده را در یک سرویس ابری ذخیره کنم. (Scan to Cloud)	Epson Connect را راه‌اندازی کنید. برای اطلاعات بیشتر درباره راه‌اندازی، به وب‌سایت پورتال Epson Connect مراجعه کنید. هنگام راه‌اندازی، به یک حساب کاربری برای سرویس حافظه ذخیره‌سازی آنلاین موردنظر برای پیونددادن نیاز دارید. https://www.epsonconnect.com/ http://www.epsonconnect.eu (فقط اروپا)

سفارشی کردن نمایشگر پنل کنترل

هدف	تنظیمات لازم
من می‌خواهم موارد نمایش یافته در پنل کنترل اسکنر را تغییر بدهم.	گزینه‌های **پیش‌تنظیمات** یا **ویرایش صفحه اصلی** را تنظیم کنید. تنظیمات اسکن دلخواه خود را می توانید در پنل کنترل ثبت کنید یا موارد نمایش یافته را ویرایش کنید. "سفارشی کردن نمایشگر پانل کنترل" در صفحه 66

تنظیم عملکردهای امنیتی پایه

هدف	تنظیمات لازم
من می‌خواهم کسی غیر از سرپرست نتواند تنظیمات اسکنر را تغییر دهد.	یک رمز عبور سرپرست برای اسکنر تنظیم کنید. "تنظیمات سرپرست سیستم" در صفحه 74
من می‌خواهم استفاده از اسکنرها از طریق اتصال USB را غیرفعال کنم.	رابط خارجی را غیرفعال کنید. "غیرفعال کردن رابط خارجی" در صفحه 82

تنظیم عملکردهای امنیتی پیشرفته

هدف	تنظیمات لازم
من می‌خواهم پروتکل‌های مورداستفاده را کنترل کنم.	پروتکل‌ها را فعال یا غیرفعال کنید. "کنترل کردن با پروتکل‌ها" در صفحه 89
من می‌خواهم مسیر ارتباطات را رمزنگاری کنم.	1. گواهی دیجیتال خود را راه‌اندازی کنید. "استفاده از گواهی دیجیتالی" در صفحه 91 2. ارتباط SSL/TLS را راه‌اندازی کنید. "ارتباط SSL/TLS با اسکنر" در صفحه 97
من می‌خواهم از ارتباطات رمزنگاری شده (IPsec) استفاده کنم. من می‌خواهم از نرم‌افزار تنها از طریق یک کامپیوتر خاص (فیلترگذاری IP) استفاده شود.	سیاست‌های فیلترکردن ترافیک را راه‌اندازی کنید. "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 98
من می‌خواهم از اسکنر در یک شبکه IEEE802.1X استفاده کنم.	شبکه IEEE802.1X را برای اسکنر راه‌اندازی کنید. "اتصال اسکنر به شبکه IEEE802.1X" در صفحه 109

همگام‌سازی اسکنر با یک سیستم احراز هویت

یک کلید محصول را از وب‌سایت اختصاصی دریافت کنید و Epson Open Platform را در اسکنر خود فعال کنید.

"استفاده از Epson Open Platform" در صفحه 117

استفاده از گزینه تأیید هویت Epson Print Admin/Epson Print Admin Serverless))

برای استفاده از این گزینه به یک کلید مجوز نیاز دارید.

برای کسب اطلاعات بیشتر، با فروشنده خود تماس بگیرید.

نکته:

هنگامی که سیستم با *Epson Open Platform* همگام است، نمی‌توانید از *Epson Print Admin Serverless* استفاده کنید.

تنظیمات شبکه

اتصال اسکنر به شبکه

این بخش شیوه متصل‌کردن اسکنر به شبکه را از طریق پنل کنترل اسکنر شرح می دهد.

نکته:
اگر اسکنر و کامپیوتر شما در یک دسته هستند، با استفاده از نصب‌کننده نیز می‌توانید وصل کنید.

برای راه‌اندازی نصب‌کننده، به وب‌سایت زیر بروید و سپس نام محصول را وارد کنید. به منوی **تنظیم** بروید و راه‌اندازی را شروع کنید.

https://epson.sn

دستورالعمل‌های استفاده را می‌توانید در دفترچه راهنمای فیلم وب ببینید. به *URL* پایین بروید.

https://support.epson.net/publist/vlink.php?code=NPD7509

قبل از برقراری اتصال شبکه

به منظور اتصال به شبکه، روش اتصال و تنظیم اطلاعات برای اتصال را از قبل تنظیم کنید.

جمع آوری اطلاعات درباره تنظیم اتصال

اطلاعات تنظیم ضروری برای اتصال را آماده کنید. اطلاعات زیر را از قبل بررسی کنید.

بخش ها	موارد	توجه
روش اتصال دستگاه	❑ اترنت ❑ Wi-Fi	روش اتصال اسکنر به شبکه را تعیین کنید. در رابطه با LAN سیمی به سوییچ LAN متصل می شود. در رابطه با Wi-Fi به شبکه (SSID) نقطه دسترسی متصل می شود.
اطلاعات اتصال LAN	❑ آدرس IP ❑ ماسک شبکه فرعی ❑ دروازه پیش فرض	آدرس IP موردنظر برای تخصیص به اسکنر را انتخاب کنید. وقتی آدرس IP ثابت تخصیص می دهید، وارد کردن همه مقادیر الزامی می باشد. وقتی آدرس IP پویا با استفاده از عملکرد DHCP تخصیص می دهید، لازم نیست این اطلاعات را وارد کنید زیرا به طور خودکار تنظیم می شوند.
اطلاعات اتصال Wi-Fi	❑ SSID ❑ رمزعبور	این موارد SSID (نام شبکه) و رمز عبور نقطه دسترسی هستند که اسکنر به آنها متصل می شود. اگر ویژگی فیلتر کردن آدرس MAC تنظیم شده است، آدرس MAC اسکنر را قبل از ثبت کردن اسکنر، ثبت نمایید. برای اطلاع از استانداردهای تحت پشتیبانی موارد زیر را ملاحظه کنید. "مشخصات شبکه" در صفحه 28
اطلاعات سرور DNS	❑ آدرس IP مربوط به DNS اولیه ❑ آدرس IP مربوط به DNS ثانویه	این موارد هنگام تعیین سرورهای DNS موردنیاز هستند. DNS ثانویه زمانی تنظیم می شود که سیستم از پیکربندی اضافی برخوردار است و یک سرور DNS ثانویه وجود دارد. اگر جزء یک سازمان کوچک هستید و سرور DNS را تنظیم نکرده اید، آدرس IP را برای روتر تنظیم کنید.

بخش ها	موارد	توجه
اطلاعات سرور پروکسی	❑ نام سرور پروکسی	این گزینه را زمانی تنظیم کنید که محیط شبکه شما از سرور پروکسی برای دسترسی به اینترنت از طریق اینترانت استفاده می کند و شما عملکردی که دسترسی مستقیم اسکنر به اینترنت را فراهم می کند را استفاده می کنید. در رابطه با عملکردهای زیر، اسکنر مستقیما به اینترنت متصل می شود. ❑ خدمات Epson Connect ❑ خدمات ابری مربوط به سایر شرکت ها ❑ بروزرسانی ثابت افزار ❑ ارسال تصاویر اسکن شده به SharePoint(WebDAV)
اطلاعات شماره درگاه	❑ شماره درگاه موردنظر برای باز کردن	شماره درگاه مورد استفاده اسکنر و رایانه را بررسی کنید و سپس درگاهی که توسط فایروال مسدود شده است را در صورت نیاز باز کنید. برای مشاهده شماره درگاه مورد استفاده اسکنر، بخش زیر را مشاهده کنید. "استفاده از درگاه برای اسکنر" در صفحه 30

تخصیص آدرس IP

حالات مختلف تخصیص آدرس IP شامل موارد زیر می‌باشند.

آدرس IP ثابت:

آدرس IP اختصاصی از پیش تعیین شده را به صورت دستی به اسکنر (میزبان) اختصاص دهید.

اطلاعات لازم برای اتصال به شبکه (ماسک شبکه فرعی، دروازه پیش‌فرض، سرور DNS و موارد مشابه) به صورت دستی تنظیم می‌شوند.

آدرس IP حتی وقتی دستگاه خاموش شود تغییر نمی‌کند، در نتیجه این تنظیم وقتی مفید است که در نظر دارید دستگاه‌ها را در محیطی تنظیم کنید که امکان تغییر آدرس IP را نخواهید داشت یا در نظر دارید دستگاه‌ها را از طریق آدرس IP مدیریت نمایید. توصیه می‌کنیم تنظیماتی برای اسکنر انتخاب کنید که بسیاری از رایانه‌ها بتوانند به آن دسترسی داشته باشند. همچنین، هنگام استفاده از قابلیت‌های امنیتی مانند فیلترگذاری IPsec/IP، یک آدرس IP ثابت تخصیص دهید تا از تغییر آن جلوگیری کنید.

تخصیص خودکار با استفاده از عملکرد DHCP (آدرس IP پویا):

با استفاده از عملکرد DHCP مربوط به سرور DHCP یا روتر، به طور خودکار یک آدرس IP به اسکنر (میزبان) تخصیص دهید.

اطلاعات لازم برای اتصال به شبکه (ماسک شبکه فرعی، دروازه پیش‌فرض، سرور DNS و موارد مشابه) به صورت خودکار تنظیم می‌شوند، در نتیجه به راحتی قادر خواهید بود دستگاه را به شبکه وصل کنید.

اگر دستگاه یا روتر خاموش شود یا بستگی به تنظیمات سرور DHCP ممکن است آدرس IP در زمان اتصال مجدد تغییر یابد.

توصیه می‌کنیم از روش‌هایی غیر از آدرس IP برای مدیریت دستگاه‌ها استفاده کنید و با پروتکل‌هایی ارتباط برقرار کنید که قادر به دنبال کردن آدرس IP می‌باشند.

نکته:
وقتی از عملکرد رزرو آدرس *IP* قابلیت *DHCP* استفاده کنید، قادر خواهید بود آدرس *IP* یکسانی را در هر زمان به دستگاه‌ها تخصیص دهید.

سرور DNS و سرور پروکسی

سرور DNS دارای یک نام میزبان، نام دامنه آدرس ایمیل و موارد دیگر در ارتباط با اطلاعات آدرس IP است.

اگر طرف دیگر ارتباط با نام میزبان، نام دامنه و غیره ثبت شده باشد، هنگامی که رایانه یا اسکنر برای برقراری ارتباط از طریق IP تلاش می کند، ارتباط برقرار نخواهد شد.

سرور DNS را برای یافتن آن اطلاعات جستجو می کند و آدرس IP طرف مقابل را دریافت می کند. این فرآیند تحت عنوان «ترجمه نام» (name resolution) شناخته می شود.

بنابراین، دستگاه هایی مانند رایانه ها و اسکنرها امکان برقراری ارتباط از طریق آدرس IP را کسب خواهند کرد.

وضوح نام برای ارتباط اسکنر با استفاده از عملکرد ایمیل یا عملکرد اتصال به اینترنت ضروری است.

وقتی این عملکردها را استفاده می کنید، تنظیمات سرور DNS را اعمال کنید.

وقتی آدرس IP اسکنر را با استفاده از عملکرد DHCP سرور DHCP یا روتر اختصاص می دهید، به طور خودکار تنظیم خواهد شد.

سرور پروکسی در دروازه بین شبکه و اینترنت قرار می گیرد و با رایانه، اسکنر و اینترنت (سرور مخالف) از طرف تک تک آنها ارتباط برقرار می کند. سرور مخالف فقط با سرور پروکسی ارتباط برقرار می کند. از این رو، اطلاعات اسکنر مانند نشانی IP و شماره درگاه خوانده نمی شود و سطح امنیت بالاتر می رود.

هنگامی که از طریق یک سرور پروکسی به اینترنت متصل می شوید، سرور پروکسی را در اسکنر پیکربندی کنید.

اتصال به شبکه از طریق پانل کنترل

اسکنر را از طریق پانل کنترل اسکنر به شبکه متصل کنید.

تخصیص آدرس IP

گزینه های ابتدایی مانند آدرس میزبان، ماسک زیرشبکه، دروازه پیش‌فرض را تنظیم کنید.

این بخش روش تنظیم یک آدرس IP ثابت را توضیح می دهد.

1. اسکنر را روشن کنید.
2. منوی **تنظیم** در صفحه اصلی پانل کنترل اسکنر را انتخاب کنید.
3. **تنظیمات شبکه** > **پیشرفته** > **TCP/IP** را انتخاب کنید.
4. گزینه **دستی** را برای **بدست آوردن آدرس IP** انتخاب کنید.

   اگر آدرس IP را با عملکرد DHCP به طور خودکار تنظیم کرده باشید، باید **خودکار** را انتخاب کنید. در این صورت، **نشانی IP**، **ماسک زیرشبکه**، و **دروازه پیش‌فرض** در مراحل 5 تا 6 نیز به طور خودکار تنظیم می شود و باید به مرحله 7 بروید.
5. آدرس IP را وارد کنید.

   وقتی ◀ یا ▶ را انتخاب کنید، فوکوس صفحه به قسمت جلو یا عقب مجزا شده توسط نقطه جابجا می شود.

   مقدار نشان داده شده در صفحه قبل را تأیید کنید.
6. **ماسک زیرشبکه** و **دروازه پیش‌فرض** را تنظیم کنید.

   مقدار نشان داده شده در صفحه قبل را تأیید کنید.

> **مهم:**
> اگر ترکیب نشانی *IP*، ماسک زیرشبکه و دروازه پیش‌فرض نادرست باشد، **تنظیمات را شروع کنید** غیرفعال و اعمال تنظیمات غیرممکن می شود. مطمئن شوید که در ورود اطلاعات خطایی رخ نداده است.

7. آدرس IP سرور DNS اولیه را وارد کنید.

   مقدار نشان داده شده در صفحه قبل را تأیید کنید.

نکته:
اگر **خودکار** را برای تنظیمات تخصیص *IP* انتخاب کنید، می توانید تنظیمات سرور *DNS* را از **دستی** یا **خودکار** انتخاب کنید. اگر نمی توانید آدرس سرور *DNS* را به طور خودکار دریافت کنید، باید **دستی** را انتخاب و آدرس سرور *DNS* را وارد کنید. سپس، آدرس سرور *DNS* ثانویه را مستقیماً وارد کنید. اگر **خودکار** را انتخاب کرده اید، به مرحله *9* بروید.

8. آدرس IP سرور ثانویه DNS را وارد کنید.
   مقدار نشان داده شده در صفحه قبل را تأیید کنید.
9. روی **تنظیمات را شروع کنید** ضربه بزنید.

تنظیم سرور پروکسی

اگر هر دو شرط زیر برقرار هستند، سرور پروکسی را تنظیم کنید.

- ❑ سرور پروکسی برای اتصال اینترنتی تهیه شده است.
- ❑ هنگام استفاده از عملکردی مانند سرویس Epson Connect یا سرویس های ابری شرکت که مستلزم اتصال مستقیم اسکنر با اینترنت می باشند.

1. **تنظیم** را در صفحه اصلی انتخاب کنید.
   پس از انجام دادن تنظیمات پس از تنظیم کردن آدرس IP، صفحه **پیشرفته** ظاهر می شود. به مرحله 3 بروید.
2. **تنظیمات شبکه** > **پیشرفته** را انتخاب کنید.
3. **پروکسی سرور** را انتخاب کنید.
4. گزینه **Use** را برای **تنظیمات پروکسی سرور** انتخاب کنید.
5. آدرس سرور پروکسی را با قالب IPv4 یا FQDN وارد کنید.
   مقدار نشان داده شده در صفحه قبل را تأیید کنید.
6. شماره درگاه سرور پروکسی را وارد کنید.
   مقدار نشان داده شده در صفحه قبل را تأیید کنید.
7. روی **تنظیمات را شروع کنید** ضربه بزنید.

اتصال به اترنت

اسکنر را با استفاده از کابل LAN به شبکه وصل کنید و سپس اتصال را بررسی کنید.

1. اسکنر و هاب (سوییچ LAN) را با کابل LAN به هم وصل کنید.
2. در صفحه اصلی، گزینه  را انتخاب کنید.
3. گزینه **روتر** را انتخاب کنید.
4. اطمینان حاصل کنید تنظیمات اتصال و نشانی IP صحیح هستند.
5. روی گزینه **بستن** ضربه بزنید.

اتصال به LAN بی سیم (Wi-Fi)

به چندین روش می توانید اسکنر را به LAN بی سیم (Wi-Fi) متصل کنید. روش اتصال سازگار با محیط و شرایط استفاده را انتخاب کنید.

اگر اطلاعات روتر بی سیم مانند SSID و رمز عبور را در اختیار داشته باشید، می توانید تنظیمات را به صورت دستی انجام دهید.

اگر روتر بی سیم از WPS پشتیبانی کند، می توانید تنظیمات را با راه اندازی دکمه فشاری انجام دهید.

پس از وصل کردن اسکنر به شبکه، از دستگاه مورد نظر برای استفاده (رایانه، دستگاه هوشمند، تبلت و غیره) به اسکنر متصل شوید.

هنگام استفاده از اتصال *Wi-Fi 5* گیگاهرتز توجه داشته باشید

این محصول معمولاً هنگام اتصال به Wi-Fi Direct (AP) ساده) از W52 ((36ch به‌عنوان کانال استفاده می‌کند. از آنجایی که کانال اتصال LAN بی‌سیم (Wi-Fi) به‌طور خودکار انتخاب می‌شود، کانال استفاده‌شده ممکن است هنگام استفاده همزمان با اتصال Wi-Fi Direct متفاوت باشد. اگر کانال‌ها متفاوت باشند، ارتباط داده‌ها با اسکنر ممکن است کند باشد. اگر با استفاده تداخلی ایجاد نمی‌کند، به SSID در باند 2.4 گیگاهرتز متصل شوید. در باند فرکانسی 2.4 گیگاهرتز، کانال‌های استفاده شده‌مطابقت دارند.

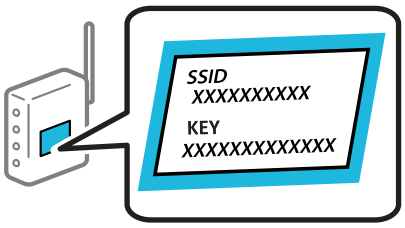
هنگام تنظیم LAN بی‌سیم روی 5 گیگاهرتز، توصیه می‌کنیم Wi-Fi Direct را غیرفعال کنید.

انجام تنظیمات *Wi-Fi* با وارد کردن *SSID* و رمز عبور

با وارد کردن اطلاعات لازم برای اتصال به یک روتر بی سیم از طریق پانل کنترل اسکنر می توانید شبکه Wi-Fi را تنظیم کنید. برای انجام تنظیم به این روش، به SSID و رمز عبور روتر بی سیم نیاز دارید.

نکته:

اگر از روتر بی‌سیم با تنظیمات پیش‌فرض آن استفاده می‌کنید، *SSID* و رمز عبور روی برچسب آن قرار دارند. اگر *SSID* و رمز عبور را نمی‌دانید، با شخصی که روتر بی‌سیم را راه‌اندازی کرده است تماس بگیرید، یا اسناد ارائه‌شده به همراه روتر بی‌سیم را ببینید.



1. در صفحه اصلی، روی  ضربه بزنید.
2. **روتر** را انتخاب کنید.
3. روی **تنظیمات را شروع کنید** ضربه بزنید.

   در صورتی که اتصال شبکه از قبل تنظیم شده است، جزئیات اتصال نمایش داده خواهند شد. برای تغییر تنظیمات، روی **به اتصال Wi-Fi تغییر دهید.** یا **تغییر تنظیمات** ضربه بزنید.
4. **راهنمای گام به گام تنظیم Wi-Fi** را انتخاب کنید.
5. برای انتخاب SSID، واردکردن رمز عبور برای روتر بی‌سیم و شروع راه‌اندازی، دستورالعمل‌های روی صفحه را دنبال کنید.

   اگر در نظر دارید وضعیت اتصال شبکه برای اسکنر را پس از تکمیل راه‌اندازی بررسی کنید، برای اطلاع از جزئیات، به پیوند اطلاعات مرتبط در زیر مراجعه کنید.

نکته:

- اگر *SSID* را نمی دانید، بررسی کنید آیا روی برچسب روتر بی سیم نوشته شده است یا خیر. اگر از روتر بی سیم با تنظیمات پیش فرض آن استفاده می کنید، از *SSID* درج شده روی برچسب استفاده نمایید. اگر هیچ اطلاعاتی پیدا نکردید، به اسناد ارائه شده همراه با روتر بی سیم مراجعه کنید.
- رمز عبور به بزرگ و کوچک بودن حروف حساس است.
- اگر رمز عبور را نمی‌دانید، بررسی کنید که آیا اطلاعات روی برچسب روتر بی‌سیم نوشته شده است یا خیر. ممکن است رمز عبور روی برچسب با عنوان های «*Network Key*» یا «*Wireless Password*» و موارد مشابه مشخص شده باشد. اگر از روتر بی سیم با تنظیمات پیش فرض آن استفاده می کنید، از رمز عبور نوشته شده روی برچسب استفاده نمایید.
- اگر نمی‌توانید *SSID* را که می‌خواهید به آن متصل شوید، ببینید، از نرم‌افزار یا برنامه‌ای برای راه‌اندازی *Wi-Fi* از کامپیوتر یا دستگاه هوشمند خود، مانند تلفن هوشمند یا تبلت، استفاده کنید. برای اطلاعات بیشتر، تیاسب‌و هباتدینک دراو دوخ رگورم رد ار «*https://epson.sn*» .دیوربمیظنت هبو دینک دراو ار دوخ لوصحم ماند ،دینک لدیپی‌سترسد

اطلاعات مرتبط

"بررسی وضعیت اتصال شبکه" در صفحه 27

انجام تنظیمات *Wi-Fi* توسط راه اندازی دکمه فشاری (*WPS*)

با فشار دادن یک دکمه روی روتر بی سیم می توانید شبکه Wi-Fi را بطور خودکار تنظیم کنید. در صورتی که شرایط زیر برقرار باشد، می توانید با استفاده از این روش تنظیم نمایید.

- روتر بی سیم با WPS (Wi-Fi Protected Setup) سازگار است.
- اتصال Wi-Fi فعلی با فشار دادن یک دکمه روی روتر بی سیم برقرار شده است.

نکته:

اگر نمی توانید دکمه را پیدا کنید یا با استفاده از نرم افزار تنظیم را انجام می دهید، به مستندات ارائه شده همراه روتر بی سیم مراجعه کنید.

1. در صفحه اصلی، روی  ضربه بزنید.
2. **روتر** را انتخاب کنید.
3. روی **تنظیمات را شروع کنید** ضربه بزنید.

   در صورتی که اتصال شبکه از قبل تنظیم شده است، جزئیات اتصال نمایش داده خواهند شد. برای تغییر تنظیمات، روی **به اتصال Wi-Fi تغییر دهید.** یا **تغییر تنظیمات** ضربه بزنید.
4. **راه اندازی پوش باتن (WPS)** را انتخاب کنید.
5. دستورالعمل های روی صفحه را دنبال کنید.

اگر در نظر دارید وضعیت اتصال شبکه برای اسکنر را پس از تکمیل راه اندازی بررسی کنید، برای اطلاع از جزئیات، به پیوند اطلاعات مرتبط در زیر مراجعه کنید.

نکته:

اگر اتصال برقرار نشد، روتر بی سیم را دوباره راه اندازی کنید، آن را به اسکنر نزدیکتر کنید و دوباره تلاش کنید.

اطلاعات مرتبط

"بررسی وضعیت اتصال شبکه" در صفحه 27

انجام تنظیمات *Wi-Fi* توسط راه اندازی پین کد (*WPS*)

با استفاده از یک پین کد می توانید به طور خودکار به یک روتر بی سیم متصل شوید. در صورتی که روتر بی سیم مجهز به WPS (تنظیم محافظت شده Wi-Fi) باشد، می توانید از این روش برای تنظیم اتصال استفاده کنید. از یک رایانه برای وارد کردن پین کد به روتر بی سیم استفاده کنید.

1. در صفحه اصلی، روی  ضربه بزنید.
2. **روتر** را انتخاب کنید.
3. روی **تنظیمات را شروع کنید** ضربه بزنید.

   در صورتی که اتصال شبکه از قبل تنظیم شده است، جزئیات اتصال نمایش داده خواهند شد. برای تغییر تنظیمات، روی **به اتصال Wi-Fi تغییر دهید.** یا **تغییر تنظیمات** ضربه بزنید.
4. **سایر موارد** > **نصب کد PIN (WPS)** را انتخاب کنید
5. دستورالعمل های روی صفحه را دنبال کنید.

اگر در نظر دارید وضعیت اتصال شبکه برای اسکنر را پس از تکمیل راه اندازی بررسی کنید، برای اطلاع از جزئیات، به پیوند اطلاعات مرتبط در زیر مراجعه کنید.

نکته:
برای جزئیات بیشتر درباره وارد کردن پین کد به مستندات عرضه شده همراه روتر بی سیم مراجعه کنید.

اطلاعات مرتبط

◆ "بررسی وضعیت اتصال شبکه" در صفحه 27

افزودن یا تعویض رایانه یا دستگاه‌ها

اتصال به یک اسکنر که به شبکه متصل شده است

وقتی یک اسکنر قبلاً به شبکه متصل شده است، یک رایانه یا دستگاه هوشمند را می توانید از طریق شبکه به آن اسکنر وصل کنید.

استفاده از یک اسکنر شبکه از رایانه دوم

توصیه می کنیم که از نصب کننده برای اتصال اسکنر به یک کامپیوتر استفاده کنید.

برای راه‌اندازی نصب‌کننده، به وب‌سایت زیر بروید و سپس نام محصول را وارد کنید. به منوی **تنظیم** بروید و راه‌اندازی را شروع کنید.

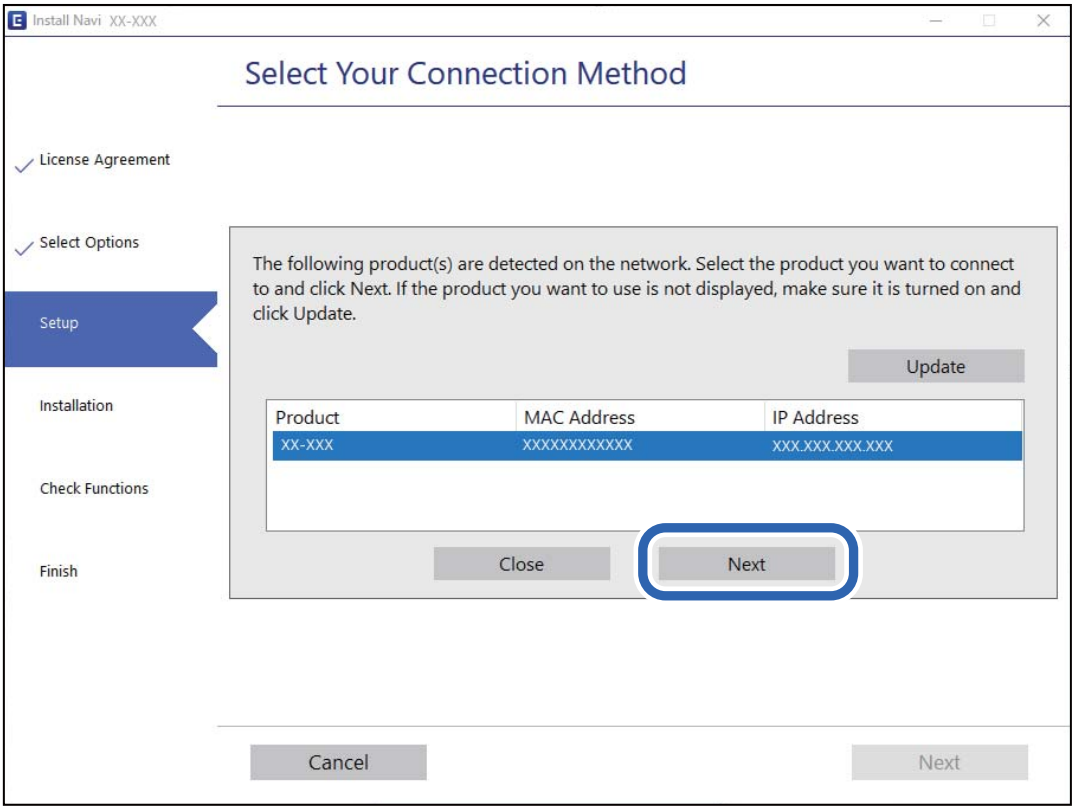
https://epson.sn

دستورالعمل‌های استفاده را می‌توانید در دفترچه راهنمای فیلم وب ببینید. به URL پایین بروید.

https://support.epson.net/publist/vlink.php?code=NPD7509

انتخاب اسکنر

دستورالعمل های روی صفحه را دنبال کنید تا صفحه زیر نمایش داده شود، نام اسکنری که می خواهید به آن وصل شوید را انتخاب کنید و در نهایت روی **بعدی** کلیک کنید.



دستورالعمل های روی صفحه را دنبال کنید.

استفاده از یک اسکنر شبکه از دستگاه هوشمند

با استفاده از یکی از روش های زیر می توانید یک دستگاه هوشمند را به اسکنر وصل کنید.

اتصال از طریق یک روتر بی سیم

دستگاه هوشمند را به همان شبکه (SSID Wi-Fi) که اسکنر وصل شده، متصل کنید.

برای اطلاعات بیشتر به بخش زیر مراجعه کنید.

"اعمال تنظیمات برای اتصال به دستگاه هوشمند" در صفحه 25

اتصال از طریق Wi-Fi Direct

دستگاه هوشمند را به طور مستقیم و بدون استفاده از روتر بی سیم به اسکنر وصل کنید.

برای اطلاعات بیشتر به بخش زیر مراجعه کنید.

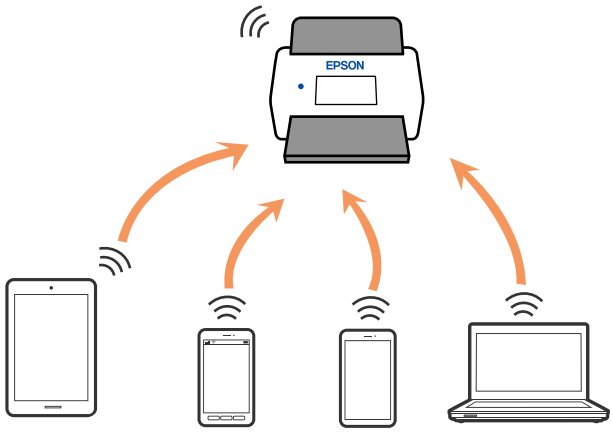
"وصل کردن مستقیم یک دستگاه هوشمند و یک اسکنر (Wi-Fi Direct)" در صفحه 23

وصل کردن مستقیم یک دستگاه هوشمند و یک اسکنر (Wi-Fi Direct)

Simple APWi-Fi Direct)) به شما امکان می دهد بدون استفاده از یک روتر بی سیم یک دستگاه هوشمند را مستقیماً به یک اسکنر وصل کنید و از طریق دستگاه هوشمند اسکن کنید.

درباره Wi-Fi Direct

از این روش اتصال زمانی استفاده کنید که از Wi-Fi در خانه یا محل کار استفاده نمی کنید، یا زمانی که می خواهید اسکنر و کامپیوتر یا دستگاه هوشمند را به صورت مستقیم به هم وصل کنید. در این حالت، اسکنر به عنوان یک روتر بی سیم عمل می کند و شما می توانید دستگاه ها را بدون نیاز به استفاده از روتر بی سیم، به اسکنر وصل کنید. با این وجود، دستگاه هایی که به صورت مستقیم به اسکنر متصل می شوند نمی توانند از طریق اسکنر با یکدیگر ارتباط برقرار کنند.



اسکنر را می توانید با استفاده از Wi-Fi یا اترنت و Simple APWi-Fi Direct)) به صورت همزمان وصل کنید. با این وجود اگر اتصال شبکه را در Simple APWi-Fi Direct)) شروع کنید و در همین حال اسکنر نیز با Wi-Fi وصل باشد، Wi-Fi موقتاً قطع می شود.

اتصال به یک دستگاه هوشمند با Wi-Fi Direct

این روش به شما امکان می دهد که اسکنر را به صورت مستقیم به دستگاه های هوشمند بدون روتر بی سیم متصل کنید.

1.  را در صفحه اصلی انتخاب کنید.
2. **Wi-Fi Direct** را انتخاب کنید.
3. **تنظیمات را شروع کنید** را انتخاب کنید.
4. Epson Smart Panel را روی دستگاه هوشمند خود راه اندازی کنید.
5. برای اتصال به اسکنر خود، دستورالعمل های نمایش داده شده روی Epson Smart Panel را دنبال کنید.
   وقتی دستگاه هوشمند شما به اسکنر متصل است، به مرحله بعدی بروید.
6. در پانل کنترل اسکنر، گزینه **کامل** را انتخاب کنید.

قطع اتصال Wi-Fi Direct (Simple AP)

دو روش برای غیرفعال کردن اتصال Simple APWi-Fi Direct)) وجود دارد؛ می‌توانید همه اتصالات را از طریق پانل کنترل اسکنر غیرفعال کنید یا هر اتصال را از طریق رایانه یا دستگاه هوشمند غیرفعال کنید.

هنگامی که در نظر دارید همه اتصالات را غیرفعال کنید، مسیر  > **Wi-Fi Direct** > **تنظیمات را شروع کنید** > **تغییر** > **غیرفعال کردن Wi-Fi Direct** را انتخاب نمایید.

> **مهم:**
> هنگامی که اتصال *Simple APWi-Fi Direct*)) قطع می‌شود، اتصال همه رایانه‌ها و دستگاه‌های هوشمند متصل به اسکنر در اتصال *Wi-Fi Direct* (*Simple AP*)) قطع می‌شود.

نکته:
اگر می‌خواهید اتصال دستگاه خاصی را قطع کنید، اتصال را به جای اسکنر، از دستگاه قطع کنید. یکی از روش‌های زیر را برای قطع اتصال *Wi-Fi Direct* (*Simple AP*)) از دستگاه استفاده کنید.

❏ اتصال *Wi-Fi* به نام شبکه (*SSID*) اسکنر را قطع کنید.

❏ به یک نام شبکه (*SSID*) دیگر وصل شوید.

تغییر تنظیمات Simple APWi-Fi Direct)) مانند SSID

وقتی اتصال Simple APWi-Fi Direct)) فعال باشد، شما می توانید تنظیمات را از طریق  > **Wi-Fi Direct** > **تنظیمات را شروع کنید** > **تغییر** تغییر دهید و سپس گزینه های منوی زیر نمایش داده می شوند.

تغییر نام شبکه

نام شبکه (SSID) مربوط به Simple APWi-Fi Direct)) مورد استفاده برای اتصال به اسکنر را به نام مدنظر خود تغییر دهید. نام شبکه (SSID) را به صورت نویسه های ASCII وارد کنید که در صفحه کلید نرم افزاری پانل کنترل نمایش داده می شوند. می توانید تا حداکثر 22 نویسه وارد کنید.

هنگام تغییر نام شبکه (SSID)، ارتباط همه دستگاه های متصل قطع خواهد شد. در صورت تمایل به اتصال مجدد دستگاه، از نام شبکه (SSID) جدید استفاده کنید.

تغییر گذرواژه

رمز عبور Simple APWi-Fi Direct)) برای اتصال دادن اسکنر را به مقدار اختیاری تغییر دهید. شما می توانید رمز عبور را به صورت نویسه های ASCII وارد کنید که در صفحه کلید نرم افزاری پانل کنترل نمایش داده می شوند. می توانید 8 الی 22 نویسه وارد کنید.

هنگام تغییر رمز عبور، ارتباط همه دستگاه های متصل قطع خواهد شد. در صورت تمایل به اتصال مجدد دستگاه، از رمز عبور جدید استفاده کنید.

تغییر دامنه فرکانس

دامنه فرکانس Wi-Fi Direct استفاده شده برای اتصال به اسکنر را تغییر دهید. شما می توانید 2.4 گیگاهرتز یا 5 گیگاهرتز را انتخاب کنید.

هنگام تغییر دامنه فرکانس، ارتباط همه دستگاه های متصل قطع خواهد شد. دستگاه را مجدداً وصل کنید.

توجه کنید که هنگام تغییر به فرکانس 5 گیگاهرتز، قادر نخواهید بود از طریق دستگاه هایی که دامنه فرکانس 5 گیگاهرتزی را پشتیبانی نمی کنند، مجدداً وصل شوید.

بسته به منطقه ممکن است این تنظیم نمایش داده نشود.

غیرفعال کردن Wi-Fi Direct

تنظیمات Simple APWi-Fi Direct)) اسکنر را غیرفعال کنید. هنگام غیرفعال کردن این تنظیمات، ارتباط همه دستگاه های متصل به اسکنر از طریق اتصال Wi-Fi Direct (Simple AP) قطع می شود.

بازگشت به تنظیمات پیش فرض

همه تنظیمات Simple APWi-Fi Direct)) را به مقادیر پیش فرض باز می گرداند.

اطلاعات اتصال Wi-Fi Direct (Simple AP) دستگاه هوشمند ذخیره شده در اسکنر حذف می شوند.

نکته:

همچنین می توانید تنظیمات زیر را از طریق زبانه ***Network*** > ***Wi-Fi Direct*** در *Web Config* اعمال نمایید.

- ❑ فعال یا غیرفعال کردن *Simple APWi-Fi Direct*))
- ❑ تغییر نام شبکه (*SSID*)
- ❑ تغییر رمز عبور
- ❑ تغییر دامنه فرکانس

  بسته به منطقه ممکن است این تنظیم نمایش داده نشود.
- ❑ بازیابی تنظیمات *Simple APWi-Fi Direct*))

تنظیم مجدد اتصال شبکه

این بخش نحوه اعمال تنظیمات اتصال شبکه و تغییر روش اتصال هنگام تعویض روتر بی سیم یا رایانه را شرح می دهد.

هنگام تعویض روتر بی سیم

هنگام تعویض روتر بی سیم ، تنظیمات اتصال بین رایانه یا دستگاه هوشمند و اسکنر را اعمال کنید.

اگر ارائه دهنده خدمات اینترنت خود و موارد مشابه را تغییر دهید، نیاز خواهید داشت این تنظیمات را اعمال کنید.

اعمال تنظیمات برای اتصال به رایانه

توصیه می کنیم که از نصب کننده برای اتصال اسکنر به یک کامپیوتر استفاده کنید.

