



WorkForce Enterprise  
**WF-C20590**

---

دليل المسؤول

## المحتويات

33. . . . . مراجع اختبار اتصال خادم البريد.

## إعدادات الوظيفة

36. . . . . برنامج للإعداد.

36. . . . . Web Config (صفحة ويب للجهاز).

37. . . . . استخدام وظائف الطباعة.

37. . . . . متطلبات الطباعة عبر الشبكة.

37. . . . . إعداد برنامج تشغيل الطابعة باستخدام اتصال العميل /

37. . . . . الخادم.

37. . . . . إعدادات برنامج تشغيل الطابعة لاتصال النظير إلى النظير

42. . . . .

44. . . . . استخدام وظائف المسح الضوئي.

44. . . . . المسح الضوئي من جهاز كمبيوتر.

45. . . . . المسح الضوئي باستخدام لوحة التحكم.

45. . . . . إدارة المسح الضوئي من لوحة التحكم (Document

45. . . . . /Capture Pro Server . . . . . Document Capture Pro46)

47. . . . . استخدام وظائف الفاكس.

47. . . . . إعداد Receive Mode.

47. . . . . استلام الفاكسات باستخدام هاتف متصل

48. . . . . (Remote Receive).

48. . . . . التعامل مع الفاكسات المستلمة.

51. . . . . وصف قائمة إعدادات الفاكس.

59. . . . . استخدام وظيفة PC-FAX.

60. . . . . استخدام جهات الاتصال.

60. . . . . ميزات إعداد الوجهة.

60. . . . . تكوين جهات الاتصال.

64. . . . . التعاون بين خادم LDAP والمستخدمين.

69. . . . . ضبط إعدادات النظام.

69. . . . . إعداد لوحة التحكم.

69. . . . . إعدادات توفير الطاقة أثناء فترة الخمول.

70. . . . . إعداد الصوت.

70. . . . . مزامنة التاريخ والوقت مع خادم الوقت.

70. . . . . إعداد القيمة الافتراضية للمسح الضوئي والنسخ (إعدادات

71. . . . . المستخدم الافتراضية).

71. . . . . تسجيل الإعدادات المستخدمة بشكل متكرر كإعداد سابق

71. . . . .

72. . . . . استخدام شبكة MS.

72. . . . . Print Settings.

73. . . . . استخدام خدمة Epson Connect.

## إعدادات سلامة المنتج

74. . . . . مقدمة عن ميزات سلامة المنتج.

75. . . . . تكوين كلمة مرور المسؤول.

75. . . . . تكوين كلمة مرور المسؤول من لوحة التحكم.

75. . . . . تكوين كلمة مرور المسؤول باستخدام Web Config.

## حقوق الطبع والنشر

## العلامات التجارية

## حول هذا الدليل

7. . . . . العلامات والرموز.

7. . . . . الأوصاف المستخدمة في هذا الدليل.

7. . . . . مراجع أنظمة التشغيل.

## مقدمة

9. . . . . مكونات الدليل.

9. . . . . تعريفات المصطلحات المستخدمة في هذا الدليل.

## التجهيز

12. . . . . تدفق إعدادات الطابعة وإدارتها.

13. . . . . مثال على بيئة الشبكة.

13. . . . . مقدمة عن إعدادات اتصال الطابعة.

15. . . . . تجهيز الاتصال بالشبكة.

15. . . . . جمع معلومات عن إعداد الاتصال.

15. . . . . مواصفات الطابعة.

15. . . . . استخدام رقم المنفذ.

16. . . . . نوع تعيين عنوان IP.

16. . . . . خادم DNS وخادم الوكيل.

16. . . . . طريقة إعداد الاتصال بالشبكة.

## الاتصال

17. . . . . الاتصال بالشبكة.

17. . . . . الاتصال بالشبكة من لوحة التحكم.

25. . . . . الاتصال بالشبكة باستخدام برنامج التثبيت.

26. . . . . الاتصال بخط هاتف.

26. . . . . خطوط الهاتف المتوافقة.

26. . . . . توصيل الطابعة بخط هاتف.

27. . . . . توصيل جهاز الهاتف الخاص بك بالطابعة.

29. . . . . ضبط إعدادات الفاكس الأساسية.

29. . . . . ضبط إعدادات الفاكس الأساسية باستخدام معالج إعداد

29. . . . . الفاكس.

30. . . . . ضبط إعدادات مصدر الورق لاستلام الفاكسات.

31. . . . . استخدام اتصال Wi-Fi Direct (نقطة الوصول البسيط).

31. . . . . تمكين شبكة Wi-Fi Direct (نقطة الوصول البسيط).

31. . . . . تكوين خادم البريد.

32. . . . . عناصر إعداد خادم البريد الإلكتروني.

33. . . . . التحقق من اتصال خادم البريد.

## المحتويات

لا يتم عرض اسم الطراز و/أو عنوان IP على تطبيق  
EpsonNet Config100. . . . .

## ملحق

101	تقديم برنامج الشبكة.
101	Epson Device Admin
101	EpsonNet Config
102	(EpsonNet Print (فقط Windows102
102	EpsonNet SetupManager
102	تعيين عنوان IP باستخدام EpsonNet Config102
102	تعيين عنوان IP باستخدام الإعدادات الدفعية.
105	تعيين عنوان IP لكل جهاز.
106	ضبط إعدادات Wi-Fi من لوحة التحكم (WPS).
107	ضبط إعدادات Wi-Fi عن طريق إعداد زر الضغط (WPS).
108	ضبط إعدادات Wi-Fi عن طريق إعداد رمز PIN التعريف الشخصي (WPS).
108	تغيير طريقة الاتصال.
109	تغيير الاتصال من الاتصال بشبكة إيثرنت إلى الاتصال بشبكة Wi-Fi.
109	تغيير الاتصال من الاتصال بشبكة Wi-Fi إلى اتصال الإيثرنت.
110	استخدام منفذ للطباعة.

## إعدادات الأمان المتقدمة لـ Enterprise

114	إعدادات الأمان ومنع وقوع المخاطر.
115	إعدادات ميزة الأمان.
115	اتصال SSL/TLS بالطباعة.
115	حول المصادقة الرقمية.
115	الحصول على شهادة موقعة من المرجع المصدق (CA) واستردادها.
119	حذف شهادة موقعة من المرجع المصدق (CA).
120	تحديث شهادة موقعة ذاتياً.
121	تهيئة CA Certificate.
123	التحكم باستخدام البروتوكولات.
123	التحكم في البروتوكولات.
124	البروتوكولات التي تستطيع تمكينها أو تعطيلها.
125	عناصر إعداد البروتوكول.
127	الاتصال المشفر باستخدام تصفية IPsec/IP.
127	حول IPsec/IP Filtering.
128	تكوين السياسة الافتراضية.
131	تكوين سياسة المجموعة.
137	أمثلة على تكوين IPsec/IP Filtering.
138	تكوين شهادة لتصفية IPsec/IP.
139	استخدام بروتوكول SNMPv3.
139	معلومات عن SNMPv3.
139	تكوين SNMPv3.
141	توصيل الطابعة بشبكة IEEE802.1X.

76	العناصر التي يتم قفلها عن طريق كلمة مرور المسؤول.
78	تغيير إعدادات العناصر المقفلة بكلمة مرور المسؤول.
78	تقييد الميزات المتوفرة.
79	تكوين التحكم في الوصول.
80	إعداد قيود الواجهة الخارجية.
81	ضبط إعدادات معالجة البيانات المحفوظة.
81	ضبط الإعدادات للحذف المتسلسل.
81	تنسيق القرص الصلب الداخلي.

## إعدادات الإدارة والتشغيل

83	تسجيل الدخول إلى الطابعة كمسؤول.
83	تسجيل الدخول إلى الطابعة باستخدام لوحة التحكم.
83	تسجيل الدخول إلى الطابعة باستخدام Web Config.
83	تأكيد معلومات أحد الأجهزة.
84	إدارة الأجهزة (Epson Device Admin).
85	استلام إعلانات البريد الإلكتروني عند وقوع أحداث.
85	حول إشعارات البريد الإلكتروني.
85	تكوين إشعارات البريد الإلكتروني.
86	تحديث البرنامج الثابت.
86	تحديث البرامج الثابتة للطابعة باستخدام لوحة التحكم.
87	تحديث البرنامج الثابت باستخدام Web Config.
87	تحديث البرنامج الثابت عن طريق استخدام Epson Firmware Updater.
88	نسخ جهات الاتصال والإعدادات احتياطياً.
88	تصدير الإعدادات.
88	استيراد الإعدادات.

## حل المشكلات

89	تلميحات لحل المشكلات.
89	فحص سجل الخادم وجهاز الشبكة.
89	تهيئة إعدادات الشبكة.
89	تعطيل Wi-Fi من تهيئة الويب.
89	قطع اتصال Wi-Fi Direct (نقطة الوصول البسيط) من تهيئة الويب.
90	إلغاء الاتصال بشبكة Wi-Fi من لوحة التحكم.
90	فصل اتصال Wi-Fi Direct (نقطة الوصول البسيطة) من لوحة التحكم.
90	استعادة إعدادات الشبكة من لوحة التحكم.
91	التحقق من الاتصال بين الأجهزة وأجهزة الكمبيوتر.
91	التحقق من الاتصال باستخدام أمر Ping —
91	التحقق من الاتصال باستخدام أمر Ping — Windows91.
91	التحقق من الاتصال باستخدام أمر Ping — Mac OS92.
94	طباعة تقرير الاتصال بالشبكة.
95	الرسائل والحلول الخاصة بتقرير اتصال الشبكة.
98	طباعة ورقة حالة الشبكة.
99	المشكلات الخاصة باستخدام برنامج الشبكة.
99	يتعذر الوصول إلى تطبيق Web Config.

## المحتويات

141	تكوين شبكة IEEE802.1X
143	تكوين شهادة لاتصال IEEE802.1X
144	التحقق من حالة شبكة IEEE802.1X
145	باستخدام Epson Open Platform
145	نظرة عامة حول Epson Open Platform
145	تكوين Epson Open Platform
146	التحقق من نظام المصادقة وتكوينه
146	تكوين جهاز المصادقة
146	إصلاح مشكلات الأمان المتقدم
146	استعادة إعدادات الأمان
147	المشكلات الخاصة باستخدام ميزات أمان الشبكة
149	المشكلات الخاصة باستخدام شهادة رقمية

## 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 2017

تُعد محتويات هذا الدليل والمواصفات عرضة للتغيير دون إشعار.

العلامات التجارية

# العلامات التجارية

EPSON® علامة تجارية مسجلة، و EPSON EXCEED YOUR VISION أو EXCEED YOUR VISION علامة تجارية لشركة Seiko Epson Corporation. □

Epson Scan 2 software is based in part on the work of the Independent JPEG Group. □

Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc. □

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

Mac OS, OS X, Bonjour 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. تخلي 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

- لقطات الشاشة الخاصة ببرنامج تشغيل الطابعة وشاشات Epson Scan 2 (برنامج تشغيل المساحة الضوئية) مأخوذة من نظام Windows 10 أو OS X El Capitan. يختلف المحتوى المعروض على الشاشات حسب الطراز والموقف.
- تعد الأشكال التوضيحية للطابعة المستخدمة في هذا الدليل مجرد أمثلة فقط. بالرغم من وجود اختلافات طفيفة بناءً على الطراز المستخدم لديك، إلا أن طريقة التشغيل تظل واحدة.
- تختلف بعض عناصر القائمة الموجودة على شاشة LCD بناءً على الطراز والإعدادات.

### مراجع أنظمة التشغيل

**Windows**

في هذا الدليل، تشير مصطلحات مثل "Windows 10"، و"Windows 8.1"، و"Windows 8"، و"Windows 7"، و"Windows Vista"، و"Windows XP"، و"Windows Server 2016"، و"Windows Server 2012 R2"، و"Windows Server 2012"، 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®

حول هذا الدليل

- نظام التشغيل Microsoft® Windows® XP
- نظام التشغيل Microsoft® Windows® XP Professional x64 Edition
- 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، تُستخدم "Mac OS" للإشارة إلى macOS Sierra، و OS X El Capitan، و OS X Yosemite، و OS X Mavericks، و OS X، و Mountain Lion، و Mac OS X v10.7.x، و Mac OS X v10.6.8.



