

دليل المسؤول

المحتويات

حقوق الطبع والنشر

العلامات التجارية

حول هذا الدليل

6. العلامات والرموز.
6. الأوصاف المستخدمة في هذا الدليل.
6. مراجع أنظمة التشغيل.

مقدمة

8. مكونات الدليل.
8. المصطلحات المستخدمة في هذا الدليل.
8. المصطلحات.
10. مثال على بيئة الشبكة.
12. أنواع الاتصال بالطابعة.

إعدادات الطابعة وإدارتها

15. تدفق إعدادات الطابعة وإدارتها.
15. اتصال الشبكة الخاص بالطابعة.
16. إعداد وظيفة الطابعة.
16. إعداد المجلد المشترك والخادم.
16. إعداد جهات الاتصال.
16. إعداد المسح الضوئي.
17. إعدادات الأمان.
17. إعداد الإدارة والتشغيل.

اتصال الشبكة

18. قبل إجراء اتصال الشبكة.
18. جمع معلومات عن إعداد الاتصال.
18. تعيين عنوان IP.
19. خادم DNS وخادم الوكيل.
19. الاتصال بالشبكة من لوحة التحكم.
19. تعيين عنوان IP.
23. الاتصال بشبكة LAN.

إعدادات الوظيفة

26. برنامج للإعداد.
26. Web Config (صفحة ويب للجهاز).
27. استخدام وظائف الطابعة.
27. إعدادات الطابعة لاتصال العميل / الخادم.
31. إعدادات الطابعة لاتصال النظير إلى النظير.
33. تحرير إعدادات الورق المخصص.

34. إعداد الخادم أو الملف المشترك.
34. العلاقة بين الخادم وكل وظيفة.
34. تكوين خادم البريد.
38. إعدادات المجلد المشترك.
54. استخدام جهات الاتصال.
54. ميزات إعداد الوجهة.
54. تكوين جهات الاتصال.
58. النسخ الاحتياطي لجهات الاتصال واستردادها.
59. استخدام وظائف المسح الضوئي.
59. المسح الضوئي باستخدام لوحة التحكم.
59. ضبط إعدادات النظام.
59. إعداد لوحة التحكم.
60. إعدادات توفير الطاقة أثناء فترة الخمول.
60. مزامنة التاريخ والوقت مع خادم الوقت.
- إعداد القيمة الافتراضية للمسح الضوئي والنسخ (إعدادات
المستخدم الافتراضية).
61. AirPrint Setup.

إعدادات سلامة المنتج

63. مقدمة حول ميزات أمان المنتج.
64. تكوين كلمة مرور المسؤول.
64. تكوين كلمة مرور المسؤول من لوحة التحكم.
64. تكوين كلمة مرور المسؤول باستخدام Web Config.
65. التحكم في تشغيل اللوحة.
65. تمكين إعداد القفل.
66. عناصر إعداد القفل المخصصة لقائمة إعدادات عامة.
69. عناصر إعداد القفل الأخرى.
70. شاشة العرض وإعداد الوظيفة بشكل فردي.
71. تقييد الميزات المتوفرة.
71. تكوين التحكم في الوصول.
72. تعطيل الواجهة الخارجية.

إعدادات الإدارة والتشغيل

74. تسجيل الدخول إلى الطابعة كمسؤول.
74. تسجيل الدخول إلى الطابعة باستخدام لوحة التحكم.
74. تسجيل الدخول إلى الطابعة باستخدام Web Config.
75. تأكيد معلومات الطابعة.
75. التحقق من المعلومات من لوحة التحكم.
75. التحقق من المعلومات من Web Config.
76. استلام إعلانات البريد الإلكتروني عند وقوع أحداث.
76. حول إشعارات البريد الإلكتروني.
76. تكوين إشعارات البريد الإلكتروني.
78. تحديث البرنامج الثابت.
78. تحديث البرامج الثابتة للطابعة باستخدام لوحة التحكم.

المحتويات

إعدادات الأمان المتقدمة لـ Enterprise

111	إعدادات الأمان ومنع وقوع المخاطر.
111	إعدادات ميزة الأمان.
112	اتصال SSL/TLS بالطابعة.
112	حول المصادقة الرقمية.
	الحصول على شهادة موقعة من المرجع المصدق (CA)
112	واستيرادها.
117	حذف شهادة موقعة من المرجع المصدق (CA).
117	تهيئة CA Certificate.
120	التحكم باستخدام البروتوكولات.
120	التحكم في البروتوكولات.
120	البروتوكولات التي تستطيع تمكينها أو تعطيلها.
121	عناصر إعداد البروتوكول.
124	الاتصال المشفر باستخدام تصفية IPsec/IP.
124	حول IPsec/IP Filtering.
124	تكوين السياسة الافتراضية.
128	تكوين سياسة المجموعة.
134	أمثلة على تكوين IPsec/IP Filtering.
135	تهيئة شهادة لتصفية IPsec/IP.
136	توصيل الطابعة بشبكة IEEE802.1X.
136	تكوين شبكة IEEE802.1X.
138	تكوين شهادة لاتصال IEEE802.1X.
138	التحقق من حالة شبكة IEEE 802.1X.
139	إصلاح مشكلات الأمان المتقدم.
139	استعادة إعدادات الأمان.
140	المشكلات الخاصة باستخدام ميزات أمان الشبكة.
142	المشكلات الخاصة باستخدام شهادة رقمية.

78	تحديث البرنامج الثابت باستخدام Web Config
79	تحديث البرامج الثابتة بدون الاتصال إلى الإنترنت.
79	نسخ الإعدادات احتياطياً.
79	تصدير الإعدادات.
80	استيراد الإعدادات.

حل المشكلات

81	تلميحات لحل المشكلات.
81	التحقق من حالة الطابعة.
81	التحقق من رسالة الخطأ.
83	طباعة تقرير الاتصال بالشبكة.
88	التحقق من حالة الاتصال.
92	إجراء اختبار الاتصال.
93	تهيئة إعدادات الشبكة.
95	حالة المشكلة.
95	يتعذر الوصول إلى تطبيق Web Config
	لا يمكن حفظ الصور الممسوحة ضوئياً في المجلد المشترك
96
98	المشكلات الحادثة عند إتاحة طابعات للمشاركة.
98	الخادم المشترك بطيء.
	إعدادات الطابعة في خادم الطباعة لا تظهر في الكمبيوتر
99	العميل.

ملحق

100	تقديم برنامج الشبكة.
100	Epson Device Admin
100	EpsonNet Config
	(EpsonNet Print فقط Windows101)
101	EpsonNet SetupManager
	تصدير جهات الاتصال وتسجيلها بشكل مجمع باستخدام
102	الأداة.
103	ضبط إعدادات Wi-Fi من لوحة التحكم (WPS).
	ضبط إعدادات Wi-Fi عن طريق الضغط على زر الإعداد
104	(WPS).
	ضبط إعدادات Wi-Fi عن طريق إعداد رمز PIN
105	التعريف الشخصي (WPS).
105	استخدام اتصال Wi-Fi Direct (نقطة الوصول البسيط).
	تمكين Wi-Fi Direct (نقطة الوصول البسيط) من لوحة
105	التحكم.
	تغيير إعدادات Wi-Fi Direct (نقطة الوصول البسيط)
106
106	تغيير طريقة الاتصال.
	تغيير الاتصال من الاتصال بشبكة إيثرنت إلى الاتصال
107	بشبكة Wi-Fi
	تغيير الاتصال من الاتصال بشبكة Wi-Fi إلى اتصال
107	الإيثرنت.
108	استخدام منفذ للطابعة.

حقوق الطبع والنشر

يُحظر إعادة إنتاج أي جزء من هذا الدليل أو تخزينه في نظام استرجاع أو نقله بأي شكل أو طريقة، إلكترونيًا أو ميكانيكيًا أو نُسخًا مصورة أو تسجيلًا أو خلاف ذلك، بدون تصريح مسبق مكتوب من شركة Seiko Epson Corporation. لا توجد مسؤولية قانونية تجاه براءة الاختراع فيما يخص استخدام المعلومات الواردة هنا. كما لا توجد أي مسؤولية قانونية تجاه الأضرار الناجمة عن استخدام المعلومات الواردة هنا. تُعد المعلومات المذكورة هنا معدة للاستخدام مع منتج Epson هذه فقط. لا تُعد Epson مسؤولة عن أي استخدام لهذه المعلومات مع منتجات أخرى.

لن تتحمل Seiko Epson Corporation أو أي من الشركات التابعة لها تجاه مشتري هذا المنتج أو أطراف أخرى المسؤولية عن الأضرار أو الخسائر أو التكاليف أو النفقات التي يتعرض لها المشتري أو أطراف أخرى كنتيجة لحادث أو سوء استخدام أو العبث بهذا المنتج أو التعديلات أو الإصلاحات أو التغييرات غير المصرح بها لهذا المنتج، أو (باستثناء الولايات المتحدة) الفشل في الالتزام الكامل بإرشادات الصيانة والتشغيل الخاصة بشركة Seiko Epson Corporation.

لن تتحمل شركة Seiko Epson Corporation والشركات التابعة لها مسؤولية أي أضرار أو مشاكل تنجم عن استخدام أي وحدات اختيارية أو أي منتجات استهلاكية غير تلك المعينة كمنتجات Epson الأصلية أو المنتجات المعتمدة من Epson بواسطة شركة Seiko Epson Corporation.

لن تتحمل شركة Seiko Epson Corporation مسؤولية أي ضرر ناجم عن التشويش الكهرومغناطيسي الذي يحدث نتيجة استخدام أي كابلات توصيل غير تلك المعينة كمنتجات معتمدة من Epson بواسطة شركة Seiko Epson Corporation.

© Seiko Epson Corporation 2021

تُعد محتويات هذا الدليل والمواصفات عرضة للتغيير دون إشعار.

العلامات التجارية

العلامات التجارية

Seiko علامة تجارية لشركة Seiko أو EPSON EXCEED YOUR VISION أو EXCEED YOUR VISION علامة تجارية لشركة Epson Corporation.

Google Cloud Print, Chrome, Chrome OS, and Android are trademarks of Google LLC.

Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.

Apple, Mac, macOS, OS X, Bonjour, ColorSync, Safari, AirPrint, iPad, iPhone, iPod touch, iTunes, TrueType, and iBeacon are trademarks of Apple Inc., registered in the U.S. and other countries.

تنبيه عام: أسماء المنتجات الأخرى المستخدمة في هذا الدليل هي لأغراض التعريف فقط وقد تكون علامات تجارية تخص مالكيها. Epson مسؤوليتها تجاه كل الحقوق في هذه العلامات.

حول هذا الدليل

العلامات والرموز



تنبيه:

التعليمات التي ينبغي اتباعها بعناية لتجنب الإصابة الجسدية.



هام:

التعليمات التي يجب الانتباه لها لمنع وقوع تلف للجهاز.

ملاحظة:

التعليمات التي تشتمل على تلميحات مفيدة وقيود خاصة بتشغيل الطابعة.

معلومات ذات صلة

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

الأوصاف المستخدمة في هذا الدليل

- قد تختلف تفاصيل لقطات الشاشة والرسوم التوضيحية حسب الطراز، لكن التعليمات تسري على جميع الطرازات.
- لقطات الشاشة مأخوذة من Windows Server 2012 R2. قد تختلف التفاصيل بين إصدارات نظام التشغيل.
- قد تختلف بعض عناصر القائمة في لقطات الكاميرا حسب الطراز.

مراجع أنظمة التشغيل

Windows

في هذا الدليل، تشير المصطلحات مثل "Windows 10"، و"Windows 8.1"، و"Windows 8"، و"Windows 7"، و"Windows Vista"، و"Windows XP"، و"Windows Server 2019"، و"Windows Server 2016"، و"Windows Server 2012 R2"، و"Windows Server"، 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.

□ نظام التشغيل Microsoft® Windows® 10

□ نظام التشغيل Microsoft® Windows® 8.1

□ نظام التشغيل Microsoft® Windows® 8

□ نظام التشغيل Microsoft® Windows® 7

□ نظام التشغيل Microsoft® Windows Vista®

□ نظام التشغيل Microsoft® Windows® XP

□ نظام التشغيل Microsoft® Windows® XP Professional x64 Edition

حول هذا الدليل

- نظام التشغيل Microsoft® Windows Server® 2019
- نظام التشغيل Microsoft® Windows Server® 2016
- نظام التشغيل Microsoft® Windows Server® 2012 R2
- نظام التشغيل Microsoft® Windows Server® 2012
- نظام التشغيل Microsoft® Windows Server® 2008 R2
- نظام التشغيل Microsoft® Windows Server® 2008
- نظام التشغيل Microsoft® Windows Server® 2003 R2
- نظام التشغيل Microsoft® Windows Server® 2003

Mac OS

في هذا الدليل، يُستخدم مصطلح "Mac OS" للإشارة إلى macOS Mojave، macOS High Sierra، و macOS Sierra، و OS X El Capitan، و OS X Yosemite، و OS X Mavericks، و OS X Mountain Lion، و Mac OS X v10.7.x، و Mac OS X v10.6.8.

مقدمة

مقدمة

يعد هذا دليلًا عامًا للمسؤول لاستخدام الطابعة متعددة الوظائف وإدارتها. يوجد وظائف غير متوفرة وقوائم غير معروضة وذلك لأن هذا يعد دليلًا عامًا. ولذلك، يتم إعطاء المعلومات بالقرب من عناصر الإعدادات أو القوائم. راجع دليل المستخدم للحصول على معلومات استخدام الوظيفة.

مكونات الدليل

إعدادات الطابعة وإدارتها

لتوضيح التدفق من اتصال الشبكة، إلى إعدادات كل وظيفة، وإلى إدارة الطابعة.

الاتصال

لتوضيح كيفية توصيل الجهاز بالشبكة. كما يوضح استخدام منفذ الطابعة، و خادم DNS و خادم الوكيل.

إعدادات الوظيفة

لتوضيح إعدادات كل وظيفة، مثل الطباعة والمسح الضوئي.

إعدادات سلامة المنتج

لتوضيح إعدادات الأمان الأساسية، مثل إعداد كلمة مرور المسؤول والتحكم في الوصول.

إعدادات الإدارة والتشغيل

لتوضيح التشغيل والإدارة بعد بدء استخدام الطابعة، مثل التحقق من معلومات الطابعة وإعدادات الإشعار عند وقوع أحد الأحداث.

أدوات حل المشاكل

لتوضيح تهيئة الإعدادات واكتشاف أخطاء الشبكة وإصلاحها.

إعدادات الأمان المتقدمة لـ Enterprise

لتوضيح إعدادات الأمان المتقدمة المستخدمة على الشبكة، مثل اتصال SSL/TLS وتصفية IPsec.

المصطلحات المستخدمة في هذا الدليل

المصطلحات

يتم استخدام المصطلحات التالية في هذا الدليل.

المسؤول

الشخص الذي تقع على عاتقه مسؤولية تثبيت الجهاز أو الشبكة وإعدادهما في المكتب أو المؤسسة. في المؤسسات الصغيرة، يتولى هذا الشخص مسؤولية إدارة كل من الجهاز والشبكة. في المؤسسات الكبرى، يتولى المسؤولون مراقبة الشبكة أو الأجهزة في وحدة مجموعة إحدى الإدارات أو الأقسام، ويتولى مسؤولو الشبكة مسؤولية إعدادات الاتصال لخارج المؤسسة، مثل الإنترنت.

مقدمة

مسؤول الشبكة

الشخص الذي تقع على عاتقه مسؤولية مراقبة اتصال الشبكة. الشخص الذي يقوم بإعداد جهاز التوجيه، و خادم الوكيل، و خادم DNS، و خادم البريد الإلكتروني لمراقبة الاتصال عبر الإنترنت أو الشبكة.

المستخدم

الشخص الذي يستخدم الأجهزة مثل الطابعات والمسحات الضوئية.

اتصال العميل/الخادم (مشاركة الطابعة باستخدام خادم Windows)

يمكن مشاركة قائمة انتظار الطابعة على الخادم، والاتصال الذي يشير إلى اتصال الطابعة بخادم Windows عبر الشبكة أو من خلال كابل USB. يتم الاتصال بين الطابعة والكمبيوتر عبر الخادم، ويتم التحكم في الطابعة على الخادم.

اتصال نظير إلى نظير (الطابعة المباشرة)

الاتصال الذي يشير إلى أن الطابعة والكمبيوتر متصلان بالشبكة عبر موزع الشبكة أو نقطة الوصول، ويمكن تنفيذ مهمة الطابعة مباشرة من الكمبيوتر.

Web Config (صفحة الويب للجهاز)

خادم الويب المضمن في الجهاز. يسمى Web Config. يمكنك التحقق من حالة الجهاز وتغييرها من خلال المتصفح.

قائمة انتظار الطابعة

في Windows، الرمز الخاص بكل منفذ معروض على الجهاز والطابعة مثل طابعة. يتم إنشاء رمزين أو أكثر أيضاً لجهاز واحد إذا كان الجهاز متصلاً بالشبكة عن طريق منفذين أو أكثر، مثل TCP/IP القياسي وشبكة WSD.

الأداة

مصطلح عام لبرنامج Epson لإعداد الجهاز أو إدارته، مثل Epson Device Admin، و EpsonNet Config، و EpsonNet Setup Manager، وما إلى ذلك.

المسح الضوئي السريع

مصطلح عام للمسح الضوئي من لوحة التحكم بالجهاز. باستخدام هذه الوظيفة، يتم حفظ نتيجة المسح الضوئي إلى أحد المجلدات، أو يتم إرفاقها إلى رسالة بريد إلكتروني.

ASCII (الشفرة القياسية الأمريكية لتبادل المعلومات)

إحدى شفرات الرموز القياسية. يتم تحديد 128 حرفاً، بما في ذلك رموز مثل الأحرف الأبجدية (A-Z، a-z)، والأرقام العربية (0-9)، والرموز، والأحرف الفارغة، وأحرف التحكم. عندما يتم توضيح "ASCII" في هذا الدليل، يشير إلى 0x20-0x7E (عدد سداسي عشري) المذكور أدناه، ولا يشمل أحرف التحكم.

	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	{		}	~	

* حرف المسافة.

مقدمة

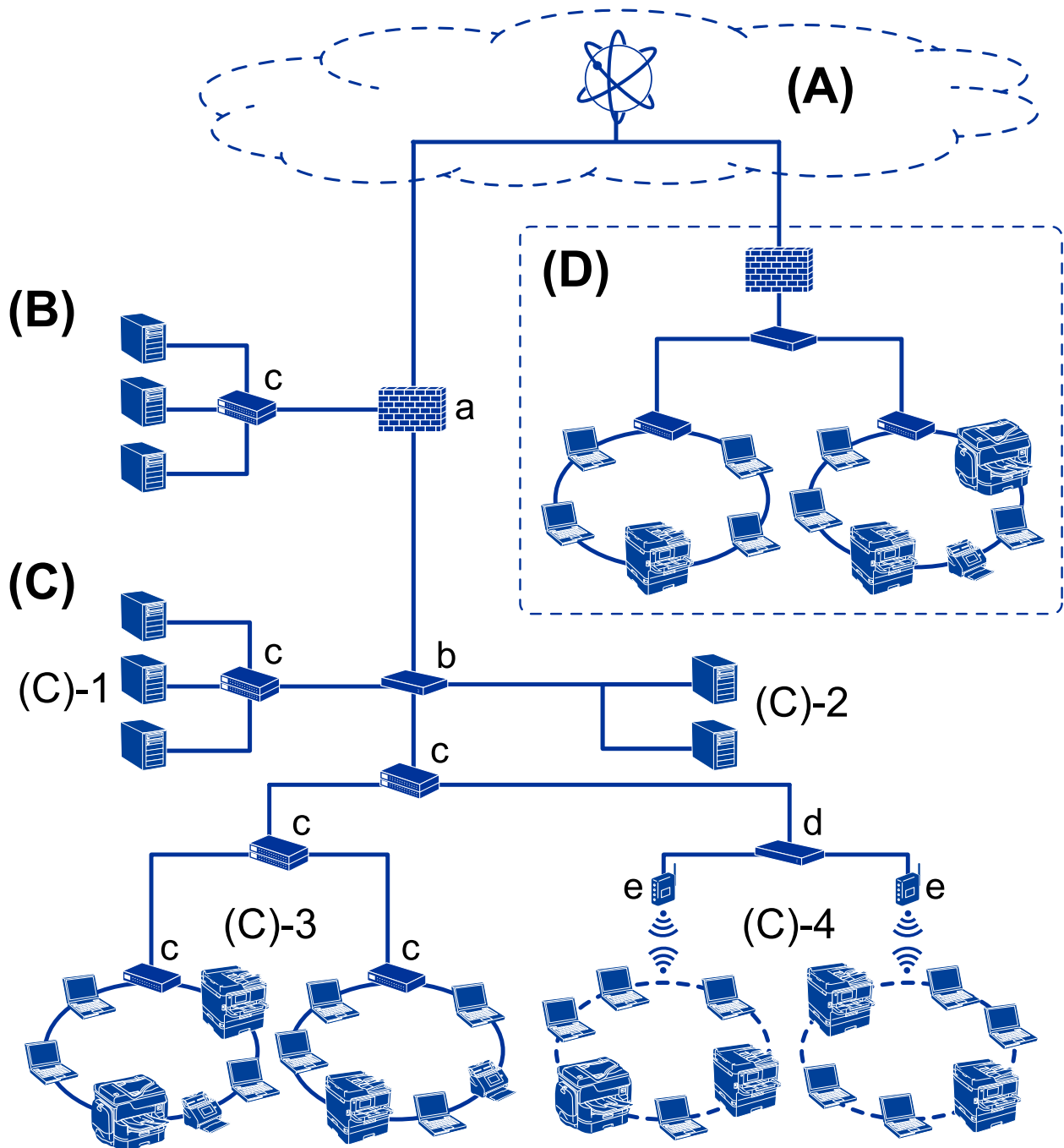
(Unicode (UTF-8

رمز قياسي دولي يحتوي على لغات عالمية مهمة. عند توضيح "UTF-8" في هذا الدليل، يشير إلى أحرف الترميز بتنسيق UTF-8.

مثال على بيئة الشبكة

يعد ذلك أحد الأمثلة على منتجات اتصال بيئة الشبكة. يمكن تضمين الوظائف والخدمات غير المتوفرة في منتجك.

مثال على بيئة الشبكة المكتبية المتوسطة إلى الكبيرة



(A): الإنترنت

مقدمة

تتوفر الخدمات التالية إذا كانت الطابعة قادرة على الاتصال بالإنترنت.

اتصال Epson

طباعة البريد الإلكتروني، والطباعة عن بُعد، وما إلى ذلك.

الخدمات السحابية

الطباعة السحابية من Google، وEvernote وما إلى ذلك.

موقع Epson

تنزيل برنامج التشغيل والبرامج وتحديث البرامج الثابتة للطابعة، وما إلى ذلك.

(B): DMZ (منطقة مجردة)

تقع هذه المنطقة بين الشبكة الداخلية (إنترنت) والشبكة الخارجية (إنترنت)، وتُعد كلتا الشبكتين جزئين معزولين بواسطة جدار الحماية. ومن الشائع وضع الخادم الذي يتم فتحه للشبكة الخارجية. كما أنها قادرة على توفير الحماية من انتشار التهديد الخارجي إلى الشبكة الداخلية. بالإضافة إلى ذلك، فهي قادرة على توفير الحماية من الوصول غير المصرح به من الشبكة الداخلية إلى الخادم الذي يتم فتحه.

خادم DNS

خادم Proxy

خادم نقل البريد الإلكتروني

خادم الويب

خادم FTP

(C): منطقة موثوقة (إنترنت)

هذه هي الشبكة الموثوقة وتتمتع بالحماية بواسطة جدار الحماية أو UTM (إدارة التهديدات الموحدة).

(C)-1: خادم داخل الإنترنت

يستخدم هذا الخادم جميع الخدمات على أجهزة الكمبيوتر الخاصة بالمؤسسة.

خادم DNS

خادم DHCP

خادم البريد الإلكتروني

خادم Active Directory

خادم الملف

(C)-2: خادم التطبيق

يعمل هذا الخادم على استخدام وظيفة تطبيق الخادم كما يلي.

مسؤول الطباعة لدى Epson

خادم Document Capture Pro

(C)-3: الشبكة المحلية السلكية (Ethernet)، (C)-4: الشبكة المحلية اللاسلكية (Wi-Fi)

وصل الطابعة، والمساحات الضوئية، وأجهزة الكمبيوتر، وما إلى ذلك بشبكة محلية باستخدام كابل LAN أو الموجة اللاسلكية.

(D): فرع آخر

هذه هي شبكة الفرع الآخر. إنها متصل عبر إنترنت، أو خط مؤجر، أو ما إلى ذلك.

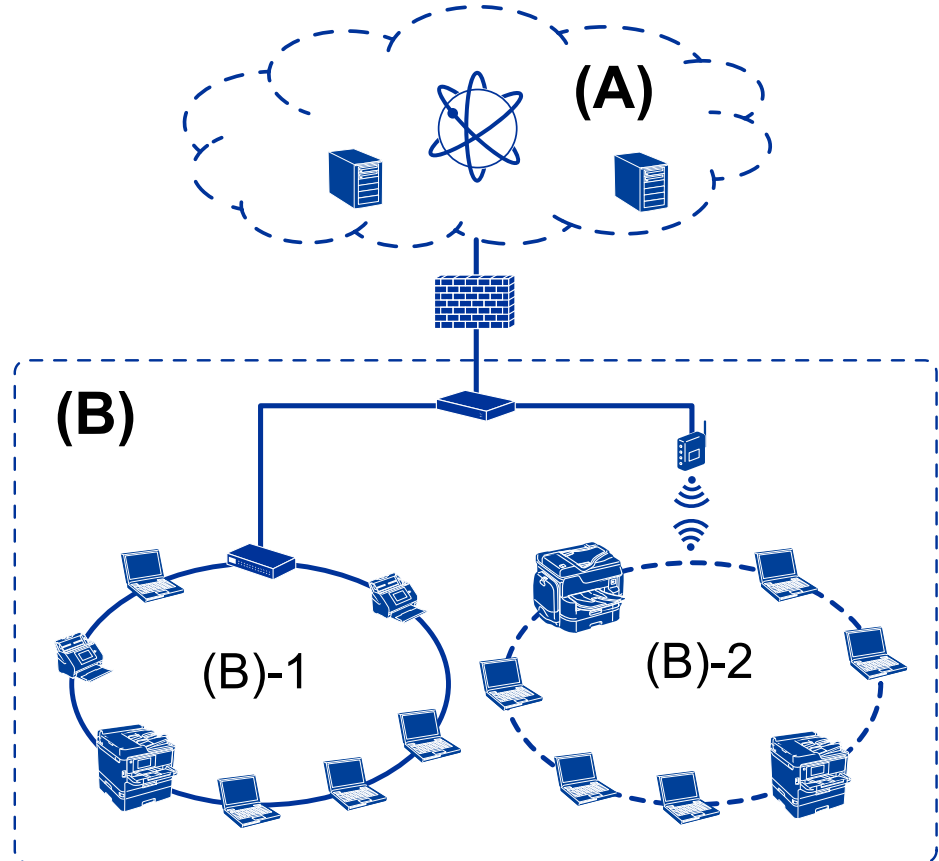
أجهزة الشبكة

أ: جدار الحماية، إدارة التهديدات الموحدة (UTM)

مقدمة

- ب: الموجه
- ج: محول الشبكة المحلية
- د: جهاز التحكم في الشبكة المحلية اللاسلكية
- هـ: نقطة الوصول

مثال على الشبكة المكتبية الصغيرة



- (A): الإنترنت
- اتصال Epson
- الخدمات السحابية
- خادم البريد الإلكتروني، خادم FTP
- (B): منطقة موثوقة (إنترنت)
- (B)-1: شبكة محلية سلكية (Ethernet)
- (B)-2: شبكة محلية لاسلكية (Wi-Fi)

أنواع الاتصال بالطابعة

تتوفر الطريقتان التاليتان لاتصال الشبكة الخاص بالطابعة.

مقدمة

□ اتصال العميل/الخادم (مشاركة الطابعة باستخدام خادم Windows)

□ اتصال نظير إلى نظير (الطباعة المباشرة)

إعدادات اتصال العميل/الخادم

هذا هو الاتصال الذي يشاركه كمبيوتر الخادم مع الطابعة. لحظر الاتصال دون المرور عبر كمبيوتر الخادم، يمكنك تعزيز الأمان. عند استخدام USB، يُمكن مشاركة الطابعة بدون وظيفة الاتصال أيضاً.

طريقة الاتصال:

قم بتوصيل الطابعة بالشبكة عبر محول الشبكة المحلية أو نقطة الوصول. يمكنك أيضاً توصيل الطابعة بالخادم مباشرة عن طريق كابل USB.

برنامج تشغيل الطابعة:

تُثبت برنامج تشغيل الطابعة على خادم Windows حسب نظام تشغيل كمبيوتر العميل. عن طريق الوصول إلى خادم Windows وربط الطابعة، يتم تثبيت برنامج تشغيل الطابعة على كمبيوتر العميل ويمكن استخدامه.

الميزات:

□ إمكانية إدارة الطابعة وبرنامج التشغيل الخاص بها دفعة واحدة.

□ حسب مواصفات الخادم، قد يستغرق بدء مهمة الطباعة وقتاً لأن جميع مهام الطباعة تتم من خلال خادم الطابعة.

□ لا يمكنك الطباعة عند إيقاف تشغيل خادم Windows.

معلومات ذات صلة

← "المصطلحات" في الصفحة 8

إعدادات اتصال نظير إلى نظير

يُعد هذا اتصال لتوصيل الطابعة على الشبكة والكمبيوتر مباشرة. لا يُمكن توصيل سوى طراز يدعم استخدام الشبكة.

طريقة الاتصال:

وصِّل الطابعة بالشبكة مباشرة عبر موزع الشبكة أو نقطة الوصول.

برنامج تشغيل الطابعة:

قم بتثبيت برنامج تشغيل الطابعة على كل كمبيوتر عميل.

عند استخدام EpsonNet SetupManager، يمكنك توفير حزمة برنامج التشغيل التي تتضمن إعدادات الطابعة.

الميزات:

□ تبدأ مهمة الطباعة في الحال لأن مهمة الطباعة يتم إرسالها إلى الطابعة مباشرة.

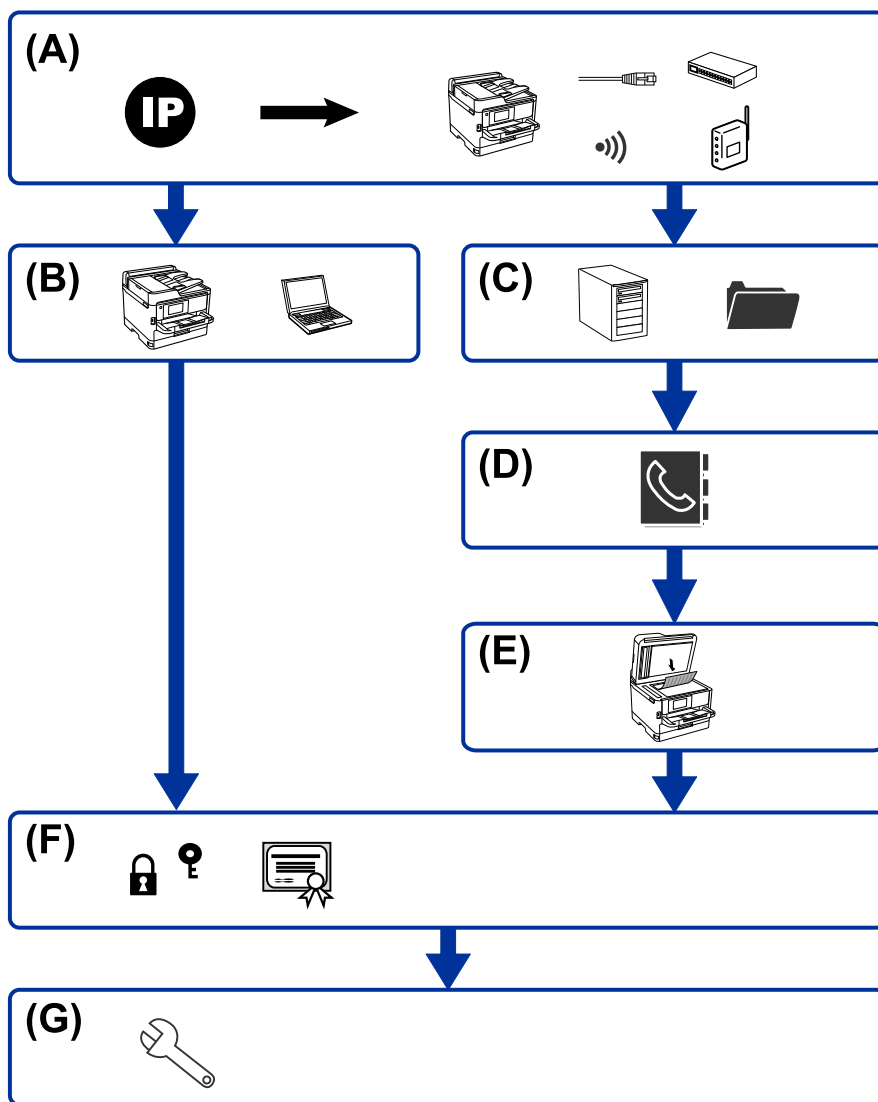
□ يمكنك الطباعة طالما الطابعة قيد التشغيل.

مقدمة

معلومات ذات صلة
← "المصطلحات" في الصفحة 8

إعدادات الطابعة وإدارتها

تدفق إعدادات الطابعة وإدارتها



إعدادات وظيفة الطابعة	B	اتصال الشبكة الخاص بالطابعة	A
إعدادات جهات الاتصال	D	إعدادات المجلد المشترك والخادم	C
إعدادات الأمان	F	إعدادات المسح الضوئي	E
		إعدادات الإدارة والتشغيل	G

اتصال الشبكة الخاص بالطابعة

عين عنوان IP للطابعة ووصله بالشبكة.

إعدادات الطابعة وإدارتها

إعداد عنوان IP

الاتصال بالشبكة (توصيل كابل LAN / إعدادات Wi-Fi)

معلومات ذات صلة

← "اتصال الشبكة" في الصفحة 18

إعدادات وظيفة الطابعة

اضبط الإعدادات لتمكين وظيفة الطابعة.

إعدادات الطابعة لاتصال العميل / الخادم

إعدادات الطابعة لاتصال النظير إلى النظير

معلومات ذات صلة

← "استخدام وظائف الطابعة" في الصفحة 27

إعدادات المجلد المشترك والخادم

اضبط إعدادات خادم البريد لإعادة توجيه البريد الإلكتروني أو إشعار البريد الإلكتروني، واضبط إعدادات المجلد المشترك وخادم FTP لمشاركة المجلد أو نقل FTP.

إعدادات خادم البريد

إعدادات خادم الملف (إعدادات المجلد المشترك)

إعدادات خادم FTP

معلومات ذات صلة

← "إعدادات الخادم أو الملف المشترك" في الصفحة 34

إعدادات جهات الاتصال

اضبط إعدادات الوجهة لإجراء عمليات المسح الضوئي.

استيراد

تسجيل جهات الاتصال

معلومات ذات صلة

← "استخدام جهات الاتصال" في الصفحة 54

إعدادات المسح الضوئي

اضبط الإعدادات لتمكين وظيفة المسح الضوئي.

إعدادات الشبكة

إعدادات الطابعة وإدارتها

معلومات ذات صلة

← "استخدام وظائف المسح الضوئي" في الصفحة 59

إعدادات الأمان

إعداد كلمة مرور المسؤول

إعداد التحكم في الوصول

التحكم باستخدام البروتوكولات

إعداد الأمان المتقدم

معلومات ذات صلة

← "إعدادات سلامة المنتج" في الصفحة 63

← "إعدادات الأمان المتقدمة لـ Enterprise" في الصفحة 110

إعداد الإدارة والتشغيل

التحقق من حالة الجهاز

الرد على تكرار الحادث

نسخ إعدادات الجهاز احتياطياً

معلومات ذات صلة

← "إعدادات الإدارة والتشغيل" في الصفحة 74

اتصال الشبكة

يوضح هذا الفصل الإجراءات اللازمة لتوصيل الطابعة بالشبكة.

قبل إجراء اتصال الشبكة

للاتصال بالشبكة، تحقق من طريقة الاتصال ومعلومات الإعداد للاتصال مسبقاً.

جمع معلومات عن إعداد الاتصال

قم بتحضير معلومات الإعداد الضرورية للاتصال. تحقق من المعلومات التالية مقدماً.

الأقسام	العناصر	ملاحظة
طريقة اتصال الجهاز	<input type="checkbox"/> شبكة الإيثرنت <input type="checkbox"/> شبكة Wi-Fi	حدد كيفية توصيل الطابعة بالشبكة. بالنسبة للشبكة المحلية اللاسلكية، تُوصَل بِمُبدَل الشبكة المحلية. بالنسبة لـ Wi-Fi، تُوصَل بِشبكة (SSID) نقطة الوصول.
معلومات اتصال LAN	<input type="checkbox"/> عنوان IP <input type="checkbox"/> قناع الشبكة الفرعية <input type="checkbox"/> البوابة الافتراضية	حدد عنوان IP للتعين للطابعة. عند تعيين عنوان IP بشكل ثابت، تكون جميع القيم مطلوبة. عند تعيين عنوان IP بشكل ديناميكي باستخدام وظيفة DHCP، لا تكون هذه المعلومات مطلوبة لأنه قد تم تعيينها تلقائياً.
معلومات اتصال Wi-Fi	<input type="checkbox"/> معرف خدمة الشبكة <input type="checkbox"/> كلمة المرور	هذا هو SSID (اسم الشبكة) وكلمة مرور لنقطة الوصول التي تتصل بها الطابعة. إذا تم تعيين تصفية عنوان MAC، قم بتسجيل عنوان MAC الخاص بالطابعة مقدماً لتسجيل الطابعة. للاطلاع على المقاييس المعتمدة، راجع دليل المستخدم.
معلومات خادم DNS	<input type="checkbox"/> عنوان IP لـ DNS الرئيسي <input type="checkbox"/> عنوان IP لـ DNS الثانوي	تكون تلك الأشياء ضرورية عند تعيين عنوان IP ثابت للطابعة. يتم تعيين DNS الثانوي عندما يحتوي النظام على تكوين متكرر ويتواجد خادم DNS ثانوي. إذا كنت عضواً في مؤسسة صغيرة ولم تعين خادم DNS، قم بتعيين عنوان IP الخاص بالموجه.
معلومات خادم الوكيل	<input type="checkbox"/> اسم خادم الوكيل	قم بتعيين هذا عندما تستخدم بيئة الشبكة خادم الوكيل للوصول إلى الإنترنت من الإنترنت، وتستخدم الوظيفة التي تجعل الطابعة تصل مباشرة للإنترنت. تتصل الطابعة مباشرة بالإنترنت من أجل القيام بالوظائف التالية. <input type="checkbox"/> تحديث البرنامج الثابت
معلومات رقم المنفذ	<input type="checkbox"/> رقم المنفذ للتحريير	تحقق من رقم المنفذ المستخدم من قبل الطابعة والكمبيوتر، ثم حرر المنفذ الذي يتم حظره بواسطة جدار حماية، وذلك إذا لزم الأمر. بالنسبة إلى رقم المنفذ الذي تستخدمه الطابعة، راجع الملحق.

تعيين عنوان IP

فيما يلي أنواع تعيين عنوان IP.

اتصال الشبكة

عنوان IP ثابت:

عين عنوان IP المحدد مسبقاً إلى الطابعة (المضيف) يدوياً.

يجب إعداد المعلومات الخاصة بالاتصال بالشبكة (قناع الشبكة الفرعية، وعنوان البوابة الافتراضية، و خادم DNS وما إلى ذلك) يدوياً. لا يتغير عنوان IP حتى عندما يكون الجهاز مغلقاً، لذلك يكون هذا مفيداً عندما ترغب في إدارة الأجهزة مع بيئة لا يمكنك فيها تغيير عنوان IP أو ترغب في إدارة الأجهزة باستخدام عنوان IP. نوصي بإجراء الإعدادات على الطابعة، والخادم، وما إلى ذلك الذي يمكن للعديد من أجهزة الكمبيوتر الوصول إليه. بالإضافة إلى ذلك، عند استخدام ميزات الأمان مثل تصفية IP/Sec، عين عنوان IP ثابت بحيث لا يتغير عنوان IP.

التعيين التلقائي باستخدام وظيفة DHCP (عنوان IP ديناميكي):

عين عنوان IP تلقائياً إلى الطابعة (المضيف) باستخدام وظيفة DHCP الخاصة بموجه أو خادم DHCP.

يتم تعيين المعلومات للاتصال بالشبكة (قناع الشبكة الفرعية، وعنوان البوابة الافتراضية، و خادم DNS وما إلى ذلك) تلقائياً، بحيث يمكنك بسهولة توصيل الجهاز بالشبكة.

إذا تم إيقاف تشغيل الموجه أو الجهاز، أو حسب إعدادات خادم DHCP، فقد يتغير عنوان IP عند إعادة الاتصال.

نحن نوصي بإدارة الأجهزة بخلاف عنوان IP والاتصال مع البروتوكولات التي يمكنها تتبع عنوان IP.

ملاحظة:

عندما تستخدم وظيفة حفظ عنوان IP من DHCP، يمكنك تعيين عنوان IP نفسه على الأجهزة في أي وقت.

خادم DNS وخادم الوكيل

لدى خادم DNS اسم مضيف، واسم مجال عنوان البريد الإلكتروني، وما إلى ذلك، مقترناً بمعلومات عنوان IP.

يكون الاتصال مستحيلاً إذا كان الطرف الآخر موصوفاً باسم المضيف واسم المجال وما إلى ذلك عندما يقوم الكمبيوتر أو الطابعة بإجراء اتصال IP.

يستعلم من خادم DNS لتلك المعلومات ويحصل على عنوان IP الخاص بالطرف الآخر. ويطلق على هذه العملية، "تحليل الاسم".

لذلك، يمكن لأجهزة مثل أجهزة الكمبيوتر والطابعات التواصل باستخدام عنوان IP.

يُعد تحليل الاسم أمراً ضرورياً للطابعة للاتصال باستخدام وظيفة البريد الإلكتروني أو وظيفة الاتصال بالإنترنت.

وعندما تستخدم تلك الوظائف، قم بضبط إعدادات خادم DNS.

عند تقوم بتعيين عنوان IP للطابعة باستخدام وظيفة DHCP الخاصة بخادم DHCP أو الموجه، يتم تعيينه تلقائياً.

يوجد خادم الوكيل في البوابة بين الشبكة والإنترنت، ويتصل بالكمبيوتر، والطابعة، والإنترنت (الخادم المقابل) بالنيابة عن كل منها. لا يتصل الخادم المقابل إلا بخادم الوكيل فقط. لذلك، يتعذر قراءة معلومات الطابعة مثل عنوان IP ورقم المنفذ ويتوقع زيادة الأمان.

عند الاتصال بالإنترنت عبر خادم Proxy، قم بتكوين خادم Proxy على الطابعة.

الاتصال بالشبكة من لوحة التحكم

قم بتوصيل الطابعة بالشبكة باستخدام لوحة تحكم الطابعة.

للتعرف على لوحة تحكم الطابعة، اطلع على دليل المستخدم للحصول على مزيد من التفاصيل.

تعيين عنوان IP

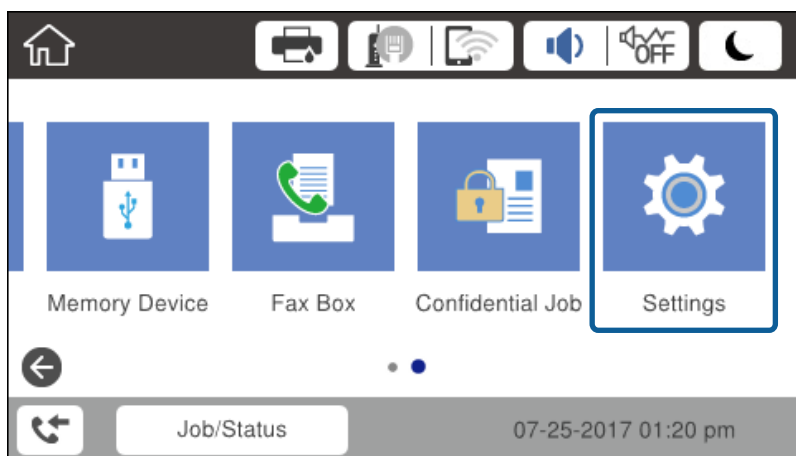
قم بإعداد العناصر الأساسية مثل عنوان المضيف قناع الشبكة الفرعية، والبوابة الافتراضية.

