EPSON
EXCEED YOUR VISION

راهنمای سرپرست

NPD5668-00 FA

محتوا

محتوا

تنظیمات امنیتی پیشرفته مربوط به شرکت

حق نسخه‌برداری

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

علایم تجاری

- ❏ ®EPSON یک علامت تجاری ثبت شده است، و EPSON EXCEED YOUR VISION یا EXCEED YOUR VISION علامت تجاری شرکت Seiko Epson است.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ اطلاعیه عمومی: سایر نام های محصول که در اینجا استفاده می شود فقط برای اهداف شناسایی بوده و ممکن است علامت های تجاری مالکان مربوطه آنها باشند. Epson حقوق مربوط به این مارک ها را از خود سلب می کند.

درباره این دفترچه راهنما

علامت ها و نمادها

!احتیاط:
دستورالعمل هایی که باید با دقت رعایت شوند تا از آسیب های بدنی اجتناب شود.

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

نکته:
دستورالعمل هایی که نکات مفید و محدودیت هایی برای عملکرد اسکنر دارند.

اطلاعات مرتبط
کلیک بر روی این نماد شما را به اطلاعات مربوطه می برد.

توضیحات استفاده شده در این دفترچه راهنما

- تصاویر گرفته شده از درایور اسکنر و صفحات Epson Scan 2 (درایور اسکن) از Windows 10 یا OS X El Capitan هستند. محتوای نشان داده شده در صفحات بسته به مدل و موقعیت متفاوت هستند.
- تصاویر استفاده شده در این دفترچه راهنما فقط مثال هستند. ممکن است بسته به مدل تفاوت های جزئی وجود داشته باشد، ولی روش راه اندازی مشابه است.
- برخی از موارد منو ی روی صفحه LCD بسته به مدل و تنظیمات متفاوت است.

مراجع سیستم عامل

Windows

در این دفترچه راهنما، اصطلاحاتی مانند "Windows 10"، "Windows 8.1"، "Windows 8"، "Windows 7"، "Windows Vista"، "Windows XP"، Windows Server 2016، "Windows Server 2012 R2"، "Windows Server 2012"، "Windows Server 2008 R2"، "Windows Server 2008"، "Windows Server 2003 R2" و "Windows Server 2003" به سیستم‌های عامل زیر اشاره می‌کند. به علاوه "Windows" برای رجوع به تمامی نسخه ها استفاده شده است.

- 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 Vista®

درباره این دفترچه راهنما

- ❑ سیستم عامل Microsoft® Windows® XP
- ❑ سیستم عامل Microsoft® Windows® XP Professional x64 Edition
- ❑ سیستم عامل Microsoft® Windows Server® 2016
- ❑ سیستم عامل Microsoft® Windows Server® 2012 R2
- ❑ سیستم عامل Microsoft® Windows Server® 2012
- ❑ سیستم عامل Microsoft® Windows Server® 2008 R2
- ❑ سیستم عامل Microsoft® Windows Server® 2008
- ❑ سیستم عامل Microsoft® Windows Server® 2003 R2
- ❑ سیستم عامل Microsoft® Windows Server® 2003

Mac OS

در این راهنما، از "Mac OS" برای اشاره به macOS Sierra، OS X El Capitan، OS X Yosemite، OS X Mavericks، OS X Mountain Lion, Mac OS X v10.7.x و Mac OS X v10.6.8 استفاده می‌شود.

مقدمه

جزء راهنما

این راهنما برای سرپرست دستگاه که مسئول ایجاد ارتباط چاپگر یا اسکنر با شبکه است در نظر گرفته شده و حاوی اطلاعاتی درباره روش اعمال تنظیمات برای استفاده از عملکردهاست.

برای آشنا شدن با روش استفاده از عملکردها به راهنماي کاربر مراجعه کنید.

آماده‌سازی

وظایف سرپرست، روش تنظیم دستگاه‌ها و نرم‌افزار مدیریت را شرح می‌دهد.

اتصال

روش اتصال دستگاه به شبکه یا خط تلفن را شرح می‌دهد. محیط شبکه، مانند استفاده از درگاه برای دستگاه، سرور DNS و اطلاعات سرور پروکسی را شرح می‌دهد.

تنظیمات عملکرد

تنظیمات مربوط به تک‌تک عملکردها را شرح می‌دهد.

تنظیمات امنیتی ابتدایی

تنظیمات هر عملکرد مانند چاپ، اسکن و نمابر را شرح می‌دهد.

تنظیمات بهره‌برداری و مدیریت

عملیات پس از شروع استفاده از دستگاه‌ها، مانند بررسی اطلاعات و نگهداری را شرح می‌دهد.

رفع مشکلات

مقداردهی اولیه تنظیمات و عیب‌یابی شبکه را شرح می‌دهد.

تنظیمات امنیتی پیشرفته مربوط به شرکت

روش تقویت امنیت دستگاه، مانند استفاده از گواهی CA، ارتباط SSL/TLS و IPsec/فیلترینگ IP را شرح می‌دهد.

بسته به مدل، برخی عملکردهای این فصل پشتیبانی نمی‌شود.

تعریف اصطلاحات استفاده شده در این دفترچه راهنما

اصطلاحات زیر در این دفترچه راهنما استفاده شده است.

سرپرست

فرد مسئول نصب و تنظیم دستگاه یا شبکه در دفتر یا سازمان. در سازمان‌های کوچک، این فرد ممکن است سرپرستی دستگاه و شبکه را همزمان بر عهده داشته باشد. در سازمان‌های بزرگ، سرپرست مسئول شبکه یا دستگاه‌های گروه بخشی است و سرپرست شبکه مسئول تنظیمات ارتباطی بیرون از سازمان، مانند اینترنت، است.

مقدمه

سرپرست شبکه

فرد مسئول نظارت بر ارتباطات شبکه. فردی که روتر، سرور پروکسی، سرور DNS و سرور ایمیل را برای پایش ارتباطات اینترنت یا شبکه تنظیم می‌کند.

کاربر

فردی که از دستگاه‌هایی مانند چاپگر یا اسکنر استفاده می‌کند.

Web Config (صفحه وب دستگاه)

سرور وب که درون دستگاه جای گرفته است. این سرور Web Config نامیده می‌شود. می‌توانید وضعیت دستگاه را با مرورگر بررسی کنید و تغییر دهید.

ابزار

عبارتی کلی برای نرم‌افزار تنظیم یا مدیریت دستگاه، مانند Epson Device Admin، EpsonNet Config، EpsonNet SetupManager و...

اسکن لحظه‌ای

عبارتی کلی برای اسکن کردن از پانل کنترل دستگاه.

اسکی (کد استاندارد آمریکا برای تبادل اطلاعات)

یکی از کدهای استاندارد نویسه. 128 نویسه تعریف می‌شود، از جمله نویسه‌های الفبایی (a–z، A–Z)، اعداد عربی (0–9)، نمادها، نویسه‌های خالی و نویسه‌های کنترلی. کاربرد "اسکی" در این راهنما به معنای 0x20–0x7E (عدد هگزادسیمال) زیر است و نویسه‌های کنترلی را شامل نمی‌شود.

*SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* نویسه فاصله.

یونیکد (UTF-8)

کد بین‌المللی استاندارد که زبان‌های بزرگ جهان را پوشش می‌دهد. UTF-8 در این راهنما به معنای نویسه‌های رمزگذاری در قالب UTF-8 است.

آماده‌سازی

این فصل نقش سرپرست و آماده‌سازی را پیش از اعمال تنظیمات شرح می‌دهد.

جریان تنظیمات و مدیریت اسکنر

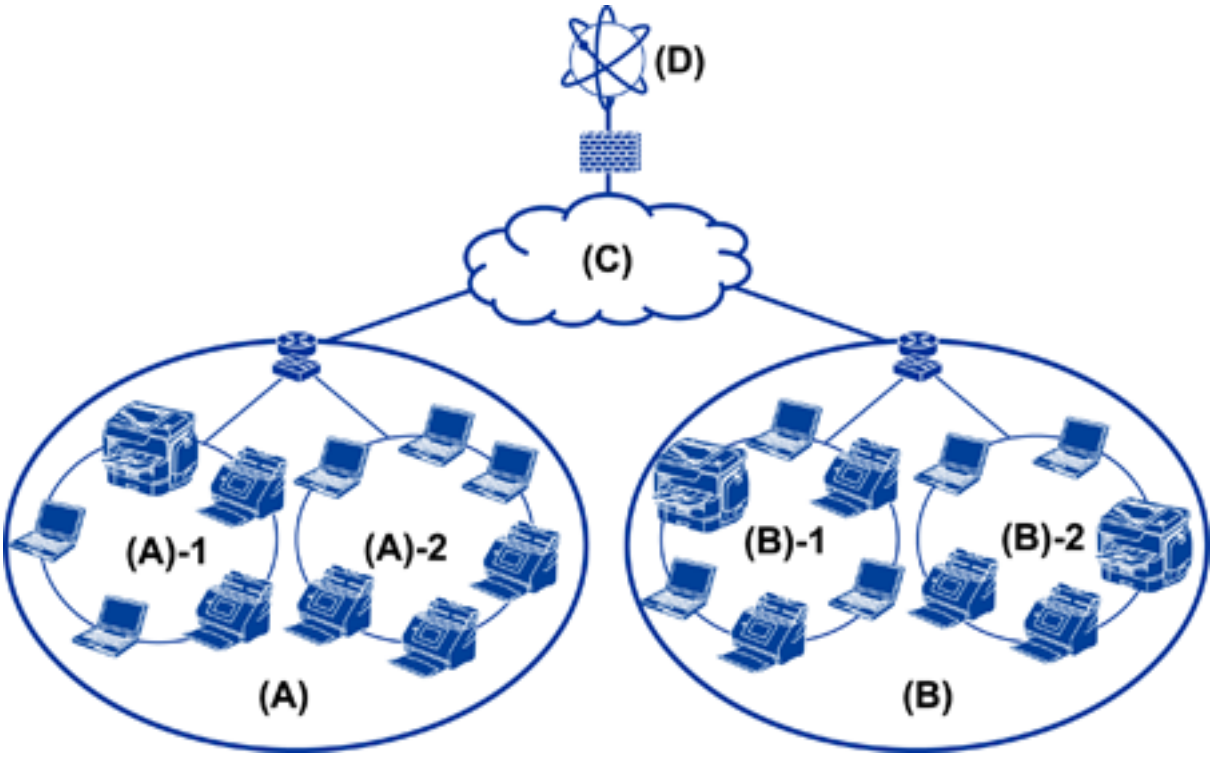
برای این که چاپگر یا اسکنر در اختیار کاربران قرار بگیرد، سرپرست باید تنظیمات اتصال شبکه را اعمال کند و راه‌اندازی و نگهداری اولیه اسکنر را انجام دهد.

1. آماده‌سازی
   - ❑ جمع‌آوری اطلاعات تنظیم اتصال
   - ❑ تصمیم‌گیری درباره روش اتصال
2. اتصال
   - ❑ اتصال شبکه از پانل کنترل اسکنر
3. راه‌اندازی عملکردها
   - ❑ تنظیمات درایور اسکنر
   - ❑ دیگر تنظیمات پیشرفته
4. تنظیمات امنیت
   - ❑ تنظیمات سرپرست
   - ❑ SSL/TLS
   - ❑ کنترل پروتکل
   - ❑ تنظیمات پیشرفته امنیت (اختیاری)
5. بهره‌برداری و مدیریت
   - ❑ بررسی وضعیت دستگاه
   - ❑ رسیدگی به رویدادها
   - ❑ پشتیبان‌گیری از تنظیمات دستگاه

اطلاعات مرتبط

- "آماده‌سازی" در صفحه 10
- "اتصال" در صفحه 15
- "تنظیمات عملکرد" در صفحه 21
- "تنظیمات امنیتی ابتدایی" در صفحه 31
- "تنظیمات بهره‌برداری و مدیریت" در صفحه 39

مثال محیط شبکه



(A): دفتر 1

- (A: LAN 1) – 1)
- (A: LAN 2) – 2)

(B): دفتر 2

- (B: LAN 1) – 1)
- (B: LAN 2) – 2)

(C): WAN

(D): اینترنت

مثال تنظیم اتصال اسکنر

بسته به روش استفاده از اسکنر دو نوع اتصال وجود دارد. هر دو روش اسکنر را با رایانه از طریق هاب به شبکه متصل می‌کنند.

- اتصال سرور/مشتری (اسکنر استفاده کننده از سرور Windows، مدیریت کار)
- اتصال همتا به همتا (اتصال مستقیم با رایانه مشتری)

اطلاعات مرتبط

- "اتصال سرور/مشتری" در صفحه 12
- "اتصال همتا به همتا" در صفحه 12

اتصال سرور/مشتری

مدیریت اسکنر و کار را با Document Capture Pro Server نصب شده بر روی سرور متمرکز کنید. برای کار شامل چندین اسکنر بهتر است تعداد فراوانی سند را در قالب معین اسکن کنید.

اطلاعات مرتبط

"تعریف اصطلاحات استفاده شده در این دفترچه راهنما" در صفحه 8

اتصال همتا به همتا

از اسکنر مستقل با درایور اسکنر مانند Epson Scan 2 نصب شده بر روی رایانه مشتری استفاده کنید. نصب کردن Document Capture Pro (Document Capture) بر روی رایانه مشتری امکان اجرای کارها در رایانه‌های مشتری اسکنر را فراهم می‌کند.

اطلاعات مرتبط

"تعریف اصطلاحات استفاده شده در این دفترچه راهنما" در صفحه 8

آماده‌سازی اتصال شبکه

جمع‌آوری اطلاعات درباره تنظیم اتصال

برای اتصال شبکه به نشانی IP، نشانی دروازه و... نیاز دارید. موارد زیر را پیشاپیش بررسی کنید.

بخشها	موارد	توجه
روش اتصال دستگاه	❑ اترنت	برای اتصال اترنت از کابل رده 5e یا بالاتر STP (جفت تابیده غلاف‌دار) استفاده کنید.
اطلاعات اتصال LAN	❑ نشانی IP ❑ ماسک شبکه فرعی ❑ دروازه پیش فرض	اگر نشانی IP را به طور خودکار با عملکرد DHCP روتر تنظیم کرده‌اید، این مورد ضروری نیست.
اطلاعات سرور DNS	❑ نشانی IP مربوط به DNS اصلی ❑ نشانی IP مربوط به DNS فرعی	اگر از نشانی IP ثابت به عنوان نشانی IP استفاده می‌کنید، سرور DNS را پیکربندی کنید. مشخص کنید که چه زمانی باید تخصیص به صورت خودکار با عملکرد DHCP انجام بگیرد و چه زمانی سرور DNS را نمی‌توان به طور خودکار تخصیص داد.
اطلاعات سرور پروکسی	❑ نام سرور پروکسی ❑ شماره درگاه	مشخص کنید که چه زمانی از سرور پروکسی برای اتصال اینترنت استفاده شود و چه زمانی از سرویس Epson Connect یا عملکرد به‌روز رسانی خودکار نرم‌افزار استفاده شود.

مشخصات اسکنر

ویژگی که اسکنر از حالت استاندارد یا اتصال پشتیبانی می‌کند، به راهنمای کاربر مراجعه کنید.

استفاده از شماره پورت

برای مشاهده شماره پورت اسکنر به "پیوست" مراجعه کنید.

اطلاعات مرتبط

"استفاده از درگاه برای اسکنر" در صفحه 57

نوع تخصیص نشانی IP

دو روش برای تخصیص نشانی IP به اسکنر وجود دارد.

تخصیص IP ثابت:

نشانی IP اختصاصی از پیش تعیین شده را به اسکنر اختصاص دهید.

این نشانی IP حتی در صورت خاموش شدن اسکنر یا روتر تغییر نمی‌کند و شما می‌توانید دستگاه را با نشانی IP مدیریت کنید.

این نوع برای شبکه‌ای که اسکنرهای فراوانی به آن متصل است، مانند شرکت بزرگ یا مدرسه، مناسب است.

تخصیص خودکار با عملکرد DHCP:

پس از برقرار شدن ارتباط بین اسکنر و روتر دارای قابلیت DHCP، نشانی IP درست به طور خودکار تخصیص می‌یابد.

اگر تغییر دادن نشانی IP دستگاه خاصی دشوار باشد، باید نشانی IP را قبلاً رزرو کنید و سپس تخصیص دهید.

سرور DNS و سرور پروکسی

در صورت استفاده از سرویس اتصال اینترنت، سرور DNS را پیکربندی کنید. اگر آن را پیکربندی نکنید، باید نشانی IP را برای دسترسی مشخص کنید زیرا ممکن است نتوانید نام را تفکیک کنید.

سرور پروکسی در دروازه بین شبکه و اینترنت قرار می‌گیرد و با رایانه، اسکنر و اینترنت (سرور مخالف) از طرف تک‌تک آنها ارتباط برقرار می‌کند. سرور مخالف فقط با سرور پروکسی ارتباط برقرار می‌کند. از این رو، اطلاعات اسکنر مانند نشانی IP و شماره درگاه خوانده نمی‌شود و سطح امنیت بالاتر می‌رود.

با استفاده از قابلیت فیلترینگ می‌توانید دسترسی URL های خاص را ممنوع کنید، زیرا سرور پروکسی می‌تواند محتوای ارتباط را بررسی کند.

روش تنظیم اتصال شبکه

برای تنظیمات اتصال مربوط به نشانی IP، ماسک زیرشبکه و دروازه پیش‌فرض اسکنر به روش زیر عمل کنید.

استفاده از پانل کنترل:

تنظیمات را با پانل کنترل اسکنر پیکربندی کنید. پس از پیکربندی تنظیمات اتصال اسکنر به شبکه وصل شوید.

استفاده از برنامه نصب:

در صورت استفاده از برنامه نصب، شبکه اسکنر و رایانه مشتری به طور خودکار تنظیم می‌شود. تنظیم با پیروی از دستورالعمل‌های برنامه نصب صورت می‌گیرد، حتی اگر چندان با شبکه آشنا نباشید.

آماده‌سازی

استفاده از ابزار:

از ابزارهای رایانه سرپرست استفاده کنید. می‌توانید اسکنر را بیابید و تنظیم نمایید، یا فایل SYLK را برای ایجاد تنظیمات دسته‌ای در اسکنرها بسازید. می‌توانید چندین اسکنر را تنظیم کنید، به شرطی که همه آنها با کابل اترنت به شبکه متصل باشند. از این رو، این زمانی پیشنهاد می‌شود که بتوانید یک شبکه اترنت برای تنظیم بسازید.

اطلاعات مرتبط

- "اتصال به شبکه از پانل کنترل" در صفحه 15
- "اتصال به شبکه با استفاده از برنامه نصب" در صفحه 19
- "تخصیص نشانی IP با استفاده از EpsonNet Config" در صفحه 53

اتصال

این فصل محیط یا روال اتصال اسکنر به شبکه را شرح می‌دهد.

اتصال به شبکه

اتصال به شبکه از پانل کنترل

اسکنر را با استفاده از پانل کنترل اسکنر به شبکه وصل کنید.

توضیحات پانل کنترل اسکنر در راهنماي كاربر ارائه شده است.

تخصیص نشانی IP

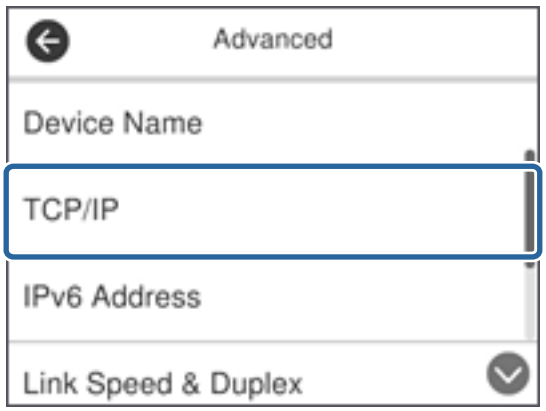
گزینه‌های ابتدایی مانند نشانی IP, ماسک زیرشبکه و دروازه پیش‌فرض را تنظیم کنید.

1. اسکنر را روشن کنید.
2. از قسمت چپ پانل کنترل اسکنر بر روی **تنظیم** تلنگر بزنید.

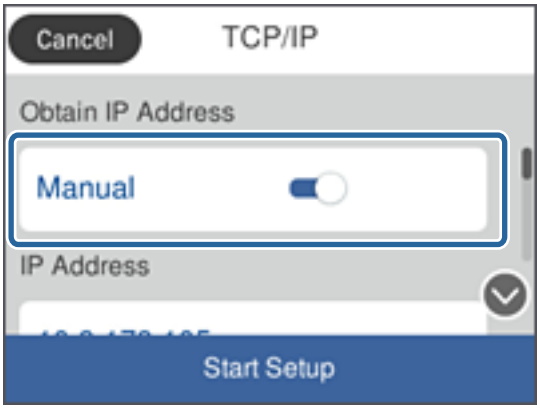
3. روی **تنظیمات شبکه** > **تغییر تنظیمات** تلنگر بزنید.

اگر گزینه نشان داده نمی‌شود، به بالای صفحه بروید و آن را نشان دهید.

4. روی **TCP/IP** ضربه بزنید.

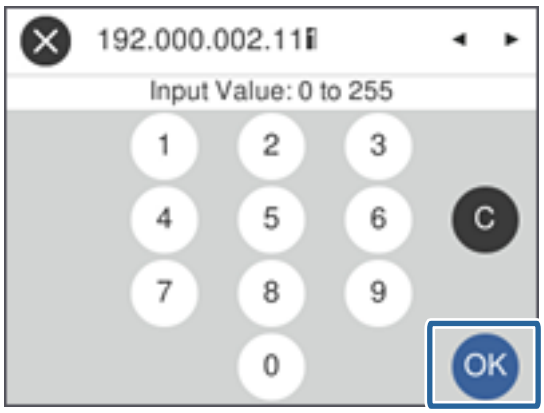


5. گزینه **دستی** را برای **بدست آوردن آدرس IP** انتخاب کنید.



نکته:
اگر نشانی *IP* را با عملکرد *DHCP* به طور خودکار تنظیم کرده باشید، باید **خودکار** را انتخاب کنید. در این صورت، **نشانی *IP***، **ماسک زیرشبکه**، و **دروازه پیش‌فرض** در مراحل *6* تا *7* نیز به طور خودکار تنظیم می‌شود و باید به مرحله *8* بروید.

6. بر روی **نشانی IP** تلنگر بزنید، نشانی IP را با صفحه کلید روی صفحه وارد کنید و بر روی **تایید** تلنگر بزنید.



مقدار نشان داده شده در صفحه قبل را تایید کنید.

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

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

8. بر روی **DNS اولیه** مربوط به **سرور DNS** تلنگر بزنید، نشانی IP سرور DNS اصلی را با صفحه کلید روی صفحه وارد کنید و بر روی **تأیید** تلنگر بزنید.

   مقدار نشان داده شده در صفحه قبل را تایید کنید.

   نکته:
   اگر **خودکار** را برای تنظیمات تخصیص *IP* انتخاب کنید، می‌توانید تنظیمات سرور *DNS* را از **دستی** یا **خودکار** انتخاب کنید. اگر نتوانید نشانی سرور *DNS* را به طور خودکار دریافت کنید، باید **دستی** را انتخاب و نشانی سرور *DNS* را وارد کنید. سپس، نشانی سرور *DNS* فرعی را مستقیماً وارد کنید. اگر **خودکار** را انتخاب کرده‌اید، به مرحله *10* بروید.

9. بر روی **DNS ثانویه** تلنگر بزنید، نشانی IP سرور DNS فرعی را با صفحه کلید روی صفحه وارد کنید و بر روی **تأیید** تلنگر بزنید.

   مقدار نشان داده شده در صفحه قبل را تایید کنید.

10. روی **تنظیمات را شروع کنید** ضربه بزنید.

11. از صفحه تایید بر روی **بستن** تلنگر بزنید.

    اگر **بستن** را فشار ندهید، صفحه به طور خودکار و پس از مدت زمان مشخصی بسته می‌شود.

اتصال به اترنت

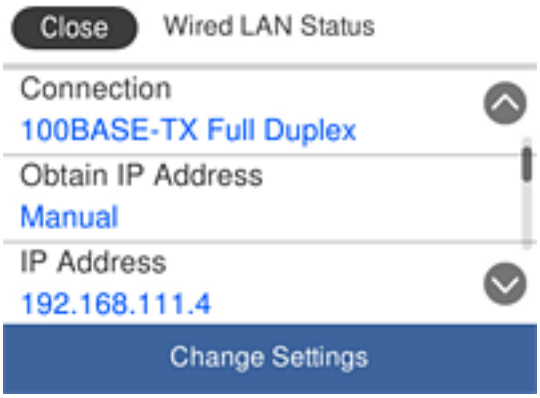
اسکنر را با استفاده از کابل اترنت به شبکه وصل کنید و اتصال را بررسی کنید.

1. اسکنر و هاب (سوییچ L2) را با کابل اترنت به هم وصل کنید.

   نماد روی صفحه به  تغییر می‌کند.

2. از صفحه اصلی، بر روی  تلنگر بزنید.

3. به بالای صفحه بروید و از درست بودن وضعیت اتصال و نشانی IP مطمئن شوید.



