

راهنمای شبکه

NPD6249-00 FA

محتوا

حق چاپ

علايم تجاری

درباره این دفترچه راهنما

مقدمه

آماده سازی

اتصال

تنظیمات عملکرد

تنظیمات امنیتی

رفع مشکلات

تنظیم درایور چاپگر با استفاده از اتصال سرور/مشری	23
تنظیمات درایور چاپگر برای اتصال همتا-به-همتا	28
تنظیمات امنیتی	
تنظیمات امنیتی و پیشگیری از خطر	30
تنظیمات عملکرد امنیتی	31
پیکربندی رمز عبور سرپرست	31
پیکربندی رمز عبور سرپرست با استفاده از Web Config	31
کنترل پروتکل ها و سرویس ها	32
کنترل پروتکل ها	32
ارتباط SSL/TLS با چاپگر	36
درباره گواهی دیجیتالی	37
دریافت و وارد کردن گواهی امضاء شده از طریق CA	37
حذف گواهی امضاء شده از طریق CA	40
به روزرسانی گواهی خود امضاء	41
ارتباط رمزگذاری شده با IPsec/فیلترینگ IP	42
درباره فیلترینگ IPsec/IP	42
سیاست پیش فرض پیکربندی	42
پیکربندی سیاست گروهی	44
پیکربندی مثال های فیلترینگ IPsec/IP	49
استفاده از پروتکل SNMPv3	50
درباره SNMPv3	50
پیکربندی SNMPv3	50
رفع مشکلات	
بررسی گزارش سرور و دستگاه شبکه	52
چاپ کردن برگه وضعیت شبکه	52
مقدار-دهی تنظیمات شبکه	52
بازیابی تنظیمات شبکه از چاپگر	52
بازیابی تنظیمات چاپگر با استفاده از EpsonNet Config	53
بررسی ارتباط دستگاه ها و رایانه	53
بررسی اتصال با دستور Ping	53
مشکلات مربوط به استفاده از نرم افزار شبکه	54
بدون دسترسی Web Config	54
نام مدل و یا آدرس IP در EpsonNet Config نشان داده نمی شود	55
رفع مشکلات مربوط به امنیت پیشرفته	55
بازگرداندن تنظیمات امنیتی	55
غیرفعال کردن عملکرد ایمنی از چاپگر	55
بازیابی عملکرد ایمنی با استفاده از Web Config	56

علايم و نشانه ها	6
توضیحات استفاده شده در این دفترچه راهنما	6
مراجع سیستم عامل	6

جزء راهنما	8
تعریف اصطلاحات استفاده شده در این دفترچه راهنما	8

زنجیره تنظیمات چاپگر	10
معرفی اتصال چاپگر	10
تنظیمات اتصال سرور/مشری	11
تنظیمات اتصال همتا به همتا	11
آماده سازی اتصال شبکه	11
جمع آوری اطلاعات درباره تنظیم اتصال	11
مشخصات چاپگر	12
نوع تخصیص نشانی IP	12
روش تنظیم اتصال شبکه	12

اتصال به شبکه	14
اتصال به LAN	14
تنظیم آدرس IP با استفاده از صفحه کنترل چاپگر	14
تخصیص آدرس IP با استفاده از EpsonNet Config	16
اتصال به شبکه با استفاده از برنامه نصب	20

Web Config (صفحه وب برای دستگاه)	22
درباره Web Config	22
دسترسی به Web Config	22
استفاده از عملکردهای چاپگر	23
شرط چاپ از طریق شبکه	23

محتوا

مشکلات مربوط به استفاده از ویژگی های امنیت شبکه	56
مشکلات مربوط به استفاده از یک گواهی دیجیتالی. . .	57

ضمیمه

معرفی نرم افزار شبکه. . .	61
Epson Device Admin . . .	61
EpsonNet Print . . .	61
EpsonNet SetupManager . . .	61

حق چاپ

حق چاپ

هیچ بخشی از این نشریه را نمی توان تکثیر کرده، در سیستم بازیابی ذخیره نمود یا به هر صورت یا وسیله ای، الکترونیکی، مکانیکی، فتوکپی، ضبط یا طرق دیگر بدون اجازه کتبی از Seiko Epson Corporation انتقال داد. با توجه به اطلاعاتی که در اینجا مورد استفاده قرار می گیرد هیچ گونه مسئولیتی در مورد حق ثبت وجود ندارد. همینطور در قبال آسیب هایی که در نتیجه استفاده از این اطلاعات روی می دهد نیز هیچ مسئولیتی وجود ندارد. اطلاعات ارائه شده در اینجا فقط برای استفاده با محصول Epson در نظر گرفته شده است. Epson در قبال هرگونه استفاده شما از این اطلاعات آنطور که در سایر محصولات عنوان شده است، مسئولیتی نخواهد داشت.

Seiko Epson Corporation و نه شرکت های وابسته به آن در برابر خریدار این محصول یا اشخاص ثالث در قبال آسیب، ضرر، هزینه، یا هزینه های متحمل شده توسط خریدار یا اشخاص ثالث که در نتیجه تصادف، سوءاستفاده یا استفاده نادرست از این محصول یا تغییرات غیرمجاز، تعمیرات یا تغییرات در این محصول یا (به جز ایالات متحده) عدم تطبیق با دستورالعمل های راه اندازی و تعمیر و نگهداری Seiko Epson Corporation روی می دهد مسئولیتی ندارند.

Seiko Epson Corporation در مقابل هرگونه زیان یا مشکلاتی که در نتیجه استفاده از هرگونه لوازم اختیاری یا محصولات مصرفی بوجود آید به غیر از آنهایی که بعنوان محصول اصلی Epson و یا محصولات مجاز Epson توسط Seiko Epson Corporation شناسایی شده اند، مسئول نخواهد بود.

Seiko Epson Corporation در قبال هر نوع آسیبی که با تداخل الکترومغناطیسی روی می دهد که در نتیجه استفاده از کابل های رابط می باشد به جز آنهایی که بعنوان محصولات تایید شده Epson که توسط Seiko Epson Corporation طراحی شده اند، مسئولیتی ندارند.

© Seiko Epson Corporation 2019

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

علایم تجاری

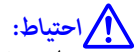
❑ EPSON® یک مارک تجاری ثبت شده و EPSON EXCEED YOUR VISION یا EXCEED YOUR VISION مارک تجاری Seiko Epson Corporation هستند.

❑ Microsoft®، Windows Server®، Windows® و Windows Vista® مارک های تجاری ثبت شده شرکت Microsoft Corporation هستند.

❑ اعلامیه 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 هرگونه حقوق حقوق عنوان شده در آنها را از خود سلب می کند.

درباره این دفترچه راهنما

علایم و نشانه ها



احتیاط:

برای پیشگیری از آسیبهای بدنی باید دستورالعمل ها با دقت پیگیری شوند.



مهم:

برای پیشگیری از آسیب به دستگاهتان باید به دستورالعمل ها توجه کنید.

توجه:

دستورالعمل ها حاوی نکات مفید و محدودیت های عملیاتی چاپگر هستند.

اطلاعات مرتبط

← کلیک بر روی این نمادها شما را به اطلاعات مرتبط می برد.

توضیحات استفاده شده در این دفترچه راهنما

تصاویر چاپگر 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.

مراجع سیستم عامل

Windows

در این دفترچه راهنما، عباراتی نظیر "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", "Windows Server 2012", "Windows Server 2012 R2", "Windows Server 2016", "Windows Server 2019", "Windows Server 2003", "Windows Server 2003 R2", "Windows Server 2008", "Server 2008 R2" و به این سیستم عامل ها اشاره دارند. به علاوه "Windows" برای رجوع به تمامی نسخه ها استفاده شده است.

☐ Microsoft® سیستم عامل Windows® 10

☐ Microsoft® سیستم عامل Windows® 8.1

☐ Microsoft® سیستم عامل Windows® 8

☐ Microsoft® سیستم عامل Windows® 7

☐ Microsoft® سیستم عامل Windows Vista®

☐ Microsoft® سیستم عامل Windows® XP

☐ Microsoft® سیستم عامل Windows® XP Professional x64 Edition

درباره این دفترچه راهنما

- ❑ Microsoft® سیستم عامل Windows Server® 2019
- ❑ Microsoft® سیستم عامل Windows Server® 2016
- ❑ Microsoft® سیستم عامل Windows Server® 2012 R2
- ❑ Microsoft® سیستم عامل Windows Server® 2012
- ❑ Microsoft® سیستم عامل Windows Server® 2008 R2
- ❑ Microsoft® سیستم عامل Windows Server® 2008
- ❑ Microsoft® سیستم عامل Windows Server® 2003 R2
- ❑ Microsoft® سیستم عامل Windows Server® 2003

مقدمه

جزء راهنما

در این دفترچه راهنما درباره نحوه اتصال چاپگر به شبکه توضیحاتی ارائه شده است، همچنین شامل اطلاعاتی درباره تنظیمات مربوط به استفاده از عملکردهای مختلف است.

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

آماده سازی

درباره تنظیم دستگاه ها و همچنین نرم افزارهای مورد استفاده برای مدیریت توضیحاتی ارائه شده است.

اتصال

درباره نحوه اتصال چاپگر به شبکه توضیح داده شده است.

تنظیمات عملکرد

درباره تنظیمات چاپ توضیح می دهد.

تنظیمات امنیتی

درباره تنظیمات امنیتی مانند تنظیمات گذرواژه سرپرست و کنترل پروتکل توضیح می دهد.

رفع مشکلات

مقداردهی اولیه تنظیمات و عیب یابی شبکه را شرح می دهد.

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

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 می کند.

کاربر

فردی که از دستگاه هایی مانند چاپگر استفاده می کند.

اتصال سرور/مشری (به اشتراک گذاشتن چاپگر با استفاده از سرور Windows)

اتصال که نشان می دهد چاپگر از طریق شبکه یا با کابل USB به Windows متصل شده است و صف چاپ تنظیم شده بر روی سرور را می توان به اشتراک گذاشت. ارتباط بین چاپگر و رایانه از طریق سرور برقرار می شود و چاپگر از روی سرور کنترل می شود.

اتصال همتا-به-همتا

اتصال که نشان می دهد چاپگر و رایانه از طریق هاب یا نقطه دسترسی به شبکه وصل شده اند و کار چاپ را می توان مستقیماً از رایانه انجام داد.

Web Config (صفحه وب دستگاه)

سرور وب که درون دستگاه جای گرفته است. به آن Web Config گفته می شود. می توانید وضعیت دستگاه را با مرورگر بررسی کنید و تغییر دهید.

مقدمه

صف چاپ

در Windows، نماد هر درگاه روی دستگاه **Device and Printer** (دستگاه و پرینتر) نمایش داده می شود مانند چاپگر. اگر دستگاه با دو یا چند درگاه مانند TCP/IP استاندارد به شبکه وصل شده باشد، دو یا چند نماد حتی برای یک دستگاه ایجاد می شود.

ابزار

عبارت کلی نرم افزار برای تنظیم یا مدیریت دستگاهی مانند Epson Device Admin، EpsonNet Config، EpsonNet SetupManager و سایر موارد.

اسکی (کد استاندارد آمریکا برای تبادل اطلاعات)

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

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
20	SP*	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
40	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
60	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w	x	y	z	{		}	~	

* نویسه فاصله.

یونیکد (UTF-8)

کد بین المللی استاندارد که زبان های بزرگ جهان را پوشش می دهد. UTF-8 در این راهنما به معنای نویسه های رمزگذاری در قالب UTF-8 است.

آماده سازی

این نویسه توضیح می دهد که قبل از انجام تنظیمات لازم است چه چیزهایی را آماده کنید.

زنجیره تنظیمات چاپگر

تنظیمات اتصال چاپگر و راه اندازی های اولیه را انجام می دهید تا چاپگر برای کاربران قابل دسترسی باشد.

1 آماده سازی

☐ جمع آوری اطلاعات تنظیم اتصال

☐ تصمیم گیری درباره روش اتصال

2 اتصال

☐ اتصال شبکه برقرار کنید

☐ تنظیمات درایور چاپگر

3 تنظیمات امنیتی

☐ تنظیمات سرپرست

☐ SSL/TLS

☐ کنترل پروتکل

☐ فیلترینگ IPsec/IP

اطلاعات مرتبط

← "اتصال" در صفحه 14

← "تنظیمات عملکرد" در صفحه 22

← "تنظیمات امنیتی" در صفحه 30

معرفی اتصال چاپگر

دو روش زیر برای شبکه مستقیم چاپگر وجود دارد.

☐ اتصال سرور/مشاریتی (به اشتراک گذاشتن چاپگر با استفاده از سرور Windows)

☐ اتصال همتا-به-همتا

اطلاعات مرتبط

← "تنظیمات اتصال سرور/مشاریتی" در صفحه 11

← "تنظیمات اتصال همتا به همتا" در صفحه 11

تنظیمات اتصال سرور/مشری

روش اتصال:

چاپگر را از طریق هاب (سوییچ L2) به شبکه وصل کنید. چاپگر را می‌توانید از طریق کابل SUB مستقیماً به سرور وصل کنید.

درایور چاپگر:

درایور چاپگر را با توجه به سیستم عامل رایانه‌های مشتری روی سرور Windows نصب کنید. با ورود به سرور Windows و برقرار کردن اتصال با چاپگر، درایور چاپگر روی رایانه مشتری نصب و قابل استفاده می‌شود.

ویژگی‌ها:

- چاپگر و درایور چاپگر را در دسته مدیریت کنید.
- بسته به ویژگی‌های سرور، کار چاپ ممکن است زمان‌بر باشد زیرا همه کارهای چاپ از سرور چاپ عبور می‌کند.
- اگر سرور Windows خاموش باشد، کار چاپ انجام نمی‌گیرد.

اطلاعات مرتبط

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

تنظیمات اتصال همتا به همتا

روش اتصال:

چاپگر را از طریق هاب (سوییچ L2) به شبکه وصل کنید.

درایور چاپگر:

درایور چاپگر را بر روی رایانه‌های مشتری نصب کنید. در قالب بسته با استفاده از EpsonNet SetupManager یا به صورت خودکار با استفاده از سیاست گروه سرور Windows ارائه شود.

ویژگی‌ها:

- کار چاپ بلافاصله آغاز می‌شود، زیرا مستقیماً به چاپگر فرستاده می‌شود.
- می‌توانید کار چاپ را تا زمان روشن بودن چاپگر ادامه دهید.

اطلاعات مرتبط

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

آماده سازی اتصال شبکه

جمع‌آوری اطلاعات درباره تنظیم اتصال

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

آماده سازی

بخشها	موارد	توجه
روش اتصال دستگاه	<input type="checkbox"/> اترنت	از کابل گروه 5e یا بالاتر STP (جفت تابیده دارای محافظ) استفاده کنید.
اطلاعات اتصال LAN	<input type="checkbox"/> آدرس IP <input type="checkbox"/> ماسک شبکه فرعی <input type="checkbox"/> دروازه پیش فرض	اگر نشانی IP را به طور خودکار با عملکرد DHCP روتر تنظیم کرده اید، این مورد ضروری نیست.
اطلاعات سرور DNS	<input type="checkbox"/> نشانی IP مربوط به DNS اصلی <input type="checkbox"/> نشانی IP مربوط به DNS فرعی	اگر از نشانی IP ثابت به عنوان نشانی IP استفاده می کنید، سرور DNS را پیکربندی کنید. زمانی که آدرس های IP را به صورت خودکار با استفاده از عملکرد DHCP تخصیص می دهید و زمانی که سرور DNS به صورت خودکار قابل تخصیص نیستند، پیکربندی کنید.

مشخصات چاپگر

ویژگی که چاپگر از حالت استاندارد یا اتصال پشتیبانی می کند، به راهنمای کاربر مراجعه کنید.

نوع تخصیص نشانی IP

دو روش برای تخصیص نشانی IP به چاپگر وجود دارد.

