

DS-790WN

راهنمای سرپرست

تنظیمات مورد نیاز برای مطابقت با نیازهای شما

تنظیمات شبکه

تنظیمات لازم برای اسکن کردن

تنظیمات امنیتی ابتدایی

تنظیمات امنیتی پیشرفته

Authentication Settings

حق نسخه برداری

تکثیر و نگهداری این نشریه در سیستم‌های بازیابی یا انتقال هر بخش از آن به روش‌های مختلف الکترونیکی، مکانیکی، فتوکپی، ضبط یا جز آن بدون کسب مجوز کتبی از شرکت Seiko Epson ممنوع است. استفاده از اطلاعات مندرج در اینجا مشمول مسئولیت حق اختراع نیست. بابت خسارات ناشی از استفاده اطلاعات در اینجا هیچ مسئولیتی پذیرفته نمی‌شود. اطلاعات مندرج در اینجا فقط برای محصولات Epson طراحی شده است. Epson بابت استفاده از این اطلاعات برای محصولات دیگر مسئولیتی نمی‌پذیرد.

نه شرکت Seiko Epson و نه شرکت‌های وابسته آن در قبال خسارت، زیان، هزینه یا مخارج تحمیل شده به خریدار یا اشخاص ثالث در نتیجه تصادف، سوءاستفاده یا استفاده نادرست از این محصول یا اصلاحات، تعمیرات یا تغییرات غیرمجاز محصول یا (به استثنای ایالات متحده) کوتاهی در رعایت دستورالعمل‌های بهره‌برداری و نگهداری شرکت Seiko Epson در برابر خریدار این محصول یا اشخاص ثالث مسئولیتی نخواهد داشت.

شرکت Seiko Epson و شرکت‌های وابسته به آن در قبال خسارات یا مشکلات ناشی از استفاده از گزینه‌ها یا محصولات مصرفی غیر از مواردی که شرکت Seiko Epson "محصولات اصل Epson" یا "محصولات مورد تایید Epson" اعلام کرده است، مسئولیتی نخواهند داشت.

شرکت Seiko Epson بابت خسارات ناشی از تداخل الکترومغناطیسی بر اثر مصرف کابل‌های رابط غیر از آنهایی که شرکت Seiko Epson "محصولات مورد تایید Epson" اعلام کرده است، مسئولیتی ندارد.

© Seiko Epson Corporation 2021

محتوای این راهنما و مشخصات این محصول ممکن است بدون اعلام قبلی تغییر کند.

علايم تجاری

SEIKO EPSON CORP.، EPSON، EXCEED YOUR VISION، و لوگوهای آنها علائم تجاری ثبت شده Seiko Epson هستند.

Microsoft®، Windows®، and Windows Server® are registered trademarks of Microsoft Corporation.

Apple، Mac، macOS، OS X، Bonjour، Safari، and AirPrint are trademarks of Apple Inc.، registered in the U.S. and other countries.

Chrome is a trademark of Google LLC.

The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum، Inc.

Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.

PaSoRi و FeliCa علائم تجاری ثبت شده Sony Corporation هستند.

MIFARE یک نشان تجاری ثبت شده NXP Semiconductor Corporation است.

اطلاعيه عمومي: ساير نام‌های محصول که در اینجا استفاده می‌شوند فقط برای اهداف شناسایی بوده و ممکن است علامت‌های تجاری مالکان مربوطه آنها باشند. Epson حقوق مربوط به این مارک‌ها را از خود سلب می‌کند.

- 144. تنظیم Scan to My Folder
- 146. Customize One-touch Functions
- Epson Device Job History گزارش‌های با استفاده از Epson Device
- 146. Admin
- 146. مواردی که می‌توان در گزارش لحاظ کرد.
- 147. وارد شدن به عنوان سرپرست از پانل کنترل.
- 147. غیرفعال کردن Authentication Settings
- حذف اطلاعات Authentication Settings (بازگرداندن تنظیمات اولیه).
- 148. حل کردن مشکلات.
- 148. کارت تأیید هویت خوانده نمی‌شود.

نگهداری

- 150. تمیز کردن قسمت خارجی اسکنر.
- 150. تمیز کردن قسمت داخلی اسکنر.
- 155. تعویض کیت مجموعه غلتک.
- 160. کدهای کیت مجموعه غلتک.
- 160. بازنشانی تعداد اسکن‌ها.
- 160. صرفه جویی در مصرف برق.
- 161. حمل و نقل اسکنر.
- 162. پشتیبان‌گیری از تنظیمات.
- 162. استخراج کردن تنظیمات.
- 163. وارد کردن تنظیمات.
- 163. بازگرداندن تنظیمات اولیه.
- 164. به روزرسانی برنامه‌ها و میان‌افزار.
- 164. بروزرسانی ثابت‌افزار اسکنر با استفاده از پانل کنترل.
- 165. به‌روزرسانی ثابت‌افزار از طریق Web Config.
- 165. به‌روزرسانی ثابت‌افزار بدون اتصال به اینترنت.

تنظیمات امنیتی پیشرفته

- 93. تنظیمات امنیتی و پیشگیری از خطر.
- 93. تنظیمات ویژگی امنیتی.
- 94. کنترل کردن با پروتکل‌ها.
- 94. کنترل پروتکل‌ها.
- 94. پروتکل‌هایی که می‌توانید فعال یا غیرفعال کنید.
- 95. موارد تنظیم پروتکل.
- 96. استفاده از گواهی دیجیتالی.
- 96. درباره گواهی دیجیتالی.
- 97. پی‌کربندی یک CA-signed Certificate.
- 100. به روزرسانی گواهی خود امضاء.
- 101. پی‌کربندی یک CA Certificate.
- 102. ارتباط SSL/TLS با اسکنر.
- 102. پی‌کربندی تنظیمات SSL/TLS ساده.
- 102. پی‌کربندی گواهی سرور برای اسکنر.
- 103. ارتباط رمزگذاری شده با IPsec/فیلترینگ IP.
- 103. درباره IPsec/IP Filtering.
- 103. پی‌کربندی سیاست پیش‌فرض.
- 107. پی‌کربندی سیاست گروه.
- 113. پی‌کربندی نمونه‌های IPsec/IP Filtering.
- 114. پی‌کربندی گواهی برای فیلترگذاری IPsec/IP.
- 114. اتصال اسکنر به شبکه IEEE802.1X.
- 114. پی‌کربندی شبکه IEEE 802.1X.
- 115. پی‌کربندی گواهی برای IEEE 802.1X.
- 116. رفع مشکلات مربوط به امنیت پیشرفته.
- 116. بازگرداندن تنظیمات امنیتی.
- مشکلات مربوط به استفاده از ویژگی‌های امنیت شبکه
- 116. مشکلات مربوط به استفاده از یک گواهی دیجیتالی.

Authentication Settings

- 123. درباره Authentication Settings
- 123. عملکردهای موجود برای Authentication Settings
- 124. درباره Authentication Method
- 125. نرم‌افزار برای راه‌اندازی.
- 126. بروزرسانی ثابت‌افزار اسکنر.
- 126. وصل کردن و پی‌کربندی یک دستگاه تأیید هویت.
- 126. لیست کارت‌خوان‌های سازگار.
- 129. وصل کردن دستگاه تأیید هویت.
- 130. تنظیمات دستگاه تأیید هویت.
- 130. ثبت و تنظیم اطلاعات.
- 130. راه‌اندازی.
- 131. فعال‌سازی تأیید هویت.
- 132. Authentication Settings
- 133. ثبت کردن User Settings
- 140. همگام‌سازی با LDAP Server
- 143. تنظیم سرور ایمیل.

مقدمه

7. محتویات این سند.

7. استفاده از این راهنما.

محتویات این سند

این سند اطلاعات زیر را برای سرپرستان اسکتر فراهم می‌آورد.

تنظیمات شبکه

آماده‌سازی عملکرد اسکن

فعال‌سازی و مدیریت تنظیمات امنیتی

فعال‌سازی و مدیریت Authentication Settings

اجرای سرویس و نگهداری روزانه

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

نکته:

این سند *Authentication Settings* را توضیح می‌دهد که تأیید هویت مستقل بدون نیاز به استفاده از سرور تأیید هویت را میسر می‌سازند. علاوه بر *Authentication Settings* معرفی شده در این دفترچه راهنما، با استفاده از یک سرور تأیید هویت نیز می‌توانید یک سیستم احراز هویت ایجاد نمایید. برای ایجاد این سیستم، از قابلیت *Document Capture Pro Server Authentication Edition* (با نام اختصاری *Document Capture Pro Server AE*) استفاده کنید.

برای کسب اطلاعات بیشتر با دفتر *Epson* در محل خود تماس بگیرید.

استفاده از این راهنما

علائم و نشان‌ها

 **احتیاط:**

دستورالعمل‌هایی که باید با دقت دنبال شود تا از آسیب بدنی جلوگیری شود.

 **مهم:**

دستورالعمل‌هایی که باید مورد توجه قرار گیرد تا از آسیب به تجهیزات جلوگیری شود.

نکته:

اطلاعات تکمیلی و مرجع ارائه می‌دهد.

اطلاعات مرتبط

← به بخش‌های مربوطه پیوند می‌دهد.

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.

ترجیحات سیستم عامل موردنظر

Windows

در این کتابچه راهنما، عباراتی از قبیل "Windows 10"، "Windows 8.1"، "Windows 8"، "Windows 7"، "Windows Server 2019"، "Windows Server 2016"، "Windows Server 2012 R2"، "Windows Server 2012"، "Windows Server 2008 R2" و "Windows Server 2019" به سیستم‌های عامل زیر اشاره دارند. همچنین، "Windows" برای اشاره به همه نسخه‌های "Windows Server" برای اشاره به "Windows Server 2019"، "Windows Server 2016"، "Windows Server 2012 R2"، "Windows Server 2012" و "Windows Server 2008 R2" استفاده می‌شود.

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® 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

Mac OS

در این راهنما از "Mac OS" برای اشاره به macOS Sierra، macOS High Sierra، macOS Mojave، macOS Catalina، macOS Big Sur و OS X Yosemite استفاده می‌شود.

تنظیمات مورد نیاز برای مطابقت با نیازهای شما

تنظیمات مورد نیاز برای مطابقت با نیازهای شما. 10.

تنظیمات مورد نیاز 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 13
من می‌خواهم اسکنر را به یک رایانه جدید وصل کنم.	تنظیمات شبکه برای اسکنر خود را در رایانه جدید تنظیم کنید. "افزودن یا تعویض رایانه یا دستگاه‌ها" در صفحه 19

تنظیمات برای اسکن کردن

هدف	تنظیمات لازم
من می‌خواهم تصاویر اسکن شده را با ایمیل ارسال کنم. (Scan to Email)	1. سرور ایمیل مورد نظر برای پیوند دادن را تنظیم کنید. "پیگر بندی سرور ایمیل" در صفحه 41 2. آدرس ایمیل گیرنده را در قسمت Contacts ثبت کنید (اختیاری). با ثبت کردن 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 61
من می‌خواهم تصاویر اسکن شده را در یک پوشه در شبکه ذخیره کنم. (Scan to Network Folder/FTP)	1. یک پوشه در شبکه و محل مورد نظر خود برای ذخیره تصاویر ایجاد کنید. "تنظیم یک پوشه اشتراک‌گذاری در شبکه" در صفحه 44 2. مسیر پوشه را در قسمت Contacts ثبت کنید (اختیاری). با ثبت کردن 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 61
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 مورد نظر برای پیوند دادن نیاز دارید. https://www.epsonconnect.com/ http://www.epsonconnect.eu (فقط اروپا)

سفارشی کردن نمایشگر پانل کنترل

هدف	تنظیمات لازم
من می‌خواهم موارد نمایش یافته در پانل کنترل اسکنر را تغییر بدهم.	گزینه‌های پیش‌تنظیمات یا ویرایش صفحه اصلی را تنظیم کنید. تنظیمات اسکنر دلخواه خود را می‌توانید در پانل کنترل ثبت کنید یا موارد نمایش یافته را ویرایش کنید. "سفارشی کردن نمایشگر پانل کنترل" در صفحه 74

تنظیم عمکردهای امنیتی پایه

تنظیمات لازم	هدف
یک رمز عبور سرپرست برای اسکتر تنظیم کنید. "تنظیمات سرپرست سیستم" در صفحه 83	من می‌خواهم کسی غیر از سرپرست نتواند تنظیمات اسکتر را تغییر دهد.
رابط خارجی را غیرفعال کنید. "غیرفعال کردن رابط خارجی" در صفحه 89	من می‌خواهم استفاده از اسکترها از طریق اتصال USB را غیرفعال کنم.

تنظیم عمکردهای امنیتی پیشرفته

تنظیمات لازم	هدف
پروتکل‌ها را فعال یا غیرفعال کنید. "کنترل کردن با پروتکل‌ها" در صفحه 94	من می‌خواهم پروتکل‌های مورد استفاده را کنترل کنم.
1. گواهی دیجیتال خود را راه‌اندازی کنید. "استفاده از گواهی دیجیتالی" در صفحه 96 2. ارتباط SSL/TLS را راه‌اندازی کنید. "ارتباط SSL/TLS با اسکتر" در صفحه 102	من می‌خواهم مسیر ارتباطات را رمزنگاری کنم.
سیاست‌های فیلتر کردن ترافیک را راه‌اندازی کنید. "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 103	من می‌خواهم از ارتباطات رمزنگاری شده (IPsec) استفاده کنم. من می‌خواهم از نرم‌افزار تنها از طریق یک رایانه خاص (فیلترگذاری IP) استفاده شود.
شبکه IEEE802.1X را برای اسکتر راه‌اندازی کنید. "اتصال اسکتر به شبکه IEEE802.1X" در صفحه 114	من می‌خواهم از اسکتر در یک شبکه IEEE802.1X استفاده کنم.

تنظیم عمکردهای موردنظر برای تأیید شدن توسط اسکتر

تنظیمات لازم	هدف
برای دریافت اطلاعات بیشتر درباره Authentication Settings و Authentication Method موجود بخش زیر را ملاحظه کنید. "درباره Authentication Settings" در صفحه 123 "درباره Authentication Method" در صفحه 124	من می‌خواهم Authentication Settings را فعال کنم.

استفاده از یک سیستم تأیید هویت

با Document Capture Pro Server Authentication Edition (یا به اختصار Document Capture Pro Server AE) می‌توانید یک سیستم تأیید هویت ایجاد کنید که از یک سرور برای تأیید هویت استفاده می‌کند.
برای کسب اطلاعات بیشتر با دفتر Epson در محل خود تماس بگیرید.

تنظیمات شبکه

- 13. اتصال اسکتر به شبکه.
- 19. افزودن یا تعویض رایانه یا دستگاهها.
- 25. بررسی وضعیت اتصال شبکه.
- 26. مشخصات شبکه.
- 30. حل کردن مشکلات.

اتصال اسکنر به شبکه

این بخش شیوه متصل کردن اسکنر به شبکه از طریق پانل کنترل اسکنر را شرح می دهد.

نکته:

اگر اسکنر و رایانه در یک قسمت باشند، می توانید آنها را با استفاده از نصب کننده نیز وصل کنید.

☐ راه اندازی از وبسایت

به وب سایت زیر دسترسی پیدا کنید و سپس نام محصول را وارد کنید. به تنظیم بروید و راه اندازی را شروع کنید.

<http://epson.sn>

☐ راه اندازی به وسیله دیسک نرم افزار (فقط برای مدل های دارای دیسک نرم افزار و کاربران دارای کامپیوترهای Windows با درایوهای دیسک).

دیسک نرم افزار را در کامپیوتر قرار دهید و سپس دستورالعمل های روی صفحه را دنبال کنید.

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 سویچ 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 ☐ رمز عبور	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 26
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	<input type="checkbox"/> نام سرور پروکسی	این گزینه را زمانی تنظیم کنید که محیط شبکه شما از سرور پروکسی برای دسترسی به اینترنت از طریق اینترنت استفاده می کند و شما عملکردی که دسترسی مستقیم اسکتر به اینترنت را فراهم می کند را استفاده می کنید. در رابطه با عملکردهای زیر، اسکتر مستقیماً به اینترنت متصل می شود. <input type="checkbox"/> خدمات Epson Connect <input type="checkbox"/> خدمات ابری مربوط به سایر شرکت ها <input type="checkbox"/> بروزرسانی ثابت افزار <input type="checkbox"/> ارسال تصاویر اسکن شده به SharePoint(WebDAV)
اطلاعات شماره درگاه	<input type="checkbox"/> شماره درگاه موردنظر برای باز کردن	شماره درگاه مورد استفاده اسکتر 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 اسکتر، بخش زیر را مشاهده کنید. "استفاده از درگاه برای اسکتر" در صفحه 29

تخصیص آدرس IP

حالات مختلف تخصیص آدرس IP شامل موارد زیر می باشد.

آدرس IP ثابت:

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

اطلاعات لازم برای اتصال به شبکه (ماسک شبکه فرعی، دروازه پیش فرض، سرور DNS و موارد مشابه) به صورت دستی تنظیم می شوند.

آدرس IP حتی وقتی دستگاه خاموش شود تغییر نمی کند، 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 می کنیم تنظیماتی برای اسکتر انتخاب کنید که بسیاری از رایانهها بتوانند به آن دسترسی داشته باشند. همچنین، هنگام استفاده از قابلیت های 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 اسکتر (میزبان) تخصیص دهید.

اطلاعات لازم برای اتصال به شبکه (ماسک شبکه فرعی، دروازه پیش فرض، سرور DNS و موارد مشابه) به صورت خودکار تنظیم می شوند، 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 می کنیم از روشهایی غیر از آدرس IP برای مدیریت دستگاهها استفاده کنید و با پروتکل هایی ارتباط برقرار کنید که قادر به دنبال کردن آدرس IP می باشند.

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 اسکتر 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 اسکترها امکان برقراری ارتباط از طریق آدرس IP را کسب خواهند کرد.

وضوح نام برای ارتباط اسکتر 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 اسکتر 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، اسکتر 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 اسکتر 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 اسکتر پیکربندی کنید.

اتصال به شبکه از طریق پانل کنترل

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

تخصیص آدرس IP

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

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

1. اسکتر را روشن کنید.

2. منوی تنظیم در صفحه اصلی پانل کنترل اسکتر 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 پیش فرض 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 پیش فرض را تنظیم کنید.

مقدار نشان داده شده در صفحه قبل را تأیید کنید.



مهم:

اگر ترکیب نشانی IP، ماسک زیرشبکه و دروازه پیش فرض 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 اسکتر 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

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

1. اسکتر و هاب (سوئیچ 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)

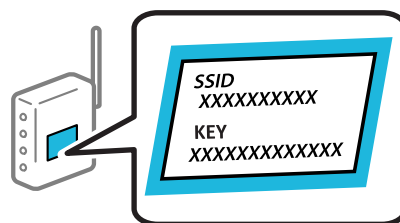
به چندین روش می توانید اسکنر را به LAN بی سیم (Wi-Fi) متصل کنید. روش اتصال سازگار با محیط و شرایط استفاده را انتخاب کنید. اگر اطلاعات روتر بی سیم مانند SSID و رمز عبور را در اختیار داشته باشید، می توانید تنظیمات را به صورت دستی انجام دهید. اگر روتر بی سیم از WPS پشتیبانی کند، می توانید تنظیمات را با 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.

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 یک روتر بی سیم با تنظیمات پیش فرض آن استفاده می کنید، SSID و کلمه عبور روی برچسب قرار دارد. اگر SSID و رمز عبور را نمی دانید، با فردی تماس بگیرید که روتر بی سیم را تنظیم کرده است یا 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. راهنمای گام به گام تنظیم Wi-Fi را انتخاب کنید.

5. برای انتخاب SSID، وارد کردن رمز عبور برای روتر بی سیم و شروع راه اندازی، 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 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 نمی دانید، بررسی کنید آیا اطلاعات روی برچسب روتر بی سیم درج 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.

اطلاعات مرتبط

← "بررسی وضعیت اتصال شبکه" در صفحه 25

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 می 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 اسکر 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 اسکر نزدیکتر کنید و دوباره تلاش کنید.

اطلاعات مرتبط

← "بررسی وضعیت اتصال شبکه" در صفحه 25

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 (WPS) PIN را انتخاب کنید

5. دستورالعمل‌های 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 25

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 می‌توانید از طریق شبکه به آن اسکنر وصل کنید.

استفاده از یک اسکنر شبکه از رایانه دوم

توصیه می‌کنیم که از نصب کننده برای اتصال اسکنر به یک کامپیوتر استفاده کنید. با استفاده از یکی از روش‌های زیر می‌توانید نصب کننده را اجرا کنید.

☐ راه اندازی از وب سایت

به وب سایت زیر دسترسی پیدا کنید و سپس نام محصول را وارد کنید. به تنظیم بروید و راه اندازی را شروع کنید.

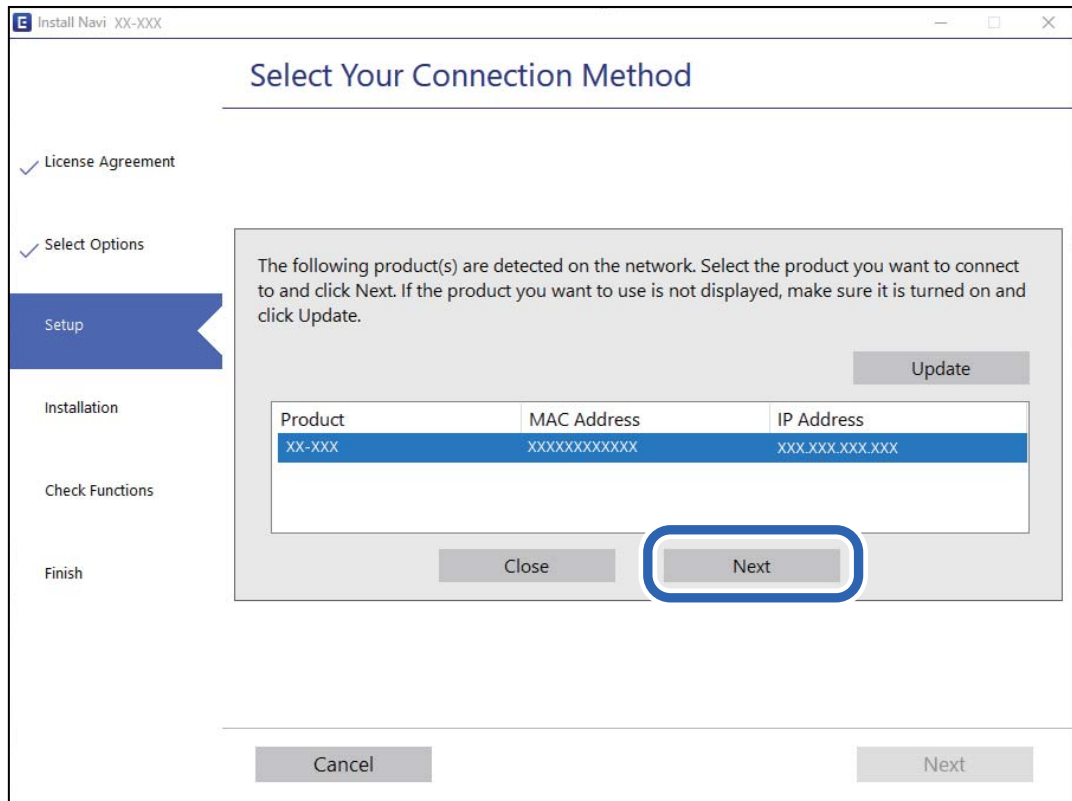
<http://epson.sn>

☐ راه اندازی به وسیله دیسک نرم افزار (فقط برای مدل‌های دارای دیسک نرم افزار و کاربران دارای کامپیوترهای Windows با درایوهای دیسک).

دیسک نرم افزار را در کامپیوتر قرار دهید و سپس دستورالعمل‌های روی صفحه را دنبال کنید.

انتخاب اسکزن

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



دستورالعمل های روی صفحه را دنبال کنید.

استفاده از یک اسکزن شبکه از دستگاه هوشمند

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

اتصال از طریق یک روتر بی سیم

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

برای اطلاعات بیشتر به بخش زیر مراجعه کنید.

["اعمال تنظیمات برای اتصال به دستگاه هوشمند" در صفحه 24](#)

اتصال از طریق Wi-Fi Direct

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

برای اطلاعات بیشتر به بخش زیر مراجعه کنید.

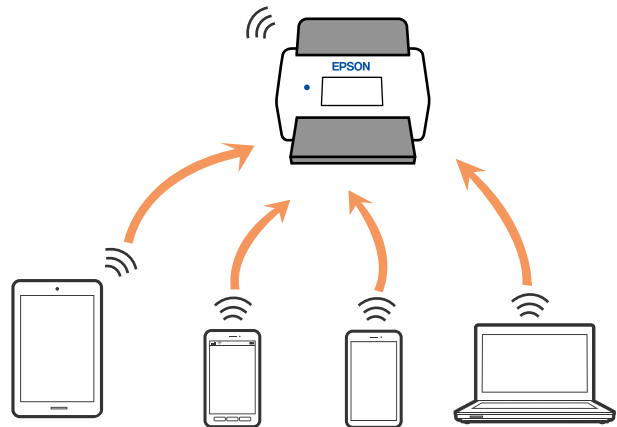
["وصل کردن مستقیم یک دستگاه هوشمند و یک اسکزن \(Wi-Fi Direct\)" در صفحه 21](#)

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

(Simple APWi-Fi Direct) به شما امکان می‌دهد بدون استفاده از یک روتر بی‌سیم 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 نمی‌کنید، یا زمانی که می‌خواهید اسکنر و کامپیوتر یا دستگاه هوشمند را به صورت مستقیم به هم وصل کنید. در این حالت، اسکنر به عنوان یک روتر بی‌سیم عمل می‌کند و شما می‌توانید دستگاه‌ها را بدون نیاز به استفاده از روتر بی‌سیم، به اسکنر وصل کنید. با این وجود، دستگاه‌هایی که به صورت مستقیم به اسکنر متصل می‌شوند نمی‌توانند از طریق اسکنر با یکدیگر ارتباط برقرار کنند.



اسکنر را می‌توانید 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 می‌شود.

اتصال به یک دستگاه هوشمند با Wi-Fi Direct

این روش به شما امکان می‌دهد که اسکنر را به صورت مستقیم به دستگاه‌های هوشمند بدون روتر بی‌سیم 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، دستورالعمل‌های 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 Wi-Fi Direct (Simple AP) وجود دارد؛ می‌توانید همه اتصالات را از طریق پانل کنترل اسکتر 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.



هنگامی که اتصال Wi-Fi Direct (Simple AP) قطع می‌شود، اتصال همه رایانه‌ها و دستگاه‌های هوشمند متصل به اسکتر در اتصال Wi-Fi Direct (Simple AP) قطع می‌شود.


نکته:

اگر می‌خواهید اتصال دستگاه خاصی را قطع کنید، اتصال را به جای اسکتر، 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) اسکتر را قطع کنید.

به یک نام شبکه (SSID) دیگر وصل شوید.

تغییر تنظیمات (Simple AP Wi-Fi Direct) مانند SSID

وقتی اتصال Wi-Fi Direct (Simple AP) فعال باشد، شما می‌توانید تنظیمات را از طریق  < Wi-Fi Direct < تنظیمات را شروع کنید < تغییر تغییر دهید و سپس گزینه‌های منوی زیر نمایش داده می‌شوند.

تغییر نام شبکه

نام شبکه (SSID) مربوط به Wi-Fi Direct (Simple AP) مورد استفاده برای اتصال به اسکتر را به نام مدنظر خود تغییر دهید. نام شبکه (SSID) را به صورت نویسه‌های ASCII وارد کنید که در صفحه کلید نرم افزاری پانل کنترل نمایش داده می‌شوند. می‌توانید تا حداکثر 22 نویسه وارد کنید.

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

تغییر گذرواژه

رمز عبور Wi-Fi Direct (Simple AP) برای اتصال دادن اسکتر را به مقدار اختیاری تغییر دهید. شما می‌توانید رمز عبور را به صورت نویسه‌های ASCII وارد کنید که در صفحه کلید نرم افزاری پانل کنترل نمایش داده می‌شوند. می‌توانید 8 الی 22 نویسه وارد کنید.

هنگام تغییر رمز عبور، ارتباط همه دستگاه‌های 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 اسکتر را تغییر دهید. شما می‌توانید 2.4 گیگاهرتز یا 5 گیگاهرتز را انتخاب کنید.

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

توجه کنید که هنگام تغییر به فرکانس 5 گیگاهرتز، قادر نخواهید بود از طریق دستگاه‌هایی که دامنه فرکانس 5 گیگاهرتزی را پشتیبانی نمی‌کنند، 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 زبان **Wi-Fi Direct < Network** 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. با استفاده از یکی از روش های زیر می توانید نصب کننده را اجرا کنید.

راه اندازی از وب سایت

به وب سایت زیر دسترسی پیدا کنید و سپس نام محصول را وارد کنید. به **تنظیم** بروید و راه اندازی را شروع کنید.

<http://epson.sn>

راه اندازی به وسیله دیسک نرم افزار (فقط برای مدل های دارای دیسک نرم افزار و کاربران دارای کامپیوترهای Windows با درایوهای دیسک.)

دیسک نرم افزار را در کامپیوتر قرار دهید و سپس دستورالعمل های روی صفحه را دنبال کنید.

انتخاب روش های اتصال

دستورالعمل های روی صفحه را دنبال کنید. در صفحه عملیات 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 30

اعمال تنظیمات برای اتصال به دستگاه هوشمند

زمانی که اسکنر 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 نمایید. به تنظیم بروید و راه اندازی را شروع کنید.

<http://epson.sn>

از همان دستگاه هوشمند مورد نظر برای اتصال به اسکنر، به وبسایت مراجعه 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 رایانه استفاده کنید. نصب کننده را می توانید به یکی از روش های زیر اجرا کنید.

☐ راه اندازی از وبسایت

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

<http://epson.sn>

☐ راه اندازی به وسیله دیسک نرم افزار (فقط برای مدل های دارای دیسک نرم افزار و کاربران دارای رایانه های Windows با درایوهای دیسک).

دیسک نرم افزار را در رایانه قرار دهید و سپس دستورالعمل های روی صفحه را دنبال کنید.

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 می شود.

اطلاعات مرتبط

◀ "اتصال به LAN بی سیم (Wi-Fi)" در صفحه 17

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.

☐ راه اندازی از وب سایت

به وب سایت زیر دسترسی پیدا کنید و سپس نام محصول را وارد کنید. به تنظیم بروید و راه اندازی را شروع کنید.

<http://epson.sn>

☐ راه اندازی به وسیله دیسک نرم افزار (فقط برای مدل های دارای دیسک نرم افزار و کاربران دارای کامپیوترهای Windows با درایوهای دیسک.)

دیسک نرم افزار را در کامپیوتر قرار دهید و سپس دستورالعمل های روی صفحه را دنبال کنید.

انتخاب تغییر روش های اتصال

دستورالعمل های روی صفحه را دنبال کنید. در صفحه عملیات 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 آیکن شبکه یا اطلاعات شبکه در پانل کنترل اسکرین می‌توانید وضعیت اتصال شبکه را بررسی کنید.

بررسی وضعیت اتصال شبکه با استفاده از آیکن شبکه

با استفاده از آیکن شبکه روی صفحه اصلی اسکرین 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	
اسکتر به یک شبکه بیسیم (Wi-Fi) متصل نیست.	
اسکتر در حال جستجوی SSID یا صفر کردن آدرس IP است یا جهت اتصال به یک شبکه بیسیم (Wi-Fi) با مشکل مواجه شده است.	
اسکتر 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.	
اسکتر به یک شبکه بیسیم (Wi-Fi) در حالت (Wi-Fi Direct (Simple AP متصل نیست.	
اسکتر به یک شبکه بیسیم (Wi-Fi) در حالت (Wi-Fi Direct (Simple AP متصل است.	
اسکتر به یک شبکه با سیم (اترنت) متصل نیست یا آدرس آن را صفر کرده است.	
اسکتر به یک شبکه با سیم (اترنت) متصل است.	

نمایش اطلاعات کامل شبکه از پانل کنترل

زمانی که اسکتر به شبکه وصل است همچنین می‌توانید 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، منوهای را که می‌خواهید بررسی نمایید انتخاب کنید.
 - وضعیت LAN/Wi-Fi سیمی
اطلاعات شبکه (نام دستگاه، اتصال، قدرت سیگنال و غیره) را برای اتصال‌های اترنت یا Wi-Fi نشان می‌دهد.
 - وضعیت Wi-Fi Direct
فعال یا غیرفعال بودن Wi-Fi Direct و نیز SSID، رمز عبور و امثال آن را برای اتصال‌های Wi-Fi Direct نشان می‌دهد.
 - وضعیت سرور ایمیل
اطلاعات شبکه سرور ایمیل را نشان می‌دهد.

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
--	--------

جدول B	استرالیا نیوزلند تایوان کره جنوبی
--------	--

جدول A

IEEE 802.11b/g/n ^{1*}	استانداردها
2.4 گیگاهرتز	دامنه فرکانس
(dBm (EIRP 20 :MHz 2483.5-2400	حداکثر نیروی فرکانس رادیویی ارسال شده
1/2/3/4/5/6/7/8/9/10/11/12/13	کانالها
(Wi-Fi Direct (Simple AP ^{2*3*} زیرساخت،	حالت‌های اتصال
WPA2/WPA3-Enterprise ,WPA3-SAE (AES) , ^{5*} WPA2-PSK (AES) ,WEP (64/128bit)	پروتکل‌های امنیتی ^{4*}

1* تنها برای HT20 در دسترس می‌باشد.

2* برای IEEE 802.11b پشتیبانی نمی‌شود.

3* حالت‌های زیرساخت و Wi-Fi Direct یا یک اتصال اترنت را می‌توان به صورت همزمان استفاده کرد.

