EPSON
EXCEED YOUR VISION

دليل شبكة الاتصال

NPD5771-00 AR

المحتويات

المحتويات

ملحق

حقوق الطبع والنشر

لا يجوز إعادة إنتاج أي جزء من هذا الدليل أو تخزينه في نظام استرجاع أو نقله بأي شكل أو طريقة، إلكترونيًا أو ميكانيكيًا، أو من خلال التصوير الفوتوغرافي أو التسجيل أو خلافه، بدون إذن كتابي مسبق من Seiko Epson Corporation. لا توجد مسؤولية قانونية تجاه براءة الاختراع في ما يخص استخدام المعلومات الواردة في هذه الوثيقة. وليس ثمة أي مسؤولية قانونية عن أية تلفيات ناجمة عن استخدام المعلومات الواردة في هذه الوثيقة. وقد تم إعداد المعلومات الواردة في هذه الوثيقة للاستخدام فقط مع هذا المنتج من Epson. ولا تتحمل Epson أي مسؤولية عن أي استخدام لهذه المعلومات مع منتجات أخرى.

لا تتحمل Seiko Epson Corporation أو أي من الشركات التابعة لمشتري هذا المنتج أو أطراف ثالثة أية مسؤولية عن أية أضرار أو خسائر أو تكاليف أو نفقات تكبدها المشتري أو أطراف ثالثة نتيجة لتعرض هذا المنتج لحادث أو سوء استخدامه أو العبث به أو إجراء أي تعديلات أو إصلاحات أو تغييرات غير مصرح بها عليه، أو (باستثناء الولايات المتحدة) الإخفاق في الالتزام الكامل بتعليمات التشغيل والصيانة الصادرة من Seiko Epson Corporation.

لا تتحمل Seiko Epson Corporation أو أي من الشركات التابعة لها المسؤولية عن أية أضرار أو مشاكل تنشأ من استخدام أي وحدات اختيارية أو منتجات استهلاكية غير تلك المعينة كمنتجات Epson أصلية أو منتجات Epson معتمدة من Seiko Epson Corporation.

لا تتحمل Seiko Epson Corporation المسؤولية عن أي ضرر ينشأ من التداخل الكهرومغناطيسي الذي يحدث نتيجة استخدام أي كبلات توصيل غير تلك المعينة كمنتجات Epson معتمدة من Seiko Epson Corporation.

©2017 Seiko Epson Corporation

محتويات هذا الدليل ومواصفات هذا المنتج عرضة للتغيير دون إشعار.

العلامات التجارية

- ❏ EPSON® علامة تجارية مسجلة، وEPSON EXCEED YOUR VISION أو EXCEED YOUR VISION علامة تجارية لشركة Seiko Epson Corporation.
- ❏ يستند برنامج Epson Scan 2 جزئيًا إلى أعمال Independent JPEG Group.
- ❏ Google Cloud Print™ وChrome™ وChrome OS™ وAndroid™ علامات تجارية لشركة Google Inc.
- ❏ Microsoft® وWindows® وWindows Server® وWindows Vista® علامات تجارية مسجلة لشركة Microsoft Corporation.
- ❏ IBM علامة تجارية مسجلة لشركة International Business Machines Corporation.
- ❏ إشعار عام: أسماء المنتجات الأخرى المستخدمة في هذه الوثيقة هي لأغراض التعريف فحسب، ويجوز أن تكون علامات تجارية لمالكيها. وتخلي Epson مسؤوليتها عن كل الحقوق في تلك العلامات.

حول هذا الدليل

العلامات والرموز

> تنبيه:
> تعليمات يجب اتباعها بعناية تجنبًا لإصابة بدنية.

> مهم:
> تعليمات يجب الالتزام بها تجنبًا لتلف الجهاز.

> ملاحظة:
> تعليمات تشتمل على تلميحات مفيدة وقيود حول تشغيل الطابعة.

معلومات ذات صلة
يؤدي النقر فوق هذا الرمز إلى عرض معلومات ذات صلة.

الأوصاف المستخدمة في هذا الدليل

تأتي الرسوم التوضيحية للطابعة المستخدمة في هذا الدليل على سبيل المثال فحسب. وبالرغم من وجود اختلافات طفيفة حسب الطراز المستخدم، إلا أن طريقة التشغيل تظل واحدة.

مراجع أنظمة التشغيل

Windows

في هذا الدليل، تشير مصطلحات مثل "Windows 10" و"Windows 8.1" و"Windows 8" و"Windows 7" و"Windows Vista" و"Windows XP" و"Windows Server 2012 R2" و"Windows Server 2012" و"Windows Server 2008 R2" و"Windows Server 2008" و"Windows Server 2003 R2" و"Windows Server 2003" إلى أنظمة التشغيل التالية. إضافة إلى ذلك، يُستخدم مصطلح "Windows" للإشارة إلى كل الإصدارات.

- ❏ Microsoft® نظام التشغيل Windows® 10
- ❏ Microsoft® نظام التشغيل Windows® 8.1
- ❏ Microsoft® نظام التشغيل Windows® 8
- ❏ Microsoft® نظام التشغيل Windows® 7
- ❏ Microsoft® نظام التشغيل Windows Vista®
- ❏ Microsoft® نظام التشغيل Windows® XP
- ❏ Microsoft® نظام التشغيل Windows® XP Professional x64 Edition

حول هذا الدليل

- ❏ Microsoft® نظام التشغيل Windows Server® 2012 R2
- ❏ Microsoft® نظام التشغيل Windows Server® 2012
- ❏ Microsoft® نظام التشغيل Windows Server® 2008 R2
- ❏ Microsoft® نظام التشغيل Windows Server® 2008
- ❏ Microsoft® نظام التشغيل Windows Server® 2003 R2
- ❏ Microsoft® نظام التشغيل Windows Server® 2003

مقدمة

مكونات الدليل

يشرح هذا الدليل كيفية توصيل الطابعة بالشبكة، ويشتمل على معلومات حول كيفية ضبط الإعدادات لاستخدام الوظائف.

راجع دليل المستخدم للاطلاع على معلومات استخدام الوظائف.

التجهيز
يشرح كيفية إعداد الأجهزة والبرامج المستخدمة للإدارة.

الاتصال
يشرح كيفية توصيل طابعة بالشبكة.

إعدادات الوظيفة
يشرح إعدادات الطباعة.

إعدادات الأمان
يشرح إعدادات الأمان، مثل إعدادات كلمة مرور المسؤول والتحكم في البروتوكول.

حل المشاكل
يشرح تهيئة الإعدادات واكتشاف أخطاء الشبكة وإصلاحها.

تعريفات المصطلحات المستخدمة في هذا الدليل

تُستخدم المصطلحات التالية في هذا الدليل.

المسؤول
الشخص المسؤول عن تركيب الجهاز وتهيئة الشبكة وإعدادهما في مكتب أو مؤسسة. ففي المؤسسات الصغيرة، قد يتولى هذا الشخص مسؤولية إدارة الجهاز والشبكة على حد سواء. وفي المؤسسات الكبرى، يتمتع المسؤولون بصلاحية مراقبة الشبكة أو الأجهزة في وحدة مجموعة إحدى الإدارات أو الأقسام، ويتولى مسؤولو الشبكة مسؤولية إعدادات الاتصال خارج المؤسسة، مثل الإنترنت.

مسؤول الشبكة
الشخص المسؤول عن مراقبة اتصال الشبكة. الشخص الذي يتولى إعداد جهاز التوجيه (الراوتر)، وخادم الوكيل، وخادم DNS، وخادم البريد الإلكتروني لمراقبة الاتصال عبر الإنترنت أو الشبكة.

المستخدم
الشخص الذي يستخدم الأجهزة، مثل الطابعات.

اتصال الخادم/العميل (إتاحة الطابعة للمشاركة باستخدام خادم Windows)
الاتصال الذي يشير إلى اتصال الطابعة بخادم Windows عبر الشبكة أو من خلال كبل USB، وإمكانية مشاركة قائمة انتظار الطباعة المعيَّنة في الخادم. يتم الاتصال بين الطابعة والكمبيوتر عبر الخادم، ويتم التحكم في الطابعة في الخادم.

اتصال نظير إلى نظير (الطباعة المباشرة)
الاتصال الذي يشير إلى اتصال الطابعة والكمبيوتر بالشبكة عبر الموزِّع أو نقطة الوصول، ويمكن تنفيذ مهمة الطباعة من الكمبيوتر مباشرة.

Web Config (صفحة الويب للجهاز)
خادم الويب المضمن في الجهاز. ويُطلق عليه اسم Web Config. يمُكنك التحقق من حالة الجهاز وتغييرها من خلال المتصفح.

مقدمة

قائمة انتظار الطباعة
في Windows، رمز كل منفذ المعروض في **Device and Printer (الجهاز والطابعة)**، مثل طابعة. ويمكن أيضًا إنشاء رمزين أو أكثر لجهاز واحد إذا كان الجهاز متصلاً بالشبكة عبر منفذين أو أكثر، مثل TCP/IP القياسي.

الأداة
مصطلح عام للبرنامج اللازم لإعداد الجهاز أو إدارته، مثل Epson Device Admin وEpsonNet Config وEpsonNet SetupManager, وما إلى ذلك.

ASCII (الشفرة القياسية الأمريكية لتبادل المعلومات)
إحدى شفرات الحروف القياسية. يتم تحديد 128 حرفًا، بما في ذلك الحروف الأبجدية (من a إلى z، ومن A إلى Z)، والأرقام العربية (من 0 إلى 9)، والرموز، والحروف الفارغة، وحروف التحكم. عندما يُذكر المصطلح "ASCII" في هذا الدليل، فإنه يشير إلى 0x20–0x7E (عدد سداسي عشري) المدرج أدناه، ولا يتضمن أي حروف تحكم.

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

* حرف المسافة.

معيار Unicode (UTF-8)
رمز قياسي دولي يغطي اللغات العالمية الرئيسية. عندما يُذكر المصطلح "UTF-8" في هذا الدليل، فإنه يشير إلى حروف الترميز بتنسيق UTF-8.

التجهيز

يشرح هذا الفصل المتطلبات اللازمة للتجهيز قبل ضبط الإعدادات.

تدفق إعدادات الطابعة

يتم ضبط إعدادات اتصال الشبكة وإجراء الإعداد الأولي بحيث تصبح الطابعة متوفرة للمستخدمين.

1 التجهيز

- ❏ جمع معلومات إعداد الاتصال
- ❏ تحديد طريقة الاتصال

2 الاتصال

- ❏ إنشاء اتصال الشبكة باستخدام EpsonNet Config

3 إعداد الطباعة

- ❏ إعدادات برنامج تشغيل الطابعة

4 إعدادات الأمان

- ❏ إعدادات المسؤول
- ❏ SSL/TLS (طبقة المقابس الآمنة/أمان طبقة النقل)
- ❏ التحكم في البروتوكول
- ❏ تصفية IPsec/IP

معلومات ذات صلة

"الاتصال" في الصفحة 14
"إعدادات الوظيفة" في الصفحة 20
"إعدادات الأمان" في الصفحة 28

مقدمة حول اتصال الطابعة

تتوفر الطريقتان التاليتان لاتصال شبكة الطابعة.

- ❏ اتصال الخادم/العميل (إتاحة الطابعة للمشاركة باستخدام خادم Windows)
- ❏ اتصال نظير إلى نظير (الطباعة المباشرة)

معلومات ذات صلة
"إعدادات اتصال الخادم/العميل" في الصفحة 11
"إعدادات اتصال نظير إلى نظير" في الصفحة 11

إعدادات اتصال الخادم/العميل

طريقة الاتصال:

وصِّل الطابعة بالشبكة عبر موزِّع (محوِّل L2). يمكنك أيضًا توصيل الطابعة بالخادم مباشرة عبر كبل USB.

برنامج تشغيل الطابعة:

ثبّت برنامج تشغيل الطابعة في خادم Windows حسب نظام تشغيل أجهزة الكمبيوتر العميلة. ومن خلال الوصول إلى خادم Windows وربط الطابعة، يتم تثبيت برنامج تشغيل الطابعة في الكمبيوتر العميل ويمكن استخدامه.

الميزات:

- ❏ إدارة الطابعة وبرنامج تشغيلها دفعة واحدة.
- ❏ حسب مواصفات الخادم، قد يستغرق بدء مهمة الطباعة وقتًا لأن جميع مهام الطباعة تتم من خلال خادم الطباعة.
- ❏ لا يمكنك الطباعة عندما يكون خادم Windows متوقفًا.

معلومات ذات صلة
"تعريفات المصطلحات المستخدمة في هذا الدليل" في الصفحة 8

إعدادات اتصال نظير إلى نظير

طريقة الاتصال:

وصِّل الطابعة بالشبكة عبر موزِّع (محوِّل L2).

برنامج تشغيل الطابعة:

ثبِّت برنامج تشغيل الطابعة في كل كمبيوتر عميل. يمكن تسليمه كحزمة باستخدام EpsonNet SetupManager أو تلقائيًا باستخدام نهج المجموعة لخادم Windows.

الميزات:

- ❏ تبدأ مهمة الطباعة في الحال؛ إذ يتم إرسالها إلى الطابعة مباشرة.
- ❏ يمكنك الطباعة ما دامت الطابعة قيد التشغيل.

معلومات ذات صلة
"تعريفات المصطلحات المستخدمة في هذا الدليل" في الصفحة 8

تجهيز الاتصال بشبكة

جمع معلومات عن إعداد الاتصال

يجب توفر عنوان IP وعنوان بوابة، وما إلى ذلك من أجل الاتصال بالشبكة. تحقق مما يلي مقدمًا.

الأقسام	العناصر	ملاحظة
طريقة اتصال الجهاز	❑ شبكة إيثرنت	استخدم كبلاً مزدوجًا مجدولاً مصفحًا (STP) من الفئة 5e أو أعلى.
معلومات اتصال LAN	❑ عنوان IP ❑ قناع الشبكة الفرعية ❑ البوابة الافتراضية	إذا عيَّنت عنوان IP تلقائيًا باستخدام وظيفة DHCP في جهاز التوجيه، فلا داعي لذلك.
معلومات خادم DNS	❑ عنوان IP لنظام DNS الرئيسي ❑ عنوان IP لنظام DNS الثانوي	إذا كنت تستخدم عنوان IP ثابتًا كعنوان IP، فهيئ خادم DNS. تتم التهيئة عند تعيين عناوين IP تلقائيًا باستخدام وظيفة DHCP وعند تعذر تعيين خادم DNS تلقائيًا.

مواصفات الطابعة

مواصفات دعم الطابعة للوضع القياسي أو وضع الاتصال، راجع دليل المستخدم.

نوع تعيين عنوان IP

يوجد نوعان لتعيين عنوان IP للطابعة.

عنوان IP ثابت:

عينّ عنوان IP الفريد المحدد مسبقًا للطابعة.

لا يتم تغيير عنوان IP حتى عند إيقاف تشغيل الطابعة أو جهاز التوجيه؛ لذلك يمكنك إدارة الجهاز باستخدام عنوان IP.

يناسب ذلك النوع أي شبكة تتم فيها إدارة العديد من الطابعات، مثل مكتب كبير أو مدرسة.

التعيين التلقائي باستخدام وظيفة DHCP:

يتم تعيين عنوان IP الصحيح تلقائيًا عند نجاح الاتصال بين الطابعة وجهاز التوجيه الذي يدعم وظيفة DHCP.

إذا لم يكن هذا النوع ملائمًا لتغيير عنوان IP لجهاز محدد، فاحتفظ بعنوان IP مقدمًا ثم عيِّنه.

ملاحظة:
بالنسبة إلى منفذ قائمة انتظار الطباعة، حدد البروتوكول الذي يمكنه اكتشاف عنوان *IP* تلقائيًا، مثل *EpsonNet Print Port*.

طريقة إعداد الاتصال بالشبكة

للحصول على إعدادات الاتصال لعنوان IP للطابعة، وقناع الشبكة الفرعية، والبوابة الافتراضية، تابع ما يلي.

استخدام EpsonNet Config:

استخدم EpsonNet Config من كمبيوتر المسؤول. يمكنك تعيين العديد من الطابعات، لكن يجب توصيلها بشكل مادي عبر كبل إيثرنت قبل الإعداد. يمكنك إبقاء المخاطر الأمنية عند مستويات منخفضة إذا تمكنت من إنشاء شبكة إيثرنت للإعداد وعيِّنت إعدادات الشبكة للطابعة ثم وصِّل الطابعة بشبكة عادية.

استخدام المثبِّت:

إذا تم استخدام المثبِّت، فسيتم تعيين شبكة الطابعة والكمبيوتر العميل تلقائيًا. يتوفر الإعداد عن طريق اتباع تعليمات المثبِّت، حتى لو لم تكن على دراية كبيرة بالشبكة. ويوصى بذلك عند تعيين الطابعة وعدد قليل من أجهزة الكمبيوتر العميل باستخدام اتصال الخادم/العميل (إتاحة الطابعة للمشاركة باستخدام خادم Windows).

معلومات ذات صلة

◆ "تعيين عنوان IP باستخدام EpsonNet Config" في الصفحة 14
◆ "الاتصال بالشبكة باستخدام المثبِّت" في الصفحة 18

تثبيت EpsonNet Config

نزِّل EpsonNet Config من موقع دعم Epson ثم ثبِّته باتباع التعليمات التي تظهر على الشاشة.

تشغيل EpsonNet Config

حدد **All Programs (كافة البرامج)** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

ملاحظة:
إذا ظهر تنبيه جدار الحماية، فاسمح بالوصول إلى *EpsonNet Config*.

الاتصال

يشرح هذا الفصل البيئة أو الإجراءات اللازمة لتوصيل الطابعة بالشبكة.

الاتصال بالشبكة

الاتصال بشبكة LAN

وصِّل الطابعة بالشبكة عبر إيثرنت.

معلومات ذات صلة

"الاتصال بالشبكة باستخدام المثبِّت" في الصفحة 18

تعيين عنوان IP باستخدام EpsonNet Config

عيِّن عنوان IP للطابعة باستخدام EpsonNet Config.

1. شغِّل الطابعة.
2. وصِّل الطابعة بالشبكة باستخدام كبل إيثرنت.
3. ابدأ EpsonNet Config.

تظهر عندئذٍ قائمة بالطابعات المتصلة بالشبكة. قد يستغرق الأمر بعض الوقت قبل عرضها.

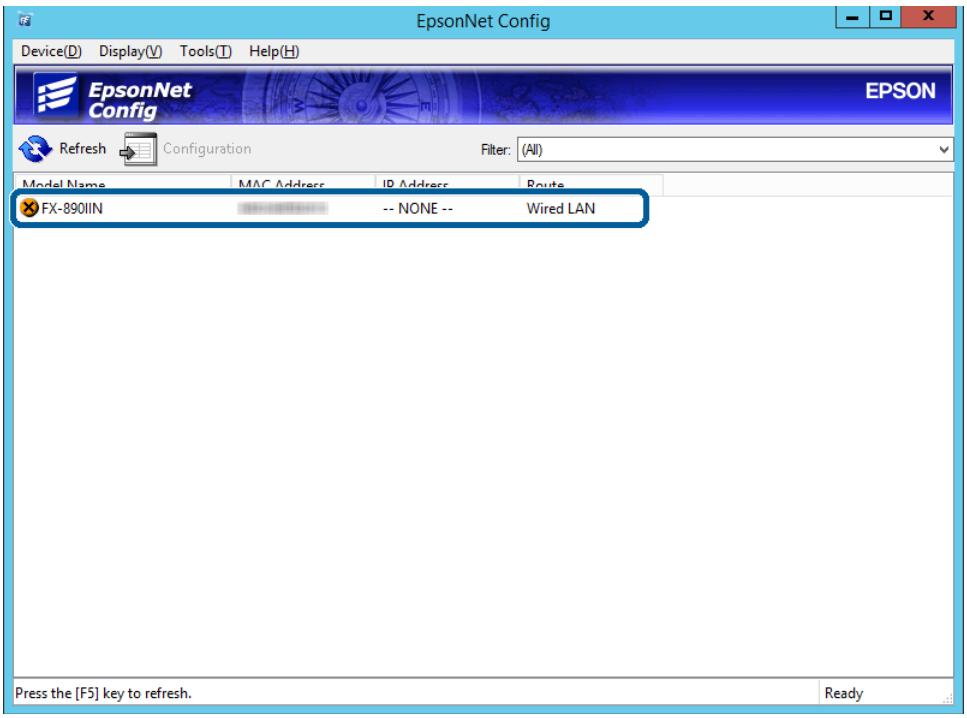
4. انقر نقرًا مزدوجًا فوق الطابعة التي تريد تعيين عنوان IP لها.