تخصیص IP ثابت:

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

این آدرس IP حتی در صورت روشن شدن چاپگر یا روتر تغییر نمی کند و شما می توانید دستگاه را با آدرس IP مدیریت کنید.

این نوع برای شبکه ای که چاپگرهای فراوانی به آن متصل است، مانند شرکت بزرگ یا مدرسه، مناسب است.

تخصیص خودکار با عملکرد DHCP:

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

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

توجه:

برای درگاه صف چاپ، پروتکلی مانند *EpsonNet Print Port* را انتخاب کنید که بتواند آدرس IP را به طور خودکار تشخیص دهد.

روش تنظیم اتصال شبکه

برای تنظیمات اتصال مربوط به نشانی IP، ماسک زیر شبکه و دروازه پیش فرض چاپگر به روش زیر عمل کنید.

استفاده از صفحه چاپگر:

با استفاده از صفحه چاپگر تنظیمات را انجام دهید. می توانید آدرس IP، ماسک شبکه فرعی، دروازه پیش فرض و سایر موارد را قبل از اتصال به شبکه تنظیم کنید.

استفاده از **EpsonNet Config**:

آماده سازی

از EpsonNet Config از کامپیوتر سرپرست استفاده کنید. می توانید چندین چاپگر را تنظیم کنید، به شرطی که همه آنها با کابل اترنت به شبکه متصل باشند. اگر بتوانید برای این تنظیم یک اترنت بسازید و تنظیم شبکه را برای چاپگر ایجاد کنید و سپس چاپگر را به شبکه معمولی وصل کنید، می توانید خطرهای امنیتی را در سطح پایین حفظ کنید.

استفاده از برنامه نصب:

در صورت استفاده از برنامه نصب، شبکه چاپگر و رایانه مشتری به طور خودکار تنظیم می شود. تنظیم با پیروی از دستورالعمل های برنامه نصب صورت می گیرد، حتی اگر چندان با شبکه آشنا نباشید. این زمانی پیشنهاد می شود که بخواهید چاپگر و چندین کامپیوتر را با اتصال سرور/مشتری (به اشتراک گذاشتن با سرور Windows) تنظیم کنید.

اطلاعات مرتبط

- ◀ "تنظیم آدرس IP با استفاده از صفحه کنترل چاپگر" در صفحه 14
- ◀ "تخصیص آدرس IP با استفاده از EpsonNet Config" در صفحه 16
- ◀ "اتصال به شبکه با استفاده از برنامه نصب" در صفحه 20

اتصال

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

اتصال به شبکه

اتصال به LAN

از طریق اترنت اجازه دهید چاپگر به شبکه وصل شود.

اطلاعات مرتبط

◀ "اتصال به شبکه با استفاده از برنامه نصب" در صفحه 20

تنظیم آدرس IP با استفاده از صفحه کنترل چاپگر

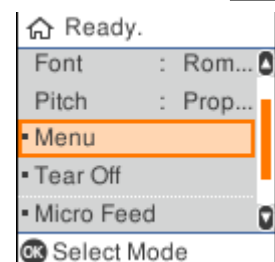
تنظیمات اولیه آدرس IP را انجام دهید مانند آدرس میزبان، ماسک شبکه فرعی، دروازه پیش فرض و سایر موارد.

در این بخش در مورد نحوه تنظیم آدرس IP ثابت توضیح داده می‌شود.

برای انتخاب موارد، از دکمه‌های ▲ ▼ ◀ ▶ برای جابجایی فوکوس استفاده کنید و سپس دکمه OK را برای تأیید انتخابتان فشار دهید.

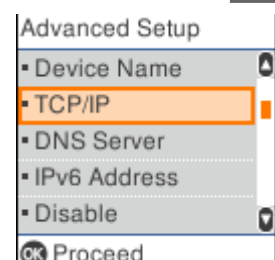
1 چاپگر را روشن کنید.

2 Menu (منو) را از صفحه اصلی صفحه کنترل انتخاب کنید.



3 Network Settings (تنظیمات شبکه) - Advanced Setup (نصب و جوی پیشرفته) را انتخاب کنید.

4 TCP/IP را انتخاب کنید.

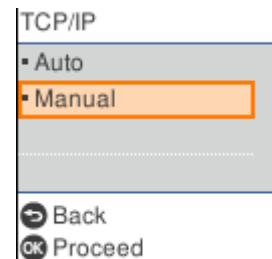


اتصال

Manual (دستی) را انتخاب کنید.

5

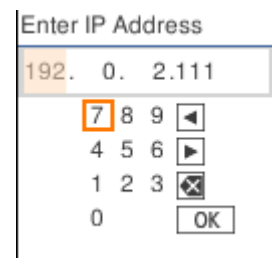
Auto (خودکار) را انتخاب کنید تا آدرس IP با استفاده از عملکرد DHCP به صورت خودکار از دستگاهی مانند روتر تنظیم شود. تنظیمات مربوط به **IP Address** (آدرس IP)، **Subnet Mask** (ماسک شبکه فرعی) و **Default Gateway** (دروازه پیش فرض) به صورت خودکار انجام می شوند و راه اندازی آدرس IP کامل می شود.



آدرس IP را وارد کنید.

6

وقتی ◀ یا ▶ را انتخاب می کنید، فوکوس بین بخش هایی که با نقطه از هم جدا شده اند به عقب و جلو جابجا می شوند.



به همین روش **Subnet Mask** (ماسک شبکه فرعی) و **Default Gateway** (دروازه پیش فرض) را نیز تنظیم کنید.

7

بعد از پایان مراحل تنظیم و راه اندازی، به صفحه **Advanced Setup** (نصب و جوی پیشرفته) باز می گردید.

توجه:

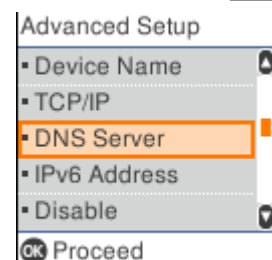
اگر ترکیب **IP Address** (آدرس IP)، **Subnet Mask** (ماسک شبکه فرعی) و **Default Gateway** (دروازه پیش فرض) اشتباه باشد، راه اندازی ادامه نخواهد یافت. بررسی کنید مقادیر وارد شده صحیح باشند.

تنظیم سرور DNS

بعد از اینکه آدرس IP را تنظیم کردید، در صورت لزوم سرور DNS را پیکربندی کنید.

DNS Server (سرور DNS) را در صفحه **Advanced Setup** (نصب و جوی پیشرفته) انتخاب کنید.

1



اتصال

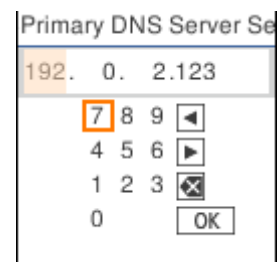
2 Auto (خودکار) یا Manual (دستی) را انتخاب کنید.

بعد از اینکه آدرس IP روی Auto (خودکار) تنظیم شد می توانید Auto (خودکار) یا Manual (دستی) را در تنظیمات سرور DNS انتخاب کنید. اگر آدرس سرور DNS را به صورت خودکار دریافت نکردید، باید Manual (دستی) را انتخاب، به مرحله بعدی بروید و آدرس سرور DNS را وارد کنید.

وقتی Auto (خودکار) را انتخاب می کنید، مراحل راه اندازی سرور DNS کامل می شود.

3 آدرس IP مربوط به DNS اولیه را وارد کنید.

وقتی ◀ یا ▶ را انتخاب می کنید، فوکوس بین بخش هایی که با نقطه از هم جدا شده اند به عقب و جلو جابجا می شوند.



4 سرور DNS دوم را به همین روش تنظیم کنید.

اگر سرور DNS دوم وجود ندارد، آن را روی "0.0.0.0" تنظیم کنید.

بعد از پایان مراحل تنظیم و راه اندازی، به صفحه **Advanced Setup (نصب و جوی پیشرفته)** باز می گردید.

تخصیص آدرس IP با استفاده از EpsonNet Config

تخصیص آدرس IP به چاپگر با استفاده از EpsonNet Config.

نصب EpsonNet Config

وقتی از EpsonNet Config استفاده می کنید، نصب کننده را از دیسک نرم افزار که همراه با چاپگر ارائه شده است اجرا کنید و دستورالعمل های روی صفحه را دنبال کنید.

اجرای EpsonNet Config

All Programs (برنامه ها) < EpsonNet < EpsonNet Config SE < EpsonNet Config را اجرا کنید.

توجه:

اگر اخطار فایروال نمایان شد، به EpsonNet Config اجازه دسترسی بدهید.

تنظیم آدرس IP

1 چاپگر را روشن کنید.

2 چاپگر را با کابل اترنت به شبکه وصل کنید.


اتصال

3. شروع EpsonNet Config

فهرست چاپگرهای متصل به شبکه ظاهر می‌شود. ظاهر شدن آنها کمی زمان می‌برد.

4

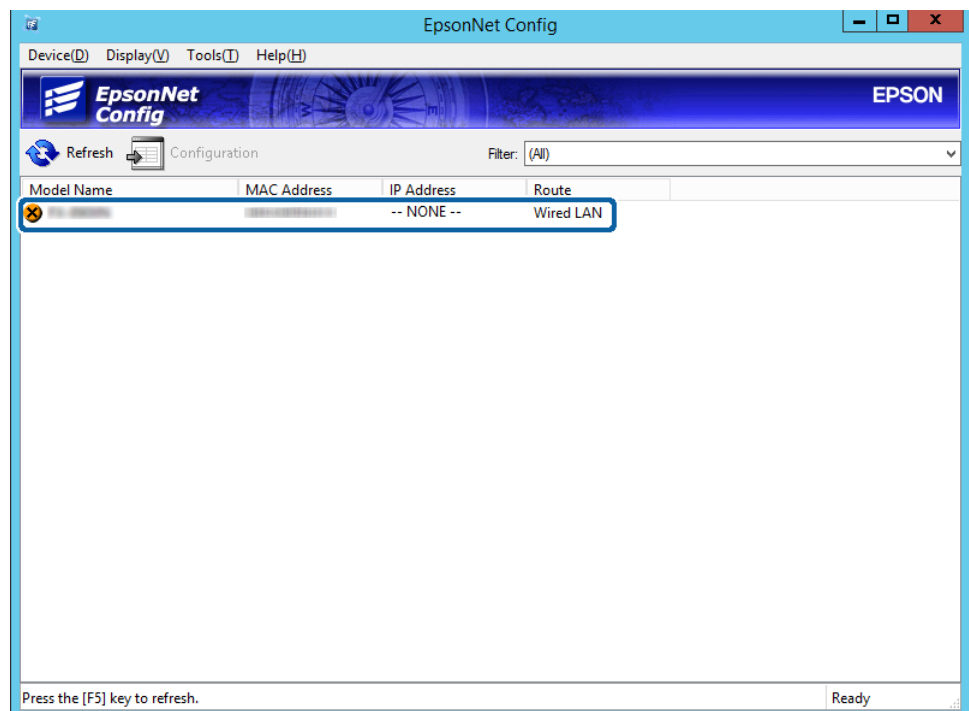
روی چاپگری که می‌خواهید راه اندازی کنید دو بار کلیک کنید.

اگر چاپگر را به شبکه ای وصل کردید که عملکرد DHCP دارد، آدرس IP با استفاده از عملکرد DHCP تخصیص داده می‌شود و سپس نمایش داده می‌شود. 

توجه:

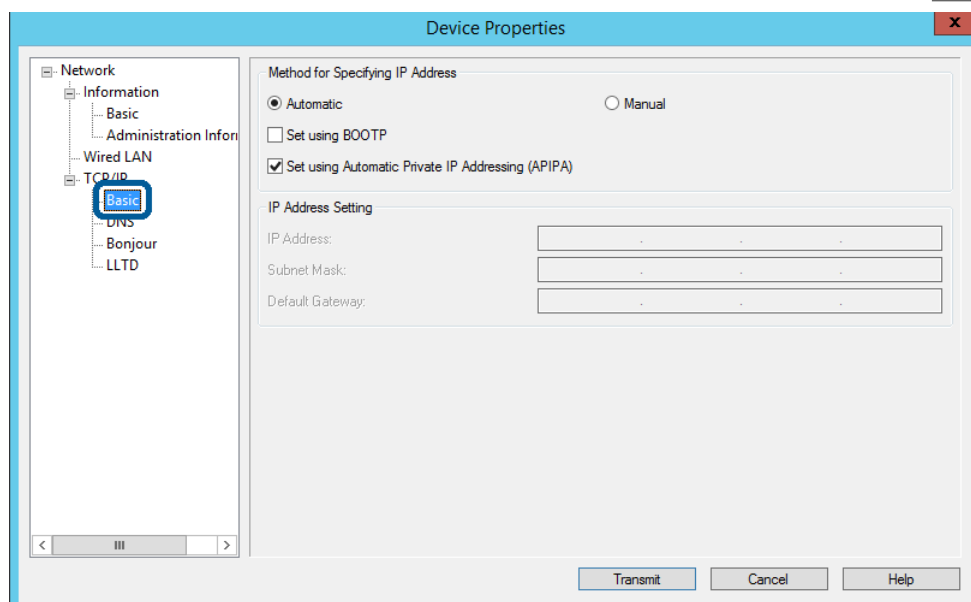
❑ اگر چندین چاپگر با مدل مشابه را متصل کرده باشید، می‌توانید چاپگر را با نشانی MAC شناسایی کنید.

❑ بعد از اتصال چاپگر به شبکه می‌توانید روش تخصیص آدرس IP را تغییر دهید.

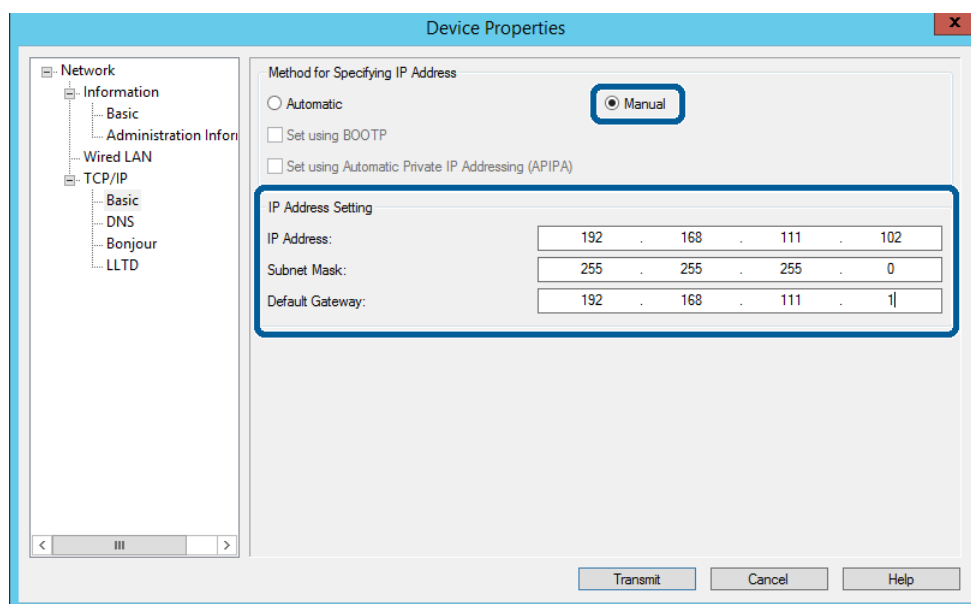


اتصال

5 **Network (شبکه) < TCP/IP < Basic (پایه) را انتخاب کنید.**



6 نشانی‌های IP Address (آدرس IP), Subnet Mask (ماسک فرعی شبکه), و Default Gateway (دروازه پیش فرض) را وارد کنید.