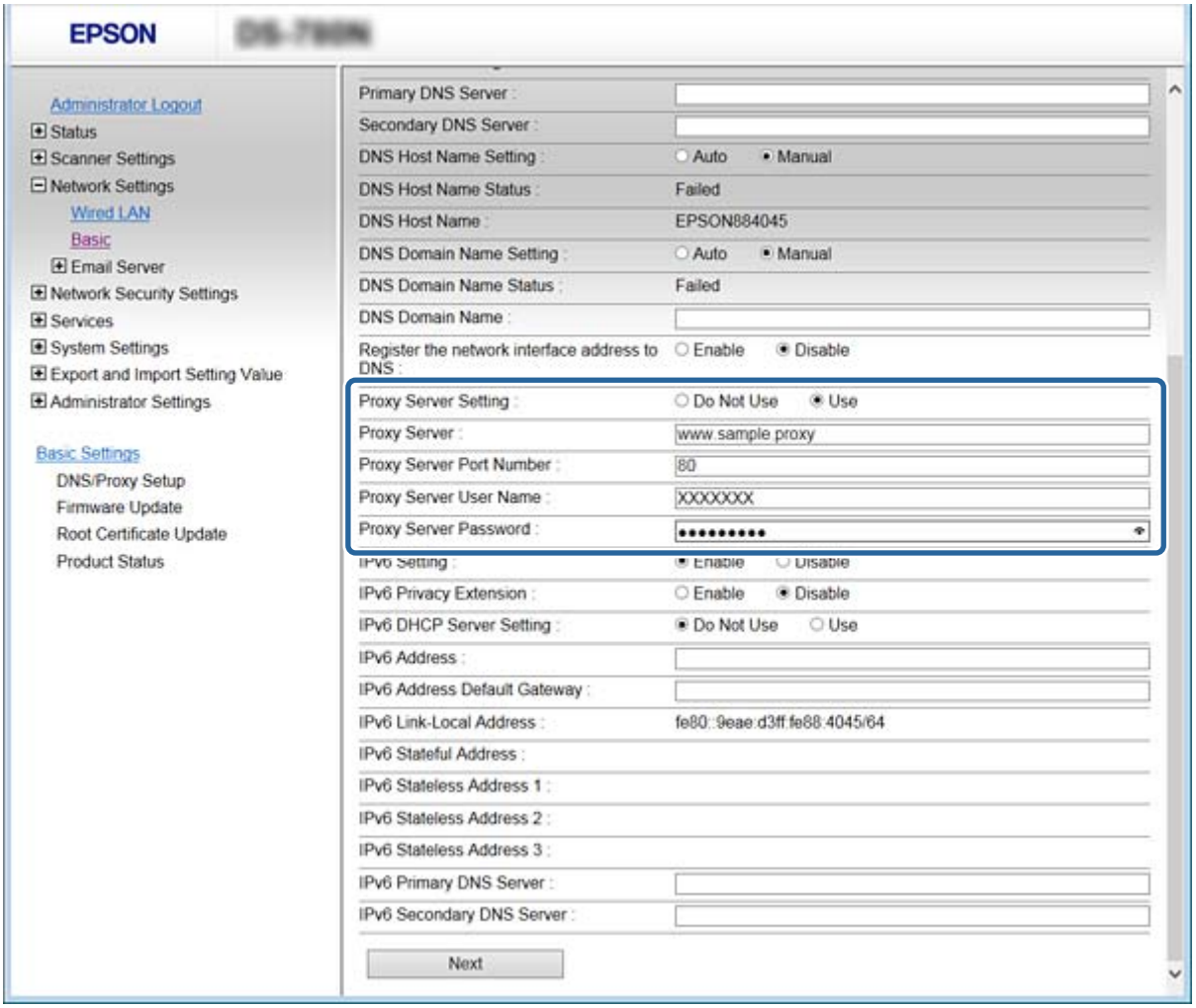
تنظیم سرور پروکسی

سرور پروکسی را نمی‌توان از روی پانل تنظیم کرد. با استفاده از Web Config پیکربندی کنید.

1. از قسمت Web Config گزینه **Network Settings** > **Basic** را انتخاب کنید.
2. **Use** را از **Proxy Server Setting** انتخاب کنید.
3. سرور پروکسی را با قالب نشانی IPv4 یا FQDN در **پروکسی سرور** مشخص کنید و شماره درگاه را در **Proxy Server Port Number** وارد کنید.

برای سرورهای پروکسی که نیازمند تایید هویت هستند، نام کاربر و گذرواژه تایید هویت سرور پروکسی را وارد کنید.

4. بر روی دکمه **Next** کلیک کنید.



5. تنظیمات را تایید کنید و بر روی **تنظیم** کلیک کنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

اتصال به شبکه با استفاده از برنامه نصب

برای وصل کردن اسکنر به رایانه بهتر است از برنامه نصب استفاده کنید. می‌توانید برنامه نصب را به یکی از روش‌های زیر اجرا کنید.

❑ راه‌اندازی از وب‌سایت

به وب سایت زیر دسترسی پیدا کنید و نام محصول را وارد نمایید. به **تنظیم** بروید و راه‌اندازی را آغاز کنید.

http://epson.sn

❑ راه‌اندازی از لوح فشرده (فقط برای مدل‌های دارای لوح فشرده و کاربرانی با رایانه دارای درایو لوح فشرده.)

لوح فشرده نرم‌افزار را در رایانه قرار دهید و سپس دستورالعمل‌های روی صفحه را دنبال کنید.

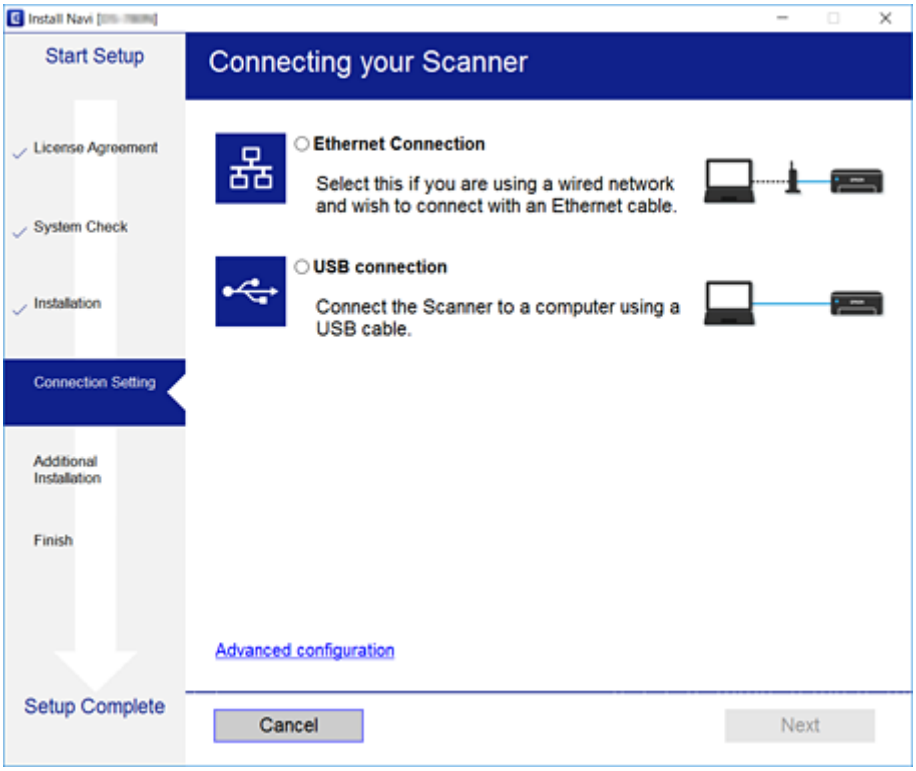
انتخاب روش اتصال

دستورالعمل‌های روی صفحه را دنبال کنید تا صفحه زیر ظاهر شود، سپس روش اتصال اسکنر به رایانه را انتخاب کنید.

اتصال

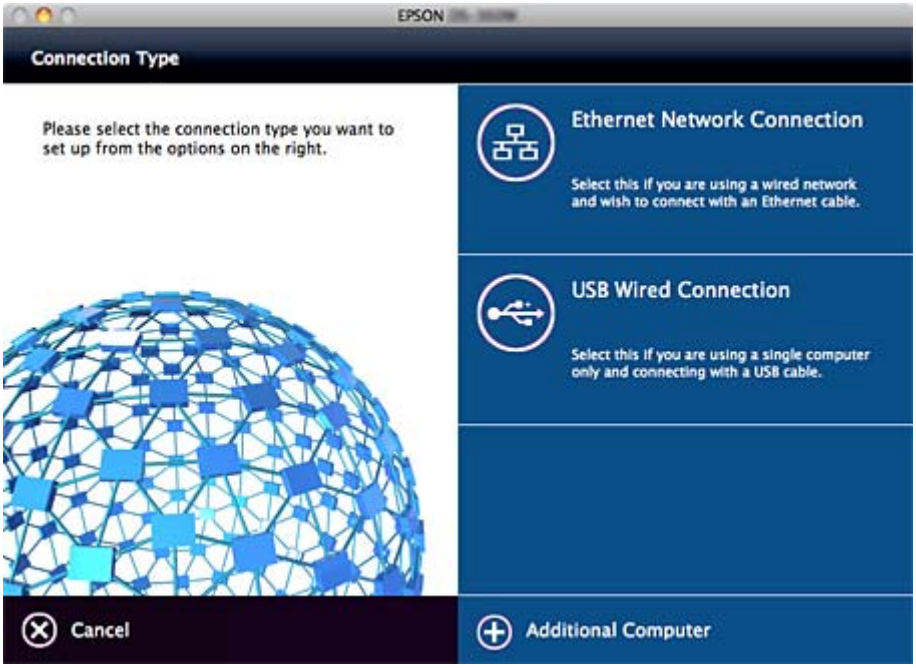
❑ Windows

نوع اتصال را انتخاب و بر روی **بعدی** کلیک کنید.



❑ Mac OS

نوع اتصال را انتخاب کنید.



دستورالعمل های روی صفحه را دنبال کنید. نرم‌افزار لازم نصب می‌شود.

تنظیمات عملکرد

این فصل نخستین تنظیماتی را که باید برای استفاده از عملکردهای دستگاه اعمال شود، شرح می‌دهد.

نرم‌افزار تنظیم

در این مبحث، روال‌های اعمال تنظیمات از رایانه سرپرست با استفاده از Web Config شرح داده می‌شود.

Web Config (صفحه وب دستگاه)

درباره Web Config

Web Config یک برنامه بر اساس مرورگر برای پیکربندی تنظیمات اسکنر است.

برای دسترسی به Web Config ابتدا باید یک آدرس IP به اسکنر اختصاص داده باشید.

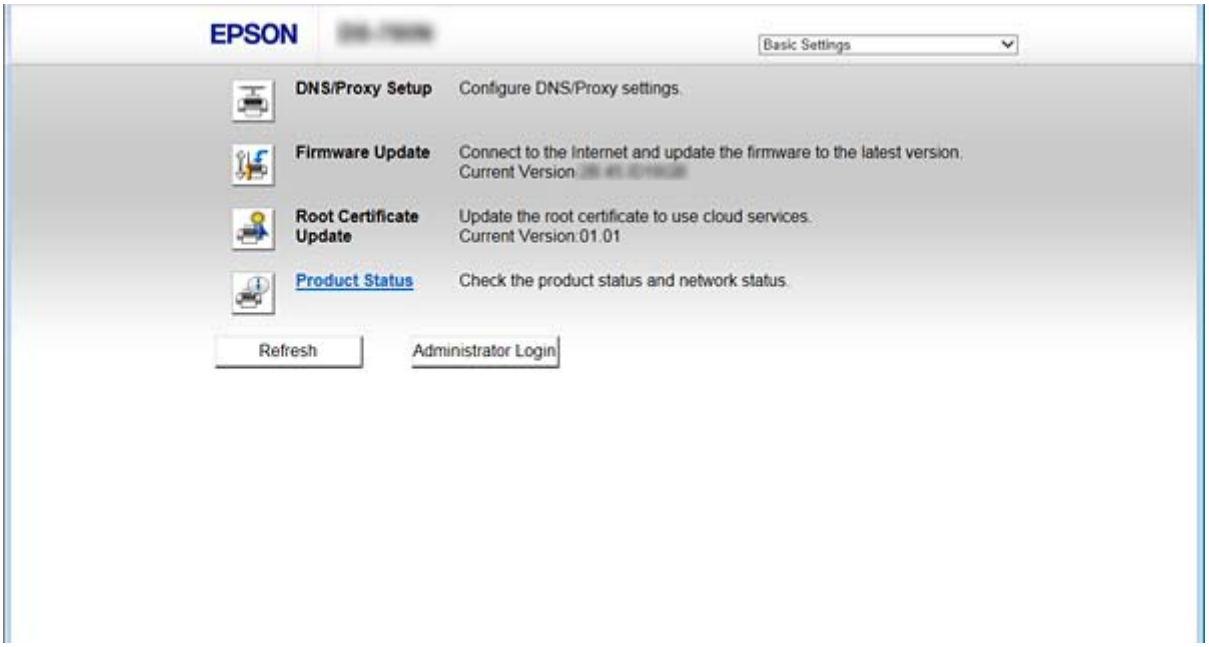
نکته:

می توانید با پیکربندی رمز عبور سرپرست برای اسکنر، تنظیمات را قفل کنید.

دو صفحه تنظیم به صورت زیر موجود است.

❑ **Basic Settings**

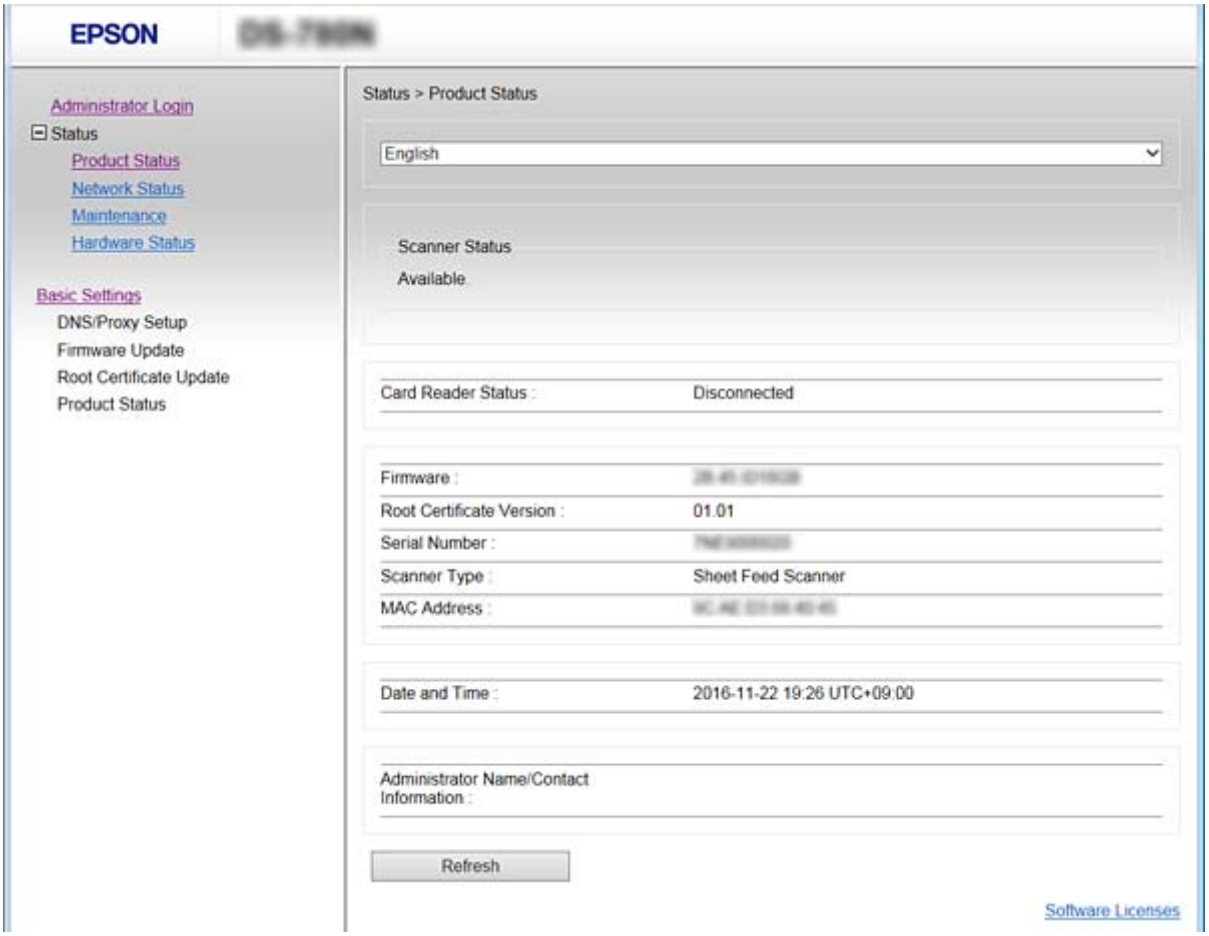
می توانید تنظیمات اصلی را برای اسکنر پیکربندی کنید.



تنظیمات عملکرد

❑ **Advanced Settings**

می توانید تنظیمات پیشرفته را برای اسکنر پیکربندی کنید. این صفحه در اصل برای سرپرست است.



دسترسی به Web Config

آدرس IP اسکنر را در یک مرورگر وب وارد کنید. JavaScript هم باید فعال باشد. هنگام دسترسی به Web Config از طریق HTTPS، یک پیام هشدار در مرورگر ظاهر می شود چون از یک گواهی خود امضاء، ذخیره شده در اسکنر، استفاده می شود.

❑ دسترسی از طریق HTTPS

IPv4: https://<آدرس IP اسکنر> (بدون < >)

IPv6: https://[آدرس IP اسکنر]/ (با [ ])

❑ دسترسی از طریق HTTP

IPv4: http://<آدرس IP اسکنر> (بدون < >)

IPv6: http://[آدرس IP اسکنر]/ (با [ ])

تنظیمات عملکرد

نکته:

❏ مثال ها

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ اگر نام اسکنر با سرور *DNS* ثبت شود، می توانید از نام اسکنر به جای آدرس *IP* اسکنر استفاده کنید.

اطلاعات مرتبط

◆ "ارتباط SSL/TLS با اسکنر" در صفحه 59

◆ "درباره گواهی دیجیتالی" در صفحه 59

استفاده از عملکردهای اسکن

بسته به روش استفاده از اسکنر، نرم‌افزار زیر را نصب کنید و تنظیمات را با آن اعمال کنید.

❏ **اسکن کردن از رایانه**

❏ اعتبار سرویس اسکن شبکه را با Web Config تایید کنید (در هنگام خروج از کارخانه معتبر است).

❏ Epson Scan 2 را بر روی رایانه نصب و نشانی IP را تنظیم کنید

❏ در هنگام اسکن کردن با استفاده از کارها، Document Capture Pro (Document Capture) را نصب و تنظیمات کار را اعمال کنید.

❏ **اسکن کردن از پانل عملیات**

❏ در هنگام استفاده از Document Capture Pro یا Document Capture Pro Server:

Document Capture Pro یا Document Capture Pro Server را نصب کنید

تنظیم DCP (حالت سرور، حالت مشتری).

❏ در صورت استفاده از پروتکل WSD:

اعتبار WSD را در Web Config یا پانل عملیات تایید کنید (در زمان خروج از کارخانه معتبر است)

دیگر تنظیمات دستگاه (رایانه دارای Windows).

اسکن کردن از رایانه

نرم‌افزار را نصب کنید و سرویس اسکن شبکه را فعال کنید تا اسکن از طریق شبکه از رایانه ممکن شود.

اطلاعات مرتبط

◆ "نرم‌افزاری که باید نصب شود" در صفحه 24

◆ "فعال کردن اسکن شبکه" در صفحه 24

نرم‌افزاری که باید نصب شود

❏ Epson Scan 2

این درایور اسکنر است. اگر از رایانه از دستگاه استفاده می‌کنید، درایور را روی تک‌تک رایانه‌های مشتری نصب کنید. اگر Document Capture Pro/Document CaptureCapture Pro نصب شود، می‌توانید کارهای اختصاص یافته به دکمه‌های دستگاه را انجام دهید.

با EpsonNet SetupManager، درایورهای چاپگر را می‌توان با هم در قالب بسته توزیع کرد.

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

روی رایانه مشتری نصب کنید. شما می‌توانید کارهای ثبت شده در رایانه را با Document Capture Pro/Document CaptureDocument Capture Pro نصب شده بر روی شبکه از پانل عملیات رایانه و اسکنر فراخوانی و اجرا کنید.

اسکن کردن از رایانه از طریق شبکه نیز ممکن است. برای اسکن کردن به Epson Scan 2 نیاز دارید.

اطلاعات مرتبط

"EpsonNet SetupManager" در صفحه 53

نشانی IP اسکنر را بر روی Epson Scan 2 تنظیم کنید

نشانی IP اسکنر را طوری تنظیم کنید که استفاده از اسکنر در شبکه ممکن شود.

1. برنامه **Epson Scan 2 Utility** را از **شروع** > **همه برنامه‌ها** > **EPSON** > **Epson Scan 2** اجرا کنید.

   اگر اسکنر دیگری از قبل ثبت شده است، به مرحله 2 بروید.

   اگر ثبت نشده است، به مرحله 4 بروید.

2. بر روی ▼ در **اسکنر** کلیک کنید.
3. روی **تنظیمات** کلیک کنید.
4. ابتدا بر روی **فعال کردن ویرایش** و سپس بر روی **افزودن** کلیک کنید.
5. نام مدل اسکنر را از **مدل** انتخاب کنید.
6. نشانی IP اسکنر مورد نظر را از **آدرس** در **جستجوی شبکه** انتخاب کنید.

   برای به‌روز رسانی فهرست ابتدا بر روی  و سپس بر روی  کلیک کنید. اگر نتوانستید IP اسکنر را بیابید، **آدرس را وارد کنید** را انتخاب و نشانی IP را وارد کنید.

7. روی **افزودن** کلیک کنید.
8. روی **تأیید** کلیک کنید.

فعال کردن اسکن شبکه

برای اسکن کردن از رایانه مشتری از طریق شبکه می‌توانید سرویس اسکن شبکه را فعال کنید. تنظیم پیش‌فرض فعال است.

1. از قسمت Web Config گزینه **Services** > **Network Scan** را انتخاب کنید.
2. از انتخاب شدن **Enable scanning** از **EPSON Scan** مطمئن شوید.

   اگر انتخاب شده باشد، این کار انجام می‌گیرد. Web Config را ببندید.

اگر پاک شده است، آن را انتخاب کنید و به مرحله بعدی بروید.

3. روی **Next** کلیک کنید.
4. روی **OK** کلیک کنید.

اتصال شبکه دوباره برقرار می‌شود و سپس تنظیمات فعال می‌گردد.

اطلاعات مرتبط

◆ "دسترسی به Web Config" در صفحه 22

اسکن کردن با استفاده از پانل کنترل

عملکرد اسکن به پوشه و اسکن به ایمیل با استفاده از پانل کنترل اسکنر، و نیز انتقال نتایج اسکن به ایمیل، پوشه و... را می‌توان از رایانه اجرا کرد.

برای انتقال نتایج اسکن، کارها را با Document Capture Pro Server یا Document Capture Pro تنظیم کنید.

برای کسب اطلاعات درباره تنظیمات و تنظیم کار، به مستندات یا راهنمای Document Capture Pro Server یا Document Capture Pro مراجعه کنید.

اطلاعات مرتبط

◆ "تنظیمات Document Capture Pro Server / " در صفحه 25Document Capture Pro
◆ "تنظیمات سرورها و پوشه‌ها" در صفحه 26

نرم‌افزار برای نصب کردن بر روی رایانه

❑ **Document Capture Pro Server**

این نسخه سرور Document Capture Pro است. آن را بر روی سرور Windows نصب کنید. با این سرور می‌توانید چندین دستگاه و کار را به صورت متمرکز مدیریت کنید. کارها را می‌توانید همزمان از چندین اسکنر اجرا کنید.

با استفاده از نسخه رسمی Document Capture Pro Server می‌توانید کارها و تاریخچه اسکن مرتبط با کاربران و گروه‌ها را مدیریت کنید.

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

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

همانند اسکن کردن از رایانه، می‌توانید کارهای ثبت شده در رایانه را از پانل کنترل فراخوانی و اجرا کنید. اجرای همزمان کارهای رایانه‌ای از چندین اسکنر ممکن نیست.

تنظیمات Document Capture Pro Server / Document Capture Pro

تنظیمات مربوط به عملکرد اسکن از پانل عملیات اسکنر را اعمال کنید.

1. از قسمت Web Config گزینه **Services** > **Document Capture Pro** را انتخاب کنید.
2. گزینه **حالت عملکرد** را انتخاب کنید.

❑ Server Mode:

این را زمانی انتخاب کنید که بخواهید از Document Capture Pro Serverاستفاده کنید یا از Document Capture Pro فقط برای کارهای تنظیم شده برای یک رایانه معین استفاده کنید.

❏ Client Mode:

این را زمانی تنظیم کنید که بخواهید تنظیم کار Document CaptureDocument Capture Pro)) نصب شده روی تک‌تک رایانه‌های مشتری شبکه را بدون مشخص کردن رایانه انتخاب کنید.

3. موارد زیر را بر اساس حالت انتخاب شده تنظیم کنید.

❏ Server Mode:

در **Server Address**، سروری را که Document Capture Pro Server روی آن نصب شده است انتخاب کنید. طول این مقدار باید 2 تا 252 نویسه در قالب IPv4، IPv6، نام میزبان یا FQDN باشد. در قالب FQDN، حروف اسکی - ایالات متحده، اعداد، الفبا و خط تیره (به جز در ابتدا و انتها) قابل استفاده است.

❏ Client Mode:

Group Settings را برای استفاده از گروه اسکنر مشخص شده از Document CaptureDocument Capture Pro)) تعیین کنید.

4. روی **تنظیم** کلیک کنید.

اطلاعات مرتبط

◆ "دسترسی به Web Config" در صفحه 22

تنظیمات سرورها و پوشه‌ها

Document Capture Pro و Document Capture Pro Server داده‌های اسکن شده را یک بار روی سرور یا رایانه مشتری ذخیره می‌کنند و از عملکرد انتقال برای اجرای عملکرد اسکن به پوشه و اسکن به ایمیل استفاده می‌کنند.

برای انتقال داده از رایانه دارای Document Capture Pro، Document Capture Pro Server به رایانه یا سرویس ابر به مجوز و اطلاعات نیاز دارید.

اطلاعات مربوط به عملکرد مورد نظر را با مراجعه به قسمت زیر آماده کنید.

با استفاده از Document Capture Pro یا Document Capture Pro Server می‌توانید تنظیمات این عملکردها را اعمال کنید. برای کسب اطلاعات درباره تنظیمات، به مستندات یا راهنمای Document Capture Pro Server یا Document Capture Pro مراجعه کنید.

نام	تنظیمات	شرط
اسکن به پوشه شبکه (SMB)	پوشه ذخیره را ایجاد و تنظیمات اشتراک آن را اعمال کنید	حساب کاربر سرپرست در رایانه‌ای که پوشه‌های ذخیره در آن ایجاد می‌شود.
	مقصد اسکن به پوشه شبکه (SMB)	نام کاربر و گذرواژه ورود به رایانه دارای پوشه ذخیره، و مجوز به‌روز رسانی پوشه ذخیره.
اسکن به پوشه شبکه (FTP)	تنظیم ورود به سرور FTP	اطلاعات ورود به سرور FTP و مجوز به‌روز رسانی پوشه ذخیره.
اسکن به ایمیل	تنظیم سرور ایمیل	اطلاعات تنظیم سرور ایمیل
اسکن کردن به Document Capture Pro (در صورت استفاده از Document Capture Pro Server)	تنظیم مربوط به ورود به خدمات ابری	محیط اتصال اینترنت ثبت حساب برای خدمات ابری

استفاده از اسکن WSD (فقط Windows)

اگر رایانه از Windows Vista یا بالاتر استفاده کند، می‌توانید از اسکن WSD استفاده کنید.