## مقدمة

### مكونات الدليل

يُعد هذا الدليل مخصصاً لمسؤول الجهاز الذي تقع على عاتقه مسؤولية توصيل الطابعة أو الماسحة الضوئية بالشبكة ويحتوي على معلومات عن كيفية ضبط الإعدادات لاستخدام الوظائف.

راجع دليل المستخدم للحصول على معلومات استخدام الوظيفة.

#### التجهيز

لتوضيح مهام المسؤول، وكيفية تعيين الأجهزة، وبرنامج الإدارة.

#### الاتصال

لتوضيح كيفية توصيل الجهاز بالشبكة أو بخط الهاتف. ويوضح أيضاً بيئة الشبكة، مثل معلومات خادم الوكيل وDNS واستخدام منفذ الجهاز.

#### إعدادات الوظيفة

لتوضيح إعدادات كل وظيفة، مثل الطابعة، والمسح الضوئي، والفاكس.

#### إعدادات سلامة المنتج

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

#### إعدادات الإدارة والتشغيل

لتوضيح عمليات التشغيل بعد بدء استخدام الأجهزة، مثل التحقق من المعلومات وتحسينها.

#### أدوات حل المشاكل

لتوضيح تهيئة الإعدادات واكتشاف أخطاء الشبكة وإصلاحها.

#### إعدادات الأمان المتقدمة لـ Enterprise

لتوضيح طريقة الإعدادات لتحسين أمان الجهاز، مثل استخدام شهادة المرجع المصدق (CA)، واتصال SSL/TLS، وتصفية IPsec/IP. لا يتم دعم بعض الوظائف الواردة في هذا الفصل، حسب الطراز.

## تعريفات المصطلحات المستخدمة في هذا الدليل

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 والمساحات 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 أو مساحة ضوئية. 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 للبرنامج لإعداد الجهاز أو إدارته، مثل Epson Device Admin، EpsonNet Config، و EpsonNet SetupManager. وما إلى ذلك.

## المسح الضوئي السريع

مصطلح عام للمسح الضوئي من لوحة التحكم بالجهاز. باستخدام هذه الوظيفة، يتم حفظ نتيجة المسح الضوئي إلى مجلد، أو يتم إرفاقها إلى رسالة بريد إلكتروني، أو يتم حفظها في الخدمات السحابية.

## ASCII (الشفرة القياسية الأمريكية لتبادل المعلومات)

إحدى شفرات الرموز القياسية. يتم تحديد 128 رمزاً، بما في ذلك رموز مثل الحروف 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.

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

\* حرف المسافة.

## 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.

# التجهيز

يوضح هذا الفصل دور المسؤول والتجهيز قبل ضبط الإعدادات.

## تدقيق إعدادات الطابعة وإدارتها

يقوم المسؤول بضبط إعدادات الاتصال بالشبكة، والإعدادات المبدئية والصيانة للطابعة أو الماسحة الضوئية بحيث تكون متوفرة للمستخدمين.

### 1. التهيئة

جمع معلومات إعدادات الاتصال

تحديد طريقة الاتصال

### 2. التوصيل

اتصال الشبكة من لوحة تحكم الطابعة

الاتصال بخط هاتف

### 3. إعداد الوظائف

إعدادات برنامج تشغيل الطابعة

إعدادات برنامج تشغيل الماسحة الضوئية

إعدادات الفاكس

التسجيل في جهات الاتصال

الاتصال بشبكة Wi-Fi Direct (نقطة الوصول البسيط)

الإعدادات المتقدمة الأخرى

الخدمات السحابية

### 4. إعدادات الأمان

إعدادات المسؤول

إعدادات التحكم في الوصول

SSL/TLS

التحكم في البروتوكول

إعدادات الأمان المتقدمة (خيار)

### 5. التشغيل والإدارة

التحقق من حالة الجهاز

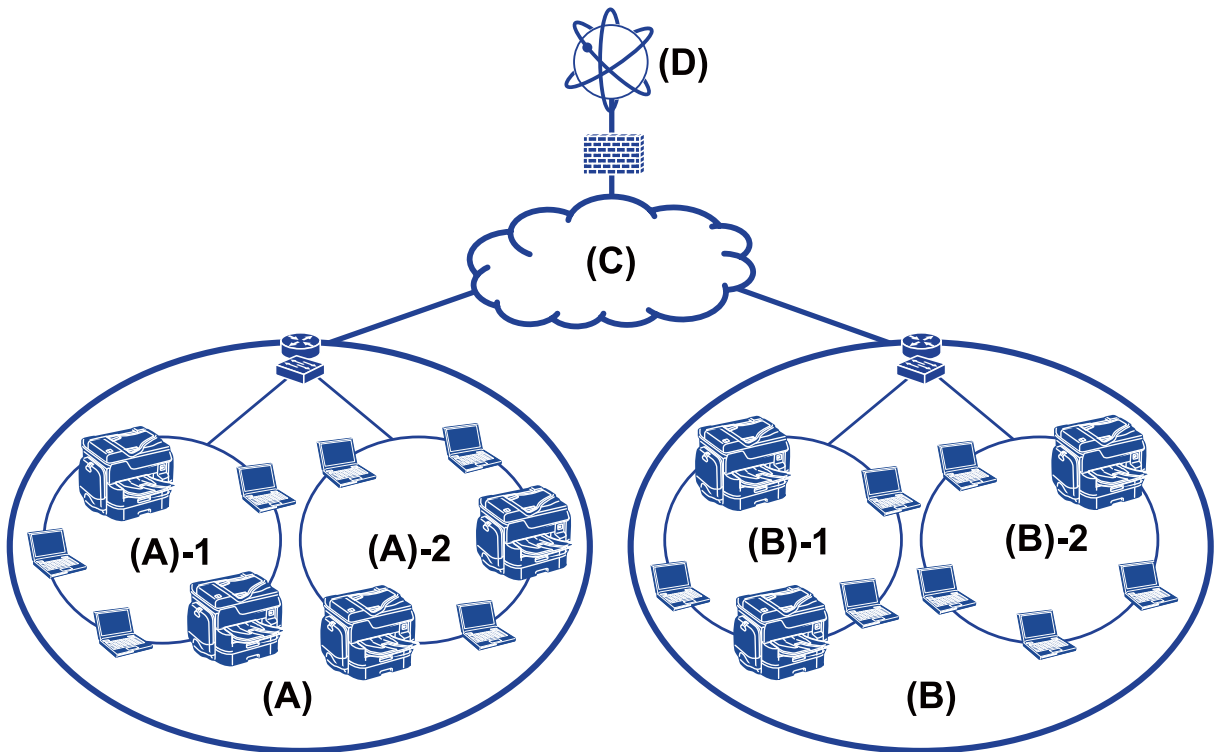
التعامل مع ظهور الأحداث

نسخ إعدادات الجهاز احتياطياً

معلومات ذات صلة

- ← "التجهيز" في الصفحة 12
- ← "الاتصال" في الصفحة 17
- ← "إعدادات الوظيفة" في الصفحة 36
- ← "إعدادات سلامة المنتج" في الصفحة 74
- ← "إعدادات الإدارة والتشغيل" في الصفحة 83

## مثال على بيئة الشبكة



Office 1 : (أ)

LAN 1 :1 - (أ) LAN 2 :2 - (أ) 

Office 2 : (ب)

LAN 1 :1 - (ب) LAN 2 :2 - (ب) 

WAN : (ج)

(د): إنترنت

## مقدمة عن إعدادات اتصال الطابعة

تتوفر الطريقتان التاليتان لاتصال الشبكة الخاص بالطابعة. تتصل الطابعة بالشبكة مباشرة من خلال كلتا الطريقتين.

## التجهيز

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

☐ اتصال نظير إلى نظير (الطباعة المباشرة)

## معلومات ذات صلة

◀ "إعدادات اتصال العميل/الخادم" في الصفحة 14

◀ "إعدادات اتصال نظير إلى نظير" في الصفحة 14

## إعدادات اتصال العميل/الخادم

## طريقة الاتصال:

وصّل الطابعة بالشبكة عبر موزع الشبكة أو نقطة الوصول. يمكنك أيضاً توصيل الطابعة بالخادم مباشرة عن طريق كابل USB.

## برنامج تشغيل الطابعة:

تُبث 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 الطباعة.

☐ لا يمكنك الطباعة عند إيقاف تشغيل خادم Windows.

## معلومات ذات صلة

◀ "تعريفات المصطلحات المستخدمة في هذا الدليل" في الصفحة 9

## إعدادات اتصال نظير إلى نظير

## طريقة الاتصال:

وصّل الطابعة بالشبكة مباشرة عبر موزع الشبكة أو نقطة الوصول.

## برنامج تشغيل الطابعة:

قم بتثبيت برنامج تشغيل الطابعة على كل كمبيوتر عميل.

يمكن تسليمه كحزمة باستخدام EpsonNet SetupManager أو تلقائياً عن طريق استخدام سياسة المجموعة لخادم Windows.

## الميزات:

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

☐ يمكنك الطباعة طالما الطابعة قيد التشغيل.

## التجهيز

معلومات ذات صلة

← "تعريفات المصطلحات المستخدمة في هذا الدليل" في الصفحة 9

## تجهيز الاتصال بالشبكة

## جمع معلومات عن إعداد الاتصال

يجب أن يكون لديك عنوان IP، وعنوان بوابة، وما إلى ذلك من أجل الاتصال بالشبكة. تحقق مما يلي مقدماً.

الأقسام	العناصر	ملاحظة
طريقة اتصال الجهاز	<input type="checkbox"/> شبكة الإيثرنت <input type="checkbox"/> شبكة Wi-Fi	استخدم كبلًا مزدوجًا مجدولاً مصفحاً (STP) من الفئة 5e أو أعلى لاتصال الإيثرنت.
معلومات اتصال LAN	<input type="checkbox"/> عنوان IP <input type="checkbox"/> قناع الشبكة الفرعية <input type="checkbox"/> البوابة الافتراضية	إذا قمت بتعيين عنوان IP تلقائياً باستخدام وظيفة DHCP في جهاز التوجيه، فلا داعي لذلك.
معلومات اتصال Wi-Fi	<input type="checkbox"/> معرف خدمة الشبكة <input type="checkbox"/> كلمة المرور	يتم دعم ما يلي: <input type="checkbox"/> التوافق: 802.11b/g/n <input type="checkbox"/> أمان شبكة Wi-Fi: WEP (64/128 بت) <input type="checkbox"/> WPA2-Enterprise، WPA-2PSK (AES)
معلومات خادم DNS	<input type="checkbox"/> عنوان IP لـ DNS الرئيسي <input type="checkbox"/> عنوان IP لـ DNS الثانوي	إذا كنت تستخدم عنوان IP ثابتاً كعنوان IP، فقم بتكوين خادم DNS. قم بتكوينه عند تعيينه تلقائياً باستخدام وظيفة DHCP وعند عدم إمكانية تعيين خادم DNS تلقائياً.
معلومات خادم الوكيل	<input type="checkbox"/> اسم خادم الوكيل <input type="checkbox"/> رقم المنفذ	قم بتكوينه عند استخدام خادم وكيل لاتصال الإنترنت وعند استخدام خدمة Epson Connect أو وظيفة التحديث التلقائية للبرنامج الثابت.

## مواصفات الطابعة

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

## استخدام رقم المنفذ

راجع "الملحق" الخاص برقم المنفذ الذي تستخدمه الطابعة.

معلومات ذات صلة

← "استخدام منفذ للطابعة" في الصفحة 110

## التجهيز

## نوع تعيين عنوان IP

يوجد نوعان لتعيين عنوان IP للطابعة.

## عنوان IP ثابت:

عنوان IP فريد محدد مسبقاً للطابعة.

لا يتم تغيير عنوان IP حتى عند إيقاف تشغيل الطابعة أو جهاز التوجيه، لذلك يمكنك إدارة الجهاز بواسطة عنوان IP. يُعد ذلك النوع مناسباً لشبكة يتم فيها إدارة العديد من الطابعات مثل مكتب كبير أو مدرسة.