برای راه‌اندازی نصب‌کننده، به وب‌سایت زیر بروید و سپس نام محصول را وارد کنید. به منوی **تنظیم** بروید و راه‌اندازی را شروع کنید.

https://epson.sn

دستورالعمل‌های استفاده را می‌توانید در دفترچه راهنمای فیلم وب ببینید. به URL پایین بروید.

https://support.epson.net/publist/vlink.php?code=NPD7509

انتخاب یک روش اتصال

دستورالعمل های روی صفحه را دنبال کنید. در صفحه **گزینه نصب را انتخاب کنید ، دوباره اتصال چاپگر را برقرار کنید (برای روتر شبکه جدید یا تغییر USB به شبکه و دیگر موارد)** را انتخاب کنید و روی **بعدی** کلیک کنید.

برای پایان یافتن نصب، دستورالعمل های روی صفحه را دنبال کنید.

اگر اتصال برقرار نمی شود، برای رفع مشکل موارد زیر را ببینید.

"اتصال به یک شبکه ممکن نیست" در صفحه 32

اعمال تنظیمات برای اتصال به دستگاه هوشمند

زمانی که چاپگر را به همان شبکه Wi-Fi (SSID) که دستگاه هوشمند متصل است وصل می کنید، می توانید از طریق یک دستگاه هوشمند از اسکنر استفاده کنید. برای استفاده از اسکنر از طریق یک دستگاه هوشمند، به وب‌سایت زیر بروید و سپس نام محصول را وارد کنید. به منوی **تنظیم** بروید و راه‌اندازی را شروع کنید.

https://epson.sn

از دستگاه هوشمند مورد نظر برای اتصال به اسکنر، به وب سایت دسترسی پیدا کنید.

هنگام تغییر رایانه

هنگام تغییر رایانه، تنظیمات اتصال بین رایانه و اسکنر را اعمال کنید.

اعمال تنظیمات برای اتصال به رایانه

توصیه می کنیم که از نصب کننده برای اتصال اسکنر به یک کامپیوتر استفاده کنید.

برای راه‌اندازی نصب‌کننده، به وب‌سایت زیر بروید و سپس نام محصول را وارد کنید. به منوی **تنظیم** بروید و راه‌اندازی را شروع کنید.

https://epson.sn

دستورالعمل‌های استفاده را می‌توانید در دفترچه راهنمای فیلم وب ببینید. به URL پایین بروید.

https://support.epson.net/publist/vlink.php?code=NPD7509

دستورالعمل های روی صفحه را دنبال کنید.

تغییر دادن روش اتصال به رایانه

این بخش نحوه تغییر دادن روش اتصال هنگامی که رایانه و اسکنر متصل هستند را توضیح می دهد.

تغییر اتصال شبکه از اترنت به *Wi-Fi*

از طریق پانل کنترل اسکنر، اتصال اترنت را به اتصال Wi-Fi تغییر دهید. تغییر دادن روش اتصال اساساً به همان صورت اعمال تنظیمات اتصال Wi-Fi انجام می‌شود.

اطلاعات مرتبط

"اتصال به LAN بی سیم (Wi-Fi)" در صفحه 19

تغییر اتصال شبکه از *Wi-Fi* به اترنت

مراحل زیر را برای تغییر از اتصال Wi-Fi به اتصال اترنت دنبال کنید.

1. در صفحه اصلی، گزینه **تنظیم** را انتخاب کنید.
2. مسیر **تنظیمات شبکه** > **تنظیم LAN سیم دار** را انتخاب کنید.
3. دستورالعمل‌های روی صفحه را دنبال کنید.

تغییر از اتصال *USB* به اتصال شبکه

استفاده از یک نصب کننده و راه اندازی مجدد با یک روش اتصال متفاوت.

به وب‌سایت زیر دسترسی پیدا کنید و سپس نام محصول را وارد کنید. به منوی **تنظیم** بروید و راه‌اندازی را شروع کنید.

https://epson.sn

انتخاب تغییر روش های اتصال

دستورالعمل‌های ارائه شده در هر پنجره را دنبال کنید. در صفحه **گزینه نصب را انتخاب کنید** ، **دوباره اتصال چاپگر را برقرار کنید (برای روتر شبکه جدید یا تغییر USB به شبکه و دیگر موارد)** را انتخاب کنید و روی **بعدی** کلیک کنید.

اتصال شبکه **اتصال از طریق شبکه بی سیم (Wi-Fi)** یا **از طریق LAN سیم دار (اترنت) وصل شوید** که در نظر دارید استفاده کنید را انتخاب نمایید و سپس روی **بعدی** کلیک کنید.

برای پایان یافتن نصب، دستورالعمل های روی صفحه را دنبال کنید.

بررسی وضعیت اتصال شبکه

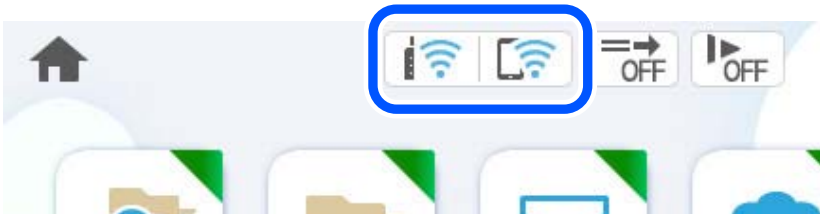
به روش زیر می‌توانید وضعیت اتصال شبکه را بررسی کنید.

بررسی وضعیت اتصال شبکه از پانل کنترل

از طریق آیکون شبکه یا اطلاعات شبکه در پانل کنترل اسکنر می توانید وضعیت اتصال شبکه را بررسی کنید.

بررسی وضعیت اتصال شبکه با استفاده از آیکن شبکه

با استفاده از آیکن شبکه روی صفحه اصلی اسکنر می‌توانید وضعیت اتصال شبکه و قوت موج رادیویی را بررسی کنید.



وضعیت اتصال شبکه را نشان می‌دهد. برای بررسی و تغییر دادن تنظیمات جاری این آیکن را انتخاب کنید. این یک میانبر دسترسی به منوی زیر است. **تنظیم** > **تنظیمات شبکه** > **نصب Wi-Fi**	
	اسکنر به یک شبکه بیسیم (Wi-Fi) متصل نیست.
	اسکنر در حال جستجوی SSID یا صفر کردن آدرس IP است یا جهت اتصال به یک شبکه بیسیم (Wi-Fi) با مشکل مواجه شده است.
	اسکنر به یک شبکه بیسیم (Wi-Fi) متصل است. تعداد نوارها، قدرت سیگنال اتصال را نشان می‌دهند. هرچه تعداد نوارها بیشتر باشد، اتصال قوی‌تر خواهد بود.
	اسکنر به یک شبکه بیسیم (Wi-Fi) در حالت Wi-Fi Direct (Simple AP) متصل نیست.
	اسکنر به یک شبکه بیسیم (Wi-Fi) در حالت Wi-Fi Direct (Simple AP) متصل است.
	اسکنر به یک شبکه با سیم (اترنت) متصل نیست یا آدرس آن را صفر کرده است.
	اسکنر به یک شبکه با سیم (اترنت) متصل است.

نمایش اطلاعات کامل شبکه از پانل کنترل

زمانی که اسکنر به شبکه وصل است همچنین می توانید سایر اطلاعات مربوط به شبکه را با انتخاب منوهای شبکه مورد نظر برای بررسی مشاهده نمایید.

1. **تنظیم** را در صفحه اصلی انتخاب کنید.
2. **تنظیمات شبکه** > **وضعیت شبکه** را انتخاب کنید.
3. برای بررسی اطلاعات، منوهایی را که می خواهید بررسی نمایید انتخاب کنید.

❑ وضعیت LAN/Wi-Fi سیمی

اطلاعات شبکه (نام دستگاه، اتصال، قدرت سیگنال و غیره) را برای اتصال های اترنت یا Wi-Fi نشان می دهد.

❑ وضعیت Wi-Fi Direct

فعال یا غیرفعال بودن Wi-Fi Direct و نیز SSID، رمز عبور و امثال آن را برای اتصال های Wi-Fi Direct نشان می دهد.

❑ وضعیت سرور ایمیل

اطلاعات شبکه سرور ایمیل را نشان می دهد.

مشخصات شبکه

مشخصات Wi-Fi

برای اطلاع از مشخصات Wi-Fi، جدول زیر را ملاحظه کنید.

کشورها یا مناطق غیر از موارد ذکر شده در لیست زیر	**جدول A**
ایرلند، بریتانیا، اتریش، آلمان، لیختن‌اشتاین، سوئیس، فرانسه، بلژیک، لوکزامبورگ، هلند، ایتالیا، پرتغال، اسپانیا، دانمارک، فنلاند، نروژ، سوئد، ایسلند، کرواسی، قبرس، یونان، مقدونیه شمالی، صربستان، اسلوونی، مالت، بوسنی و هرزگوین، کوزوو، مونته‌نگرو، آلبانی، بلغارستان، جمهوری چک، استونی، مجارستان، لتونی، لیتوانی، لهستان، رومانی، اسلواکی، اسرائیل، استرالیا، نیوزیلند، تایوان	**جدول B**
ترکیه	:DS-900WN شماره‌های سریال که با XDA8 شروع می‌شود: **جدول A** شماره‌های سریال که با XDA7 شروع می‌شود: **جدول B**
	:DS-800WN شماره‌های سریال که با XDA2 شروع می‌شود: **جدول A** شماره‌های سریال که با XD9Z شروع می‌شود: **جدول B**

جدول A

استانداردها	[1*]IEEE 802.11b/g/n
دامنه فرکانس	2400–2483.5 مگاهرتز

حداکثر نیروی فرکانس رادیویی ارسال‌شده	(20 dBm (EIRP
کانال‌ها	1/2/3/4/5/6/7/8/9/10/11/12/13
حالت های اتصال	زیرساخت، Wi-Fi Direct (Simple AP)[*2][*3]
پروتکل‌های امنیتی[*4]	WEP (64/128bit)، WPA2-PSK (AES)[*5]، WPA3-SAE (AES)، WPA2/WPA3-Enterprise

*1 تنها برای HT20 در دسترس می باشد.

*2 برای IEEE 802.11b پشتیبانی نمی شود.

*3 حالت های زیرساخت و Wi-Fi Direct یا یک اتصال اترنت را می توان به صورت همزمان استفاده کرد.

*4 قابلیت Wi-Fi Direct تنها از WPA2-PSK (AES) پشتیبانی می کند.

*5 با استانداردهای WPA2 با پشتیبانی برای WPA/WPA2 Personal مطابقت دارد.

جدول B

استانداردها	IEEE 802.11a/b/g/n/ac[1*]		
محدوده‌های فرکانس	IEEE 802.11b/g/n: 2.4 GHz، IEEE 802.11a/n/ac: 5 GHz		
کانال‌ها	Wi-Fi	2.4 گیگاهرتز	1/2/3/4/5/6/7/8/9/10/11/12/13[*1][*2][*2]
		5 گیگاهرتز[*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 گیگاهرتز	1/2/3/4/5/6/7/8/9/10/11/12/13[*1][*2][*2]
		5 گیگاهرتز[*3]	W52 (36/40/44/48) W58 (149/153/157/161/165)
حالت‌های اتصال	زیرساخت، Wi-Fi Direct (AP ساده)[*4]، [*5]		
پروتکل‌های امنیتی[*6]	WEP (64/128bit)، WPA2-PSK (AES)[*7]، WPA3-SAE (AES)، WPA2/WPA3-Enterprise		

*1 تنها برای HT20 در دسترس می باشد.

*2 در تایوان ارائه نمی شود.

*3 موجود بودن این کانال ها و استفاده از محصول در فضاهای باز از طیرق این کانال ها بر اساس موقعیت متفاوت خواهد بود. جهت کسب اطلاعات بیشتر، http://support.epson.net/wifi5ghz/ را ببینید

*4 برای IEEE 802.11b پشتیبانی نمی‌شود

*5 حالت های زیرساخت و Wi-Fi Direct یا یک اتصال اترنت را می توان به صورت همزمان استفاده کرد.

*6 Wi-Fi Direct تنها از WPA2-PSK (AES) پشتیبانی می کند.

*7 با استانداردهای WPA2 با پشتیبانی برای WPA/WPA2 Personal مطابقت دارد.

مشخصات اترنت

استانداردها	[1*](10BASE-T) IEEE802.3i [1*](100BASE-TX) IEEE802.3u [1*](1000BASE-T) IEEE802.3ab [2*] IEEE802.3az (اترنت کم-مصرف)
حالت ارتباط	خودکار، 10 Mbps فول دوپلکس، 10 Mbps نیمه دوپلکس، 100 Mbps فول دوپلکس، 100 Mbps نیمه دوپلکس
رابط	RJ-45

*1 برای جلوگیری از بروز تداخل رادیویی از کابل STP (جفت تابیده غلاف‌دار) رده 5e یا بالاتر استفاده کنید.

*2 دستگاه متصل باید با استاندارد IEEE802.3az سازگار باشد.

ویژگی های شبکه و پشتیبانی IPv4/IPv6

ویژگی‌های	پشتیبانی شده
Epson Scan 2	IPv4، IPv6
Document Capture Pro/Document Capture	IPv4

پروتکل امنیتی

*IEEE802.1X	
IPsec/IP Filtering	
SSL/TLS	HTTPS Server/Client
SMTPS (STARTTLS), SMTPS (SSL/TLS)	
SNMPv3	

* استفاده از دستگاه اتصال سازگار با IEEE802.1X ضروری است.

استفاده از درگاه برای اسکنر

اسکنر از درگاه زیر استفاده می‌کند. سرپرست شبکه می‌بایست در صورت لزوم، دسترسی به این درگاه‌ها را اجازه دهد.

وقتی فرستنده (سرویس‌گیرنده) اسکنر است

موارد استفاده	مقصد (سرور)	پروتکل	شماره درگاه
ارسال فایل (وقتی قابلیت اسکن و ارسال به پوشه شبکه از اسکنر استفاده شود)	سرور FTP/FTPS	FTP/FTPS (TCP)	20
			21
	سرور فایل	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	سرور WebDAV	پروتکل HTTP (TCP)	80
		پروتکل HTTPS(TCP)	443
ارسال ایمیل (وقتی قابلیت اسکن و ارسال به ایمیل از اسکنر استفاده شود)	سرور SMTP	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP پیش از اتصال SMTP (وقتی قابلیت اسکن و ارسال به ایمیل در اسکنر استفاده شود)	سرور POP	POP3 (TCP)	110
در صورت استفاده از Epson Connect	سرور Epson Connect	HTTPS	443
		XMPP	5222
جمع آوری اطلاعات کاربر (با استفاده از مخاطبین اسکنر)	سرور LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
تأیید هویت هنگام جمع آوری اطلاعات کاربر (در صورت استفاده از مخاطبین اسکنر) تأیید هویت کاربر هنگام استفاده از قابلیت "اسکن و ارسال به پوشه شبکه" (SMB) اسکنر	سرور KDC	Kerberos	88
Control WSD	رایانه سرویس‌گیرنده	WSD (TCP)	5357
جستجوی رایانه هنگام استفاده از قابلیت اسکن و ارسال همزمان از طریق یک برنامک	رایانه سرویس‌گیرنده	کشف اسکن و ارسال همزمان به شبکه	2968

وقتی فرستنده (سرویس‌گیرنده) رایانه سرویس‌گیرنده است

موارد استفاده	مقصد (سرور)	پروتکل	شماره درگاه
اسکنر را از برنامه‌ای مانند EpsonNet Config و درایور اسکنر کشف کنید.	اسکنر	ENPC (UDP)	3289
از برنامه‌ای مانند EpsonNet Config و درایور اسکنر، اطلاعات MIB را جمع‌آوری و تنظیم کنید.	اسکنر	SNMP (UDP)	161
جستجوی اسکنر WSD	اسکنر	WS-Discovery (UDP)	3702
پیش-ارسال داده‌های اسکن از یک برنامک	اسکنر	اسکن شبکه (TCP)	1865

موارد استفاده	مقصد (سرور)	پروتکل	شماره درگاه
جمع‌آوری اطلاعات کار هنگام استفاده از قابلیت اسکن و ارسال همزمان از طریق یک برنامک	اسکنر	اسکن و ارسال همزمان به شبکه	2968
Web Config	اسکنر	HTTP (TCP)	80
		HTTPS (TCP)	443

حل کردن مشکلات

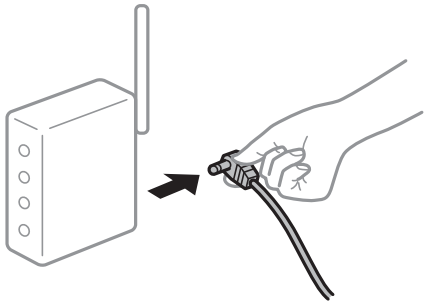
اتصال به یک شبکه ممکن نیست

ممکن است این مشکل بنا به یکی از دلایل زیر رخ داده باشد.

مشکلی در رابطه با دستگاه های شبکه برای اتصال Wi-Fi وجود دارد.

راهکارها

دستگاه هایی که می خواهید به شبکه متصل کنید را خاموش کنید. حدود 10 ثانیه صبر کنید و سپس دستگاه ها را به این ترتیب روشن کنید: روتر بی سیم، رایانه یا دستگاه هوشمند و سپس اسکنر. اسکنر و رایانه یا دستگاه هوشمند را به روتر بی سیم نزدیک کنید تا ارتباط امواج رادیویی بهتر شود و سپس سعی کنید تنظیمات شبکه را دوباره انجام دهید.



دستگاه ها نمی توانند سیگنال ها را از روتر بی سیم دریافت کنند زیرا بسیار دور از هم هستند.

راهکارها

پس از انتقال دادن رایانه یا دستگاه هوشمند و اسکنر به نزدیکی روتر بی سیم ، روتر بی سیم را خاموش و سپس مجدداً روشن کنید.

هنگام تغییر روتر بی‌سیم، تنظیمات با روتر جدید مطابقت ندارند.

راهکارها

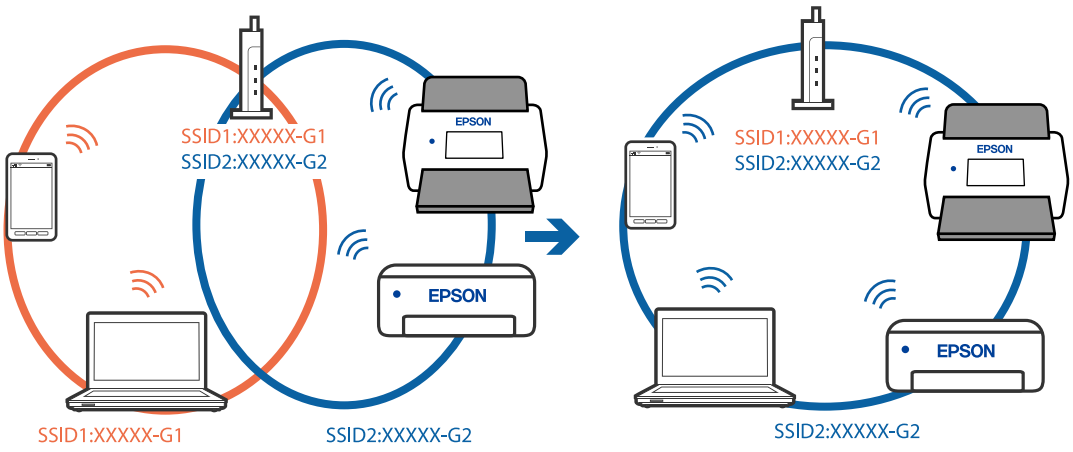
تنظیمات اتصال را مجدداً به نحوی اعمال کنید تا با روتر بی‌سیم جدید مطابقت داشته باشند.

SSID های متصل شده از رایانه یا دستگاه هوشمند و رایانه متفاوت هستند.

راهکارها

هنگامی که از چندین روتر بی سیم به صورت همزمان استفاده می کنید یا روتر بی سیم چندین SSID دارد و دستگاه ها به SSIDهای متفاوتی متصل هستند، نمی توانید به روتر بی سیم وصل شوید.

رایانه یا دستگاه هوشمند را به همان SSID که اسکنر متصل است وصل کنید.



یک جداکننده حریم خصوصی در روتر بی سیم در دسترس می باشد.

راهکارها

اغلب روترهای بی سیم یک ویژگی جداکننده حریم خصوصی دارند که ارتباط بین دستگاه متصل را مسدود می کند. اگر با وجود وصل بودن به یک شبکه یکسان، نمی توانید بین اسکنر و رایانه یا دستگاه هوشمند ارتباط برقرار کنید، جدا کننده حریم خصوصی را روی روتر بی سیم غیرفعال کنید. برای جزئیات بیشتر به مستندات عرضه شده با روتر بی سیم مراجعه کنید.

آدرس IP به درستی تخصیص نیافته است.

راهکارها

اگر نشانی IP اسکنر XXX.XXX.169.254 و ماسک زیرشبکه 255.255.0.0 باشد، نشانی IP را نمی‌توان به درستی تخصیص داد.

تنظیم > **تنظیمات شبکه** > **پیشرفته** > **TCP/IP** را در پانل کنترل اسکنر انتخاب کنید و سپس آدرس IP و ماسک شبکه فرعی تخصیص یافته به اسکنر را بررسی کنید.

روتر بی‌سیم را دوباره راه‌اندازی کنید یا تنظیمات شبکه اسکنر را بازنشانی کنید.

مشکلی در رابطه با تنظیمات شبکه در رایانه وجود دارد.

راهکارها

سعی کنید از طریق رایانه به یک وب‌سایت وارد شوید تا اطمینان حاصل کنید که تنظیمات شبکه رایانه شما صحیح است. اگر نمی‌توانید به هیچ وب‌سایتی دسترسی پیدا کنید، مشکلی در رایانه وجود دارد.

اتصال شبکه رایانه را بررسی کنید. برای جزئیات بیشتر به مستندات عرضه شده به همراه رایانه مراجعه کنید.

اسکنر توسط اترنت از طریق دستگاه هایی که IEEE 802.3az (اترنت با بازده انرژی بالا) را پشتیبانی می کنند متصل است.

راهکارها

وقتی اسکنر را از طریق اترنت با استفاده از دستگاه های پشتیبانی کننده IEEE 802.3az (اترنت با بازده انرژی بالا) متصل می کنید، ممکن است بسته به هاب یا روتر مورد استفاده مشکلات زیر بروز کنند.

- ❏ اتصال دچار نوسان می شود، اسکنر بارها قطع و وصل می شود.
- ❏ اتصال به اسکنر امکان‌پذیر نیست.
- ❏ سرعت اتصال آهسته می شود.

برای غیرفعال کردن IEEE 802.3az مربوط به اسکنر، مراحل زیر را دنبال کنید و سپس متصل شوید.

1. کابل اترنت متصل به رایانه و اسکنر را جدا کنید.
2. وقتی IEEE 802.3az مخصوص رایانه فعال است، آن را غیرفعال کنید.
   برای جزئیات بیشتر به مستندات عرضه شده به همراه رایانه مراجعه کنید.
3. رایانه و اسکنر را با کمک یک کابل اترنت به طور مستقیم به یکدیگر وصل کنید.
4. در اسکنر، تنظیمات شبکه را بررسی کنید.
   مسیر **تنظیم** > **تنظیمات شبکه** > **وضعیت شبکه** > **وضعیت LAN/Wi-Fi سیمی** را انتخاب کنید.
5. نشانی IP اسکنر را بررسی کنید.
6. در رایانه، به Web Config وارد شوید.
   یک مرورگر وب را اجرا کنید و سپس آدرس IP اسکنر را وارد نمایید.
   "اجرای Web Config در یک مرورگر وب" در صفحه 36
7. زبانه **Network** > **Wired LAN** را انتخاب کنید.
8. گزینه **OFF** را برای **IEEE 802.3az** انتخاب کنید.
9. روی **Next** کلیک کنید.
10. روی **OK** کلیک کنید.
11. کابل اترنت متصل به رایانه و اسکنر را جدا کنید.
12. اگر IEEE 802.3az مخصوص رایانه را در مرحله 2 غیرفعال کردید، آن را فعال نمایید.
13. کابل های اترنت که در مرحله 1 جدا کرده بودید را به رایانه و اسکنر متصل کنید.

اگر مشکل هنوز باقی مانده است، ممکن است مشکل به دستگاه هایی غیر از اسکنر مربوط باشد.

اسکنر خاموش است.

راهکارها

اطمینان حاصل کنید که اسکنر روشن است.

همچنین منتظر بمانید تا چشمک زدن چراغ وضعیت تمام شود که این امر نشان می دهد اسکنر برای اسکن کردن آماده است.

نرم‌افزار برای راه‌اندازی اسکنر

برنامه پیکربندی عملیات اسکنر (Web Config)

Web Config برنامه‌ای است که در مرورگرهای وب نظیر Microsoft Edge و Safari در رایانه یا دستگاه هوشمند اجرا می‌شود. می توانید وضعیت اسکنر را تأیید کنید یا سرویس شبکه و تنظیمات اسکنر را تغییر دهید. برای استفاده از Web Config، اسکنر و رایانه یا دستگاه را به شبکه یکسانی متصل کنید.

از مرورگرهای زیر پشتیبانی می‌شود. از جدیدترین نسخه استفاده کنید.

Microsoft Edge، Windows Internet Explorer، Firefox، Chrome، Safari

نکته:
ممکن است هنگام استفاده از این دستگاه در پیام‌واره‌ای از شما خواسته شود رمز عبور سرپرست را وارد کنید. برای اطلاع از جزئیات بیشتر در مورد رمز عبور سرپرست، بخش زیر را ببینید.

"نکاتی در مورد رمز عبور سرپرست" در صفحه *10*

اطلاعات مرتبط

◆ "عدم دسترسی به Web Config" در صفحه 63

اجرای Web Config در یک مرورگر وب

اسکنر، با نرم‌افزار یکپارچه به نام Web Config تحویل داده می‌شود (یک صفحه وب که در آن می‌توانید تنظیمات را انجام دهید). برای دسترسی به Web Config، کافی است آدرس IP یک اسکنر متصل به شبکه را در مرورگر خود وارد کنید.

1. آدرس IP اسکنر را بررسی کنید.

   گزینه **تنظیم** > **تنظیمات شبکه** > **وضعیت شبکه** را در پانل کنترل اسکنر انتخاب کنید. سپس روش اتصال فعال (**وضعیت LAN/Wi-Fi سیمی** یا **وضعیت Wi-Fi Direct**) را برای تأیید نشانی IP اسکنر انتخاب کنید.

   آدرس IP نمونه: 192.168.100.201

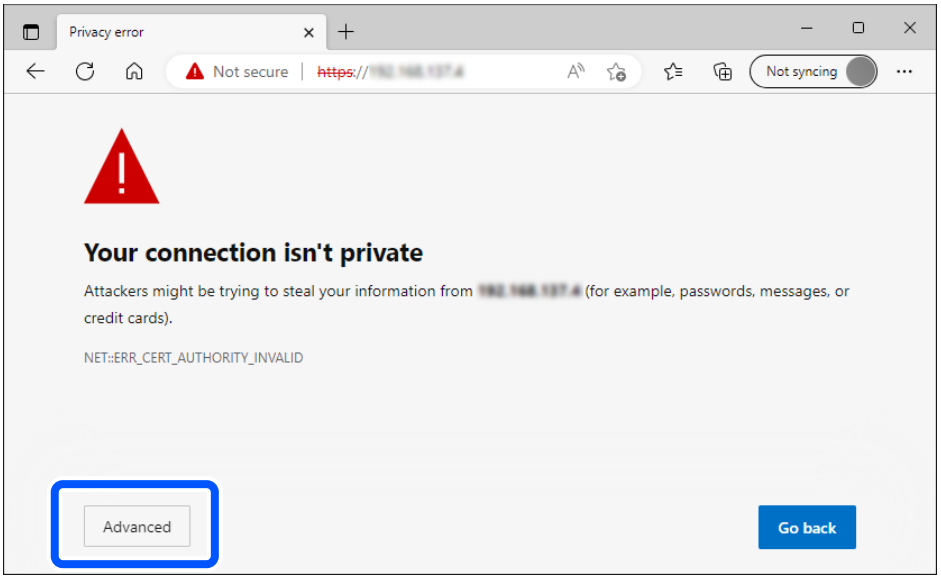
2. یک مرورگر را از کامپیوتر یا دستگاه هوشمند خود راه‌اندازی کنید و سپس آدرس IP اسکنر را در نوار آدرس وارد کنید.

   فرمت: http://آدرس IP اسکنر/

   مثال: http://192.168.100.201/

   اگر یک صفحه هشدار در مرورگرتان ظاهر شد، می‌توانید با اطمینان هشدار را نادیده بگیرید و صفحه وب را نمایش دهید (Web Config). از آنجا که اسکنر از یک گواهی خود-امضاء شونده هنگام دسترسی به HTTPS استفاده می کند وقتی Web Config را راه اندازی کنید، یک هشدار در مرورگر نمایش داده می شود؛ این بدان معنا نیست که مشکلی وجود دارد و با خیال راحت می توانید از آن صرفنظر کنید. بسته به مرورگرتان، ممکن است لازم باشد روی **تنظیمات پیشرفته** کلیک کنید تا صفحه وب را ببینید.

مثال: برای Microsoft Edge



نکته:

- اگر یک صفحه هشدار ظاهر نشد، به مرحله بعد بروید.
- برای نشانی‌های *IPv6*، از فرمت زیر استفاده کنید.

  فرمت: *http://*[نشانی *IP* اسکنر]/

  مثال: *http://[2001:db8::1000:1]/*

3. برای تغییر تنظیمات اسکنر، باید به عنوان یک سرپرست Web Config وارد شوید.

روی **Log in** در گوشه بالا سمت راست صفحه کلیک کنید. **User Name** و **Current password** را وارد کنید و سپس روی **OK** کلیک کنید.

در بخش زیر، مقادیر اولیه برای اطلاعات سرپرست Web Config ارائه می‌شوند.

·نام کاربری: هیچ‌کدام (خالی)

·رمز عبور: بستگی به برچسب چسبانده‌شده به محصول دارد.

اگر برچسب «PASSWORD» به پشت چسبانده شده است، عدد 8 رقمی درج‌شده روی برچسب را وارد کنید. اگر برچسب «PASSWORD» چسبانده نشده است، شماره سریال روی برچسب چسبانده‌شده به پشت محصول را برای رمز عبور سرپرست اولیه وارد کنید.

نکته:

- اگر ***Log out*** در سمت راست بالای صفحه نمایش داده شود، شما قبلاً به‌عنوان سرپرست وارد سیستم شده‌اید.
- اگر تقریباً *20* دقیقه فعالیت نداشته باشید، به‌طور خودکار از سیستم خارج خواهید شد.

Epson Device Admin

Epson Device Admin برنامه‌ای چندکاره است که به شما اجازه می‌دهد دستگاه‌های روی شبکه را مدیریت کنید.

برای اعمال تنظیمات یکپارچه به چندین اسکنر در یک شبکه، می‌توانید از الگوهای پیکربندی استفاده کنید تا آن را برای نصب و مدیریت چندین اسکنر مناسب نمایید.

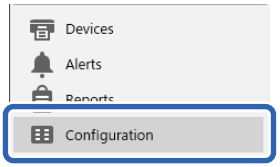
برنامه Epson Device Admin را می‌توانید از وب‌سایت پشتیبانی Epson دانلود کنید. جهت مشاهده جزئیات نحوه استفاده از این برنامه، مستندات مربوطه یا راهنمای Epson Device Admin را ملاحظه کنید.

الگوی پیکربندی

ایجاد کردن الگوی پیکربندی

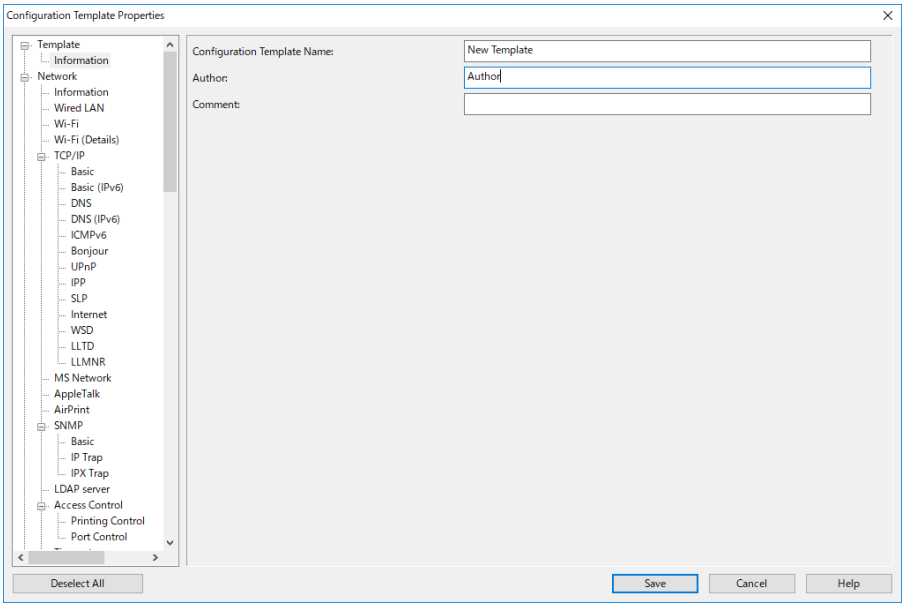
یک الگوی پیکربندی جدید ایجاد کنید.

1. Epson Device Admin را آغاز کنید.
2. گزینه **Configuration** را در منوی نوار کارهای جانبی انتخاب کنید.



3. گزینه **New** در منوی روبان را انتخاب کنید.

4. هر مورد را تنظیم کنید.



مورد	توضیحات
Configuration Template Name	نام الگوی پیکربندی. تا 1024 نویسه یونیکد (UTF-8) وارد کنید.
Author	اطلاعات مربوط به ایجاد کننده الگو. تا 1024 نویسه یونیکد (UTF-8) وارد کنید.

مورد	توضیحات
Comment	اطلاعات غیرواقعی وارد کنید. تا 1024 نویسه یونیکد (UTF-8) وارد کنید.

5. مواردی را که در نظر دارید تنظیم کنید در سمت چپ انتخاب کنید.

نکته:
روی گزینه‌های منو در سمت چپ کلیک کنید تا به هر صفحه جابجا شوید. اگر صفحه را تغییر دهید مقدار تنظیم شده حفظ می‌شود، اما در صورت لغو صفحه آن را از دست می‌دهید. وقتی کار همه تنظیمات به پایان رسید، بر روی گزینه ***Save*** کلیک کنید.

اعمال کردن الگوی پیکربندی

الگوی پیکربندی ذخیره شده را به اسکنر اعمال کنید. موارد انتخاب‌شده در الگو اعمال می‌شوند. اگر اسکنر مقصد فاقد عملکرد مناسب باشد، این تنظیم اعمال نمی‌گردد.

نکته:
وقتی یک رمز عبور سرپرست برای اسکنر تعریف می‌کنید، ابتدا رمز عبور را پیکربندی نمایید.

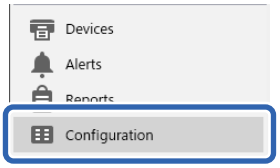
1. در منوی روبان صفحه لیست دستگاه‌ها، مسیر ***Options*** > ***Password manager*** را انتخاب کنید.

2. ***Enable automatic password management*** را انتخاب کنید و سپس روی ***Password manager*** کلیک کنید.

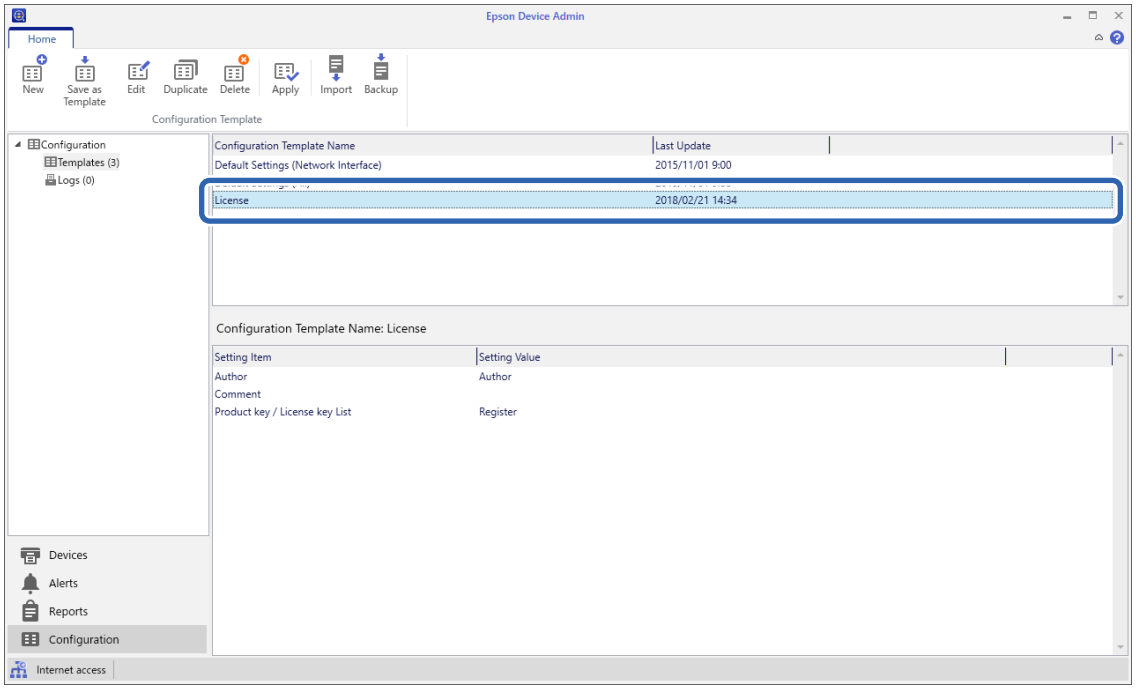
3. اسکنر مناسب را انتخاب کنید و سپس روی گزینه ***Edit*** کلیک کنید.

4. رمز عبور را تعیین کنید و سپس روی گزینه ***OK*** کلیک کنید.

1. گزینه **Configuration** را در منوی نوار کارهای جانبی انتخاب کنید.



2. الگوی پیکربندی را از بخش **Configuration Template Name** انتخاب کنید.



3. روی گزینه **Apply** در منوی روبان کلیک کنید.