اگر پروتکل WSD قابل استفاده باشد، منو **رایانه (WSD)** روی پانل کنترل اسکنر ظاهر می‌شود.

1. از قسمت Web Config گزینه **Services** > **Protocol** را انتخاب کنید.
2. مطمئن شوید که **Enable WSD** در **WSD Settings** علامت خورده باشد.
   اگر علامت خورده باشد، کار شما کامل شده است و می‌توانید Web Config را ببندید.
   اگر علامت نخورده باشد، آن را علامت بزنید و به مرحله بعد بروید.
3. بر روی دکمه **Next** کلیک کنید.
4. تنظیمات را تایید کنید و بر روی **تنظیم** کلیک کنید.

اعمال تنظیمات سیستم

انجام تنظیمات سیستم از پانل کنترل

تنظیم روشنایی صفحه

روشنایی صفحه LCD را تنظیم کنید.

1. از صفحه اصلی، بر روی **تنظیم** تلنگر بزنید.
2. روی **تنظیمات معمول** > **روشنایی LCD** تلنگر بزنید.
3. برای تنظیم روشنایی بر روی یا تلنگر بزنید.
   مقدار تنظیم از 1 تا 9 متغیر است.
4. روی **تأیید** ضربه بزنید.

تنظیم صدا

صدای کار پانل و صدای خطا را تنظیم کنید.

1. از صفحه اصلی، بر روی **تنظیم** تلنگر بزنید.
2. روی **تنظیمات معمول** > **صدا** تلنگر بزنید.
3. در صورت نیاز موارد زیر را تنظیم کنید.
   - ❏ صدای عملکرد
     صدای استفاده از عملکردهای پانل را تنظیم کنید.
   - ❏ صدای خطا
     صدای خطا را تنظیم کنید.
4. روی **تأیید** ضربه بزنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

تشخیص تغذیه دوگانه سند اصلی

عملکرد تشخیص تغذیه دوگانه سند اصلی و توقف عمل اسکن در صورت وقوع تغذیه چندگانه را تنظیم کنید.

برای اسکن کردن اسنادی که مشمول تغذیه چندگانه هستند، مانند پاکت یا کاغذ دارای برچسب، آن را بر روی خاموش تنظیم کنید.

نکته:

آن را می‌توانید از *Web Config* یا *Epson Scan 2* نیز تنظیم کنید.

1. از صفحه اصلی، بر روی **تنظیم** تلنگر بزنید.
2. روی **تنظیمات اسکن خارجی** > **تشخیص اولتراسونیک دو سند** تلنگر بزنید.
3. برای فعال یا غیرفعال کردن آن بر روی **تشخیص اولتراسونیک دو سند** تلنگر بزنید.
4. روی **بستن** ضربه بزنید.

تنظیم حالت کم-سرعت

با انتخاب اسکن با حالت کم-سرعت از گیر کردن کاغذ در هنگام اسکن کردن اسنادی مانند آگهی جلوگیری کنید.

1. از صفحه اصلی، بر روی **تنظیم** تلنگر بزنید.
2. روی **تنظیمات اسکن خارجی** > **آهسته** تلنگر بزنید.
3. برای فعال یا غیرفعال کردن آن بر روی **آهسته** تلنگر بزنید.
4. روی **بستن** ضربه بزنید.

اعمال تنظیمات سیستم با Web Config

تنظیمات صرفه‌جویی در نیرو در مدت بیکار ماندن

تنظیم صرفه‌جویی در نیرو را برای دوره بیکاری اسکنر اعمال کنید. زمان را بر اساس محیط استفاده تنظیم کنید.

نکته:

می‌توانید تنظیمات صرفه‌جویی را از پانل کنترل اسکنر نیز اعمال کنید.

1. از قسمت Web Config گزینه **System Settings** > **Power Saving** را انتخاب کنید.
2. زمان **Sleep Timer** را برای ورود به حالت صرفه‌جویی در وضعیت بیکاری وارد کنید.
   می‌توانید تا 240 دقیقه بر حسب دقیقه وارد کنید.
3. زمان خاموش شدن را برای **Power Off Timer** انتخاب کنید.
4. روی **OK** کلیک کنید.

تنظیمات عملکرد

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

تنظیم پانل کنترل

پانل کنترل اسکنر را راه‌اندازی کنید. راه‌اندازی به روش زیر صورت می‌گیرد.

1. از قسمت Web Config گزینه **System Settings** > **Control Panel** را انتخاب کنید.
2. در صورت نیاز موارد زیر را تنظیم کنید.

❏ Language

زبان نمایش داده شده در پانل کنترل را انتخاب کنید.

❏ Panel Lock

اگر **ON** را انتخاب کنید، داشتن گذرواژه سرپرست برای انجام دادن کاری که نیازمند مجوز سرپرست است، ضروری خواهد بود. اگر گذرواژه سرپرست تنظیم نشود، ساعت پانل غیرفعال می‌شود.

❏ Operation Timeout

اگر **ON** را انتخاب کنید، در صورت ورود به عنوان سرپرست، اگر در مدت معین شده کاری انجام نگیرد، به طور خودکار خارج می‌شوید و به صفحه اصلی هدایت می‌شوید.

می‌توانید مقداری از 10 ثانیه تا 240 دقیقه را بر حسب ثانیه وارد کنید.

3. روی **OK** کلیک کنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

تنظیم محدودیت رابط خارجی

می‌توانید اتصال USB از رایانه را محدود کنید. با تنظیم آن می‌توانید موارد اسکن غیر شبکه را محدود کنید.

1. از قسمت Web Config گزینه **System Settings** > **External Interface** را انتخاب کنید.
2. **Enable** یا **Disable** را انتخاب کنید.

برای محدود کردن، **Disable** را انتخاب کنید.

3. روی **OK** ضربه بزنید.

همگام‌سازی تاریخ و ساعت با سرور زمان

در صورت استفاده از گواهی CA، می‌توانید مانع بروز مشکلات مربوط به زمان شوید.

1. از قسمت Web Config گزینه **System Settings** > **Date and Time** > **Time Server** را انتخاب کنید.
2. گزینه **Use** را برای **Use Time Server** انتخاب کنید.

تنظیمات عملکرد

3. نشانی سرور زمان را برای **Time Server Address** وارد کنید.

   می توانید از قالب IPv4، IPv6 یا FQDN استفاده کنید. حداکثر 252 نویسه وارد کنید. اگر این را مشخص نمی‌کنید، قسمت مرتبط را خالی بگذارید.

4. **Update Interval (min)** را وارد کنید.

   می‌توانید تا 10, 800 دقیقه بر حسب دقیقه وارد کنید.

5. روی **OK** کلیک کنید.

نکته:
می‌توانید وضعیت اتصال به سرور زمان را در ***Time Server Status*** تایید کنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

تنظیمات امنیتی ابتدایی

این فصل تنظیمات امنیتی پایه را که نیازمند محیط ویژه نیست، شرح می‌دهد.

معرفی امکانات امنیتی ابتدایی

ما امکانات امنیتی ابتدایی دستگاه‌های Epson را معرفی می‌کنیم.

نام قابلیت	نوع قابلیت	آنچه باید تنظیم شود	آنچه باید جلوگیری شود
تنظیم گذرواژه سرپرست	تنظیمات مربوط به سیستم، مانند تنظیمات شبکه و اتصال USB را قفل کنید تا کسی به جز سرپرست نتواند آنها را تغییر دهد.	سرپرست گذرواژه دستگاه را تنظیم می‌کند. پیکربندی یا به‌روز رسانی از هر کجای Web Config، پانل کنترل، Epson Device Admin و EpsonNet Config امکان‌پذیر است.	مانع خواندن و تغییر دادن غیرمجاز اطلاعات ذخیره شده در دستگاه مانند شناسه، گذرواژه، تنظیمات شبکه و مخاطبان می‌شود. همچنین، طیف گسترده‌ای از خطرهای امنیتی مانند نشت اطلاعات از محیط شبکه یا سیاست امنیتی را کاهش می‌دهد.
ارتباط SSL/TLS	در هنگام ایجاد ارتباط اینترنتی بین سرور Epson و دستگاه، مانند ارتباط بین رایانه از طریق مرورگر یا به‌روز رسانی نرم‌افزار، محتویات ارتباط با ارتباط SSL/TLS رمزگذاری می‌شود.	یک گواهی دارای امضای CA بگیرید و آن را وارد اسکنر کنید.	پاک کردن شناسه دستگاه با گواهی دارای امضای CA مانع جعل هویت و دسترسی غیرمجاز می‌شود. در ضمن، محتوای ارتباط SSL/TLS محافظت می‌شود و بدین ترتیب از نشت محتویات مربوط به داده‌های چاپ و اطلاعات تنظیم جلوگیری می‌گردد.
پروتکل‌های کنترلی	پروتکل‌های کنترلی برای ایجاد ارتباط بین دستگاه و رایانه و فعال/غیرفعال کردن عملکردها به کار می‌رود.	پروتکل یا سرویسی که بر روی قابلیت‌ها اعمال می‌شود، جداگانه مجاز یا غیرمجاز می‌گردد.	کاهش احتمال بروز خطرهای ناشی از استفاده ناخواسته از طریق جلوگیری از دسترسی کاربران به عملکردهای غیرضروری.

اطلاعات مرتبط

- "درباره Web Config" در صفحه 21
- "EpsonNet Config" در صفحه 52
- "Epson Device Admin" در صفحه 52
- "پیکربندی رمز عبور سرپرست" در صفحه 31
- "کنترل پروتکل ها" در صفحه 34

پیکربندی رمز عبور سرپرست

اگر برای سرپرست گذرواژه تعیین کنید، کاربران غیر از سرپرست نمی‌توانند تنظیمات سرپرستی سیستم را تغییر دهند. برای تنظیم کردن و تغییر دادن گذرواژه سرپرست می‌توانید از Web Config، پانل کنترل اسکنر یا نرم‌افزار (Epson Device Admin یا EpsonNet Config) استفاده کنید. در صورت استفاده از نرم‌افزار، به مستندات آن مراجعه کنید.

اطلاعات مرتبط

- "پیکربندی گذرواژه سرپرست از پانل کنترل" در صفحه 32
- "پیکربندی گذرواژه سرپرست با Web Config" در صفحه 32
- "EpsonNet Config" در صفحه 52

"Epson Device Admin" در صفحه 52

پیکربندی گذرواژه سرپرست از پانل کنترل

می‌توانید گذرواژه سرپرست را از پانل کنترل اسکنر تنظیم کنید.

1. از صفحه اصلی، بر روی **تنظیم** تلنگر بزنید.
2. روی **سرپرست سیستم** > **تنظیمات سرپرست** تلنگر بزنید.
   اگر گزینه نشان داده نمی‌شود، به بالای صفحه بروید و آن را نشان دهید.
3. روی **رمز عبور سرپرست** > **ثبت** تلنگر بزنید.
4. گذرواژه را وارد کنید و بر روی **تأیید** تلنگر بزنید.
5. گذرواژه را دوباره وارد کنید و بر روی **تأیید** تلنگر بزنید.
6. از صفحه تایید بر روی **تأیید** تلنگر بزنید.
   صفحه تنظیمات سرپرست نمایش داده می‌شود.
7. بر روی **تنظیم قفل** تلنگر بزنید و **تأیید** را در صفحه تایید لمس کنید.
   تنظیم قفل بر روی **On** تنظیم می‌شود و گذرواژه سرپرست برای استفاده از منو قفل شده ضروری می‌گردد.

نکته:

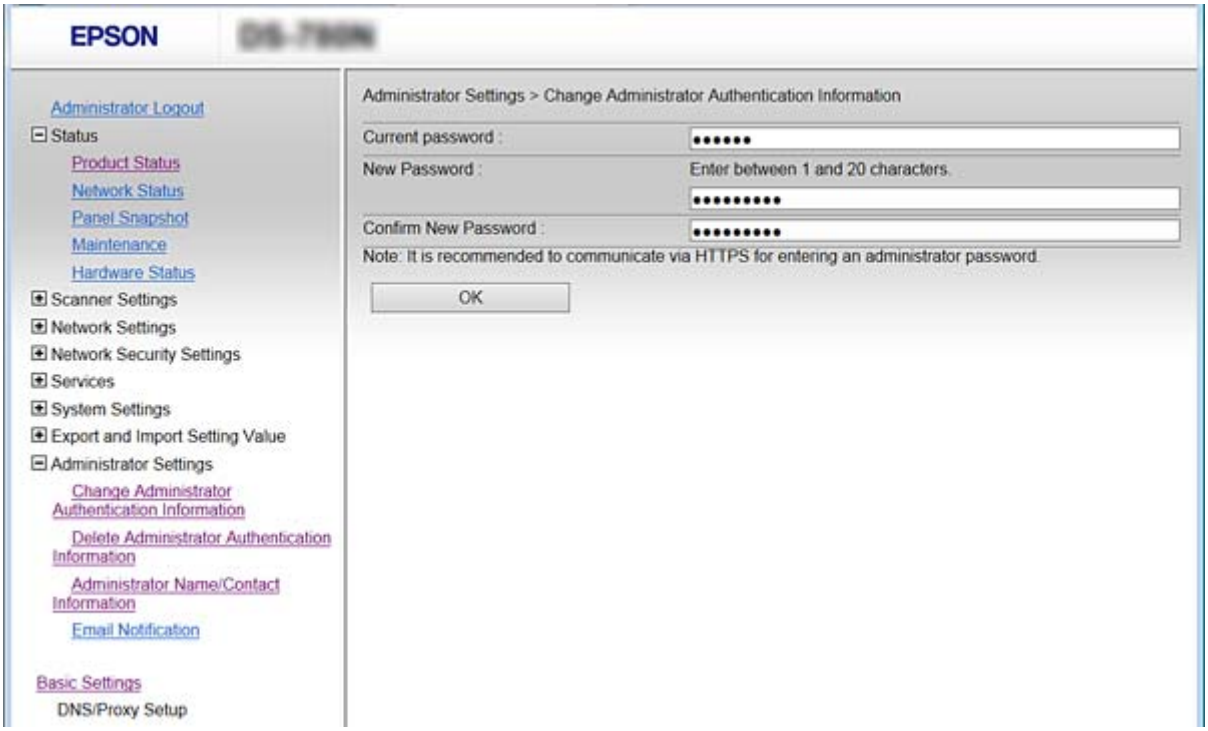
- اگر **تنظیم** > **تنظیمات معمول** > **فرصت زمانی عملکرد** را بر روی ***On*** تنظیم کنید، اسکن شما را پس از مدتی بیکار ماندن پانل کنترل از سامانه خارج می‌کند.
- با انتخاب **تغییر** یا **بازنشانی** از صفحه **رمز عبور سرپرست** و وارد کردن گذرواژه سرپرست می‌توانید گذرواژه سرپرست یا حذف کنید یا تغییر دهید.

پیکربندی گذرواژه سرپرست با Web Config

می‌توانید گذرواژه سرپرست را با Web Config تنظیم کنید.

1. از قسمت Web Config گزینه **Administrator Settings** > **Change Administrator Authentication Information** را انتخاب کنید.

2. یک رمز عبور در **New Password** و **Confirm New Password** وارد کنید. در صورت لزوم نام کاربر را وارد کنید.
اگر می خواهید رمز عبور را به رمز عبور جدیدی تغییر دهید، رمز عبور فعلی را وارد کنید.



3. گزینه **OK** را انتخاب کنید.

نکته:

- برای تنظیم کردن یا تغییر دادن گزینه‌های قفل شده منو، بر روی ***Administrator Login*** کلیک کنید و گذرواژه سرپرست را وارد کنید.
- برای حذف کردن گذرواژه سرپرست، بر روی ***Administrator Settings*** > ***Delete Administrator Authentication Information*** کلیک کنید و گذرواژه سرپرست را وارد کنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

مواردی که با گذرواژه سرپرست قفل می‌شود

سرپرست دارای حق تغییر و تنظیم برای همه امکانات دستگاه است.

همچنین، اگر روی دستگاه گذرواژه سرپرست تنظیم کرده باشید، می‌توانید آن را قفل کنید تا کسی نتواند موارد مربوط به مدیریت دستگاه را تغییر دهد.

سرپرست می‌تواند موارد زیر را کنترل کند.

موارد	شرح
تنظیم اسکنر	تنظیم تشخیص تغذیه دوگانه و حالت کم-سرعت.
تنظیمات اتصال اترنت	نام و نشانی IP دستگاه‌ها را تغییر دهید، سرور DNS یا سرور پروکسی تنظیم کنید و تنظیمات مربوط به اتصال شبکه را تغییر دهید.

تنظیمات امنیتی ابتدایی

موارد	شرح
تنظیم خدمات کاربر	تنظیم مربوط به کنترل پروتکل‌های ارتباطی، اسکن شبکه و خدمات Document Capture Pro.
تنظیم سرور ایمیل	تنظیم سرور ایمیل که دستگاه‌ها مستقیماً با آن ارتباط برقرار می‌کنند.
تنظیم امنیت	تنظیمات مربوط به امنیت شبکه، مانند ارتباط SSL/TLS، IPsec/فیلترینگ IP و IEEE802.1X.
به‌روز رسانی گواهی ریشه	به‌روز رسانی گواهی‌های ریشه لازم برای تایید هویت Document Capture Pro Server و به‌روز رسانی نرم‌افزار از Web Config.
به‌روز رسانی نرم‌افزار	بررسی و به‌روز رسانی نرم‌افزار دستگاه‌ها.
زمان، تنظیم زمان‌سنج	زمان ورود به حالت خواب، خاموش شدن خودکار، تاریخ/ساعت، زمان‌سنج بیکاری، دیگر تنظیمات مربوط به زمان‌سنج.
بازگشت به تنظیمات پیش‌فرض	تنظیم بازگرداندن اسکنر به تنظیمات کارخانه.
تنظیم سرپرست	تنظیم قفل سرپرست یا گذرواژه سرپرست.
تنظیم دستگاه گواهی شده	تنظیم شناسه دستگاه تایید هویت. در صورت استفاده از اسکنر در سیستم تایید هویت پشتیبانی کننده از دستگاه‌های تایید هویت تنظیم کنید.

کنترل پروتکل ها

می توانید با استفاده از گذرگاه ها و پروتکل های مختلف اسکن کنید. می‌توانید از چندین رایانه شبکه از قابلیت اسکن شبکه استفاده کنید. مثلاً، اسکن کردن فقط با استفاده از مسیرها و پروتکل‌های مشخص امکان‌پذیر است. می توانید با محدود کردن اسکن از گذرگاه های مشخص یا با کنترل عملکردهای موجود خطرات ناخواسته امنیتی را کاهش دهید.

تنظیمات پروتکل را پیکربندی کنید.

1. از قسمت Web Config گزینه **Services** > **Protocol** را انتخاب کنید.
2. هر مورد را پیکربندی کنید.
3. روی **Next** کلیک کنید.
4. روی **OK** کلیک کنید.

تنظیمات در اسکنر اعمال می شوند.

اطلاعات مرتبط

- "دسترسی به Web Config" در صفحه 22
- "پروتکل هایی که می توانید فعال یا غیرفعال کنید" در صفحه 34
- "موارد تنظیم پروتکل" در صفحه 36

پروتکل هایی که می توانید فعال یا غیرفعال کنید

پروتکل	شرح
Bonjour Settings	می توانید مشخص کنید آیا از Bonjour استفاده شود یا خیر. Bonjour برای جستجوی دستگاه ها، اسکن و مانند این استفاده می شود.

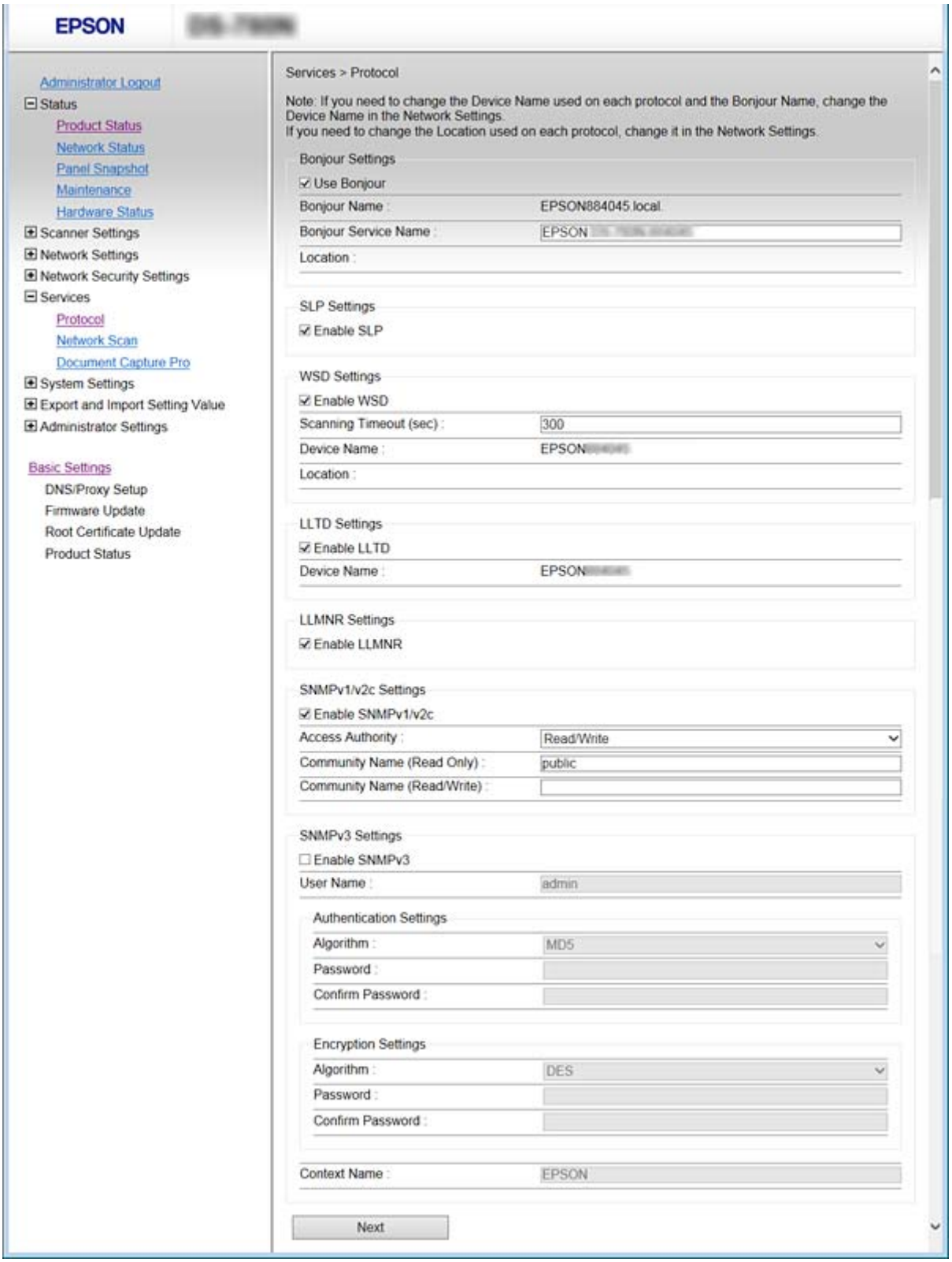
تنظیمات امنیتی ابتدایی

پروتکل	شرح
SLP Settings	می توانید عملکرد SLP را فعال یا غیرفعال کنید. SLP برای Epson Scan 2 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 یا از درگاه WSD اسکن کنید.
LLTD Settings	می توانید عملکرد LLTD را فعال یا غیرفعال کنید. زمانی که فعال باشد، بر روی نقشه شبکه Windows نشان داده می شود.
LLMNR Settings	می توانید عملکرد LLMNR را فعال یا غیرفعال کنید. زمانی که فعال باشد، می توانید از جداسازی نام بدون NetBIOS استفاده کنید حتی اگر نتوانید از DNS استفاده کنید.
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 رمزگذاری شده، کنترل و... استفاده می شود.

اطلاعات مرتبط

- "کنترل پروتکل ها" در صفحه 34
- "موارد تنظیم پروتکل" در صفحه 36

موارد تنظیم پروتکل



موارد	تنظیم مقدار و توضیحات
Bonjour Settings	

تنظیمات امنیتی ابتدایی

موارد	تنظیم مقدار و توضیحات
Use Bonjour	برای جستجو یا استفاده از دستگاه ها از طریق Bonjour این را انتخاب کنید.
Bonjour Name	نام Bonjour را نمایش می دهد.
Bonjour Service Name	می‌توانید نام سرویس Bonjour را نمایش دهید و تنظیم کنید.
Location	نام مکان Bonjour را نمایش می دهد.
SLP Settings	
Enable SLP	برای فعال سازی عملکرد SLP این را انتخاب کنید. این برای کشف شبکه در Epson Scan 2 و EpsonNet Config به کار می‌رود.
WSD Settings	
Enable WSD	برای فعال کردن دستگاه ها با استفاده از WSD و چاپ و اسکن از پورت WSD این را انتخاب کنید.
Scanning Timeout (sec)	مقدار زمان وقفه را برای اسکن کردن WSD بین 3 تا 3600 ثانیه وارد کنید.
Device Name	نام دستگاه WSD را نمایش می دهد.
Location	نام مکان WSD را نمایش می دهد.
LLTD Settings	
Enable LLTD	این را انتخاب کنید تا LLTD فعال شود. اسکنر در نقشه شبکه Windows نمایش داده می شود.
Device Name	نام دستگاه LLTD را نمایش می دهد.
LLMNR Settings	
Enable LLMNR	این را انتخاب کنید تا LLMNR فعال شود. می توانید از جداسازی نام بدون NetBIOS استفاده کنید حتی اگر نتوانید از DNS استفاده کنید.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	انتخاب کنید تا SNMPv1/v2c فعال شود. فقط اسکنرهایی که از SNMPv3 پشتیبانی می کنند نمایش داده می شوند.
Access Authority	وقتی SNMPv1/v2c فعال است، مرجع دسترسی را تنظیم کنید. **Read Only** یا **Read/Write** را انتخاب کنید.
Community Name (Read Only)	بین 0 تا 32 نویسه اسکی (0x20 تا 0x7E) وارد کنید.
Community Name (Read/Write)	بین 0 تا 32 نویسه اسکی (0x20 تا 0x7E) وارد کنید.
SNMPv3 Settings	
Enable SNMPv3	زمانی که کادر علامت داشته باشد، SNMPv3 فعال می شود.
User Name	بین 1 تا 32 نویسه با استفاده از نویسه های 1 بایتی وارد کنید.
Authentication Settings	
Algorithm	الگوریتم تایید هویت را برای SNMPv3 انتخاب کنید.