إذا وصلت الطابعة بشبكة بوظيفة DHCP متوفرة, يتم تعيين عنوان IP باستخدام وظيفة DHCP، ويظهر بعد ذلك الرمز .

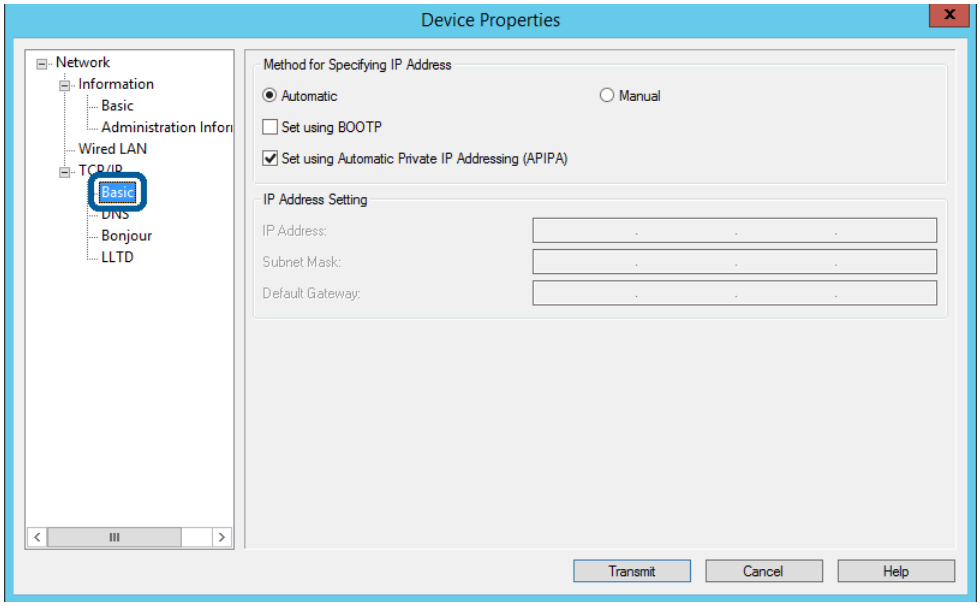
ملاحظة:

- إذا وصلت عدة طابعات من الطراز نفسه، يمكنك تحديد الطابعة باستخدام عنوان *MAC*.
- بعد توصيل الطابعة بالشبكة، يمكنك تغيير طريقة تعيين عنوان *IP*.

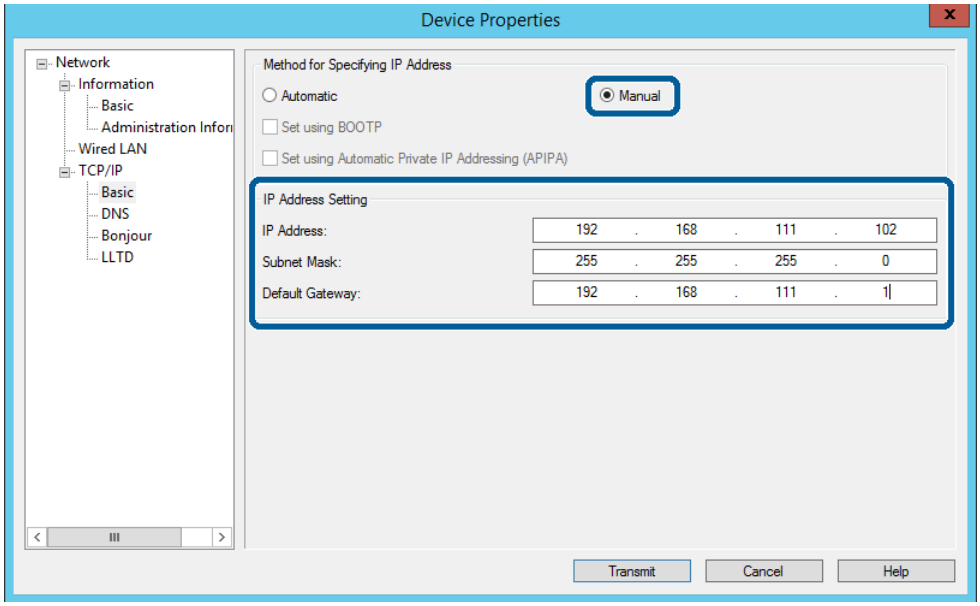
الاتصال



5 حدد **Network** (الشبكة) > **TCP/IP** > **Basic** (أساسي).



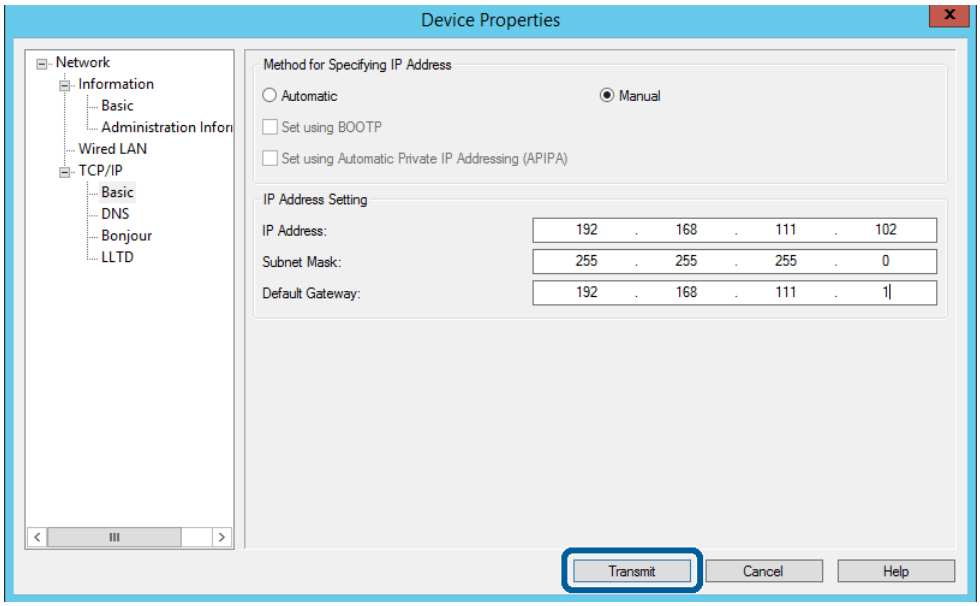
6 أدخل العناوين في **IP Address (عنوان IP)**، و**Subnet Mask (قناع الشبكة الفرعية)**، و**Default Gateway (البوابة الافتراضية)**.



ملاحظة:

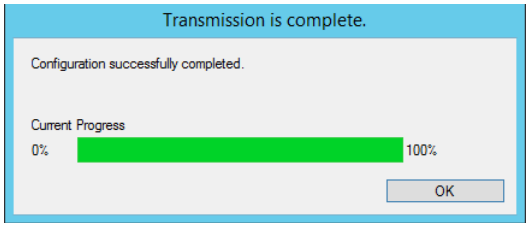
- ❏ أدخل عنوانًا ثابتًا عند توصيل الطابعة بشبكة آمنة.
- ❏ في قائمة *TCP/IP*، يمكنك ضبط إعدادات *DNS* في شاشة *DNS*.

7 انقر فوق **Transmit (إرسال)**.

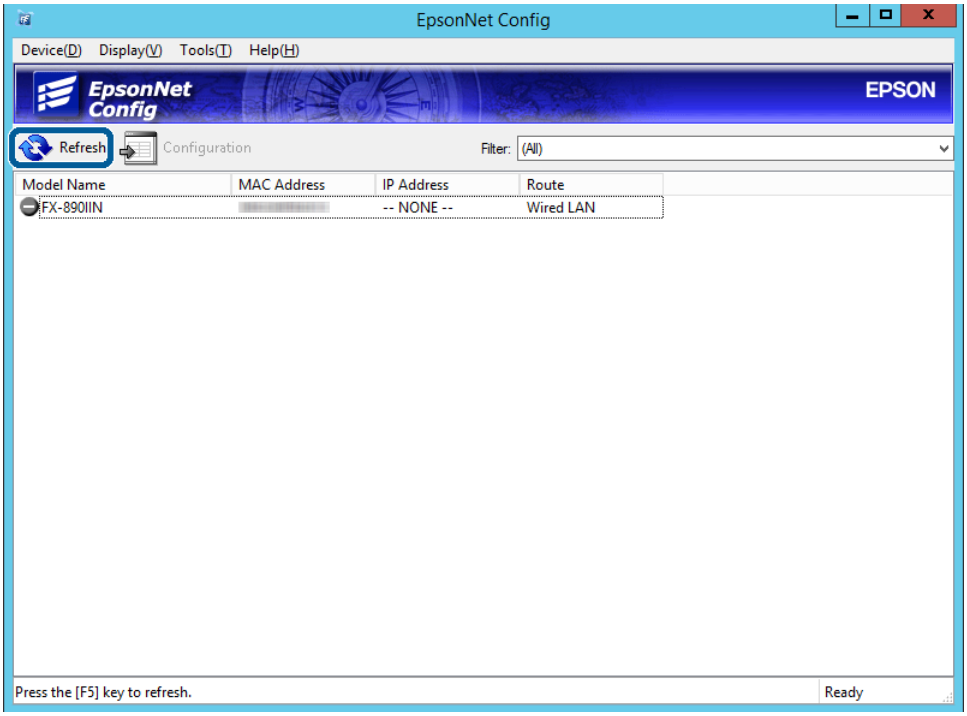


8 انقر فوق **OK (موافق)** في شاشة التأكيد.

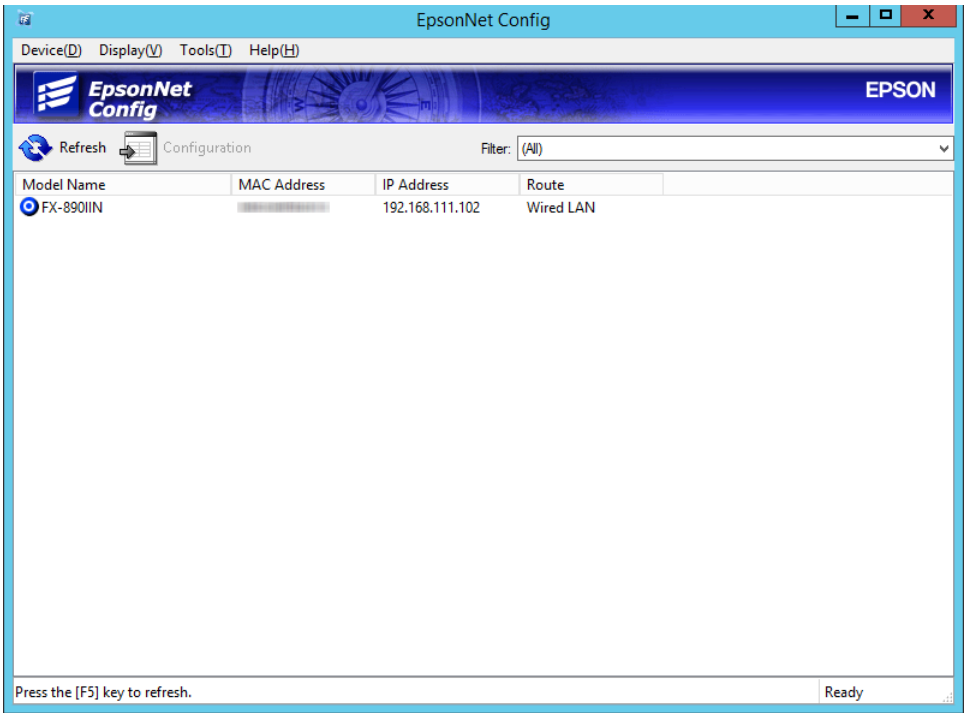
9 انقر فوق **OK** (**موافق**).



10 انقر فوق **Refresh** (**تحديث**).



تحقق من تعيين عنوان IP.

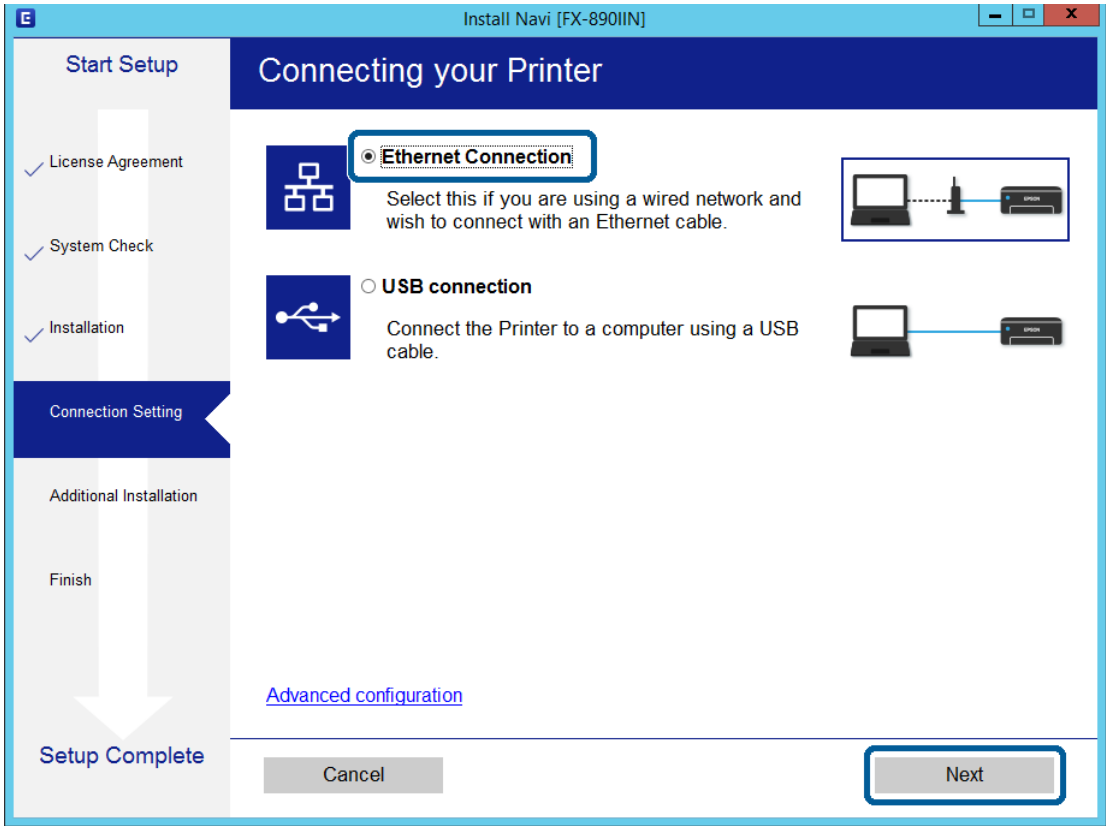


الاتصال بالشبكة باستخدام المثبِّت

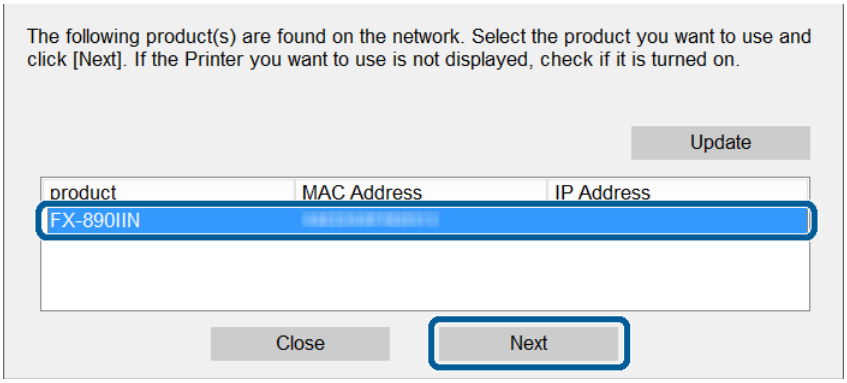
نوصي باستخدام المثبِّت لتوصيل الطابعة بكمبيوتر.

1 أدخل قرص البرامج في الكمبيوتر ثم اتبع التعليمات المعروضة على الشاشة.

2 اتبع التعليمات المعروضة على الشاشة حتى تظهر الشاشة التالية، وحدد **Ethernet Connection** (**اتصال إيثرنت**) ثم انقر فوق **Next** (**التالي**).



تظهر الشاشة التالية إذا وصلت الطابعة بالشبكة باستخدام كبل إيثرنت. حدد الطابعة ثم انقر فوق **Next** (**التالي**).



3 اتبع التعليمات المعروضة على الشاشة.

إعدادات الوظيفة

يشرح هذا الفصل الإعدادات الأولى الواجب ضبطها لاستخدام جميع وظائف الجهاز.

يشرح هذا الموضوع إجراءات ضبط الإعدادات من كمبيوتر المسؤول باستخدام Web Config.

Web Config (صفحة ويب للجهاز)

حول Web Config

Web Config هو تطبيق مستند إلى متصفح لتهيئة إعدادات الطابعة.

للوصول إلى Web Config، يجب أولاً تعيين عنوان IP للطابعة.

ملاحظة:
يمكنك قفل الإعدادات من خلال تهيئة كلمة مرور المسؤول للطابعة.

الوصول إلى Web Config

توجد طريقتان للوصول إلى Web Config. يجب تمكين JavaScript في المتصفح.

إدخال عنوان IP

ابدأ EpsonNet Config ثم انقر نقرًا مزدوجًا فوق الطابعة في القائمة.

أدخل عنوان IP للطابعة في متصفح ويب. عند الوصول إلى Web Config عبر HTTPS، ستظهر رسالة تحذير في المتصفح نظرًا لاستخدام شهادة موقعة ذاتيًا مخزنة في الطابعة.

- الوصول عبر HTTPS
  IPv4: <للطابعة IP عنوان>https://: (بدون استخدام < >)
  IPv6: /[للطابعة IP عنوان]https://: (باستخدام [ ])

- الوصول عبر HTTP
  IPv4: <للطابعة IP عنوان>http://: (بدون استخدام < >)
  IPv6: /[للطابعة IP عنوان]http://: (باستخدام [ ])

ملاحظة:

❏ أمثلة

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ إذا كان اسم الطابعة مسجلاً في خادم *DNS*، يمكنك استخدام اسم الطابعة بدلاً من عنوان *IP* الخاص بها.

❏ لا يتم عرض جميع القوائم عند الوصول إلى *Web Config* عبر *HTTP*. لعرض جميع القوائم، قم بالوصول إلى *Web Config* عبر *HTTPS*.

معلومات ذات صلة

"اتصال SSL/TLS بالطابعة" في الصفحة 33

"حول الشهادة الرقمية" في الصفحة 34

استخدام وظائف الطباعة

مكّن استخدام وظيفة الطباعة في الطابعة.