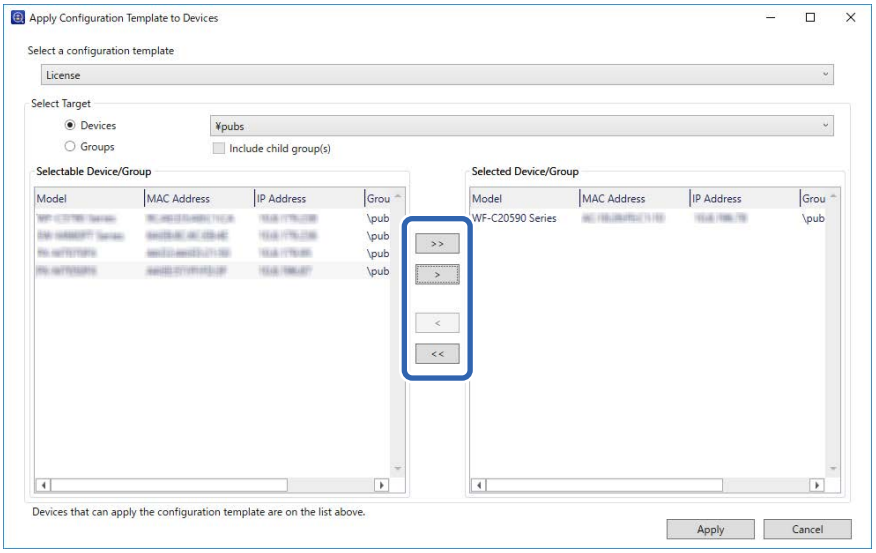
صفحه انتخاب دستگاه نمایش داده می‌شود.

4. الگوی پیکربندی مورد نظر برای اعمال کردن را انتخاب کنید.

نکته:

- وقتی ***Devices*** و گروه‌های حاوی دستگاه‌ها را از منوی کرکره‌ای انتخاب می‌کنید، هر دستگاه نمایش داده می‌شود.
- وقتی گزینه ***Groups*** را انتخاب کنید، گروه‌ها نمایش داده می‌شوند. برای انتخاب خودکار گروه‌های زیرمجموعه درون گروه انتخاب شده، گزینه ***Include child group(s)*** را انتخاب کنید.

5. اسکنر یا گروه‌هایی را که در نظر دارید الگو به آنها اعمال شود به **Selected Device/Group** انتقال دهید.



6. روی **Apply** کلیک کنید.

یک صفحه تأیید برای الگوی پیکربندی مورد نظر جهت اعمال کردن نمایش داده می‌شود.

7. برای اعمال الگوی پیکربندی، روی گزینه **OK** کلیک کنید.

8. وقتی پیام تکمیل شدن پروسه برایتان نمایش داده می‌شود، روی گزینه **OK** کلیک کنید.

9. روی گزینه **Details** کلیک کرده و اطلاعات را بررسی کنید.

وقتی گزینه روی مواردی که اعمال می‌کنید نمایش داده می‌شود، برنامه با موفقیت نصب شده است.

10. روی **Close** کلیک کنید.

تنظیمات لازم برای اسکن کردن

ثبت دوباره یک سرور ایمیل

قبل از پیکربندی سرور ایمیل، موارد زیر را بررسی کنید.

❑ اسکنر به شبکه وصل باشد

❑ اطلاعات تنظیم برای سرور ایمیل

هنگام استفاده از یک سرور ایمیل مبتنی بر اینترنت، اطلاعات مربوط به تنظیمات را از ارائه‌دهنده یا وبسایت کنترل کنید.

روش ثبت

به بخش Web Config وارد شوید و **Network** > **Email Server** > **Basic** را انتخاب کنید.

"اجرای Web Config در یک مرورگر وب" در صفحه 36

تنظیمات را می توانید از طریق پانل کنترل اسکنر نیز اعمال کنید. مسیر **تنظیم** > **تنظیمات شبکه** > **پیشرفته** > **سرور ایمیل** > **تنظیمات سرور** را انتخاب کنید.

موارد تنظیم سرور ایمیل

مورد	تنظیمات و توضیحات	
Authentication Method	روش تأیید اعتبار اسکنر برای دسترسی به سرور ایمیل را مشخص کنید.	
	Off	تأیید اعتبار زمان ارتباط با سرور ایمیل غیرفعال است.
	SMTP AUTH	لازم است سرور ایمیل از تأیید اعتبار SMTP پشتیبانی کند.
	POP before SMTP	هنگام انتخاب این مورد، یک سرور POP3 را تعیین کنید.
Authenticated Account	اگر **SMTP AUTH** یا **POP before SMTP** را به عنوان **Authentication Method** انتخاب کنید، نام حساب معتبر را وارد کنید. حداکثر 0 تا 255 نویسه اسکی (0x20–0x7E) وارد کنید.	
Authenticated Password	اگر **SMTP AUTH** یا **POP before SMTP** را به عنوان **Authentication Method** انتخاب کنید، رمز معتبر را وارد کنید. بین 0 تا 20 نویسه با قالب اسکی ((0x20–0x7E وارد کنید.	
Sender's Email Address	آدرس ایمیلی را که برای فرستادن ایمیل‌ها از اسکنر استفاده خواهد شد تعیین کنید. اگرچه می‌توانید از یک ایمیل موجود استفاده کنید، توصیه می‌کنیم یک آدرس ایمیل اختصاصی تعیین کنید تا از ایمیل‌هایی که از اسکنر فرستاده می‌شوند متمایز باشد. بین 0 تا 255 نویسه با فرمت اسکی (0x20–0x7E) به جز برای : ( ) < > [ ] ; ¥ وارد کنید. نقطه «.» نمی تواند اولین نویسه باشد.	
SMTP Server Address	بین 0 تا 255 نویسه را با استفاده از A–Z a–z 0–9 وارد کنید. یا خط تیره (-). می توانید از فرمت IPv4 یا FQDN استفاده کنید.	
SMTP Server Port Number	عددی بین 1 تا 65535 وارد کنید.	
Secure Connection	روش اتصال ایمن را برای این سرور ایمیل مشخص کنید.	
	None	اگر **POP before SMTP** را در **Authentication Method** انتخاب کنید، روش اتصال روی **None** تنظیم می شود.
	SSL/TLS	این زمانی موجود است که **Authentication Method** روی **Off** یا **SMTP AUTH** تنظیم باشد.
	STARTTLS	این زمانی موجود است که **Authentication Method** روی **Off** یا **SMTP AUTH** تنظیم باشد.
Certificate Validation (فقط Web Config)	زمانی که این فعال باشد گواهی تأیید می شود. توصیه می‌کنیم آن را روی **Enable** تنظیم کنید اگر **Secure Connection** روی گزینه‌ای غیر از **None** تنظیم شده است.	

مورد	تنظیمات و توضیحات
POP3 Server Address	اگر **POP before SMTP** را به عنوان **Authentication Method** انتخاب می‌کنید، آدرس سرور POP3 را وارد کنید. می‌توانید بین 0 تا 255 نویسه را با استفاده از A–Z a–z 0–9 وارد کنید. می توانید از فرمت IPv4 یا FQDN استفاده کنید.
POP3 Server Port Number	هنگامی که **POP before SMTP** را انتخاب می‌کنید، روی **Authentication Method** تنظیم کنید. عددی بین 1 تا 65535 وارد کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

بررسی اتصال سرور ایمیل

1. منوی تست اتصال را انتخاب کنید.

❑ **هنگام تنظیم از Web Config:**

زبانه **Network** سپس > **Email Server** > **Connection Test** > **Start** را انتخاب کنید.

❑ **هنگام تنظیم از پانل کنترل:**

مسیر **تنظیم** > **تنظیمات شبکه** > **پیشرفته** > **سرور ایمیل** > **بررسی اتصال** را انتخاب کنید.

بررسی اتصال به سرور ایمیل شروع می شود.

2. نتایج تست را کنترل کنید.

❑ این تست زمانی موفق است که پیام **Connection test was successful.** ظاهر شود.

❑ اگر یک پیام خطا ظاهر شود، دستورات موجود در پیام را دنبال کنید تا خطا را برطرف کنید.

"مرجع های بررسی اتصال سرور ایمیل" در صفحه 44

مرجع های بررسی اتصال سرور ایمیل

پیام	علت
SMTP server communication error. Check the following. - Network Settings	این پیام زمانی ظاهر می‌شود که ❑ اسکنر به شبکه وصل نباشد ❑ سرور SMTP فعال نباشد ❑ ارتباط با سرور در حین تبادل اطلاعات قطع شود ❑ داده ناقص دریافت شود
POP3 server communication error. Check the following. - Network Settings	این پیام زمانی ظاهر می‌شود که ❑ اسکنر به شبکه وصل نباشد ❑ سرور POP3 فعال نباشد ❑ ارتباط با سرور در حین تبادل اطلاعات قطع شود ❑ داده ناقص دریافت شود

پیام	علت
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	این پیام زمانی ظاهر می‌شود که ❏ ارتباط با سرور DNS برقرار نشود ❏ تفکیک نام برای سرور SMTP ناموفق باشد
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	این پیام زمانی ظاهر می‌شود که ❏ ارتباط با سرور DNS برقرار نشود ❏ تفکیک نام برای یک سرور POP3 ناموفق باشد
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	این پیام زمانی ظاهر می‌شود که تایید هویت سرور SMTP ناموفق باشد.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	این پیام زمانی ظاهر می‌شود که تایید هویت سرور POP3 ناموفق باشد.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	این پیام طمانی ظاهر می‌شود که بخواهید با پروتکل‌های پشتیبانی نشده ارتباط برقرار کنید.
Connection to SMTP server failed. Change Secure Connection to None.	این پیام زمانی ظاهر می‌شود که ناسازگاری SMTP بین سرور و مشتری رخ بدهد، یا سرور از اتصال امن SMTP (اتصال SSL) پشتیبانی نکند.
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	این پیام زمانی ظاهر می‌شود که ناسازگاری SMTP بین سرور و مشتری رخ بدهد، یا سرور خواستار استفاده از اتصال SSL/TLS برای اتصال امن SMTP باشد.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	این پیام زمانی ظاهر می‌شود که ناسازگاری SMTP بین سرور و مشتری رخ بدهد، یا سرور خواستار استفاده از اتصال STARTTLS برای اتصال امن SMTP باشد.
The connection is untrusted. Check the following. - Date and Time	این پیام زمانی ظاهر می‌شود که تنظیم تاریخ و ساعت اسکنر نادرست باشد یا گواهی منقضی شده باشد.
The connection is untrusted. Check the following. - CA Certificate	این پیام زمانی ظاهر می‌شود که اسکنر فاقد گواهی ریشه متناظر با سرور باشد یا CA Certificate وارد نشده باشد.
The connection is not secured.	این پیام زمانی ظاهر می‌شود که گواهی کسب شده آسیب دیده باشد.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	این پیام زمانی ظاهر می‌شود که ناسازگاری روش تایید هویت بین سرور و مشتری رخ دهد. سرور از SMTP AUTH پشتیبانی می‌کند.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	این پیام زمانی ظاهر می‌شود که ناسازگاری روش تایید هویت بین سرور و مشتری رخ دهد. سرور از SMTP AUTH پشتیبانی نمی‌کند.
Sender's Email Address is incorrect. Change to the email address for your email service.	این پیام زمانی ظاهر می‌شود که نشانی ایمیل فرستنده معین نادرست باشد.
Cannot access the product until processing is complete.	این پیام زمانی ظاهر می‌شود که اسکنر مشغول باشد.

ایجاد یک پوشه اشتراک‌گذاری

یک پوشه شبکه در کامپیوترتان ایجاد کنید. کامپیوتر باید به همان شبکه‌ای که اسکنر متصل است وصل باشد.

روش تنظیم پوشه شبکه، بسته به محیط متفاوت است. این مثالی است از ایجاد یک پوشه شبکه در دسکتاپ یک کامپیوتر در محیط زیر.

- سیستم عامل: Windows 10
- محل ایجاد پوشه اشتراک گذاری: دسکتاپ
- مسیر پوشه: C:\Users\xxxx\Desktop\scan_folder\ (یک پوشه شبکه با نام «scan_folder» در دسکتاپ درست کنید)

1. در کامپیوتری که می‌خواهید پوشه شبکه را در آن ایجاد کنید، با یک حساب کاربری که اختیارات سرپرست را دارد وارد شوید.

نکته:
اگر نمی‌دانید کدام حساب کاربری اختیارات سرپرست را دارد، از سرپرست کامپیوترتان بپرسید.

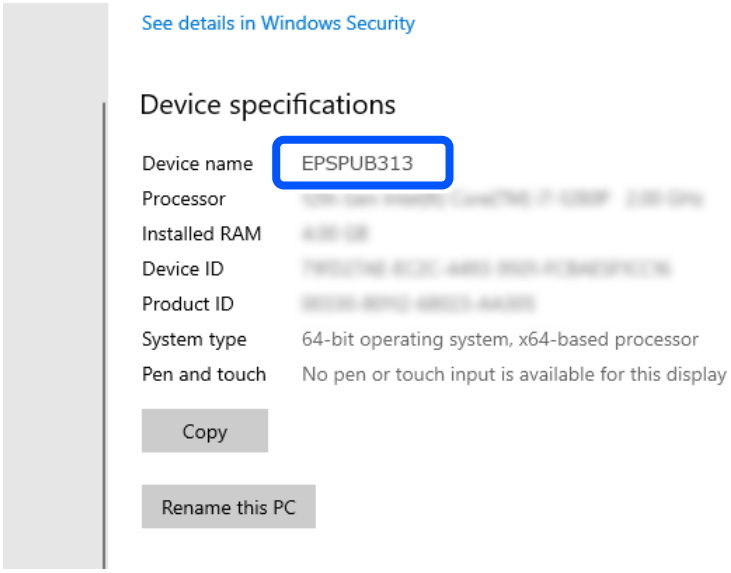
2. مطمئن شوید که نام دستگاه (نام کامپیوتر) شامل کاراکترهای دوبایتی نیست. روی دکمه شروع Windows کلیک کنید و سپس  **تنظیمات** > **سیستم** > **درباره** را انتخاب کنید.

نکته:
اگر کاراکترهای دوبایتی در نام دستگاه وجود داشته باشند، ذخیره کردن فایل ممکن است ناموفق باشد.

3. کنترل کنید که ردیف ظاهر شده در **مشخصات دستگاه** > **نام دستگاه** شامل هیچ کاراکتر دوبایتی نباشد.

اگر نام دستگاه فقط دارای کاراکترهای یک‌بایتی باشد، مشکلی نباید وجود داشته باشد. صفحه را ببندید.

مثال: EPSPUB313



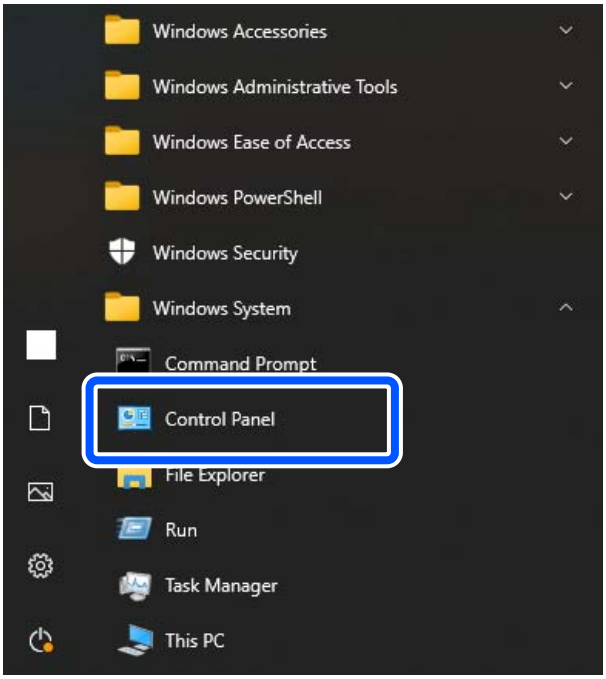
مهم:

اگر نام دستگاه شامل کاراکترهای دوبایتی باشد، از کامپیوتری استفاده کنید که از کاراکترهای دوبایتی استفاده نمی‌کند یا نام دستگاه را عوض کنید.

اگر باید نام دستگاه را عوض کنید، حتما قبلا با سرپرست کامپیوترتان کنترل کنید، چون ممکن است بر مدیریت کامپیوتر و دسترسی به منابع تاثیر بگذارد.

سپس تنظیمات کامپیوترتان را کنترل کنید.

4. روی دکمه شروع Windows کلیک کنید و سپس **سیستم** > **Windowsپانل کنترل** را انتخاب کنید.



5. در پانل کنترل، روی **شبکه و اینترنت** > **شبکه و مرکز اشتراک‌گذاری** > **تنظیمات پیشرفته اشتراک‌گذاری را تغییر دهید** کلیک کنید.

پروفایل شبکه نمایش داده می‌شود.

6. مطمئن شوید که **اشتراک‌گذاری فایل و چاپگر را روشن کنید** در **اشتراک‌گذاری فایل و چاپگر** برای پروفایل شبکه (پروفایل جاری) انتخاب می‌شود.

در صورتی که از قبل انتخاب شده است، روی **لغو** کلیک کنید و پنجره را ببندید.

وقتی تنظیمات را تغییر دادید، روی **ذخیره تنظیمات** کلیک کنید و پنجره را ببندید.

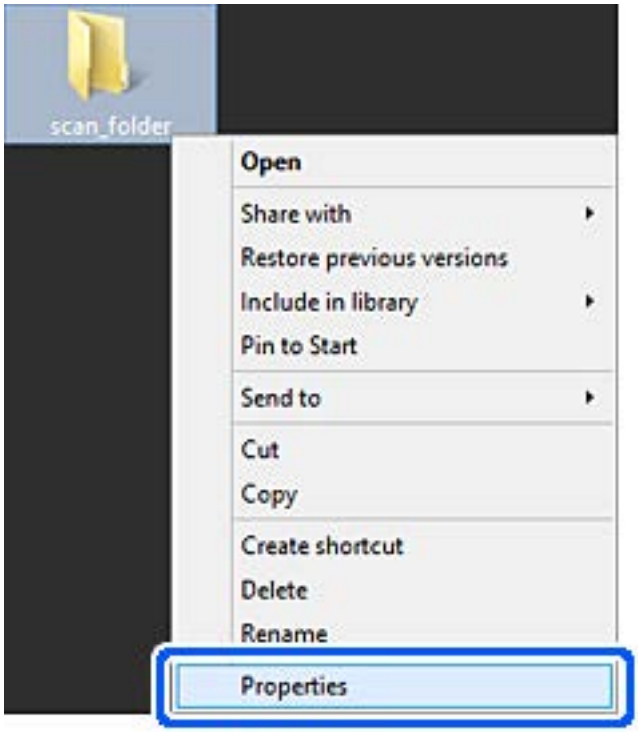
سپس یک پوشه شبکه ایجاد کنید.

7. یک پوشه در دسکتاپ خود ایجاد و نام‌گذاری کنید.

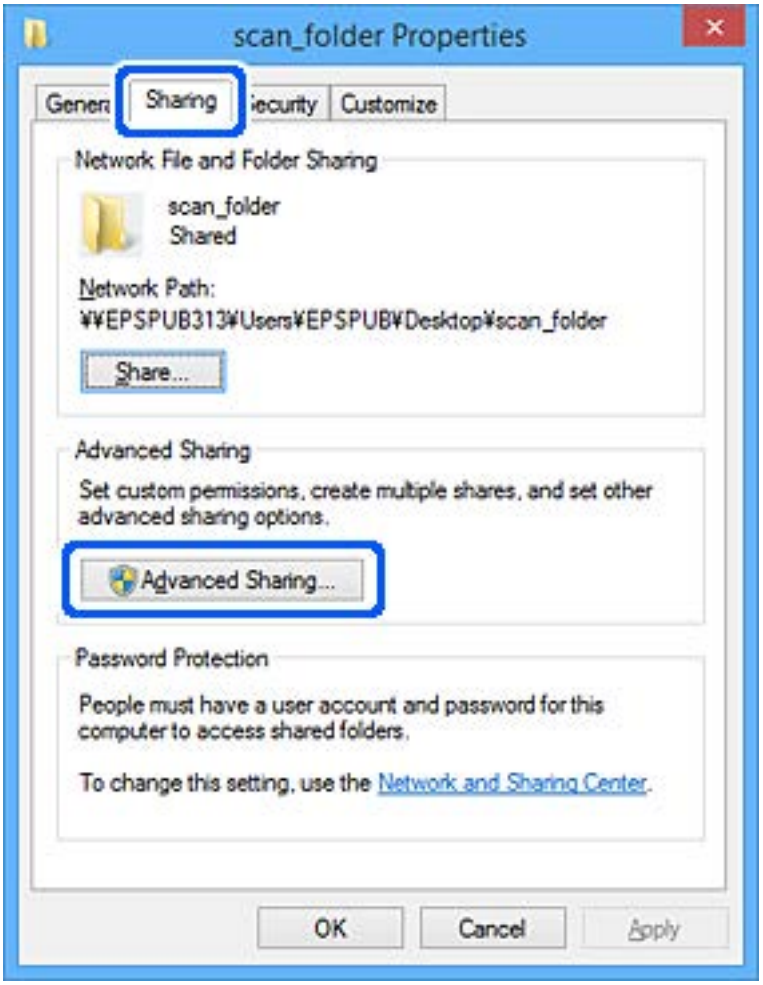
نام پوشه را با 1 تا 12 نویسه الفبایی عددی وارد کنید. در صورتی که تعداد نویسه‌ها از 12 مورد فراتر برود، بسته به سیستم شما ممکن است قادر به دسترسی به پوشه نباشید.

مثال: scan_folder

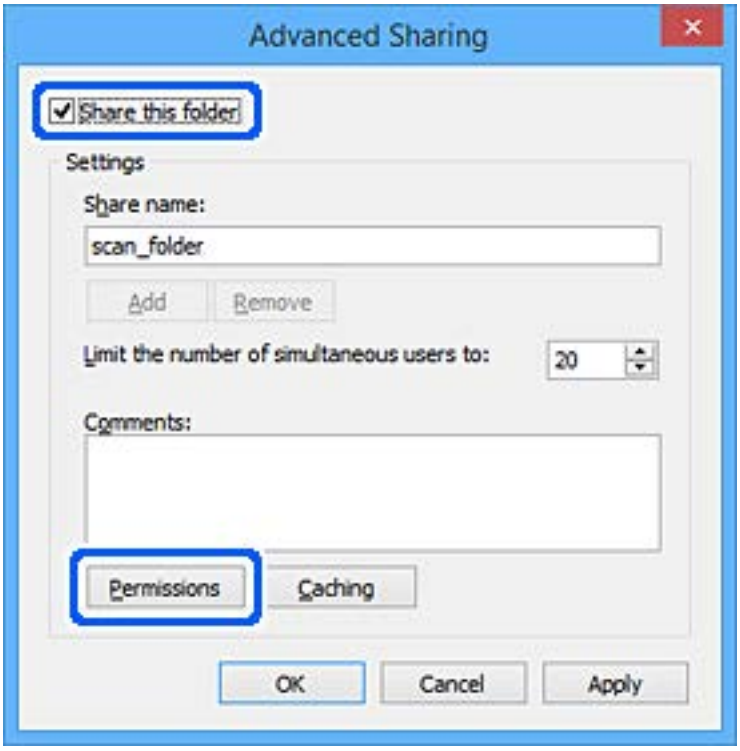
8. روی پوشه کلیک راست کرده و سپس **ویژگی ها** را انتخاب کنید.



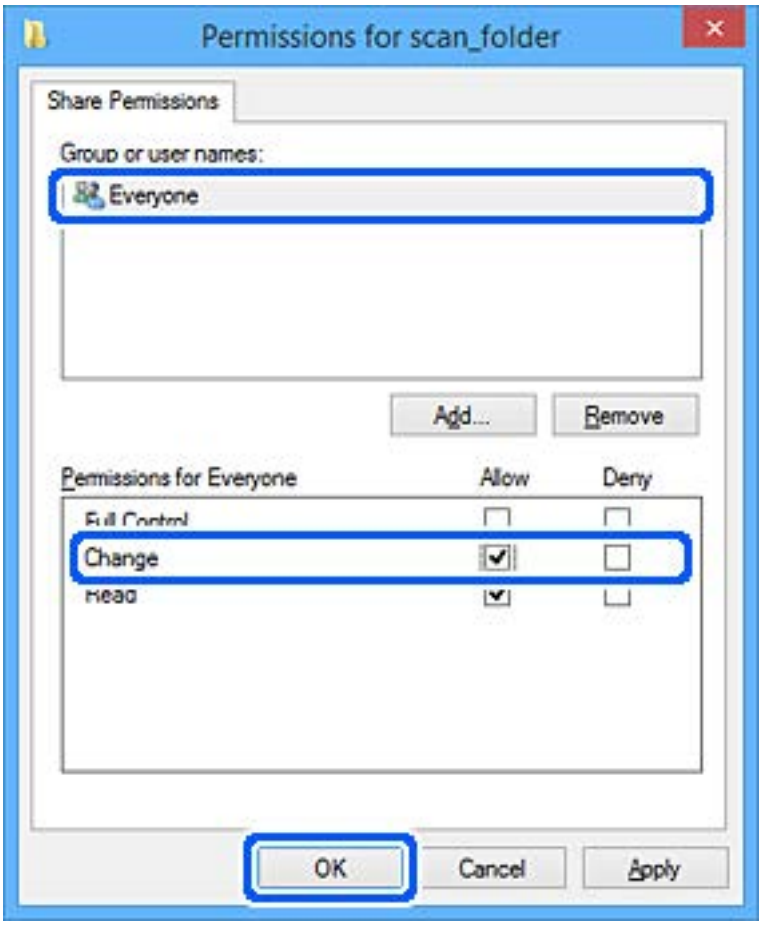
9. روی **اشتراک گذاری پیشرفته** در زبانه **اشتراک گذاری** کلیک کنید.



10. گزینه **اشتراک گذاری این پوشه** را انتخاب کنید و سپس روی **مجوزها** کلیک کنید.



11. گزینه **همه** در قسمت **نام کاربران یا گروه ها** را انتخاب کنید و سپس گزینه **اجازه دادن** در قسمت **تغییر** را برگزینید و روی **OK** کلیک کنید.

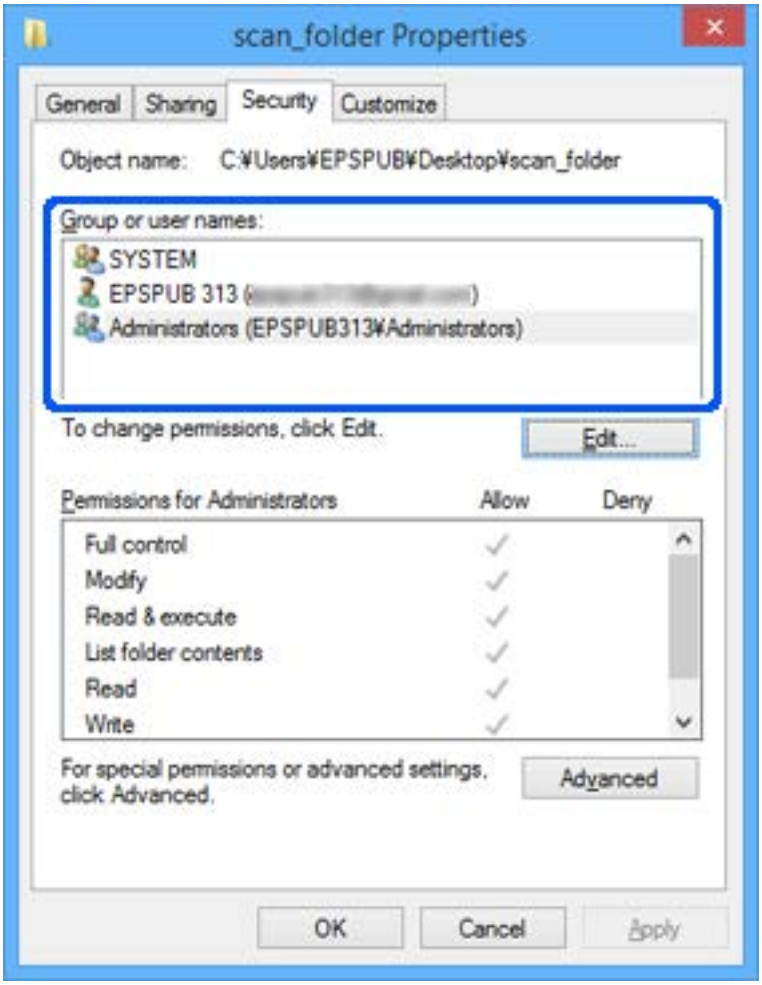


12. روی **OK** کلیک کنید تا صفحه را ببندید. و به پنجره «ویژگی‌ها» برگردید.

نکته:

می‌توانید کنترل کنید کدام گروه‌ها یا کاربران به پوشه شبکه در زبانه **امنیت** > **نام گروه یا کاربران** دسترسی دارند.

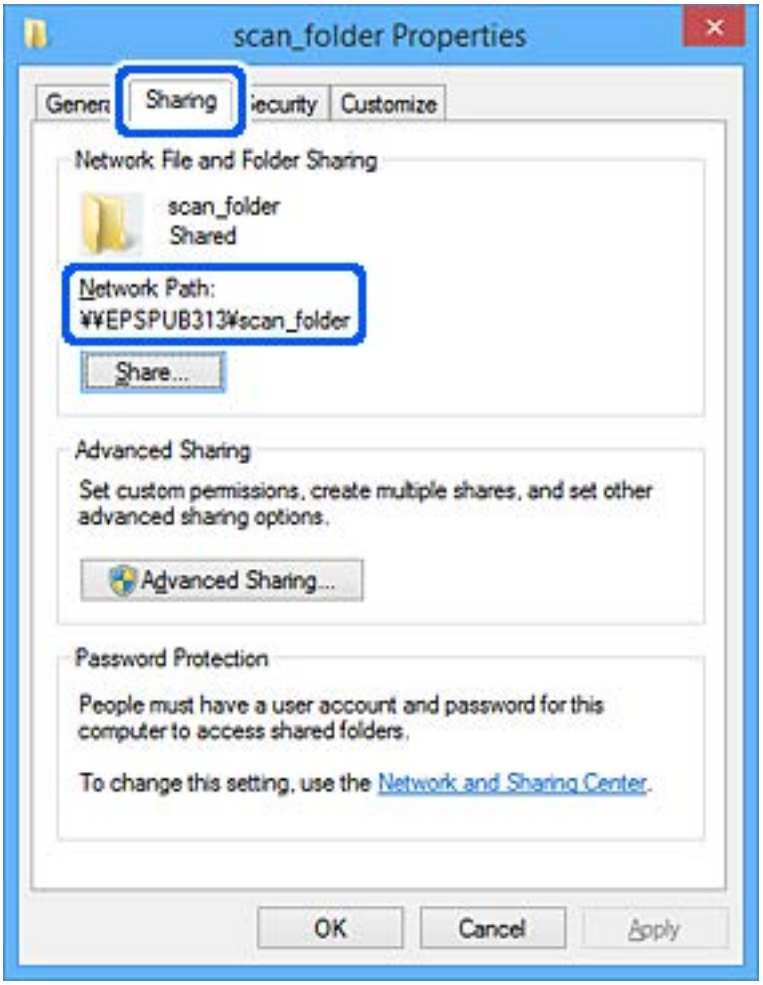
مثال: هنگامی که کاربر وارد کامپیوتر شده و سرپرستان نیز می‌توانند به پوشه شبکه دسترسی داشته باشند



13. زبانه **اشتراک گذاری** را انتخاب کنید.

مسیر شبکه مربوط به پوشه شبکه نمایش داده می‌شود. این مسیر هنگام ثبت در لیست مخاطبین اسکنر شما استفاده می شود. لطفاً آن را یادداشت کنید.

مثال: \\EPSPUB313\scan_folder\



14. برای بستن پنجره، روی **بستن** یا **تایید** کلیک کنید.

این کار، ایجاد یک پوشه شبکه را تکمیل می‌کند.

در دسترس قرار دادن مخاطبین

ثبت کردن مقصدها در لیست مخاطبین اسکنر به شما اجازه می‌دهد تا هنگام اسکن کردن به راحتی وارد مقصد شوید.

شما می‌توانید انواع مقصدهای زیر را در لیست مخاطبین ثبت کنید. در مجموع تا 300 ورودی را می‌توانید ثبت کنید.

نکته:

همچنین می‌توانید از سرور *LDAP* (جستجوی *LDAP*) برای ورود به مقصد استفاده کنید.

ایمیل	مقصد برای ایمیل. قبل از هر چیز باید تنظیمات سرور ایمیل را پیکربندی کنید.
پوشه شبکه	مقصد برای داده‌های اسکن. باید از قبل پوشه شبکه را آماده کنید.

اطلاعات مرتبط

"همکاری بین کاربران سرور LDAP و کاربران" در صفحه 59

مقایسه پیکربندی مخاطبین

سه ابزار برای پیکربندی مخاطبین اسکنر وجود دارد: Web Config، Epson Device Admin و پانل کنترل اسکنر. تفاوت‌های بین این سه ابزار در جدول زیر عنوان شده است.

ویژگی‌ها	Web Config*	Epson Device Admin	پانل کنترل اسکنر
ثبت یک مقصد	✓	✓	✓
ویرایش یک مقصد	✓	✓	✓
افزودن یک گروه	✓	✓	✓
ویرایش یک گروه	✓	✓	✓
حذف یک مقصد یا گروه‌ها	✓	✓	✓
حذف همه مقصدها	✓	✓	-
وارد کردن یک فایل	✓	✓	-
استخراج کردن به یک فایل	✓	✓	-

* برای اعمال تنظیمات به عنوان سرپرست به حساب خود وارد شوید.

ثبت یک مقصد برای مخاطبین با استفاده از Web Config

نکته:
همچنین می توانید مخاطبین را در پانل کنترل اسکنر ثبت کنید.

1. وارد Web Config شوید و زبانه **Scan** > **Contacts** را انتخاب کنید.
2. عددی را که می خواهید ثبت کنید انتخاب نمایید و سپس روی **Edit** کلیک کنید.
3. **Name** و **Index Word** را وارد کنید.
4. نوع مقصد را به عنوان گزینه **Type** انتخاب کنید.

   نکته:
   پس از پایان یافتن فرآیند ثبت نمی توانید گزینه ***Type*** را تغییر دهید. اگر بخواهید نوع را تغییر دهید، باید مقصد را حذف و دوباره ثبت کنید.
5. مقداری برای هر گزینه وارد کنید و روی **Apply** کلیک کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

موارد تنظیم مقصد

موارد	تنظیمات و توضیحات
تنظیمات عمومی	
Name	نامی را که باید در مخاطبین ظاهر شود با حداکثر 30 نویسه یونیکد (UTF-16) وارد کنید. اگر نمی‌خواهید این قسمت را مشخص کنید، خالی بگذارید.
Index Word	نام موردنظرتان را با استفاده از 30 نویسه یا کمتر در قالب یونیکد (UTF-16) وارد کنید تا مخاطبین در پانل کنترل اسکنر جستجو شوند. اگر نمی‌خواهید این قسمت را مشخص کنید، خالی بگذارید.
Type	نوع نشانی‌ای را که می‌خواهید ثبت کنید انتخاب کنید.
Assign to Frequent Use	برای تنظیم نشانی ثبت‌شده به‌عنوان نشانی پرکاربرد انتخاب کنید. در صورت تنظیم کردن به‌عنوان نشانی پرکاربرد، در صفحه بالایی اسکن نمایش داده می‌شود و می‌توانید مقصد را بدون نمایش مخاطبین مشخص کنید.
Email	
Email Address	بین 1 تا 255 نویسه را با استفاده از A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @ وارد کنید.
Network Folder (SMB)	
Save to	\\«مسیر پوشه» مکان پوشه هدف را با 1 تا 253 نویسه یونیکد (UTF-16) بدون «\\» وارد کنید. مسیر شبکه نمایش‌یافته در صفحه ویژگی‌های پوشه را وارد کنید. برای کسب اطلاعات بیشتر درباره تنظیم مسیر شبکه، بخش زیر را ببینید. "ایجاد یک پوشه اشتراک‌گذاری" در صفحه 45
User Name	نام کاربری برای دسترسی به پوشه شبکه را با حداکثر 30 نویسه یونیکد (UTF-16) وارد کنید. هرچند، نباید از نویسه‌های کنترلی (0x00 تا 0x1f، 0x7F) استفاده کنید.
Password	رمز عبور برای دسترسی به پوشه شبکه را با 0 تا 20 نویسه با قالب یونیکد (UTF-16) وارد کنید. هرچند، نباید از نویسه‌های کنترلی (0x00 تا 0x1f، 0x7F) استفاده کنید.
FTP	
Secure Connection	FTP یا FTPS را مطابق با پروتکل انتقال فایلی که سرور FTP پشتیبانی می‌کند انتخاب کنید. گزینه **FTPS** را انتخاب کنید تا به اسکنر اجازه دهید با معیارهای امنیتی ارتباط برقرار کند.
Save to	نام سرور را با 1 تا 253 نویسه در قالب یونیکد (UTF-16) بدون «ftp://:» یا «ftps://:» وارد کنید.
User Name	نام کاربری برای دسترسی به سرور FTP را با حداکثر 30 نویسه یونیکد (UTF-16) وارد کنید. هرچند، نباید از نویسه‌های کنترلی (0x00 تا 0x1f، 0x7F) استفاده کنید. اگر سرور اتصالات بی‌نام را مجاز بداند، باید نام کاربری مانند Anonymous و FTP وارد کنید. اگر نمی‌خواهید این قسمت را مشخص کنید، خالی بگذارید.
Password	رمز عبور برای دسترسی به سرور FTP را با 0 تا 20 نویسه در قالب یونیکد (UTF-16) وارد کنید. هرچند، نباید از نویسه‌های کنترلی (0x00 تا 0x1f، 0x7F) استفاده کنید. اگر نمی‌خواهید این قسمت را مشخص کنید، خالی بگذارید.
Connection Mode	حالت اتصال را از منو انتخاب کنید. اگر دیوار آتشی بین اسکنر و سرور FTP تنظیم شده است، **Passive Mode** را انتخاب کنید.
Port Number	شماره درگاه سرور FTP را از 1 تا 65535 وارد کنید.