تنظیمات امنیتی ابتدایی

موارد	تنظیم مقدار و توضیحات
Password	گذرواژه تایید هویت را برای SNMPv3 وارد کنید. بین 8 تا 32 نویسه با فرمت ASCII ((0x20–0x7E) وارد کنید. اگر این را مشخص نمی‌کنید، قسمت مرتبط را خالی بگذارید.
Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید وارد نمایید.
Encryption Settings	
Algorithm	الگوریتم رمزگذاری را برای .SNMPv3 انتخاب کنید.
Password	گذرواژه رمزگذاری را برای SNMPv3 وارد کنید. بین 8 تا 32 نویسه با فرمت ASCII ((0x20–0x7E) وارد کنید. اگر این را مشخص نمی‌کنید، قسمت مرتبط را خالی بگذارید.
Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید وارد نمایید.
Context Name	حداکثر 32 نویسه یونیکد (UTF-8) وارد کنید. اگر این را مشخص نمی‌کنید، قسمت مرتبط را خالی بگذارید. تعداد نویسه‌های مجاز بسته به زبان فرق می‌کند.

اطلاعات مرتبط

- "کنترل پروتکل ها" در صفحه 34
- "پروتکل هایی که می توانید فعال یا غیرفعال کنید" در صفحه 34

تنظیمات بهره‌برداری و مدیریت

این فصل موارد مربوط به بهره‌برداری و مدیریت روزانه دستگاه را شرح می‌دهد.

اطلاعات دستگاه را تایید کنید

می‌توانید این اطلاعات دستگاه را از **Status** با استفاده از Web Config بررسی کنید.

❏ Product Status

زبان، وضعیت، شماره دستگاه، نشانی MAC و... را بررسی کنید.

❏ Network Status

اطلاعات وضعیت اتصال شبکه، نشانی IP، سرور DNS و... را بررسی کنید.

❏ Panel Snapshot

عکس صفحه را که بر روی پانل کنترل دستگاه نمایش داده می‌شود، نمایش دهید.

❏ Maintenance

تاریخ شروع، اطلاعات اسکن و... را بررسی کنید.

❏ Hardware Status

وضعیت اسکنر را بررسی کنید.

اطلاعات مرتبط

◆ "دسترسی به Web Config" در صفحه 22

مدیریت دستگاه‌ها (Epson Device Admin)

با Epson Device Admin می‌توانید دستگاه‌های متعدد را مدیریت و به کار بگیرید. Epson Device Admin به شما امکان می‌دهد که دستگاه‌های شبکه‌های دیگر را مدیریت کنید. امکانات اصلی مدیریت در ادامه شرح داده شده است.

برای کسب اطلاعات بیشتر درباره عملکردها و استفاده از نرم‌افزار، به مستندات یا راهنمای Epson Device Admin مراجعه کنید.

❏ کشف دستگاه‌ها

می‌توانید دستگاه‌های شبکه را کشف و آنها را به فهرست اضافه کنید. اگر دستگاه‌های Epson مانند چاپگر و اسکنر به همان بخشی از شبکه که رایانه سرپرست به آن متصل است، متصل باشند، می‌توانید آنها را بیابید حتی اگر نشانی IP به آنها تخصیص داده نشده باشد.

همچنین می‌توانید دستگاه‌هایی را که با کابل USB به شبکه متصل شده‌اند، بیابید. باید Epson Device USB Agent را روی رایانه نصب کنید.

❏ تنظیم دستگاه‌ها

می توانید یک الگو تهیه کنید که شامل موارد تنظیم مانند رابط شبکه و منبع کاغذ باشد و آن را در سایر دستگاه ها به عنوان تنظیمات مشترک اعمال کنید. پس از ایجاد ارتباط با شبکه، می‌توانید به دستگاهی که نشانی IP ندارد، یک نشانی IP اختصاص دهید.

❏ پایش دستگاه‌ها

می‌توانید وضعیت و اطلاعات مشروح دستگاه‌های شبکه را مرتباً کسب کنید. می‌توانید دستگاه‌هایی که با کابل USB به رایانه‌های شبکه وصل شده‌اند، و دستگاه‌های دیگر شرکت‌ها که در فهرست دستگاه‌ها ثبت شده‌اند، را پایش کنید. برای پایش دستگاه‌های متصل به وسیله کابل USB، باید Epson Device USB Agent را نصب کنید.

❏ مدیریت هشدار

می‌توانید هشدارهای مربوط به وضعیت دستگاه‌ها و اقلام مصرفی را پایش کنید. سیستم بسته به شرایط تنظیم شده به طور خودکار ایمیل هشدار به سرپرست می‌فرستد.

❏ مدیریت گزارش‌ها

می‌توانید با استفاده از داده‌های سیستمی درباره استفاده از دستگاه و اقلام مصرفی گزارش‌های منظم تهیه کنید. می‌توانید گزارش‌های ایجاد شده را ذخیره و با ایمیل ارسال کنید.

اطلاعات مرتبط

◆ "Epson Device Admin" در صفحه 52

دریافت اعلان های ایمیل زمانی که رویدادها اتفاق می افتند

درباره اعلان های ایمیل

می توانید از این ویژگی برای دریافت هشدارها از طریق ایمیل برای زمانی که رویدادهایی اتفاق می افتند استفاده کنید. می توانید تا 5 آدرس ایمیل را ثبت کنید و انتخاب کنید برای چه رویدادهایی می خواهید اعلان دریافت کنید.

برای استفاده از این عملکرد باید سرور ایمیل را پیکربندی کنید.

اطلاعات مرتبط

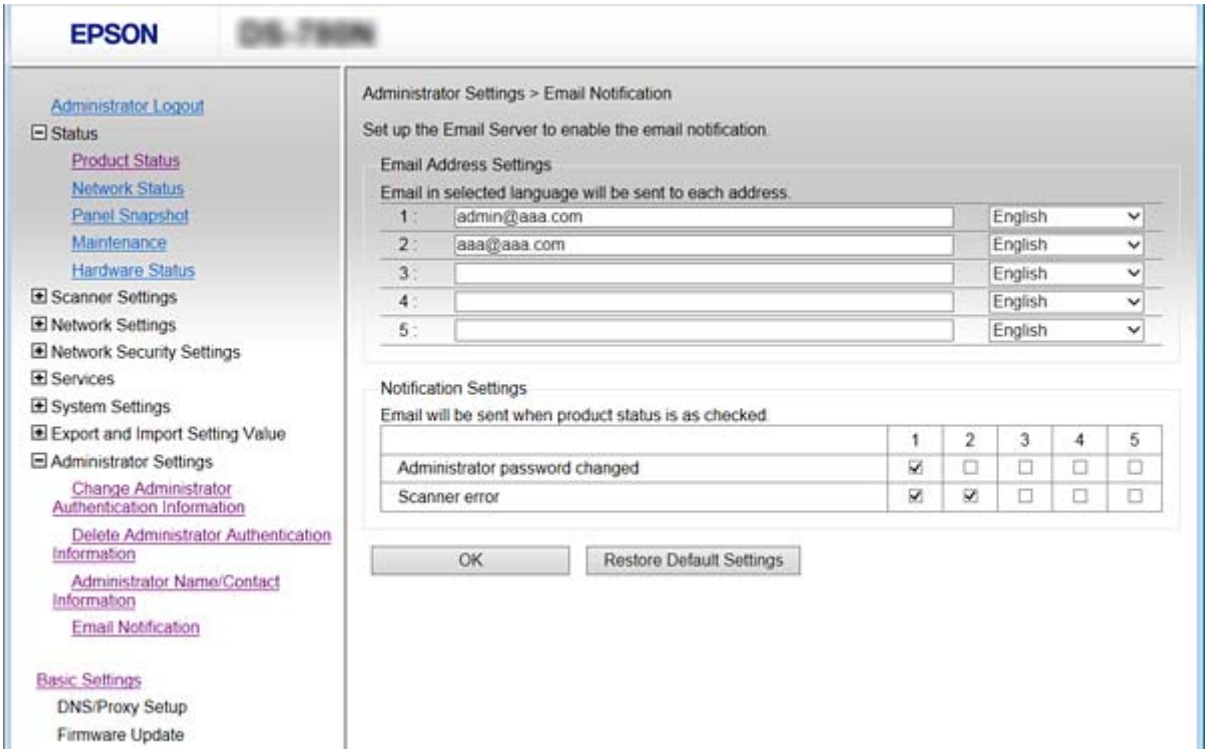
◆ "پیکربندی سرور ایمیل" در صفحه 41

پیکربندی اعلان ایمیل

برای استفاده از ویژگی لازم است یک سرور ایمیل پیکربندی کنید.

1. به Web Config دسترسی یابید و **Administrator Settings** > **Email Notification** را انتخاب کنید.
2. یک آدرس ایمیل وارد کنید که می خواهید از طریق آن اعلان های ایمیل دریافت کنید.
3. زبان را برای اعلان های ایمیل انتخاب کنید.

4. کادرها را برای اعلان هایی که می خواهید دریافت کنید علامت بزنید.



5. روی **OK** کلیک کنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

"پیکربندی سرور ایمیل" در صفحه 41

پیکربندی سرور ایمیل

قبل از پیکربندی موارد زیر را بررسی کنید.

❑ اسکنر به شبکه وصل باشد.

❑ اطلاعات سرور ایمیل رایانه.

1. به Web Config دسترسی یابید و **Network Settings** > **Email Server** > **Basic** را انتخاب کنید.
2. برای هر مورد یک مقدار وارد کنید.
3. **OK** را انتخاب کنید.

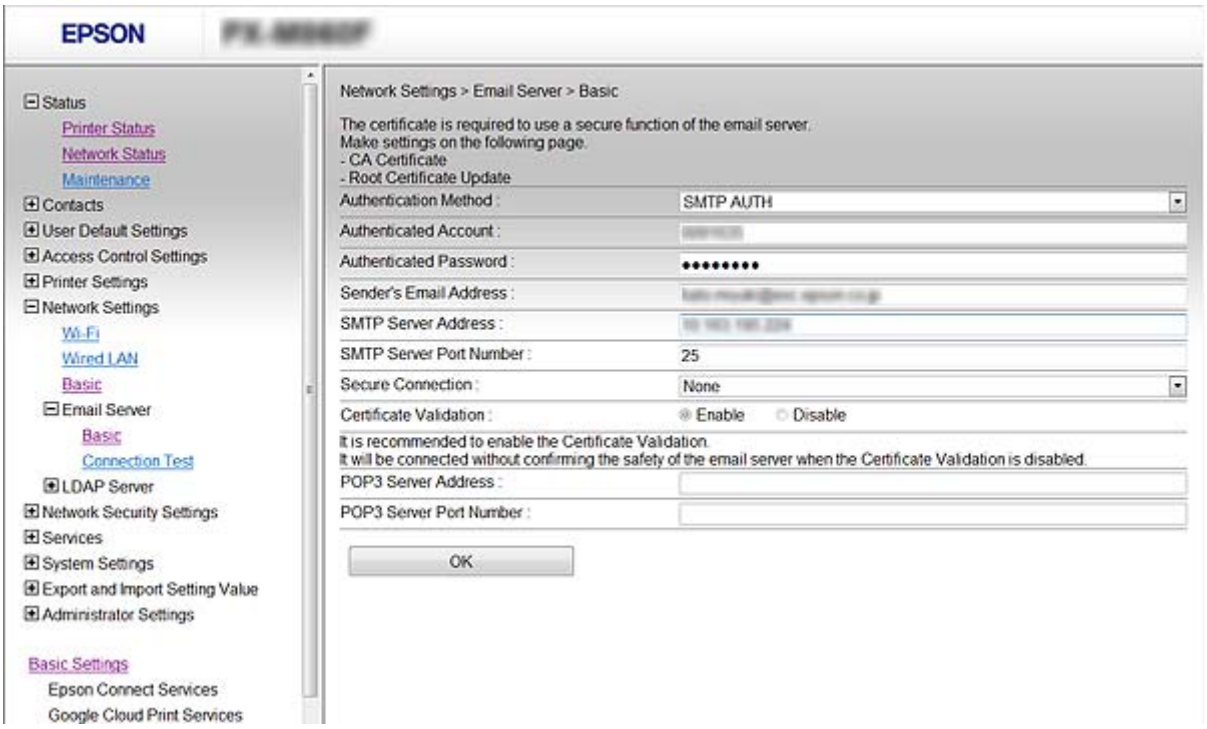
تنظیماتی که انتخاب کرده اید نشان داده می شود.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

"موارد تنظیم سرور ایمیل" در صفحه 42

موارد تنظیم سرور ایمیل



موارد	تنظیمات و توضیحات	
Authentication Method	روش تأیید اعتبار اسکنر برای دسترسی به سرور ایمیل را مشخص کنید.	
	Off	تأیید اعتبار زمان ارتباط با سرور ایمیل غیرفعال است.
	SMTP AUTH	سرور ایمیل باید از تأیید اعتبار SMTP پشتیبانی کند.
	POP before SMTP	زمان انتخاب این روش، سرور POP3 را پیکربندی کنید.
Authenticated Account	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 Password	اگر **SMTP AUTH** یا **POP before SMTP** را به عنوان **Authentication Method** انتخاب کنید، رمز عبور تأیید شده را از 0 تا 20 نویسه با استفاده از این موارد وارد کنید A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	آدرس ایمیل فرستنده را وارد کنید. بین 0 تا 255 نویسه با فرمت ASCII (0x20–0x7E) به جز برای : ( ) < > [ ] ; ¥ وارد کنید. نقطه "." نمی تواند اولین نویسه باشد.	
SMTP Server Address	بین 0 تا 255 نویسه با استفاده از این موارد وارد کنید A–Z a–z 0–9 . - . می توانید از فرمت IPv4 یا FQDN استفاده کنید.	
SMTP Server Port Number	عددی بین 1 تا 65535 وارد کنید.	
Secure Connection	روش اتصال ایمن را برای این سرور ایمیل مشخص کنید.	
	None	اگر **POP before SMTP** را در **Authentication Method** انتخاب کنید، روش اتصال بر روی **None** تنظیم می شود.
	SSL/TLS	این زمانی موجود است که **Authentication Method** بر روی **Off** یا **SMTP AUTH** تنظیم باشد.
	STARTTLS	این زمانی موجود است که **Authentication Method** بر روی **Off** یا **SMTP AUTH** تنظیم باشد.

موارد	تنظیمات و توضیحات
Certificate Validation	زمانی که این فعال باشد گواهی تأیید می شود. ما توصیه می کنیم این روی **Enable** تنظیم باشد.
POP3 Server Address	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 A–Z a–z 0–9 . - . می توانید از فرمت IPv4 یا FQDN استفاده کنید.
POP3 Server Port Number	اگر **POP before SMTP** را به عنوان **Authentication Method** انتخاب کنید، عددی بین 1 تا 65535 وارد کنید.

اطلاعات مرتبط

"پیکربندی سرور ایمیل" در صفحه 41

بررسی اتصال سرور ایمیل

1. به Web Config دسترسی یابید و **Network Settings** > **Email Server** > **Connection Test** را انتخاب کنید.
2. **Start** را انتخاب کنید.

بررسی اتصال به سرور ایمیل شروع می شود. بعد از بررسی، گزارش این بررسی نشان داده می شود.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22
"مرجع های بررسی اتصال سرور ایمیل" در صفحه 43

مرجع های بررسی اتصال سرور ایمیل

پیام ها	توضیحات
Connection test was successful.	این پیام زمانی ظاهر می شود که اتصال به سرور انجام می شود.
SMTP server communication error. Check the following. - Network Settings	این پیام زمانی ظاهر می شود که ❑ اسکنر به شبکه وصل نباشد ❑ سرور SMTP کار نمی کند ❑ اتصال شبکه زمان ارتباط قطع شده است ❑ داده های ناکامل دریافت شده است
POP3 server communication error. Check the following. - Network Settings	این پیام زمانی ظاهر می شود که ❑ اسکنر به شبکه وصل نباشد ❑ سرور POP3 کار نمی کند ❑ اتصال شبکه زمان ارتباط قطع شده است ❑ داده های ناکامل دریافت شده است
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	این پیام زمانی ظاهر می شود که ❑ اتصال به سرور DNS انجام نشود ❑ جداسازی نام برای سرور SMTP انجام نشود

تنظیمات بهره‌برداری و مدیریت

پیام ها	توضیحات
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	این پیام زمانی ظاهر می شود که ❏ اتصال به سرور DNS انجام نشود ❏ جداسازی نام برای سرور POP3 انجام نشود
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	این پیام زمانی ظاهر می شود که تأیید اعتبار سرور SMTP انجام نشود.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	این پیام زمانی ظاهر می شود که تأیید اعتبار سرور POP3 انجام نشود.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	این پیام زمانی ظاهر می شود که تلاش می کنید با پروتکل های پشتیبانی شده ارتباط برقرار کنید.
Connection to SMTP server failed. Change Secure Connection to None.	این پیام زمانی ظاهر می شود که عدم تطابق SMTP بین سرور و کلاینت روی می دهد، یا زمانی که سرور از اتصال ایمن SMTP پشتیبانی نمی کند (اتصال SSL).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	این پیام زمانی ظاهر می شود که عدم تطابق SMTP بین سرور و کلاینت روی می دهد، یا زمانی که سرور درخواست استفاده از یک اتصال SSL/TLS برای اتصال ایمن SMTP دارد.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	این پیام زمانی ظاهر می شود که عدم تطابق SMTP بین سرور و کلاینت روی می دهد، یا زمانی که سرور درخواست استفاده از یک اتصال STARTTLS برای اتصال ایمن SMTP دارد.
The connection is untrusted. Check the following. - Date and Time	این پیام زمانی ظاهر می شود که تنظیم تاریخ و زمان اسکنر صحیح نیست یا گواهی منقضی شده است.
The connection is untrusted. Check the following. - CA Certificate	این پیام زمانی ظاهر می شود که اسکنر مطابق با سرور دارای گواهی ریشه نیست یا CA Certificate وارد نشده است.
The connection is not secured.	این پیام زمانی که گواهی دریافت شده خراب شده باشد.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	این پیام زمانی ظاهر می شود که عدم تطابق روش تأیید اعتبار بین سرور و کلاینت روی می 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 عدم تطابق روش تأیید اعتبار بین سرور و کلاینت روی می 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 آدرس ایمیل فرستنده تعیین شده اشتباه باشد.
Cannot access the product until processing is complete.	این پیام زمانی که اسکنر مشغول است ظاهر می شود.

اطلاعات مرتبط

◆ "بررسی اتصال سرور ایمیل" در صفحه 43

به‌روز رسانی نرم‌افزار داخلی

به‌روز رسانی نرم‌افزار داخلی با Web Config

نرم‌افزار داخلی را با Web Config به‌روز می‌کند. دستگاه باید به اینترنت متصل باشد.

1. از قسمت Web Config گزینه **Basic Settings** > **Firmware Update** را انتخاب کنید.
2. روی **Start** کلیک کنید.

   فرآیند تایید نرم‌افزار آغاز می‌شود و در صورت وجود نرم‌افزار به‌روز شده، اطلاعات نرم‌افزار نمایش داده می‌شود.
3. بر روی **Start** کلیک کنید و دستورالعمل‌های روی صفحه را دنبال نمایید.

نکته:
به‌روز رسانی نرم‌افزار با استفاده از *Epson Device Admin* نیز ممکن است. می‌توانید اطلاعات نرم‌افزار را در فهرست دستگاه‌ها ببینید. این قابلیت زمانی سودمند است که بخواهید نرم‌افزار چندین دستگاه را به‌روز کنید. برای کسب اطلاعات بیشتر به راهنمای *Epson Device Admin* مراجعه کنید.

اطلاعات مرتبط

◆ "دسترسی به Web Config" در صفحه 22
◆ "Epson Device Admin" در صفحه 52

به‌روز رسانی نرم‌افزار داخلی با Epson Firmware Updater

می‌توانید نرم‌افزار داخلی دستگاه را از وب‌سایت Epson بر روی رایانه خود بارگیری کنید و سپس دستگاه و رایانه را با کابل USB به هم وصل کنید تا به‌روز رسانی نرم‌افزار انجام بگیرد. اگر نتوانستید به‌روز رسانی را از طریق شبکه انجام دهید، این روش را امتحان کنید.

1. وارد وب‌سایت Epson شوید و نرم‌افزار داخلی را به‌روز نمایید.
2. رایانه حاوی نرم‌افزار دانلود شده را با کابل USB به دستگاه وصل کنید.
3. بر روی فایل .exe دانلود شده دو بار متوالی کلیک کنید.

   Epson Firmware Updater اجرا می‌شود.
4. دستورالعمل های روی صفحه را دنبال کنید.

پشتیبان‌گیری از تنظیمات

با صدور موارد تنظیم از Web Config می‌توانید آنها را در اسکنرهای دیگر کپی کنید.

صادر کردن تنظیمات

هر یک از تنظیمات اسکنر را صادر کنید.

1. به Web Config دسترسی یابید و سپس **Export and Import Setting Value** > **Export** را انتخاب کنید.

2. تنظیماتی را که می خواهید صادر کنید، انتخاب نمایید.

تنظیماتی را که می خواهید صادر کنید، انتخاب نمایید. اگر طبقه بندی اصلی را انتخاب کنید، طبقه بندی های فرعی نیز انتخاب می شون. با این حال طبقه بندی های فرعی که با تکرار در یک شبکه یکسان باعث بروز خطا می شوند (مانند آدرس های IP و مانند آن) را نمی توان انتخاب کرد.

3. یک رمز عبور برای رمزگذاری فایل صادر شده وارد کنید.

برای وارد کردن فایل به این رمز عبور نیاز خواهید داشت. اگر نمی خواهید فایل را رمز گذاری کنید، این قسمت را خالی نگه دارید.

4. روی **Export** کلیک کنید.

> **مهم:**
> اگر می خواهید تنظیمات شبکه اسکنر ماند نام اسکنر و آدرس *IP* را صادر کنید، ***Enable to select the individual settings of device*** را انتخاب کنید و موارد بیشتر را انتخاب کنید. برای اسکنر تعویضی فقط از مقادیر انتخاب شده استفاده کنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

وارد کردن تنظیمات

فایل Web Config صادر شده را بر اسکنر وارد کنید.

> **مهم:**
> هنگام وارد کردن مقادیری که شامل اطلاعات مجزا است مانند نام اسکنر یا آدرس *IP* دقت کنید که آدرس *IP* مشابه ای در شبکه وجود نداشته باشد. اگر آدرس *IP* همپوشانی و تکرار داشته باشد، اسکنر مقدار را منعکس نمی کند.

1. به Web Config دسترسی یابید و سپس **Import** < **Export and Import Setting Value** را انتخاب کنید.

2. فایل صادر شده را انتخاب کنید و سپس رمز عبور رمزگذاري شده را وارد کنید.

3. روی **Next** کلیک کنید.

4. تنظیماتی را که می خواهید وارد کنید انتخاب کرده و سپس روی **Next** کلیک کنید.

5. روی **OK** کلیک کنید.

تنظیمات در اسکنر اعمال می شوند.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

حل مشکل

نکاتی درباره حل مشکلات

می توانید اطلاعات بیشتری از دفترچه های راهنمای زیر پیدا کنید.

❑ راهنماي كاربر

دستورالعمل های استفاده از اسکنر، نگهداری و حل مشکلات را ارائه می دهد.

بررسی گزارش سرور و دستگاه شبکه

در صورت بروز مشکل در اتصال شبکه، ممکن است بتوانید دلیل آن را با بررسی گزارش سرور ایمیل، سرور LDAP و...، بررسی وضعیت با گزارش شبکه تجهیزات سیستم و فرمان‌ها، مانند روتر، شناسایی کنید.

مقدار-دهی تنظیمات شبکه

بازگردانی تنظیمات شبکه از صفحه کنترل

می توانید همه تنظیمات شبکه را به حالت پیش فرض بازگردانید.

1. از صفحه اصلی، بر روی **تنظیم** تلنگر بزنید.
2. بر روی **سرپرست سیستم** > **بازگشت به تنظیمات پیش فرض** > **تنظیمات شبکه** تلنگر بزنید.
3. پیام را بررسی کنید و بر روی **بله** تلنگر بزنید.
4. پس از ظاهر شدن پیام تکمیل فرآیند، بر روی **بستن** تلنگر بزنید.

اگر **بستن** را فشار ندهید، صفحه به طور خودکار و پس از مدت زمان مشخصی بسته می‌شود.

بررسی ارتباط دستگاه‌ها و رایانه

بررسی اتصال با دستور Ping — Windows

برای حصول اطمینان از درستی اتصال رایانه به اسکنر می‌توانید از دستور Ping استفاده کنید. برای بررسی اتصال با دستور Ping مراحل زیر را طی کنید.

1. نشانی IP اسکنر را در اتصال مورد استفاده بررسی کنید.

   این کار را می‌توانید با Epson Scan 2 انجام دهید.

حل مشکل

2. صفحه اعلان خط فرمان رایانه را نمایش دهید.

❑ Windows 10

بر روی دکمه Start راست-کلیک کنید یا آن را فشرده نگه دارید و **خط فرمان** را انتخاب کنید.

❑ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

صفحه برنامه را نشان دهید و سپس **خط فرمان** را انتخاب کنید.

❑ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 یا جدیدتر

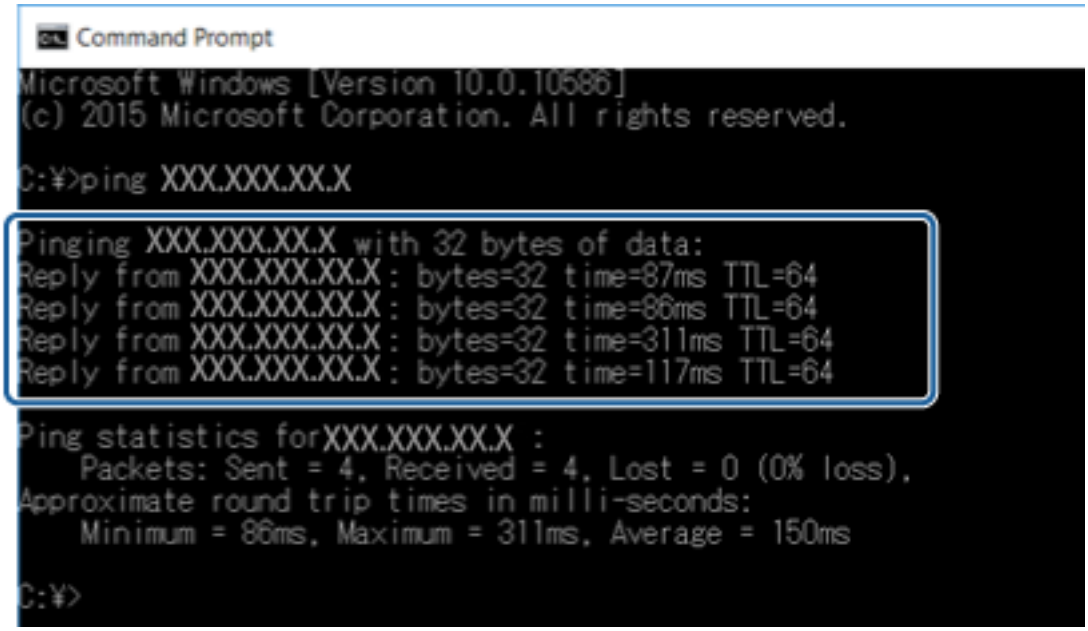
روی دکمه شروع کلیک کنید و **همه برنامه ها** یا **برنامه ها** > **برنامه های جانبی** > **خط فرمان** را انتخاب کنید.