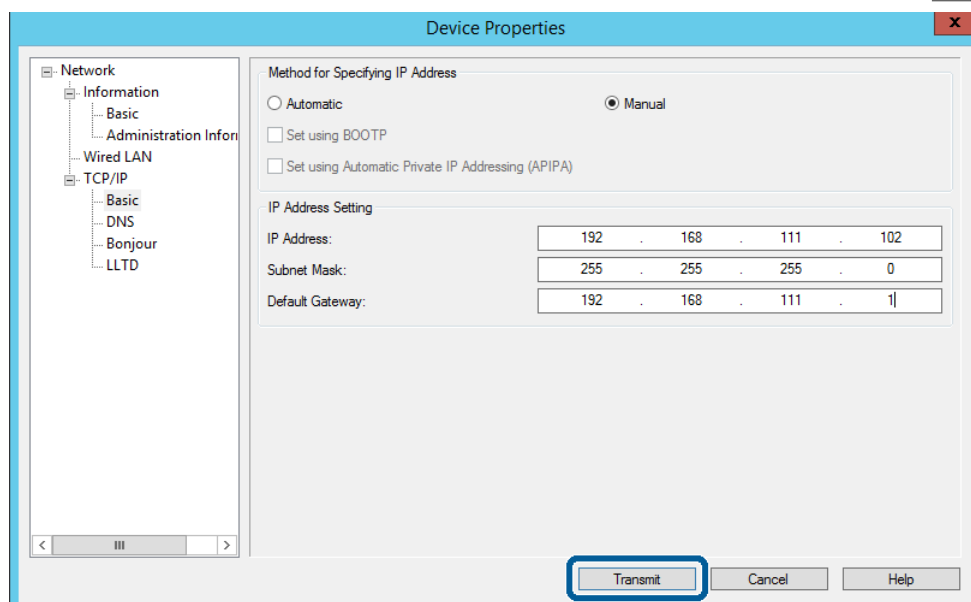


توجه:

- ❑ برای متصل کردن چاپگر به شبکه امن نشانی ثابت وارد کنید.
- ❑ در منوی TCP/IP می‌توانید تنظیماتی را برای DNS در صفحه DNS انجام دهید.

روی Transmit (مخابره) کلیک کنید.

7

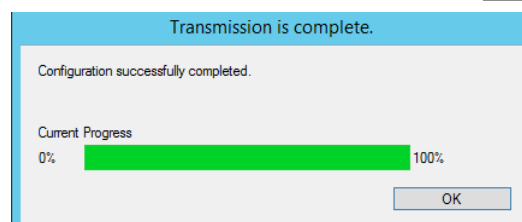


در صفحه تأیید روی OK (تایید) کلیک کنید.

8

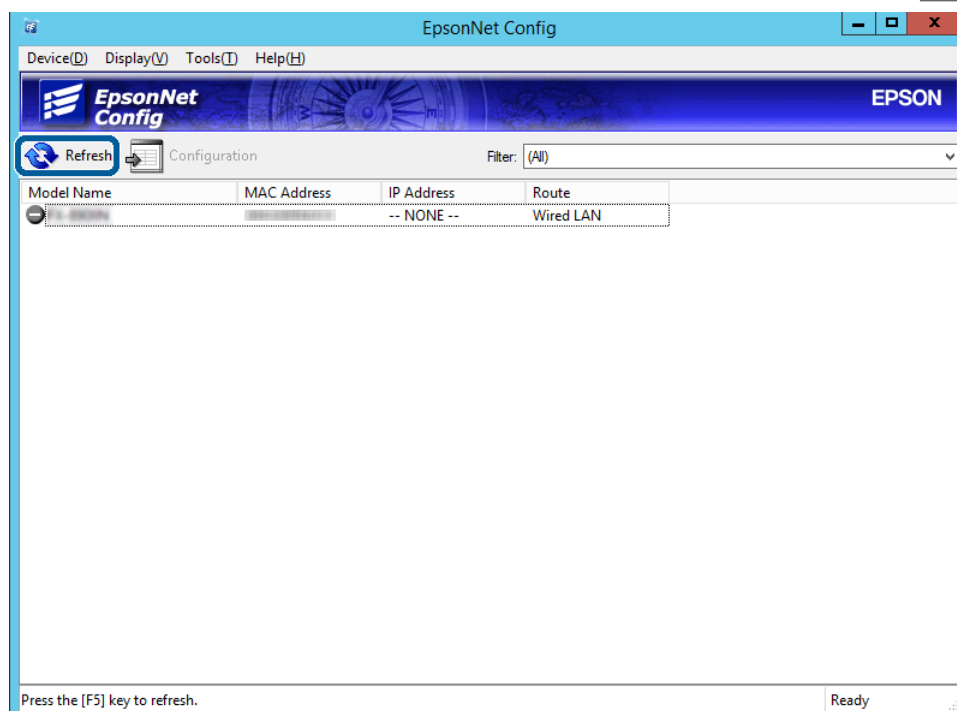
بر روی OK (تایید) کلیک کنید.

9

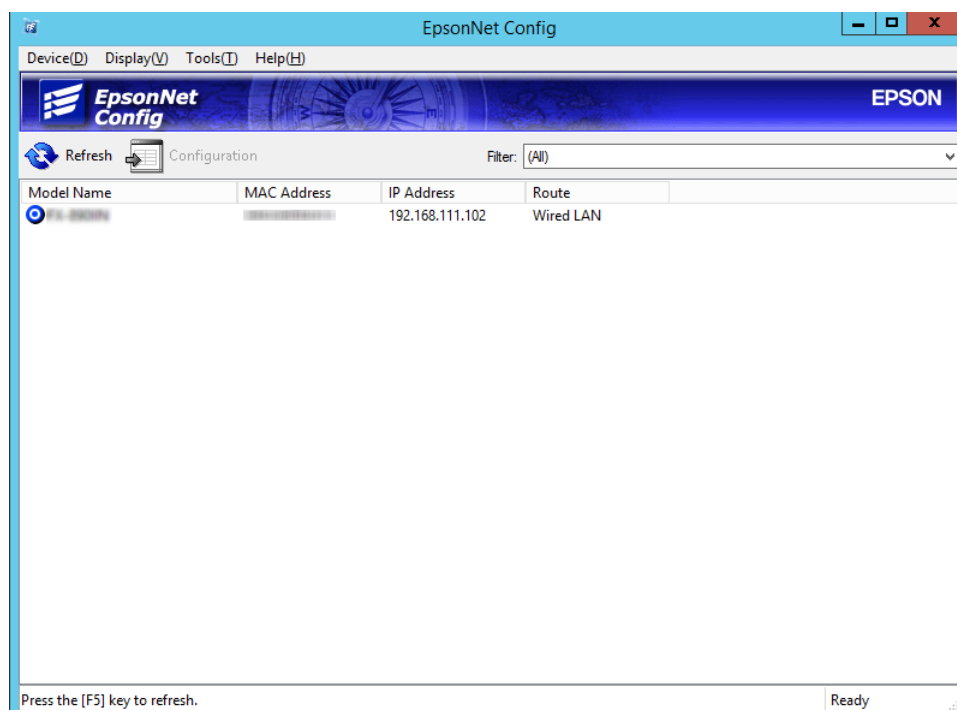


اتصال

10 روی Refresh (تازه کردن) کلیک کنید.



روی آدرس IP تخصیص داده شده کلیک کنید.



اتصال به شبکه با استفاده از برنامه نصب

برای وصل کردن چاپگر به رایانه بهتر است از برنامه نصب استفاده کنید.

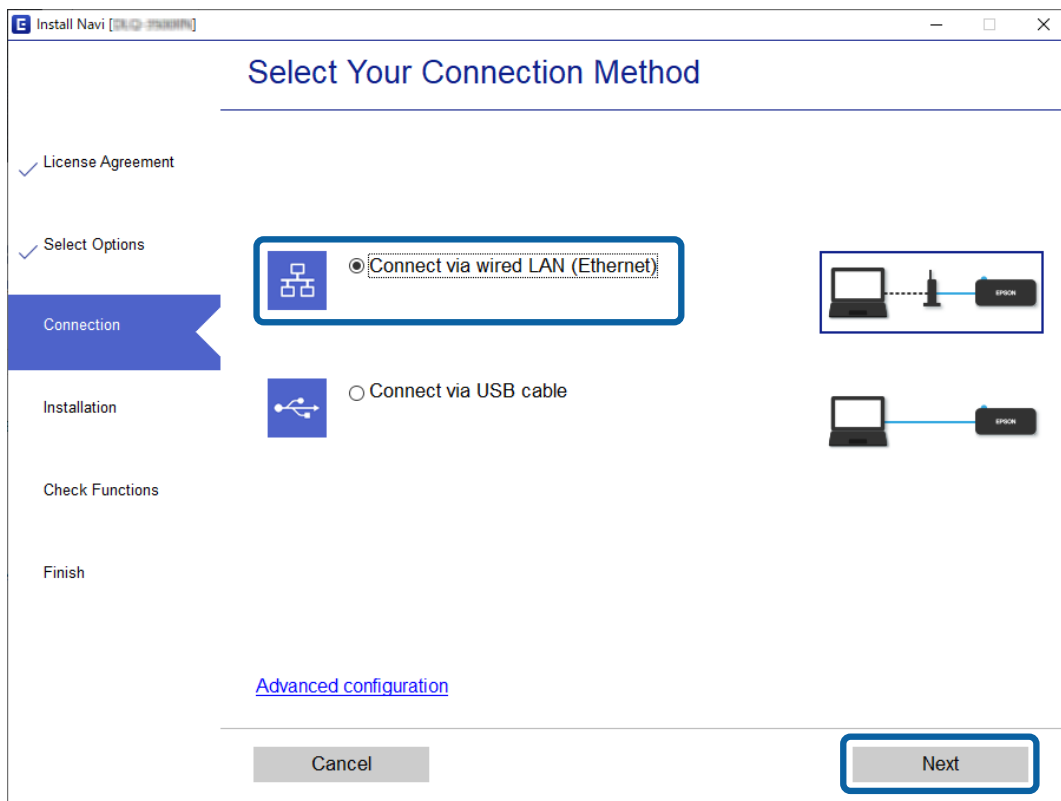
اتصال

1

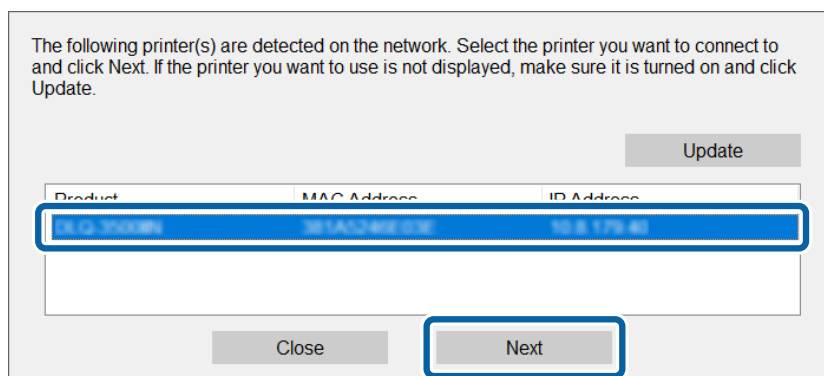
لوح فشرده نرم افزار را در رایانه قرار دهید و سپس دستورالعمل های روی صفحه را دنبال کنید.

2

دستورالعمل های روی صفحه را دنبال کنید تا زمانی که صفحه نمایش داده شود، **Ethernet Connection** (اتصال اینترنت) را انتخاب کنید و سپس روی **Next** (بعدی) کلیک کنید.



اگر چاپگر را با استفاده از کابل اینترنت به شبکه وصل می کنید، صفحه بعدی را که نمایش داده می شود دنبال کنید. چاپگر را انتخاب کنید و سپس روی **Next** (بعدی) کلیک کنید.



3

دستورالعمل های روی صفحه را دنبال کنید.

تنظیمات عملکرد

این فصل نخستین تنظیماتی را که باید برای استفاده از عملکردهای دستگاه اعمال شود، شرح می‌دهد. در این مبحث، روال‌های اعمال تنظیمات از رایانه سرپرست با استفاده از Web Config شرح داده می‌شود.

Web Config (صفحه وب برای دستگاه)

درباره Web Config

Web Config یک برنامه بر اساس مرورگر برای پیکربندی تنظیمات چاپگر است. برای دسترسی به Web Config ابتدا باید یک آدرس IP به چاپگر اختصاص داده باشید.

توجه:

می‌توانید با پیکربندی رمز عبور سرپرست برای چاپگر، تنظیمات را قفل کنید.

دسترسی به Web Config

دو روش برای دسترسی به Web Config وجود دارد. JavaScript باید در مرورگر فعال باشد.

وارد کردن آدرس IP

EpsonNet Config را شروع کنید و سپس روی چاپگر در لیست دو بار کلیک کنید.

آدرس IP چاپگر را در یک مرورگر وب وارد کنید. اگر از طریق HTTPS به Web Config دسترسی پیدا می‌کنید، پیام هشدار روی صفحه ظاهر می‌شود، زیرا در این حالت از گواهی خود-امضا شده ذخیره شده در چاپگر استفاده می‌شود.

دسترسی از طریق HTTPS

IPv4: <آدرس IP چاپگر> https:// (بدون < >)
IPv6: https://[آدرس IP چاپگر]/ (با [])

دسترسی از طریق HTTP

IPv4: <آدرس IP چاپگر> http:// (بدون < >)
IPv6: http://[آدرس IP چاپگر]/ (با [])

تنظیمات عملکرد

توجه:

❑ مثال ها

:IPv4

`https://192.0.2.111/`

`http://192.0.2.111/`

:IPv6

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

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

❑ اگر نام چاپگر با سرور DNS ثبت شود، می توانید از نام چاپگر به جای آدرس IP چاپگر استفاده کنید.

❑ هنگام دسترسی به Web Config از طریق HTTP همه منوها نشان داده می شوند. برای مشاهده همه منوها، از طریق HTTPS به Web Config بروید.

اطلاعات مرتبط

◀ "ارتباط SSL/TLS با چاپگر" در صفحه 36

◀ "درباره گواهی دیجیتالی" در صفحه 37

استفاده از عملکردهای چاپگر

برای استفاده از عملکرد چاپ چاپگر این گزینه را فعال کنید.

شرط چاپ از طریق شبکه

برای چاپ از طریق شبکه شرط زیر باید برقرار باشد. می توانید این تنظیمات را با استفاده از درایور چاپگر و عملکردهای سیستم عامل پیکربندی کنید.

❑ نصب کردن درایور چاپگر

❑ ایجاد صف چاپ برای رایانه

❑ تنظیم درگاه شبکه

تنظیم درایور چاپگر با استفاده از اتصال سرور/مشری

چاپگر را تنظیم کنید تا چاپ کردن از رایانه ای که قبلاً به عنوان سرور چاپ تنظیم شده است، فعال شود؛ سپس چاپگر را به اشتراک بگذارید. درایور چاپگر را برای سرور و مشتری روی سرور چاپ نصب کنید. در صورت استفاده از برنامه نصب، تنظیم شبکه چاپگر یا رایانه، نصب درایور و ساختن صف چاپ به طور خودکار انجام می گیرد.

تنظیم درگاه های استاندارد TCP/IP — Windows

درگاه استاندارد TCP/IP را در سرور چاپ تنظیم کنید و صف چاپ را برای چاپ شبکه ایجاد کنید.

صفحه دستگاه ها و چاپگرها را باز کنید.

1

❑ Windows 10/Windows Server 2019/Windows Server 2016

روی شروع < Windows System (سیستم Windows) < Control Panel (صفحه کنترل) < Hardware and Sound (سخت

افزار و صدا) < Devices and Printers (دستگاه ها و چاپگرها) کلیک کنید.

تنظیمات عملکرد

Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012 ☐
Desktop (میزکار) < **Settings** (تنظیمات) < **Control Panel** (پانل کنترل) < **Hardware and Sound** (سخت افزار و صدا) یا
Hardware (سخت افزار) < **Devices and Printers** (دستگاه ها و چاپگرها).

Windows 7/Windows Server 2008 R2 ☐
 روی شروع < **Control Panel** (پانل کنترل) < **Hardware and Sound** (سخت افزار و صدا) (یا **Hardware** (سخت افزار)) <
Devices and Printers (دستگاه ها و چاپگرها) کلیک کنید.