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

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

جدول B

IEEE 802.11a/b/g/n ^{1*} ac	استانداردها
IEEE 802.11a/n/ac :GHz 5 ,IEEE 802.11b/g/n :GHz 2.4	دامنه‌های فرکانس
2.4 گیگاهرتز 2 ² /13 [*] 1/2/3/4/5/6/7/8/9/10/11/12	کانالها
5 گیگاهرتز ^{3*} (36/40/44/48) W52 (52/56/60/64) W53 (100/104/108/112/116/120/124/128/132/136/140/144) W56 (149/153/157/161/165) W58	
2.4 گیگاهرتز 2 ² /13 [*] 1/2/3/4/5/6/7/8/9/10/11/12	Wi-Fi Direct
5 گیگاهرتز ^{3*} (36/40/44/48) W52 (149/153/157/161/165) W58	
(Wi-Fi Direct (Simple AP ^{4*} , ^{5*}	حالت‌های اتصال
WPA2/WPA3-Enterprise ,WPA3-SAE (AES) , ^{7*} WPA2-PSK (AES) ,WEP (64/128bit)	پروتکل‌های امنیتی ^{6*}

1* تنها برای HT20 در دسترس می‌باشد.

2* در تایوان ارائه نمی‌شود.

- 3* موجود بودن این کانالها و استفاده از محصول در فضاهای باز از طریق این کانالها 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* حالت‌های زیرساخت و Wi-Fi Direct یا یک اتصال اترنت را می‌توان به صورت همزمان استفاده کرد.
- 6* Wi-Fi Direct تنها از WPA2-PSK (AES) پشتیبانی می‌کند.
- 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*(اترنت کم-مصرف) IEEE802.3az
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.

عملکردهای شبکه و IPv4/IPv6

عملکردها	پشتیبانی شده
Epson Scan 2	IPv6, IPv4
Document Capture Pro /Document Capture	IPv4
Document Capture Pro Server	IPv6, IPv4

پروتکل امنیتی

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

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

استفاده از درگاه برای اسکتر

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

وقتی فرستنده (سرویس‌گیرنده) اسکتر است

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

وقتی فرستنده (سرویس‌گیرنده) رایانه سرویس‌گیرنده است

شماره درگاه	پروتکل	مقصد (سرور)	موارد استفاده
3289	ENPC (UDP)	اسکتر	اسکتر را از برنامه‌ای مانند EpsonNet Config و درایور اسکتر کشف کنید.

شماره درگاه	پروتکل	مقصد (سرور)	موارد استفاده
161	SNMP (UDP)	اسکتر	از برنامه‌های مانند EpsonNet Config و درایور اسکتر، اطلاعات MIB را جمع‌آوری و تنظیم کنید.
3702	(WS-Discovery (UDP	اسکتر	جستجوی اسکتر WSD
1865	اسکن شبکه (TCP)	اسکتر	پیش-ارسال داده‌های اسکن از یک برنامه
2968	اسکن و ارسال همزمان به شبکه	اسکتر	جمع‌آوری اطلاعات کار هنگام استفاده از قابلیت اسکن و ارسال همزمان از طریق یک برنامه
80	HTTP (TCP)	اسکتر	Web Config
443	HTTPS (TCP)		

حل کردن مشکلات

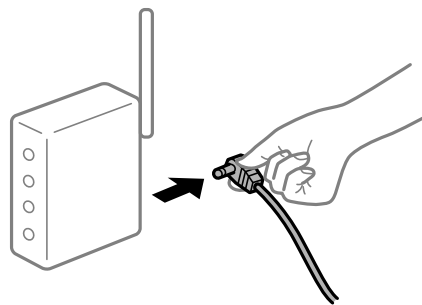
اتصال به یک شبکه ممکن نیست

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

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

راهکارها

دستگاه‌هایی که می‌خواهید به شبکه متصل کنید را خاموش کنید. حدود 10 ثانیه صبر کنید و سپس دستگاه‌ها را به این ترتیب روشن کنید: روتر بی‌سیم، رایانه یا دستگاه هوشمند و سپس اسکتر. اسکتر و رایانه یا دستگاه هوشمند را به روتر بی‌سیم نزدیک کنید تا ارتباط امواج رادیویی بهتر شود و سپس سعی کنید تنظیمات شبکه را دوباره انجام دهید.



دستگاه‌ها نمی‌توانند سیگنال‌ها را از روتر بی‌سیم دریافت کنند زیرا بسیار دور از هم هستند.

راهکارها

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

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

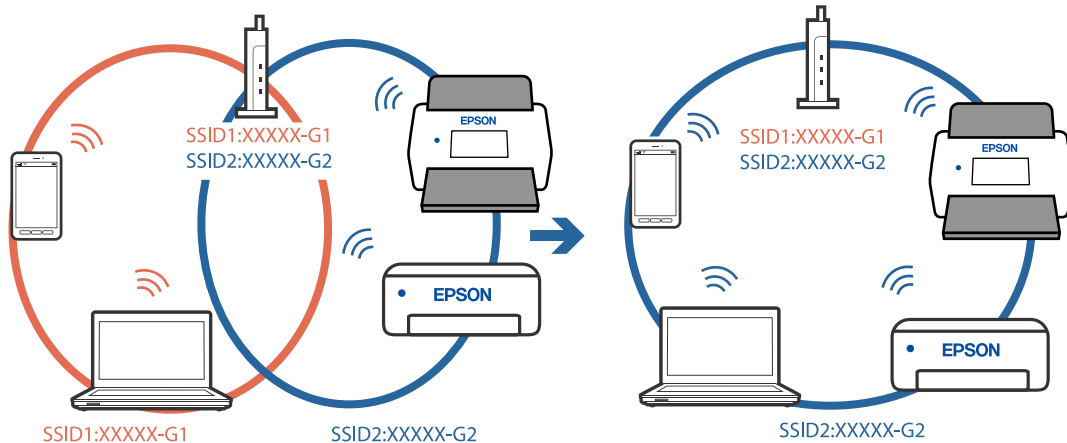
راهکارها

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 SSID های متفاوتی متصل هستند، نمی توانید به روتر بی سیم وصل شوید. رایانه یا دستگاه هوشمند را به همان SSID که اسکرین 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 اسکرین و رایانه یا دستگاه هوشمند ارتباط برقرار کنید، جداکننده 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 اسکرین XXX.XXX.169.254 و ماسک زیرشبکه 255.255.0.0 باشد، نشانی IP را نمی توان به درستی تخصیص داد.

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

روتر بی سیم را دوباره راه اندازی کنید یا تنظیمات شبکه اسکرین 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 نمی توانید 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.

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

راهکارها

وقتی اسکتر 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، اسکتر بارها قطع و وصل می شود.

❑ اتصال به اسکتر امکان پذیر نیست.

❑ سرعت اتصال آهسته می شود.

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

1. کابل اترنت متصل به رایانه و اسکتر 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 اسکتر را با کمک یک کابل اترنت به طور مستقیم به یکدیگر وصل کنید.
4. در اسکتر، تنظیمات شبکه را بررسی کنید.
مسیر تنظیم < تنظیمات شبکه < وضعیت شبکه < وضعیت LAN/Wi-Fi سیمی را انتخاب کنید.
5. نشانی IP اسکتر را بررسی کنید.
6. در رایانه، به Web Config وارد شوید.
یک مرورگر وب را اجرا کنید و سپس آدرس IP اسکتر را وارد نمایید.
["اجرای Web Config در مرورگر وب" در صفحه 35](#)
7. زبانه **Wired LAN < Network** 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 اسکتر 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 اسکتر متصل کنید.
اگر مشکل هنوز باقی مانده است، ممکن است مشکل به دستگاه هایی غیر از اسکتر 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.

نرم افزار برای راه اندازی اسکنر

35.Web Config

36.Epson Device Admin

Web Config

Web Config برنامه ای است که در مرورگرهای وب نظیر Internet Explorer و Safari در رایانه اجرا می شود. می توانید وضعیت اسکتر را تأیید کنید یا سرویس شبکه و تنظیمات اسکتر را تغییر دهید. از آنجا که اسکترها به طور مستقیم از طریق شبکه دسترسی و اجرا می شوند، مناسب است که در هر زمان یک اسکتر را تنظیم نمایید. برای استفاده از Web Config، رایانه خود را به همان شبکه اسکتر متصل کنید. از مرورگرهای زیر پشتیبانی می شود.

* Microsoft Edge، Windows Internet Explorer 8 یا نسخه جدیدتر، * Firefox، * Chrome، * Safari
* از جدیدترین نسخه استفاده کنید.

اجرای Web Config در مرورگر وب

1. آدرس IP اسکتر را بررسی کنید.
گزینه تنظیم < تنظیمات شبکه > وضعیت شبکه را در پانل کنترل اسکتر انتخاب کنید. سپس وضعیت روش اتصال فعال (وضعیت LAN/Wi-Fi سیمی یا وضعیت Wi-Fi Direct) را برای تأیید آدرس IP اسکتر انتخاب کنید.
2. مرورگر وب را از رایانه یا دستگاه هوشمند راه اندازی کنید و نشانی IP اسکتر را در آن وارد کنید.
فرمت:
IPv4: http://نشانی IP اسکتر/
IPv6: http://[نشانی IP اسکتر]/
مثالها:
IPv4: http://192.168.100.201/
IPv6: http://[1000:1::db8:2001]/
نکته:
از آنجا که اسکتر 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؛ البته این بدان معنا نیست که مشکلی وجود دارد و با خیال راحت می توانید از آن صرف نظر کنید.
3. به عنوان یک سرپرست وارد شوید و تنظیمات اسکتر را تغییر دهید.
روی Administrator Login در گوشه بالا سمت راست صفحه کلیک کنید. User Name و Current password را وارد کنید و سپس روی OK کلیک کنید.
نکته:
 در بخش زیر، مقادیر اولیه برای اطلاعات سرپرستی Web Config ارائه می شوند.
• نام کاربری: هیچ (خالی)
• رمز عبور: شماره سریال اسکتر
• شماره سریال را با بررسی برچسب متصل به پشت اسکتر ملاحظه کنید.
 اگر Administrator Logout در قسمت بالای سمت راست صفحه نمایش مشخص شود، شما قبلاً به عنوان سرپرست وارد سیستم شده اید.

اجرای Web Config در Windows

هنگام وصل کردن رایانه به اسکتر توسط WSD، مراحل زیر را برای اجرای Web Config دنبال کنید.

1. فهرست اسکنر را در رایانه باز کنید.

Windows 10

روی دکمه شروع کلیک کنید و سپس سیستم < Windows پانل کنترل < مشاهده دستگاهها و چاپگرها از سخت افزار و صدا را انتخاب کنید.

Windows 8.1/Windows 8

دسک تاپ < تنظیمات < پانل کنترل < مشاهده دستگاهها و چاپگرها از سخت افزار و صدا (یا سخت افزار) را انتخاب کنید.

Windows 7

روی دکمه شروع کلیک کنید و پانل کنترل < مشاهده دستگاهها و چاپگرها از سخت افزار و صدا را انتخاب کنید.

2. روی اسکنر کلیک راست کرده و ویژگیها را انتخاب کنید.

3. زبانه سرویس وب را انتخاب کرده و روی URL کلیک کنید.

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؛ البته این بدان معنا نیست که مشکلی وجود دارد و با خیال راحت می توانید از آن صرف نظر کنید.

نکته:

در بخش زیر، مقادیر اولیه برای اطلاعات سرپرستی Web Config ارائه می شوند.

• نام کاربری: هیچ (خالی)

• رمز عبور: شماره سریال اسکنر

شماره سریال را با بررسی برچسب متصل به پشت اسکنر ملاحظه کنید.

اگر گزینه Administrator Logout در قسمت بالای سمت راست صفحه نمایش مشخص شود، شما قبلاً به عنوان سرپرست وارد سیستم شده اید.

Epson Device Admin

Epson Device Admin برنامه ای چندکاره است که به شما اجازه می دهد دستگاههای روی شبکه را مدیریت کنید.

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

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

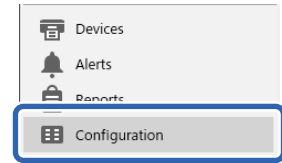
الگوی پیکربندی

ایجاد کردن الگوی پیکربندی

یک الگوی پیکربندی جدید ایجاد کنید.

1. Epson Device Admin را آغاز کنید.

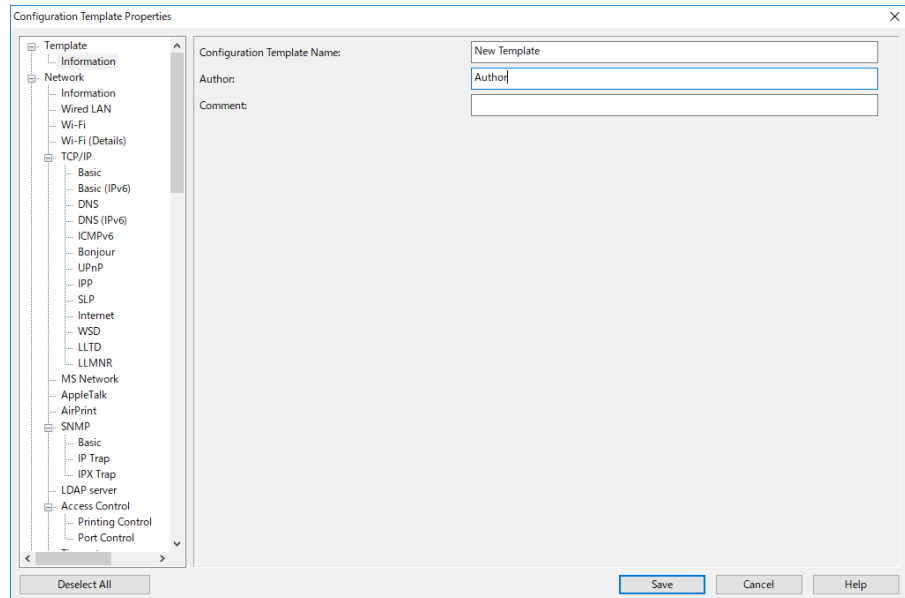
2. گزینه **Configuration** را در منوی نوار کارهای جانبی انتخاب کنید.



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.
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 گزینه های منو در سمت چپ کلیک کنید تا به هر صفحه جابجا شوید. اگر صفحه را تغییر دهید مقدار تنظیم شده حفظ می شود، اما در صورت لغو صفحه آن را از دست می دهید. 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 انتخاب شده در الگو اعمال می شوند. اگر اسکنر مقصد فاقد عملکرد مناسب باشد، این تنظیم اعمال نمی گردد.

نکته:

وقتی یک رمز عبور سرپرست برای اسکنر تعریف می کنید، ابتدا رمز عبور را پیکربندی نمایید.

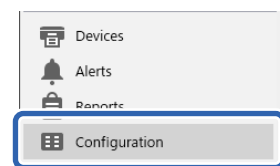
1. در منوی روبان صفحه لیست دستگاه ها، مسیر **Options < Password manager** را انتخاب کنید.

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

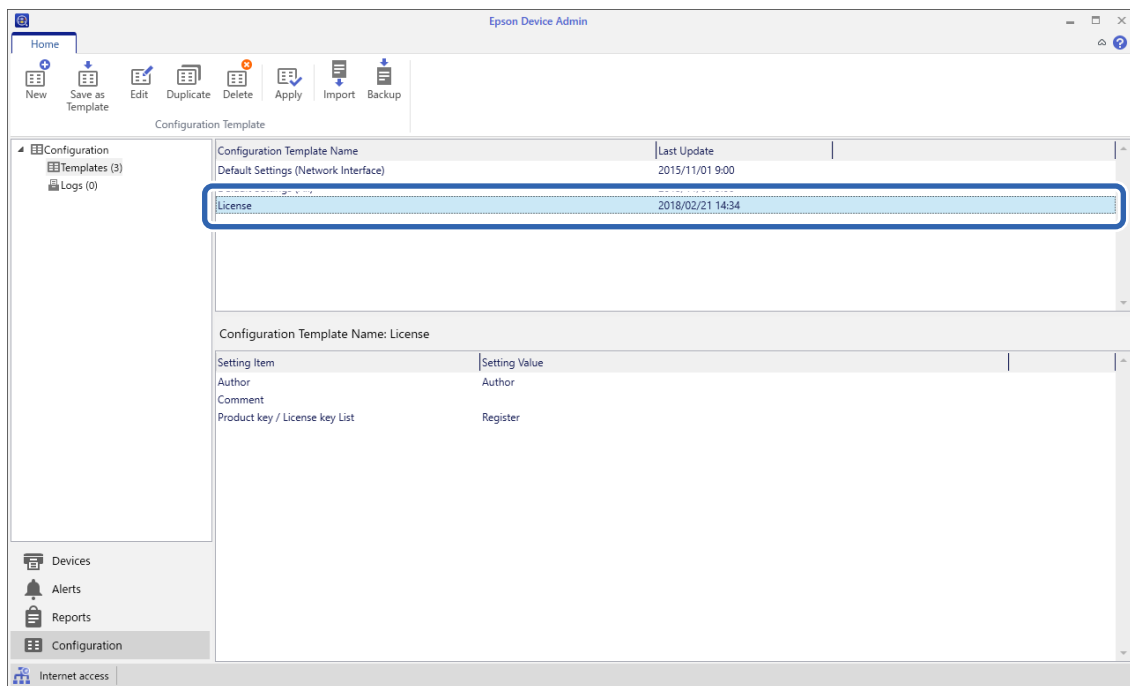
3. اسکنر مناسب را انتخاب کنید و سپس روی گزینه **Edit** کلیک کنید.

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 می شود.



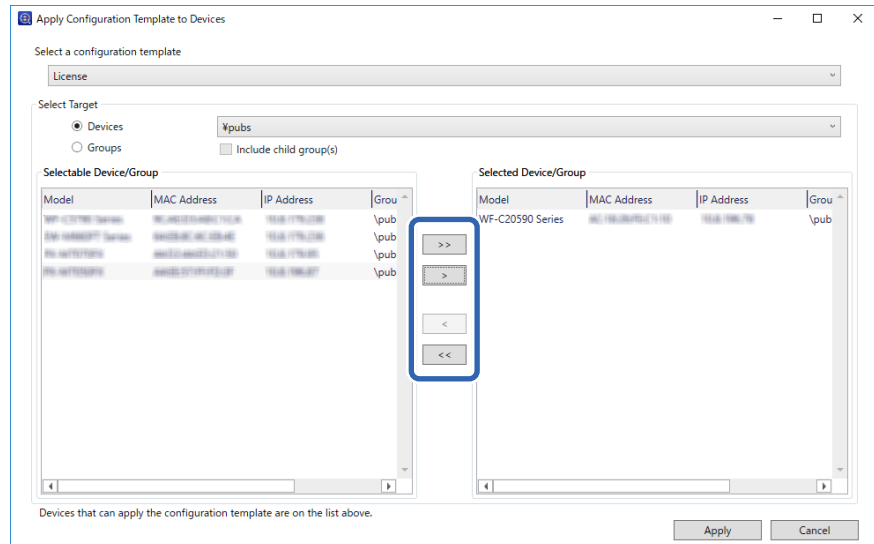
4. الگوی پیکربندی مورد نظر برای اعمال کردن را انتخاب کنید.

نکته:

وقتی **Devices** و گروه های حاوی دستگاه ها را از منوی کرکره ای انتخاب می کنید، هر دستگاه نمایش داده می شود.

وقتی گزینه **Groups** را انتخاب کنید، گروه ها نمایش داده می شوند. برای انتخاب خودکار گروه های زیرمجموعه درون گروه انتخاب شده، گزینه **Include child group(s)** را انتخاب کنید.

5. اسکتر یا گروه هایی 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 می شود.

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

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

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

وقتی گزینه روی مواردی که اعمال می کنید نمایش داده می شود، برنامه با موفقیت نصب شده است.

10. روی **Close** کلیک کنید.

تنظیمات لازم برای اسکن کردن

- 41. پیکربندی سرور ایمیل.
- 44. تنظیم یک پوشه اشتراک گذاری در شبکه.
- 61. در دسترس قرار دادن مخاطبین.
- 71. استفاده از Document Capture Pro Server.
- 71. راه اندازی AirPrint.
- 72. مشکلات هنگام تهیه اسکن شبکه.

پیکربندی سرور ایمیل

سرور ایمیل را از طریق Web Config تنظیم کنید.

وقتی از طریق تنظیم سرور ایمیل اسکن از امکان ارسال ایمیل برخوردار می‌گردد، موارد زیر امکان پذیر می‌باشند.

انتقال نتایج اسکن از طریق ایمیل

دریافت اعلان ایمیلی از طرف اسکن

قبل از انجام تنظیمات، موارد زیر را بررسی کنید.

اسکنر به شبکه‌ای متصل است که می‌تواند به سرور ایمیل دسترسی پیدا کند.

اطلاعات تنظیم ایمیل در رایانه‌ای که به همان سرور ایمیل اسکنر متصل می‌باشد.

نکته:

وقتی سرور ایمیل مبتنی بر اینترنت را استفاده می‌کنید، اطلاعات تنظیم دریافتی از طرف عرضه کننده یا وبسایت را تأیید نمایید.

از طریق پانل کنترل نیز می‌توانید سرور ایمیل را تنظیم کنید. به صورت زیر به آن وارد شوید.

تنظیم < تنظیمات شبکه > پیشرفته < سرور ایمیل > تنظیمات سرور

1. وارد Web Config شوید و زبانه **Basic < Email Server < Network** را انتخاب کنید.

2. برای هر مورد یک مقدار وارد کنید.

3. گزینه **OK** را انتخاب کنید.

تنظیمات انتخاب شده نمایش داده می‌شود.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

موارد تنظیم سرور ایمیل

تنظیمات و توضیحات	موارد
روش تأیید اعتبار اسکنر برای دسترسی به سرور ایمیل را مشخص کنید.	Authentication Method
تأیید اعتبار زمان ارتباط با سرور ایمیل غیرفعال است.	Off
سرور ایمیل باید از تأیید اعتبار SMTP پشتیبانی کند.	SMTP AUTH
زمان انتخاب این روش، سرور POP3 را پیکربندی کنید.	POP before SMTP
اگر SMTP AUTH یا POP before SMTP را به عنوان Authentication Method انتخاب کنید، نام حساب تأیید شده را از 0 تا 255 نویسه به فرمت ASCII ((0x20-0x7E) وارد کنید.	Authenticated Account
اگر SMTP AUTH یا POP before SMTP را به عنوان Authentication Method انتخاب کنید، باید گذرواژه تأیید شده را از 0 تا 20 نویسه به فرمت ASCII ((0x20-0x7E) وارد کنید.	Authenticated Password
آدرس ایمیل فرستنده را وارد کنید. بین 0 تا 255 نویسه با فرمت ASCII ((0x20-0x7E) به جز برای (< > ; [] ; ¥) وارد کنید. نقطه «.» نمی‌تواند اولین نویسه باشد.	Sender's Email Address
بین 0 تا 255 نویسه را با استفاده از 9-a-z0-A-Z وارد کنید. یا خط تیره (-). می‌توانید از فرمت IPv4 یا FQDN استفاده کنید.	SMTP Server Address

تنظیمات و توضیحات	موارد	
عددی بین 1 تا 65535 وارد کنید.	SMTP Server Port Number	
روش اتصال ایمن را برای این سرور ایمیل مشخص کنید.	Secure Connection	
اگر POP before SMTP را در Authentication Method انتخاب کنید، روش اتصال روی None تنظیم می شود.		None
این زمانی موجود است که Authentication Method روی Off یا SMTP AUTH تنظیم باشد.		SSL/TLS
این زمانی موجود است که Authentication Method روی Off یا SMTP AUTH تنظیم باشد.	STARTTLS	
زمانی که این فعال باشد گواهی تأیید می شود. ما توصیه می کنیم این روی Enable تنظیم باشد.	Certificate Validation	
اگر POP before SMTP را به عنوان Authentication Method انتخاب کنید، آدرس سرور POP3 را از 0 تا 255 نویسه با استفاده از این موارد وارد کنید 0-9 a-z A-Z. یا خط تیره (-). می توانید از فرمت IPv4 یا FQDN استفاده کنید.	POP3 Server Address	
اگر POP before SMTP را به عنوان Authentication Method انتخاب کنید، عددی بین 1 تا 65535 وارد کنید.	POP3 Server Port Number	

بررسی اتصال سرور ایمیل

اتصال به سرور ایمیل را می توانید از طریق بررسی اتصال ارزیابی کنید.

1. وارد Web Config شوید و زبانه **Network < Email Server < Connection Test** را انتخاب کنید.

2. **Start** را انتخاب کنید.

بررسی اتصال به سرور ایمیل شروع می شود. پس از آزمایش، گزارش بررسی نمایش داده می شود.

نکته:

همچنین می توانید اتصال به سرور را از طریق پانل کنترل نیز بررسی کنید. به صورت زیر به آن وارد شوید.

تنظیم < تنظیمات شبکه < پیشرفته < سرور ایمیل < بررسی اتصال

مرجع‌های بررسی اتصال سرور ایمیل

پیامها	علت
Connection test was successful.	این پیام زمانی ظاهر می‌شود که ارتباط با سرور با موفقیت برقرار شود.
SMTP server communication error. Check the following. - Network Settings	این پیام زمانی ظاهر می‌شود که <input type="checkbox"/> اسکز به شبکه وصل نباشد <input type="checkbox"/> سرور SMTP فعال نباشد <input type="checkbox"/> ارتباط با سرور در حین تبادل اطلاعات قطع شود <input type="checkbox"/> داده ناقص دریافت شود

پیامها	علت
POP3 server communication error. Check the following. - Network Settings	این پیام زمانی ظاهر می شود که <input type="checkbox"/> اسکتر به شبکه وصل نباشد <input type="checkbox"/> سرور POP3 فعال نباشد <input type="checkbox"/> ارتباط با سرور در حین تبادل اطلاعات قطع شود <input type="checkbox"/> داده ناقص دریافت شود
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	این پیام زمانی ظاهر می شود که <input type="checkbox"/> ارتباط با سرور DNS برقرار نشود <input type="checkbox"/> 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 می شود که <input type="checkbox"/> ارتباط با سرور DNS برقرار نشود <input type="checkbox"/> تفکیک نام برای سرور POP3 ناموفق باشد
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	این پیام زمانی ظاهر می شود که تایید هویت سرور SMTP ناموفق باشد.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	این پیام زمانی ظاهر می شود که تایید هویت سرور POP3 ناموفق باشد.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	این پیام طمانی ظاهر می شود که بخواهید با پروتکل های پشتیبانی نشده ارتباط برقرار کنید.
Connection to SMTP server failed. Change Secure Connection to None.	این پیام زمانی ظاهر می شود 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 می شود 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 می شود 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 می شود که تنظیم تاریخ و ساعت اسکتر نادرست باشد یا گواهی منقضی شده باشد.
The connection is untrusted. Check the following. - CA Certificate	این پیام زمانی ظاهر می شود که اسکتر فاقد گواهی ریشه متناظر با سرور باشد یا CA Certificate وارد نشده باشد.
The connection is not secured.	این پیام زمانی ظاهر می شود که گواهی کسب شده آسیب دیده باشد.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	این پیام زمانی ظاهر می شود که ناسازگاری روش تایید هویت بین سرور و مشتری رخ دهد. سرور از SMTP AUTH پشتیبانی می کند.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	این پیام زمانی ظاهر می شود که ناسازگاری روش تایید هویت بین سرور و مشتری رخ دهد. سرور از SMTP AUTH پشتیبانی نمی کند.
Sender's Email Address is incorrect. Change to the email address for your email service.	این پیام زمانی ظاهر می شود که نشانی ایمیل فرستنده معین نادرست باشد.

پیامها	علت
Cannot access the product until processing is complete.	این پیام زمانی ظاهر می‌شود که اسکنر مشغول باشد.

تنظیم یک پوشه اشتراک گذاری در شبکه

یک پوشه اشتراک گذاری در شبکه را تعیین کنید تا تصویر اسکن شده در آن ذخیره شود. هنگام ذخیره یک فایل در پوشه، اسکنر با همان مشخصات کاربری رایانه که پوشه در آن ایجاد شده است، وارد می‌شود.

ایجاد پوشه اشتراک گذاری

اطلاعات مرتبط

- ◀ "قبل از ایجاد پوشه اشتراک گذاری" در صفحه 44
- ◀ "بررسی کردن نمایه شبکه" در صفحه 44
- ◀ "موقعیتی که پوشه اشتراک گذاری در آن ایجاد می‌شود و یک نمونه امنیتی" در صفحه 45
- ◀ "افزودن گروه یا کاربری که اجازه دسترسی داشته باشد" در صفحه 58

قبل از ایجاد پوشه اشتراک گذاری

قبل از ایجاد پوشه اشتراک گذاری، موارد زیر را بررسی کنید.


- اسکنر به شبکه ای متصل است که از طریق آن می‌تواند به رایانه ای دسترسی داشته باشد که قرار است پوشه اشتراک گذاری در آن ایجاد شود.
- یک نویسه چندبایتی در نام رایانه ای که قرار است پوشه اشتراک گذاری در آن ایجاد شود وجود ندارد.

مهم!

وقتی یک نویسه چندبایتی در نام رایانه ای که قرار است پوشه اشتراک گذاری در آن ایجاد شود وجود داشته باشد، ممکن است فایل در پوشه اشتراک گذاری ذخیره نشود. در این قبیل موارد، به رایانه ای که نام آن حاوی نویسه چندبایتی نیست جابجا شوید یا نام رایانه فعلی را تغییر دهید. هنگام تغییر نام رایانه، از قبل با سرپرست هماهنگ کنید زیرا ممکن است برخی تنظیمات از قبیل مدیریت رایانه، دسترسی منابع و غیره تحت تاثیر قرار گیرند.

بررسی کردن نمایه شبکه

در رایانه ای که پوشه اشتراک گذاری در آن ایجاد خواهد شد، بررسی کنید آیا قابلیت اشتراک گذاری پوشه در دسترس می‌باشد.

1. از طریق حساب کاربری مرجع سرپرست به رایانه ای وارد شوید که پوشه اشتراک گذاری در آن ایجاد خواهد شد.
2. پانل کنترل < شبکه و اینترنت > شبکه و مرکز اشتراک گذاری را انتخاب کنید.
3. روی تغییر تنظیمات اشتراک گذاری پیشرفته و سپس  برای نمایه دارای (نمایه فعلی) در نمایه های شبکه نمایش یافته کلیک کنید.

4. بررسی کنید آیا فعال سازی اشتراک گذاری فایل و چاپگر در قسمت اشتراک گذاری فایل و چاپگر انتخاب شده است. 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.

موقعیتی که پوشه اشتراک گذاری در آن ایجاد می شود و یک نمونه امنیتی

بسته به موقعیتی که در آن پوشه اشتراک گذاری ایجاد می شود، قابلیت های امنیتی و سهولت دسترسی متفاوت خواهند بود. برای کار با پوشه اشتراک گذاری از طریق اسکرها یا سایر رایانه ها، مجوزهای خواندن و نوشتن زیر برای پوشه مورد نیاز می باشند.

□ زبانه اشتراک گذاری < اشتراک گذاری پیشرفته > مجوزها

این قسمت مجوز دسترسی شبکه مربوط به پوشه اشتراک گذاری را کنترل می کند.

□ مجوز دسترسی زبانه امنیتی

این قسمت مجوز دسترسی شبکه و دسترسی محلی مربوط به پوشه اشتراک گذاری را کنترل می کند.

وقتی گزینه همه را برای پوشه اشتراک گذاری که به عنوان یک نمونه ایجاد پوشه اشتراک گذاری در دسک تاپ ایجاد شده است تنظیم کنید، همه کاربرانی که امکان دسترسی به رایانه را دارند به پوشه نیز دسترسی خواهند داشت.

با این حال، کاربری که امکان دسترسی رایانه را ندارد، به پوشه نیز دسترسی نخواهد داشت زیرا دسک تاپ (پوشه) تحت کنترل پوشه کاربر قرار دارد و بنابراین، تنظیمات امنیتی پوشه کاربر نیز روی آن اعمال می گردند. کاربری که اجازه دسترسی را از طریق زبانه امنیتی کسب کرده است (کاربری که وارد شده است و در این مورد، سرپرست)، قادر به کار با پوشه خواهد بود.

برای ایجاد موقعیت مناسب، ادامه را ببینید.

این نمونه مربوط به زمان ایجاد پوشه «scan_folder» است.

اطلاعات مرتبط

← "نمونه پیکربندی برای سرورهای فایل" در صفحه 45

← "نمونه پیکربندی یک رایانه شخصی" در صفحه 52

نمونه پیکربندی برای سرورهای فایل

این توضیح نمونه ایجاد پوشه اشتراک گذاری در ریشه درایو در رایانه اشتراک گذاری شده مانند سرور فایل تحت شرایط زیر می باشد.

کاربران دارای دسترسی قابل کنترل از قبیل اشخاصی که دارای دامنه یکسان با رایانه ای که قرار است پوشه اشتراک گذاری در آن ایجاد شود هستند، می توانند به پوشه اشتراک گذاری دسترسی پیدا کنند.

این پیکربندی را در مواردی اعمال کنید که به یک کاربر اجازه خواندن و نگارش در پوشه اشتراک گذاری در رایانه از قبیل سرور فایل یا رایانه اشتراک گذاشته شده را می دهید.

□ محل ایجاد پوشه اشتراک گذاری: ریشه درایو

□ مسیر پوشه: scan_folder\C

□ اجازه دسترسی از طریق شبکه (مجوزهای اشتراک گذاری): همه

□ مجوز دسترسی به سیستم فایل (امنیتی): کاربران احراز هویت شده

1. از طریق حساب کاربری مرجع سرپرست به رایانه ای وارد شوید که پوشه اشتراک گذاری در آن ایجاد خواهد شد.

2. کاوشگر فایل را راه اندازی کنید.