## التعيين التلقائي عن طريق وظيفة DHCP:

يتم تعيين عنوان IP الصحيح تلقائياً عند نجاح الاتصال بين الطابعة وجهاز التوجيه الذي يدعم وظيفة DHCP. إذا لم يكن هذا النوع ملائماً لتغيير عنوان IP لجهاز محدد، فقم بحفظ عنوان IP مقدماً ثم قم بتعيينه.

## ملاحظة:

بالنسبة لمنفذ قائمة انتظار الطابعة، حدد البروتوكول الذي يمكن أن يكتشف عنوان IP تلقائياً، مثل *EpsonNet Print Port*.

## خادم DNS وخادم الوكيل

إذا كنت تستخدم خدمة الاتصال بالإنترنت، فقم بتكوين خادم DNS. إذا لم تقم بتكوينه، فيجب عليك تحديد عنوان IP للوصول لأنك قد تفشل في تحليل الاسم.

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.

لا يمكنك حظر الوصول إلى URL محدد عن طريق استخدام وظيفة التصفية، لأن خادم الوكيل قادر على التحقق من محتويات الاتصال.

## طريقة إعداد الاتصال بالشبكة

للحصول على إعدادات الاتصال الخاصة بعنوان IP الطابعة، وقناع الشبكة الفرعية، والبوابة الافتراضية، تابع ما يلي.

## استخدام لوحة التحكم:

قم بتكوين الإعدادات باستخدام لوحة تحكم الطابعة لكل طابعة. اتصل بالشبكة بعد تكوين إعدادات الاتصال الخاصة بالطابعة.

## استخدام برنامج التثبيت:

إذا تم استخدام برنامج التثبيت، فسيتم تعيين شبكة الطابعة والكمبيوتر العميل تلقائياً. يتوفر الإعداد عن طريق اتباع إرشادات برنامج التثبيت، حتى إذا لم يكن لديك معرفة كبيرة بالشبكة. يوصى بذلك عند تعيين الطابعة وعدد قليل من أجهزة الكمبيوتر العميل عن طريق استخدام اتصال العميل/الخادم (مشاركة الطابعة باستخدام خادم Windows the)

## استخدام أداة:

استخدم أداة من كمبيوتر المسؤول. يمكنك اكتشاف إحدى الطابعات ثم تعيين الطابعة، أو إنشاء ملف SYLK لضبط الإعدادات الدفعية للطابعات. يمكنك تعيين العديد من الطابعات، لكن يجب توصيلها بشكل مادي بواسطة كابل إيثرنت قبل الإعداد. لذلك، يوصى بذلك إذا كنت قادراً على إنشاء شبكة إيثرنت للإعداد.

## معلومات ذات صلة

- ◀ "الاتصال بالشبكة من لوحة التحكم" في الصفحة 17
- ◀ "الاتصال بالشبكة باستخدام برنامج التثبيت" في الصفحة 25
- ◀ "تعيين عنوان IP باستخدام" في الصفحة 102 EpsonNet Config



# الاتصال

يوضح هذا الفصل البيئة أو الإجراءات اللازمة لتوصيل الطابعة بالشبكة.

## الاتصال بالشبكة

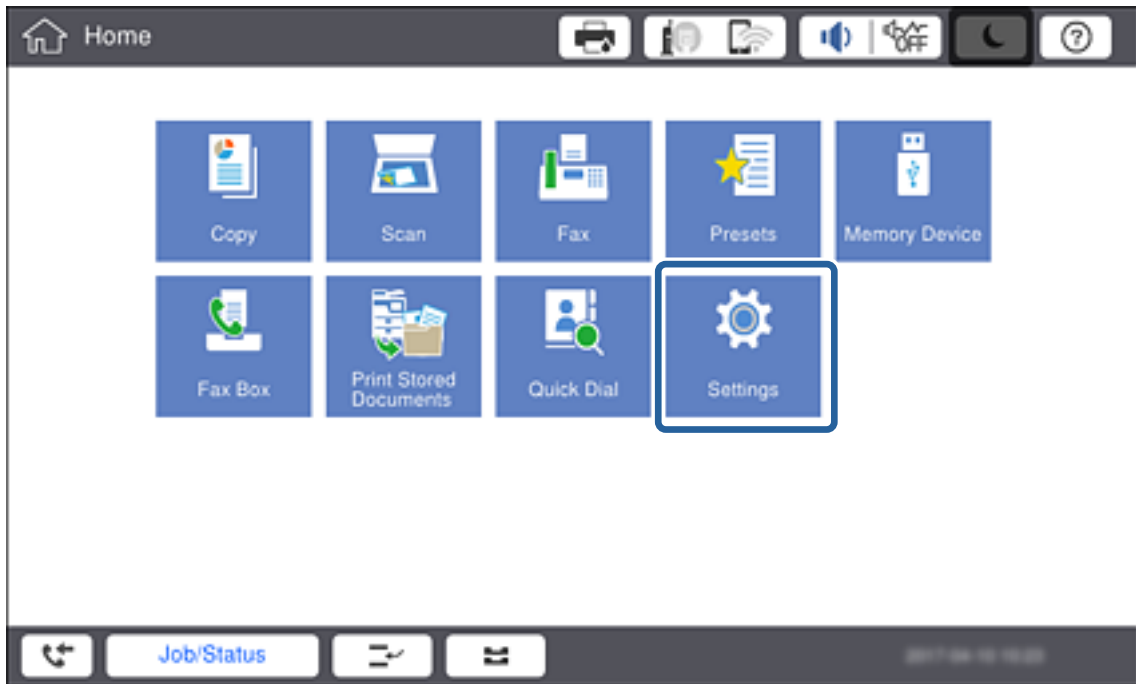
### الاتصال بالشبكة من لوحة التحكم

قم بتوصيل الطابعة بالشبكة باستخدام لوحة تحكم الطابعة. للتعرف على لوحة تحكم الطابعة، اطّلع على دليل المستخدم للحصول على مزيد من التفاصيل.

### تعيين عنوان IP

قم بإعداد العناصر الأساسية مثل عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية.

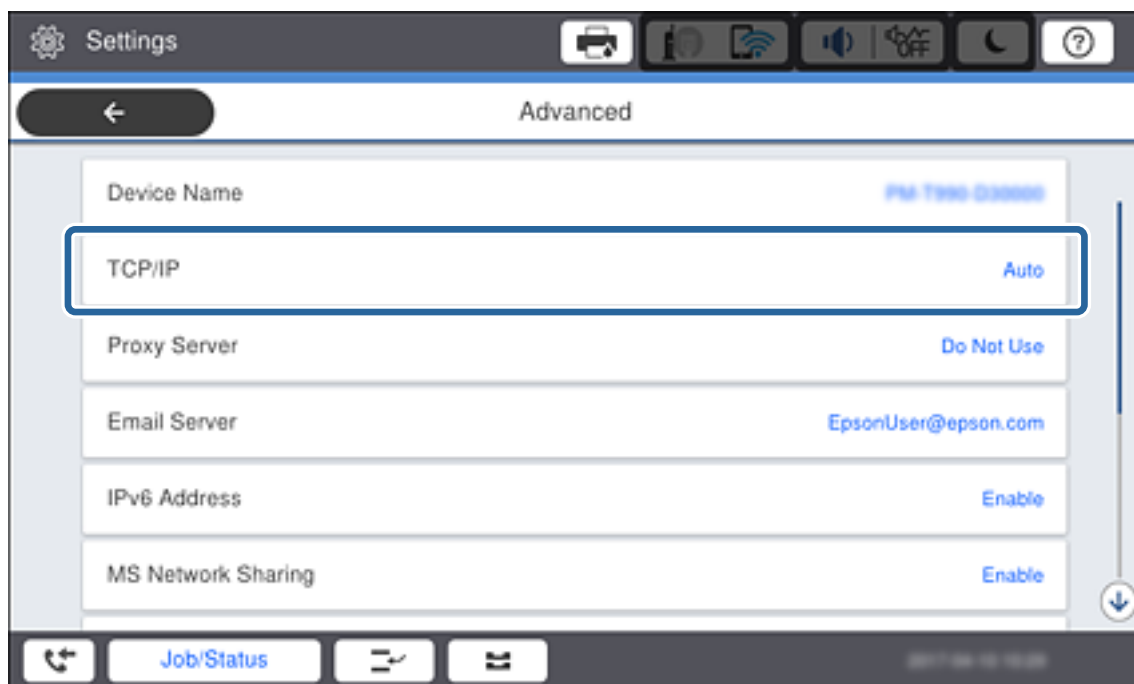
1. قم بتشغيل الطابعة.
2. اضغط على الإعدادات على الشاشة الرئيسية في لوحة التحكم بالطابعة.



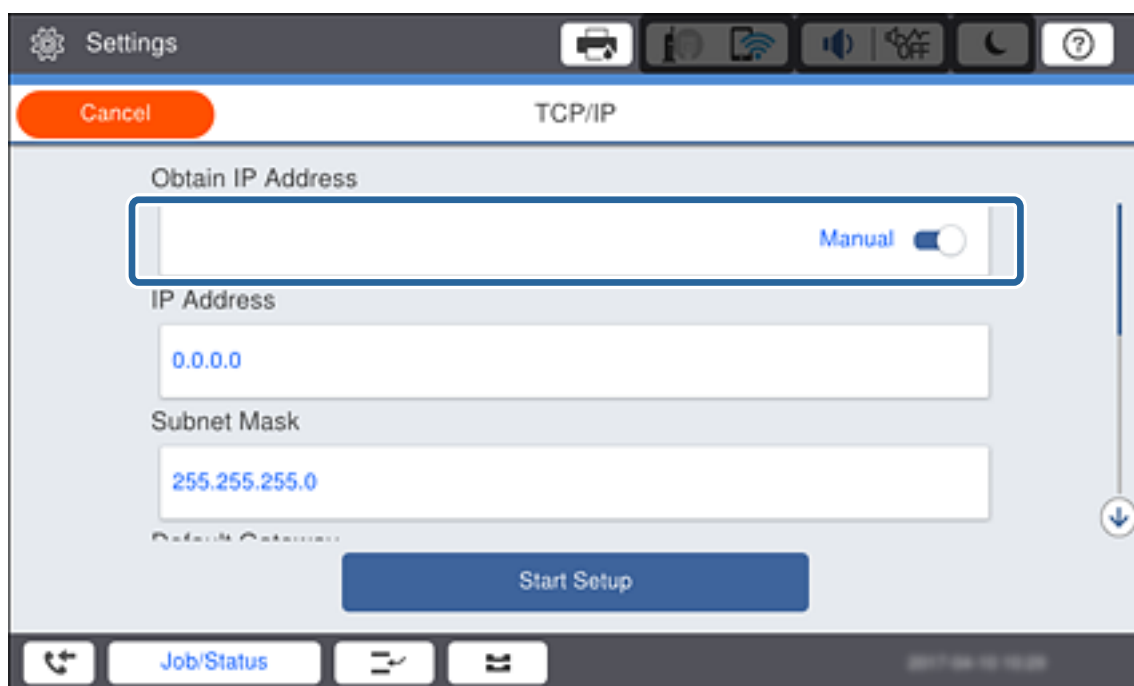
3. اضغط على إعدادات عامة < إعدادات الشبكة > متقدم.

## الاتصال

4. اضغط على TCP/IP.



5. حدد يدوي ل الحصول على عنوان IP.