موارد	تنظیمات و توضیحات
Certificate Validation	زمانی که این گزینه فعال باشد، گواهی سرور FTP تأیید می‌شود. این گزینه زمانی موجود است که **FTPS** برای **Secure Connection** انتخاب شده باشد. برای انجام دادن تنظیمات، لازم است CA Certificate را به اسکنر وارد کنید.
*SharePoint(WebDAV)	
Secure Connection	HTTP یا HTTPS را مطابق با پروتکل انتقال فایلی که سرور پشتیبانی می‌کند انتخاب کنید. گزینه **HTTPS** را انتخاب کنید تا به اسکنر اجازه دهید با معیارهای امنیتی ارتباط برقرار کند.
Save to	نام سرور را با 1 تا 253 نویسه در قالب یونیکد (UTF-16) بدون «http://:» یا «https://:» وارد کنید.
User Name	نام کاربری برای دسترسی به سرور را با حداکثر 30 نویسه یونیکد (UTF-16) وارد کنید. هرچند، نباید از نویسه‌های کنترلی (0x00 تا 0x1f، 0x7F) استفاده کنید. اگر نمی‌خواهید این قسمت را مشخص کنید، خالی بگذارید.
Password	رمز عبور برای دسترسی به سرور را با 0 تا 20 نویسه در قالب یونیکد (UTF-16) وارد کنید. هرچند، نباید از نویسه‌های کنترلی (0x00 تا 0x1f، 0x7F) استفاده کنید. اگر نمی‌خواهید این قسمت را مشخص کنید، خالی بگذارید.
Certificate Validation	زمانی که این گزینه فعال باشد، گواهی سرور تأیید می‌شود. این گزینه زمانی موجود است که **HTTPS** برای **Secure Connection** انتخاب شده باشد. برای انجام دادن تنظیمات، لازم است CA Certificate را به اسکنر وارد کنید.
Proxy Server	انتخاب کنید که آیا می‌خواهید از یک سرور پروکسی استفاده کنید یا خیر.

* SharePoint Online هنگام اسکن کردن به پوشه شبکه از پانل کنترل اسکنر پشتیبانی نمی‌شود.

اگر می‌خواهید تصویر اسکن‌شده را در SharePoint Online ذخیره کنید، از Document Capture Pro پس از نصب SharePoint Online Connector استفاده کنید. برای اطلاع از جزئیات، به دفترچه راهنمای Document Capture Pro مراجعه کنید.

https://support.epson.net/dcp/

ثبت مقصدها به عنوان گروه از طریق Web Config

اگر نوع مقصد روی **Email** تنظیم شده باشد، می توانید مقصدها را به عنوان گروه ثبت کنید.

1. وارد Web Config شوید و زبانه **Scan** > **Contacts** را انتخاب کنید.
2. عددی را که می خواهید ثبت کنید انتخاب نمایید و سپس روی **Edit** کلیک کنید.
3. از **Type** یک گروه انتخاب کنید.
4. روی **Select** مربوط به **Contact(s) for Group** کلیک کنید.
   مقصدهای موجود نمایش داده می شود.
5. مقصدهایی را که می خواهید در گروه ثبت شوند انتخاب کنید و روی **Select** کلیک کنید.
6. **Name** و **Index Word** را وارد کنید.
7. انتخاب کنید که آیا گروه ثبت شده را به گروه پرکاربرد تخصیص می دهید یا خیر.
   نکته:
   مقصدها را می توان در چندین گروه ثبت کرد.
8. روی **Apply** کلیک کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

پشتیبان گیری و وارد کردن مخاطبین

با استفاده از Web Config یا سایر ابزارها می توانید از مخاطبین نسخه پشتیبان تهیه کرده و آنها را وارد کنید.

در رابطه با Web Config، می توانید با استخراج تنظیمات اسکنر که شامل مخاطبین نیز می شود، از مخاطبین نسخه پشتیبان تهیه کنید. فایل استخراج شده قابل ویرایش نمی باشد زیرا به صورت یک فایل دودویی استخراج می شود.

هنگام وارد کردن تنظیمات اسکنر به اسکنر، مخاطبین جاگذاری می شوند.

در رابطه با Epson Device Admin، تنها مخاطبین را می توان از طریق صفحه مشخصات دستگاه استخراج کرد. همچنین، اگر موارد مرتبط با امنیت را استخراج نکنید، می توانید مخاطبین استخراج شده را ویرایش کرده و آنها را وارد کنید زیرا این را می توان به صورت یک فایل SYLK یا CSV ذخیره کرد.

وارد کردن مخاطبین از طریق Web Config

اگر چاپگری دارید که اجازه می دهد از مخاطبین نسخه پشتیبان تهیه کنید و با اسکنر جاری سازگار است، قادر خواهید بود به راحتی مخاطبین را با وارد کردن فایل پشتیبان ثبت کنید.

نکته:
برای مشاهده دستورالعمل های تهیه نسخه پشتیبان از مخاطبین اسکنر، دفترچه راهنمای ارائه شده به همراه اسکنر را مشاهده کنید.

برای وارد کردن مخاطبین به این اسکنر مراحل زیر را طی کنید.

1. به بخش Web Config وارد شوید و **Device Management** > **Export and Import Setting Value** > **Import** را انتخاب کنید.
2. فایل پشتیبان که در **File** ایجاد کرده اید را انتخاب کنید، رمز عبور را وارد کنید و سپس روی **Next** کلیک کنید.
3. کادر علامت گذاری **Contacts** را انتخاب کرده و سپس روی **Next** کلیک کنید.

تهیه نسخه پشتیبان از مخاطبین با استفاده از Web Config

در صورت اشکال در کارکرد اسکنر، ممکن است داده های مخاطبین حذف شوند. توصیه می کنیم در هنگام به روز رسانی داده ها، از آنها پشتیبان گیری کنید. Epson در مورد از دست دادن هر نوع داده، برای پشتیبان گیری یا بازیابی داده و یا تنظیمات حتی در طول دوره ضمانت مسئولیتی ندارد.

با استفاده از Web Config، می توانید از داده های تماس ذخیره شده در اسکنر در رایانه نسخه پشتیبان تهیه کنید.

1. وارد Web Config شوید و سپس زبانه **Device Management** > **Export and Import Setting Value** > **Export** را انتخاب کنید.
2. کادر علامت گذاری **Contacts** در زیر دسته **Scan** را انتخاب کنید.
3. برای رمزنگاری فایل استخراج شده، رمز عبور وارد کنید.
   برای وارد کردن فایل به رمز عبور نیاز دارید. اگر نمی خواهید فایل را رمزنگاری کنید، اینجا را خالی بگذارید.
4. روی **Export** کلیک کنید.

استخراج و ثبت گروهی مخاطبین با استفاده از ابزار

در صورت استفاده از Epson Device Admin، قادر خواهید بود از مخاطبین نسخه پشتیبان تهیه کرده و فایل های استخراج شده را ویرایش نمایید و سپس آنها را یکجا ثبت کنید.

این قابلیت در مواردی به کار می آید که در نظر دارید فقط از مخاطبین نسخه پشتیبان تهیه کنید یا اسکنر را تعویض نمایید و مخاطبین را از دستگاه قدیمی به دستگاه جدید انتقال دهید.

استخراج کردن مخاطبین

اطلاعات مخاطبین را در یک فایل ذخیره کنید.

فایل های ذخیره شده با قالب SYLK یا csv را می توانید با استفاده از برنامه های صفحه گسترده یا ویرایشگر متن ویرایش نمایید. شما می توانید پس از حذف یا افزودن اطلاعات، همه را با هم ثبت کنید.

اطلاعاتی که موارد امنیتی مانند رمز عبور و اطلاعات شخصی را در بردارند را می توان به صورت یک فایل دودویی حفاظت شونده با رمز عبور ذخیره کرد. شما نمی توانید فایل را ویرایش کنید. این را می توان به عنوان فایل پشتیبان اطلاعاتی که شامل موارد امنیتی هستند، استفاده کرد.

1. Epson Device Admin را آغاز کنید.
2. گزینه **Devices** را در منوی نوار کارهای جانبی انتخاب کنید.
3. دستگاه موردنظر خود برای پیکربندی را از لیست دستگاه ها انتخاب کنید.
4. روی **Device Configuration** در زبانه **Home** از منوی روبان کلیک کنید.

   پس از تنظیم رمز عبور سرپرست، رمز عبور را وارد کرده و روی **OK** کلیک کنید.
5. روی **Common** > **Contacts** کلیک کنید.
6. قالب استخراج را از طریق **Export** > **Export items** انتخاب کنید.

   ❑ All Items

   فایل دودویی رمزنگاری شده را استخراج کنید. زمان هایی که در نظر دارید موارد امنیتی مانند رمز عبور و اطلاعات شخصی شامل شوند را انتخاب کنید. شما نمی توانید فایل را ویرایش کنید. در صورت انتخاب آن، لازم است رمز عبور تنظیم کنید. روی **Configuration** کلیک کنید و یک رمز عبور با طول بین 8 تا 63 نویسه در ASCII وارد کنید. این رمز عبور برای وارد کردن فایل دودویی مورد نیاز می باشد.

   ❑ Items except Security Information

   فرمت SYLK یا فایل های csv را استخراج کنید. مواردی که در نظر دارید اطلاعات فایل استخراج شده قابل ویرایش باشند را انتخاب کنید.
7. روی **Export** کلیک کنید.
8. محل مورد نظر برای ذخیره فایل و نوع فایل را انتخاب کنید و سپس روی **Save** کلیک کنید.

   یک پیام تکمیل نشان داده می شود.
9. روی **OK** کلیک کنید.

   بررسی کنید آیا فایل در محل مشخص شده ذخیره می گردد.

وارد کردن مخاطبین

اطلاعات مخاطبین را از فایل وارد کنید.

شما می توانید فایل های ذخیره شده با قالب SYLK یا csv را وارد کنید یا از فایل دودویی که شامل موارد امنیتی است، نسخه پشتیبان تهیه کنید.

1. Epson Device Admin را آغاز کنید.
2. گزینه **Devices** را در منوی نوار کارهای جانبی انتخاب کنید.
3. دستگاه موردنظر خود برای پیکربندی را از لیست دستگاه ها انتخاب کنید.
4. روی **Device Configuration** در زبانه **Home** از منوی روبان کلیک کنید.
   پس از تنظیم رمز عبور سرپرست، رمز عبور را وارد کرده و روی **OK** کلیک کنید.
5. روی **Common** > **Contacts** کلیک کنید.
6. روی **Browse** در **Import** کلیک کنید.
7. فایلی را که می خواهید وارد کنید انتخاب کرده و سپس روی **Open** کلیک کنید.
   وقتی فایل دودویی را انتخاب می کنید، در قسمت **Password** همان رمزی که هنگام استخراج فایل تنظیم کرده بودید را وارد کنید.
8. روی **Import** کلیک کنید.
   صفحه تأییدیه نمایش داده می شود.
9. روی **OK** کلیک کنید.
   نتیجه تأیید نمایش داده می شود.
   - ❏ Edit the information read
     وقتی در نظر دارید اطلاعات را به صورت جداگانه ویرایش کنید، کلیک نمایید.
   - ❏ Read more file
     وقتی در نظر دارید چندین فایل را وارد کنید، کلیک نمایید.
10. روی **Import** و سپس **OK** در صفحه تکمیل وارد کردن کلیک کنید.
    به صفحه مشخصات دستگاه برگردید.
11. روی **Transmit** کلیک کنید.
12. روی **OK** در پیام تأییدیه کلیک کنید.
    تنظیمات به اسکنر ارسال می شوند.
13. در صفحه تکمیل ارسال، روی **OK** کلیک کنید.
    اطلاعات چاپگر به روز می شوند.
    مخاطبین را از طریق Web Config یا پانل کنترل اسکنر باز کنید و سپس بررسی کنید مخاطبین به روز هستند.

همکاری بین کاربران سرور LDAP و کاربران

هنگام همکاری با سرور LDAP، می توانید اطلاعات آدرس ثبت شده در سرور LDAP را به عنوان مقصد ایمیل ثبت کنید.

پیکربندی سرور LDAP

برای استفاده از اطلاعات سرور LDAP، اسکنر را در آن ثبت کنید.

1. وارد Web Config شوید و زبانه **Network** > **LDAP Server** > **Basic** را انتخاب کنید.
2. برای هر مورد یک مقدار وارد کنید.
3. **OK** را انتخاب کنید.

تنظیمات انتخاب شده نمایش داده می شود.

گزینه های تنظیم سرور *LDAP*

موارد	تنظیمات و توضیحات
Use LDAP Server	گزینه **Use** یا **Do Not Use** را انتخاب کنید.
LDAP Server Address	نشانی سرور LDAP را وارد کنید. 1 تا 255 نویسه را در قالب IPv4، IPv6 یا FQDN وارد کنید. برای قالب FQDN، می توانید از نویسه های الفبایی-عددی اسکی ASCII (0x20–0x7E) و «-» به جز در ابتدا و انتهای نشانی استفاده کنید.
LDAP server Port Number	شماره درگاه سرور LDAP را از 1 تا 65535 وارد کنید.
Secure Connection	روش تأیید اعتبار هنگام دسترسی اسکنر به سرور LDAP را تعیین کنید.
Certificate Validation	وقتی این گزینه فعال باشد، اعتبار گواهی سرور LDAP تأیید می شود. ما توصیه می کنیم این روی **Enable** تنظیم باشد. برای تنظیم آن، لازم است **CA Certificate** به اسکنر وارد شود.
Search Timeout (sec)	مدت زمان جستجو پیش از وقوع وقفه را از 5 تا 300 وارد کنید.
Authentication Method	یکی از روش ها را انتخاب کنید. اگر **Kerberos Authentication** را انتخاب کرده اید، برای اعمال تنظیمات موردنظر برای Kerberos، گزینه **Kerberos Settings** را انتخاب کنید. برای انجام Kerberos Authentication، شرایط زیر ضروری می باشند. ❑ اسکنر و سرور DNS می توانند ارتباط برقرار کنند. ❑ زمان اسکنر، سرور KDC و سرور مورد نیاز برای تأیید اعتبار (سرور LDAP، سرور SMTP، سرور File) همگام می شوند. ❑ وقتی سرور خدمات به عنوان آدرس IP تخصیص داده می شود، FQDN سرور خدمات در سرور DNS متضاد با منطقه جستجو ثبت می شود.
Kerberos Realm to be Used	اگر **Kerberos Authentication** را برای **Authentication Method** انتخاب کنید، باید محدوده Kerberos مورد نظر را انتخاب کنید.
Administrator DN / User Name	نام کاربر سرور LDAP را با حداکثر 128 نویسه یونیکد (UTF-8) وارد کنید. استفاده از نویسه های کنترلی مانند 0x00–0x1F و 0x7F مجاز نیست. این تنظیم در صورتی که **Anonymous Authentication** به عنوان **Authentication Method** انتخاب شود، کاربرد ندارد. اگر نمی خواهید این را مشخص کنید، خالی بگذارید.
Password	رمز عبور مربوط به تایید هویت سرور LDAP را با حداکثر 128 نویسه یونیکد (UTF-8) وارد کنید. استفاده از نویسه های کنترلی مانند 0x00–0x1F و 0x7F مجاز نیست. این تنظیم در صورتی که **Anonymous Authentication** به عنوان **Authentication Method** انتخاب شود، کاربرد ندارد. اگر نمی خواهید این را مشخص کنید، خالی بگذارید.

تنظیمات *Kerberos*

اگر **Kerberos Authentication** را برای **Authentication Method** مربوط به **LDAP Server** > **Basic** انتخاب می کنید، تنظیمات Kerberos زیر را از زبانه **Network** > **Kerberos Settings** اعمال کنید. می توانید تا 10 تنظیم را برای تنظیمات Kerberos ثبت کنید.

موارد	تنظیمات و توضیحات
Realm (Domain)	محدوده تایید هویت Kerberos را با حداکثر 255 نویسه اسکی ASCII (0x20–0x7E) وارد کنید. اگر نمی خواهید این گزینه را ثبت کنید، آن را خالی بگذارید.
KDC Address	نشانی سرور تایید هویت Kerberos را وارد کنید. حداکثر 255 نویسه را در قالب IPv4، IPv6 یا FQDN وارد کنید. اگر نمی خواهید این گزینه را ثبت کنید، آن را خالی بگذارید.
Port Number (Kerberos)	شماره درگاه سرور Kerberos را از 1 تا 65535 وارد کنید.

پیکربندی تنظیمات جستجوی سرور LDAP

وقتی تنظیمات جستجو را اعمال کنید، می توانید از آدرس ایمیل ثبت شده در سرور LDAP استفاده کنید.

1. وارد Web Config شوید و زبانه **Network** > **LDAP Server** > **Search Settings** را انتخاب کنید.
2. برای هر مورد یک مقدار وارد کنید.
3. روی **OK** کلیک کنید تا نتیجه تنظیم نمایش داده شود.
   تنظیمات انتخاب شده نمایش داده می شود.

گزینه های تنظیم جستجوی سرور *LDAP*

موارد	تنظیمات و توضیحات
Search Base (Distinguished Name)	اگر می خواهید دامنه ای اختیاری را جستجو کنید، باید نام دامنه سرور LDAP را مشخص کنید. از 0 تا 128 نویسه یونیکد (UTF-8) وارد کنید. اگر مشخصه اختیاری را جستجو نمی کنید، این قسمت را خالی بگذارید. نمونه دایرکتوری سرور محلی: dc=server, dc=local
Number of search entries	تعداد مدخل های جستجو را از 5 تا 500 مشخص کنید. عدد مشخص شده مدخل های جستجو شده ذخیره می و موقتاً نمایش داده می شود. حتی اگر تعداد مدخل های جستجو بیش از عدد مشخص شده باشد و پیام خطا ظاهر شود، می توان جستجو را انجام داد.
User name Attribute	نام مشخصه ای که باید در هنگام جستجوی نام کاربر نمایش داده شود، تعیین کنید. از 1 تا 255 نویسه یونیکد (UTF-8) وارد کنید. نویسه اول باید a–z یا A–Z باشد. مثال: cn، uid
User name Display Attribute	نام مشخصه ای که باید به عنوان نام کاربر نمایش داده شود، تعیین کنید. از 0 تا 255 نویسه یونیکد (UTF-8) وارد کنید. نویسه اول باید a–z یا A–Z باشد. مثال: cn، sn
Email Address Attribute	نام مشخصه ای که باید در هنگام جستجوی نشانی های ایمیل نمایش داده شود، تعیین کنید. ترکیبی از نویسه های بین 1 و 255 را با A–Z، a–z، 0–9 و - وارد کنید. نویسه اول باید a–z یا A–Z باشد. مثال: mail

موارد	تنظیمات و توضیحات
- Arbitrary Attribute 1 Arbitrary Attribute 4	می توانید دیگر مشخصه های اختیاری را برای جستجو مشخص کنید. از 0 تا 255 نویسه یونیکد (UTF-8) وارد کنید. نویسه اول باید a-z یا A-Z باشد. اگر نمی خواهید مشخصه های اختیاری را جستجو کنید، این قسمت را خالی بگذارید. مثال: o، ou

بررسی اتصال سرور LDAP

تست اتصال به سرور LDAP را با استفاده از مجموعه پارامتر موجود در **LDAP Server** > **Search Settings** انجام دهید.

1. وارد Web Config شوید و زبانه **Network** > **LDAP Server** > **Connection Test** را انتخاب کنید.
2. **Start** را انتخاب کنید.

آزمایش اتصال آغاز می شود. پس از آزمایش، گزارش بررسی نمایش داده می شود.

مراجع آزمایش اتصال سرور *LDAP*

پیام ها	توضیحات
Connection test was successful.	این پیام زمانی ظاهر می‌شود که ارتباط با سرور با موفقیت برقرار شود.
Connection test failed. Check the settings.	این پیام به دلایل زیر ظاهر می شود: ❑ نشانی سرور LDAP یا شماره درگاه نادرست است. ❑ وقفه رخ داده است. ❑ گزینه **Do Not Use** به عنوان حالت **Use LDAP Server** انتخاب شده است. ❑ اگر **Kerberos Authentication** به عنوان **Authentication Method** انتخاب شده است، تنظیماتی مانند **Realm (Domain)**, **KDC Address** و **Port Number (Kerberos)** نادرست باشند.
Connection test failed. Check the date and time on your product or server.	این پیام زمانی ظاهر می شود که اتصال به دلیل ناسازگاری تنظیمات زمان اسکنر و سرور LDAP قطع شود.
Authentication failed. Check the settings.	این پیام به دلایل زیر ظاهر می شود: ❑ **User Name** و/یا **Password** نادرست باشد. ❑ اگر **Kerberos Authentication** به عنوان **Authentication Method** انتخاب شود، ممکن است ساعت/تاریخ پیکربندی نشود.
Cannot access the product until processing is complete.	این پیام زمانی ظاهر می شود که اسکنر مشغول باشد.

راه‌اندازی AirPrint

به بخش Web Config بروید، زبانه **Network** و سپس گزینه **AirPrint Setup** را انتخاب کنید.

موارد	توضیحات
Bonjour Service Name	یک نام سرویس Bonjour با استفاده از متن ASCII (0x20–0x7E) و تا حداکثر 41 نویسه وارد کنید.
Bonjour Location	توضیحات مربوط به موقعیت اسکنر را با استفاده از متن Unicode (UTF-8) و تا حداکثر 127 بایت وارد کنید.
Wide-Area Bonjour	مشخص کنید که آیا از Wide-Area Bonjour استفاده شود یا خیر. در صورت استفاده از آن، لازم است اسکنر در سرور DNS ثبت باشند تا جستجوی اسکنر از طریق بخش شبکه موردنظر ممکن باشد.
Enable AirPrint	Bonjour و AirPrint (سرویس اسکن) را فعال می‌کند. این دکمه فقط زمانی در دسترس است که AirPrint غیرفعال باشد. **نکته:** اگر *AirPrint* غیرفعال است، *Mopria* اسکن از *Chromebooks*، *Windows* و برنامه *Mopria Scan* نیز غیرفعال می‌شود.

مشکلات هنگام تهیه اسکن شبکه

راهنمایی‌های حل کردن مشکلات

❑ بررسی پیام خطا

وقتی مشکلی رخ می‌دهد، ابتدا بررسی کنید آیا هیچ پیامی در رابطه با آن در پانل کنترل اسکنر یا صفحه درایور وجود دارد. اگر تنظیمات را به نحوی اعمال کنید که هنگام وقوع رویداد اعلان ایمیلی ارسال شود، بلافاصله می‌توانید از وضعیت آن مطلع شوید.

❑ بررسی وضعیت ارتباط

وضعیت ارتباطات رایانه سرور یا رایانه سرویس‌گیرنده را با استفاده از فرمانی مانند ping و ipconfig بررسی کنید.

❑ تست اتصال

جهت بررسی اتصال بین اسکنر و سرور ایمیل، تست اتصال را از اسکنر انجام دهید. همچنین، اتصال رایانه سرویس گیرنده به سرور را نیز بررسی کنید تا وضعیت ارتباطی آنها نیز ارزیابی شود.

❑ مقداردهی اولیه تنظیمات

اگر وضعیت تنظیمات و ارتباطات هیچ خطایی را نشان ندهد، ممکن است قادر باشید مشکلات را با غیرفعال کردن یا مقداردهی اولیه تنظیمات شبکه اسکنر و سپس تنظیم مجدد آنها برطرف نمایید.

عدم دسترسی به Web Config

آدرس IP به اسکنر تخصیص داده نشده است.

راهکارها

آدرس IP معتبر به اسکنر تخصیص داده نشده است. آدرس IP را از طریق پانل کنترل اسکنر پیکربندی کنید. می‌توانید از طریق پانل کنترل اسکنر، اطلاعات تنظیم فعلی را تأیید کنید.

مروگر وب از قدرت رمزنگاری برای SSL/TLS پشتیبانی نمی‌کند.

راهکارها

SSL/TLS دارای Encryption Strength است. شما می‌توانید Web Config را با استفاده از یک مرورگر وب که از رمزنگاری دسته‌ای پشتیبانی می‌کند، مطابق با آنچه در ادامه نشان داده شده است باز کنید. بررسی کنید آیا از یک مرورگر تحت پشتیبانی استفاده می‌کنید.

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

CA-signed Certificate منقضی شده است.

راهکارها

اگر مشکلی در رابطه با تاریخ انقضای گواهی وجود داشته باشد، هنگام اتصال به Web Config از طریق ارتباط SSL/TLS (https))، پیام "گواهی منقضی شده است" نمایش داده می‌شود. اگر پیام قبل از تاریخ انقضای آن ظاهر شود، دقت کنید تاریخ اسکنر به درستی پیکربندی شده باشد.

نام مشترک گواهی و اسکنر مطابقت ندارد.

راهکارها

اگر نام مشترک گواهی و اسکنر مطابقت نداشته باشد، هنگام اتصال به Web Config از طریق ارتباط SSL/TLS (https)، پیام «نام گواهی امنیتی مطابقت ندارد...» نمایش داده می شود. دلیل بروز این مشکل عدم مطابقت آدرس های IP زیر است.

- ❑ آدرس IP اسکنر وارد شده برای نام مشترک به منظور ایجاد یک Self-signed Certificate یا CSR
- ❑ آدرس IP وارد شده در مرورگر وب هنگام اجرای Web Config

در رابطه با Self-signed Certificate، گواهی را بروزرسانی کنید.

در رابطه با CA-signed Certificate، گواهی را مجدداً از اسکنر دریافت کنید.

تنظیمات سرور پروکسی آدرس محلی در مرورگر وب اعمال نشده‌اند.

راهکارها

وقتی تنظیمات اسکنر به گونه‌ای باشند که از یک سرور پروکسی استفاده نماید، مرورگر وب را به نحوی تنظیم کنید که از طریق سرور پروکسی به آدرس محلی متصل نشود.

- ❑ Windows:

گزینه **پانل کنترل** > **شبکه و اینترنت** > **گزینه‌های اینترنت** > **اتصالات** > **تنظیمات** > **LANسرور پراکسی** را انتخاب کنید و سپس پیکربندی کنید که از سرور پراکسی برای LAN (آدرس‌های محلی) استفاده نشود.

- ❑ Mac OS:

گزینه **ترجیحات سیستم** (یا **تنظیمات سیستم**) > **شبکه** > **پیشرفته** > **پراکسی ها** را انتخاب کنید و سپس آدرس محلی برای **نادیده گرفتن تنظیمات پراکسی برای این میزبان ها و دامنه ها** را ثبت کنید.

مثال:

192.168.1.*: آدرس محلی XXX.192.168.1، پوشش زیر شبکه 255.255.255.0

192.168.*.*: آدرس محلی 192.168.XXX.XXX، پوشش زیر شبکه 255.255.0.0

DHCP در تنظیمات رایانه غیرفعال شده است.

راهکارها

اگر DHCP برای دریافت آدرس IP به طور خودکار در رایانه غیرفعال شده باشد، امکان دسترسی به Web Config را نخواهید داشت. DHCP را فعال کنید.

مثال مربوط به Windows 10:

پانل کنترل را باز کرده و روی گزینه‌های **شبکه و اینترنت** > **مرکز شبکه و اشتراک‌گذاری** > **تغییر تنظیمات آداپتور** کلیک کنید. صفحه ویژگی‌های اتصال مورد استفاده خود و در ادامه صفحه ویژگی‌های مربوط به **پروتکل اینترنت نسخه 4 (TCP/IPv4)** یا **پروتکل اینترنت نسخه 6 (TCP/IPv6)** را باز کنید. در صفحه نمایش یافته بررسی کنید گزینه **دریافت خودکار آدرس IP** انتخاب شده باشد.

سفارشی کردن نمایشگر پانل کنترل

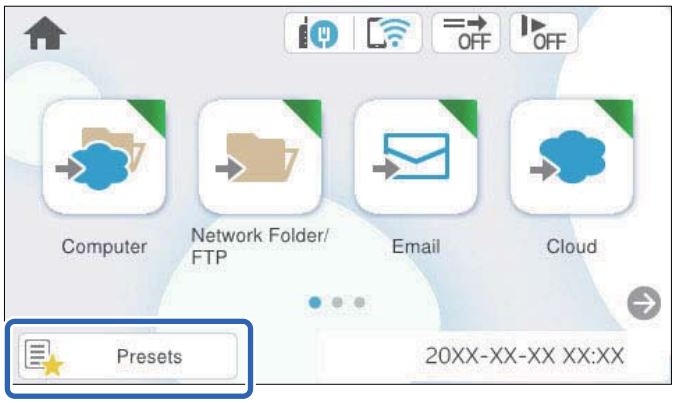
ثبت پیش‌تنظیمات

می توانید تنظیمات اسکن که اغلب استفاده می‌شوند را با گزینه **پیش‌تنظیمات** ثبت کنید. می‌توانید تا 48 مورد پیش‌تنظیم را ثبت کنید.

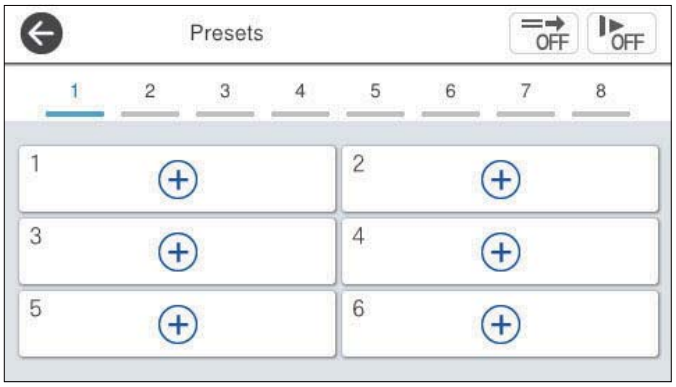
نکته:

- تنظیمات جاری را می‌توانید با انتخاب گزینه ★ در صفحه شروع اسکن ثبت کنید.
- می توانید ***Presets*** را در *Web Config* ثبت کنید.
  زبانه ***Scan*** > ***Presets*** را انتخاب کنید.
- اگر هنگام ثبت گزینه **ذخیره اسکن در رایانه** را انتخاب کنید قادر خواهید بود کار ایجاد شده را در بخش *Document Capture Pro* به عنوان ***Presets*** ثبت کنید. این تنها برای رایانه‌های متصل از طریق شبکه در دسترس می‌باشد. کار را از قبل در *Document Capture Pro* ثبت کنید.
- اگر عملکرد تأیید هویت فعال شود، تنها سرپرست می‌تواند ***Presets*** را ثبت نماید.

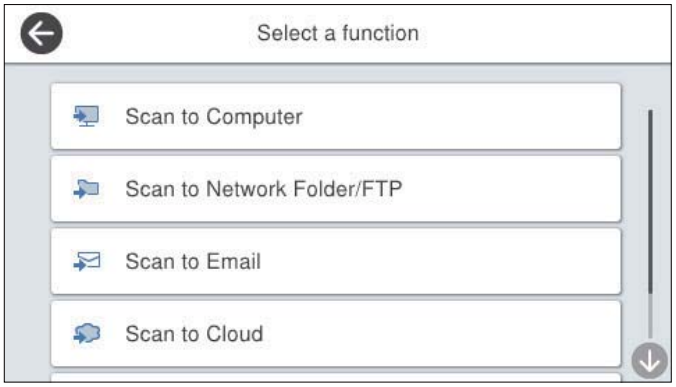
1. منوی **پیش‌تنظیمات** در صفحه اصلی پانل کنترل اسکنر را انتخاب کنید.



2. گزینه ⊕ را انتخاب کنید.



3. منوی مورد نظر برای ثبت یک تنظیم از پیش تعیین شده را انتخاب کنید.

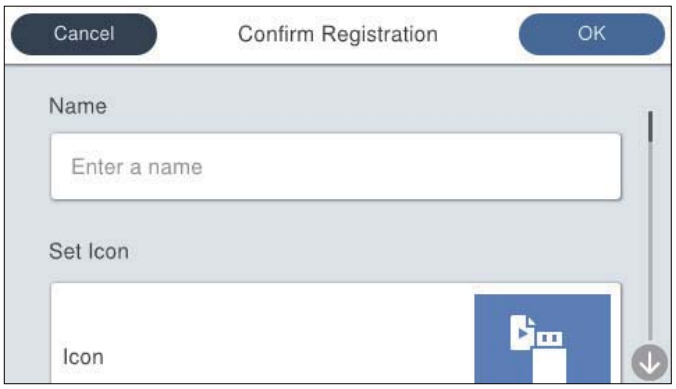


4. هر مورد را تنظیم کنید و سپس ☆+ را انتخاب کنید.

نکته:
وقتی گزینه **ذخیره اسکن در رایانه** را انتخاب می‌کنید، رایانه‌ای را که در آن *Document Capture Pro* نصب است انتخاب کنید و سپس یک کار ثبت شده را انتخاب نمایید. این تنها برای رایانه‌های متصل از طریق شبکه در دسترس می‌باشد.

5. تنظیمات از پیش تعیین شده را ایجاد کنید.

- ❑ **نام**: نام را تنظیم کنید.
- ❑ **تنظیم نماد**: تصویر و رنگ آیکن مدنظر جهت نمایش را تنظیم کنید.
- ❑ **تنظیم ارسال فوری**: بلافاصله با انتخاب تنظیمات از پیش تعیین شده، اسکن بدون تأیید شروع می‌شود.
- ❑ **فهرست مطالب**: تنظیمات اسکن را بررسی کنید.



6. گزینه **OK** را انتخاب کنید.

گزینه های منو پیش‌تنظیمات

تنظیمات از پیش تعیین شده را می توانید با انتخاب گزینه > در هر تنظیم از پیش تعیین شده تغییر دهید.

تغییر نام:

نام پیش‌تنظیم را تغییر می‌دهد.

تغییر نماد:

تصویر آیکن و رنگ پیش‌تنظیم را تغییر می دهد.

تنظیم ارسال فوری:

بلافاصله با انتخاب تنظیمات از پیش تعیین شده، اسکن بدون تأیید شروع می شود.

تغییر محل:

ترتیب نمایش تنظیمات از پیش تعیین شده را تغییر می‌دهد.

حذف:

مورد پیش‌تنظیم را حذف می‌کند.

افزودن یا حذف نماد در صفحه اصلی:

آیکن از پیش تعیین شده را اضافه کرده یا حذف می کند.

تأیید جزئیات:

تنظیمات یک مورد پیش‌تنظیم را ببینید. با انتخاب گزینه **استفاده از این تنظیمات**، مورد پیش‌تنظیم را بارگیری کنید.

ویرایش صفحه اصلی پانل کنترل

شما می‌توانید صفحه اصلی را با انتخاب گزینه **تنظیم** > **ویرایش صفحه اصلی** از پانل کنترل اسکنر شخصی‌سازی کنید.

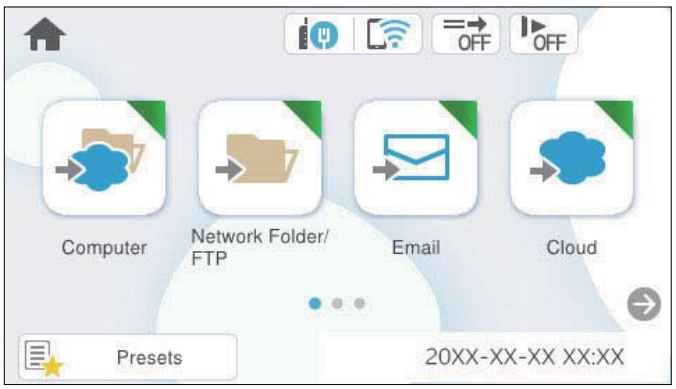
- صفحه‌بندی: شیوه نمایش آیکن‌های منو را تغییر می‌دهد.
"تغییر صفحه‌بندی صفحه اصلی" در صفحه 69
- افزودن نماد: آیکن‌ها را به تنظیمات **پیش‌تنظیمات** که ایجاد کرده‌اید اضافه می‌کند، یا آیکن‌های حذف شده از صفحه را بازیابی می‌کند.
"افزودن نماد" در صفحه 70
- حذف نماد: آیکن‌ها را از صفحه اصلی حذف می‌کند.
"حذف نماد" در صفحه 71
- جابجایی نماد: ترتیب نمایش آیکن‌ها را تغییر می‌دهد.
"جابجایی نماد" در صفحه 72
- بازیابی نمایشگر نماد پیش فرض: تنظیمات پیش‌فرض نشان داده شده در صفحه اصلی را بازگردانی می‌کند.

تغییر صفحه‌بندی صفحه اصلی

1. گزینه **تنظیم** > **ویرایش صفحه اصلی** > **صفحه‌بندی** را در پانل کنترل اسکنر انتخاب کنید.

2. گزینه **خط** یا **ماتریس** را انتخاب کنید.

خط:



ماتریس:

3. برای بازگشت و بررسی صفحه اصلی، را انتخاب کنید.

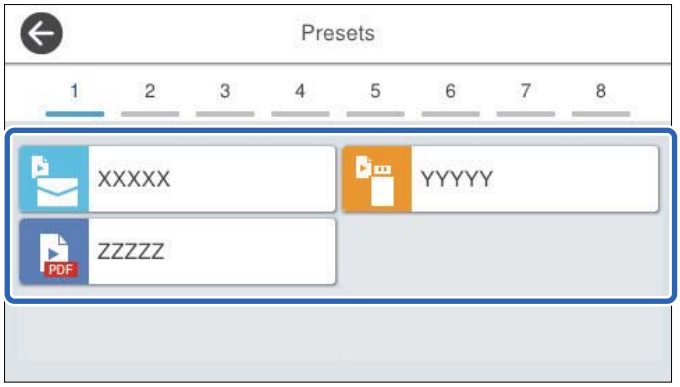
افزودن نماد

1. گزینه **تنظیم** > **ویرایش صفحه اصلی** > **افزودن نماد** را در پانل کنترل اسکنر انتخاب کنید.
2. گزینه **کارکرد** یا **پیش‌تنظیمات** را انتخاب کنید.

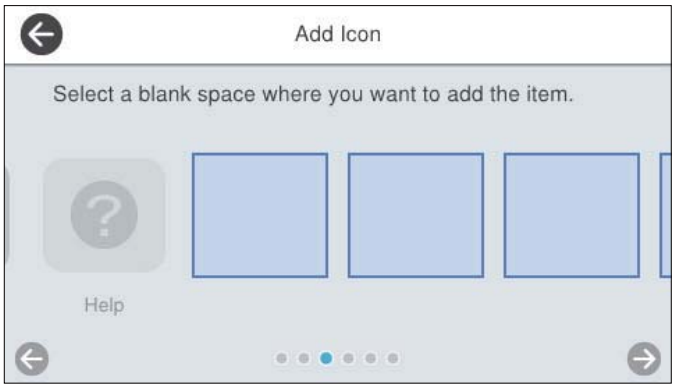
❑ کارکرد: عملکردهای پیش‌فرض نشان داده شده در صفحه اصلی را نشان می‌دهد.