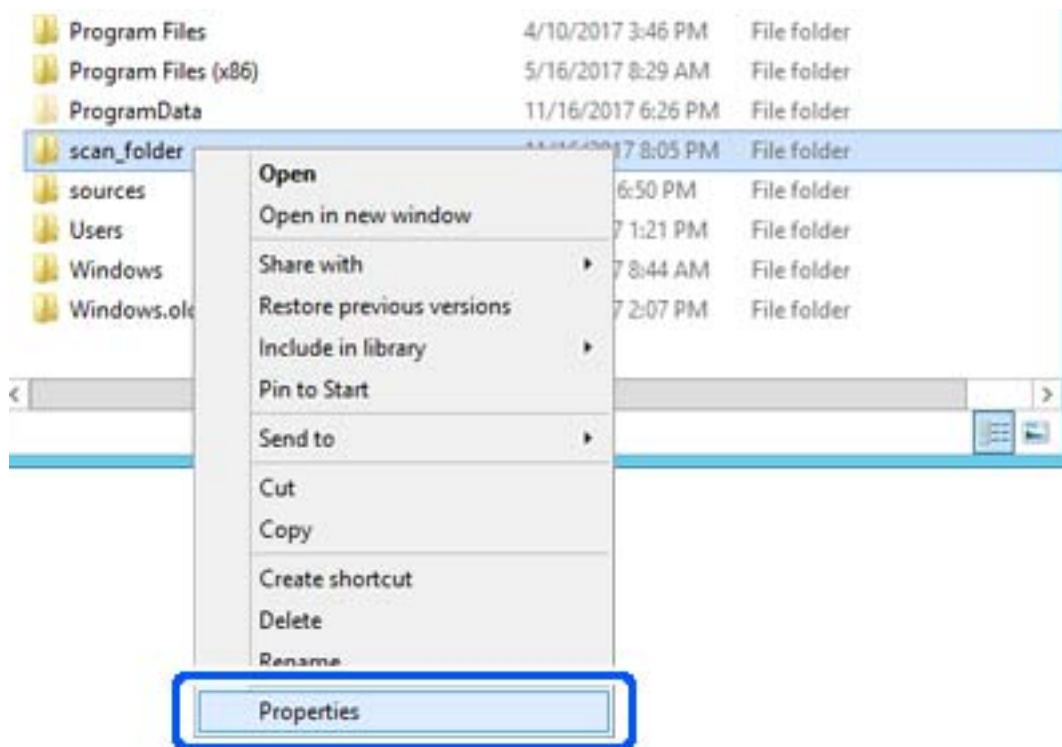
3.

یک پوشه در ریشه درایو ایجاد کرده و به صورت «scan_folder» نام گذاری کنید.

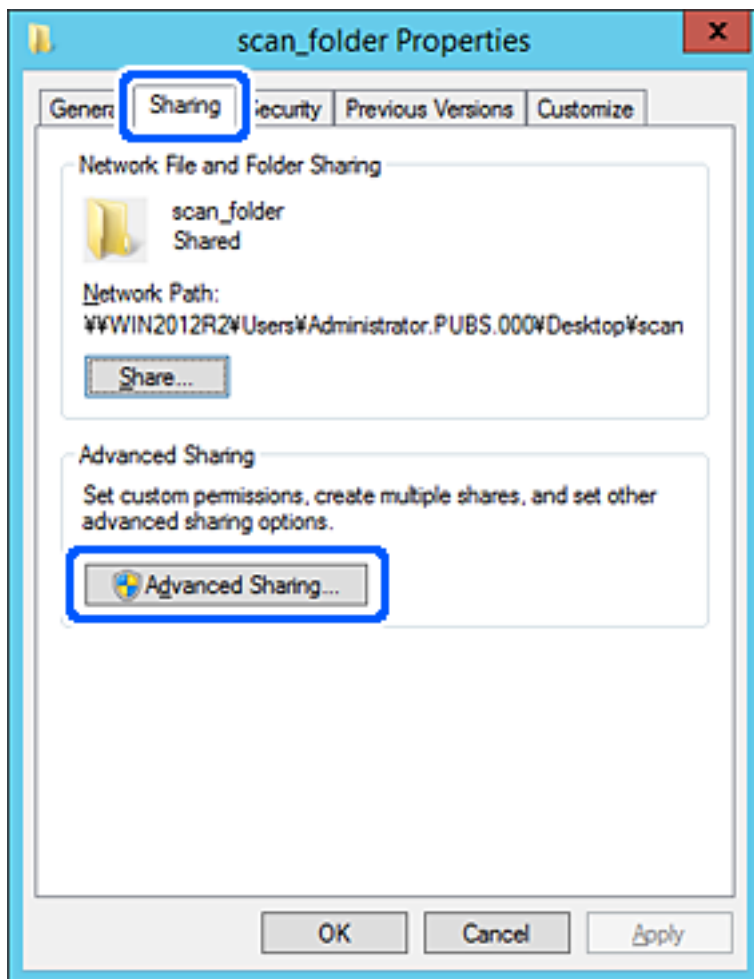
نام پوشه را با 1 تا 12 نویسه الفبایی عددی وارد کنید. اگر تعداد نویسه های نام پوشه از محدودیت مشخص شده بیشتر باشد، ممکن است قادر به دسترسی معمول آن در محیط تغییر یافته نباشید.

4.

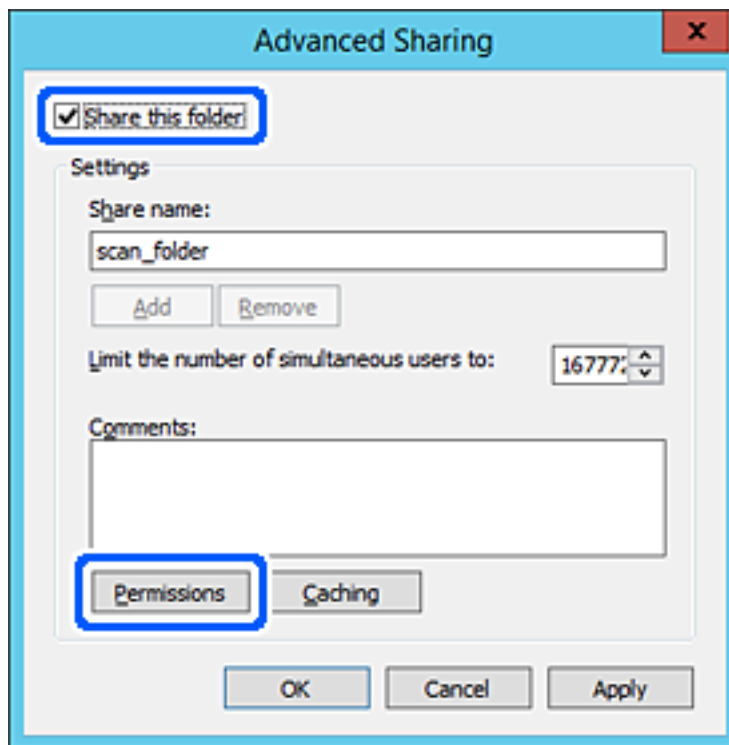
روی پوشه کلیک راست کرده و سپس ویژگی ها را انتخاب کنید.



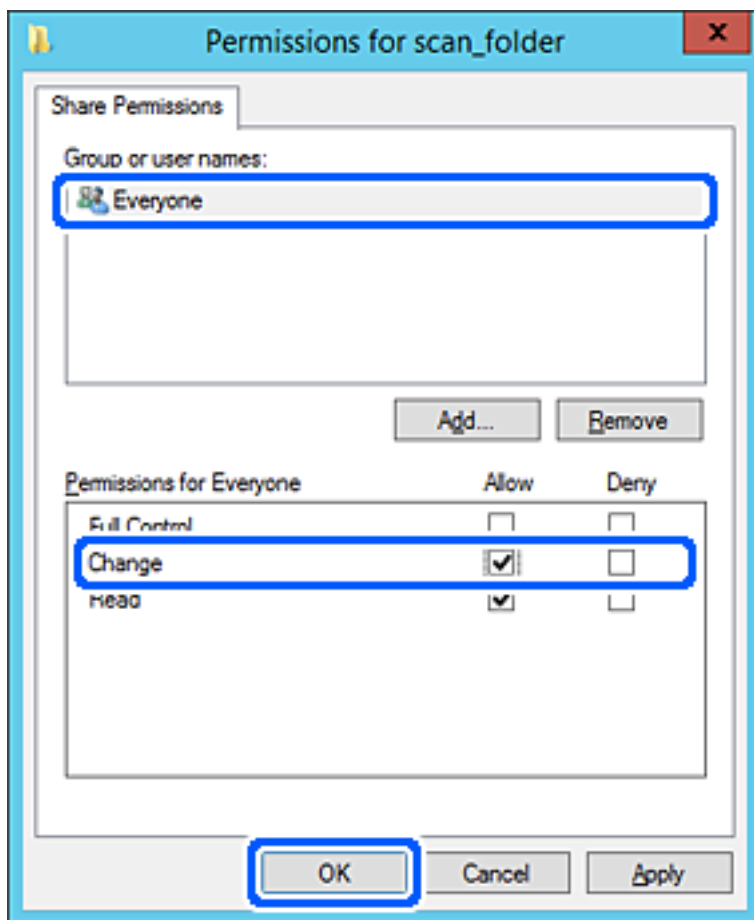
5. روی اشتراک گذاری پیشرفته در زبانه اشتراک گذاری کلیک کنید.



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

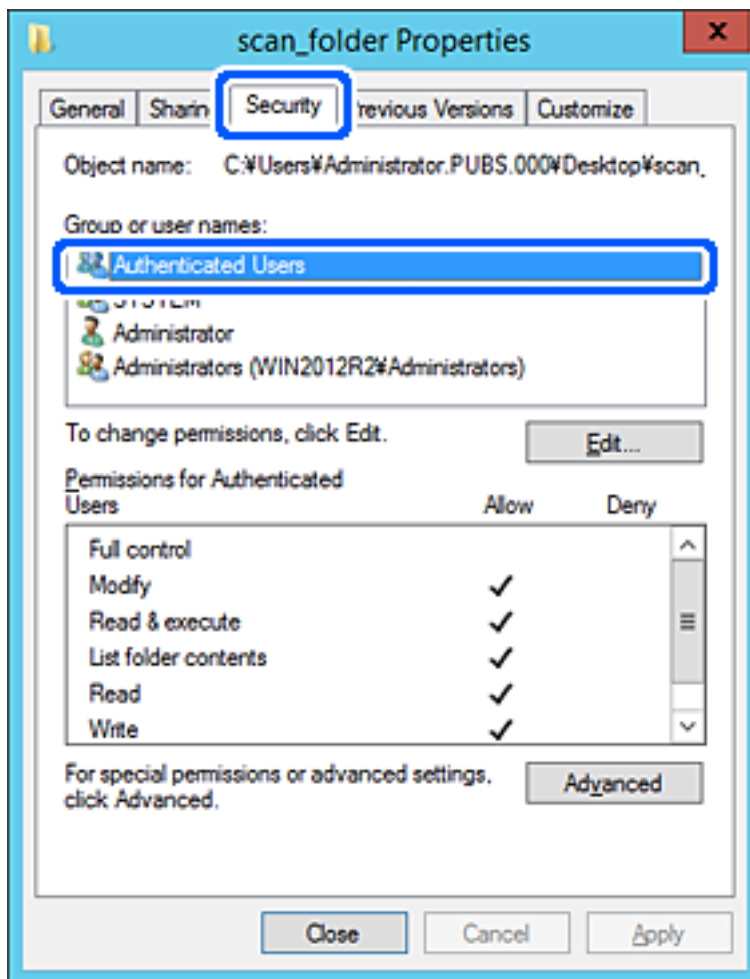


7. گروه همه در قسمت نام کاربران یا گروه ها را انتخاب کنید و سپس گزینه اجازه دادن در قسمت تغییر را برگزینید و در نهایت روی OK کلیک کنید.



8. روی OK کلیک کنید.

9. ابتدا زبانه امنیت و سپس کاربران احراز هویت شده در قسمت نام کاربران یا گروه‌ها را انتخاب کنید.



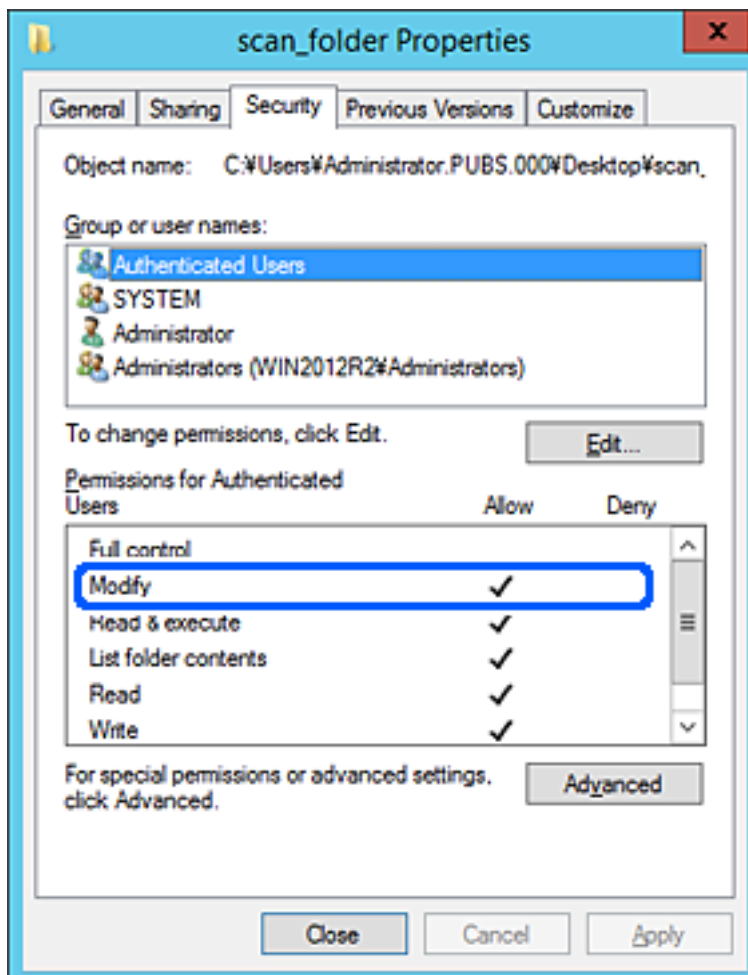
«کاربران احراز هویت شده» گروه خاصی است که همه کاربرانی که می‌تواند به دامنه یا رایانه وارد شوند را شامل می‌شوند. این گروه تنها زمانی نمایش داده می‌شود که پوشه بلافاصله زیر پوشه ریشه ایجاد شده باشد.

در صورت عدم نمایش، با کلیک کردن روی ویرایش می‌توانید آن را به صورت دستی اضافه کنید. جهت کسب اطلاعات بیشتر، بخش «اطلاعات مرتبط» را مشاهده کنید.

10.

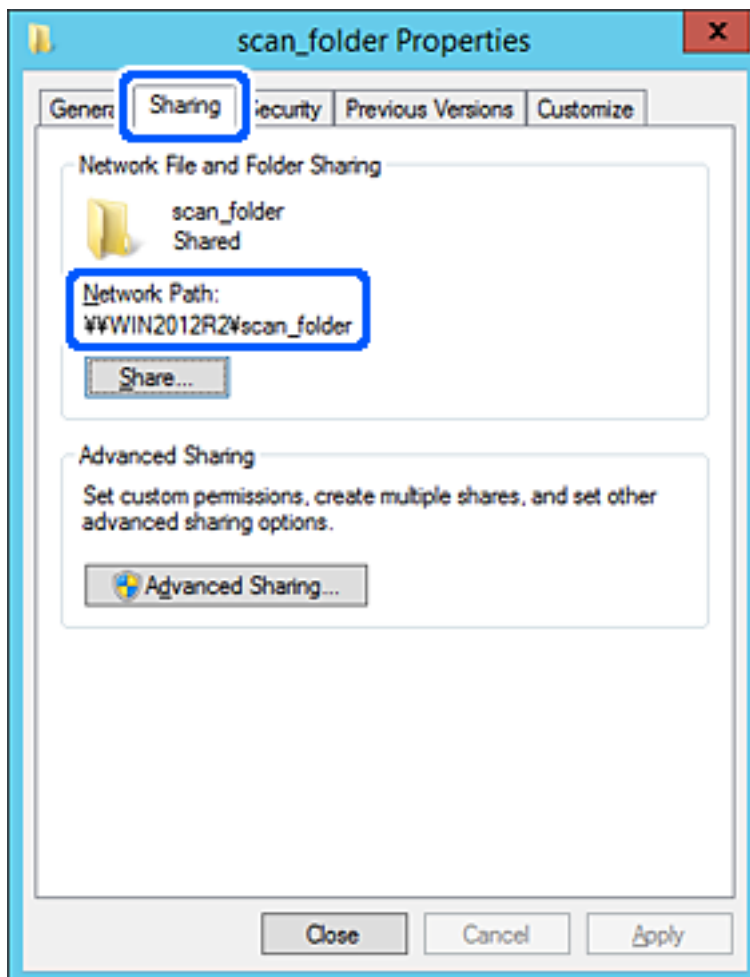
بررسی کنید گزینه اجازه دادن در قسمت تصحیح در بخش مجوزها برای کاربران احراز هویت شده انتخاب شده باشد.

اگر انتخاب نشده است، گزینه کاربران احراز هویت شده را انتخاب کنید و سپس روی ویرایش کلیک کرده و گزینه اجازه دادن را در قسمت تصحیح در مجوزها برای کاربران احراز هویت شده انتخاب نمایید و در نهایت روی OK کلیک کنید.



11. زبانه اشتراک گذاری را انتخاب کنید.

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



12. برای بستن صفحه، روی OK یا بستن کلیک کنید.

بررسی کنید آیا فایل موجود در پوشه اشتراک گذاری از طریق رایانه های با دامنه مشابه قابل نگارش یا خواندن می باشد.

اطلاعات مرتبط

- ◀ "افزودن گروه یا کاربری که اجازه دسترسی داشته باشد" در صفحه 58
- ◀ "ثبت یک مقصد برای مخاطبین با استفاده از Web Config" در صفحه 62

فونه پیکربندی یک رایانه شخصی

این توضیح فونه ای برای ایجاد پوشه اشتراک گذاری در دسک تاپ کاربری است که در حال حاضر به رایانه وارد شده است.

کاربری که به رایانه وارد می شود و شخصی که دارای اختیارات سرپرست است، به پوشه دسک تاپ و پوشه سند که زیرمجموعه پوشه «کاربر» می باشند دسترسی خواهند داشت.

این پیکربندی را وقتی اعمال کنید که در نظر دارید به کاربر دیگر اجازه ندهید پوشه اشتراک گذاری در یک رایانه شخصی را بخواند یا در جایی نگارش کند.

□ محل ایجاد پوشه اشتراک گذاری: دسک تاپ

مسیر پوشه: Users\xxxx\Desktop\scan_folder\C

اجازه دسترسی از طریق شبکه (مجوز های اشتراک گذاری): همه

اجازه دسترسی در سیستم فایل (امنیت): به دلخواه خود یا چیزی اضافه نکنید یا نام های کاربر/گروه ها را برای اجازه دادن دسترسی اضافه نمایید

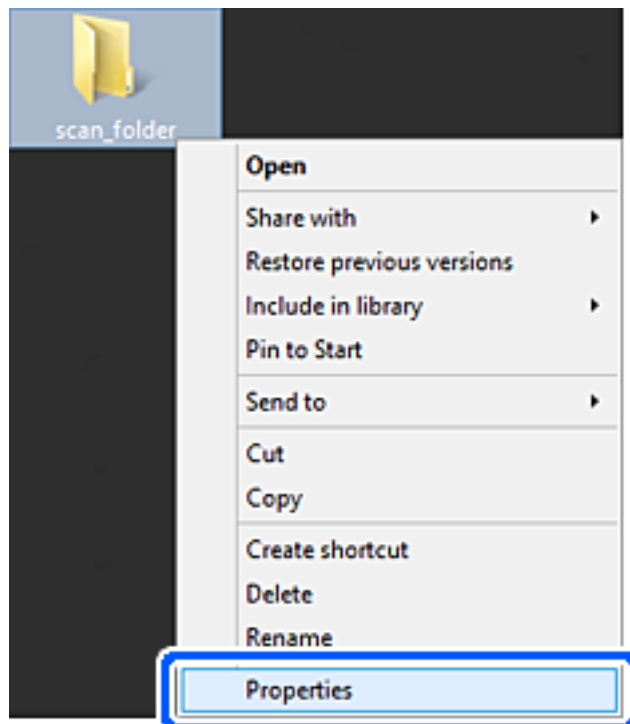
1. از طریق حساب کاربری مرجع سرپرست به رایانه ای وارد شوید که پوشه اشتراک گذاری در آن ایجاد خواهد شد.

2. کاوشگر فایل را راه اندازی کنید.

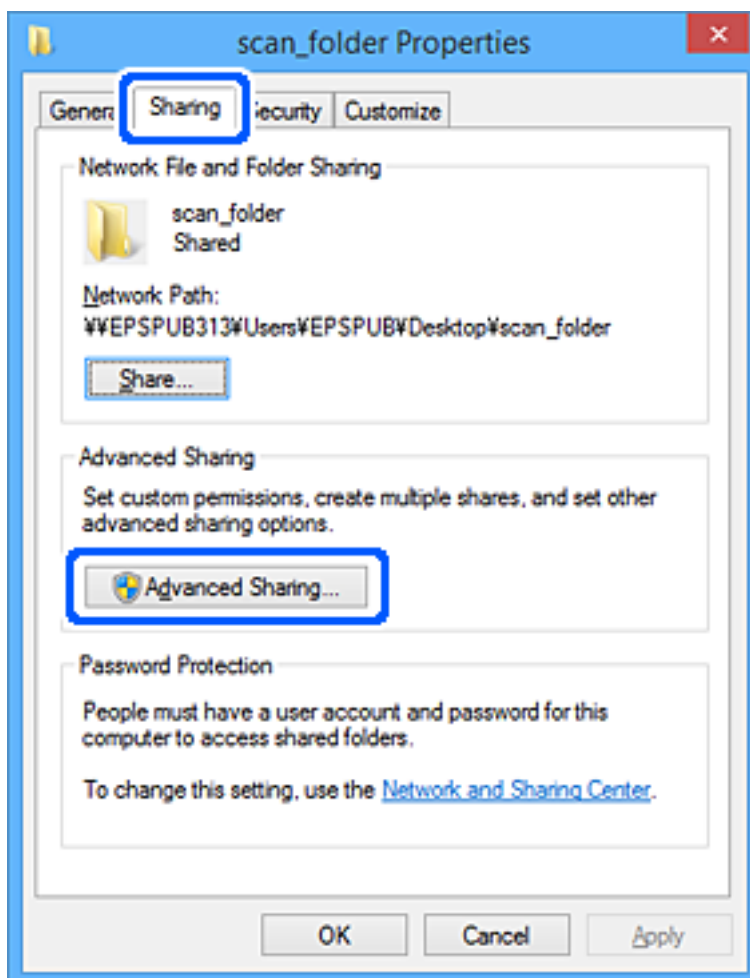
3. یک پوشه در دسک تاپ ایجاد کرده و به صورت «scan_folder» نام گذاری کنید.

نام پوشه را با 1 تا 12 نویسه الفبایی عددی وارد کنید. اگر تعداد نویسه های نام پوشه از محدودیت مشخص شده بیشتر باشد، ممکن است قادر به دسترسی معمول آن در محیط تغییر یافته نباشید.

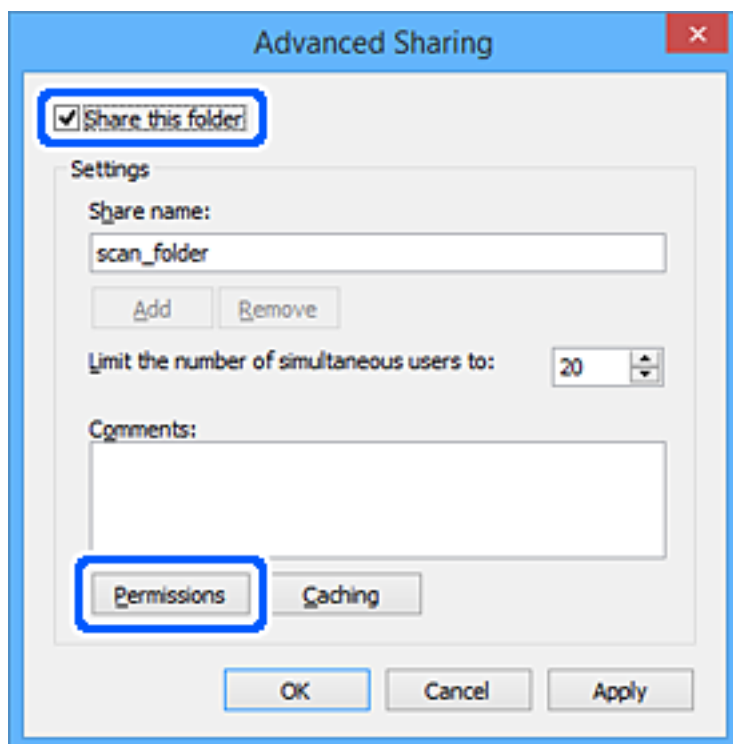
4. روی پوشه کلیک راست کرده و سپس ویژگی ها را انتخاب کنید.



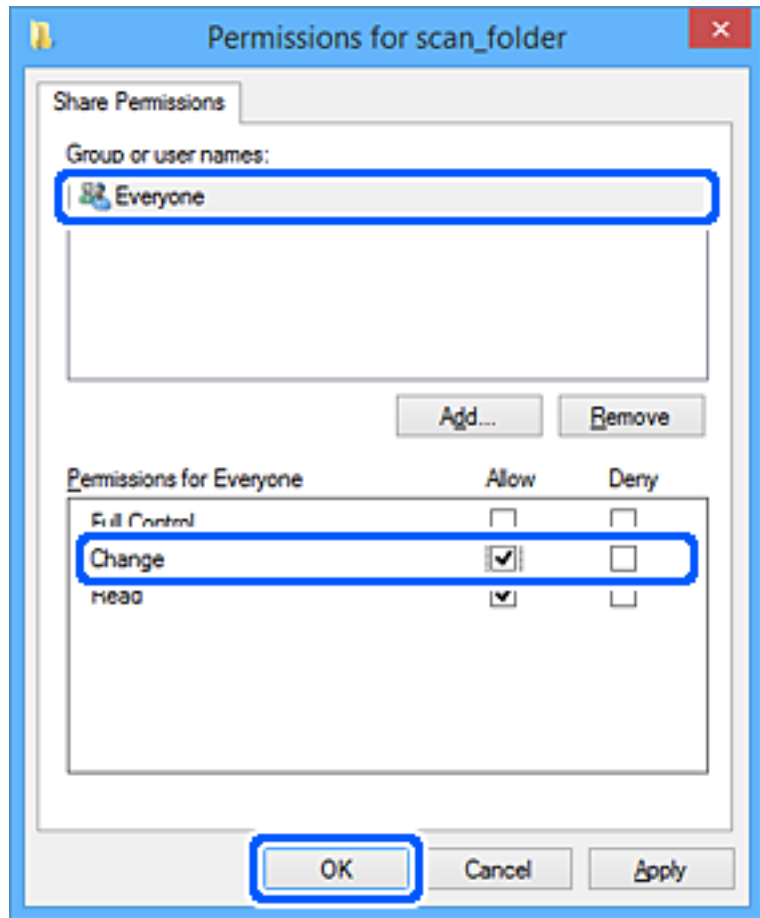
5. روی اشتراک گذاری پیشرفته در زبانه اشتراک گذاری کلیک کنید.



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



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



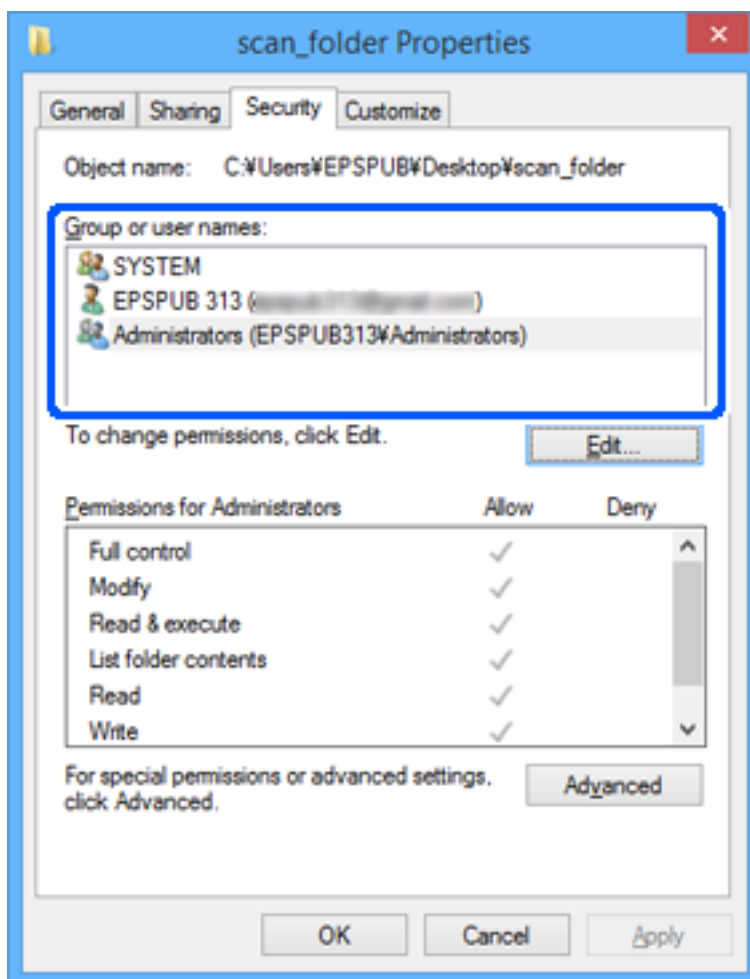
8. روی OK کلیک کنید.

9. زبانه امنیت را انتخاب کنید.

10. گروه یا کاربر را در قسمت نام های کاربر یا گروه بررسی کنید.

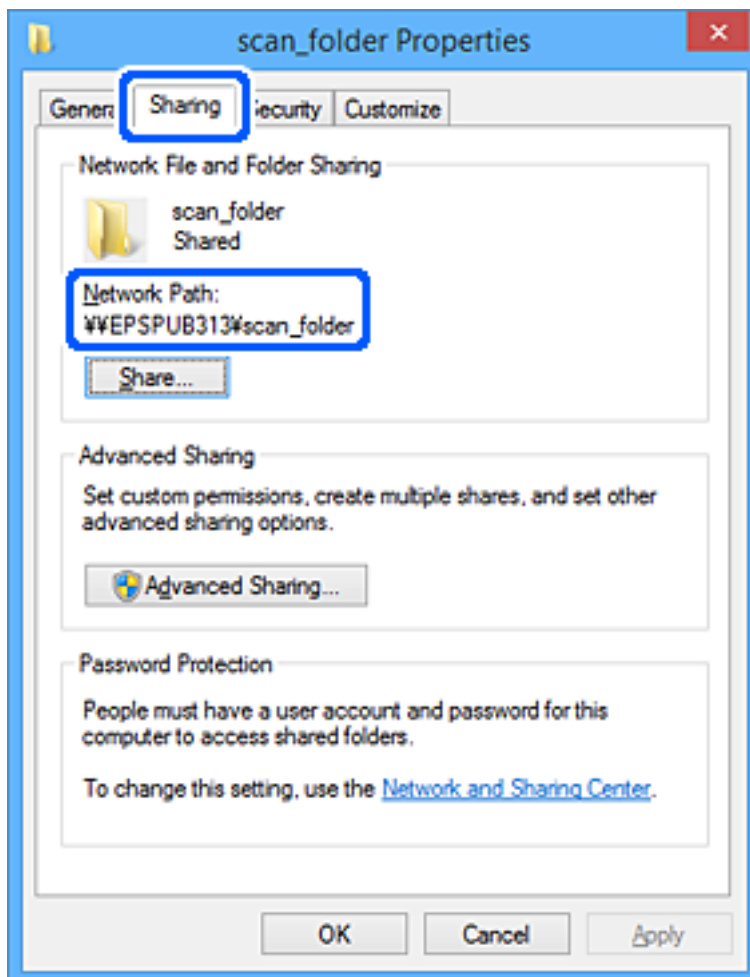
گروه یا کاربری که در اینجا نمایش داده می شود، قادر به دسترسی پوشه اشتراک گذاری می باشد. در این مورد، کاربری که به این رایانه وارد شده باشد به همراه سرپرست قادر به دسترسی پوشه اشتراک گذاری خواهند بود.

در صورت نیاز، مجوز دسترسی را اضافه کنید. با کلیک روی ویرایش می توانید آن را اضافه کنید. جهت کسب اطلاعات بیشتر، بخش «اطلاعات مرتبط» را مشاهده کنید.



11. زبانه اشتراک گذاری را انتخاب کنید.

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



12. برای بستن صفحه، روی OK یا بستن کلیک کنید.

بررسی کنید آیا فایل موجود در پوشه اشتراک گذاری از طریق رایانه های کاربران یا گروه های دارای اجازه دسترسی قابل نگارش یا خواندن می باشد.

اطلاعات مرتبط

- ◀ "افزودن گروه یا کاربری که اجازه دسترسی داشته باشد" در صفحه 58
- ◀ "ثبت یک مقصد برای مخاطبین با استفاده از Web Config" در صفحه 62

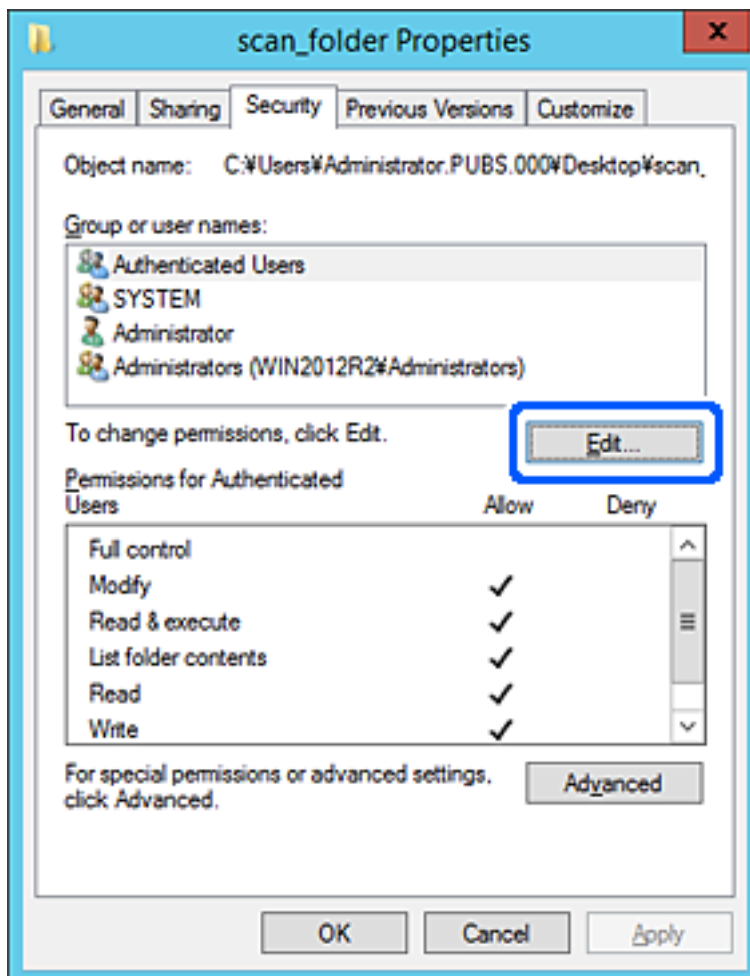
افزودن گروه یا کاربری که اجازه دسترسی داشته باشد

شما می توانید گروه یا کاربری که اجازه دسترسی داشته باشد را اضافه کنید.