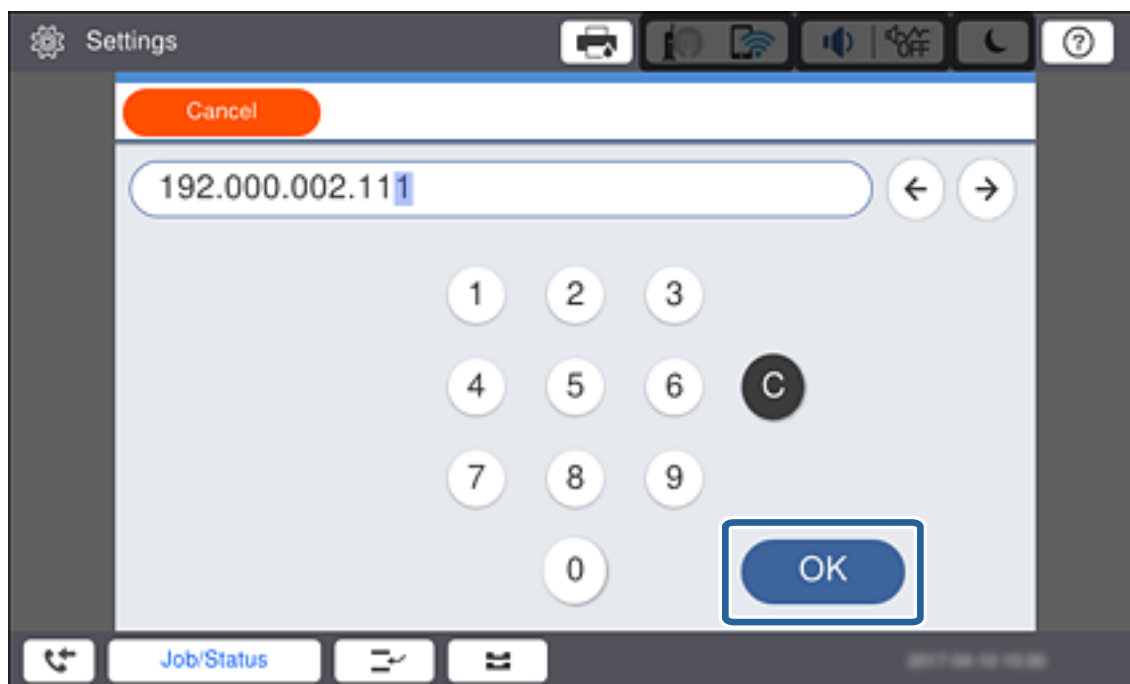


## ملاحظة:

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.

## الاتصال

6. اضغط على خانة عنوان IP وأدخل عنوان IP باستخدام لوحة المفاتيح المعروضة على الشاشة، ثم اضغط على تم بنجاح.



تأكد من عرض القيمة على الشاشة السابقة.

7. اضغط قناع الشبكة الفرعية والبوابة الافتراضية.

تأكد من عرض القيمة على الشاشة السابقة.

**ملاحظة:**

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. اضغط على خانة DNS أساسي لـ خادم DNS، وأدخل عنوان IP لخادم DNS الرئيسي باستخدام لوحة المفاتيح المعروضة على الشاشة، ثم اضغط على موافق.

تأكد من عرض القيمة على الشاشة السابقة.

**ملاحظة:**

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

9. اضغط على خانة DNS ثانوي وأدخل عنوان IP لخادم DNS الثانوي باستخدام لوحة المفاتيح المعروضة على الشاشة، ثم اضغط على موافق.

تأكد من عرض القيمة على الشاشة السابقة.

10. اضغط على بدء الإعداد.

11. اضغط على إغلاق على شاشة التأكيد.

**إعداد خادم الوكيل**

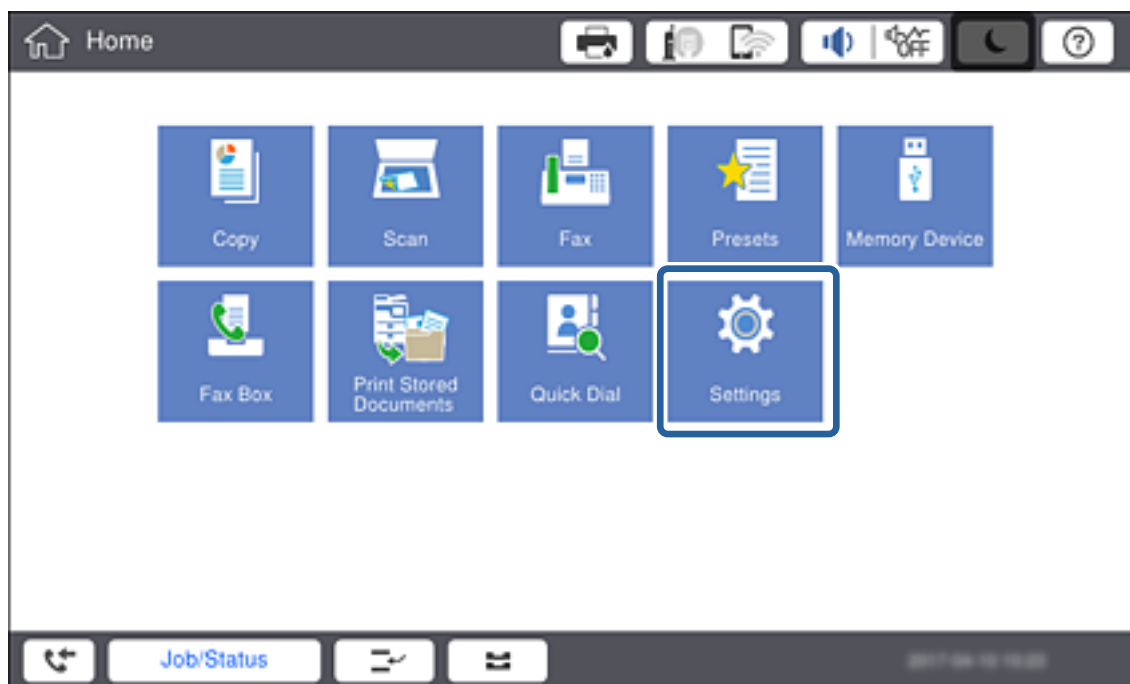
إذا قمت بإنشاء خادم وكيل في بيئة شبكتك، فقم بإعداد خادم الوكيل.

## الاتصال

1. اضغط على الإعدادات على الشاشة الرئيسية.

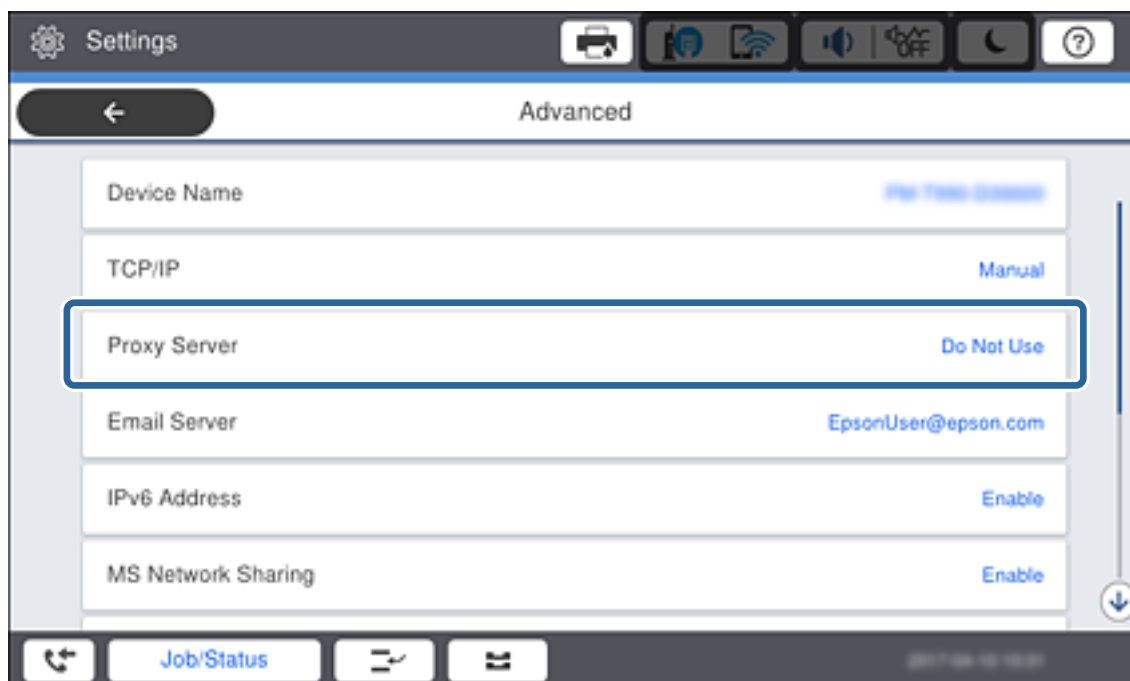
ملاحظة:

عند ضبط الإعدادات بعد تعيين عنوان IP، يتم عرض شاشة متقدم. انتقل إلى الخطوة 3.



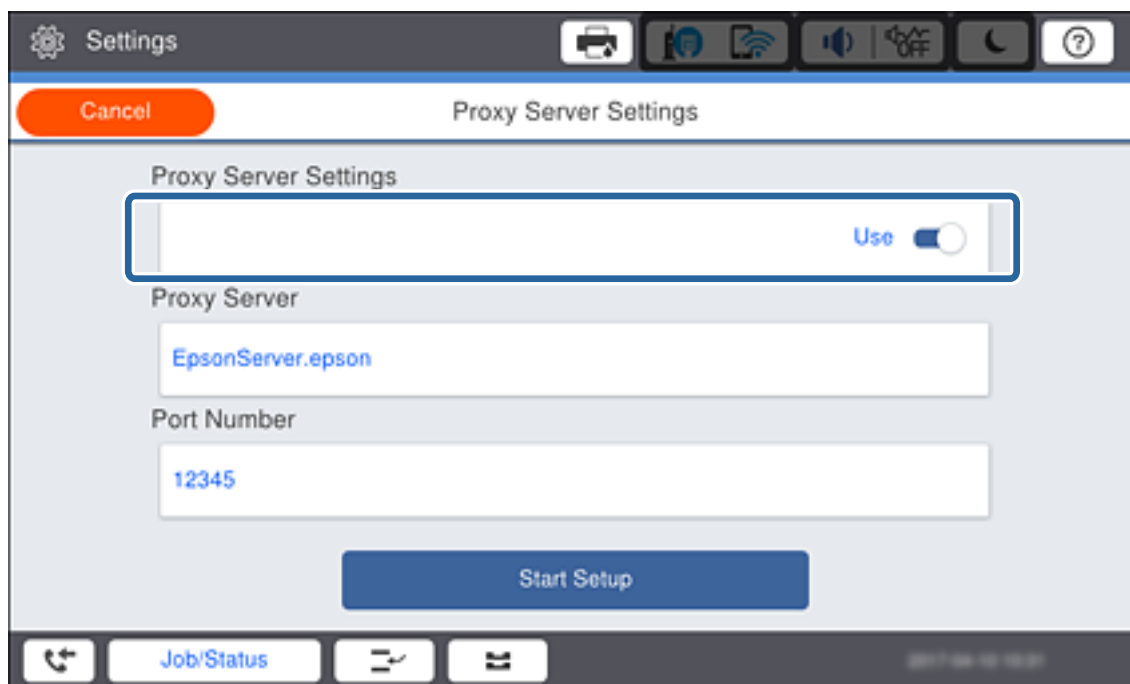
2. اضغط على إعدادات عامة < إعدادات الشبكة > متقدم.

3. اضغط على الخادم الوكيل.

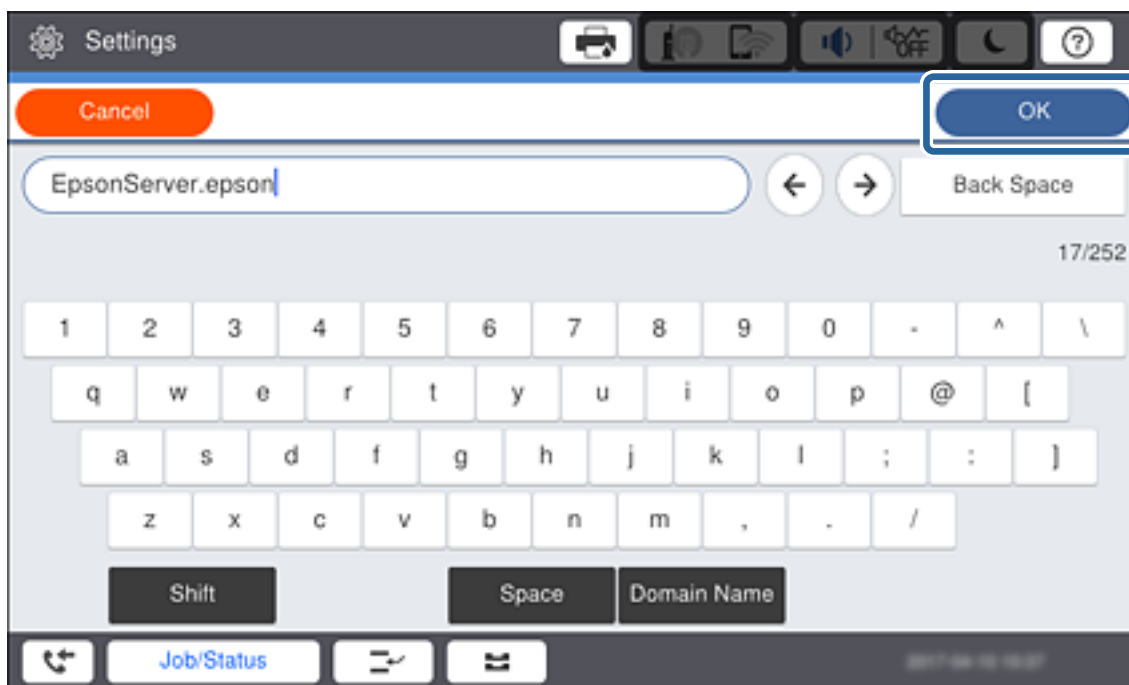


## الاتصال

4. حدد استخدم لـ إعدادات الخادم الوكيل.