3. بنویسید «ping xxx.xxx.xxx.xxx» و سپس کلید Enter را فشار دهید.

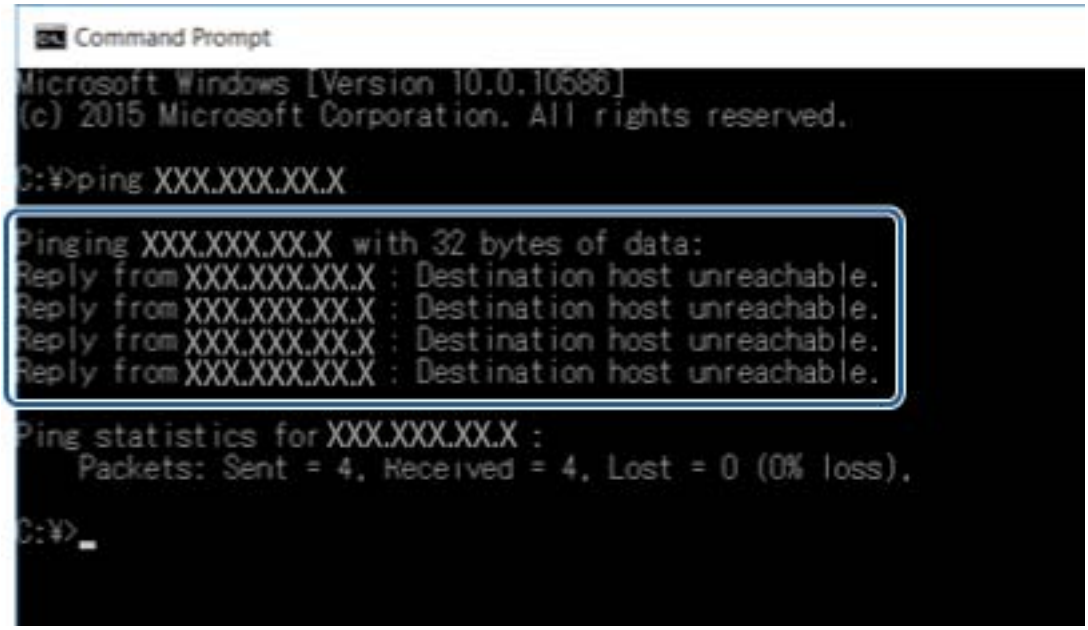
در قسمت xxx.xxx.xxx.xxx نشانی IP اسکنر را بنویسید.

4. وضعیت تبادل اطلاعات را بررسی کنید.

اگر اسکنر و رایانه در حال تبادل اطلاعات باشند، پیام زیر نشان داده می شود.



اگر اسکنر و رایانه در حال تبادل اطلاعات نباشند، پیام زیر نشان داده می شود.



بررسی اتصال با دستور Ping — Mac OS

برای حصول اطمینان از درستی اتصال رایانه به اسکنر می‌توانید از دستور Ping استفاده کنید. برای بررسی اتصال با دستور Ping مراحل زیر را طی کنید.

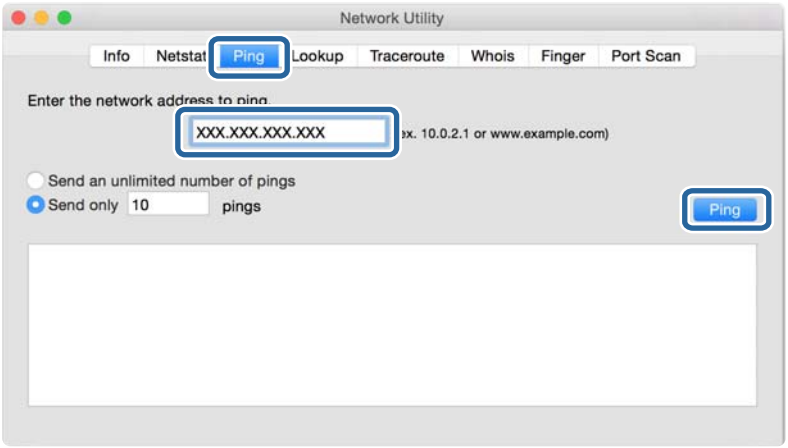
1. نشانی IP اسکنر را در اتصال مورد استفاده بررسی کنید.

   این کار را می‌توانید با Epson Scan 2 انجام دهید.

2. برنامه کمکی شبکه را اجرا کنید.

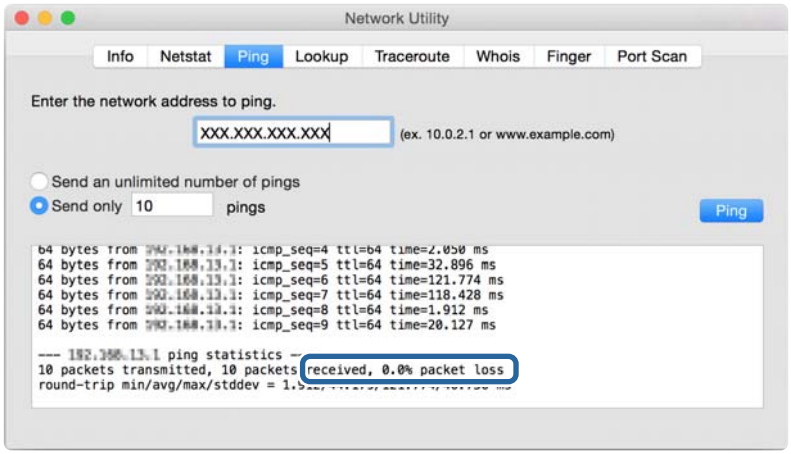
   در **Spotlight** "ابزار شبکه" را وارد کنید.

3. روی برگه **Ping** کلیک کنید و آدرس IP ای که می خواهید در مرحله 1 بررسی کنید را وارد کنید و سپس روی **Ping** کلیک کنید.

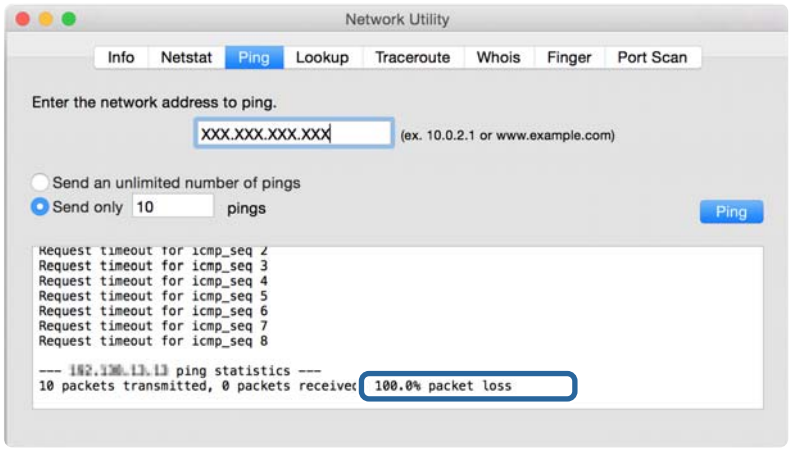


4. وضعیت تبادل اطلاعات را بررسی کنید.

اگر اسکنر و رایانه در حال تبادل اطلاعات باشند، پیام زیر نشان داده می شود.



اگر اسکنر و رایانه در حال تبادل اطلاعات نباشند، پیام زیر نشان داده می شود.



مشکلات مربوط به استفاده از نرم افزار شبکه

دسترسی به Web Config ممکن نیست

آیا آدرس IP اسکنر به درستی پیکربندی شده است؟

با استفاده از Epson Device Admin یا EpsonNet Config آدرس IP را پیکربندی کنید.

آیا مرورگر شما از رمزگذاری های عمده Encryption Strength برای SSL/TLS پشتیبانی می کند؟

رمزگذاری های عمده Encryption Strength برای SSL/TLS بصورت زیر هستند. Web Config فقط از مرورگری که از رمزگذاری های عمده زیر پشتیبانی می کند قابل دسترسی است. پشتیبانی رمزگذاری مرورگر خود را بررسی کنید.

- 80 بیت: AES256/AES128/3DES
- 112 بیت: AES256/AES128/3DES
- 128 بیت: AES256/AES128

❑ 192 بیت: AES256

❑ 256 بیت: AES256

پیام تاریخ گذشته زمان دسترسی به Web Config با استفاده از SSL (https) ارتباط.

اگر تاریخ گواهی گذشته است، دوباره گواهی را دریافت کنید. اگر پیام قبل از تاریخ انقضای آن ظاهر شود، دقت کنید تاریخ اسکنر به درستی پیکربندی شده باشد.

پیام "نام گواهی امنیتی مطابقت ندارد..." زمان دسترسی به Web Config با استفاده از SSL (https) ارتباط ظاهر می شود.

آدرس IP اسکنر وارد شده برای **Common Name** برای ایجاد یک گواهی خود امضاء یا CSR با آدرس وارد شده در مرورگر مطابقت ندارد. دوباره گواهی را دریافت و وارد کنید یا نام اسکنر را تغییر دهید.

اسکنر از طریق سرور پراکسی قابل دسترسی است.

اگر برای اسکنر از یک سرور پراکسی استفاده می کنید، لازم است تنظیمات پراکسی مرورگر خود را پیکربندی کنید.

❑ Windows:

گزینه **پانل کنترل** > **شبکه و اینترنت** > **گزینه های اینترنت** > **اتصالات** > **تنظیمات LAN** > **سرور پراکسی** را انتخاب کنید و سپس پیکربندی کنید که از سرور پراکسی برای آدرس های محلی استفاده نشود.

❑ Mac OS:

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

مثال ها:

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

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

اطلاعات مرتبط

◆ "دسترسی به Web Config" در صفحه 22

◆ "تخصیص نشانی IP" در صفحه 15

◆ "تخصیص نشانی IP با استفاده از " در صفحه 53EpsonNet Config

نام مدل و یا آدرس IP در EpsonNet Config نشان داده نمی شود

آیا مسدود کردن، لغو یا خاموش کردن را زمان نمایش صفحه امنیتی Windows یا صفحه فایروال انتخاب کردید؟

اگر **مسدود کردن**، **لغو** یا **خاموش کردن** را انتخاب کنید، آدرس IP و نام مدل در EpsonNet Config یا EpsonNet Setup نشان داده نمی شود.

برای تصحیح این مورد، EpsonNet Config را با استفاده از فایروال Windows و نرم افزار امنیتی تجاری به عنوان یک استثنا ثبت کنید. اگر از یک آنتی ویروس یا برنامه امنیتی استفاده می کنید، آن را ببندید و سپس از EpsonNet Config استفاده کنید.

آیا تنظیم زمان وقفه خطای ارتباطی بسیار کوتاه است؟

EpsonNet Config را اجرا کنید و **Tools** > **Options** > **Timeout** را انتخاب نمایید و سپس مدت زمان را برای تنظیم **Communication Error** افزایش دهید. توجه داشته باشید اینکار می تواند موجب کندتر اجرا شدن EpsonNet Config شود.

اطلاعات مرتبط

◆ "اجرای EpsonNet Config — " در صفحه 53Windows

◆ "اجرای EpsonNet Config — " در صفحه 53Mac OS

ضمیمه

معرفی نرم‌افزار شبکه

شرح نرم‌افزار پیکربندی و مدیریت دستگاه‌ها در ادامه می‌آید.

Epson Device Admin

Epson Device Admin برنامه ای است که به شما اجازه می دهد دستگاه ها را در شبکه نصب کنید، و سپس دستگاه ها را پیکربندی و مدیریت نمایید. دریافت اطلاعات مشروح دستگاه‌ها، مانند وضعیت و مواد مصرفی، ارسال پیام‌های هشدار و ایجاد گزارش مصرف دستگاه امکان‌پذیر است. می توانید یک الگو تهیه کنید که شامل موارد تنظیم باشد و آن را در سایر دستگاه ها به عنوان تنظیمات مشترک اعمال کنید. می توانید Epson Device Admin را از وب سایت پشتیبانی Epson دانلود کنید. برای دریافت اطلاعات بیشتر، به اسناد یا راهنمای Epson Device Admin مراجعه کنید.

اجرا کردن Epson Device Admin (فقط Windows)

همه برنامه‌ها > **EPSON** > **Epson Device Admin** > **Epson Device Admin** را انتخاب کنید.

نکته:
اگر هشدار فایروال ظاهر شود، به *Epson Device Admin* اجازه دسترسی دهید.

EpsonNet Config

EpsonNet Config به سرپرست اجازه می دهد تنظیمات شبکه اسکنر مانند تخصیص یک آدرس IP و تغییر حالت اتصال را پیکربندی کند. ویژگی تنظیم دسته‌ای در Windows پشتیبانی می شود. برای دریافت اطلاعات بیشتر، به اسناد یا راهنمای EpsonNet Config مراجعه کنید.

ضمیمه

اجرای WindowsEpsonNet Config —

همه برنامه ها > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config** را انتخاب کنید.

نکته:
اگر هشدار فایروال ظاهر شود، به *EpsonNet Config* اجازه دسترسی دهید.

اجرای Mac OSEpsonNet Config —

برو > **برنامه‌ها** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config** را انتخاب کنید.

EpsonNet SetupManager

EpsonNet SetupManager نرم افزاری برای ایجاد یک بسته برای نصب آسان اسکنر می باشد، مانند نصب و پیکربندی درایور اسکنر و نصب Document Capture Pro. این نرم افزار به سرپرست اجازه می دهد بسته نرم افزاری منحصر به فردی ایجاد کند و آنها را در میان گروه ها توزیع نماید.

برای دریافت اطلاعات بیشتر، از وب سایت محلی Epson دیدن نمایید.

تخصیص نشانی IP با استفاده از EpsonNet Config

با استفاده از EpsonNet Config می‌توانید نشانی IP به اسکنر اختصاص دهید. EpsonNet Config به شما امکان می‌دهد که پس از ایجاد اتصال با کابل اترنت، به اسکنر فاقد نشانی IP یک نشانی IP اختصاص بدهید.

تخصیص نشانی IP با تنظیمات دسته‌ای

ایجاد فایل برای تنظیمات دسته‌ای

با استفاده از نشانی MAC و نام مدل به عنوان کلید، می‌توانید فایل SYLK جدیدی برای تنظیم نشانی IP بسازید.

1. یک برنامه صفحه گسترده (مانند Microsoft Excel) یا ویرایشگر متن باز کنید.
2. Info_MACAddress، Info_ModelName و TCPIP_IPAddress را به عنوان نام گزینه تنظیم در نخستین سطر وارد کنید.

   گزینه‌های تنظیم را برای رشته‌های متنی زیر وارد کنید. برای ایجاد تمایز بین نویسه‌های بزرگ/کوچک و دو-بایتی/تک-بایتی، اگر فقط یک نویسه متفاوت باشد، مورد تشخیص داده نمی‌شود.

   نام گزینه تنظیم را به شکل زیر وارد کنید؛ در غیر این صورت، EpsonNet Config نمی‌تواند گزینه‌های تنظیم را تشخیص دهد.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. نشانی MAC، نام مدل و نشانی IP را برای همه رابط‌های شبکه وارد کنید.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102

0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. یک نام وارد کنید و به عنوان فایل SYLK (با پسوند .slk) ذخیره کنید.

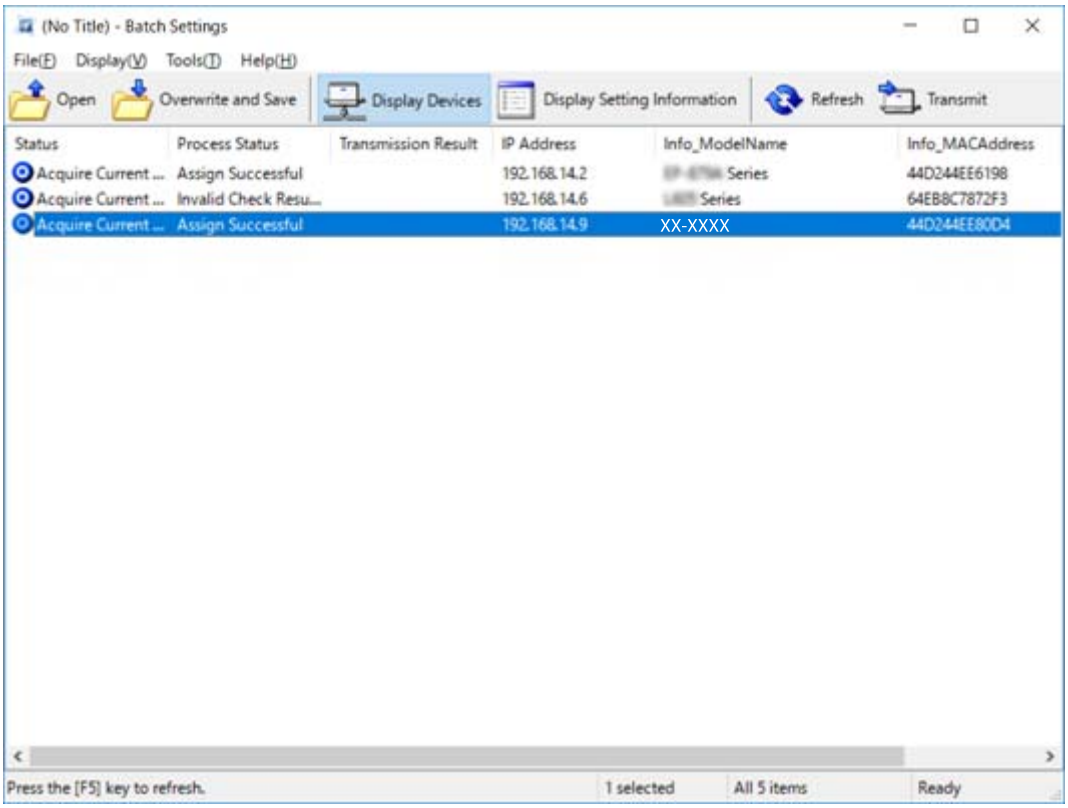
اعمال تنظیمات دسته‌ای با فایل پیکربندی

نشانی‌های IP را یک-باره در فایل پیکربندی (فایل SYLK) تخصیص دهید. فایل پیکربندی را باید پیش از تخصیص بسازید.

1. همه دستگاه‌ها را با کابل اترنت به شبکه وصل کنید.
2. اسکنر را روشن کنید.
3. EpsonNet Config را آغاز کنید.

   فهرست اسکنرهای متصل به شبکه ظاهر می‌شود. ظاهر شدن آنها کمی زمان می‌برد.
4. بر روی **Tools** > **Batch Settings** کلیک کنید.
5. روی **Open** کلیک کنید.
6. در صفحه انتخاب فایل، فایل حاوی تنظیمات (*.slk) را انتخاب و بر روی **Open** کلیک کنید.
7. دستگاه‌هایی را که می‌خواهید تنظیمات دسته‌ای را در آنها اعمال کنید انتخاب نمایید. برای این کار ستون **Status** را بر روی **Unassigned** و **Process Status** را بر روی **Assign Successful** تنظیم کنید.

   برای انتخاب چندین گزینه، دکمه Ctrl یا Shift را فشار دهید و کلیک کنید یا ماوس را بکشید.



8. روی **Transmit** کلیک کنید.

9. پس از ظاهر شدن صفحه ورود گذرواژه، آن را وارد و بر روی **OK** کلیک کنید.
تنظیمات را منتقل کنید.

نکته:
تا زمانی که نوار پیشرفت کامل شود، اطلاعات به رابط شبکه منتقل می‌شود. از خاموش کردن دستگاه یا آداپتور بی‌سیم و فرستادن داده به دستگاه بپرهیزید.

10. در صفحه **Transmitting Settings** بر روی **OK** کلیک کنید.

11. وضعیت دستگاه تنظیم شده را بررسی کنید.

برای دستگاه‌هایی که یا را نشان می‌دهند، محتویات فایل تنظیمات یا راه‌اندازی طبیعی دستگاه را بررسی کنید.

آیکون	Status	Process Status	توضیحات
	Setup Complete	Setup Successful	راه‌اندازی به صورت طبیعی انجام گرفته است.
	Setup Complete	Rebooting	پس از انتقال اطلاعات، اعمال تنظیمات مستلزم راه‌اندازی دوباره دستگاه است. بررسی صورت می‌گیرد تا مشخص شود که آیا دستگاه را می‌توان پس از راه‌اندازی متصل کرد یا خیر.
	Setup Complete	Reboot Failed	تایید دستگاه پس از انتقال تنظیمات ممکن نیست. از روشن بودن دستگاه یا راه‌اندازی عادی آن مطمئن شوید.
	Setup Complete	Searching	جستجوی دستگاه ثبت شده در فایل تنظیمات.*
	Setup Complete	Search Failed	بررسی دستگاه‌های قبلاً تنظیم شده ممکن نیست. از روشن بودن دستگاه یا راه‌اندازی عادی آن مطمئن شوید.*

* فقط در صورتی که اطلاعات تنظیم نمایش داده شود.

اطلاعات مرتبط

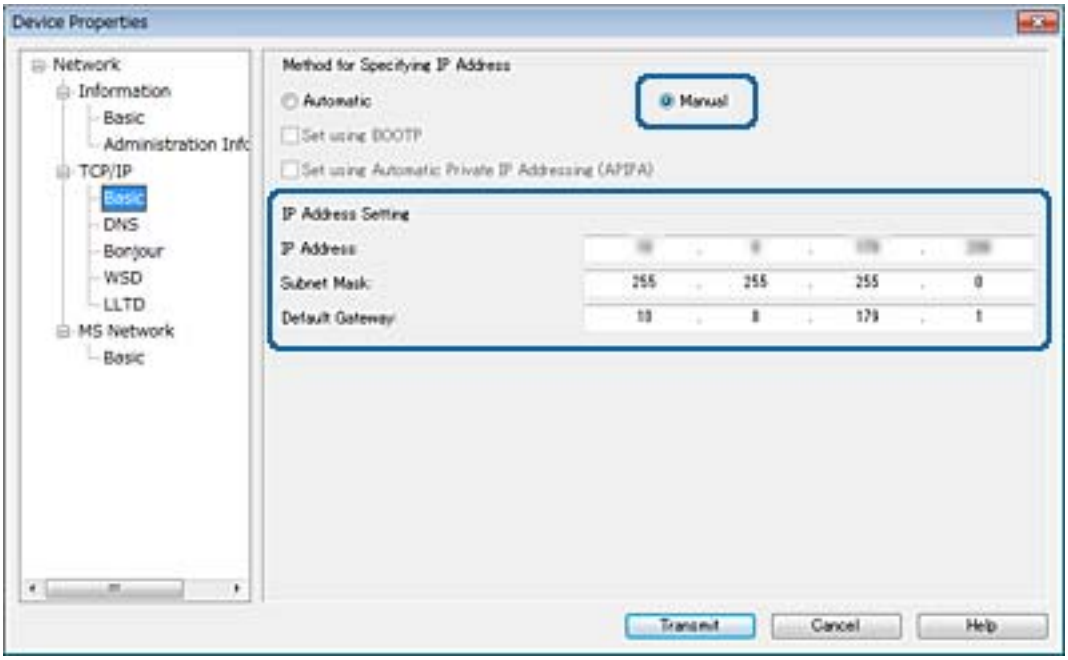
"اجرای EpsonNet Config — " در صفحه 53 Windows
"اجرای EpsonNet Config — " در صفحه 53 Mac OS

تخصیص دادن نشانی IP به دستگاه‌ها

با EpsonNet Config می‌توانید به اسکنر نشانی IP اختصاص دهید.

ضمیمه

1. اسکنر را روشن کنید.
2. اسکنر را با کابل اترنت به شبکه وصل کنید.
3. EpsonNet Config را آغاز کنید.
   فهرست اسکنرهای متصل به شبکه ظاهر می‌شود. ظاهر شدن آنها کمی زمان می‌برد.
4. روی اسکنری که می خواهید به آن نشانی تخصیص دهید دو بار کلیک کنید.
   نکته:
   اگر چندین اسکنر با مدل مشابه را متصل کرده باشید، می‌توانید اسکنر را با نشانی *MAC* شناسایی کنید.
5. **Network** < **TCP/IP** < **Basic** را انتخاب کنید.
6. نشانی‌های **IP Address**, **Subnet Mask** و **Default Gateway** را وارد کنید.



نکته:
برای متصل کردن اسکنر به شبکه امن نشانی ثابت وارد کنید.

7. روی **Transmit** کلیک کنید.
   صفحه تایید انتقال اطلاعات نمایش داده می‌شود.
8. روی **OK** کلیک کنید.
   صفحه تکمیل فرآیند انتقال نمایش داده می‌شود.

نکته:
اطلاعات به دستگاه منتقل می‌شود و پیام «پیکربندی با موفقیت انجام گرفت» نمایش داده می‌شود. از خاموش کردن دستگاه و فرستادن داده به سرویس بپرهیزید.

9. روی **OK** کلیک کنید.

اطلاعات مرتبط

◆ "اجرای EpsonNet Config — " در صفحه 53Windows

"اجرای EpsonNet Config — " در صفحه 53 Mac OS

استفاده از درگاه برای اسکنر

اسکنر از درگاه زیر استفاده می‌کند. سرپرست شبکه در صورت لزوم باید این درگاه‌ها را در دسترس قرار دهد.