❑ پیش‌تنظیمات: تنظیمات از پیش تنظیم شده را نشان می‌دهد.

3. قابلیت مدنظر خود را که می‌خواهید به صفحه اصلی اضافه کنید نشان دهید.



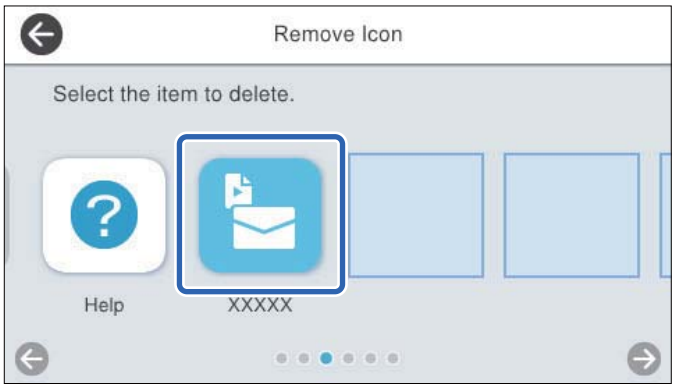
4. فضای خالی را که می‌خواهید در آن موردی اضافه کنید انتخاب کنید.
اگر می‌خواهید چندین آیکن اضافه کنید، مراحل 3 تا 4 را تکرار کنید.



5. برای بازگشت و بررسی صفحه اصلی، گزینه را انتخاب کنید.

حذف نماد

1. گزینه **تنظیم** > **ویرایش صفحه اصلی** > **حذف نماد** را در پانل کنترل اسکنر انتخاب کنید.
2. آیکن مورد نظر برای حذف را انتخاب کنید.



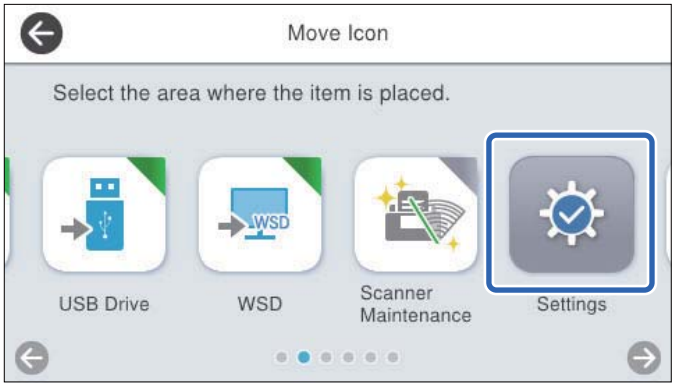
3. برای پایان دادن، گزینه **بله** را انتخاب کنید.
اگر می‌خواهید چندین آیکن را حذف کنید، مراحل 2 تا 3 را تکرار کنید.

4. برای بازگشت و بررسی صفحه اصلی، گزینه را انتخاب کنید.

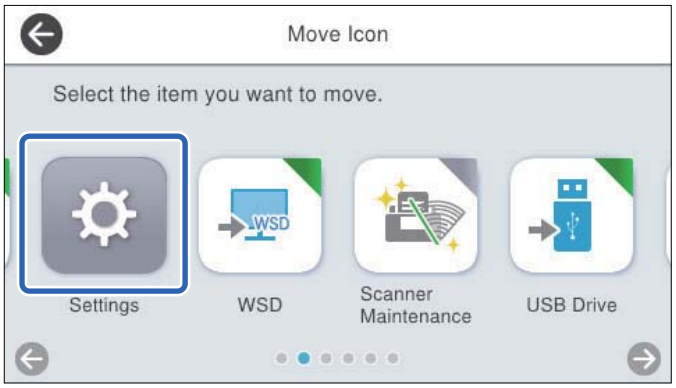
جابجایی نماد

1. گزینه **تنظیم** > **ویرایش صفحه اصلی** > **جابجایی نماد** را در پانل کنترل اسکنر انتخاب کنید.

2. آیکن مورد نظر برای جابجایی را انتخاب کنید.



3. چارچوب مقصد را دوباره انتخاب کنید.
اگر آیکن دیگری قبلاً در کادر مقصد تنظیم شده باشد، آیکن‌ها جایگزین می‌شوند.



4. برای بازگشت و بررسی صفحه اصلی، گزینه را انتخاب کنید.

تنظیمات امنیتی ابتدایی

معرفی امکانات امنیتی محصول

این بخش عملکرد امنیتی دستگاه‌های Epson را معرفی می‌کند.

نام قابلیت	نوع قابلیت	آنچه باید تنظیم شود	آنچه باید جلوگیری شود
پیکربندی رمز عبور سرپرست	تنظیمات سیستم، مانند تنظیم اتصال شبکه یا USB را قفل می کند.	سرپرست رمز عبور دستگاه را تنظیم می کند. تنظیمات یا تغییرات آنها را می توانید از طریق Web Config و همچنین پانل کنترل اسکنر انجام دهید.	مانع خواندن و تغییر دادن غیرمجاز اطلاعات ذخیره شده در دستگاه مانند شناسه، رمز عبور، تنظیمات شبکه و موارد مشابه می شود. همچنین، طیف گسترده ای از خطرهای امنیتی مانند نشت اطلاعات از محیط شبکه یا سیاست امنیتی را کاهش می دهد.
Access Control Settings	اگر با یک حساب کاربری که از قبل ثبت‌نام کرده‌اید وارد دستگاه شوید، می‌توانید از دستگاه استفاده کنید.	یک حساب کاربری ثبت کنید. می توانید تا 10 حساب کاربری را ثبت کنید.	محدودکردن کاربران از استفاده غیرمجاز از دستگاه جلوگیری می‌کند.
راه‌اندازی برای رابط خارجی	رابطی که به دستگاه وصل می شود را کنترل می کند.	اتصال USB به رایانه را فعال یا غیرفعال کنید.	اتصال USB رایانه: با ممنوع کردن اسکن بدون ورود به شبکه، مانع استفاده غیرمجاز از دستگاه می شود.

اطلاعات مرتبط

- "پیکربندی رمز عبور سرپرست" در صفحه 74
- "غیرفعال کردن رابط خارجی" در صفحه 82

تنظیمات سرپرست سیستم

پیکربندی رمز عبور سرپرست

وقتی رمز عبور سرپرست را تنظیم کنید، می‌توانید از تغییر تنظیمات مدیریت سیستم توسط کاربران جلوگیری کنید. مقادیر پیش‌فرض در زمان خرید تنظیم می‌شوند. در صورت لزوم، آنها را تغییر دهید.

نکته:

در بخش زیر، مقادیر پیش‌فرض برای اطلاعات سرپرست ارائه می‌شوند.

- نام کاربری (فقط برای *Web Config* استفاده می‌شود): هیچ‌کدام (خالی)
- رمز عبور: بستگی به برچسب چسبانده‌شده به محصول دارد.

  اگر برچسب «*PASSWORD*» به پشت چسبانده شده است، عدد *8* رقمی درج‌شده روی برچسب را وارد کنید. اگر برچسب «*PASSWORD*» چسبانده نشده است، شماره سریال روی برچسب چسبانده‌شده به پشت محصول را برای رمز عبور سرپرست اولیه وارد کنید.

برای تغییر رمز عبور سرپرست می‌توانید از Web Config، پانل کنترل اسکنر یا Epson Device Admin استفاده کنید. هنگام استفاده از Epson Device Admin، راهنمای کاربری یا راهنمای Epson Device Admin را ملاحظه کنید.

تغییر رمز عبور سرپرست با استفاده از Web Config

رمز عبور سرپرست را در Web Config تغییر دهید.

1. وارد Web Config شوید و زبانه **Product Security** > **Change Administrator Password** را انتخاب کنید.

2. اطلاعات ضروری را در **Current password**, **User Name**, **New Password** و **Confirm New Password** وارد کنید.

رمز عبور جدید باید 8 تا 20 نویسه داشته باشد و فقط شامل نویسه‌ها و نمادهای الفبایی-عددی تک‌بایتی باشد.

نکته:
در بخش زیر، مقادیر پیش‌فرض برای اطلاعات سرپرست ارائه می‌شوند.

- نام کاربری: هیچ‌کدام (خالی)
- رمز عبور: بستگی به برچسب چسبانده‌شده به محصول دارد.

اگر برچسب «*PASSWORD*» به پشت چسبانده شده است، عدد *8* رقمی درج‌شده روی برچسب را وارد کنید. اگر برچسب «*PASSWORD*» چسبانده نشده است، شماره سریال روی برچسب چسبانده‌شده به پشت محصول را برای رمز عبور سرپرست اولیه وارد کنید.

مهم:
حتماً رمز عبور سرپرستی را که تنظیم کرده‌اید به خاطر بسپارید. اگر رمز عبور خود را فراموش کنید، نمی‌توانید آن را بازنشانی کنید و باید از کارکنان خدمات درخواست کمک کنید.

3. **OK** را انتخاب کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

تغییر رمز عبور سرپرست از طریق پانل کنترل اسکنر

می‌توانید رمز عبور سرپرست را از طریق پانل کنترل اسکنر تغییر دهید.

1. گزینه **تنظیم** را در پانل کنترل اسکنر انتخاب کنید.
2. **سرپرست سیستم** > **تنظیمات سرپرست** را انتخاب کنید.
3. **رمز عبور سرپرست** > **تغییر** را انتخاب کنید.
4. رمز عبور فعلی خود را وارد کنید.

نکته:
رمز عبور سرپرست اولیه (پیش‌فرض) در زمان خرید، بسته به برچسب چسبانده‌شده روی محصول متفاوت است. اگر برچسب «*PASSWORD*» به پشت چسبانده شده است، عدد *8* رقمی درج‌شده روی برچسب را وارد کنید. اگر برچسب «*PASSWORD*» چسبانده نشده است، شماره سریال روی برچسب چسبانده‌شده به پشت محصول را برای رمز عبور سرپرست اولیه وارد کنید.

5. رمز عبور جدید خود را وارد کنید.

رمز عبور جدید باید 8 تا 20 نویسه داشته باشد و فقط شامل نویسه‌ها و نمادهای الفبایی-عددی تک‌بایتی باشد.

مهم:
حتماً رمز عبور سرپرستی را که تنظیم کرده‌اید به خاطر بسپارید. اگر رمز عبور خود را فراموش کنید، نمی‌توانید آن را بازنشانی کنید و باید از کارکنان خدمات درخواست کمک کنید.

6. رمز عبور جدید را مجدداً برای تأیید وارد کنید.

پیام تکمیل نشان داده می‌شود.

استفاده از تنظیم قفل برای پنل کنترل

برای قفل‌کردن پنل کنترل به‌منظور جلوگیری کاربران از تغییر موارد مرتبط با تنظیمات سیستم می‌توانید از گزینه تنظیم قفل استفاده کنید.

تنظیم تنظیم قفل از پانل کنترل

1. اگر در نظر دارید گزینه **تنظیم قفل** را پس از اینکه فعال شده است، لغو کنید، روی گزینه در گوشه بالا سمت راست صفحه اصلی برای ورود به سیستم در نقش سرپرست ضربه بزنید.

   در صورت غیرفعال بودن **تنظیم قفل** نمایش داده نمی‌شود. در صورتی که می‌خواهید این تنظیم را فعال کنید، به مرحله بعدی بروید.

2. گزینه **تنظیم** را انتخاب کنید.
3. مسیر **سرپرست سیستم** > **تنظیمات سرپرست** را انتخاب کنید.
4. گزینه **On** یا **Off** را به عنوان **تنظیم قفل** انتخاب کنید.

تنظیم تنظیم قفل از طریق Web Config

1. زبانه **Control Panel** > **Device Management** را انتخاب کنید.
2. گزینه **ON** یا **OFF** را برای **Panel Lock** انتخاب کنید.
3. روی **OK** کلیک کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

گزینه‌های تنظیم قفل روی منوی تنظیم

این لیست گزینه‌هایی است که در منوی **تنظیم** در پانل کنترل با تنظیم قفل قفل می‌شوند.

✓: باید قفل شود.

-: لازم نیست قفل شود.

منوی تنظیم	تنظیم قفل
تنظیمات اصلی	-

منوی تنظیم		تنظیم قفل
	روشنایی LCD	-
	صداها	-
	تایمر خواب	✓
	زمان‌سنج خاموش کردن	✓
	روشن کردن مستقیم	✓
	تاریخ / تنظیمات زمان	✓
	زبان/Language	✓/-*
	صفحه کلید (ممکن است بسته به منطقه خود، این ویژگی وجود نداشته باشد.)	-
	وقفه عملیات	✓
	اتصال رایانه از طریق USB	✓
تنظیمات اسکنر		-
	آهسته	-
	زمان توقف ورود دوتایی	✓
	عملکرد DFDS	-
	محافظت کاغذ	✓
	تشخیص کثیفی شیشه	✓
	تشخیص اولتراسونیک دو سند	✓
	پایان فرصت حالت تغذیه خودکار	✓
	تأیید گیرنده	✓
ویرایش صفحه اصلی		✓
	صفحه‌بندی	✓
	افزودن نماد	✓
	حذف نماد	✓
	جابجایی نماد	✓
	بازیابی نمایشگر نماد پیش فرض	✓
تنظیمات کاربر		✓

منوی تنظیم		تنظیم قفل
	پوشه شبکه/FTP	✓
	ایمیل	✓
	اینترنتی	✓
	درایو USB	✓
تنظیمات شبکه		✓
	نصب Wi-Fi	✓
	تنظیم LAN سیم دار	✓
	وضعیت شبکه	✓
	پیشرفته	✓
تنظیمات سرویس وب		✓
	خدمات اتصال Epson	✓
Document Capture Pro		-
	تغییر تنظیمات	✓
مدیر مخاطبان		-
	ثبت/حذف	✓/-*
	مکرر	-
	مشاهده گزینه ها	-
	گزینه های جستجو	-
سرپرست سیستم		✓
	مدیر مخاطبان	✓
	تنظیمات سرپرست	✓
	محدودیت ها	✓
	کنترل دسترسی	✓
	رمزگذاری رمز عبور	✓
	تحقیق مشتری	✓
	تنظیمات WSD	✓
	بازگرداندن تنیظیمات اولیه	✓
	به‌روز رسانی میان افزار	✓
اطلاعات دستگاه		-

منوی تنظیم			تنظیم قفل
	شماره سریال		-
	نسخه فعلی		-
	تعداد کل اسکن ها		-
	تعداد اسکن های 1 رو		-
	تعداد اسکن های 2 رو		-
	تعداد اسکن های برگه حامل		-
	تعداد اسکن ها بعد از تعویض غلطک		-
	تعداد اسکن ها بعد از تمیز کردن مرتب		-
	وضعیت دستگاه تأیید هویت		-
	اطلاعات Epson Open Platform		-
	بازنشانی تعداد اسکن ها)		✓
تعمیر و نگهداری اسکنر			-
	تمیز کردن رولر		-
	تعویض غلطک		-
		بازنشانی تعداد اسکن ها	✓
		آشنایی با نحوه تعویض	-
	تمیز کردن مرتب		-
		بازنشانی تعداد اسکن ها	✓
		نحوه پاک کردن	-
	پاک کردن شیشه		-
تنظیم هشدار تعویض رولر			✓
	تنظیم هشدار تعداد		✓
تنظیمات هشدار تمیز کردن به طور منظم			✓
	تنظیمات هشدار		✓
	تنظیم هشدار تعداد		✓

* شما می‌توانید تنظیم کنید که آیا تغییرات در **سرپرست سیستم** > **محدودیت ها** اجازه داده شوند یا خیر.

وارد شدن به‌عنوان سرپرست از پنل کنترل

وقتی **تنظیم قفل** فعال است، می‌توانید از یکی از روش‌های زیر برای ورود از پنل کنترل اسکنر استفاده کنید.

1. روی گزینه در گوشه بالا سمت راست صفحه ضربه بزنید.

2. وقتی صفحه **انتخاب کاربر** نمایش داده شد، **سرپرست** را انتخاب کنید.
3. رمز عبور را برای ورود به سیستم وارد کنید.

پیام تکمیل ورود به سیستم نمایش داده می‌شود و سپس صفحه اصلی در پنل کنترل نمایش داده می‌شود.

برای خروج از سیستم، روی در سمت راست بالای صفحه ضربه بزنید یا دکمه را فشار دهید.

محدودکردن ویژگی‌های موجود)کنترل دسترسی)

می‌توانید با ثبت حساب‌های کاربری در اسکنر، کاربران را محدود کنید.

هنگامی که کنترل دسترسی فعال است، کاربر می‌تواند با واردکردن رمز عبور در پنل کنترل اسکنر و ورود به سیستم، از عملکردهای اسکن استفاده کند. اگر وارد سیستم نشوید، نمی‌توانید اسکن کنید.

با ثبت نام کاربر و رمز عبور خود در درایور اسکنر (Epson Scan 2) می‌توانید از کامپیوتر اسکن کنید. برای جزئیات بیشتر در مورد انجام تنظیمات، به راهنمای Epson Scan 2 یا راهنمای کاربر محصول مراجعه کنید.

ایجاد حساب کاربری

می‌توانید یک حساب کاربری کنترل دسترسی ایجاد کنید.

1. به Web Config وارد شوید و سپس زبانه **Product Security** > **Access Control Settings** > **User Settings** را انتخاب کنید.
2. روی **Add** مربوط به شماره‌ای که می‌خواهید ثبت کنید، کلیک نمایید.

> **مهم:**
> هنگام استفاده از اسکنر با سیستم تأیید هویت از *Epson* یا شرکت دیگری، *User Name* را در *Access Control Settings* در شیار شماره *2* تا *10* ثبت کنید.
>
> نرم‌افزارهای کاربردی مانند سیستم تأیید هویت از شیار شماره *1* استفاده می‌کنند، به‌طوری‌که نام کاربری در کنترل پنل اسکنر نمایش داده نمی‌شود.

3. هر مورد را تنظیم کنید.

❏ User Name:

نامی که در لیست نام‌های کاربری نمایش داده می‌شود را با طول 1 تا 14 نویسه الفبایی عددی وارد کنید.

❏ Password:

یک رمز عبور را تا 20 نویسه در ASCII ((0x20–0x7E) وارد کنید. هنگام مقداردهی اولیه رمز عبور، کادر آن را خالی بگذارید.

❏ Select the check box to enable or disable each function.

اگر می‌خواهید به عملکردهای اسکن اجازه فعالیت دهید، **Scan** را انتخاب کنید.

4. روی **Apply** کلیک کنید.

ویرایش حساب کاربری

می‌توانید حساب کاربری‌ثبت‌شده کنترل دسترسی را ویرایش کنید.

1. به Web Config وارد شوید و سپس زبانه **Product Security** > **Access Control Settings** > **User Settings** را انتخاب کنید.

2. برای شماره‌ای که می‌خواهید ویرایش کنید، روی **Edit** کلیک کنید.
3. هر مورد را تغییر دهید.
4. روی گزینه **Apply** کلیک کنید.

حذف حساب کاربری

می‌توانید حساب کاربری‌ثبت‌شده کنترل دسترسی را حذف کنید.

1. به Web Config وارد شوید و سپس زبانه **Product Security** > **Access Control Settings** > **User Settings** را انتخاب کنید.
2. برای شماره‌ای که می‌خواهید حذف کنید، روی **Edit** کلیک کنید.
3. روی گزینه **Delete** کلیک کنید.

مهم:
با کلیک روی ***Delete***، حساب کاربری بدون پیام تأیید حذف می‌شود. هنگام حذف حساب احتیاط کنید.

فعال سازی کنترل دسترسی

هنگام فعال‌کردن کنترل دسترسی، فقط کاربر ثبت‌شده می‌تواند از اسکنر استفاده کند.

نکته:
هنگامی‌که *Access Control Settings* فعال است، باید اطلاعات حساب کاربری را به اطلاع کاربر برسانید.

1. به Web Config وارد شوید و سپس زبانه **Product Security** > **Access Control Settings** > **Basic** را انتخاب کنید.
2. **Enables Access Control** را انتخاب کنید.

   اگر Access Control Settings را فعال کرده و از کامپیوتری که اطلاعات تأیید هویت ندارد اسکن می‌کنید، **Allow printing and scanning without authentication information from a computer** را انتخاب کنید.
3. روی **OK** کلیک کنید.

ورود به اسکنر که کنترل دسترسی در آن فعال است

وقتی **کنترل دسترسی** فعال است، می‌توانید از یکی از روش‌های زیر برای ورود از پنل کنترل اسکنر استفاده کنید.

1. روی گزینه در گوشه بالا سمت راست صفحه ضربه بزنید.
2. وقتی صفحه **انتخاب کاربر** نمایش داده شد، کاربر را انتخاب کنید.
3. رمز عبور را برای ورود به سیستم وارد کنید.

پیام تکمیل ورود به سیستم نمایش داده می‌شود و سپس صفحه اصلی در پنل کنترل نمایش داده می‌شود.

برای خروج از سیستم، روی در سمت راست بالای صفحه ضربه بزنید یا دکمه را فشار دهید.

غیرفعال کردن رابط خارجی

شما می توانید رابطی که برای اتصال دستگاه به اسکنر استفاده می شود را غیرفعال کنید. برای محدود کردن اسکن غیر از شبکه تنظیمات محدودیت را انجام دهید.

نکته:
تنظیمات محدودیت را می توانید از طریق پانل کنترل اسکنر نیز اعمال کنید.

اتصال رایانه از طریق *USB*: **تنظیم** > **تنظیمات اصلی** > **اتصال رایانه از طریق *USB***

1. وارد Web Config شوید و زبانه **Product Security** > **External Interface** را انتخاب کنید.
2. گزینه **Disable** را برای عملکردهایی که می خواهید تنظیم کنید انتخاب نمایید.
   گزینه **Enable** را وقتی انتخاب کنید که در نظر دارید کنترل را لغو نمایید.
   اتصال رایانه از طریق USB
   می توانید استفاده از اتصال USB کامپیوتر را محدود کنید. اگر می خواهید آن را محدود کنید، **Disable** را انتخاب کنید.
3. روی **OK** کلیک کنید.
4. بررسی کنید درگاه غیرفعال شده قابل استفاده نباشد.
   اتصال رایانه از طریق USB
   اگر درایور در رایانه نصب شده است
   اسکنر را بوسیله یک کابل USB به رایانه متصل کنید و سپس تأیید نمایید که اسکنر قادر به اسکن نمی باشد.
   اگر درایور در رایانه نصب نشده است
   Windows:
   منوی مدیر دستگاه را باز کنید و به همین صورت نگه دارید، اسکنر را از طریق کابل USB به رایانه وصل کنید و سپس تأیید نمایید که محتوای صفحه مدیر دستگاه بدون تغییر باقی می ماند.
   Mac OS:
   اسکنر را بوسیله یک کابل USB به رایانه متصل کنید و سپس تأیید نمایید نمی توانید اسکنر را از **چاپگرها و اسکنرها** اضافه کنید.

اطلاعات مرتبط

◆ "اجرای Web Config در یک مرورگر وب" در صفحه 36

فعال کردن تأیید برنامه در راه‌اندازی

اگر ویژگی تأیید هویت برنامه را فعال کنید، اسکنر در هنگام راه‌اندازی تأیید هویت را انجام می‌دهد تا بررسی کند که آیا اشخاص ثالث غیرمجاز برنامه را دست‌کاری کرده‌اند یا خیر. اگر مشکلی شناسایی شود، اسکنر شروع به کار نمی‌کند.

نکته:
فعال‌کردن این عملکرد زمان راه‌اندازی اسکنر را افزایش می‌دهد.

1. وارد Web Config شوید و سپس زبانه **Product Security** > **Program Verification on Start Up** را انتخاب کنید.

   نکته:
   تنظیمات را می‌توانید از طریق پنل کنترل اسکنر نیز اعمال کنید.

   تنظیم> سرپرست سیستم> تأیید برنامه هنگام شروع به کار
2. **ON** را انتخاب کنید تا **Program Verification on Start Up** فعال شود.

3. روی گزینه **OK** کلیک کنید.

غیرفعال کردن اسکن شبکه از کامپیوتر شما

می‌توانید تنظیمات زیر را در Web Config انجام دهید تا اسکن شبکه با استفاده از Epson Scan 2 را از کامپیوترتان غیرفعال کنید.

1. وارد Web Config شوید و سپس زبانه **Network Scan** > **Scan** را انتخاب کنید.
2. در **Epson Scan 2** علامت کادر **Enable scanning** را پاک کنید.
3. روی **Next** کلیک کنید.
   صفحه تایید تنظیم ظاهر می‌شود.
4. روی **OK** کلیک کنید.

فعال یا غیرفعال‌کردن WSD Scan

نکته:
تنظیمات را می‌توانید از طریق پنل کنترل اسکنر نیز اعمال کنید. **تنظیم** > **سرپرست سیستم** > **تنظیمات *WSD*** را انتخاب کنید.

می‌توانید اسکن WSD را فعال یا غیرفعال کنید.
اگر نمی‌خواهید کامپیوتر شما اسکنر را به‌عنوان دستگاه اسکن WSD پیکربندی کند، تنظیمات WSD را غیرفعال کنید.

1. وارد Web Config شوید و سپس زبانه **Network Security** > **Protocol** را انتخاب کنید.
2. در **WSD Settings**، کادر بررسی **Enable WSD** را تغییر دهید.
3. روی **Next** کلیک کنید.
   صفحه تایید تنظیم ظاهر می‌شود.
4. روی **OK** کلیک کنید.

نکته:
اگر کامپیوتر شما همچنان اسکنر را به‌عنوان دستگاه اسکن *WSD* پیکربندی می‌کند، زبانه ***Network Scan*** > ***Scan*** را انتخاب کنید و سپس کادر بررسی ***Enable scanning*** را در ***AirPrint*** پاک کنید.

اگر *AirPrint* غیرفعال است، *Mopria* اسکن از *Chromebooks*، *Windows* و برنامه *Mopria Scan* نیز غیرفعال می‌شود.

پایش یک اسکنر راه دور

بررسی اطلاعات برای یک اسکنر راه دور

می توانید این اطلاعات اسکنر را از **Status** با استفاده از Web Config بررسی کنید.

❑ Product Status

وضعیت، سرویس ابر، شماره دستگاه، آدرس MAC و موارد مشابه را بررسی کنید.

❑ Network Status

اطلاعات وضعیت اتصال شبکه، آدرس IP، سرور DNS و موارد مشابه را بررسی کنید.

❑ Usage Status

نخستین روز اسکن، تعداد اسکن و موارد مشابه را بررسی کنید.

❑ Hardware Status

وضعیت هر کدام از عملکردهای اسکنر را بررسی کنید.

❑ Panel Snapshot

یک عکس فوری از صفحه نمایش داده شده در پانل کنترل اسکنر را نشان می دهد.

دریافت اعلان های ایمیل زمانی که رویدادها اتفاق می افتند

درباره اعلان‌های ایمیلی

این عملکرد اعلانی است که وقتی رویدادهایی مانند توقف اسکن و خطای اسکن رخ دهند، پیام ایمیل به آدرس مشخص شده ارسال می‌گردد.

شما می‌توانید تا پنج مقصد را ثبت کنید و تنظیمات اعلان را برای هر مقصد تعیین نمایید.

برای استفاده از این عملکرد، لازم است سرور ایمیل را قبل از تنظیم اعلان‌ها تنظیم نمایید.

اطلاعات مرتبط

"ثبت دوباره یک سرور ایمیل" در صفحه 43

پیکربندی اعلان ایمیلی

اعلان ایمیل را از طریق Web Config پیکربندی کنید.

1. وارد Web Config شوید و زبانه **Email Notification** < **Device Management** را انتخاب کنید.
2. عنوان اعلان ایمیلی را تنظیم کنید.

محتوای موردنظر برای نمایش در قسمت عنوان را از طریق دو منوی کشویی موجود انتخاب کنید.

❑ محتواهای انتخاب شده در کنار **Subject** نمایش داده می شوند.

❑ تنظیم محتوای یکسان در دو سمت چپ و راست امکان پذیر نمی باشد.

❑ وقتی تعداد نویسه ها در **Location** از 32 بایت فراتر می رود، نویسه های اضافه بر 32 بایت حذف خواهند شد.

3. آدرس ایمیل موردنظر برای ارسال ایمیل اعلان را وارد کنید.

از نویسه های زیر استفاده کنید A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @، و از 1 تا 255 نویسه وارد کنید.

4. زبان را برای اعلان های ایمیل انتخاب کنید.
5. کادر علامت گذاری مربوط به رویدادی که مایلید اعلان آن را دریافت کنید را انتخاب کنید.

شماره **Notification Settings** با شماره مقصد مشخص شده در **Email Address Settings** مرتبط می باشد.

مثال:

اگر در نظر داشته باشید یک اعلان به آدرس ایمیلی که به عنوان شماره 1 در **Email Address Settings** تنظیم شده است، ارسال شود، وقتی رمز عبور سرپرست تغییر می کند، ستون کادر علامت گذاری **1** در خط **Administrator password changed** را انتخاب کنید.

6. روی **OK** کلیک کنید.

تأیید کنید در صورت وقوع مشکل، یک اعلان ایمیلی ارسال خواهد شد.

مثال: تغییر رمز عبور سرپرست را اطلاع می دهد.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

گزینه های مربوط به اعلان ایمیلی

موارد	تنظیمات و توضیحات
Administrator password changed	تغییر رمز عبور سرپرست را اطلاع می دهد.
Scanner error	وقوع خطای اسکنر را اطلاع می دهد.
ایراد Wi-Fi	وقوع خطای رابط LAN بی سیم را اطلاع می دهد.

استفاده از Web Config برای کنترل منبع تغذیه اسکنر

اگر کامپیوتر شما از اسکنر فاصله دارد، همچنان می‌توانید از Web Config برای خاموش‌کردن یا راه‌اندازی مجدد اسکنر استفاده کنید.

1. وارد Web Config شوید و سپس زبانه **Device Management** > **Power** را انتخاب کنید.
2. **Power Off** یا **Reboot** را انتخاب کنید.
3. روی **Execute** کلیک کنید.

بازیابی تنظیمات پیش‌فرض

می‌توانید تنظیمات شبکه یا سایر تنظیمات ذخیره‌شده در اسکنر را انتخاب کنید تا آن‌ها را به حالت پیش‌فرض خود بازگردانید.

1. وارد Web Config شوید و سپس زبانه **Device Management** > **Restore Default Settings** را انتخاب کنید.

نکته:
تنظیمات را می‌توانید از طریق پنل کنترل اسکنر نیز اعمال کنید.
تنظیم> سرپرست سیستم> بازگشت به تنظیمات پیش فرض

2. مواردی را که می‌خواهید بازیابی کنید، انتخاب کنید.
3. روی **Execute** کلیک کنید.

در نهایت، دستورالعمل‌های روی صفحه را دنبال کنید.

اطلاعات Epson Remote Services

Epson Remote Services سرویسی است که به‌صورت دوره‌ای اطلاعات اسکنر را از طریق اینترنت جمع‌آوری می‌کند. این را می‌توان برای پیش‌بینی زمان نیاز به تعویض یا پر کردن مجدد اقلام مصرفی و تعویضی و برای رفع سریع هرگونه خطا یا مشکل استفاده کرد.

برای کسب اطلاعات بیشتر در مورد Epson Remote Services با فروشنده خود تماس بگیرید.

حل کردن مشکلات

رمز عبور سرپرست خود را فراموش کرده اید

شما به کمک از طرف متخصصین سرویس نیاز دارید. با فروشنده محلی تماس بگیرید.

نکته:
در بخش زیر، مقادیر اولیه برای سرپرست *Web Config* ارائه می‌شوند.

- نام کاربری: هیچ‌کدام (خالی)
- رمز عبور: بستگی به برچسب چسبانده‌شده به محصول دارد.

  اگر برچسب «*PASSWORD*» به پشت چسبانده شده است، عدد *8* رقمی درج‌شده روی برچسب را وارد کنید.

  اگر برچسب «*PASSWORD*» چسبانده نشده است، شماره سریال روی برچسب چسبانده‌شده به پشت محصول را برای رمز عبور سرپرست اولیه وارد کنید.

اگر رمز عبور سرپرست را بازیابی کنید، به مقدار اولیه در زمان خرید بازنشانی می‌شود.

تنظیمات امنیتی پیشرفته

تنظیمات امنیتی و پیشگیری از خطر

اگر اسکنر به شبکه متصل شود، می توانید از راه دور به آن دسترسی پیدا کنید. در ضمن، بسیاری از افراد می توانند اسکنر را به اشتراک بگذارند و کارآیی و راحتی را افزایش دهند. هر چند، احتمال دسترسی غیرقانونی، استفاده غیرمجاز و دستکاری داده ها افزایش می یابد. اگر از اسکنر در محیط متصل به اینترنت استفاده کنید، مخاطرات بیشتر نیز می شوند.

برای اسکنر های فاقد محافظ دسترسی خارجی، امکان خواندن مخاطبین مرتب شده در اسکنر از طریق اینترنت وجود دارد.

برای پیشگیری از این خطرها، اسکنر های Epson از فناوری های امنیتی مختلفی بهره می گیرند.

در صورت لزوم اسکنر را بر اساس شرایط محیطی که در اطلاعات محیط مشتری گنجانده شده است تنظیم کنید.

نام	نوع قابلیت	آنچه باید تنظیم شود	آنچه باید جلوگیری شود
کنترل پروتکل	پروتکل ها و خدماتی را که قرار است بین اسکنر ها و رایانه ها به کار گرفته شود کنترل می کند و امکانات را فعال و غیرفعال می کند.	پروتکل یا سرویسی که روی قابلیت ها اعمال می شود، جداگانه مجاز یا غیرمجاز می گردد.	کاهش احتمال بروز خطرهای ناشی از استفاده ناخواسته از طریق جلوگیری از دسترسی کاربران به عملکردهای غیرضروری.
ارتباط SSL/TLS	در هنگام برقراری ارتباط بین سرور Epson و دستگاه در محیط اینترنت از اسکنر، برای مثال ارتباط با رایانه از طریق مرورگر وب، استفاده از Epson Connect و به روزرسانی ثابت افزار، محتوای ارتباطی با ارتباطات SSL/ TLS رمزنگاری می شود.	یک گواهی دارای امضای CA بگیرید و آن را وارد اسکنر کنید.	پاک کردن شناسه اسکنر با گواهی دارای امضای CA مانع جعل هویت و دسترسی غیرمجاز می شود. در ضمن، محتوای ارتباط SSL/TLS محافظت می شود و بدین ترتیب از نشت محتویات مربوط به داده های اسکن و اطلاعات تنظیم جلوگیری می گردد.
فیلترگذاری IPsec/IP	می توانید ترتیبی دهید که ارسال به سرور و قطع ارتباط داده هایی که از طرف سرویس گیرنده خاصی است یا نوع خاصی دارند، ممکن شود. از آنجا که IPsec با واحد بسته IP (رمزنگاری و تأیید هویت) از داده ها محافظت می کند، می توانید پروتکل را بدون خطر منتقل کنید.	سیاستی ابتدایی و سیاستی فردی ایجاد کنید و سرویس گیرنده یا نوع داده دارای قابلیت دسترسی به اسکنر را مشخص نمایید.	از دسترسی غیرمجاز و رهگیری داده های ارتباط با اسکنر جلوگیری کنید.
IEEE 802.1X	تنها به کاربران تأیید هویت شده اجازه می دهد به شبکه متصل شوند. فقط به کاربر مجاز اجازه استفاده از اسکنر را می دهد.	تنظیم تأیید هویت در سرور RADIUS (سرور تأیید هویت).	از دسترسی غیرمجاز و استفاده غیرمجاز از اسکنر جلوگیری کنید.

اطلاعات مرتبط

- "کنترل کردن با پروتکل‌ها" در صفحه 89
- "ارتباط SSL/TLS با اسکنر" در صفحه 97
- "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 98
- "اتصال اسکنر به شبکه IEEE802.1X" در صفحه 109

تنظیمات ویژگی امنیتی

هنگام تنظیم فیلترگذاری IPsec/IP یا IEEE 802.1X، توصیه می‌شود از طریق SSL/TLS به Web Config وارد شوید تا اطلاعات تنظیمات را به منظور کاهش خطرات امنیتی مانند دسترسی غیرمجاز یا استراق سمع مبادله کنید.

قبل از تنظیم فیلترگذاری IPsec/IP یا IEEE 802.1X، مطمئن شوید رمز عبور سرپرست را پیکربندی می‌کنید.

کنترل کردن با پروتکل‌ها

می توانید با استفاده از گذرگاه ها و پروتکل های مختلف اسکن کنید. همچنین، می توانید از تعداد نامشخص رایانه های شبکه از اسکن شبکه استفاده کنید.

می توانید با محدود کردن اسکن از گذرگاه های مشخص یا با کنترل عملکردهای موجود خطرات ناخواسته امنیتی را کاهش دهید.

کنترل پروتکل ها

تنظیمات پروتکل پشتیبانی شده توسط اسکنر را پیکربندی کنید.

1. وارد Web Config شوید و زبانه **Network Security** tab > **Protocol** را انتخاب کنید.
2. هر مورد را پیکربندی کنید.
3. روی **Next** کلیک کنید.
4. روی **OK** کلیک کنید.

تنظیمات به اسکنر اعمال می شوند.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

پروتکل هایی که می توانید فعال یا غیرفعال کنید

پروتکل	شرح
Bonjour Settings	می توانید مشخص کنید آیا از Bonjour استفاده شود یا خیر. Bonjour برای جستجوی دستگاه ها، اسکن و مانند این استفاده می شود.
SLP Settings	می توانید عملکرد SLP را فعال یا غیرفعال کنید. SLP برای اسکن و ارسال همزمان و جستجوی شبکه در EpsonNet Config استفاده می شود.
WSD Settings	می توانید عملکرد WSD را فعال یا غیرفعال کنید. زمانی که فعال باشد، می توانید دستگاه های WSD را اضافه کنید و از طریق درگاه WSD اسکن کنید.
LLTD Settings	می توانید عملکرد LLTD را فعال یا غیرفعال کنید. زمانی که فعال باشد، روی نقشه شبکه Windows نشان داده می شود.
LLMNR Settings	می توانید عملکرد LLMNR را فعال یا غیرفعال کنید. هنگامی که این فعال باشد، می توانید از وضوح نام بدون NetBIOS استفاده کنید حتی اگر نمی توانید از آن استفاده کنید.DNS
SNMPv1/v2c Settings	می توانید مشخص کنید آیا SNMPv1/v2c فعال شود یا خیر. از این برای تنظیم دستگاه ها، کنترل و مانند این استفاده می شود.
SNMPv3 Settings	می توانید مشخص کنید آیا SNMPv3 فعال شود یا خیر. از این برای تنظیم دستگاه های رمزنگاری شده، پایش و غیره استفاده می شود.