Windows Vista/Windows Server 2008 ☐
 بر روی شروع < **Control Panel** (پانل کنترل) < **Hardware and Sound** (سخت افزار و صدا) < **Printers** (چاپگرها) کلیک
 کنید.

Windows XP/Windows Server 2003 R2/Windows Server 2003 ☐
 روی شروع < **Control Panel** (پانل کنترل) < **Printers and Other Hardware** (چاپگرها و سایر سخت افزار) < **Printers**
and Faxes (چاپگرها و فکس ها) کلیک کنید.

افزودن چاپگر.

2

Windows 10/Windows 8.1/Windows 8/Windows Server 2019/Windows Server 2016/Windows Server 2012 ☐
 R2/Windows Server 2012
 روی **Add printer** (افزودن چاپگر) کلیک کنید و سپس **The printer that I want isn't listed** (چاپگری که می خواهم در
 فهرست نیست) را انتخاب کنید.

Windows 7/Windows Server 2008 R2 ☐
 روی **Add printer** (افزودن چاپگر) کلیک کنید.

Windows Vista/Windows Server 2008 ☐
 روی **Install Printer** (نصب چاپگر) کلیک کنید.

Windows XP/Windows Server 2003 R2/Windows Server 2003 ☐
 روی **Install Printer** (نصب چاپگر) کلیک کنید و سپس روی **Next** (بعدی) کلیک کنید.

افزودن یک چاپگر محلی.

3

Windows 10/Windows 8.1/Windows 8/Windows Server 2019/Windows Server 2016/Windows Server 2012 ☐
 R2/Windows Server 2012
Add a local printer or network printer with manual settings (افزودن چاپگر محلی یا چاپگر شبکه با تنظیمات دستی)
 را انتخاب کرده و سپس روی **Next** (بعدی) کلیک کنید.

Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 ☐
 روی **Add a local printer** (افزودن چاپگر محلی) کلیک کنید.

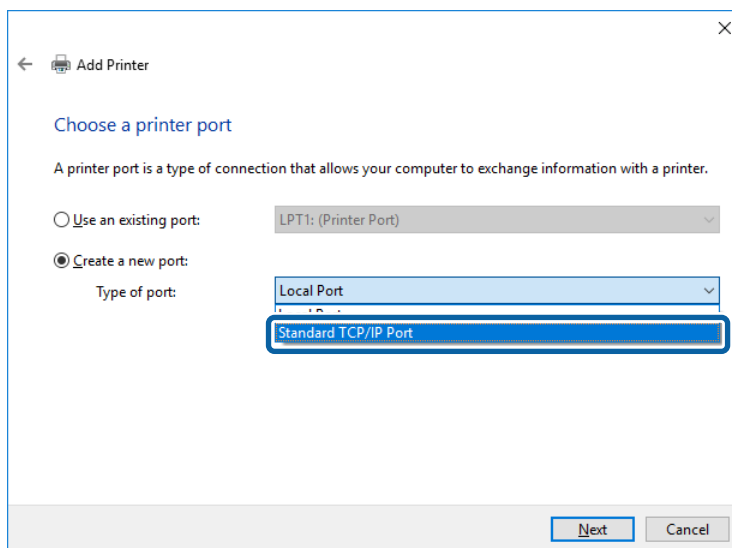
Windows XP/Windows Server 2003 R2/Windows Server 2003 ☐
Local printer attached to this computer (چاپگر محلی متصل به این رایانه) را انتخاب کنید و روی **Next** (بعدی) کلیک
 کنید.

تنظیمات عملکرد

4

Create a new port (ایجاد درگاه جدید) را انتخاب کنید و **Standard TCP/IP Port** (درگاه استاندارد TCP/IP) را به عنوان نوع درگاه انتخاب کنید و سپس روی **Next** (بعدی) کلیک کنید.

برای Windows XP/Windows Server 2003 R2/Windows Server 2003 روی **Next** (بعدی) در صفحه **Add Standard TCP/IP Printer Port Wizard** (ویزارد افزودن درگاه چاپگر استاندارد TCP/IP) کلیک کنید.



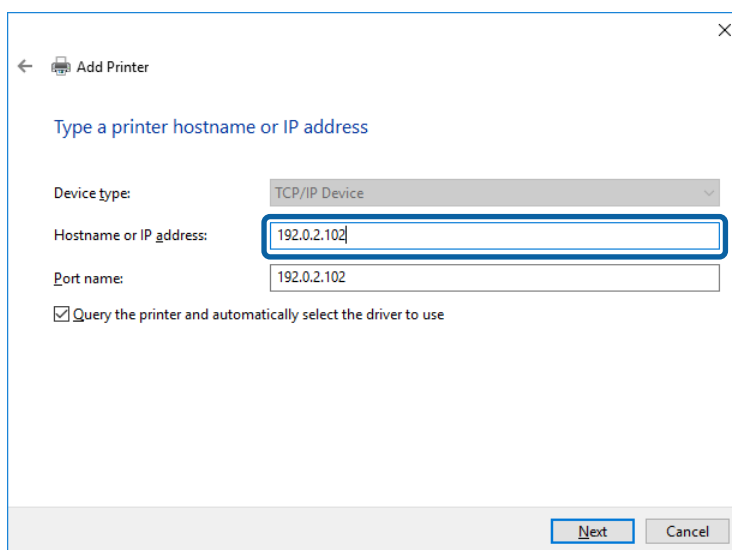
5

نشانی IP یا نام چاپگر را در **Host Name or IP Address** (نام میزبان یا آدرس IP) یا **Printer Name or IP Address** (نام چاپگر یا آدرس IP) وارد کنید و سپس روی **Next** (بعدی) کلیک کنید.

Port name (نام درگاه) را عوض نکنید.

روی **Continue** (ادامه) کلیک کنید وقتی صفحه **User Account Control** (کنترل دسترسی کاربر) نمایش داده می شود.

برای Windows XP/Windows Server 2003 R2/Windows Server 2003 روی **Done** (انجام شد) در صفحه **Standard TCP/IP Printer Port** (استاندارد TCP / IP پورت چاپگر) کلیک کنید.



توجه:

اگر نام چاپگر را در شبکه دارای قابلیت تفکیک نام مشخص کنید، نشانی IP رهگیری می شود، حتی اگر DHCP نشانی IP چاپگر را تغییر داده باشد. می توانید نام چاپگر را از صفحه وضعیت شبکه در پانل کنترل چاپگر یا برگه وضعیت شبکه بررسی کنید.

تنظیمات عملکرد

6

راه انداز چاپگر را تنظیم کنید.

❑ اگر راه انداز چاپگر قبلاً نصب شده است:
Manufacturer (سازنده) و Printers (چاپگرها) را انتخاب کنید. روی **Next (بعدی)** کلیک کنید.

❑ اگر راه انداز چاپگر قبلاً نصب نشده است:
 روی **Have Disc (دیسک دارم)** کلیک کنید و لوح فشرده نرم افزار ارائه شده با چاپگر را وارد کنید. روی **Browse (مرور)** کلیک کنید و سپس پوشه شامل راه انداز چاپگر را در سی دی انتخاب کنید. مطمئن شوید که پوشه درست را انتخاب کرده اید. محل پوشه ممکن است بسته به سیستم عامل شما متفاوت باشد.
 نسخه 32 بیتی Windows: WINX86
 نسخه 64 بیتی Windows: WINX64

7

دستورالعمل های روی صفحه را دنبال کنید.

برای Windows Vista/ Windows XP/ Windows Server 2003 R2/ Windows Server 2003 راه اندازی کامل شده است. برای Windows Server 2008 و جدیدتر، پیکربندی پورت را بررسی کنید.

در هنگام استفاده از چاپگر با اتصال سرور/مشرتی (به اشتراک گذاشتن چاپگر با سرور Windows)، تنظیمات اشتراک چاپگر را اعمال کنید.

اطلاعات مرتبط

← "اشتراک گذاری چاپگر" در صفحه 27

بررسی پیکربندی درگاه — Windows

بررسی کنید که آیا درگاه مناسب برای صف چاپ تنظیم شده است یا خیر.

1

صفحه دستگاه ها و چاپگرها را باز کنید.

❑ Windows 10/Windows Server 2019/Windows Server 2016
 روی **Windows System > start (سیستم Windows) > Control Panel (صفحه کنترل) < Hardware and Sound (سخت افزار و صدا) < Devices and Printers (دستگاه ها و چاپگرها)** کلیک کنید.

❑ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Desktop (میز کار) < Settings (تنظیمات) < Control Panel (پانل کنترل) < Hardware and Sound (سخت افزار و صدا) یا Hardware (سخت افزار) < Devices and Printers (دستگاه ها و چاپگرها).

❑ Windows 7/Windows Server 2008 R2
 روی شروع **Control Panel (پانل کنترل) < Hardware and Sound (سخت افزار و صدا) (یا Hardware (سخت افزار)) < Devices and Printers (دستگاه ها و چاپگرها)** کلیک کنید.

❑ Windows Vista/Windows Server 2008
 بر روی شروع **Control Panel (پانل کنترل) < Hardware and Sound (سخت افزار و صدا) < Printers (چاپگرها)** کلیک کنید.

2

صفحه ویژگی های چاپگر را باز کنید.

❑ Windows 10/Windows 8.1/Windows 8/Windows 7/Windows Server 2019/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012/ Windows Server 2008 R2
 روی آیکون چاپگر کلیک راست کرده و سپس روی **Printer properties (خصوصیات چاپگر)** کلیک کنید.

❑ Windows Vista
 روی آیکون چاپگر کلیک راست کرده و سپس **Run as administrator (اجرا به عنوان مدیر) < Properties (خصوصیات)** را انتخاب کنید.

تنظیمات عملکرد

Windows Server 2008 


روی آیکون چاپگر کلیک راست کرده و سپس روی **Properties (خصوصیات)** کلیک کنید.

3


روی برگه **Ports (درگاه ها)** کلیک کنید و **Standard TCP/IP Port (درگاه استاندارد TCP/IP)** را انتخاب کنید و سپس روی **Configure Port (پیکربندی درگاه)** کلیک کنید.

4

پیکربندی درگاه را بررسی کنید.

برای حالت RAW 

در بررسی کنید که Raw در بخش **Protocol (پروتکل)** انتخاب شده باشد و سپس روی **OK (تایید)** کلیک کنید.

برای LPR 

بررسی کنید که LPR در بخش **Protocol (پروتکل)** انتخاب شده باشد. "PASSTHRU" را در **Queue name (نام صف)** از LPR **Settings (تنظیمات LPR)** وارد کنید. **LPR Byte Counting Enabled (فعال سازی شمارش بایت LPR)** را انتخاب کرده و سپس روی **OK (تایید)** کلیک کنید.

اشتراک گذاری چاپگر

در هنگام استفاده از چاپگر با اتصال سرور/مشرتی (به اشتراک گذاشتن چاپگر با سرور Windows)، اشتراک چاپگر را از سرور چاپ تنظیم کنید.

1

Control Panel (پانل کنترل) > View devices and printers (مشاهده دستگاهها و چاپگرها) را از سرور چاپ انتخاب کنید.

2

روی نماد چاپگر (صف چاپ)ی که می خواهید به اشتراک بگذارید راس-کلیک راست کنید و سپس روی زبانه **Printer Properties (ویژگی های چاپگر) > Sharing (اشتراک گذاری)** کلیک نمایید.

3

Share this printer (اشتراک گذاری این چاپگر) را انتخاب کنید و سپس **Share name (نام اشتراک)** را وارد کنید.

برای Windows Server 2012، بر روی **Change Sharing Options (تغییر گزینه های اشتراک گذاری)** کلیک کنید و تنظیمات را پیکربندی کنید.

نصب درایورهای دیگر

اگر نسخه Windows سرور و مشرتی متفاوت باشد، پیشنهاد می شود که درایورهای دیگری را روی سرور چاپ نصب کنید.

1

Control Panel (پانل کنترل) > View devices and printers (مشاهده دستگاهها و چاپگرها) را از سرور چاپ انتخاب کنید.

2

روی نماد چاپگری که می خواهید با کلاینت ها به اشتراک بگذارید کلیک راست کرده و سپس روی زبانه **Printer Properties (ویژگی های چاپگر) > Sharing (اشتراک گذاری)** کلیک کنید.

3

روی **Additional Drivers (درایورهای دیگر)** کلیک کنید.

برای Windows Server 2012، بر روی **Change Sharing Options (تغییر گزینه های اشتراک گذاری)** کلیک کنید و تنظیمات را پیکربندی کنید.

4

نسخه های Windows را برای مشرتی ها انتخاب کنید و سپس بر روی **OK (تایید)** کلیک کنید.

5

فایل اطلاعات درایور چاپگر (inf.*) را انتخاب و درایور را نصب کنید.

تنظیمات عملکرد

اطلاعات مرتبط

← "استفاده از چاپگر مشترک" در صفحه 28

استفاده از چاپگر مشترک

لازم است سرپرست کلاینت ها را از نام رایانه اختصاص یافته به سرور چاپ و نحوه افزودن آن به رایانه های خودشان مطلع سازد. اگر هنوز درایورهای دیگری پیکربندی نشده اند، به کلاینت ها نحوه استفاده از **Devices and Printers** (دستگاه ها و چاپگرها) برای افزودن چاپگر مشترک را اطلاع دهید.

اگر از قبل درایورهای دیگری در سرور چاپ پیکربندی شده اند، این مراحل را دنبال کنید:

1

نام تخصیص یافته به سرور چاپ را در **Windows Explorer** انتخاب کنید.

2

روی چاپگری که می خواهید استفاده کنید دو بار کلیک کنید.

اطلاعات مرتبط

← "اشتراک گذاری چاپگر" در صفحه 27

← "نصب درایورهای دیگر" در صفحه 27

تنظیمات درایور چاپگر برای اتصال همتا-به-همتا

برای اتصال همتا-به-همتا (چاپ مستقیم)، درایور چاپگر باید روی تک تک رایانه های مشتری نصب شده باشد.

اطلاعات مرتبط

← "تنظیم درایور چاپگر" در صفحه 28

تنظیم درایور چاپگر

برای سازمان های کوچک، نصب درایور چاپگر بر روی همه رایانه های مشتری پیشنهاد می شود.

توجه:

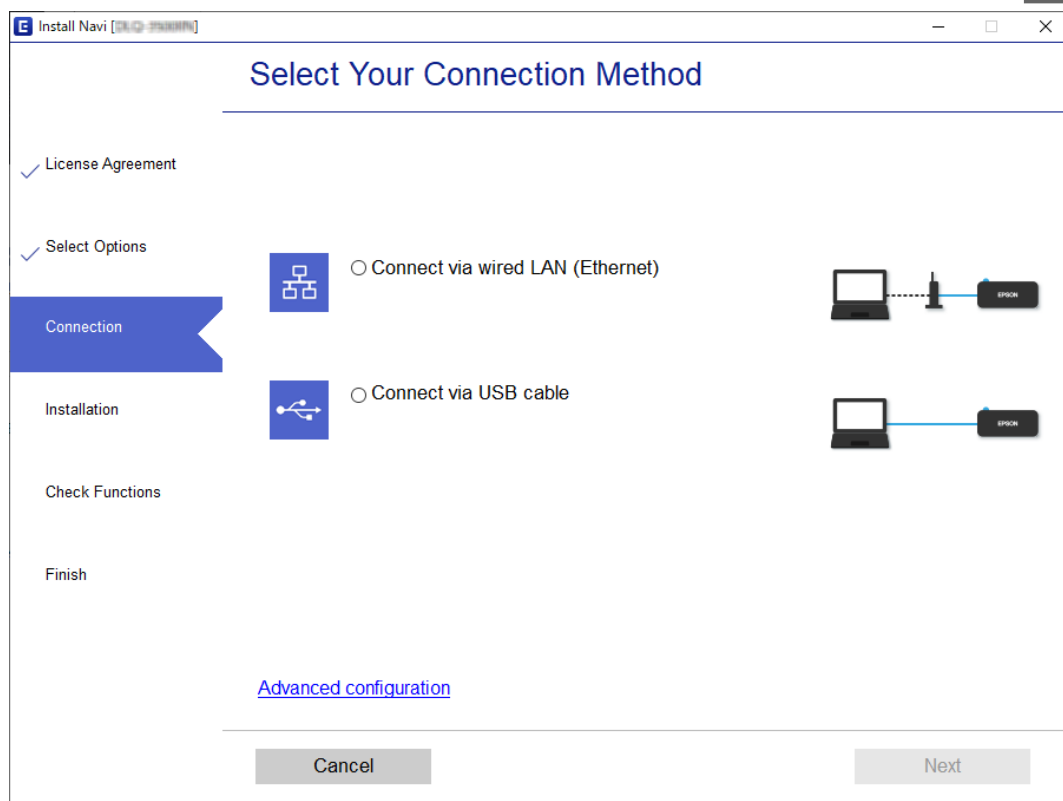
اگر قرار است چندین رایانه مشتری از چاپگر استفاده کنند، با استفاده از *EpsonNet SetupManager* و تحویل دادن درایور در قالب بسته، زمان نصب کاهش چشمگیری می یابد.