5. اضغط على خانة الخادم الوكيل وأدخل عنوان خادم الوكيل بتنسيق IPv4 أو FQDN باستخدام لوحة المفاتيح المعروضة على الشاشة، ثم اضغط على موافق.



تأكد من عرض القيمة على الشاشة السابقة.

6. اضغط على خانة رقم المنفذ وأدخل رقم المنفذ لخادم الوكيل باستخدام لوحة المفاتيح المعروضة على الشاشة، ثم اضغط على تم بنجاح. تأكد من عرض القيمة على الشاشة السابقة.

7. اضغط على بدء الإعداد.

## الاتصال

8. اضغط على إغلاق بعد شاشة التأكيد.

## الاتصال بشبكة LAN

قم بتوصيل الطابعة بالشبكة باستخدام إيثرنت أو Wi-Fi.

معلومات ذات صلة

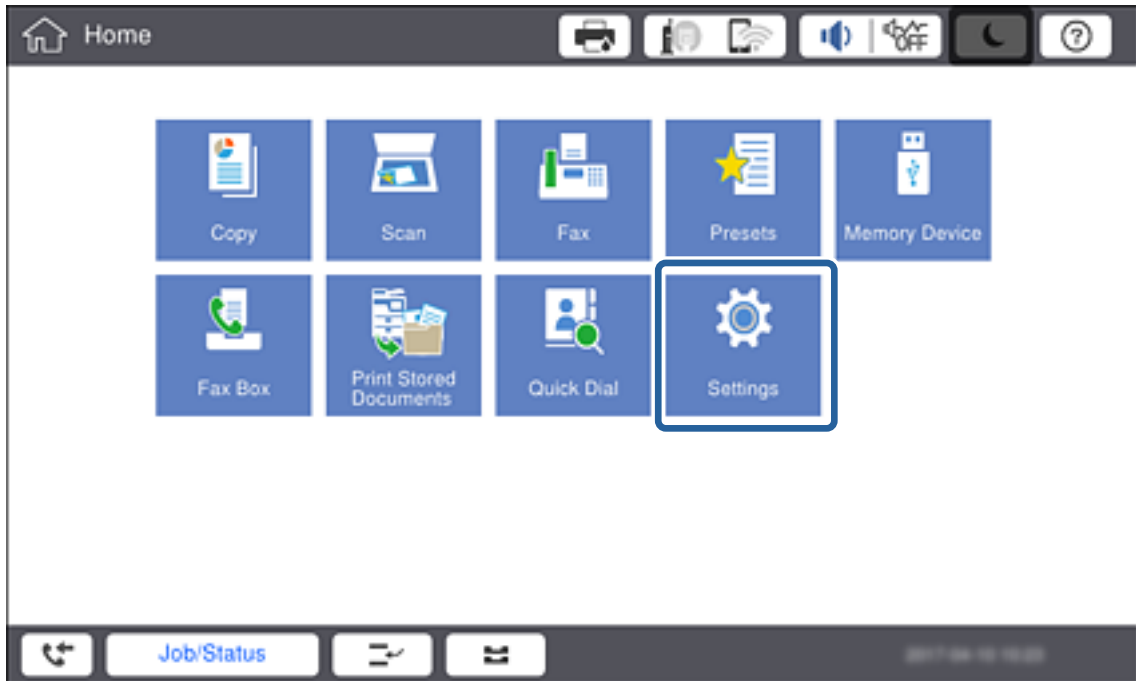
- ← "الاتصال بشبكة الإيثرنت" في الصفحة 22
- ← "ضبط إعدادات Wi-Fi يدوياً من خلال لوحة التحكم" في الصفحة 23
- ← "الاتصال بالشبكة باستخدام برنامج التثبيت" في الصفحة 25

## الاتصال بشبكة الإيثرنت

وصّل الطابعة بالشبكة باستخدام كابل الإيثرنت، وتحقق من الاتصال.

1. وصل الطابعة وموزع الشبكة (جهاز التبديل L2) بكابل إيثرنت.

2. اضغط على الإعدادات على الشاشة الرئيسية.



3. اضغط على إعدادات عامة > إعدادات الشبكة.

4. اضغط على التحقق من الاتصال.

يتم عرض نتيجة تشخيص الاتصال. تأكد من صحة الاتصال.

5. اضغط على موافق.

ملاحظة:

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

## الاتصال

## معلومات ذات صلة

← "تغيير الاتصال من الاتصال بشبكة إيثرنت إلى الاتصال بشبكة Wi-Fi" في الصفحة 109

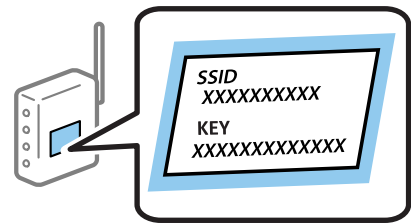
## ضبط إعدادات Wi-Fi يدوياً من خلال لوحة التحكم

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

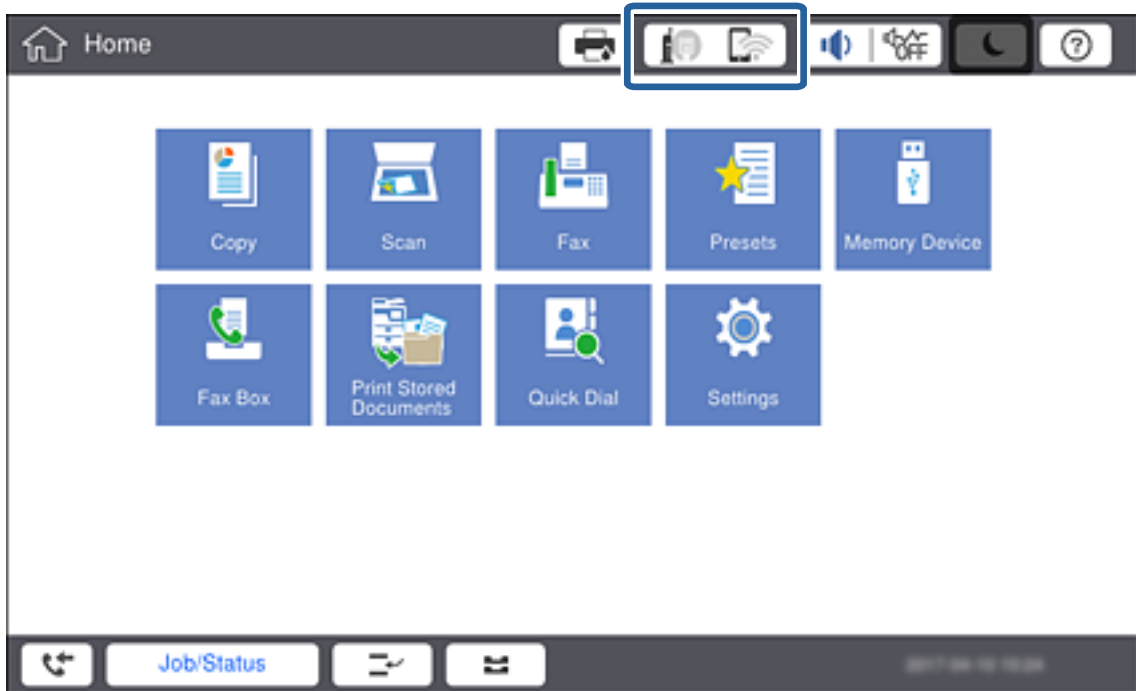
عندما تدعم نقطة الوصول WPS، يمكنك ضبط إعدادات اتصال Wi-Fi تلقائياً عن طريق استخدام زر الضغط أو رمز PIN، دون استخدام SSID وكلمة المرور.

## ملاحظة:

إذا كنت تستخدم نقطة وصول مع الإعدادات الافتراضية الخاصة بها، فستجد معرف الشبكة وكلمة المرور على الملصق. إذا كنت تجهل معرف الشبكة وكلمة المرور، فاتصل بالشخص الذي قام بإعداد نقطة الوصول، أو راجع الوثائق المرفقة مع نقطة الوصول.

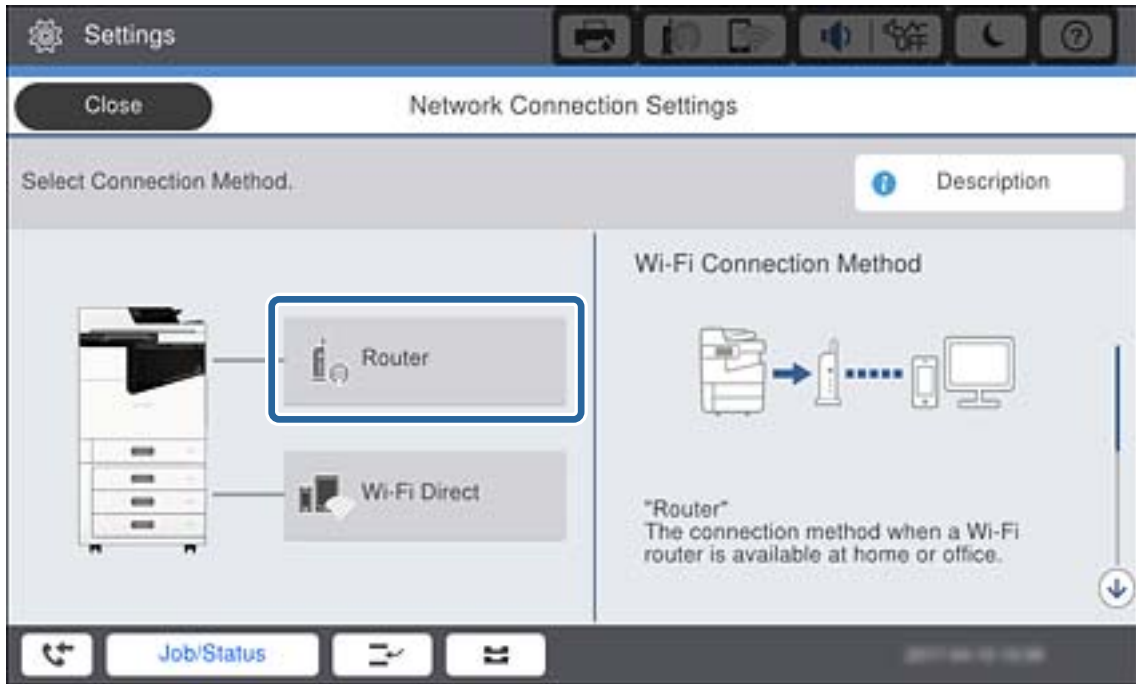


1. اضغط على  |  في لوحة تحكم الطابعة.



## الاتصال

2. اضغط على راوتر.



3. اضغط على بدء الإعداد.

4. اضغط على إعداد Wi-Fi.

إذا قمت بضبط إعدادات الإيثرنت، فتتحقق من الرسالة ثم اضغط على نعم.

5. اضغط على معالج إعداد Wi-Fi.

6. حدد SSID الخاص بنقطة الوصول.

ملاحظة:

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

إذا كنت لا تعرف SSID، فتتحقق من كتابتها على الملصق الخاص بنقطة الوصول. إذا كنت تستخدم نقطة الوصول بإعداداتها الافتراضية، فاستخدم SSID المكتوبة على الملصق.