موارد تنظیم پروتکل

Bonjour Settings

موارد	مقدار و توضیحات تنظیم
Use Bonjour	برای جستجو یا استفاده از دستگاه ها از طریق Bonjour این را انتخاب کنید.
Bonjour Name	نام Bonjour را نمایش می دهد.
Bonjour Service Name	نام سرویس Bonjour را نمایش می دهد.
Location	نام مکان Bonjour را نمایش می دهد.
Wide-Area Bonjour	مشخص کنید آیا از Wide-Area Bonjour استفاده شود.

SLP Settings

موارد	مقدار و توضیحات تنظیم
Enable SLP	برای فعال سازی عملکرد SLP این را انتخاب کنید. ااین همانند جستجوی شبکه در EpsonNet Config استفاده می شود.

WSD Settings

موارد	مقدار و توضیحات تنظیم
Enable WSD	برای فعال کردن دستگاه ها با استفاده از WSD و اسکن از طریق درگاه WSD این را انتخاب کنید.
Scanning Timeout (sec)	مقدار زمان پایان مهلت ارتباط برای اسکن WSD را بین 3 تا 3600 ثانیه وارد کنید.
Device Name	نام دستگاه WSD را نمایش می دهد.
Location	نام مکان WSD را نمایش می دهد.

LLTD Settings

موارد	مقدار و توضیحات تنظیم
Enable LLTD	این را انتخاب کنید تا LLTD فعال شود. اسکنر در نقشه شبکه Windows نمایش داده می شود.
Device Name	نام دستگاه LLTD را نمایش می دهد.

LLMNR Settings

موارد	مقدار و توضیحات تنظیم
Enable LLMNR	این را انتخاب کنید تا LLMNR فعال شود. می توانید از جداسازی نام بدون NetBIOS استفاده کنید حتی اگر نتوانید از DNS استفاده کنید.

SNMPv1/v2c Settings

موارد	مقدار و توضیحات تنظیم
Enable SNMPv1/v2c	انتخاب کنید تا SNMPv1/v2c فعال شود.

موارد	مقدار و توضیحات تنظیم
Access Authority	وقتی SNMPv1/v2c فعال است، مرجع دسترسی را تنظیم کنید. گزینه **Read Only** یا **Read/Write** را انتخاب کنید.
Community Name (Read Only)	بین 0 تا 32 نویسه ASCII (0x20 تا 0x7E) وارد کنید.
Community Name (Read/Write)	بین 0 تا 32 نویسه ASCII (0x20 تا 0x7E) وارد کنید.

SNMPv3 Settings

موارد		مقدار و توضیحات تنظیم
Enable SNMPv3		زمانی که کادر علامت داشته باشد، SNMPv3 فعال می شود.
User Name		بین 1 تا 32 نویسه با استفاده از نویسه های 1 بایتی وارد کنید.
Authentication Settings		
	Algorithm	یک الگوریتم تأیید هویت برای SNMPv3 انتخاب کنید.
	Password	رمز عبور تأیید هویت را برای SNMPv3 وارد کنید. بین 8 تا 32 نویسه با قالب ASCII ((0x20–0x7E) وارد کنید. اگر نمی خواهید این را مشخص کنید، خالی بگذارید.
	Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید را وارد نمایید.
Encryption Settings		
	Algorithm	یک الگوریتم رمزنگاری برای SNMPv3 انتخاب کنید.
	Password	رمز عبور رمزنگاری را برای SNMPv3 وارد کنید. بین 8 تا 32 نویسه با قالب ASCII ((0x20–0x7E) وارد کنید. اگر نمی خواهید این را مشخص کنید، خالی بگذارید.
	Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید را وارد نمایید.
Context Name		با 32 نویسه یا کمتر در قالب Unicode (UTF-8) وارد کنید. اگر نمی خواهید این را مشخص کنید، خالی بگذارید. تعداد نویسه های مجاز بسته به زبان فرق می کند.

استفاده از گواهی دیجیتالی

درباره گواهی دیجیتالی

❑ CA-signed Certificate

این یک گواهی امضا شده توسط CA (مرجع صدور گواهی) است. /شما می توانید آن را برای اعمال به مرجع صدور گواهی به دست آورید. این گواهی تأیید می کند که اسکنر موجود است و برای برقراری ارتباط SSL/TLS استفاده می شود، در نتیجه می توانید درباره امنیت تبادل داده ها اطمینان حاصل کنید.

وقتی از آن برای ارتباط SSL/TLS استفاده می کنید، به عنوان گواهی سرور استفاده خواهد شد.

وقتی روی فیلترگذاری IPsec/IP یا ارتباط IEEE 802.1X تنظیم می شود، به عنوان گواهی سرویس گیرنده استفاده خواهد شد.

❑ گواهی CA

این یک گواهی است که در زنجیره CA-signed Certificate بکار برده می شود و گواهی CA حدواسط نیز نامیده می شود. این گواهی توسط مرورگر وب برای تأیید اعتبار مسیر گواهی اسکنر هنگام دسترسی سرور طرف مقابل یا Web Config استفاده می شود.

در رابطه با گواهی CA، زمان تأیید اعتبار گواهی سرور تحت دسترسی از طریق اسکنر را تنظیم کنید. در رابطه با اسکنر، تنظیمات را برای تأیید مسیر CA-signed Certificate برای ارتباط SSL/TLS تنظیم کنید.

شما می توانید گواهی CA اسکنر را از طریق مرجع صدور گواهی که گواهی CA را صادر می کند به دست بیاورید.

همچنین، گواهی CA مورد استفاده برای تأیید اعتبار سرور طرف مقابل را می توانید از طریق مرجع صدور گواهی که CA-signed Certificate سرور دیگر را صادر کرده است، به دست بیاورید.

❑ Self-signed Certificate

این یک گواهی است که اسکنر امضا و صادر می کند. به آن «گواهی اصلی» نیز گفته می شود. از آنجا که صادر کننده خود تأیید کننده نیز می باشد، قابل اطمینان نمی باشد و قادر به جلوگیری از جعل هویت نمی باشد.

هنگام اعمال تنظیمات امنیتی و برقراری ارتباط SSL/TLS ساده بدون CA-signed Certificate، از آن را استفاده کنید.

اگر از این گواهی برای یک ارتباط SSL/TLS استفاده کنید، ممکن است یک هشدار امنیتی روی مرورگر نشان داده شود، زیرا گواهی در یک مرورگر وب ثبت نشده است. از Self-signed Certificate تنها برای ارتباط SSL/TLS استفاده کنید.

اطلاعات مرتبط

- "پیکربندی یک CA-signed Certificate" در صفحه 92
- "به روزرسانی گواهی خود امضاء" در صفحه 95
- "پیکربندی یک CA Certificate" در صفحه 96

پیکربندی یک CA-signed Certificate

دریافت گواهی امضاء شده از طریق CA

برای دریافت گواهی امضاء شده از طریق CA، یک CSR (درخواست امضای گواهی) ایجاد کنید و برای درخواست آن را برای مرجع صدور گواهی ارسال کنید. می توانید با استفاده از Web Config و رایانه یک CSR ایجاد کنید.

مراحل ایجاد CSR را دنبال کنید و با استفاده از Web Config یک گواهی امضاء شده از طریق CA دریافت کنید. زمان ایجاد CSR با استفاده از Web Config، گواهی دارای فرمت PEM/DER است.

1. وارد Web Config شوید و زبانه **Network Security** را انتخاب کنید. سپس **SSL/TLS** > **Certificate** یا **IPsec/IP Filtering** > **Client Certificate** یا **IEEE802.1X** > **Client Certificate** را انتخاب کنید.

   هر کدام را انتخاب کنید، می‌توانید همان گواهی را به دست بیاورید و آن را به صورت مشترک استفاده کنید.

2. روی **Generate** از **CSR** کلیک کنید.

   صفحه ایجاد CSR باز می‌شود.

3. برای هر مورد یک مقدار وارد کنید.

   نکته:
   طول کلید موجود و مخفف سازی‌ها بر اساس مرجع صدور گواهی فرق دارد. طبق قوانین مرجع صدور گواهی یک درخواست ایجاد کنید.

4. روی **OK** کلیک کنید.

   یک پیام تکمیل نشان داده می‌شود.

5. زبانه **Network Security** را انتخاب کنید. سپس **SSL/TLS** > **Certificate** یا **IPsec/IP Filtering** > **Client Certificate** یا **IEEE802.1X** > **Client Certificate** را انتخاب کنید.

6. طبق فرمت مشخص شده از طرف مرجع صدور گواهی برای دانلود CSR در رایانه، روی یکی از دکمه‌های دانلود **CSR** کلیک کنید.

> **مهم:**
> دوباره یک *CSR* ایجاد نکنید. اگر اینکار را انجام دهید، ممکن است نتوانید *CA-signed Certificate* صادر شده را وارد کنید.

7. CSR را برای مرجع صدور گواهی ارسال کنید و یک CA-signed Certificate دریافت کنید.
قوانین مربوط به مرجع صدور گواهی برای شکل و روش ارسال را دنبال کنید.

8. CA-signed Certificate صادر شده را در رایانه متصل به اسکنر ذخیره کنید.
زمانی که گواهی را در مقصد ذخیره کنید دریافت CA-signed Certificate کامل است.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

گزینه های تنظیم *CSR*

موارد	تنظیمات و توضیحات
Key Length	طول کلید را برای یک CSR انتخاب کنید.
Common Name	می توانید بین 1 تا 128 نویسه وارد کنید. اگر این یک آدرس IP است، باید یک آدرس IP ثابت باشد. شما می توانید 1 تا 5 آدرس IPv4، آدرس IPv6، نام میزبان و FQDN های وارد کنید و با استفاده از ویرگول بین آنها فاصله بگذارید. نخستین جزء در کادر نام مشترک ذخیره می شود و سایر اجزاء در کادر نام مستعار مربوط به موضوع گواهی ذخیره می گردند. مثال: آدرس IP اسکنر: 192.0.2.123، نام اسکنر: EPSONA1B2C3 Common Name: EPSONA1B2C3, EPSONA1B2C3.local, 192.0.2.123
Organization/ Organizational Unit/ Locality/ State/Province	می توانید بین 0 تا 64 نویسه با قالب ASCII ((0x20–0x7E) وارد کنید. می توانید نام های متمایز را با ویرگول جدا کنید.
Country	یک کد کشور دو رقمی که توسط ISO-3166 تعیین شده وارد کنید.
Sender's Email Address	شما می توانید آدرس ایمیل فرستنده را برای تنظیمات سرور ایمیل وارد کنید. همان آدرس ایمیل **Sender's Email Address** را برای زبانه **Network** > **Email Server** > **Basic** وارد کنید.

وارد کردن گواهی امضاء شده از طریق CA

CA-signed Certificate کسب شده را به اسکنر وارد کنید.

> **مهم:**
> ❑ دقت کنید که تاریخ و زمان اسکنر به درستی تنظیم شده باشد. ممکن است گواهی نامعتبر باشد.
> ❑ اگر با استفاده از *CSR* که از *Web Config* ایجاد شده است یک گواهی دریافت کنید، می توانید هر بار یک گواهی وارد کنید.

1. وارد Web Config شوید و سپس زبانه **Network Security** را انتخاب کنید. سپس **SSL/TLS** > **Certificate** یا **IPsec/IP Filtering** > **Client Certificate** یا **IEEE802.1X** > **Client Certificate** را انتخاب کنید.

2. روی **Import** کلیک کنید

صفحه وارد کردن گواهی باز می شود.

3. برای هر مورد یک مقدار وارد کنید. هنگام تأیید مسیر گواهی در مرورگر وبی که به اسکنر دسترسی دارد، **CA Certificate 1** و **CA Certificate 2** را تنظیم کنید.

بسته به اینکه کجا یک CSR ایجاد می کنید و فرمت فایل گواهی، ممکن است تنظیمات مورد نیاز فرق داشته باشد. مقادیر را برای موارد مورد نیاز طبق شرایط زیر وارد کنید.

❏ یک گواهی با قالب PEM/DER از Web Config دریافت شد

❏ **Private Key**: پیکربندی نکنید زیرا اسکنر محتوی یک کلید خصوصی است.

❏ **Password**: پیکربندی نکنید.

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

❏ یک گواهی با قالب PEM/DER از رایانه دریافت شده باشد

❏ **Private Key**: لازم است تنظیم کنید.

❏ **Password**: پیکربندی نکنید.

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

❏ یک گواهی با قالب PKCS#12 از رایانه دریافت شده باشد

❏ **Private Key**: پیکربندی نکنید.

❏ **Password**: اختیاری

❏ **CA Certificate 2/CA Certificate 1**: پیکربندی نکنید.

4. روی **OK** کلیک کنید.

یک پیام تکمیل نشان داده می شود.

نکته:
روی ***Confirm*** برای تأیید اطلاعات گواهی کلیک کنید.

اطلاعات مرتبط

◆ "اجرای Web Config در یک مرورگر وب" در صفحه 36

موارد تنظیم وارد کردن گواهی امضاء شده از طریق *CA*

موارد	تنظیمات و توضیحات
Server Certificate یا Client Certificate	فرمت گواهی را انتخاب کنید. در رابطه با اتصال SSL/TLS، وضعیت Server Certificate نمایش داده می‌شود. در رابطه با فیلترگذاری IPsec/IP یا IEEE 802.1X، وضعیت Client Certificate نمایش داده می‌شود.
Private Key	اگر با استفاده از یک CSR که از طریق رایانه ایجاد شده است، گواهی با قالب PEM/DER دریافت می‌کنید، یک فایل کلید خصوصی که با گواهی مطابقت دارد تعیین کنید.
Password	اگر قالب فایل **Certificate with Private Key (PKCS#12)** است، رمز عبور مربوطه برای رمزنگاری کلید خصوصی که هنگام دریافت گواهی تنظیم شده بود را وارد کنید.

موارد	تنظیمات و توضیحات
CA Certificate 1	اگر قالب گواهی **Certificate (PEM/DER)** است، یک گواهی از مرجع صدور گواهی که CA-signed Certificate مورد استفاده به عنوان گواهی سرور را صادر می‌کند وارد کنید. اگر نیاز است یک فایل تعیین کنید.
CA Certificate 2	اگر قالب گواهی **Certificate (PEM/DER)** است، یک گواهی از مرجع صدور گواهی که CA Certificate 1 صادر می‌کند وارد کنید. اگر نیاز است یک فایل تعیین کنید.

حذف گواهی امضاء شده از طریق CA

زمانی که گواهی منقضی شده است یا زمانی که دیگر به اتصال رمزگذاری شده نیازی نیست می توانید گواهی وارد شده را حذف کنید.

مهم:
اگر با استفاده از یک *CSR* که از *Web Config* ایجاد شده است، یک گواهی دریافت کنید، نمی توانید گواهی حذف شده را دوباره وارد کنید.در این حالت یک *CSR* ایجاد کرده و دوباره گواهی را دریافت کنید.

1. وارد Web Config شوید و زبانه **Network Security** را انتخاب کنید.سپس **SSL/TLS** > **Certificate** یا **IPsec/IP Filtering** > **Client Certificate** یا **IEEE802.1X** > **Client Certificate** را انتخاب کنید.
2. روی **Delete** کلیک کنید.
3. در پیام نشان داده شده، تایید کنید که می خواهید گواهی را حذف کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

به روزرسانی گواهی خود امضاء

از آنجا که Self-signed Certificate توسط اسکنر صادر می‌شود، در صورت انقضا یا تغییر محتوای تشریح‌شده قادر خواهید بود آن را به‌روز کنید.

1. وارد Web Config شوید و زبانه **Network Security** tab > **SSL/TLS** > **Certificate** را انتخاب کنید.
2. روی گزینه **Update** کلیک کنید.
3. **Common Name** را وارد کنید.

شما می‌توانید تا 5 آدرس IPv4، آدرس IPv6، نام میزبان و FQDN های شامل 1 الی 128 نویسه را وارد کنید و با استفاده از ویرگول بین آنها فاصله بگذارید. نخستین پارامتر در کادر نام مشترک ذخیره می‌شود و سایر موارد در کادر نام مستعار مربوط به موضوع گواهی ذخیره می‌گردند.

مثال:

آدرس IP اسکنر: 192.0.2.123، نام اسکنر: EPSONA1B2C3

نام مشترک: EPSONA1B2C3, EPSONA1B2C3.local, 192.0.2.123

4. یک دوره اعتبار برای گواهی مشخص کنید.
5. روی گزینه **Next** کلیک کنید.

یک پیام تأیید نشان داده می‌شود.

6. روی گزینه **OK** کلیک کنید.

اسکنر به روزرسانی می‌شود.

نکته:
اطلاعات گواهی را می‌توانید از طریق زبانه ***Network Security*** و سپس > ***SSL/TLS*** > ***Certificate*** > ***Self-signed Certificate*** و در نهایت با کلیک روی گزینه ***Confirm*** بررسی کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

پیکربندی یک CA Certificate

وقتی CA Certificate را تنظیم می کنید، می توانید اعتبار مسیر گواهی CA سروری که اسکنر به آن دسترسی دارد را ارزیابی کنید. این می تواند از جعل هویت جلوگیری کند.

CA Certificate را می توانید از طریق مرجع صدور گواهی صادر کننده CA-signed Certificate به دست بیاورید.

وارد کردن CA Certificate

CA Certificate را به اسکنر وارد کنید.

1. وارد Web Config شوید و سپس زبانه **Network Security** > **CA Certificate** را انتخاب کنید.
2. روی **Import** کلیک کنید.
3. CA Certificate که می خواهید وارد کنید را مشخص کنید.
4. روی **OK** کلیک کنید.

وقتی وارد کردن تکمیل شد به صفحه **CA Certificate** بازگردانده می شود و CA Certificate وارد شده، نمایش داده می شود.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

حذف یک CA Certificate

می توانید CA Certificate وارد شده را حذف کنید.

1. وارد Web Config شوید و سپس زبانه **Network Security** > **CA Certificate** را انتخاب کنید.
2. روی **Delete** در کنار CA Certificate که می‌خواهید حذف کنید، کلیک کنید.
3. در پیام نشان داده شده، تأیید کنید که می‌خواهید گواهی را حذف کنید.
4. روی **Reboot Network** کلیک کنید و سپس بررسی کنید گواهی CA حذف شده در صفحه به‌روز شده لیست نشده است.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

ارتباط SSL/TLS با اسکنر

اگر گواهی سرور با ارتباط SSL/TLS (لایه سوکت امن/امنیت لایه حمل) با اسکنر تنظیم شود، می‌توانید مسیر ارتباط بین رایانه‌ها را رمزگذاری کنید. اگر می‌خواهید مانع دسترسی راه دور و غیرمجاز شوید، از این روش استفاده کنید.

پیکربندی تنظیمات SSL/TLS ساده

اگر اسکنر از قابلیت سرور HTTPS پشتیبانی می‌کند، شما می‌توانید از ارتباط SSL/TLS برای رمزنگاری مکاتبات استفاده کنید. ضمن اطمینان خاطر بابت امنیت، می‌توانید اسکنر را از طریق Web Config پیکربندی و مدیریت کنید.

قدرت رمزنگاری و قابلیت هدایت مجدد را پیکربندی کنید.

1. وارد Web Config شوید و زبانه **Network Security** > **SSL/TLS** > **Basic** را انتخاب کنید.
2. برای هر مورد یک مقدار انتخاب کنید.
   - ❏ Encryption Strength

     سطح قدرت رمزنگاری را انتخاب کنید.
   - ❏ Redirect HTTP to HTTPS

     هدایت مجدد به HTTPS هنگامی که HTTP دسترسی می‌شود.
3. روی گزینه **Next** کلیک کنید.

   یک پیام تأیید نشان داده می‌شود.
4. روی گزینه **OK** کلیک کنید.

   اسکنر به روزرسانی می‌شود.

اطلاعات مرتبط

◆ "اجرای Web Config در یک مرورگر وب" در صفحه 36

پیکربندی گواهی سرور برای اسکنر

1. وارد Web Config شوید و زبانه **Network Security** > **SSL/TLS** > **Certificate** را انتخاب کنید.
2. گواهی موردنظر برای استفاده در **Server Certificate** را مشخص کنید.
   - ❏ Self-signed Certificate

     یک گواهی خود امضاء از طریق اسکنر ایجاد شده است. اگر یک گواهی امضاء شده توسط CA را در اختیار ندارید، از این مورد استفاده کنید.
   - ❏ CA-signed Certificate

     اگر یک گواهی امضاء شده توسط CA را از قبل کسب نموده یا وارد کرده اید، می توانید این را مشخص کنید.
3. روی **Next** کلیک کنید.

   یک پیام تأیید نشان داده می شود.
4. روی **OK** کلیک کنید.

   اسکنر به روزرسانی می شود.

اطلاعات مرتبط

- "اجرای Web Config در یک مرورگر وب" در صفحه 36
- "پیکربندی یک CA-signed Certificate" در صفحه 92
- "پیکربندی یک CA Certificate" در صفحه 96

ارتباط رمزگذاری شده با IPsec/فیلترینگ IP

درباره IPsec/IP Filtering

ترافیک داده‌ها را می‌توانید با استفاده از عملکرد فیلترگذاری IPsec/IP، بر اساس آدرس‌های IP، سرویس‌ها و درگاه فیلتر کنید. با ترکیب فیلترینگ، می‌توانید اسکنر را برای پذیرفتن یا مسدود کردن سرویس‌گیرنده‌های تعیین شده و داده‌های تعیین شده پیکربندی کنید. علاوه بر این، می‌توانید سطح امنیتی را با استفاده از یک IPsec بهبود ببخشید.

نکته:
رایانه‌هایی که با *Windows Vista* یا نسخه جدیدتر یا *Windows Server 2008* یا نسخه جدیدتر کار می‌کنند از *IPsec* پشتیبانی می‌کنند.

پیکربندی سیاست پیش‌فرض

برای فیلتر کردن ترافیک، سیاست پیش‌فرض را پیکربندی کنید. سیاست پیش‌فرض برای هر کاربر یا گروه متصل به اسکنر اعمال می‌شود. برای کنترل دقیق‌تر کاربران و گروه‌های کاربران، سیاست‌های گروهی را پیکربندی کنید.

1. وارد Web Config شوید و زبانه **Network Security** > **IPsec/IP Filtering** > **Basic** را انتخاب کنید.
2. برای هر مورد یک مقدار وارد کنید.
3. روی **Next** کلیک کنید.
   یک پیام تأیید نشان داده می‌شود.
4. روی **OK** کلیک کنید.
   اسکنر به روزرسانی می‌شود.

اطلاعات مرتبط

- "اجرای Web Config در یک مرورگر وب" در صفحه 36

موارد تنظیمDefault Policy

Default Policy

موارد	تنظیمات و توضیحات
IPsec/IP Filtering	قابلیت فیلترگذاری IPsec/IP را می توانید فعال یا غیرفعال کنید.

❑ Access Control

یک روش کنترل برای ترافیک بسته های IP پیکربندی کنید.

موارد	تنظیمات و توضیحات
Permit Access	برای مجاز کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.
Refuse Access	برای رد کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.
IPsec	برای مجاز کردن عبور بسته های IPsec پیکربندی شده، این را انتخاب کنید.

❏ **IKE Version**

گزینه **IKEv1** یا **IKEv2** را برای **IKE Version** انتخاب کنید. یکی از آنها را با توجه به دستگاه متصل به اسکنر انتخاب کنید.

❏ IKEv1

اگر **IKEv1** را برای **IKE Version** انتخاب کنید، موارد زیر نمایش داده می شود.

موارد	تنظیمات و توضیحات
Authentication Method	برای انتخاب **Certificate**، لازم است از قبل یک گواهی امضاء شده از طریق CA دریافت و وارد کنید.
Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.

❏ IKEv2

اگر **IKEv2** را برای **IKE Version** انتخاب کنید، موارد زیر نمایش داده می شود.

موارد		تنظیمات و توضیحات
Local	Authentication Method	برای انتخاب **Certificate**، لازم است از قبل یک گواهی امضاء شده از طریق CA دریافت و وارد کنید.
	ID Type	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب کنید، باید نوع شناسه اسکنر را انتخاب کنید.
	ID	شناسه اسکنر را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «=» را نیز در نظر بگیرید. **IP Address**: قالب IPv4 یا IPv6 را وارد کنید. **FQDN**: ترکیبی بین 1 و 255 نویسه با استفاده از A–Z، a–z، 0–9، - و نقطه (.) وارد کنید. **Email Address**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «@» را نیز در نظر بگیرید. **Key ID**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.

موارد		تنظیمات و توضیحات
Remote	Authentication Method	برای انتخاب **Certificate**، لازم است از قبل یک گواهی امضاء شده از طریق CA دریافت و وارد کنید.
	ID Type	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، باید نوع شناسه را برای دستگاهی که می خواهید تأیید کنید، انتخاب نمایید.
	ID	شناسه اسکنری را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «=» را نیز در نظر بگیرید. **IP Address**: قالب IPv4 یا IPv6 را وارد کنید. **FQDN**: ترکیبی بین 1 و 255 نویسه با استفاده از A–Z، a–z، 0–9، - و نقطه (.) وارد کنید. **Email Address**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «@» را نیز در نظر بگیرید. **Key ID**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.

❑ Encapsulation

اگر **IPsec** را برای **Access Control** انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.

موارد	تنظیمات و توضیحات
Transport Mode	اگر در LAN مشابه فقط از اسکنر استفاده می کنید، این را انتخاب کنید. بسته های IP لایه 4 یا لایه بالاتر رمزنگاری می شوند.
Tunnel Mode	اگر از اسکنر در شبکه دارای اینترنت مانند IPsec-VPN استفاده می کنید، این گزینه را انتخاب کنید. عنوان و داده های بسته های IP رمزنگاری می شوند. **Remote Gateway(Tunnel Mode)**: اگر گزینه **Tunnel Mode** را برای **Encapsulation** انتخاب می کنید، یک آدرس درگاه بین 1 و 39 نویسه وارد کنید.

❑ Security Protocol

اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید.

موارد	تنظیمات و توضیحات
ESP	برای اطمینان از یکپارچگی تأیید اعتبار و داده ها، این گزینه را انتخاب کنید و داده ها را رمزنگاری کنید.
AH	برای اطمینان از یکپارچگی تأیید اعتبار و داده ها، این گزینه را انتخاب کنید. حتی اگر رمزنگاری داده ها ممنوع باشد، می توانید از IPsec استفاده کنید.

❑ **Algorithm Settings**

توصیه می شود گزینه **Any** را برای همه تنظیمات انتخاب کنید یا یک مورد غیر از **Any** برای هر تنظیم انتخاب نمایید. اگر **Any** را برای برخی از تنظیمات انتخاب کنید و موردی غیر از **Any** را برای تنظیمات دیگر انتخاب کنید، دستگاه ممکن است بسته به دستگاه دیگری که قصد تأیید آن را دارید ارتباط برقرار نکند.

موارد		تنظیمات و توضیحات
IKE	Encryption	الگوریتم رمزنگاری را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می کند.
	Authentication	الگوریتم تأیید هویت را برای IKE انتخاب کنید.
	Key Exchange	الگوریتم تبادل کلید را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می کند.
ESP	Encryption	الگوریتم رمزنگاری را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
	Authentication	الگوریتم تأیید هویت را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
AH	Authentication	الگوریتم رمزنگاری را برای AH انتخاب کنید. این زمانی موجود است که **AH** برای **Security Protocol** انتخاب شده باشد.

پیکربندی سیاست گروه

سیاست گروهی یک یا تعداد بیشتری از قوانین است که برای یک کاربر یا یک گروه کاربر اعمال می‌شود. اسکنر بسته‌های IP را که با سیاست‌های پیکربندی شده مطابقت دارند کنترل می‌کند. بسته‌های IP به ترتیب یک سیاست گروهی 1 تا 10 سپس یک سیاست پیش‌فرض تأیید می‌شوند.

1. وارد Web Config شوید و زبانه **Network Security** > **IPsec/IP Filtering** > **Basic** را انتخاب کنید.
2. روی زبانه عددی که می‌خواهید پیکربندی کنید کلیک نمایید.
3. برای هر مورد یک مقدار وارد کنید.
4. روی **Next** کلیک کنید.
   یک پیام تأیید نشان داده می‌شود.
5. روی **OK** کلیک کنید.
   اسکنر به روزرسانی می‌شود.

موارد تنظیم Group Policy

موارد	تنظیمات و توضیحات
Enable this Group Policy	می توانید یک سیاست گروهی را فعال یا غیرفعال کنید.

Access Control

یک روش کنترل برای ترافیک بسته های IP پیکربندی کنید.

موارد	تنظیمات و توضیحات
Permit Access	برای مجاز کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.
Refuse Access	برای رد کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.
IPsec	برای مجاز کردن عبور بسته های IPsec پیکربندی شده، این را انتخاب کنید.

Local Address (Scanner)

آدرس IPv4 یا آدرس IPv6 را انتخاب کنید که با محیط شبکه مطابقت داشته باشد. اگر یک آدرس IP به طور خودکار تعیین شود، می توانید **Use auto-obtained IPv4 address** را انتخاب کنید.

نکته:
اگر یک آدرس *IPv6* به طور خودکار تعیین شود، ممکن است اتصال قابل دسترسی نباشد. یک آدرس *IPv6* ثابت پیکربندی کنید.

Remote Address(Host)

برای کنترل دسترسی یک آدرس IP دستگاه وارد کنید. آدرس IP باید حداکثر 43 نویسه باشد. اگر آدرس IP وارد نکنید، همه آدرس ها کنترل می شوند.

نکته:
اگر یک آدرس *IP* به طور خودکار تعیین شود (مثلاً از طریق *DHCP* تعیین شود)، ممکن است اتصال قابل دسترسی نباشد. یک آدرس *IP* ثابت پیکربندی کنید.

Method of Choosing Port

روشی برای تعیین درگاه ها انتخاب کنید.

❏ Service Name

اگر **Service Name** را برای **Method of Choosing Port** انتخاب می کنید، یک گزینه انتخاب نمایید.

❏ Transport Protocol

اگر **Port Number** را برای **Method of Choosing Port** انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.

موارد	تنظیمات و توضیحات
Any Protocol	برای کنترل انواع پروتکل ها این را انتخاب کنید.
TCP	برای کنترل داده ها برای حالت تک بخشی این را انتخاب کنید.
UDP	برای کنترل داده ها برای پخش و حالت چند بخشی این را انتخاب کنید.
ICMPv4	برای کنترل فرمان ping این را انتخاب کنید.

❏ Local Port

اگر **Port Number** را برای **Method of Choosing Port** و **TCP** یا **UDP** را برای **Transport Protocol** انتخاب می کنید، شماره های درگاه را برای کنترل بسته های دریافتی وارد کرده و آنها را با ویرگول جدا نمایید. می توانید حداکثر تا 10 شماره درگاه وارد کنید.

مثال: 20, 80, 119, 5220

اگر شماره درگاه را وارد نکنید، همه درگاه ها کنترل می شوند.

❏ Remote Port

اگر **Port Number** را برای **Method of Choosing Port** و **TCP** یا **UDP** را برای **Transport Protocol** انتخاب می کنید، شماره های درگاه را برای کنترل ارسال بسته ها وارد کرده و آنها را با ویرگول جدا نمایید. می توانید حداکثر تا 10 شماره درگاه وارد کنید.

مثال: 25, 80, 143, 5220

اگر شماره درگاه را وارد نکنید، همه درگاه ها کنترل می شوند.

IKE Version

گزینه **IKEv1** یا **IKEv2** را برای **IKE Version** انتخاب کنید. یکی از آنها را با توجه به دستگاه متصل به اسکنر انتخاب کنید.

❑ IKEv1

اگر **IKEv1** را برای **IKE Version** انتخاب کنید، موارد زیر نمایش داده می شود.

موارد	تنظیمات و توضیحات
Authentication Method	اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید. گواهی استفاده شده با یک سیاست پیش فرض همراه است.
Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.

❑ IKEv2

اگر **IKEv2** را برای **IKE Version** انتخاب کنید، موارد زیر نمایش داده می شود.

موارد		تنظیمات و توضیحات
Local	Authentication Method	اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید. گواهی استفاده شده با یک سیاست پیش فرض همراه است.
	ID Type	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب کنید، باید نوع شناسه اسکنر را انتخاب کنید.
	ID	شناسه اسکنر را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «=» را نیز در نظر بگیرید. **IP Address**: قالب IPv4 یا IPv6 را وارد کنید. **FQDN**: ترکیبی بین 1 و 255 نویسه با استفاده از A–Z، a–z، 0–9، - و نقطه (.) وارد کنید. **Email Address**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «@» را نیز در نظر بگیرید. **Key ID**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.
Remote	Authentication Method	اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید. گواهی استفاده شده با یک سیاست پیش فرض همراه است.
	ID Type	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، باید نوع شناسه را برای دستگاهی که می خواهید تأیید کنید، انتخاب نمایید.
	ID	شناسه اسکنری را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «=» را نیز در نظر بگیرید. **IP Address**: قالب IPv4 یا IPv6 را وارد کنید. **FQDN**: ترکیبی بین 1 و 255 نویسه با استفاده از A–Z، a–z، 0–9، - و نقطه (.) وارد کنید. **Email Address**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «@» را نیز در نظر بگیرید. **Key ID**: بین 1 تا 255 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.

Encapsulation

اگر **IPsec** را برای **Access Control** انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.

موارد	تنظیمات و توضیحات
Transport Mode	اگر در LAN مشابه فقط از اسکنر استفاده می کنید، این را انتخاب کنید. بسته های IP لایه 4 یا لایه بالاتر رمزنگاری می شوند.

موارد	تنظیمات و توضیحات
Tunnel Mode	اگر از اسکنر در شبکه دارای اینترنت مانند IPsec-VPN استفاده می کنید، این گزینه را انتخاب کنید. عنوان و داده های بسته های IP رمزنگاری می شوند. **Remote Gateway(Tunnel Mode)**: اگر گزینه **Tunnel Mode** را برای **Encapsulation** انتخاب می کنید، یک آدرس درگاه بین 1 و 39 نویسه وارد کنید.

Security Protocol

اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید.

موارد	تنظیمات و توضیحات
ESP	برای اطمینان از یکپارچگی تأیید اعتبار و داده ها، این گزینه را انتخاب کنید و داده ها را رمزنگاری کنید.
AH	برای اطمینان از یکپارچگی تأیید اعتبار و داده ها، این گزینه را انتخاب کنید. حتی اگر رمزنگاری داده ها ممنوع باشد، می توانید از IPsec استفاده کنید.

Algorithm Settings

توصیه می شود گزینه **Any** را برای همه تنظیمات انتخاب کنید یا یک مورد غیر از **Any** برای هر تنظیم انتخاب نمایید. اگر **Any** را برای برخی از تنظیمات انتخاب کنید و موردی غیر از **Any** را برای تنظیمات دیگر انتخاب کنید، دستگاه ممکن است بسته به دستگاه دیگری که قصد تأیید آن را دارید ارتباط برقرار نکند.

موارد		تنظیمات و توضیحات
IKE	Encryption	الگوریتم رمزنگاری را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می کند.
	Authentication	الگوریتم تأیید هویت را برای IKE انتخاب کنید.
	Key Exchange	الگوریتم تبادل کلید را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می کند.
ESP	Encryption	الگوریتم رمزنگاری را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
	Authentication	الگوریتم تأیید هویت را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
AH	Authentication	الگوریتم رمزنگاری را برای AH انتخاب کنید. این زمانی موجود است که **AH** برای **Security Protocol** انتخاب شده باشد.

ترکیب Local Address (Scanner) و Remote Address(Host) در Group Policy

		تنظیم **Local Address (Scanner)**		
		IPv4	IPv6*2	Any addresses*3
تنظیم Remote Address(Host)	IPv4*1	✓	-	✓
	IPv6*1، *2	-	✓	✓
	خالی	✓	✓	✓

*1 اگر **IPsec** برای **Access Control** انتخاب شود، نمی توانید طول پیشوند را تعیین کنید.

*2 اگر **IPsec** برای **Access Control** انتخاب شود می توانید یک آدرس لینک محلی (fe80::) انتخاب کنید ولی سیاست گروهی غیرفعال می شود.

*3 به جز آدرس های لینک محلی IPv6.

اطلاعات مرتبط

◀ "اجرای Web Config در یک مرورگر وب" در صفحه 36

مرجع نام سرویس در سیاست گروهی

نکته:
سرویس‌هایی که موجود نباشند نمایش داده می‌شوند ولی نمی‌توانند انتخاب شوند.

نام سرویس	نوع پروتکل	شماره درگاه محلی	شماره درگاه راه‌دور	ویژگی های کنترل شده
Any	–	–	–	همه سرویس‌ها
ENPC	UDP	3289	هر درگاه	جستجو برای اسکنر از برنامه‌هایی مانند Epson Device Admin و یک درایور اسکنر
SNMP	UDP	161	هر درگاه	دستیابی و پیکربندی MIB از برنامه‌هایی مانند Epson Device Admin و درایور اسکنر Epson
WSD	TCP	هر درگاه	5357	کنترل WSD
WS-Discovery	UDP	3702	هر درگاه	جستجوی اسکنرهای WSD
Network Scan	TCP	1865	هر درگاه	باز-ارسال داده‌های اسکن شده از Document Capture Pro
Network Push Scan	TCP	هر درگاه	2968	دریافت اطلاعات کار برای فرآیند اسکن و ارسال همزمان از طریق برنامه Document Capture Pro
Network Push Scan Discovery	UDP	2968	هر درگاه	جستجوی رایانه از اسکنر
FTP Data (Remote)	TCP	هر درگاه	20	سرویس‌گیرنده FTP (باز-ارسال داده‌های اسکن‌شده) با این حال، این فقط می‌تواند یک سرور FTP را کنترل کند که از درگاه راه دور شماره 20 استفاده می‌کند.
FTP Control (Remote)	TCP	هر درگاه	21	سرویس‌گیرنده FTP (کنترل داده‌های اسکن‌شده باز-ارسال شده)
CIFS (Remote)	TCP	هر درگاه	445	سرویس‌گیرنده CIFS (باز-ارسال داده‌های اسکن‌شده به یک پوشه)
NetBIOS Name Service (Remote)	UDP	هر درگاه	137	سرویس‌گیرنده CIFS (باز-ارسال داده‌های اسکن‌شده به یک پوشه)
NetBIOS Datagram Service (Remote)	UDP	هر درگاه	138	
NetBIOS Session Service (Remote)	TCP	هر درگاه	139	

نام سرویس	نوع پروتکل	شماره درگاه محلی	شماره درگاه راه‌دور	ویژگی های کنترل شده
HTTP (Local)	TCP	80	هر درگاه	سرور HTTP(S) (ارسال داده Web Config و WSD)
HTTPS (Local)	TCP	443	هر درگاه	
HTTP (Remote)	TCP	هر درگاه	80	سرویس‌گیرنده HTTP(S) (بروزرسانی ثابت‌افزار و گواهی اصلی)
HTTPS (Remote)	TCP	هر درگاه	443	

پیکربندی نمونه های IPsec/IP Filtering

صرفاً دریافت بسته های IPsec

این نمونه صرفاً برای پیکربندی یک سیاست پیش فرض است.