فرستنده (مشتری)	مصرف	مقصد (سرور)	پروتکل	شماره درگاه
اسکنر	فرستادن ایمیل (اعلان ایمیل)	سرور SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP پیش از اتصال SMTP (اعلان ایمیل	سرور POP	(POP3 (TCP	110
	Control WSD	رایانه مشتری	WSD (TCP)	5357
	جستجوی رایانه در صورت اسکن لحظه‌ای از Document Capture Pro	رایانه مشتری	کشف اسکن لحظه‌ای شبکه	2968
	جمع‌آوری اطلاعات کار در صورت اسکن لحظه‌ای از Document Capture Pro	رایانه مشتری	اسکن لحظه‌ای شبکه	2968
رایانه مشتری	اسکنر را از برنامه‌ای مانند EpsonNet Config و درایور اسکنر کشف کنید.	اسکنر	ENPC (UDP)	3289
	از برنامه‌ای مانند EpsonNet Config و درایور اسکنر اطلاعات MIB جمع‌آوری و تنظیم کنید.	اسکنر	SNMP (UDP)	161
	جستجوی اسکنر WSD	اسکنر	WS-Discovery ((UDP	3702
	انتقال داده اسکن از Document Capture Pro	اسکنر	اسکن شبکه (TCP)	1865

تنظیمات امنیتی پیشرفته مربوط به شرکت

در این فصل، ما امکانات امنیتی پیشرفته را شرح می‌دهیم.

تنظیمات امنیتی و پیشگیری از خطر

اگر دستگاهی به شبکه متصل شود، می‌توانید از راه دور به آن دسترسی پیدا کنید. در ضمن، بسیاری از افراد می‌توانند دستگاه را به اشتراک بگذارند و کارآیی و راحتی را افزایش دهند. هر چند، احتمال دسترسی غیرقانونی، استفاده غیرمجاز و دستگاری داده‌ها افزایش می‌یابد. اگر از دستگاه در محیط متصل به اینترنت استفاده کنید، خطرها بیشتر نیز می‌شود.

برای پیشگیری از این خطرها، دستگاه‌های Epson از فناوری‌های امنیتی مختلفی بهره می‌گیرند.

در صورت لزوم دستگاه 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
ارتباط SSL/TLS	مسیر ارتباط رایانه و دستگاه با ارتباط SSL/TLS رمزگذاری می‌شود. محتوای انتقال از طریق مرورگر، محافظت می‌شود.	برای سرور گواهی CA تنظیم کنید. این گواهی را CA (نهاد صدور گواهی) برای دستگاه صادر می‌کند.	مانع نشت اطلاعات تنظیم و محتویات داده‌های منتقل شده از رایانه به اسکنر شوید. مسیر دسترسی اینترنتی به سرور Epson از دستگاه را می‌توان با به‌روز رسانی نرم‌افزار و... محافظت کرد.
IP فیلترینگ/IPsec	می‌توانید ترتیبی دهید که بریدن و قطع کردن داده‌هایی که از طرف مشتری خاصی است یا نوع خاصی دارد، ممکن شود. از آنجا که IPsec با واحد بسته IP (رمزگذاری و تایید هویت) از داده‌ها محافظت می‌کند، می‌توانید پروتکل اسکن را بدون خطر منتقل کنید.	سیاستی ابتدایی و سیاستی فردی ایجاد کنید و مشتری یا نوع داده دارای قابلیت دسترسی به دستگاه را مشخص نمایید.	از دسترسی غیرمجاز و رهگیری داده‌های ارتباط با دستگاه جلوگیری کنید.
SNMPv3	قابلیت‌هایی مانند پایش دستگاه‌های متصل، سلامت داده‌های پروتکل کنترل SNMP، رمزگذاری، تایید هویت کاربر و... افزوده شده است.	SNMPv3 را فعال و روش تایید هویت و رمزگذاری را مشخص کنید.	تغییر تنظیمات از شبکه و محرمانه بودن پایش وضعیت را تضمین کنید.
IEEE802.1X	فقط به کاربری که هویت آن برای اترنت تایید شده است، اجازه اتصال می‌دهد. فقط به کاربر مجاز اجازه استفاده از دستگاه را می‌دهد.	تنظیم تایید هویت در سرور RADIUS (سرور تایید هویت).	از دسترسی غیرمجاز و استفاده غیرمجاز از دستگاه جلوگیری کنید.
خواندن کارت شناسایی	با نگه داشتن کارت شناسایی روی دستگاه تایید هویت متصل می‌توانید از دستگاه استفاده کنید. می‌توانید دریافت گزارش مربوط به کاربران و دستگاه و نیز کاربرد دستگاه و قابلیت‌های آن برای هر کاربر و گروه را محدود کنید.	دستگاه تایید هویت را به دستگاه وصل کنید و اطلاعات کاربر را در سیستم تایید هویت تنظیم کنید.	مانع تقلب و استفاده غیرمجاز از دستگاه شوید.

اطلاعات مرتبط

- "ارتباط SSL/TLS با اسکنر" در صفحه 59
- "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 67
- "استفاده از پروتکل SNMPv3" در صفحه 77
- "اتصال اسکنر به شبکه IEEE802.1X" در صفحه 79

تنظیمات عملکرد امنیتی

در هنگام تنظیم کردن IPsec/فیلترینگ IP یا IEEE802.1X، برای انتقال اطلاعات تنظیم بهتر است با استفاده از SSL/TLS وارد Web Config شوید تا مشکلات امنیتی مانند دستکاری یا رهگیری کاهش یابد.

ارتباط SSL/TLS با اسکنر

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

درباره گواهی دیجیتالی

❏ گواهی امضاء شده از طریق CA

گواهی امضاء شده از طریق CA (مرجع صدور گواهی) باید از یک مرجع صدور گواهی به دست آمده باشد. با استفاده از گواهی امضاء شده از طریق CA می توانید از ارتباطات ایمن اطمینان داشته باشید. می توانید از گواهی امضاء شده از طریق CA برای هر ویژگی امنیتی استفاده کنید.

❏ گواهی CA

گواهی CA نشان می دهد شخص ثالث هویت سرور را تأیید کرده است. این یک مؤلفه مهم در سبک امنیت از طریق افزونه web-of-trust است. لازم است یک گواهی CA از CA (مرجع صدور گواهی) که آن را صادر می کند برای تأیید اعتبار سرور دریافت کنید.

❏ گواهی خود امضاء

گواهی خود امضاء گواهی است که اسکنر صادر و آن را امضاء می کند. این گواهی غیرقابل اعتماد است و نمی تواند از تقلب جلوگیری کند. اگر از این گواهی برای یک گواهی SSL/TLS استفاده کنید، ممکن است یک هشدار امنیتی بر روی مرورگر نشان داده شود. از این گواهی فقط می توانید برای یک ارتباط SSL/TLS استفاده کنید.

اطلاعات مرتبط

- "دریافت و وارد کردن گواهی امضاء شده از طریق CA" در صفحه 59
- "حذف گواهی امضاء شده از طریق CA" در صفحه 63
- "به روزرسانی گواهی خود امضاء" در صفحه 64

دریافت و وارد کردن گواهی امضاء شده از طریق CA

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. به Web Config دسترسی یابید و سپس **Network Security Settings** را انتخاب کنید. سپس **SSL/TLS** > **Certificate** یا **IPsec/IP Filtering** > **Client Certificate** یا **IEEE802.1X** > **Client Certificate** را انتخاب کنید.
2. روی **Generate** از **CSR** کلیک کنید.

   صفحه ایجاد CSR باز می شود.

تنظیمات امنیتی پیشرفته مربوط به شرکت

3. برای هر مورد یک مقدار وارد کنید.

نکته:
طول کلید موجود و مخفف سازی ها 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. **Network Security Settings** را انتخاب کنید. سپس **SSL/TLS** > **Certificate** یا **IPsec/IP Filtering** > **Client Certificate** یا **IEEE802.1X** > **Client Certificate** را انتخاب کنید.

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

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

7. CSR را برای مرجع صدور گواهی ارسال کنید و یک CA-signed Certificate دریافت کنید.

قوانین مربوط به مرجع صدور گواهی برای شکل و روش ارسال را دنبال کنید.

8. CA-signed Certificate صادر شده را در رایانه متصل به اسکنر ذخیره کنید.

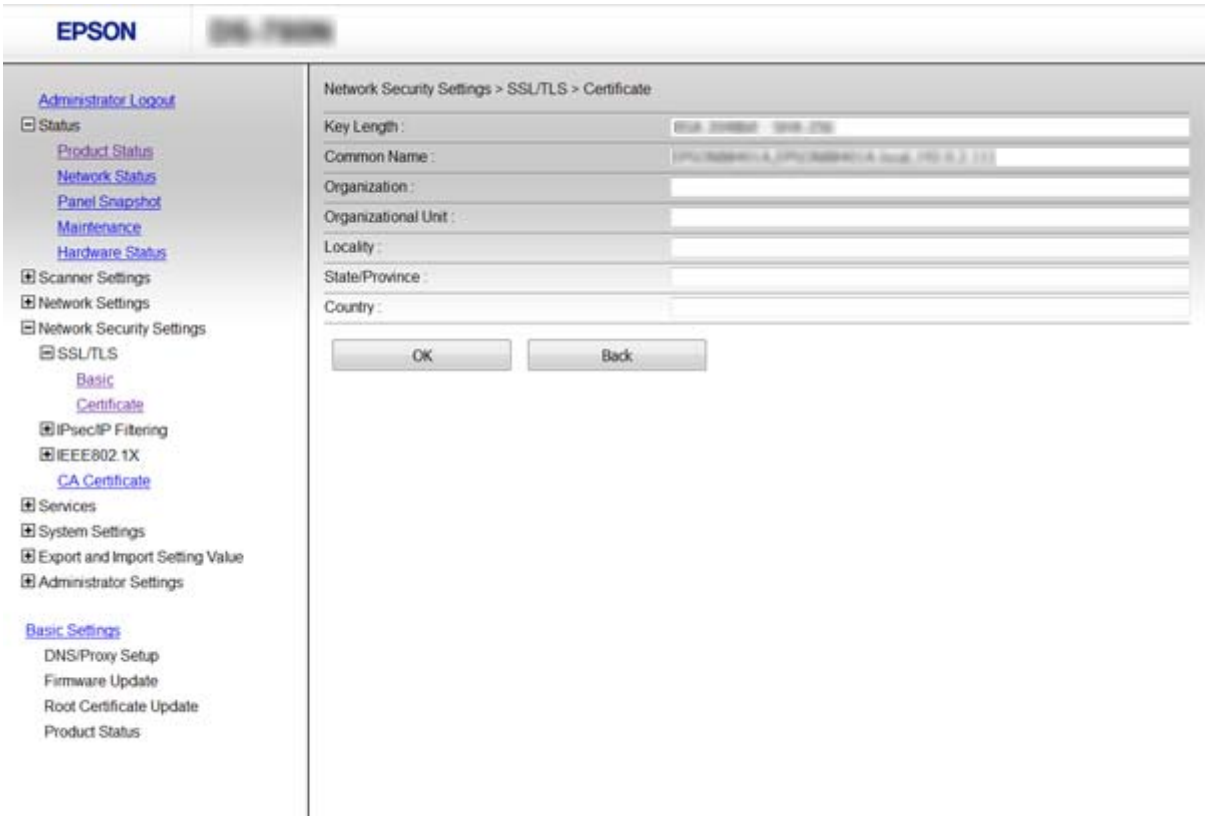
زمانی که گواهی را در مقصد ذخیره کنید دریافت CA-signed Certificate کامل است.

اطلاعات مرتبط

- "دسترسی به Web Config" در صفحه 22
- "موارد تنظیم مقصد" در صفحه 61
- "وارد کردن گواهی امضاء شده از طریق CA" در صفحه 61

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد تنظیم مقصد



موارد	تنظیمات و توضیحات
Key Length	طول کلید را برای یک CSR انتخاب کنید.
Common Name	می توانید بین 1 تا 128 نویسه وارد کنید. اگر این یک آدرس IP است، باید یک آدرس IP ایستا باشد. مثال ها: URL برای دسترسی به Web Config: https://10.152.12.225 نام مشترک: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	می توانید بین 0 تا 64 نویسه با فرمت ASCII (0x20–0x7E) وارد کنید. می توانید نام های متمایز را با ویرگول جدا کنید.
Country	یک کد کشور دو رقمی که توسط ISO-3166 تعیین شده وارد کنید.

اطلاعات مرتبط

"دریافت گواهی امضاء شده از طریق CA" در صفحه 59

وارد کردن گواهی امضاء شده از طریق CA

مهم:

- دقت کنید که تاریخ و زمان اسکنر به درستی تنظیم شده باشد.
- اگر با استفاده از *CSR* که از *Web Config* ایجاد شده است یک گواهی دریافت کنید، می توانید زمانی یک گواهی وارد کنید.

تنظیمات امنیتی پیشرفته مربوط به شرکت

1. به Web Config دسترسی یابید و سپس **Network Security Settings** را انتخاب کنید. سپس **SSL/TLS** > **Certificate** یا **IPsec/IP Filtering** > **Client Certificate** یا **IEEE802.1X** > **Client Certificate** را انتخاب کنید.
2. روی **Import** کلیک کنید.

   صفحه وارد کردن گواهی باز می شود.
3. برای هر مورد یک مقدار وارد کنید.

   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 فرمت PEM/DER از قسمت زیر دریافت شده باشد Web Config
     - **Private Key**: پیکربندی نکنید زیرا اسکنر محتوی یک کلید خصوصی است.
     - **Password**: پیکربندی نکنید.
     - **CA Certificate 2/CA Certificate 1**: اختیاری
   - یک گواهی با فرمت 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 فرمت 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:

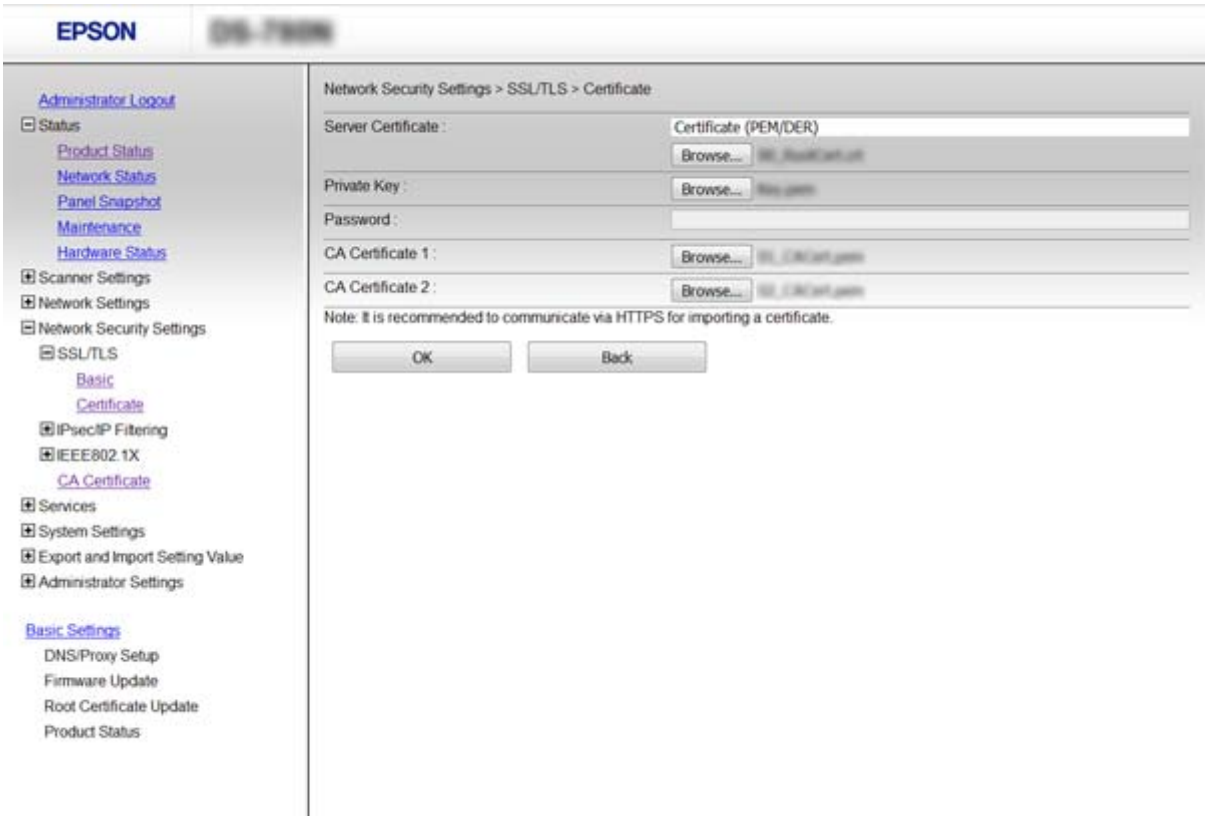
بر روی ***Confirm*** برای تأیید اطلاعات گواهی کلیک کنید.

اطلاعات مرتبط

- "دسترسی به Web Config" در صفحه 22
- "موارد تنظیم وارد کردن گواهی امضاء شده از طریق CA" در صفحه 63

تنظیمات امنیتی پیشرفته مربوط به شرکت

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



موارد	تنظیمات و توضیحات
Server Certificate یا Client Certificate	فرمت گواهی را انتخاب کنید.
Private Key	اگر با استفاده از یک CSR که از رایانه ایجاد شده است، گواهی با فرمت PEM/DER دریافت کنید، یک فایل کلید خصوصی که با گواهی مطابقت دارد تعیین کنید.
Password	یک رمز عبور برای رمزگذاری کلید خصوصی وارد کنید.
CA Certificate 1	اگر فرمت گواهی **Certificate (PEM/DER)** است، یک گواهی از مرجع صدور گواهی که گواهی سرور صادر می کند وارد کنید. اگر نیاز است یک فایل تعیین کنید.
CA Certificate 2	اگر فرمت گواهی **Certificate (PEM/DER)** است، یک گواهی از مرجع صدور گواهی که **CA Certificate 1** صادر می کند وارد کنید. اگر نیاز است یک فایل تعیین کنید.

اطلاعات مرتبط

"وارد کردن گواهی امضاء شده از طریق CA" در صفحه 61

حذف گواهی امضاء شده از طریق CA

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

مهم:

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

تنظیمات امنیتی پیشرفته مربوط به شرکت

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

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

به روزرسانی گواهی خود امضاء

اگر اسکنر از ویژگی سرور HTTPS پشتیبانی می کند، می توانید گواهی خود امضاء را به روزرسانی کنید. زمان دسترسی به Web Config با استفاده از گواهی خود امضاء، یک پیام هشدار ظاهر می شود.

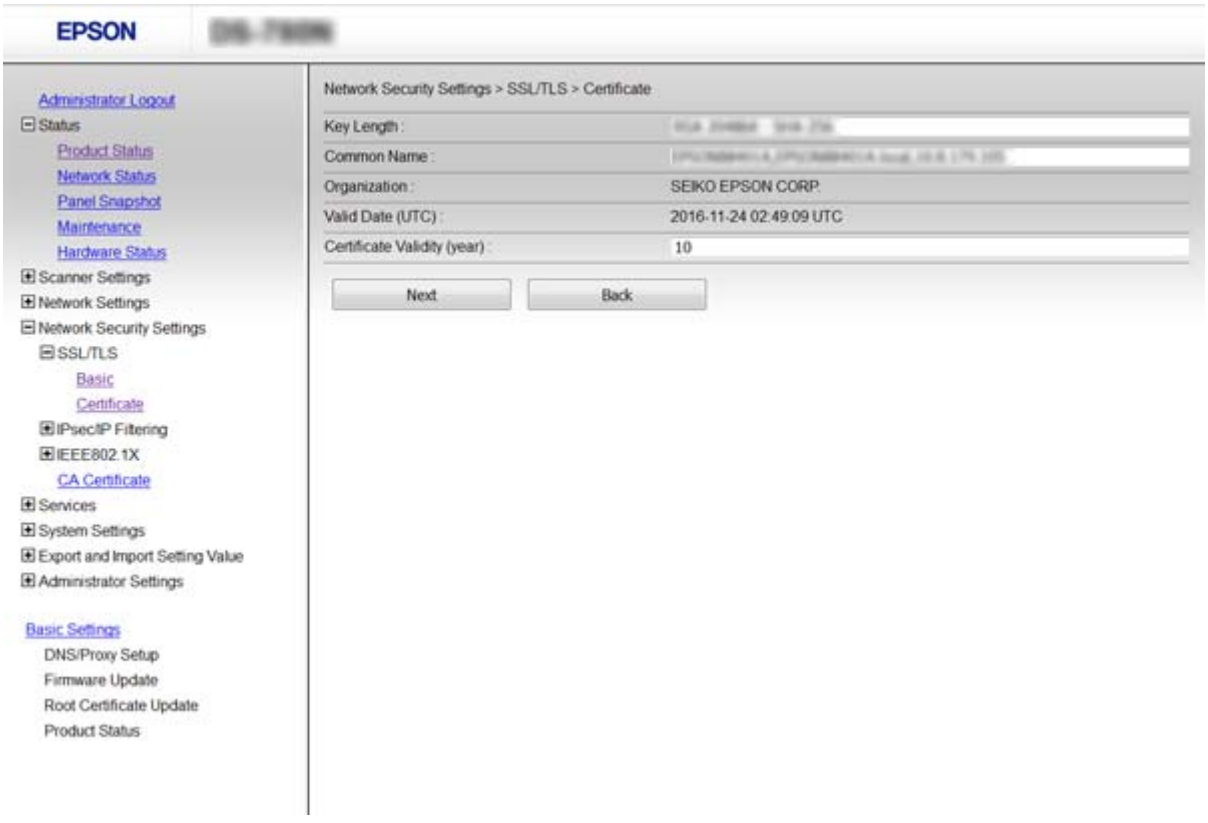
از گواهی خود امضاء به طور موقت استفاده کنید تا گواهی امضاء شده از طریق CA را دریافت و وارد کنید.

1. به Web Config دسترسی یابید و **Network Security Settings** > **SSL/TLS** > **Certificate** را انتخاب کنید.
2. روی **Update** کلیک کنید.
3. **Common Name** را وارد کنید.

یک آدرس IP یا یک تأیید کننده مانند یک نام FQDN برای اسکنر وارد کنید. می توانید بین 1 تا 128 نویسه وارد کنید.

نکته:
می توانید نام های متمایز (*CN*) را با ویرگول جدا کنید.

4. یک دوره اعتبار برای گواهی مشخص کنید.



5. روی **Next** کلیک کنید.
   یک پیام تأیید نشان داده می شود.
6. روی **OK** کلیک کنید.
   اسکنر به روزرسانی می شود.

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

اطلاعات مرتبط

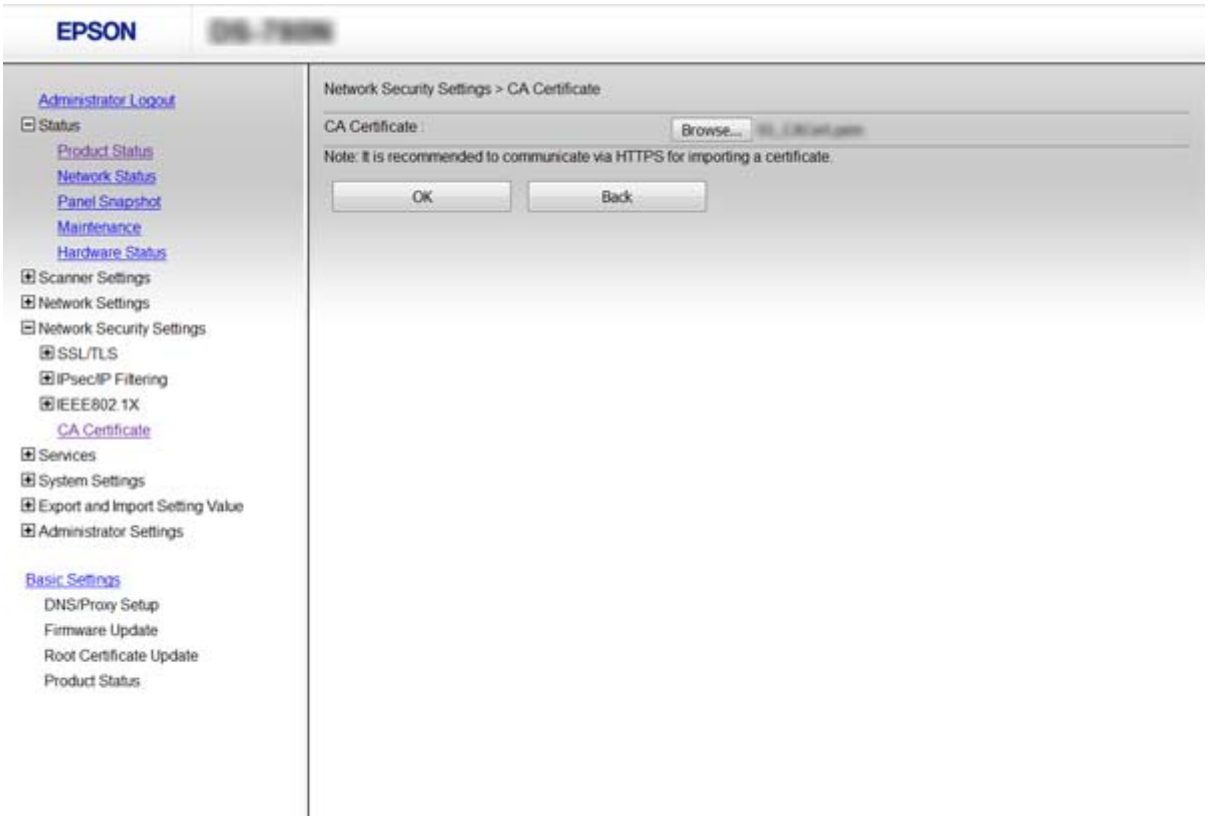
"دسترسی به Web Config" در صفحه 22

CA Certificate را پیکربندی کنید

می توانید CA Certificate را وارد کنید، نمایش دهید یا حذف کنید.

وارد کردن CA Certificate

1. به Web Config دسترسی یابید و سپس **Network Security Settings** > **CA Certificate** را انتخاب کنید.
2. روی **Import** کلیک کنید.
3. CA Certificate که می خواهید وارد کنید را مشخص کنید.



4. روی **OK** کلیک کنید.