متطلبات الطباعة عبر شبكة

يجب تلبية المتطلبات التالية للطباعة عبر شبكة. ويمكنك تهيئة هذه الإعدادات باستخدام برنامج تشغيل الطابعة ووظائف نظام التشغيل.

❏ تثبيت برنامج تشغيل الطابعة

❏ إنشاء قائمة انتظار الطباعة لكمبيوتر

❏ تعيين المنفذ لشبكة

إعداد برنامج تشغيل الطابعة باستخدام اتصال الخادم/العميل

عينّ الطابعة على تمكين الطباعة من الكمبيوتر الذي تم تعيينه سابقًا كخادم الطباعة، وأتح الطابعة للمشاركة. ثبّت برنامج تشغيل الطابعة لكل من الخادم والعميل في خادم الطباعة. إذا تم استخدام المثبِّت، يتم تلقائيًا إعداد الشبكة أو الكمبيوتر للطابعة وتثبيت برنامج التشغيل وإنشاء قائمة انتظار الطباعة.

إعداد منافذ TCP/IP القياسية - Windows

قم بإعداد منفذ TCP/IP القياسي في خادم الطباعة، وأنشئ قائمة انتظار الطباعة لإجراء الطباعة عبر الشبكة.

1 افتح شاشة الأجهزة والطابعات.

❏ Windows 10/Windows Server 2016

انقر بزر الماوس الأيمن فوق زر البدء أو اضغط عليه مع الاستمرار ثم حدد **Control Panel (لوحة التحكم)** > **Hardware and Sound (الأجهزة والصوت)** > **Devices and Printers (الأجهزة والطابعات)**.

إعدادات الوظيفة

❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Desktop (سطح المكتب) > **Settings (إعدادات)** > **Control Panel (لوحة التحكم)** > **Hardware and Sound (الأجهزة والصوت)** أو **Hardware (الأجهزة)** > **Devices and Printers (الأجهزة والطابعات)**.

❏ Windows 7/Windows Server 2008 R2
انقر فوق زر البدء > **Control Panel (لوحة التحكم)** > **Hardware and Sound (الأجهزة والصوت)** (أو **Hardware (الأجهزة)**) > **Devices and Printers (الأجهزة والطابعات)**.

❏ Windows Vista/Windows Server 2008
انقر فوق زر البدء > **Control Panel (لوحة التحكم)** > **Hardware and Sound (الأجهزة والصوت)** > **Printers (الطابعات)**.

❏ Windows XP/Windows Server 2003 R2/Windows Server 2003
اضغط على زر البدء > **Control Panel (لوحة التحكم)** > **Printers and Other Hardware (الطابعات والأجهزة الأخرى)** > **Printers and Faxes (الطابعات والفاكسات)**.

2 أضف طابعة.

❏ Windows 10/Windows 8.1/Windows 8/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012
انقر فوق **Add printer (إضافة طابعة)** ثم حدد **The printer that I want isn't listed (الطابعة المطلوبة غير مدرجة)**.

❏ Windows 7/Windows Server 2008 R2
انقر فوق **Add printer (إضافة طابعة)**.

❏ Windows Vista/Windows Server 2008
انقر فوق **Install Printer (تثبيت طابعة)**.

❏ Windows XP/Windows Server 2003 R2/Windows Server 2003
انقر فوق **Install Printer (تثبيت طابعة)** ثم انقر فوق **Next (التالي)**.

3 أضف طابعة محلية.

❏ Windows 10/Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
حدد **Add a local printer or network printer with manual settings (إضافة طابعة محلية أو طابعة متصلة بشبكة باستخدام الإعدادات اليدوية)** ثم انقر فوق **Next (التالي)**.

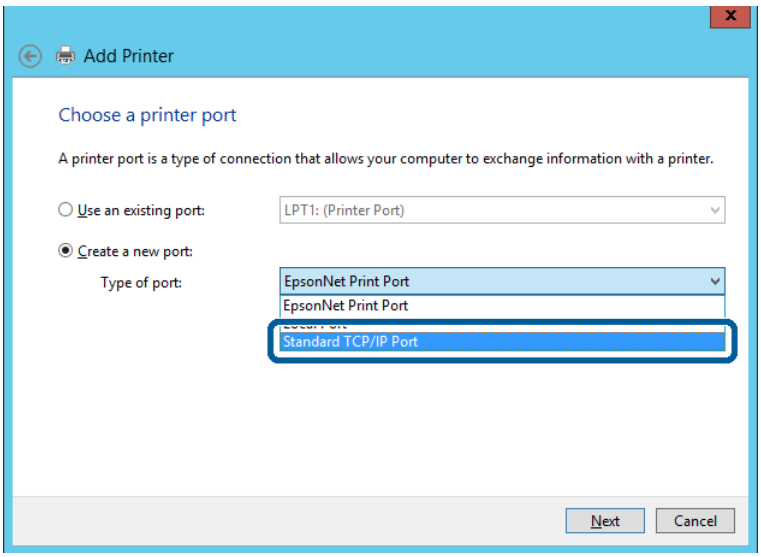
❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008
انقر فوق **Add a local printer (إضافة طابعة محلية)**.

❏ Windows XP/Windows Server 2003 R2/Windows Server 2003
حدد **Local printer attached to this computer (الطابعة المحلية الملحقة بهذا الكمبيوتر)** ثم انقر فوق **Next (التالي)**.

إعدادات الوظيفة

4 حدد **Create a new port (إنشاء منفذ جديد)**، وحدد **Standard TCP/IP Port (منفذ TCP/IP قياسي)** في نوع المنفذ ثم انقر فوق **Next (التالي)**.

في نظام التشغيل Windows XP/Windows Server 2003 R2/Windows Server 2003، انقر فوق **Next (التالي)** في شاشة **Add Standard TCP/IP Printer Port Wizard (معالج "إضافة منفذ طابعة TCP/IP قياسي")**.

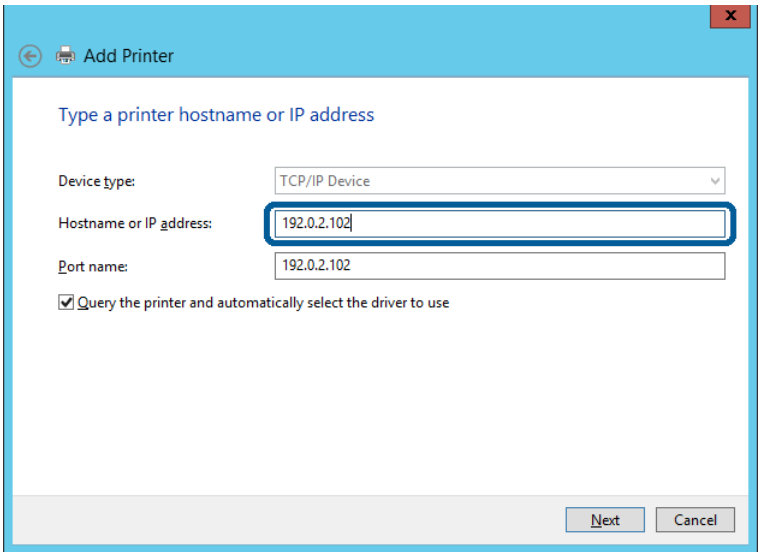


5 أدخل عنوان IP للطابعة أو اسمها في **Host Name or IP Address (اسم المضيف أو عنوان IP)** أو **Printer Name or IP Address (اسم الطابعة أو عنوان IP)** ثم انقر فوق **Next (التالي)**.

لا تغيِّر **Port name (اسم المنفذ)**.

انقر فوق **Continue (متابعة)** عند ظهور شاشة **User Account Control (التحكم في حساب المستخدم)**.

في نظام التشغيل Windows XP/Windows Server 2003 R2/Windows Server 2003، انقر فوق **Done (تم)** في شاشة **Standard TCP/IP Printer Port (إضافة منفذ طابعة TCP/IP قياسي)**.



ملاحظة:
إذا حددت اسم الطابعة في الشبكة التي يتوفر بها تحليل الاسم، يتم تتبع عنوان *IP* حتى لو تم تغيير عنوان *IP* للطابعة باستخدام *DHCP*.
يمكنك تأكيد اسم الطابعة من شاشة حالة الشبكة في لوحة تحكم الطابعة أو ورقة حالة الشبكة.

إعدادات الوظيفة

6 قم بإعداد برنامج تشغيل الطابعة.

❏ إذا كان برنامج تشغيل الطابعة مثبَّتًا من قبل:
حدد **Manufacturer** (**الشركة المصنّعة**) و**Printers** (**الطابعات**). انقر فوق **Next** (**التالي**).

❏ إذا لم يكن برنامج تشغيل الطابعة مثبَّتًا:
انقر فوق **Have Disc** (**قرص خاص**) ثم أدخل قرص البرامج المرفق بالطابعة. انقر فوق **Browse** (**استعراض**) ثم حدد المجلد في القرص الذي يحتوي على برنامج تشغيل الطابعة. تأكد من اختيار المجلد الصحيح. قد يتغير مكان المجلد حسب نظام التشغيل الذي تستخدمه.
إصدار 32 بت من Windows: WINX86
إصدار 64 بت من Windows: WINX64

7 اتبع التعليمات المعروضة على الشاشة.

في نظام التشغيل Windows XP/Windows Server 2003 R2/Windows Server 2003، يكون الإعداد مكتملاً. في Windows Vista/ Windows Server 2008 أو أحدث, تحقق من تهيئة المنفذ.

عند استخدام الطابعة ضمن اتصال الخادم/العميل (إتاحة الطابعة للمشاركة باستخدام خادم Windows)، اضبط إعدادات المشاركة الواردة أدناه.

معلومات ذات صلة
◆ "إتاحة الطابعة للمشاركة" في الصفحة 25

تحقق من تهيئة المنفذ - *Windows*

تحقق من تعيين المنفذ الصحيح لقائمة انتظار الطباعة.

1 افتح شاشة الأجهزة والطابعات.

❏ Windows 10/Windows Server 2016
انقر بزر الماوس الأيمن فوق زر البدء أو اضغط عليه مع الاستمرار ثم حدد **Control Panel** (**لوحة التحكم**) > **Hardware and Sound** (**الأجهزة والصوت**) > **Devices and Printers** (**الأجهزة والطابعات**).

❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Desktop (**سطح المكتب**) > **Settings** (**إعدادات**) > **Control Panel** (**لوحة التحكم**) > **Hardware and Sound** (**الأجهزة والصوت**) أو **Hardware** (**الأجهزة**) > **Devices and Printers** (**الأجهزة والطابعات**).

❏ Windows 7/Windows Server 2008 R2
انقر فوق زر البدء > **Control Panel** (**لوحة التحكم**) > **Hardware and Sound** (**الأجهزة والصوت**) (أو **Hardware** (**الأجهزة**)) > **Devices and Printers** (**الأجهزة والطابعات**).

❏ Windows Vista/Windows Server 2008
انقر فوق زر البدء > **Control Panel** (**لوحة التحكم**) > **Hardware and Sound** (**الأجهزة والصوت**) > **Printers** (**الطابعات**).

2 افتح شاشة خصائص الطابعة.

❏ Windows 10/Windows 8.1/Windows 8/Windows 7/Windows Server 2016/Windows Server 2012 R2/ Windows Server 2012/ Windows Server 2008 R2
انقر بزر الماوس الأيمن فوق رمز الطابعة ثم انقر فوق **Printer properties** (**خصائص الطابعة**).

❏ Windows Vista
انقر بزر الماوس الأيمن فوق رمز الطابعة ثم حدد **Run as administrator** (**تشغيل كمسؤول**) > **Properties** (**خصائص**).

❏ Windows Server 2008
انقر بزر الماوس الأيمن فوق رمز الطابعة ثم انقر فوق **Properties (خصائص)**.

3 انقر فوق علامة التبويب **Ports (المنافذ)**، وحدد **Standard TCP/IP Port (منفذ TCP/IP قياسي)** ثم انقر فوق **Configure Port (تكوين المنفذ)**.

4 تحقق من تهيئة المنفذ.

❏ بالنسبة إلى RAW
تأكد من تحديد التنسيق **Raw** في **Protocol (البروتوكول)** ثم انقر فوق **OK (موافق)**.

❏ بالنسبة إلى LPR
تأكد من تحديد التنسيق **LPR** في **Protocol (البروتوكول)**. أدخل "PASSTHRU" في **Queue name (اسم قائمة الانتظار)** من **LPR Settings (إعدادات LPR)**. حدد **LPR Byte Counting Enabled (تمكين عد بايت LPR)** ثم انقر فوق **OK (موافق)**.

إتاحة الطابعة للمشاركة

عند استخدام الطابعة ضمن اتصال الخادم/العميل (إتاحة الطابعة للمشاركة باستخدام خادم Windows)، قم بإعداد إجراءات إتاحة الطابعة للمشاركة من خادم الطباعة.

1 حدد **Control Panel (لوحة التحكم)** > **View devices and printers (عرض الأجهزة والطابعات)** في خادم الطباعة.

2 انقر بزر الماوس الأيمن فوق رمز الطابعة (قائمة انتظار الطباعة) التي تريد إتاحتها للمشاركة ثم حدد **Printer Properties (خصائص الطابعة)** > علامة التبويب **Sharing (مشاركة)**.

3 حدد **Share this printer (مشاركة هذه الطابعة)** ثم ادخل **Share name (مشاركة الاسم)**.

في نظام التشغيل Windows Server 2012، انقر فوق **Change Sharing Options (تغيير خيارات المشاركة)** ثم هيئ الإعدادات.

تثبيت برامج تشغيل إضافية

إذا كانت إصدارات Windows مختلفة لخادم أو عميل، فمن المستحسن تثبيت برامج تشغيل إضافية لخادم الطباعة.

1 حدد **Control Panel (لوحة التحكم)** > **View devices and printers (عرض الأجهزة والطابعات)** في خادم الطباعة.

2 انقر بزر الماوس الأيمن فوق رمز الطابعة التي تريد إتاحتها للمشاركة مع الأجهزة العميلة ثم انقر فوق **Printer Properties (خصائص الطابعة)** > علامة التبويب **Sharing (مشاركة)**.

3 انقر فوق **Additional Drivers (برامج تشغيل إضافية)**.

في نظام التشغيل Windows Server 2012، انقر فوق **Change Sharing Options (تغيير خيارات المشاركة)** ثم هيئ الإعدادات.

4 حدد إصدارات نظام التشغيل Windows للأجهزة العميلة ثم انقر فوق **OK (موافق)**.

5 حدد ملف معلومات برنامج تشغيل الطابعة (*.inf) ثم ثبّت برنامج التشغيل.

معلومات ذات صلة
◆ "استخدام طابعة مشتركة" في الصفحة 26

استخدام طابعة مشتركة

يجب على المسؤول إبلاغ العملاء باسم الكمبيوتر المخصص لخادم الطباعة وكيفية إضافته إلى أجهزة الكمبيوتر التابعة لهم. إذا لم تتم تهيئة برنامج أو برامج تشغيل إضافية حتى الآن، فأخبر العملاء بكيفية استخدام **Devices and Printers (الأجهزة والطابعات)** لإضافة الطابعة المشتركة.

إذا تمت تهيئة برنامج أو برامج تشغيل إضافية بالفعل في خادم الطباعة، فاتبع هذه الخطوات:

1. حدد الاسم المعيَّن لخادم الطباعة في **Windows Explorer (مستكشف Windows)**.
2. انقر نقرًا مزدوجًا فوق الطابعة التي تريد استخدامها.

معلومات ذات صلة

"إتاحة الطابعة للمشاركة" في الصفحة 25
"تثبيت برامج تشغيل إضافية" في الصفحة 25

إعدادات برنامج تشغيل الطابعة لاتصال النظير إلى النظير

لاتصال النظير إلى النظير (الطباعة المباشرة)، يجب تثبيت برنامج تشغيل الطابعة في كل كمبيوتر عميل.

معلومات ذات صلة

"إعداد برنامج تشغيل الطابعة" في الصفحة 26

إعداد برنامج تشغيل الطابعة

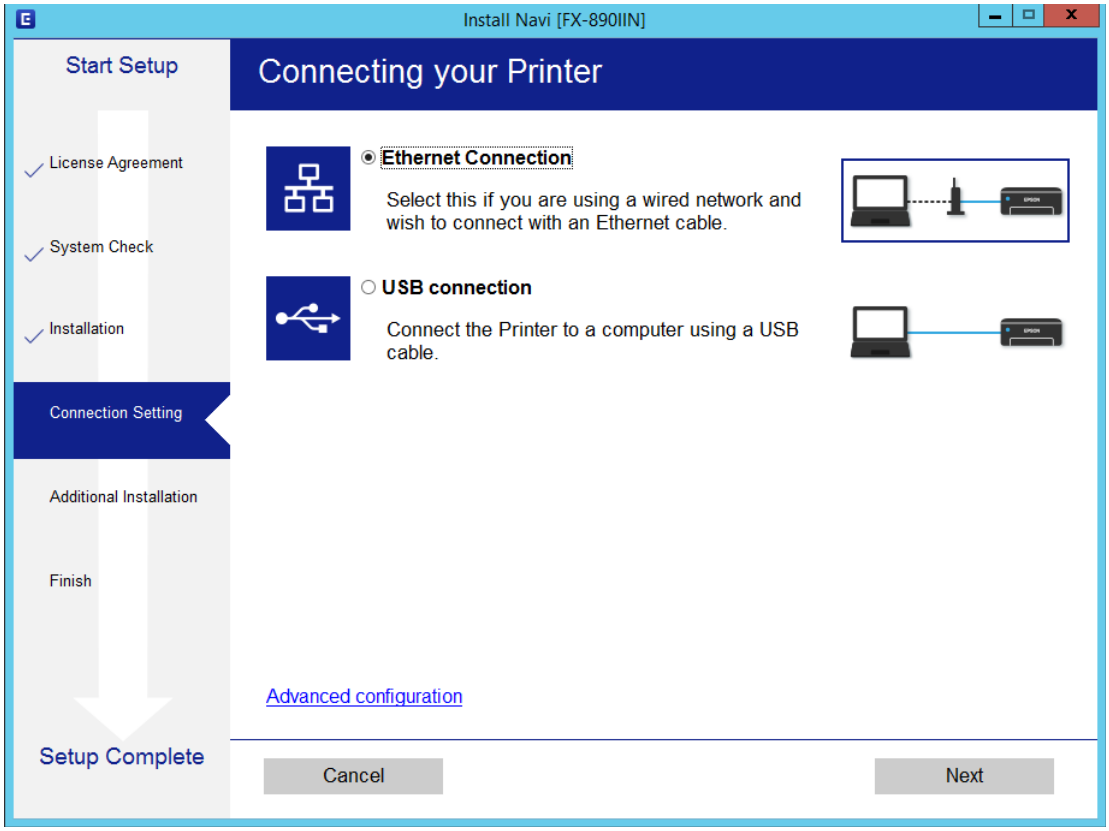
في المؤسسات الصغيرة، نوصي بتثبيت برنامج تشغيل الطابعة في كل كمبيوتر عميل.

ملاحظة:
عند استخدام الطابعة من عدة أجهزة عميلة، عن طريق استخدام *EpsonNet SetupManager* وتسليم برنامج التشغيل كحزمة، يمكن تقليل مدة تشغيل عملية التثبيت بشكل كبير.

1. شغِّل المثبِّت.

إعدادات الوظيفة

2 حدد طريقة اتصال الطابعة ثم انقر فوق **Next** (**التالي**).



ملاحظة:
إذا تم عرض ***Select Software Installation*** (**حدد تثبيت البرنامج**) فحدد ***Change or re-set the connection method*** (**تغيير طريقة الاتصال أو إعادة تعيينها**) ثم انقر فوق ***Next*** (**التالي**).

3 اتبع التعليمات المعروضة على الشاشة.