Default Policy:

- **IPsec/IP Filtering**: **Enable**
- **Access Control**: **IPsec**
- **Authentication Method**: **Pre-Shared Key**
- **Pre-Shared Key**: تا حداکثر 127 نویسه وارد کنید.

Group Policy: پیکربندی نکنید.

دریافت داده های اسکن و تنظیمات اسکنر

این نمونه اجازه تبادل داده های اسکن و پیکربندی اسکنر از طریق خدمات مشخص شده را می دهد.

Default Policy:

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

Group Policy:

- **Enable this Group Policy**: کادر را علامت بزنید.
- **Access Control**: **Permit Access**
- **Remote Address(Host)**: آدرس IP یک سرویس گیرنده
- **Method of Choosing Port**: **Service Name**
- **Service Name**: کادر **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)** و **Network Scan** را علامت بزنید.

دریافت امکان دسترسی تنها از یک آدرس IP خاص

این نمونه اجازه دسترسی اسکنر را به یک آدرس IP خاص می دهد.

Default Policy:

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

Group Policy:

- **Enable this Group Policy**: کادر را علامت بزنید.

❑ **Access Control: Permit Access**

❑ **Remote Address(Host)**: آدرس IP یک سرویس گیرنده سرپرست

نکته:
صرفنظر از پیکربندی سیاست، سرویس گیرنده قادر خواهد بود به اسکنر دسترسی داشته و آن را پیکربندی نماید.

پیکربندی گواهی برای فیلترگذاری IPsec/IP

گواهی سرویس‌گیرنده برای فیلترگذاری IPsec/IP را پیکربندی کنید. وقتی آن را تنظیم کنید، قادر خواهید بود گواهی را به عنوان یک روش تأیید هویت برای فیلترگذاری IPsec/IP انتخاب کنید. اگر می‌خواهید مرجع صدور گواهی را پیکربندی کنید به **CA Certificate** بروید.

1. وارد Web Config شوید و زبانه **Network Security** > **IPsec/IP Filtering** > **Client Certificate** را انتخاب کنید.
2. گواهی را در **Client Certificate** وارد کنید.

اگر قبلاً یک گواهی نشر شده توسط مرجع صدور گواهی را وارد کرده‌اید، می‌توانید گواهی را کپی کنید و در فیلترگذاری IPsec/IP کپی کنید. برای کپی کردن، گواهی را از **Copy From** انتخاب کنید و سپس روی **Copy** کلیک کنید.

اطلاعات مرتبط

◀ "اجرای Web Config در یک مرورگر وب" در صفحه 36
◀ "پیکربندی یک CA-signed Certificate" در صفحه 92
◀ "پیکربندی یک CA Certificate" در صفحه 96

اتصال اسکنر به شبکه IEEE802.1X

پیکربندی شبکه IEEE 802.1X

وقتی IEEE 802.1X را در اسکنر تنظیم می‌کنید، قادر خواهید بود از آن در شبکه متصل به یک سرور RADIUS، یک سوییچ LAN با عملکرد تأیید هویت یا یک نقطه دسترسی استفاده کنید.

1. وارد Web Config شوید و زبانه **Network Security** > **IEEE802.1X** > **Basic** را انتخاب کنید.
2. برای هر مورد یک مقدار وارد کنید.

اگر می‌خواهید از اسکنر روی شبکه Wi-Fi استفاده کنید، روی **Wi-Fi Setup** کلیک کنید و یک SSID انتخاب یا وارد کنید.

نکته:
می توانید تنظیمات را بین اترنت و *Wi-Fi* به اشتراک بگذارید.

3. روی **Next** کلیک کنید.

یک پیام تأیید نشان داده می‌شود.

4. روی **OK** کلیک کنید.

اسکنر به روزرسانی می‌شود.

اطلاعات مرتبط

◀ "اجرای Web Config در یک مرورگر وب" در صفحه 36

موارد تنظیم شبکه IEEE802.1X

موارد	تنظیمات و توضیحات	
IEEE802.1X (Wired LAN)	می توانید تنظیمات صفحه (**IEEE802.1X** > **Basic**) برای LANIEEE802.1X (باسیم) را فعال یا غیرفعال کنید.	
IEEE802.1X (Wi-Fi)	وضعیت اتصال IEEE802.1X(Wi-Fi) نمایش داده می‌شود.	
Connection Method	روش اتصال شبکه فعلی نشان داده می شود.	
EAP Type	گزینه ای برای یک روش تأیید اعتبار بین اسکنر و سرور RADIUS انتخاب کنید.	
	EAP-TLS	شما باید یک گواهی امضاء شده توسط CA دریافت و وارد کنید.
	PEAP-TLS	
	PEAP/MSCHAPv2	شما باید یک رمز عبور پیکربندی کنید.
	EAP-TTLS	
User ID	برای استفاده از تأیید اعتبار یک سرور RADIUS، یک شناسه پیکربندی کنید. بین 1 تا 128 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید.	
Password	برای تایید اسکنر یک رمز عبور پیکربندی کنید. بین 1 تا 128 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. اگر از سرور Windows به‌عنوان سرور RADIUS استفاده می‌کنید، می‌توانید حداکثر 127 نویسه را وارد کنید.	
Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید را وارد نمایید.	
Server ID	می توانید یک شناسه سرور برای تأیید اعتبار با یک سرور RADIUS تعیین شده پیکربندی کنید. تأییدکننده بررسی می‌کند که آیا شناسه سرور در فیلد subject/subjectAltName گواهی سروری که از یک سرور RADIUS ارسال شده است وجود دارد یا خیر. بین 0 تا 128 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید.	
LAN) Certificate Validation سیمی)	اگر می‌خواهید **Certificate Validation** را با استفاده از **IEEE802.1X (Wired LAN)** اجرا کنید، **Enable** را انتخاب کنید. اگر فعال‌کردن را انتخاب کنید، اطلاعات مربوطه را ببینید و **CA Certificate** را وارد کنید. توجه داشته باشید که Certificate Validation همیشه در IEEE802.1X (Wi-Fi) فعال است. حتما CA Certificate را وارد کنید.	
Anonymous Name	اگر **PEAP-TLS** یا **PEAP/MSCHAPv2** را برای **EAP Type** انتخاب کنید، می‌توانید یک نام ناشناس را به‌جای شناسه کاربری برای فاز 1 تأیید هویت PEAP پیکربندی کنید. بین 0 تا 128 نویسه 1 ASCII-بایتی (0x20 تا 0x7E) وارد کنید.	
Encryption Strength	می‌توانید یکی از موارد زیر را انتخاب کنید.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

اطلاعات مرتبط

"پیکربندی یک CA Certificate" در صفحه 96

پیکربندی گواهی برای IEEE 802.1X

گواهی سرویس‌گیرنده برای IEEE802.1X را پیکربندی کنید. وقتی آن را تنظیم می‌کنید، قادر خواهید بود **EAP-TLS** و **PEAP-TLS** را به عنوان روش تأیید هویت IEEE 802.1X استفاده کنید. اگر می‌خواهید گواهی مرجع صدور گواهی را پیکربندی کنید به **CA Certificate** بروید.

1. وارد Web Config شوید و زبانه **Network Security** > **IEEE802.1X** > **Client Certificate** را انتخاب کنید.
2. در **Client Certificate** یک گواهی وارد کنید.

اگر قبلاً یک گواهی نشر شده توسط مرجع صدور گواهی را وارد کرده‌اید، می‌توانید گواهی را کپی کنید و در IEEE802.1X استفاده نمایید. برای کپی کردن، گواهی را از **Copy From** انتخاب کنید و سپس روی **Copy** کلیک کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

رفع مشکلات مربوط به امنیت پیشرفته

بازگرداندن تنظیمات امنیتی

اگر می خواهید محیطی بسیار امن مانند IPsec/IP Filtering ایجاد کنید، تنظیمات نادرست یا بروز مشکل در دستگاه یا سرور ممکن است مانع ایجاد ارتباط با دستگاه ها شود. در این صورت، تنظیمات امنیتی را بازگردانید تا تنظیمات مربوط به دستگاه دوباره اعمال شود یا امکان استفاده موقت شما فراهم گردد.

غیرفعال کردن عملکرد امنیتی با استفاده از Web Config

می‌توانید IPsec/IP Filtering را با استفاده از Web Config غیر فعال کنید.

1. وارد Web Config شوید و زبانه **Network Security** > **IPsec/IP Filtering** > **Basic** را انتخاب کنید.
2. **IPsec/IP Filtering** را غیرفعال کنید.

مشکلات مربوط به استفاده از ویژگی های امنیت شبکه

فراموش کردن کلید از قبل اشتراک گذاشته شده

یک کلید از قبل اشتراک گذاشته شده را پیکربندی مجدد کنید.

برای تغییر کلید، به Web Config وارد شوید و زبانه **Network Security** > **IPsec/IP Filtering** > **Basic** > **Default Policy** یا **Group Policy** را انتخاب کنید.

پس از تغییر دادن کلید پیش-مشترک، کلید پیش-مشترک را برای رایانه‌ها پیکربندی کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36
"ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 98

نمی توانید با IPsec Communication ارتباط برقرار کنید

الگوریتمی که اسکنر یا رایانه پشتیبانی نمی کند را مشخص کنید.

اسکنر از الگوریتم های زیر پشتیبانی می کند. تنظیمات رایانه را بررسی کنید.

روش های امنیتی	الگوریتم ها
الگوریتم رمزگذاری IKE	AES-CBC-128، AES-CBC-192، AES-CBC-256، AES-GCM-128*، AES-GCM-192*، AES-256*، 3DES
الگوریتم تایید هویت IKE	SHA-1، SHA-256، SHA-384، SHA-512، MD5
الگوریتم تبادل کلید 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*
الگوریتم رمزگذاری ESP	AES-CBC-128، AES-CBC-192، AES-CBC-256، AES-GCM-128، AES-GCM-192، AES-GCM-256، 3DES
الگوریتم تایید هویت ESP	SHA-1، SHA-256، SHA-384، SHA-512، MD5
الگوریتم تایید هویت AH	SHA-1، SHA-256، SHA-384، SHA-512، MD5

* فقط برای IKEv2 در دسترس است

اطلاعات مرتبط

"ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 98

نمی تواند به طور ناگهانی ارتباط برقرار کند

آدرس IP اسکنر تغییر یافته یا قابل استفاده نمی باشد.

هنگامی که آدرس IP ثبت شده در آدرس محلی در Group Policy تغییر یافته باشد یا قابل استفاده نباشد، ارتباط IPsec شکل نمی گیرد. از قسمت پانل کنترل اسکنر IPsec را غیرفعال کنید.

اگر تاریخ DHCP گذشته است، دوباره راه اندازی می شود یا تاریخ آدرس IPv6 گذشته است یا دریافت نشده است، ممکن است آدرس IP ثبت شده برای زبانه Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) اسکنر یافت نشود.

از آدرس IP ایستا استفاده کنید.

آدرس IP رایانه تغییر یافته یا قابل استفاده نمی باشد.

هنگامی که آدرس IP ثبت شده در آدرس راه دور در Group Policy تغییر یافته باشد یا قابل استفاده نباشد، ارتباط IPsec شکل نمی گیرد.

از قسمت پانل کنترل اسکنر IPsec را غیرفعال کنید.

اگر تاریخ DHCP گذشته است، دوباره راه اندازی می شود یا تاریخ آدرس IPv6 گذشته است یا دریافت نشده است، ممکن است آدرس IP ثبت شده برای زبانه Web Config (**Network Security** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) اسکنر یافت نشود.

از آدرس IP ایستا استفاده کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36
"ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 98

عدم امکان اتصال بعد از پیکربندی فیلترگذاری IPsec/IP

تنظیمات فیلترگذاری IPsec/IP نادرست می‌باشند.

فیلترگذاری IPsec/IP را از طریق پانل کنترل اسکنر غیرفعال کنید. اسکنر و رایانه را به هم وصل کنید و تنظیمات فیلترگذاری IPsec/IP را مجدداً اعمال کنید.

اطلاعات مرتبط

"ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 98

بعد از پیکربندی IEEE 802.1X نمی توانید به دستگاه دسترسی داشته باشید

تنظیمات IEEE 802.1X نادرست می باشند.

از پانل کنترل اسکنر، IEEE 802.1X و Wi-Fi را غیرفعال کنید. اسکنر و رایانه را وصل کنید و سپس دوباره IEEE 802.1X را پیکربندی کنید.

اطلاعات مرتبط

"پیکربندی شبکه IEEE 802.1X" در صفحه 109

مشکلات مربوط به استفاده از یک گواهی دیجیتالی

عدم موفقیت در وارد کردن CA-signed Certificate

CA-signed Certificate و اطلاعات ارائه شده در CSR مطابقت ندارند.

اگر CA-signed Certificate و CSR اطلاعات یکسانی نداشته باشند، CSR قابل وارد کردن نیست. موارد زیر را بررسی کنید:

- ❑ آیا می‌خواهید گواهی را در دستگاهی وارد کنید که اطلاعات مشابهی ندارد؟
  اطلاعات CSR را بررسی کنید و سپس گواهی را در دستگاهی که اطلاعات مشابه دارد وارد کنید.
- ❑ آیا بعد از ارسال CSR به مرجع صدور گواهی، CSR ذخیره شده در اسکنر را رونویسی کردید؟
  گواهی امضاء شده از طریق CA را دوباره از طریق CSR دریافت کنید.

حجم CA-signed Certificate بیش از 5 کیلوبایت است.

شما نمی‌توانید CA-signed Certificate را که بزرگ‌تر از 5 کیلوبایت است وارد کنید.

رمز عبور برای وارد کردن گواهی نادرست است.

رمز عبور صحیح را وارد کنید. اگر رمز عبور را فراموش کنید، نمی‌توانید گواهی را وارد کنید. CA-signed Certificate را مجدداً دریافت کنید.

اطلاعات مرتبط

"وارد کردن گواهی امضاء شده از طریق CA" در صفحه 93

نمی توانید گواهی خود امضاء را به روزرسانی کنید

Common Name وارد نشده است.

Common Name باید وارد شود.

نویسه‌های پشتیبانی نشده در کادر Common Name وارد شده‌اند.

بین 1 و 128 نویسه از IPv4، IPv6، نام میزبان یا فرمت FQDN در قالب (ASCII (0x20–0x7E وارد کنید.

یک ویرگول یا فاصله در کادر نام مشترک وارد شده است.

اگر ویرگول وارد شده است، **Common Name** در آن نقطه تقسیم می‌شود. اگر فقط یک فاصله قبل یا بعد از ویرگول وارد شده باشد، خطایی روی می‌دهد.

اطلاعات مرتبط

"به روزرسانی گواهی خود امضاء" در صفحه 95

نمی توانید CSR ایجاد کنید

Common Name وارد نشده است.

Common Name باید وارد شود.

نویسه‌های پشتیبانی نشده در Common Name، Organization، Organizational Unit، Locality و State/Province وارد شده‌اند.

نویسه‌هایی از IPv4، IPv6، نام میزبان یا قالب FQDN در قالب (ASCII (0x20–0x7E وارد کنید.

در کادر Common Name از ویرگول یا فاصله استفاده شده است.

اگر ویرگول وارد شده است، **Common Name** در آن نقطه تقسیم می‌شود. اگر فقط یک فاصله قبل یا بعد از ویرگول وارد شده باشد، خطایی روی می‌دهد.

اطلاعات مرتبط

"دریافت گواهی امضاء شده از طریق CA" در صفحه 92

هشداری مربوط به یک گواهی دیجیتالی ظاهر می شود

پیام ها	علت/باید چه کاری انجام داد
Enter a Server Certificate.	**علت:** فایلی را برای وارد کردن انتخاب نکرده اید. **باید چه کاری انجام داد:** یک فایل انتخاب کرده و روی **Import** کلیک کنید.

پیام ها	علت/باید چه کاری انجام داد
CA Certificate 1 is not entered.	**علت:** گواهی CA شماره 1 وارد نشده است و فقط گواهی CA شماره 2 وارد شده است. **باید چه کاری انجام داد:** ابتدا گواهی CA شماره 1 را وارد کنید.
Invalid value below.	**علت:** نویسه های پشتیبانی نشده ای در مسیر فایل و یا رمز عبور قرار دارد. **باید چه کاری انجام داد:** دقت کنید نویسه ها به طور صحیح برای مورد وارد شوند.
Invalid date and time.	**علت:** تاریخ و زمان اسکنر تنظیم نشده اند. **باید چه کاری انجام داد:** با استفاده از Web Config یا EpsonNet Config تاریخ و زمان را تنظیم کنید.
Invalid password.	**علت:** رمز عبور تنظیم شده برای گواهی CA و رمز عبور وارد شده مطابقت ندارند. **باید چه کاری انجام داد:** رمز عبور صحیح را وارد کنید.
Invalid file.	**علت:** فایل گواهی با فرمت X509 وارد نمی کنید. **باید چه کاری انجام داد:** دقت کنید گواهی صحیحی را که از طرف مرجع مورد اعتماد صدور گواهی ارسال شده است انتخاب کنید.
	علت: فایلی که وارد کرده اید بسیار بزرگ است. حداکثر اندازه فایل 5 کیلوبایت است. **باید چه کاری انجام داد:** اگر فایل صحیح را انتخاب کرده اید، ممکن است گواهی خراب یا جعلی باشد.
	علت: زنجیره موجود در گواهی نامعتبر است. **باید چه کاری انجام داد:** برای اطلاعات بیشتر درباره گواهی، به وب سایت مرجع صدور گواهی مراجعه کنید.
Cannot use the Server Certificates that include more than three CA certificates.	**علت:** فایل گواهی با فرمت PKCS#12 بیشتر از 3 گواهی CA دارد. **باید چه کاری انجام داد:** هر گواهی را با تبدیل از فرمت PKCS#12 به فرمت PEM وارد کنید یا فایل گواهی با فرمت PKCS#12 وارد کنید که 2 گواهی CA دارد.

پیام ها	علت/باید چه کاری انجام داد
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**علت:** تاریخ گواهی گذشته است. **باید چه کاری انجام داد:** ❑ اگر تاریخ گواهی گذشته است، گواهی جدیدی دریافت و وارد کنید. ❑ اگر گواهی تاریخ گذشته نیست، دقت کنید تاریخ و زمان اسکنر به درستی تنظیم شده باشند.
Private key is required.	**علت:** کلید خصوصی جفت شده ای با گواهی وجود ندارد. **باید چه کاری انجام داد:** ❑ اگر گواهی فرمت PEM/DER دارد و با استفاده از یک CSR و از طریق رایانه دریافت شده باشد، فایل کلید خصوصی را مشخص کنید. ❑ اگر گواهی فرمت PKCS#12 دارد و با استفاده از یک CSR و از طریق رایانه دریافت شده باشد، فایلی ایجاد کنید که محتوی کلید خصوصی باشد.
	علت: گواهی PEM/DER دریافت شده از طریق CSR و با استفاده از Web Config را دوباره وارد کرده اید. **باید چه کاری انجام داد:** اگر گواهی فرمت PEM/DER دارد و با استفاده از یک CSR و از طریق Web Config دریافت شده باشد، فقط می توانید یک بار آن را وارد کنید.
Setup failed.	**علت:** نمی توانید پیکربندی را تمام کنید زیرا ارتباط بین اسکنر و رایانه برقرار نشده است یا به دلیل خطاهایی، فایل قابل خواندن نیست. **باید چه کاری انجام داد:** بعد از بررسی فایل مشخص شده و ارتباط، دوباره فایل را وارد کنید.

اطلاعات مرتبط

"درباره گواهی دیجیتالی" در صفحه 91

حذف گواهی امضاء شده از طریق CA به اشتباه

هیچ فایل پشتیبان برای گواهی امضا شده توسط CA وجود ندارد.

اگر فایل پشتیبان دارید، دوباره گواهی را وارد کنید.

اگر با استفاده از یک CSR که از Web Config ایجاد شده است، یک گواهی دریافت کنید، نمی‌توانید گواهی حذف شده را دوباره وارد کنید. یک CSR ایجاد کنید و گواهی جدیدی دریافت کنید.

اطلاعات مرتبط

"وارد کردن گواهی امضاء شده از طریق CA" در صفحه 93
"حذف گواهی امضاء شده از طریق CA" در صفحه 95

استفاده از Epson Open Platform

Epson Open Platform کلیات

Epson Open Platform پلتفرمی است که به شما امکان می‌دهد از سیستم‌های تأیید هویت با این اسکنر استفاده کنید.

از آن می‌توان همراه با Epson Print Admin (سیستم تأیید هویت Epson) یا سیستم تأیید هویت شخص ثالث استفاده کرد. می‌توانید گزارش‌ها را بر اساس دستگاه و کاربر دریافت کنید، دستگاه‌هایی را که کاربران و گروه‌ها می‌توانند استفاده کنند، پیکربندی کنید، محدودیت هایی را برای عملکردها تعیین کنید و اقدامات دیگری را انجام دهید.

اگر به دستگاه تأیید هویت متصل شوید، می‌توانید تأیید هویت کاربر را با استفاده از کارت شناسایی نیز انجام دهید.

پیکربندی Epson Open Platform

برای اینکه بتوانید از طریق سیستم احراز هویت، دستگاه را استفاده کنید، Epson Open Platform را فعال نمایید.

1. کلید محصول را از وب‌سایت اختصاصی دریافت کنید.

   برای کسب جزئیات بیشتر، مانند نحوه دریافت کلید محصول، به دفترچه راهنمای Epson Open Platform مراجعه کنید.

2. وارد Web Config شوید و سپس زبانه **Epson Open Platform** > **Product Key or License Key** را انتخاب کنید.

3. هر مورد را بررسی و تنظیم کنید.

   ❑ Serial Number

   شماره‌سریال دستگاه نمایش داده می‌شود.

   ❑ Epson Open Platform Version

   نسخه Epson Open Platform را انتخاب کنید. بسته به سیستم احراز هویت، نسخه مربوطه متفاوت خواهد بود.

   ❑ Product Key or License Key

   کلید محصولی را که به دست آورده‌اید، وارد کنید.

4. روی **Next** کلیک کنید.

   صفحه تایید تنظیم ظاهر می‌شود.

5. روی **OK** کلیک کنید.

   تنظیمات روی اسکنر اعمال می‌شود.

نکته:
هنگامی که سیستم با *Epson Open Platform* همگام است، نمی‌توانید از *Epson Print Admin Serverless* استفاده کنید.

اعتبارسنجی Epson Open Platform

می‌توانید اعتبار Epson Open Platform را با استفاده از یکی از روش‌های زیر بررسی کنید.

❑ Web Config

کلید محصولی که در زبانه **Epson Open Platform** > **Product Key or License Key** > **Product Key or License Key** و زبانه **Epson Open Platform** > **Authentication System** وارد شده است در سمت چپ درخت منو نمایش داده می‌شود.

❑ پنل کنترل اسکنر

بررسی کنید که کلید محصول در **تنظیم**> **اطلاعات دستگاه**> **اطلاعات Epson Open Platform** نمایش داده شود.

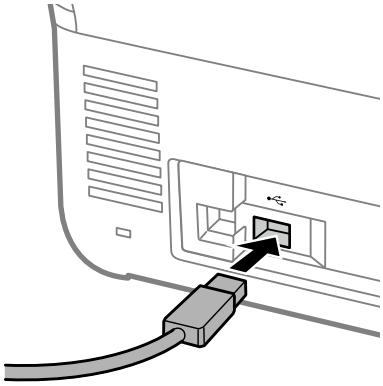
نصب یک دستگاه احراز هویت

وصل کردن دستگاه تأیید هویت

نکته:
هنگام استفاده از سیستم تأیید هویت از یک دستگاه تأیید هویت استفاده می‌شود.

مهم:
وقتی دستگاه تأیید هویت را به چندین اسکنر وصل می‌کنید، از محصولی با شماره مدل یکسان استفاده کنید.

کابل USB کارت‌خوان را به درگاه USB رابط خارجی اسکنر وصل کنید.



بررسی عملیات برای دستگاه تأیید هویت

از طریق پانل کنترل اسکنر می‌توانید وضعیت اتصال شبکه و تشخیص کارت تأیید هویت برای دستگاه تأیید هویت را بررسی کنید.
اگر مسیر **تنظیم** > **اطلاعات دستگاه** > **وضعیت دستگاه تأیید هویت** را انتخاب کنید، اطلاعات نمایش داده می‌شوند.

تأیید شناسایی کارت احراز هویت

می‌توانید قابل شناسایی بودن کارت‌های احراز هویت را با استفاده از Web Config بررسی کنید.

1. وارد Web Config شوید و سپس زبانه **Device Management** > **Card Reader** را انتخاب کنید.
2. کارت تأیید هویت را بالای دستگاه کارت‌خوان تأیید هویت نگه دارید.
3. روی **Check** کلیک کنید.
   نتیجه، نمایش داده می‌شود.

عیب‌یابی دستگاه احراز هویت

خواندن کارت احراز هویت ممکن نیست

موارد زیر را بررسی کنید.

- ❑ بررسی کنید که آیا دستگاه تأیید هویت به‌درستی به اسکنر متصل شده است یا خیر.
  دستگاه تأیید هویت را به درگاه USB رابط خارجی واقع در پشت اسکنر وصل کنید.
- ❑ بررسی کنید که آیا دستگاه تأیید هویت و کارت تأیید هویت، تأیید شده است یا خیر.
  برای کسب اطلاعات در مورد دستگاه‌ها و کارت‌های احراز هویت پشتیبانی‌شده، با فروشنده خود تماس بگیرید.

نگهداری

تمیز کردن قسمت خارجی اسکنر

هر گونه لکه روی روکش بیرونی را توسط یک دستمال خشک یا یک دستمال نمدار با پاک کننده ملایم و آب پاک کنید.

مهم:

- ❑ هرگز از الکل، تینر یا هر حلال خورنده دیگر برای تمیز کردن اسکنر استفاده نکنید. ممکن است تغییر شکل یا تغییر رنگ رخ دهد.
- ❑ اجازه ندهید آب به داخل محصول وارد شود. این امر سبب بروز نقص در کارکرد دستگاه می‌شود.
- ❑ هرگز قاب اسکنر را باز نکنید.

1. دکمه ⏻ را برای خاموش کردن اسکنر فشار دهید.
2. آداپتور AC را از اسکنر جدا کنید.
3. قاب بیرونی را با یک دستمال مرطوب شده با ماده شوینده ملایم و آب تمیز کنید.

نکته:
صفحه لمسی را با دستمال نرم و خشک تمیز کنید.

تمیز کردن قسمت داخلی اسکنر

پس از مدتی استفاده از اسکنر، ممکن است کاغذ و گرد و غبار اتاق روی غلتک یا قسمت داخلی شیشه اسکنر بنشیند و باعث بروز اشکال در تغذیه کاغذ یا کیفیت تصویر اسکن شده گردد. قسمت داخلی اسکنر را پس از هر 5, 000 اسکن تمیز کنید.

آخرین عدد اسکن ها را می توانید در پانل کنترل یا Epson Scan 2 Utility بررسی کنید.

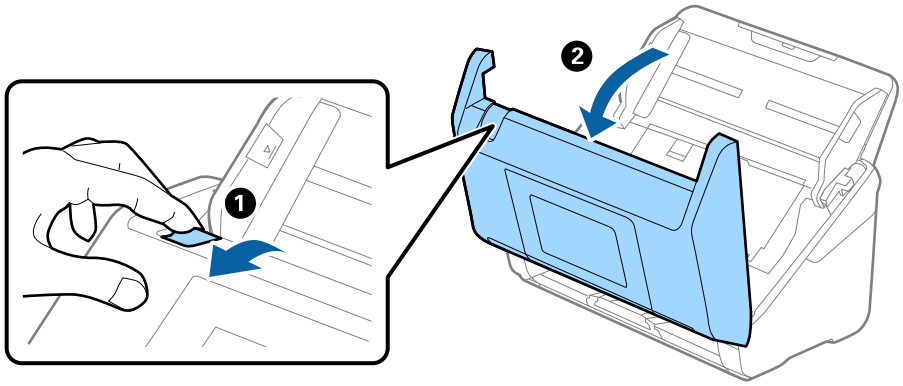
اگر سطح به موادی که زدودن آنها دشوار است آغشته شده است، برای تمیز کردن آن از کیت تمیز کردن اصل Epson استفاده کنید. برای ازبین‌بردن لکه‌ها از مقدار کمی پاک‌کننده روی دستمال تمیزکننده استفاده کنید.

مهم:

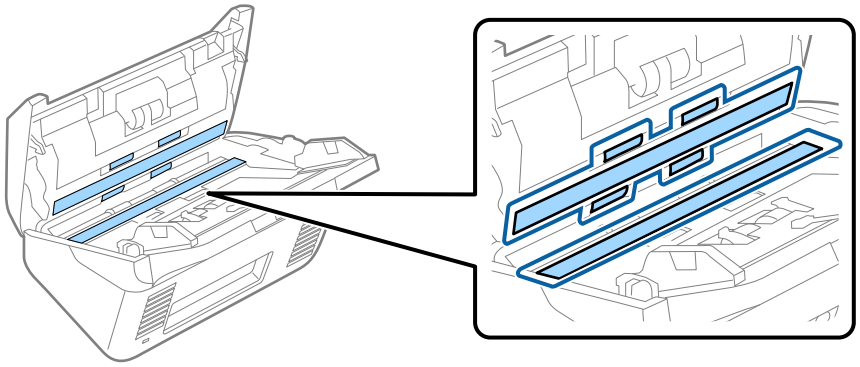
- ❑ هرگز از الکل، تینر یا هر حلال خورنده ای برای تمیز کردن اسکنر استفاده نکنید. ممکن است تغییر شکل یا تغییر رنگ رخ دهد.
- ❑ هرگز هیچ گونه مایع یا روانکار را روی اسکنر نپاشید. آسیب دیدن تجهیزات یا مدارها ممکن است باعث عملکرد غیرعادی شود.
- ❑ هرگز قاب اسکنر را باز نکنید.

1. دکمه ⏻ را برای خاموش کردن اسکنر فشار دهید.
2. آداپتور برق متناوب را از اسکنر جدا کنید.

3. اهرم را بکشید و قاب اسکنر را باز کنید.



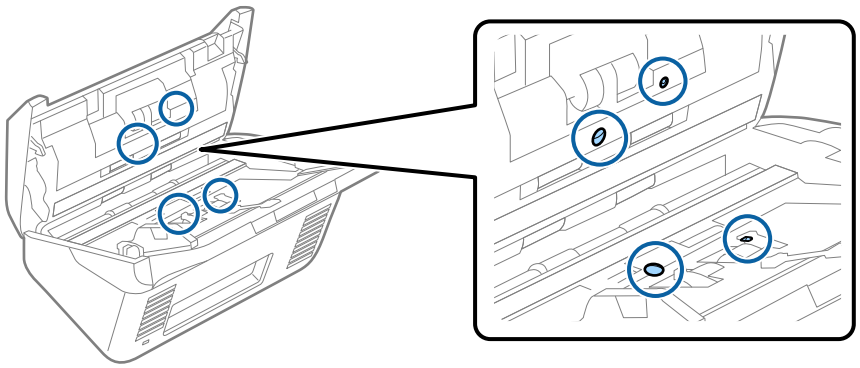
4. هرگونه لکه روی غلتک پلاستیکی (۴ مکان) و سطح شیشه‌ای در پایین درپوش اسکنر را پاک کنید. با یک دستمال نرم و بدون پُرز که کمی با تمیزکننده اختصاصی یا آب مرطوب شده است، پاک کنید.



مهم:

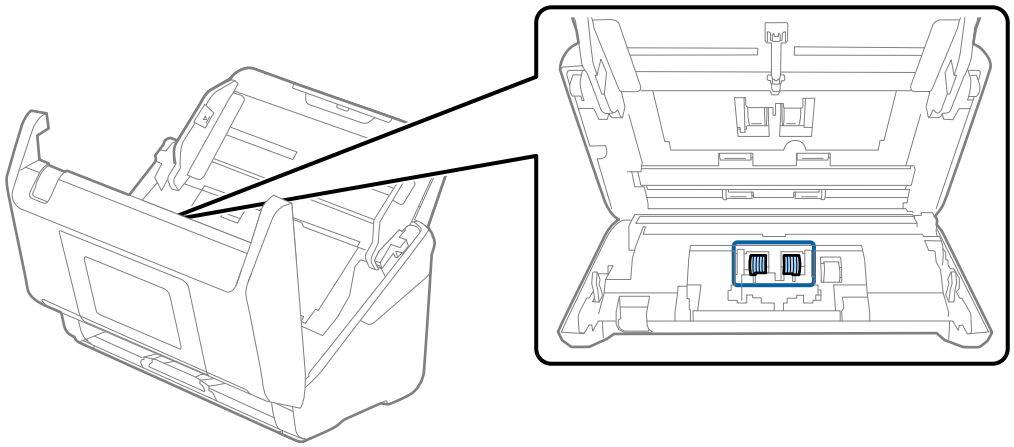
- ❏ فشار خیلی زیاد روی سطح شیشه وارد نکنید.
- ❏ از برس یا ابزار سخت استفاده نکنید. ایجاد هرگونه خراش روی شیشه ممکن است بر کیفیت اسکن تأثیر بگذارد.
- ❏ پاک‌کننده را مستقیماً روی سطح شیشه اسپری نکنید.

5. هرگونه لکه روی سنسورها را با یک گوش پاک کن پاک کنید.

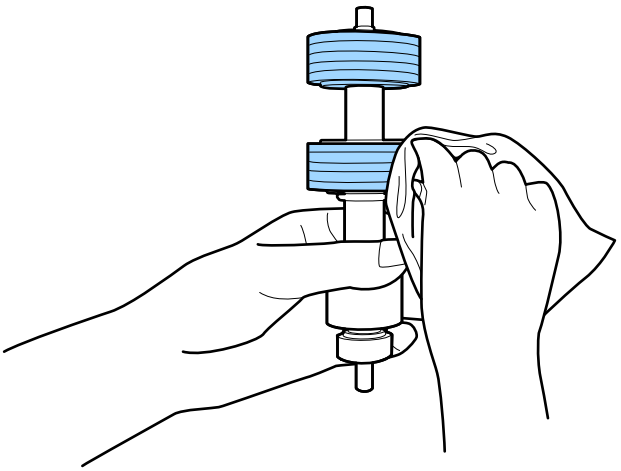


مهم:
از مایعاتی نظیر شوینده ها روی گوش پاک کن استفاده نکنید.

6. قاب را باز کرده و غلتک جداکننده را بیرون بیاورید.
برای کسب جزئیات بیشتر به «تعویض کیت مونتاژ غلتکی» مراجعه کنید.

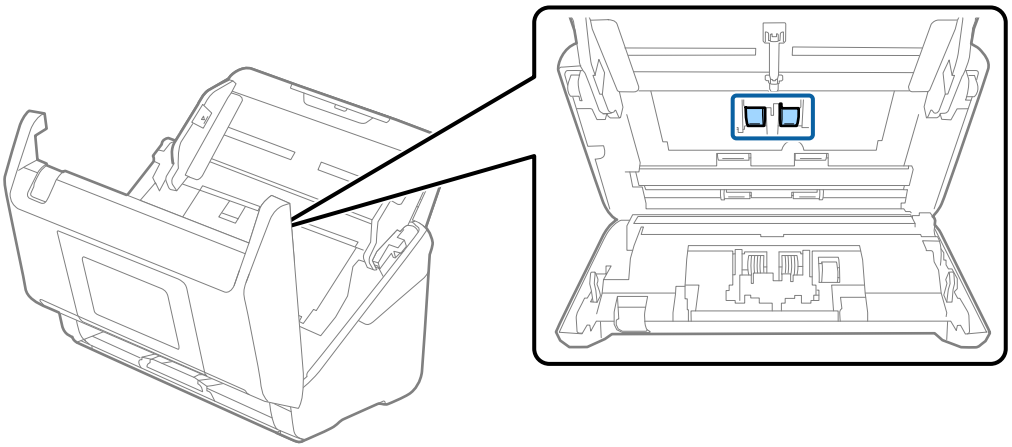


7. غلتک جداکننده را پاک کنید. با یک دستمال نرم و بدون پُرز که کمی با تمیزکننده اختصاصی یا آب مرطوب شده است پاک کنید.

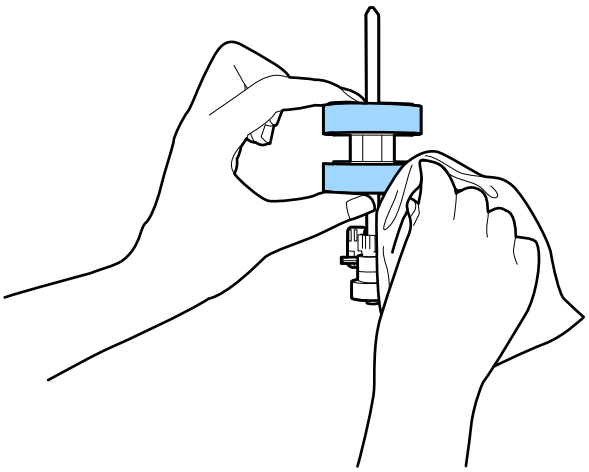


مهم:
برای تمیزکردن غلتک فقط از یک کیت تمیزکننده اصلی *Epson* یا یک دستمال نرم و مرطوب استفاده کنید. دستمال خشک ممکن است به سطح غلتک آسیب برساند.

8. درپوش را باز کرده و غلتک بلندکننده را بیرون بیاورید.
برای کسب جزئیات بیشتر به «تعویض کیت مونتاژ غلتکی» مراجعه کنید.