تنظیمات امنیتی پیشرفته مربوط به شرکت

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

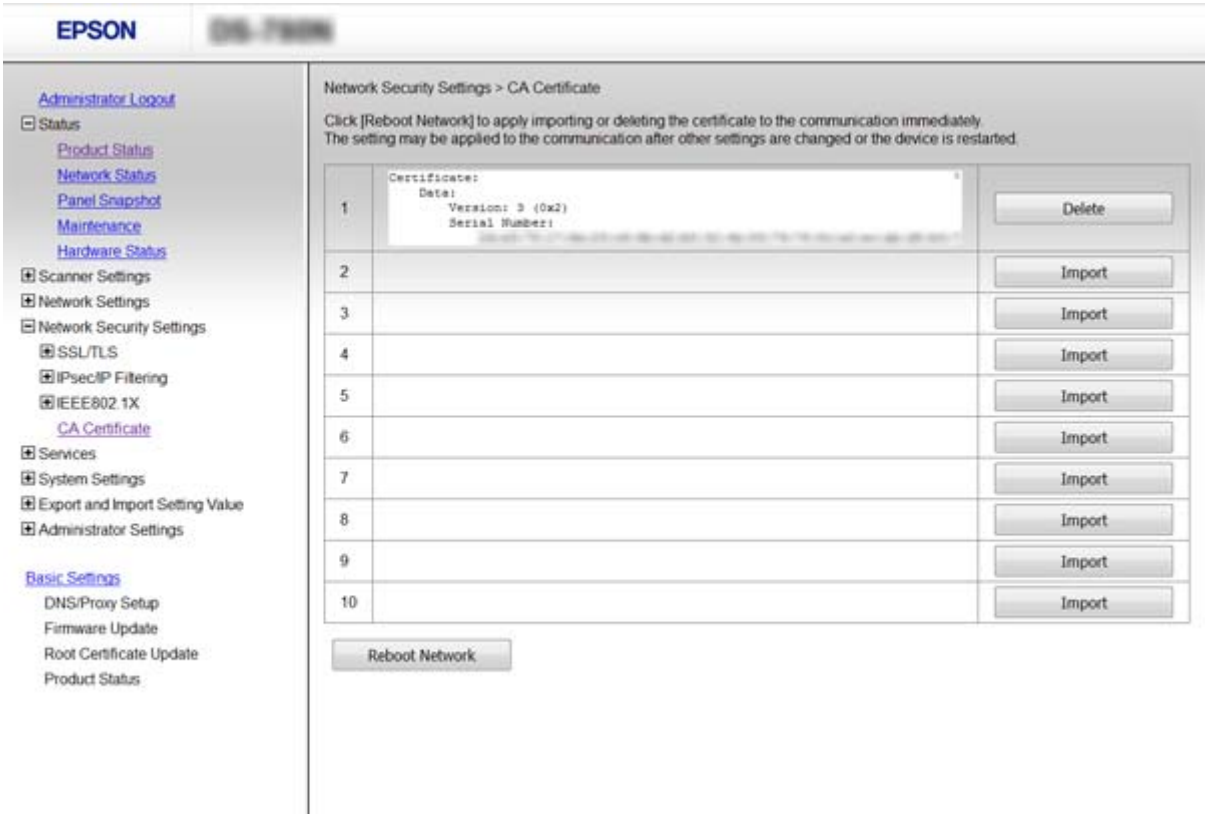
اطلاعات مرتبط

"دسترسی به Web Config در صفحه 22"

حذف یک CA Certificate

می توانید CA Certificate وارد شده را حذف کنید.

1. به Web Config دسترسی یابید و سپس **Network Security Settings** > **CA Certificate** را انتخاب کنید.
2. روی **Delete** در کنار CA Certificate که می خواهید حذف کنید، کلیک کنید.



3. در پیام نشان داده شده، تایید کنید که می خواهید گواهی را حذف کنید.

اطلاعات مرتبط

"دسترسی به Web Config در صفحه 22"

ارتباط رمزگذاری شده با IPsec/فیلترینگ IP

درباره IPsec/IP Filtering

اگر اسکنر از IPsec/IP Filtering پشتیبانی می کند، می توانید بر اساس آدرس های IP، سرویس ها و پورت، ترافیک را فیلتر کنید. با ترکیب فیلترینگ، می توانید اسکنر را برای پذیرفتن یا مسدود کردن کلاینت های تعیین شده و داده های تعیین شده پیکربندی کنید. علاوه بر این، می توانید سطح امنیتی را با استفاده از یک IPsec بهبود ببخشید.

برای فیلتر کردن ترافیک، سیاست پیش فرض را پیکربندی کنید. سیاست پیش فرض برای هر کاربر یا گروه متصل به اسکنر اعمال می شود. برای کنترل دقیق تر کاربران و گروه های کاربران، سیاست های گروهی را پیکربندی کنید. 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.

نکته:
رایانه هایی که با *Windows Vista* یا نسخه جدیدتر یا *Windows Server 2008* یا نسخه جدیدتر کار می کنند از *IPsec* پشتیبانی می کنند.

پیکربندی Default Policy

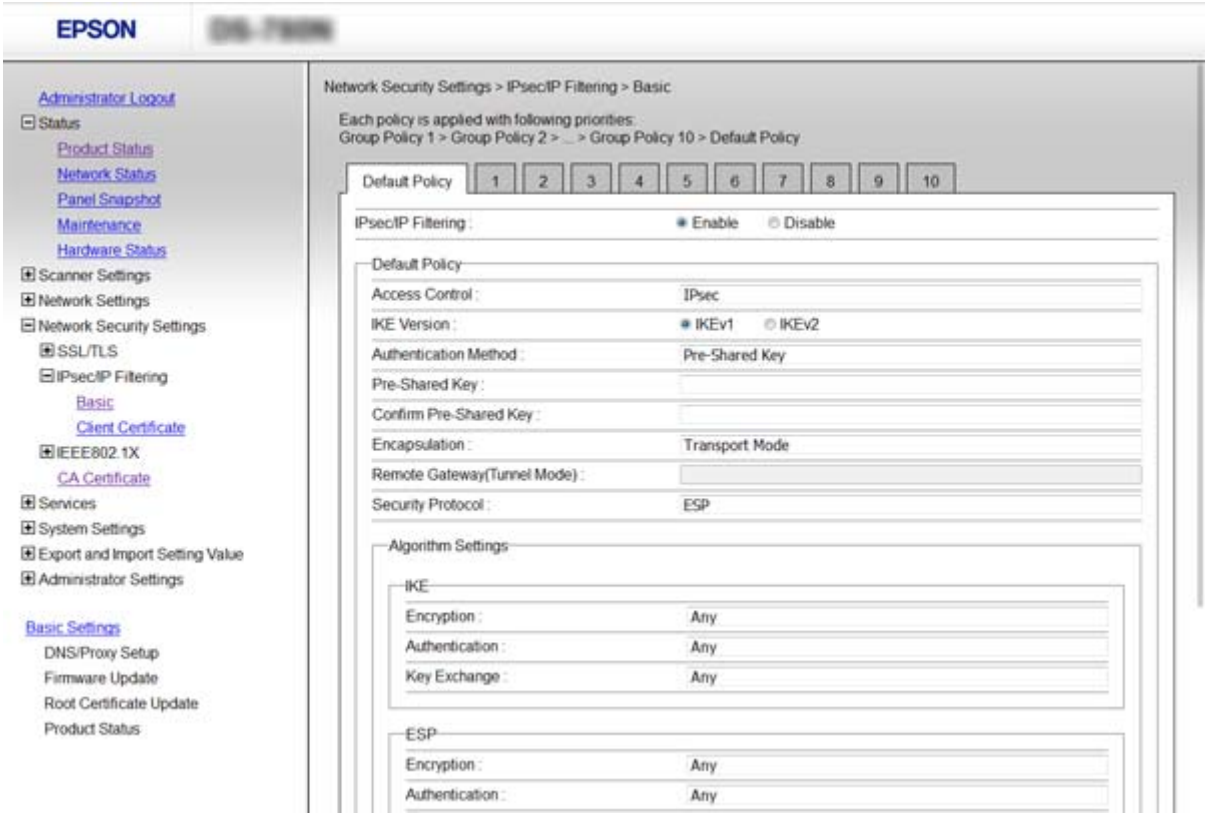
1. به Web Config دسترسی یابید و **Network Security Settings** > **IPsec/IP Filtering** > **Basic** را انتخاب کنید.
2. برای هر مورد یک مقدار وارد کنید.
3. روی **Next** کلیک کنید.
   یک پیام تأیید نشان داده می شود.
4. روی **OK** کلیک کنید.
   اسکنر به روزرسانی می شود.

اطلاعات مرتبط

◆ "دسترسی به Web Config" در صفحه 22
◆ "موارد تنظیم Default Policy" در صفحه 68

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد تنظیم Default Policy



موارد	تنظیمات و توضیحات	
IPsec/IP Filtering	می توانید ویژگی IPsec/فیلترینگ IP را فعال یا غیرفعال کنید.	
Access Control	یک روش کنترل برای ترافیک بسته های IP پیکربندی کنید.	
	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	IKEv1 یا IKEv2 را برای نسخه IKE انتخاب کنید. یکی از آنها را با توجه به دستگاه متصل به اسکنر انتخاب کنید.	
IKEv1	اگر **IKEv1** را برای **IKE Version** انتخاب کنید، موارد زیر نمایش داده می‌شود.	
	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 می‌شود.	

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد		تنظیمات و توضیحات
Local	Authentication Method	برای انتخاب **Certificate**، لازم است از قبل یک گواهی امضاء شده از طریق CA دریافت و وارد کنید.
	ID Type	نوع شناسه اسکنر را انتخاب کنید.
	ID	شناسه اسکنر را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. = را نیز باید حساب کنید. **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 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. @ را نیز باید حساب کنید. **Key ID**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.
Remote	Authentication Method	برای انتخاب **Certificate**، لازم است از قبل یک گواهی امضاء شده از طریق CA دریافت و وارد کنید.
	ID Type	نوع شناسه را برای دستگاهی که می‌خواهید تایید کنید، انتخاب نمایید.
	ID	شناسه اسکنر را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. = را نیز باید حساب کنید. **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 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. @ را نیز باید حساب کنید. **Key ID**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.
Encapsulation	اگر **IPsec** را برای **Access Control** انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.	
	Transport Mode	اگر در LAN مشابه فقط از اسکنر استفاده می کنید، این را انتخاب کنید. بسته های IP لایه 4 یا لایه بعد رمزگذاری می شوند.
	Tunnel Mode	اگر از اسکنر در شبکه دارای اینترنت مانند IPsec-VPN استفاده می کنید، این گزینه را انتخاب کنید. عنوان و داده بسته های IP رمزگذاری می شوند.
Remote Gateway(Tunnel Mode)	اگر **Tunnel Mode** را برای **Encapsulation** انتخاب می کنید، یک آدرس درگاه بین 1 و 39 نویسه وارد کنید.	

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد		تنظیمات و توضیحات
Security Protocol		**IPsec** برای **Access Control**، یک گزینه انتخاب کنید.
	ESP	برای اطمینان از یکپارچگی تأیید اعتبار و داده این را انتخاب کنید، و داده را رمزگذاری کنید.
	AH	برای اطمینان از یکپارچگی تأیید اعتبار و داده این را انتخاب کنید. حتی اگر رمزگذاری داده ممنوع باشد، می توانید از IPsec استفاده کنید.
Algorithm Settings		
IKE	Encryption	الگوریتم رمزگذاری را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می‌کند.
	Authentication	الگوریتم تایید هویت را برای IKE انتخاب کنید.
	Key Exchange	الگوریتم تبادل کلید را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می‌کند.
ESP	Encryption	الگوریتم رمزگذاری را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
	Authentication	الگوریتم تایید هویت را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
AH	Authentication	الگوریتم رمزگذاری را برای AH انتخاب کنید. این زمانی موجود است که **AH** برای **Security Protocol** انتخاب شده باشد.

اطلاعات مرتبط

"پیکربندی Default Policy" در صفحه 67

پیکربندی Group Policy

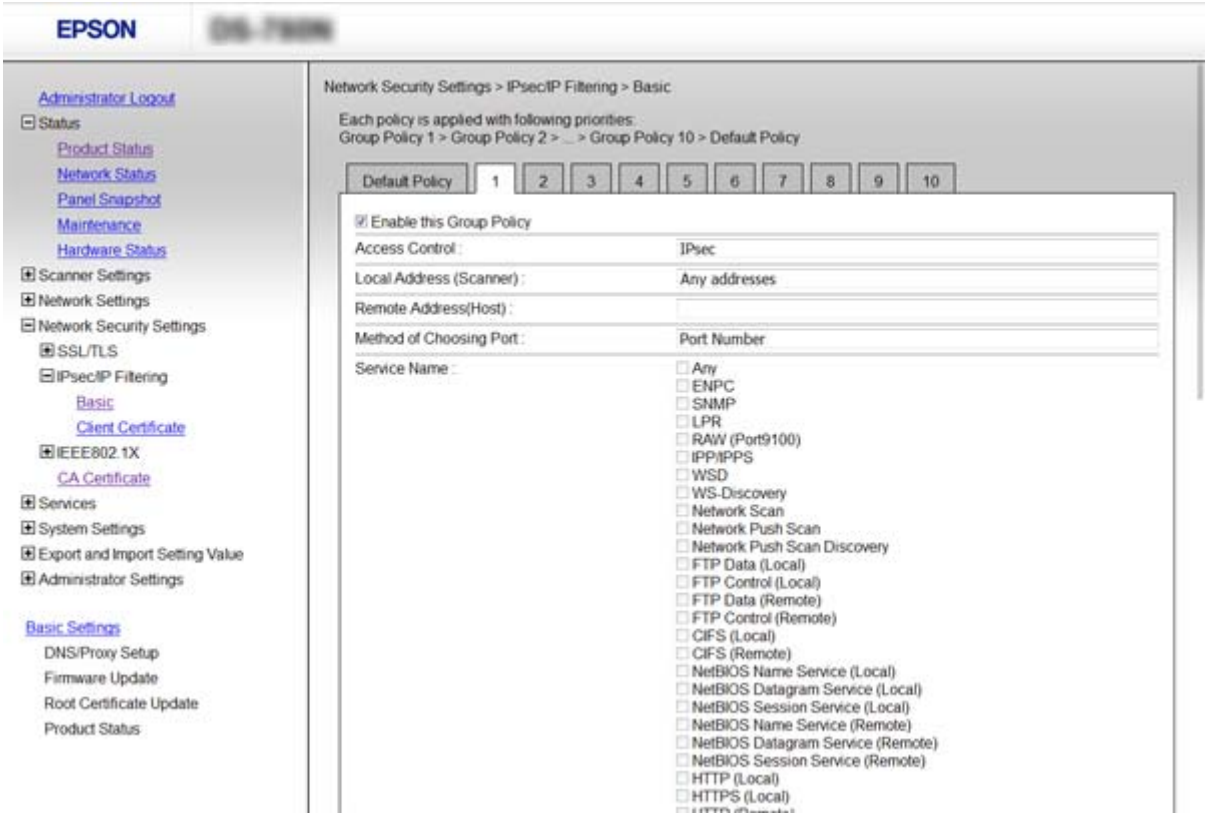
1. به Web Config دسترسی یابید و **Network Security Settings** > **IPsec/IP Filtering** > **Basic** را انتخاب کنید.
2. روی زبانه عددی که می خواهید پیکربندی کنید کلیک نمایید.
3. برای هر مورد یک مقدار وارد کنید.
4. روی **Next** کلیک کنید.
   یک پیام تأیید نشان داده می شود.
5. روی **OK** کلیک کنید.
   اسکنر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

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22
"موارد تنظیم Group Policy" در صفحه 71

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد تنظیم Group Policy



موارد	تنظیمات و توضیحات	
Enable this Group Policy	می توانید یک سیاست گروهی را فعال یا غیرفعال کنید.	
Access Control	یک روش کنترل برای ترافیک بسته های IP پیکربندی کنید.	
	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.	
Remote Address(Host)	برای کنترل دسترسی یک آدرس IP دستگاه وارد کنید. نشانی 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* ایستا پیکربندی کنید.	
Method of Choosing Port	روشی برای تعیین پورت ها انتخاب کنید.	
Service Name	اگر **Service Name** را برای **Method of Choosing Port** انتخاب می کنید، یک گزینه انتخاب نمایید.	

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد	تنظیمات و توضیحات	
Transport Protocol	اگر **Port Number** را برای **Method of Choosing Port** انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.	
	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 پینگ این را انتخاب کنید.
Local Port	اگر **Port Number** را برای **Method of Choosing Port** و اگر **TCP** یا **UDP** را برای **Transport Protocol** انتخاب می کنید، شماره های پورت را برای کنترل بسته های دریافتی، جداسازی آنها با ویرگول وارد نمایید. می توانید حداکثر تا 10 شماره پورت وارد کنید. مثلاً: 20، 80، 119، 5220 اگر شماره پورت را وارد نکنید، همه پورت ها کنترل می شوند.	
Remote Port	اگر **Port Number** را برای **Method of Choosing Port** و اگر **TCP** یا **UDP** را برای **Transport Protocol** انتخاب می کنید، شماره های پورت را برای کنترل بسته های ارسالی، جداسازی آنها با ویرگول وارد نمایید. می توانید حداکثر تا 10 شماره پورت وارد کنید. مثلاً: 25، 80، 143، 5220 اگر شماره پورت را وارد نکنید، همه پورت ها کنترل می شوند.	
IKE Version	IKEv1 یا IKEv2 را برای نسخه IKE انتخاب کنید. یکی از آنها را با توجه به دستگاه متصل به اسکنر انتخاب کنید.	
IKEv1	اگر **IKEv1** را برای **IKE Version** انتخاب کنید، موارد زیر نمایش داده می‌شود.	
	Authentication Method	اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید. گواهی استفاده شده با یک سیاست پیش فرض همراه است.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.
IKEv2	اگر **IKEv2** را برای **IKE Version** انتخاب کنید، موارد زیر نمایش داده می‌شود.	

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد	تنظیمات و توضیحات	
Local	Authentication Method	اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید. گواهی استفاده شده با یک سیاست پیش فرض همراه است.
	ID Type	نوع شناسه اسکنر را انتخاب کنید.
	ID	شناسه اسکنر را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. = را نیز باید حساب کنید. **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 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. @ را نیز باید حساب کنید. **Key ID**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.
Remote	Authentication Method	اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید. گواهی استفاده شده با یک سیاست پیش فرض همراه است.
	ID Type	نوع شناسه را برای دستگاهی که می‌خواهید تایید کنید، انتخاب نمایید.
	ID	شناسه اسکنر را که با نوع شناسه مطابقت دارد وارد کنید. نویسه نخست نباید @، # یا = باشد. **Distinguished Name**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. = را نیز باید حساب کنید. **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 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید. @ را نیز باید حساب کنید. **Key ID**: بین 1 تا 128نویسه اسکی یک-بایتی (0x20 تا 0x7E) وارد کنید.
	Pre-Shared Key	اگر **Pre-Shared Key** را برای **Authentication Method** انتخاب می کنید، یک کلید از قبل مشترک شده بین 1 و 127 نویسه وارد کنید.
	Confirm Pre-Shared Key	کلیدی که برای تأیید پیکربندی کردید وارد نمایید.
Encapsulation	اگر **IPsec** را برای **Access Control** انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.	
	Transport Mode	اگر در LAN مشابه فقط از اسکنر استفاده می کنید، این را انتخاب کنید. بسته های IP لایه 4 یا لایه بعد رمزگذاری می شوند.
	Tunnel Mode	اگر از اسکنر در شبکه دارای اینترنت مانند IPsec-VPN استفاده می کنید، این گزینه را انتخاب کنید. عنوان و داده بسته های IP رمزگذاری می شوند.
Remote Gateway(Tunnel Mode)	اگر **Tunnel Mode** را برای **Encapsulation** انتخاب می کنید، یک آدرس درگاه بین 1 و 39 نویسه وارد کنید.	

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد		تنظیمات و توضیحات
Security Protocol		اگر **IPsec** را برای **Access Control** انتخاب می کنید، یک گزینه انتخاب نمایید.
	ESP	برای اطمینان از یکپارچگی تأیید اعتبار و داده این را انتخاب کنید، و داده را رمزگذاری کنید.
	AH	برای اطمینان از یکپارچگی تأیید اعتبار و داده این را انتخاب کنید. حتی اگر رمزگذاری داده ممنوع باشد، می توانید از IPsec استفاده کنید.
Algorithm Settings		
IKE	Encryption	الگوریتم رمزگذاری را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می‌کند.
	Authentication	الگوریتم تایید هویت را برای IKE انتخاب کنید.
	Key Exchange	الگوریتم تبادل کلید را برای IKE انتخاب کنید. موارد بسته به نسخه IKE فرق می‌کند.
ESP	Encryption	الگوریتم رمزگذاری را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
	Authentication	الگوریتم تایید هویت را برای ESP انتخاب کنید. این زمانی موجود است که **ESP** برای **Security Protocol** انتخاب شده باشد.
AH	Authentication	الگوریتم تایید هویت را برای AH انتخاب کنید. این زمانی موجود است که **AH** برای **Security Protocol** انتخاب شده باشد.

اطلاعات مرتبط

- "پیکربندی Group Policy" در صفحه 70
- "ترکیب Local Address (Scanner) و Remote Address(Host) در Group Policy" در صفحه 74
- "مرجع نام سرویس در سیاست گروهی" در صفحه 75

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

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

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

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

*3 به جز آدرس های لینک محلی IPv6.

مرجع نام سرویس در سیاست گروهی

نکته:
سرویس های که موجود نباشند نمایش داده می شوند ولی نمی توانند انتخاب شوند.

نام سرویس	نوع پروتکل	شماره پورت محلی	شماره پورت از راه دور	ویژگی های کنترل شده
Any	-	-	-	همه سرویس ها
ENPC	UDP	3289	هر پورتی	جستجو برای اسکنر از برنامه هایی مانند EpsonNet Config، و درایور اسکنر
SNMP	UDP	161	هر پورتی	دستیابی و پیکربندی MIB از برنامه هایی مانند EpsonNet Config و درایور اسکنر Epson
WSD	TCP	هر پورتی	5357	کنترل WSD
WS-Discovery	UDP	3702	هر پورتی	جستجو برای اسکنر از WSD
Network Scan	TCP	1865	هر پورتی	ارسال داده اسکن از Document Capture Pro
Network Push Scan Discovery	UDP	2968	هر پورتی	جستجوی رایانه از اسکنر.
Network Push Scan	TCP	هر پورتی	2968	دستیابی به اطلاعات کار اسکن لحظه‌ای از Document Capture Pro یا Document Capture
HTTP (Local)	TCP	80	هر پورتی	سرور HTTP (ارسال داده Web Config و WSD)
HTTPS (Local)	TCP	443	هر پورتی	
HTTP (Remote)	TCP	هر پورتی	80	کلاینت HTTP(S) (ارتباط بین به روزرسانی نرم افزار داخلی و به روزرسانی گواهی ریشه)
HTTPS (Remote)	TCP	هر پورتی	443	

پیکربندی مثال های IPsec/IP Filtering

دریافت فقط بسته های IPsec

این مثال فقط برای پیکربندی یک سیاست پیش فرض است.

Default Policy:

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

Group Policy:

پیکربندی نکنید.

پذیرش اسکن با استفاده از Epson Scan 2 و تنظیمات اسکنر

این مثال ارتباطات داده اسکن و پیکربندی اسکنر از سرویس های تعیین شده را مجاز می کند.

تنظیمات امنیتی پیشرفته مربوط به شرکت

Default Policy:

❑ **IPsec/IP Filtering**: **Enable**

❑ **Access Control**: **Refuse Access**

Group Policy:

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

❑ **Access Control**: **Permit Access**

❑ **Remote Address(Host)**: آدرس IP کلاینت

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

❑ **Service Name**: کادر **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** و **HTTPS (Local)** را علامت بزنید.

دریافت دسترسی فقط از یک آدرس IP تعیین شده

این مثال آدرس IP تعیین شده برای دسترسی به اسکنر را مجاز می کند.

Default Policy:

❑ **IPsec/IP Filtering**: **Enable**

❑ **Access Control**:**Refuse Access**

Group Policy:

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

❑ **Access Control**: **Permit Access**

❑ **Remote Address(Host)**: آدرس IP از یک کلاینت سرپرست

نکته:

با وجود پیکربندی سیاست، کلاینت می تواند به اسکنر دسترسی داشته باشد و آن را پیکربندی کند.

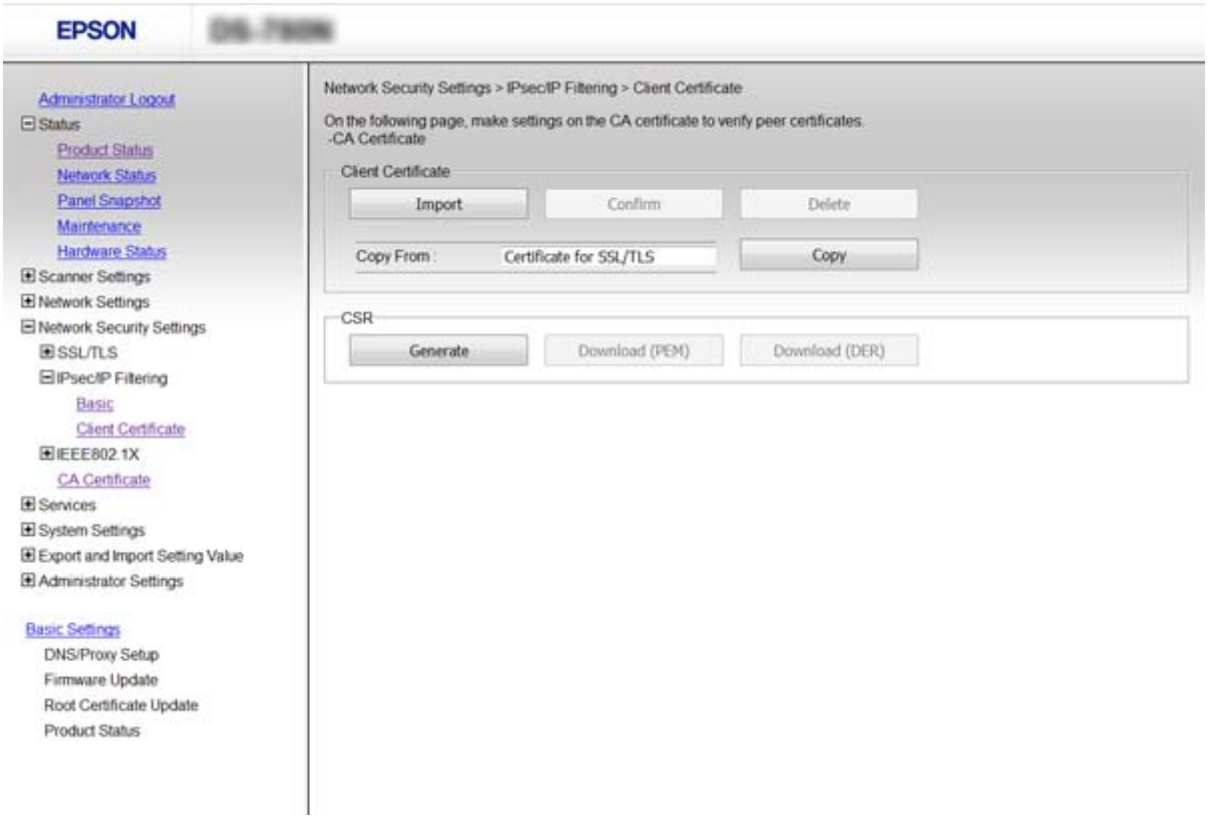
پیکربندی گواهی برای IPsec/IP Filtering

گواهی کلاینت برای فیلترینگ IPsec/IP را پیکربندی کنید. اگر می خواهید مرجع صدور گواهی را پیکربندی کنید به **CA Certificate** بروید.