يوضح هذا القسم إجراءات إعداد عنوان IP ثابت.

1. قم بتشغيل الطابعة.

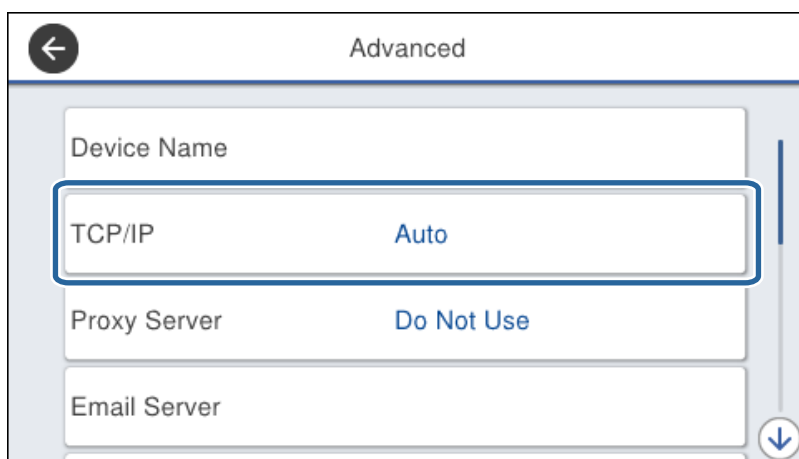
اتصال الشبكة

2. حدد الإعدادات في الشاشة الرئيسية في لوحة التحكم بالطابعة.



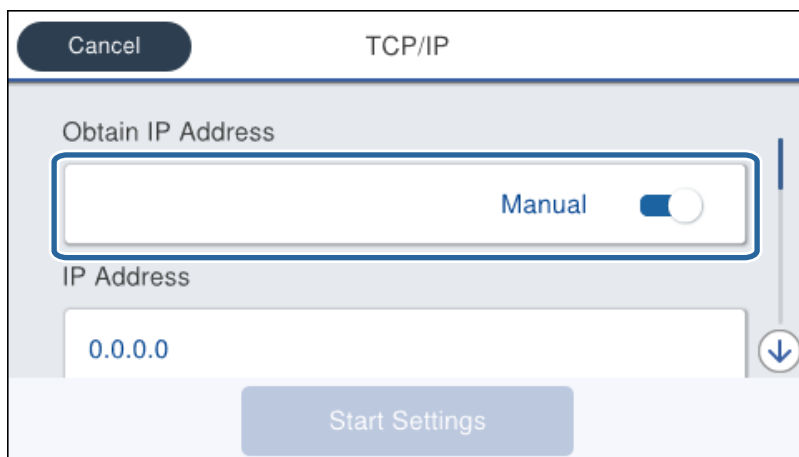
3. حدد إعدادات عامة < إعدادات الشبكة > متقدم.

4. حدد TCP/IP.



5. حدد يدوي ل الحصول على عنوان IP.

عند تعيين عنوان IP تلقائياً باستخدام وظيفة DHCP في جهاز التوجيه، حدد تلقائياً. في هذه الحالة، تم تعيين عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية في الخطوات من 6 إلى 7 تلقائياً أيضاً، لذلك انتقل إلى الخطوة 8.



اتصال الشبكة

6. أدخل عنوان IP.

ينتقل التركيز إلى الجزء الأمامي أو الجزء الخلفي مفصلاً بنقطة إذا قمت بتحديد ◀ و ▶.



تأكد من عرض القيمة على الشاشة السابقة.

7. قم بإعداد قناع الشبكة الفرعية والبوابة الافتراضية.

تأكد من عرض القيمة على الشاشة السابقة.

هام!

إذا كانت مجموعة عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية غير صحيحة، تكون بدء الإعداد غير نشطة ولا يمكن أن تتابع باستخدام هذه الإعدادات. تأكد من عدم وجود خطأ في الإدخال.

8. أدخل عنوان IP ل خادم DNS الأساسي.

تأكد من عرض القيمة على الشاشة السابقة.

ملاحظة:

عند تحديد تلقائي لإعدادات تعيين عنوان IP، يمكنك تحديد إعدادات خادم DNS من يدوي أو تلقائي. إذا لم تتمكن من الحصول على عنوان خادم DNS تلقائياً، حدد يدوي وأدخل عنوان خادم DNS. ثم أدخل عنوان خادم DNS الثانوي مباشرة. إذا حددت تلقائي، فانتقل إلى الخطوة 10.

9. أدخل عنوان IP ل خادم DNS الثانوي.

تأكد من عرض القيمة على الشاشة السابقة.

10. اضغط على بدء الإعداد.

11. أغلق شاشة التأكيد.

إعداد خادم الوكيل

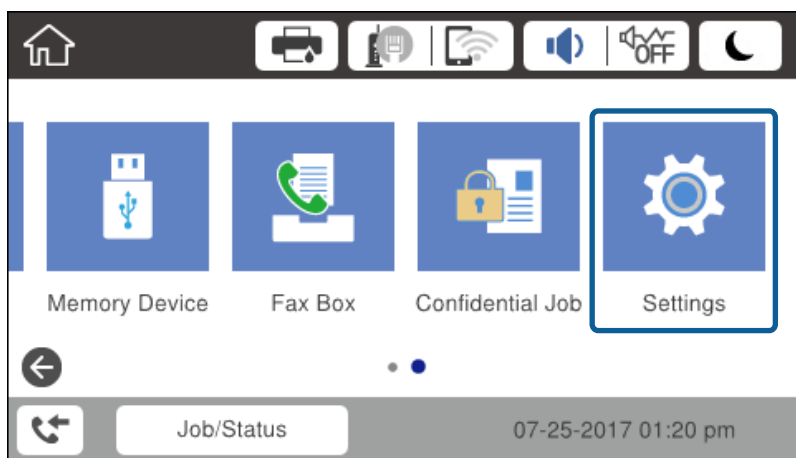
إعداد خادم الوكيل إذا كان كل مما يلي صحيحاً.

يتم إنشاء خادم الوكيل لاتصال الإنترنت.

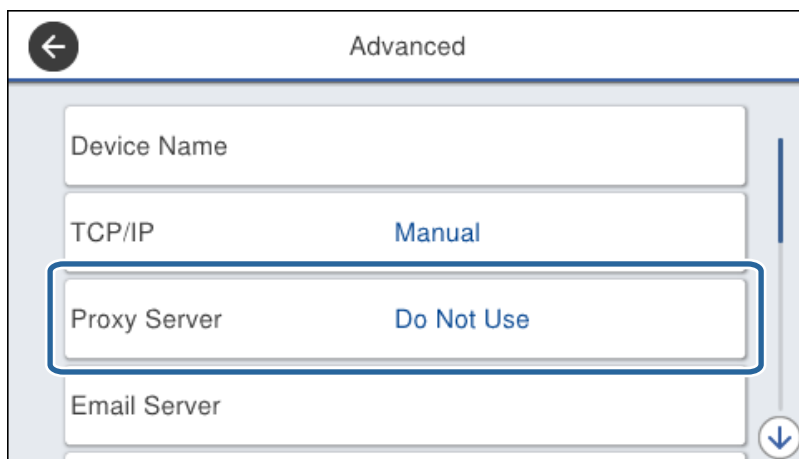
إذا كنت تريد تحديث البرنامج الثابت للطابعة عبر الإنترنت من لوحة التحكم بالطابعة أو من Web Config.

اتصال الشبكة

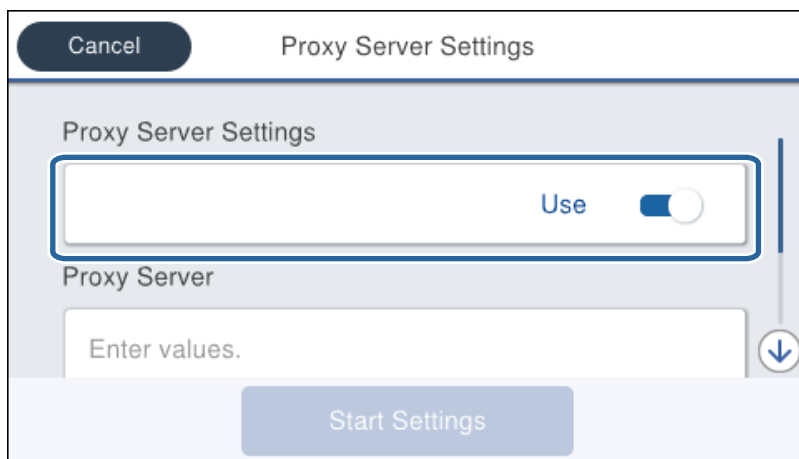
1. حدد الإعدادات في الصفحة الرئيسية. عند ضبط الإعدادات بعد تعيين عنوان IP، يتم عرض شاشة متقدم. انتقل إلى الخطوة 3.



2. حدد إعدادات عامة < إعدادات الشبكة > متقدم.
3. حدد الخادم الوكيل.

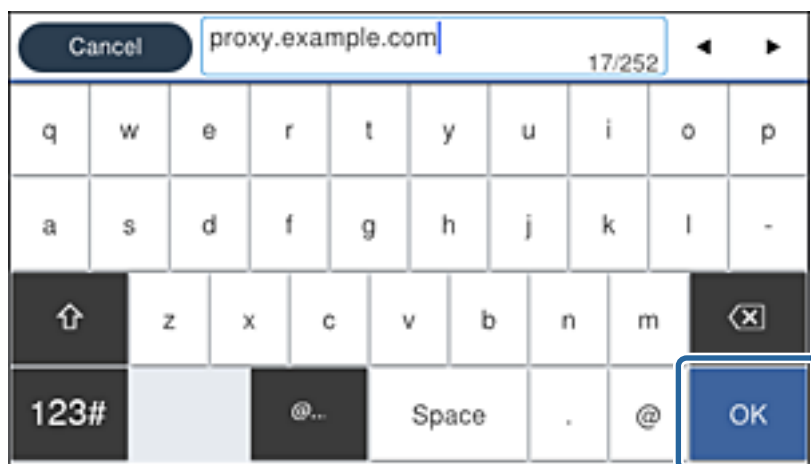


4. حدد استخدم لـ إعدادات الخادم الوكيل.



اتصال الشبكة

5. أدخل عنوان خادم الوكيل بتنسيق IPv4 أو FQDN.



تأكد من عرض القيمة على الشاشة السابقة.

6. أدخل رقم المنفذ الخاص بخادم الوكيل.

تأكد من عرض القيمة على الشاشة السابقة.

7. اضغط على بدء الإعداد.

8. أغلق شاشة التأكيد.

الاتصال بشبكة LAN

قم بتوصيل الطابعة بالشبكة باستخدام إيثرنت أو Wi-Fi.

معلومات ذات صلة

← "الاتصال بشبكة الإيثرنت" في الصفحة 23

← "الاتصال بالشبكة المحلية اللاسلكية (Wi-Fi)" في الصفحة 24

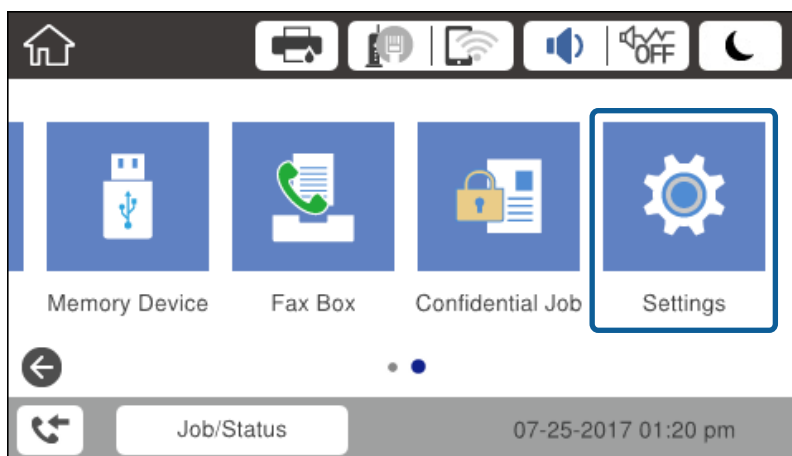
الاتصال بشبكة الإيثرنت

وصّل الطابعة بالشبكة باستخدام كابل الإيثرنت، وتحقق من الاتصال.

1. وصّل الطابعة وموزع الشبكة (محول الشبكة المحلية) بكابل إيثرنت.

اتصال الشبكة

2. حدد الإعدادات في الصفحة الرئيسية.



3. حدد إعدادات عامة < إعدادات الشبكة.

4. حدد التحقق من الاتصال.

يتم عرض نتيجة تشخيص الاتصال. تأكد من صحة الاتصال.

5. اضغط على موافق للإبقاء.

عند الضغط على طباعة تقرير الفحص، يمكنك طباعة نتيجة التشخيص. اتبع الإرشادات المعروضة على الشاشة لطباعتها.

معلومات ذات صلة

← "تغيير الاتصال من الاتصال بشبكة إيثرنت إلى الاتصال بشبكة Wi-Fi" في الصفحة 107

الاتصال بالشبكة المحلية اللاسلكية (Wi-Fi)

يمكنك إعداد المعلومات اللازمة يدوياً للاتصال بإحدى نقاط الوصول من لوحة التحكم بالطابعة. لإجراء الإعداد بشكل يدوي، فأنت في حاجة إلى معرف خدمة الشبكة وكلمة المرور الخاصين بنقطة الوصول.

ملاحظة:

عندما تدعم نقطة الوصول WPS، يمكنك ضبط إعدادات اتصال Wi-Fi تلقائياً عن طريق استخدام زر الضغط أو رمز PIN، دون استخدام SSID وكلمة المرور.

1. اضغط على  |  في الشاشة الرئيسية.

2. حدد راوتر.

3. اضغط على بدء الإعداد.

إذا تم إعداد اتصال الشبكة بالفعل، فسيتم عرض تفاصيل الاتصال. اضغط على تغيير الإعدادات لتغيير الإعدادات.

إذا كانت الطابعة متصلة بالفعل عبر Ethernet، فسيتم عرض تفاصيل الاتصال. اضغط على غير إلى اتصال Wi-Fi. ثم اضغط على نعم بعد تأكيد الرسالة.

4. حدد معالج إعداد Wi-Fi.

5. حدد معرف خدمة الشبكة (SSID) الخاص بنقطة الوصول.

إذا كان SSID الذي ترغب في الاتصال به غير معروض على لوحة التحكم بالطابعة، فاضغط على البحث مجدداً لتحديث القائمة. إذا استمر في عدم الظهور، فاضغط إدخال يدوي، ثم أدخل معرف ضبط الخدمة (SSID) مباشرة.

اتصال الشبكة

6. اضغط على إدخال كلمة المرور، ثم أدخل كلمة المرور.
ملاحظة:
 كلمة المرور حساسة لحالة الأحرف.
 إذا أدخلت SSID مباشرة، فحدد متوفر لـ كلمة المرور، ثم أدخل كلمة المرور.
7. عند الانتهاء من ذلك، اضغط على موافق.
8. تحقق من الإعدادات، ثم اضغط على بدء الإعداد.
9. اضغط على موافق للإنتهاء.
- إذا فشلت في الاتصال، فحدد طباعة تقرير الفحص لطباعة تقرير اتصال الشبكة، ثم تحقق من الحلول المطبوعة.
10. أغلق شاشة إعدادات الاتصال بالشبكة.

معلومات ذات صلة

- ← "الرسائل والحلول الخاصة بتقرير اتصال الشبكة" في الصفحة 84
- ← "ضبط إعدادات Wi-Fi من لوحة التحكم (WPS)" في الصفحة 103
- ← "تغيير الاتصال من الاتصال بشبكة Wi-Fi إلى اتصال الإيثرنت" في الصفحة 107

إعدادات الوظيفة

يوضح هذا الفصل الإعدادات الأولى التي يجب عليك ضبطها لاستخدام جميع وظائف الجهاز.

برنامج للإعداد

في هذا الموضوع يتم توضيح إجراء ضبط الإعدادات من كمبيوتر المسؤول باستخدام Web Config.

Web Config (صفحة ويب للجهاز)

حول تهيئة الويب

Web Config هي صفحة ويب مضمنة خاصة بالطابعة لتكوين إعدادات الطابعة. يمكنك تشغيل الطابعة المتصلة بالشبكة من جهاز الكمبيوتر.

للوصول إلى تطبيق Web Config، يجب أن تقوم أولاً بتعيين عنوان IP للطابعة.

ملاحظة:

يمكنك تأمين الإعدادات من خلال تكوين كلمة مرور المسؤول للطابعة.

The screenshot shows the Epson Web Config interface for an L3-10000 printer. The main section is titled 'Product Status' and includes a language dropdown menu set to 'English'. Below this, there are status indicators for the Printer (Available) and Scanner (Available). A row of ink level indicators shows BK (Black), Y (Yellow), M (Magenta), and C (Cyan) with corresponding level bars. Below the ink indicators, there are input fields for Black (BK), Yellow (Y), Magenta (M), Cyan (C), and Maintenance Box, each with a 'Level' label. The Card Reader Status is shown as 'Disconnected'. At the bottom, the Cassette 1 settings are displayed, including Paper Size (Auto(A4(Vertical))), Paper Type (plain papers 1), and Paper Remaining Level (Low). A 'Refresh' button is located at the bottom left, and a 'Software Licenses' link is at the bottom right.

إعدادات الوظيفة

الوصول إلى تطبيق Web Config

أدخل عنوان IP للطابعة في مستعرض الويب. يجب تمكين JavaScript. عند الوصول إلى تطبيق Web Config عبر HTTPS، ستظهر رسالة تحذير في المستعرض نظراً لاستخدام الشهادة الموقعة ذاتياً، المخزنة في الطابعة، لكن لا توجد مشكلة.

الوصول عبر HTTPS

< > (دون) :https://:عنوان IP للطابعة

([] (مع)) :https://:عنوان IP للطابعة

الوصول عن طريق بروتوكول HTTP

< > (دون) :http://:عنوان IP للطابعة

([] (مع)) :http://:عنوان IP للطابعة

أمثلة

:IPv4

/192.0.2.111//:https

/192.0.2.111//:http

:IPv6

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

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

ملاحظة:

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

معلومات ذات صلة

← "اتصال SSL/TLS بالطابعة" في الصفحة 112

← "حول المصادقة الرقمية" في الصفحة 112

استخدام وظائف الطابعة

قم بتمكين استخدام وظيفة الطابعة عبر الشبكة.

لاستخدام الطابعة على الشبكة، يجب عليك تعيين منفذ اتصال الشبكة في جهاز الكمبيوتر وكذلك اتصال شبكة الطابعة.

الاتصال العميل / الخادم: عين المنفذ في كمبيوتر الخادم

بالنسبة لاتصال العميل / الخادم، وضح كيفية تعيين المنفذ يدوياً.

الاتصال النظير إلى النظير: عين المنفذ في كل كمبيوتر

بالنسبة لاتصال النظير إلى النظير، وضح كيفية تعيين المنفذ تلقائياً باستخدام البرنامج المثبت المتوفر من قرص البرنامج أو موقع Epson.

إعدادات الطابعة لاتصال العميل / الخادم

قم بتمكين الطابعة من الطابعة المتصلة باعتبارها اتصال الخادم / العميل.

بالنسبة لاتصال العميل / الخادم، قم بإعداد خادم الطابعة أولاً، ثم شارك الطابعة على الشبكة.

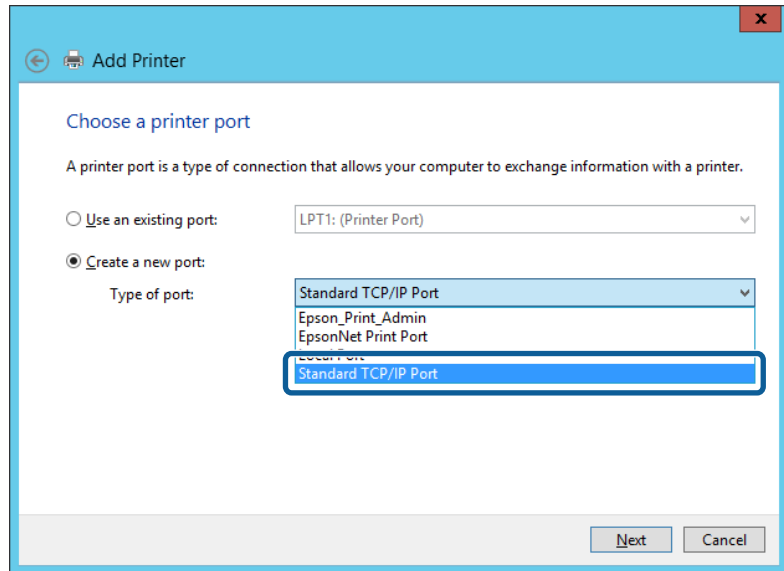
عند استخدام كابل USB للاتصال بالخادم، عين أيضاً خادم الطابعة أولاً، ثم شارك الطابعة على الشبكة.

إعدادات الوظيفة

إعداد منافذ الشبكة

قم بإنشاء قائمة انتظار الطباعة للطباعة على الشبكة على خادم الطباعة وذلك باستخدام TCP/IP، ثم تعيين منفذ الشبكة. هذا المثال عند استخدام Windows Server 2012 R2.

1. افتح شاشة الأجهزة والطابعات.
- سطح المكتب < إعدادات < لوحة التحكم < الجهاز والصوت أو الجهاز < أجهزة وطابعات.
2. إضافة طابعة.
- انقر فوق إضافة طابعة، ثم حدد الطابعة التي أرغب في الاتصال بها غير مدرجة.
3. إضافة طابعة محلية.
- حدد إضافة طابعة محلية أو شبكة طابعة بإعدادات يدوية، ثم اضغط على التالي.
4. حدد إنشاء منفذ جديد، حدد منفذ TCP/IP قياسي كنوع المنفذ، ثم اضغط على التالي.



5. أدخل عنوان IP الخاص بالطابعة أو اسمها في اسم المضيف أو عنوان IP أو اسم الطابعة أو عنوان IP، ثم انقر فوق التالي.

مثال:

اسم الطابعة: EPSONA1A2B3C

عنوان IP: 192.0.2.111

لا تقم بتغيير اسم المنفذ.

إعدادات الوظيفة

انقر فوق متابعة عندما يتم عرض شاشة التحكم في حساب المستخدم.

ملاحظة:

إذا قمت بتحديد اسم الطابعة على الشبكة التي يتوفر عليها تحليل الاسم، يتم تتبع عنوان IP حتى إذا تم تغيير عنوان IP الخاص بالطابعة بواسطة DHCP. يمكنك تأكيد اسم الطابعة من شاشة حالة الشبكة على لوحة تحكم الطابعة أو من ورقة حالة الشبكة.

6. إعداد برنامج تشغيل الطابعة.

إذا تم تثبيت برنامج تشغيل الطابعة من قبل:

حدد المصنِّع والطابعات. اضغط على التالي.

إذا لم يتم تثبيت برنامج تشغيل الطابعة:

اضغط على قرص خاص ثم أدخل قرص البرنامج المقدم مع الطابعة. اضغط على استعراض، ثم حدد المجلد في القرص المحتوي على برنامج تشغيل الطابعة. تأكد من اختيارك للمجلد الصحيح. قد يتغير مكان المجلد وفقاً لنظام التشغيل الخاص بك.

إصدار 32-بت لنظام Windows :WINX86

إصدار 64-بت لنظام Windows :WINX64

7. اتبع التعليمات المعروضة على الشاشة.

عند استخدام الطابعة ضمن اتصال العميل/الخادم (مشاركة الطابعة باستخدام خادم Windows)، اضبط إعدادات المشاركة فيما يلي.

معلومات ذات صلة

← "مشاركة الطابعة (Windows فقط)" في الصفحة 30

تحقق من تكوين منفذ — Windows

تحقق مما إذا كان تم تعيين المنفذ الصحيح لقائمة انتظار الطابعة.

1. افتح شاشة الأجهزة والطابعات.

سطح المكتب < إعدادات < لوحة التحكم < الجهاز والصوت أو الجهاز < أجهزة وطابعات.

2. افتح شاشة خصائص الطابعة.

انقر بزر الماوس الأيمن على رمز الطابعة، ثم اضغط خصائص الطابعة.

إعدادات الوظيفة

3. اضغط على علامة المنافذ وحدد منفذ TCP/IP قياسي، ثم اضغط على تكوين منفذ.

4. تحقق من تكوين المنفذ.

خاص بـ RAW

تأكد من أن تنسيق Raw محدد في البروتوكول، ثم اضغط على موافق.

خاص بـ LPR

تأكد من أن LPR محددة في البروتوكول. أدخل وظيفة "PASSTHRU" في عنوان الانتظار من إعدادات LPR. حدد تمكين عد بايت LPR، ثم اضغط على موافق.

مشاركة الطابعة (Windows فقط)

عند استخدام الطابعة ضمن اتصال العميل/الخادم (مشاركة الطابعة باستخدام خادم Windows)، قم بإعداد مشاركة الطابعة من خادم الطابعة.

1. حدد لوحة التحكم < عرض الأجهزة والطابعات على خادم الطابعة.

2. انقر بزر الماوس الأيمن فوق رمز الطابعة (قائمة انتظار الطابعة) الذي تريد مشاركته، ثم حدد علامة التبويب خصائص الطابعة < مشاركة.

3. حدد مشاركة هذه الطابعة ثم أدخل مشاركة الاسم.

بالنسبة لنظام التشغيل Windows Server 2012، انقر فوق تغيير خيارات المشاركة ثم قم بتكوين الإعدادات.

ملاحظة:

المشكلات الحادثة عند إتاحة طابعات للمشاركة

"الخادم المشترك بطيء" في الصفحة 98

"إعدادات الطابعة في خادم الطابعة لا تظهر في الكمبيوتر العميل" في الصفحة 99

تثبيت برامج تشغيل إضافية (Windows فقط)

إذا كان الكمبيوتر الخادم والكمبيوتر العميل يعملان بإصدارات Windows بمعدلات بت مختلفة، يوصى بتثبيت الإصدارات المعنية من برنامج تشغيل الطابعة في خادم الطابعة.

1. انقر بزر الماوس الأيمن فوق ملف برنامج تشغيل الطابعة الإضافي (*.exe)، وحدد إعادة تسمية، ثم غير امتداد الملف إلى zip.

يمكنك تنزيل برنامج تشغيل الطابعة الأحدث عبر موقع Epson على الويب.

<https://www.epson.com>

2. انقر بزر الماوس الأيمن فوق الملف المعادة تسميته، ثم حدد استخراج الكل لفك ضغط ملف zip.

3. حدد لوحة التحكم < عرض الأجهزة والطابعات على خادم الطابعة.

4. انقر بزر الماوس الأيمن فوق رمز الطابعة الذي تريد مشاركته مع الأجهزة التابعة، ثم انقر فوق خصائص الطابعة < مشاركة.

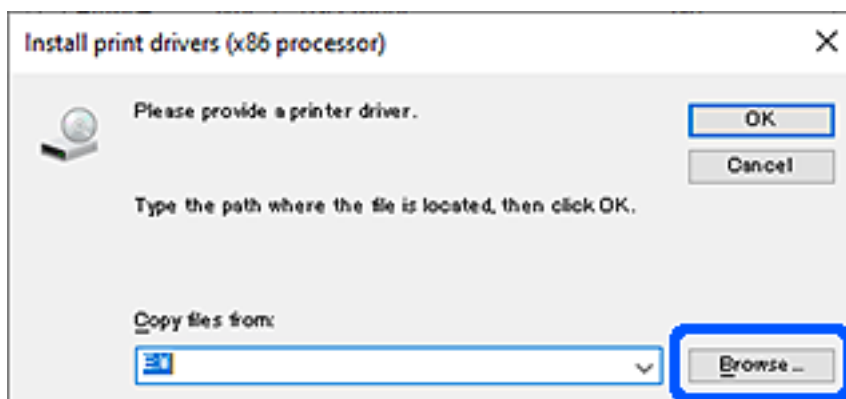
5. انقر فوق برامج تشغيل إضافية.

في Windows Server 2012، انقر فوق Change Sharing Options ثم قم بتكوين الإعدادات.

6. حدد إصدارات نظام التشغيل Windows للأجهزة التابعة، ثم انقر فوق موافق.

إعدادات الوظيفة

7. عند ظهور الشاشة التالية، انقر فوق استعراض. وحدد المجلد المستخرج في الخطوة 2، ثم حدد ملف المعلومات (*.inf) في مجلد .WINX**.



إذا ظهر ملفا معلومات اثنان أو أكثر، فبإمكانك تحديد أي منهما.

8. انقر فوق موافق لبدء عملية التثبيت.

معلومات ذات صلة

← "استخدام طابعة مشتركة - Windows" في الصفحة 31

استخدام طابعة مشتركة - Windows

يجب أن يُبلغ المسؤول العملاء باسم جهاز الكمبيوتر المخصص لخدام الطابعة وكيفية إضافته إلى هذه الأجهزة. في حالة عدم تكوين برنامج (برامج) تشغيل إضافي بعد، أخبر العملاء بكيفية استخدام الأجهزة والطابعات لإضافة الطابعة المشتركة.

في حالة وجود برنامج (برامج) تشغيل إضافي مكون بالفعل على خادم الطابعة، اتبع هذه الخطوات:

1. حدد الاسم المعين لخادم الطابعة في مستكشف Windows.

2. انقر نقرًا مزدوجًا فوق الطابعة التي تريد استخدامها.

معلومات ذات صلة

← "مشاركة الطابعة (فقط Windows)" في الصفحة 30

← "تثبيت برامج تشغيل إضافية (فقط Windows)" في الصفحة 30

إعدادات الطابعة لاتصال النظير إلى النظير

لاتصال النظير إلى النظير (الطابعة المباشرة)، يجب أن يتمتع كمبيوتر العميل والطابعة بعلاقة واحد إلى واحد.

يجب تثبيت برنامج تشغيل الطابعة على جميع أجهزة كمبيوتر العميل.

معلومات ذات صلة

← "إعداد برنامج تشغيل الطابعة" في الصفحة 32

إعدادات الوظيفة

إعداد برنامج تشغيل الطابعة

بالنسبة للمؤسسات الصغيرة، نحن نوصي بتثبيت برنامج تشغيل الطابعة على كل كمبيوتر عميل. استخدم برنامج التثبيت على موقع Epson على الويب أو على قرص البرامج.

ملاحظة:

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

1. قم بتشغيل برنامج التثبيت.

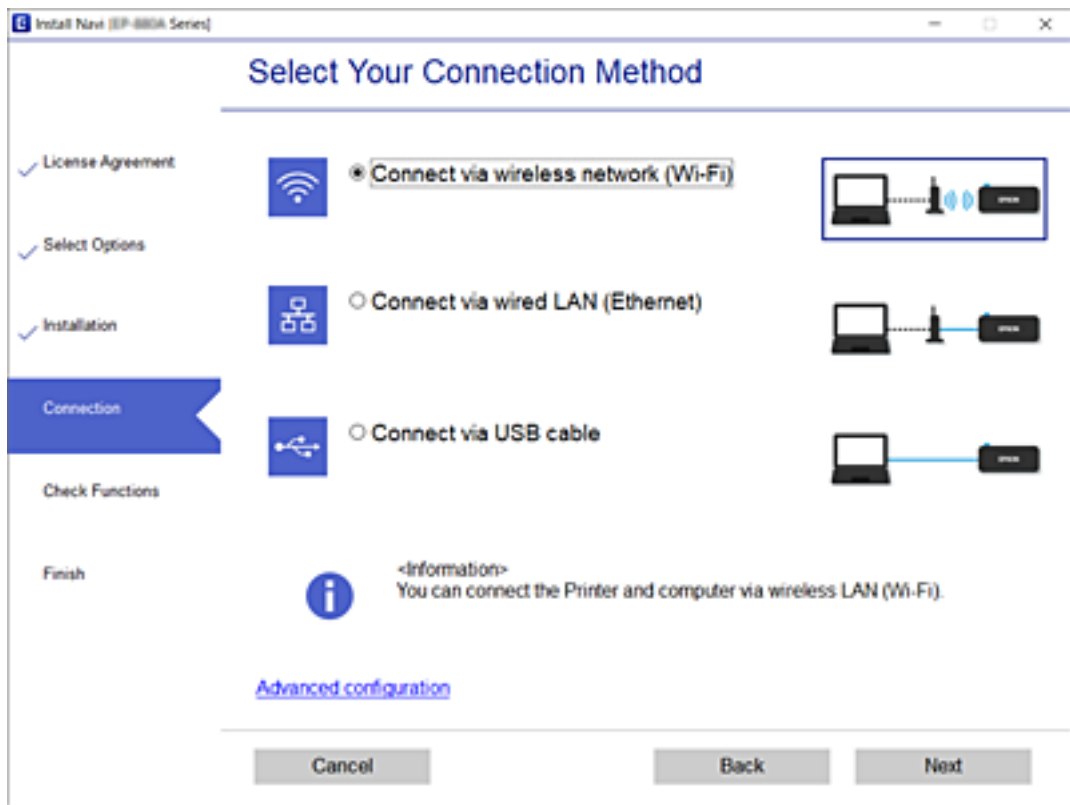
التشغيل من موقع الويب

قم بزيارة الموقع التالي، ثم أدخل اسم المنتج. انتقل إلى الإعداد، وثبت البرنامج، ثم شغله.

<http://epson.sn>

التشغيل من قرص البرامج (فقط للطرز المزودة بقرص برامج والمستخدمين الذين يمتلكون أجهزة كمبيوتر مزودة بمحركات أقراص). أدخل قرص البرامج في الكمبيوتر.

2. حدد طريقة اتصال الطابعة، ثم انقر فوق التالي.



ملاحظة:

إذا تم عرض تثبيت البرامج فحدد قم بإعداد اتصال الطابعة مرة أخرى (لراوتر الشبكة الجديدة أو تغيير *USB* إلى شبكة، وما إلى ذلك) ثم انقر فوق التالي.

3. اتبع التعليمات المعروضة على الشاشة.

معلومات ذات صلة

← "EpsonNet SetupManager" في الصفحة 101

إعدادات الوظيفة

تحرير إعدادات الورق المخصص

يمكنك تحرير إعدادات الورق المخصص. يمكن استخدام إعدادات الورق المخصص التي تم تحريرها عن طريق الاتصال من لوحة التحكم بالطابعة.

1. ادخل إلى Web Config وحدد علامة التبويب **Custom Paper Setting < Print**.

2. انقر فوق الدائرة الموجودة بجوار الرقم الذي تريد تحريره، ثم انقر فوق **تحرير**.

3. عين كل عنصر.

Custom Paper Name

أدخل اسم الورق المخصص الذي ترغب بتسجيله. يتم عرض الاسم المسجل هنا في قائمة نوع الورق.

Reference Paper

يمكنك تحديد نوع الوسائط الأقرب إلى الورق الذي تستخدمه.

Platen Gap

حدد فجوة الأسطوانة، والتي تُعد بمنزلة المسافة بين رأس الطباعة والورق. نظراً لأنه تم تعيين فجوة الأسطوانة الخاصة بـ Reference Paper المحدد، فلن تحتاج إلى تغيير القيمة عادةً. إذا تلطخت الصور المطبوعة بالحبر، فانقل إلى إعداد أوسع.

Top/Bottom Margins

قم بتعيين هامش منطقة الطباعة. ستظل الهوامش اليسرى واليمنى عند قيمة 3 ملم بغض النظر عن هذا الإعداد. إذا كان الجزء العلوي من الصورة المطبوعة متسخاً، فقم بتغيير الهامش العلوي إلى إعداد أوسع.

Paper Suction

قم بتعيين مقدار السحب الملائم للورق المستخدم للحفاظ على المسافة المناسبة بين الورق ورأس الطباعة. سيؤدي اختيار قيمة عالية جداً للورق الرفيع أو الورق الناعم إلى زيادة المسافة بين الورق ورأس الطباعة، مما يتسبب في انخفاض جودة الطباعة أو عدم تغذية الورق بصورة صحيحة. في مثل هذه الحالات، ستحتاج إلى تقليل قيمة سحب الورق. تقل قوة السحب عند خفض المعلمة. قد لا يتم عرض هذا العنصر وفقاً للطراز.

Back Tension

اضبط ضغط الورق. إذا تجعد الورق أثناء الطباعة، فحدد **High** أو **Extra High**.

Drying Time per Pass

قد يستغرق الحبر فترة وجيزة ليُجف وذلك تبعاً لنوع الورق. قم بتعيين الوقت المناسب لإيقاف حركة (تمرير) رأس الطباعة للمساعدة في تجفيف الحبر. إذا ترك الحبر بقعاً على الورق، فعين فترة أطول لتجفيف الحبر. كلما طال وقت التجفيف، زادت المدة المطلوبة للطباعة.

Drying Time per Page

قد يستغرق الحبر فترة وجيزة ليُجف وذلك تبعاً لكثافة الحبر أو نوع الورق. حدد المدة التي تتوقف فيها الطباعة مؤقتاً للسماح للحبر بالجفاف بعد طباعة كل صفحة. إذا ترك الحبر بقعاً على الورق، فعين فترة أطول لتجفيف الحبر. كلما طال وقت التجفيف، زادت المدة المطلوبة للطباعة.

Paper Size Check

عند ضبط الورق، حدد ما إذا كانت الطباعة تقوم باكتشاف عرض الورق تلقائياً أو عدم اكتشافه. جرب أن تختار **Off** إذا تم عرض رسالة خطأ بشأن إعداد الورق عند تحميل الورق بصورة صحيحة. ومع ذلك، يجرى ملاحظة أن الطباعة قد تطبع خارج الورق عند تحديد **Off**. ويتم تطبيق الإعدادات التي تم تغييرها بعد إعادة تحميل الورق. قد لا يتم عرض هذا العنصر وفقاً للطراز.

Auto Cut

حدد ما إذا كنت تريد أن تقوم الطباعة بقص بكرة الورق تلقائياً عند طباعة كل صفحة أم لا. وعند تحديد **On**، يتم إجراء قص الحافة الأمامية تلقائياً عندما لا تكون الحافة الأمامية للورق المحدد أفقية. كما يحصل الإعداد المحدد باستخدام برنامج تشغيل الطباعة على الأولوية عند استخدام برنامج تشغيل الطباعة.

إعدادات الوظيفة

Remove Skew

حدد ما إذا كنت تريد تقليل تغذية الورق بصورة قطرية أو منعه. قد لا يتم عرض هذا العنصر وفقاً للطراز.

4. تحقق من الإعدادات، ثم انقر فوق OK.

ملاحظة:

يمكن تصدير إعدادات الورق المخصص إلى أحد الملفات كما يمكن استيرادها من أحد الملفات. يعد هذا مناسباً عند تثبيت العديد من الطابعات وعندما تريد استخدام إعدادات الورق الشائعة المخصصة لها.

إعداد الخادم أو الملف المشترك

عين الخادم أو الملف المشترك الضروري عندما تستخدم وظيفة الماسحة الضوئية أو البريد الإلكتروني.

معلومات ذات صلة

← "العلاقة بين الخادم وكل وظيفة" في الصفحة 34

العلاقة بين الخادم وكل وظيفة

فيما يلي بيان للعلاقة ما بين وظيفة الطابعة والخادم أو المجلد المشترك.

قم بتعيين الخادم أو المجلد المشترك في حال استخدامك لكل وظيفة.

خادم الملف (المجلد المشترك)	خادم FTP	خادم البريد الإلكتروني	
		✓	المسح الضوئي إلى البريد الإلكتروني
	✓		المسح الضوئي إلى FTP
✓			المسح الضوئي لمجلد الشبكة
		✓	إشعار البريد الإلكتروني

معلومات ذات صلة

← "تكوين خادم البريد" في الصفحة 34

← "إعدادات المجلد المشترك" في الصفحة 38

تكوين خادم البريد

قم بتعيين خادم البريد من Web Config.

عندما تتمكن الطابعة من إرسال البريد الإلكتروني عن طريق إعداد خادم البريد، تكون كل الأمور التالية ممكنة.

نقل نتائج المسح الضوئي باستخدام البريد الإلكتروني

تلقي إشعار البريد الإلكتروني من الطابعة

تحقق أدناه قبل الإعداد.

أصبحت الطابعة متصلة بالشبكة التي يمكنها الوصول إلى خادم البريد.

معلومات إعداد البريد الإلكتروني للكمبيوتر الذي يستخدم خادم البريد نفسه المتصل بالطابعة.

إعدادات الوظيفة

ملاحظة:

- عند استخدام خادم البريد على الإنترنت، قم بتأكيد معلومات الإعداد من موفر الخدمة أو موقع الويب.
- يمكنك أيضاً تعيين خادم البريد من لوحة التحكم الخاصة بالطابعة. قم بالوصول باتباع ما يلي.
- الإعدادات > إعدادات عامة > إعدادات الشبكة > متقدم > خادم البريد الإلكتروني > إعدادات الخادم

1. ادخل إلى Web Config وحدد علامة التبويب **Basic < Email Server < Network**.

2. أدخل قيمة لكل عنصر.

3. حدد **OK**.

يتم عرض الإعدادات التي قمت بتحديدتها.
عند اكتمال الإعداد، قم بإجراء التحقق من الاتصال.

معلومات ذات صلة

- ◀ "التحقق من اتصال خادم البريد" في الصفحة 36
- ◀ "عناصر إعداد خادم البريد الإلكتروني" في الصفحة 35
- ◀ "الوصول إلى تطبيق Web Config" في الصفحة 27

عناصر إعداد خادم البريد الإلكتروني

EPSON L8-10000P

Status Print Scan/Copy Fax **Network** Network Security Product Security Device Management Epson Open Platform

Basic
Wi-Fi
Wired LAN
Wi-Fi Direct
Email Server
»Basic
»Connection Test
LDAP Server
»Basic
»Search Settings
»Connection Test
Kerberos Settings
MS Network
Epson Connect Services
Google Cloud Print Services

Email Server > Basic

The certificate is required to use a secure function of the email server.
Make settings on the following page.
- CA Certificate
- Root Certificate Update

Authentication Method : SMTP AUTH

Authenticated Account : 000000X

Authenticated Password : *****

Sender's Email Address : epson@epson-test.com

SMTP Server Address : 192.0.2.127

SMTP Server Port Number : 25

Secure Connection : None

Certificate Validation : Enable Disable

It is recommended to enable the Certificate Validation.
It will be connected without confirming the safety of the email server when the Certificate Validation is disabled.

POP3 Server Address :

POP3 Server Port Number :

OK

إعدادات الوظيفة

العناصر	الإعدادات والشرح
Authentication Method	حدد أسلوب المصادقة الذي يتيح للطابعة الوصول إلى خادم البريد الإلكتروني.
	Off عينه عندما لا يحتاج خادم البريد الإلكتروني إلى مصادقة.
	SMTP AUTH يصادق على خادم SMTP (خادم البريد الصادر) عند إرسال البريد الإلكتروني. يحتاج خادم البريد الإلكتروني إلى دعم مصادقة SMTP.
Authenticated Account	POP before SMTP يصادق على خادم POP3 (خادم البريد الوارد) قبل إرسال البريد الإلكتروني. عندما تحدد هذا العنصر، عين خادم POP3.
	إذا قمت بتحديد SMTP AUTH أو POP before SMTP في شكل Authentication Method، فأدخل اسم الحساب الذي تمت مصادقته المكون من عدة أحرف تتراوح ما بين 0 و 255 حرفاً في (ASCII 0x20-0x7E). عندما تحدد SMTP AUTH، أدخل حساب خادم SMTP. عندما تحدد POP before SMTP، أدخل حساب خادم POP3.
Authenticated Password	إذا قمت بتحديد SMTP AUTH أو POP before SMTP في شكل Authentication Method، فأدخل كلمة المرور التي تمت مصادقتها المكونة من عدة أحرف تتراوح ما بين 0 و 20 حرفاً في (ASCII 0x20-0x7E). عندما تحدد SMTP AUTH، أدخل الحساب الذي تمت مصادقته لخادم SMTP. إذا قمت بتحديد POP before SMTP، فأدخل الحساب الذي تمت مصادقته لخادم POP3.
	أدخل عنوان البريد الإلكتروني الخاص بالمرسل مثل عنوان البريد الإلكتروني لمسؤول النظام. يتم استخدام هذا العنوان عند المصادقة، لذلك أدخل عنوان بريد إلكتروني صالحاً تم تسجيله إلى خادم البريد. أدخل عدة رموز ما بين 0 و 255 رمزاً بتنسيق (ASCII 0x20-0x7E) فيما عدا: () < > [] ؛ % لا يمكن أن تكون الفاصلة الزمنية ". الرمز الأول.
SMTP Server Address	أدخل عدداً من الرموز يتراوح ما بين 0 إلى 255 رمزاً باستخدام A-Z، و a-z، و 0-9. - . يمكنك استخدام تنسيق IPv4 أو FQDN.
SMTP Server Port Number	أدخل عدداً بين 1 و 65535.
Secure Connection	حدد طريقة تشفير الاتصال إلى خادم البريد الإلكتروني.
	None إذا قمت بتحديد POP before SMTP في Authentication Method، فلن يتم تشفير الاتصال.
	SSL/TLS هذا يكون متاحاً عندما يتم ضبط Authentication Method على الوضع Off أو SMTP AUTH. يُشفر الاتصال من البداية.
Certificate Validation	STARTTLS هذا يكون متاحاً عندما يتم ضبط Authentication Method على الوضع Off أو SMTP AUTH. لا يتم تشفير الاتصال من البداية، ولكن يتم تغييرها حسب بيئة الشبكة، سواء تم تشفير الاتصال أم لا.
	يتم التحقق من صحة الشهادة عند تمكين هذا الوضع. كما يوصي بضبطها على وضع Enable. للإعداد، يجب استيراد CA Certificate إلى الطابعة.
POP3 Server Address	إذا حددت POP before SMTP في شكل Authentication Method، فأدخل عنوان خادم POP3 الذي يتكون من عدة رموز تتراوح ما بين 0 و 255 رمزاً باستخدام A-Z، و a-z، و 0-9. - . يمكنك استخدام تنسيق IPv4 أو FQDN.
POP3 Server Port Number	إذا حددت POP before SMTP في شكل Authentication Method فأدخل عدداً ما بين 1 و 65535.