1

نصب کننده را اجرا کنید.

تنظیمات عملکرد

2 روش اتصال چاپگر را انتخاب و بر روی **Next** (بعدی) کلیک کنید.



توجه:

در صورت ظاهر شدن **Select Software Installation** (انتخاب نصب نرم افزار)، گزینه **Change or re-set the connection method** (تغییر یا تنظیم مجدد روش اتصال) را انتخاب و بر روی **Next** (بعدی) کلیک کنید.

3 دستورالعمل های روی صفحه را دنبال کنید.

اطلاعات مرتبط

← "EpsonNet SetupManager" در صفحه 61

تنظیمات امنیتی

در این بخش درباره تنظیمات امنیتی توضیح داده شده است.

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 کارایی و راحتی را افزایش دهند. هر چند، احتمال دسترسی غیرقانونی، استفاده غیرمجاز و دستکاری داده‌ها افزایش می‌یابد.

برای پیشگیری از این خطر، چاپگرهای 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 قابلیت	نوع قابلیت	آنچه باید تنظیم شود	آنچه باید جلوگیری شود
تنظیم گذرواژه سرپرست	تنظیمات امنیتی را قفل می‌کند مانند تنظیمات مربوط به شبکه یا USB.	سرپرست گذرواژه دستگاه را تنظیم می‌کند. پیکربندی یا به روز رسانی از همه جا از Web Config و Epson Device Admin موجود 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.
پروتکل و کنترل سرویس	پروتکل‌ها و خدماتی را که قرار است بین دستگاه‌ها و رایانه‌ها به کار گرفته شود کنترل می‌کند و امکاناتی مانند چاپ را فعال و غیرفعال می‌کند.	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.
ارتباطات SSL/TLS	مسیر ارتباط رایانه و چاپگر با ارتباط SSL/TLS رمزگذاری می‌شود. محتوای ارتباط با تنظیمات چاپگر و با پروتکل IPPS از طریق مرورگر محافظت می‌شود.	یک گواهی دارای امضای CA بگیرید و آن را وارد چاپگر 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.
فیلتر کردن IPsec/IP	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 چاپ غیرامن و 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.

تنظیمات امنیتی

اطلاعات مرتبط

- ← "پیکربندی رمز عبور سرپرست" در صفحه 31
- ← "کنترل پروتکل ها و سرویس ها" در صفحه 32
- ← "ارتباط SSL/TLS با چاپگر" در صفحه 36

تنظیمات عملکرد امنیتی

در هنگام تنظیم کردن فیلترینگ IPsec توصیه می شود با استفاده از SSL/TLS به Web Config دسترسی پیدا کنید تا اطلاعات مربوط به تنظیمات را جابجا کنید و مشکلات امنیتی مانند دستکاری یا رهگیری کاهش یابد.

پیکربندی رمز عبور سرپرست

اگر گذرواژه سرپرست ایجاد کنید، کاربران غیر از سرپرست نمی توانند تنظیمات مربوط به سرپرست سیستم را تغییر دهند. با استفاده از Web Config می توانید رمز عبور سرپرست را تنظیم کرده و تغییر دهید.

اطلاعات مرتبط

- ← "پیکربندی رمز عبور سرپرست با استفاده از Web Config" در صفحه 31

پیکربندی رمز عبور سرپرست با استفاده از Web Config

با استفاده از Web Config می توانید رمز عبور سرپرست را تنظیم کنید.

1 به Web Config بروید و **Administrator Settings** (تنظیمات سرپرست) > **Change Administrator Password** (تغییر رمز عبور مدیر) را انتخاب کنید.

2 یک رمز عبور در **New Password** (رمز ورود جدید) و **Confirm New Password** (تأیید رمز ورود جدید) وارد کنید.

اگر می خواهید رمز عبور را به رمز عبور جدیدی تغییر دهید، رمز عبور فعلی را وارد کنید.

EPSON

Administrator Settings > Change Administrator Password

Current password :

New Password : Enter between 1 and 20 characters.

Confirm New Password :

Note: It is recommended to communicate via HTTPS for entering an administrator password.

OK

OK (تایید) را انتخاب کنید.

3

توجه:

- ☐ برای تنظیم کردن یا تغییر دادن گزینه‌های قفل شده منو، بر روی **Administrator Login** (ورود سرپرست) کلیک کنید و گذرواژه سرپرست را وارد کنید.
- ☐ برای حذف کردن رمز عبور سرپرست، روی **Administrator Settings** (تنظیمات سرپرست) < **Delete Administrator Password** (رمز ورود مدیر را حذف کنید) کلیک کنید و رمز عبور سرپرست را وارد کنید.

اطلاعات مرتبط

← "دسترسی به Web Config" در صفحه 22

کنترل پروتکل ها و سرویس ها

می توانید با استفاده از گذرگاه ها و پروتکل های مختلف چاپ کنید. می توانید با محدود کردن چاپ از گذرگاه های مشخص یا با کنترل عملکردهای موجود خطرات ناخواسته امنیتی را کاهش دهید.

کنترل پروتکل ها

تنظیمات پروتکل را پیکربندی کنید.

1 به Web Config بروید و **Services** (سرویس ها) < **Protocol** (پروتکل) را انتخاب کنید.

2 هر مورد را پیکربندی کنید.

3 روی **Next** (بعدی) کلیک کنید.

4 بر روی **OK** (تایید) کلیک کنید.

تنظیمات در چاپگر اعمال می شوند.

اطلاعات مرتبط

← "دسترسی به Web Config" در صفحه 22

← "پروتکل هایی که می توانید فعال یا غیرفعال کنید" در صفحه 32

← "موارد تنظیم پروتکل" در صفحه 34

پروتکل هایی که می توانید فعال یا غیرفعال کنید

پروتکل	شرح
Bonjour Settings (Bonjour تنظیمات)	می توانید مشخص کنید آیا از Bonjour استفاده شود یا خیر. Bonjour برای جستجوی دستگاه ها، چاپ و سایر استفاده موارد می شود.
SLP Settings (تنظیمات SLP)	می توانید عملکرد SLP را فعال یا غیرفعال کنید. از SLP برای جستجوی شبکه در EpsonNet Config استفاده می شود.
LLTD Settings (تنظیمات LLTD)	می توانید عملکرد LLTD را فعال یا غیرفعال کنید. زمانی که فعال باشد، بر روی نقشه شبکه Windows نشان داده می شود.

تنظیمات امنیتی

شرح	پروتکل
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.	LLMNR Settings (تنظیمات LLMNR)
می توانید مشخص کنید چاپ LPR مجاز باشد یا خیر. زمانی که فعال باشد، می توانید از پورت LPR چاپ کنید.	LPR Settings (تنظیمات LPR)
می توانید مشخص کنید که آیا چاپ از پورت RAW مجاز باشد یا خیر (پورت 9100). زمانی که فعال باشد، می توانید از پورت RAW چاپ کنید (پورت 9100).	Settings (Port9100)RAW (تنظیمات RAW (پورت 9100))
می توانید مشخص کنید که آیا چاپ از پورت RAW مجاز باشد یا خیر (پورت سفارشی). زمانی که فعال باشد، می توانید از پورت RAW چاپ کنید (پورت سفارشی).	Settings (Custom Port)RAW (تنظیمات RAW (پورت سفارشی))
می توانید مشخص کنید که آیا چاپ از IPP مجاز باشد یا خیر. زمانی که فعال باشد، می توانید از طریق اینترنت چاپ کنید.	IPP Settings (تنظیمات IPP)
می توانید مشخص کنید چاپ FTP مجاز باشد یا خیر. زمانی که فعال باشد، می توانید از طریق سرور FTP چاپ کنید.	FTP Settings (تنظیمات FTP)
می توانید مشخص کنید آیا SNMPv1/v2c فعال شود یا خیر. از این برای تنظیم دستگاه ها، کنترل و مانند این استفاده می شود.	SNMPv1/v2c Settings (تنظیمات SNMPv1/v2c)
می توانید مشخص کنید آیا SNMPv3 فعال شود یا خیر. از این برای تنظیم دستگاه های رمزگذاری شده، کنترل و... استفاده می شود.	SNMPv3 Settings (تنظیمات SNMPv3)

اطلاعات مرتبط

- ◀ "کنترل پروتکل ها" در صفحه 32
- ◀ "موارد تنظیم پروتکل" در صفحه 34

تنظیمات امنیتی

موارد تنظیم پروتکل

EPSON

FX 6800N

[Administrator Logout](#)
☐ Status
[Product Status](#)
[Network Status](#)
☒ Network Settings
☒ Network Security Settings
☐ Services
[Protocol](#)
☒ Administrator Settings

Services > Protocol

 Note: If you need to change the Device Name used on each protocol and the Bonjour Name, change the Device Name in the Network Settings.
 If you need to change the Location used on each protocol, change it in the Network Settings.

Bonjour Settings
☒ Use Bonjour
 Bonjour Name : EPSON[XXXXXXXXXX].local.
 Bonjour Service Name : EPSON [XXXXXXXXXX]
 Location :
 Top Priority Protocol : IPP

SLP Settings
☒ Enable SLP

LLTD Settings
☒ Enable LLTD
 Device Name : EPSON[XXXXXXXXXX]

LLMNR Settings
☒ Enable LLMNR

LPR Settings
☒ Allow LPR Port Printing
 Printing Timeout (sec) : 300

☐ RAW(Port9100) Settings

تنظیم مقدار و توضیحات	موارد
Bonjour Settings (تنظیمات Bonjour)	
برای جستجو یا استفاده از دستگاه ها از طریق Bonjour از آن استفاده کنید.	Use Bonjour (استفاده از Bonjour)
نام Bonjour را نمایش می دهد.	Bonjour Name (نام Bonjour)
نام سرویس Bonjour را نمایش می دهد.	Bonjour Service Name (نام سرویس Bonjour)
نام مکان Bonjour را نمایش می دهد.	Location (مکان)
پروتکل اولویت برتر را برای چاپ Bonjour انتخاب کنید.	Top Priority Protocol (پروتکل اولویت برتر)
SLP Settings (تنظیمات SLP)	
برای فعال سازی عملکرد SLP این گزینه را انتخاب کنید. از این گزینه برای جستجوی شبکه در EpsonNet Config استفاده می شود.	Enable SLP (فعال کردن SLP)
LLTD Settings (تنظیمات LLTD)	
این گزینه را انتخاب کنید تا LLTD فعال شود. چاپگر در نقشه شبکه Windows نمایش داده می شود.	Enable LLTD (فعال کردن LLTD)
نام دستگاه LLTD را نمایش می دهد.	Device Name (نام دستگاه)
LLMNR Settings (تنظیمات LLMNR)	

تنظیمات امنیتی

موارد	تنظیم مقدار و توضیحات
Enable LLMNR (فعال کردن LLMNR)	این گزینه را انتخاب کنید تا LLMNR فعال شود. می توانید از جداسازی نام بدون NetBIOS استفاده کنید حتی اگر نتوانید از DNS استفاده کنید.
LPR Settings (تنظیمات LPR)	
Allow LPR Port Printing (چاپ پورت LPR مجاز است)	برای مجاز کردن چاپ کردن از پورت LPR این گزینه را انتخاب کنید.
Printing Timeout (sec) (فرصت زمانی چاپ (ثانی))	مقدار زمان وقفه را برای چاپ کردن LPR بین 0 تا 3,600 ثانیه وارد کنید. اگر زمان وقفه زمان را نمی خواهید، 0 را وارد کنید.
RAW Settings (Port9100) (تنظیمات RAW (پورت 9100))	
Allow RAW Printing (Port9100) (چاپ RAW (پورت 9100) مجاز)	برای مجاز بودن چاپ از پورت RAW (پورت 9100) این را انتخاب کنید.
Printing Timeout (sec) (فرصت زمانی چاپ (ثانی))	مقدار زمان وقفه را برای چاپ کردن RAW (پورت 9100) بین 0 تا 3,600 ثانیه وارد کنید. اگر زمان وقفه زمان را نمی خواهید، 0 را وارد کنید.
RAW Settings (Custom Port) (تنظیمات RAW (پورت سفارشی))	
Allow RAW Printing (Custom Port) (چاپ RAW (پورت سفارشی) مجاز)	برای مجاز بودن چاپ از پورت RAW (پورت سفارشی) این را انتخاب کنید.
Port Number (شماره درگاه)	شماره پورت RAW (پورت سفارشی) را بین 1024 تا 65535 بجز 9100، 1865 و 2968 وارد کنید.
Printing Timeout (sec) (فرصت زمانی چاپ (ثانی))	مقدار زمان وقفه را برای چاپ کردن RAW (پورت سفارشی) بین 0 تا 3,600 ثانیه وارد کنید. اگر زمان وقفه زمان را نمی خواهید، 0 را وارد کنید.
IPP Settings (تنظیمات IPP)	
Enable IPP (فعال کردن IPP)	انتخاب کنید تا ارتباط از طریق IPP فعال شود. فقط چاپگرهایی که از IPP پشتیبانی می کنند نمایش داده می شوند.
Allow Non-secure Communication (ارتباط غیرایمن مجاز است)	انتخاب کنید تا به چاپگر اجازه بدهید بدون معیارهای امنیتی (IPP) ارتباط برقرار کند.
Communication Timeout (sec) (فرصت زمانی ارتباط (ثانی))	مقدار زمان وقفه را برای چاپ کردن IPP بین 0 تا 3,600 ثانیه وارد کنید.
URL (Network) (شبکه))	وقتی چاپگر توسط LAN سیم دار وصل شده است، URL های IPP (http و https) را نشان می دهد. URL مقداری ترکیبی از آدرس IP چاپگر، شماره پورت و نام چاپگر IPP است.
Printer Name (نام چاپگر)	نام چاپگر IPP را نمایش می دهد.
Location (مکان)	مکان IPP را نمایش می دهد.
FTP Settings (تنظیمات FTP)	
Enable FTP Server (فعال کردن سرور FTP)	انتخاب کنید تا چاپ کردن از طریق FTP فعال شود. فقط چاپگرهایی که از چاپ FTP پشتیبانی می کنند نمایش داده می شوند.
Communication Timeout (sec) (فرصت زمانی ارتباط (ثانی))	مقدار زمان وقفه را برای ارتباط FTP بین 0 تا 3,600 ثانیه وارد کنید. اگر زمان وقفه زمان را نمی خواهید، 0 را وارد کنید.
SNMPv1/v2c Settings (تنظیمات SNMPv1/v2c)	
Enable SNMPv1/v2c (فعال کردن SNMPv1/v2c)	انتخاب کنید تا SNMPv1/v2c فعال شود. فقط چاپگرهایی که از SNMPv3 پشتیبانی می کنند نمایش داده می شوند.
Access Authority (اجازه دسترسی)	وقتی SNMPv1/v2c فعال است، اجازه دسترسی را تنظیم کنید. Read Only (فقط خواندن) یا Read/Write (خواندن/نوشتن) را انتخاب کنید.