معلومات ذات صلة

"EpsonNet SetupManager" في الصفحة 59

إعدادات الأمان

يشرح هذا الفصل إعدادات الأمان.

إعدادات الأمان ومنع المخاطر

عند توصيل جهاز بشبكة، يمكنك الوصول إليه من مكان بعيد. إضافة إلى ذلك، يمكن للعديد من الأشخاص إتاحة الجهاز للمشاركة، مما يفيد في تحسين الكفاءة التشغيلية والراحة. ومع ذلك، تزداد المخاطر مثل الوصول غير القانوني، والاستخدام غير القانوني، والعبث بالبيانات.

لتجنب هذه المخاطر، تشتمل طابعات Epson على مجموعة متنوعة من تقنيات الأمان. عيّن الجهاز حسب الضرورة ووفقًا للظروف البيئية التي تم إنشاؤها باستخدام معلومات بيئة العميل.

اسم الميزة	نوع الميزة	الإعدادات المطلوب تعيينها	المخاطر المطلوب منعها
إعداد كلمة مرور المسؤول	يقفل إعدادات النظام، مثل إعداد اتصال الشبكة أو USB.	يعيّن أحد المسؤولين كلمة مرور للجهاز. تتوفر التهيئة أو التحديث في أي مكان من Web Config و Epson Device Admin.	منع قراءة المعلومات المخزنة في الجهاز، مثل المعرِّف وكلمة المرور وإعدادات الشبكة وجهات الاتصال، وتغييرها بشكل غير قانوني. يتم أيضًا تضييق نطاق مجموعة كبيرة من المخاطر الأمنية، مثل تسرب المعلومات المتعلقة ببيئة الشبكة أو سياسة الأمان.
بروتوكول الخدمة والتحكم بها	يتحكم في البروتوكولات والخدمات المستخدمة للاتصال بين الأجهزة وأجهزة الكمبيوتر، ويمكّن ميزات، مثل الطباعة، ويعطلها.	بروتوكول أو خدمة يتم تطبيقها بشكل منفصل على الميزات المسموح بها أو المحظورة.	الحد من المخاطر الأمنية التي قد تحدث بسبب الاستخدام غير المصرح به من خلال منع المستخدمين من استخدام الوظائف غير الضرورية.
اتصالات SSL/TLS	يتم تشفير مسار اتصال كمبيوتر وطابعة باستخدام اتصال SSL/TLS. تتم حماية محتوى الاتصال عن طريق إعدادات الطابعة ومطبوعات بروتوكول IPPS عبر متصفح.	احصل على شهادة موقعة من مرجع مصدق (CA) ثم استوردها إلى الطابعة.	يؤدي مسح معرِّف الجهاز بالشهادة الموقعة من مرجع مصدق إلى منع انتحال الشخصية والوصول غير المصرح به. إضافة إلى ذلك، تتم حماية محتويات اتصال SSL/TLS، ومنع تسريب بيانات الطباعة ومعلومات الإعداد.
تصفية IPsec/IP	يمكنك تعيينها للسماح بفصل البيانات المستلمة من عميل معين أو التي تُعد من نوع خاص وعزلها. وبما أن IPsec تحمي البيانات عن طريق وحدة حزمة IP (التشفير والمصادقة)، يمكنك توصيل بروتوكول المسح الضوئي والطباعة غير الآمن بسلامة.	أنشئ سياسة أساسية وأخرى فردية لتعيين العميل ونوع البيانات التي يمكن أن تصل إلى الجهاز.	امنع الوصول غير المصرح به والعبث ببيانات اتصال الجهاز واعتراضها.
SNMPv3	تمت إضافة ميزات، مثل مراقبة الأجهزة المتصلة في الشبكة، وسلامة البيانات بروتوكول SNMP للتحكم والتشفير ومصادقة المستخدم، وما إلى ذلك.	مكّن SNMPv3 ثم عيّن طريقة المصادقة والتشفير.	تأكد من إعدادات التغيير عبر الشبكة والسرية في مراقبة الحالة.

معلومات ذات صلة

- "تهيئة كلمة مرور المسؤول" في الصفحة 29
- "التحكم في البروتوكولات والخدمات" في الصفحة 30
- "اتصال SSL/TLS بالطابعة" في الصفحة 33

إعدادات ميزة الأمان

عند إعداد تصفية IPsec/IP، يوصى بالوصول إلى Web Config باستخدام SSL/TLS لتوصيل معلومات الإعدادات للحد من مخاطر الأمان، مثل العبث بالبيانات أو اعتراضها.

تهيئة كلمة مرور المسؤول

عند تعيين كلمة مرور المسؤول، لن يتمكن أي مستخدمين آخرين غير المسؤولين من تغيير إعدادات مسؤول النظام. يمكنك تعيين كلمة مرور المسؤول وتغييرها باستخدام Web Config.

معلومات ذات صلة

"تهيئة كلمة مرور المسؤول باستخدام Web Config" في الصفحة 29

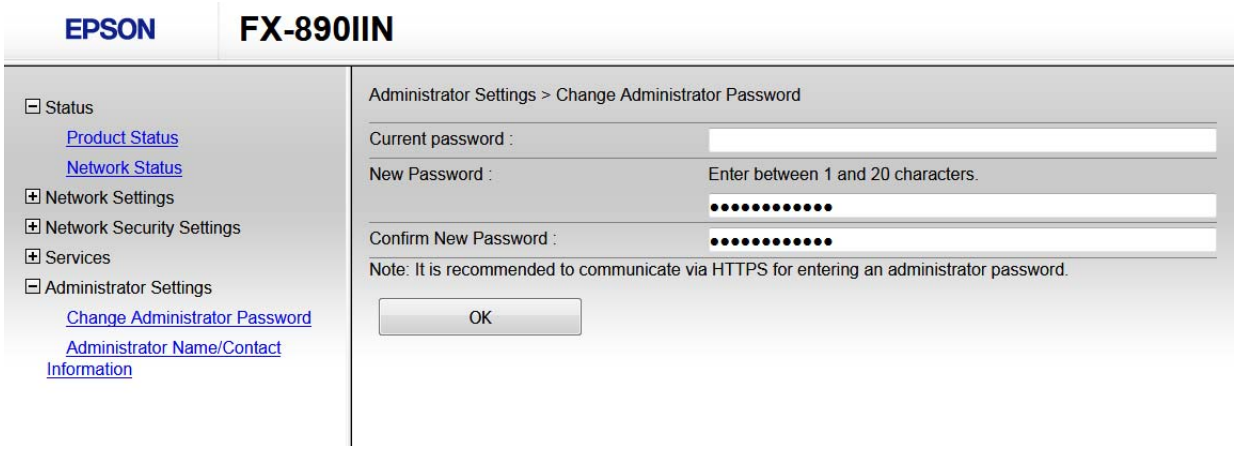
تهيئة كلمة مرور المسؤول باستخدام Web Config

يمكنك تعيين كلمة مرور المسؤول باستخدام Web Config.

1 ادخل إلى Web Config وحدد **Administrator Settings** (**إعدادات المسؤول**) > **Change Administrator Password** (**تغيير كلمة مرور المسؤول**).

2 أدخل كلمة مرور في **New Password** (**كلمة مرور جديدة**) و **Confirm New Password** (**تأكيد كلمة المرور الجديدة**).

إذا كنت تريد تغيير كلمة المرور إلى أخرى جديدة، فأدخل كلمة مرور حالية.



3 انقر فوق **OK** (**موافق**).

ملاحظة:

- لتعيين عناصر القائمة المقفلة أو تغييرها، انقر فوق ***Administrator Login*** (**تسجيل دخول المسؤول**) ثم أدخل كلمة مرور المسؤول.
- لحذف كلمة مرور المسؤول، انقر فوق ***Administrator Settings*** (**إعدادات المسؤول**) > ***Delete Administrator Authentication Information*** (**حذف معلومات مصادقة المسؤول**) ثم أدخل كلمة مرور المسؤول.

معلومات ذات صلة

"الوصول إلى Web Config" في الصفحة 20

التحكم في البروتوكولات والخدمات

يمكنك الطباعة باستخدام العديد من المسارات والبروتوكولات. يمكنك تقليل المخاطر الأمنية غير المقصودة من خلال تقييد الطباعة من مسارات محددة أو عن طريق التحكم في الوظائف المتاحة.

التحكم في البروتوكولات

هيئ إعدادات البروتوكول.

1. ادخل Web Config وحدد **Services** (الخدمات) > **Protocol** (البروتوكول).
2. هيئ كل عنصر.
3. انقر فوق **Next** (التالي).
4. انقر فوق **OK** (موافق).

يتم تطبيق الإعدادات على الطابعة.

معلومات ذات صلة

"الوصول إلى Web Config" في الصفحة 20
"البروتوكولات القابلة للتمكين أو التعطيل" في الصفحة 30
"عناصر إعداد البروتوكول" في الصفحة 31

البروتوكولات القابلة للتمكين أو التعطيل

البروتوكول	الوصف
Bonjour Settings (إعدادات Bonjour)	يمكنك تحديد مدى إمكانية استخدام Bonjour. يُستخدم Bonjour للبحث عن أجهزة والطباعة (AirPrint)، وما إلى ذلك.
SLP Settings (إعدادات SLP)	يمكنك تمكين وظيفة SLP أو تعطيلها. تُستخدم وظيفة SLP لبحث الشبكة في EpsonNet Config.
LLTD Settings (إعدادات LLTD)	يمكنك تمكين وظيفة LLTD أو تعطيلها. عند تمكينها، يتم عرضها في خريطة شبكة Windows.
LLMNR Settings (إعدادات LLMNR)	يمكنك تمكين وظيفة LLMNR أو تعطيلها. عند تمكينها، يمكنك استخدام تحليل الاسم بدون NetBIOS حتى لو تعذر عليك استخدام DNS.
LPR Settings (إعدادات LPR)	يمكنك تحديد ما إذا كنت تريد السماح بالطباعة عبر LPR أم لا. عند تمكينها، يمكنك الطباعة من منفذ LPR.
RAW(Port9100) Settings (إعدادات RAW (المنفذ 9100))	يمكنك تحديد ما إذا كنت تريد السماح بالطباعة من منفذ RAW (المنفذ 9100) أم لا. عند تمكينها، يمكنك الطباعة من منفذ RAW (المنفذ 9100).
RAW(Custom Port) Settings (إعدادات RAW (المنفذ المخصص))	يمكنك تحديد ما إذا كنت تريد السماح بالطباعة من منفذ RAW (المنفذ المخصص) أم لا. عند تمكينها، يمكنك الطباعة من منفذ RAW (المنفذ المخصص).
IPP Settings (إعدادات IPP)	يمكنك تحديد ما إذا كنت تريد السماح بالطباعة من IPP أم لا. عند تمكينها، يمكنك الطباعة عبر الإنترنت (بما في ذلك AirPrint).
FTP Settings (إعدادات FTP)	يمكنك تحديد ما إذا كنت تريد السماح بالطباعة عبر FTP أم لا. عند تمكينها، يمكنك الطباعة عبر خادم FTP.

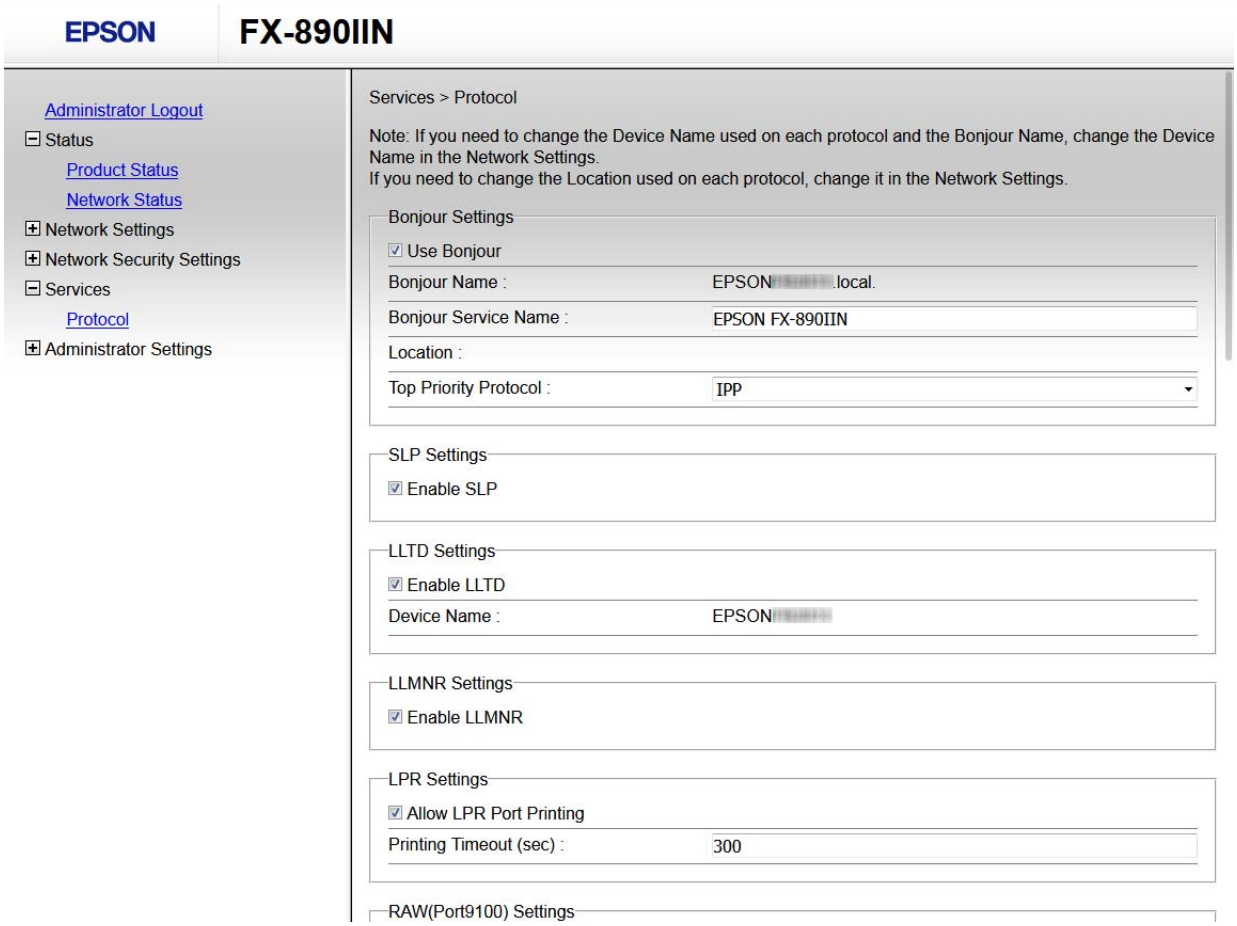
إعدادات الأمان

البروتوكول	الوصف
SNMPv1/v2c Settings (إعدادات SNMPv1/v2c)	يمكنك تحديد ما إذا كنت تريد تمكين SNMPv1/v2c أم لا. ويُستخدم هذا البروتوكول لإعداد الأجهزة والمراقبة وما إلى ذلك.
SNMPv3 Settings (إعدادات SNMPv3)	يمكنك تحديد ما إذا كنت تريد تمكين SNMPv3 أم لا. يُستخدم هذا البروتوكول لإعداد الأجهزة المشفرة والمراقبة، وما إلى ذلك.

معلومات ذات صلة

"التحكم في البروتوكولات" في الصفحة 30
"عناصر إعداد البروتوكول" في الصفحة 31

عناصر إعداد البروتوكول



العناصر	تعيين القيمة والوصف
Bonjour Settings (إعدادات Bonjour)	
Use Bonjour (استخدام Bonjour)	حدد هذا العنصر للبحث عن أجهزة أو استخدامها عبر Bonjour. ولا يمكنك استخدام AirPrint إذا تم مسح هذا العنصر.
Bonjour Name (اسم Bonjour)	يعرض اسم Bonjour.
Bonjour Service Name (اسم خدمة Bonjour)	يعرض اسم خدمة Bonjour.
Location (الموقع)	يعرض اسم موقع Bonjour.

إعدادات الأمان

العناصر	تعيين القيمة والوصف
Top Priority Protocol (بروتوكول الاولوية القصوى)	حدد بروتوكول الأولوية القصوى للطباعة عبر Bonjour.
SLP Settings (إعدادات SLP)	
Enable SLP (تمكين SLP)	حدد هذا العنصر لتمكين وظيفة SLP. تُستخدم وظيفة SLP لبحث الشبكة في EpsonNet Config.
LLTD Settings (إعدادات LLTD)	
Enable LLTD (تمكين LLTD)	حدد هذا العنصر لتمكين LLTD. يتم عرض الطابعة في خريطة شبكة Windows.
Device Name (اسم الخدمة)	يعرض اسم جهاز LLTD.
LLMNR Settings (إعدادات LLMNR)	
Enable LLMNR (تمكين LLMNR)	حدد هذا العنصر لتمكين LLMNR. يمكنك استخدام تحليل الاسم بدون NetBIOS حتى لو تعذر عليك استخدام DNS.
LPR Settings (إعدادات LPR)	
Allow LPR Port Printing (السماح بالطباعة عبر منفذ LPR)	حدد هذا العنصر للسماح بالطباعة من منفذ LPR.
Printing Timeout (sec) (مهلة الطباعة (ثوانٍ))	أدخل قيمة مهلة الطباعة عبر LPR بين 0 و3,600 ثانية. وإذا لم ترغب في استخدام مهلة، فأدخل 0.
RAW(Port9100) Settings (إعدادات RAW (المنفذ 9100))	
Allow RAW(Port9100) Printing [السماح بالطباعة عبر RAW (المنفذ 9100)]	حدد هذا العنصر للسماح بالطباعة عبر منفذ RAW (المنفذ 9100).
Printing Timeout (sec) (مهلة الطباعة (ثوانٍ))	أدخل قيمة مهلة الطباعة عبر RAW (المنفذ 9100) بين 0 و3,600 ثانية. وإذا لم ترغب في استخدام مهلة، فأدخل 0.
RAW(Custom Port) Settings (إعدادات RAW (المنفذ المخصص))	
Allow RAW(Custom Port) Printing (السماح بالطباعة عبر RAW (المنفذ المخصص))	حدد هذا العنصر للسماح بالطباعة عبر منفذ RAW (المنفذ المخصص).
Port Number (رقم المنفذ)	أدخل رقم منفذ الطباعة عبر RAW (المنفذ المخصص) بين 1024 و65535 باستثناء 9100 و1865 و2968.
Printing Timeout (sec) (مهلة الطباعة (ثوانٍ))	أدخل قيمة مهلة الطباعة عبر RAW (المنفذ المخصص) بين 0 و3,600 ثانية. وإذا لم ترغب في استخدام مهلة، فأدخل 0.
IPP Settings (إعدادات IPP)	
Enable IPP (تمكين IPP)	حدد هذا العنصر لتمكين اتصال IPP. يتم عرض الطابعات التي تدعم IPP فقط. ولا يمكنك استخدام AirPrint إذا تم تعطيل هذا العنصر.
Allow Non-secure Communication (السماح باتصال غير آمن)	حدد هذا العنصر للسماح للطابعة بالاتصال بدون أي تدابير أمنية (IPP).
Communication Timeout (sec) (مهلة الاتصال (ثوانٍ))	أدخل قيمة مهلة الطباعة عبر IPP بين 0 و3,600 ثانية.
URL(Network) (الشبكة))	يعرض عناوين URL المستخدمة عبر IPP (http وhttps) عندما تكون الطابعة متصلة بشبكة LAN سلكية. وعنوان URL هو قيمة مجمعة تشمل عنوان IP للطابعة ورقم المنفذ واسم طابعة IPP.
Printer Name (اسم الطابعة)	يعرض اسم طابعة IPP.
Location (الموقع)	يعرض موقع IPP.
FTP Settings (إعدادات FTP)	