معلومات ذات صلة

← "تكوين خادم البريد" في الصفحة 34

التحقق من اتصال خادم البريد

يُمكنك التحقق من اتصال خادم البريد من خلال إجراء التحقق من الاتصال.

إعدادات الوظيفة

1. ادخل إلى Web Config وحدد علامة التبويب **Network < Email Server < Connection Test**.

2. حدد **Start**.

تم بدء اختبار التوصيل بخادم البريد الإلكتروني. بعد الاختبار، يتم عرض تقرير الفحص.

ملاحظة:

يمكنك أيضاً التحقق من الاتصال إلى خادم البريد من لوحة التحكم بالطابعة. قم بالوصول باتباع ما يلي.

الإعدادات < إعدادات عامة < إعدادات الشبكة < متقدم < خادم البريد الإلكتروني < التحقق من الاتصال

معلومات ذات صلة

◀ "الوصول إلى تطبيق Web Config" في الصفحة 27

◀ "مراجع اختبار اتصال خادم البريد" في الصفحة 37

مراجع اختبار اتصال خادم البريد

السبب	الرسائل
تظهر هذه الرسالة عند نجاح الاتصال بالخادم.	Connection test was successful.
تظهر هذه الرسالة عند <input type="checkbox"/> عدم اتصال الطابعة بالشبكة <input type="checkbox"/> تعطل خادم SMTP <input type="checkbox"/> قطع الاتصال بالشبكة أثناء الاتصال <input type="checkbox"/> عدم اكتمال البيانات المستلمة	SMTP server communication error. Check the following. - Network Settings
تظهر هذه الرسالة عند <input type="checkbox"/> عدم اتصال الطابعة بالشبكة <input type="checkbox"/> تعطل خادم POP3 <input type="checkbox"/> قطع الاتصال بالشبكة أثناء الاتصال <input type="checkbox"/> عدم اكتمال البيانات المستلمة	POP3 server communication error. Check the following. - Network Settings
تظهر هذه الرسالة عند <input type="checkbox"/> فشل الاتصال بخادم DNS <input type="checkbox"/> فشل تحليل الاسم لخادم SMTP	An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server
تظهر هذه الرسالة عند <input type="checkbox"/> فشل الاتصال بخادم DNS <input type="checkbox"/> فشل تحليل الاسم لخادم POP3	An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server
تظهر هذه الرسالة عند تعذر مصافة خادم SMTP.	SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password
تظهر هذه الرسالة عند تعذر مصافة خادم POP3.	POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password

إعدادات الوظيفة

السبب	الرسائل
تظهر هذه الرسالة عند محاولة الاتصال بروتوكولات غير معتمدة.	Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number
تظهر هذه الرسالة عند حدوث عدم توافق SMTP بين الخادم وأحد العملاء أو عندما لا يدعم الخادم الاتصال الآمن لـ SMTP (اتصال SSL).	Connection to SMTP server failed. Change Secure Connection to None.
تظهر هذه الرسالة عند حدوث عدم توافق SMTP بين الخادم وأحد العملاء أو عندما يطلب الخادم استخدام اتصال SSL/TLS للاتصال الآمن بـ SMTP.	Connection to SMTP server failed. Change Secure Connection to SSL/TLS.
تظهر هذه الرسالة عند حدوث عدم توافق SMTP بين الخادم وأحد العملاء أو عندما يطلب الخادم استخدام اتصال STARTTLS للاتصال الآمن بـ SMTP.	Connection to SMTP server failed. Change Secure Connection to STARTTLS.
تظهر هذه الرسالة عندما تكون إعدادات التاريخ والوقت للطابعة غير صحيحة أو إذا انتهت صلاحية الشهادة.	The connection is untrusted. Check the following. - Date and Time
تظهر هذه الرسالة عندما لا تحتوي الطابعة على شهادة جذر تتوافق مع الخادم أو لم يتم استيراد CA Certificate.	The connection is untrusted. Check the following. - CA Certificate
تظهر هذه الرسالة عند تلف الشهادة التي تم الحصول عليها.	The connection is not secured.
تظهر هذه الرسالة عندما يحدث عدم توافق في طريقة المصادقة بين الخادم وأحد العملاء. يدعم الخادم SMTP AUTH.	SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.
تظهر هذه الرسالة عندما يحدث عدم توافق في طريقة المصادقة بين الخادم وأحد العملاء. لا يدعم الخادم خاصية SMTP AUTH.	SMTP server authentication failed. Change Authentication Method to POP before SMTP.
تظهر هذه الرسالة عندما يكون عنوان البريد الإلكتروني للمرسل المحدد خاطئ.	Sender's Email Address is incorrect. Change to the email address for your email service.
تظهر هذه الرسالة عندما تكون الطابعة مشغولة.	Cannot access the printer until processing is complete.

معلومات ذات صلة

← "التحقق من اتصال خادم البريد" في الصفحة 36

إعدادات المجلد المشترك

قم بإعداد المجلد المشترك لحفظ نتيجة المسح الضوئي.
تعمل الطابعة على كتابة البيانات على المجلد المشترك عن طريق تسجيل الدخول إلى الكمبيوتر كمستخدم.
قم بإعداد شبكة MS مع المجلد المشترك.
يمكن تحديد المجلد المشترك الذي تم إعداده هنا باعتباره وجهة للمسح الضوئي.

إنشاء مجلد مشترك

قبل إنشاء المجلد المشترك

قبل إنشاء المجلد المشترك، تحقق مما يلي.

□ اتصال الطابعة بالشبكة حيث يمكنها الوصول إلى الكمبيوتر الذي سيتم إنشاء المجلد المشترك عليه.

إعدادات الوظيفة


❑ عدم تضمين الأحرف عديدة البابت في اسم الكمبيوتر الذي سيتم إنشاء المجلد المشترك عليه.

هام!

عند تضمين حرف متعدد البابت في اسم الكمبيوتر، يُمكن أن تفشل عملية حفظ الملف إلى المجلد المشترك. وفي هذه الحالة، قم بالتغيير إلى الكمبيوتر الذي لا يتضمن حرفاً متعدد البابت في الاسم أو قم بتغيير اسم الكمبيوتر. عند تغيير اسم الكمبيوتر، احرص على التأكيد باستخدام المسؤول مسبقاً لأنه قد يؤثر على بعض الإعدادات، مثل إدارة الكمبيوتر، والوصول إلى الموارد، وما إلى ذلك.

التحقق من ملف تعريف الشبكة

على جهاز الكمبيوتر الذي سيتم إنشاء المجلد المشترك عليه، تحقق مما إذا كانت مشاركة المجلد متاحة أم لا.

1. قم بتسجيل الدخول إلى الكمبيوتر الذي سيتم إنشاء المجلد المشترك عليه بواسطة حساب مستخدم يتمتع بصلاحيات المسؤول.
2. حدد لوحة التحكم > الشبكة والإنترنت > مركز المشاركة والشبكة.
3. انقر فوق إعدادات المشاركة المتقدمة، ثم انقر فوق  بالنسبة لملف التعريف الذي يتضمن (ملف التعريف الحالي) في ملفات تعريف الشبكة المعروضة.
4. تحقق مما إذا كان تشغيل مشاركة الملفات والطابعات محدداً في مشاركة الملفات والطابعات أم لا. إذا كان محدداً بالفعل، فانقر فوق إلغاء وأغلق النافذة. عندما تقوم بتغيير الإعدادات، انقر فوق حفظ التغييرات وأغلق النافذة.

الموقع الذي يتم إنشاء المجلد المشترك به ومثال على الأمان

حسب الموقع الذي يتم إنشاء المجلد المشترك، تختلف الموافقة والأمان. لتشغيل المجلد المشترك من الطابعات أو أجهزة الكمبيوتر الأخرى، يلزم قراءة أذونات المجلد التالية وتغييرها.

❑ علامة التبويب مشاركة > مشاركة متقدمة > أذونات

يعمل على التحكم في إذن الوصول إلى الشبكة الخاصة بالمجلد المشترك.

❑ إذن الوصول الخاص بعلامة التبويب الأمان

تعمل على التحكم في إذن الوصول إلى الشبكة والوصول المحلي للمجلد المشترك.

عند تعيين الجميع للوصول إلى المجلد المشترك الذي تم إنشاؤه على سطح المكتب، كمثل على إنشاء أحد المجلدات المشتركة، سيتم السماح لجميع المستخدمين الذين يتمتعون بإمكانية الوصول إلى الكمبيوتر بالوصول إليه.

ومع ذلك، فإن المستخدم الذي لا يتمتع بالصلاحيات لن يتمكن من الوصول إليها وذلك لأن سطح المكتب (المجلد) يخضع للتحكم مجلد المستخدم، ومن ثم يتم تسليم إعدادات الأمان الخاصة بمجلد المستخدم إليه. يمكن للمستخدم المسموح له بالوصول إلى علامة التبويب الأمان (المستخدم الذي قام بتسجيل الدخول والمسؤول في هذه الحالة) تشغيل المجلد.

انظر أدناه لإنشاء الموقع المناسب.

هذا المثال عند إنشاء مجلد «مجلد_الفحص».

مثال لتكوين خوادم الملفات

هذا التوضيح هو مثال على إنشاء المجلد المشترك على جذر محرك الأقراص على الكمبيوتر المشترك، مثل خادم الملفات أسفل الشرط التالي.

يسمح الوصول للمستخدمين القابلين للتحكم بهم — مثل الشخص الذي لديه المجال نفسه لجهاز الكمبيوتر لإنشاء مجلد مشترك — بالوصول إلى المجلد المشترك.

إعدادات الوظيفة

عين هذا التكوين عندما تسمح لأي مستخدم بالقراءة والكتابة على المجلد المشترك على الكمبيوتر، مثل خادم الملفات والكمبيوتر المشترك.

مكان إنشاء المجلد المشترك: جذر محرك الأقراص

مسار المجلد: C:\مجلد_الفحص

إذن الوصول عبر الشبكة (مشاركة الأذونات): الجميع

إذن الوصول في نظام الملفات (الأمان): المستخدمون المصرح لهم

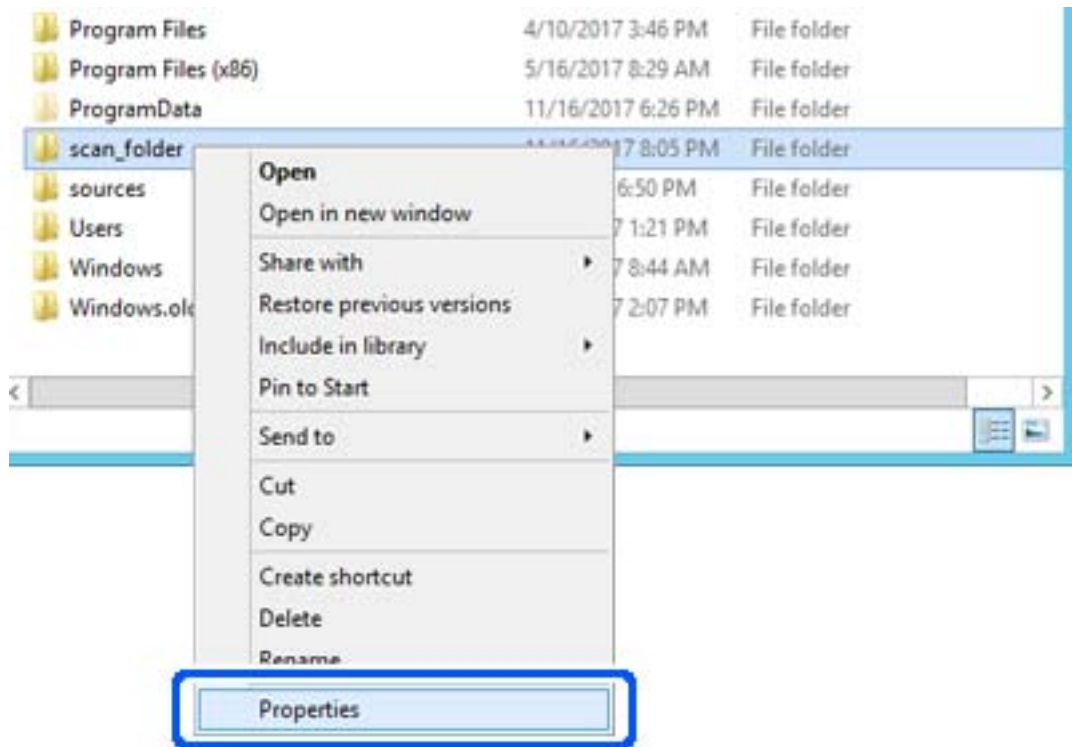
1. قم بتسجيل الدخول إلى الكمبيوتر الذي سيتم إنشاء المجلد المشترك عليه بواسطة حساب مستخدم يتمتع بصلاحيات المسؤول.

2. بدء المستكشف.

3. قم بإنشاء المجلد على جذر محرك الأقراص، ثم قم بتسميته «مجلد_الفحص».

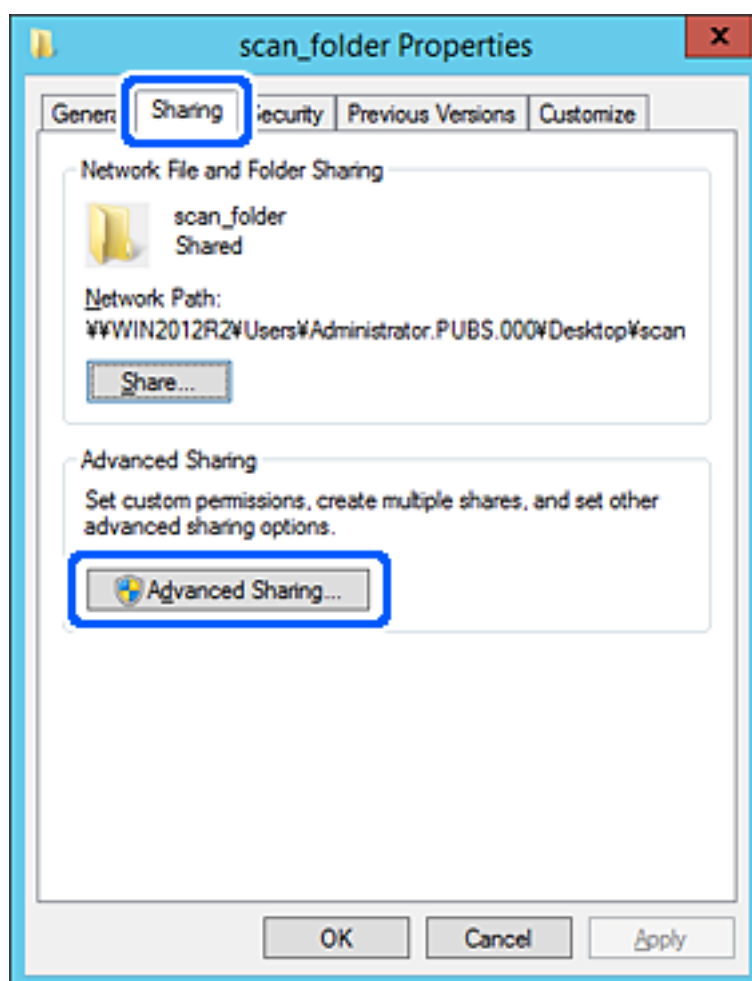
بالنسبة لاسم المجلد، أدخل ما بين 1 و12 حرفاً أبجدياً رقمياً. إذا تم تجاوز عدد الأحرف المسموح بها لاسم المجلد، فقد لا تتمكن من الوصول إليه بشكل عادي من خلال البيئة المتنوعة.

4. انقر بزر الماوس الأيمن على المجلد، ثم حدد خصائص.



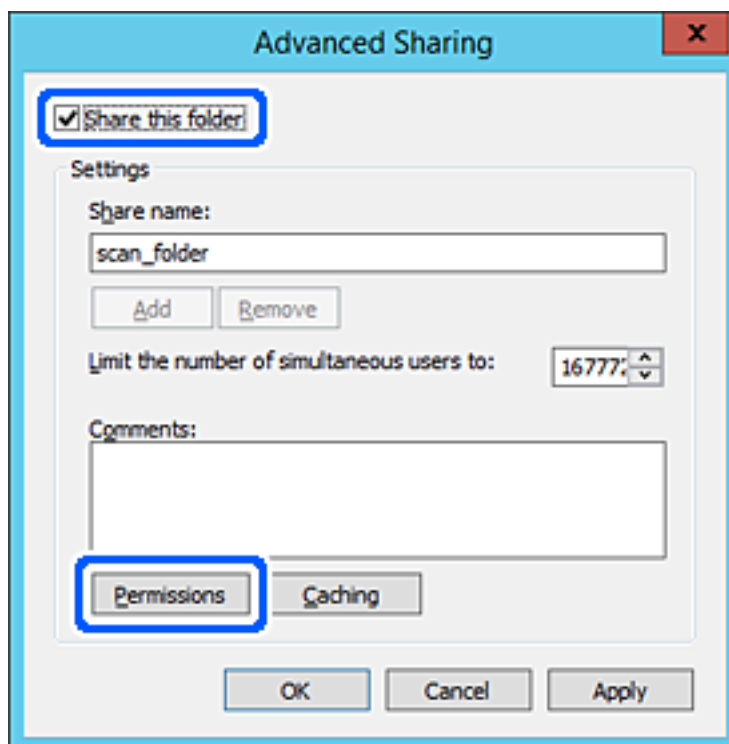
إعدادات الوظيفة

5. انقر فوق المشاركة المتقدمة من علامة التبويب مشاركة.

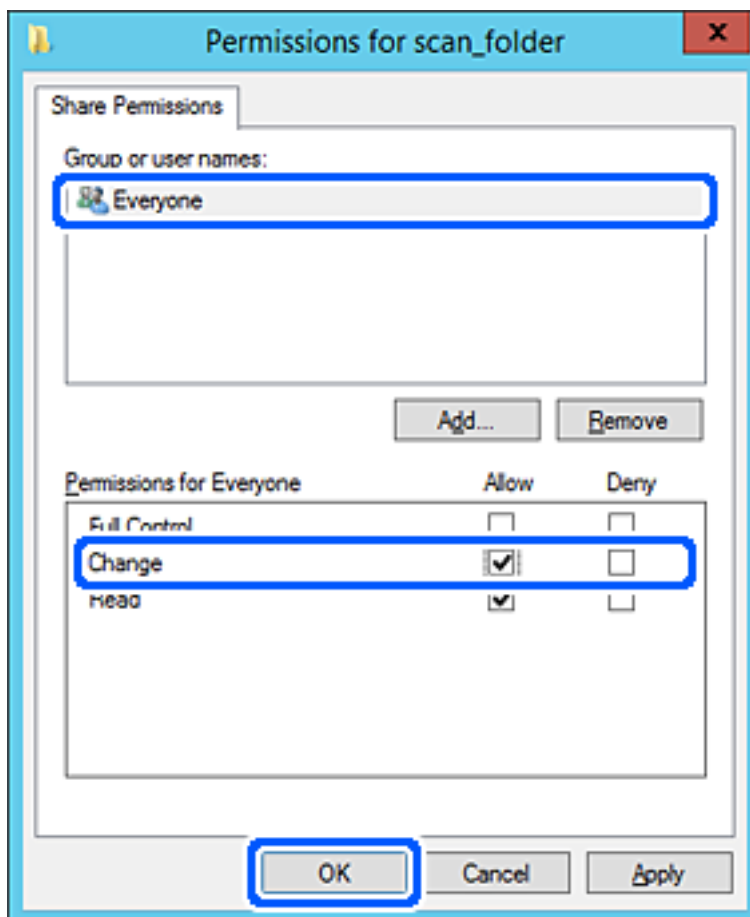


إعدادات الوظيفة

6. حدد مشاركة هذا المجلد، ثم انقر فوق الأذونات.



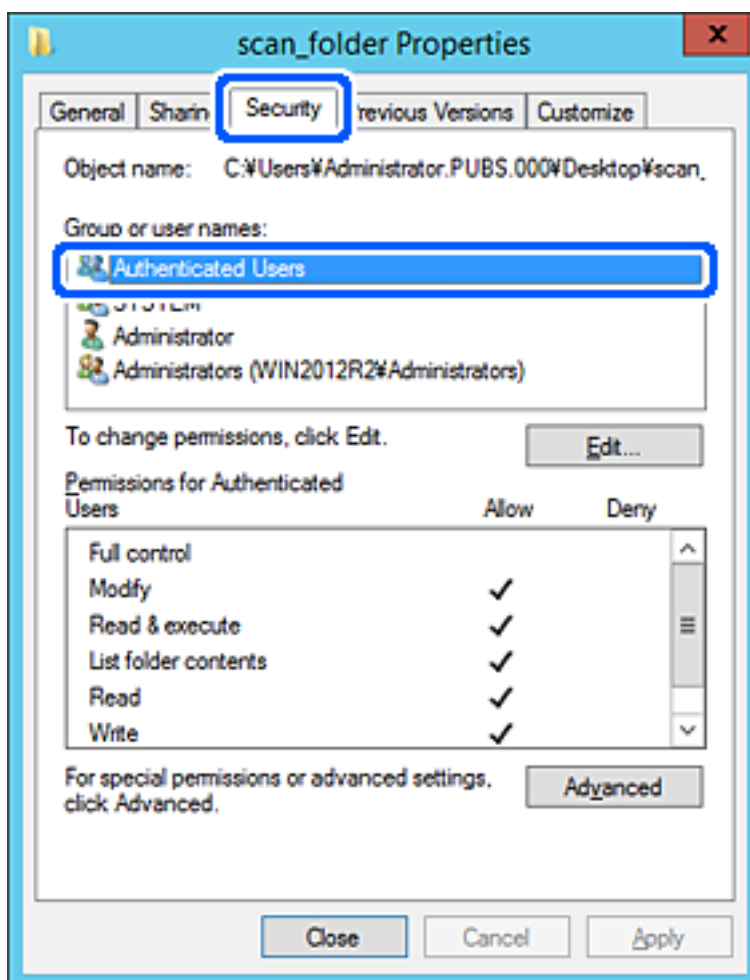
7. حدد مجموعة الجميع من أسماء المستخدمين أو المجموعات، وحدد السماح على تغيير، ثم انقر فوق موافق.



إعدادات الوظيفة

8. انقر موافق.

9. حدد علامة التبويب الأمان، ثم حدد المستخدمون المصرح لهم في أسماء المستخدمين أو المجموعات.



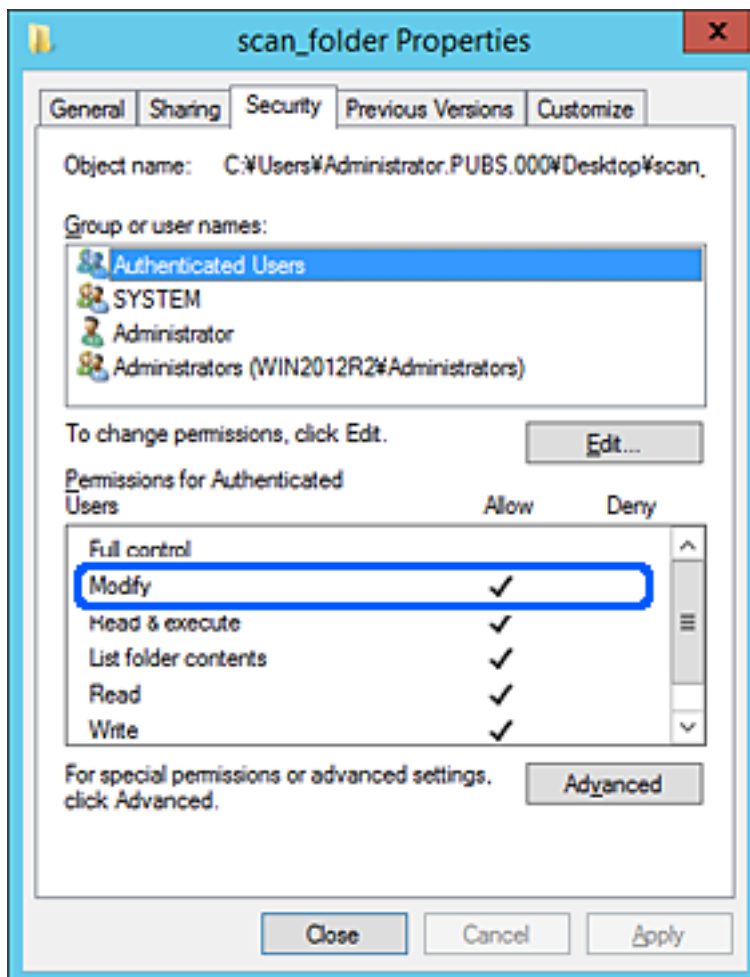
«المستخدمون المصرح لهم» هي مجموعة خاصة تتضمن جميع المستخدمين الذين يمكنهم تسجيل الدخول إلى المجال أو الكمبيوتر. يتم عرض هذه المجموعة فقط عند إنشاء المجلد أسفل مجلد الجذر.

إذا لم يتم عرضه، يمكنك إضافته من خلال النقر فوق تحرير. لمزيد من التفاصيل، تفضل بالاطلاع على «المعلومات ذات الصلة».

إعدادات الوظيفة

10. تأكد من تحديد السماح على تعديل في أذونات المستخدمين المصرح لهم.

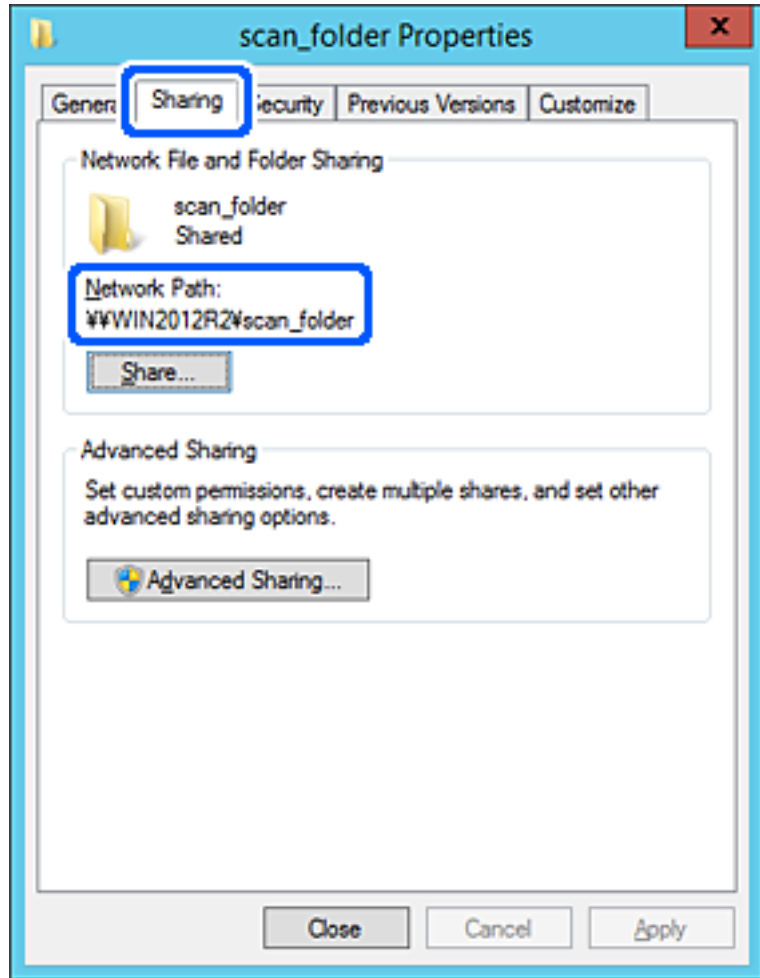
إذا لم يتم تحديدها، فحدد المستخدمون المصرح لهم، وانقر فوق تحرير، وحدد السماح على تعديل في أذونات المستخدمين المصرح لهم، ثم انقر فوق موافق.



إعدادات الوظيفة

11. حدد علامة التبويب مشاركة.

يتم عرض مسار الشبكة الخاص بالمجلد المشترك. ويُستخدم ذلك عند التسجيل بجهات اتصال الطابعة. يُرجى كتابته.



12. انقر فوق موافق أو إغلاق لإغلاق الشاشة.

تحقق مما إذا كان يمكن كتابة الملف أو قراءته على المجلد المشترك من أجهزة الكمبيوتر المتصلة بالمجال نفسه أم لا.

معلومات ذات صلة

← "إضافة مجموعة أو مستخدم يسمح بالوصول" في الصفحة 50

مثال على التهيئة لجهاز الكمبيوتر الشخصي

هذا التوضيح هو مثال لإنشاء المجلد المشترك على سطح مكتب المستخدم المسجل دخولاً حالياً إلى الكمبيوتر.

يمكن للمستخدم الذي يقوم بتسجيل الدخول إلى الكمبيوتر والذي يتمتع بصلاحيات المسؤول الوصول إلى مجلد سطح المكتب ومجلد المستند الموجودين أسفل مجلد المستخدم.

عين هذا التكوين عندما لا تسمح بالقراءة والكتابة لمستخدم آخر للمجلد المشترك على أحد أجهزة الكمبيوتر الشخصية.

مكان إنشاء المجلد المشترك: سطح المكتب

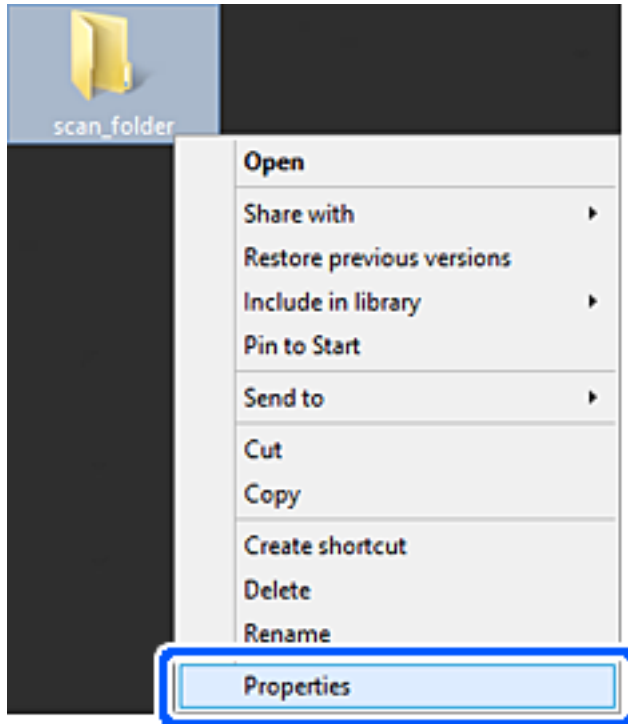
مسار المجلد: C:\Users\xxxx\Desktop\مجلد_الفحص

إذن الوصول عبر الشبكة (مشاركة الأذونات): مع الجميع

إعدادات الوظيفة

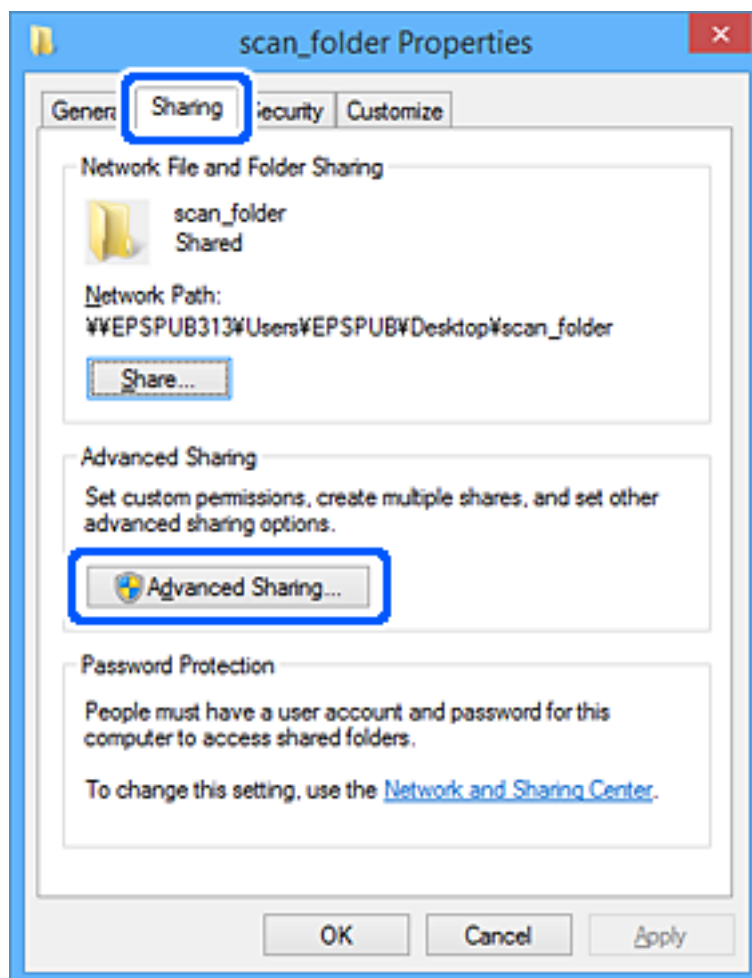
□ إذن الوصول في نظام الملفات (الأمان): أي عدم الإضافة أو إضافة أسماء المجموعة/المستخدم للسماح لهم بالوصول

1. قم بتسجيل الدخول إلى الكمبيوتر الذي سيتم إنشاء المجلد المشترك عليه بواسطة حساب مستخدم يتمتع بصلاحيات المسؤول.
 2. بدء المستكشف.
 3. قم بإنشاء المجلد على سطح المكتب، ثم قم بتسميته «مجلد_الفحص».
- بالنسبة لاسم المجلد، أدخل ما بين 1 و 12 حرفاً أبجدياً رقمياً. إذا تم تجاوز عدد الأحرف المسموح بها لاسم المجلد، فقد لا تتمكن من الوصول إليه بشكل عادي من خلال البيئة المتنوعة.
4. انقر بزر الماوس الأيمن على المجلد، ثم حدد **خصائص**.



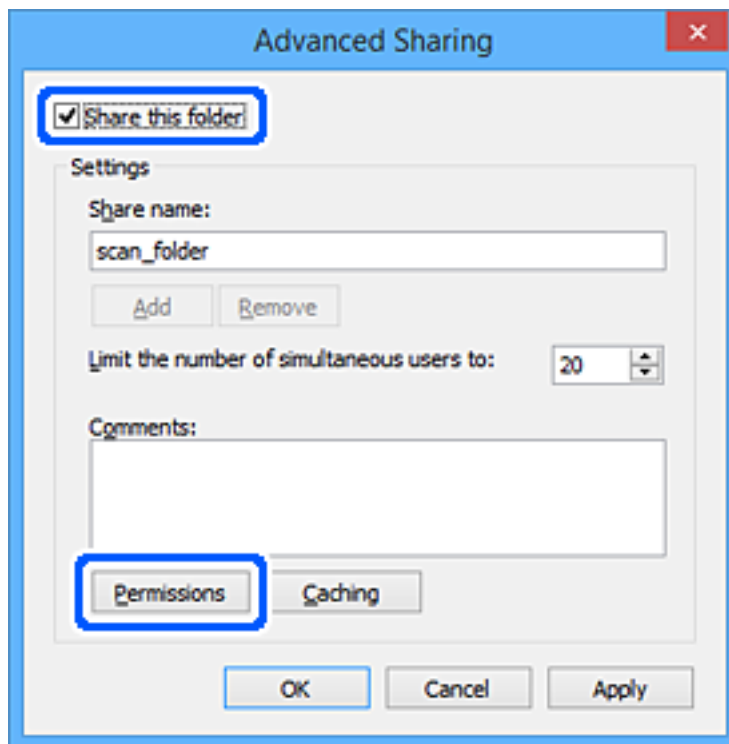
إعدادات الوظيفة

5. انقر فوق المشاركة المتقدمة من علامة التبويب مشاركة.

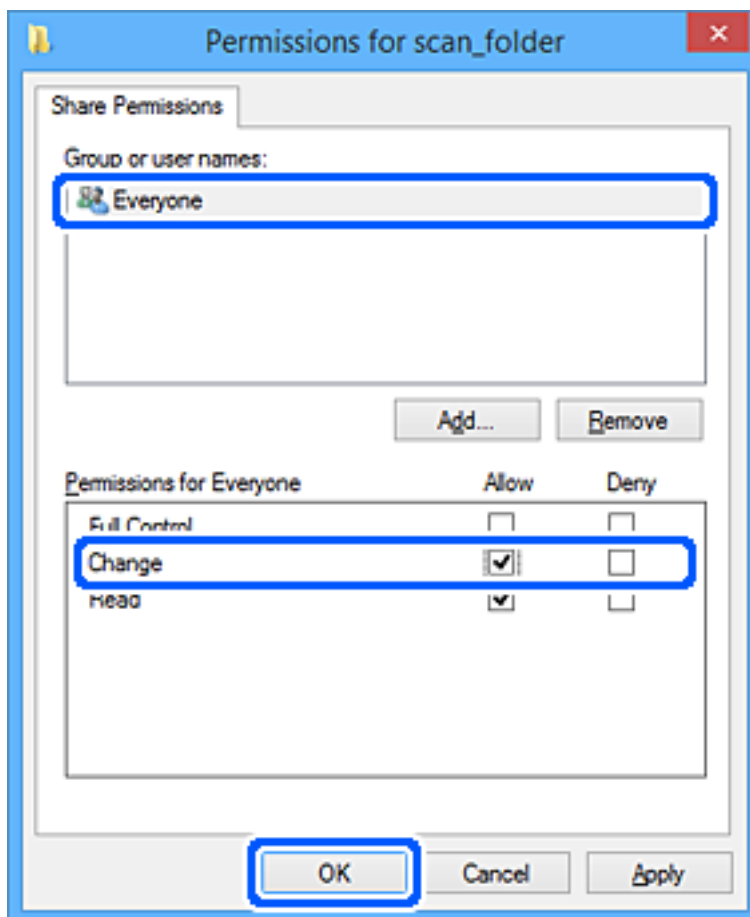


إعدادات الوظيفة

6. حدد مشاركة هذا المجلد، ثم انقر فوق الأذونات.

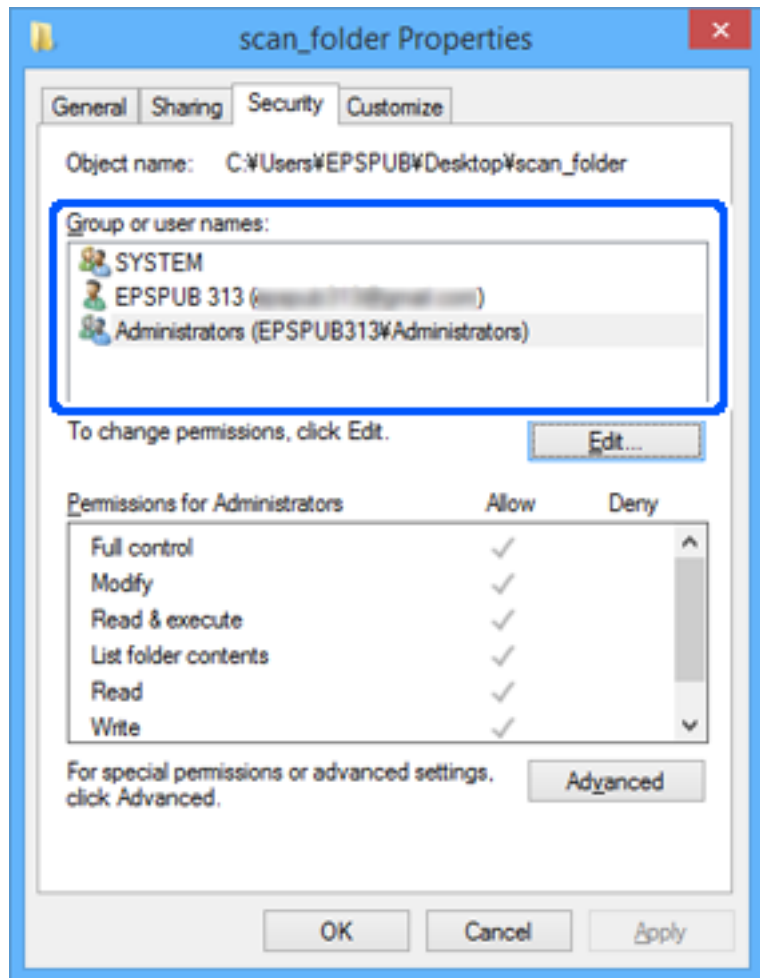


7. حدد مجموعة الجميع من أسماء المستخدمين أو المجموعات، وحدد السماح على تغيير، ثم انقر فوق موافق.



إعدادات الوظيفة

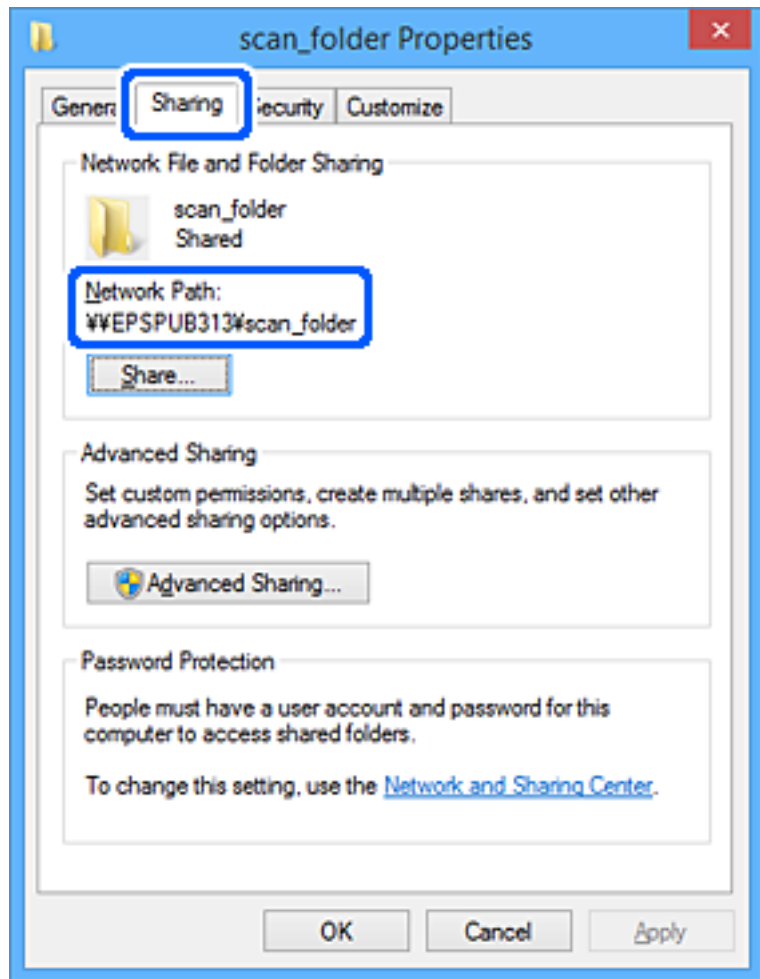
8. انقر فوق موافق.
9. حدد علامة التبويب الأمان.
10. تحقق من المجموعة أو المستخدم في أسماء المستخدمين أو المجموعات. يمكن للمجموعة أو المستخدم الذي يتم عرضه هنا الوصول إلى المجلد المشترك. في هذه الحالة، يمكن للمستخدم الذي يقوم بتسجيل الدخول إلى هذا الكمبيوتر والمسؤول الوصول إلى المجلد المشترك. أضف إذن الوصول، إذا لزم الأمر. يمكنك إضافته من خلال النقر فوق تحرير. للحصول على مزيد من التفاصيل، تفضل بالاطلاع على «المعلومات ذات الصلة».