تنظیمات امنیتی

موارد		تنظیم مقدار و توضیحات
Community Name (Read Only) (نام انجمن (فقط خواندن))		بین 0 تا 32 نویسه اسکی (0x20 تا 0x7E) وارد کنید.
Community Name (Read/Write) (نام انجمن (خواندن/نوشتن))		بین 0 تا 32 نویسه اسکی (0x20 تا 0x7E) وارد کنید.
IP Trap 1 to 4 (IP Trap 1 تا 4)		
Enable IP Trap X (IP Trap X را فعال کنید)	برای فعال کردن IP traps 1، 2، و 3 یا 4 انتخاب کنید.	
Address (آدرس)	آدرس IP مربوط به مقصد ترپ را وارد کنید.	
Community Name (نام انجمن)	نام انجمن را وارد کنید. می توانید حداکثر 32 نویسه حرفی عددی تک بایتی، فاصله و نمادهای زیر را وارد کنید. ~ ^ @ ? = :: -, + * () ' & % \$! ~ _ ^ @ ? = :: -, + * () ' & % \$!	
Port Number (شماره درگاه)	شماره پورت میزبان دریافت کننده Trap را به صورت اعشاری 0 تا 65535 وارد کنید.	
SNMPv3 Settings (تنظیمات SNMPv3)		
Enable SNMPv3 (فعال کردن SNMPv3)	زمانی که کادر علامت داشته باشد، SNMPv3 فعال می شود.	
User Name (نام کاربری)	بین 1 تا 32 نویسه با استفاده از نویسه های 1 بایتی وارد کنید.	
Authentication Settings (تنظیمات تأیید اعتبار)		
Algorithm (الگوریتم)	الگوریتم تأیید هویت را برای SNMPv3 انتخاب کنید.	
Password (رمز عبور)	گذرواژه تأیید هویت را برای SNMPv3 وارد کنید. بین 8 تا 32 نویسه با فرمت ASCII (0x20-0x7E) وارد کنید. اگر این را مشخص نمی کنید، قسمت مرتبط را خالی بگذارید.	
Confirm Password (تأیید رمز عبور)	رمز عبوری که برای تأیید پیکربندی کردید وارد نمایید.	
Encryption Settings (تنظیمات رمزگذاری)		
Algorithm (الگوریتم)	الگوریتم رمزگذاری را برای SNMPv3 انتخاب کنید.	
Password (رمز عبور)	گذرواژه رمزگذاری را برای SNMPv3 وارد کنید. بین 8 تا 32 نویسه با فرمت ASCII (0x20-0x7E) وارد کنید. اگر این را مشخص نمی کنید، قسمت مرتبط را خالی بگذارید.	
Confirm Password (تأیید رمز عبور)	رمز عبوری که برای تأیید پیکربندی کردید وارد نمایید.	
Context Name (نام محتوا)	حداکثر 32 نویسه یونیکد (UTF-8) وارد کنید. اگر این را مشخص نمی کنید، قسمت مرتبط را خالی بگذارید. تعداد نویسه های مجاز بسته به زبان فرق می کند.	

اطلاعات مرتبط

◀ "کنترل پروتکل ها" در صفحه 32

◀ "پروتکل هایی که می توانید فعال یا غیرفعال کنید" در صفحه 32

ارتباط SSL/TLS با چاپگر

اگر گواهی سرور با ارتباط SSL/TLS (لایه سوکت امن/امنیت لایه حمل) با چاپگر تنظیم شود، می توانید مسیر ارتباط بین رایانه ها را رمزگذاری کنید. اگر می خواهید 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 چاپگر 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 37
- ◀ "حذف گواهی امضاء شده از طریق CA" در صفحه 40
- ◀ "به روزرسانی گواهی خود امضاء" در صفحه 41

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 (تنظیمات امنیتی شبکه)** را انتخاب کنید. سپس **SSL/TLS < Certificate (گواهی)** را انتخاب کنید.

2 روی **Generate (ایجاد کردن)** از CSR کلیک کنید.

صفحه ایجاد CSR باز می شود.

3 برای هر مورد یک مقدار وارد کنید.

توجه:

طول کلید موجود و مخفف سازی ها بر اساس مرجع صدور گواهی فرق دارد. طبق قوانین مرجع صدور گواهی یک درخواست ایجاد کنید.

4 بر روی **OK (تایید)** کلیک کنید.

یک پیام تکمیل نشان داده می شود.

5 **Network Security Settings (تنظیمات امنیتی شبکه)** را انتخاب کنید. سپس **SSL/TLS < Certificate (گواهی)** را انتخاب کنید.

تنظیمات امنیتی

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

6



مهم:

دوباره یک CSR ایجاد نکنید. اگر اینکار را انجام دهید، ممکن است نتوانید گواهی امضاء شده از طریق CA صادر شده را وارد کنید.

CSR را برای مرجع صدور گواهی ارسال کنید و یک گواهی امضاء شده از طریق CA دریافت کنید.

7

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

گواهی امضاء شده از طریق CA صادر شده را در رایانه متصل به چاپگر ذخیره کنید.

8

زمانی که گواهی را در مقصد ذخیره کنید دریافت گواهی امضاء شده از طریق CA کامل است.

اطلاعات مرتبط

◀ "دسترسی به Web Config" در صفحه 22

◀ "موارد تنظیم مقصد" در صفحه 38

◀ "وارد کردن گواهی امضاء شده از طریق CA" در صفحه 39

موارد تنظیم مقصد

تنظیمات و توضیحات	موارد
طول کلید را برای یک CSR انتخاب کنید.	Key Length (طول کلید)
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	Common Name (نام معمول)
می توانید بین 0 تا 64 نویسه با فرمت ASCII (0x20-0x7E) وارد کنید. می توانید نام های متمایز را با ویرگول جدا کنید.	Organization (سازمان) / Organizational Unit (واحد سازمانی) / Locality (محل) / State/Province (استان/ایالت)
یک کد کشور دو رقمی که توسط ISO-3166 تعیین شده وارد کنید.	Country (کشور)

تنظیمات امنیتی

اطلاعات مرتبط

← "دریافت گواهی امضاء شده از طریق CA" در صفحه 37

وارد کردن گواهی امضاء شده از طریق CA

مهم!

- ☐ دقت کنید که تاریخ و زمان چاپگر 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.

1

به Web Config بروید و سپس **Network Security Settings** (تنظیمات امنیتی شبکه) را انتخاب کنید. سپس **SSL/TLS < Certificate** (گواهی) را انتخاب کنید.

2

روی **Import** (وارد کردن) 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 Web Config دریافت شده باشد
- **Private Key** (کلید خصوصی): پیکربندی نکنید زیرا چاپگر محتوی یک کلید خصوصی است.
- **Password** (رمز عبور): پیکربندی نکنید.
- **CA Certificate 1** (گواهی CA 1) / **CA Certificate 2** (گواهی CA 2): اختیاری

- ☐ یک گواهی با فرمت PEM/DER از رایانه دریافت شده باشد
- **Private Key** (کلید خصوصی): لازم است تنظیم کنید.
- **Password** (رمز عبور): پیکربندی نکنید.
- **CA Certificate 1** (گواهی CA 1) / **CA Certificate 2** (گواهی CA 2): اختیاری

- ☐ یک گواهی با فرمت PKCS#12 از رایانه دریافت شده باشد
- **Private Key** (کلید خصوصی): پیکربندی نکنید.
- **Password** (رمز عبور): اختیاری
- **CA Certificate 1** (گواهی CA 1) / **CA Certificate 2** (گواهی CA 2): پیکربندی نکنید.

4

بر روی **OK** (تایید) کلیک کنید.

یک پیام تکمیل نشان داده می شود.

توجه:

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

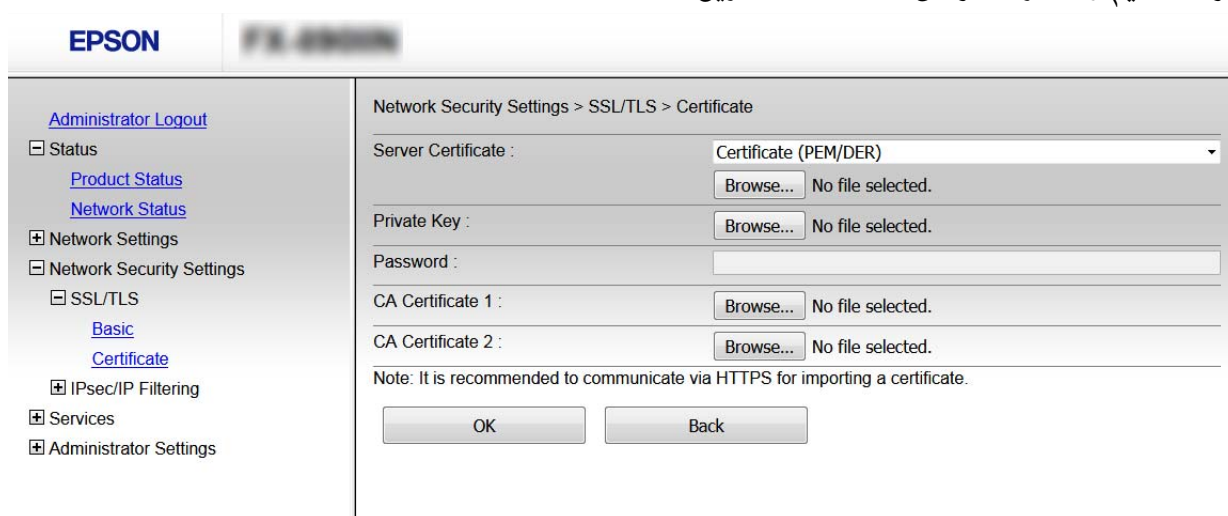
اطلاعات مرتبط

← "دسترسی به Web Config" در صفحه 22

← "موارد تنظیم وارد کردن گواهی امضاء شده از طریق CA" در صفحه 40

تنظیمات امنیتی

موارد تنظیم وارد کردن گواهی امضاء شده از طریق CA



موارد	تنظیمات و توضیحات
Server Certificate (گواهی سرور) یا Client Certificate (گواهی کلاینت)	فرمت گواهی را انتخاب کنید.
Private Key (کلید خصوصی)	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 (رمز عبور)	یک رمز عبور برای رمزگذاری کلید خصوصی وارد کنید.
CA Certificate 1 (گواهی CA 2)	اگر فرمت گواهی PEM/DER Certificate (گواهی 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 (گواهی CA 2)	اگر فرمت گواهی PEM/DER Certificate (گواهی PEM/DER)) است، یک گواهی از مرجع صدور گواهی که گواهی CA Certificate 1 (گواهی CA 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 39

حذف گواهی امضاء شده از طریق CA

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



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

1 به Web Config دسترسی یابید و سپس **Network Security Settings (تنظیمات امنیتی شبکه)** را انتخاب کنید. سپس **SSL/TLS > Certificate (گواهی)** را انتخاب کنید.

2 روی **Delete (حذف)** کلیک کنید.

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

به روزرسانی گواهی خود امضاء

اگر چاپگر از ویژگی سرور HTTPS پشتیبانی می کند، می توانید گواهی خود امضاء را به روزرسانی کنید. زمان دستری 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 بروید و **Network Security Settings (تنظیمات امنیتی شبکه) < SSL/TLS < Certificate (گواهی)** را انتخاب کنید.

2 روی **Update (به روز رسانی)** کلیک کنید.

3 **Common Name (نام معمول)** را وارد کنید.

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

توجه:

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

4 یک دوره اعتبار برای گواهی مشخص کنید.

5 روی **Next (بعدی)** کلیک کنید.

یک پیام تأیید نشان داده می شود.

6 بر روی **OK (تایید)** کلیک کنید.

چاپگر به روزرسانی می شود.

توجه:

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

اطلاعات مرتبط

← "دسترس به Web Config" در صفحه 22

ارتباط رمزگذاری شده با IPsec/فیلترینگ IP

درباره فیلترینگ IPsec/IP

اگر چاپگر از IPsec/IP Filtering (فیلتر کردن IPsec/IP) پشتیبانی می کند، می توانید بر اساس آدرس های IP، سرویس ها و پورت، ترافیک را فیلتر کنید. با ترکیب فیلترینگ، می توانید چاپگر 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 چاپگر 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. چاپگر 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.

توجه:

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

سیاست پیش فرض پیکربندی

1 به Web Config بروید و **Network Security Settings** (تنظیمات امنیتی شبکه) < **IPsec/IP Filtering** (فیلتر کردن IPsec/IP) < **Basic** (ابتدایی) را انتخاب کنید.

2 برای هر مورد یک مقدار وارد کنید.

3 روی **Next** (بعدی) کلیک کنید.

یک پیام تأیید نشان داده می شود.

4 بر روی **OK** (تأیید) کلیک کنید.

چاپگر به روزرسانی می شود.

اطلاعات مرتبط

← "دسترس به Web Config" در صفحه 22

← "موارد تنظیم پیش فرض سیاست" در صفحه 43

تنظیمات امنیتی

موارد تنظیم پیش فرض سیاست

EPSON **FW-3000**

[Administrator Logout](#)

- Status
 - [Product Status](#)
 - [Network Status](#)
- Network Settings
 - Network Security Settings
 - SSL/TLS
 - IPsec/IP Filtering
 - [Basic](#)
 - Services
 - Administrator Settings

Network Security Settings > IPsec/IP Filtering > Basic

Each policy is applied with following priorities:
Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy

Default Policy 1 2 3 4 5 6 7 8 9 10

IPsec/IP Filtering : ☒ Enable ☐ Disable

Default Policy

Access Control : IPsec

Authentication Method : Pre-Shared Key

Pre-Shared Key :

Confirm Pre-Shared Key :

Encapsulation : Transport Mode

Remote Gateway(Tunnel Mode) :

Security Protocol : ESP

Next

تنظیمات و توضیحات	موارد
می توانید ویژگی IPsec/IP Filtering (فیلتر کردن IPsec/IP) را فعال یا غیرفعال کنید.	IPsec/IP Filtering (فیلتر کردن IPsec/IP)
یک روش کنترل برای ترافیک بسته های IP پیکربندی کنید.	Access Control (کنترل دسترسی)
برای مجاز کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.	Permit Access (دسترسی مجاز)
برای رد کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.	Refuse Access (دسترسی غیرمجاز)
برای مجاز کردن عبور بسته های IPsec پیکربندی شده، این را انتخاب کنید.	IPsec
نسخه IKE را نمایش می دهد.	IKE Version (نسخه IKE)
روش های تأیید اعتبار سازگار را نمایش می دهد.	Authentication Method (روش تأیید اعتبار)
یک کلید از قبل اشتراک گذاری شده بین 1 و 127 نویسه را وارد کنید.	Pre-Shared Key (کلید از قبل به اشتراک گذاشته شده)
کلیدی که برای تأیید پیکربندی گردید وارد نمایید.	Confirm Pre-Shared Key (کلید از قبل به اشتراک گذاشته شده را تأیید کنید)
اگر IPsec را برای Access Control (کنترل دسترسی) انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.	Encapsulation (بسته بندی)
اگر در LAN مشابه فقط از چاپگر استفاده می کنید، این را انتخاب کنید. بسته های IP لایه 4 یا لایه بعد رمزگذاری می شوند.	Transport Mode (حالت جابجایی)
اگر از چاپگر در شبکه دارای اینترنت مانند IPsec-VPN استفاده می کنید، این گزینه را انتخاب کنید. عنوان و داده بسته های IP رمزگذاری می شوند.	Tunnel Mode (حالت تونل)

تنظیمات امنیتی

تنظیمات و توضیحات	موارد
اگر Tunnel Mode (حالت تونل) را برای Encapsulation (بسته بندی) انتخاب می کنید، یک آدرس درگاه بین 1 و 39 نویسه وارد کنید.	Remote Gateway (Tunnel Mode) (دروازه راه دور (حالت تونل))
اگر IPsec را برای Access Control (کنترل دسترسی) انتخاب می کنید، یک گزینه انتخاب نمایید.	Security Protocol (پروتکل امنیتی)
برای اطمینان از یکپارچگی تأیید اعتبار و داده این را انتخاب کنید، و داده را رمزگذاری کنید.	
برای اطمینان از یکپارچگی تأیید اعتبار و داده این را انتخاب کنید. حتی اگر رمزگذاری داده ممنوع باشد، می توانید از IPsec استفاده کنید.	