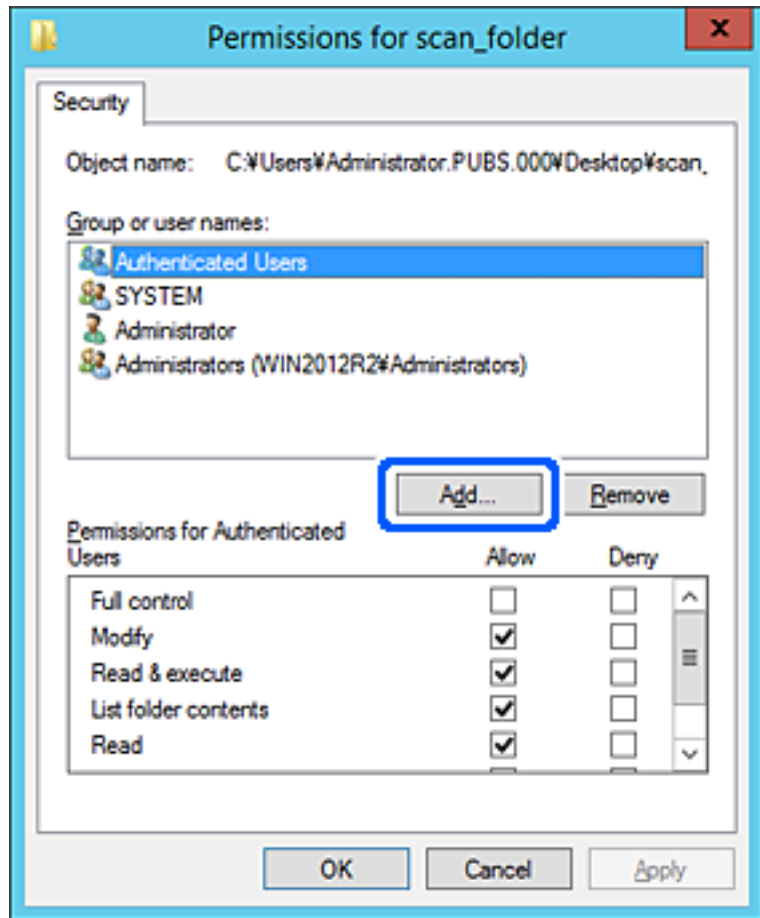
1. روی پوشه کلیک راست کرده و سپس ویژگی ها را انتخاب کنید.

2. زبانه امنیت را انتخاب کنید.

3. روی ویرایش کلیک کنید.



4. روی گزینه افزودن زیر نام کاربران یا گروه‌ها کلیک کنید.

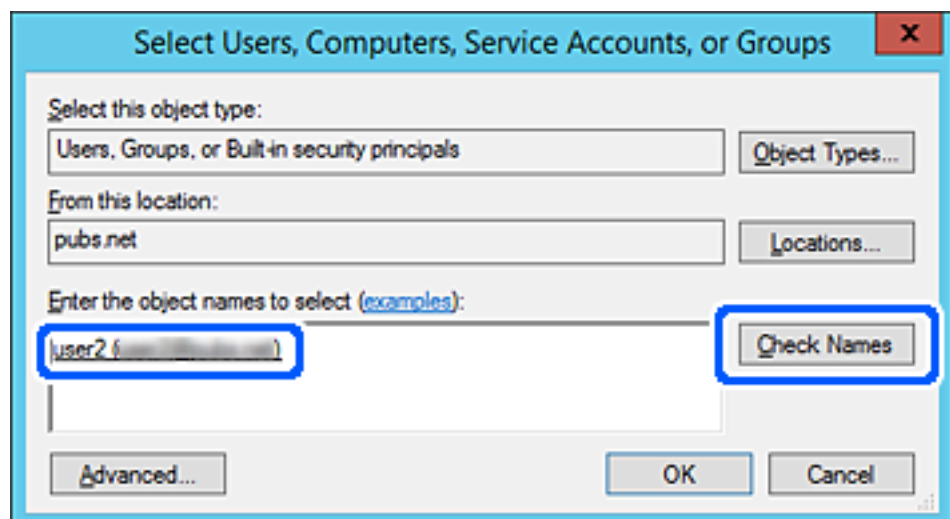


5. نام کاربر یا گروهی که در نظر دارید اجازه دسترسی داشته باشد را وارد کنید و سپس روی بررسی نام‌ها کلیک کنید. یک زیرخط به نام اضافه می‌شود.

نکته:

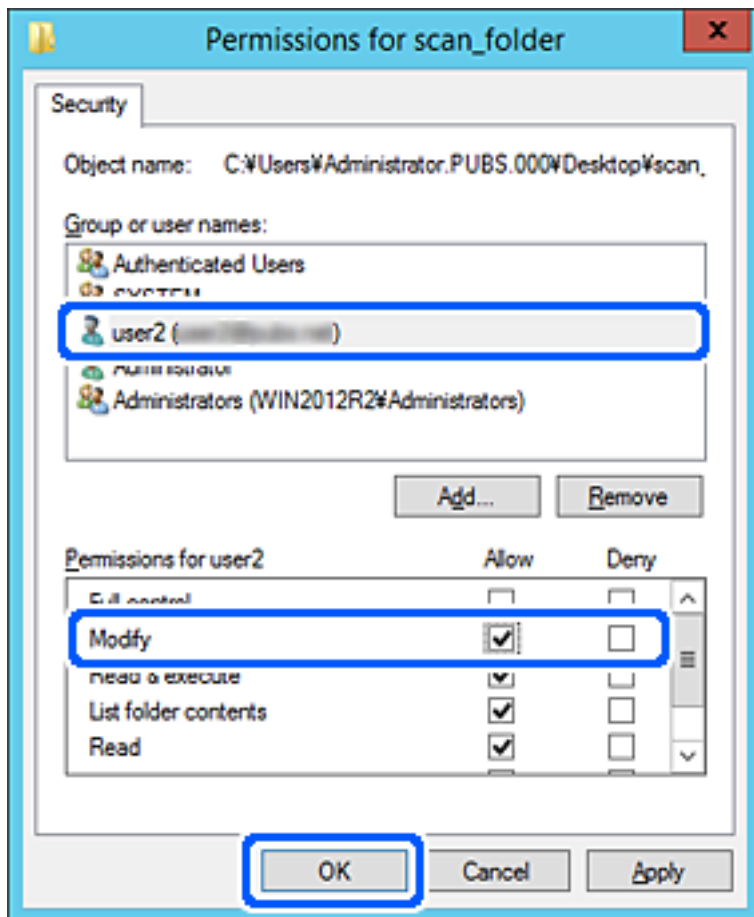
اگر نام کامل گروه یا کاربر را نمی‌دانید، بخشی از نام را وارد کنید و سپس روی گزینه بررسی نام‌ها کلیک کنید. نام‌های گروه یا نام‌های کاربری که با آن بخش از نام مطابقت دارند لیست می‌شوند و سپس می‌توانید نام کامل را از لیست انتخاب کنید.

اگر تنها یک نام مطابقت داشته باشد، نام کامل با زیرخط در قسمت نام شی را برای انتخاب وارد کنید نمایش داده می‌شود.



6. روی تأیید کلیک کنید.

7. در صفحه مجوز، نام کاربری که در قسمت نام کاربران یا گروه‌ها وارد شده است را انتخاب کنید و سپس در قسمت «تغییر»، اجازه دسترسی را انتخاب کنید و در نهایت روی گزینه تأیید کلیک کنید.



8. برای بستن صفحه، روی تأیید یا بستن کلیک کنید.

بررسی کنید آیا فایل موجود در پوشه اشتراک‌گذاری از طریق رایانه‌های کاربران یا گروه‌های دارای اجازه دسترسی قابل نگارش یا خواندن می‌باشد.

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 68

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 می‌توانید مخاطبین را در پانل کنترل اسکنر ثبت کنید.

1. وارد Web Config شوید و زبانه **Scan < Contacts** را انتخاب کنید.

2. عددی را که می‌خواهید 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 می‌توانید 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 مرورگر وب" در صفحه 35

گزینه‌های تنظیم مقصد

تنظیمات و توضیحات	موارد
تنظیمات عمومی	
Name	نامی را که باید در مخاطبان ظاهر شود با حداکثر 30 نویسه یونیکد (UTF-8) وارد کنید. اگر نمی‌خواهید این را مشخص کنید، خالی بگذارید.
Index Word	نام موردنظرتان را با استفاده از 30 نویسه یا کمتر در قالب (Unicode (UTF-8 وارد کنید تا مخاطبین در پانل کنترل اسکنر جستجو شوند. اگر نمی‌خواهید این را مشخص کنید، خالی بگذارید.
Type	نوع آدرسی را که می‌خواهید ثبت کنید انتخاب نمایید.
Assign to Frequent Use	برای تنظیم نشانی ثبت شده به عنوان نشانی پرکاربرد انتخاب نمایید. در صورت تنظیم کردن به عنوان آدرس پرکاربرد، در صفحه بالایی اسکنر ظاهر می‌شود و شما می‌توانید مقصد را بدون نشان دادن 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-8) بدون "\" وارد کنید. مسیر شبکه نمایش یافته در صفحه ویژگی‌های پوشه را وارد کنید. برای دریافت اطلاعات بیشتر درباره تنظیم مسیر شبکه بخش زیر را ببینید. "نمونه پیکربندی یک رایانه شخصی" در صفحه 52
User Name	نام کاربر برای دسترسی به پوشه شبکه را با حداکثر 30 نویسه یونیکد (UTF-8) وارد کنید. هر چند، نباید از نویسه‌های کنترلی (0x7F, 0x00-0x1F) استفاده کنید.
Password	رمز عبور برای دسترسی به پوشه شبکه را با حداکثر 20 نویسه یونیکد (UTF-8) وارد کنید. هر چند، نباید از نویسه‌های کنترلی (0x7F, 0x00-0x1F) استفاده کنید.
FTP	
Secure Connection	FTP یا FTPS را مطابق با پروتکل انتقال فایل که سرور FTP پشتیبانی می‌کند، انتخاب کنید. گزینه FTPS را انتخاب کنید تا به اسکنر اجازه بدهید با معیارهای امنیتی ارتباط برقرار کند.
Save to	نام سرور را با 1 تا 253 نویسه در قالب ASCII (0x20-0x7E) بدون "ftp://" یا "ftps://" وارد کنید.
User Name	نام کاربر برای دسترسی به سرور FTP را با حداکثر 30 نویسه یونیکد (UTF-8) وارد کنید. هر چند، نباید از نویسه‌های کنترلی (0x7F, 0x00-0x1F) استفاده کنید. اگر سرور اتصالات بی نام را مجاز بداند، باید نام کاربری مانند Anonymous و FTP وارد کنید. اگر نمی‌خواهید این را مشخص کنید، خالی بگذارید.
Password	رمز عبور برای دسترسی به سرور FTP را با حداکثر 20 نویسه یونیکد (UTF-8) وارد کنید. هر چند، نباید از نویسه‌های کنترلی (0x7F, 0x00-0x1F) استفاده کنید. اگر نمی‌خواهید این را مشخص کنید، خالی بگذارید.
Connection Mode	حالت اتصال را از منو انتخاب کنید. اگر بین اسکنر و سرور FTP، فایروال تنظیم شده است، گزینه Passive Mode را انتخاب کنید.
Port Number	شماره درگاه سرور FTP را از 1 تا 65535 وارد کنید.
Certificate Validation	زمانی که این فعال باشد گواهی سرور FTP تأیید می‌شود. این زمانی موجود است که FTPS برای Secure Connection انتخاب شده باشد. برای انجام تنظیمات لازم است CA Certificate را به اسکنر وارد کنید.

تنظیمات و توضیحات	موارد
	SharePoint(WebDAV)
HTTP یا HTTPS را مطابق با پروتکل انتقال فایلی که سرور پشتیبانی می‌کند، انتخاب کنید. گزینه HTTPS را انتخاب کنید تا به اسکنر اجازه بدهید با معیارهای امنیتی ارتباط برقرار کند.	Secure Connection
نام سرور را با 1 تا 253 نویسه در قالب ASCII (0x20-0x7E) بدون "http://" یا "https://" وارد کنید.	Save to
نام کاربر برای دسترسی به یک سرور را با حداکثر 30 نویسه یونیکد (UTF-8) وارد کنید. هر چند، نباید از نویسه‌های کنترلی (0x00-0x1F, 0x7F) استفاده کنید. اگر نمی‌خواهید این را مشخص کنید، خالی بگذارید.	User Name
رمز عبور برای دسترسی به سرور را با حداکثر 20 نویسه یونیکد (UTF-8) وارد کنید. هر چند، نباید از نویسه‌های کنترلی (0x00-0x1F, 0x7F) استفاده کنید. اگر نمی‌خواهید این را مشخص کنید، خالی بگذارید.	Password
زمانی که این فعال باشد گواهی سرور تأیید می‌شود. این زمانی موجود است که HTTPS برای Secure Connection انتخاب شده باشد. برای انجام تنظیمات لازم است CA Certificate را به اسکنر وارد کنید.	Certificate Validation
انتخاب کنید که آیا می‌خواهید از یک سرور پروکسی استفاده کنید یا خیر.	Proxy Server

ثبت مقصدها به عنوان گروه از طریق Web Config

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

1. وارد Web Config شوید و زبانه **Scan < Contacts** را انتخاب کنید.
2. عددی را که می‌خواهید 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 می‌شود.
5. مقصدهایی را که می‌خواهید 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 می‌دهید یا خیر.
نکته:
مقصدها را می‌توان در چندین گروه ثبت کرد.
8. روی **Apply** کلیک کنید.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

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.
4. 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 **Basic < LDAP Server < Network** 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. <input type="checkbox"/> اسکنر و سرور DNS می توانند ارتباط برقرار کنند. <input type="checkbox"/> زمان اسکنر، سرور KDC و سرور مورد نیاز برای تأیید اعتبار (سرور LDAP، سرور SMTP، سرور File) همگام می شوند. <input type="checkbox"/> 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.

تنظیمات و توضیحات	موارد
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.	Password

تنظیمات Kerberos

اگر **Kerberos Authentication Method** 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.

تنظیمات و توضیحات	موارد
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.	Realm (Domain)
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.	KDC Address
شماره درگاه سرور Kerberos را از 1 تا 65535 وارد کنید.	Port Number (Kerberos)

پیگیری 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 **LDAP Server < Network < 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

تنظیمات و توضیحات	موارد
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. فهرته دایرکتوری سرور محلی: dc=server, dc=local	Search Base (Distinguished Name)
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.	Number of search entries
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: uid, cn	User name Attribute

تنظیمات و توضیحات	موارد
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	User name Display 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	Email Address Attribute
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: ou, o	- Arbitrary Attribute 1 Arbitrary Attribute 4

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 **LDAP Server < Network < 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

توضیحات	پیام ها
این پیام زمانی ظاهر می شود که ارتباط با سرور با موفقیت برقرار شود.	Connection test was successful.
این پیام به دلایل زیر ظاهر می شود: <input type="checkbox"/> نشانی سرور LDAP یا شماره درگاه نادرست است. <input type="checkbox"/> وقفه رخ داده است. <input type="checkbox"/> گزینه Do Not Use به عنوان حالت Use LDAP Server انتخاب شده است. <input type="checkbox"/> 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 settings.
این پیام زمانی ظاهر می شود که اتصال به دلیل ناسازگاری تنظیمات زمان اسکت و سرور LDAP قطع شود.	Connection test failed. Check the date and time on your product or server.
این پیام به دلایل زیر ظاهر می شود: <input type="checkbox"/> User Name و/یا Password نادرست باشد. <input type="checkbox"/> اگر Kerberos Authentication به عنوان Authentication Method انتخاب شود، ممکن است ساعت/تاریخ پیکربندی نشود.	Authentication failed. Check the settings.
این پیام زمانی ظاهر می شود که اسکت مشغول باشد.	Cannot access the product until processing is complete.

استفاده از Document Capture Pro Server

با استفاده از Document Capture Pro Server می‌توانید روش مرتب‌سازی، قالب ذخیره‌سازی و مقصد انتقال نتیجه اسکن اجرا شده را از پانل کنترل اسکنر مدیریت کنید. می‌توانید کار قبلاً ثبت شده در سرور را از پانل کنترل اسکنر فراخوانی و اجرا کنید.

آن را روی رایانه سرور نصب کنید.

برای کسب اطلاعات بیشتر درباره Document Capture Pro Server با دفتر محلی Epson تماس بگیرید.

تنظیم حالت سرور

برای استفاده از Document Capture Pro Server، به روش زیر عمل کنید.

1. وارد Web Config شوید و زبانه **Document Capture Pro < Scan** را انتخاب کنید.
2. گزینه **Server Mode** را برای **Mode** انتخاب کنید.
3. آدرس سرور را با Document Capture Pro Server نصب شده روی آن برای **Server Address** وارد کنید.
بین 2 تا 255 نویسه از IPv4، IPv6، نام میزبان یا قالب FQDN وارد کنید. برای قالب FQDN، می‌توانید از نویسه‌های الفبایی عددی با قالب ASCII ((0x20-0x7E) و «-» به جز برای شروع و انتهای آدرس استفاده کنید.
4. روی **OK** کلیک کنید.
اتصال شبکه دوباره برقرار می‌شود و سپس تنظیمات فعال می‌گردد.

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 UTF-8 (Unicode) 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) فعال هستند.

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 سرویس‌گیرنده 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.

■ مرورگر 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 اسکن 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 می‌شود. 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 < LAN سرور پراکسی را انتخاب کنید و سپس پیکربندی کنید که از سرور پراکسی برای LAN (آدرس‌های محلی) استفاده نشود.

Mac OS:

گزینه ترجیحات سیستم < شبکه > پیشرفته < پراکسی‌ها را انتخاب کنید و سپس آدرس محلی برای نادیده گرفتن تنظیمات پراکسی برای این میزبان‌ها و دامنه‌ها را ثبت کنید.

مثال:

192.168.*: 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 اشتراک گذاری > تغییر تنظیمات آداپتور کلیک کنید. صفحه ویژگی‌های اتصال مورد استفاده خود و در ادامه صفحه ویژگی‌های مربوط به پروتکل اینترنت نسخه 4 (TCP/IP4) یا پروتکل اینترنت نسخه 6 (TCP/IP6) را باز کنید. در صفحه نمایش یافته بررسی کنید گزینه دریافت خودکار آدرس IP انتخاب شده باشد.


سفارشی کردن نمایشگر پانل کنترل

75. ثبت پیش تنظیمات.

77. ویرایش صفحه اصلی پانل کنترل.

ثبت پیش‌تنظیمات

می‌توانید 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.

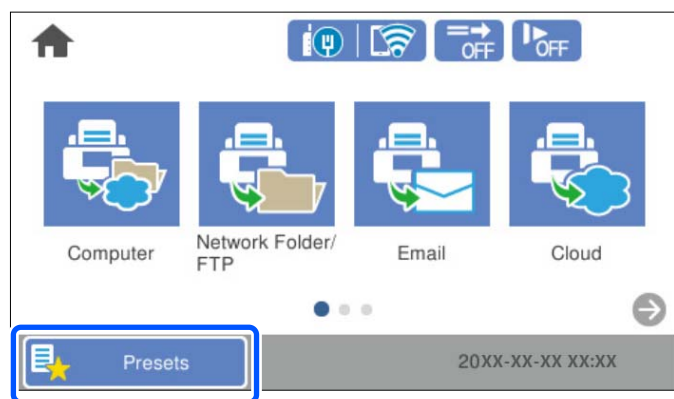
می‌توانید **Presets** را در **Web Config** ثبت کنید.

زبان **Scan < Presets** را انتخاب کنید.

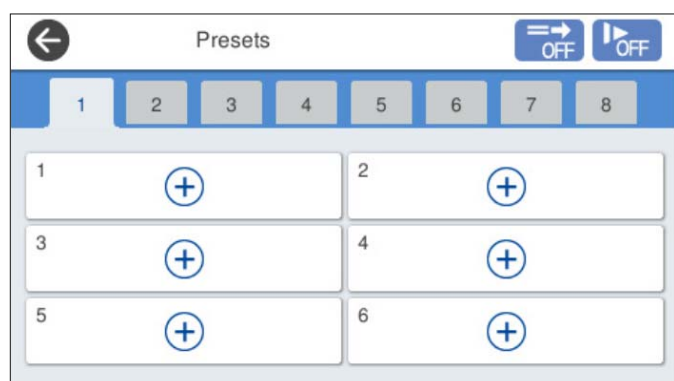
اگر هنگام ثبت گزینه ذخیره اسکن در رایانه را انتخاب کنید قادر خواهید بود کار ایجاد شده را در بخش **Document Capture Pro** به عنوان **Presets** ثبت کنید. این تنها برای رایانه‌های متصل از طریق شبکه در دسترس می‌باشد. کار را از قبل در **Document Capture Pro** ثبت کنید.

اگر عملکرد تأیید هویت فعال شود، تنها سرپرست می‌تواند **Presets** را ثبت نماید.

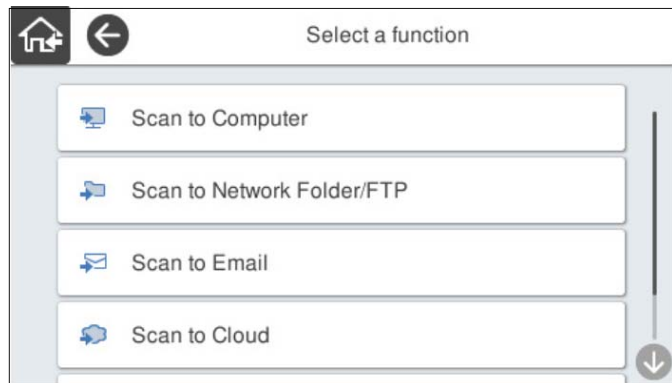
1. منوی **پیش‌تنظیمات** در صفحه اصلی پانل کنترل اسکن را انتخاب کنید.




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.

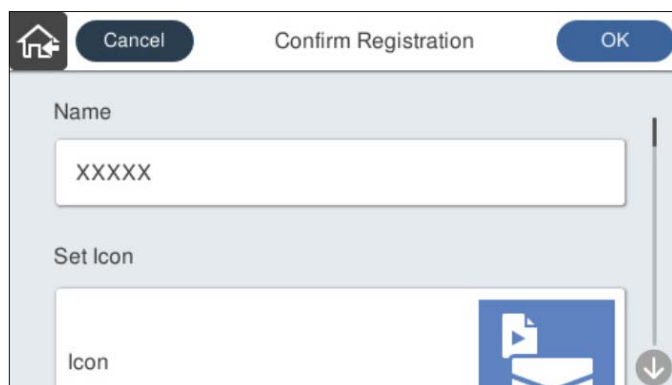
نام: نام را تنظیم کنید.

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.


وقتی از Document Capture Pro Server استفاده می‌کنید حتی اگر نرم‌افزار را برای تأیید محتوای کار قبل از اسکن تنظیم نمایید، گزینه تنظیم ارسال فوری در حالت پیش‌تنظیم اسکن بر نرم‌افزار اولویت خواهد داشت.

فهرست مطالب: تنظیمات اسکن را بررسی کنید.



6. گزینه OK را انتخاب کنید.

گزینه های منو پیش‌تنظیمات

تنظیمات از پیش تعیین شده را می‌توانید 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 می‌دهد.

تنظیم ارسال فوری:

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

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 می‌کند.

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 77

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 78

حذف نماد: آیکن‌ها را از صفحه اصلی حذف می‌کند.

"حذف نماد" در صفحه 79

جابجایی نماد: ترتیب نمایش آیکن‌ها را تغییر می‌دهد.

"جابجایی نماد" در صفحه 80

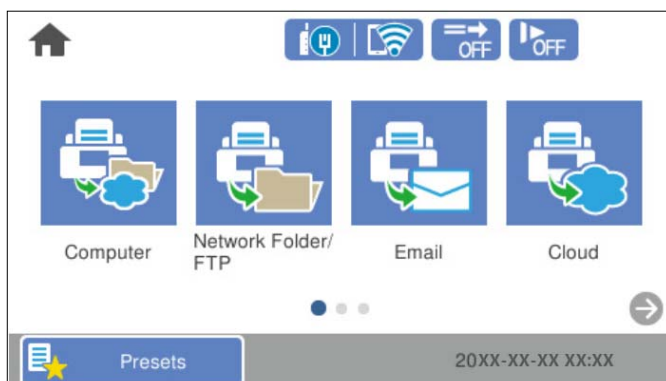
بازیابی نمایشگر نماد پیش فرض: تنظیمات پیش‌فرض نشان داده شده در صفحه اصلی را بازگردانی می‌کند.

کاغذ دیواری: رنگ زمینه صفحه اصلی را تغییر دهید.

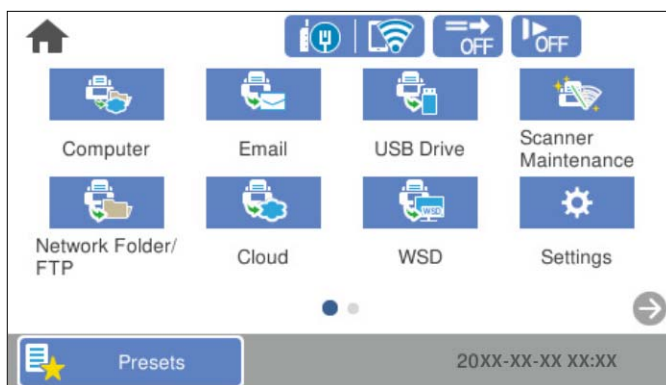
تغییر صفحه‌بندی صفحه اصلی


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

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



ماتریس:

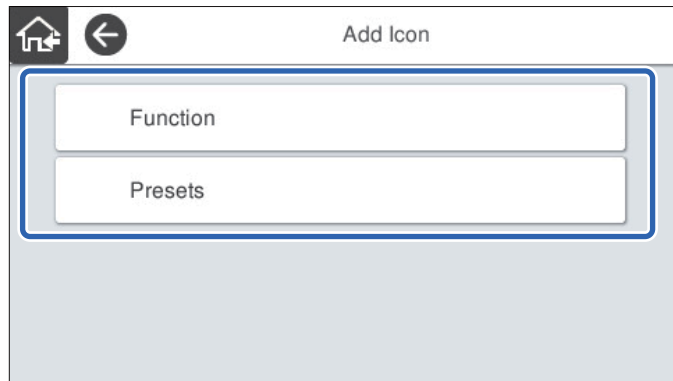


3. برای بازگشت و بررسی صفحه اصلی،  را انتخاب کنید.

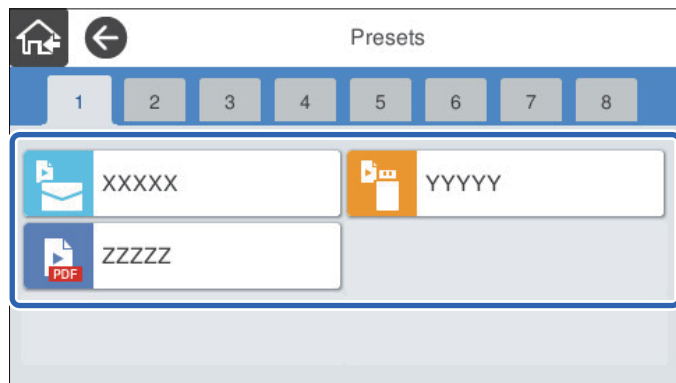
افزودن نماد

1. گزینه تنظیم < ویرایش صفحه اصلی < افزودن نماد را در پانل کنترل اسکرین انتخاب کنید.
 2. گزینه کارکرد یا پیش‌تنظیمات را انتخاب کنید.
- کارکرد: عملکردهای پیش‌فرض نشان داده شده در صفحه اصلی را نشان می‌دهد.

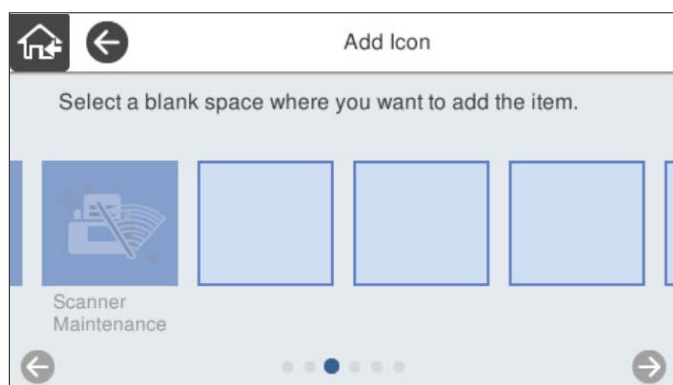
پیش‌تنظیمات: تنظیمات از پیش تنظیم شده را نشان می‌دهد.



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.

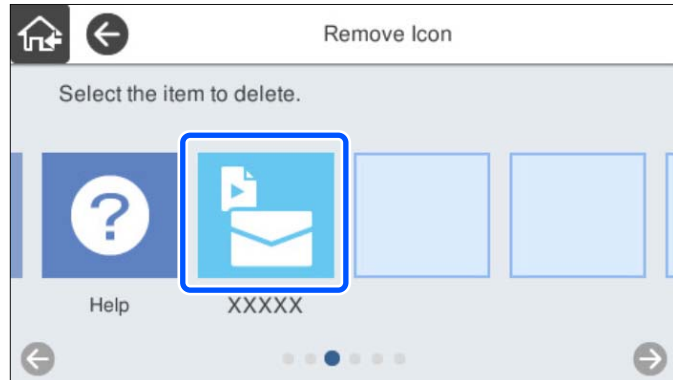


5. برای بازگشت و بررسی صفحه اصلی، گزینه  را انتخاب کنید.

حذف نماد

1. گزینه تنظیم < ویرایش صفحه اصلی < حذف نماد را در پانل کنترل اسکرین انتخاب کنید.

2. آیکن مورد نظر برای حذف را انتخاب کنید.



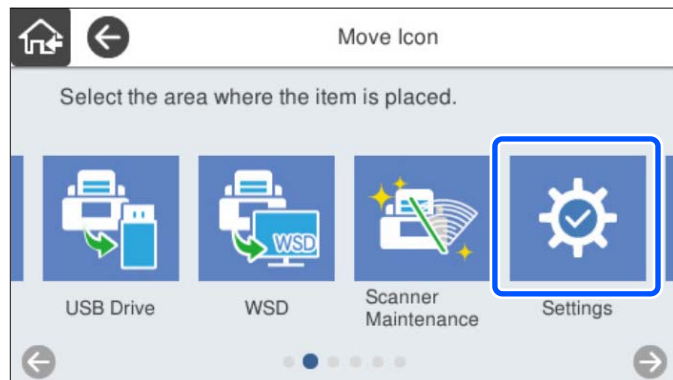
3. برای پایان دادن، گزینه بله را انتخاب کنید.
اگر می‌خواهید چندین آیکن را حذف کنید، مراحل 2 تا 3 را تکرار کنید.

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

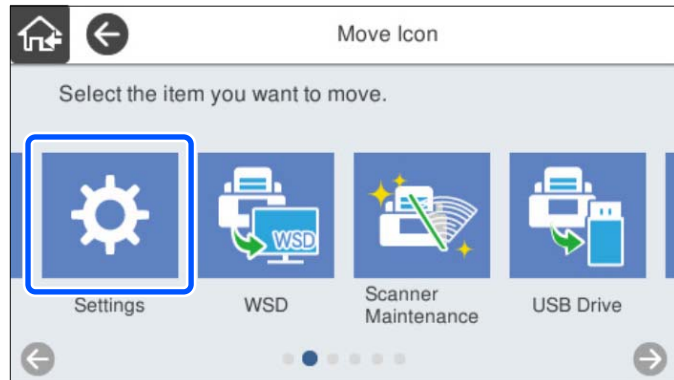
جابجایی نماد


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

83. معرفی امکانات امنیتی محصول.

83. تنظیمات سرپرست سیستم.

89. غیرفعال کردن رابط خارجی.

90. پایش یک اسکنر راه دور.

91. حل کردن مشکلات.

معرفی امکانات امنیتی محصول

این بخش عملکرد امنیتی دستگاه های Epson را شرح می دهد.

نام قابلیت	نوع قابلیت	آنچه باید تنظیم شود	آنچه باید جلوگیری شود
تنظیم 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 اسکتر 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.
راه اندازی 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 اسکتر بدون ورود به شبکه، مانع استفاده غیرمجاز از دستگاه می شود.

اطلاعات مرتبط

◀ "پیکربندی رمز عبور سرپرست" در صفحه 83

◀ "غیرفعال کردن رابط خارجی" در صفحه 89

تنظیمات سرپرست سیستم

پیکربندی رمز عبور سرپرست

وقتی رمز عبور سرپرست را تنظیم کنید، می توانید از تغییر تنظیمات مدیریت سیستم توسط کاربران جلوگیری کنید. مقادیر پیش فرض همزمان با خرید تنظیم می شوند. در صورت نیاز آنها را تغییر دهید.