إعدادات الأمان

العناصر	تعيين القيمة والوصف
Enable FTP Server (تمكين خادم FTP)	حدد هذا العنصر لتمكين الطباعة عبر FTP. يتم عرض الطابعات التي تدعم الطباعة عبر FTP فقط.
Communication Timeout (sec) (مهلة الاتصال (ثوانٍ))	أدخل قيمة مهلة اتصال FTP بين 0 و3,600 ثانية. وإذا لم ترغب في استخدام مهلة، فأدخل 0.
SNMPv1/v2c Settings (إعدادات SNMPv1/v2c)	
Enable SNMPv1/v2c (تمكين SNMPv1/v2c)	حدد هذا العنصر لتمكين SNMPv1/v2c. يتم عرض الطابعات التي تدعم SNMPv3 فقط.
Access Authority (صلاحية الوصول)	حدد صلاحية الوصول عند تمكين SNMPv1/v2c. حدد **Read Only (للقراءة فقط)** أو **Read/Write (قراءة/كتابة)**.
Community Name (Read Only) (اسم المجتمع (للقراءة فقط))	أدخل من 0 إلى 32 حرفًا بتنسيق ASCII (من 0x20 إلى 0x7E).
Community Name (Read/Write) (اسم المجتمع (قراءة/كتابة))	أدخل من 0 إلى 32 حرفًا بتنسيق ASCII (من 0x20 إلى 0x7E).
SNMPv3 Settings (إعدادات SNMPv3)	
Enable SNMPv3 (تمكين SNMPv3)	يتم تمكين SNMPv3 عند تحديد خانة الاختيار.
User Name (اسم المستخدم)	أدخل من 1 إلى 32 حرفًا أحادي البايت.
Authentication Settings (إعدادات المصادقة)	
Algorithm (الخوارزمية)	حدد خوارزمية لمصادقة SNMPv3.
Password (كلمة المرور)	أدخل كلمة مرور لمصادقة SNMPv3. أدخل من 8 إلى 32 حرفًا بتنسيق ASCII (0x20–0x7E). إذا لم تحدد ذلك، فاتركه فارغًا.
Confirm Password (تأكيد كلمة المرور)	أدخل كلمة المرور التي هيئتها للتأكيد.
Encryption Settings (إعدادات التشفير)	
Algorithm (الخوارزمية)	حدد خوارزمية لتشفير SNMPv3.
Password (كلمة المرور)	أدخل كلمة المرور لتشفير SNMPv3. أدخل من 8 إلى 32 حرفًا بتنسيق ASCII (0x20–0x7E). إذا لم تحدد ذلك، فاتركه فارغًا.
Confirm Password (تأكيد كلمة المرور)	أدخل كلمة المرور التي هيئتها للتأكيد.
Context Name (اسم السياق)	أدخل ما يصل إلى 32 حرفًا أو أقل بتنسيق Unicode (UTF-8). إذا لم تحدد ذلك، فاتركه فارغًا. يختلف عدد الأحرف التي يمكن إدخالها حسب اللغة.

معلومات ذات صلة

- "التحكم في البروتوكولات" في الصفحة 30
- "البروتوكولات القابلة للتمكين أو التعطيل" في الصفحة 30

اتصال SSL/TLS بالطابعة

عند تعيين شهادة الخادم باستخدام اتصال SSL/TLS (طبقة المقابس الآمنة/أمان طبقة النقل) بالطابعة، يمكنك تشفير مسار الاتصال بين أجهزة الكمبيوتر. أجرِ ذلك إذا كنت تريد منع الوصول عن بُعد والوصول غير المصرح به.

حول الشهادة الرقمية

❏ شهادة موقعة من مرجع مصدق (CA)
يجب الحصول على شهادة موقعة من مرجع مصدق. ويمكنك ضمان إجراء اتصالات آمنة باستخدام شهادة موقعة من مرجع مصدق. ويمكنك استخدام شهادة موقعة من مرجع مصدق لكل ميزة أمان.

❏ شهادة المرجع المصدق (CA)
تشير شهادة المرجع المصدق إلى التحقق من صحة هوية أحد الخوادم بواسطة طرف ثالث. ويشكِّل هذا الإجراء ركنًا أساسيًا في نمط الأمان "الويب الموثوق فيه". ويجب الحصول على شهادة مرجع مصدق لمصادقة الخادم من المرجع المصدق الذي أصدر الشهادة.

❏ الشهادة الموقعة ذاتيًا
الشهادة الموقعة ذاتيًا هي شهادة تصدرها الطابعة وتوقعها ذاتيًا. ولا يُعتمد على هذه الشهادة ويتعذر عليها تجنب الاحتيال. إذا كنت تستخدم هذه الشهادة لإحدى شهادات SSL/TLS، فقد يظهر تنبيه أمان في المتصفح. يمكنك استخدام هذه الشهادة لاتصال SSL/TLS فقط.

معلومات ذات صلة

- "الحصول على شهادة موقعة من مرجع مصدق واستيرادها" في الصفحة 34
- "حذف شهادة موقعة من مرجع مصدق" في الصفحة 37
- "تحديث شهادة موقعة ذاتيًا" في الصفحة 38

الحصول على شهادة موقعة من مرجع مصدق واستيرادها

الحصول على شهادة موقعة من مرجع مصدق

للحصول على شهادة موقعة من مرجع مصدق، أنشئ طلب توقيع شهادة (CSR) وقدِّمه إلى المرجع المصدق. يمكنك إنشاء CSR باستخدام Web Config وكمبيوتر.

اتبع خطوات إنشاء CSR والحصول على شهادة موقعة من مرجع مصدق باستخدام Web Config. عند إنشاء CSR باستخدام Web Config، تكون الشهادة بتنسيق PEM/DER.

1. ادخل Web Config ثم حدد **Network Security Settings (إعدادات أمان الشبكة)**. حدد بعد ذلك **SSL/TLS** > **Certificate (الشهادة)**.
2. انقر فوق **Generate (إنشاء)** في إعداد **CSR**.
   يتم عندئذٍ فتح صفحة إنشاء CSR.
3. أدخل قيمة لكل عنصر.

> **ملاحظة:**
> يختلف طول المفتاح والاختصارات المتاحة حسب المرجع المصدق. أنشئ طلبًا باتباع قواعد كل مرجع مصدق.

4. انقر فوق **OK (موافق)**.
   تظهر عندئذٍ رسالة اكتمال الطلب.
5. حدد **Network Security Settings (إعدادات أمان الشبكة)**. حدد بعد ذلك **SSL/TLS** > **Certificate (الشهادة)**.

6 انقر فوق أحد أزرار تنزيل **CSR** حسب التنسيق المحدد بواسطة كل مرجع مصدق لتنزيل طلب CSR إلى كمبيوتر.

> **مهم:**
> لا تنشئ *CSR* مرة أخرى؛ وإلا، فقد لا تتمكن من استيراد شهادة موقعة ذاتيًا تم إصدارها.

7 أرسل CSR إلى مرجع مصدق واحصل على شهادة موقعة منه.

اتبع قواعد كل مرجع مصدق بشأن طريقة الإرسال والنموذج.

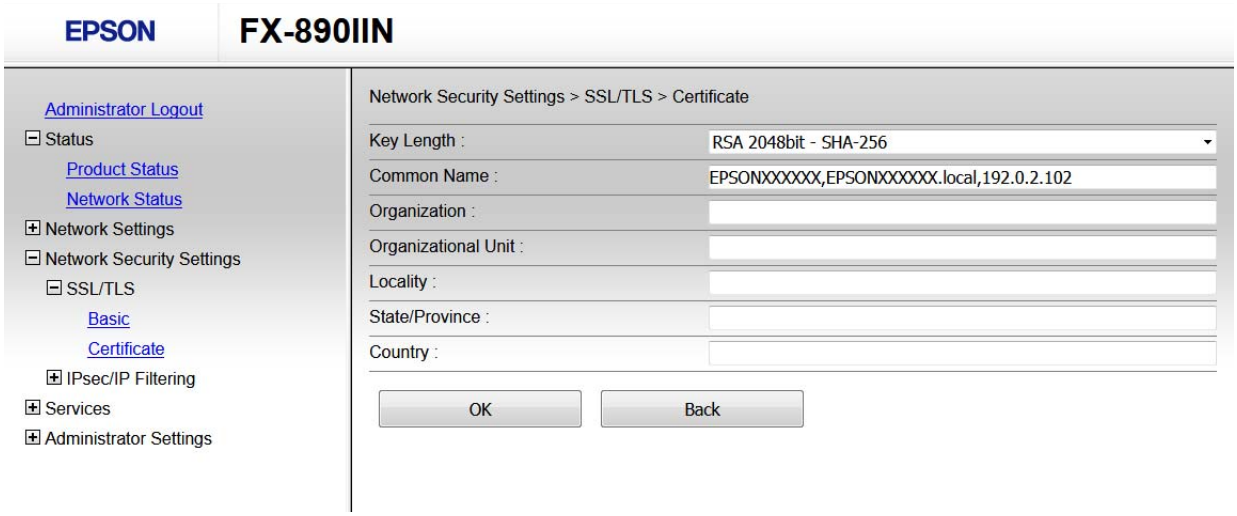
8 احفظ الشهادة الصادرة والموقعة من المرجع المصدق في كمبيوتر متصل بالطابعة.

يكتمل الحصول على شهادة موقعة من مرجع مصدق عندما تحفظ الشهادة في وجهة.

معلومات ذات صلة

- "الوصول إلى Web Config" في الصفحة 20
- "عناصر إعداد CSR" في الصفحة 35
- "استيراد شهادة موقعة من مرجع مصدق" في الصفحة 36

عناصر إعداد *CSR*



العناصر	الإعدادات والشرح
Key Length (طول المفتاح)	حدد طول مفتاح طلب CSR.
Common Name (الاسم الشائع)	يمكن إدخال من 1 إلى 128 حرفًا. إذا كان هذا عنوان IP، فلا بد أن يكون عنوان IP ثابتًا. مثال: عنوان URL للوصول إلى Web Config: https://10.152.12.225 الاسم الشائع: 10.152.12.225
Organization (المؤسسة)/ Organizational Unit (الوحدة المؤسسية)/ Locality (المركز)/ State/Province (المحافظة/الإقليم)	يمكنك إدخال من 0 إلى 64 حرفًا بتنسيق ASCII (0x20-0x7E). ويمكنك فصل الأسماء المميزة باستخدام فاصلات.
Country (البلد)	أدخل رمز البلد على هيئة عدد مكون من رقمين محددين باستخدام ISO-3166.

معلومات ذات صلة

- "الحصول على شهادة موقعة من مرجع مصدق" في الصفحة 34

استيراد شهادة موقعة من مرجع مصدق

مهم:
- ❏ تأكد من صحة تعيين تاريخ الطابعة ووقتها.
- ❏ إذا كنت تحصل على شهادة باستخدام طلب *CSR* تم إنشاؤه من *Web Config*، فبإمكانك استيراد شهادة واحدة في المرة الواحدة.

1. ادخل Web Config ثم حدد **Network Security Settings (إعدادات أمان الشبكة)**. حدد بعد ذلك **SSL/TLS** > **Certificate (الشهادة)**.
2. انقر فوق **Import (استيراد)**.

   يتم عندئذٍ فتح صفحة استيراد شهادة.
3. أدخل قيمة لكل عنصر.

   قد تختلف الإعدادات المطلوبة حسب مكان إنشاء CSR وتنسيق ملف الشهادة. أدخل قيماً للعناصر المطلوبة وفقًا لما يلي.

   - ❏ شهادة بتنسيق PEM/DER تم الحصول عليها من Web Config
     - **Private Key (مفتاح خاص)**: تجنب التهيئة؛ لأن الطابعة تحتوي على مفتاح خاص.
     - **Password (كلمة المرور)**: تجنب التهيئة.
     - **CA Certificate 1 (شهادة المرجع المصدق 1)**/**CA Certificate 2 (شهادة المرجع المصدق 2)**: اختياري
   - ❏ شهادة بتنسيق PEM/DER تم الحصول عليها من كمبيوتر
     - **Private Key (مفتاح خاص)**: يجب تعيينه.
     - **Password (كلمة المرور)**: تجنب التهيئة.
     - **CA Certificate 1 (شهادة المرجع المصدق 1)**/**CA Certificate 2 (شهادة المرجع المصدق 2)**: اختياري
   - ❏ شهادة بتنسيق PKCS#12 تم الحصول عليها من كمبيوتر
     - **Private Key (مفتاح خاص)**: تجنب التهيئة.
     - **Password (كلمة المرور)**: اختياري
     - **CA Certificate 1 (شهادة المرجع المصدق 1)**/**CA Certificate 2 (شهادة المرجع المصدق 2)**: تجنب التهيئة.
4. انقر فوق **OK (موافق)**.

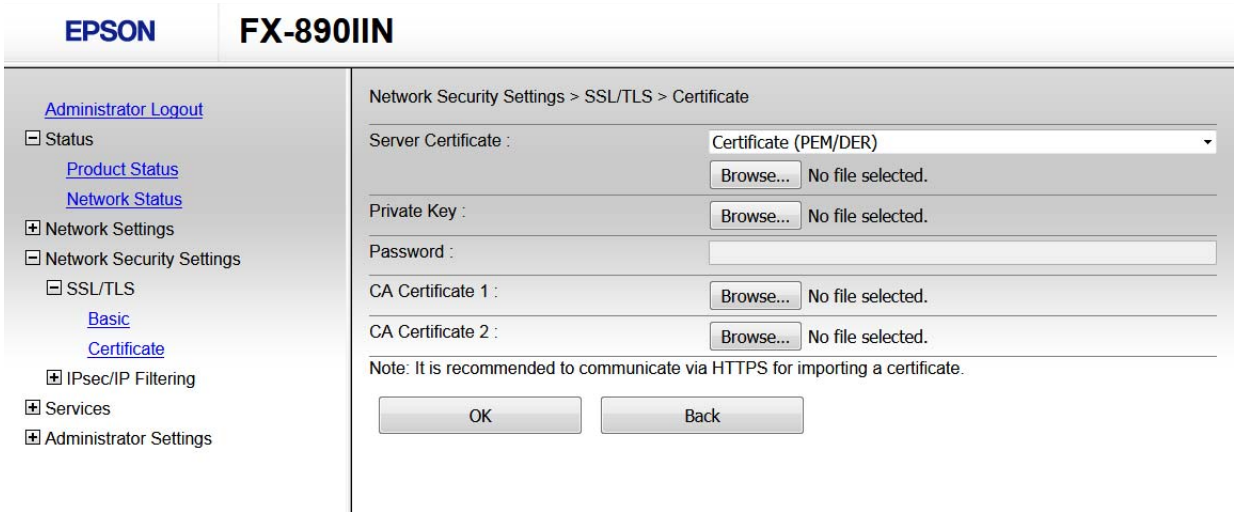
   تظهر عندئذٍ رسالة اكتمال الطلب.

ملاحظة:
انقر فوق ***Confirm* (تأكيد)** للتحقق من صحة معلومات الشهادة.

معلومات ذات صلة

- ← "الوصول إلى Web Config" في الصفحة 20
- ← "عناصر إعداد استيراد شهادة موقعة من مرجع مصدق" في الصفحة 37

عناصر إعداد استيراد شهادة موقعة من مرجع مصدق



العناصر	الإعدادات والشرح
Server Certificate (شهادة الخادم) أو Client Certificate (شهادة العميل)	حدد تنسيق شهادة.
Private Key (مفتاح خاص)	إذا كنت تحصل على شهادة بتنسيق PEM/DER باستخدام طلب CSR تم إنشاؤه من كمبيوتر، فحدد ملف مفتاح خاص يطابق الشهادة.
Password (كلمة المرور)	أدخل كلمة مرور لتشفير مفتاح خاص.
CA Certificate 1 (شهادة المرجع المصدق 1)	إذا كان تنسيق الشهادة هو **Certificate (PEM/DER)** (**شهادة (PEM/DER)**)، فاستورد شهادة من المرجع المصدق الذي يصدر شهادة خادم. وحدد ملفًا عند الضرورة.
CA Certificate 2 (شهادة المرجع المصدق 2)	إذا كان تنسيق الشهادة هو **Certificate (PEM/DER)** (**شهادة (PEM/DER)**)، فاستورد شهادة من المرجع المصدق الذي يصدر **CA Certificate 1** (**شهادة المرجع المصدق 1**). وحدد ملفًا عند الضرورة.

معلومات ذات صلة

"استيراد شهادة موقعة من مرجع مصدق" في الصفحة 36

حذف شهادة موقعة من مرجع مصدق

يمكنك حذف شهادة تم استيرادها عند انتهاء صلاحيتها أو عند عدم وجود ضرورة لاستخدام اتصال مشفر.

مهم:
إذا كنت تحصل على شهادة باستخدام طلب *CSR* تم إنشاؤه من *Web Config*، فلا يمكنك استيراد شهادة محذوفة مجدداً. وفي هذه الحالة، أنشئ طلب *CSR* واحصل على شهادة مرة أخرى.

1. ادخل Web Config ثم حدد **Network Security Settings** (**إعدادات أمان الشبكة**). حدد بعد ذلك **SSL/TLS** > **Certificate** (**الشهادة**).
2. انقر فوق **Delete** (**حذف**).
3. أكِّد رغبتك في حذف الشهادة في الرسالة المعروضة.

معلومات ذات صلة

"الوصول إلى Web Config" في الصفحة 20

تحديث شهادة موقعة ذاتيًا

إذا كانت الطابعة تدعم ميزة خادم HTTPS، يمكنك تحديث شهادة موقعة ذاتيًا. تظهر رسالة تحذير عند الوصول إلى Web Config باستخدام شهادة موقعة ذاتيًا.

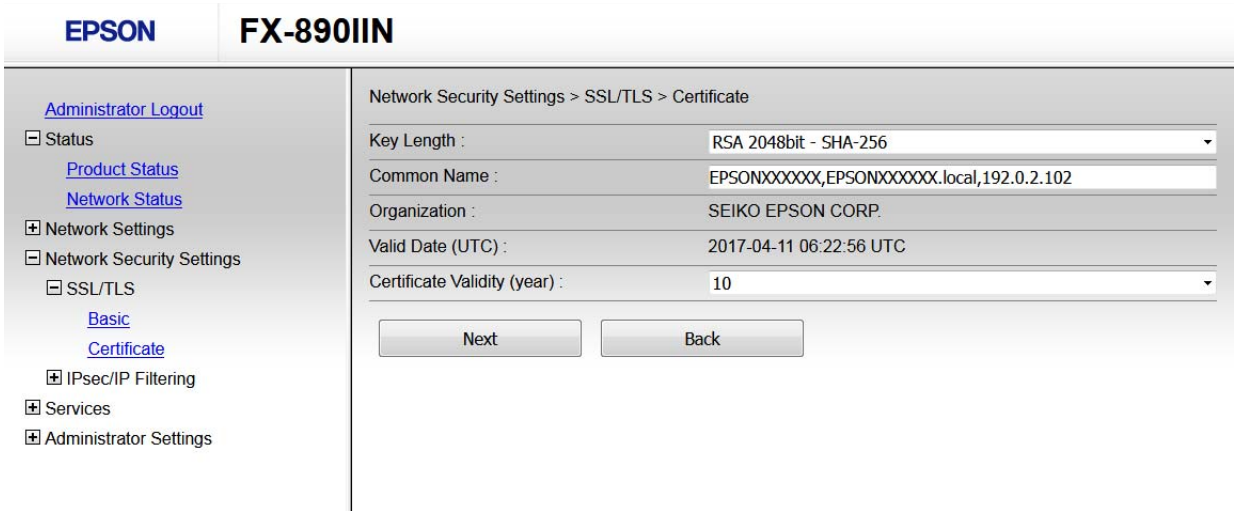
استخدم شهادة موقعة ذاتيًا مؤقتًا لحين الحصول على شهادة موقعة من مرجع مصدق واستيرادها.