اطلاعات مرتبط

← "سیاست پیش فرض پیکربندی" در صفحه 42

پیکربندی سیاست گروهی

1 به Web Config چاپگر بروید و **Network Security Settings** (تنظیمات امنیتی شبکه) < **IPsec/IP Filtering** (فیلتر کردن IPsec/IP) < **Basic** (ابتدایی) 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** (بعدی) کلیک کنید.

یک پیام تأیید نشان داده می شود.

5 بر روی **OK** (تایید) کلیک کنید.

چاپگر به روزرسانی می شود.

اطلاعات مرتبط

← "دسترسی به Web Config" در صفحه 22

← "موارد تنظیم سیاست گروهی" در صفحه 45

تنظیمات امنیتی

موارد تنظیم سیاست گروهی

EPSON **F8.00000**

[Administrator Logout](#)
☐ Status
[Product Status](#)
[Network Status](#)
☒ Network Settings
☒ Network Security Settings
☒ SSL/TLS
☒ IPsec/IP Filtering
[Basic](#)
☒ Services
☒ Administrator Settings

Network Security Settings > IPsec/IP Filtering > Basic

Each policy is applied with following priorities:
 Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy

Default Policy 1 2 3 4 5 6 7 8 9 10

☒ Enable this Group Policy

Access Control : IPsec

Local Address(Printer) : Any addresses

Remote Address(Host) :

Method of Choosing Port : Port Number

Service Name : ☐ Any
☐ ENPC
☐ SNMP
☐ LPR
☐ RAW (Port9100)
☐ RAW (Custom Port)
☐ IPP/PPS
☐ WSD
☐ WS-Discovery
☐ Network Scan
☐ Network Push Scan
☐ Network Push Scan Discovery
☐ FTP Data (Local)
☐ FTP Control (Local)
☐ FTP Data (Remote)
☐ FTP Control (Remote)
☐ CIFS (Local)
☐ CIFS (Remote)
☐ HTTP (Local)
☐ HTTPS (Local)
☐ HTTP (Remote)
☐ HTTPS (Remote)

Transport Protocol : Any Protocol

تنظیمات و توضیحات		موارد
می توانید یک سیاست گروهی را فعال یا غیرفعال کنید.		Enable this Group Policy (فعال کردن سیاست گروهی)
یک روش کنترل برای ترافیک بسته های IP پیکربندی کنید.		Access Control (کنترل دسترسی)
برای مجاز کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.	Permit Access (دسترسی مجاز)	
برای رد کردن عبور بسته های IP پیکربندی شده، این را انتخاب کنید.	Refuse Access (دسترسی غیرمجاز)	
برای مجاز کردن عبور بسته های IPsec پیکربندی شده، این را انتخاب کنید.	IPsec	
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 (استفاده از آدرس IPv4 خودکار به دست آمده) را انتخاب کنید.		Local Address (Printer) (آدرس محلی (چاپگر))
برای کنترل دسترسی یک آدرس IP دستگاه وارد کنید. آدرس IP باید بین 0 و 43 نویسه باشد. اگر آدرس IP وارد نکنید، همه آدرس ها کنترل می شوند. توجه: 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.		Remote Address (Host) (آدرس راه دور (میزبان))

تنظیمات امنیتی

موارد	تنظیمات و توضیحات
Method of Choosing Port (روش انتخاب پورت)	روشی برای تعیین پورت ها انتخاب کنید.
Service Name (نام سرویس)	اگر Service Name (نام سرویس) را برای Method of Choosing Port (روش انتخاب پورت) انتخاب می کنید، یک گزینه را انتخاب کنید.
Transport Protocol (پروتکل جابجایی)	اگر Port Number (شماره درگاه) را برای Method of Choosing Port (روش انتخاب پورت) انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.
	Any Protocol (هر پروتکلی)
	TCP
	UDP
	ICMPv4
Local Port (پورت محلی)	اگر Port Number (شماره درگاه) را برای Method of Choosing Port (روش انتخاب پورت) و اگر TCP یا UDP را برای Transport Protocol (پروتکل جابجایی) 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 (پورت راه دور)	اگر Port Number (شماره درگاه) را برای Method of Choosing Port (روش انتخاب پورت) و اگر TCP یا UDP را برای Transport Protocol (پروتکل جابجایی) 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 (نسخه IKE)	نسخه IKE را نمایش می دهد.
Authentication Method (روش تایید اعتبار)	اگر IPsec را برای Access Control (کنترل دسترسی) انتخاب می کنید، یک گزینه انتخاب نمایید.
Pre-Shared Key (کلید از قبل به اشتراک گذاشته شده)	یک کلید از قبل اشتراک گذاری شده بین 1 و 127 نویسه را وارد کنید.
Confirm Pre-Shared Key (کلید از قبل به اشتراک گذاشته شده را تایید کنید)	کلیدی که برای تایید پیکربندی کردید وارد نمایید.
Encapsulation (بسته بندی)	اگر IPsec را برای Access Control (کنترل دسترسی) انتخاب می کنید، لازم است یک حالت بسته بندی پیکربندی کنید.
	Transport Mode (حالت جابجایی)
	Tunnel Mode (حالت تونل)
Remote Gateway (دروازه راه دور (حالت تونل))	اگر Tunnel Mode (حالت تونل) را برای Encapsulation (بسته بندی) انتخاب می کنید، یک آدرس درگاه بین 1 و 39 نویسه وارد کنید.

تنظیمات امنیتی

موارد	تنظیمات و توضیحات
Security Protocol (پروتکل امنیتی)	اگر IPsec را برای Access Control (کنترل دسترسی) 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.

اطلاعات مرتبط

- ◀ "پیکربندی سیاست گروهی" در صفحه 44
- ◀ "ترکیب آدرس محلی (چاپگر) و آدرس راه دور (میزبان) در سیاست گروهی" در صفحه 47
- ◀ "مرجع نام سرویس در سیاست گروهی" در صفحه 47

ترکیب آدرس محلی (چاپگر) و آدرس راه دور (میزبان) در سیاست گروهی

تنظیم آدرس محلی (چاپگر)				
هر آدرسی ^{3*}	IPv6 ^{2*}	IPv4		
✓	-	✓	IPv4 ^{1*}	تنظیم آدرس راه دور (میزبان)
✓	✓	-	IPv6 ^{2*1*}	
✓	✓	✓	خالی	

*1: اگر IPsec برای Access Control (کنترل دسترسی) انتخاب شود، نمی توانید طول پیشوند را تعیین کنید.

*2: اگر IPsec برای Access Control (کنترل دسترسی) انتخاب شود، نمی توانید طول آدرس پیوند محلی (fe80::) را تعیین کنید. و سیاست گروهی غیرفعال می شود.

*3: بجز آدرس های محلی پیوند IPv6.

مرجع نام سرویس در سیاست گروهی

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

Service Name (نام سرویس)	نوع پروتکل	شماره پورت محلی	شماره پورت از راه دور	ویژگی های کنترل شده
Any (هر)	-	-	-	همه سرویس ها
ENPC	UDP	3289	هر پورته	جستجو برای چاپگر از برنامه هایی مانند EpsonNet Config، درایور چاپگر و درایور اسکنر
SNMP	UDP	161	هر پورته	دریافت و پیکربندی MIB از برنامه هایی مانند EpsonNet Config، درایور چاپگر Epson و درایور اسکنر Epson
LPR	TCP	515	هر پورته	ارسال داده LPR

تنظیمات امنیتی

Service Name (نام سرویس)	نوع پروتکل	شماره پورت محلی	شماره پورت از راه دور	ویژگی های کنترل شده
RAW (Port9100) RAW (RAW پورت 9100)	TCP	9100	هر پورتنی	ارسال داده RAW
RAW (Custom Port) RAW (RAW پورت سفارشی)	TCP	2501 (پیش فرض)	هر پورتنی	ارسال داده RAW
IPP/IPPS	TCP	631	هر پورتنی	ارسال داده IPP/IPPS
WSD	TCP	هر پورتنی	5357	کنترل WSD
WS-Discovery	UDP	3702	هر پورتنی	جستجو برای چاپگر از WSD
Network Scan (جستجوی شبکه)	TCP	1865	هر پورتنی	ارسال داده جستجو از Document Capture Pro
Network Push Scan (اسکن لحظه ای شبکه)	TCP	هر پورتنی	2968	دریافت اطلاعات کار جستجو از Document Capture Pro
Network Push Scan Discovery (کشف اسکن لحظه ای شبکه)	UDP	2968	هر پورتنی	جستجو برای رایانه زمانی که کار اسکن شده برای ارسال از Document Capture Pro انجام می شود
FTP Data (Local) (داده FTP (محلی))	TCP	20	هر پورتنی	سرور FTP (ارسال داده از چاپ FTP)
FTP Control (Local) (کنترل FTP (محلی))	TCP	21	هر پورتنی	سرور FTP (کنترل چاپ FTP)
FTP Data (Remote) (داده FTP (راه دور))	TCP	هر پورتنی	20	کلاینت FTP (ارسال داده اسکن و داده فاکس دریافت شده) با اینحال این فقط می تواند یک سرور FTP را کنترل کند که از شماره پورت از راه دور 20 استفاده می کند.
FTP Control (Remote) (کنترل FTP (راه دور))	TCP	هر پورتنی	21	کلاینت FTP (کنترل برای ارسال داده اسکن و داده فاکس دریافت شده)
CIFS (Local) CIFS (محلی)	TCP	445	هر پورتنی	سرور CIFS (اشتراک یک پوشه شبکه)
CIFS (Remote) CIFS (راه دور)	TCP	هر پورتنی	445	مشتری CIFS (ارسال داده اسکن و داده فاکس دریافت شده به یک پوشه)
HTTP (Local) HTTP (محلی)	TCP	80	هر پورتنی	سرور HTTP(S) (ارسال داده Web Config و WSD)
HTTP (Local) HTTPS (محلی)	TCP	443	هر پورتنی	

تنظیمات امنیتی

ویژگی های کنترل شده	شماره پورت از راه دور	شماره پورت محلی	نوع پروتکل	Service Name (نام سرویس)
کلاینت HTTP(S) (ارتباط بین Epson Connect یا Google Cloud Print، به روزرسانی نرم افزار و به روزرسانی گواهی ریشه)	80	هر پورته	TCP	HTTP (Remote) (HTTP (راه دور))
	443	هر پورته	TCP	HTTPS (Remote) (HTTP (راه دور))

پیکربندی مثال های فیلترینگ IPsec/IP

دریافت فقط بسته های IPsec
این مثال فقط برای پیکربندی یک سیاست پیش فرض است.

سیاست پیش فرض:

☐ IPsec/IP Filtering (فیلترینگ IPsec/IP): Enable (فعال سازی)

☐ Access Control (کنترل دسترسی): IPsec

☐ Authentication Method (روش تأیید اعتبار): Pre-Shared Key (کلید از قبل به اشتراک گذاشته شده)

☐ Pre-Shared Key (کلید از قبل به اشتراک گذاشته شده): تا 127 نویسه وارد کنید.

سیاست گروهی:

پیکربندی نکنید.

دریافت داده چاپ و تنظیمات چاپگر
این مثال ارتباطات داده چاپ و پیکربندی چاپگر از سرویس های تعیین شده را مجاز می کند.

سیاست پیش فرض:

☐ IPsec/IP Filtering (فیلترینگ IPsec/IP): Enable (فعال سازی)

☐ Access Control (کنترل دسترسی): Refuse Access (دسترسی غیرمجاز)

سیاست گروهی:

☐ Enable this Group Policy (فعال کردن سیاست گروهی): کادر را علامت بزنید.

☐ Access Control (کنترل دسترسی): Permit Access (دسترسی مجاز)

☐ Remote Address (Host) (آدرس راه دور (میزبان)): آدرس IP کلاینت

☐ Method of Choosing Port (روش انتخاب پورت): Service Name (نام سرویس)

☐ Service Name (نام سرویس): کادر HTTP، SNMP، HTTP، (Local) ENPC، (Local) HTTP، (Local) HTTPS، (Local) HTTPS (محلی) و RAW (Port9100) (پورت 9100) را علامت بزنید.

دریافت دسترسی فقط از یک آدرس IP تعیین شده
این مثال آدرس IP تعیین شده برای دسترسی به چاپگر را مجاز می کند.

سیاست پیش فرض:

تنظیمات امنیتی

☐ IPsec/IP Filtering (فیلترینگ IPsec/IP): Enable (فعال سازی)

☐ Access Control (کنترل دسترسی): Refuse Access (دسترسی غیرمجاز)

سیاست گروهی:

☐ Enable this Group Policy (فعال کردن سیاست گروهی): کادر را علامت بزنید.

☐ Access Control (کنترل دسترسی): Permit Access (دسترسی مجاز)

☐ Remote Address (Host) (آدرس راه دور (میزبان)): آدرس IP از یک کلاینت سرپرست

توجه:

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

استفاده از پروتکل SNMPv3

درباره SNMPv3

SNMP پروتکلی است که کار پایش و کنترل را برای جمع آوری اطلاعات دستگاه های متصل به شبکه انجام می دهد. SNMPv3 نسخه قابلیت امنیت مدیریت است که توسعه یافته است.

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

پیکربندی SNMPv3

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

1 به Web Config بروید و **Services (سرویس ها) < Protocol (پروتکل)** را انتخاب کنید.

2 مقداری برای هر مورد **SNMPv3 Settings (تنظیمات SNMPv3)** وارد کنید.

3 روی **Next (بعدی)** کلیک کنید.

یک پیام تأیید نشان داده می شود.

4 بر روی **OK (تایید)** کلیک کنید.

چاپگر به روزرسانی می شود.

اطلاعات مرتبط

◀ "دسترسی به Web Config" در صفحه 22

◀ "موارد تنظیم SNMPv3" در صفحه 51

تنظیمات امنیتی

موارد تنظیم SNMPv3

EPSON F8-000000

[Administrator Logout](#)

- Status
 - [Product Status](#)
 - [Network Status](#)
- Network Settings
- Network Security Settings
 - Services
 - [Protocol](#)
- Administrator Settings

Communication Timeout (sec) : 120

SNMPv1/v2c Settings

☒ Enable SNMPv1/v2c

Access Authority : Read/Write

Community Name (Read Only) : public

Community Name (Read/Write) :

SNMPv3 Settings

☒ Enable SNMPv3

User Name : admin

Authentication Settings

Algorithm : MD5

Password :

Confirm Password :

Encryption Settings

Algorithm : DES

Password :

Confirm Password :

Context Name : EPSON

Next

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

اطلاعات مرتبط

← "پیکربندی SNMPv3" در صفحه 50

رفع مشکلات

بررسی گزارش سرور و دستگاه شبکه

اگر در اتصال شبکه مشکلی رخ دهد، می‌توانید دلیل بروز مشکل را با بررسی گزارش سرور ایمیل یا سرور LDAP یا وضعیت از طریق گزارش سیستم دستگاه شبکه، مانند روتر، یا فرمان‌ها بیابید.

چاپ کردن برگه وضعیت شبکه

می‌توانید اطلاعات شبکه را بررسی کرده و چاپ کنید.

1 کاغذ را درون دستگاه قرار دهید.

2 از صفحه اصلی **Menu** (منو) را انتخاب کنید.