نکته:

در بخش زیر، مقادیر پیش فرض برای اطلاعات سرپرستی ارائه می شوند.

☐ نام کاربری (مورد استفاده صرفاً برای Web Config): هیچ کدام (خالی)

☐ رمز عبور: شماره سریال اسکتر

شماره سریال را با بررسی برچسب متصل به پشت اسکتر ملاحظه کنید.

رمز عبور سرپرست می توانید از طریق Web Config، پانل کنترل اسکتر یا Epson Device Admin تغییر دهید. هنگام استفاده از Epson Device Admin، راهنمای کاربری یا راهنمای Epson Device Admin را ملاحظه کنید.

تغییر رمز عبور سرپرست با Web Config

رمز عبور سرپرست را در قسمت Web Config تغییر دهید.

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

2. اطلاعات لازم را در کادرهای **Current password**، **User Name**، **New Password** و **Confirm New Password** وارد کنید.

حداقل یک نویسه برای رمز عبور جدید وارد کنید.

نکته:

در بخش زیر، مقادیر پیش فرض برای اطلاعات سرپرستی ارائه می شوند.

نام کاربری: هیچ (خالی)

رمز عبور: شماره سریال اسکتر

شماره سریال را با بررسی برچسب متصل به پشت اسکتر ملاحظه کنید.

مهم!

مطمئن باشید رمز عبور سرپرست را که تنظیم می کنید بخاطر می سپارید. اگر رمز عبور را فراموش کنید، قادر نخواهید بود آن را بازنشانی کنید و نیاز خواهید داشت از پرسنل خدماتی تقاضای کمک کنید.

3. گزینه OK را انتخاب کنید.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

تغییر رمز عبور سرپرست از طریق پانل کنترل

رمز عبور سرپرست را می توانید از طریق پانل کنترل اسکتر تغییر دهید.

1. گزینه تنظیم را در پانل کنترل اسکتر انتخاب کنید.

2. مسیر سرپرست سیستم < تنظیمات سرپرست را انتخاب کنید.

3. مسیر رمز عبور سرپرست < تغییر را انتخاب کنید.

4. رمز عبور فعلی را وارد کنید.

نکته:

تنظیم در زمان خرید (مقدار پیش فرض) برای رمز عبور سرپرست معادل شماره سریال اسکتر است.

شماره سریال را با بررسی برچسب متصل به پشت اسکتر ملاحظه کنید.

5. رمز عبور جدیدتان را وارد کنید.

حداقل یک نویسه وارد کنید.

مهم!

مطمئن باشید رمز عبور سرپرست را که تنظیم می کنید بخاطر می سپارید. اگر رمز عبور را فراموش کنید، قادر نخواهید بود آن را بازنشانی کنید و نیاز خواهید داشت از پرسنل خدماتی تقاضای کمک کنید.

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

یک پیام تکمیل نشان داده می شود.

استفاده از تنظیم قفل برای پانل کنترل


برای قفل کردن پانل کنترل به منظور جلوگیری از تغییر موارد مرتبط با تنظیمات سیستم می‌توانید از گزینه تنظیم قفل استفاده کنید.


نکته:

اگر گزینه *Authentication Settings* در اسکرین را فعال کنید، گزینه تنظیم قفل نیز برای پانل کنترل فعال می‌شود. وقتی گزینه *Authentication Settings* فعال باشد، قفل پانل کنترل را نمی‌توان باز کرد.

حتی اگر *Authentication Settings* را غیرفعال کنید، گزینه تنظیم قفل فعال باقی می‌ماند. اگر در نظر دارید آن را غیرفعال کنید، قادر خواهید بود تنظیمات را از پانل کنترل یا *Web Config* اعمال 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 مرورگر وب" در صفحه 35

موارد تنظیم قفل در منوی تنظیم

این لیست مواردی است که در منوی تنظیم پانل کنترل از طریق گزینه تنظیم قفل قفل شده‌اند.

✓: باید قفل شود.

- : لازم نیست قفل شود.

منوی تنظیم	تنظیم قفل
تنظیمات اصلی	-

تنظیم قفل	منوی تنظیم	
-	روشنایی LCD	
-	صداها	
✓	تایمر خواب	
✓	زمان سنج خاموش کردن	
✓	تاریخ / تنظیمات زمان	
*-/✓	زبان/Language	
-	صفحه کلید (ممکن است بسته به منطقه این ویژگی وجود نداشته باشد).	
✓	وقفه عملیات	
✓	اتصال رایانه از طریق USB	
✓	روشن کردن مستقیم	
-	تنظیمات اسکر	
-	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	
✓	صفحه بندی	
✓	افزودن نماد	
✓	حذف نماد	
✓	جابجایی نماد	
✓	بازیابی نمایشگر نماد پیش فرض	
✓	کاغذ دیواری	
✓	تنظیمات کاربر	


تنظیم قفل	منوی تنظیم	
✓	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	
✓	رمزگذاری رمز عبور	
✓	تحقیق مشتری	
✓	تنظیمات WSD	
✓	بازگرداندن تنظیمات اولیه	
✓	به روز 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	-
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 آیا تغییرات در سرپرست سیستم < محدودیت ها اجازه داده شوند یا خیر.

وارد شدن به عنوان سرپرست از پانل کنترل

هر کدام از روش‌های زیر را می‌توانید برای ورود به سیستم به عنوان سرپرست از طریق پانل کنترل اسکنر استفاده کنید.

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


وقتی گزینه Authentication Settings فعال باشد، آیکن در صفحه خوش آمدید (صفحه آماده بکار تأیید هویت) نمایش داده می‌شود.

وقتی گزینه Authentication Settings غیرفعال باشد، آیکن در صفحه اصلی نمایش داده می‌شود.

2. هنگام نمایش صفحه تأیید، روی گزینه **بله** ضربه بزنید.

3. رمز عبور سرپرست سیستم را وارد نمایید.

پیام تکمیل ورود نمایش داده می‌شود و سپس صفحه اصلی در پانل کنترل نمایش داده می‌شود.

برای خروج، روی گزینه  در گوشه بالا سمت راست صفحه اصلی ضربه بزنید.

غیرفعال کردن رابط خارجی

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

نکته:

تنظیمات محدودیت را می‌توانید 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 **External Interface < Product Security** را انتخاب کنید.

2. گزینه **Disable** را برای عملکردهایی که می‌خواهید تنظیم کنید انتخاب نمایید.

گزینه **Enable** را وقتی انتخاب کنید که در نظر دارید کنترل را لغو نمایید.

اتصال رایانه از طریق **USB**

می‌توانید استفاده از اتصال **USB** کامپیوتر را محدود کنید. اگر می‌خواهید 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 نمی‌باشد.

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 می‌ماند.

:Mac OS

اسکنر را بوسیله یک کابل **USB** به رایانه متصل کنید و سپس تأیید نمایید نمی‌توانید اسکنر را از چاپگرها و اسکنرها اضافه کنید.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

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 اعلان های ایمیلی

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

شما می توانید 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

← "پیکربندی سرور ایمیل" در صفحه 41

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.

محتوای 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 0-9 a-z A-Z ! # \$ % & * ' + . - / = ? ^ _ { | } ~ @ ، 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 مرورگر وب" در صفحه 35

گزینه های مربوط به اعلان ایمیلی

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

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 سرپرستی Web Config ارائه می شوند.

□ نام کاربری: هیچ (خالی)

□ رمز عبور: شماره سریال اسکنر

شماره سریال را با بررسی پرچسب متصل به پشت اسکنر ملاحظه کنید. اگر تنظیمات پیش فرض رمز عبور سرپرست را بازبازی کنید، به مقادیر اولیه بازگردانده می شود.

تنظیمات امنیتی پیشرفته

- 93. تنظیمات امنیتی و پیشگیری از خطر.
- 94. کنترل کردن با پروتکل‌ها.
- 96. استفاده از گواهی دیجیتالی.
- 102. ارتباط SSL/TLS با اسکنز.
- 103. ارتباط رمزگذاری شده با IPsec/فیلترینگ IP.
- 114. اتصال اسکنز به شبکه IEEE802.1X.
- 116. رفع مشکلات مربوط به امنیت 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 بگیریید 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 اسکنر 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 94
- ◀ "ارتباط SSL/TLS با اسکنر" در صفحه 102
- ◀ "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 103
- ◀ "اتصال اسکنر به شبکه IEEE802.1X" در صفحه 114

تنظیمات ویژگی امنیتی

هنگام تنظیم فیلترگذاری IPsec/IP یا IEEE 802.1X، توصیه می شود 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 می کنید.

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 **Protocol < tab Network Security** 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 مرورگر وب" در صفحه 35

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

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

SLP Settings

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

WSD Settings

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

LLTD Settings

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

LLMNR Settings

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

SNMPv1/v2c Settings

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

SNMPv3 Settings

مقدار و توضیحات تنظیم	موارد
زمانی که کادر علامت داشته باشد، SNMPv3 فعال می شود.	Enable SNMPv3
بین 1 تا 32 نویسه با استفاده از نویسه های 1 بیتی وارد کنید.	User Name
Authentication Settings	
یک الگوریتم تأیید هویت برای SNMPv3 انتخاب کنید.	Algorithm
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.	Password
رمز عبوری که برای تأیید پیکربندی کردید را وارد نمایید.	Confirm Password
Encryption Settings	
یک الگوریتم رمزنگاری برای SNMPv3 انتخاب کنید.	Algorithm
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.	Password
رمز عبوری که برای تأیید پیکربندی کردید را وارد نمایید.	Confirm Password
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.	Context Name

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 اسکتر 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 اسکتر 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 اسکتر را تنظیم کنید. در رابطه با اسکتر، تنظیمات را برای تأیید مسیر CA-signed Certificate برای ارتباط SSL/TLS تنظیم کنید. شما می توانید گواهی CA اسکتر 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 اسکتر 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 97
- ◀ "به روزرسانی گواهی خود امضاء" در صفحه 100
- ◀ "پیکربندی یک CA Certificate" در صفحه 101

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 < IPsec/IP Filtering یا Client Certificate < IEEE802.1X را انتخاب کنید.

هر کدام را انتخاب کنید، می توانید 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 می شود.

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 می شود.

5. زبانه **Network Security** را انتخاب کنید. سپس **Certificate < SSL/TLS** یا **Certificate < IPsec/IP Filtering** یا **Client Certificate** یا **Client Certificate < IEEE802.1X** 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 اسکتر ذخیره کنید. زمانی که گواهی را در مقصد ذخیره کنید دریافت *CA-signed Certificate* کامل است.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

گزینه های تنظیم CSR

تنظیمات و توضیحات	موارد
طول کلید را برای یک CSR انتخاب کنید.	Key Length
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 اسکتر: 192.0.2.123، نام اسکتر: EPSONA1B2C3 Common Name: EPSONA1B2C3.local, 192.0.2.123	Common Name
می توانید بین 0 تا 64 نویسه با قالب ASCII ((0x20-0x7E) وارد کنید. می توانید نام های متمایز را با ویرگول جدا کنید.	/Organizational Unit /Organization State/Province /Locality
یک کد کشور دو رقمی که توسط ISO-3166 تعیین شده وارد کنید.	Country
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.	Sender's Email Address

وارد کردن گواهی امضاء شده از طریق CA

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

مهم!

دقت کنید که تاریخ و زمان اسکتر 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 < IPsec/IP Filtering** یا **Client Certificate < IEEE802.1X** یا **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 اسکتر 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 اسکتر 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 مرورگر وب" در صفحه 35

موارد تنظیم وارد کردن گواهی امضاء شده از طریق CA

تنظیمات و توضیحات	موارد
فرمت گواهی را انتخاب کنید. در رابطه با اتصال SSL/TLS، وضعیت Server Certificate نمایش داده می شود. در رابطه با فیلترگذاری IPsec/IP یا IEEE 802.1X، وضعیت Client Certificate نمایش داده می شود.	Client Certificate یا Server Certificate

تنظیمات و توضیحات	موارد
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.	Private Key
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.	Password
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 1
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.	CA Certificate 2

حذف گواهی امضاء شده از طریق CA

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

مهم!

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. 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 **Certificate < SSL/TLS** یا **IPsec/IP Filtering** < Client Certificate یا **Client Certificate < IEEE802.1X** را انتخاب کنید.
2. روی **Delete** کلیک کنید.
3. در پیام نشان داده شده، تایید کنید که می‌خواهید گواهی را حذف کنید.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

به روزرسانی گواهی خود امضاء

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

1. وارد Web Config شوید و زبانه Network Security < tab **Certificate < SSL/TLS** 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 اسکتر: 192.0.2.123، نام اسکتر: EPSONA1B2C3

نام مشترک: EPSONA1B2C3.local ,EPSONA1B2C3 ,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.

اسکتر به روزرسانی می‌شود.

نکته:

اطلاعات گواهی را می‌توانید از طریق زبان **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 مرورگر وب" در صفحه 35

پیکربندی یک CA Certificate

وقتی CA Certificate را تنظیم می‌کنید، می‌توانید اعتبار مسیر گواهی CA سروری که اسکتر به آن دسترسی دارد را ارزیابی کنید. این می‌تواند از جعل هویت جلوگیری کند.

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

وارد کردن CA Certificate

CA Certificate را به اسکتر وارد کنید.

1. وارد Web Config شوید و سپس زبان **CA Certificate < Network Security** را انتخاب کنید.

2. روی **Import** کلیک کنید.

3. CA Certificate که می‌خواهید وارد کنید را مشخص کنید.

4. روی **OK** کلیک کنید.

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

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

حذف یک CA Certificate

می‌توانید CA Certificate وارد شده را حذف کنید.

1. وارد Web Config شوید و سپس زبان **CA Certificate < Network Security** 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 مرورگر وب" در صفحه 35

ارتباط SSL/TLS با اسکتر

اگر گواهی سرور با ارتباط SSL/TLS (لایه سوکت امن/امنیت لایه حمل) با اسکتر 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 اسکتر از قابلیت سرور HTTPS پشتیبانی می‌کند، شما می‌توانید از ارتباط SSL/TLS برای رمزنگاری مکاتبات استفاده کنید. ضمن اطمینان خاطر بابت امنیت، می‌توانید اسکتر 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 **Basic < SSL/TLS < Network Security** 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.

اسکتر به روزرسانی می‌شود.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

پیکربندی گواهی سرور برای اسکتر

1. وارد Web Config شوید و زبانه **Certificate < SSL/TLS < Network Security** را انتخاب کنید.

2. گواهی موردنظر برای استفاده در **Server Certificate** را مشخص کنید.

Self-signed Certificate

یک گواهی خود امضاء از طریق اسکز 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.

اسکز به روزرسانی می شود.

اطلاعات مرتبط

← [اجرای Web Config در مرورگر وب](#) در صفحه 35

← [پیکربندی یک CA-signed Certificate](#) در صفحه 97

← [پیکربندی یک CA Certificate](#) در صفحه 101

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 اسکز 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 پیش فرض

برای فیلتر کردن ترافیک، سیاست پیش فرض را پیکربندی کنید. سیاست پیش فرض برای هر کاربر یا گروه متصل به اسکز 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.

اسکز به روزرسانی می‌شود.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

موارد تنظیم Default 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 اسکتر انتخاب کنید.

IKEv1

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

مورد	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.

مورد	تنظیمات و توضیحات
Local	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 اسکتر را انتخاب کنید.
ID	شناسه اسکتر را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. Distinguished Name : بین 1 تا 255 نویسه 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 ASCII-بایتی (0x20 تا 0x7E) وارد کنید. باید نویسه «@» را نیز در نظر بگیرید. Key ID : بین 1 تا 255 نویسه 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.

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

Encapsulation

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

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

Security Protocol

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

تنظیمات و توضیحات	موارد	
برای اطمینان از یکپارچگی تأیید اعتبار و داده ها، این گزینه را انتخاب کنید و داده ها را رمزنگاری کنید.	ESP	
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.	AH	

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.

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

پیکربندی سیاست گروه

سیاست گروهی یک یا تعداد بیشتری از قوانین است که برای یک کاربر یا یک گروه کاربر اعمال می شود. اسکنر بسته های IP را که با سیاست های پیکربندی شده مطابقت دارند کنترل می کند. بسته های IP به ترتیب یک سیاست گروهی 1 تا 10 سپس یک سیاست پیش فرض تأیید می شوند.

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

موارد تنظیم Group Policy

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

Access Control

یک روش کنترل برای ترافیک بسته های IP پیکربندی کنید.

منابع	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.

منابع	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 اسکتر انتخاب کنید.

IKEv1

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

منابع	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 گردید وارد نمایید.

IKEv2 □

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

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

Encapsulation

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

تنظیمات و توضیحات	موارد
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.	Transport Mode

موارد	تنظیمات و توضیحات
Tunnel Mode	اگر از اسکتر 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 Group Policy در Remote Address(Host) و Local Address (Scanner)

تنظیم Local Address (Scanner)				
Any addresses ^{3*}	IPv6 ²	IPv4		
✓	-	✓	IPv4 ^{1*}	تنظیم Remote Address(Host)
✓	✓	-	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 مرورگر وب" در صفحه 35

مرجع نام سرویس در سیاست گروهی

نکته:

سرویس هایی که موجود نباشند نمایش داده می شوند ولی نمی توانند انتخاب شوند.

نام سرویس	نوع پروتکل	شماره درگاه محلی	شماره درگاه راه دور	ویژگی های کنترل شده
Any	-	-	-	همه سرویس ها
ENPC	UDP	3289	هر درگاه	جستجو برای اسکتر از برنامه هایی مانند Epson Device Admin و یک درایور اسکتر
SNMP	UDP	161	هر درگاه	دستیابی و پیکربندی MIB از برنامه هایی مانند Epson Device Admin و درایور اسکتر
WSD	TCP	هر درگاه	5357	کنترل WSD
WS-Discovery	UDP	3702	هر درگاه	جستجوی اسکترهای WSD
Network Scan	TCP	1865	هر درگاه	باز-ارسال داده های 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 اسکتر
FTP Data (Remote)	TCP	هر درگاه	20	سرویس گیرنده FTP (باز-ارسال داده های اسکن شده) با این حال، این فقط می تواند یک سرور FTP را کنترل کند که از درگاه راه دور شماره 20 استفاده می کند.
FTP Control (Remote)	TCP	هر درگاه	21	سرویس گیرنده FTP (کنترل داده های اسکن شده باز-ارسال شده)
CIFS (Remote)	TCP	هر درگاه	445	سرویس گیرنده CIFS (باز-ارسال داده های اسکن شده به یک پوشه)
NetBIOS Name Service (Remote)	UDP	هر درگاه	137	سرویس گیرنده CIFS (باز-ارسال داده های اسکن شده به یک پوشه)
NetBIOS Datagram Service (Remote)	UDP	هر درگاه	138	
NetBIOS Session Service (Remote)	TCP	هر درگاه	139	

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

پیکربندی نمونه های IPsec/IP Filtering

صرفاً دریافت بسته های IPsec

این نمونه صرفاً برای پیکربندی یک سیاست پیش فرض است.

:Default Policy

Enable :IPsec/IP Filtering

IPsec :Access Control

Pre-Shared Key :Authentication Method

Pre-Shared Key: تا حداکثر 127 نویسه وارد کنید.

Group Policy: پیکربندی نکنید.

دریافت داده های اسکن و تنظیمات اسکن

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

:Default Policy

Enable :IPsec/IP Filtering

Refuse Access :Access Control

:Group Policy

Enable this Group Policy: کادر را علامت بزنید.

Permit Access :Access Control

Remote Address(Host): آدرس IP یک سرویس گیرنده

Service Name :Method of Choosing Port

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 اسکن را به یک آدرس IP خاص می دهد.

:Default Policy

Enable :IPsec/IP Filtering

Refuse Access:Access Control

:Group Policy

Enable this Group Policy: کادر را علامت بزیند.

Permit Access :Access Control

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

نکته:

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

پیکربندی گواهی برای فیلترگذاری IPsec/IP

گواهی سرویس گیرنده 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 می خواهید 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 کرده اید، می توانید 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 مرورگر وب" در صفحه 35

◀ "پیکربندی یک CA-signed Certificate" در صفحه 97

◀ "پیکربندی یک CA Certificate" در صفحه 101

اتصال اسکتر به شبکه IEEE802.1X

پیکربندی شبکه IEEE 802.1X

وقتی IEEE 802.1X را در اسکتر تنظیم می کنید، قادر خواهید بود از آن در شبکه متصل به یک سرور RADIUS، یک سویچ 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 می خواهید از اسکتر 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 می شود.

4. روی **OK** کلیک کنید.

اسکتر به روزرسانی می شود.

اطلاعات مرتبط

← "اجرای Web Config در مرورگر وب" در صفحه 35

گزینه های تنظیم شبکه IEEE 802.1X

تنظیمات و توضیحات	موارد
می توانید تنظیمات صفحه Basic < IEEE802.1X برای IEEE802.1X (LAN) باسیم را فعال یا غیرفعال کنید.	IEEE802.1X (Wired LAN)
وضعیت اتصال IEEE802.1X (Wi-Fi) (Wi-Fi) نشان داده می شود.	IEEE802.1X (Wi-Fi)
روش اتصال شبکه فعلی نشان داده می شود.	Connection Method
گزینه ای برای یک روش تأیید اعتبار بین اسکتر و سرور RADIUS انتخاب کنید.	EAP Type
شما باید یک گواهی امضاء شده توسط CA دریافت و وارد کنید.	EAP-TLS
	PEAP-TLS
شما باید یک رمز عبور پیکربندی کنید.	PEAP/MSCHAPv2
	EAP-TTLS
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.	User ID
برای تأیید اسکتر یک رمز عبور پیکربندی کنید. بین 1 تا 128 نویسه 1-ASCII-بایتی (0x20 تا 0x7E) وارد کنید. اگر از سرور Windows به عنوان سرور RADIUS استفاده می کنید می توانید تا 127 نویسه را وارد کنید.	Password
رمز عبوری که برای تأیید پیکربندی کردید را وارد نمایید.	Confirm Password
می توانید یک شناسه سرور برای تأیید اعتبار با یک سرور RADIUS تعیین شده پیکربندی کنید. تأیید کننده تأیید می کند آیا شناسه سرور در قسمت موضوع/نام دیگر موضوع، گواهی سرور که از سرور RADIUS ارسال می شود قرار دارد یا خیر. بین 0 تا 128 نویسه 1-ASCII-بایتی (0x20 تا 0x7E) وارد کنید.	Server ID
مستقل از روش تأیید اعتبار می توانید تأیید گواهی را تعیین کنید. گواهی را در CA Certificate وارد کنید.	Certificate Validation
اگر PEAP-TLS یا PEAP/MSCHAPv2 را برای EAP Type انتخاب کنید، می توانید یک نام ناشناس به جای شناسه کاربر برای مرحله 1 تأیید اعتبار PEAP پیکربندی کنید. بین 0 تا 128 نویسه 1-ASCII-بایتی (0x20 تا 0x7E) وارد کنید.	Anonymous Name
شما می توانید یکی از موارد زیر را انتخاب کنید.	Encryption Strength
AES256/3DES	High
AES256/3DES/AES128/RC4	Middle

پیکربندی گواهی برای IEEE 802.1X

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

1. وارد Web Config شوید و زبانه **Client Certificate < IEEE802.1X < Network Security** 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 مرورگر وب" در صفحه 35

رفع مشکلات مربوط به امنیت پیشرفته

بازگرداندن تنظیمات امنیتی

اگر می‌خواهید محیطی بسیار امن مانند IPsec/IP Filtering ایجاد کنید، تنظیمات نادرست یا بروز مشکل در دستگاه یا سرور ممکن است مانع ایجاد ارتباط با دستگاه‌ها 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 غیرفعال کنید.

1. وارد Web Config شوید و زبانه **Basic < IPsec/IP Filtering < Network Security** 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 **Default Policy < Basic < IPsec/IP Filtering < Network Security** 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 مرورگر وب" در صفحه 35

◀ "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 103

می توانید با IPsec Communication ارتباط برقرار کنید

الگوریتمی که اسکنر یا رایانه پشتیبانی می 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-128 ,AES-CBC-192 ,AES-CBC-256 ,AES-GCM-128 ,AES-GCM-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 ,DH Group16 ,DH Group17 ,DH Group18 ,DH Group19 ,DH Group20 ,DH ,DH Group21 ,DH Group22 ,DH Group23 ,DH Group24 ,DH ,DH Group25 ,DH Group26 ,DH Group27 ,DH Group28 ,DH Group29 ,DH Group30 *
الگوریتم رمزگذاری ESP	AES-128 ,AES-CBC-192 ,AES-CBC-256 ,AES-GCM-128 ,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 103

می تواند به طور ناگهانی ارتباط برقرار کند

آدرس IP اسکنر تغییر یافته یا قابل استفاده می 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 می 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 مرورگر وب" در صفحه 35
- ◀ "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 103

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 103

بعد از پیکربندی IEEE 802.1X نمی‌توانید به اسکنر دسترسی داشته باشید

تنظیمات IEEE 802.1X نادرست می‌باشند.

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.

اسکنر و رایانه را وصل کنید و سپس دوباره IEEE 802.1X را پیکربندی کنید.

اطلاعات مرتبط

- ◀ "پیکربندی شبکه IEEE 802.1X" در صفحه 114

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 98

می 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 100

می 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 97

هشدار مربوط به یک گواهی دیجیتالی ظاهر می‌شود

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

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

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.	<p>علت: تاریخ گواهی گذشته است.</p> <p>باید چه کاری انجام داد:</p> <p><input type="checkbox"/> اگر تاریخ گواهی گذشته است، گواهی جدیدی دریافت و وارد کنید.</p> <p><input type="checkbox"/> اگر گواهی تاریخ گذشته نیست، دقت کنید تاریخ و زمان اسکنر به درستی تنظیم شده باشند.</p>
Private key is required.	<p>علت: کلید خصوصی جفت شده ای با گواهی وجود ندارد.</p> <p>باید چه کاری انجام داد:</p> <p><input type="checkbox"/> 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.</p> <p><input type="checkbox"/> 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.</p>
Setup failed.	<p>علت: گواهی PEM/DER دریافت شده از طریق CSR و با استفاده از Web Config را دوباره وارد کرده اید.</p> <p>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.</p>
Setup failed.	<p>علت: می توانید پیکربندی را تمام کنید زیرا ارتباط بین اسکنر و رایانه برقرار نشده است یا به دلیل خطاهایی، فایل قابل خواندن نیست.</p> <p>باید چه کاری انجام داد: بعد از بررسی فایل مشخص شده و ارتباط، دوباره فایل را وارد کنید.</p>

اطلاعات مرتبط

◀ "دوباره گواهی دیجیتالی" در صفحه 96

حذف گواهی امضاء شده از طریق CA به اشتباه

هیچ فایل پشتیبان برای گواهی امضاء 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، نمی توانید گواهی حذف شده را دوباره وارد کنید. یک CSR ایجاد کنید و گواهی جدیدی دریافت کنید.

اطلاعات مرتبط

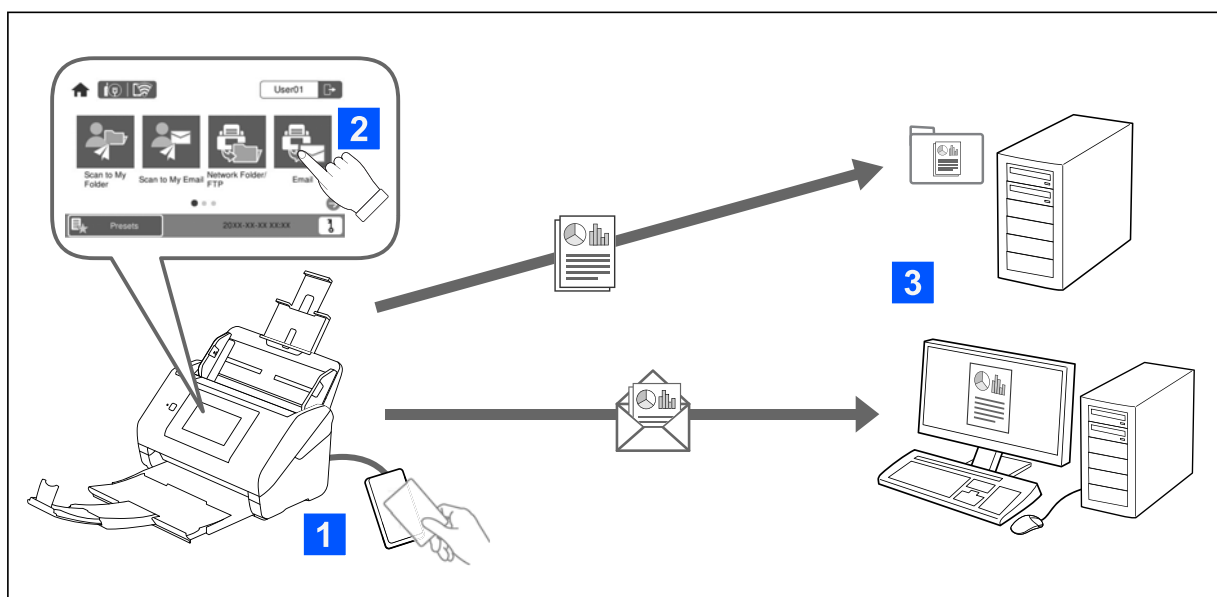
◀ "وارد کردن گواهی امضاء شده از طریق CA" در صفحه 98

◀ "حذف گواهی امضاء شده از طریق CA" در صفحه 100

Authentication Settings

- 123 Authentication Settings درباره
- 124 Authentication Method درباره
- 125 نرم افزار برای راه اندازی.
- 126 بروزرسانی ثابت افزار اسکتر.
- 126 وصل کردن و پیکربندی یک دستگاه تأیید هویت.
- 130 ثبت و تنظیم اطلاعات.
- 146 Job History گزارش های با استفاده از Epson Device Admin.
- 147 وارد شدن به عنوان سرپرست از پانل کنترل.
- 147 Authentication Settings کردن غیرفعال
- 148 حذف اطلاعات Authentication Settings (بازگرداندن تنظیمات اولیه).
- 148 حل کردن مشکلات.

درباره Authentication Settings



وقتی Authentication Settings فعال باشد، تأیید هویت کاربر برای شروع اسکن کردن ضروری می‌باشد. روش‌های اسکن قابل استفاده توسط هر کاربر را می‌توانید تنظیم کنید و از عملیات‌های تصادفی جلوگیری کنید.

آدرس ایمیل کاربر تأیید هویت شده را می‌توانید به عنوان مقصد اسکن انتخاب کنید (Scan to My Email). یا داده‌های هر کاربر را در یک پوشه شخصی ذخیره کنید (Scan to My Folder). سایر روش‌های اسکن را نیز می‌توانید تخصیص دهید.

نکته:

وقتی گزینه Authentication Settings فعال باشد می‌توانید از طریق یک رایانه یا دستگاه هوشمند اسکن را انجام دهید.

علاوه بر Authentication Settings معرفی شده در این دفترچه راهنما، با استفاده از یک سرور تأیید هویت نیز می‌توانید یک سیستم احراز هویت ایجاد نمایید. برای ایجاد این سیستم، از قابلیت Authentication Edition (با نام اختصاری Document Capture Pro Server AE) استفاده کنید. برای کسب اطلاعات بیشتر با دفتر Epson در محل خود تماس بگیرید.

عملکردهای موجود برای Authentication Settings

Authentication Settings		عملکرد اسکن کردن در پانل کنترل
هنگام غیرفعال بودن	هنگام فعال بودن	
-	✓	اسکن و ارسال به پوشه من تصاویر را در پوشه تخصیص یافته به کاربر تأیید هویت شده ذخیره می‌کند.
-	✓	اسکن و ارسال به ایمیل من تصاویر را به پوشه تخصیص یافته به کاربر تأیید هویت شده ارسال می‌کند.
✓	✓	اسکن در پوشه شبکه/FTP تصاویر را در یک پوشه در شبکه ذخیره می‌کند.

Authentication Settings		عملکرد اسکن کردن در پانل کنترل
هنگام غیرفعال بودن	هنگام فعال بودن	
✓	*✓	ذخیره اسکن در رایانه با استفاده از کارهای ایجاد شده در بخش Document Capture Pro (Windows)/Document Capture (Mac OS)) تصاویر را در یک رایانه متصل شده ذخیره می‌کند. * وقتی Authentication Settings فعال باشد، تنها می‌توانید از کارهای ثبت شده در بخش پیش‌تنظیمات استفاده کنید.
✓	✓	اسکن در ایمیل تصاویر را به آدرس ایمیلی که تنظیم کرده‌اید ارسال می‌کند.
✓	✓	ذخیره اسکن در فضای ابری تصاویر را به سرویس ابری که تنظیم کرده‌اید ارسال می‌کند.
✓	✓	اسکن و ارسال به درایو USB تصاویر را در یک درایو USB متصل به اسکنر ذخیره می‌کند. این تنها زمانی در دسترس است که هیچ دستگاه تأیید هویتی به اسکنر متصل نباشد.
✓	-	اسکن در WSD تصاویر را در یک رایانه متصل شده از طریق ویژگی WSD ذخیره می‌کند.
✓	✓	پیش‌تنظیمات می‌توانید تا 48 عملکرد اسکن پیش‌تنظیم را ثبت کنید. می‌توانید تا حداکثر پنج مورد پیش‌تنظیمات برای کاربران ثبت شده در Local DB تخصیص دهید. موارد پیش‌تنظیمات تخصیص یافته تنها برای کاربر مذکور در دسترس خواهند بود. موارد پیش‌تنظیمات که به هیچ کاربری تخصیص نیافته‌اند، برای همه کاربران قابل استفاده خواهند بود.

درباره Authentication Method

این اسکنر می‌تواند تأیید هویت را از طریق روش‌های زیر و بدون نیاز به ایجاد یک سرور تأیید هویت ارائه دهد.