1. به Web Config دسترسی یابید و **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate** را انتخاب کنید.

2. گواهی را در **Client Certificate** وارد کنید.

اگر قبلا یک گواهی نشر شده توسط مرجع صدور گواهی را در IEEE802.1X یا SSL/TLS وارد کرده اید، می توانید گواهی را کپی کنید و در فیلترینگ IPsec/IP کپی کنید. برای کپی کردن، گواهی را از **Copy From** انتخاب کنید و سپس روی **Copy** کلیک کنید.



اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22
"دریافت و وارد کردن گواهی امضاء شده از طریق CA" در صفحه 59

استفاده از پروتکل SNMPv3

درباره SNMPv3

SNMP پروتکلی است که کار پایش و کنترل را برای جمع‌آوری اطلاعات دستگاه‌های متصل به شبکه انجام می‌دهد. SNMPv3 نسخه قابلیت امنیت مدیریت است که توسعه یافته است.

در صورت استفاده از SNMPv3، پایش وضعیت و تغییرات تنظیم ارتباط SNMP (بسته) را می‌توان برای محافظت از ارتباط SNMP (بسته) در برابر خطرهای شبکه مانند استراق سمع، جعل هویت و دستکاری، تایید و رمزگذاری کرد.

پیکربندی SNMPv3

اگر اسکنر از پروتکل SNMPv3 پشتیبانی می کند، می توانید دسترسی به اسکنر را کنترل کنید.

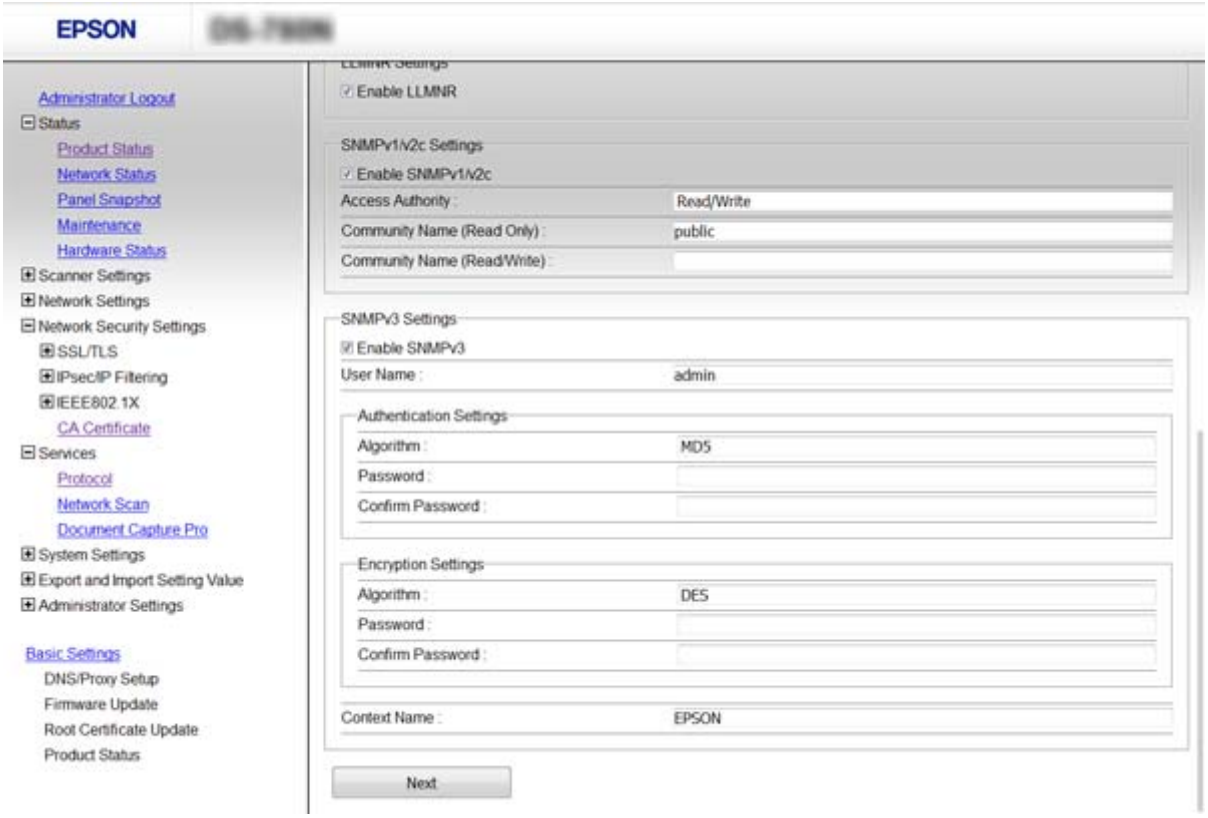
1. به Web Config دسترسی یابید و **Protocol** < **Services** را انتخاب کنید.

2. مقداری برای هر مورد **SNMPv3 Settings** وارد کنید.
3. روی **Next** کلیک کنید.
   یک پیام تأیید نشان داده می شود.
4. روی **OK** کلیک کنید.
   اسکنر به روزرسانی می شود.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22
"موارد تنظیم SNMPv3" در صفحه 78

موارد تنظیم SNMPv3



موارد	تنظیمات و توضیحات
Enable SNMPv3	زمانی که کادر علامت داشته باشد، SNMPv3 فعال می شود.
User Name	بین 1 تا 32 نویسه با استفاده از نویسه های 1 بایتی وارد کنید.
Authentication Settings	
Algorithm	یک الگوریتم برای تأیید اعتبار انتخاب کنید.
Password	بین 8 تا 32 نویسه با فرمت ASCII ((0x20–0x7E)) وارد کنید.
Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید وارد نمایید.

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد	تنظیمات و توضیحات
Encryption Settings	
Algorithm	یک الگوریتم برای رمزگذاری انتخاب کنید.
Password	بین 8 تا 32 نویسه با فرمت ASCII ((0x20–0x7E) وارد کنید.
Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید وارد نمایید.
Context Name	بین 1 تا 32 نویسه با استفاده از نویسه های 1 بایتی وارد کنید.

اطلاعات مرتبط

"پیکربندی SNMPv3" در صفحه 77

اتصال اسکنر به شبکه IEEE802.1X

پیکربندی شبکه IEEE802.1X

اگر اسکنر از IEEE802.1X پشتیبانی می کند، می توانید از اسکنر بر روی شبکه دارای تأیید که به سرور RADIUS و یک هاب به عنوان تأیید کننده وصل است استفاده کنید.

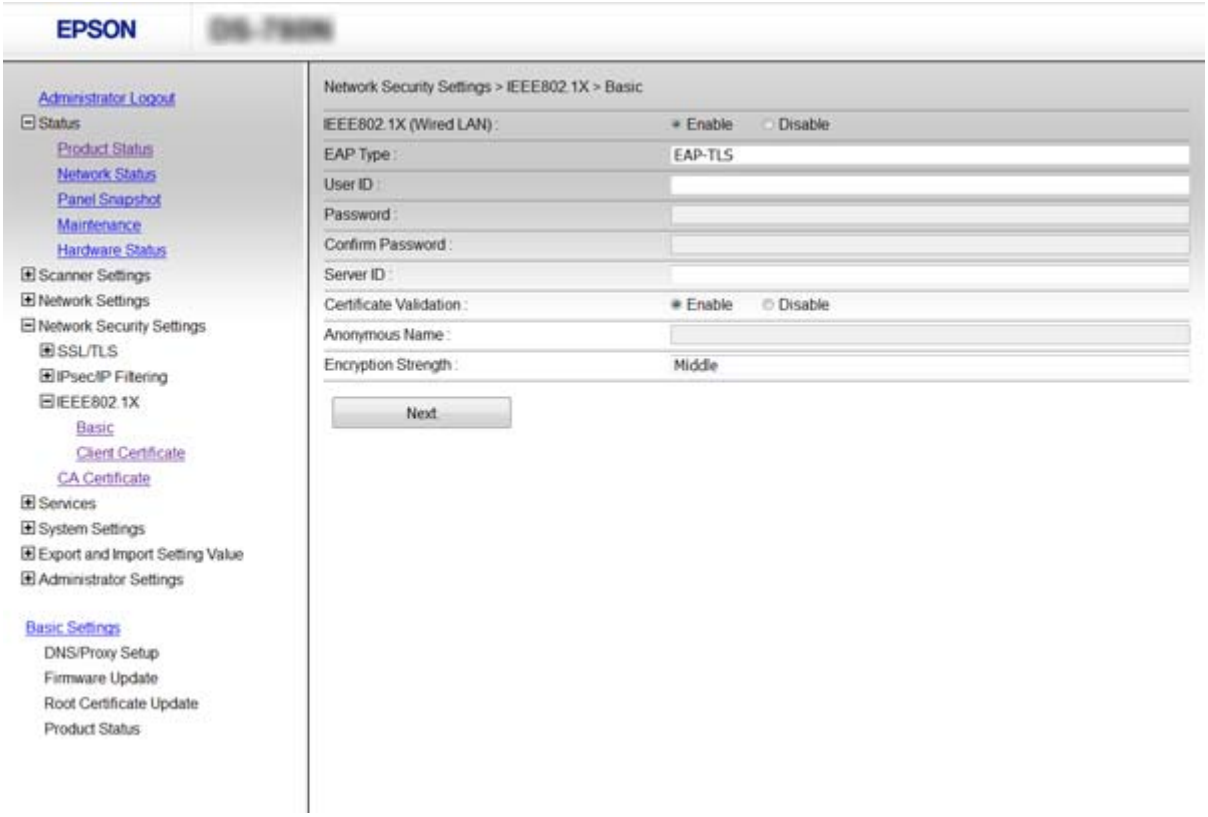
1. به Web Config دسترسی یابید و **Network Security Settings** > **IEEE802.1X** > **Basic** را انتخاب کنید.
2. برای هر مورد یک مقدار وارد کنید.
3. روی **Next** کلیک کنید.
   یک پیام تأیید نشان داده می شود.
4. روی **OK** کلیک کنید.
   اسکنر به روزرسانی می شود.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22
"موارد تنظیم شبکه IEEE802.1X" در صفحه 80
"بعد از پیکربندی IEEE802.1X نمی توانید به چاپگر یا اسکنر دسترسی داشته باشید" در صفحه 84

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد تنظیم شبکه IEEE802.1X



موارد	تنظیمات و توضیحات	
IEEE802.1X (Wired LAN)	می توانید تنظیمات صفحه (**Basic** < **IEEE802.1X**) برای LANIEEE802.1X باسیم) را فعال یا غیرفعال کنید.	
EAP Type	گزینه ای برای یک روش تأیید اعتبار بین اسکنر و سرور RADIUS انتخاب کنید.	
	EAP-TLS	لازم است یک گواهی امضاء شده از طریق CA دریافت و وارد کنید.
	PEAP-TLS	
	PEAP/MSCHAPv2	لازم است یک رمز عبور پیکربندی کنید.
User ID	برای استفاده از تأیید اعتبار یک سرور RADIUS، یک شناسه پیکربندی کنید. بین 1 تا 128نویسه اسکی 1-بایت (0x20 تا 0x7E) وارد کنید.	
Password	برای تأیید اعتبار اسکنر یک رمز عبور پیکربندی کنید. بین 1 تا 128نویسه اسکی 1-بایت (0x20 تا 0x7E) وارد کنید. اگر از سرور Windows به عنوان سرور RADIUS استفاده می کنید می توانید تا 127 نویسه را وارد کنید.	
Confirm Password	رمز عبوری که برای تأیید پیکربندی کردید وارد نمایید.	
Server ID	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 128نویسه اسکی 1-بایت (0x20 تا 0x7E) وارد کنید.	
Certificate Validation	مستقل از روش تأیید اعتبار می توانید تایید گواهی را تعیین کنید. گواهی را در **CA Certificate** وارد کنید.	

تنظیمات امنیتی پیشرفته مربوط به شرکت

موارد	تنظیمات و توضیحات	
Anonymous Name	اگر **PEAP-TLS** یا **PEAP/MSCHAPv2** را برای **Authentication Method** انتخاب کنید، می توانید یک نام ناشناس به جای شناسه کاربر برای مرحله 1 تأیید اعتبار PEAP پیکربندی کنید. بین 0 تا 128نویسه اسکی 1-بایت (0x20 تا 0x7E) وارد کنید.	
Encryption Strength	می توانید یکی از موارد زیر را انتخاب کنید.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

اطلاعات مرتبط

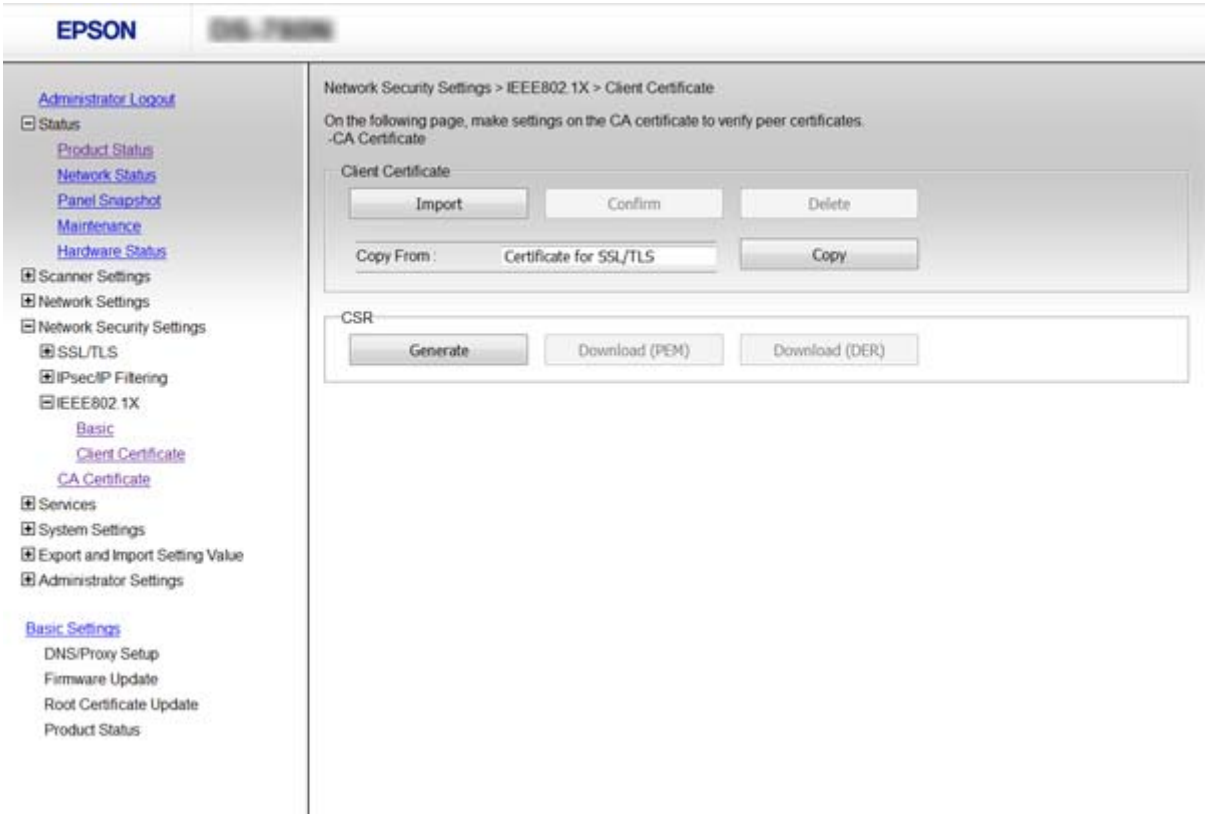
"پیکربندی شبکه IEEE802.1X" در صفحه 79

پیکربندی گواهی برای IEEE802.1X

گواهی کلاینت برای IEEE802.1X را پیکربندی کنید. اگر می خواهید گواهی مرجع صدور گواهی را پیکربندی کنید به **CA Certificate** بروید.

1. به Web Config دسترسی یابید و **Network Security Settings** < **IEEE802.1X** < **Client Certificate** را انتخاب کنید.
2. در **Client Certificate** یک گواهی وارد کنید.

اگر گواهی توسط مرجع صدور گوای منتشر شده باشد، می توانید گواهی را کپی کنید. برای کپی کردن، گواهی را از **Copy From** انتخاب کنید و سپس روی **Copy** کلیک کنید.



اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22
"دریافت و وارد کردن گواهی امضاء شده از طریق CA" در صفحه 59

رفع مشکلات مربوط به امنیت پیشرفته

بازگرداندن تنظیمات امنیتی

اگر می‌خواهید محیطی بسیار امن مانند IPsec/فیلترینگ IP یا IEEE802.1X 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 پانل کنترل

IPsec/فیلترینگ IP یا IEEE802.1X را می‌توانید از پانل کنترل اسکنر غیرفعال کنید.

1. روی **تنظیم** > **تنظیمات شبکه** تلنگر بزنید.
2. روی **تغییر تنظیمات** ضربه بزنید.
3. بر روی گزینه مورد نظر برای غیرفعال کردن تلنگر بزنید.
   - ❏ **فیلتر IPsec/IP**
   - ❏ **IEEE802.1X**
4. پس از ظاهر شدن پیام تکمیل فرآیند، بر روی **ادامه** تلنگر بزنید.

بازگرداندن عملکرد امنیتی با استفاده از Web Config

برای IEEE802.1X، شناسایی دستگاه‌ها ممکن است بر روی شبکه ممکن نباشد. در این صورت، عملکرد را با استفاده از پانل کنترل اسکنر غیرفعال کنید.

برای IPsec/فیلترینگ IP، اگر بتوانید از رایانه به دستگاه دسترسی پیدا کنید، می‌توانید عملکرد راغیرفعال کنید.

غیرفعال کردن *IPsec*/فیلترینگ *IP* با *Web Config*

1. از قسمت Web Config گزینه **Network Security Settings** > **IPsec/IP Filtering** > **Basic** را انتخاب کنید.
2. **Disable** را برای **IPsec/IP Filtering** در **Default Policy** انتخاب کنید.
3. بر روی **Next** کلیک کنید و **Enable this Group Policy** را برای همه سیاست‌های گروه پاک نمایید.
4. روی **OK** کلیک کنید.

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

مشکلات مربوط به استفاده از ویژگی های امنیت شبکه

فراموش کردن کلید از قبل مشترک شده

دوباره کلید را با استفاده از Web Config پیکربندی کنید.

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

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

اطلاعات مرتبط

"دسترسی به Web Config" در صفحه 22

نمی توانید با IPsec Communication ارتباط برقرار کنید

آیا از الگوریتم پشتیبانی نشده ای برای تنظیمات رایانه استفاده می کنید؟

اسکنر از الگوریتم های زیر پشتیبانی می کند.

روش های امنیتی	الگوریتم ها
الگوریتم رمزگذاری IKE	AES-CBC-128، AES-CBC-192، AES-CBC-256، AES-GCM-128*، AES-GCM-192*، 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 Group16، DH Group17، DH Group18، DH Group19، DH Group20، DH Group21، DH Group22، DH Group23، DH Group24، DH Group25، DH Group26، DH Group27*، DH Group28*، DH Group29*، DH Group30*
الگوریتم رمزگذاری ESP	AES-CBC-128، AES-CBC-192، AES-CBC-256، AES-GCM-128، AES-GCM-192، AES-GCM-256، 3DES
الگوریتم تایید هویت ESP	SHA-1، SHA-256، SHA-384، SHA-512، MD5
الگوریتم تایید هویت AH	SHA-1، SHA-256، SHA-384، SHA-512، MD5

* فقط برای IKEv2

اطلاعات مرتبط

"ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 67

نمی تواند به طور ناگهانی ارتباط برقرار کند

آیا آدرس IP اسکنر نامعتبر است یا تغییر کرده است؟

از قسمت پانل کنترل اسکنر IPsec را غیرفعال کنید.

تنظیمات امنیتی پیشرفته مربوط به شرکت

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 Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) اسکنر یافت نشود.

از آدرس IP ایستا استفاده کنید.

آیا آدرس IP رایانه نامعتبر است یا تغییر کرده است؟

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 Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) اسکنر یافت نشود.

از آدرس IP ایستا استفاده کنید.

اطلاعات مرتبط

- "دسترسی به Web Config" در صفحه 22
- "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 67

بعد از پیکربندی IPsec/فیلترینگ IP نمی توانید وصل شوید

ممکن است مقدار تنظیم صحیح نباشد.

IPsec/فیلترینگ IP را از پانل کنترل اسکنر غیرفعال کنید. اسکنر و رایانه را به هم وصل کنید و دوباره تنظیمات IPsec/فیلترینگ IP را انجام دهید.

اطلاعات مرتبط

- "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 67

بعد از پیکربندی IEEE802.1X نمی توانید به چاپگر یا اسکنر دسترسی داشته باشید

ممکن است تنظیمات صحیح نباشند.

از پانل کنترل اسکنر IEEE802.1X را غیرفعال کنید. اسکنر و رایانه را وصل کنید و سپس دوباره IEEE802.1X را پیکربندی کنید.

اطلاعات مرتبط

- "پیکربندی شبکه IEEE802.1X" در صفحه 79

مشکلات مربوط به استفاده از یک گواهی دیجیتالی

نمی توانید گواهی امضاء شده از طریق CA را وارد کنید

آیا گواهی امضاء شده از طریق CA و اطلاعات روی CSR مطابقت دارند؟

اگر گواهی امضاء شده از طریق CA و CSR اطلاعات مشابهی ندارند، CSR قابل وارد کردن نیست. موارد زیر را بررسی کنید:

❑ آیا می خواهید 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.

آیا گواهی امضاء شده از طریق CA بیشتر از 5 کیلوبایت است؟

نمی توانید گواهی امضاء شده از طریق CA را که بیشتر از 5 کیلوبایت است وارد کنید.

آیا رمز عبور برای وارد کردن گواهی صحیح است؟

اگر رمز عبور را فراموش کردید، نمی توانید گواهی را وارد کنید.

اطلاعات مرتبط

⬅ "وارد کردن گواهی امضاء شده از طریق CA" در صفحه 61

نمی توانید گواهی خود امضاء را به روزرسانی کنید

آیا Common Name وارد شده است؟

Common Name باید وارد شود.

نویسه های پشتیبانی نشده ای برای Common Name وارد شده است؟ برای مثال، نویسه ژاپنی پشتیبانی نمی شود.

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

ویرگول یا فاصله ای در Common Name قرار دارد؟

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

اطلاعات مرتبط

⬅ "به روزرسانی گواهی خود امضاء" در صفحه 64

نمی توانید CSR ایجاد کنید

آیا Common Name وارد شده است؟

Common Name باید وارد شود.

نویسه های پشتیبانی نشده ای برای Common Name, Organization, Organizational Unit, Locality, State/Province وارد شده است؟ برای مثال، نویسه ژاپنی پشتیبانی نمی شود.

نویسه هایی از IPv4، IPv6، نام میزبان یا فرمت FQDN با فرمت (ASCII (0x20–0x7E وارد کنید.

ویرگول یا فاصله ای در Common Name قرار دارد؟

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

تنظیمات امنیتی پیشرفته مربوط به شرکت

اطلاعات مرتبط

"دریافت گواهی امضاء شده از طریق CA" در صفحه 59

هشداری مربوط به یک گواهی دیجیتالی ظاهر می شود

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

تنظیمات امنیتی پیشرفته مربوط به شرکت

پیام ها	علت/باید چه کاری انجام داد
Cannot use the Server Certificates that include more than three CA certificates.	**علت:** فایل گواهی با فرمت PKCS#12 بیشتر از 3 گواهی CA دارد. **باید چه کاری انجام داد:** هر گواهی را با تبدیل از فرمت PKCS#12 به فرمت PEM وارد کنید یا فایل گواهی با فرمت PKCS#12 وارد کنید که 2 گواهی CA دارد.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**علت:** تاریخ گواهی گذشته است. **باید چه کاری انجام داد:** ❑ اگر تاریخ گواهی گذشته است، گواهی جدیدی دریافت و وارد کنید. ❑ اگر گواهی تاریخ گذشته نیست، دقت کنید تاریخ و زمان اسکنر به درستی تنظیم شده باشند.
Private key is required.	**علت:** کلید خصوصی جفت شده ای با گواهی وجود ندارد. **باید چه کاری انجام داد:** ❑ اگر گواهی فرمت PEM/DER دارد و با استفاده از یک CSR و از طریق رایانه دریافت شده باشد، فایل کلید خصوصی را مشخص کنید. ❑ اگر گواهی فرمت PKCS#12 دارد و با استفاده از یک CSR و از طریق رایانه دریافت شده باشد، فایلی ایجاد کنید که محتوی کلید خصوصی باشد.
	علت: گواهی PEM/DER دریافت شده از طریق CSR و با استفاده از Web Config را دوباره وارد کرده اید. **باید چه کاری انجام داد:** اگر گواهی فرمت PEM/DER دارد و با استفاده از یک CSR و از طریق Web Config دریافت شده باشد، فقط می توانید یک بار آن را وارد کنید.
Setup failed.	**علت:** نمی توانید پیکربندی را تمام کنید زیرا ارتباط بین اسکنر و رایانه برقرار نشده است یا به دلیل خطاهایی، فایل قابل خواندن نیست. **باید چه کاری انجام داد:** بعد از بررسی فایل مشخص شده و ارتباط، دوباره فایل را وارد کنید.

اطلاعات مرتبط

◆ "درباره گواهی دیجیتالی" در صفحه 59

حذف گواهی امضاء شده از طریق CA به اشتباه

آیا برای گواهی فایل پشتیبان وجود دارد؟

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.

تنظیمات امنیتی پیشرفته مربوط به شرکت

اطلاعات مرتبط

- "حذف گواهی امضاء شده از طریق CA" در صفحه 63
- "وارد کردن گواهی امضاء شده از طریق CA" در صفحه 61