برای انتخاب موارد، از دکمه‌های ▲ ▼ ◀ ▶ برای جابجایی فوکوس استفاده کنید و سپس دکمه **OK** را برای تأیید انتخابتان فشار دهید.

3 **Network Settings** (همه تنظیمات Wi-Fi/شبکه) - **Print Status Sheet** (برگه وضعیت چاپ) را انتخاب کنید.

4 دکمه **OK** را فشار دهید.

5 در پیام تأیید نمایش داده شده، دکمه **OK** را فشار دهید.

به صفحه اصلی باز می‌گردید.

مقدار-دهی تنظیمات شبکه

بازیابی تنظیمات شبکه از چاپگر

می‌توانید تنظیمات شبکه را به موارد پیش فرض بازگردانید.

1 از صفحه اصلی **Menu** (منو) را انتخاب کنید.

برای انتخاب موارد، از دکمه‌های ▲ ▼ ◀ ▶ برای جابجایی فوکوس استفاده کنید و سپس دکمه **OK** را برای تأیید انتخابتان فشار دهید.

2 **Network Settings** (همه تنظیمات Wi-Fi/شبکه) - **Restore Default Settings** (بازگشت به تنظیمات پیش فرض) را انتخاب کنید.

رفع مشکلات

3 دکمه OK را فشار دهید.

4 در پیام تأیید نمایش داده شده، دکمه OK را فشار دهید.

به صفحه اصلی باز می گردید.

بازیابی تنظیمات چاپگر با استفاده از EpsonNet Config

می توانید تنظیمات شبکه را با استفاده از EpsonNet Config به موارد پیش فرض بازگردانید.

1 شروع EpsonNet Config.

2 چاپگری را انتخاب کنید که می خواهید تنظیمات شبکه آن را بازیابی کنید.

3 روی نام چاپگر کلیک راست کنید، سپس Default Settings (تنظیمات پیش فرض) < Network Interface (رابط شبکه) را انتخاب کنید.

4 در صفحه تأیید روی OK (تایید) کلیک کنید.

5 بر روی OK (تایید) کلیک کنید.

بررسی ارتباط دستگاه‌ها و رایانه

بررسی اتصال با دستور Ping

برای حصول اطمینان از درستی اتصال رایانه به چاپگر می توانید از دستور Ping استفاده کنید. برای بررسی اتصال با دستور Ping مراحل زیر را طی کنید.

1 آدرس IP اتصال مورد استفاده را بررسی کنید.

این آدرس را می توانید از ستون IP Address (آدرس IP) برگه وضعیت شبکه بررسی کنید.

2 صفحه اعلان خط فرمان رایانه را نمایش دهید.

3 موارد زیر را در خط فرمان وارد کنید و سپس Enter را فشار دهید.

ping 192.0.2.111 (اگر آدرس IP کامپیوتری که می خواهید بررسی کنید 192.0.2.111 است)

رفع مشکلات

4

اگر مورد زیر نشان داده شد، تأییدیه کامل است. **Command Prompt (خط فرمان)** را ببندید.

آمار را برای 192.0.2.111 پینگ کنید:

Packets: Sent = 4, Received = 4, Lost = 0 (loss 0%),

Round-trip time: (ms):

Minimum = 0ms, Maximum = 0ms, Average = 0ms

مشکلات مربوط به استفاده از نرم افزار شبکه

بدون دسترسی Web Config

آیا آدرس IP چاپگر به درستی پیکربندی شده است؟

با استفاده از EpsonNet Config یا صفحه کنترل چاپگر، آدرس IP را پیکربندی کنید. می توانید از طریق صفحه وضعیت شبکه یا از پانل کنترل چاپگر، اطلاعات تنظیم فعلی را تأیید کنید.

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

رمزگذاری عمده برای قدرت رمزگذاری برای SSL/TLS به صورت زیر است. Web Config فقط از طریق مرورگری قابل دسترسی است که از رمزگذاری های عمده زیر پشتیبانی می کند. 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 communication (https).

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

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

آدرس IP چاپگر وارد شده برای Common Name (نام معمول) 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 چاپگر را تغییر دهید.

چاپگر از طریق سرور پراکسی قابل دسترسی است.

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

گزینه **Control Panel** (پانل کنترل) < **Network and Internet** (شبکه و اینترنت) < **Internet Options** (گزینه های اینترنت) < **Connections** (اتصالات) < **LAN settings** (تنظیمات LAN) < **Proxy server** (سرور پراکسی) را انتخاب کنید و سپس پیکربندی کنید که از سرور پراکسی برای آدرس های محلی استفاده نشود.

رفع مشکلات

مثال ها:

*.192.168.1: آدرس محلی 192.168.1.XXX، پوشش زیر شبکه 255.255.255.0
 *.192.168.XXX.XXX: آدرس محلی 192.168.XXX.XXX، پوشش زیر شبکه 255.255.0.0

اطلاعات مرتبط

← "دسترس به Web Config" در صفحه 22

← "تخصیص آدرس IP با استفاده از EpsonNet Config" در صفحه 16

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 **Block** (مسدود کردن)، **Cancel** (لغو) یا **Shut down** (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** (ابزارها) < **Options** (گزینه ها) < **Timeout** (مهلت زمانی) را انتخاب نمایید و سپس مدت زمان را برای تنظیم **Communication Error** (خطای گفتگو) افزایش دهید. توجه داشته باشید اینکار می تواند موجب کندتر اجرا شدن EpsonNet Config شود.

رفع مشکلات مربوط به امنیت پیشرفته

بازگرداندن تنظیمات امنیتی

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

غیرفعال کردن عملکرد ایمنی از چاپگر

می توانید فیلترینگ IPsec/IP را از چاپگر غیرفعال کنید.

1 **Menu** (منو) - **Network Settings** (همه تنظیمات Wi-Fi/شبکه) را انتخاب کنید.

2 **Advanced Setup** (نصب و جوی پیشرفته) را انتخاب کنید.

3 **Disable IPsec/IP Filtering** (فیلتر IPsec / IP را غیرفعال کنید) را انتخاب کنید.

4 دکمه **OK** را در صفحه تأیید فشار دهید.

5 با نمایش پیام تکمیل مراحل راه اندازی، دکمه **OK** را فشار دهید.

بازیابی عملکرد ایمنی با استفاده از Web Config

اگر بتوانید از کامپیوتر به دستگاه دسترسی پیدا کنید می توانید این عملکرد را غیرفعال کنید.

غیرفعال کردن فیلترینگ IPsec/IP با استفاده از Web Config

1 به Web Config بروید و Network Security Settings (تنظیمات امنیتی شبکه) < IPsec/IP Filtering (فیلتر کردن IPsec/IP) < Basic (ابتدایی) را انتخاب کنید.

2 Disable (غیرفعال کردن) را برای IPsec/IP Filtering (فیلتر کردن IPsec/IP) در Default Policy (سیاست پیش فرض) انتخاب کنید.

3 بر روی Next (بعدی) کلیک کنید و Enable this Group Policy (فعال کردن سیاست گروهی) را برای همه سیاست‌های گروه پاک نمایید.

4 بر روی OK (تایید) 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 به اشتراک گذاشته شده-

کلید را دوباره با استفاده از Web Config پیکربندی کنید.

برای تغییر کلید، به Web Config بروید و Network Security Settings (تنظیمات امنیتی شبکه) < IPsec/IP Filtering (فیلتر کردن IPsec/IP) < Basic (ابتدایی) < Default Policy (سیاست پیش فرض) یا Group Policy (سیاست گروهی) را انتخاب کنید.

اطلاعات مرتبط

◀ "دسترسی به Web Config" در صفحه 22

می توانید با IPsec Communication ارتباط برقرار کنید

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

چاپگر از الگوریتم های زیر پشتیبانی می کند.

الگوریتم ها	روش های امنیتی
AES-CBC 128, AES-CBC 192, AES-CBC 256, 3DES-CBC, DES-CBC	الگوریتم رمزگذاری
SHA-1, SHA2-256, SHA2-384, SHA2-512, MD5	الگوریتم هش
*Diffie e-Hellman Group14, *Diffie e-Hellman Group1, Diffie e-Hellman Group2 *Elliptic Curve Diffie e-Hellman P-384, *Elliptic Curve Diffie e-Hellman P-256	الگوریتم جابجایی کلید

* ممکن است روش موجود بر اساس مدل فرق داشته باشد.

اطلاعات مرتبط

◀ "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 42

رفع مشکلات

می تواند به طور ناگهانی ارتباط برقرار کند

آیا آدرس IP چاپگر نامعتبر است یا تغییر کرده است؟

از قسمت پانل کنترل چاپگر 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 چاپگر (Network Security Settings) (تنظیمات امنیتی شبکه) < IPsec/IP Filtering (فیلتر کردن IPsec/IP) < Basic (ابتدایی) < Group Policy (سیاست گروهی) < (Printer)Local Address (آدرس محلی (چاپگر)) یافت نشود. از آدرس IP ایستا استفاده کنید.

آیا آدرس IP رایانه نامعتبر است یا تغییر کرده است؟

از قسمت پانل کنترل چاپگر 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) (تنظیمات امنیتی شبکه) < IPsec/IP Filtering (فیلتر کردن IPsec/IP) < Basic (ابتدایی) < Group Policy (سیاست گروهی) < (Host)Remote Address (آدرس راه دور (میزبان)) 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 42

می توانید پورت چاپ IPP ایمنی ایجاد کنید

گواهی صحیحی به عنوان گواهی سرور برای ارتباط SSL/TLS تعیین شده است؟

اگر گواهی تعیین شده صحیح نباشد، پورت ایجاد نمی شود. دقت کنید از گواهی صحیحی استفاده کنید.

آیا گواهی CA در رایانه ای وارد می شود که به چاپگر دسترسی دارد؟

اگر گواهی CA در رایانه وارد نمی شود، پورت ایجاد نمی شود. مطمئن شوید گواهی CA وارد شود.

اطلاعات مرتبط

◀ "دسترسی به Web Config" در صفحه 22

بعد از پیکربندی IPsec/IP Filtering (فیلتر کردن IPsec/IP) می توانید وصل شوید

ممکن است مقدار تنظیم صحیح نباشد.

IPsec/IP Filtering (فیلتر کردن IPsec/IP) را از پانل کنترل چاپگر غیرفعال کنید. چاپگر و رایانه را به هم وصل کنید و دوباره تنظیمات IPsec/IP Filtering (فیلتر کردن IPsec/IP) را انجام دهید.

اطلاعات مرتبط

◀ "ارتباط رمزگذاری شده با IPsec/فیلترینگ IP" در صفحه 42

مشکلات مربوط به استفاده از یک گواهی دیجیتالی

می توانید گواهی امضاء شده از طریق CA را وارد کنید

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

رفع مشکلات

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 چاپگر 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؟

می 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، می توانید گواهی را وارد کنید.

اطلاعات مرتبط

❖ "وارد کردن گواهی امضاء شده از طریق CA" در صفحه 39

می توانید گواهی خود امضاء را به روزرسانی کنید

آیا Common Name (نام معمول) وارد شده است؟

Common Name (نام معمول) باید وارد شود.

نویسه های پشتیبانی نشده ای برای Common Name (نام معمول) 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.

کاما یا فاصله ای در Common Name (نام معمول) قرار دارد؟

اگر ویرگول وارد شده است، Common Name (نام معمول) 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 41

می توانید CSR ایجاد کنید

آیا Common Name (نام معمول) وارد شده است؟

Common Name (نام معمول) باید وارد شود.

نویسه های پشتیبانی نشده ای برای Common Name (نام معمول)، Organization (سازمان)، Organizational Unit (واحد سازمانی)، Locality (محل)، State/Province (استان/ایالت) 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.

کاما یا فاصله ای در Common Name (نام معمول) قرار دارد؟

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

رفع مشکلات

اطلاعات مرتبط

← "دریافت گواهی امضاء شده از طریق CA" در صفحه 37

هشداري مربوط به يك گواهي ديجيتالي ظاهر مي شود

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

رفع مشکلات

پیام ها	علت/باید چه کاری انجام داد
Cannot use the Server Certificates that include more than three CA certificates. (می توانید از گواهی های سروری که بیش از سه گواهی CA دارند استفاده کنید.)	علت: فایل گواهی با فرمت PKCS#12 بیشتر از 3 گواهی CA دارد. چه باید کرد: 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 your printer. (گواهی منقضی شده است. بررسی کنید گواهی معتبر باشد یا تاریخ و ساعت روی چاپگر را بررسی کنید.)	علت: تاریخ گواهی گذشته است. چه باید کرد: <input type="checkbox"/> اگر تاریخ گواهی گذشته است، گواهی جدیدی دریافت و وارد کنید. <input type="checkbox"/> اگر گواهی تاریخ گذشته نیست، دقت کنید تاریخ و زمان چاپگر به درستی تنظیم شده باشند.
Private key is required. (کلید خصوصی لازم است.)	علت: کلید خصوصی جفت شده ای با گواهی وجود ندارد. چه باید کرد: <input type="checkbox"/> اگر گواهی فرمت PEM/DER دارد و با استفاده از یک CSR و از طریق رایانه دریافت شده باشد، فایل کلید خصوصی را مشخص کنید. <input type="checkbox"/> اگر گواهی فرمت PKCS#12 دارد و با استفاده از یک CSR و از طریق رایانه دریافت شده باشد، فایلی ایجاد کنید که محتوی کلید خصوصی باشد.
	علت: گواهی PEM/DER دریافت شده از طریق CSR و با استفاده از Web Config را دوباره وارد کرده اید. چه باید کرد: 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. (راه اندازی نشد.)	علت: می توانید پیکربندی را تمام کنید زیرا ارتباط بین چاپگر و رایانه برقرار نشده است یا به دلیل خطاهایی، فایل قابل خواندن نیست. چه باید کرد: بعد از بررسی فایل مشخص شده و ارتباط، دوباره فایل را وارد کنید.

اطلاعات مرتبط

◀ "دوباره گواهی دیجیتالی" در صفحه 37

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، می توانید گواهی حذف شده را دوباره وارد کنید. یک CSR ایجاد کنید و گواهی جدیدی دریافت کنید.

اطلاعات مرتبط

◀ "حذف گواهی امضاء شده از طریق CA" در صفحه 40

◀ "وارد کردن گواهی امضاء شده از طریق CA" در صفحه 39

ضمیمه

معرفی نرم افزار شبکه

شرح نرم افزار پیکربندی و مدیریت دستگاه ها در ادامه می آید.

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 دستگاه ها، مانند وضعیت و مواد مصرفی، ارسال پیام های هشدار و ایجاد گزارش مصرف دستگاه امکان پذیر 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 وبسایت پشتیبانی Epson دانلود کنید. برای دریافت اطلاعات بیشتر، به اسناد یا راهنمای Epson Device Admin مراجعه کنید.

اجرای Epson Device Admin (فقط Windows)

All Programs (برنامه ها) < EPSON < Epson Device Admin < Epson Device Admin را اجرا کنید.

توجه:

اگر اخطار فایروال نمایان شد، به Epson Device Admin اجازه دسترسی بدهید.

EpsonNet Print

EpsonNet Print نرم افزاری برای چاپ در شبکه TCP/IP است. ویژگی ها و محدودیت هایی وجود دارد که در زیر عنوان می شود.

- ☐ وضعیت چاپگر بر روی صفحه اسپولر (جمع کننده) نشان داده می شود.
- ☐ اگر آدرس IP چاپگر از طریق DHCP تغییر کند، چاپگر هنوز هم شناسایی می شود.
- ☐ می توانید از چاپگری که در قسمت دیگری از شبکه قرار دارد استفاده کنید.
- ☐ می توانید با یکی از چندین پروتکل مختلف چاپ کنید.
- ☐ آدرس IPv6 پشتیبانی نمی شود.

EpsonNet SetupManager

EpsonNet SetupManager نرم افزاری برای ایجاد یک بسته برای نصب آسان چاپگر می باشد مانند نصب درایور چاپگر، نصب EPSON Status Monitor و ایجاد یک پورت چاپگر. 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.