Local DB and LDAP	LDAP	Local DB	
<p>حافظه اسکنر و سرور LDAP</p> <p>ابتدا اطلاعات کاربر ثبت شده در اسکنر (1) را بررسی کنید و سپس در صورتی که مورد مطابقت وجود نداشته باشد، اطلاعات کاربر را در مقابل سرور (2) LDAP بررسی کنید.</p>	<p>سرور LDAP*</p> <p>این روش تأیید هویت، اطلاعات کاربر سرور LDAP همگام شده با اسکنر را بررسی می کند. از آنجا که امکان ذخیره موقتی تا حداکثر 300 مورد اطلاعات کاربری از سرور LDAP به صورت حافظه نهان در اسکنر وجود دارد، در صورت از کار افتادن سرور LDAP، تأیید هویت را می توان با استفاده از حافظه نهان وجود خواهد داشت.</p> <p>* سروری که سرویس دایرکتوری با قابلیت ارتباط با LDAP را فراهم می کند.</p>	<p>حافظه اسکنر</p> <p>این روش تأیید هویت، اطلاعات کاربر ثبت شده در اسکنر را بررسی و با کاربری که از عملکرد اسکن استفاده می کند، مقایسه می کند.</p>	محل اطلاعات کاربر
			
<p>50 (حافظه اسکنر) نامحدود (سرور LDAP)</p>	<p>نامحدود (سرور LDAP)</p>	<p>50 (حافظه اسکنر)</p>	تعداد کاربران ثبت شده
<p>حداکثر 300 (50 شیار حافظه نهان با User Settings در Local DB به اشتراک گذاشته می شوند)</p>	<p>300</p>	<p>-</p>	حافظه نهان اسکنر
<p>شما می توانید هر کدام از روش های زیر را استفاده کنید.</p> <p><input type="checkbox"/> یک کارت تأیید هویت ارائه دهید یا User ID و Password را وارد کنید</p> <p><input type="checkbox"/> یک کارت تأیید هویت ارائه دهید یا ID Number را وارد کنید</p> <p><input type="checkbox"/> User ID و Password را وارد کنید</p> <p><input type="checkbox"/> یک User ID وارد کنید</p> <p><input type="checkbox"/> یک ID Number وارد کنید</p>			روش های ورود
<p>کاربران Local DB: تنظیم به صورت مجزا کاربران LDAP: تنظیمات یکسان برای همه کاربران</p>	<p>تنظیمات یکسان برای همه کاربران LDAP</p>	<p>تنظیم به صورت مجزا برای هر کاربر</p>	محدودیت های ویژگی «اسکن به»
<p>کاربران Local DB: تا حداکثر 5 مورد به ازای هر کاربر کاربران LDAP: -</p>	<p>- (تنظیم مجزا ممکن نیست)</p>	<p>تا حداکثر 5 مورد به ازای هر کاربر</p>	تخصیص موارد پیش تنظیمات به همه کاربران

نرم افزار برای راه اندازی

با استفاده از Web Config یا Epson Device Admin راه اندازی کنید.

□ هنگام استفاده از Web Config، اسکنر را تنها می‌توانید از طریق یک مرورگر وب راه‌اندازی کنید.
["Web Config" در صفحه 35](#)

□ هنگام استفاده از Epson Device Admin، چندین اسکنر را می‌توانید یک جا از طریق یک الگوی پیکربندی راه‌اندازی کنید.
["Epson Device Admin" در صفحه 36](#)

بروزرسانی ثابت‌افزار اسکنر

قبل از فعال‌سازی Authentication Settings، ثابت‌افزار اسکنر را به تازه‌ترین نسخه بروزرسانی کنید. اسکنر را از قبل به اینترنت وصل کنید.



در حین بروزرسانی، رایانه یا اسکنر را خاموش نکنید.

هنگام تنظیم از Web Config:

مسیر زبانه **Firmware Update < Device Management** را انتخاب کنید و سپس برای بروزرسانی ثابت‌افزار، دستورالعمل‌های روی صفحه را دنبال کنید.

هنگام تنظیم از Epson Device Admin:

مسیر **Home < Firmware < Update** را در صفحه لیست دستگاه‌ها انتخاب کنید و سپس برای بروزرسانی ثابت‌افزار، دستورالعمل‌های روی صفحه را دنبال کنید.

نکته:

اگر تازه‌ترین ثابت‌افزار از قبل نصب است، نیازی نیست بروزرسانی کنید.

وصل کردن و پیکربندی یک دستگاه تأیید هویت

اگر در نظر دارید یک دستگاه تأیید هویت مانند یک کارت‌خوان IC را وصل و استفاده کنید، لازم است ابتدا دستگاه را پیکربندی نمایید. در صورتی که از یک دستگاه تأیید هویت استفاده می‌کنید، این ضرورت ندارد.

اطلاعات مرتبط

◀ "وصل کردن دستگاه تأیید هویت" در صفحه 129

◀ "تنظیمات دستگاه تأیید هویت" در صفحه 130

لیست کارت‌خوان‌های سازگار

همه عملیات‌ها برای کارت‌خوان‌های درج شده در لیست تضمین نمی‌شوند.

بلی: تحت پشتیبانی (خوانش اطلاعات شناسایی با تنظیمات استاندارد کارت‌خوان مقدور می‌باشد).

خیر: سازگار نیست

حالت	کارت تأیید هویت							شماره مدل	مدل	تولید کننده
	IEC/ISO14443 (TypeB) Compliance	FeliCa™		MIFARE		DMZ	HID Global			
		Lite/Lite-S	Standard	Ultralight	Classic	EM4002	iClass			
صفحه کلید د	خیر	خیر	خیر	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	بلی	RDR-80081AKU	pcProx Plus	RF IDEAS
صفحه کلید د	خیر	خیر	خیر	بلی	بلی	خیر	بلی ^{1*}	RDR-7081BKU	pcProx	RF IDEAS
صفحه کلید د	خیر	خیر	خیر	بلی ^{1*}	بلی ^{1*}	خیر	بلی	RDR-7581AKU	pcProx	RF IDEAS
صفحه کلید د	خیر	خیر	خیر	بلی	بلی	خیر	خیر	T3DT-MB2BEL T3DT-MB2WEL	TWN3 MIFARE	ELATE C
صفحه کلید د	بلی	بلی	بلی	بلی	بلی	خیر	بلی	T3DT-FB2BEL T3DT-FB2WEL	TWN3 MIFARE NFC	ELATE C
صفحه کلید د	بلی	بلی	بلی	بلی	بلی	بلی	بلی	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	TWN4 MULTITECH	ELATE C
صفحه کلید د	بلی	بلی	بلی	بلی	بلی	بلی	بلی	T4LK-FB4BLZ-PI	TWN4 MultiTech 2 BLE-PI	ELATE C
صفحه کلید د	بلی	بلی	بلی	بلی	بلی	بلی	بلی	T4QC-FC3B7	TWN4 Slim	ELATE C
صفحه کلید د ^{1*}	بلی	خیر	بلی	بلی	بلی	بلی	بلی	OMNI KEY5427CK OMNI KEY5427CK gen2	OMNI KEY 5427	HID Global
PC/SC	بلی ^{2*}	خیر	بلی	بلی ^{2*}	بلی ^{2*}	خیر	خیر	ACR122U	ACR122U	ACS

حالت	کارت تأیید هویت							شماره مدل	مدل	تولید کننده
	IEC/ISO14443 (TypeB) Compliance	FeliCa™		MIFARE		DMZ	HID Global			
		Lite/Lite-S	Standard	Ultralight	Classic	EM4002	iClass			
PC/SC	بلی ^{2*}	بلی	بلی	بلی ^{2*}	بلی ^{2*}	خیر	خیر	ACR1252	ACR1252	ACS
PaSoRi	بلی ^{2*}	بلی ^{2*}	بلی ^{2*}	بلی ^{2*}	بلی ^{2*}	خیر	خیر	RC-S330/S	PaSoRi	Sony
PaSoRi	بلی ^{2*}	بلی ^{2*}	بلی ^{2*}	بلی ^{2*}	بلی ^{2*}	خیر	خیر	RC-S380/P RC-S380/S	PaSoRi	Sony
صفحه کلید _د	بلی	بلی	بلی	بلی	بلی	بلی	بلی	DMZ008	Leitor RFID Universal	DMZ
صفحه کلید _د	خیر	خیر	خیر	خیر	خیر	بلی	خیر	DMZ087	Leitor RFID Multi-125	DMZ
صفحه کلید _د	خیر	خیر	خیر	بلی	بلی	خیر	خیر	DMZ088	Leitor RFID Mifare	DMZ
صفحه کلید _د	خیر	خیر	خیر	خیر	خیر	بلی	خیر	DMZ073	Biometric & RFID Reader	DMZ
صفحه کلید _د	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	SCR708	SCR708	inepro
صفحه کلید _د	بلی	بلی	بلی	بلی	بلی	بلی	بلی	MU0388	YU03088 001	Y Soft
صفحه کلید _د	بلی	خیر	خیر	بلی	بلی	خیر	خیر	ZTCM3-MIFARE	TCM3 Cartadis MiFare Card Reader	Cartadis
صفحه کلید _د	بلی	خیر	خیر	بلی	بلی	خیر	خیر	mCR-600	EM & Mifare Card Reader	MICI Network Co., Ltd.
صفحه کلید _د	بلی	بلی	بلی	بلی	بلی	بلی	بلی	T4DT-FB4WU-F-PI	MiCard MultiTech4-PI	NT-ware

حالت	کارت تأیید هویت							شماره مدل	مدل	تولید کننده
	IEC/ISO14443 (TypeB) Compliance	FeliCa™		MIFARE		DMZ	HID Global			
		Lite/Lite-S	Standard	Ultralight	Classic	EM4002	iClass			
صفحه کلید ۱	خیر	خیر	خیر	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	بلی ^{1*}	RDR-80081AGU-NT2-20	MiCard Plus-2-V2	NT-ware
صفحه کلید ۱	خیر	بلی	بلی	بلی	بلی	بلی	بلی	MiCard V3 Multi	MiCard V3 Multi	NT-ware

1* شما باید تنظیمات کارت خوان را با استفاده از نرم افزار تحت مالکیت ارائه شده توسط سازنده کارت خوان تغییر دهید.

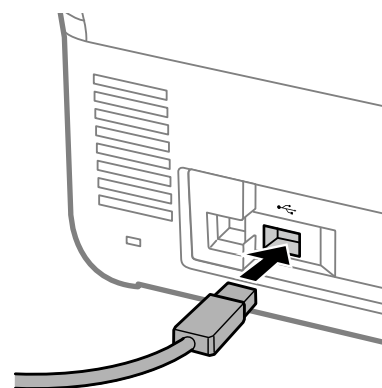
2* اگر نیاز دارید از داده های موجود در یک ناحیه خاص کارت غیر از شناسه استاندارد کارت به عنوان شناسه تأیید هویت از طریق پیکربندی تنظیمات محصول استفاده کنید، لطفاً جهت دریافت اطلاعات بیشتر درباره روش راه اندازی محصول با شریک Epson یا نماینده محلی تماس بگیرید.

وصل کردن دستگاه تأیید هویت



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

کابل USB کارت خوان را به درگاه USB رابط خارجی اسکنر وصل کنید.



بررسی عملیات برای دستگاه تأیید هویت

از طریق پانل کنترل اسکنر می توانید 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 می شوند.

تنظیمات دستگاه تأیید هویت

قالب خوانش اطلاعات تأیید هویت دریافتی از یک کارت تأیید هویت را تنظیم کنید.

شما می‌توانید روش خوانش زیر را برای دستگاه تأیید هویت تنظیم کنید.

خواندن ناحیه خاص کارت تأیید هویت مانند کد اشتغال یا شناسه شخصی.

استفاده از اطلاعات کارت تأیید هویت بجز UID (اطلاعات کارت تأیید هویت مانند شماره سریال).

از یک ابزار نیز می‌توانید برای ایجاد پارامترهای عملیاتی استفاده کنید. جزئیات مربوطه را از نماینده فروش جویا شوید.

نکته:

استفاده از کارت‌های تأیید هویت تولید شرکت‌های مختلف:

هنگام استفاده از اطلاعات کارت UID (اطلاعات کارت شناسایی مانند شماره سریال) می‌توانید ترکیبی از انواع مختلف کارت‌های تأیید هویت را استفاده نمایید. هنگام استفاده از اطلاعات کارت دیگر امکان استفاده ترکیبی را نخواهید داشت.

هنگام تنظیم از Web Config:

زبان **Card Reader < Device Management** را انتخاب کنید.

هنگام تنظیم از Epson Device Admin:

مسیر **Card Reader < Authentication Settings < Administrator Settings** را از الگوی پیکربندی انتخاب کنید.

مورد	توضیحات
Vendor ID	شناسه فروشنده دستگاه تأیید هویت با لزوم رعایت محدودیت 0000 تا FFFF را با استفاده 4 نویسه الفبایی عددی تنظیم نمایید. اگر مایل به تعیین محدودیت نیستید، عدد 0000 را وارد کنید.
Product ID	شناسه محصول دستگاه تأیید هویت با لزوم رعایت محدودیت 0000 تا FFFF را با استفاده 4 نویسه الفبایی عددی تنظیم نمایید. اگر مایل به تعیین محدودیت نیستید، عدد 0000 را وارد کنید.
Operational parameter	پارامتر عملیات دستگاه تأیید هویت را بین 0 تا 8192 نویسه وارد کنید. A~Z، a~z، 9~0، +، /، =، فاصله و فید خط قابل استفاده هستند.
Card Reader	قالب تبدیل مربوط به دستگاه تأیید هویت را انتخاب کنید. جزئیات قالب را می‌توانید بررسی کنید. پیوند ارائه شده در توضیحات مورد را ملاحظه نمایید.
Authentication Card ID save format	قالب تبدیل مربوط به اطلاعات تأیید هویت یک کارت شناسایی را انتخاب کنید. جزئیات قالب را می‌توانید بررسی کنید. پیوند ارائه شده در توضیحات مورد را ملاحظه نمایید.
Set card ID range	مشخصات موقعیت خوانش را فعال کنید.
Text Start Position	موقعیت شروع متن برای خوانش اطلاعات شناسایی را مشخص کنید. می‌توانید مقداری بین 1 تا 4096 تعیین کنید.
Number of Characters	تعداد نویسه‌های مورد نظر برای خوانش از موقعیت شروع اطلاعات شناسایی را مشخص کنید. می‌توانید مقداری بین 1 تا 4096 تعیین کنید.

ثبت و تنظیم اطلاعات

راه‌اندازی

تنظیمات لازم را بسته به Authentication Method و روش اسکن مورد استفاده خود اعمال کنید.



مهم:

قبل از راه‌اندازی تنظیمات، بررسی کنید تنظیم زمان برای اسکتر درست است.

در صورتی که تنظیم زمان نادرست باشد، پیام خطای «مجاز منقضی شده است» نمایش داده می‌شود که ممکن است منجر به ایراد در راه‌اندازی اسکتر شود. همچنین، به منظور استفاده از یک عملکرد امنیتی مانند ارتباطات SSL/TLS یا IPsec، لازم است زمان صحیح تنظیم شود. زمان را می‌توانید به روش زیر تنظیم کنید.

Web Config: **Date and Time < Date and Time < Device Management**

پانل کنترل اسکتر: **تنظیم < تنظیمات اصلی < تاریخ / تنظیمات زمان.**

تنظیمات	Local DB	LDAP	Local DB and LDAP
فعال‌سازی تأیید هویت قبل از اعمال تنظیمات تأیید هویت لازم است تأیید هویت را فعال نمایید. "فعال‌سازی تأیید هویت" در صفحه 131	✓	✓	✓
Authentication Settings تنظیم Authentication Method و نحوه تأیید هویت هر کاربر. "Authentication Settings" در صفحه 132	✓	✓	✓
ثبت کردن User Settings ثبت کردن تنظیمات برای هر کاربر. همچنین می‌توانید کاربران را به صورت دسته‌ای با استفاده از یک فایل CSV ثبت کنید. "ثبت کردن User Settings" در صفحه 133	✓	-	✓
همگام‌سازی با LDAP Server اعمال تنظیمات همگام‌سازی سرور LDAP. "همگام‌سازی با LDAP Server" در صفحه 140	-	✓	✓
تنظیم کردن Email Server تعیین تنظیمات سرور ایمیل. هنگام استفاده از عملکردهایی که به تنظیمات سرور ایمیل از قبیل Scan to My Email نیاز دارند، این را تعیین کنید. "تنظیم سرور ایمیل" در صفحه 143	✓	✓	✓
تنظیم Scan to My Folder تنظیم پوشه‌های مقصد. هنگام استفاده از عملکرد Scan to My Folder این را تعیین کنید. "تنظیم Scan to My Folder" در صفحه 144	✓	✓	✓
Customize One-touch Functions هنگام تغییر موارد نمایش یافته در پانل کنترل اسکتر این گزینه را تعیین کنید. تنها می‌توانید آیکن‌هایی را که در پانل کنترل نیاز دارید نمایش دهید یا ترتیب آیکن‌ها را تغییر دهید. "Customize One-touch Functions" در صفحه 146	✓	✓	✓

فعال‌سازی تأیید هویت

قبل از اعمال تنظیمات تأیید هویت لازم است تأیید هویت را فعال نمایید.

هنگام تنظیم از Web Config:

گزینه روشن (دستگاه/سرور LDAP) را از زبانه Authentication < Basic < Product Security انتخاب کنید.

هنگام تنظیم از Epson Device Admin:

در الگوی پیکربندی، گزینه روشن (دستگاه/سرور LDAP) را از مسیر Authentication Settings < Administrator Settings < Basic انتخاب کنید.

نکته:

اگر گزینه Authentication Settings در اسکنر را فعال کنید، گزینه تنظیم قفل نیز برای پانل کنترل فعال می‌شود. وقتی گزینه Authentication Settings فعال باشد، قفل پانل کنترل را نمی‌توان باز کرد.

حتی اگر Authentication Settings را غیرفعال کنید، گزینه تنظیم قفل فعال باقی می‌ماند. اگر در نظر دارید آن را غیرفعال کنید، قادر خواهید بود تنظیمات را از پانل کنترل یا Web Config اعمال کنید.

اطلاعات مرتبط

◀ "تنظیم تنظیم قفل از پانل کنترل" در صفحه 85

◀ "تنظیم تنظیم قفل از طریق Web Config" در صفحه 85

Authentication Settings

تنظیم Authentication Method و نحوه تأیید هویت هر کاربر.

هنگام تنظیم از Web Config:

زبانه Authentication Settings < Product Security را انتخاب کنید.

هنگام تنظیم از Epson Device Admin:

مسیر Authentication Settings < Authentication Settings < Administrator Settings را از الگوی پیکربندی انتخاب کنید.

مورد	توضیحات
Authentication Method	<p>مسیر Authentication Method را انتخاب کنید.</p> <p>Local DB <input type="checkbox"/></p> <p>با استفاده از User Settings ثبت شده در اسکنر تأیید هویت کنید. ضروری است کاربر را در اسکنر ثبت کنید.</p> <p>LDAP <input type="checkbox"/></p> <p>با استفاده از اطلاعات کاربر در سرور LDAP همگام شده با اسکنر تأیید هویت را انجام دهید. قبل از هر چیز باید تنظیمات سرور LDAP را پیکربندی کنید.</p> <p>Local DB and LDAP <input type="checkbox"/></p> <p>با استفاده از اطلاعات کاربر ثبت شده در اسکنر یا در سرور LDAP همگام شده با اسکنر تأیید هویت را انجام دهید. شما باید کاربر را در اسکنر ثبت کنید یا سرور LDAP را تنظیم کنید.</p>

مورد	توضیحات
How to Authenticate User	<p>نحوه تأیید هویت کاربر را انتخاب کنید.</p> <p><input type="checkbox"/> Card or User ID and Password</p> <p>از یک کارت تأیید هویت برای تأیید هویت کاربران استفاده کنید. از یک شناسه کاربری و رمز عبور نیز می‌توانید برای تأیید هویت کاربران استفاده کنید.</p> <p><input type="checkbox"/> User ID and Password</p> <p>از یک شناسه کاربری و رمز عبور برای تأیید هویت کاربران استفاده کنید.</p> <p>در صورت انتخاب این عملکرد، از یک کارت تأیید هویت نمی‌توانید برای تأیید هویت استفاده کنید.</p> <p><input type="checkbox"/> User ID</p> <p>تنها از یک شناسه کاربری برای تأیید هویت کاربران استفاده کنید. نیازی به تنظیم رمز عبور نیست.</p> <p><input type="checkbox"/> Card or ID Number</p> <p>از یک کارت تأیید هویت برای تأیید هویت کاربران استفاده کنید. از یک ID Number نیز می‌توانید استفاده کنید.</p> <p><input type="checkbox"/> ID Number</p> <p>تنها از یک شناسه کاربری برای تأیید هویت کاربران استفاده کنید.</p>
Allow users to register authentication cards	<p>اگر به کاربران اجازه می‌دهید کارت تأیید هویت را در سیستم ثبت کنند، این گزینه را فعال کنید.</p> <p>اگر LDAP را برای Authentication Method انتخاب کنید، نمی‌توانید آن را تنظیم کنید.</p> <p>جهت کسب اطلاعات بیشتر درباره اینکه چگونه کاربران می‌توانند کارت‌های تأیید هویت خود را ثبت کنند، بخش «ثبت کردن یک کارت تأیید هویت» در راهنمای کاربر را ملاحظه کنید.</p>
The Minimum Digit Number of ID Number	<p>حداقل تعداد رقم‌های لازم برای شماره شناسه را انتخاب کنید.</p>
Caching for LDAP authenticated users	<p>هنگام استفاده از تأیید هویت سرور LDAP، می‌توانید تنظیم کنید از حافظه نهان برای اطلاعات کاربر استفاده شود.</p>
Use user information in SMTP authentication	<p>هنگام استفاده از شناسه کاربری و رمز عبور برای تأیید هویت می‌توانید تنظیم کنید آیا از اطلاعات کاربر برای تأیید هویت SMTP استفاده شود یا خیر. سیستم از آخرین شناسه کاربری و رمز عبور که با آن وارد شده‌اید استفاده می‌کند.</p>
Restrictions for LDAP authenticated users	<p>اگر از LDAP استفاده کنید، قادر خواهید بود عملکردهای در دسترس برای کاربر را تنظیم کنید.</p>

ثبت کردن User Settings

User Settings استفاده شده برای تأیید هویت کاربر را ثبت کنید. شما می‌توانید از طریق هر کدام از روش‌های زیر ثبت کنید.

ثبت کردن User Settings به صورت مورد به مورد (Web Config)

ثبت کردن چندین User Settings به صورت دسته‌ای با استفاده از یک فایل (CSV (Web Config)

ثبت کردن User Settings در چندین اسکنر به صورت یک دسته از طریق یک الگوی پیکربندی (Epson Device Admin)

اطلاعات مرتبط

← "ثبت کردن User Settings به صورت جداگانه (Web Config)" در صفحه 134

← "ثبت کردن چندین User Settings با استفاده از یک فایل (CSV (Web Config)" در صفحه 135

← "ثبت کردن User Settings در چندین اسکنر به صورت یک دسته (Epson Device Admin)" در صفحه 137

ثبت کردن User Settings به صورت جداگانه (Web Config)

به Web Config وارد شوید و زبانه **Add < User Settings < Product Security** و سپس User Settings را وارد کنید.

مورد	توضیحات
User ID	شناسه کاربری را که در نظر دارید برای تأیید هویت در محدوده 1 تا 83 بایت قابل بیان در Unicode (UTF-8)) استفاده کنید وارد نمایید. از آنجا که شناسه کاربری به بزرگی حروف حساس نیست، می‌توانید با استفاده از حروف بزرگ یا کوچک وارد شوید.
User name Display	نام کاربری نمایش یافته در پانل کنترل اسکتر را با بازه طولی 32 نویسه قابل بیان در قالب Unicode (UTF-16)) وارد کنید. اینجا را می‌توانید خالی بگذارید.
Password	رمز عبور مدنظر خود برای استفاده جهت تأیید هویت را در بازه طولی 32 نویسه ASCII وارد کنید. رمز عبور به بزرگ و کوچک بودن حروف حساس است. در صورتی که گزینه User ID را برای How to Authenticate User انتخاب کردید، این را خالی بگذارید.
Authentication Card ID	شناسه کارت تأیید هویت مدنظر را در بازه طولی 116 نویسه ASCII وارد کنید. اینجا را می‌توانید خالی بگذارید. وقتی Allow users to register authentication cards را برای Authentication Settings اجازه دهید، نتیجه ثبت شده توسط کاربران تحت تأثیر قرار می‌گیرد.
ID Number	وقتی Card or ID Number یا ID Number در Authentication Settings < How to Authenticate User انتخاب شده باشد، این مورد نمایش داده می‌شود. عددی وارد کنید که بین مقدار تنظیم شده در Authentication Settings < The Minimum Digit Number of ID Number و تا حداکثر 8 رقم باشد.
Auto Generate	وقتی Card or ID Number یا ID Number در Authentication Settings < How to Authenticate User انتخاب شده باشد، این مورد نمایش داده می‌شود. برای ایجاد خودکار یک شماره شناسه با همان تعداد رقم‌هایی که در The Minimum Digit Number of ID Number انتخاب کرده‌اید، کلیک کنید.
Department	نام بخش و موارد دیگر شناسایی کننده کاربر را با بازه طولی 40 نویسه قابل بیان در قالب Unicode (UTF-16)) وارد کنید. اینجا را می‌توانید خالی بگذارید.
Email Address	آدرس کاربر را در بازه طولی 200 نویسه ASCII وارد کنید. این به عنوان مقصد برای Scan to My Email استفاده می‌شود. اینجا را می‌توانید خالی بگذارید.
Scan to My Folder	وقتی گزینه Individual را در مسیر Scan to My Folder < Setting Type < Scan to My Folder انتخاب می‌کنید، مقصدهای ذخیره‌سازی را به صورت جداگانه تنظیم کنید. برای دریافت اطلاعات بیشتر درباره تنظیم موارد، بخش زیر را ملاحظه کنید. "تنظیم Scan to My Folder" در صفحه 144
Restrictions	عملکردهای را می‌توانید برای هر کاربر محدود کنید. عملکردی را انتخاب کنید که اجازه استفاده آن را می‌دهد.

مورد	توضیحات
Presets	<p>شما می‌توانید پنج مورد پیش‌تنظیم مشخص کنید که تنها برای کاربر انتخاب شده از Presets ثبت شده در اسکرین قابل دسترسی باشند.</p> <p><input type="checkbox"/> موارد Presets که به یک کاربر تخصیص یافته‌اند، تنها توسط همان کاربر قابل استفاده خواهند بود.</p> <p>موارد Presets که به هیچ کاربری تخصیص نیافته‌اند، برای همه کاربران قابل استفاده خواهند بود.</p> <p><input type="checkbox"/> اگر برای یک کاربر تنها یکی از Presets قابل دسترسی باشد، این مورد پس از تأیید هویت به طور خودکار بارگذاری خواهد شد. اگر چندین مورد از Presets قابل دسترسی باشند، لیستی از Presets پس از تأیید هویت نمایش داده می‌شود.</p> <p><input type="checkbox"/> شما می‌توانید Presets را که از عملکردهای محدود شده در Restrictions استفاده می‌کنند، ایجاد کرده یا نمایش دهید.</p>

ثبت کردن چندین User Settings با استفاده از یک فایل (Web Config CSV)

تنظیمات مربوط به هر کاربر را در یک فایل CSV وارد کرده و آنها را به صورت یک دسته ثبت کنید.

ایجاد یک فایل CSV

یک فایل CSV برای وارد کردن User Settings ایجاد کنید.

نکته:

اگر یک یا تعداد بیشتری از User Settings را از قبل ثبت کنید و سپس فایل قالب‌بندی شده (فایل CSV) را استخراج کنید، قادر خواهید بود از تنظیمات ثبت شده به عنوان مرجع وارد کردن موارد تنظیمات استفاده کنید.

1. وارد Web Config شوید و زبانه **User Settings < Product Security** را انتخاب کنید.

2. روی **Export** کلیک کنید.

3. قالب فایل مورد نظر را برای **File Format** انتخاب کنید.

آن را با مراجعه به بخش زیر انتخاب کنید.

مورد	توضیحات
CSV UTF-16 (Tab delimited)	وقتی ویرایش فایل را با استفاده از Microsoft Excel انجام می‌دهید آن را انتخاب کنید. هر پارامتر توسط یک «[]» (براکت) احاطه شده است. پارامترها را در «[]» وارد کنید. توصیه می‌کنیم هنگام بروزرسانی فایل، نسخه فایل موجود را جایگذاری کنید. اگر اخیراً فایل را ذخیره کرده‌اید، گزینه Unicode text (*.txt) را به عنوان قالب فایل انتخاب کنید.
CSV UTF-8 (Comma delimited)	وقتی ویرایش فایل را با استفاده از یک ویرایشگر متن یا ماکرو بدون استفاده از Microsoft Excel انجام می‌دهید آن را انتخاب کنید.
CSV UTF-8 (Semicolon delimited)	

4. روی **Export** کلیک کنید.

5. این فایل CSV را در یک برنامه صفحه گسترده مانند Microsoft Excel یا در یک ویرایشگر متن ویرایش کرده و ذخیره کنید.



مهم:

هنگام ویرایش فایل، انکدینگ و اطلاعات سرصفحه فایل را تغییر ندهید.

موارد تنظیم فایل CSV

مورد	تنظیمات و توضیحات
UserID	شناسه کاربری مورد استفاده برای تأیید هویت را بین 1 و 83 بایت در Unicode وارد کنید.
UserName	برای ورود به سیستم، نام کاربری نمایش یافته در پانل کنترل اسکتر با بازه طولی 32 نویسه Unicode وارد کنید. اینجا را می‌توانید خالی بگذارید.
Password	رمز عبور مدنظر برای استفاده جهت تأیید هویت را در بازه طولی 32 نویسه ASCII وارد کنید. هنگام وارد کردن، بجای EncPassword، این به عنوان رمز عبور تعیین می‌شود. در صورتی که گزینه User ID را برای How to Authenticate User انتخاب کردید، این را خالی بگذارید. هنگام استخراج کردن، این همیشه خالی می‌ماند.
AuthenticationCardID	نتیجه خوانش کارت تأیید هویت را تعیین کنید. وقتی Allow users to register authentication cards را در Authentication Settings اجازه دهید، نتیجه ثبت شده توسط کاربران تحت تأثیر قرار می‌گیرد. نامی در بازه طولی 116 نویسه ASCII وارد کنید. اینجا را می‌توانید خالی بگذارید.
IDNumber	وقتی Card or ID Number یا ID Number در Authentication Settings < How to Authenticate User انتخاب شده باشد، این مورد نمایش داده می‌شود. عددی وارد کنید که بین مقدار تنظیم شده در Authentication Settings < The Minimum Digit Number of ID Number و تا حداکثر 8 رقم باشد. کارت شناسایی نمی‌تواند تکراری باشد. در صورت تکراری بودن، هنگام وارد کردن فایل با پیام خطا مواجه خواهید شد. وقتی خالی گذاشته شود، به طور خودکار یک عدد به آن تخصیص می‌یابد.
Department	نام بخش را به صورت غیرواقعی وارد کنید تا هویت کاربران مخفی بماند. مقداری در بازه طولی 40 نویسه Unicode وارد کنید. اینجا را می‌توانید خالی بگذارید.
MailAddress	آدرس ایمیل کاربران را تنظیم کنید. این به عنوان مقصد برای Scan to My Email استفاده می‌شود. شما می‌توانید از نویسه‌های A-Z، a-z، 0-9، @، ~، _، {، }، ^، =، /، *، &، %، #، ! استفاده کنید. حداکثر 200 نویسه وارد کنید. نمی‌توانید از نویسه «» (کاما) به عنوان اولین نویسه استفاده کنید. اینجا را می‌توانید خالی بگذارید.
FolderProtocol	نوع عملکرد Scan to My Folder را تنظیم کنید. پوشه شبکه/FTP (SMB): 0، FTP: 1
FolderPath	مقصد ذخیره را برای عملکرد Scan to My Folder تنظیم کنید.
FolderUserName	نام کاربری را برای عملکرد Scan to My Folder تنظیم کنید.
FolderPassword	یک رمز عبور برای تأیید هویت پوشه مقصد برای عملکرد Scan to My Folder وارد کنید که در بازه طولی 32 نویسه ASCII باشد. هنگام وارد کردن، بجای EncPassword، این به عنوان رمز عبور تعیین می‌شود. هنگام استخراج کردن، این همیشه خالی می‌ماند.
FtpPassive	حالت اتصال را برای سرور FTP در مواردی که گزینه FTP به عنوان Type عملکرد Scan to My Folder تعیین شده باشد، تنظیم کنید. حالت فعال: 0، حالت غیرفعال: 1
FtpPort	شماره درگاه برای ارسال داده‌های اسکن شده به سرور FTP از میان 0 تا 65535 برای مواردی که گزینه FTP به عنوان Type عملکرد Scan to My Folder تعیین شده باشد، تنظیم کنید.
ScanToMemory	محدودیت‌های Scan to USB Drive را تنظیم کنید. غیر مجاز: 0، مجاز: 1

مورد	تنظیمات و توضیحات
ScanToMail	محدودیت‌های Scan to Email را تنظیم کنید. گزینه اسکن و ارسال به ایمیل من را تنها زمانی می‌توانید تنظیم کنید که Scan to Email غیرفعال باشد. غیر مجاز: 0، مجاز: 1
ScanToFolder	محدودیت‌های Scan to Network Folder/FTP را تنظیم کنید. گزینه اسکن و ارسال به پوشه من را تنها زمانی می‌توانید تنظیم کنید که Scan to Network Folder/FTP غیرفعال باشد. غیر مجاز: 0، مجاز: 1
ScanToCloud	محدودیت‌های Scan to Cloud را تنظیم کنید. غیر مجاز: 0، مجاز: 1
ScanToComputer	محدودیت‌های ذخیره اسکن در رایانه را تنظیم کنید. غیر مجاز: 0، مجاز: 1
PresetIndex	موارد Presets را که مایلید به کاربر مرتبط نمایید تنظیم کنید. تا حداکثر شماره ثبت Presets را می‌توانید به صورت جدا شده با کاما وارد کنید.
EncPassword	هنگام استخراج تنظیمات کاربر، پارامتر تنظیم شده برای Password رمزنگاری می‌شود، سپس مقدار بر اساس BASE64 و خروجی کدگذاری مجدد می‌گردد. هنگام وارد کردن در حالتی که رمز عبور جدید برای Password تعیین شده است، این مقدار صرفنظر می‌شود. اگر Password خالی باشد، این مقدار استفاده شده و رمز عبور به همان صورت قبل از استخراج باقی می‌ماند.
EncFolderPath	هنگام استخراج، پارامتر تنظیم شده برای FolderPassword رمزنگاری می‌شود، سپس مقدار بر اساس BASE64 و خروجی کدگذاری مجدد می‌گردد. هنگام وارد کردن در حالتی که رمز عبور جدید برای FolderPassword تعیین شده است، این مقدار صرفنظر می‌شود. اگر FolderPassword خالی باشد، این مقدار استفاده شده و رمز عبور به همان صورت قبل از استخراج باقی می‌ماند.