إعدادات الوظيفة

11. حدد علامة التبويب مشاركة.

يتم عرض مسار الشبكة الخاص بالمجلد المشترك. ويُستخدم ذلك عند التسجيل في جهات اتصال الطابعة. يُرجى كتابته.



12. انقر فوق موافق أو إغلاق لإغلاق الشاشة.

تحقق مما إذا كان يمكن كتابة الملف أو قراءته على المجلد المشترك من أجهزة الكمبيوتر الخاصة بالمستخدمين أو المجموعات التي لديها إذن بالوصول أم لا.

معلومات ذات صلة

← "إضافة مجموعة أو مستخدم يسمح بالوصول" في الصفحة 50

إضافة مجموعة أو مستخدم يسمح بالوصول

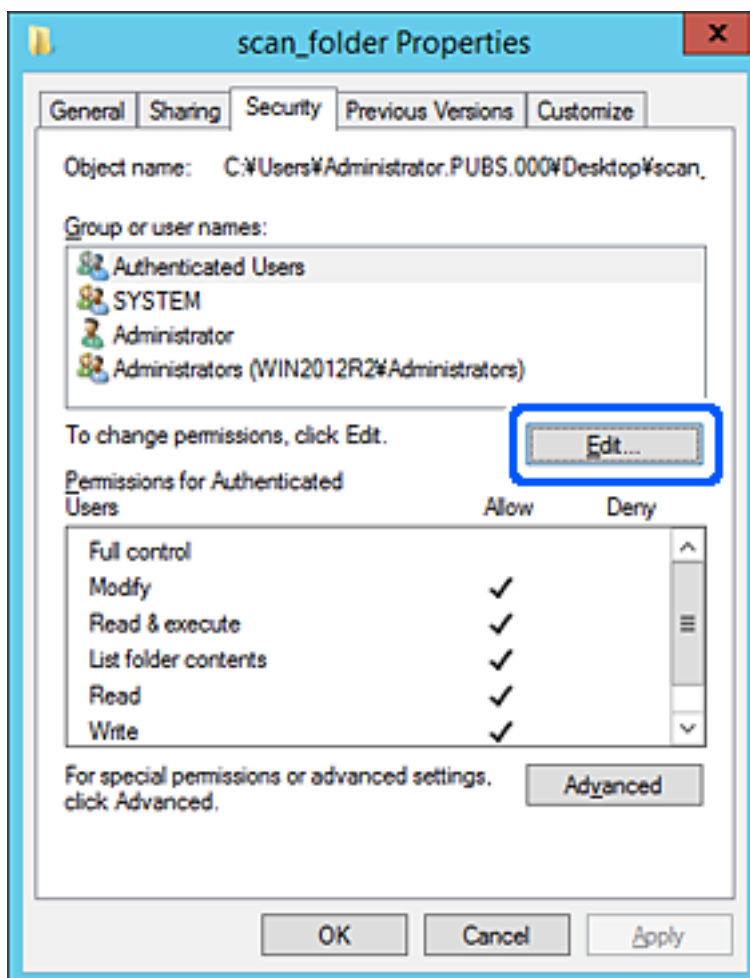
يمكنك إضافة مجموعة أو مستخدم يسمح بالوصول.

1. انقر بزر الماوس الأيمن فوق المجلد وحدد خصائص.

2. حدد علامة التبويب الأمان.

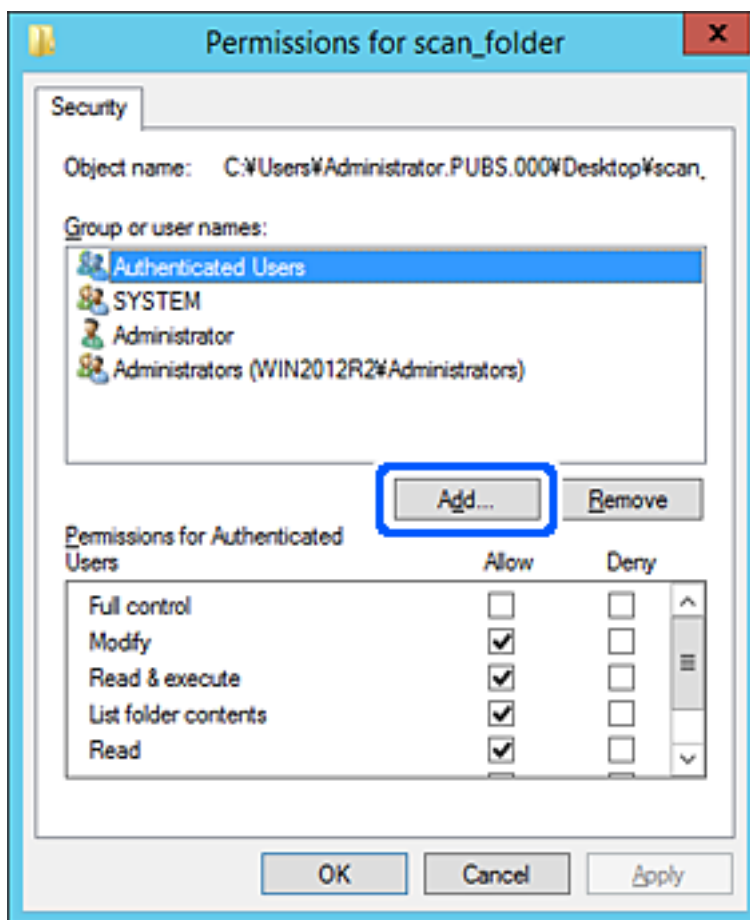
إعدادات الوظيفة

3. انقر فوق التعديل.



إعدادات الوظيفة

4. انقر على إضافة أسفل أسماء المستخدمين أو المجموعات.

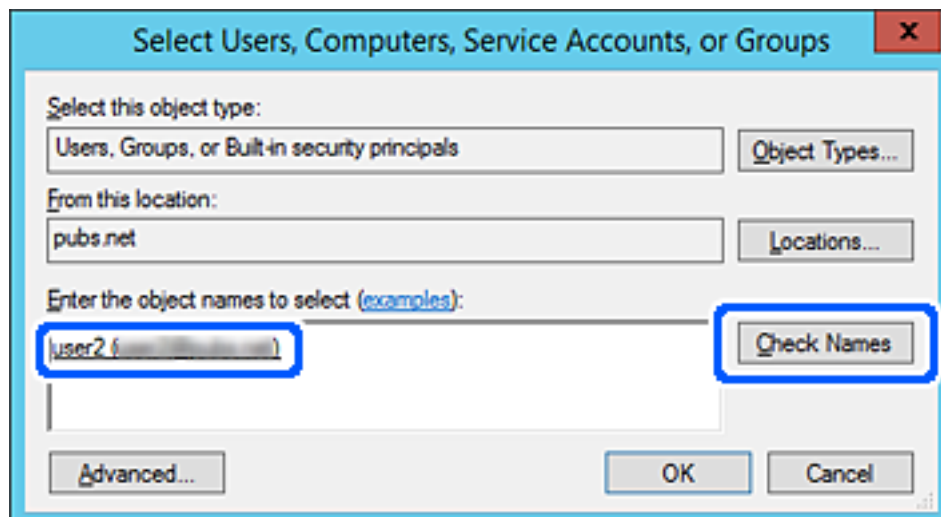


5. أدخل اسم المستخدم أو المجموعة التي ترغب في السماح بالوصول إليها، ثم انقر فوق التحقق من الأسماء. تتم إضافة خط أسفل الاسم.

ملاحظة:

إذا كنت لا تعرف الاسم الكامل للمجموعة أو المستخدم، أدخل جزءاً من الاسم، ثم انقر فوق التحقق من الأسماء. يتم سرد أسماء المجموعات أو أسماء المستخدمين التي تطابق جزء الاسم الذي أدخلته، ثم يمكنك تحديد الاسم الكامل من القائمة.

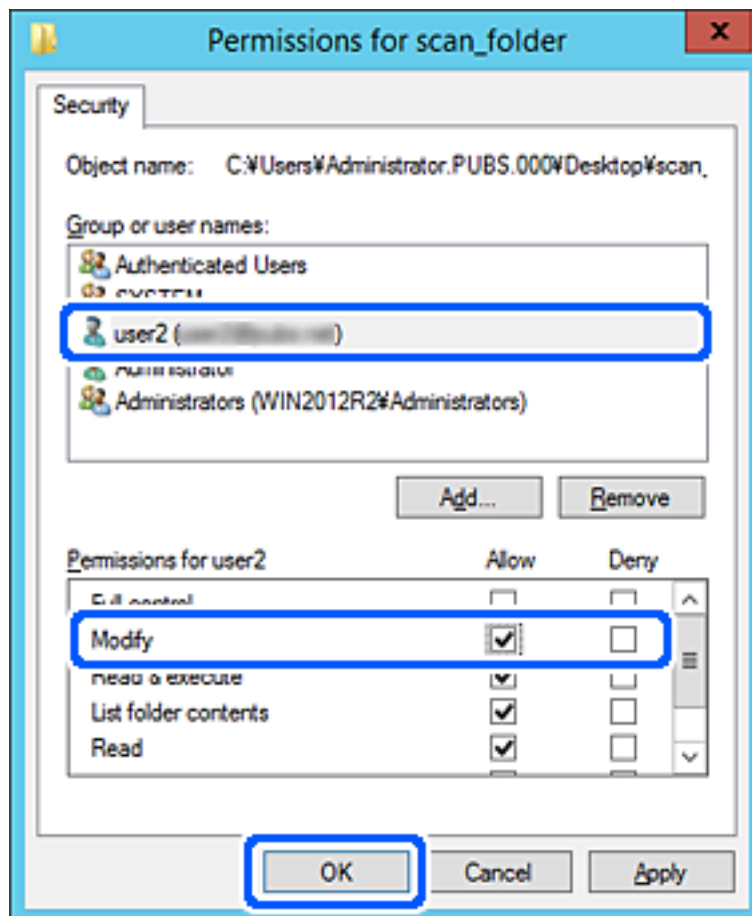
إذا تطابق اسم واحد فقط، يتم عرض الاسم الكامل مع وضع خط أسفله في أدخل اسم الكائن المطلوب تحديده.



إعدادات الوظيفة

6. انقر موافق.

7. في شاشة الإذن، حدد اسم المستخدم الذي تم إدخاله في أسماء المستخدمين أو المجموعات، وحدد إذن الوصول على تعديل، ثم انقر فوق OK.



8. انقر فوق موافق أو إغلاق لإغلاق الشاشة.

تحقق مما إذا كان يمكن كتابة الملف أو قراءته على المجلد المشترك من أجهزة الكمبيوتر الخاصة بالمستخدمين أو المجموعات التي لديها إذن بالوصول أم لا.

معلومات ذات صلة

← "استخدام جهات الاتصال" في الصفحة 54

استخدام مشاركة شبكة Microsoft

عند تمكينه، سيتوف لك ما يلي.

□ يُشارك جهاز تخزين USB عبر الشبكة المتصلة بالطابعة.

□ يُعيد توجيه نتيجة المسح الضوئي إلى المجلد المشترك على جهاز الكمبيوتر.

1. قم بالوصول إلى Web Config وحدد علامة التبويب MS Network < Network.

2. حدد Use Microsoft network sharing.

إعدادات الوظيفة

3. عين كل عنصر.
4. انقر فوق **Next**.
5. أكد الإعدادات، ثم انقر فوق **OK**.
6. أدخل ما يلي على مستكشف الكمبيوتر، ثم اضغط على مفتاح الإدخال.
تحقق من وجود مجلد شبكة وأنتك تستطيع الوصول إليه.
\\عنوان IP للطابعة
مثال: \\192.0.2.111

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

عناصر إعداد شبكة MS

العناصر	الشرح
Use Microsoft network sharing	حدده عند تمكين مشاركة شبكة MS.
Host Name	اعرض اسم مضيف شبكة MS الخاص بالطابعة. لتغيير ذلك، حدد علامة التبويب Basic < Network ، ثم قم بتغيير Device Name .
Workgroup Name	أدخل اسم مجموعة العمل الخاصة بشبكة MS. أدخل ما بين 0 إلى 15 حرفاً بتنسيق ASCII.

استخدام جهات الاتصال

ميزات إعداد الواجهة

يمكنك استخدام قائمة جهات الاتصال الخاصة بالطابعة كواجهة لميزات المسح الضوئي.

ملاحظة:

لاستخدام ميزات البريد الإلكتروني، يجب أن تقوم بتكوين خادم البريد الإلكتروني.

معلومات ذات صلة

← "تكوين جهات الاتصال" في الصفحة 54

← "تكوين خادم البريد" في الصفحة 34

تكوين جهات الاتصال

يمكن أن تتضمن قائمة جهات الاتصال الأنواع التالية من الواجهات:

 Email: وجهة البريد الإلكتروني

 FTP/Network Folder (SMB): وجهة بيانات المسح

إعدادات الوظيفة

مقارنة تكوين جهات الاتصال

توجد ثلاث أدوات لتكوين جهات اتصال الطابعة: Web Config، Epson Device Admin، ولوحة تحكم الطابعة. يتضمن الجدول أدناه الفروق بين هذه الأدوات.

لوحة تحكم الطابعة	Epson Device Admin	Web Config	الميزات
✓	✓	✓	تسجيل الوجهة
✓	✓	✓	تحرير الوجهة
✓	✓	✓	إضافة مجموعة
✓	✓	✓	تحرير مجموعة
✓	✓	✓	حذف وجهة أو مجموعات
-	✓	✓	حذف جميع الوجهات
-	✓	✓	استيراد ملف
-	✓	✓	التصدير إلى ملف
✓	✓	✓	تعيين وجهات للاستخدام المتكرر
✓	-	-	فرز الوجهات المعينة للاستخدام المتكرر

تسجيل وجهة لجهات الاتصال باستخدام Web Config

ملاحظة:

يمكنك أيضاً تسجيل جهات الاتصال على لوحة تحكم الطابعة.

1. قم بالوصول إلى Web Config وحدد علامة التبويب **Contacts < Scan/Copy**.

2. حدد العدد الذي تريد تسجيله، ثم انقر فوق **Edit**.

3. أدخل **Name** و **Index Word**.

4. حدد نوع الوجهة في خيار **Type**.

ملاحظة:

لا يمكنك تغيير خيار **Type** بعد اكتمال التسجيل. إذا أردت تغيير النوع، احذف الوجهة ثم قم بالتسجيل مرةً أخرى.

5. أدخل قيمةً لكل عنصر، ثم انقر فوق **Apply**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "عناصر إعدادات الوجهة" في الصفحة 56

← "نسخ الإعدادات احتياطياً" في الصفحة 79

إعدادات الوظيفة

عناصر إعدادات الوجهة

EPSON L3-10000P

Status Print Scan/Copy Fax Network Network Security Product Security Device Management Epson Open Platform

Send Settings

- »Basic
- »Send Stored Document Box
- »Polling Send Box
- »Board Box

Receive Settings

- »Basic
- »Fax Output
- »Conditions Output Settings
- »Fax Block Settings
- »Inbox
- »Personal Box

Report Settings

Line Settings

Security Settings

Contacts

Presets

User Default Settings

- »Fax

Contacts

Number : 2

Name : _____

Index Word : _____

Type : Fax

Assign to Frequent Use : ON OFF

Fax Number : _____

Fax Speed : Follow Communication Setting

Subaddress (SUB/SEP) : _____

Password (SIDIPWD) : _____

Apply Back

العناصر	الإعدادات والشرح
إعدادات عامة	
Name	أدخل الاسم المعروف في جهات الاتصال مع مراعاة أن يتكون 30 حرفاً أو أقل بتنسيق (Unicode UTF-8). إذا لم تحدد ذلك، فاتركه فارغاً.
Index Word	أدخل كلمات للبحث مكونة من 30 حرفاً أو أقل بتنسيق (Unicode UTF-8). إذا لم تحدد ذلك، فاتركه فارغاً.
Type	حدد نوع العنوان الذي تريد تسجيله.
Assign to Frequent Use	حدد تعيين العنوان المسجل باعتباره عنواناً يتم استخدامه بشكل متكرر. عند تعيينه باعتباره عنواناً يتم استخدامه بشكل متكرر، يُعرض على الشاشة العلوية للمسح الضوئي، ويمكنك تحديد الوجهة دون عرض جهات الاتصال.
Email	
Email Address	أدخل عدداً من الأحرف يتراوح بين حرف واحد إلى 255 حرفاً باستخدام A-Z، a-z، 0-9، و!@#\$%^&*+، -./?^_ ~.
Network Folder (SMB)	
Save to	\\مسار المجلد أدخل المكان الذي يوجد به المجلد المستهدف ما بين حرف واحد و253 حرفاً بتنسيق (Unicode UTF-8)، مع حذف "\".

إعدادات الوظيفة

العناصر	الإعدادات والشرح
User Name	أدخل اسم المستخدم للوصول إلى مجلد الشبكة بنحو 30 حرفاً أو أقل بتنسيق (UTF-8 Unicode). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1F ، 0x7F).
Password	أدخل كلمة المرور للوصول إلى مجلد الشبكة بنحو 20 حرفاً أو أقل بتنسيق (UTF-8 Unicode). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1F ، 0x7F).
FTP	
Secure Connection	حدّد FTPS للسماح للطابعة بالاتصال بالإجراءات الأمنية.
Save to	أدخل اسم الخادم ما بين حرف واحد إلى 253 حرفاً بتنسيق (ASCII 0x20-0x7E)، مع حذف "://ftp".
User Name	أدخل اسم المستخدم للوصول إلى خادم FTP بنحو 30 حرفاً أو أقل بتنسيق (UTF-8 Unicode). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1F ، 0x7F). إذا كان الخادم يسمح بالاتصالات المجهولة، فأدخل اسم المستخدم كمجهول و FTP . إذا لم تحدد ذلك، فاتركه فارغاً.
Password	أدخل كلمة مرور للوصول إلى خادم FTP حتى 20 حرفاً أو أقل بتنسيق (UTF-8 Unicode). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1F ، 0x7F). إذا لم تحدد ذلك، فاتركه فارغاً.
Connection Mode	حدد وضع الاتصال من القائمة. في حالة تحديد جدار حماية بين الطابعة وخادم FTP ، فحدد Passive Mode .
Port Number	أدخل رقم منفذ خادم FTP ما بين حرف واحد إلى 65535 حرفاً.
Certificate Validation	يتم التحقق من صحة شهادة خادم FTP عند تمكين هذا الوضع. يتوفر ذلك عند تحديد FTPS لـ Secure Connection . للإعداد، يجب استيراد CA Certificate إلى الطابعة.

معلومات ذات صلة

← "تسجيل وجهة لجهات الاتصال باستخدام Web Config" في الصفحة 55

تسجيل وجهة بمثابة مجموعة

في حالة تعيين نوع الوجهة على **Email**، يمكنك تسجيل الوجهة بمثابة مجموعة.

1. قم بالوصول إلى **Web Config** وحدد علامة التبويب **Scan/Copy < Contacts**.
2. حدد العدد الذي تريد تسجيله، ثم انقر فوق **Edit**.
3. حدد مجموعة من **Type**.
4. انقر فوق **Select** لـ **Contact(s) for Group**. يتم عرض الوجهات المتاحة.

إعدادات الوظيفة

5. حدد الوجهة التي ترغب في تسجيلها في مجموعة، ثم انقر فوق **Select**.

EPSON L8-10000P

Status Print Scan/Copy **Fax** Network Network Security Product Security Device Management Epson Open Platform

Send Settings

- »Basic
- »Send Stored Document Box
- »Polling Send Box
- »Board Box

Receive Settings

- »Basic
- »Fax Output
- »Conditions Output Settings
- »Fax Block Settings
- »Inbox
- »Personal Box

Report Settings

Line Settings

Security Settings

Contacts

Presets

User Default Settings

- »Fax

Contacts

Check the entries you want to register for group.
If you finish selecting entries, back to the Edit a Contact Page by pressing "Select" button.
To reflect the settings, press "Apply" button on the Edit a Contact Page.

< 1 >

	Number	Name	Index Word	Type	Destination
<input type="checkbox"/>	6	AAAA Corp.	AAAA	Email	aaa@XXXX.com

Select **Cancel**

6. أدخل **Name** و **Index Word**.

7. حدد سواء كنت قمت بتعيين المجموعة المسجلة إلى المجموعة المستخدمة بشكل متكرر أم لا.

ملاحظة:

يمكن تسجيل الوجهات لمجموعات متعددة.

8. انقر فوق **Apply**.

معلومات ذات صلة

◀ "الوصول إلى تطبيق Web Config" في الصفحة 27

◀ "نسخ الإعدادات احتياطياً" في الصفحة 79

النسخ الاحتياطي لجهات الاتصال واستردادها

باستخدام Web Config أو الأدوات الأخرى، يُمكنك إجراء عملية النسخ الاحتياطي لجهات الاتصال واستردادها.

بالنسبة لـ Web Config، يُمكنك إجراء النسخ الاحتياطي لجهات الاتصال من خلال تصدير إعدادات الطابعة التي تتضمن جهات الاتصال. لا يُمكن تحرير الملف المصدر لأنه يتم تصديره باعتباره ملف ثنائي.

عند استيراد إعدادات الطابعة إلى الطابعة، سيتم استبدال جهات الاتصال.

بالنسبة لـ Epson Device Admin، يُمكن تصدير جهات الاتصال فقط من شاشة خصائص الجهاز. بالإضافة إلى ذلك، إذا لم تقم بتصدير العناصر المتعلقة بالأمان، يُمكنك تحرير جهات الاتصال التي تم تصديرها واستيرادها لأنه يُمكن حفظها باعتبارها ملف SYLK أو ملف CSV.

استخدام وظائف المسح الضوئي

يُمكنك استخدام وظائف المسح الضوئي باستخدام لوحة تحكم الطابعة.

المسح الضوئي باستخدام لوحة التحكم

يتم إجراء المسح الضوئي لوظيفة مجلد الشبكة والمسح الضوئي لوظيفة البريد باستخدام لوحة تحكم الطابعة، بالإضافة إلى نقل نتائج المسح الضوئي إلى البريد، والمجلدات، وما إلى ذلك عن طريق تنفيذ إحدى المهام من الكمبيوتر.

معلومات ذات صلة

← "إعدادات الخوادم والمجلدات" في الصفحة 59

إعدادات الخوادم والمجلدات

الاسم	الإعدادات	الموقع	المتطلبات
المسح الضوئي إلى مجلد الشبكة (SMB)	إنشاء مشاركة مجلد الحفظ وإعداده	كمبيوتر يحتوي على موقع مجلد الحفظ	حساب المستخدم الإداري في الكمبيوتر الذي يقوم بإنشاء مجلدات الحفظ.
وجهة المسح الضوئي في مجلد الشبكة (SMB)	وجهة المسح الضوئي في مجلد الشبكة (SMB)	جهات اتصال الجهاز	اسم مستخدم وكلمة مرور لتسجيل الدخول للكمبيوتر الذي يحتوي على مجلد حفظ، وميزة تحديثه.
المسح الضوئي إلى مجلد الشبكة (FTP)	إعداد تسجيل الدخول لخادم FTP	جهات اتصال الجهاز	معلومات تسجيل الدخول لخادم الحفظ. وميزة تحديث مجلد الحفظ.
المسح الضوئي إلى البريد الإلكتروني	الإعداد الخاص بخادم البريد الإلكتروني	الجهاز	معلومات إعداد خادم البريد الإلكتروني

معلومات ذات صلة

← "تكوين خادم البريد" في الصفحة 34

ضبط إعدادات النظام

إعداد لوحة التحكم

إعداد لوحة تحكم الطابعة. يمكنك ضبط الإعدادات على النحو التالي.

1. ادخل إلى Web Config وحدد علامة التبويب **Control Panel < Device Management**.

2. اضبط العناصر التالية حسب الضرورة.

Language

حدد اللغة المعروضة على لوحة التحكم.

إعدادات الوظيفة

Panel Lock

إذا حددت **ON**، فلن تتمكن من تحديد العناصر التي تطلب صلاحية المسؤول. لتحديدها، قم بتسجيل الدخول إلى الطابعة كمسؤول. إذا لم يتم تعيين كلمة مرور المسؤول، فسيتم تعطيل قفل اللوحة.

Operation Timeout

إذا حددت **ON**، عند تسجيل دخولك بصفتك مستخدم التحكم في الوصول أو مسؤول، فسيتم تسجيل خروجك تلقائياً والانتقال إلى الشاشة الأولية إذا لم توجد أي مهام قيد التشغيل لفترة معينة من الوقت. يمكنك تعيين فترة تتراوح بين 10 ثوانٍ حتى 240 دقيقة بحساب الثواني.

ملاحظة:

يُمكنك أيضاً الإعداد من لوحة تحكم الطابعة.

Language : الإعدادات < إعدادات عامة < الإعدادات الأساسية < اللغة/Language Panel Lock : الإعدادات < إعدادات عامة < إدارة النظام < إعدادات الأمان < إعدادات المسؤول < إعداد القفل

انتهى وقت العملية : الإعدادات < إعدادات عامة < الإعدادات الأساسية < انتهى وقت العملية (يُمكن تحديد تشغيل أو إيقاف التشغيل).

3. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

إعدادات توفير الطاقة أثناء فترة الخمول

يمكنك إعداد الوقت للتحويل إلى وضع توفير الطاقة أو لإيقاف تشغيل الطاقة عند عدم تشغيل لوحة تحكم الطابعة لفترة زمنية معينة. عين الوقت حسب بيئة الاستخدام.

1. ادخل إلى Web Config وحدد علامة التبويب **Power Saving < Device Management**.

2. ادخل فترة **Sleep Timer** للانتقال إلى وضع توفير الطاقة عندما يكون الجهاز في فترة الخمول.

ملاحظة:

يُمكنك أيضاً الإعداد من لوحة تحكم الطابعة.

الإعدادات < إعدادات عامة < الإعدادات الأساسية < مؤقت النوم

3. حدد مدة إيقاف التشغيل لـ **Power Off Timer**.

ملاحظة:

يُمكنك أيضاً الإعداد من لوحة تحكم الطابعة.

الإعدادات < إعدادات عامة < الإعدادات الأساسية < مؤقت إيقاف الطاقة

4. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

مزمنة التاريخ والوقت مع خادم الوقت

عند إجراء المزمنة مع خادم الوقت (خادم NTP)، يمكنك مزمنة وقت الطابعة والكمبيوتر على الشبكة. يمكن تشغيل خادم الوقت داخل المؤسسة أو نشره على الإنترنت.

إعدادات الوظيفة

- عند استخدام شهادة المرجع المصدق (CA)، يمكن منع المشكلات المتعلقة بالوقت من خلال المزامنة مع خادم الوقت.
1. ادخل إلى Web Config وحدد علامة التبويب **Time Server < Date and Time < Device Management**.
 2. حدد **Use Time Server**.
 3. أدخل عنوان خادم الوقت لـ **Time Server Address**. يمكنك استخدام تنسيق IPv4، أو IPv6، أو FQDN. أدخل حرفاً أو أقل. إذا لم تحدد ذلك، فاتركه فارغاً.
 4. أدخل **Update Interval (min)**. يمكنك تعيين فترة تصل إلى 10080 دقيقة بحساب الدقائق.
 5. انقر فوق **OK**.
- ملاحظة:
يمكنك تأكيد حالة الاتصال بخادم الوقت على **Time Server Status**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

إعداد القيمة الافتراضية للمسح الضوئي والنسخ (إعدادات المستخدم الافتراضية)

- يمكنك تعيين القيمة الافتراضية للوظائف.
- يمكنك تعيين الوظائف التالية.
- Scan to Network Folder/FTP
- Scan to Email
- Scan to Memory Device
- Copy
1. ادخل إلى Web Config وحدد الوظائف التي ترغب في تعيين القيم الافتراضية لها لعلامة التبويب **Scan/Copy < User Default Settings**.
 2. عين كل عنصر.
 3. انقر فوق **OK**.
- إذا كان مجموعة القيم غير صالحة، فسيتم تعديلها تلقائياً، ثم يتم تعيين قيمة صالحة.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

AirPrint Setup

- قم بالضبط عند استخدام الطباعة عبر AirPrint.
- ادخل إلى Web Config وحدد علامة التبويب **AirPrint Setup < Network**.

إعدادات الوظيفة

العناصر	الشرح
Bonjour Service Name	أدخل اسم خدمة Bonjour بين 1 إلى 41 حرفاً بتنسيق (0x20-0x7E ASCII).
Bonjour Location	أدخل معلومات الموقع مثل موضع الطابعة ضمن 127 بايت أو أقل بتنسيق (UTF-8 Unicode).
Geolocation Latitude and Longitude (WGS84)	أدخل معلومات موقع الطابعة. هذا الإدخال اختياري. أدخل القيم باستخدام معطى WGS-84، والذي يفصل بين خط العرض وخط الطول بفاصلة. يُمكن إدخال من -90 إلى +90 بالنسبة لقيمة خط العرض، وما بين -180 إلى +180 بالنسبة لقيمة خط الطول. يُمكنك إدخال قيمة أقل من رقم له ست خانوات عشرية، ويُمكنك حذف "+".
Top Priority Protocol	حدد بروتوكول الأولوية القصوى من IPP وPort9100.
Wide-Area Bonjour	عين ما إذا كان يتم استخدام Bonjour واسم النطاق أم لا. إذا كنت تستخدمه، فيجب أن تكون الطابعات مسجلة على خادم DNS لتكون قادراً على البحث في الطابعة على المقطع.
iBeacon Transmission	حدد إما تمكين وظيفة إرسال iBeacon أو تعطيلها. عند تمكينها، يمكنك البحث عن الطابعة من الأجهزة التي تدعم iBeacon.
Enable AirPrint	تم تمكين IPP، و Bonjour، و AirPrint، وتم تأسيس IPP فقط باستخدام الاتصال الآمن.

إعدادات سلامة المنتج

يوضح هذا الفصل إعدادات الأمان للجهاز.

مقدمة حول ميزات أمان المنتج

يقدم هذا القسم وظيفة أمان أجهزة Epson.

اسم الميزة	نوع الميزة	ما يجب تعيينه	ما يتم حظره
إعداد كلمة مرور المسؤول	يقفل إعدادات النظام، مثل إعداد اتصال الشبكة أو USB والإعدادات الافتراضية للمستخدم.	يعين أحد المسؤولين كلمة مرور للجهاز. يمكنك الضبط أو التغيير من خلال كل من Web Config ولوحة تحكم الطابعة.	يتم حظر قراءة المعلومات المخزنة في الجهاز وتغييرها مثل المعرف، وكلمة المرور، وإعدادات الشبكة، وجهات الاتصال بصورة غير قانونية. يتم أيضاً الحد من مجموعة كبيرة من المخاطر الأمنية مثل تسرب المعلومات المتعلقة ببيئة الشبكة أو سياسة الأمان.
إعداد التحكم في الوصول	تعمل على الحد من الوظائف التي يمكن استخدامها على الأجهزة، مثل الطابعة، والمسح الضوئي، وإرسال نسخة لكل مستخدم. إذا قمت بتسجيل الدخول باستخدام حساب مستخدم مسجل مقدماً، فسيتم السماح لك باستخدام بعض الوظائف المحددة. وبالإضافة إلى ذلك، بعد تسجيل الدخول من لوحة التحكم، سيتم تسجيل خروجك تلقائياً إذا لم يتم إجراء أي نشاط لفترة محددة من الوقت.	سجل أي حساب مستخدم، ثم حدد الوظيفة التي ترغب في السماح لك باستخدامها، مثل النسخ والمسح الضوئي. يمكنك تسجيل ما يصل إلى 10 حسابات مستخدم.	يمكن الحد من مخاطر تسرب البيانات وعرضها بصورة غير مشروعة عن طريق تقليل عدد الوظائف وفقاً للمحتوى التجاري ودور المستخدم.
إعداد للواجهة الخارجية	تتحكم في الواجهة، مثل منفذ USB المتصل بالجهاز.	قم بتمكين منفذ USB أو تعطيله لتوصيل الأجهزة الخارجية مثل ذاكرة USB واتصال USB بالكمبيوتر.	<input type="checkbox"/> التحكم في منفذ USB: يقلل من إمكانية أخذ البيانات عبر المسح الضوئي غير المشروع للمستندات السرية. <input type="checkbox"/> اتصال USB بجهاز الكمبيوتر: يعمل ذلك على منع الاستخدام غير المصرح به للجهاز عن طريق حظر الطابعة دون المرور عبر الشبكة.

معلومات ذات صلة

- ← "حول تهيئة الويب" في الصفحة 26
- ← "EpsonNet Config" في الصفحة 100
- ← "تكوين كلمة مرور المسؤول" في الصفحة 64
- ← "تقييد الميزات المتوفرة" في الصفحة 71
- ← "تعطيل الواجهة الخارجية" في الصفحة 72

تكوين كلمة مرور المسؤول

عندما تضبط كلمة مرور المسؤول، يُمكنك منع المستخدمين من تغيير إعدادات إدارة النظام. يُمكنك تعيين كلمة مرور المسؤول وتغييرها باستخدام إما Web Config، وإما لوحة تحكم الطابعة، وإما البرنامج (Epson Device Admin). عند استخدام البرنامج، راجع المستند المتعلق بكل برنامج.

معلومات ذات صلة

- ◀ "تكوين كلمة مرور المسؤول من لوحة التحكم" في الصفحة 64
- ◀ "تكوين كلمة مرور المسؤول باستخدام Web Config" في الصفحة 64
- ◀ "Epson Device Admin" في الصفحة 100

تكوين كلمة مرور المسؤول من لوحة التحكم

يُمكنك تعيين كلمة مرور المسؤول من لوحة تحكم الطابعة.

1. حدد الإعدادات في لوحة تحكم الطابعة.
 2. حدد إعدادات عامة > إدارة النظام > إعدادات الأمان.
 3. حدد إعدادات المسؤول.
 4. حدد كلمة مرور المسؤول > تسجيل.
 5. أدخل كلمة المرور الجديدة.
 6. أعد إدخال كلمة المرور.
 7. أغلق شاشة التأكيد.
- يتم عرض شاشة إعدادات المسؤول.

ملاحظة:

يُمكنك تغيير كلمة مرور المسؤول أو حذفها عند تحديد تغيير أو إعادة تعيين على شاشة كلمة مرور المسؤول وإدخال كلمة مرور المسؤول.

تكوين كلمة مرور المسؤول باستخدام Web Config

يُمكنك تعيين كلمة مرور المسؤول باستخدام Web Config.

1. ادخل إلى Web Config وحدد علامة التبويب **Change Administrator Password < Product Security**.

إعدادات سلامة المنتج

2. أدخل كلمة مرور لإعداد **New Password** و **Confirm New Password**. أدخل اسم المستخدم عند الضرورة. إذا كنت ترغب في تغيير كلمة المرور إلى أخرى جديدة، فأدخل كلمة المرور الحالية.

3. حدد **OK**.

ملاحظة:

- لتعيين عناصر القائمة المغلقة أو تغييرها، انقر فوق **Log in**، ثم أدخل كلمة مرور المسؤول.
- لحذف كلمة مرور المسؤول، انقر فوق علامة التبويب **Delete Administrator Password < Product Security**، ثم أدخل كلمة مرور المسؤول.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

التحكم في تشغيل اللوحة


إذا قمت بتعيين كلمة مرور المسؤول وتمكين إعداد القفل، يمكنك قفل العناصر المتعلقة بإعدادات نظام الطابعة بحيث لا يمكن للمستخدمين تغييرها.

تمكين إعداد القفل

قم بتمكين إعداد القفل للطابعة الذي تم تعيين كلمة مرور لها. حدد كلمة مرور المسؤول أولاً.

إعدادات سلامة المنتج

تمكين إعداد القفل من لوحة التحكم

1. حدد الإعدادات في لوحة تحكم الطابعة.
2. حدد إعدادات عامة < إدارة النظام < إعدادات الأمان.
3. حدد إعدادات المسؤول.
4. حدد شغل في إعداد القفل.
5. حدد نعم على شاشة التأكيد.
6. حدد .

تحقق من عرض  على الشاشة الرئيسية.

تمكين إعداد القفل من تكوين الويب

1. قم بالوصول إلى Web Config وانقر فوق Log in.
2. أدخل اسم المستخدم وكلمة مروره، ثم انقر فوق OK.
3. حدد علامة التبويب Control Panel < Device Management.
4. في Panel Lock، حدد ON.
5. انقر فوق OK.
6. تحقق من عرض  على الشاشة الرئيسية على لوحة تحكم الطابعة.

عناصر إعداد القفل المخصصة لقائمة إعدادات عامة

هذه قائمة عناصر إعداد القفل الموجودة في الإعدادات < إعدادات عامة في لوحة التحكم. يمكن تعيين بعض الوظائف بحيث يتم تمكينها أو تعطيلها على حدة.

Panel Lock	قائمة إعدادات عامة
-	الإعدادات الأساسية

إعدادات سلامة المنتج

Panel Lock	قائمة إعدادات عامة
-	سطوع LCD
-	الصوت
✓	موقت النوم
✓	مؤقت إيقاف الطاقة
✓	Circuit Breaker Interlock Startup
✓	إعدادات التاريخ/الوقت
1+ ✓	اللغة/Language
✓	انتهى وقت العملية
-	لوحة المفاتيح
-	Length Unit
-	إعدادات الطابعة
-	إعدادات مصدر الورق
-	Custom Paper Setting
✓	لغة الطابعة
✓	إعدادات الطباعة العامة
✓	HP-GL/2 Unique Settings
✓	واجهة جهاز الذاكرة
1+ ✓	ورق سميك
✓	Self Check and Cleaning
-	ثنائي الاتجاه
✓	الاتصال بكمبيوتر عبر USB
✓	إعداد مهلة USB I/F
✓	إعدادات الشبكة

إعدادات سلامة المنتج

Panel Lock	قائمة إعدادات عامة		
✓	إعدادات Wi-Fi		
✓	إعداد شبكة LAN السلكية		
✓	حالة الشبكة		
2+ ✓	وضع LAN/Wi-Fi السلكي		
2+ ✓	حالة Wi-Fi Direct		
2+ ✓	حالة خادم البريد الإلكتروني		
2+ ✓	ورقة حالة الطباعة		
3+ ✓	التحقق من الاتصال		
✓	متقدم		
✓	اسم الجهاز		
✓	TCP/IP		
✓	الخادم الوكيل		
✓	خادم البريد الإلكتروني		
✓	Shared Folder		
✓	عنوان IPv6		
✓	سرعة الارتباط والازدواج		
✓	إعادة توجيه HTTP إلى HTTPS		
✓	تعطيل تصفية IPsec/IP		
✓	تعطيل IEEE802.1X		
✓	الإرسال عبر iBeacon		
✓	إعدادات مسح ضوئي		
✓	تأكيد المستلم		
✓	خادم البريد الإلكتروني		
✓	Scan Options		
✓	إدارة النظام		

إعدادات سلامة المنتج


Panel Lock	قائمة إعدادات عامة	
✓	مدير جهات الاتصال	
4* ✓, 1*	تسجيل/حذف	
4* ✓	الأكثر استخداماً	
✓	طباعة جهات الاتصال	
4* ✓	عرض الخيارات	
4* ✓	خيارات البحث	
✓	إعدادات الأمان	
✓	القيود	
✓	التحكم في الوصول	
✓	إعدادات المسؤول	
✓	كلمة مرور المسؤول	
✓	إعداد القفل	
✓	استعادة الإعدادات الافتراضية	
✓	تحديث البرامج الثابتة	

✓ = يجب أن تُقفل.

- = يجب ألا تُقفل.

1* : يمكنك تمكين القفل أو تعطيله من إعدادات عامة < إدارة النظام < إعدادات الأمان < القيود.

2* : على الرغم من أنه يمكن قفل العناصر الموجودة بالمستوى العلوي بواسطة قفل المسؤول، فلا يزال بإمكانك الوصول إليها من خلال القائمة التي تحمل الاسم نفسه الخاصة بـ الإعدادات < حالة الطابعة/طباعة.

3* : على الرغم من أنه يمكن قفل العناصر الموجودة بالمستوى العلوي بواسطة قفل المسؤول، فلا يزال بإمكانك الوصول إليها من الصفحة الرئيسية <  < الوصف < عند تعذر الاتصال بالشبكة.

4* : على الرغم من أنه يمكن قفل العناصر الموجودة بالمستوى العلوي بواسطة قفل المسؤول، فلا يزال بإمكانك الوصول إليها من خلال القائمة التي تحمل الاسم نفسه الخاصة بـ الإعدادات < مدير جهات الاتصال.

معلومات ذات صلة

← "العناصر التي يمكن تعيينها على حدة" في الصفحة 70

عناصر إعداد القفل الأخرى

إلى جانب قائمة إعدادات عامة، سيتم تمكين إعداد القفل على العناصر التالية.

إعدادات سلامة المنتج

- تعيين مسبق
- إضافة جديد
- حذف
- إعادة تسمية
- تغيير إعدادات المستخدم

شاشة العرض وإعداد الوظيفة بشكل فردي

بالنسبة للعناصر المستهدفة ل إعداد القفل، يمكنك تعيين ما إذا كان يتم تمكينها أو تعطيلها بشكل فردي. يمكنك تعيين كل توفر للمستخدم عند الضرورة، مثل تسجيل جهات الاتصال أو تغييرها، وعرض سجل المهام، وما إلى ذلك.

1. حدد الإعدادات في لوحة تحكم الطابعة.
2. حدد إعدادات عامة < إدارة النظام > إعدادات الأمان.
3. حدد القيود.
4. حدد العنصر الخاص بالوظيفة التي تريد تغيير إعدادها، ثم قم بتعيين شغل أو إيقاف.

العناصر التي يمكن تعيينها على حدة

يمكن للمسؤول السماح بعرض العناصر أدناه وتغيير الإعدادات على حدة.

- الوصول لتسجيل/حذف جهات الاتصال: الإعدادات < مدير جهات الاتصال > تسجيل/حذف
تحكم في تسجيل جهات الاتصال وتغييرها. حدد شغل لتسجيل جهات الاتصال أو تغييرها.
- الوصول إلى آخر مسح ضوئي إلى البريد الإلكتروني: مسح < البريد الإلكتروني > المستلم < محفوظات
تحكم في عرض السجل الخاص بوظيفة المسح الضوئي إلى البريد. حدد شغل لعرض السجل.
- الوصول إلى إظهار سجل الإرسال في مسح ضوئي إلى البريد الإلكتروني: مسح < البريد الإلكتروني > القائمة < إظهار سجل الإرسال
تحكم في عرض سجل إرسال البريد الإلكتروني الخاص بوظيفة المسح الضوئي إلى البريد. حدد شغل لعرض سجل إرسال البريد الإلكتروني.
- الوصول إلى اللغة: الإعدادات < اللغة/ Language
تحكم في تغيير اللغة المعروضة في لوحة التحكم. حدد شغل لتغيير اللغات.
- الوصول إلى ورق سميك: الإعدادات < إعدادات عامة > إعدادات الطابعة < ورق سميك
تحكم في تغيير إعدادات وظيفة ورق سميك. حدد شغل لتغيير الإعدادات.
- حماية البيانات الشخصية:
تحكم في عرض معلومات الوجهة في تسجيل الطلب السريع. حدد شغل لعرض الوجهة على أنها (***) .

معلومات ذات صلة

← عناصر إعداد القفل الأخرى" في الصفحة 69

تقييد الميزات المتوفرة

يمكنك تسجيل حسابات المستخدمين على الطابعة وربطها بالوظائف ووظائف التحكم التي يمكن للمستخدمين استخدامها. عند تمكين التحكم في الوصول، يمكن للمستخدم استخدام وظائف مثل النسخ، وما إلى ذلك عن طريق إدخال كلمة المرور في لوحة تحكم الطابعة وتسجيل الدخول إلى الطابعة. ستظهر الوظائف غير المتوفرة باللون الرمادي وسيتعذر تحديدها.

تكوين التحكم في الوصول

لاستخدام التحكم في الوصول، قم بإنشاء حساب المستخدم وتمكين وظيفة التحكم في الوصول.

إنشاء حساب المستخدم

قم بإنشاء حساب المستخدم للتحكم في الوصول.

1. ادخل إلى Web Config وحدد علامة التبويب **User Settings < Access Control Settings < Product Security**.
 2. انقر فوق **Add** وفقاً للعدد الذي ترغب في تسجيله.
 3. عين كل عنصر.

User Name:

أدخل الاسم المعروض في قائمة اسم المستخدم بطول يتراوح بين 1 إلى 14 حرفاً باستخدام الأحرف الأبجدية الرقمية.