1. ادخل Web Config وحدد **Network Security Settings** (**إعدادات أمان الشبكة**) > **SSL/TLS** > **Certificate** (**الشهادة**).
2. انقر فوق **Update** (**تحديث**).
3. أدخل **Common Name** (**الاسم الشائع**).

   أدخل عنوان IP أو معرفًا مثل اسم FQDN للطابعة. يمكن إدخال من 1 إلى 128 حرفًا.

> **ملاحظة:**
> يمكنك فصل الأسماء المميزة (*CN*) باستخدام فاصلات.

4. حدد فترة صلاحية للشهادة.



5. انقر فوق **Next** (**التالي**).

   تظهر عندئذٍ رسالة تأكيد.
6. انقر فوق **OK** (**موافق**).

   وبذلك يتم تحديث الطابعة.

> **ملاحظة:**
> انقر فوق *Confirm* (تأكيد) للتحقق من صحة معلومات الشهادة.

معلومات ذات صلة
"الوصول إلى Web Config" في الصفحة 20

الاتصال المشفر باستخدام تصفية IPsec/IP

حول تصفية IPsec/IP

إذا كانت الطابعة تدعم تصفية IPsec/IP، يمكنك تصفية بيانات حركة مرور الشبكة حسب عناوين IP والخدمات والمنفذ. ومن خلال تجميع عوامل التصفية، يمكنك تهيئة الطابعة لقبول أجهزة عميلة وبيانات محددة أو حظرها. إضافة إلى ذلك، يمكنك تحسين مستوى الأمان باستخدام IPsec.

لتصفية بيانات حركة مرور الشبكة، هيئ السياسة الافتراضية. وتسري السياسة الافتراضية على جميع المستخدمين أو المجموعات المتصلة بالطابعة. ولمزيد من التحكم الدقيق في مستخدمين أو مجموعات مستخدمين، هيئ سياسات المجموعة. وسياسة المجموعة عبارة عن قاعدة واحدة أو أكثر تسري على مستخدم واحد أو مجموعة من المستخدمين. وتتحكم الطابعة في حزم IP المطابقة للسياسات التي تمت تهيئتها. إذا كانت حزم IP مصدقًا عليها بترتيب إحدى سياسات المجموعة من 1 إلى 10، فسيتم استخدام السياسة الافتراضية.

ملاحظة:
يمكن استخدام *IPsec* في أجهزة الكمبيوتر التي تعمل بنظام التشغيل *Windows Vista* أو أحدث أو *Windows Server 2008* أو أحدث.

تهيئة السياسة الافتراضية

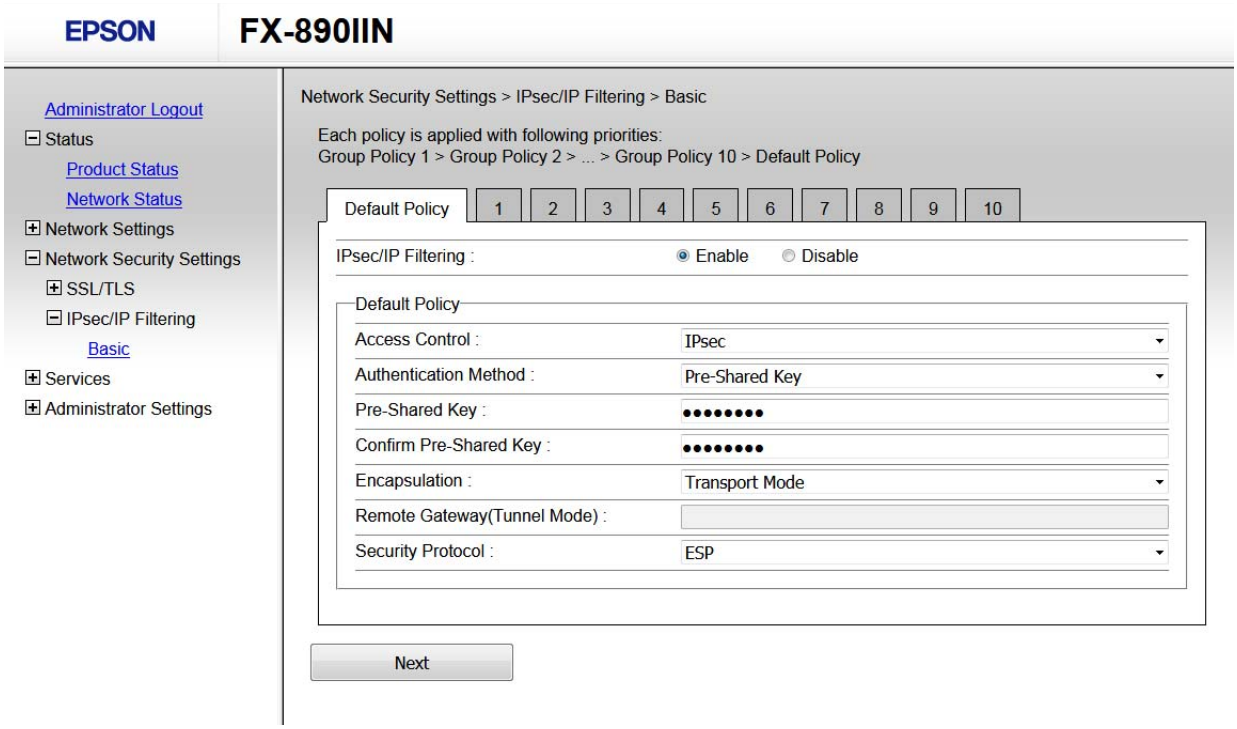
1. ادخل Web Config وحدد **Network Security Settings (إعدادات أمان الشبكة)** > **IPsec/IP Filtering (تصفية IPsec/IP)** > **Basic (أساسي)**.
2. أدخل قيمة لكل عنصر.
3. انقر فوق **Next (التالي)**.

   تظهر عندئذٍ رسالة تأكيد.
4. انقر فوق **OK (موافق)**.

   وبذلك يتم تحديث الطابعة.

معلومات ذات صلة
"الوصول إلى Web Config" في الصفحة 20
"عناصر إعداد السياسة الافتراضية" في الصفحة 40

عناصر إعداد السياسة الافتراضية



العناصر	الإعدادات والشرح	
IPsec/IP Filtering (تصفية IPsec/IP)	يمكنك تمكين ميزة تصفية IPsec/IP أو تعطيلها.	
Access Control (التحكم في الوصول)	هيئ طريقة تحكم لحركة مرور حزم IP.	
	Permit Access (السماح بالوصول)	حدد هذا الإعداد للسماح بمرور حزم IP التي تمت تهيئتها.
	Refuse Access (رفض الوصول)	حدد هذا الإعداد لرفض مرور حزم IP التي تمت تهيئتها.
	IPsec	حدد هذا الإعداد للسماح بمرور حزم IPsec التي تمت تهيئتها.
Authentication Method (طريقة المصادقة)	يعرض طرق المصادقة المتوافقة.	
Pre-Shared Key (المفتاح المتاح للمشاركة مسبقًا)	أدخل مفتاحًا متاحًا للمشاركة مسبقًا من 1 إلى 127 حرفًا.	
Confirm Pre-Shared Key (تأكيد المفتاح المتاح للمشاركة مسبقًا)	أدخل المفتاح الذي تمت تهيئته للتأكيد.	
Encapsulation (تغليف)	إذا حددت **IPsec** في **Access Control (التحكم في الوصول)**، يجب تهيئة وضع تغليف.	
	Transport Mode (وضع النقل)	حدد هذا الإعداد إذا كنت تستخدم الطابعة في شبكة LAN نفسها فقط. ويتم تشفير حزم IP من الطبقة 4 فما فوق.
	Tunnel Mode (وضع النفق)	حدد هذا الإعداد إذا كنت تستخدم طابعة متصلة بشبكة وتدعم استخدام الإنترنت مثل IPsec-VPN. ويتم تشفير عنوان حزم IP وبياناتها.
Remote Gateway(Tunnel Mode) (البوابة البعيدة (وضع النفق))	إذا حددت **Tunnel Mode (وضع النفق)** في **Encapsulation (تغليف)**، فأدخل عنوان بوابة من 1 إلى 39 حرفًا.	

إعدادات الأمان

العناصر	الإعدادات والشرح	
Security Protocol (بروتوكول الأمان)	حدد خيارًا إذا حددت **IPsec** في **Access Control** (**التحكم في الوصول**).	
	ESP	حدد هذا الخيار لضمان سلامة المصادقة والبيانات وتشفير البيانات.
	AH	حدد هذا الخيار لضمان سلامة المصادقة والبيانات. ويمكنك استخدام IPsec حتى في حالة حظر تشفير البيانات.

معلومات ذات صلة

"تهيئة السياسة الافتراضية" في الصفحة 39

تهيئة السياسة الافتراضية

1. ادخل Web Config وحدد **Network Security Settings** (**إعدادات أمان الشبكة**) > **IPsec/IP Filtering** (**تصفية IPsec/IP**) > **Basic** (**أساسي**).
2. انقر فوق علامة التبويب المرقمة التي تريد تهيئتها.
3. أدخل قيمة لكل عنصر.
4. انقر فوق **Next** (**التالي**).

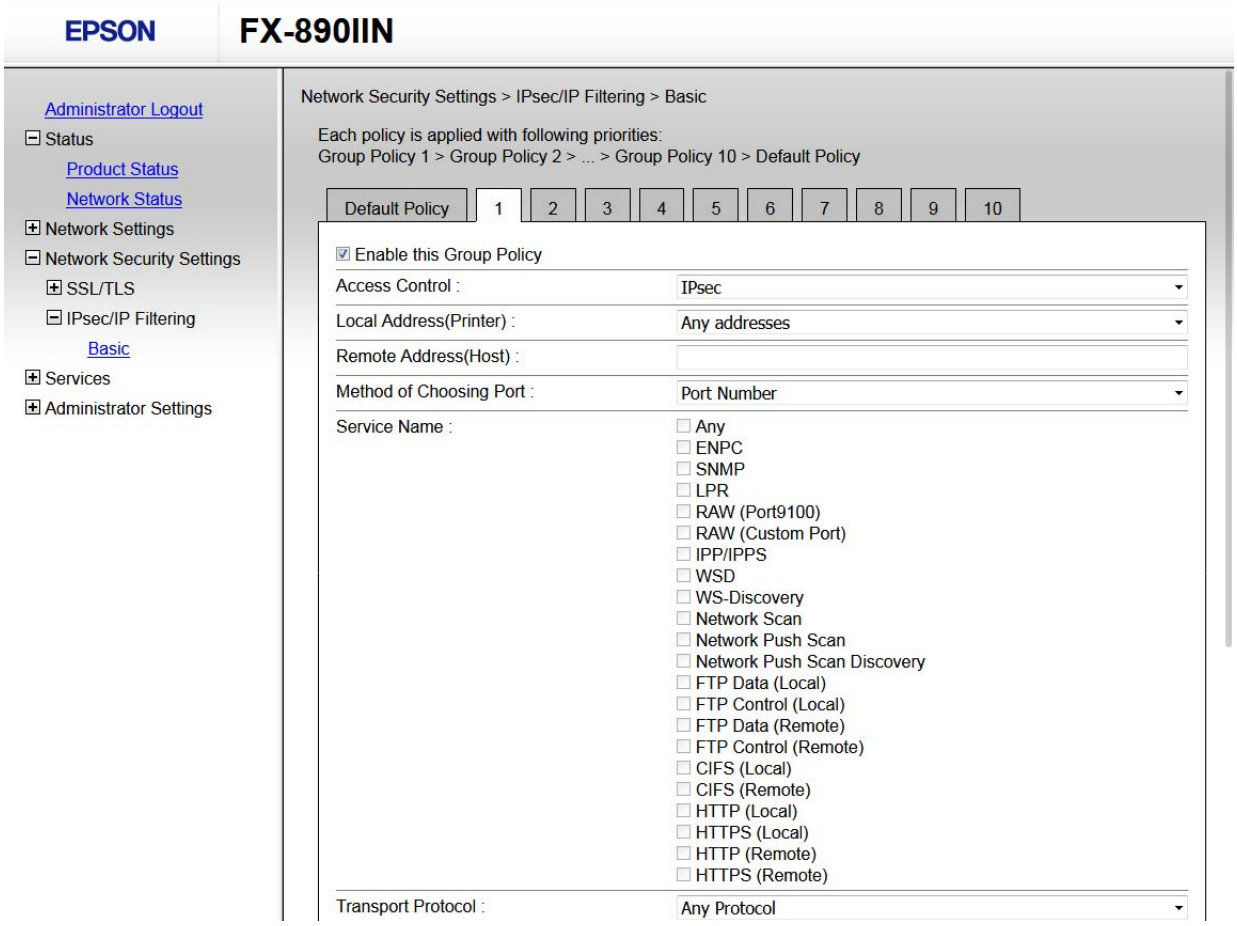
   تظهر عندئذٍ رسالة تأكيد.
5. انقر فوق **OK** (**موافق**).

   وبذلك يتم تحديث الطابعة.

معلومات ذات صلة

"الوصول إلى Web Config" في الصفحة 20
"عناصر إعداد سياسة المجموعة" في الصفحة 42

عناصر إعداد سياسة المجموعة



العناصر	الإعدادات والشرح	
Enable this Group Policy (تمكين سياسة المجموعة هذه)	يمكنك تمكين سياسة مجموعة أو تعطيلها.	
Access Control (التحكم في الوصول)	هيئ طريقة تحكم لحركة مرور حزم IP.	
	Permit Access (السماح بالوصول)	حدد هذا الإعداد للسماح بمرور حزم IP التي تمت تهيئتها.
	Refuse Access (رفض الوصول)	حدد هذا الإعداد لرفض مرور حزم IP التي تمت تهيئتها.
	IPsec	حدد هذا الإعداد للسماح بمرور حزم IPsec التي تمت تهيئتها.
Local Address(Printer) (العنوان المحلي (الطابعة))	حدد عنوان IPv4 أو عنوان IPv6 المطابق لبيئة شبكتك. إذا تم تعيين عنوان IP تلقائيًا، يمكنك تحديد **Use auto-obtained IPv4 address (استخدام عنوان IPv4 الذي تم الحصول عليه تلقائيًا)**.	
Remote Address(Host) (العنوان البعيد (المضيف))	أدخل عنوان IP لأحد الأجهزة للتحكم في الوصول. يجب أن يتراوح طول عنوان IP بين 0 و43 حرفًا. إذا لم تدخل عنوان IP، فسيتم التحكم في جميع العناوين. ملاحظة: إذا تم تعيين عنوان IP تلقائيًا (على سبيل المثال، التعيين عبر DHCP)، فقد يصبح الاتصال غير متوفر. هيئ عنوان IP ثابتًا.	
Method of Choosing Port (طريقة اختيار المنفذ)	حدد طريقةً لتعيين المنافذ.	

إعدادات الأمان

العناصر	الإعدادات والشرح	
Service Name (اسم الخدمة)	حدد خيارًا إذا حددت **Service Name (اسم الخدمة)** في **Method of Choosing Port (طريقة اختيار المنفذ)**.	
Transport Protocol (بروتوكول النقل)	إذا حددت **Port Number (رقم المنفذ)** في **Method of Choosing Port (طريقة اختيار المنفذ)**، يجب تهيئة وضع تغليف.	
	Any Protocol (أي بروتوكول)	حدد هذا الإعداد للتحكم في جميع أنواع البروتوكولات.
	TCP	حدد هذا الإعداد للتحكم في بيانات البث الأحادي.
	UDP	حدد هذا الإعداد للتحكم في بيانات البث واسع النطاق والبث المتعدد.
	ICMPv4	حدد هذا الإعداد للتحكم في أمر ping.
Local Port (المنفذ المحلي)	إذا حددت **Port Number (رقم المنفذ)** في **Method of Choosing Port (طريقة اختيار المنفذ)**، وإذا حددت **TCP** أو **UDP** في **Transport Protocol (بروتوكول النقل)**، فأدخل أرقام المنافذ للتحكم في استلام حزم البيانات، مع الفصل بينها باستخدام فاصلات. يمكنك إدخال 10 أرقام منافذ كحدٍ أقصى. مثال: 20,80,119,5220 وإذا لم تدخل رقم منفذ، فسيتم التحكم في جميع المنافذ.	
Remote Port (المنفذ البعيد)	إذا حددت **Port Number (رقم المنفذ)** في **Method of Choosing Port (طريقة اختيار المنفذ)**، وإذا حددت **TCP** أو **UDP** في **Transport Protocol (بروتوكول النقل)**، فأدخل أرقام المنافذ للتحكم في إرسال حزم البيانات، مع الفصل بينها باستخدام فاصلات. يمكنك إدخال 10 أرقام منافذ كحدٍ أقصى. مثال: 25,80,143,5220 وإذا لم تدخل رقم منفذ، فسيتم التحكم في جميع المنافذ.	
Authentication Method (طريقة المصادقة)	حدد خيارًا إذا حددت **IPsec** في **Access Control (التحكم في الوصول)**.	
Pre-Shared Key (المفتاح المتاح للمشاركة مسبقًا)	أدخل مفتاحًا متاحًا للمشاركة مسبقًا من 1 إلى 127 حرفًا.	
Confirm Pre-Shared Key (تأكيد المفتاح المتاح للمشاركة مسبقًا)	أدخل المفتاح الذي تمت تهيئته للتأكيد.	
Encapsulation (تغليف)	إذا حددت **IPsec** في **Access Control (التحكم في الوصول)**، يجب تهيئة وضع تغليف.	
	Transport Mode (وضع النقل)	حدد هذا الإعداد إذا كنت تستخدم الطابعة في شبكة LAN نفسها فقط. ويتم تشفير حزم IP من الطبقة 4 فما فوق.
	Tunnel Mode (وضع النفق)	حدد هذا الإعداد إذا كنت تستخدم طابعة متصلة بشبكة وتدعم استخدام الإنترنت مثل IPsec-VPN. ويتم تشفير عنوان حزم IP وبياناتها.
Remote Gateway(Tunnel Mode) (البوابة البعيدة (وضع النفق))	إذا حددت **Tunnel Mode (وضع النفق)** في **Encapsulation (تغليف)**، فأدخل عنوان بوابة من 1 إلى 39 حرفًا.	
Security Protocol (بروتوكول الأمان)	حدد خيارًا إذا حددت **IPsec** في **Access Control (التحكم في الوصول)**.	
	ESP	حدد هذا الخيار لضمان سلامة المصادقة والبيانات وتشفير البيانات.
	AH	حدد هذا الخيار لضمان سلامة المصادقة والبيانات. ويمكنك استخدام IPsec حتى في حالة حظر تشفير البيانات.

معلومات ذات صلة

- "تهيئة السياسة الافتراضية" في الصفحة 41
- "الجمع بين العنوان المحلي (الماسحة الضوئية) و العنوان البعيد (المضيف) في سياسة المجموعة" في الصفحة 44
- "مراجع اسم الخدمة في سياسة المجموعة" في الصفحة 44

الجمع بين العنوان المحلي (الماسحة الضوئية) و العنوان البعيد (المضيف) في سياسة المجموعة

		إعداد العنوان المحلي (الطابعة)		
		IPv4	IPv6*2	أي عناوين*3
إعداد العنوان البعيد (المضيف)	IPv4*1	✓	-	✓
	IPv6*1*2	-	✓	✓
	فارغ	✓	✓	✓

*1: إذا كان **IPsec** محدداً في **Access Control** (**التحكم في الوصول**), فلا يمكنك التحديد بطول بادئة.