7. اضغط على إدخال كلمة المرور، وأدخل كلمة المرور، ثم اضغط على موافق.

ملاحظة:

كلمة المرور حساسة لحالة الأحرف.

إذا كنت لا تعرف كلمة المرور، فتتحقق من كتابتها على الملصق الخاص بنقطة الوصول. إذا كنت تستخدم نقطة الوصول بإعداداتها الافتراضية، فاستخدم كلمة المرور المكتوبة على الملصق. فد يُطلق على كلمة المرور أيضاً "مفتاح"، و"عبارة مرور"، وما إلى ذلك.

إذا أدخلت SSID مباشرة، فحدد متوفر لـ كلمة المرور، ثم أدخل كلمة المرور.

إذا كنت لا تعرف كلمة المرور الخاصة بنقطة الوصول، فانظر في الوثائق المرفقة مع نقطة الوصول أو اتصل بالشخص الذي قام بإعدادها.

8. عند اكتمال الإدخال، اضغط على بدء الإعداد.

9. اضغط على موافق.

ملاحظة:

إذا فشلت في الاتصال، فقم بتحميل ورق عادي بحجم A4، واضغط على طباعة تقرير الفحص لطباعة تقرير الاتصال بالشبكة.



## الاتصال

10. اضغط على إغلاق على شاشة إعدادات اتصال الشبكة.

معلومات ذات صلة

- ◀ "ضبط إعدادات Wi-Fi من لوحة التحكم (WPS)" في الصفحة 106
- ◀ "تغيير الاتصال من الاتصال بشبكة Wi-Fi إلى اتصال الإيثرنت" في الصفحة 109

## الاتصال بالشبكة باستخدام برنامج التثبيت

نوصي باستخدام برنامج التثبيت لتوصيل الطابعة بالكمبيوتر. يمكنك تشغيل برنامج التثبيت باستخدام إحدى الطرق التالية.

□ الإعداد من موقع الويب

قم بزيارة الموقع التالي، ثم أدخل اسم المنتج. انتقل إلى الإعداد، ثم قم ببدء الإعداد.

<http://epson.sn>

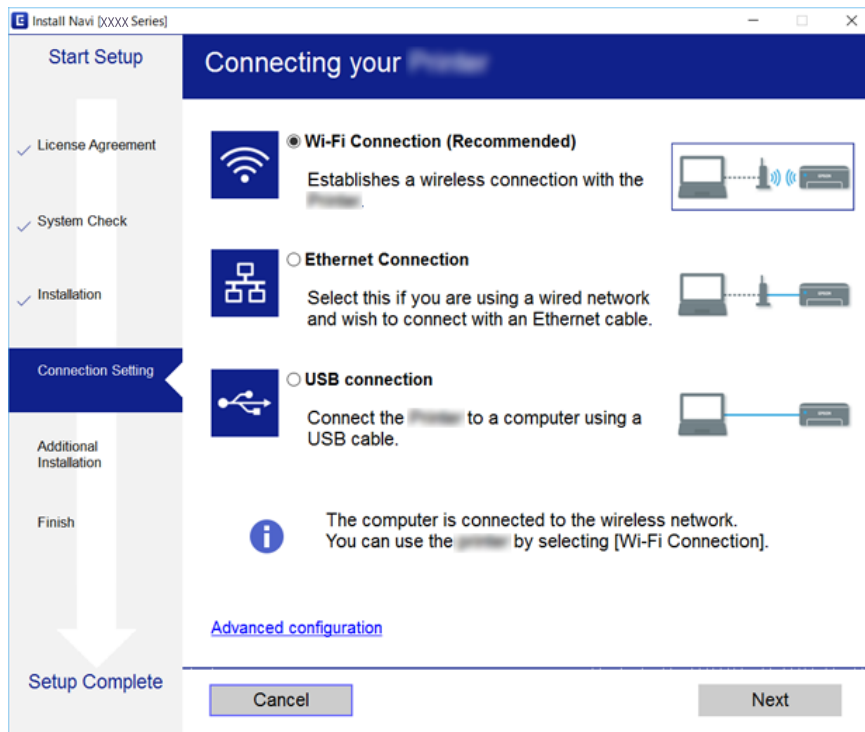
□ الإعداد باستخدام قرص البرامج (فقط للطرز المزودة بقرص برامج والمستخدمين الذين يمتلكون أجهزة كمبيوتر مزودة بمحركات أقراص).  
أدخل قرص البرامج داخل جهاز الكمبيوتر، ثم اتبع التعليمات المعروضة على الشاشة.

تحديد طرق الاتصال

اتباع التعليمات المعروضة على الشاشة إلى أن يتم عرض الشاشة التالية، ثم حدد طريقة اتصال الطابعة بالكمبيوتر.

□ Windows

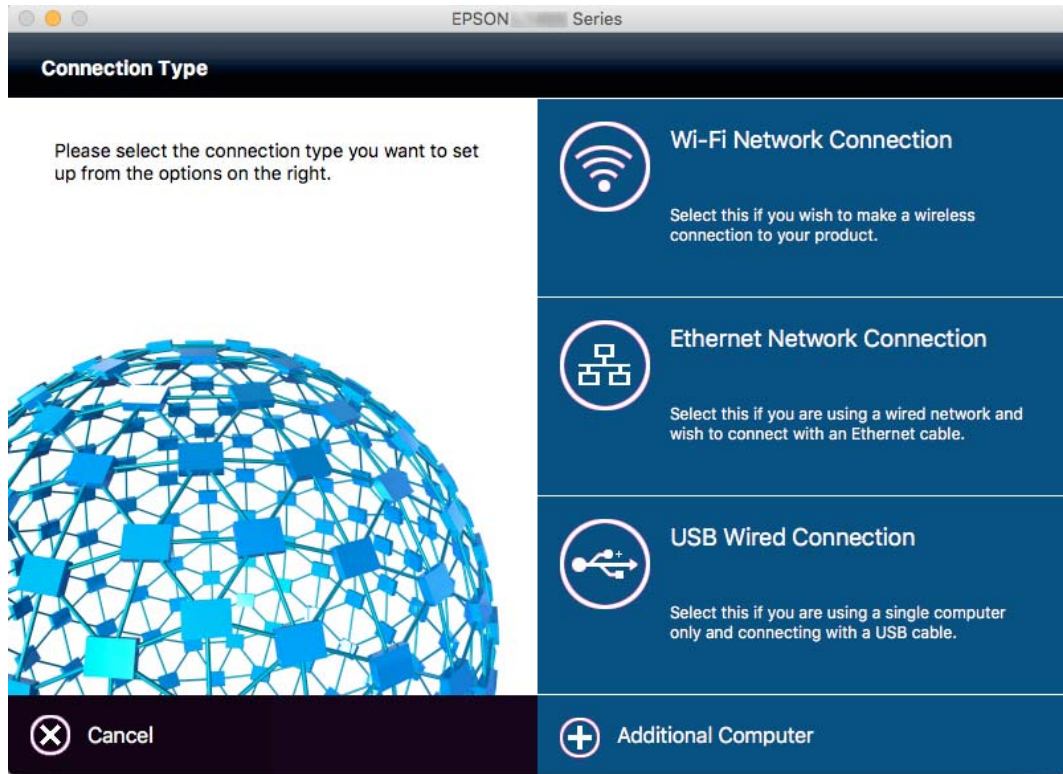
حدد نوع الاتصال ثم انقر فوق التالي.



## الاتصال

Mac OS 

حدد نوع الاتصال.



اتبع التعليمات المعروضة على الشاشة. تم تثبيت البرنامج الضروري.

## الاتصال بخط هاتف

### خطوط الهاتف المتوافقة

يمكنك استخدام الطابعة على خطوط الهاتف التناظرية القياسية (PSTN = الشبكة العامة لتحويل الهاتف) و أنظمة الهاتف PBX (شبكة الهاتف الخاصة).

قد لا تتمكن من استخدام الطابعة مع خطوط أو أنظمة الهاتف التالية.

خط الهاتف الذي يستخدم خدمة VoIP (خدمة الهاتف عبر بروتوكول الإنترنت) مثل DSL أو خدمة الألياف الضوئية الرقمية.

خط الهاتف الرقمي (ISDN)

بعض أنظمة شبكة الهاتف الخاصة (PBX)

عندما تكون هناك محولات مثل المحولات الطرفية، محولات VoIP، المقسمات، أو موجه DSL تصل بين مقبس الهاتف الموجود بالحائط والطابعة.

### توصيل الطابعة بخط هاتف

وصِّل الطابعة بمقبس هاتف بالحائط باستخدام كبل هاتف RJ-11 (6P2C). عند توصيل هاتف بالطابعة، استخدم كبل هاتف RJ-11 (6P2C) آخر.

## الاتصال

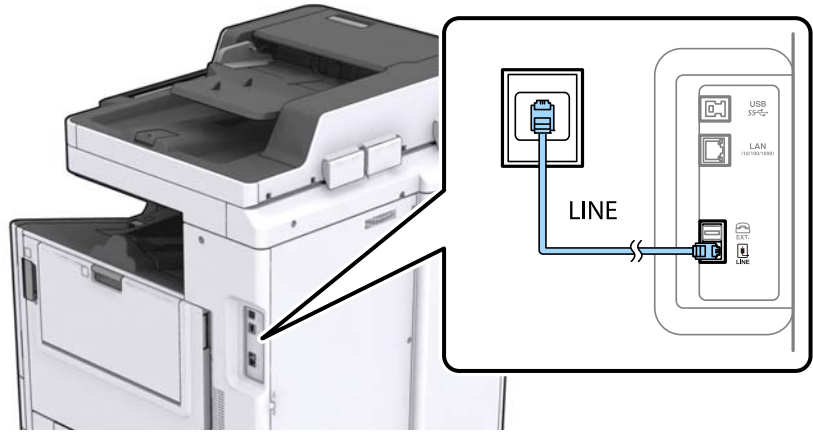
وفقاً للمنطقة، قد يكون كابل الهاتف مرفقاً مع الطابعة. فإذا كان مرفقاً، استخدم هذا الكابل. قد تحتاج إلى توصيل خط الهاتف بالمحول المرفق خصيصاً لدولتك أو منطقتك.

## ملاحظة:

قم بإزالة الغطاء من منفذ *EXT* الموجود بالطابعة فقط عند توصيل هاتفك بالطابعة. لا تقم بإزالة الغطاء في حالة عدم توصيل هاتفك. في المناطق التي تضربها الصواعق بشكل متكرر، نوصي باستخدام جهاز حماية ضد التيار المتغير.

## التوصيل بخط هاتف قياسي (PSTN) أو (PBX)

قم بتوصيل كابل الهاتف من مقبس الهاتف الموجود بالحائط أو منفذ PBX بمنفذ LINE الموجود في الجزء الخلفي من الطابعة.

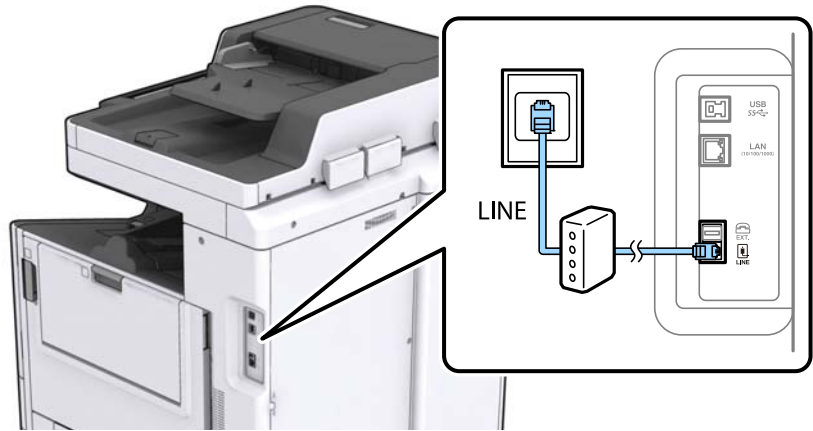


## التوصيل بخط DSL أو ISDN

قم بتوصيل كابل الهاتف من مودم DSL أو محول ISDN الطرفي بمنفذ LINE الموجود في الجزء الخلفي من الطابعة. انظر الوثائق المرفقة مع المودم أو المحول للتعرف على التفاصيل.