Password:

أدخل كلمة المرور بطول يتراوح بين 0 إلى 20 حرفاً بتنسيق (ASCII (0x20-0x7E). عند تهيئة كلمة المرور، اتركها فارغة.

Select the check box to enable or disable each function.

حدد الوظيفة التي تسمح باستخدامها.
 4. انقر فوق **Apply**.
- ارجع إلى قائمة إعداد المستخدم بعد مدة محددة من الزمن.
- تحقق من أن اسم المستخدم الذي سجلته في **User Name** معروض وغير **Add** إلى **Edit**.

تحرير حساب المستخدم

قم بتحرير الحساب المسجل للتحكم في الوصول.

1. ادخل إلى Web Config وحدد علامة التبويب **User Settings < Access Control Settings < Product Security**.
 2. انقر فوق **Edit** وفقاً للعدد الذي ترغب في تحريره.
 3. غير كل عنصر.
 4. انقر فوق **Apply**.
- ارجع إلى قائمة إعداد المستخدم بعد مدة محددة من الزمن.

إعدادات سلامة المنتج

حذف حساب المستخدم

احذف الحساب المسجل للتحكم في الوصول.

1. ادخل إلى Web Config وحدد علامة التبويب **User Settings < Access Control Settings < Product Security**.
2. انقر فوق **Edit** وفقاً للعدد الذي ترغب في حذفه.
3. انقر فوق **Delete**.



هام:

عند النقر فوق **Delete**، سيتم حذف حساب المستخدم دون رسالة تأكيد. انتبه عند حذف الحساب.

ارجع إلى قائمة إعدادات المستخدم بعد مدة محددة من الزمن.

تمكين التحكم في الوصول

عند تمكين التحكم في الوصول، لا يتمكن سوى المستخدم المسجل من استخدام الطابعة.

1. ادخل إلى تهيئة الويب وحدد علامة التبويب **Basic < Access Control Settings < Product Security**.
 2. حدد **Enables Access Control**.
 3. انقر فوق **OK**.
- يتم عرض رسالة الانتهاء بعد فترة معينة من الزمن.
تأكد من ظهور الرموز مثل النسخ والمسح الضوئي باللون الرمادي في لوحة تحكم الطابعة.

تعطيل الواجهة الخارجية

يُمكنك تعطيل الواجهة المُستخدمة لتوصيل الجهاز بالطابعة. قم بتعيين إعدادات التقييد حتى لا تتم الطباعة إلا عبر الشبكة.

ملاحظة:

يمكنك أيضاً تعيين إعدادات التقييد على لوحة تحكم الطابعة.

Memory Device: الإعدادات < إعدادات عامة < إعدادات الطابعة < واجهة جهاز الذاكرة < جهاز الذاكرة

الاتصال بكمبيوتر عبر **USB**: الإعدادات < إعدادات عامة < إعدادات الطابعة < الاتصال بكمبيوتر عبر **USB**

1. ادخل إلى Web Config وحدد علامة التبويب **External Interface < Product Security**.

2. حدد **Disable** في الوظائف التي تريد تعيينها.

حدد **Enable** عندما تريد إلغاء التحكم.

Memory Device

تجنّب حفظ البيانات في الذاكرة الخارجية عبر منفذ **USB** للاتصال بالجهاز الخارجي.

الاتصال بكمبيوتر عبر **USB**

يمكنك تقييد استخدام اتصال **USB** من الكمبيوتر. إذا كنت ترغب في تقييده، فحدد **Disable**.

3. انقر فوق **OK**.

إعدادات سلامة المنتج

4. تحقق من أنه لا يمكن استخدام المنفذ المُعطّل.

Memory Device

تأكد أنه لا توجد أي استجابة عند توصيل أي جهاز تخزين مثل ذاكرة USB بمنفذ USB للواجهة الخارجية.

الاتصال بكمبيوتر عبر USB

إذا تم تثبيت برنامج تشغيل الطابعة على الكمبيوتر
قم بتوصيل الطابعة بجهاز الكمبيوتر باستخدام كابل USB، ثم تأكد من أن الطابعة لا تطبع.
إذا لم يتم تثبيت برنامج التشغيل على الكمبيوتر

:Windows

افتح مدير الجهاز واحتفظ به، ثم وصل الطابعة بالكمبيوتر باستخدام كابل USB، ثم تأكد من بقاء محتويات شاشة مدير الجهاز دون تغيير.

:Mac OS

قم بتوصيل الطابعة بجهاز الكمبيوتر باستخدام كابل USB، ثم تأكد من عدم إدراج الطابعة إذا كنت ترغب في إضافة الطابعة من الطابعات والماسحات الضوئية.

معلومات ذات صلة

◀ "الوصول إلى تطبيق Web Config" في الصفحة 27


إعدادات الإدارة والتشغيل

يوضح هذا الفصل العناصر المرتبطة بعمليات تشغيل الجهاز وإدارته بشكل يومي.

تسجيل الدخول إلى الطابعة كمسؤول

إذا تم تعيين كلمة مرور المسؤول إلى الطابعة، تحتاج إلى تسجيل الدخول كمسؤول لتشغيل عناصر القائمة المقفلة.


تسجيل الدخول إلى الطابعة باستخدام لوحة التحكم

1. اضغط على .

2. اضغط على المسؤول.

3. أدخل كلمة مرور المسؤول.

4. اضغط على موافق.

 يتم عرضه عند المصادقة، ثم يمكنك تشغيل عناصر القائمة المقفلة.

اضغط على  لتسجيل الخروج.

ملاحظة:

عند تحديد شغل لإعدادات < إعدادات عامة > الإعدادات الأساسية < انتهى وقت العملية > يمكنك تسجيل الخروج تلقائياً بعد مرور فترة زمنية محددة إذا لم يكن هناك نشاط على لوحة التحكم.

تسجيل الدخول إلى الطابعة باستخدام Web Config

عند تسجيل الدخول إلى تكوين الويب كمسؤول، يمكنك تشغيل العناصر التي عُينت في إعداد القفل.

1. أدخل عنوان IP الخاص بالطابعة في المستعرض لإجراء Web Config.

2. انقر فوق Log in.

3. أدخل اسم المستخدم وكلمة مرور المسؤول في User Name و Current password.

4. انقر فوق OK.

يتم عرض العناصر المؤمنة و Administrator Logout عند المصادقة.

انقر فوق Administrator Logout لتسجيل الخروج.

ملاحظة:

عند تحديد ON لعلامة التبويب **Device Management < Control Panel < Operation Timeout**، يمكنك تسجيل الخروج تلقائياً بعد مرور فترة زمنية محددة إذا لم يكن هناك نشاط على لوحة التحكم.

تأكيد معلومات الطابعة

التحقق من المعلومات من لوحة التحكم

يمكنك التحقق من المعلومات التالية وطباعتها من لوحة التحكم.

الإمداد

الإعدادات > حالة التوريد

يمكنك التحقق من المعلومات المتعلقة بالحبر وصندوق الصيانة.

ورقة حالة المنتج

الإعدادات > حالة الطابعة/طباعة > طباعة ورقة الحالة

يمكنك طباعة ورقة الحالة، مثل معلومات الطابعة ومعلومات المواد المستهلكة.

معلومات الشبكة



الإعدادات > إعدادات عامة > إعدادات الشبكة > حالة الشبكة

الإعدادات > حالة الطابعة/طباعة > الشبكة

يمكنك التحقق من المعلومات المتعلقة بالشبكة مثل حالة اتصال الشبكة وإعدادات خادم البريد وما إلى ذلك وكذلك طباعة ورقة حالة الشبكة.

تقرير اتصال الشبكة

الإعدادات > إعدادات عامة > إعدادات الشبكة > التحقق من الاتصال

الصفحة الرئيسية >  |  > الوصف > عند تعذر الاتصال بالشبكة

يمكنك تشخيص حالة اتصال الشبكة الخاصة بالطابعة وطباعة التقرير.

حالة اتصال الشبكة

الصفحة الرئيسية >  |  > راوتر

يمكنك التحقق من حالة الاتصال الخاصة بالشبكة السلكية/شبكة الاتصال المحلية اللاسلكية.

التحقق من المعلومات من Web Config

يمكنك التحقق من المعلومات التالية لطابعة التشغيل من Status باستخدام Web Config.

Product Status

تحقق من اللغة، والحالة، ورقم المنتج، وعنوان MAC، وما إلى ذلك.

Network Status

تحقق من معلومات حالة الاتصال بالشبكة، وعنوان IP، وخادم DNS، وما إلى ذلك.

Hardware Status

تحقق من حالة كل شبكة Wi-Fi، وما إلى ذلك.

Panel Snapshot

اعرض لقطة لصورة الشاشة التي يتم عرضها على لوحة التحكم في الجهاز.

استلام إعلانات البريد الإلكتروني عند وقوع أحداث

حول إشعارات البريد الإلكتروني

تتمثل وظيفة الإشعار في أنه يرسل بريداً إلكترونياً إلى العنوان المحدد عندما تحدث أمور مثل توقف عملية الطباعة وحدوث عطل في الطباعة.

يمكنك تسجيل ما يصل إلى خمس وجهات وتعيين إعدادات الإشعارات لكل وجهة. لاستخدام هذه الوظيفة، أنت بحاجة إلى إعداد خادم البريد الإلكتروني قبل إعداد الإشعارات.

معلومات ذات صلة

← "تكوين خادم البريد" في الصفحة 34

تكوين إشعارات البريد الإلكتروني

قم بتهيئة إشعار البريد الإلكتروني باستخدام Web Config.

1. ادخل إلى Web Config وحدد علامة التبويب **Email Notification < Device Management**.
2. عين موضوع إشعار البريد الإلكتروني.
حدد المحتويات المعروضة في الموضوع من القائمتين المنسدلتين.
 تُعرض المحتويات المحددة إلى جانب **Subject**.
 لا يمكن تعيين المحتوى نفسه في الجهة اليسرى واليمنى.
 عندما يتجاوز عدد الأحرف في **Location** 32 بايت، تُحذف الأحرف التي تتجاوز 32 بايت.
3. أدخل عنوان البريد الإلكتروني لإرسال بريد الإعلام.
استخدم 0-9 a-z A-Z # \$ % & * ' - . / ? ^ _ { | } ~ @، وأدخل ما بين 1 إلى 255 حرفاً.
4. حدد لغة إشعارات البريد الإلكتروني.
5. حدد خانة الاختيار على الحدث الذي ترغب في تلقي إشعار حوله.
يرتبط عدد **Notification Settings** برقم الوجهة الخاص بـ **Email Address Settings**.
مثال:

إعدادات الإدارة والتشغيل

إذا كنت ترغب في إرسال إشعار إلى عنوان البريد الإلكتروني المحدد للرقم 1 في **Email Address Settings** عندما ينفد الورق من الطابعة، فحدد عمود خانة الاختيار 1 في صف **Paper out**.

EPSON L8-10000P

Status Print Scan/Copy Fax Network Network Security Product Security **Device Management** Epson Open Platform

Email Notification

Set up the Email Server to enable the email notification.

Email Address Settings

Email in selected language will be sent to each address.

1:	Admin@AAA.com	English
2:	General@AAA.com	English
3:		English
4:		English
5:		English

Notification Settings

Email will be sent when product status is as checked.

	1	2	3	4	5
Ink cartridge(s) to be replaced	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ink low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintenance box: end of service life	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintenance box: nearing end	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administrator password changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paper out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paper Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Printing stopped*	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Printer error	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scanner error	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fax error	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wi-Fi failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HDD failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NFC failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

* Notified when an error occurs, such as paper jam, paper cassette unset, or mismatch of paper size or type.

OK Restore Default Settings

6. انقر فوق **OK**.

التأكيد على أنه سيتم إرسال إشعار البريد الإلكتروني حسب التسبب في أحد الأحداث. مثال: الطباعة عن طريق تحديد مصدر الورق عند عدم تعيين الورق.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "تكوين خادم البريد" في الصفحة 34

عناصر خاصة بإشعارات البريد الإلكتروني

العناصر	الإعدادات والشرح
Ink supply unit(s) to be replaced	إشعار عند نفاد الحبر.
Ink low	إشعار عندما يكون الحبر على وشك النفاد.
Maintenance box: end of service life	إشعار عندما تكون علبة الصيانة ممتلئة.
Maintenance box: nearing end	إشعار عندما تكون علبة الصيانة على وشك الامتلاء.
Administrator password changed	إشعار عند تغيير كلمة مرور المسؤول.

إعدادات الإدارة والتشغيل

العناصر	الإعدادات والشرح
Paper out	إشعار عند حدوث خطأ نفاذ الورق في مصدر الورق المحدد.
Paper Low	إشعار عند حدوث خطأ انخفاض عدد الورق في مصدر الورق المحدد.
Printing stopped*	إشعار عند توقف الطباعة بسبب انحسار الورق أو عدم تطابق حجم الورق/نوع الورق.
Printer error	إشعار عند حدوث خطأ بالطابعة.
Scanner error	إشعار عند حدوث خطأ الماسحة الضوئية.
فشل Wi-Fi	إشعار عند حدوث خطأ واجهة شبكة LAN اللاسلكية.
Print Job Completion *2	ترسل الطابعة رسالة عن طريق البريد الإلكتروني في كل مرة يتم فيها إكمال عدد مهام الطباعة التي تم تعيينها في القائمة المنسدلة.

تحديث البرنامج الثابت

عند توفر البرامج الثابتة الجديدة، يؤدي تحديث البرامج الثابتة للطابعة إلى تحسين الوظيفة أو حل المشكلة.

تحديث البرامج الثابتة للطابعة باستخدام لوحة التحكم

يمكنك تحديث البرامج الثابتة للطابعة باستخدام لوحة التحكم، في حال كان بالإمكان توصيل الطابعة بالإنترنت. يمكنك أيضاً ضبط الطابعة للتحقق بانتظام من توافر تحديثات للبرامج الثابتة وإشعارك عند توافر أي تحديثات.

1. حدد الإعدادات في الصفحة الرئيسية.

2. حدد إعدادات عامة < إدارة النظام < تحديث البرامج الثابتة < تحديث.

ملاحظة:

حدد إشعار < شغل لضبط الطابعة للتحقق بانتظام من تحديثات البرامج الثابتة المتوفرة.

3. حدد بدء التحقق.

تبدأ الطابعة في البحث عن التحديثات المتوفرة.

4. إذا أبلغت الرسالة المعروضة على شاشة LCD بتوفر تحديثات للبرامج الثابتة، فاتباع التعليمات المعروضة على الشاشة لتبدأ التحديث.

هام: 

لا تغلق الطابعة أو تفصلها حتى يكتمل التحديث؛ وإلا قد تتعطل الطابعة.

في حالة عدم اكتمال التحديث أو عدم نجاحه، لا تبدأ الطابعة في العمل بصورة طبيعية ويظهر "Recovery Mode" على شاشة LCD في المرة التالية لتشغيل الطابعة. في هذه الحالة، أنت بحاجة إلى تحديث البرامج الثابتة مرة أخرى باستخدام جهاز كمبيوتر. قم بتوصيل الطابعة بالحاسوب من خلال كبل USB. أثناء ظهور "Recovery Mode" على الطابعة، لا يمكنك تحديث البرامج الثابتة عبر اتصال شبكة. من خلال الكمبيوتر، قم بزيارة موقع Epson المحلي، ثم قم بتنزيل أحدث إصدار من البرامج الثابتة للطابعة. راجع التعليمات على موقع الويب لمعرفة الخطوات التالية.

تحديث البرنامج الثابت باستخدام Web Config

عندما يُمكن للطابعة الاتصال بالإنترنت، يُمكنك تحديث البرامج الثابتة من Web Config.

إعدادات الإدارة والتشغيل

1. ادخل إلى Web Config وحدد علامة التبويب **Firmware Update < Device Management**.

2. انقر فوق **Start**.

يتم بدء تأكيد البرنامج الثابت، ويتم عرض معلومات البرنامج الثابت إذا تم العثور على برنامج ثابت محدث.

3. انقر فوق **Start**، واتبع الإرشادات الظاهرة على الشاشة.

ملاحظة:

يمكنك أيضاً تحديث البرامج الثابتة *Epson Device Admin*. يمكنك التأكد بعينك من معلومات البرنامج الثابت على قائمة الجهاز. يُعد ذلك مفيداً عندما ترغب في تحديث عدة برامج ثابتة للأجهزة. راجع دليل *Epson Device Admin* أو التعليمات للحصول على مزيد من التفاصيل.

معلومات ذات صلة

◀ "الوصول إلى تطبيق Web Config" في الصفحة 27

◀ "Epson Device Admin" في الصفحة 100

تحديث البرامج الثابتة بدون الاتصال إلى الإنترنت

يمكنك تنزيل البرنامج الثابت للجهاز من موقع Epson على الويب على الكمبيوتر، ثم وصل الجهاز والكمبيوتر بكابل USB لتحديث البرنامج الثابت. إذا لم تتمكن من التحديث عبر الشبكة، فجرب هذه الطريقة.

1. انتقل إلى موقع Epson على الويب ونزل البرنامج الثابت.

2. وصل الكمبيوتر الذي يحتوي على برنامج ثابت تم تنزيله على الطابعة عن طريق كابل USB.

3. انقر نقرًا مزدوجًا على ملف exe الذي تم تنزيله.

تشغيل Epson Firmware Updater.

4. اتبع التعليمات المعروضة على الشاشة.

نسخ الإعدادات احتياطياً

يمكنك تصدير قيمة الإعداد المحددة من Web Config إلى الملف. يمكنك استخدامها لنسخ جهات الاتصال احتياطياً، وتحديد القيم، واستبدال الطابعة، وما إلى ذلك.

لا يمكن تحرير الملف المصدر لأنه يتم تصديره باعتباره ملفاً ثنائياً.

تصدير الإعدادات

قم بتصدير الإعداد إلى الطابعة.

1. ادخل إلى Web Config ثم حدد علامة التبويب **Export < Export and Import Setting Value < Device Management**.

2. حدّد الإعدادات التي تريد تصديرها.

حدّد الإعدادات التي تريد تصديرها. إذا قمت بتحديد الفئة الأصلية، فسيتم اختيار فئات فرعية أيضاً. ومع ذلك، لا يمكن تحديد الفئات الفرعية التي تتسبب في حدوث أخطاء أثناء التكرار في الشبكة نفسها (مثل عناوين IP وغيرها).

3. أدخل كلمة مرور لتشفير الملف الذي تم تصديره.

ستحتاج إلى كلمة المرور لاستيراد الملف. اترك هذه الخانة فارغة إذا لم ترغب في تشفير الملف.

إعدادات الإدارة والتشغيل

4. انقر فوق **Export**.هام: 

إذا كنت ترغب في تصدير إعدادات الشبكة للطابعة مثل اسم الجهاز وعنوان IPv6، فحدّد *Enable to select the individual settings of device* ثم حدّد عناصر أخرى. استخدم القيم المحددة للطابعة الاستبدال.

معلومات ذات صلة

← ["الوصول إلى تطبيق Web Config" في الصفحة 27](#)

استيراد الإعدادات

قم باستيراد ملف Web Config الذي تم تصديره إلى الطابعة.

هام: 

عند استيراد القيم التي تشمل المعلومات الفردية مثل اسم الطابعة أو عنوان IP، تأكد من عدم وجود عنوان IP نفسه على الشبكة نفسها. عندما يتداخل عنوان IP، فإن الطابعة لا تعكس القيمة.

1. ادخل إلى Web Config ثم حدّد علامة التبويب **Device Management < Export and Import Setting Value < Import**.
 2. حدّد الملف الذي تم تصديره، ثم أدخل كلمة المرور المشفرة.
 3. انقر فوق **Next**.
 4. حدّد الإعدادات التي تريد استيرادها، ثم انقر فوق **Next**.
 5. انقر فوق **OK**.
- تم تطبيق الإعدادات على الطابعة.

حل المشكلات

تلميحات لحل المشكلات

- ❑ التحقق من رسالة الخطأ عند حدوث مشكلة، تحقق أولاً مما إذا كانت هناك أي رسائل على لوحة تحكم الطابعة أو شاشة برنامج التشغيل أم لا. إذا كان لديك بريد إعلام مضبوطاً عند حدوث الأحداث، يمكنك معرفة الحالة على الفور.
- ❑ تقرير اتصال الشبكة شخّص حالة الطابعة والشبكة، ثم اطبع النتيجة. يمكنك العثور على الخطأ الذي تم تشخيصه من جانب الطابعة.
- ❑ التحقق من حالة الاتصال تحقق من حالة الاتصال في كمبيوتر الخادم أو كمبيوتر العميل باستخدام الأمر مثل ping و ipconfig.
- ❑ اختبار الاتصال للتحقق من الاتصال بين الطابعة إلى خادم البريد الإلكتروني، أجرِ اختبار الاتصال من الطابعة. بالإضافة إلى ذلك، تحقق من الاتصال من كمبيوتر العميل إلى الخادم للتحقق من حالة الاتصال.
- ❑ تهيئة الإعدادات إذا لم تُظهر الإعدادات وحالة الاتصال أي مشكلة، فقد يتم حل المشكلات عن طريق تعطيل إعدادات الشبكة للطابعة أو تهيئتها، ثم إعدادها مرة أخرى.

التحقق من حالة الطابعة

لتحديد سبب المشكلة، تحقق من حالة الطابعة والشبكة.

التحقق من رسالة الخطأ

التحقق من رسالة الخطأ من إشعار البريد الإلكتروني

عند إعداد إشعار البريد الإلكتروني، تحقق من إرسال رسالة الخطأ من الطابعة. إذا كانت التعليمات المتعلقة بكيفية التعامل مع المشكلة واردة في إشعار البريد الإلكتروني، فيرجى اتباعها.

معلومات ذات صلة

← "استلام إعلانات البريد الإلكتروني عند وقوع أحداث" في الصفحة 76

فحص الرسائل المعروضة على شاشة LCD

إذا تم عرض رسالة خطأ على شاشة LCD، فاتبع الإرشادات المعروضة على الشاشة أو الحلول أدناه لحل المشكلة.

حل المشكلات

رسائل الخطأ	الأسباب والحلول
خطأ بالطابعة. أوقف تشغيل الطاقة وشغِّها مجدداً. للتفاصيل، راجع الوثائق المتوفرة لديك.	<p><input type="checkbox"/> الأسباب: توجد مادة غريبة داخل الطابعة أو حدثت إحدى أخطاء الطابعة.</p> <p><input type="checkbox"/> الحلول: أزل أي ورق أو مواد واقية من الطابعة. إذا استمرت رسالة الخطأ في الظهور، فاتصل بدعم Epson.</p>
يجب استبدال خرطوشة الحبر.	<p><input type="checkbox"/> الأسباب: نقد الحبر.</p> <p><input type="checkbox"/> الحلول: للتأكد من الحصول على جودة طباعة فائقة وللمساعدة في حماية رأس الطابعة، يبقى مخزون أمان مختلف من الحبر في الخرطوشة عند إشارة الطابعة إلى أن وقت استبدال الخرطوشة قد حان. استبدل الخرطوشة عندما يُطلب منك ذلك.</p>
لم يتم اكتشاف صندوق الصيانة. رُكِّه بشكل صحيح.	<p><input type="checkbox"/> الأسباب: لم يتم تركيب علبة الصيانة على نحو صحيح.</p> <p><input type="checkbox"/> الحلول: تحقق من حالة تركيب علبة الصيانة، ثم قم بتركيبها بصورة صحيحة.</p>
وصل صندوق الصيانة إلى نهاية عمره الافتراضي. يجب استبداله.	<p><input type="checkbox"/> الأسباب: هذا يعني أن العمر الافتراضي لعلبة الصيانة على وشك الانتهاء.</p> <p><input type="checkbox"/> الحلول: استبدل علبة الصيانة وفقاً للإرشادات.</p>
There is not enough space in maintenance box to perform head cleaning. You can continue printing until replacement is required.	<p><input type="checkbox"/> الأسباب: ليس لدى صندوق الصيانة السعة الكافية لتنظيف الرأس.</p> <p><input type="checkbox"/> الحلول: افصل طاقة الطابعة، ثم استبدل علبة الصيانة. يمكنك استخدام علبة الصيانة التي تم استبدالها مرة أخرى بعد تنظيف الرأس.</p>
فُك صندوق الصيانة وأعد تركيبه.	<p><input type="checkbox"/> الأسباب: لم يتم التعرف على علبة الصيانة على نحو صحيح.</p> <p><input type="checkbox"/> الحلول: أزل علبة الصيانة على الفور، ثم أعد تركيبها مرة أخرى. وإذا لم يتم التعرف عليها بعد كل ذلك، فاستبدلها بعلبة صيانة جديدة.</p>
توليفة عنوان IP وقناع الشبكة الفرعية غير صالحة. راجع الوثائق المتوفرة لديك للاطلاع على مزيد من التفاصيل.	<p><input type="checkbox"/> الأسباب: مجموعة عنوان IP التي عينتها غير صالحة.</p> <p><input type="checkbox"/> الحلول: قم بإدخال عنوان IP أو البوابة الافتراضية.</p>
حدِّث الشهادة الجذر لاستخدام الخدمات السحابية.	<p><input type="checkbox"/> الأسباب: انتهت صلاحية شهادة الجذر للخدمات السحابية.</p> <p><input type="checkbox"/> الحلول: قم بتشغيل Web Config، ثم قم بتحديث شهادة المصدر. Root Certificate Update — Network Security</p>

حل المشكلات

رسائل الخطأ	الأسباب والحلول
Recovery Mode	<p>❑ الأسباب:</p> <p>فشل تحديث البرنامج الثابت ولا يمكن العودة إلى الوضع العادي.</p> <p>❑ الحلول:</p> <p>بدأ تشغيل الطابعة في وضع الاستعادة نظراً لتعذر تحديث البرامج الثابتة. اتبع الخطوات أدناه لتحديث البرامج الثابتة مرة أخرى.</p> <p>1. وصل الكمبيوتر بالطابعة باستخدام كابل USB. (أثناء وضع الاستعادة، لا يمكنك تحديث البرامج الثابتة خلال اتصال شبكة).</p> <p>2. تفضل بزيارة موقع ويب Epson المحلي للحصول على المزيد من الإرشادات.</p>

التحقق من شاشة لوحة الطابعة البعيدة

يمكنك التحقق من شاشة لوحة الطابعة البعيدة باستخدام Web Config.

1. شغل Web Config الخاص بالطابعة التي ترغب في التحقق منها.
عندما تتلقى إشعار البريد الإلكتروني، يمكنك تشغيل تكوين الويب من عنوان URL على البريد الإلكتروني.
2. حدد علامة التبويب **Panel Snapshot < Status**.
يتم عرض لوحة الطابعة الحالية على Web Config.
للتحديث، انقر فوق **Refresh**.

طباعة تقرير الاتصال بالشبكة

يمكنك طباعة تقرير اتصال شبكة ما للتحقق من الحالة بين الطابعة والموجه اللاسلكي.

1. قم بتحميل الورق.
2. حدد الإعدادات في الصفحة الرئيسية.
3. حدد إعدادات عامة < إعدادات الشبكة < التحقق من الاتصال.
يبدأ فحص الاتصال.
4. حدد طباعة تقرير الفحص.
5. قم بطباعة تقرير اتصال الشبكة.
إذا حدث خطأ، فتتحقق من تقرير الاتصال بالشبكة، ثم اتبع الحلول المطبوعة.
6. أغلق الشاشة.

معلومات ذات صلة

← "الرسائل والحلول الخاصة بتقرير اتصال الشبكة" في الصفحة 84

حل المشكلات

الرسائل والحلول الخاصة بتقرير اتصال الشبكة

تحقق من الرسائل ورموز الخطأ الموجودة في تقرير اتصال الشبكة، ثم اتبع الحلول التالية.

Check Network Connection

Check Result: FAIL

Error code: (E-2)

See the Network Status and check if the Network Name (SSID) is the SSID you want to connect. If the SSID is correct, make sure to enter the correct password and try again.

If your problems persist, see your documentation for help and networking tips.

Checked Items

Wireless Network Name (SSID) Check	FAIL
Communication Mode Check	Unchecked
Security Mode Check	Unchecked
MAC Address Filtering Check	Unchecked
Security Key/Password Check	Unchecked
IP Address Check	Unchecked
Detailed IP Setup Check	Unchecked

Network Status

Printer Name	EPSON XXXXXX
Printer Model	XX-XXX Series
IP Address	169.254.137.8
Subnet Mask	255.255.0.0
Default Gateway	
Network Name (SSID)	EpsonNet
Security	None
Signal Strength	Poor
MAC Address	F8:D0:27:40:C0:AC

أ- رمز الخطأ

ب- رسائل حول بيئة الشبكة

E-1

الحلول:

- تأكد من إحكام توصيل كبل Ethernet بالطابعة وبالموزع أو أجهزة الشبكة الأخرى.
- تأكد من تشغيل الموزع أو جهاز الشبكة الآخر.
- إذا أردت توصيل الطابعة عبر Wi-Fi، فاضبط إعدادات Wi-Fi للطابعة مرة أخرى؛ حيث إنها معطلة.

E-2 و E-3 و E-7

الحلول:

- تأكد من تشغيل الرواوتر اللاسلكي.

حل المشكلات

- تأكد من صحة توصيل الكمبيوتر أو الجهاز بالراوتر اللاسلكي.
- أوقف تشغيل الراوتر اللاسلكي. وانتظر 10 ثوانٍ تقريباً ثم شغِّه.
- قَرِّب الطابعة من الراوتر اللاسلكي وأزِل أي عوائق بينهما.
- إذا كنت قد أدخلت SSID يدوياً، فتحقق من صحته. تحقق من SSID من الجزء **Network Status** في تقرير الاتصال بالشبكة.
- إذا كانت هناك عدة معرفات SSID لراوتر لاسلكي، فحدد معرف SSID المعروف. وعندما يستخدم معرف SSID تردداً غير متوافق، فلا تعرضه الطابعة.
- إذا كنت تستخدم ميزة إعداد الزر الانضغاطي لإنشاء اتصال شبكة، فتأكد من أن الراوتر اللاسلكي يدعم WPS. ولا يمكنك استخدام ميزة إعداد الزر الانضغاطي إذا كان الراوتر اللاسلكي لا يدعم WPS.
- تأكد من أن معرف SSID لا يستخدم سوى حروف ASCII (رموز وحروف أبجدية رقمية). ولا يمكن أن تعرض الطابعة معرف SSID يحتوي على حروف أخرى غير ASCII.
- تأكد من أنك على علم بمعرف SSID وكلمة المرور التابعين لك قبل الاتصال بالراوتر اللاسلكي. إذا كنت تستخدم رواتر لاسلكياً بإعداداته الافتراضية، يوجد معرف SSID وكلمة المرور في ملصق على الراوتر اللاسلكي. إذا لم تكن على علم بمعرف SSID وكلمة المرور التابعين لك، فاتصل بالشخص الذي قام بإعداد الراوتر اللاسلكي أو راجع الوثائق المرفقة بالراوتر اللاسلكي.
- إذا كنت تتصل بمعرف SSID تم إنشاؤه من جهاز ذكي يدعم وظيفة الربط، فتتحقق بحثاً عن معرف SSID وكلمة المرور في الوثائق المرفقة بالجهاز الذكي.
- إذا انقطع اتصال Wi-Fi فجأة، فتتحقق بحثاً عن الحالات أدناه. وإذا توفرت أي من هذه الحالات، فأعد ضبط إعدادات الشبكة من خلال تنزيل وتشغيل البرنامج من موقع الويب التالي.
<http://epson.sn> < الإعداد
- إضافة جهاز ذكي آخر إلى الشبكة باستخدام إعداد الزر الانضغاطي.
- تعيين شبكة Wi-Fi باستخدام أي طريقة أخرى غير إعداد الزر الانضغاطي.

E-5

الحلول:

- تأكد من ضبط نوع الأمان الخاص بالموجه اللاسلكي على أحد الخيارات التالية. وإذا لم يتم ضبطه على هذا النحو، فقم بتغيير نوع الأمان بالموجه اللاسلكي ثم قم بإعادة ضبط إعدادات شبكة الطابعة.
- WEP-64 بت (40 بت)
 - WEP-128 بت (104 بت)
 - WPA PSK (TKIP/AES)^{1*}
 - WPA2 PSK (TKIP/AES)^{1*}
 - (WPA (TKIP/AES
 - (WPA2 (TKIP/AES
 - WPA3-SAE (AES)^{2*}
 - WPA2/WPA3-Enterprise^{2*}

^{1*} يُعرف أيضاً WPA PSK باسم WPA الشخصي. يعرف أيضاً WPA2 PSK باسم WPA2 الشخصي.

^{2*} قد لا يكون WPA3-SAE (AES) و WPA2/WPA3-Enterprise مدعومين حسب الطراز. للاطلاع على التفاصيل، راجع وثائق الطابعة.

حل المشكلات

E-6

الحلول:

□ تحقق مما إذا كانت وظيفة ترشيح عنوان MAC معطلة أم لا. إذا كانت ممكنة، فسجل عنوان MAC للطابعة بحيث لا يمكن ترشيحه. راجع الوثائق المرفقة بالراوتر اللاسلكي للاطلاع على التفاصيل. يمكنك التحقق من عنوان MAC للطابعة من الجزء **Network Status** في تقرير الاتصال بالشبكة.

□ إذا كان الراوتر اللاسلكي يستخدم مصادقة مشتركة مع أمان WEP، فتأكد من صحة مفتاح المصادقة والمؤشر.

□ إذا كان عدد الأجهزة القابلة للتوصيل في الراوتر اللاسلكي أقل من عدد أجهزة الشبكة التي تريد توصيلها، فاضبط الإعدادات في الراوتر اللاسلكي لزيادة عدد الأجهزة القابلة للتوصيل. راجع الوثائق المرفقة بالراوتر اللاسلكي لضبط الإعدادات.

E-8

الحلول:

□ قم بتمكين وظيفة DHCP في الموجه اللاسلكي إذا تم تعيين إعدادات عنوان IP الذي تم الحصول عليه للطابعة على التشغيل التلقائي.

□ إذا تم ضبط إعدادات عنوان IP الذي تم الحصول عليه للطابعة إلى وضع التشغيل اليدوي، فإن عنوان IP الذي قمت بضبطه يدوياً غير صالح لأنه خارج النطاق (على سبيل المثال: 0.0.0.0). عين عنوان IP صالحاً من لوحة التحكم بالطابعة.

E-9

الحلول:

تحقق مما يلي.

□ تشغيل الأجهزة.

□ إمكانية الوصول إلى الإنترنت وأجهزة الكمبيوتر أو الأجهزة الأخرى المتصلة بالشبكة نفسها من الأجهزة التي تريد توصيلها بالطابعة.

إذا ما زال توصيل الطابعة وأجهزة الشبكة متعذراً بعد التأكد مما سبق، فأوقف تشغيل الراوتر اللاسلكي. وانتظر 10 ثوانٍ تقريباً ثم شغله. ثم أعد تعيين إعدادات الشبكة من خلال تنزيل وتشغيل المثبت من موقع الويب التالي.

<http://epson.sn> < الإعداد

E-10

الحلول:

تحقق مما يلي.

□ تم تشغيل الأجهزة الأخرى على نفس الشبكة.

□ تكون عناوين الشبكة (عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية) صحيحة إذا قمت بضبط التشغيل اليدوي لعنوان IP الذي تم الحصول عليه للطابعة.

أعد ضبط عنوان الشبكة إذا كانت تلك الخطوات غير صحيحة. يمكنك التحقق من عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية من خلال الجزء الخاص بـ **Network Status** بتقرير اتصال الشبكة.

إذا تم تمكين وظيفة DHCP، فقم بتغيير إعدادات عنوان IP الذي تم الحصول عليه للطابعة إلى تلقائي. إذا كنت تريد ضبط عنوان IP يدوياً، فتحقق من عنوان IP الخاص بالطابعة من خلال الجزء الخاص بـ **Network Status** بتقرير اتصال الشبكة، ثم حدد التشغيل اليدوي من على شاشة إعدادات الشبكة. قم بضبط قناع الشبكة الفرعية على القيمة [255.255.255.0].

حل المشكلات

في حال استمرار عدم توصيل الطابعة وأجهزة الشبكة، فأوقف تشغيل جهاز التوجيه اللاسلكي. انتظر حوالي 10 ثوانٍ، ثم قم بتشغيلها.

E-11

الحلول:

تحقق مما يلي.

صحة عنوان البوابة الافتراضية إذا عيّنت إعداد TCP/IP للطابعة على "يدوي".

تشغيل الجهاز الذي تم تعيينه كبوابة افتراضية.

عَيِّن عنوان البوابة الافتراضية الصحيح. يمكنك التحقق من عنوان البوابة الافتراضية من الجزء **Network Status** في تقرير الاتصال بالشبكة.

E-12

الحلول:

تحقق مما يلي.

تشغيل أجهزة أخرى متصلة بالشبكة.

صحة عناوين الشبكة (عنوان IP وقناع الشبكة الفرعية والبوابة الافتراضية) في حالة إدخالها يدوياً.

تطابق عناوين الشبكة للأجهزة الأخرى (قناع الشبكة الفرعية والبوابة الافتراضية).

عدم تعارض عنوان IP مع أجهزة أخرى.

إذا ما زال توصيل الطابعة وأجهزة الشبكة متعذراً بعد التأكد مما سبق، فجرِّب ما يلي.

أوقف تشغيل الراوتر اللاسلكي. وانتظر 10 ثوانٍ تقريباً ثم شغِّه.

اضبط إعدادات الشبكة مرة أخرى باستخدام المثبَّت. الذي يمكنك تشغيله من موقع الويب التالي.

<http://epson.sn> < الإعداد

يمكنك تسجيل عدة كلمات مرور في راوتر لاسلكي يستخدم نوع أمان WEP. وفي حالة تسجيل عدة كلمات مرور، تحقق من تعيين كلمة المرور الأولى المسجَّلة في الطابعة.

E-13

الحلول:

تحقق مما يلي.

تشغيل أجهزة الشبكة، مثل راوتر لاسلكي وموزَّع وراوتر غير لاسلكي.

عدم إعداد TCP/IP يدوياً لأجهزة الشبكة. (إذا تم إعداد TCP/IP للطابعة تلقائياً أثناء إعداد TCP/IP يدوياً لأجهزة شبكة أخرى، فقد تختلف شبكة الطابعة عن شبكة الأجهزة الأخرى.)

إذا لم تُحل المشكلة بعد التحقق مما سبق، فجرِّب ما يلي.

أوقف تشغيل الراوتر اللاسلكي. وانتظر 10 ثوانٍ تقريباً ثم شغِّه.

حل المشكلات

❑ اضبط إعدادات الشبكة في الكمبيوتر المتصل بالشبكة نفسها المتصلة بها الطابعة باستخدام المثبت. الذي يمكنك تشغيله من موقع الويب التالي.

<http://epson.sn> < الإعداد

❑ يمكنك تسجيل عدة كلمات مرور في راوتر لاسلكي يستخدم نوع أمان WEP. وفي حالة تسجيل عدة كلمات مرور، تحقق من تعيين كلمة المرور الأولى المسجلة في الطابعة.

رسالة حول بيئة الشبكة

الرسالة	الحل
The Wi-Fi environment needs to be improved. Turn the wireless router off and then turn it on. If the connection does not improve, see the documentation for the wireless router.	بعد وضع الطابعة بالقرب من الموجة اللاسلكي، وإزالة أي عوائق بين نقطة الوصول والطابعة، قم بإيقاف تشغيل الموجة اللاسلكي. انتظر حوالي 10 ثوانٍ، ثم قم بتشغيلها. إذا ظلت غير متصلة، فراجع الوثائق المرفقة مع الموجة اللاسلكي.
*No more devices can be connected. Disconnect one of the connected devices if you want to add another one.	يتم توصيل جهاز الكمبيوتر والأجهزة الذكية، التي يمكن توصيلها في آن واحد، بالكامل بشبكة اتصال Wi-Fi مباشرة (نقطة الوصول البسيط). لإضافة جهاز كمبيوتر أو جهاز ذكي آخر، قم أولاً بفصل أحد الأجهزة المتصلة أو توصيله بالشبكة الأخرى. يمكنك تأكيد عدد الأجهزة اللاسلكية التي يمكن توصيلها في آن واحد وعدد الأجهزة المتصلة من خلال التحقق من ورقة حالة الشبكة أو لوحة تحكم الطابعة.
The same SSID as Wi-Fi Direct exists in the environment. Change the Wi-Fi Direct SSID if you cannot connect a smart device to the printer.	على لوحة التحكم الخاصة بالطابعة، انتقل إلى شاشة إعداد شبكة Wi-Fi Direct، وحدد القائمة لتغيير الإعداد. يمكنك تغيير اسم الشبكة التي تلي DIRECT-XX. أدخل في نطاق 22 حرفاً.

التحقق من حالة الاتصال

تحقق ما إذا كان الاتصال بين الطابعة والكمبيوتر صحيح، ويؤدي إلى حل المشكلات أم لا.

فحص سجل الخادم وجهاز الشبكة

إذا حدثت مشكلة في اتصال الشبكة، فقد يكون من الممكن تحديد السبب عن طريق تأكيد سجل خادم البريد الإلكتروني أو خادم LDAP وما إلى ذلك، أو التحقق من الحالة باستخدام سجل الشبكة لسجلات معدات النظام والأوامر الخاصة بها، مثل أجهزة التوجيه.

طباعة ورقة حالة الشبكة

يمكنك التحقق من المعلومات المفصلة حول الشبكة عن طريق طباعتها.

1. حمل الورق.
2. حدد الإعدادات في الصفحة الرئيسية.
3. حدد إعدادات عامة < إعدادات الشبكة < حالة الشبكة.
4. حدد ورقة حالة الطباعة.
5. تحقق من الرسالة، ثم اطبع ورقة حالة الشبكة.

حل المشكلات

6. أغلق الشاشة.

تغلق الشاشة تلقائياً بعد فترة زمنية محددة.

التحقق من الاتصال بين الأجهزة وأجهزة الكمبيوتر

التحقق من الاتصال باستخدام أمر *Ping* - Windows

يُمكنك استخدام أمر *Ping* للتأكد من اتصال الحاسوب بالطابعة. اتبع الخطوات التالية للتحقق من الاتصال باستخدام أمر *Ping*.

1. تحقق من عنوان IP الخاص بوحدة الطباعة للاتصال الذي ترغب في التحقق منه.
يمكنك التحقق من هذا من شاشة حالة الشبكة على لوحة تحكم الطباعة، أو تقرير الاتصال، أو عمود IP Address لورقة حالة الشبكة.
2. عرض شاشة موجة أوامر جهاز الحاسوب.
اعرض شاشة التطبيق، ثم اختر **موجه الأوامر**.
3. أدخل "ping xxx.xxx.xxx.xxx"، ثم اضغط على مفتاح الإدخال.
أدخل عنوان IP الخاص بوحدة الطباعة لـ xxx.xxx.xxx.xxx.
4. تحقق من حالة الاتصال.
إذا كانت وحدة الطباعة وجهاز الحاسوب متصلين، يتم عرض الرسالة التالية.

```
Administrator: Command Prompt
c:\>ping 192.168.111.20
Pinging 192.168.111.20 with 32 bytes of data:
Reply from 192.168.111.20: bytes=32 time=88ms TTL=64
Reply from 192.168.111.20: bytes=32 time=11ms TTL=64
Reply from 192.168.111.20: bytes=32 time=15ms TTL=64
Reply from 192.168.111.20: bytes=32 time=9ms TTL=64
Ping statistics for 192.168.111.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 88ms, Average = 30ms
c:\>_
```

إذا كانت وحدة الطباعة وجهاز الحاسوب غير متصلين، يتم عرض الرسالة التالية.