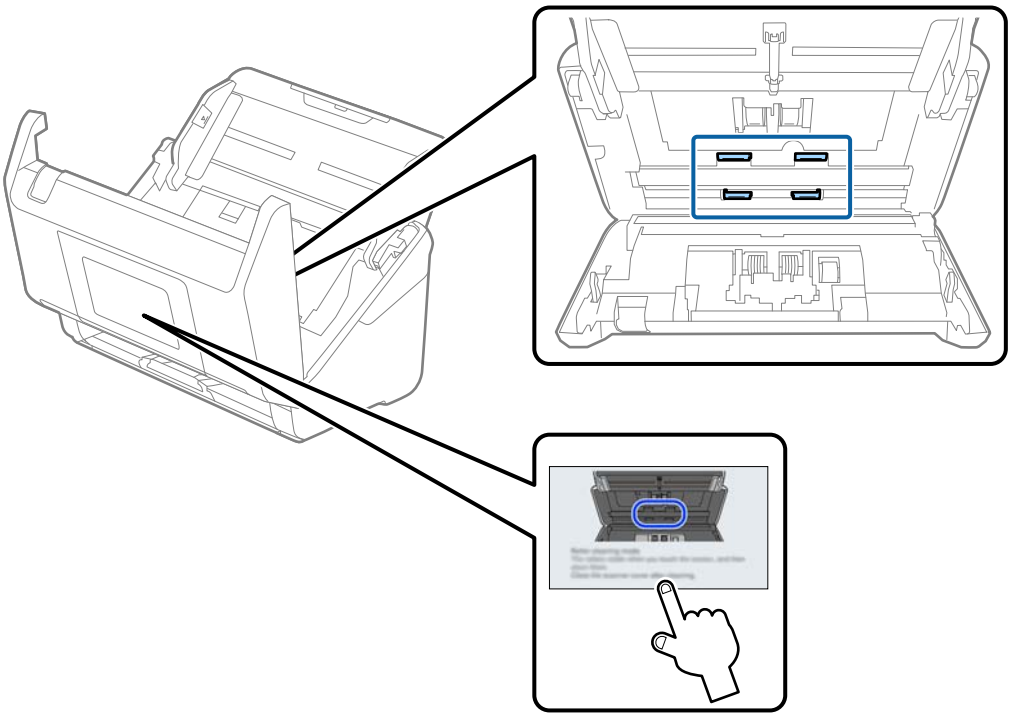
9. غلتک بلندکننده را پاک کنید. با یک دستمال نرم و بدون پُرز که کمی با تمیزکننده اختصاصی یا آب مرطوب شده است پاک کنید.



مهم:
برای تمیزکردن غلتک فقط از یک کیت تمیزکننده اصلی *Epson* یا یک دستمال نرم و مرطوب استفاده کنید. دستمال خشک ممکن است به سطح غلتک آسیب برساند.

10. قاب اسکنر را ببندید.
11. آداپتور برق متناوب را به پریز وصل کنید و سپس اسکنر را روشن کنید.
12. گزینه **تعمیر و نگهداری اسکنر** را از صفحه اصلی انتخاب کنید.
13. در صفحه **تعمیر و نگهداری اسکنر**، گزینه **تمیز کردن رولر** را انتخاب کنید.
14. اهرم را بکشید و قاب اسکنر را باز کنید.
اسکنر وارد حالت تمیزکردن غلتک می‌شود.

15. با ضربه زدن به هر نقطه از LCD، غلتک‌ها را به آرامی از پایین بچرخانید. سطح غلتک‌ها را با کیت تمیزکننده اصل Epson یا دستمال نرم آغشته به آب تمیز کنید. این کار را تا تمیز شدن کامل غلتک‌ها ادامه دهید.



احتیاط:!

هنگام کار با غلتک مراقب باشید دست‌ها یا موهایتان در مکانیسم دستگاه گیر نکند. ممکن است منجر به جراحت شود.

16. درپوش اسکنر را ببندید.

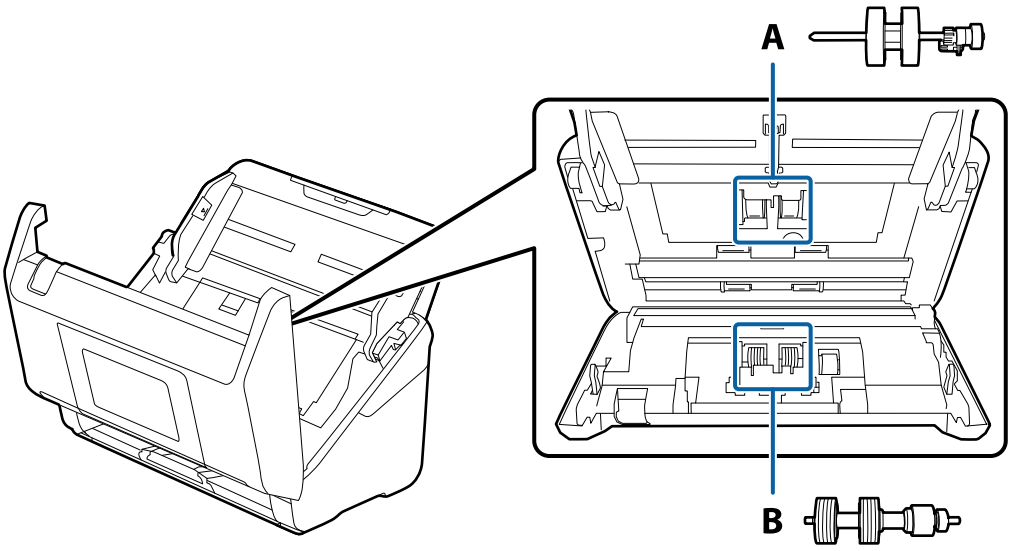
اسکنر از حالت تمیزکردن غلتک خارج می‌شود.

اطلاعات مرتبط

"تعویض کیت مجموعه غلتک" در صفحه 128

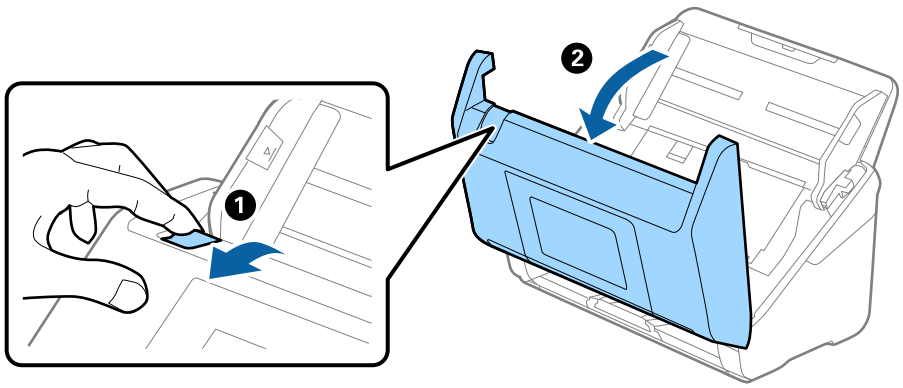
تعویض کیت مجموعه غلتک

هنگامی‌که تعداد اسکن‌ها از چرخه عمر غلتک‌ها بیشتر شود، کیت مجموعه غلتک (غلتک بلندکننده و غلتک جداکننده) باید تعویض شود. هنگامی که یک پیام تعویض در پانل کنترل یا صفحه رایانه نمایش داده می‌شود، مراحل زیر را برای تعویض آن دنبال کنید.

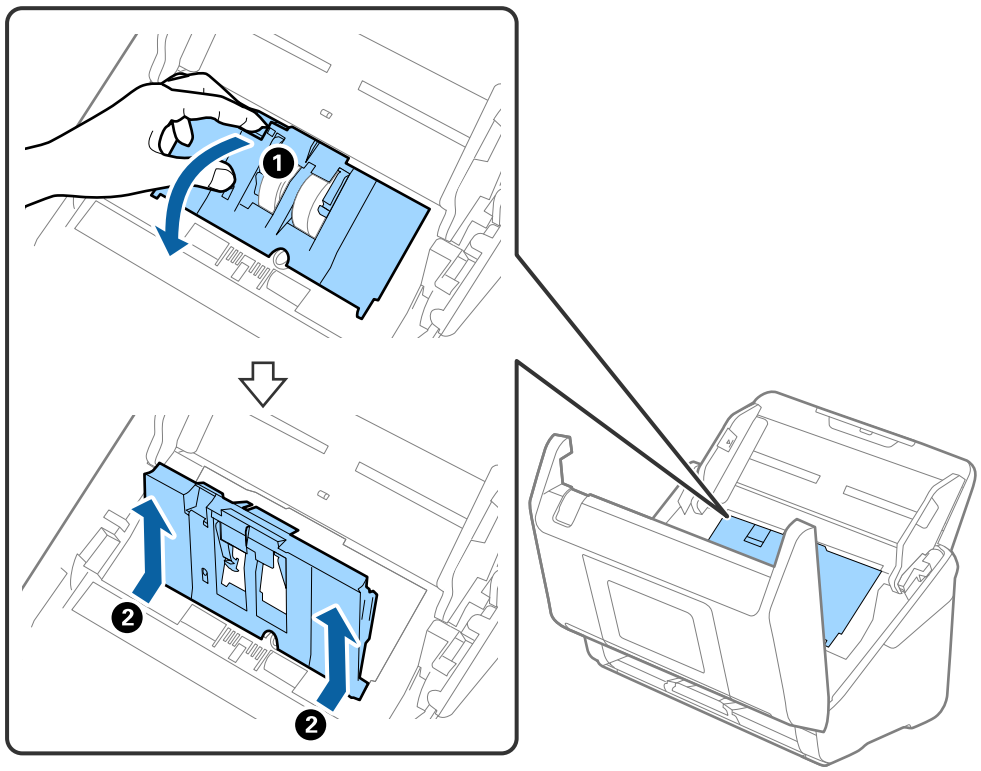


A: غلتک بلندکننده، B: غلتک جداکننده

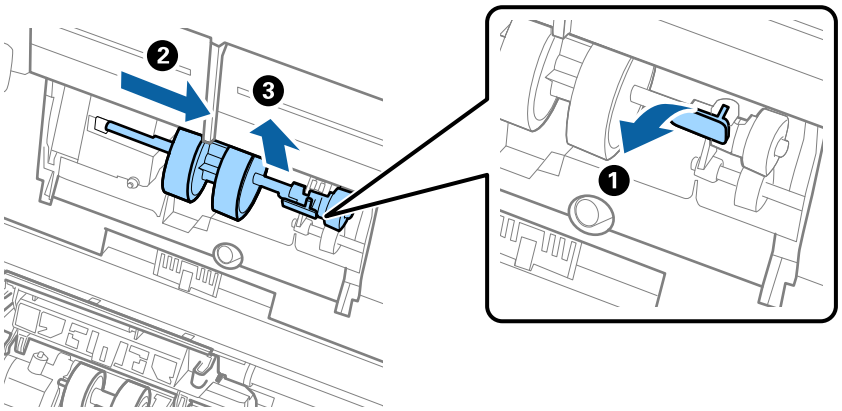
1. دکمه ⏻ را برای خاموش کردن اسکنر فشار دهید.
2. آداپتور AC را از اسکنر جدا کنید.
3. اهرم را بکشید و قاب اسکنر را باز کنید.



4. روکش غلتک بلندکننده را باز کنید و سپس آن را بلغزانید و خارج کنید.

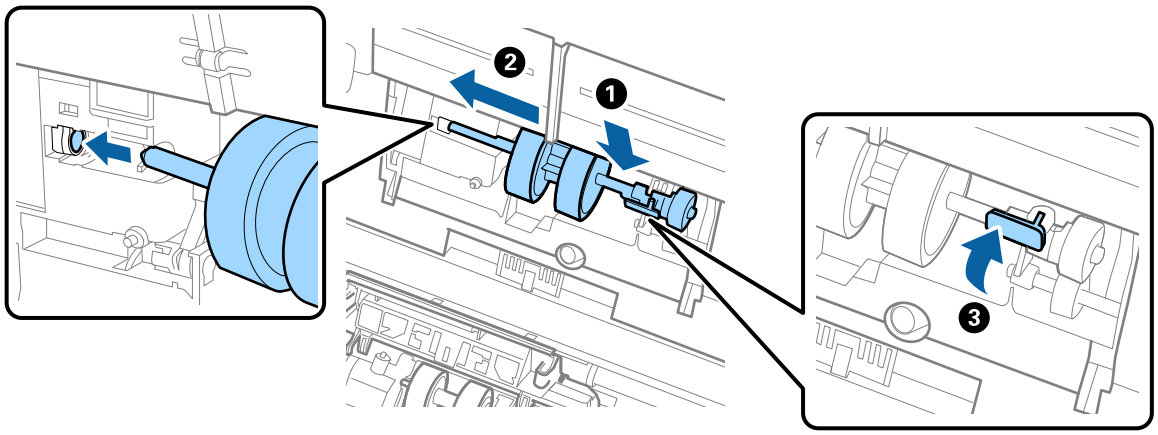


5. نگهدارنده محور غلتک را به سمت پایین بکشید و سپس غلتک‌های بلندکننده نصب شده را بلغزانید و خارج نمایید.

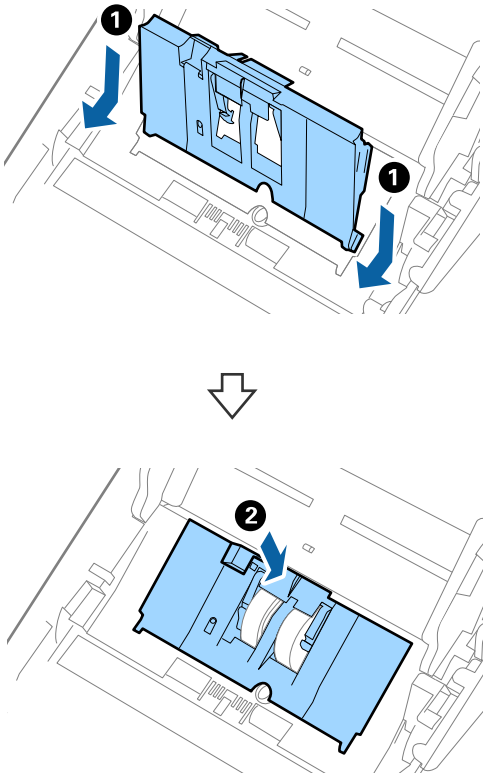


مهم:
غلتک بلندکننده را با فشار بیرون نکشید. این کار ممکن است به قسمت داخلی اسکنر آسیب بزند.

6. در حالی که نگهدارنده را پایین نگه داشته اید، غلتک بلندکننده جدید را به سمت چپ بلغزانید و آن را داخل سوراخ اسکتر قرار دهید. نگهدارنده را فشار دهید تا محکم شود.



7. لبه روکش غلتک بلندکننده را داخل شیار قرار داده و بلغزانید. روکش را محکم ببندید.

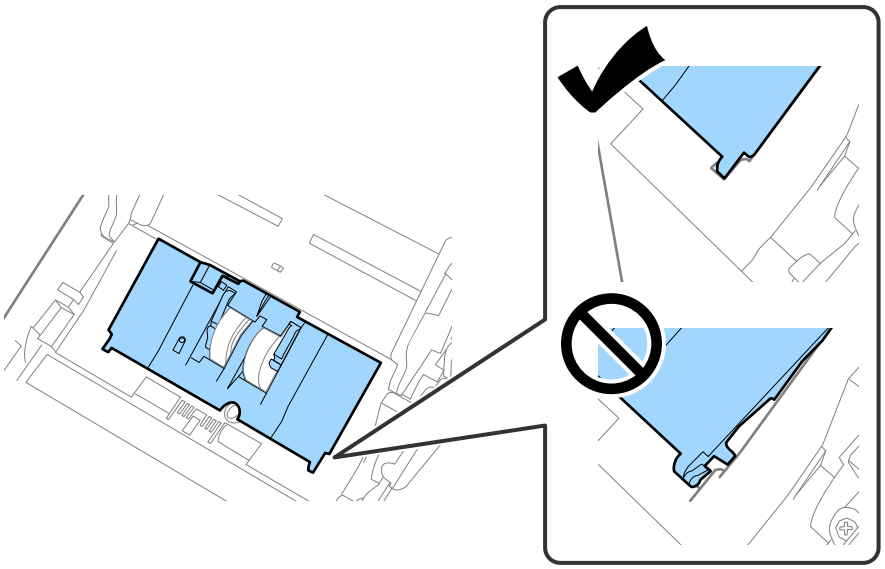


مهم:

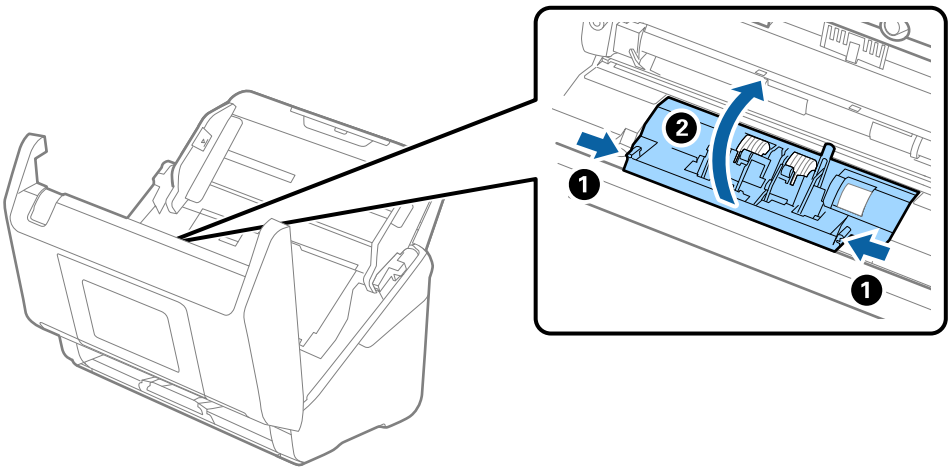
❑ اطمینان حاصل کنید که روکش بلندکننده به طور صحیح بسته شود.

❑ در صورتی که بستن روکش سخت است، اطمینان حاصل کنید که غلتک‌های بلندکننده به طور صحیح نصب شده باشند.

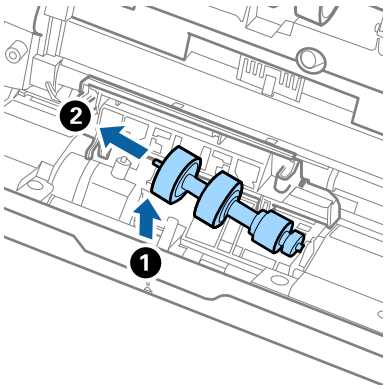
❑ در صورتی که روکش بلند شده است آن را نصب نکنید.



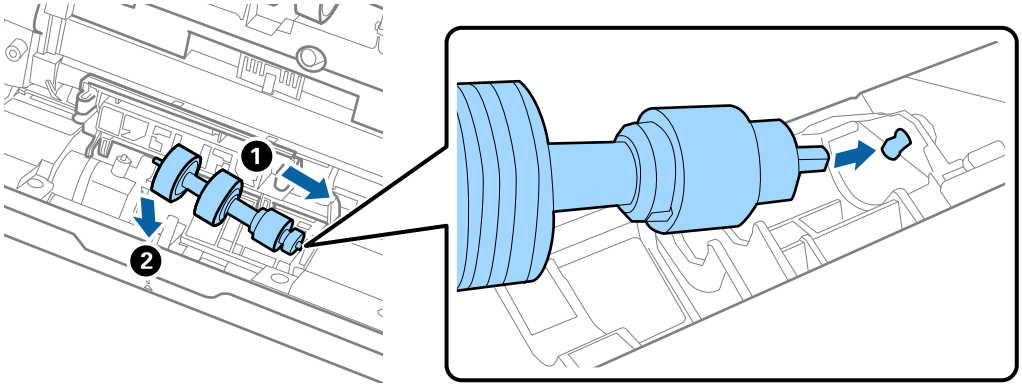
8. قلاب‌های دو طرف انتهایی روکش غلتک جداکننده را فشار دهید تا روکش باز شود.



9. سمت چپ غلتک جداکننده را بلند کنید و سپس غلتک‌های جداکننده نصب شده را بلغزانید و خارج نمایید.



10. محور غلتک جداکننده جدید را داخل سوراخ سمت راست قرار دهید و سپس غلتک را پایین بیاورید.



11. روکش غلتک جداکننده را ببندید.

مهم:
اگر بستن قاب دشوار است، باید از نصب صحیح غلتک‌های جداکننده مطمئن شوید.

12. قاب اسکنر را ببندید.

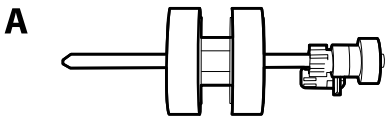
13. آداپتور AC را وصل کنید و سپس اسکنر را روشن کنید.

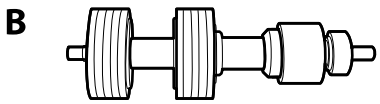
14. تعداد اسکن را می‌توانید در پانل کنترل بازنشانی کنید.

نکته:
غلتک بلندکننده و غلتک جداکننده را براساس قوانین و مقررات مسئولین محلی خود دور بیندازید. قطعات آنها را از هم جدا نکنید.

کدهای کیت مجموعه غلتک

هنگامی‌که تعداد اسکن‌ها از شماره سرویس بیشتر می‌شود، قطعه‌های (غلتک بلندکننده و یک غلتک جداکننده) باید تعویض شوند. آخرین عدد اسکن‌ها را می‌توانید در پانل کنترل یا Epson Scan 2 Utility بررسی کنید.





A: غلتک بلندکننده، B: غلتک جداکننده

نام قطعه	کدها	چرخه عمر
کیت اتصال غلتک 2	B12B819711 B12B819721 (فقط هند)	200,000*

* این عدد به واسطه اسکن‌های پشت سرهم با استفاده از کاغذهای سند آزمایش Epson حاصل می‌شود و یک راهنما برای دوره تعویض است. بسته به انواع مختلف کاغذ، نظیر کاغذی که غبار زیادی تولید می‌کند یا کاغذی که دارای سطح ناصافی است که باعث کوتاه شدن چرخه عمر می‌شود، ممکن است دوره تعویض متفاوت باشد.

بازنشانی تعداد اسکن‌ها پس از تعویض کردن غلتک‌ها

پس از تعویض کیت مجموعه غلتک، با استفاده از پانل کنترل یا Epson Scan 2 Utility تعداد اسکن ها را بازنشانی کنید.

این بخش نحوه بازنشانی را با استفاده از پانل کنترل را شرح می‌دهد.

1. در صفحه اصلی، روی **تعمیر و نگهداری اسکنر** ضربه بزنید.
2. روی **تعویض غلطک** ضربه بزنید.
3. روی گزینه **بازنشانی تعداد اسکن ها** ضربه بزنید.
4. گزینه **تعداد اسکن ها بعد از تعویض غلطک** را انتخاب کنید و سپس روی **بله** ضربه بزنید.

نکته:
برای بازنشانی از *Epson Scan 2 Utility*، نخست *Epson Scan 2 Utility* را روشن کنید، روی زبانه **شمارشگر** کلیک کنید، سپس روی **تنظیم مجدد** در **کیت اتصال غلتک** کلیک کنید.

اطلاعات مرتبط

"تعویض کیت مجموعه غلتک" در صفحه 128

صرفه‌جویی در انرژی

هنگامی که هیچ عملیاتی توسط اسکنر اجرا نمی شود، با استفاده از حالت خواب یا خاموشی خودکار می توانید در مصرف برق صرفه جویی کنید. مدت زمانی که طول می کشد تا اسکنر وارد حالت خواب شود یا به صورت خودکار خاموش گردد را می توانید تنظیم کنید. هر گونه افزایش، روی بهره وری انرژی محصول تاثیر می گذارد. پیش از انجام هرگونه تغییر، لطفاً محیط زیست را در نظر بگیرید.

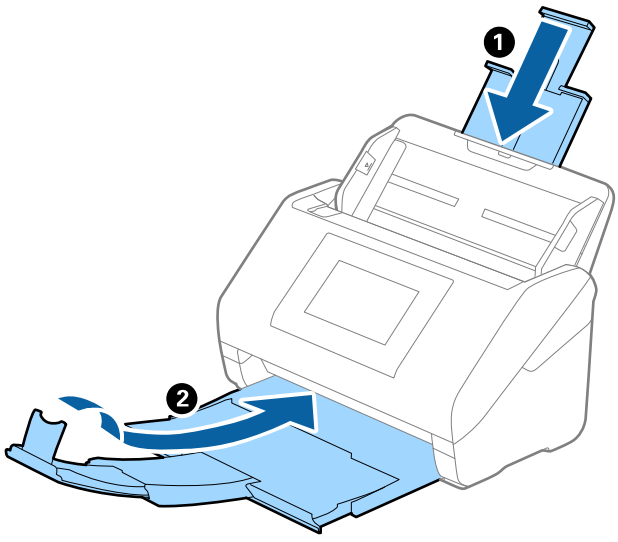
1. در صفحه اصلی، گزینه **تنظیم** را انتخاب کنید.
2. **تنظیمات اصلی** را انتخاب کنید.
3. گزینه **تایمر خواب** یا **تنظیم خاموش کردن** را انتخاب کنید و سپس تنظیمات را انجام دهید.

نکته:
ویژگی های موجود با توجه به محل خرید ممکن است متفاوت باشد.

حمل و نقل اسکنر

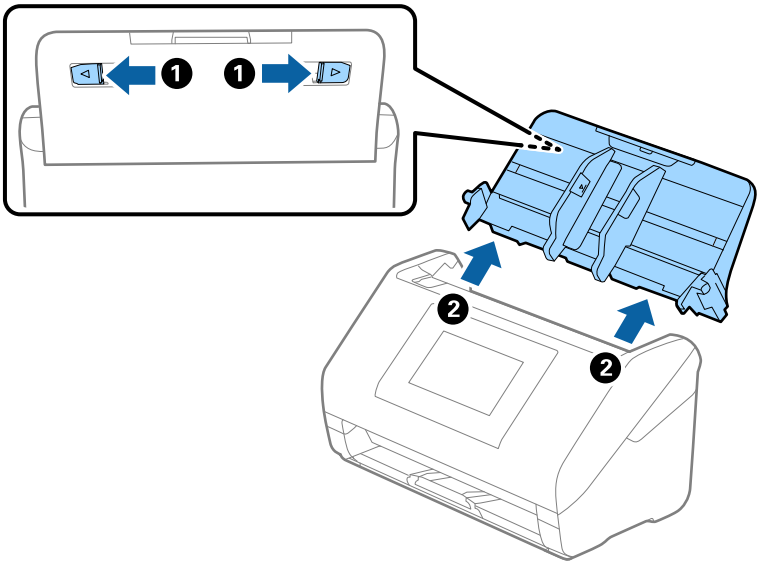
هنگامی‌که نیاز به حمل و نقل اسکنر به منظور جابجایی یا انجام تعمیرات دارید، مراحل زیر را برای بسته بندی اسکنر دنبال کنید.

1. دکمه ⏻ را برای خاموش کردن اسکنر فشار دهید.
2. آداپتور برق متناوب را جدا کنید.
3. کابل‌ها و دستگاه‌ها را جدا کنید.
   در صورت پیوست، Paper Alignment Plate اختیاری یا ارائه‌شده را حذف کنید.
4. رابط سینی ورودی و سینی خروجی را ببندید.



مهم:
اطمینان حاصل کنید که سینی خروجی به‌طور محکم بسته باشد؛ درغیراین‌صورت ممکن است در حین اسکن کردن آسیب ببیند.

5. سینی ورودی را بردارید.



6. مواد بسته‌بندی که به همراه اسکنر ارائه شده است را سر جای خود قرار دهید و سپس اسکنر را در جعبه اصلی خود یا در جعبه‌ای محکم مجدداً بسته‌بندی نمایید.

پشتیبان‌گیری از تنظیمات

مجموعه مقدار تنظیم را می‌توانید از Web Config به فایل استخراج کنید. سپس می‌توانید آن را برای تهیه نسخه پشتیبان مخاطبین، مقادیر تنظیمات، تعویض اسکنر و موارد مشابه استفاده کنید.

فایل استخراج شده قابل ویرایش نمی‌باشد زیرا به صورت یک فایل دودویی استخراج می‌شود.

استخراج کردن تنظیمات

تنظیمات اسکنر را استخراج کنید.

1. وارد Web Config شوید و زبانه **Device Management** > **Export and Import Setting Value** > **Export** را انتخاب کنید.
2. تنظیماتی را که می‌خواهید استخراج کنید، انتخاب نمایید.

تنظیماتی را که می‌خواهید استخراج کنید، انتخاب نمایید. اگر دسته اصلی را انتخاب کنید، دسته‌های فرعی نیز انتخاب می‌شوند. با این حال دسته‌های فرعی که با تکثیر در یک شبکه واحد باعث بروز خطا می‌شوند (مانند آدرس‌های IP و مانند آن) را نمی‌توان انتخاب کرد.

3. برای رمزنگاری فایل استخراج شده رمز عبور وارد کنید.

برای وارد کردن فایل به رمز عبور نیاز دارید. اگر نمی‌خواهید فایل را رمزنگاری کنید، اینجا را خالی بگذارید.

4. روی **Export** کلیک کنید.

مهم:

اگر می‌خواهید تنظیمات شبکه اسکنر مانند نام دستگاه و آدرس *IPv6* را استخراج کنید، ***Enable to select the individual settings of device*** را انتخاب کنید و موارد بیشتر را انتخاب کنید. برای اسکنر تعویضی فقط از مقادیر انتخاب شده استفاده کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

وارد کردن تنظیمات

فایل استخراج شده Web Config را وارد اسکنر کنید.

مهم:
هنگام وارد کردن مقادیری که شامل اطلاعات شخصی از قبیل نام اسکنر یا آدرس *IP* هستند، مطمئن شوید همان آدرس *IP* در همان شبکه وجود نداشته باشد.

1. به Web Config وارد شوید و زبانه **Device Management** > **Export and Import Setting Value** > **Import** را انتخاب کنید.
2. فایل استخراج شده را انتخاب کنید و سپس رمز عبور رمزنگاری شده را وارد کنید.
3. روی گزینه **Next** کلیک کنید.
4. تنظیماتی را که می‌خواهید وارد کنید انتخاب نمایید و سپس روی **Next** کلیک کنید.
5. روی گزینه **OK** کلیک کنید.

تنظیمات به اسکنر اعمال می‌شوند.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

بازگرداندن تنظیمات اولیه

در پنل کنترل، مسیر **تنظیم**> **سرپرست سیستم**> **بازگرداندن تنظیمات اولیه** را انتخاب کنید و سپس موارد موردنظر برای بازگرداندن به تنظیمات پیش‌فرض را انتخاب نمایید.

- ❑ تنظیمات شبکه: تنظیمات مربوط به شبکه را به وضعیت اولیه آنها بازگردانید.
- ❑ همه موارد بجز تنظیمات شبکه: همه تنظیمات غیر از تنظیمات مربوط به شبکه را به وضعیت اولیه آنها بازگردانید.
- ❑ همه تنظیمات: همه تنظیمات را به وضعیت زمان خرید بازگردانید.

مهم:
اگر **همه تنظیمات** را انتخاب و اجرا کنید، همه داده‌های تنظیمات ثبت‌شده در اسکنر ازجمله مخاطبین حذف خواهند شد. تنظیمات حذف‌شده قابل بازیابی نیستند.

نکته:
همچنین می‌توانید تنظیمات را در *Web Config* انجام دهید.

زبانه ***Device Management*** > ***Restore Default Settings***

به‌روزرسانی برنامه‌ها و سفت‌افزار (فریمور)

ممکن است با به‌روزرسانی برنامه‌ها و سیستم عامل بتوانید برخی مشکلات را از بین برده و باعث بهبود یا افزودن شدن به عملکردهای آنها شوید. اطمینان حاصل کنید که از جدیدترین نسخه برنامه‌ها و سیستم عامل استفاده می‌کنید.

مهم:

❏ در حین به روزرسانی کامپیوتر یا اسکنر را خاموش نکنید.

نکته:

وقتی اسکنر امکان اتصال به اینترنت را دارد، می توانید ثابت افزار را از طریق *Web Config* به روز کنید. زبانه ***Device Management*** را از > ***Firmware Update*** انتخاب کنید، پیام نمایش داده شده را بررسی کنید و سپس روی ***Start*** کلیک کنید.

1. مطمئن شوید که اسکنر و رایانه به هم متصل بوده و رایانه به اینترنت وصل شده باشد.
2. EPSON Software Updater را باز کرده و برنامه ها یا میان افزار را به روز رسانی کنید.

نکته:

از سیستم عامل های *Windows Server* پشتیبانی نمی شود.

❏ Windows 11

روی دکمه شروع کلیک کنید و سپس **همه برنامه ها** > **Epson Software** > **EPSON Software Updater** را انتخاب کنید.

❏ Windows 10

روی دکمه شروع کلیک کنید و سپس **Epson Software** > **EPSON Software Updater** را انتخاب کنید.

❏ Windows 8.1/Windows 8

نام برنامه را در قسمت جستجو وارد کنید و سپس آیکون نشان داده شده را انتخاب نمایید.

❏ Windows 7

روی دکمه شروع کلیک کنید و سپس **همه برنامه ها** یا **برنامه ها** > **Epson Software** > **EPSON Software Updater** را انتخاب کنید.

❏ Mac OS

گزینه **Finder** > **برو** > **برنامه‌ها** > **Epson Software** > **EPSON Software Updater** را انتخاب کنید.

نکته:

اگر برنامه مورد نظر برای بروزرسانی را در لیست برنامه ها پیدا نمی کنید، نمی توانید از طریق *EPSON Software Updater* بروزرسانی را انجام دهید. وجود جدیدترین نسخه برنامه ها را در وب سایت *Epson* مربوط به کشور خود بررسی کنید.

http://www.epson.com

بروزرسانی ثابت‌افزار اسکنر با استفاده از پانل کنترل

اگر اسکنر امکان اتصال به اینترنت را دارد، ثابت‌افزار اسکنر را می‌توانید از طریق پانل کنترل بروزرسانی کنید. همچنین می‌توانید اسکنر را طوری تنظیم کنید که به طور منظم بروزرسانی‌های ثابت‌افزار را بررسی کرده و در صورت وجود، به شما اطلاع دهد.

1. در صفحه اصلی، **تنظیم** را انتخاب کنید.
2. مسیر **سرپرست سیستم** > **به‌روز رسانی میان افزار** > **به‌روز رسانی** را انتخاب کنید.

نکته:

برای تنظیم اسکنر به طوری که بروزرسانی‌های ثابت‌افزار را به‌طور منظم بررسی کند، **اعلامیه** > ***On*** را انتخاب کنید.

3. پیام روی صفحه را بررسی کنید تا جستجوی بروزرسانی‌های موجود آغاز شود.

4. اگر پیامی روی صفحهٔ LCD نمایش داده شد مبنی بر اینکه به‌روزرسانی نرم‌افزار داخلی موجود است، دستورالعمل‌های روی صفحه را دنبال کنید تا به‌روزرسانی شروع شود.

مهم:

- تا پایان بروزرسانی، اسکنر را خاموش نکرده یا آن را از پریز برق نکشید؛ در غیر این صورت ممکن است اسکنر دچار ایراد عملکردی شود.
- اگر به‌روزرسانی نرم‌افزار داخلی به اتمام نرسید یا ناموفق بود، اسکنر به صورت عادی شروع نمی‌کند و دفعه بعد که اسکنر روشن می‌شود، «*Recovery Mode*» روی صفحهٔ *LCD* نمایش داده می‌شود. در این وضعیت، باید دوباره ثابت‌افزار را با استفاده از رایانه بروزرسانی کنید. اسکنر را توسط یک کابل *USB* به یک رایانه متصل کنید. درحالی‌که «*Recovery Mode*» در اسکنر نشان داده شده است، نمی‌توانید ثابت‌افزار را از طریق اتصال شبکه بروزرسانی کنید. در رایانه، به وب‌سایت *Epson* محلی خود وارد شوید و سپس جدیدترین ثابت‌افزار اسکنر را دانلود نمایید. برای اطلاع از مراحل بعدی، به دستورالعمل‌های ارائه شده در وب‌سایت مراجعه کنید.

به‌روزرسانی ثابت‌افزار از طریق Web Config

وقتی اسکنر امکان اتصال به اینترنت را دارد، می‌توانید ثابت افزار را از طریق Web Config به روز کنید.

1. وارد Web Config شوید و زبانه **Device Management** > **Firmware Update** را انتخاب کنید.
2. روی گزینه **Start** کلیک کنید و سپس دستورالعمل‌های روی صفحه را دنبال کنید.

فرآیند تأیید ثابت‌افزار آغاز می‌شود و در صورت وجود ثابت‌افزار به‌روز شده، اطلاعات مربوط به آن نمایش داده می‌شود.

نکته:
به‌روز رسانی ثابت‌افزار با استفاده از *Epson Device Admin* نیز امکان‌پذیر است. اطلاعات ثابت‌افزار را می‌توانید در لیست دستگاه‌ها مشاهده کنید. این امر زمانی سودمند است که در نظر داشته باشید چند ثابت‌افزار دستگاه را به‌روز کنید. برای کسب اطلاعات بیشتر به راهنمای *Epson Device Admin* مراجعه کنید.

اطلاعات مرتبط

"اجرای Web Config در یک مرورگر وب" در صفحه 36

به‌روزرسانی ثابت‌افزار بدون اتصال به اینترنت

می‌توانید نرم‌افزار داخلی دستگاه را از وب‌سایت Epson بر روی رایانه خود بارگیری کنید و سپس دستگاه و رایانه را با کابل USB به هم وصل کنید تا به‌روز رسانی نرم‌افزار انجام بگیرد. If you cannot update over the network, try this method.

نکته:
پیش از به‌روز رسانی، مطمئن شوید که درایور اسکنر *Epson Scan 2* در کامپیوترتان نصب شده است. اگر *Epson Scan 2* نصب نیست، دوباره آن را نصب کنید.

1. آخرین به‌روزرسانی میان‌افزار را در وبسایت Epson جستجو کنید.

   http://www.epson.com

   - اگر میان‌افزاری برای اسکنر شما وجود دارد، آن را دانلود کنید و به مرحله بعدی بروید.
   - اگر اطلاعات میان‌افزار در وبسایت موجود نیست، در این صورت شما از آخرین نسخه میان‌افزار استفاده می‌کنید.

2. رایانه حاوی میان‌افزار دانلود شده را با کابل USB به اسکنر وصل کنید.
3. بر روی فایل .exe دانلود شده دو بار متوالی کلیک کنید.

   Epson Firmware Updater شروع می شود.

4. دستورالعمل های روی صفحه را دنبال کنید.