## ملاحظة:

إذا لم يكن مودم DSL الخاص بك مزوداً بوحدة تصفية DSL مدمجة، قم بتوصيل وحدة تصفية DSL منفصلة.



## توصيل جهاز الهاتف الخاص بك بالطابعة

عند استخدام الطابعة والهاتف الخاص بك على خط هاتف واحد، قم بتوصيل الهاتف بالطابعة.

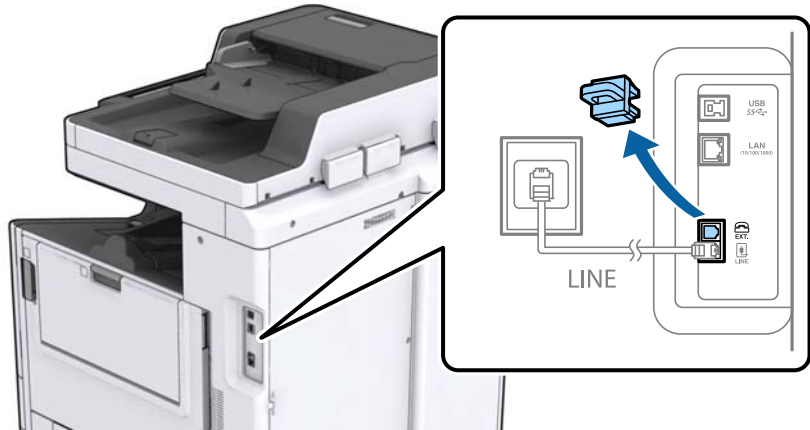
## الاتصال

## ملاحظة:

□ إذا كان جهاز الهاتف الخاص بك مزوداً بوظيفة الفاكس، قم بتعطيل وظيفة الفاكس قبل التوصيل. انظر الأدلة المرفقة مع جهاز الهاتف للتعرف على التفاصيل.

□ إذا وصّمت جهاز رد آلي، فتأكد من ضبط إعدادات عدد رنات الرد للطابعة على عدد أكبر من الرنات التي تم ضبط جهاز الرد الآلي عليه للرد على مكالمته.

1. قم بإزالة الغطاء من منفذ EXT الموجود بالجزء الخلفي من الطابعة.



2. قم بتوصيل جهاز الهاتف ومنفذ EXT باستخدام كابل الهاتف.



## ملاحظة:

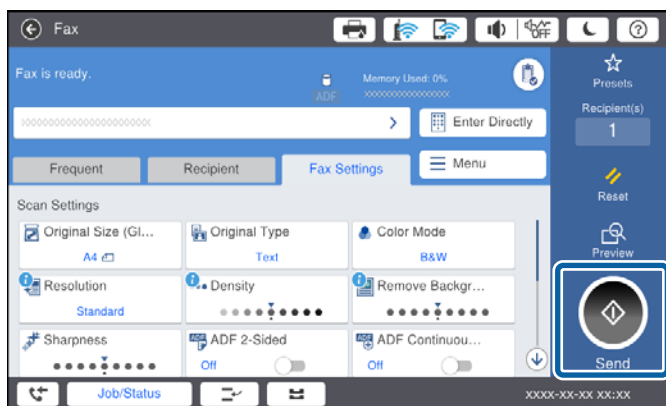
عند الاستخدام المشترك لكابل هاتف واحد، تأكد من توصيل جهاز الهاتف بمنفذ EXT الموجود بالطابعة. إذا قمت بتقسيم الخط لتوصيل جهاز الهاتف والطابعة بشكل منفصل، لا يعمل الهاتف والطابعة بالشكل الصحيح.

3. اضغط على الفاكس على الشاشة الرئيسية.

## الاتصال

4. التقط السماعة.

يتم تكوين الاتصال عند تفعيل (إرسال) وفقاً للشاشة التالية.



معلومات ذات صلة

← "الإعدادات الخاصة بجهاز الرد الآلي" في الصفحة 47

## ضبط إعدادات الفاكس الأساسية

يختلف عنصر إعداد الفاكس حسب منطقة الاستخدام أو دولته.

ادخل إلى تهيئة الويب وحدد علامة التبويب **Country/Region < Device Management** لضبط إعدادات دولتك أو منطقتك قبل البدء في ضبط الإعدادات الأخرى.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## ضبط إعدادات الفاكس الأساسية باستخدام معالج إعداد الفاكس

قم بضبط الإعدادات الأساسية باتباع التعليمات المعروضة على الشاشة.

1. قم بتوصيل الطابعة بخط الهاتف.

ملاحظة:

نظراً لإجراء الفحص التلقائي لاتصال الفاكس في نهاية المعالج، تأكد من توصيل الطابعة بخط الهاتف قبل بدء المعالج.

2. اضغط على الإعدادات على الشاشة الرئيسية.

3. اضغط على إعدادات عامة &lt; إعدادات الفاكس &lt; معالج إعداد الفاكس.

4. على شاشة تأكيد اضغط على موافق.

المعالج يبدأ.

5. في شاشة إدخال الترويسة الخاصة بالفاكس، أدخل اسم المرسل على سبيل المثال اسم شركتك، ثم اضغط على تم بنجاح.

ملاحظة:

يظهر اسم المرسل ورقم الفاكس الخاص بك كترويسة في الفاكسات الصادرة.

## الاتصال

6. في شاشة إدخال رقم الهاتف، قم بإدخال رقم الفاكس، ثم اضغط على **تم بنجاح**.
7. من شاشة إعداد **Distinctive Ring Detection (DRD)**، قم بضبط الإعدادات التالية.
- إذا كنت مشتركاً في خدمة الرنين المميز من شركة الاتصالات التي تتعامل معها: فاضغط على **متابعة**، ثم حدد نمط الرنين المطلوب استخدامه للفاكسات الواردة.
- إذا حددت الكل، فانتقل إلى الخطوة 8.
- إذا حددت أي إعداد آخر، فسيتم تعيين **وضع الاستلام على تلقاء تلقائياً**. انتقل إلى الخطوة 10.
- إذا لم ترغب في إعداد هذا الخيار: فاضغط على **تخطي**، ثم انتقل إلى الخطوة 10.
- ملاحظة:**
- خدمات الرنين المميز، التي توافرها العديد من شركات الهاتف (يختلف اسم الخدمة باختلاف الشركة)، تسمح لك باستخدام أرقام هاتف متعددة على خط هاتف واحد. يتم تحديد نمط رنين مختلف لكل رقم. يمكنك استخدام رقم واحد للمكالمات الصوتية وخط آخر لمكالمات الفاكس. حدد نمط الرنين المخصص لمكالمات الفاكس في **DRD**.
- وفقاً للمنطقة، تظهر تشغيل و إيقاف كخيارات **DRD**. حدد تشغيل لاستخدام ميزة الرنين المميز.
8. من شاشة إعداد **وضع الاستلام**، حدد ما إذا كنت تستخدم جهاز الهاتف الخاص بك وهو متصل بالطابعة.
- عند اتصاله: اضغط على **نعم**، ثم انتقل إلى الخطوة التالية.
- عند عدم اتصاله: اضغط على **لا**، ثم انتقل إلى الخطوة 10. **وضع الاستلام** يتم ضبطه على **الوضع تلقاء**.
9. من شاشة إعداد **وضع الاستلام**، حدد ما إذا كنت تريد استلام الفاكسات بشكل تلقائي.
- للاستلام التلقائي: اضغط على **نعم**. **وضع الاستلام** يتم ضبطه على **الوضع تلقاء**.
- للاستلام اليدوي: اضغط على **لا**. **وضع الاستلام** يتم ضبطه على **الوضع يدوي**.
10. من شاشة **متابعة** راجع الإعدادات التي قمت بضبطها، ثم اضغط على **متابعة**.
- لتصحيح الإعدادات أو تغييرها، اضغط على .
11. اضغط على **بدء التحقق** لإجراء فحص اتصال الفاكس، وعندما يظهر لك على الشاشة طلب طباعة نتيجة الفحص، اضغط على **طباعة**. تتم طباعة تقرير نتيجة الفحص التي تظهر حالة الاتصال.
- ملاحظة:**
- في حالة الإبلاغ بوجود أية أخطاء، اتبع التعليمات الواردة في التقرير لمعالجة تلك الأخطاء.
- في حالة ظهور شاشة **تحديد نوع الخط**، حدد نوع الخط.
- في حالة توصيلك للطابعة بنظام هاتف **PBX** أو محول طرفي، حدد **PBX**.
- في حالة توصيلك للطابعة بخط هاتف قياسي (**PSTN**)، حدد **تعطيل** على شاشة تأكيد المعروضة. ولكن، ضبط هذا الإعداد على **تعطيل** قد يؤدي إلى تخطي الطابعة للخدمة الرقمية الأولى من رقم الفاكس عند الاتصال وإرسال الفاكس إلى رقم خاطئ.

## معلومات ذات صلة

← "توصيل الطابعة بخط هاتف" في الصفحة 26

← "وصف قائمة إعدادات الفاكس" في الصفحة 51

## ضبط إعدادات مصدر الورق لاستلام الفاكسات

يمكنك ضبط الطابعة بحيث لا يتم استخدام بعض مصادر الورق المحددة في طباعة المستندات المستلمة وتقارير الفاكس. يتم تمكين جميع مصادر الورق لطباعة الفاكس افتراضياً. استخدم هذه الميزة إذا كنت لا ترغب في استخدام الورق في مصدر ورق معين لطباعة الفاكس.

## الاتصال

1. اضغط على الإعدادات على الشاشة الرئيسية.
2. اضغط على إعدادات عامة < إعدادات الطابعة < إعدادات مصدر الورق < إعدادات التحديد التلقائي < الفاكس.
3. اضغط على جميع صناديق مصادر الورق الذي لا ترغب في استخدامها لطباعة الفاكس. يتم تغيير إعداد مصدر الورق إلى إيقاف ويتم تعطيل استخدامه لطباعة الفاكسات.

## استخدام اتصال Wi-Fi Direct (نقطة الوصول البسيط)

يمكنك الاتصال بالطابعة مباشرة دون المرور عبر الشبكة المتصلة عن طريق استخدام Wi-Fi Direct (نقطة الوصول البسيط) من هاتف ذكي أو كمبيوتر لوحي عندما يسمح المسؤول بالاتصال المباشر. عند استخدام NFC من هاتف ذكي أو كمبيوتر لوحي، يجب تمكين Wi-Fi Direct (نقطة الوصول البسيط).

### تمكين شبكة Wi-Fi Direct (نقطة الوصول البسيط)

1. ادخل إلى Web Config وحدد علامة التبويب **Wi-Fi Direct < Network**.
  2. حدد **Wi-Fi Direct** Enable.
  3. انقر فوق **Next**.
  4. انقر فوق **OK**.
- إذا تمت إعادة توصيل الشبكة، فسيتم تمكين Wi-Fi Direct (نقطة الوصول البسيط).
- ملاحظة:  
عن طريق النقر فوق **Delete** يمكنك حذف معلومات الجهاز المسجلة المتصل عبر **Wi-Fi Direct** (نقطة الوصول البسيط).

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## تكوين خادم البريد

كُون هذا عندما تريد استخدام وظيفة المسح الضوئي باستخدام البريد الإلكتروني أو عندما تريد تلقي رسائل الأحداث من الأجهزة. تحقق من النقاط التالية قبل التكوين.

الطابعة متصلة بالشبكة.

معلومات خادم البريد الإلكتروني للكمبيوتر.

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.