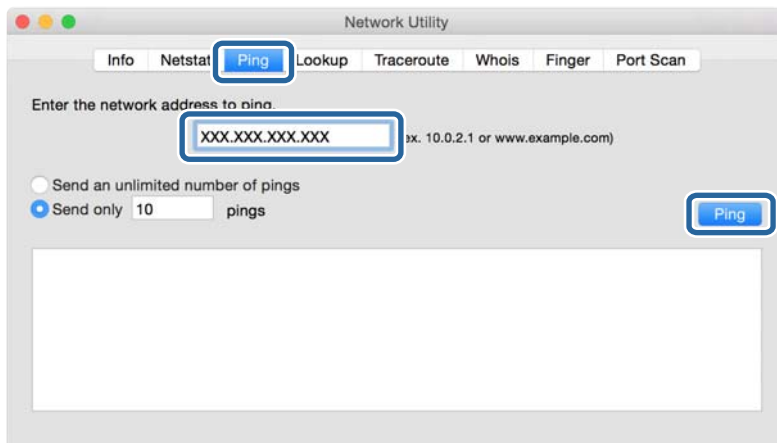
```
Administrator: Command Prompt
c:\>ping 192.168.111.30
Pinging 192.168.111.30 with 32 bytes of data:
Reply from 192.168.111.10: Destination host unreachable.
Reply from 192.168.111.10: Destination host unreachable.
Reply from 192.168.111.10: Destination host unreachable.
Reply from 192.168.111.10: Destination host unreachable.
Ping statistics for 192.168.111.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
c:\>_
```

التحقق من الاتصال باستخدام أمر *Ping* - Mac OS

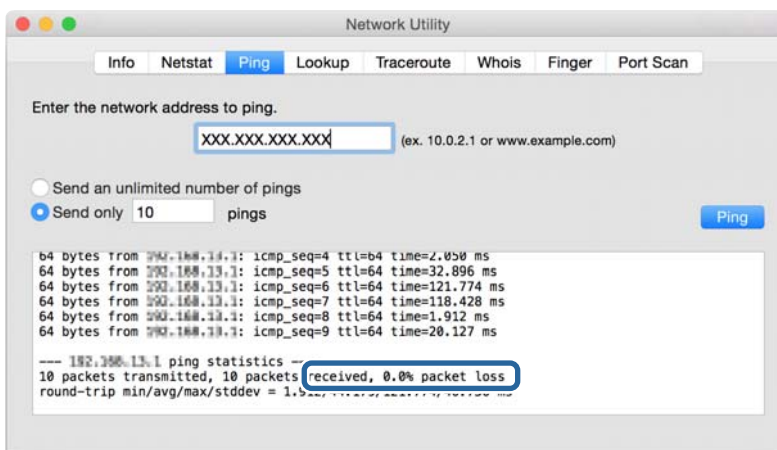
يُمكنك استخدام أمر *Ping* للتأكد من اتصال الحاسوب بالطابعة. اتبع الخطوات التالية للتحقق من الاتصال باستخدام أمر *Ping*.

حل المشكلات

1. تحقق من عنوان IP الخاص بوحدة الطباعة للاتصال الذي ترغب في التحقق منه. يمكنك التحقق من هذا من شاشة حالة الشبكة على لوحة تحكم الطباعة، أو تقرير الاتصال، أو عمود IP Address لورقة حالة الشبكة.
2. تشغيل أداة مساعدة للشبكة.
أدخل "أداة مساعدة للشبكة" في Spotlight.
3. اضغط على علامة Ping، أدخل عنوان IP الذي قمت بالتحقق منه في الخطوة رقم 1 ثم اضغط على Ping.

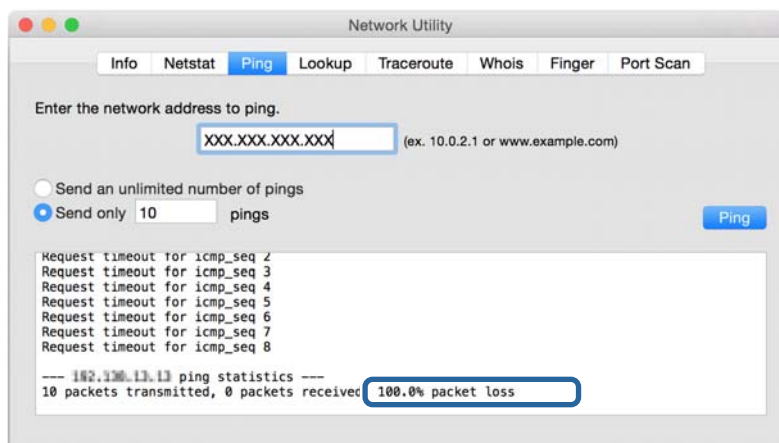


4. تحقق من حالة الاتصال. إذا كانت وحدة الطباعة وجهاز الحاسوب متصلين، يتم عرض الرسالة التالية.



حل المشكلات

إذا كانت وحدة الطباعة وجهاز الحاسوب غير متصلين، يتم عرض الرسالة التالية.



التحقق من شبكة الكمبيوتر - Windows

باستخدام موجه الأوامر، تحقق من حالة اتصال الكمبيوتر ومسار الاتصال إلى الطباعة. سيساعدك ذلك في حل المشكلات.

□ أمر ipconfig

اعرض حالة اتصال واجهة الشبكة المستخدمة حالياً من قبل الكمبيوتر.

من خلال مقارنة معلومات الإعداد مع الاتصال الفعلي، يمكنك التحقق مما إذا كان الاتصال صحيحاً أم لا. في حالة وجود العديد من خوادم DHCP على الشبكة نفسها، يمكنك معرفة العنوان الفعلي المعين إلى الكمبيوتر، وخادم DNS المشار إليه، وما إلى ذلك.

□ التنسيق: ipconfig /all

□ أمثلة:

```
Administrator: Command Prompt
c:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN2012R2
Primary Dns Suffix . . . . . : pubs.net
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : pubs.net

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . : 
Description . . . . . : Gigabit Network Connection
Physical Address. . . . . : xx-xx-xx-xx-xx-xx
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::38fb:7546:18a8:d20e%14(Preferred)
IPv4 Address. . . . . : 192.168.111.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.111.1
DHCPv6 Iaid . . . . . : 283142549
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-40-2F-45-00-1D-73-6A-44-08
DNS Servers . . . . . : 192.168.111.2
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{00000000-ABCD-EFGH-IJK-LMNOPQRSTUUV}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

c:\>
```

حل المشكلات

□ أمر pathping

يمكنك تأكيد قائمة الموجهات التي تمر عبر مضيف الوجهة وتوجيه الاتصال.

□ التنسيق: pathping xxx.xxx.xxx.xxx

□ أمثلة: pathping 192.0.2.222

```

Administrator: Command Prompt
c:\>pathping 192.168.111.20
Tracing route to EPSONAB12AB [192.168.111.20]
over a maximum of 30 hops:
 0  WIN2012R2.pubs.net [192.168.111.10]
 1  EPSONAB12AB [192.168.111.20]

Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0           0/ 100 = 0%      0/ 100 = 0%      WIN2012R2.pubs.net [192.168.111.10]
 1  38ms     0/ 100 = 0%      0/ 100 = 0%      EPSONAB12AB [192.168.111.20]

Trace complete.
c:\>_

```

إجراء اختبار الاتصال

من الطابعة أو الكمبيوتر المتصل بالمقطع نفسه المتصل به الطابعة، تحقق مما إذا كان الاتصال بالخادم والمجلد صحيحاً أم لا. سيساعدك ذلك في حل المشكلات.

خادم البريد

تحقق من الاتصال بين الطابعة وخادم البريد الإلكتروني باستخدام وظيفة اختبار الاتصال الخاصة بالطابعة.

معلومات ذات صلة

← "التحقق من اتصال خادم البريد" في الصفحة 36

خادم FTP

تحقق من اتصال خادم FTP من الكمبيوتر في المقطع نفسه. تحقق مما إذا كان يمكنك الوصول إلى خادم FTP المسجل في جهات الاتصال من مستكشف الكمبيوتر على شبكة المقطع نفسه الذي تتصل به الطابعة أم لا.

□ مثال لتحديد المسار:

□ اسم خادم FTP: eponftp

□ اسم المجلد: يدوي

□ /eponftp/manual//:ftp

في هذه الحالة، قم بتسجيل الدخول كمجهول. عند تعيين اسم المستخدم وكلمة المرور، أدخلهما في مربع الحوار المعروف في حالة فشل المصادقة، أو قم بتضمينهما على النحو التالي.

password@eponftp:username//:ftp (عندما يكون اسم المستخدم هو "ftpusername"، وكلمة المرور هي "ftppassword").

حل المشكلات

□ مثال على مقطع الشريحة نفسها.

□ عنوان IP الخاص بالطابعة: 192.168.111.12، قناع الشبكة الفرعية: 255.255.255.0

□ تأكد من الكمبيوتر أن عنوان IP هو من 192.168.111.2 إلى 192.168.111.255.

معلومات ذات صلة

← "تسجيل وجهة لجهات الاتصال باستخدام Web Config" في الصفحة 55

مجلد مشترك

تحقق من اتصال المجلد المشترك من الكمبيوتر في المقطع نفسه. تحقق مما إذا كان يمكنك الوصول إلى المجلد المشترك المسجل في جهات الاتصال من مستكشف الكمبيوتر على شبكة المقطع نفسه الذي تتصل به الطابعة أم لا.

معلومات ذات صلة

← "تسجيل وجهة لجهات الاتصال باستخدام Web Config" في الصفحة 55

خادم DNS

تحقق من خادم DNS الذي يُشار إليه بواسطة الكمبيوتر. تأكد من حالة محول الشبكة الخاص بالكمبيوتر على المقطع الشبكي نفسه الذي تتصل به الطابعة، وتأكد ما إذا كان هو إعداد DNS نفسه الخاص بالطابعة أم لا.

يُمكنك التحقق من إعداد DNS الخاص بالكمبيوتر كما يلي.

□ Windows : لوحة التحكم < الشبكة والإنترنت < مركز المشاركة والشبكة < تغيير إعدادات المحول
عندما يكون هناك العديد من واجهات الشبكة، يمكنك التحقق من خلال إدخال "ipconfig/all" في موجه الأوامر.

□ Mac OS : تفضيل النظام < الشبكة < متقدمة... < DNS

معلومات ذات صلة

← "تسجيل وجهة لجهات الاتصال باستخدام Web Config" في الصفحة 55

تهيئة إعدادات الشبكة

تعطيل شبكة Wi-Fi من خلال Web Config

تعطيل Wi-Fi من Web Config. إذا قمت بتمكين Wi-Fi أثناء اتصال بعض الأجهزة بواسطة Wi-Fi، فسيتم قطع اتصالها.

1. قم بالوصول إلى Web Config وحدد علامة التبويب **Wi-Fi < Network**، ثم حدد **Disable Wi-Fi**.

2. قم بفحص الرسالة، ثم حدد **OK**.

قطع اتصال Wi-Fi Direct (نقطة الوصول البسيط) من تهيئة الويب

قم بقطع اتصال شبكة Wi-Fi المباشرة (نقطة الوصول البسيط) من تهيئة الويب.

1. ادخل إلى Web Config وحدد علامة التبويب **Wi-Fi Direct < Network**.

حل المشكلات

2. حدد **Disable** لـ **Wi-Fi Direct**.

3. انقر فوق **Next**

4. قم بفحص الرسالة، ثم حدد **OK**.

إلغاء الاتصال بشبكة Wi-Fi من لوحة التحكم

عند إلغاء الاتصال بشبكة Wi-Fi، يتم فصل شبكة Wi-Fi.

1. اضغط على  في الشاشة الرئيسية.

2. حدد راوتر.

يتم عرض حالة الشبكة.

3. اضغط على **تغيير الإعدادات**.


4. حدد **أخرى > تعطيل Wi-Fi**.

5. تحقق من الرسالة، ثم قم ببدء الإعداد.

6. عندما يتم عرض رسالة الانتهاء، أغلق الشاشة.

تغلق الشاشة تلقائياً بعد فترة زمنية محددة.

7. أغلق شاشة إعدادات اتصال الشبكة.

8. اضغط على زر .

قطع اتصال Wi-Fi Direct (نقطة الوصول البسيط) من لوحة التحكم

ملاحظة:

عند تعطيل اتصال *Wi-Fi Direct* (نقطة الوصول البسيطة)، يتم قطع الاتصال بجميع أجهزة الكمبيوتر والأجهزة الذكية المتصلة بالطابعة في وضع *Wi-Fi Direct* (نقطة الوصول البسيطة). إذا رغبت في فصل جهاز محدد، فقم بفصله من الجهاز بدلاً من فصله من الطابعة.

1. اضغط على  في الشاشة الرئيسية.

2. حدد **Wi-Fi Direct**.

يتم عرض معلومات **Wi-Fi Direct**.

3. اضغط على **تغيير الإعدادات**.

4. حدد **تعطيل Wi-Fi Direct**.

5. اضغط على **تعطيل الإعدادات**.

6. عندما يتم عرض رسالة الانتهاء، أغلق الشاشة.

تغلق الشاشة تلقائياً بعد فترة زمنية محددة.

حل المشكلات

استعادة إعدادات الشبكة من لوحة التحكم

يمكنك استعادة جميع إعدادات الشبكة إلى الأوضاع الافتراضية.

1. حدد الإعدادات في الصفحة الرئيسية.
2. حدد إعدادات عامة <إدارة النظام> استعادة الإعدادات الافتراضية < إعدادات الشبكة.
3. قم بفحص الرسالة، ثم حدد نعم.
4. عندما يتم عرض رسالة الانتهاء، أغلق الشاشة. تغلق الشاشة تلقائياً بعد فترة زمنية محددة.

حالة المشكلة

يتعذر الوصول إلى تطبيق Web Config

لم يتم تعيين عنوان IP للطابعة.

قد لا يتم تعيين عنوان IP صالح للطابعة. قم بتكوين عنوان IP باستخدام لوحة تحكم الطابعة. يمكنك التأكد من معلومات الإعداد الحالية باستخدام ورقة حالة الشبكة أو من لوحة تحكم الطابعة.

لا يدعم متصفح الويب Encryption Strength لـ SSL/TLS.

يمكن فتح Web Config بواسطة متصفح الويب الذي يدعم تشفيرات مجموعة البيانات التالية كما يلي. تحقق من دعم التشفير في المستعرض لديك.

80 بت: AES256/AES128/3DES

112 بت: AES256/AES128/3DES

128 بت: AES256/AES128

192 بت: AES256

256 بت: AES256

انتهت صلاحية CA-signed Certificate.

إذا كانت هناك مشكلة في تاريخ انتهاء صلاحية الشهادة، يتم عرض رسالة "انتهت صلاحية الشهادة" عند التوصل بـ Web Config مع اتصال (https) SSL/TLS. إذا كانت الرسالة تظهر قبل تاريخ انتهاء صلاحية الشهادة، فتأكد من تكوين تاريخ الطابعة بشكل صحيح.

لا يتطابق الاسم الشائع للشهادة والطابعة.

إذا كان الاسم الشائع للشهادة لا يتطابق مع الطابعة، يتم عرض رسالة "اسم شهادة الأمان غير متطابق..." عند الوصول إلى تهيئة الويب باستخدام اتصال (https) SSL/TLS. يحدث ذلك بسبب عدم تطابق عناوين IP التالية.

تم إدخال عنوان IP الخاص بالطابعة إلى الاسم الشائع لإنشاء Self-signed Certificate أو CSR

يتم إدخال عنوان IP إلى متصفح الويب عند تشغيل Web Config

وبالنسبة لـ Self-signed Certificate، قم بتغيير اسم الطابعة. تم تحديث الشهادة ويمكن توصيل الطابعة.

وبالنسبة لـ CA-signed Certificate، احصل على الشهادة مرة أخرى للطابعة.

حل المشكلات

لا يتم تعيين إعداد خادم الوكيل للعنوان المحلي في متصفح الويب.

عندما يتم تعيين الطابعة لاستخدام خادم الوكيل، قم بتكوين متصفح الويب بعدم التوصيل بالعنوان المحلي عبر خادم الوكيل.

Windows:

حدد لوحة التحكم < الشبكة والإنترنت > خيارات الإنترنت < الاتصالات > إعدادات < LAN خادم وكيل، ثم قم بتكوين عدم استخدام خادم وكيل للعناوين المحلية.

Mac OS:

حدد تفضيلات النظام < الشبكة > الخيارات المتقدمة < الوكلاء، ثم قم بتسجيل العنوان المحلي لإعدادات تجاوز الوكيل للمضيفين والنطاقات.

مثال:

192.168.1.XXX: العنوان المحلي XXX.192.168.1، قناع الشبكة الفرعية 255.255.255.0

192.168.XX.XX: العنوان المحلي XXX.XXX.192.168، قناع الشبكة الفرعية 255.255.0.0

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "تعيين عنوان IP" في الصفحة 19

لا يمكن حفظ الصور الممسوحة ضوئياً في المجلد المشترك

التحقق من الرسائل على الطابعة

يتم عرض رسائل الأخطاء لوحة تحكم الطابعة عند حدوث خطأ ما.

الرسائل	الحلول
خطأ في DNS. راجع إعدادات DNS.	<p>تأكد من توافق العنوان الموجود في قائمة جهات الاتصال في الطابعة مع عنوان المجلد المشترك.</p> <p>إذا كان عنوان IP الخاص بالكمبيوتر ثابتاً وتم تعيينه يدوياً، فقم بتغيير اسم جهاز الكمبيوتر في نطاق الشبكة إلى عنوان IP.</p> <p>مثال: \\EPSON02\SCAN إلى \\192.168.xxx.xxx\SCAN</p> <p>تأكد من تشغيل جهاز الكمبيوتر وأنه ليس في وضع السكون. إذا كان الكمبيوتر في وضع السكون، فلن تتمكن من حفظ الصور الممسوحة ضوئياً في المجلد المشترك.</p> <p>قم بتعطيل برنامج جدار الحماية وبرامج الأمان مؤقتاً. إذا قام ذلك بإزالة الخطأ، تحقق من الإعدادات في برنامج الأمان.</p> <p>إذا كنت تستخدم كمبيوتر محمولاً، وتم تعيين عنوان IP كDHCP، فقد يتغير عنوان IP عند إعادة الاتصال بالشبكة. الحصول على عنوان IP مجدداً.</p> <p>حدد الإعدادات < إعدادات عامة > إعدادات الشبكة < متقدم > TCP/IP، ثم راجع إعدادات (DNS) نظام أسماء النطاقات.</p> <p>راجع إعدادات (DNS) نظام أسماء النطاقات بالنسبة للخادم، أو الكمبيوتر، أو نقطة الوصول.</p> <p>قد يختلف اسم الكمبيوتر وعنوان IP عند عدم تحديث جدول إدارة خادم DNS. تحقق من اسم الكمبيوتر وعنوان IP.</p>
خطأ بالمصادقة. تحقق من طريقة المصادقة، والحساب المصادق عليه، وكلمة المرور المصادق عليها.	<p>تأكد من صحة اسم المستخدم وكلمة المرور في جهاز الكمبيوتر وفي جهات الاتصال في الطابعة. أيضاً، تأكد من عدم انتهاء صلاحية كلمة المرور.</p> <p>راجع إعدادات الموقع.</p>

حل المشكلات

الرسائل	الحلول
خطأ في الاتصال. تحقق من اتصال Wi-Fi/الشبكة.	<input type="checkbox"/> تأكد من تمكين شبكة MS. <input type="checkbox"/> تأكد من توافق العنوان الموجود في قائمة جهات الاتصال في الطابعة مع عنوان المجلد المشترك. <input type="checkbox"/> يجب أن تتم إضافة حقوق الوصول الخاصة بالمستخدم في قائمة جهات الاتصال في علامة التثبيت المشاركة وعلامة التثبيت الأمان في خصائص المجلد المشترك. أيضاً، يجب تعيين أذونات المستخدم إلى "مسموح". <input type="checkbox"/> راجع إعدادات الموقع. <input type="checkbox"/> اطبع تقرير اتصال بالشبكة للتحقق مما إذا كانت الطابعة متصلة بالشبكة أم لا.
اسم الملف قيد الاستخدام بالفعل. أعد تسمية الملف وامسحه ضوئياً مرة أخرى.	<input type="checkbox"/> احذف الملف الذي يحمل الاسم نفسه. <input type="checkbox"/> قم بتغيير بادئة اسم الملف في إعدادات الملف.
الملف أو الملفات الممسوحة ضوئياً أكبر مما ينبغي. تم إرسال XX من الصفحات فقط. تأكد من وجود مساحة كافية في الموقع.	<input type="checkbox"/> قم بزيادة مساحة التخزين في المجلد المحدد. <input type="checkbox"/> قلل عدد المستندات. <input type="checkbox"/> قلل درجة دقة المسح الضوئي أو قم بزيادة نسبة الضغط لتصغير حجم الصورة الممسوحة ضوئياً.
Failed to connect to the FTP server. Change Communication Mode to FTP.	غير وضع الاتصال في قائمة جهات الاتصال إلى FTP. انظر دليل المستخدم للتعرف على وضع الاتصال.
Failed to connect to the FTP server. Change Communication Mode to FTPS.	غير وضع الاتصال في قائمة جهات الاتصال إلى FTPS. انظر دليل المستخدم للتعرف على وضع الاتصال.
الاتصال بالخادم غير موثوق به. تحقق مما يلي. إعدادات التاريخ/الوقت	<input type="checkbox"/> تأكد من تعيين تاريخ الطابعة ووقتها بشكل صحيح. <input type="checkbox"/> قم بتشغيل Web Config، ثم تحقق من CA Certificate. CA Certificate < Network Security <input type="checkbox"/> قم بتشغيل Web Config، ثم قم بتحديث شهادة المصدر. Root Certificate Update < Network Security
الاتصال بالخادم غير موثوق به. تحقق من شهادة CA في Epson Web Config.	قم بتشغيل Web Config، ثم استورد CA Certificate إلى الطابعة. CA Certificate < Network Security
الاتصال بالخادم غير موثوق به.	تظهر هذه الرسالة عند تلف الشهادة التي تم الحصول عليها. قم بتشغيل Web Config، ثم تحقق من CA Certificate. CA Certificate < Network Security

التحقق من النقطة التي حدث فيها الخطأ

عند حفظ الصور الممسوحة ضوئياً في المجلد المشترك، تجري عملية الحفظ على النحو التالي. يمكنك ذلك التحقق من النقطة التي حدث فيها الخطأ.

حل المشكلات

العناصر	التشغيل	رسائل الخطأ
التوصيل	قم بالاتصال بجهاز الكمبيوتر من الطابعة.	خطأ في DNS. راجع إعدادات DNS. Failed to connect to the FTP server. Change Communication Mode to FTP. Failed to connect to the FTP server. Change Communication Mode to FTPS. الاتصال بالخادم غير موثوق به. تحقق مما يلي. الاتصال بالخادم غير موثوق به. تحقق من شهادة CA في Epson Web Config. الاتصال بالخادم غير موثوق به.
تسجيل الدخول إلى جهاز الكمبيوتر	تسجيل الدخول إلى جهاز الكمبيوتر بواسطة اسم المستخدم وكلمة المرور.	خطأ بالمصادقة. تحقق من طريقة المصادقة، والحساب المصادق عليه، وكلمة المرور المصادق عليها.
التحقق من المجلد المراد حفظه	التحقق من مسار الشبكة الخاص بالمجلد المشترك.	خطأ في الاتصال. تحقق من اتصال Wi-Fi/الشبكة.
التحقق من اسم الملف	التحقق مما إذا كان هناك ملف يحمل اسماً مشابهاً للملف الذي تريد حفظه في المجلد.	اسم الملف قيد الاستخدام بالفعل. أعد تسمية الملف وامسحه ضوئياً مرة أخرى.
كتابة الملف	كتابة ملف جديد.	الملف أو الملفات الممسوحة ضوئياً أكبر مما ينبغي. تم إرسال XX من الصفحات فقط. تأكد من وجود مساحة كافية في الموقع.

حفظ الصور الممسوحة ضوئياً يستغرق وقتاً طويلاً

تحقق من النقاط التالية.

- حدد الإعدادات < إعدادات عامة < إعدادات الشبكة < متقدم < TCP/IP، ثم راجع إعدادات (DNS) نظام أسماء النطاقات.
- راجع إعدادات (DNS) نظام أسماء النطاقات بالنسبة للخادم، أو الكمبيوتر، أو نقطة الوصول.

المشكلات الحادثة عند إتاحة طابعات للمشاركة

الخادم المشترك بطيء

اتبع الخطوات أدناه إذا كانت العمليات تتم ببطء في طابعات مشتركة.

1. في كيبوتر خادم الطباعة، حدد لوحة التحكم < الأجهزة والطابعات.
2. انقر بزر الماوس الأيمن فوق رمز الطباعة (قائمة انتظار الطباعة) التي تريد إتاحتها للمشاركة، ثم حدد علامة التبويب خصائص الطباعة < عام < التفضيلات.
3. حدد تفضيلات المراقبة في علامة التبويب Utility في برنامج تشغيل الطباعة.
4. حدد Allow monitoring of shared printers.

حل المشكلات

إعدادات الطابعة في خادم الطابعة لا تظهر في الكمبيوتر العميل

اتباع الخطوات أدناه لإعادة تثبيت برنامج التشغيل في الكمبيوتر العميل.

1. في كيبوت خادام الطابعة، حدد لوحة التحكم < الأجهزة والطابعات.
2. انقر بزر الماوس الأيمن فوق رمز الطابعة التي تريد إتاحتها للمشاركة، ثم حدد علامة التبويب خصائص الطابعة < متقدم.
3. حدد افتراضيات الطابعة، واضبط إعدادات الطابعة، ثم انقر فوق موافق.
4. أزل تثبيت برنامج تشغيل الطابعة المشتركة من الكمبيوتر العميل.
5. أعد تثبيت برنامج تشغيل الطابعة في الكمبيوتر العميل.

ملاحظة:

إذا غيِّت إعدادات الطابعة في الكمبيوتر العميل، فإن إعدادات الطابعة الموجودة في خادم الطابعة (مثل الإعدادات الافتراضية) لا تظهر في الكمبيوتر العميل.

بعض الإعدادات، مثل *Select Setting* ومعرف من قبل المستخدم و *Custom Settings* و *Menu Arrangement* وما إلى ذلك، لا تظهر في الكمبيوتر العميل. يمكنك إظهار تلك الإعدادات من خلال تصدير ملف إعدادات (مثل إعداداتك المفضلة) من برنامج تشغيل الطابعة الخاص بخادم الطابعة، واستيراده إلى الكمبيوتر العميل.

ملحق

تقديم برنامج الشبكة

يوضح ما يلي البرنامج الذي يكوّن الأجهزة ويديرها.

Epson Device Admin

يُعرف Epson Device Admin على أنه برنامج تطبيق متعدد الوظائف يدير الجهاز على الشبكة. تتوفر الوظائف التالية.

- مراقبة ما يصل إلى 2000 طابعة أو ماسح ضوئي على المقطع
- إعداد تقرير مفصل، مثل حالة المستهلك أو المنتج
- تحديث البرنامج الثابت للمنتج
- إدخال الجهاز إلى الشبكة
- طبّق الإعدادات الموحدة في أجهزة متعددة.

يمكنك تنزيل Epson Device Admin من موقع الويب الخاص بدعم Epson. لمزيد من المعلومات، انظر الوثائق أو التعليمات الخاصة بتطبيق Epson Device Admin.

تشغيل Epson Device Admin (فقط Windows)

حدد كل البرامج < EPSON < Epson Device Admin < Epson Device Admin.

ملاحظة:

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

EpsonNet Config

يُعرف EpsonNet Config على أنه برنامج تطبيق يمكنه إجراء الإعدادات للجهاز على الشبكة. عند توصيل الأجهزة بالشبكة عبر الإيثرنيت، يمكنك إجراء الإعدادات، مثل تعيين عنوان IP، وتغيير طريقة الاتصال وما إلى ذلك حتى بالنسبة للأجهزة التي لم يتم تعيينها في عنوان IP. يمكن استخدام هذا أيضاً لإجراء إعدادات الشبكة في الأجهزة بدون لوحة التحكم.

ملحق

لمزيد من المعلومات، انظر الوثائق أو التعليمات الخاصة بتطبيق EpsonNet Config.



تشغيل تطبيق EpsonNet Config Windows

حدد كل البرامج < EpsonNet Config SE < EpsonNet Config < EpsonNet.

ملاحظة:

إذا ظهر تنبيه جدار الحماية، فاسمح بالوصول إلى تطبيق EpsonNet Config.

تشغيل تطبيق EpsonNet Config Mac OS

حدد الانتقال إلى < التطبيقات < Epson Software < EpsonNet < EpsonNet Config SE < EpsonNet Config < EpsonNet.

WindowsEpsonNet Print (فقط)

EpsonNet Print هو برنامج للنسخ على شبكة TCP/IP. ويتم تثبيته من البرنامج المثبت مع برنامج تشغيل الطابعة. لإجراء طباعة الشبكة، قم بإنشاء منفذ طباعة EpsonNet. توجد ميزات وقيود موضحة أدناه.

يتم عرض حالة الطابعة على شاشة المخزن المؤقت.

إذا قام بروتوكول DHCP بتغيير عنوان IP للطابعة، فإن الطابعة تظل مكتشفة.

يمكنك استخدام طابعة موجودة على قسم مختلفة من الشبكة.

يمكنك أيضاً الطباعة باستخدام أحد البروتوكولات المتنوعة.

عنوان IPv6 غير مدعوم.

EpsonNet SetupManager

EpsonNet SetupManager هو برنامج خاص بإنشاء حزمة للتثبيت البسيط للطابعة، مثل تثبيت برنامج تشغيل الطابعة، وتثبيت EPSON Status Monitor وإنشاء منفذ للطابعة. يتيح هذا البرنامج للمسؤول إنشاء حزم برمجية متميزة وتوزيعها بين المجموعات.

لمزيد من المعلومات، تفضل بزيارة موقع الويب الإقليمي لشركة Epson.

ملحق

تصدير جهات الاتصال وتسجيلها بشكل مجمع باستخدام الأداة

إذا كنت تستخدم Epson Device Admin، يمكنك إنشاء نسخة احتياطية فقط لجهات الاتصال وتحرير الملفات المصدرية، ثم تسجيلها جميعاً مرة واحدة.

يُعد ذلك مفيداً إذا كنت ترغب في إنشاء نسخة احتياطية فقط من جهات الاتصال أو عند استبدال الطابعة وترغب في نقل جهات الاتصال من الطابعة القديمة إلى الأخرى الجديدة.

تصدير جهات الاتصال

احفظ معلومات جهات الاتصال على الملف.

يمكنك تحرير الملفات المحفوظة بتنسيق sylk أو تنسيق csv باستخدام تطبيق جدول البيانات أو محرر النصوص. كما يمكنك تسجيلها جميعاً مرة واحدة بعد حذف المعلومات أو إضافتها.

يمكن حفظ المعلومات التي تتضمن عناصر الأمان مثل المعلومات الشخصية وكلمة المرور في تنسيق ثنائي بكلمة المرور. لا يمكنك تحرير الملف. حيث يمكن استخدام هذا باعتباره ملف النسخ الاحتياطي للمعلومات بما في ذلك عناصر الأمان.

1. ابدأ تشغيل Epson Device Admin.

2. حدد **Devices** في قائمة شريط المهام الجانبي.

3. حدد الجهاز الذي ترغب في تهيئته من قائمة الجهاز.

4. انقر فوق **Device Configuration** في علامة التبويب **Home** على قائمة الشريط.

عند تعيين كلمة مرور المسؤول، أدخل كلمة المرور وانقر فوق **OK**.

5. انقر فوق **Common < Contacts**.

6. حدد تنسيق التصدير من **Export < Export items**.

All Items

قم بتصدير ملف ثنائي مشفر. حدد التوقيت الذي ترغب فيه في تضمين عناصر الأمان مثل المعلومات الشخصية وكلمة المرور. لا يمكنك تحرير الملف. إذا قمت بتحديد، فيجب عليك تعيين كلمة المرور. انقر فوق **Configuration** وعين كلمة مرور يتراوح طولها بين 8 إلى 63 حرفاً بتنسيق ASCII. تُعد كلمة المرور هذه مطلوبة عند استيراد الملف الثنائي.

Items except Security Information

قم بتصدير الملفات ذات تنسيق sylk أو تنسيق csv. حدد التوقيت الذي ترغب فيه في تحرير معلومات الملف المصدر.

7. انقر فوق **Export**.

8. حدد المكان لحفظ الملف، وحدد نوع الملف، ثم انقر فوق **Save**.

تُعرض رسالة الاكتمال.

9. انقر فوق **OK**.

تأكد من حفظ الملف في المكان المحدد.

استيراد جهات الاتصال

قم باستيراد معلومات جهات الاتصال من الملف.

يمكنك استيراد الملفات المحفوظة بتنسيق SYLK أو تنسيق csv أو الملف الثنائي المنسوخ احتياطياً الذي يتضمن عناصر الأمان.

ملحق

1. ابدأ تشغيل Epson Device Admin.
2. حدد **Devices** في قائمة شريط المهام الجانبي.
3. حدد الجهاز الذي ترغب في تهيئته من قائمة الجهاز.
4. انقر فوق **Device Configuration** في علامة التبويب **Home** على قائمة الشريط. عند تعيين كلمة مرور المسؤول، أدخل كلمة المرور وانقر فوق **OK**.
5. انقر فوق **Common < Contacts**.
6. انقر فوق **Browse** على **Import**.
7. حدد الملف الذي ترغب في استرداده، ثم انقر فوق **Open**. عندما تحدد الملف الثنائي، في **Password** أدخل كلمة المرور التي قمت بتعيينها عند تصدير الملف.
8. انقر فوق **Import**. يتم عرض شاشة تأكيد.
9. انقر فوق **OK**. يتم عرض نتيجة التحقق.
- انقر فوق **Edit the information read**. انقر فوقه عندما ترغب في تحرير المعلومات بشكل فردي.
- انقر فوق **Read more file**. انقر فوقه عندما ترغب في استيراد الملفات المتعددة.
10. انقر فوق **Import**. ثم انقر فوق **OK** على شاشة إكمال الاستيراد. ارجع إلى شاشة خصائص الجهاز.
11. انقر فوق **Transmit**.
12. انقر فوق **OK** على رسالة التأكيد. تم إرسال الإعدادات إلى الطابعة.
13. على شاشة إكمال الإرسال، انقر فوق **OK**. يتم تحديد معلومات الطابعة. افتح جهات الاتصال من Web Config أو لوحة تحكم الطابعة، ثم تحقق من تحديث جهات الاتصال.

ضبط إعدادات Wi-Fi من لوحة التحكم (WPS)

يمكنك الاتصال بشبكة Wi-Fi من لوحة التحكم بالطابعة باستخدام وظيفة WPS.

معلومات ذات صلة

- ◀ "ضبط إعدادات Wi-Fi عن طريق الضغط على زر الإعداد (WPS)" في الصفحة 104
- ◀ "ضبط إعدادات Wi-Fi عن طريق إعداد رمز PIN التعريف الشخصي (WPS)" في الصفحة 105

ملحق

ضبط إعدادات Wi-Fi عن طريق الضغط على زر الإعداد (WPS)



يمكنك إعداد شبكة Wi-Fi تلقائياً بالضغط على الزر في نقطة الوصول. إذا تم الامتثال للشروط التالية، فيمكنك الإعداد باستخدام هذه الطريقة.

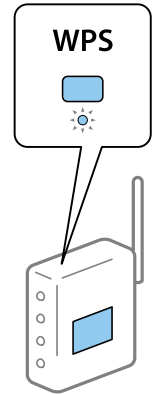
☐ توافق نقطة الوصول مع إعداد Wi-Fi المحمي (WPS).

☐ تم إنشاء الاتصال بشبكة Wi-Fi الحالية بالضغط على الزر في نقطة الوصول.

ملاحظة:

إذا لم تتمكن من إيجاد الزر أو قمت بالإعداد باستخدام البرنامج، فانظر الوثائق المرفقة مع نقطة الوصول.

1. اضغط على  |  في الشاشة الرئيسية.
2. حدد راوتر.
3. اضغط على بدء الإعداد.
- إذا تم إعداد اتصال الشبكة بالفعل، فسيتم عرض تفاصيل الاتصال. اضغط على غير إلى اتصال Wi-Fi. أو تغيير الإعدادات لتغيير الإعدادات.
4. حدد إعداد زر الضغط (WPS).
5. اضغط باستمرار على زر (WPS) في نقطة الوصول حتى وميض ضوء الحماية.



إذا كنت لا تعرف مكان زر (WPS)، أو لا توجد أزرار على نقطة الوصول، فانظر الوثائق المرفقة مع نقطة الوصول للحصول على التفاصيل.

6. اضغط على بدء الإعداد.
7. أغلق الشاشة.
تغلق الشاشة تلقائياً بعد فترة زمنية محددة.
- ملاحظة:
في حالة فشل الاتصال، قم بإعادة تشغيل نقطة الوصول ونقلها بالقرب من الطابعة، وحاول مرة أخرى. إذا كان الاتصال لا يعمل، فقم بطباعة تقرير الاتصال بالشبكة وتحقق من الحل.
8. أغلق شاشة إعدادات الاتصال بالشبكة.

ملحق

ضبط إعدادات Wi-Fi عن طريق إعداد رمز PIN التعريف الشخصي (WPS)



يمكنك الاتصال تلقائياً بنقطة الوصول باستخدام رمز التعريف الشخصي. يمكنك استخدام هذه الطريقة لتحديد ما إذا كانت نقطة الوصول قادرة على إعداد Wi-Fi المحمي (WPS). استخدم جهاز الحاسوب لإدخال رمز المعرف الشخصي في نقطة الوصول.

1. اضغط على  |  في الشاشة الرئيسية.
2. حدد راوتر.
3. اضغط على بدء الإعداد.
- إذا تم إعداد اتصال الشبكة بالفعل، فسيتم عرض تفاصيل الاتصال. اضغط على غير إلى اتصال Wi-Fi. أو تغيير الإعدادات لتغيير الإعدادات.
4. حدد أخرى < إعداد رمز PIN (WPS)
5. استخدم جهاز الحاسوب لإدخال رمز التعريف الشخصي (عدد مكون من ثمانية أرقام) معروض على لوحة التحكم بالطابعة في نقطة الوصول خلال دقيقتين.
- ملاحظة:**
انظر الوثائق المرفقة مع نقطة الوصول للحصول على تفاصيل حول إدخال رمز التعريف الشخصي.
6. اضغط على بدء الإعداد.
7. أغلق الشاشة.
- تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بتحديد إغلاق.
- ملاحظة:**
في حالة فشل الاتصال، قم بإعادة تشغيل نقطة الوصول ونقلها بالقرب من الطابعة، وحاول مرة أخرى. إذا كان الاتصال لا يعمل، فقم بطباعة تقرير الاتصال وحدد الحل.
8. أغلق شاشة إعدادات الاتصال بالشبكة.

استخدام اتصال Wi-Fi Direct (نقطة الوصول البسيط)

يعمل اتصال Wi-Fi Direct (نقطة الوصول البسيط) على التوصيل بين الطابعة والأجهزة مباشرة. نظراً لأنه يمكن توصيل الطابعة مباشرة دون المرور عبر الشبكة المتصلة، يمكن استخدامها كاتصال مؤقت للجهاز بالطابعة المتصلة بالشبكة دون ترخيص دخول.

تمكين Wi-Fi Direct (نقطة الوصول البسيط) من لوحة التحكم

1. حدد  |  في لوحة التحكم بالطابعة.
2. حدد Wi-Fi Direct.
- عند تمكين توصيل Wi-Fi Direct (نقطة الوصول البسيط)، يتم عرض معلومات اتصال Wi-Fi.
3. حدد بدء الإعداد.
4. حدد بدء الإعداد.
- عند تمكين توصيل Wi-Fi Direct (نقطة الوصول البسيط)، يتم عرض الشبكة (SSID) وكلمة المرور.


ملحق

5. أغلق الشاشة.

ملاحظة:

ومن الأجهزة الذكية، اتصل بالطابعة باستخدام الشبكة (SSID) وكلمة المرور المعروضة في لوحة التحكم الخاصة بالطابعة.

تغيير إعدادات Wi-Fi Direct (نقطة الوصول البسيط)

عند تمكين اتصال Wi-Fi Direct (نقطة الوصول البسيط)، يمكنك تغيير الإعدادات من  < Wi-Fi Direct > تغيير الإعدادات، ومن ثم تُعرض عناصر القائمة التالية.

تغيير اسم الشبكة

غير اسم الشبكة Wi-Fi Direct (نقطة الوصول البسيط) (SSID) المستخدمة لتوصيل الطابعة باسمك العشوائي. يمكنك تعيين اسم الشبكة (SSID) باستخدام مجموعة أحرف ASCII التي يتم عرضها على لوحة مفاتيح البرامج في لوحة التحكم.

عند تغيير اسم الشبكة (SSID)، يتم فصل جميع الأجهزة المتصلة. استخدم الاسم الجديد للشبكة (SSID) إذا كنت تريد إعادة الاتصال بالجهاز.

تغيير كلمة المرور

غير كلمة مرور Wi-Fi Direct (نقطة الوصول البسيط) لتوصيل الطابعة بقيمتك العشوائية. يمكنك تعيين كلمة المرور باستخدام مجموعة أحرف ASCII التي يتم عرضها على لوحة مفاتيح البرامج في لوحة التحكم.

عند تغيير كلمة المرور، يتم فصل جميع الأجهزة المتصلة. استخدم كلمة المرور الجديدة إذا كنت تريد إعادة الاتصال بالجهاز.

تعطيل Wi-Fi Direct

قم بتعطيل إعدادات Wi-Fi Direct (نقطة الوصول البسيط) الخاصة بالطابعة. عند تعطيلها، يتم قطع اتصال جميع الأجهزة المتصلة بالطابعة في اتصال شبكة Wi-Fi Direct (نقطة الوصول البسيط).

استعادة الإعدادات الافتراضية

قم باستعادة جميع إعدادات Wi-Fi Direct (نقطة الوصول البسيط) إلى إعداداتها الافتراضية.

يتم حذف معلومات اتصال شبكة Wi-Fi Direct (نقطة الوصول البسيط) الخاصة بالجهاز الذي والمحافظة في الطابعة.

ملاحظة:

كما يمكنك أيضاً الإعداد من علامة التبويب **Wi-Fi Direct < Network** في **Web Config** للإعدادات التالية.

تمكين **Wi-Fi Direct** (نقطة الوصول البسيط) أو تعطيلها

تغيير اسم الشبكة (SSID)

تغيير كلمة المرور

استعادة إعدادات **Wi-Fi Direct** (نقطة الوصول البسيط)

تغيير طريقة الاتصال

قم بتغيير طريقة الاتصال. اضبط هذا الإعداد على حالة تفعيل الشبكة.

إذا كان إعداد تعيين عنوان IP يدوياً، فتأكد مع مسؤول الشبكة ما إذا كان استخدام عنوان IP نفسه على الشبكة الجديدة ممكناً أم لا.

ملاحظة:

عند تفعيل اتصال **Wi-Fi**، يتم تعطيل اتصال الإيثرنت.

ملحق

معلومات ذات صلة

- ← "تغيير الاتصال من الاتصال بشبكة إيثرنت إلى الاتصال بشبكة Wi-Fi" في الصفحة 107
- ← "تغيير الاتصال من الاتصال بشبكة Wi-Fi إلى اتصال إيثرنت" في الصفحة 107

تغيير الاتصال من الاتصال بشبكة إيثرنت إلى الاتصال بشبكة Wi-Fi

التغيير إلى الاتصال بشبكة Wi-Fi من لوحة التحكم

قم بتغيير اتصال إيثرنت إلى الاتصال بشبكة Wi-Fi من لوحة تحكم الطابعة. تُعد طريقة الاتصال المتغيرة متماثلة مع إعدادات الاتصال بشبكة Wi-Fi في الأساس. اطلع على الموضوع الوارد في هذا الدليل حول إعدادات الاتصال بشبكة Wi-Fi من لوحة تحكم الطابعة.

معلومات ذات صلة

- ← "الاتصال بالشبكة المحلية اللاسلكية (Wi-Fi)" في الصفحة 24

التغيير إلى الاتصال بشبكة Wi-Fi باستخدام Web Config

قم بتغيير اتصال إيثرنت إلى الاتصال بشبكة Wi-Fi باستخدام Web Config.

1. ادخل إلى Web Config وحدد علامة التبويب **Wi-Fi < Network**.
عند عدم تعيين كلمة مرور المسؤول، فسجّل الدخول كمسؤول عن طريق إدخال اسم المستخدم وكلمة المرور.
2. انقر فوق **Setup**.
3. حدد SSID لنقطة الوصول وأدخل كلمة المرور.
إذا لم يتم عرض SSID الذي ترغب في الاتصال به، فحدد **Enter SSID**. ثم أدخل SSID.
4. انقر فوق **Next**.
5. تأكد من الرسالة المعروضة وانقر فوق **OK**.
6. افصل كابل إيثرنت من الطابعة.

ملاحظة:

يمكنك أيضاً تغيير طريقة الاتصال باستخدام *Epson Device Admin*. للحصول على التفاصيل، تفضل بالاطلاع على الدليل أو التعليمات حول *Epson Device Admin*.

معلومات ذات صلة

- ← "الوصول إلى تطبيق Web Config" في الصفحة 27
- ← "Epson Device Admin" في الصفحة 100

تغيير الاتصال من الاتصال بشبكة Wi-Fi إلى اتصال إيثرنت

تغيير اتصال الشبكة إلى إيثرنت باستخدام لوحة التحكم

اتبع الخطوات الموضحة أدناه لتغيير اتصال الشبكة إلى إيثرنت من Wi-Fi باستخدام لوحة التحكم.