*2: إذا كان **IPsec** محدداً في **Access Control** (**التحكم في الوصول**), يمكنك تحديد عنوان ارتباط شبكة محلية (fe80::)، لكن سيتم تعطيل سياسة المجموعة.

*3: باستثناء عناوين ارتباط بيانات الشبكة المحلية IPv6.

مراجع اسم الخدمة في سياسة المجموعة

ملاحظة:
يتم عرض الخدمات غير المتوفرة، لكن لا يمكن تحديدها.

اسم الخدمة	نوع البروتوكول	رقم المنفذ المحلي	رقم المنفذ البعيد	الميزات المتحكم بها
Any (أي خدمة)	-	-	-	جميع الخدمات
ENPC	UDP	3289	أي منفذ	البحث عن طابعة من تطبيقات مثل EpsonNet Config، وبرنامج تشغيل طابعة، وبرنامج تشغيل ماسحة ضوئية
SNMP	UDP	161	أي منفذ	الحصول على MIB وتهيئته من تطبيقات مثل EpsonNet Config، وبرنامج تشغيل طابعة Epson، وبرنامج تشغيل ماسحة ضوئية من Epson
LPR	TCP	515	أي منفذ	إعادة توجيه بيانات LPR
RAW(Port9100) (RAW (منفذ 9100))	TCP	9100	أي منفذ	إعادة توجيه بيانات RAW
RAW(Custom Port) (RAW (المنفذ المخصص))	TCP	2501 (افتراضي)	أي منفذ	إعادة توجيه بيانات RAW
IPP/IPPS	TCP	631	أي منفذ	إعادة توجيه بيانات AirPrint (الطباعة عبر IPP/IPPS)
WSD	TCP	أي منفذ	5357	تحكم WSD
WS-Discovery	UDP	3702	أي منفذ	البحث عن طابعة من WSD
Network Scan (فحص الشبكة)	TCP	1865	أي منفذ	إعادة توجيه بيانات الفحص من Document Capture Pro

اسم الخدمة	نوع البروتوكول	رقم المنفذ المحلي	رقم المنفذ البعيد	الميزات المتحكم بها
Network Push Scan (الفحص بالدفع عبر الشبكة)	TCP	أي منفذ	2968	الحصول على معلومات مهمة الفحص بالدفع من Document Capture Pro
Network Push Scan Discovery (اكتشاف الفحص بالدفع عبر الشبكة)	UDP	2968	أي منفذ	يتم تنفيذ البحث عن كمبيوتر عند الفحص بالدفع من Document Capture Pro
(Local) FTP Data (بيانات FTP (محلي))	TCP	20	أي منفذ	خادم FTP (إعادة توجيه بيانات الطباعة عبر FTP)
(Local) FTP Control (تحكم FTP (محلي))	TCP	21	أي منفذ	خادم FTP (التحكم في الطباعة عبر FTP)
(Remote) FTP Data (بيانات FTP (بعيد))	TCP	أي منفذ	20	عميل FTP (إعادة توجيه بيانات الفحص وبيانات الفاكس المستلم) لكن، لا يمكن لهذا الأمر التحكم إلا بخادم FTP الذي يستخدم المنفذ البعيد رقم 20.
(Remote) FTP Control (تحكم FTP (بعيد))	TCP	أي منفذ	21	عميل FTP (التحكم لإعادة توجيه بيانات الفحص وبيانات الفاكس المستلم)
CIFS) (Local) CIFS (محلي))	TCP	445	أي منفذ	خادم CIFS (إتاحة مجلد شبكة للمشاركة)
CIFS) (Remote) CIFS (بعيد))	TCP	أي منفذ	445	عميل CIFS (إعادة توجيه بيانات الفحص وبيانات الفاكس المستلم إلى مجلد)
HTTP) (Local) HTTP (محلي))	TCP	80	أي منفذ	خادم HTTP(S) (إعادة توجيه بيانات Web Config وWSD)
(Local) HTTPS (HTTPS (محلي))	TCP	443	أي منفذ	
(Remote) HTTP (HTTP (بعيد))	TCP	أي منفذ	80	عميل HTTP(S) (اتصال بين Epson Connect أو Google Cloud Print، وتحديث البرامج الثابتة، وتحديث الشهادة الجذر)
(Remote) HTTPS (HTTPS (بعيد))	TCP	أي منفذ	443	

أمثلة على تهيئة وظيفة تصفية IPsec/IP

استلام حزم IPsec فقط
يُستخدم هذا المثال لتهيئة سياسة افتراضية فقط.

السياسة الافتراضية:

- ❏ **IPsec/IP Filtering (تصفية IPsec/IP): Enable (تمكين)**
- ❏ **Access Control (التحكم في الوصول): IPsec**

إعدادات الأمان

- ❏ **Authentication Method (طريقة المصادقة)**: **Pre-Shared Key (المفتاح المتاح للمشاركة مسبقًا)**
- ❏ **Pre-Shared Key (المفتاح المتاح للمشاركة مسبقًا)**: أدخل حتى 127 حرفًا.

سياسة المجموعة:
تجنب التهيئة.

استلام بيانات الطباعة وإعدادات الطابعة
يشرح هذا المثال كيفية السماح بالربط بين بيانات الطباعة وتهيئة الطابعة من خدمات محددة.

السياسة الافتراضية:

- ❏ **IPsec/IP Filtering (تصفية IPsec/IP)**: **Enable (تمكين)**
- ❏ **Access Control (التحكم في الوصول)**: **Refuse Access (رفض الوصول)**

سياسة المجموعة:

- ❏ **Enable this Group Policy (تمكين سياسة المجموعة هذه)**: حدد خانة الاختيار.
- ❏ **Access Control (التحكم في الوصول)**: **Permit Access (السماح بالوصول)**
- ❏ **Remote Address(Host) (العنوان البعيد (المضيف))**: عنوان IP لجهاز عميل
- ❏ **Method of Choosing Port (طريقة اختيار المنفذ)**: **Service Name (اسم الخدمة)**
- ❏ **Service Name (اسم الخدمة)**: حدد خانة اختيار **ENPC** و**SNMP** و**HTTP (Local)** و**HTTP (محلي)** و**HTTPS (Local)** و**HTTPS (محلي)** و**RAW(Port9100) (RAW (المنفذ 9100))**.

استلام حق الوصول من عنوان IP محدد فقط
يشرح هذا المثال كيفية السماح لعنوان IP محدد بالوصول إلى الطابعة.

السياسة الافتراضية:

- ❏ **IPsec/IP Filtering (تصفية IPsec/IP)**: **Enable (تمكين)**
- ❏ **Access Control (التحكم في الوصول)**: **Refuse Access (رفض الوصول)**

سياسة المجموعة:

- ❏ **Enable this Group Policy (تمكين سياسة المجموعة هذه)**: حدد خانة الاختيار.
- ❏ **Access Control (التحكم في الوصول)**: **Permit Access (السماح بالوصول)**
- ❏ **Remote Address(Host) (العنوان البعيد (المضيف))**: عنوان IP لجهاز عميل تابع لمسؤول

ملاحظة:
بصرف النظر عن تهيئة السياسة، سيتمكن الجهاز العميل من الوصول إلى الطابعة وتهيئتها.

استخدام بروتوكول SNMPv3

حول SNMPv3

يشير SNMP إلى بروتوكول يجري عمليات مراقبة وتحكم لجمع معلومات الأجهزة المتصلة بالشبكة. وSNMPv3 هو إصدار ميزة أمان الإدارة الذي تم تحسينه.

عند استخدام SNMPv3، يمكن مصادقة مراقبة حالة اتصال SNMP وتعيين تغييراته (الحزمة) وتشفيرها لحماية اتصال SNMP (الحزمة) من مخاطر الشبكة، مثل التصنت على المحادثات الهاتفية وانتحال الشخصية والعبث بالبيانات.

تهيئة SNMPv3

إذا كانت الطابعة تدعم بروتوكول SNMPv3، يمكنك مراقبة الوصول إلى الطابعة والتحكم فيه.

1. ادخل Web Config وحدد **Services** (**الخدمات**) > **Protocol** (**البروتوكول**).
2. أدخل قيمة لكلٍ من عناصر **SNMPv3 Settings** (**إعدادات SNMPv3**).
3. انقر فوق **Next** (**التالي**).

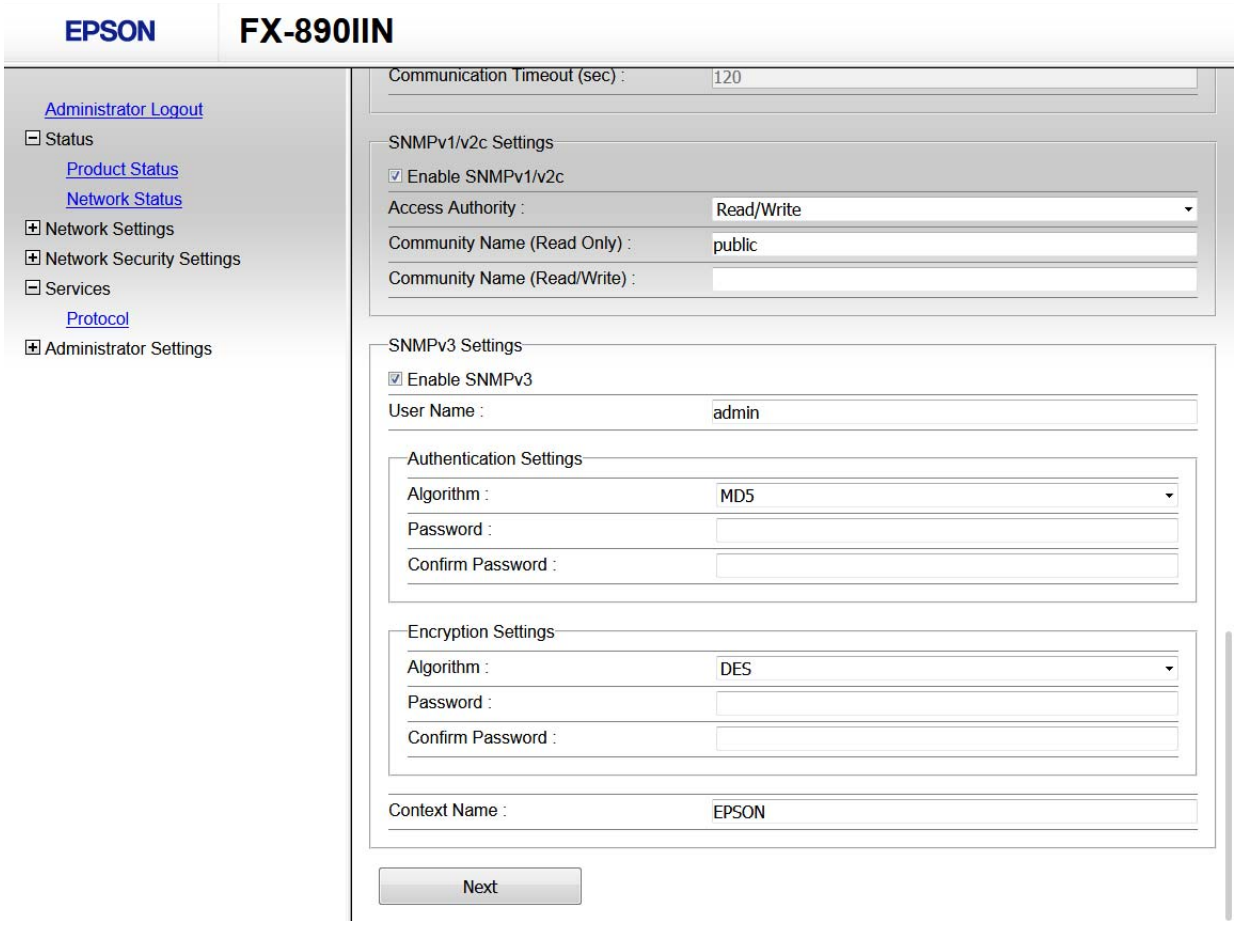
   تظهر عندئذٍ رسالة تأكيد.
4. انقر فوق **OK** (**موافق**).

   وبذلك يتم تحديث الطابعة.

معلومات ذات صلة

"الوصول إلى Web Config" في الصفحة 20
"عناصر إعداد SNMPv3" في الصفحة 48

عناصر إعداد SNMPv3



العناصر	الإعدادات والشرح
Enable SNMPv3 (تمكين SNMPv3)	يتم تمكين SNMPv3 عند تحديد خانة الاختيار.
User Name (اسم المستخدم)	أدخل من 1 إلى 32 حرفًا أحادي البايت.
Authentication Settings (إعدادات المصادقة)	
Algorithm (الخوارزمية)	حدد خوارزمية لإجراء مصادقة.
Password (كلمة المرور)	أدخل من 8 إلى 32 حرفًا بتنسيق ASCII (0x20–0x7E).
Confirm Password (تأكيد كلمة المرور)	أدخل كلمة المرور التي هيئتها للتأكيد.
Encryption Settings (إعدادات التشفير)	
Algorithm (الخوارزمية)	حدد خوارزمية لإجراء تشفير.
Password (كلمة المرور)	أدخل من 8 إلى 32 حرفًا بتنسيق ASCII (0x20–0x7E).
Confirm Password (تأكيد كلمة المرور)	أدخل كلمة المرور التي هيئتها للتأكيد.
Context Name (اسم السياق)	أدخل من 1 إلى 32 حرفًا أحادي البايت.

معلومات ذات صلة

"تهيئة SNMPv3" في الصفحة 47

حل المشاكل

التحقق من السجل للاطلاع على الخادم وجهاز الشبكة

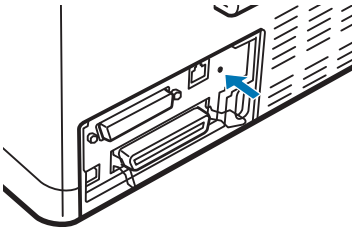
إذا حدثت مشكلة في اتصال الشبكة، يمكنك تحديد السبب عن طريق التحقق من السجل للاطلاع على خادم البريد الإلكتروني أو خادم LDAP أو الحالة باستخدام سجل نظام جهاز الشبكة، مثل جهاز توجيه أو الأوامر.

طباعة ورقة حالة شبكة

يمكنك طباعة معلومات الشبكة التفصيلية والتحقق منها.

1. حمِّل ورقًا.
2. اضغط مع الاستمرار لمدة ثلاث ثوانٍ على زر ورقة الحالة.

تتم عندئذٍ طباعة ورقة حالة الشبكة.



تهيئة إعدادات الشبكة

استعادة إعدادات الشبكة من الطابعة

يمكنك إعادة إعدادات الشبكة إلى قيمها الافتراضية.

1. أوقف تشغيل الطابعة.
2. اضغط مع الاستمرار على زر ورقة الحالة أثناء تشغيل الطابعة.

استعادة إعادة الشبكة باستخدام EpsonNet Config

يمكنك إعادة إعدادات الشبكة إلى قيمها الافتراضية باستخدام EpsonNet Config.

1. ابدأ EpsonNet Config.

2 حدد الطابعة التي تريد استعادة إعدادات الشبكة لها.

3 انقر بزر الماوس الأيمن فوق اسم الطابعة ثم حدد **Default Settings (الإعدادات الافتراضية)** > **Network Interface (واجهة الشبكة)**.

4 انقر فوق **OK (موافق)** في شاشة التأكيد.

5 انقر فوق **OK (موافق)**.

التحقق من الاتصال بين الأجهزة وأجهزة الكمبيوتر

تحقق من الاتصال باستخدام أمر Ping

يُمكنك استخدام أمر Ping للتأكد من اتصال الكمبيوتر بالطابعة. اتبع الخطوات أدناه للتحقق من الاتصال باستخدام أمر Ping.

1 تحقق من عنوان IP للطابعة في ما يخص الاتصال الذي تريد التحقق منه.

يمكنك التحقق من هذا من خلال عمود **IP Address (عنوان IP)** في ورقة حالة الشبكة.

2 اعرض شاشة موجة أوامر الكمبيوتر.

- ❏ Windows 10
  انقر بزر الماوس الأيمن فوق زر البدء أو اضغط عليه مع الاستمرار ثم حدد **Command Prompt (موجه الأوامر)**.
- ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
  اعرض شاشة التطبيق ثم حدد **Command Prompt (موجه الأوامر)**.
- ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 أو أقدم
  اضغط على زر البدء، وحدد **All Programs (كافة البرامج)** أو **Programs (البرامج)** > **Accessories (الملحقات)** > **Command Prompt (موجه الأوامر)**.

3 أدخل ما يلي في سطر الأوامر ثم اضغط على Enter.

اختبر اتصال 192.0.2.111 باستخدام أمر Ping (إذا كان عنوان IP للكمبيوتر الذي تريد التحقق منه هو 192.0.2.111)

4 يكتمل التأكيد إذا تم عرض ما يلي. أغلق **Command Prompt (موجه الأوامر)**.

إحصاءات Ping للعنوان 192.0.2.111:
حزم البيانات: المرسل = 4, المستلم = 4, المفقود = 0 (0% فقدان للبيانات),
وقت اختبار الإرسال ثم التلقي: (مللي ثانية):
الحد الأدنى = 0 مللي ثانية, الحد الأقصى = 0 مللي ثانية, المتوسط = 0 مللي ثانية

مشكلات استخدام برامج الشبكة

تعذر وصول Web Config

هل تمت تهيئة عنوان IP للطابعة بشكلٍ صحيح؟

هيئ عنوان IP باستخدام EpsonNet Config أو لوحة تحكم الطابعة. يمكنك تأكيد معلومات الإعداد الحالية باستخدام ورقة حالة شبكة أو من لوحة تحكم الطابعة.

هل المتصفح الذي تستخدمه يدعم تشفيرات مجموعة بيانات "قوة التشفير" لمعيار SSL/TLS؟

في ما يلي تشفيرات مجموعة بيانات "قوة التشفير" لمعيار SSL/TLS. ولا يمكن وصول Web Config إلا بمتصفح يدعم تشفيرات مجموعة البيانات التالية. تحقق من دعم التشفير في المتصفح الذي تستخدمه.

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

تظهر رسالة "منتهي الصلاحية" عند الوصول إلى تطبيق Web Config باستخدام اتصال SSL (https).

إذا كانت الشهادة منتهية الصلاحية، فاحصل عليها مجددًا. وإذا كانت الرسالة تظهر قبل تاريخ انتهاء صلاحية الشهادة، فتأكد من صحة تهيئة تاريخ الطابعة.

تظهر الرسالة "اسم شهادة الأمان غير متطابق..." عند الوصول إلى تطبيق Web Config باستخدام اتصال SSL (http).

لا يتطابق عنوان IP للطابعة الذي تم إدخاله لإعداد Common Name (الاسم الشائع) من أجل إنشاء شهادة موقعة ذاتيًا أو طلب CSR مع العنوان الذي تم إدخاله في المتصفح. احصل على شهادة واستوردها مجددًا أو غيِّر اسم الطابعة.

يتم الوصول إلى الطابعة عبر خادم وكيل.

إذا كنت تستخدم خادمًا وكيلاً مع الطابعة، يجب تهيئة إعدادات الوكيل في المتصفح الذي تستخدمه.

حدد **Control Panel (لوحة التحكم)** > **Network and Internet (الشبكة والإنترنت)** > **Internet Options (خيارات الإنترنت)** > **Connections (الاتصالات)** > **LAN settings (إعدادات LAN)** > **Proxy server (خادم وكيل)** ثم هيئ الإعدادات بحيث لا يتم استخدام الخادم الوكيل لعناوين محلية.