وارد کردن یک فایل CSV

1. وارد Web Config شوید و زبانه **User Settings < Product Security** را انتخاب کنید.
2. روی **Import** کلیک کنید.
3. فایل مورد نظر برای وارد کردن را انتخاب کنید.
4. روی **Import** کلیک کنید.
5. پس از بررسی کردن اطلاعات نمایش یافته، روی گزینه **OK** کلیک کنید.

ثبت کردن User Settings در چندین اسکنر به صورت یک دسته (Epson Device Admin)

شما می‌توانید User Settings استفاده شده در Local DB را به صورت یک دسته از طریق یک سرور LDAP یا یک فایل CSV/ENE ثبت کنید.

نکته:

یک فایل *ENE* فایل باینری ارائه شده توسط *Epson* است که اطلاعات مربوط به *Contacts* از قبیل اطلاعات شخصی و *User Settings* را رمزنگاری و ذخیره می‌کند. این فایل را می‌توان از طریق *Epson Device Admin* استخراج کرد و می‌توانید برای آن رمز عبور نیز تعیین کنید. این زمانی مفید است که در نظر داشته باشید *User Settings* را از یک فایل پشتیبان وارد کنید.

وارد کردن از فایل CSV/ENE

1. مسیر **User Settings < Authentication Settings < Administrator Settings** را از الگوی پیکربندی انتخاب کنید.
2. روی **Import** کلیک کنید.
3. گزینه **CSV or ENE File** را از بخش **Import Source** انتخاب کنید.
4. روی **Browse** کلیک کنید.
صفحه انتخاب فایل نمایش داده می‌شود.
5. فایل مورد نظر برای وارد کردن را انتخاب کنید تا باز شود.
6. یک روش وارد کردن را انتخاب کنید.
 Overwrite and Add: اگر همان شناسه کاربری از قبل وجود داشته باشد آن را جایگزین می‌کند؛ در صورتی که وجود نداشته باشد، یک شناسه جدید اضافه می‌کند.
 Replace All: همه چیز را با تنظیمات کاربر مورد نظر برای وارد کردن جایگزین می‌کند.
7. روی **Import** کلیک کنید.
صفحه تأیید تنظیمات نمایش داده می‌شود.
8. روی **OK** کلیک کنید.
نتیجه تأیید نمایش داده می‌شود.

نکته:

اگر تعداد تنظیمات کاربری وارد شده بیش از تعداد مجاز باشد، پیامی مبنی بر حذف برخی تنظیمات کاربری نمایش داده می‌شود. هر تنظیمات کاربر اضافی را قبل از وارد کردن حذف کنید.

تنظیمات کاربری را که می‌خواهید قبل از وارد کردن انتخاب نمایید و سپس روی **Delete** کلیک کنید.

9. روی **Import** کلیک کنید.
تنظیمات کاربر در الگوی پیکربندی وارد می‌شوند.

وارد کردن از سرور LDAP

1. مسیر **User Settings < Authentication Settings < Administrator Settings** را از الگوی پیکربندی انتخاب کنید.
2. روی **Import** کلیک کنید.
3. گزینه **LDAP** را از بخش **Import Source** انتخاب کنید.

4.

روی **Settings** کلیک کنید.

تنظیمات **LDAP Server** نمایش داده می‌شوند.

نکته:

این تنظیمات سرور **LDAP** برای وارد کردن تنظیمات کاربری از سرور **LDAP** می‌باشند. تنظیمات کاربر وارد شده (کپی شده) برای تأیید هویت کاربران با استفاده از خود اسکنر استفاده می‌شوند.

به عبارتی دیگر، هنگامی که **LDAP** یا **Local DB and LDAP** را به عنوان روش تأیید هویت انتخاب کنید، کاربران از طریق ارتباط با سرور **LDAP** تأیید هویت می‌شوند.

5.

هر مورد را تنظیم کنید.

هنگام وارد کردن تنظیمات کاربر از یک سرور **LDAP** قادر خواهید بود تنظیمات زیر را علاوه بر تنظیمات **LDAP** پیکربندی کنید. در رابطه با سایر موارد، بخش «اطلاعات مرتبط» را مشاهده کنید.

مورد	توضیحات
LDAP Server Type	اجازه می‌دهد نوع سرور LDAP را انتخاب کنید.
LDAP Server Settings	
Search Filter	متن استفاده شده برای فیلتر جستجوی LDAP را تنظیم کنید. گزینه Custom را برای ویرایش متن جستجو انتخاب کنید.
Type	شما می‌توانید نوع مقصد ذخیره‌سازی برای Scan To My Folder را تنظیم کنید.
Options	
Connection Mode	وقتی Type روی گزینه FTP تنظیم شده باشد، می‌توانید حالت اتصال FTP را تنظیم کنید.
Port Number	وقتی Type روی گزینه FTP تنظیم شده باشد، می‌توانید شماره درگاه مورد نظر برای استفاده را تنظیم کنید.

6.

تست اتصال را در صورت ضرورت با کلیک کردن روی گزینه **Connection Test** انجام دهید.

10 تنظیم کاربر را از سرور **LDAP** کسب کرده و نمایش دهید.

7.

روی **OK** کلیک کنید.

8.

یک روش وارد کردن را انتخاب کنید.

Overwrite and Add: اگر همان شناسه کاربری از قبل وجود داشته باشد آن را جایگزین می‌کند؛ در صورتی که وجود نداشته باشد، یک شناسه جدید اضافه می‌کند.

Replace All: همه چیز را با تنظیمات کاربر مورد نظر برای وارد کردن جایگزین می‌کند.

9.

روی **Import** کلیک کنید.

صفحه تأیید تنظیمات نمایش داده می‌شود.

10.

روی **OK** کلیک کنید.

نتیجه تأیید نمایش داده می‌شود.

11.

روی **Import** کلیک کنید.

تنظیمات کاربر در الگوی پیکربندی وارد می‌شوند.

اطلاعات مرتبط

← "پی‌کرندگی سرور LDAP" در صفحه 140

← "پی‌کرندگی تنظیمات جستجوی سرور LDAP" در صفحه 142

همگام‌سازی با LDAP Server

تنظیمات LDAP Server را برای اسکنر انجام دهید.

تنظیمات مربوط به هر دو سرور اولیه و ثانویه را حسب ضرورت انجام دهید.

نکته:

تنظیمات LDAP Server با *Contacts* به اشتراک گذاشته می‌شوند.

سرویس‌های موجود

سرویس‌های دایرکتوری زیر پشتیبانی می‌شوند.

نام سرویس	نسخه
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

پی‌کرندگی سرور LDAP

برای استفاده از سرور LDAP، باید سرور LDAP را پی‌کرندگی کنید.

هنگام تنظیم از **Web Config**:

زبان **Network < LDAP Server < Basic (Primary Server)** یا **Basic (Secondary Server)** را انتخاب کنید.

اگر گزینه **Kerberos Authentication** را به عنوان **Authentication Method** انتخاب می‌کنید، برای اعمال تنظیمات برای Kerberos، مسیر **Network < Kerberos Settings** را انتخاب نمایید.

هنگام تنظیم از **Epson Device Admin**:

مسیر **Network < LDAP server < Server Settings (Primary Server)** یا **Server Settings (Secondary Server)** را از الگوی پی‌کرندگی انتخاب کنید.

اگر گزینه **Kerberos Authentication** را به عنوان **Authentication Method** انتخاب می‌کنید، برای اعمال تنظیمات برای Kerberos، مسیر **Security — Network < Kerberos Settings** را انتخاب نمایید.

مورد	تنظیمات و توضیحات
Use LDAP Server	گزینه Use یا Do Not Use را انتخاب کنید.
LDAP Server Address	آدرس سرور LDAP را وارد کنید. 1 تا 255 نویسه را در قالب IPv4، IPv6 یا FQDN وارد کنید. برای قالب FQDN، می‌توانید از نویسه‌های الفبایی-عددی در قالب ASCII (0x20-0x7E) و خطوط تیره به جز در ابتدا و انتهای آدرس استفاده کنید.
(Port number) LDAP server Port Number	شماره درگاه سرور LDAP را از 1 تا 65535 وارد کنید.
Secure Connection	روش تأیید اعتبار اسکنر برای دسترسی به سرور LDAP را مشخص کنید.

مورد	تنظیمات و توضیحات
Certificate Validation	زمانی که این فعال باشد گواهی سرور LDAP تأیید می‌شود. توصیه می‌کنیم این را روی حالت Enable تنظیم کنید. برای تنظیم آن، لازم است CA Certificate به اسکتر وارد شود.
Search Timeout (sec)	مدت زمان جستجو پیش از وقوع وقفه را از 5 تا 300 ثانیه وارد کنید.
Authentication Method	روش تأیید هویت را انتخاب کنید. اگر Kerberos Authentication را انتخاب می‌کنید، تنظیمات مربوط به Kerberos را ابتدا انتخاب کنید. برای انجام Kerberos Authentication، شرایط زیر ضروری می‌باشند. <input type="checkbox"/> اسکتر و سرور DNS می‌توانند ارتباط برقرار کنند. <input type="checkbox"/> زمان اسکتر، سرور KDC و سرور مورد نیاز برای تأیید اعتبار (سرور LDAP، سرور SMTP، سرور File) همگام می‌شوند. <input type="checkbox"/> وقتی سرور خدمات به عنوان آدرس IP تخصیص داده می‌شود، FQDN سرور خدمات در سرور DNS متضاد با منطقه جستجو ثبت می‌شود.
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 (UTF-8 Unicode) وارد کنید. استفاده از نویسه‌های کنترلی مانند 0x00 تا 0x1F و 0x7F مجاز نیست. این تنظیم در صورتی که Anonymous Authentication به عنوان Authentication Method انتخاب شود، کاربرد ندارد. اگر نمی‌خواهید این را مشخص کنید، آن را خالی بگذارید.
Password	رمز عبور مربوط به تأیید هویت سرور LDAP را با حداکثر 128 نویسه یونیکد (UTF-8) وارد کنید. استفاده از نویسه‌های کنترلی مانند 0x00 تا 0x1F و 0x7F مجاز نیست. این تنظیم در صورتی که Anonymous Authentication به عنوان Authentication Method انتخاب شود، کاربرد ندارد. اگر نمی‌خواهید این را مشخص کنید، آن را خالی بگذارید.

تنظیمات Kerberos

اگر گزینه **Kerberos Authentication** به عنوان **Authentication Method** انتخاب شده باشد، نیاز خواهید داشت تنظیمات Kerberos را اعمال کنید. می‌توانید تا 10 تنظیم Kerberos را ثبت کنید.

هنگام تنظیم از **Web Config**:

زبان **Network < Kerberos Settings** را انتخاب کنید.

هنگام تنظیم از **Epson Device Admin**:

مسیر **Network < Security < Kerberos Settings** را از الگوی پیکربندی انتخاب کنید.

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

پی‌کر بندی تنظیمات جستجوی سرور LDAP

مشخصات جستجو برای تنظیمات کاربر را تنظیم می‌کند.

هنگام تنظیم از Web Config:

زبان Network < LDAP Server < Search Settings (Authentication) را انتخاب کنید.

هنگام تنظیم از Epson Device Admin:

مسیر Administrator Settings < Authentication Settings < LDAP server < Search Settings (Authentication) را از الگوی پی‌کر بندی انتخاب کنید.

مورد	تنظیمات و توضیحات
Search Base (Distinguished Name)	مشخص کردن موقعیت شروع هنگام جستجو برای اطلاعات کاربر از سرور LDAP. از 0 تا 128 نویسه یونیکد (UTF-8) وارد کنید. اگر مشخصه اختیاری را جستجو نمی‌کنید، این قسمت را خالی بگذارید. نمونه دایرکتوری سرور محلی: dc=local,dc=server
User ID Attribute	تعیین کردن نام مشخصه‌ای که باید در هنگام جستجوی شماره شناسه نمایش داده شود. بین 1 تا 255 نویسه با قالب ASCII وارد کنید. نویسه اول باید a-z یا A-Z باشد. مثال: uid, cn
User name Display Attribute	تعیین کردن نام مشخصه‌ای که باید به عنوان نام کاربر نمایش داده شود، تعیین کنید. بین 0 تا 255 نویسه با قالب ASCII وارد کنید. نویسه اول باید a-z یا A-Z باشد. این قسمت را می‌توانید خالی بگذارید. مثال: name, cn
Authentication Card ID Attribute	تعیین کردن نام مشخصه‌ای که باید به عنوان شناسه کارت تأیید هویت نمایش داده شود، تعیین کنید. بین 0 تا 255 نویسه با قالب ASCII وارد کنید. نویسه اول باید a-z یا A-Z باشد. این قسمت را می‌توانید خالی بگذارید. مثال: sn, cn
ID Number Attribute	تعیین کردن نام مشخصه‌ای که باید در هنگام جستجوی شماره شناسه نمایش داده شود. بین 1 تا 255 نویسه با قالب ASCII وارد کنید. نویسه اول باید a-z یا A-Z باشد. مثال: id, cn
Department Attribute	تعیین کردن نام مشخصه‌ای که باید به عنوان نام بخش نمایش داده شود، تعیین کنید. بین 0 تا 255 نویسه با قالب ASCII وارد کنید. نویسه اول باید a-z یا A-Z باشد. این قسمت را می‌توانید خالی بگذارید. مثال: ou-cl, ou
Email Address Attribute	تعیین کردن نام مشخصه‌ای که باید در هنگام جستجوی آدرس‌های ایمیل نمایش داده شود. بین 1 تا 255 نویسه با قالب ASCII وارد کنید. نویسه اول باید a-z یا A-Z باشد. مثال: mail
Save To Attribute	تعیین کردن نام مشخصه‌ای که به مقصد Scan To My Folder مربوط می‌شود. بین 0 تا 255 نویسه با قالب ASCII وارد کنید. مثال: homeDirectory

بررسی اتصال سرور LDAP

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

1. وارد Web Config شوید و زبان 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.

مراجعه آزمایش اتصال سرور LDAP

پیام ها	توضیحات
Connection test was successful.	این پیام زمانی ظاهر می شود که ارتباط با سرور با موفقیت برقرار شود.
Connection test failed. Check the settings.	این پیام به دلایل زیر ظاهر می شود: <input type="checkbox"/> نشانی سرور LDAP یا شماره درگاه نادرست است. <input type="checkbox"/> وقفه رخ داده است. <input type="checkbox"/> گزینه Do Not Use به عنوان حالت Use LDAP Server انتخاب شده است. <input type="checkbox"/> 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 اسکت و سرور LDAP قطع شود.
Authentication failed. Check the settings.	این پیام به دلایل زیر ظاهر می شود: <input type="checkbox"/> User Name و/یا Password نادرست باشد. <input type="checkbox"/> 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 اسکت مشغول باشد.

تنظیم سرور ایمیل

وقتی از Scan to My Email استفاده می کنید، سرور ایمیل را تنظیم کنید.

نکته:

گزینه Scan to My Email را تنها زمانی می توانید تنظیم کنید که Scan to Email غیرفعال باشد.

هنگام تنظیم از Web Config:

زبان Basic < Email Server < Network را انتخاب کنید.

هنگام تنظیم از Epson Device Admin:

مسیر Common < Email Server < Mail Server Settings را از الگوی پیکربندی انتخاب کنید.

مورد	تنظیمات و توضیحات	
Authentication Method	روش تأیید اعتبار اسکت 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، سرور POP3 را تنظیم کنید.

تنظیمات و توضیحات	مورد	
اگر گزینه SMTP AUTH یا POP before SMTP را به عنوان Authentication Method انتخاب می‌کنید، نام حساب تأیید شده را وارد کنید. بین 0 و 255 نویسه با قالب ASCII (0x20-0x7E) وارد کنید.	Authenticated Account	
اگر گزینه SMTP AUTH یا POP before SMTP را به عنوان Authentication Method انتخاب می‌کنید، رمز عبور تأیید شده را وارد کنید. بین 0 و 20 نویسه با قالب ASCII (0x20-0x7E) وارد کنید.	Authenticated Password	
آدرس ایمیل فرستنده را وارد کنید. بین 0 و 255 نویسه در قالب ASCII (0x20-0x7E) به جز برای () < > ; [] ¥ وارد کنید. نقطه «.» نمی‌تواند اولین نویسه باشد.	Sender's Email Address	
بین 0 تا 255 نویسه را با استفاده از 0-9 a-z A-Z - . وارد کنید. می‌توانید از فرمت IPv4 یا FQDN استفاده کنید.	SMTP Server Address	
عدد بین 1 تا 65535 وارد کنید.	SMTP Server Port Number	
روش اتصال ایمن را برای این سرور ایمیل مشخص کنید.	Secure Connection	
اگر POP before SMTP را در Authentication Method انتخاب کنید، روش اتصال روی گزینه None تنظیم می‌شود.		None
این زمانی موجود است که Authentication Method روی Off یا SMTP AUTH تنظیم باشد.		SSL/TLS
این زمانی موجود است که Authentication Method روی Off یا SMTP AUTH تنظیم باشد.	STARTTLS	
زمانی که این فعال باشد گواهی تأیید می‌شود. توصیه می‌کنیم این را روی حالت Enable تنظیم کنید.	Certificate Validation	
اگر گزینه POP before SMTP را به عنوان Authentication Method انتخاب می‌کنید، آدرس سرور POP3 را وارد کنید. بین 0 و 255 نویسه با استفاده از نویسه‌های 0-9 a-z A-Z - . وارد کنید. می‌توانید از فرمت IPv4 یا FQDN استفاده کنید.	POP3 Server Address	
اگر گزینه POP before SMTP را به عنوان Authentication Method انتخاب می‌کنید، شماره درگاه را مشخص کنید. عددی بین 1 تا 65535 وارد کنید.	POP3 Server Port Number	

تنظیم Scan to My Folder

تصاویر اسکن شده در پوشه تخصیص یافته به هر کاربر ذخیره می‌شوند. پوشه زیر را می‌توانید به عنوان یک پوشه اختصاصی تنظیم کنید.

نکته:

گزینه Scan To My Folder را تنها زمانی می‌توانید تنظیم کنید که Scan to Network Folder/FTP غیرفعال باشد.

موقعیت تنظیم مسیر پوشه	Authentication Method	ذخیره در تنظیمات
اسکنر (تنظیم Scan to My Folder)	Local DB <input type="checkbox"/> LDAP <input type="checkbox"/> Local DB and LDAP <input type="checkbox"/>	تعیین یک پوشه شبکه برای همه Authentication Settings برای ایجاد خودکار یک پوشه شخصی تحت پوشه معین شده با استفاده از نام شناسه کاربری.
اسکنر (User Settings)	Local DB	پوشه‌های شبکه مختلف را به صورت جداگانه به هر کاربر اختصاص می‌دهد.
مشخصات LDAP	LDAP	
اسکنر (User Settings) یا مشخصات LDAP	Local DB and LDAP	

هنگام تنظیم از Web Config:

زبان Product Security < Scan to Network Folder/FTP را انتخاب کنید.

هنگام تنظیم از Epson Device Admin:

مسیر Administrator Settings < Authentication Settings < Scan to Network Folder/FTP < Scan to My Folder را از الگوی پیکربندی انتخاب کنید.

مورد	توضیحات
Save To Setting	<p><input type="checkbox"/> Shared:</p> <p>به طور خودکار یک پوشه با نام شناسه کاربری زیر مسیر پوشه یا URL مشخص شده در Save to ایجاد کرده و تصاویر اسکن شده را در این پوشه ذخیره می‌کند.</p> <p><input type="checkbox"/> Individual:</p> <p>مقصد ذخیره‌سازی برای نتایج اسکن هر کاربر را تنظیم می‌کند. کاربران Local DB را می‌توان در تنظیمات کاربر مشخص کرد. کاربران LDAP از موقعیت ذخیره‌سازی دریافت شده از مشخصات جستجوی سرور LDAP استفاده می‌کنند.</p>
Type	<p>پروتکل انتقال را مطابق با مقصد خروجی اسکن انتخاب کنید.</p> <p>برای یک پوشه شبکه: Network Folder (SMB)</p> <p>برای یک سرور FTP:FTP</p>
Save to	<p>مسیر یا URL مسیر خروجی را مشخص کنید.</p> <p>مقداری در بازه طولی 160 نویسه (UTF-16Unicode) وارد کنید.</p>
Connection Mode	<p>وقتی گزینه FTP را در Type انتخاب می‌کنید، تنظیم نمایید.</p> <p>یک حالت اتصال به سرور FTP را انتخاب کنید.</p>
Port Number	<p>وقتی گزینه FTP را در Type انتخاب می‌کنید، تنظیم نمایید.</p> <p>شماره درگاه مورد نظر برای ارسال داده‌های اسکن شده به یک سرور FTP را بین شماره‌های 0 و 65535 انتخاب کنید.</p>
Authentication Settings	<p>وقتی گزینه Individual را به عنوان Setting Type در Save To Setting انتخاب می‌کنید، این را تنظیم کنید.</p> <p>برای دسترسی به پوشه، «User Name» و «Password» را تنظیم کنید.</p> <p><input type="checkbox"/> Shared:</p> <p>از یک User Name و Password مشترک برای همه کاربران استفاده کنید.</p> <p><input type="checkbox"/> Individual:</p> <p>برای کاربران Local DB، مقادیر User Name و Password را به صورت جداگانه در بخش تنظیمات کاربر تنظیم کنید. کاربران LDAP را نمی‌توان به صورت جداگانه پیکربندی کرد. مقادیر User Name و Password تنظیم شده توسط این گزینه به صورت دسته‌ای استفاده می‌شوند.</p>
User Name	<p>برای دسترسی به پوشه مقصد خروجی اسکن نام کاربری را وارد کنید.</p> <p>مقداری در بازه طولی 30 نویسه (UTF-16Unicode) وارد کنید. این گزینه را وقتی از یک سرور Shared یا سرور LDAP استفاده می‌کند تنظیم نمایید.</p>
Password	<p>رمز عبور متناظر با User Name را وارد کنید.</p> <p>مقداری در بازه طولی 20 نویسه (UTF-16Unicode) وارد کنید. این گزینه را وقتی از یک سرور Shared یا سرور LDAP استفاده می‌کند تنظیم نمایید.</p>

جلوگیری از تغییر مقصد برای Scan to Network Folder/FTP

مورد	توضیحات
Prohibit manual entry of destination	وقتی فعال باشد، کاربر نمی‌تواند مقصد پیش‌فرض را تغییر دهد.

Customize One-touch Functions

از طریق ویرایش چیدمان آیکن‌های نمایش یافته در صفحه اصلی برای پانل کنترل می‌توانید تنها آیکن‌های ضروری را نمایش دهید.

هنگام تنظیم از Web Config:

زبانہ Customize One-touch Functions < Product Security را انتخاب کنید.

هنگام تنظیم از Epson Device Admin:

مسیر Customize One-touch Functions < Authentication Settings < Administrator Settings را از الگوی پیکربندی انتخاب کنید.

نکته:

در موارد زیر، آیکن‌های مربوط به عملکردهای خاص در صفحه اصلی نمایش داده می‌شوند.

وقتی عملکردهایی را انتخاب کنید که به دلیل **Restrictions** مجاز نیستند.

وقتی آدرس ایمیل برای یک کاربر وارد شده به سیستم ثبت نشده است. (Scan to My Email)

وقتی پوشه مقصد تنظیم نشده است. (Scan to My Folder)

مورد	توضیحات
Maximum functions per screen	انتخاب چیدمان آیکن‌های نمایش یافته در پانل کنترل. تصویر مطابق با چیدمان انتخابی تغییر می‌کند.
Screen(s)	انتخاب تعداد صفحات.
Number	انتخاب عملکردهایی که مایدی برای هر موقعیت شماره گذاری شده نمایش یابند.

Job History گزارش‌های با استفاده از Epson Device Admin

شما می‌توانید یک گزارش Job History برای هر گروه و هر کاربر از طریق استفاده از Epson Device Admin ایجاد کنید. تا حداکثر 3000 نمونه تاریخیچه استفاده را می‌توانید در اسکرین ذخیره کنید. گزارش را می‌توانید با تعیین کردن یک دوره یا تنظیم برای یک برنامه منظم استفاده کنید.

برای تهیه خروجی Job History به صورت یک گزارش، مسیر Epson Print Admin Serverless/Authentication Settings < Options را از منوی روبان در صفحه لیست دستگاه‌ها انتخاب کنید.

برای اطلاع از جزئیات نحوه تهیه گزارش، مستندات Epson Device Admin را ببینید.



مواردی که می‌توان در گزارش لحاظ کرد

موارد زیر را می‌توانید در خروجی گزارش کاربر لحاظ کنید.

:Scan/Destination :Scan/Destination type :Scan/Result details/Result/Department/User ID/Operation/Job ID/Date
:Devices/Serial Number :Devices/IP Address :Devices/Model :Devices/Pages :Scan/Color :Scan/2-Sided :Scan/Paper Size
Note :Devices/Remark :Devices/Location :Devices/Department

وارد شدن به عنوان سرپرست از پانل کنترل

هر کدام از روش‌های زیر را می‌توانید برای ورود به سیستم به عنوان سرپرست از طریق پانل کنترل اسکتر استفاده کنید.

1. روی گزینه  در گوشه بالا سمت راست صفحه ضربه بزنید.
وقتی گزینه Authentication Settings فعال باشد، آیکن در صفحه خوش آمدید (صفحه آماده بکار تأیید هویت) نمایش داده می‌شود.
وقتی گزینه Authentication Settings غیرفعال باشد، آیکن در صفحه اصلی نمایش داده می‌شود.
2. هنگام نمایش صفحه تأیید، روی گزینه بله ضربه بزنید.
3. رمز عبور سرپرست سیستم را وارد نمایید.
پیام تکمیل ورود نمایش داده می‌شود و سپس صفحه اصلی در پانل کنترل نمایش داده می‌شود.
برای خروج، روی گزینه  در گوشه بالا سمت راست صفحه اصلی ضربه بزنید.

غیرفعال کردن Authentication Settings

می‌توانید Authentication Settings را با استفاده از Web Config غیر فعال کنید.

نکته:

User Settings ثبت شده در اسکتر ذخیره خواهند شد حتی اگر Authentication Settings غیر فعال باشد. آنها را می‌توانید با بازیابی اسکتر به تنظیمات پیش فرض حذف کنید.

1. وارد پوشه Web Config شوید.
2. زبانه **Authentication < Basic < Product Security** را انتخاب کنید.
3. گزینه **OFF** را انتخاب کنید.
4. روی **Next** کلیک کنید.
5. روی **OK** کلیک کنید.

نکته:

حتی اگر Authentication Settings را غیرفعال کنید، گزینه تنظیم قفل فعال باقی می‌ماند. اگر در نظر دارید آن را غیرفعال کنید، قادر خواهید بود تنظیمات را از پانل کنترل یا Web Config اعمال کنید.

اطلاعات مرتبط

- ← "تنظیم تنظیم قفل از پانل کنترل" در صفحه 85
- ← "تنظیم تنظیم قفل از طریق Web Config" در صفحه 85

حذف اطلاعات Authentication Settings (بازگرداندن تنظیمات اولیه)

برای حذف همه اطلاعات Authentication Settings (Card Reader, Authentication Method, User Settings و امثال آن)، همه تنظیمات اسکر را به تنظیمات پیش فرض زمان خرید بازیابی کنید. مسیر تنظیم < سرپرست سیستم > بازگرداندن تنظیمات اولیه < همه تنظیمات را در پانل کنترل انتخاب کنید.



مهم:

همه مخاطبین و سایر تنظیمات شبکه نیز حذف خواهند شد. تنظیمات حذف شده قابل بازیابی نیستند.

حل کردن مشکلات

کارت تأیید هویت خوانده نمی‌شود

موارد زیر را بررسی کنید.

- بررسی کنید آیا دستگاه تأیید هویت به درستی به اسکر متصل است. دستگاه تأیید هویت را به درگاه USB رابط خارجی واقع در پشت اسکر وصل کنید.
- بررسی کنید آیا دستگاه تأیید هویت و کارت تأیید هویت پشتیبانی می‌شوند.

نگهداری


150. تمیز کردن قسمت خارجی اسکتر.
150. تمیز کردن قسمت داخلی اسکتر.
155. تعویض کیت مجموعه غلتک.
160. بازنشانی تعداد اسکن ها.
160. صرفه جویی در مصرف برق.
161. حمل و نقل اسکتر.
162. پشتیبان گیری از تنظیمات.
163. بازگرداندن تنظیمات اولیه.
164. به روزرسانی برنامه ها و میان افزار.

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، تیز 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 بنشینند 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 اسکن‌ها را می‌توانید 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. مقدار کمی تمیز کننده روی دستمال نظیف بریزید و برای پاک کردن لکه‌ها استفاده کنید.

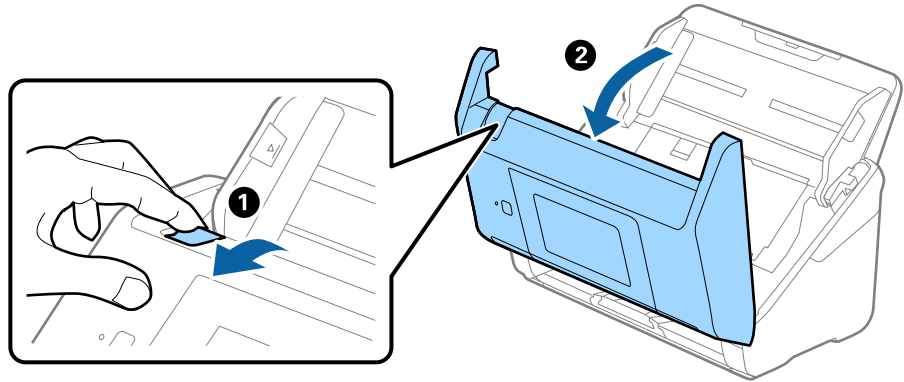
مهم!

- هرگز از الکل، تیز یا هر حلال خورنده دیگر 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.

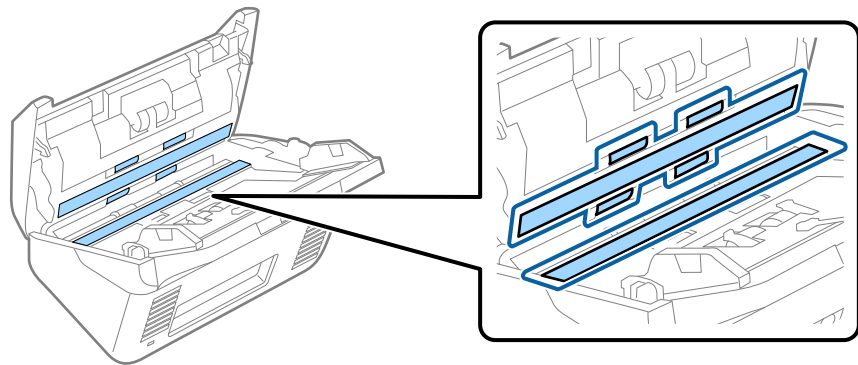
1. دکمه  را برای خاموش کردن اسکنر فشار دهید.

2. آداپتور AC را از اسکنر جدا کنید.

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



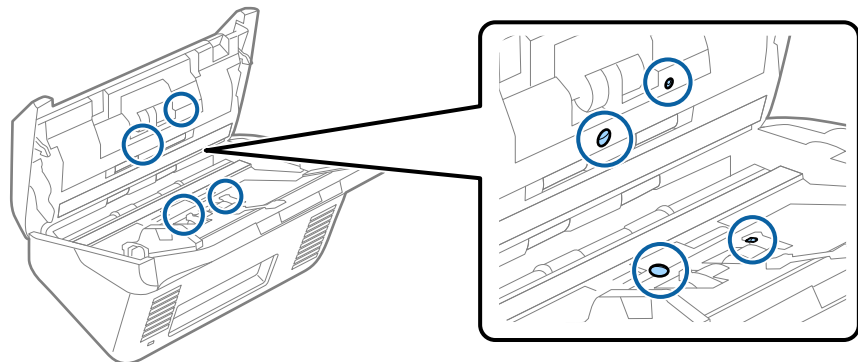
4. هرگونه لکه روی غلتک اعتباری و سطح شیشه‌ای قسمت داخلی و انتهایی قاب اسکنر را با استفاده از یک دستمال نرم یا کیت تمیزکاری اصلی Epson پاک کنید.



مهم:

- فشار 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.
- تمیزکننده را به طور مستقیم روی سطح شیشه اسپری نکنید.