ملحق

1. حدد الإعدادات في الصفحة الرئيسية.
2. حدد إعدادات عامة < إعدادات الشبكة > إعداد شبكة LAN السلكية.
3. اضغط على بدء الإعداد.
4. تحقق من الرسالة، ثم أغلق الشاشة.
- تغلق الشاشة تلقائياً بعد فترة زمنية محددة.
5. وصل الطابعة بجهاز توجيه باستخدام كابل الإيثرنت.

معلومات ذات صلة

← "الاتصال بشبكة الإيثرنت" في الصفحة 23

التغيير إلى الاتصال بشبكة إيثرنت باستخدام تهيئة الويب

قم بتغيير اتصال Wi-Fi إلى اتصال الإيثرنت باستخدام Web Config.

1. ادخل إلى Web Config وحدد علامة التبويب **Wi-Fi < Network**.
- عند عدم تعيين كلمة مرور المسؤول، فسجل الدخول كمسؤول عن طريق إدخال اسم المستخدم وكلمة المرور.
2. انقر فوق **Disable Wi-Fi**.
3. تحقق من الرسالة، ثم حدد موافق.
4. وصل الطابعة وموزع الشبكة (محول الشبكة المحلية) بكابل إيثرنت.

ملاحظة:

يمكنك أيضاً تغيير طريقة الاتصال باستخدام *Epson Device Admin*. للحصول على التفاصيل، تفضل بالاطلاع على دليل *Epson Device Admin* أو تعليماته.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "Epson Device Admin" في الصفحة 100

استخدام منفذ للطابعة

تستخدم الطابعة المنفذ التالي. يجب أن يسمح مسؤول الشبكة بتوفير هذه المنافذ حسب الضرورة.

ملحق

رقم المنفذ	البروتوكول	الوجهة (الخادم)	الاستخدام	المُرسل (العميل)
20	(TCP) FTP	خادم FTP	إرسال الملف (عند استخدام المسح الضوئي على مجلد الشبكة من الطابعة)	الطابعة
21				
445	(TCP) SMB	خادم الملف		
137	(UDP) NetBIOS			
138				
139	(TCP) NetBIOS			
25	(TCP) SMTP	خادم SMTP	إرسال رسالة البريد الإلكتروني (عند استخدام المسح الضوئي إلى البريد الإلكتروني من الطابعة)	
465	(TCP) SMTP SSL/TLS			
587	(TCP) SMTP STARTTLS			
110	(TCP) POP3	خادم POP	اتصال POP قبل SMTP (عند استخدام المسح الضوئي إلى البريد من الطابعة)	
5357	(TCP) WSD	كمبيوتر عميل	التحكم في خدمات الويب للأجهزة (WSD)	
20	(TCP) FTP	الطابعة	إرسال الملف (عند استخدام طباعة FTP من الطابعة)	كمبيوتر عميل
21				
3289	(UDP) ENPC	الطابعة	اكتشف الطابعة من أي تطبيق مثل EpsonNet Config، وبرنامج تشغيل الطابعة.	
161	(UDP) SNMP	الطابعة	اجمع معلومات قاعدة المعلومات الإدارية (MIB) وقم بإعدادها من تطبيق ما مثل EpsonNet Config، وبرنامج تشغيل الطابعة.	
515	(TCP) LPR	الطابعة	إرسال بيانات LPR	
9100	(RAW (Port9100) (TCP	الطابعة	إرسال بيانات RAW	
631	(TCP) IPP/IPPS	الطابعة	إعادة توجيه بيانات AirPrint (طباعة IPP/IPPS)	
3702	(UDP) WS-Discovery	الطابعة	البحث عن طابعة WSD	

إعدادات الأمان المتقدمة لـ Enterprise

في هذا الفصل، نقوم بتوضيح ميزات الأمان المتقدمة.

إعدادات الأمان ومنع وقوع المخاطر

عند توصيل الطابعة بشبكة، يمكنك الوصول إليها من مكان بعيد. وبالإضافة إلى ذلك، يمكن أن يشارك العديد من الأشخاص على الطابعة نفسها، وهو أمر مفيد في تحسين الكفاءة التشغيلية والموافقة. ومع ذلك، فإن المخاطر مثل الوصول غير القانوني، والاستخدام غير القانوني، والتلاعب بالبيانات تتزايد. إذا كنت تستخدم الطابعة في بيئة يمكن فيها الوصول إلى الإنترنت، يكون معدل التعرض للمخاطر مرتفعاً جداً. بالنسبة للطابعات التي لم تحصل على الحماية من الخارج، فسيكون من الممكن قراءة سجلات مهمة الطباعة المخزنة في الطابعة من الإنترنت. لتجنب التعرض لهذه المخاطر، فإن طابعات Epson تحتوي على مجموعة متنوعة من تقنيات الأمان. عين الطابعة حسب الضرورة وفقاً للحالات البيئية التي تم إنشاؤها باستخدام معلومات البيئة الخاصة بالعميل.

الاسم	نوع الميزة	ما يجب تعيينه	ما يتم حظره
اتصالات SSL/TLS	يتم تشفير محتوى الاتصال باستخدام اتصالات SSL/TLS عند الوصول إلى خادم Epson من الطابعة، مثل الاتصال بالكمبيوتر من خلال مستعرض ويب، أو تحديث البرنامج الثابت.	احصل على شهادة موقعة من جهة تصديق (CA)، ثم قم باستيرادها إلى الطابعة.	يحظر مسح أي معلومات خاصة بتعريف الطابعة بالشهادة الموقعة من جهة تصديق (CA) التعرض لأي عملية انتحال والوصول غير المصرح به. وبالإضافة إلى ذلك، تتم حماية محتويات اتصال SSL/TLS، ويحظر تسريب بيانات الطباعة ومعلومات الإعداد.
التحكم في البروتوكول	يتحكم في البروتوكولات والخدمات المستخدمة للاتصال بين الطابعات وأجهزة الكمبيوتر، وكذلك يمكن الميزات ويعطلها.	البروتوكول أو الخدمة التي يتم تطبيقها على الميزات المسموح بها أو المحظورة بشكل منفصل.	الحد من مخاطر الأمان التي قد تحدث من خلال الاستخدام غير المقصود عن طريق منع المستخدمين من استخدام الوظائف غير الضرورية.
تشفية IPsec/IP	يمكنك تعيينها للسماح بفصل البيانات المستلمة من عميل معين أو التي تُعد من نوع خاص وعزلها. عندما تقوم بحماية البيانات عن طريق وحدة حزمة IP (التشفير والمصادقة)، يمكنك توصيل بروتوكول غير مؤمن بسلامة.	قم بإنشاء سياسة أساسية وأخرى فردية لتعيين العميل ونوع البيانات التي يمكن أن تصل إلى الطابعة.	قم بحماية الوصول غير المعتمد، والتلاعب ببيانات الاتصال للطابعة واعتراضها.
IEEE 802.1X	لا يسمح إلا للمستخدم المصرح له الاتصال بشبكة Wi-Fi وإيثرنت فقط. لا يسمح إلا للمستخدم المسموح له باستخدام الطابعة فقط.	إعداد المصادقة لخادم RADIUS (خادم المصادقة).	قم بحماية الاستخدام والوصول غير المعتمد للطابعة.

معلومات ذات صلة

- ← "اتصال SSL/TLS بالطابعة" في الصفحة 112
- ← "التحكم باستخدام البروتوكولات" في الصفحة 120
- ← "الاتصال المشفر باستخدام تشفية IPsec/IP" في الصفحة 124
- ← "توصيل الطابعة بشبكة IEEE802.1X" في الصفحة 136

إعدادات ميزة الأمان

عند إعداد تشفية IPsec/IP أو IEEE802.1X، يوصى بالوصول إلى Web Config باستخدام SSL/TLS لتوصيل معلومات الإعدادات للحد من مخاطر الأمان مثل التلاعب أو الاعتراضات.

يمكنك أيضاً استخدام Web Config عن طريق توصيل الطابعة مباشرة بالكمبيوتر باستخدام كابل إيثرنت، ثم إدخال عنوان IP في مستعرض الويب. يمكن توصيل الطابعة في بيئة آمنة بعد إكمال إعدادات الأمان.

اتصال SSL/TLS بالطابعة

عندما يتم تعيين شهادة الخادم باستخدام اتصال SSL/TLS (طبقة مأخذ توصيل آمنة/بروتوكول أمان طبقة النقل) بالطابعة، يمكنك تشفير مسار الاتصال بين أجهزة الكمبيوتر. قم بتطبيق ذلك إذا كنت ترغب في منع الوصول عن بُعد والوصول غير المعتمد.

حول المصادقة الرقمية

CA-signed Certificate

هذه شهادة موقعة من CA (المرجع المصدق). يمكنك الحصول عليها لتقديمها إلى المرجع المصدق. تقر هذه الشهادة بوجود الطابعة واستخدامها لاتصال SSL/TLS بحيث يمكنك ضمان سلامة اتصال البيانات. عندما يتم استخدامها لاتصال SSL/TLS، تُستخدم باعتبارها شهادة الخادم. عندما يتم تعيينها إلى تصفية IPsec/IP أو اتصال IEEE802.1x، تُستخدم باعتبارها شهادة عميل.

شهادة المرجع المصدق (CA)

هذه الشهادة تقع ضمن سلسلة CA-signed Certificate، ويُطلق عليها أيضاً شهادة المرجع المصدق الوسيطة. يتم استخدامها من قبل متصفح الويب للتحقق من مسار شهادة الطابعة عند الوصول إلى خادم الجهة الأخرى أو تكوين الويب. للحصول على شهادة المرجع المصدق (CA)، حدد توقيت التحقق من مسار الوصول إلى شهادة الخادم من الطابعة. بالنسبة للطابعة، عين لتوضيح مسار CA-signed Certificate لاتصال SSL/TLS. يمكنك الحصول على شهادة المرجع المصدق (CA) الخاصة بالطابعة من المرجع المصدق حيث يتم إصدار شهادة المرجع المصدق (CA). كما يمكنك أيضاً الحصول على شهادة المرجع المصدق (CA) المستخدمة للتحقق من خادم الجهة الأخرى من المرجع المصدق الذي أصدر CA-signed Certificate الخاصة بالخادم الآخر.

Self-signed Certificate

هذه هي الشهادة التي توقعها الطابعة وتصدرها بنفسها. إنها تُسمى أيضاً شهادة الجذر. وذلك لأن المصدر يقرّ بنفسه، فهو غير موثوق ولا يمكنه منع انتحال الهوية. استخدمها عند ضبط إعداد الأمان وإجراء اتصال SSL/TLS بسيط بدون CA-signed Certificate. إذا كنت تستخدم هذه الشهادة لاتصال SSL/TLS، فقد يتم عرض تنبيه الأمان على متصفح الويب لأن الشهادة غير مسجلة على متصفح الويب. يمكنك استخدام Self-signed Certificate فقط لاتصال SSL/TLS.

معلومات ذات صلة

- ← "الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها" في الصفحة 112
- ← "حذف شهادة موقعة من المرجع المصدق (CA)" في الصفحة 117
- ← "تحديث شهادة موقعة ذاتياً" في الصفحة 119

الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها

الحصول على شهادة موقعة من المرجع المصدق (CA)

للحصول على شهادة موقعة من المرجع المصدق (CA)، قم بإنشاء CSR (طلب توقيع شهادة) وقدمه إلى المرجع المصدق. يمكنك إنشاء طلب CSR باستخدام تطبيق Web Config وجهاز كمبيوتر. اتبع الخطوات الخاصة بإنشاء طلب CSR والحصول على شهادة موقعة من المرجع المصدق (CA) باستخدام تطبيق Web Config. عند إنشاء طلب CSR باستخدام تطبيق Web Config، تكون الشهادة بتنسيق PEM/DER.

إعدادات الأمان المتقدمة لـ Enterprise

1. ادخل إلى Web Config, ثم حدد علامة التبويب **Network Security**. بعد ذلك، حدد **SSL/TLS < Certificate**. أو **IPsec/IP Filtering** **Client Certificate < IEEE802.1X** أو **Client Certificate < Certificate**.
مهما اخترت، يمكنك الحصول على الشهادة نفسها واستخدامها في الأمور الشائعة.
2. انقر فوق خيار **Generate** الخاص بإعداد **CSR**.
يتم فتح صفحة إنشاء طلب **CSR**.
3. أدخل قيمة لكل عنصر.
ملاحظة:
يتمتع طول المفتاح والاختصارات المتاحة وفقاً للمرجع المصدق. قم بإنشاء طلب وفقاً لقواعد كل مرجع مصدق.
4. انقر فوق **OK**.
يتم عرض رسالة اكتمال الطلب.
5. حدد علامة التبويب **Network Security**. بعد ذلك، حدد **SSL/TLS < Certificate**. أو **IPsec/IP Filtering < Client Certificate** أو **Client Certificate < IEEE802.1X**.
6. انقر فوق أحد أزرار تنزيل **CSR** وفقاً للتنسيق المحدد بواسطة كل مرجع مصدق لتنزيل طلب **CSR** على الكمبيوتر.



هام:

تجنب إنشاء **CSR** مرة أخرى. عند القيام بذلك، قد لا تتمكن من استيراد **CA-signed Certificate** التي تم إصدارها.

7. أرسل **CSR** إلى المرجع المصدق، ثم احصل على **CA-signed Certificate**.
اتباع القواعد الخاصة بكل مرجع مصدق حول طريقة الإرسال والنموذج.
8. احفظ **CA-signed Certificate** التي تم إصدارها إلى أحد أجهزة الكمبيوتر المتصلة بالطابعة.
يكتمل الحصول على **CA-signed Certificate** عندما تحفظ إحدى الشهادات في إحدى الواجهات.

إعدادات الأمان المتقدمة لـ Enterprise

عناصر إعداد طلب CSR

العناصر	الإعدادات والشرح
Key Length	حدد طول مفتاح طلب CSR.
Common Name	يمكن إدخال عدة أحرف تتراوح ما بين حرف واحد حتى 128 حرفاً. إذا كان هذا عنوان IP، فلا بد أن يكون عنوان IP ثابتاً. يمكنك إدخال من 1 إلى 5 عناوين IPv4، وعناوين IPv6، والأسماء المضيفة، و FQDNs من خلال فصلها بفواصل. كما يتم تخزين أول عنصر بالاسم الشائع، ويتم تخزين العناصر الأخرى إلى حقل الاسم المستعار لموضوع الشهادة. مثال: عنوان IP الخاص بالطابعة: 192.0.2.123، اسم الطابعة: EPSONA1B2C3 Common Name : EPSONA1B2C3 ,192.0.2.123 ,EPSONA1B2C3.local
/Organizational Unit /Organization State/Province /Locality	يمكنك إدخال ما بين 0 إلى 64 حرفاً (Organizational Unit) ولا يمكن أن تتجاوز 55 حرفاً) بتنسيق ASCII (0x20-0x7E). يمكنك فصل الأسماء المميزة باستخدام الفواصل.
Country	أدخل رمز الدولة على شكل عدد مكون من رقمين مفصولين باستخدام ISO-3166.

معلومات ذات صلة

← "الحصول على شهادة موقعة من المرجع المصدق (CA)" في الصفحة 112

استيراد شهادة موقعة من المرجع المصدق (CA)

قم باستيراد CA-signed Certificate التي تم الحصول عليها إلى الطابعة.

هام!

- تأكد من تعيين تاريخ الطابعة ووقتها بشكل صحيح. قد تكون الشهادة غير صالحة.
- إذا كنت تحصل على شهادة باستخدام طلب CSR تم إنشاؤه من تطبيق *Web Config*، فسيمكنك استيراد الشهادة مرةً واحدة.

1. ادخل إلى Web Config ثم حدد علامة التبويب **Network Security**. بعد ذلك، حدد **SSL/TLS < Certificate**، أو **IPsec/IP Filtering < Client Certificate** أو **Client Certificate < IEEE802.1X**.

2. انقر فوق **Import**

يتم فتح صفحة استيراد شهادة.

3. أدخل قيمة لكل عنصر. عين **CA Certificate 1** و **CA Certificate 2** عند التحقق من مسار الشهادة على متصفح الويب الذي يصل إلى الطابعة.

بناءً على مكان إنشاء طلب CSR وتنسيق ملف الشهادة، يمكن أن تتنوع الإعدادات المطلوبة. أدخل قيمًا للعناصر المطلوبة وفقاً لما يلي.

شهادة بتنسيق PEM/DER تم الحصول عليها من تطبيق Web Config

Private Key: لا تقم بالتكوين لاحتواء الطابعة على مفتاح خاص.

Password: يجب عدم التكوين.

CA Certificate 2/CA Certificate 1: اختياري

شهادة بتنسيق PEM/DER تم الحصول عليها من الكمبيوتر

Private Key: يجب أن تقوم بتعيينه.

Password: يجب عدم التكوين.

CA Certificate 2/CA Certificate 1: اختياري

شهادة بتنسيق PKCS#12 تم الحصول عليها من الكمبيوتر

Private Key: يجب عدم التكوين.

Password: اختياري

CA Certificate 2/CA Certificate 1: يجب عدم التكوين.

4. انقر فوق **OK**.

يتم عرض رسالة اكتمال الطلب.

ملاحظة:

انقر فوق **Confirm** للتأكد من معلومات الشهادة.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "عناصر إعداد استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 116

إعدادات الأمان المتقدمة لـ Enterprise

عناصر إعداد استيراد شهادة موقعة من المرجع المصدق (CA)

The screenshot shows the EPSON Network Security configuration interface. The 'SSL/TLS > Certificate' section is active. It includes the following fields and controls:

- Server Certificate:** A dropdown menu set to 'Certificate (PEM/DER)' with a 'Browse...' button.
- Private Key:** A text field with a 'Browse...' button.
- Password:** A text field.
- CA Certificate 1:** A text field with a 'Browse...' button.
- CA Certificate 2:** A text field with a 'Browse...' button.

A note at the bottom of the form reads: "Note: it is recommended to communicate via HTTPS for importing a certificate." At the bottom of the page, there are 'OK' and 'Back' buttons.

العناصر	الإعدادات والشرح
Client Certificate أو Server Certificate	حدد تنسيق الشهادة. بالنسبة لاتصال SSL/TLS، يتم عرض Server Certificate. بالنسبة لتصفية IPsec/IP أو IEEE802.1x، يتم عرض Client Certificate.
Private Key	إذا كنت تحصل على شهادة بتنسيق PEM/DER باستخدام طلب CSR تم إنشاؤه من جهاز كمبيوتر، فحدد ملف مفتاح خاص يطابق الشهادة.
Password	إذا كان تنسيق الملف هو Certificate with Private Key (PKCS#12)، فأدخل كلمة المرور. لتشفير المفتاح الخاص الذي تم تعيينه عندما تحصل على الشهادة.
CA Certificate 1	إذا كان تنسيق الشهادة Certificate (PEM/DER)، فقم باستيراد شهادة من المرجع المصدق CA-signed Certificate الذي يصدر شهادة الخادم. حدد ملفاً عند الضرورة.
CA Certificate 2	إذا كان تنسيق الشهادة Certificate (PEM/DER)، فقم باستيراد شهادة من المرجع المصدق الذي يصدر CA Certificate 1. حدد ملفاً عند الضرورة.

معلومات ذات صلة

← "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 115

حذف شهادة موقعة من المرجع المصدق (CA)

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

هام: 

إذا كنت تحصل على شهادة باستخدام طلب CSR تم إنشاؤه من تطبيق *Web Config*، فلن تتمكن من استيراد الشهادة المحذوفة مرةً أخرى. في هذه الحالة، قم بإنشاء طلب CSR واحصل على الشهادة مرةً أخرى.

1. ادخل إلى تهيئة الويب، ثم حدد علامة التبويب **Network Security**. بعد ذلك، حدد **SSL/TLS < Certificate** أو **IPsec/IP Filtering < Client Certificate** أو **Client Certificate < IEEE802.1X**.
2. انقر فوق **Delete**.
3. قم بالتأكيد على أنك تريد حذف الشهادة في الرسالة المعروضة.

تهيئة CA Certificate

عند تعيين CA Certificate، يمكنك التحقق من المسار إلى شهادة المرجع المصدق (CA) من الخادم الذي تصل إليه الطابعة. يمكن لهذا أن يمنع انتحال الهوية.

يمكنك الحصول على CA Certificate من المرجع المصدق حيث يتم إصدار CA-signed Certificate.

معلومات ذات صلة

- ← "الوصول إلى تطبيق Web Config" في الصفحة 27
- ← "عناصر إعداد طلب CSR" في الصفحة 114
- ← "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 115

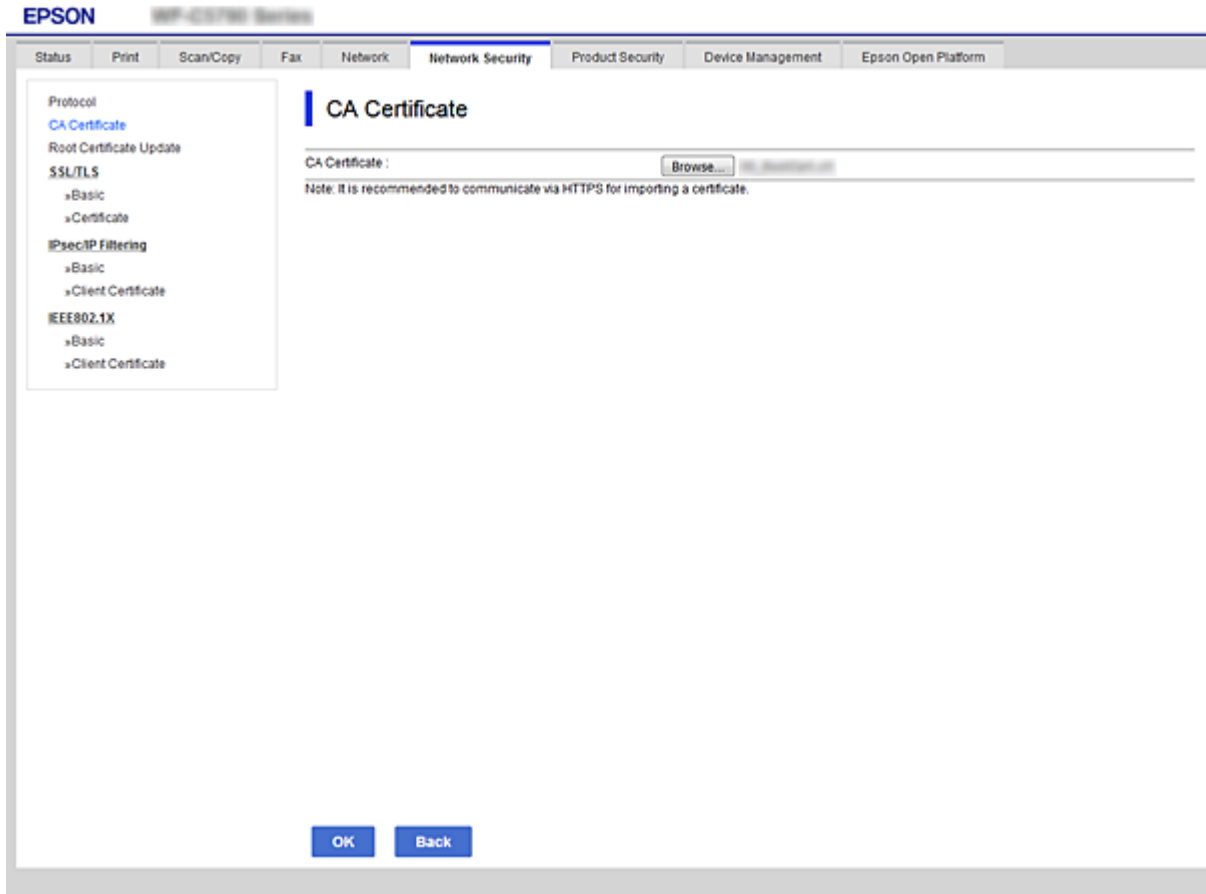
استيراد CA Certificate

قم باستيراد CA Certificate إلى الطابعة.

1. قم بالوصول إلى Web Config ثم حدد علامة التبويب **Network Security < CA Certificate**.
2. انقر فوق **Import**.

إعدادات الأمان المتقدمة لـ Enterprise

3. حدد CA Certificate الذي تريد استيرادها.



4. انقر فوق OK.

عند اكتمال الاستيراد، يتم الرجوع إلى شاشة CA Certificate مع عرض CA Certificate التي تم استيرادها.

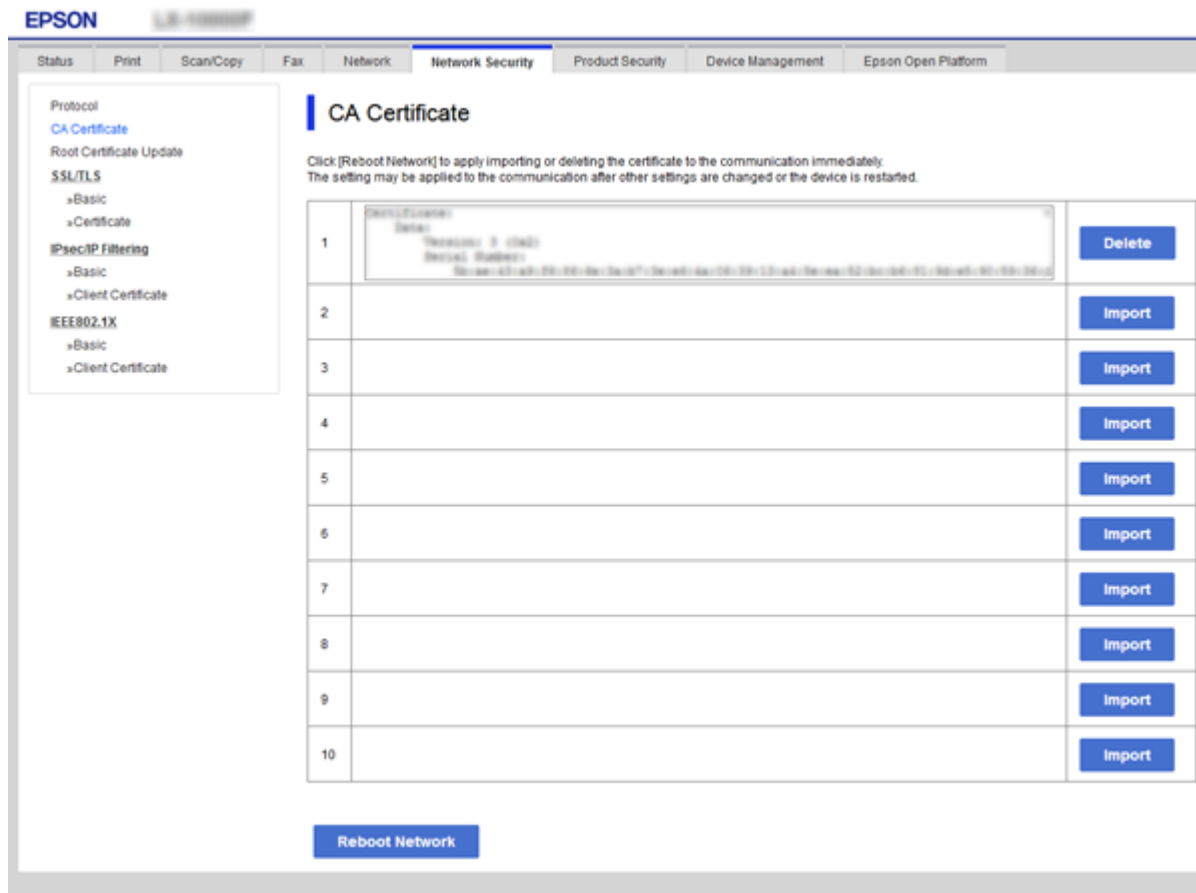
حذف CA Certificate

يمكنك حذف CA Certificate التي تم استيرادها.

1. ادخل إلى Web Config ثم حدد علامة التبويب CA Certificate < Network Security.

إعدادات الأمان المتقدمة لـ Enterprise

2. انقر فوق **Delete** بجانب CA Certificate التي ترغب في حذفها.



3. قم بالتأكيد على أنك تريد حذف الشهادة في الرسالة المعروضة.

4. انقر فوق **Reboot Network**، ثم تحقق من عدم إدراج شهادة المرجع المصدق (CA) المحذوفة على الشاشة المحدثة.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

تحديث شهادة موقعة ذاتياً

لأنه يتم إصدار Self-signed Certificate بواسطة الطابعة، يمكنك تحديثها عند انتهاء صلاحيتها أو عند تغيير المحتوى الموصوف.

1. ادخل إلى Web Config وحدد علامة التبويب **Network Security < SSL/TLS < Certificate**.

2. انقر فوق **Update**.

3. أدخل **Common Name**.

يمكنك إدخال ما يصل إلى 5 عناوين IPv4، وعناوين IPv6، وأسماء المضيفين، وأسماء FQDN بين 1 إلى 128 حرف وفصلها باستخدام الفواصل. يتم تخزين أول معلمة في الاسم الشائع، ويتم تخزين الباقي في حقل الاسم المستعار لموضوع الشهادة.

مثال:

عنوان IP للطابعة: 192.0.2.123، اسم الطابعة: EPSONA1B2C3

اسم شائع: EPSONA1B2C3، EPSONA1B2C3.local، 192.0.2.123

إعدادات الأمان المتقدمة لـ Enterprise

4. حدد فترة صلاحية للشهادة.

5. انقر فوق **Next**.

يتم عرض رسالة تأكيد.

6. انقر فوق **OK**.

الطابعة قيد التحديث.

ملاحظة:

يمكنك التحقق من معلومات الشهادة من علامة التبويب **Network Security < SSL/TLS < Certificate < Self-signed Certificate** والنقر فوق **Confirm**.

معلومات ذات صلة

← ["الوصول إلى تطبيق Web Config" في الصفحة 27](#)

التحكم باستخدام البروتوكولات

يمكنك الطابعة باستخدام مجموعة متنوعة من الممرات والبروتوكولات. يمكنك خفض المخاطر الأمنية غير المقصودة من خلال تقييد الطابعة من ممرات محددة أو عن طريق التحكم في الوظائف المتاحة.

التحكم في البروتوكولات

قم بتهيئة إعدادات البروتوكول.

1. ادخل إلى Web Config ثم حدد علامة التبويب **Protocol < Network Security**.

2. قم بتهيئة كل عنصر.

3. انقر فوق **Next**.

4. انقر فوق **OK**.

تم تطبيق الإعدادات على الطابعة.

البروتوكولات التي تستطيع تمكينها أو تعطيلها

البروتوكول	الوصف
Bonjour Settings	يمكنك تحديد إمكانية استخدام Bonjour. يتم استخدام Bonjour للبحث عن الأجهزة، وللطابعة، وما إلى ذلك.
iBeacon Settings	يمكنك أيضاً تمكين وظيفة إرسال iBeacon أو تعطيلها. عند تمكينها، يمكنك البحث عن الطابعة من الأجهزة التي تدعم iBeacon.
SLP Settings	من الممكن أيضاً تمكين وظيفة SLP أو تعطيلها. تُستخدم SLP مع وظيفتي المسح الضوئي بالدفع وبحث الشبكة في EpsonNet Config.
WSD Settings	من الممكن أيضاً تمكين وظيفة WSD أو تعطيلها. عند تمكين هذه الخاصية، يمكنك إضافة أجهزة WSD والطابعة من منفذ WSD.
LLTD Settings	من الممكن أيضاً تمكين وظيفة LLTD أو تعطيلها. عند تمكينها، يتم عرضها أيضاً على خريطة شبكة Windows.

إعدادات الأمان المتقدمة لـ Enterprise

البروتوكول	الوصف
LLMNR Settings	من الممكن أيضاً تمكين وظيفة LLMNR أو تعطيلها. عند تمكينها، يمكنك استخدام تحليل الاسم بدون NetBIOS حتى وإن لم يمكنك استخدام DNS.
LPR Settings	يمكنك تحديد ما إذا كان يجب السماح بطباعة LPR أم لا. عند تمكينها، يمكنك الطباعة من منفذ LPR.
RAW (Port9100) Settings	يمكنك تحديد ما إذا كان يجب السماح بالطباعة من منفذ RAW (منفذ 9100) أم لا. عند تمكينها، يمكنك الطباعة من منفذ RAW (منفذ 9100).
IPP Settings	يمكنك تحديد ما إذا كان يمكن السماح بالطباعة من IPP أم لا. عند تمكين هذه الخاصية، يمكنك الطباعة عبر الإنترنت.
FTP Settings	يمكنك تحديد ما إذا كان يجب السماح بطباعة FTP أم لا. عند تمكينها، يمكنك الطباعة عبر خادم FTP.
SNMPv1/v2c Settings	يمكنك تحديد ما إذا كان يجب تمكين SNMPv1/v2c أم لا. حيث تستخدم لإعداد الأجهزة والمراقبة وما إلى ذلك.
SNMPv3 Settings	يمكنك تحديد ما إذا كان يجب تمكين SNMPv3 أم لا. يتم استخدام ذلك لإعداد الأجهزة المشفرة، والمراقبة، وما إلى ذلك.

عناصر إعداد البروتوكول

Bonjour Settings

العناصر	إعداد القيمة والوصف
Use Bonjour	حدد هذه الخاصية للبحث عن الجهاز أو استخدامه من خلال Bonjour.

إعدادات الأمان المتقدمة لـ Enterprise

العناصر	إعداد القيمة والوصف
Bonjour Name	يعرض اسم Bonjour.
Bonjour Service Name	يعرض اسم خدمة Bonjour.
Location	يعرض اسم موقع Bonjour.
Top Priority Protocol	حدد بروتوكول الأولوية القصوى لطباعة Bonjour.
Wide-Area Bonjour	عين ما إذا كنت ترغب في استخدام Wide-Area Bonjour أم لا.

iBeacon Settings

العناصر	إعداد القيمة والوصف
Enable iBeacon Transmission	حدد هذا العنصر لتمكين وظيفة إرسال iBeacon.

SLP Settings

العناصر	إعداد القيمة والوصف
Enable SLP	حدد هذا العنصر لتمكين وظيفة SLP. يُستخدم هذا العنصر مثل بحث الشبكة في EpsonNet Config.

WSD Settings

العناصر	إعداد القيمة والوصف
Enable WSD	حدد هذا العنصر لتمكين إضافة أجهزة تستخدم WSD، وإجراء الطباعة والمسح الضوئي من منفذ WSD.
Printing Timeout (sec)	أدخل قيمة مهلة الاتصال لطباعة WSD في مدة تتراوح بين 3 إلى 3600 ثانية.
Device Name	يعرض اسم جهاز WSD.
Location	يعرض اسم موقع WSD.

LLTD Settings

العناصر	إعداد القيمة والوصف
Enable LLTD	حدد هذا العنصر لتمكين LLTD. يتم عرض الطابعة في خريطة شبكة Windows.
Device Name	يعرض اسم جهاز LLTD.

LLMNR Settings

العناصر	إعداد القيمة والوصف
Enable LLMNR	حدد هذا العنصر لتمكين LLMNR. يمكنك استخدام تحليل الاسم بدون NetBIOS حتى وإن لم يمكنك استخدام DNS.

LPR Settings

إعدادات الأمان المتقدمة لـ Enterprise

العناصر	إعداد القيمة والوصف
Allow LPR Port Printing	حدّد هذا العنصر للسماح بالطباعة من منفذ LPR.
Printing Timeout (sec)	أدخل قيمة المهلة لطباعة LPR في مدة تتراوح بين 0 إلى 3600 ثانية. وعند الرغبة في عدم استخدام المهلة أدخل 0.

RAW(Port9100) Settings

العناصر	إعداد القيمة والوصف
Allow RAW(Port9100) Printing	حدد هذا العنصر للسماح بالطباعة عبر منفذ RAW (المنفذ 9100).
Printing Timeout (sec)	أدخل قيمة المهلة لـ RAW في مدة تتراوح بين 0 إلى 3600 ثانية (المنفذ 9100). وعند الرغبة في عدم استخدام المهلة أدخل 0.

IPP Settings

العناصر	إعداد القيمة والوصف
Enable IPP	حدد هذا العنصر لتمكين اتصال IPP. يتم عرض الطابعات التي تدعم IPP فقط.
Allow Non-secure Communication	حدّد هذا العنصر للسماح للطباعة بالاتصال دون أي تدابير أمنية (IPP).
Communication Timeout (sec)	أدخل قيمة المهلة لطباعة IPP في مدة تتراوح بين 0 إلى 3600 ثانية.
URL (الشبكة)	لعرض عناوين URL (http وhttps) الخاصة بـ IPP عندما تكون الطابعة متصلة بالشبكة. يُعد URL قيمة مشتركة لعنوان IP الخاص بالطابعة ورقم المنفذ واسم طابعة IPP.
URL (شبكة Wi-Fi Direct)	يعرض URLs (http وhttps) لـ IPP عندما تكون الطابعة متصلة بشبكة Wi-Fi Direct. يُعد URL قيمة مشتركة لعنوان IP الخاص بالطابعة ورقم المنفذ واسم طابعة IPP.
Printer Name	يعرض اسم طابعة IPP.
Location	يعرض موقع IPP.

FTP Settings

العناصر	إعداد القيمة والوصف
Enable FTP Server	حدّد هذا العنصر لتمكين طباعة FTP. يتم عرض الطابعات التي تدعم طباعة FTP فقط.
Communication Timeout (sec)	أدخل قيمة المهلة لاتصال FTP في مدة تتراوح بين 0 إلى 3600 ثانية. وعند الرغبة في عدم استخدام المهلة أدخل 0.

SNMPv1/v2c Settings

العناصر	إعداد القيمة والوصف
Enable SNMPv1/v2c	حدّد هذا العنصر لتمكين SNMPv1/v2c.
Access Authority	حدّد حق الوصول عند تمكين SNMPv1/v2c. حدّد Read Only أو Read/Write .

إعدادات الأمان المتقدمة لـ Enterprise

العناصر	إعداد القيمة والوصف
Community Name (Read Only)	أدخل من 0 إلى 32 (0x20 ASCII إلى 0x7E) حرفًا.
Community Name (Read/Write)	أدخل من 0 إلى 32 (0x20 ASCII إلى 0x7E) حرفًا.

SNMPv3 Settings

العناصر	إعداد القيمة والوصف
Enable SNMPv3	يتم تمكين SNMPv3 عند تحديد المربع.
User Name	أدخل عددًا من الأحرف يتراوح بين حرف واحد إلى 32 حرفًا باستخدام الأحرف ذات البايث الواحد.
Authentication Settings	
Algorithm	حدد خوارزمية للمصادقة لـ SNMPv3.
Password	أدخل كلمة مرور للمصادقة لـ SNMPv3. أدخل ما بين 8 إلى 32 حرفًا بتنسيق ASCII (0x20-0x7E). إذا لم تحدد ذلك، فاتركه فارغًا.
Confirm Password	أدخل كلمة المرور التي قمت بتكوينها للتأكيد.
Encryption Settings	
Algorithm	حدد خوارزمية للتشفير لـ SNMPv3.
Password	أدخل كلمة مرور للتشفير لـ SNMPv3. أدخل ما بين 8 إلى 32 حرفًا بتنسيق ASCII (0x20-0x7E). إذا لم تحدد ذلك، فاتركه فارغًا.
Confirm Password	أدخل كلمة المرور التي قمت بتكوينها للتأكيد.
Context Name	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.

الاتصال المشفر باستخدام تصفية IPsec/IP

حول IPsec/IP Filtering

يمكنك تصفية البيانات الواردة إلى الشبكة حسب عناوين IP، والخدمات، والمنفذ باستخدام وظيفة تصفية IPsec/IP. من خلال تجميع عوامل التصفية، يمكنك تكوين الطابعة لقبول أجهزة تابعة وبيانات محددة أو منع أيٍ منهما. بالإضافة إلى هذا، يمكنك تحسين مستوى الأمان من خلال استخدام بروتوكول IPsec.

ملاحظة:

أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows Vista أو أحدث أو Windows Server 2008 أو أحدث تدعم IPsec.

تكوين السياسة الافتراضية

لتصفية البيانات الواردة إلى الشبكة، قم بتكوين السياسة الافتراضية. تسري السياسة الافتراضية على جميع المستخدمين أو المجموعات المتصلة بالطابعة. للتحكم بصورة أكثر دقة في المستخدمين أو مجموعات المستخدمين، قم بتكوين سياسات المجموعة.

إعدادات الأمان المتقدمة لـ Enterprise

1. ادخل إلى Web Config ثم حدد علامة التبويب **Basic < IPsec/IP Filtering < Network Security**.
2. أدخل قيمة لكل عنصر.
3. انقر فوق **Next**.
- يتم عرض رسالة تأكيد.
4. انقر فوق **OK**.
- الطابعة قيد التحديث.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "عناصر إعداد Default Policy" في الصفحة 125

عناصر إعداد Default Policy

Default Policy

العناصر	الإعدادات والشرح
IPsec/IP Filtering	يمكنك تمكين ميزة تصفية IPsec/IP أو تعطيلها.

Access Control

قم بتكوين طريقة تحكم لنقل حزم بيانات IP.

العناصر	الإعدادات والشرح
Permit Access	حدد هذه الطريقة للسماح بمرور حزم بيانات IP المكونة.
Refuse Access	حدد هذه الطريقة لرفض مرور حزم بيانات IP المكونة.
IPsec	حدد هذه الطريقة للسماح بمرور حزم بيانات IPsec المكونة.

إعدادات الأمان المتقدمة لـ Enterprise

IKE Version

حدد IKEv1 أو IKEv2 لـ IKE Version. حدد أحدهما وفقاً للجهاز المتصل به الطابعة.

IKEv1

يتم عرض العناصر التالية عند تحديد IKEv1 لـ IKE Version.

العناصر	الإعدادات والشرح
Authentication Method	لتحديد Certificate ، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدماً.
Pre-Shared Key	إذا قمت بتحديد Pre-Shared Key من أجل Authentication Method ، فأدخل مفتاحاً مشتركاً مسبقاً مكوناً من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 127 حرفاً.
Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.

IKEv2

يتم عرض العناصر التالية عند تحديد IKEv2 لـ IKE Version.

العناصر	الإعدادات والشرح
Local	Authentication Method لتحديد Certificate ، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدماً.
ID	ID Type إذا قمت بتحديد Pre-Shared Key لـ Authentication Method ، فحدد نوع معرف الطابعة.
	ID أدخل معرف الطابعة الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، "#"، و"=" بدلاً من الحرف الأول. Distinguished Name : أدخل من 1 إلى 255 بايت (0x20 إلى 0x7E) حرفاً. يجب عليك إدراج "=". IP Address : أدخل تنسيق IPv4 أو IPv6. FQDN : أدخل مزيجاً من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفاً باستخدام A-Z، وa-z، و0-9، و"-، و"نقطة (.)". Email Address : أدخل من 1 إلى 255 بايت (0x20 إلى 0x7E) حرفاً. يجب عليك إدراج "@". Key ID : أدخل من 1 إلى 255 بايت (0x20 إلى 0x7E) حرفاً.
	Pre-Shared Key إذا قمت بتحديد Pre-Shared Key من أجل Authentication Method ، فأدخل مفتاحاً مشتركاً مسبقاً مكوناً من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 127 حرفاً.
Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.

إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح
Remote	Authentication Method لتحديد Certificate، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدماً.
ID Type	إذا حددت Authentication Method لـ Pre-Shared Key، فحدد نوع معرف الجهاز الذي تريد مصادقته.
ID	أدخل معرف الطابعة الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، "#"، و"=" بدلاً من الحرف الأول. Distinguished Name : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفاً. يجب عليك إدراج "=". IP Address : أدخل تنسيق IPv4 أو IPv6. FQDN : أدخل مزيجاً من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفاً باستخدام A-Z، و a-z، و 0-9، و "-"، و نقطة (.). Email Address : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفاً. يجب عليك إدراج "@". Key ID : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفاً.
Pre-Shared Key	إذا قمت بتحديد Pre-Shared Key من أجل Authentication Method، فأدخل مفتاحاً مشتركاً مسبقاً مكوناً من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 127 حرفاً.
Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.

Encapsulation

إذا قمت بتحديد IPsec من أجل Access Control، فلا بد أن تقوم بتكوين وضع تغليف.

العناصر	الإعدادات والشرح
Transport Mode	إذا كنت تستخدم الطابعة على شبكة LAN نفسها فقط، فحدد هذا. يتم تشفير حزم بيانات IP الطبقة 4 أو ما بعدها.
Tunnel Mode	إذا كنت تستخدم طابعة على شبكة تدعم استخدام الإنترنت مثل IPsec-VPN، فحدد هذا الخيار. يتم تشفير عنوان حزم بيانات IP وبياناتها. Remote Gateway(Tunnel Mode) : إذا قمت بتحديد Tunnel Mode من أجل Encapsulation، فأدخل عنوان البوابة الافتراضي المكون من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 39 حرفاً.