مثال:
192.168.1.*: العنوان المحلي 192.168.1.XXX، قناع الشبكة الفرعية 255.255.255.0
192.168.*.*: لعنوان المحلي 192.168.XXX، قناع الشبكة الفرعية 255.255.0.0

معلومات ذات صلة

◆ "الوصول إلى Web Config" في الصفحة 20
◆ "تعيين عنوان IP باستخدام EpsonNet Config" في الصفحة 14

لا يتم عرض اسم الطراز و/أو عنوان IP في EpsonNet Config

هل حددت Block (حظر) أو Cancel (إلغاء) أو Shut down (إيقاف التشغيل) عند عرض شاشة أمان Windows أو شاشة جدار حماية؟

إذا حددت **Block (حظر)** أو **Cancel (إلغاء)** أو **Shut down (إيقاف التشغيل)**، فلن يتم عرض عنوان IP واسم الطراز في EpsonNet Config أو EpsonNet Setup.

لتصحيح هذا الأمر، سجِّل EpsonNet Config كاستثناء باستخدام جدار حماية Windows وبرنامج أمان متوفر تجاريًا. وإذا كنت تستخدم برنامجًا مضادًا للفيروسات أو برنامج أمان، فأغلقه ثم جرِّب استخدام EpsonNet Config.

هل تم تعيين مهلة أقصر مما ينبغي لخطأ الاتصال؟

شغِّل EpsonNet Config وحدد **Tools (أدوات)** > **Options (خيارات)** > **Timeout (المهلة)** ثم زد طول الفترة الزمنية لإعداد **Communication Error (خطأ في الاتصال)**. تجدر الإشارة إلى أن إجراء ذلك قد يؤدي إلى تشغيل EpsonNet Config بشكل أبطأ.

حل مشاكل الأمان المتقدم

استعادة إعدادات الأمان

عند إنشاء بيئة عالية الأمان مثل تصفية IPsec/IP، قد لا تتمكن من الاتصال بأجهزة بسبب إعدادات غير صحيحة أو مشكلة في الجهاز أو الخادم. وفي هذه الحالة، استعد إعدادات الأمان لضبط إعدادات الجهاز مرة أخرى أو للسماح لك بالاستخدام لفترة مؤقتة.

تعطيل وظيفة الأمان من الطابعة

يمكنك تعطيل وظيفة تصفية IPsec/IP من الطابعة.

1. تأكد من تحميل ورق.
2. اضغط على أزرار **Menu** (**Pitch** و**Tear Off/Bin**) إلى أن تصدر الطابعة صوت تنبيه مرة واحدة وتضيء مصابيح **Menu** (مصباحا **Tear Off/Bin**).

   تدخل الطابعة في وضع الإعداد الافتراضي وتطبع رسالة تطلب منك تحديد اللغة لقائمة الإعداد الافتراضي. وتشير اللغة التي تحتها خط إلى الإعداد الحالي.
3. إذا لم يتم تحديد اللغة التي تريدها، فاضغط على الزر **Item⬇** (Font) إلى أن تشير المطبوعات إلى اللغة التي تريدها.
4. اضغط على الزر **Set** (**Tear Off/Bin**) لتحديد اللغة المطلوبة.
5. إذا أردت طباعة الإعدادات الحالية، فاضغط على الزر **Set**. وإذا أردت تجاوز طباعة الإعدادات الحالية، فاضغط على الزر **Item⬇** أو الزر **Item⬆**.

   تطبع الطابعة القائمة الأولى والقيمة الحالية للقائمة.
6. اضغط على الزر **Item⬇** أو الزر **Item⬆** لتحديد قائمة معلّمات **IPsec/IP Filtering**. اضغط على الزر **Set** للتمرير عبر القيم في إطار المعلّمة المحددة إلى أن تعثر على **Off**.

7 بعد الانتهاء من ضبط الإعدادات، اضغط على الأزرار **Menu** (**Pitch** و**Tear Off/Bin**).

تنطفئ مصابيح **Menu** (مصباحا **Tear Off/Bin**) وتخرج الطابعة من وضع الإعداد الافتراضي.
ويتم حفظ الإعدادات التي ضبطها كقيمة جديدة.

ملاحظة:
إذا أوقفت تشغيل الطابعة قبل الخروج من وضع الإعداد الافتراضي، يتم إلغاء أي تغييرات ربما تكون قد أجريتها وعدم حفظها.

استعادة وظيفة الأمان باستخدام Web Config

يمكنك تعطيل الوظيفة إذا تمكنت من الوصول إلى الجهاز من الكمبيوتر.

تعطيل وظيفة تصفية IPsec/IP باستخدام Web Config

1 ادخل Web Config وحدد **Network Security Settings** (**إعدادات أمان الشبكة**) > **IPsec/IP Filtering** > **Basic** (**أساسي**) > **IPsec/IP** (**تصفية IPsec/IP**).

2 حدد **Disable** (**تعطيل**) في **IPsec/IP Filtering** (**تصفية IPsec/IP**) ضمن **Default Policy** (**السياسة الافتراضية**).

3 انقر فوق **Next** (**التالي**) ثم ألغِ تحديد **Enable this Group Policy** (**تمكين سياسة المجموعة هذه**) لجميع سياسات المجموعات.

4 انقر فوق **OK** (**موافق**).

معلومات ذات صلة
"الوصول إلى Web Config" في الصفحة 20

مشكلات استخدام ميزات أمان الشبكة

نسيان مفتاح متاحة للمشاركة مسبقًا

هيئ المفتاح مرةً أخرى باستخدام Web Config.

لتغيير المفتاح، ادخل Web Config وحدد **Network Security Settings** (**إعدادات أمان الشبكة**) > **IPsec/IP Filtering** > **Basic** (**أساسي**) > **Default Policy** (**السياسة الافتراضية**) أو **Group Policy** (**سياسة المجموعة**).

معلومات ذات صلة
"الوصول إلى Web Config" في الصفحة 20

تعذر الاتصال باستخدام ميزة اتصال IPsec

هل تستخدم خوارزمية غير مدعمة لإعدادات الكمبيوتر؟

تدعم الطابعة الخوارزميات التالية.

طرق الأمان	الخوارزميات
خوارزمية التشفير	AES-CBC 128 وAES-CBC 192 وAES-CBC 256 و3DES-CBC وDES-CBC

طرق الأمان	الخوارزميات
خوارزمية التجزئة	SHA-1 وSHA2-256 وSHA2-384 وSHA2-512 وMD5
خوارزمية تبادل المفاتيح	Diffi e-Hellman Group2 وDiffi e-Hellman Group1* وDiffi e-Hellman Group14* Elliptic Curve Diffi e- Hellman P-256* وElliptic Curve Diffi e-Hellman P-384*

* قد تختلف الطريقة المتوفرة باختلاف الطرز.

معلومات ذات صلة

"الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 39

تعذر الاتصال فجأة

هل عنوان IP للطابعة غير صالح أو تم تغييره؟

عطِّل IPsec باستخدام لوحة تحكم الطابعة.

في حالة انتهاء صلاحية بروتوكول DHCP أو إعادة التشغيل أو انتهاء صلاحية عنوان IPv6 أو عدم الحصول عليه، ربما لم يتم العثور على عنوان IP المسجل لتطبيق Web Config الخاص بالطابعة (**Network Security Settings** (**إعدادات أمان الشبكة**) > **IPsec/IP Filtering** (**تصفية IPsec/IP**) > **Basic** (**أساسي**) > **Group Policy** (**سياسة المجموعة**) > **Local Address(Printer)** (**العنوان المحلي (الطابعة)**)). استخدم عنوان IP ثابتًا.

هل عنوان IP للكمبيوتر غير صالح أو تم تغييره؟

عطِّل IPsec باستخدام لوحة تحكم الطابعة.

في حالة انتهاء صلاحية بروتوكول DHCP أو إعادة التشغيل أو انتهاء صلاحية عنوان IPv6 أو عدم الحصول عليه، ربما لم يتم العثور على عنوان IP المسجل لتطبيق Web Config الخاص بالطابعة (**Network Security Settings** (**إعدادات أمان الشبكة**) > **IPsec/IP Filtering** (**تصفية IPsec/IP**) > **Basic** (**أساسي**) > **Group Policy** (**سياسة المجموعة**) > **Remote Address(Host)** (**العنوان البعيد (المضيف)**)). استخدم عنوان IP ثابتًا.

معلومات ذات صلة

"الوصول إلى Web Config" في الصفحة 20
"الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 39

تعذر إنشاء منفذ طباعة آمنة عبر IPP

هل تم تحديد الشهادة الصحيحة كشهادة خادم اتصال SSL/TLS؟

إذا كانت الشهادة المحددة غير صحيحة، فقد تفشل عملية إنشاء منفذ. تأكد من استخدام الشهادة الصحيحة.

هل تم استيراد شهادة مرجع مصدق (CA) إلى الكمبيوتر الذي يصل إلى الطابعة؟

إذا لم يتم استيراد شهادة مرجع مصدق للكمبيوتر، فقد تفشل عملية إنشاء منفذ. تأكد من استيراد شهادة مرجع مصدق.

معلومات ذات صلة

"الوصول إلى Web Config" في الصفحة 20

تعذر الاتصال بعد تهيئة إعدادات تصفية IPsec/IP

قد تكون القيمة المعينة غير صحيحة.

عطِّل ميزة تصفية IPsec/IP من لوحة تحكم الطابعة. وصِّل الطابعة والكمبيوتر واضبط إعدادات تصفية IPsec/IP مرة أخرى.

معلومات ذات صلة

"الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 39

مشكلات استخدام شهادة رقمية

تعذر استيراد شهادة موقعة من مرجع مصدق (CA)

هل تتطابق الشهادة الموقعة من المرجع المصدق مع المعلومات في طلب CSR؟

إذا لم تكن الشهادة الموقعة من المرجع المصدق وطلب CSR يحتويان على المعلومات نفسها، فلا يمكن استيراد طلب CSR. تحقق مما يلي:

- ❏ هل تحاول استيراد الشهادة إلى جهاز لا يحتوي على المعلومات نفسها؟

  تحقق من معلومات طلب CSR ثم استورد الشهادة إلى جهاز يحتوي على المعلومات نفسها.

- ❏ هل استبدلت طلب CSR المحفوظ في الطابعة بعد إرساله إلى مرجع مصدق؟

  احصل على شهادة موقعة من المرجع المصدق مرةً أخرى باستخدام CSR.

هل حجم الشهادة الموقعة من المرجع المصدق أكبر من 5 كيلوبايت؟

لا يمكنك استيراد شهادة موقعة من مرجع مصدق بحجم أكبر من 5 كيلوبايت.

هل كلمة مرور استيراد الشهادة صحيحة؟

إذا نسيت كلمة المرور، فلا يمكنك استيراد الشهادة.

معلومات ذات صلة

"استيراد شهادة موقعة من مرجع مصدق" في الصفحة 36

تعذر تحديث شهادة موقعة ذاتيًا

هل تم إدخال الاسم الشائع؟

يجب إدخال **Common Name (الاسم الشائع)**.

هل تم إدخال حروف غير مدعومة في الاسم الشائع؟ على سبيل المثال، الحروف اليابانية غير مدعومة.

أدخل من 1 إلى 128 حرفًا بتنسيق IPv4 أو IPv6 أو اسم المضيف أو FQDN بتنسيق ASCII (0x20-0x7E).

هل تم إدخال فاصلة أو مسافة في الاسم الشائع؟

إذا تم إدخال فاصلة، يتم تقسيم **Common Name (الاسم الشائع)** عند ذلك الموضع. ويحدث خطأ إذا تم إدخال مسافة فقط قبل فاصلة أو بعدها.

معلومات ذات صلة

"تحديث شهادة موقعة ذاتيًا" في الصفحة 38

تعذر إنشاء طلب CSR

هل تم إدخال الاسم الشائع؟

يجب إدخال **Common Name (الاسم الشائع)**.

هل تم إدخال حروف غير مدعومة في الاسم الشائع أو المؤسسة أو الوحدة المؤسسية أو المركز أو المحافظة/الإقليم؟ على سبيل المثال، الحروف اليابانية غير مدعومة.

أدخل حروفًا بتنسيق IPv4 أو IPv6 أو اسم مضيف أو FQDN بتنسيق ASCII (0x20-0x7E).

هل تم إدخال فاصلة أو مسافة في الاسم الشائع؟

إذا تم إدخال فاصلة، يتم تقسيم **Common Name (الاسم الشائع)** عند ذلك الموضع. ويحدث خطأ إذا تم إدخال مسافة فقط قبل فاصلة أو بعدها.

معلومات ذات صلة

◆ "الحصول على شهادة موقعة من مرجع مصدق" في الصفحة 34

ظهور تحذير بشأن شهادة رقمية

الرسائل	السبب/الحل
Enter a Server Certificate. (أدخل شهادة خادم.)	**السبب:** لم تحدد ملفًا لاستيراده. **الحل:** حدد ملفًا وانقر فوق Import (استيراد).
CA Certificate 1 is not entered. (لم يتم إدخال شهادة المرجع المصدق 1.)	**السبب:** لم يتم إدخال شهادة المرجع المصدق 1 وتم إدخال شهادة المرجع المصدق 2 فقط. **الحل:** استورد شهادة المرجع المصدق 1 أولاً.
Invalid value below. (القيمة التالية غير مسموح بها.)	**السبب:** توجد حروف غير مدعمة في مسار الملف و/أو كلمة المرور. **الحل:** تأكد من صحة إدخال حروف العنصر.
Invalid date and time. (التاريخ والوقت غير صالحين.)	**السبب:** لم يتم تعيين تاريخ الطابعة ووقتها. **الحل:** عيِّن التاريخ والوقت باستخدام Web Config أو Epson Device Admin.
Invalid password. (كلمة المرور غير صالحة.)	**السبب:** لا تتطابق كلمة المرور المعينة لشهادة المرجع المصدق مع كلمة المرور التي تم إدخالها. **الحل:** أدخل كلمة المرور الصحيحة.

حل المشاكل

الرسائل	السبب/الحل
Invalid file. (الملف غير صالح.)	**السبب:** لم تستورد ملف شهادة بتنسيق X509. **الحل:** للاطلاع على مزيد من المعلومات حول الشهادة، راجع موقع ويب المرجع المصدق.
	السبب: حجم الملف الذي استوردته أكبر مما ينبغي. الحد الأقصى لحجم الملف هو 5 كيلوبايت. **الحل:** إذا حددت الملف الصحيح، فقد تكون الشهادة تالفة أو ملفقة.
	السبب: السلسلة المضمنة في الشهادة غير صحيحة. **الحل:** للاطلاع على مزيد من المعلومات حول الشهادة، راجع موقع ويب المرجع المصدق.
Cannot use the Server Certificates that include more than three CA certificates. (يتعذر استخدام شهادات الخادم التي تتضمن أكثر من ثلاث شهادات مرجع مصدق.)	**السبب:** يحتوي ملف الشهادة بتنسيق PKCS#12 على أكثر من 3 شهادات مرجع مصدق. **الحل:** استورد كل شهادة عند التحويل من تنسيق PKCS#12 إلى تنسيق PEM، أو استورد ملف الشهادة بتنسيق PKCS#12 الذي يحتوى على ما يصل إلى شهادتي مرجع مصدق.
The certificate has expired. Check if the certificate is valid, or check the date and time on your printer. (انتهت صلاحية الشهادة. تحقق من صلاحية الشهادة أو تحقق من التاريخ والوقت في الطابعة.)	**السبب:** الشهادة منتهية الصلاحية. **الحل:** ❏ إذا كانت الشهادة منتهية الصلاحية، فاحصل على شهادة جديدة واستوردها. ❏ إذا كانت الشهادة غير منتهية الصلاحية، فتأكد من صحة تعيين تاريخ الطابعة ووقتها.
Private key is required. (المفتاح الخاص مطلوب.)	**السبب:** لا يوجد مفتاح خاص مقترن بالشهادة. **الحل:** ❏ إذا كانت الشهادة بتنسيق PEM/DER وتم الحصول عليها من طلب CSR باستخدام كمبيوتر، فحدد ملف المفتاح الخاص. ❏ إذا كانت الشهادة بتنسيق PKCS#12 وتم الحصول عليها من طلب CSR باستخدام كمبيوتر، فأنشئ ملفًا يتضمن المفتاح الخاص.
	السبب: تمت إعادة استيراد شهادة PEM/DER التي تم الحصول عليها من طلب CSR باستخدام Web Config. **الحل:** إذا كانت الشهادة بتنسيق PEM/DER وتم الحصول عليها من طلب CSR باستخدام Web Config، يمكنك استيرادها مرةً واحدةً فقط.
Setup failed. (اخفقت عملية الإعداد.)	**السبب:** يتعذر إتمام التهيئة بسبب فشل الاتصال بين الطابعة والكمبيوتر أو تعذر قراءة الملف بسبب بعض الأخطاء. **الحل:** بعد التحقق من الملف المحدد والاتصال، أعد استيراد الملف.

معلومات ذات صلة

"حول الشهادة الرقمية" في الصفحة 34

حذف شهادة موقعة من مرجع مصدق بطريق الخطأ

هل يوجد ملف احتياطي للشهادة؟

في حالة وجود ملف احتياطي، استورد الشهادة مرةً أخرى.

إذا حصلت على شهادة باستخدام طلب CSR تم إنشاؤه من Web Config، فلا يمكنك استيراد شهادة محذوفة مجددًا. أنشئ طلب CSR واحصل على شهادة جديدة.

معلومات ذات صلة

"حذف شهادة موقعة من مرجع مصدق" في الصفحة 37
"استيراد شهادة موقعة من مرجع مصدق" في الصفحة 36

ملحق

التعريف ببرامج الشبكة

في ما يلي شرح للبرامج المستخدمة في تهيئة الأجهزة وإدارتها.

Epson Device Admin

برنامج Epson Device Admin هو تطبيق يتيح لك تثبيت الأجهزة في الشبكة ثم تهيئة الأجهزة وإدارتها. يمكنك الحصول على معلومات تفصيلية عن الجهاز، مثل الحالة والمواد المستهلكة، وإرسال إعلامات التنبيهات، وإنشاء تقارير حول استخدام الجهاز. ويمكنك أيضًا إنشاء نموذج يحتوي على عناصر الإعداد وتطبيقه على أجهزة أخرى كإعدادات متاحة للمشاركة. يمكنك تنزيل Epson Device Admin من موقع ويب دعم Epson. للاطلاع على مزيد من المعلومات، راجع وثائق Epson Device Admin أو تعليماته.

تشغيل Epson Device Admin (لأنظمة تشغيل Windows فقط)

حدد **All Programs (كافة البرامج)** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

ملاحظة:
إذا ظهر تنبيه جدار الحماية، فاسمح بالوصول إلى *Epson Device Admin*.

EpsonNet Print

برنامج EpsonNet Print هو تطبيق للطباعة عبر شبكة TCP/IP. وفي ما يلي بعض الميزات والقيود.

- يتم عرض حالة الطابعة في شاشة المخزن المؤقت.
- إذا تم تغيير عنوان IP للطابعة عبر بروتوكول DHCP، فلا تزال الطابعة مكتشفة.
- يمكنك استخدام طابعة موجودة في قسم مختلف من الشبكة.
- يمكنك الطباعة باستخدام أحد البروتوكولات المتنوعة.
- عنوان IPv6 غير مدعوم.

EpsonNet SetupManager

برنامج EpsonNet SetupManager هو تطبيق لإنشاء حزمة لتثبيت الطابعة بشكل بسيط، مثل تثبيت برنامج تشغيل الطابعة، وتثبيت EPSON Status Monitor وإنشاء منفذ للطابعة. يتيح هذا البرنامج للمسؤول إنشاء حزم برمجية فريدة وتوزيعها بين المجموعات.

للاطلاع على مزيد من المعلومات، تفضل بزيارة موقع الويب الإقليمي لشركة Epson.