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



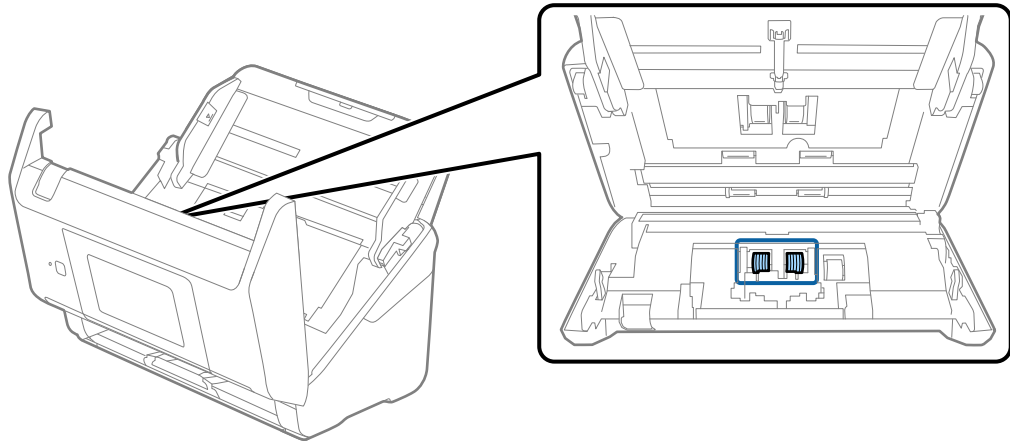


مهم:

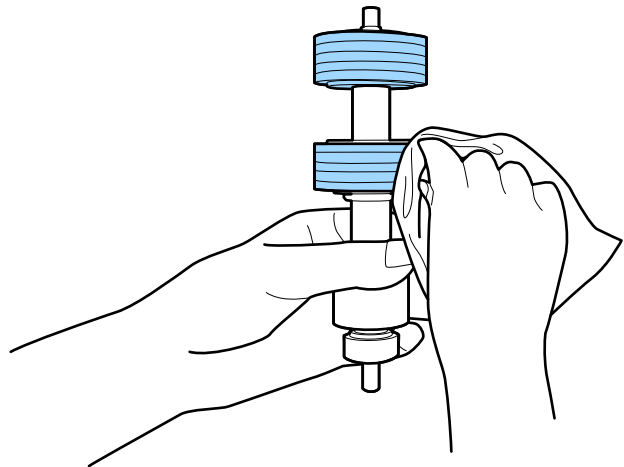
از مایعاتی نظیر شوینده‌ها روی گوشه‌پاک‌کن استفاده نکنید.

6. قاب را باز کرده و غلتک جداکننده را بیرون بیاورید.

برای کسب اطلاعات بیشتر به "تعویض کیت مجموعه غلتک" مراجعه کنید.



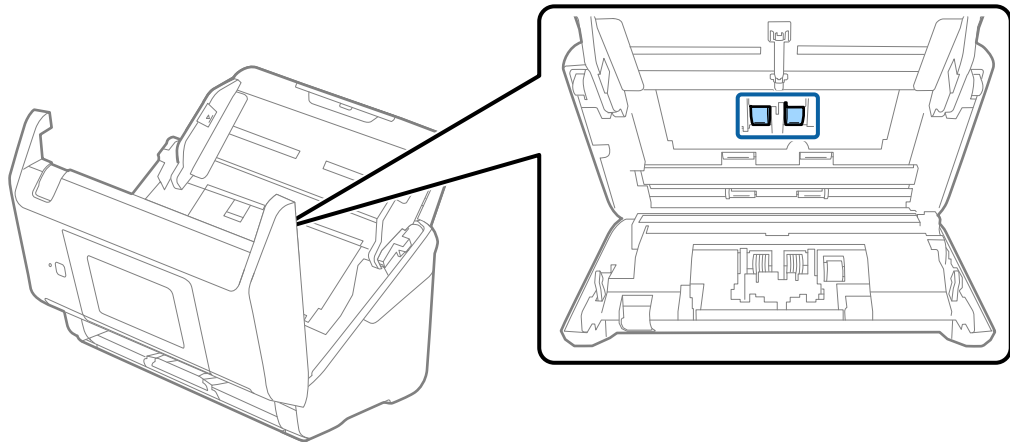
7. گرد و خاک یا آلودگی روی غلتک جداکننده را می‌توانید با کیت تمیز کننده اصل Epson یا دستمال نرم و مرطوب پاک کنید.



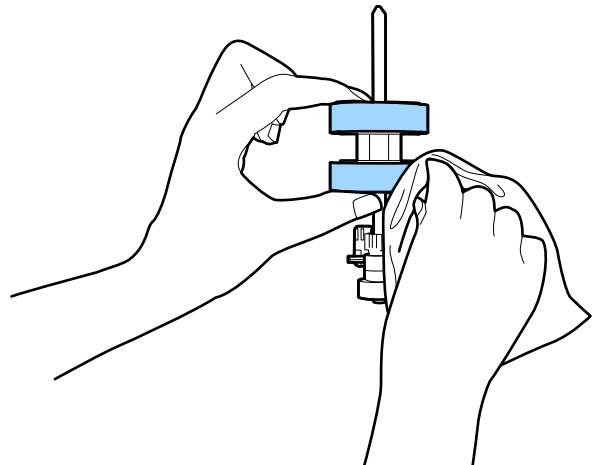
مهم:

برای تمیز کردن غلتک از کیت تمیز کننده اصل Epson یا دستمال نرم و مرطوب استفاده کنید. دستمال خشک ممکن است به سطح غلتک آسیب برساند.

8. قاب را باز کرده و غلتک بلندکننده را بیرون بیاورید.
برای کسب اطلاعات بیشتر به "تعویض کیت مجموعه غلتک" مراجعه کنید.



9. گرد و خاک یا آلودگی روی غلتک بلند کننده را می‌توانید با کیت تمیز کننده اصل Epson یا دستمال نرم و مرطوب پاک کنید.

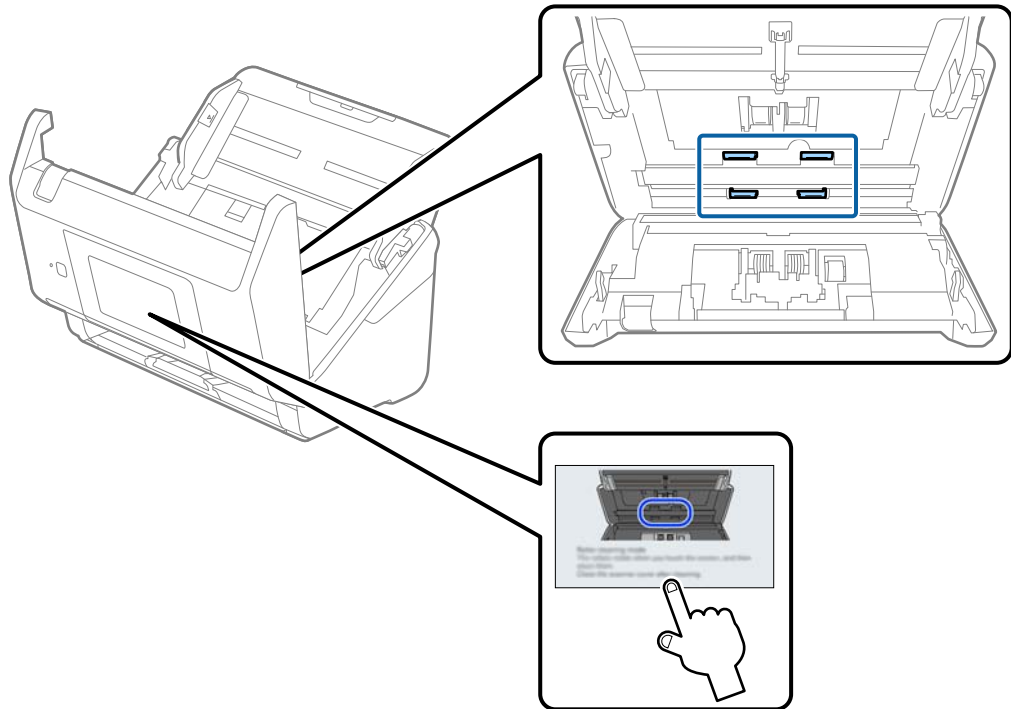


مهم!

برای تمیز کردن غلتک از کیت تمیز کننده اصل Epson یا دستمال نرم و مرطوب استفاده کنید. دستمال خشک ممکن است به سطح غلتک آسیب برساند.

10. قاب اسکنر را ببندید.
11. آداپتور AC را 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 تمیزکاری 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 کردن غلتک مراقب باشید دست‌ها یا موهای شما در قطعات گیر نکنند. ممکن است منجر به جراحت شود.

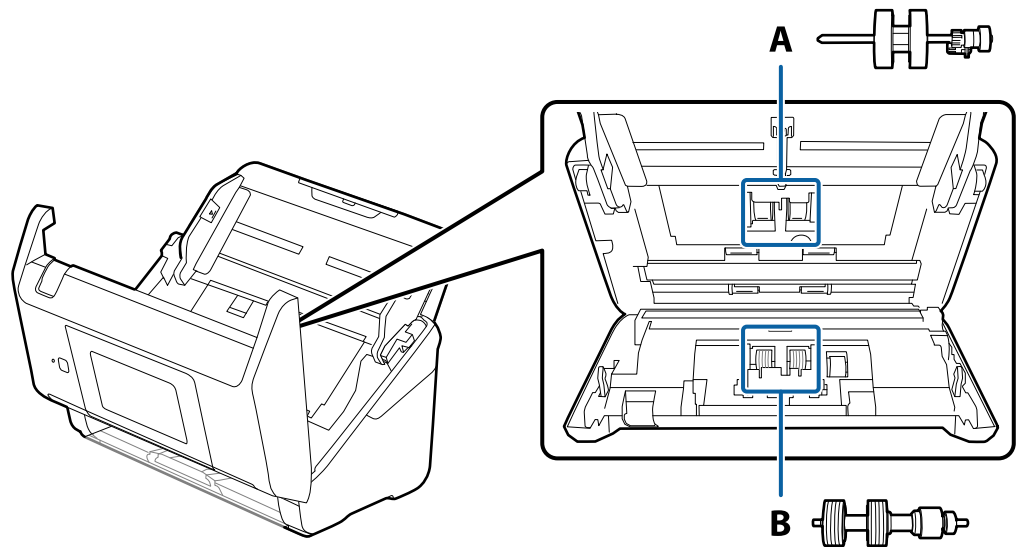
16. قاب اسکنر را ببندید.
اسکنر از حالت تمیزکاری غلتک خارج می‌شود.

اطلاعات مرتبط


← "تعویض کیت مجموعه غلتک" در صفحه 155

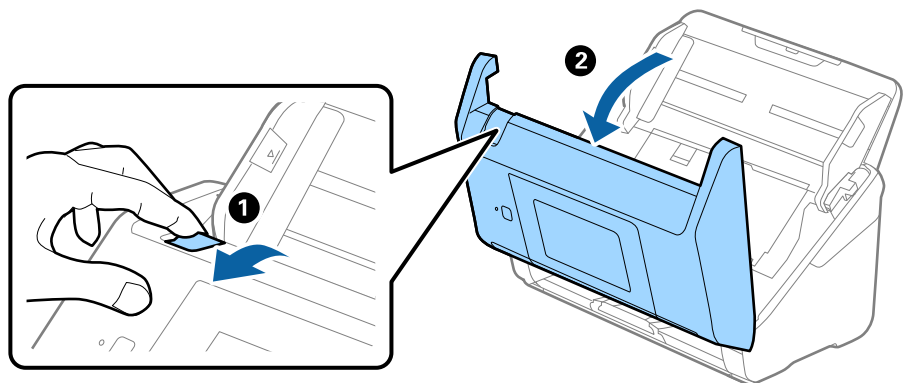
تعویض کیت مجموعه غلتک

هنگامی که 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.

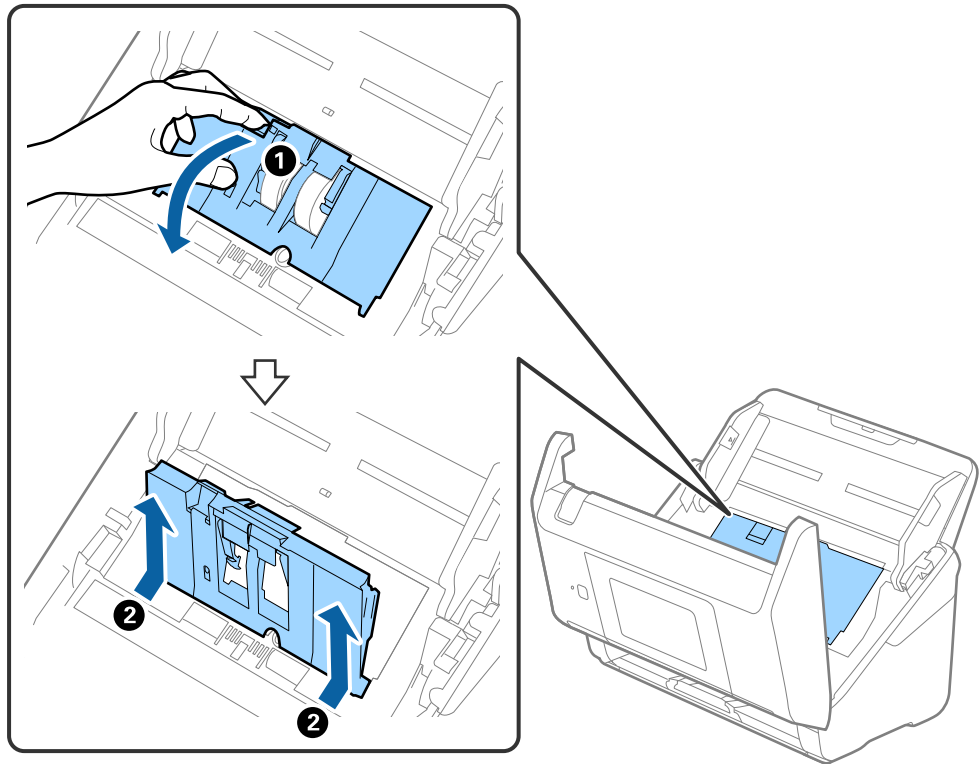


A: غلتک بلندکننده، B: غلتک جداکننده

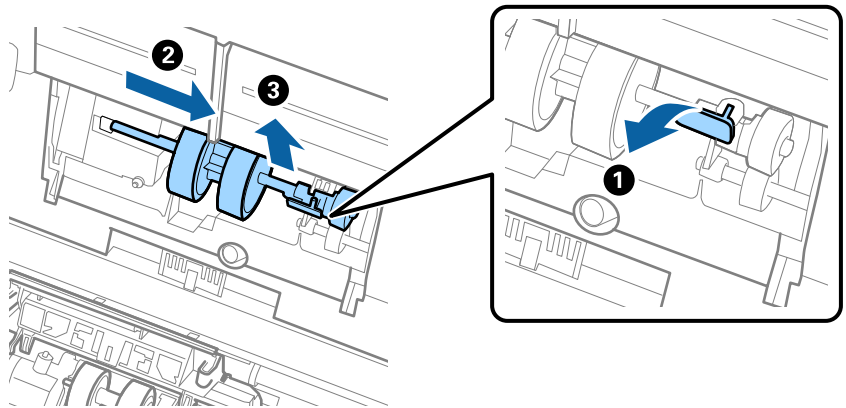
1. دکمه  را برای خاموش کردن اسکنر فشار دهید.
2. آداپتور AC را از اسکنر جدا کنید.
3. اهرم را بکشید و قاب اسکنر را باز کنید.



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



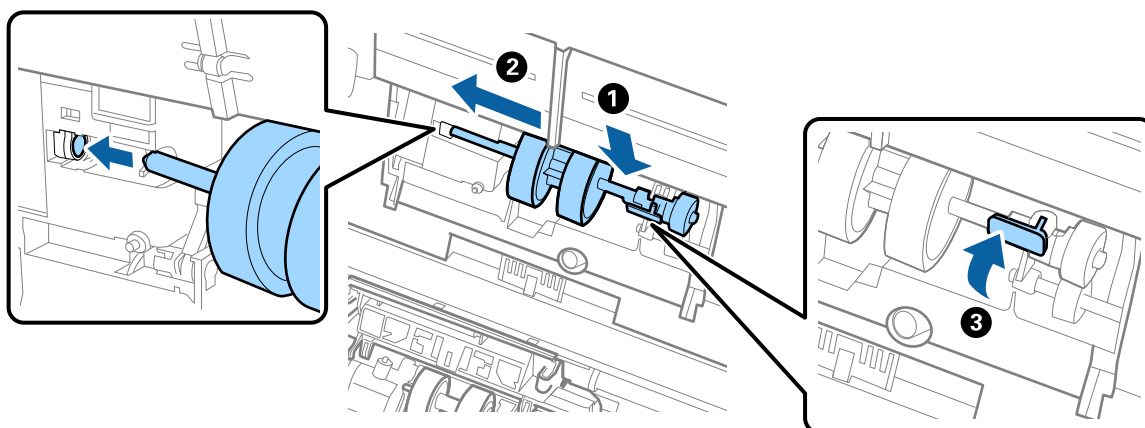
5. نگهدارنده محور غلتک را به سمت پایین بکشید و سپس غلتک‌های بلندکننده نصب شده را بلغزانید و خارج نمایید.



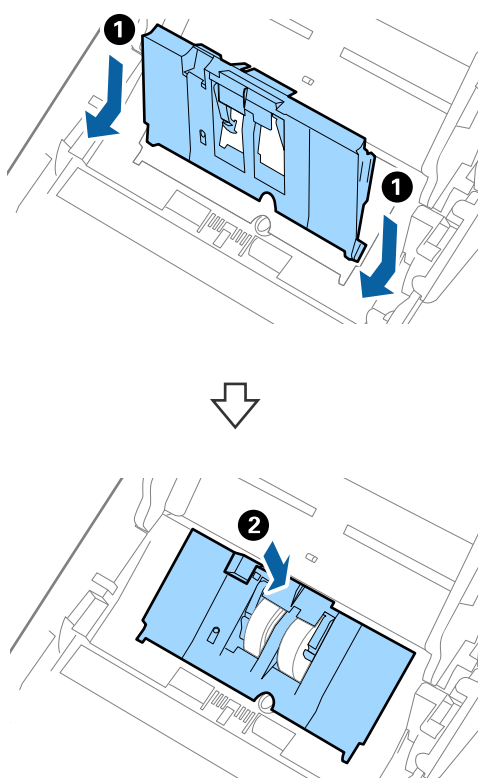
مهم!

غلتک بلندکننده را با فشار بیرون نکشید. این کار ممکن است به قسمت داخلی اسکرaper 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 اسکنر قرار دهید. نگهدارنده را فشار دهید تا محکم شود.

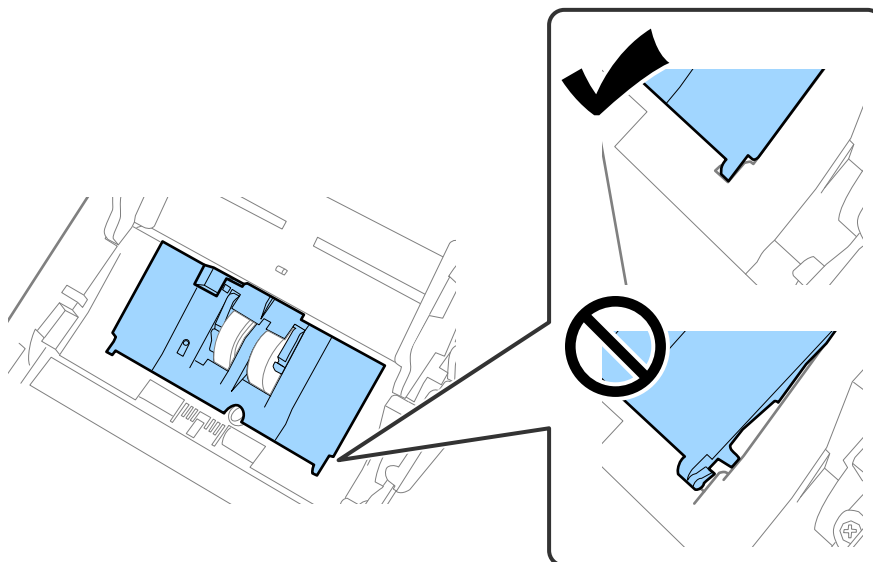


7. لبه روکش غلتک بلندکننده را داخل شیار قرار داده و بلغزانید. روکش را محکم ببندید.

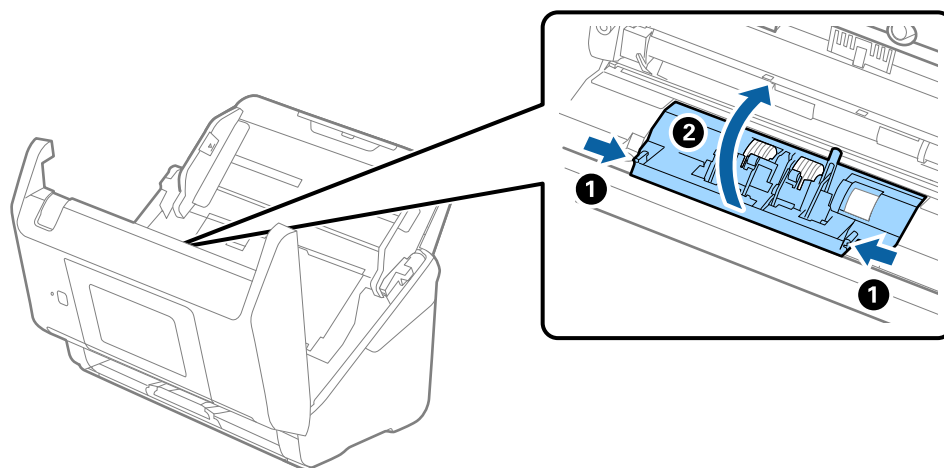


مهم!

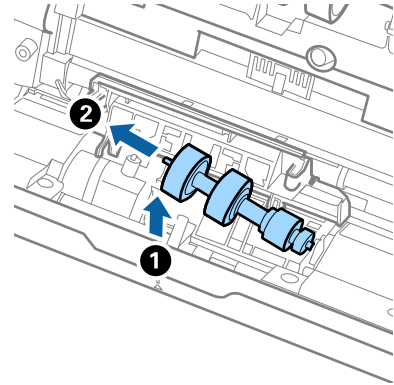
- ❑ اطمینان حاصل کنید که روکش بلندکننده به طور صحیح بسته شود.
- ❑ در صورتی که بستن روکش سخت است، اطمینان حاصل کنید که غلتک‌های بلندکننده به طور صحیح نصب شده باشند.
- ❑ در صورتی که روکش بلند شده است آن را نصب نکنید.



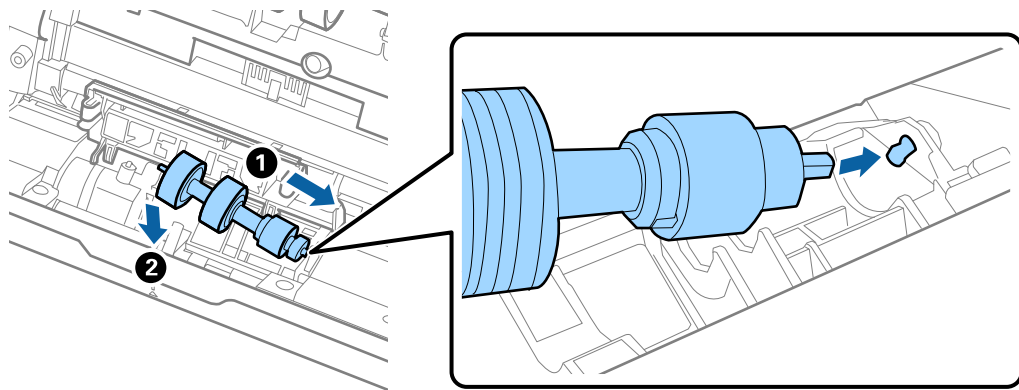
8. قلاب‌های دو طرف انتهایی روکش غلتک جداکننده را فشار دهید تا روکش باز شود.



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.

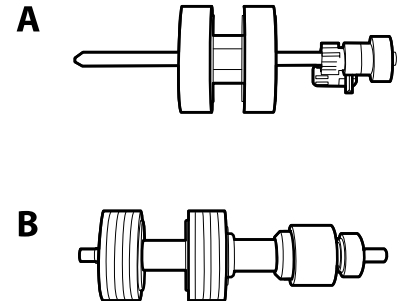
14. تعداد اسکن را می‌توانید در پانل کنترل بازنشانی کنید.

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

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



A: غلتک بلندکننده، B: غلتک جداکننده

چرخه عمر	کدها	نام قطعه
*000,200	B12B819671 B12B819681 (فقط هند)	کیت مجموعه غلتک

* 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 کیت مجموعه غلتک، تعداد اسکن‌ها را دوباره تنظیم می‌کند.

1. از صفحه اصلی، تنظیم < اطلاعات دستگاه > بازنشانی تعداد اسکن‌ها < تعداد اسکن‌ها بعد از تعویض غلطک را انتخاب کنید.
2. روی بله ضربه بزنید.

اطلاعات مرتبط

← "تعویض کیت مجموعه غلتک" در صفحه 155

صرفه جویی در مصرف برق

هنگامی که هیچ عملیاتی توسط اسکنر اجرا نمی‌شود، با استفاده از حالت خواب یا خاموشی خودکار می‌توانید در مصرف برق صرفه جویی کنید. مدت زمانی که طول می‌کشد تا اسکنر وارد حالت خواب شود یا به صورت خودکار خاموش گردد را می‌توانید تنظیم کنید. هر گونه افزایش، روی بهره‌وری انرژی محصول تاثیر می‌گذارد. قبل از هر تغییری، محیط را در نظر بگیرید.


1. تنظیم را در صفحه اصلی انتخاب کنید.

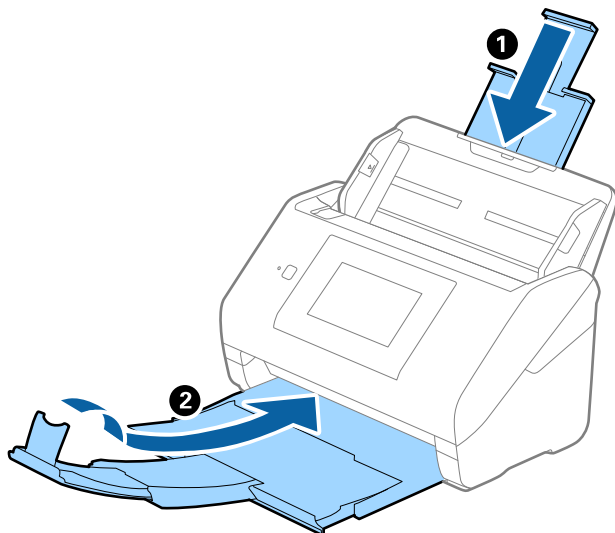
2. تنظیمات اصلی را انتخاب کنید.

3. تنظیم خاموش کردن را انتخاب کرده و تنظیمات را انجام دهید.
 نکته:
 ویژگی های موجود با توجه به محل خرید ممکن است متفاوت باشد.

حمل و نقل اسکنر

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

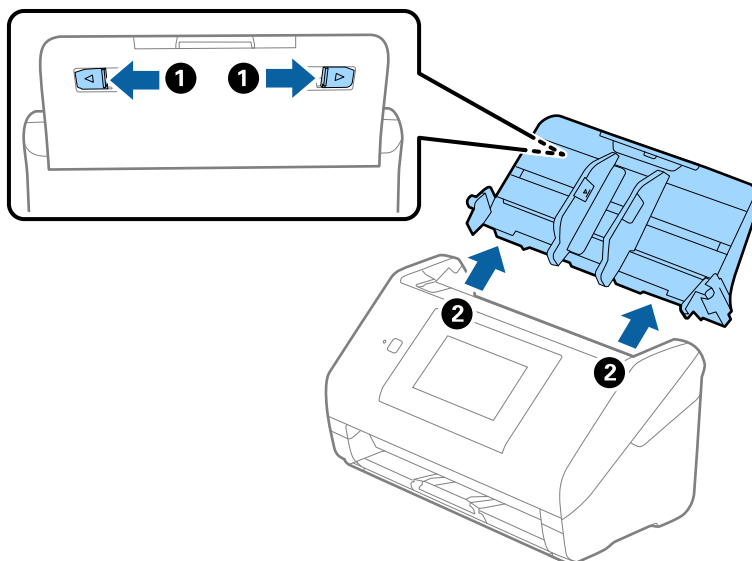
1. دکمه  را برای خاموش کردن اسکنر فشار دهید.
2. آداپتور برق متناوب را جدا کنید.
3. کابلها و دستگاهها را جدا کنید.
4. رابط سینی ورودی و سینی خروجی را ببندید.



مهم! 

اطمینان حاصل کنید که سینی خروجی به طور محکم بسته باشد؛ در غیر این صورت 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 تکیه 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 اسکتر 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 اسکتر تعویضی فقط از مقادیر انتخاب شده استفاده کنید.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

وارد کردن تنظیمات

فایل استخراج شده Web Config را وارد اسکتر کنید.

مهم: 

هنگام وارد کردن مقادیری که شامل اطلاعات شخصی از قبیل نام اسکتر 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 اسکتر اعمال می‌شوند.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

بازگرداندن تنظیمات اولیه

در پانل کنترل، مسیر **تنظیم < سرپرست سیستم < بازگرداندن تنظیمات اولیه** را انتخاب کنید و سپس موارد مورد نظر برای بازگرداندن به تنظیمات پیش فرض 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.



اگر گزینه همه تنظیمات را انتخاب و اجرا کنید، همه داده های تنظیمات ثبت شده در اسکر شامل مخاطبین و تنظیمات کاربری تأیید هویت حذف خواهند شد. تنظیمات حذف شده قابل بازیابی نیستند.

به روزرسانی برنامه ها و میان افزار

ممکن است با به روزرسانی برنامه ها 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 برنامه ها و سیستم عامل استفاده می کنید.



در حین به روزرسانی کامپیوتر یا اسکر را خاموش نکنید.

نکته:

وقتی اسکر 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 اسکر 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 روزرسانی کنید.

نکته:

از سیستم عامل های *Windows Server* پشتیبانی نمی شود.

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 < برنامه ها < Epson Software < EPSON Software Updater* را انتخاب کنید.

نکته:

اگر برنامه مورد نظر برای بروزرسانی را در لیست برنامه ها پیدا نمی کنید، می توانید با استفاده از *EPSON Software Updater* بروزرسانی کنید. وجود جدیدترین نسخه برنامه ها را در وب سایت *Epson* مربوط به کشور خود بررسی کنید.

<http://www.epson.com>

بروزرسانی ثابت افزار اسکر با استفاده از پانل کنترل

اگر اسکر امکان اتصال به اینترنت را دارد، ثابت افزار اسکر را می توانید از طریق پانل کنترل بروزرسانی کنید. همچنین می توانید اسکر را طوری تنظیم کنید که به طور منظم بروزرسانی های ثابت افزار را بررسی کرده و در صورت وجود، به شما اطلاع دهد.

1. در صفحه اصلی، تنظیم را انتخاب کنید.

- مسیر سرپرست سیستم < به روز رسانی میان افزار > به روز رسانی را انتخاب کنید.
نکته:
برای تنظیم اسکتز به طوری که به روزرسانی های ثابت افزار را به طور منظم بررسی کند، اعلامیه < On > را انتخاب کنید.
- پیام روی صفحه را بررسی کنید تا جستجوی به روزرسانی های موجود آغاز شود.
- اگر پیامی روی صفحه LCD نمایش داده شد مبنی بر اینکه به روزرسانی نرم افزار داخلی موجود است، دستورالعمل های روی صفحه را دنبال کنید تا به روزرسانی شروع شود.

مهم!

تا پایان به روزرسانی، اسکتز را خاموش نکرده یا آن را از پریز برق نکشید؛ در غیر این صورت ممکن است اسکتز دچار ایراد عملکردی شود.

اگر به روزرسانی نرم افزار داخلی به اتمام نرسید یا ناموفق بود، اسکتز به صورت عادی شروع نمی کند و دفعه بعد که اسکتز روشن می شود، «Recovery Mode» روی صفحه LCD نمایش داده می شود. در این وضعیت، باید دوباره ثابت افزار را با استفاده از رایانه به روزرسانی کنید. اسکتز را توسط یک کابل USB به یک رایانه متصل کنید. در حالی که «Recovery Mode» در اسکتز نشان داده شده است، نمی توانید ثابت افزار را از طریق اتصال شبکه به روزرسانی کنید. در رایانه، به وبسایت Epson محلی خود وارد شوید و سپس جدیدترین ثابت افزار اسکتز را دانلود نمایید. برای اطلاع از مراحل بعدی، به دستورالعمل های ارائه شده در وبسایت مراجعه کنید.

به روزرسانی ثابت افزار از طریق Web Config

وقتی اسکتز امکان اتصال به اینترنت را دارد، می توانید ثابت افزار را از طریق Web Config به روز کنید.

- وارد Web Config شوید و زبانه **Device Management < Firmware Update** را انتخاب کنید.
- روی گزینه **Start** کلیک کنید و سپس دستورالعمل های روی صفحه را دنبال کنید.
فرآیند تأیید ثابت افزار آغاز می شود و در صورت وجود ثابت افزار به روز شده، اطلاعات مربوط به آن نمایش داده می شود.

نکته:

به روز رسانی ثابت افزار با استفاده از *Epson Device Admin* نیز امکان پذیر است. اطلاعات ثابت افزار را می توانید در لیست دستگاه ها مشاهده کنید. این امر زمانی سودمند است که در نظر داشته باشید چند ثابت افزار دستگاه را به روز کنید. برای کسب اطلاعات بیشتر به راهنمای *Epson Device Admin* مراجعه کنید.

اطلاعات مرتبط

◀ "اجرای Web Config در مرورگر وب" در صفحه 35

به روزرسانی ثابت افزار بدون اتصال به اینترنت

می توانید نرم افزار 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 به روز رسانی نرم افزار انجام بگیرد. اگر نتوانستید به روز رسانی را از طریق شبکه انجام دهید، این روش را امتحان کنید.

نکته:

قبل از به روزرسانی، مطمئن شوید در ایور اسکتز *Epson Scan 2* در رایانه شما نصب شده است. اگر *Epson Scan 2* نصب نیست، دوباره آن را نصب کنید.

- برای دسترسی به جدیدترین نسخه های به روزرسانی ثابت افزار به وبسایت Epson مراجعه کنید.

<http://www.epson.com>

- در صورتی که ثابت افزار مربوط به اسکنر شماست، آن را دانلود کنید و به مرحله بعدی بروید.
 - در صورتی که هیچ اطلاعات ثابت افزاری در وبسایت وجود ندارد، شما قبلاً از جدیدترین ثابت افزار استفاده می کنید.
2. رایانه حاوی ثابت افزار 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 راه اندازی می شود.
 4. دستورالعمل های روی صفحه را دنبال کنید.