Security Protocol

إذا قمت بتحديد IPsec من أجل Access Control، فحدد خياراً.

العناصر	الإعدادات والشرح
ESP	حدد هذا الخيار لضمان سلامة المصادقة والبيانات وتشفير البيانات.
AH	حدد هذا الخيار لضمان سلامة المصادقة والبيانات. حتى في حالة حظر تشفير البيانات، فإنه يمكنك استخدام IPsec.

إعدادات الأمان المتقدمة لـ Enterprise

Algorithm Settings

يُوصى بتحديد Any لجميع الإعدادات أو تحديد عنصر آخر غير Any لكل إعداد. إذا حددت Any لبعض الإعدادات وحددت عنصراً آخر غير Any للإعدادات الأخرى، فقد لا يتصل الجهاز حسب الجهاز الآخر الذي تريد مصادقته.

العناصر	الإعدادات والشرح
IKE	Encryption حدد خوارزمية التشفير لـ IKE. تختلف العناصر حسب إصدار IKE.
	Authentication حدد خوارزمية المصادقة لـ IKE.
	Key Exchange حدد خوارزمية تبادل المفاتيح لـ IKE. تختلف العناصر حسب إصدار IKE.
ESP	Encryption حدد خوارزمية التشفير لـ ESP. يتوفر ذلك عند تحديد ESP لـ Security Protocol.
	Authentication حدد خوارزمية المصادقة لـ ESP. يتوفر ذلك عند تحديد ESP لـ Security Protocol.
AH	Authentication حدد خوارزمية التشفير لـ AH. يتوفر ذلك عند تحديد AH لـ Security Protocol.

معلومات ذات صلة

← "تكوين السياسة الافتراضية" في الصفحة 124

تكوين سياسة المجموعة

سياسة المجموعة عبارة عن قاعدة أو أكثر تسري على مستخدم أو مجموعة مستخدمين. تتحكم الطابعة في حزم بيانات IP التي تتناسب مع السياسات المكونة. إذا كانت حزم البيانات مصدق عليها بترتيب سياسة المجموعات 1 إلى 10، فسيتم استخدام السياسة الافتراضية.

1. ادخل إلى Web Config وحدد علامة التبويب **Basic < IPsec/IP Filtering < Network Security**.

2. انقر فوق علامة التبويب المرقمة التي ترغب في تكوينها.

3. أدخل قيمة لكل عنصر.

4. انقر فوق **Next**.

يتم عرض رسالة تأكيد.

5. انقر فوق **OK**.

الطابعة قيد التحديث.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "عناصر إعداد Group Policy" في الصفحة 129

إعدادات الأمان المتقدمة لـ Enterprise

عناصر إعداد Group Policy

العناصر	الإعدادات والشرح
Enable this Group Policy	يمكنك تمكين سياسة إحدى المجموعات أو تعطيلها.

Access Control

قم بتكوين طريقة تحكم لنقل حزم بيانات IP.

العناصر	الإعدادات والشرح
Permit Access	حدد هذه الطريقة للسماح بمرور حزم بيانات IP المكونة.
Refuse Access	حدد هذه الطريقة لرفض مرور حزم بيانات IP المكونة.
IPsec	حدد هذه الطريقة للسماح بمرور حزم بيانات IPsec المكونة.

Local Address(Printer)

حدد عنوان IPv4 أو عنوان IPv6 الذي يتوافق مع بيئة شبكتك. إذا تم تعيين عنوان IP تلقائياً، يمكنك تحديد **Use auto-obtained IPv4 address**.

ملاحظة:

في حالة تعيين عنوان IPv6 تلقائياً، فقد يصبح الاتصال غير متوفر. كونه عنوان IPv6 ثابتاً.

Remote Address(Host)

أدخل عنوان IP للجهاز من أجل التحكم في الوصول. يجب أن يتكون عنوان IP من 43 حرفاً أو أقل. إذا لم تدخل عنوان IP، فسيتم التحكم في جميع العناوين.

ملاحظة:

في حال تعيين عنوان IP تلقائياً (على سبيل المثال، بواسطة بروتوكول DHCP)، قد يصبح الاتصال غير متاح. قم بتكوين عنوان IP ثابت.

Method of Choosing Port

حدد طريقةً لتحديد المنافذ.

Service Name

إذا قمت بتحديد Service Name من أجل Method of Choosing Port، فحدد خياراً.

Transport Protocol

إذا قمت بتحديد Port Number من أجل Method of Choosing Port، فلا بد أن تقوم بتكوين وضع تغليف.

العناصر	الإعدادات والشرح
Any Protocol	حدد هذا للتحكم في جميع أنواع البروتوكولات.
TCP	حدد هذا للتحكم في بيانات البث الأحادي.
UDP	حدد هذا للتحكم في بيانات البث واسع النطاق والبث المتعدد.
ICMPv4	حدد هذا للتحكم في أمر ping.

إعدادات الأمان المتقدمة لـ Enterprise

Local Port

إذا حددت **Port Number** من أجل **Method of Choosing Port** وحددت **TCP** أو **UDP** من أجل **Transport Protocol**، فأدخل أرقام المنفذ للتحكم في استلام حزم البيانات، مع الفصل بينها باستخدام فاصلة. يمكنك إدخال 10 أرقام منفذ كحد أقصى.

مثال: 20, 80, 119, 5220

إذا لم تقم بإدخال رقم منفذ، فسيتم التحكم في جميع المنافذ.

Remote Port

إذا حددت **Port Number** من أجل **Method of Choosing Port** وحددت **TCP** أو **UDP** من أجل **Transport Protocol**، فأدخل أرقام المنفذ للتحكم في إرسال حزم البيانات، مع الفصل بينها باستخدام فاصلة. يمكنك إدخال 10 أرقام منفذ كحد أقصى.

مثال: 25, 80, 143, 5220

إذا لم تقم بإدخال رقم منفذ، فسيتم التحكم في جميع المنافذ.

IKE Version

حدد **IKEv1** أو **IKEv2** لـ **IKE Version**. حدد أحدهما وفقاً للجهاز المتصل به الطابعة.

IKEv1

يتم عرض العناصر التالية عند تحديد **IKEv1** لـ **IKE Version**.

العناصر	الإعدادات والشرح
Authentication Method	إذا قمت بتحديد IPsec من أجل Access Control ، فحدد خياراً. تعتبر الشهادة المستخدمة هي السياسة الافتراضية نفسها.
Pre-Shared Key	إذا قمت بتحديد Pre-Shared Key من أجل Authentication Method ، فأدخل مفتاحاً مشتركاً مسبقاً مكوناً من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 127 حرفاً.
Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.

إعدادات الأمان المتقدمة لـ Enterprise

IKEv2

يتم عرض العناصر التالية عند تحديد IKEv2 لـ IKE Version.

العناصر	الإعدادات والشرح
Local	Authentication Method
	إذا قمت بتحديد IPsec من أجل Access Control، فحدد خيارًا. تعتبر الشهادة المستخدمة هي السياسة الافتراضية نفسها.
	ID Type
	ID
	أدخل معرف الطابعة الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، "#"، و"=" بدلاً من الحرف الأول. Distinguished Name : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفًا. يجب عليك إدراج "=". IP Address : أدخل تنسيق IPv4 أو IPv6. FQDN : أدخل مزيجًا من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفًا باستخدام A-Z، و a-z، و 0-9، و"-"، و"نقطة". Email Address : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفًا. يجب عليك إدراج "@". Key ID : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفًا.
	Pre-Shared Key
	إذا قمت بتحديد Pre-Shared Key من أجل Authentication Method، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 127 حرفًا.
	Confirm Pre-Shared Key
	أدخل المفتاح الذي قمت بتكوينه للتأكيد.
Remote	Authentication Method
	إذا قمت بتحديد IPsec من أجل Access Control، فحدد خيارًا. تعتبر الشهادة المستخدمة هي السياسة الافتراضية نفسها.
	ID Type
	إذا حددت Pre-Shared Key لـ Authentication Method، فحدد نوع معرف الجهاز الذي تريد مصادقته.
	ID
	أدخل معرف الطابعة الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، "#"، و"=" بدلاً من الحرف الأول. Distinguished Name : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفًا. يجب عليك إدراج "=". IP Address : أدخل تنسيق IPv4 أو IPv6. FQDN : أدخل مزيجًا من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفًا باستخدام A-Z، و a-z، و 0-9، و"-"، و"نقطة". Email Address : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفًا. يجب عليك إدراج "@". Key ID : أدخل من 1 إلى 255 بايت (0x20 ASCII إلى 0x7E) حرفًا.
	Pre-Shared Key
	إذا قمت بتحديد Pre-Shared Key من أجل Authentication Method، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 127 حرفًا.
	Confirm Pre-Shared Key
	أدخل المفتاح الذي قمت بتكوينه للتأكيد.

Encapsulation

إذا قمت بتحديد IPsec من أجل Access Control، فلا بد أن تقوم بتكوين وضع تغليف.

إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح
Transport Mode	إذا كنت تستخدم الطابعة على شبكة LAN نفسها فقط، فحدد هذا. يتم تشفير حزم بيانات IP الطبقة 4 أو ما بعدها.
Tunnel Mode	إذا كنت تستخدم طابعة على شبكة تدعم استخدام الإنترنت مثل IPsec-VPN، فحدد هذا الخيار. يتم تشفير عنوان حزم بيانات IP وبياناتها. Remote Gateway(Tunnel Mode): إذا قمت بتحديد Tunnel Mode من أجل Encapsulation، فأدخل عنوان البوابة الافتراضي المكون من عددٍ من الأحرف يتراوح ما بين حرف واحد إلى 39 حرفًا.

Security Protocol

إذا قمت بتحديد IPsec من أجل Access Control، فحدد خيارًا.

العناصر	الإعدادات والشرح
ESP	حدد هذا الخيار لضمان سلامة المصادقة والبيانات وتشفير البيانات.
AH	حدد هذا الخيار لضمان سلامة المصادقة والبيانات. حتى في حالة حظر تشفير البيانات، فإنه يمكنك استخدام IPsec.

Algorithm Settings

يُوصى بتحديد Any لجميع الإعدادات أو تحديد عنصر آخر غير Any لكل إعداد. إذا حددت Any لبعض الإعدادات وحددت عنصرًا آخر غير Any للإعدادات الأخرى، فقد لا يتصل الجهاز حسب الجهاز الآخر الذي تريد مصادقته.

العناصر	الإعدادات والشرح
IKE	Encryption حدد خوارزمية التشفير لـ IKE. تختلف العناصر حسب إصدار IKE.
	Authentication حدد خوارزمية المصادقة لـ IKE.
	Key Exchange حدد خوارزمية تبادل المفاتيح لـ IKE. تختلف العناصر حسب إصدار IKE.
ESP	Encryption حدد خوارزمية التشفير لـ ESP. يتوفر ذلك عند تحديد ESP لـ Security Protocol.
	Authentication حدد خوارزمية المصادقة لـ ESP. يتوفر ذلك عند تحديد ESP لـ Security Protocol.
AH	Authentication حدد خوارزمية التشفير لـ AH. يتوفر ذلك عند تحديد AH لـ Security Protocol.

معلومات ذات صلة

- ← "تكوين سياسة المجموعة" في الصفحة 128
- ← "الجمع بين Local Address(Printer) و Remote Address(Host) على Group Policy" في الصفحة 133
- ← "مراجع أسماء الخدمة في سياسة المجموعة" في الصفحة 133

إعدادات الأمان المتقدمة لـ Enterprise

الجمع بين Local Address(Printer) و Remote Address(Host) على Group Policy

إعداد Local Address(Printer)				
3* Any addresses	2* IPv6	IPv4		
✓	-	✓	1* IPv4	إعداد Remote Address(Host)
✓	✓	-	2*1* IPv6	
✓	✓	✓	فارغ	

1* إذا كان IPsec محددًا لـ Access Control، فلا يمكنك تحديد طول للبادئة.

2* إذا كان IPsec محددًا لـ Access Control، يمكنك تحديد عنوان ارتباط محلي (::fe80::) ولكن سيتم تعطيل نهج المجموعة.

3* باستثناء عناوين الارتباط المحلي لـ IPv6.

مراجع أسماء الخدمة في سياسة المجموعة

ملاحظة:

تُعرض الخدمات غير المتوفرة ولكن لا يمكن تحديدها.

اسم الخدمة	نوع البروتوكول	رقم المنفذ المحلي	رقم المنفذ البعيد	الميزات المتحكم بها
Any	-	-	-	جميع الخدمات
ENPC	UDP	3289	أي منفذ	جار البحث عن طابعة من التطبيقات مثل Epson Device Admin، وبرنامج تشغيل الطابعة
SNMP	UDP	161	أي منفذ	الحصول على MIB وتكوينه من تطبيقات مثل Epson Device Admin، وبرنامج تشغيل الطابعة
LPR	TCP	515	أي منفذ	إرسال بيانات LPR
RAW (Port9100)	TCP	9100	أي منفذ	إرسال بيانات RAW
IPP/IPPS	TCP	631	أي منفذ	إعادة توجيه بيانات طباعة IPP/IPPS
WSD	TCP	أي منفذ	5357	تحكم WSD
WS-Discovery	UDP	3702	أي منفذ	البحث عن طابعة من WSD
FTP Data (Local)	TCP	20	أي منفذ	خادم FTP (إرسال بيانات طباعة FTP)
FTP Control (Local)	TCP	21	أي منفذ	خادم FTP (التحكم في طباعة FTP)
FTP Data (Remote)	TCP	أي منفذ	20	عميل FTP (إعادة توجيه بيانات المسح الضوئي) على الرغم من ذلك، يمكن لهذا الأمر التحكم بخادم FTP فقط الذي يستخدم المنفذ البعيد رقم 20.
FTP Control (Remote)	TCP	أي منفذ	21	عميل FTP (التحكم في إعادة توجيه بيانات المسح الضوئي)
CIFS (Remote)	TCP	أي منفذ	445	عميل CIFS (إعادة توجيه بيانات المسح الضوئي إلى أحد المجلدات)

إعدادات الأمان المتقدمة لـ Enterprise

اسم الخدمة	نوع البروتوكول	رقم المنفذ المحلي	رقم المنفذ البعيد	الميزات المتحكم بها
NetBIOS Name Service (Remote)	UDP	أي منفذ	137	عميل CIFS (إعادة توجيه بيانات المسح الضوئي إلى أحد المجلدات)
NetBIOS Datagram Service (Remote)	UDP	أي منفذ	138	
NetBIOS Session Service (Remote)	TCP	أي منفذ	139	
HTTP (Local)	TCP	80	أي منفذ	خادم (HTTP(S) إعادة توجيه بيانات Web Config وWSD)
HTTPS (Local)	TCP	443	أي منفذ	
HTTP (Remote)	TCP	أي منفذ	80	عميل (HTTP(S) تحديث البرامج الثابتة وتحديث شهادة الجذر)
HTTPS (Remote)	TCP	أي منفذ	443	

أمثلة على تكوين IPsec/IP Filtering

استلام حزم بيانات IPsec فقط

هذا المثال خاص بتكوين سياسة افتراضية فقط.

Default Policy:

Enable :IPsec/IP Filtering

IPsec :Access Control

Pre-Shared Key :Authentication Method

Pre-Shared Key: أدخل حتى 127 حرفاً.

:Group Policy

لا تقم بالتكوين.

استلام بيانات الطباعة وإعدادات الطباعة

يوضح هذا المثال السماح بالربط بين بيانات الطباعة وتكوين الطباعة باستخدام خدمات محددة.

Default Policy:

Enable :IPsec/IP Filtering

Refuse Access :Access Control

:Group Policy

Enable this Group Policy حدد المربع.

Permit Access :Access Control

Remote Address(Host) عنوان IP للجهاز التابع

Service Name :Method of Choosing Port

Service Name: حدد مربع ENPC ,SNMP ,HTTP (Local) ,HTTPS (Local) و RAW (Port9100).

إعدادات الأمان المتقدمة لـ Enterprise

استلام الوصول من عنوان IP محدد فقط
يسمح هذا المثال لعنوان IP محدد بالوصول إلى الطابعة.

:Default Policy

Enable :IPsec/IP Filtering

Refuse Access:Access Control

:Group Policy

Enable this Group Policy حدد المربع.

Permit Access :Access Control

Remote Address(Host) عنوان IP للجهاز التابع للمسؤول

ملاحظة:

بغض النظر عن تكوين السياسة، سيتمكن الجهاز التابع من الوصول إلى الطابعة وتكوينها.

تهيئة شهادة لتصفية IPsec/IP

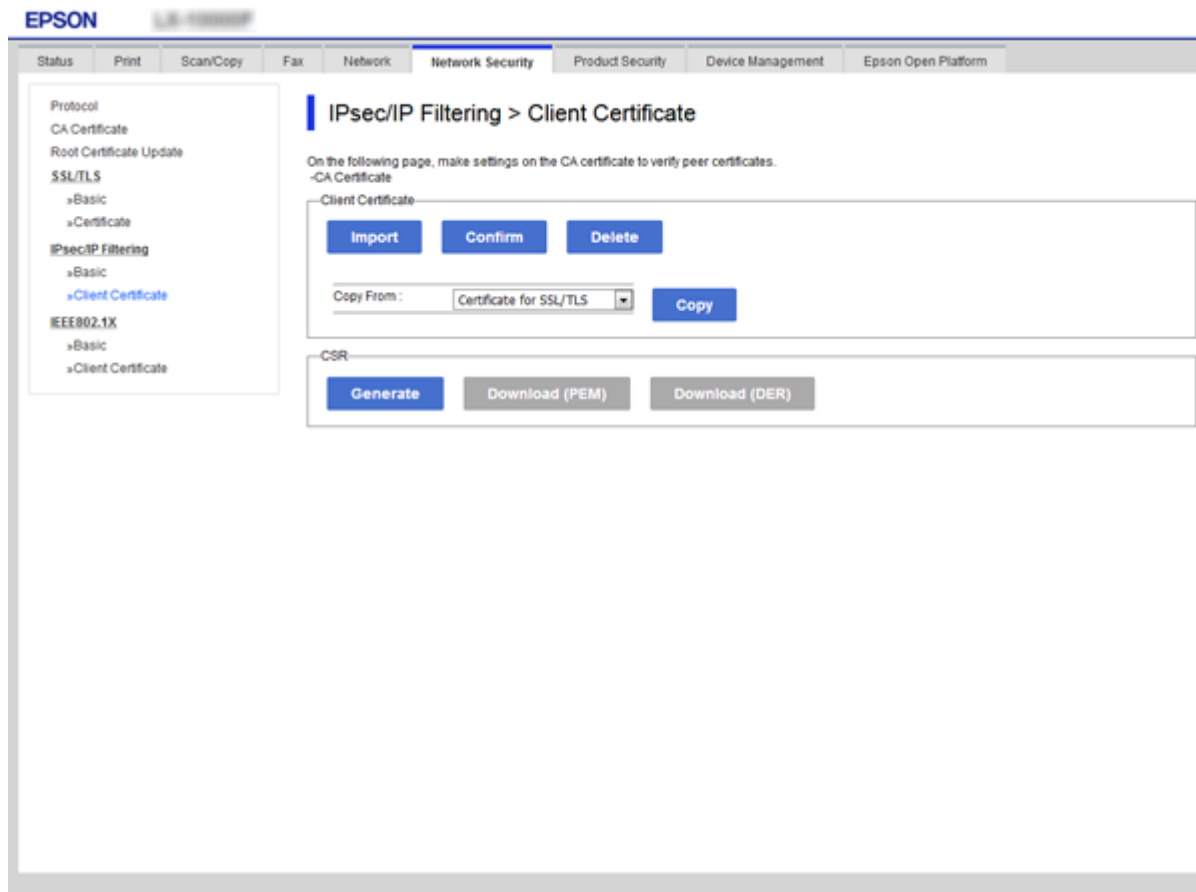
قم بتهيئة شهادة العميل لتصفية IPsec/IP. عند تعيينها، يمكنك استخدام الشهادة كإحدى طرق المصادقة لتصفية IPsec/IP. إذا كنت ترغب في تهيئة المرجع المصدق، فإذهب إلى **CA Certificate**.

1. ادخل إلى Web Config وحدد علامة التبويب **Client Certificate < IPsec/IP Filtering < Network Security**.

إعدادات الأمان المتقدمة لـ Enterprise

2. قم باستيراد الشهادة في **Client Certificate**.

إذا تم استيراد الشهادة المنشورة بواسطة المرجع المصدق في IEEE 802.1X أو SSL/TLS بالفعل، يمكنك نسخ الشهادة واستخدامها في تصفية IPsec/IP. للنسخ، حدد الشهادة من **Copy From**، ثم انقر فوق **Copy**.



معلومات ذات صلة

- ← "الوصول إلى تطبيق Web Config" في الصفحة 27
- ← "الحصول على شهادة موقعة من المرجع المصدق (CA)" في الصفحة 112

توصيل الطابعة بشبكة IEEE802.1X

تكوين شبكة IEEE802.1X

عندما تقوم بتعيين IEEE802.1X للطابعة، يمكنك استخدامه على الشبكة المتصلة بخادم RADIUS، أو بمحول شبكة محلية ذات وظيفة مصادقة، أو نقطة الوصول.

1. ادخل إلى Web Config وحدد علامة التبويب **Network Security < IEEE802.1X < Basic**.

2. أدخل قيمة لكل عنصر.

إذا كنت ترغب في استخدام الطابعة على شبكة Wi-Fi، فانقر فوق **Wi-Fi Setup** وحدد معرف الشبكة أو أدخله.

ملاحظة:

يمكنك مشاركة الإعدادات بين شبكة الإيثرنت وشبكة Wi-Fi.

إعدادات الأمان المتقدمة لـ Enterprise

3. انقر فوق Next.

يتم عرض رسالة تأكيد.

4. انقر فوق OK.

الطابعة قيد التحديث.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "عناصر إعداد شبكة IEEE 802.1X" في الصفحة 137

← "تعذر الوصول إلى الطابعة أو الماسحة الضوئية بعد تكوين IEEE802.1X" في الصفحة 142

عناصر إعداد شبكة IEEE 802.1X

العناصر	الإعدادات والشرح
IEEE802.1X (Wired LAN)	يمكنك تمكين إعدادات الصفحة أو تعطيلها (Basic < IEEE802.1X) بالنسبة إلى IEEE802.1X (LAN) السلكية).
IEEE802.1X (Wi-Fi)	يتم عرض حالة توصيل IEEE802.1X (Wi-Fi).
Connection Method	يتم عرض أسلوب التوصيل للشبكة الحالية.
EAP Type	حدد أحد الخيارات لأسلوب المصادقة بين الطابعة وخادم RADIUS.
	تحتاج إلى الحصول على شهادة موقعة من مرجع مصدق (CA) واستيرادها.
	EAP-TLS
	PEAP-TLS
	EAP-TTLS
	تحتاج إلى تكوين كلمة مرور.
	PEAP/MSCHAPv2
User ID	قم بتكوين معرف لاستخدامه كأسلوب مصادقة لأحد خوادم RADIUS. أدخل من 1 إلى 128 -بايت (0x20 ASCII إلى 0x7E) حرفاً.
Password	قم بتكوين كلمة مرور لمصادقة الطابعة. أدخل من 1 إلى 128 -بايت (0x20 ASCII إلى 0x7E) حرفاً. إذا كنت تستخدم أحد خوادم Windows كخادم RADIUS يمكنك إدخال ما يصل إلى 127 حرفاً.
Confirm Password	أدخل كلمة المرور التي قمت بتكوينها للتأكيد.
Server ID	يمكن تكوين معرف خادم للمصادقة مع خادم RADIUS محدد. يتحقق المصدق مما إذا كان معرف الخادم ورد في خانة subject/subjectAltName لشهادة الخادم المرسل من خادم RADIUS أم لا. أدخل من 0 إلى 128 -بايت (0x20 ASCII إلى 0x7E) حرفاً.
Certificate Validation	يمكنك تعيين التحقق من صحة الشهادة بغض النظر عن أسلوب المصادقة. قم باستيراد الشهادة في CA Certificate.
Anonymous Name	إذا قمت بتحديد PEAP-TLS، أو EAP-TTLS، أو PEAP/MSCHAPv2 من أجل EAP Type، فيمكنك تكوين اسم مجهول بدلاً من معرف المستخدم للعبارة 1 من مصادقة PEAP. أدخل من 0 إلى 128 -بايت (0x20 ASCII إلى 0x7E) حرفاً.
Encryption Strength	يمكنك تحديد إحدى القيم التالية.
High	AES256/3DES
Middle	AES256/3DES/AES128/RC4

إعدادات الأمان المتقدمة لـ Enterprise

معلومات ذات صلة

← "تكوين شبكة IEEE802.1X" في الصفحة 136

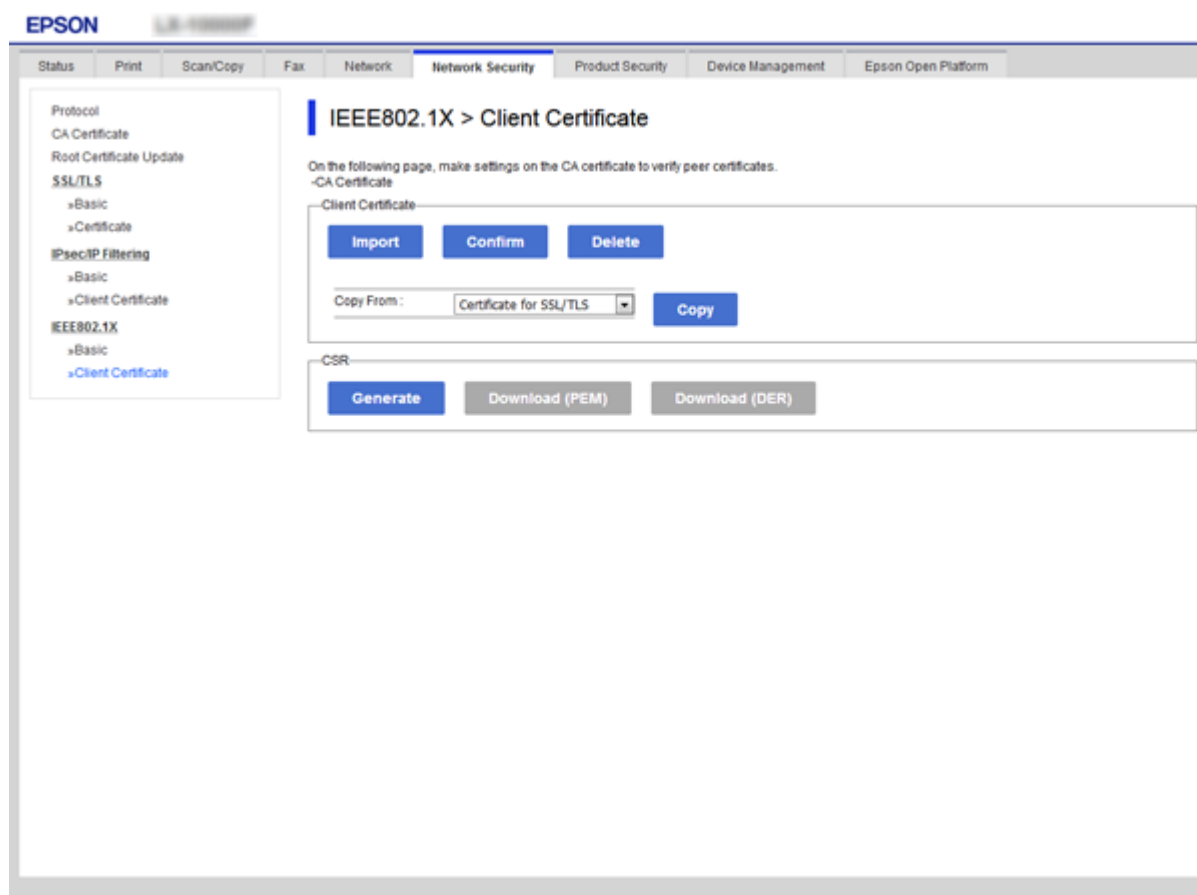
تكوين شهادة لاتصال IEEE802.1X

تهيئة شهادة العميل لـ IEEE802.1X. عند تعيينها، يمكنك استخدام EAP-TLS و PEAP-TLS كطريقة المصادقة لـ IEEE802.1x. إذا كنت ترغب في تهيئة شهادة المرجع المصدق، فإذهب إلى CA Certificate.

1. ادخل إلى Web Config وحدد علامة التبويب Client Certificate < IEEE802.1X < Network Security.

2. أدخل شهادة في Client Certificate.

يمكنك نسخ الشهادة في حال نشرها من خلال المرجع المصدق. للنسخ، حدد الشهادة من Copy From، ثم انقر فوق Copy.



معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها" في الصفحة 112

التحقق من حالة شبكة IEEE 802.1X

يمكنك التحقق من حالة شبكة IEEE 802.1X من خلال طباعة ورقة حالة الشبكة. لمزيد من المعلومات حول طباعة ورقة حالة الشبكة، انظر وثائق الطابعة.

إعدادات الأمان المتقدمة لـ Enterprise

حالة IEEE 802.1X	معرف الحالة
ميزة IEEE 802.1X معطلة.	Disable
نجحت مصادقة IEEE 802.1X والاتصال بالشبكة متاح.	EAP Success
لم تكتمل مصادقة IEEE 802.1X.	Authenticating
فشلت المصادقة حيث لم يتم تعيين معرف المستخدم.	Config Error
فشلت المصادقة حيث إن شهادة العميل منتهية الصلاحية.	Client Certificate Error
فشلت المصادقة حيث لا يوجد رد من خادم RADIUS و/أو المصدق.	Timeout Error
فشلت المصادقة لعدم صحة معرف مستخدم الطابعة و/أو بروتوكول الشهادة.	User ID Error
فشلت المصادقة لعدم تطابق معرف خادم شهادة الخادم ومعرف الخادم.	Server ID Error
فشلت المصادقة نظراً لوجود الأخطاء التالية في شهادة الخادم. <input type="checkbox"/> شهادة الخادم منتهية الصلاحية. <input type="checkbox"/> سلسلة شهادة الخادم غير صحيحة.	Server Certificate Error
فشلت المصادقة لوجود الأخطاء التالية في شهادة المرجع المصدق (CA). <input type="checkbox"/> شهادة المرجع المصدق (CA) غير صحيحة. <input type="checkbox"/> لم يتم استيراد شهادة المرجع المصدق (CA) الصحيحة. <input type="checkbox"/> شهادة المرجع المصدق (CA) منتهية الصلاحية.	CA Certificate Error
فشلت المصادقة نظراً لوجود الأخطاء التالية في إعدادات الطابعة. <input type="checkbox"/> إذا كان EAP Type هو EAP-TLS أو PEAP-TLS، فذلك يعني أن شهادة العميل غير صحيحة أو تحتوي على بعض المشكلات المعينة. <input type="checkbox"/> إذا كان EAP Type هو EAP-TTLS أو PEAP/MSCHAPv2، فسيكون معرف المستخدم غير صحيح أو كلمة المرور غير صحيحة.	EAP Failure

إصلاح مشكلات الأمان المتقدم

استعادة إعدادات الأمان

عند إنشاء بيئة آمنة بشكل كبير مثل تصفية IPsec/IP أو IEEE802.1X، قد لا تتمكن من الاتصال بالأجهزة بسبب الإعدادات غير الصحيحة أو حدوث مشكلة في الجهاز أو الخادم. في هذه الحالة، قم باستعادة إعدادات الأمان لضبط إعدادات الجهاز مرة أخرى أو للسماح لك بالاستخدام لفترة مؤقتة.

تعطيل وظيفة الأمان باستخدام لوحة التحكم

يمكنك تعطيل تصفية IPsec/IP أو IEEE802.1X باستخدام لوحة تحكم الطابعة.

1. حدد الإعدادات < إعدادات عامة > إعدادات الشبكة.

2. حدد متقدم.

إعدادات الأمان المتقدمة لـ Enterprise

3. حدد العنصر الذي ترغب في تعطيله من العناصر التالية.

تعطيل تصفية IPsec/IP

تعطيل IEEE802.1X

4. حدد متابعة على شاشة التأكيد.

5. عندما تظهر رسالة الاكتمال، حدد إغلاق.

تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بتحديد إغلاق.

المشكلات الخاصة باستخدام ميزات أمان الشبكة

نسيان مفتاح مشترك مسبقاً

أعد تهيئة المفتاح المشترك مسبقاً.

لتغيير المفتاح، ادخل إلى Web Config وحدد علامة التبويب **Default Policy < Basic < IPsec/IP Filtering < Network Security** Group Policy.

عندما تُغير المفتاح المشترك مسبقاً، قم بتهيئته لأجهزة الحاسوب.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

يتعذر الاتصال باستخدام اتصال IPsec

حدد الخوارزمية التي لا تدعمها الطابعة أو الكمبيوتر.

تدعم الطابعة الخوارزميات التالية. تحقق من إعدادات الكمبيوتر.

الخوارزميات	أساليب الأمان
AES-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, و AES-3DES, AES-GCM-256*, و AES-192	خوارزمية التشفير IKE
SHA-1, SHA-256, SHA-384, و SHA-512, و MD5	خوارزمية المصادقة IKE
DH, DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27, DH Group28*, DH Group29*, DH Group30*	خوارزمية تبادل المفاتيح IKE
AES-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, و AES-3DES, AES-GCM-256, و AES-192	خوارزمية التشفير ESP
SHA-1, SHA-256, SHA-384, و SHA-512, و MD5	خوارزمية المصادقة ESP
SHA-1, SHA-256, SHA-384, و SHA-512, و MD5	خوارزمية المصادقة AH

* متوفر IKEv2 فقط

إعدادات الأمان المتقدمة لـ Enterprise

معلومات ذات صلة

← "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 124

يتعذر الاتصال فجأة

تم تغيير عنوان IP الخاص بالطابعة أو يتعذر استخدامه.

عندما يتم تغيير عنوان IP المسجل بالعنوان المحلي في Group Policy أو عندما يتعذر استخدامه، حينها سيتعذر إجراء اتصال IPsec. قم بتعطيل IPsec باستخدام لوحة تحكم الطابعة.

إذا كان DHCP منتهي الصلاحية، وكانت عملية إعادة التمهيد أو عنوان IPv6 منتهي الصلاحية أو لم يتم الحصول عليهما، فقد لا يتم العثور على عنوان IP المسجل لـ Web Config الخاصة بالطابعة (علامة التبويب < Network Security < IPsec/IP Filtering < Basic < Group Policy < (Local Address(Printer)).

استخدم عنوان IP ثابت.

تم تغيير عنوان IP الخاص بجهاز الكمبيوتر أو يتعذر استخدامه.

عندما يتم تغيير عنوان IP المسجل بالعنوان البعيد في Group Policy أو عندما يتعذر استخدامه، حينها سيتعذر إجراء اتصال IPsec.

قم بتعطيل IPsec باستخدام لوحة تحكم الطابعة.

إذا كان DHCP منتهي الصلاحية، وكانت عملية إعادة التمهيد أو عنوان IPv6 منتهي الصلاحية أو لم يتم الحصول عليهما، فقد لا يتم العثور على عنوان IP المسجل لـ Web Config الخاصة بالطابعة (علامة التبويب < Network Security < IPsec/IP Filtering < Basic < Group Policy < (Remote Address(Host)).

استخدم عنوان IP ثابت.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 27

← "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 124

يتعذر إنشاء منفذ طباعة IPP آمن

لم يتم تحديد الشهادة الصحيحة باعتبارها شهادة الخادم لاتصال SSL/TLS.

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

لم يتم استيراد شهادة المرجع المصدق (CA) إلى كمبيوتر الوصول إلى الطابعة.

إذا لم يتم استيراد شهادة مرجع مصدق للكمبيوتر، فقد تفشل عملية إنشاء منفذ. تأكد من استيراد شهادة المرجع المصدق (CA).

معلومات ذات صلة

← "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 124

تعذر الاتصال بعد تهيئة تصفية IPsec/IP

إعدادات تصفية IPsec/IP غير صحيحة.

قم بتعطيل تصفية IPsec/IP من لوحة التحكم للطابعة. ثم قم بتوصيل الطابعة والكمبيوتر وإجراء إعدادات تصفية IPsec/IP مرة أخرى.

إعدادات الأمان المتقدمة لـ Enterprise

معلومات ذات صلة

← "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 124

تعذر الوصول إلى الطابعة أو الماسحة الضوئية بعد تكوين IEEE802.1X

إعدادات IEEE802.1X غير صحيحة.

قم بتعطيل IEEE802.1X وشبكة Wi-Fi من لوحة التحكم بالطابعة. قم بتوصيل الطابعة والحاسوب، ثم قم بتكوين IEEE802.1X مرة أخرى.

معلومات ذات صلة

← "تكوين شبكة IEEE802.1X" في الصفحة 136

المشكلات الخاصة باستخدام شهادة رقمية

يتعذر استيراد CA-signed Certificate

CA-signed Certificate والمعلومات الموجودة في طلب CSR غير متطابقة.

إذا لم تكن CA-signed Certificate وطلب CSR يحتويان على معلومات متماثلة، فإنه يتعذر استيراد طلب CSR. تحقق من الآتي:

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

تحقق من المعلومات الموجودة على طلب CSR ثم قم باستيراد الشهادة إلى جهاز يحتوي على المعلومات نفسها.

هل قمت باستبدال طلب CSR المحفوظ في الطابعة بعد إرسال الطلب إلى المراجع المصدق؟

احصل على شهادة موقعة من المراجع المصدق مرةً أخرى باستخدام طلب CSR.

CA-signed Certificate أكبر من 5 كيلوبايت.

لا يمكنك استيراد CA-signed Certificate أكبر من 5 كيلو بايت.

كلمة مرور استيراد الشهادة غير صحيحة.

أدخل كلمة المرور الصحيحة. إذا نسيت كلمة المرور، فإنه يتعذر عليك استيراد الشهادة. أعد الحصول على CA-signed Certificate.

معلومات ذات صلة

← "استيراد شهادة موقعة من المراجع المصدق (CA)" في الصفحة 115

تعذر تحديث شهادة ذاتية التوقيع

لم يتم إدخال Common Name.

لا بد من إدخال Common Name.

تم إدخال أحرف غير مدعومة إلى Common Name.

أدخل عدداً من الرموز يتراوح ما بين 1 إلى 128 رمزاً بتنسيق IPv4، أو IPv6، أو الاسم المضيف، أو FQDN (بلغة 0x20-0x7E ASCII).

إعدادات الأمان المتقدمة لـ Enterprise

تم تضمين فاصلة أو مسافة في الاسم الشائع.

إذا تم تضمين الفاصلة، فإنه يتم تقسيم Common Name عند هذا الموضع. إذا تم فقط إدخال مسافة قبل أو بعد الفاصلة، يحدث خطأ.

معلومات ذات صلة

← "تحديث شهادة موقعة ذاتياً" في الصفحة 119

يتعذر إنشاء طلب CSR

لم يتم إدخال Common Name.

لا بد من إدخال Common Name.

تم إدخال أحرف غير مدعومة إلى Common Name، و Organization، و Organizational Unit، و Locality، و State/Province. أدخل عدداً من الرموز بتنسيق IPv4، أو IPv6، أو الاسم المضيف، أو FQDN (بلغة ASCII (0x20-0x7E)).

تم تضمين فاصلة أو مسافة في Common Name.

إذا تم تضمين الفاصلة، فإنه يتم تقسيم Common Name عند هذا الموضع. إذا تم فقط إدخال مسافة قبل أو بعد الفاصلة، يحدث خطأ.

معلومات ذات صلة

← "الحصول على شهادة موقعة من المرجع المصدق (CA)" في الصفحة 112

ظهور تحذير مرتبط بشهادة رقمية

الرسائل	السبب/الحل
Enter a Server Certificate.	السبب: لم يتم تحديد ملف لاستيراده. الحل: حدد ملفاً وانقر فوق Import .
CA Certificate 1 is not entered.	السبب: لم يتم إدخال شهادة المرجع المصدق (1 CA) وتم إدخال شهادة المرجع المصدق (2 CA) فقط. الحل: قم باستيراد شهادة المرجع المصدق (1 CA) أولاً.
Invalid value below.	السبب: توجد رموز غير مدعومة في مسار الملف و/أو كلمة المرور. الحل: تأكد من إدخال الرموز بشكل صحيح للعنصر.
Invalid date and time.	السبب: لم يتم تعيين تاريخ الطابعة ووقتها. الحل: قم بتعيين التاريخ والوقت باستخدام Web Config، أو EpsonNet Config أو لوحة تحكم الطابعة.

إعدادات الأمان المتقدمة لـ Enterprise

السبب/الحل	الرسائل
<p>السبب: لا تتطابق كلمة المرور المعينة لشهادة المرجع المصدق (CA) وكلمة المرور المدخلة.</p> <p>الحل: أدخل كلمة المرور الصحيحة.</p>	Invalid password.
<p>السبب: لم تقم باستيراد ملف شهادة بتنسيق X.509.</p> <p>الحل: تأكد من تحديد الشهادة الصحيحة المرسله بواسطة مرجع مصدق موثوق فيه.</p>	Invalid file.
<p>السبب: الملف الذي تقوم باستيراده كبير للغاية. يصل الحد الأقصى لحجم الملف إلى 5 كيلو بايت.</p> <p>الحل: إذا قمت بتحديد الملف الصحيح، فقد تكون الشهادة تالفة أو ملفقة.</p>	
<p>السبب: السلسلة المضمنة في الشهادة غير صحيحة.</p> <p>الحل: لمزيدٍ من المعلومات حول الشهادة، انظر موقع الويب الخاص بالمرجع المصدق.</p>	
<p>السبب: يحتوي ملف الشهادة بتنسيق PKCS#12 على أكثر من 3 شهادات مرجع مصدق (CA).</p> <p>الحل: قم باستيراد كل شهادة عند التحويل من تنسيق PKCS#12 إلى تنسيق PEM، أو قم باستيراد ملف الشهادة بتنسيق PKCS#12 الذي يتضمن حتى شهادتي مرجع مصدق (CA).</p>	Cannot use the Server Certificates that include more than three CA certificates.
<p>السبب: الشهادة منتهية الصلاحية.</p> <p>الحل: <input type="checkbox"/> إذا كانت الشهادة منتهية الصلاحية، فاحصل على شهادة جديدة وقم باستيرادها. <input type="checkbox"/> إذا كانت الشهادة غير منتهية الصلاحية، فتأكد من تعيين تاريخ الطابعة ووقتها بشكلٍ صحيح.</p>	The certificate has expired. Check if the certificate is valid, or check the date and time on your printer.
<p>السبب: لا يوجد مفتاح خاص مزدوج مع الشهادة.</p> <p>الحل: <input type="checkbox"/> إذا كانت الشهادة بتنسيق PEM/DER وتم الحصول عليها من طلب CSR باستخدام جهاز كمبيوتر، فحدد ملف المفتاح الخاص. <input type="checkbox"/> إذا كانت الشهادة بتنسيق PKCS#12 وتم الحصول عليها من طلب CSR باستخدام جهاز كمبيوتر، فقم بإنشاء الملف الذي يتضمن المفتاح الخاص.</p>	Private key is required.
<p>السبب: قمت بإعادة استيراد شهادة PEM/DER التي تم الحصول عليها من طلب CSR باستخدام تطبيق Web Config.</p> <p>الحل: إذا كانت الشهادة بتنسيق PEM/DER وتم الحصول عليها من طلب CSR باستخدام تطبيق Web Config، يمكنك استيرادها مرةً واحدةً فقط.</p>	

إعدادات الأمان المتقدمة لـ Enterprise

السبب/الحل	الرسائل
<p>السبب: يتعذر إتمام التكوين بسبب فشل الاتصال بين الطابعة والكمبيوتر أو تعذرت قراءة الملف نتيجة لبعض الأخطاء.</p> <p>الحل: بعد فحص الملف المحدد والاتصال، قم باستيراد الملف مرةً أخرى.</p>	Setup failed.

معلومات ذات صلة

← "حول المصادقة الرقمية" في الصفحة 112

حذف الشهادة الموقعة من المرجع المصدق (CA) عن طريق الخطأ

لا يوجد ملف النسخة الاحتياطية للشهادة الموقعة من المرجع المصدق (CA).

في حالة وجود ملف نسخة احتياطية، قم باستيراد الشهادة مرةً أخرى.

إذا كنت تحصل على شهادة باستخدام طلب CSR تم إنشاؤه من تطبيق Web Config، فلن تتمكن من استيراد الشهادة المحذوفة مرةً أخرى. قم بإنشاء طلب CSR واحصل على شهادة جديدة.

معلومات ذات صلة

← "حذف شهادة موقعة من المرجع المصدق (CA)" في الصفحة 117

← "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 115