## الاتصال

معلومات ذات صلة

- ← "الوصول إلى تطبيق Web Config" في الصفحة 37
- ← "عناصر إعداد خادم البريد الإلكتروني" في الصفحة 32

## عناصر إعداد خادم البريد الإلكتروني

العناصر	الإعدادات والشرح
Authentication Method	حدد أسلوب المصادقة الذي يتيح للطابعة الوصول إلى خادم البريد الإلكتروني.
	Off يتم تعطيل المصادقة عند الاتصال بخادم البريد الإلكتروني.
	SMTP AUTH يتطلب دعم خادم البريد الإلكتروني مصادقة SMTP.
	POP before SMTP قم بتكوين خادم POP3 عند تحديد هذا الأسلوب.
Authenticated Account	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).
Authenticated Password	إذا قمت بتحديد SMTP AUTH أو POP before SMTP في شكل Authentication Method، فأدخل كلمة المرور التي تمت مصادقتها وتتكون من عدة رموز تتراوح ما بين 0 و 20 رمزاً باستخدام 0-9 a-z A-Z ! # \$ % & * ' / . ? _ ^ }   ~ @ .
Sender's Email Address	أدخل عنوان البريد الإلكتروني للمرسل. أدخل عدة رموز ما بين 0 و 255 رمزاً بتنسيق (ASCII (0x20-0x7E) فيما عدا: ( ) < ; [ ] \. لا يمكن أن تكون الفاصلة الزمنية ". الرمز الأول.



## الاتصال

العناصر	الإعدادات والشرح
SMTP Server Address	أدخل عددًا من الرموز يتراوح ما بين 0 إلى 255 رمزًا باستخدام A-Z، و a-z، و 0-9. - يمكنك استخدام تنسيق IPv4 أو FQDN.
SMTP Server Port Number	أدخل عددًا بين 1 و 65535.
Secure Connection	حدّد طريقة التوصيل الآمنة لخدم البريد الإلكتروني.
	None إذا قمت بتحديد POP before SMTP في Authentication Method، فسيتم ضبط طريقة التوصيل على None.
	SSL/TLS هذا يكون متاحًا عندما يتم ضبط Authentication Method على الوضع Off أو SMTP AUTH.
STARTTLS هذا يكون متاحًا عندما يتم ضبط Authentication Method على الوضع Off أو SMTP AUTH.	
Certificate Validation	يتم التحقق من صحة الشهادة عند تمكين هذا الوضع. كما يوصي بضبطها على وضع Enable.
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 رمزًا 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 عددًا ما بين 1 و 65535.

معلومات ذات صلة

← "تكوين خادم البريد" في الصفحة 31

## التحقق من اتصال خادم البريد

1. ادخل إلى Web Config وحدد علامة التبويب Network &lt; Email Server &lt; Connection Test.

2. حدد Start.

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

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "مراجع اختبار اتصال خادم البريد" في الصفحة 33

## مراجع اختبار اتصال خادم البريد

الرسائل	الشرح
Connection test was successful.	تظهر هذه الرسالة عند نجاح الاتصال بالخادم.

## الاتصال

الرسائل	الشرح
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 SMTP <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"/> 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
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 SMTP
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	تظهر هذه الرسالة عند <input type="checkbox"/> فشل الاتصال بخادم DNS <input type="checkbox"/> فشل تحليل الاسم لخادم POP3
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	تظهر هذه الرسالة عند تعذر مصافحة خادم SMTP.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	تظهر هذه الرسالة عند تعذر مصافحة خادم POP3.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	تظهر هذه الرسالة عند محاولة الاتصال ببروتوكولات غير معتمدة.
Connection to SMTP server failed. Change Secure Connection to None.	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 SSL/TLS.	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 STARTTLS.	تظهر هذه الرسالة عند حدوث عدم توافق SMTP بين الخادم وأحد العملاء أو عندما يطلب الخادم استخدام اتصال STARTTLS للاتصال الآمن بـ SMTP.
The connection is untrusted. Check the following. - Date and Time	تظهر هذه الرسالة عندما تكون إعدادات التاريخ والوقت للطابعة غير صحيحة أو إذا انتهت صلاحية الشهادة.
The connection is untrusted. Check the following. - CA Certificate	تظهر هذه الرسالة عندما لا تحتوي الطابعة على شهادة جذر تتوافق مع الخادم أو لم يتم استيراد CA Certificate.
The connection is not secured.	تظهر هذه الرسالة عند تلف الشهادة التي تم الحصول عليها.

## الاتصال

الرسائل	الشرح
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	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 POP before SMTP.	تظهر هذه الرسالة عندما يحدث عدم توافق في طريقة المصادقة بين الخادم وأحد العملاء. لا يدعم الخادم خاصية SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	تظهر هذه الرسالة عندما يكون عنوان البريد الإلكتروني للمرسل المحدد خاطئ.
Cannot access the printer until processing is complete.	تظهر هذه الرسالة عندما تكون الطابعة مشغولة.

## معلومات ذات صلة

← "التحقق من اتصال خادم البريد" في الصفحة 33

# 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 هو تطبيق مستند على المستعرض وخاص بتكوين إعدادات الطابعة.

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 displays the Epson Web Config interface for the L3-10000F printer. The main content area is titled "Product Status" and includes a language dropdown menu set to "English". Below this, there are sections for "Printer Status" (Available) and "Scanner Status" (Available). A row of ink level indicators shows Black (BK), Yellow (Y), Magenta (M), and Cyan (C) levels. A table below provides specific ink levels: Black (BK) at LXB01, Yellow (Y) at LY01, Magenta (M) at LXM01, and Cyan (C) at LXC01. The Maintenance Box level is LMB01. The Card Reader Status is Disconnected. The Cassette 1 section shows Paper Size as Auto(A4(Vertical)), Paper Type as plain papers 1, and Paper Remaining Level as Low. A Refresh button and a link to Software Licenses are located at the bottom of the page.

## 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.

الوصول عبر HTTPS

IPv4: https://<عنوان IP للطابعة> (دون < >)

IPv6: https://[عنوان IP للطابعة]/ (مع [ ])

الوصول عن طريق بروتوكول HTTP

IPv4: http://<عنوان IP للطابعة> (دون < >)

IPv6: http://[عنوان IP للطابعة]/ (مع [ ])

ملاحظة:

أمثلة

IPv4

https://192.0.2.111/

http://192.0.2.111/

IPv6

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

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

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 115

← "حول المصادقة الرقمية" في الصفحة 115

## استخدام وظائف الطابعة

مكّن استخدام وظيفة الطابعة في الطابعة.

## متطلبات الطابعة عبر الشبكة

يُعد ما يلي مطلوباً للطابعة عبر الشبكة.

يمكنك تكوين هذه الإعدادات باستخدام برنامج تشغيل الطابعة ووظائف نظام التشغيل.

تثبيت برنامج تشغيل الطابعة

ضبط قائمة انتظار الطابعة لأحد أجهزة الكمبيوتر

ضبط منفذ لإحدى الشبكات

## إعداد برنامج تشغيل الطابعة باستخدام اتصال العميل/الخادم

عين الطابعة على تمكين الطابعة من جهاز الكمبيوتر الذي تم تعيينه سابقاً كخادم طباعة، ومشاركة الطابعة.

ثبّت برنامج تشغيل الطابعة لكلا الخادمين والعميل على خادم الطابعة.

## إعدادات الوظيفة

إذا تم استخدام برنامج التثبيت، فسيتم إجراء إعداد شبكة الطابعة أو الكمبيوتر، وتثبيت برنامج التشغيل، وضبط قائمة انتظار الطابعة تلقائياً.

## إعداد منافذ TCP/IP القياسية — Windows

قم بإعداد منفذ TCP/IP القياسي على خادم الطابعة، وقم بإنشاء قائمة انتظار الطابعة للطابعة على الشبكة.

1. افتح شاشة الأجهزة والطابعات.

Windows 10/Windows Server 2016

انقر بزر الماوس الأيمن فوق زر البدء أو اضغط عليه مع الاستمرار ثم حدد لوحة التحكم < الأجهزة والطابعات.

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

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

Windows 7/Windows Server 2008 R2

اضغط بدأ < لوحة التحكم < الجهاز والصوت (أو الجهاز) < أجهزة وطابعات.

Windows Vista/Windows Server 2008

اضغط بدأ < لوحة التحكم < الجهاز والصوت < طابعات.

Windows XP/Windows Server 2003 R2/Windows Server 2003

اضغط ابدأ < لوحة التحكم < طابعات وأجهزة أخرى < طابعات وفاكسات.

2. إضافة طابعة.

Windows 10/Windows 8.1/Windows 8/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012

انقر فوق إضافة طابعة، ثم حدد الطابعة التي أرغب في الاتصال بها غير مدرجة.

Windows 7/Windows Server 2008 R2

اضغط على إضافة طابعة.

Windows Vista/Windows Server 2008

اضغط على تثبيت طابعة.

Windows XP/Windows Server 2003 R2/Windows Server 2003

اضغط على تثبيت طابعة، ثم اضغط على التالي.

3. إضافة طابعة محلية.

Windows 10/Windows 8.1/Windows 8/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012

حدد إضافة طابعة محلية أو شبكة طابعة بإعدادات يدوية، ثم اضغط على التالي.

Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008

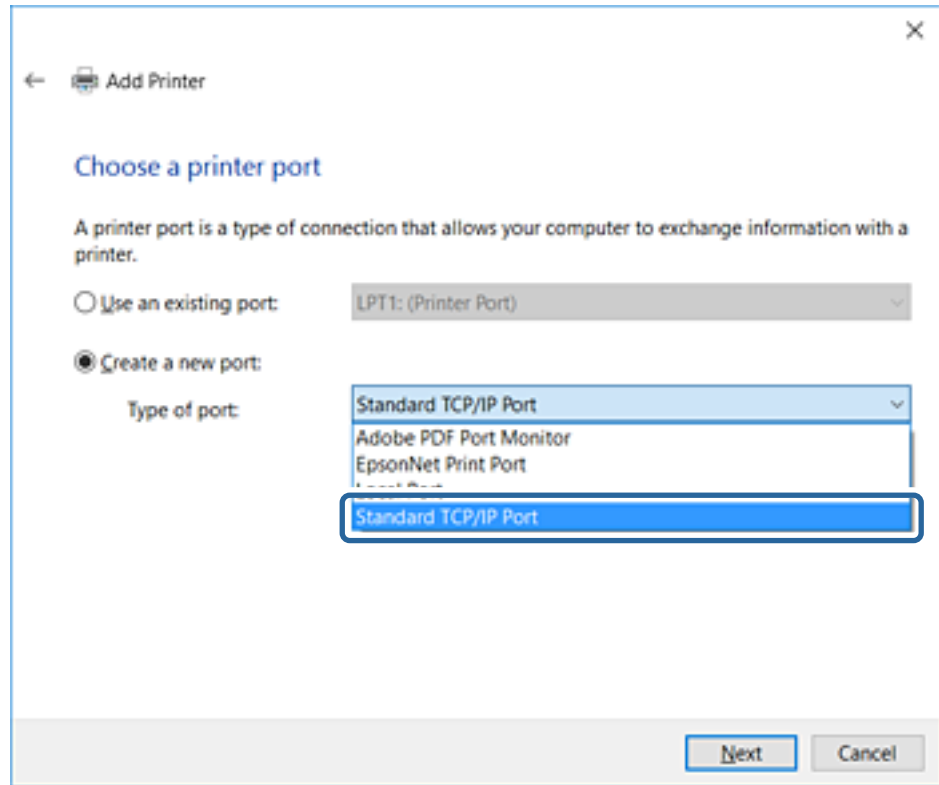
اضغط على إضافة طابعة محلية.

Windows XP/Windows Server 2003 R2/Windows Server 2003

حدد الطابعة المحلية المملوكة بهذا الحاسوب، ثم اضغط على التالي.

## إعدادات الوظيفة

4. حدد إنشاء منفذ جديد، حدد منفذ TCP/IP قياسي كنوع المنفذ، ثم اضغط على التالي.  
بالنسبة لنظام Windows XP/Windows Server 2003 R2/Windows Server 2003، انقر فوق التالي على شاشة إضافة معالج منفذ طابعة TCP/IP قياسي.



5. أدخل عنوان IP الخاص بالطابعة أو اسمها في اسم المضيف أو عنوان IP أو اسم الطابعة أو عنوان IP، ثم اضغط على التالي.  
لا تقوم بتغيير اسم المنفذ.  
انقر فوق متابعة عندما يتم عرض شاشة التحكم في حساب المستخدم.

## إعدادات الوظيفة

بالنسبة لنظام Windows XP/Windows Server 2003 R2/Windows Server 2003، انقر فوق تم على شاشة منفذ طابعة TCP/IP قياسي.

## ملاحظة:

إذا قمت بتحديد اسم الطابعة على الشبكة التي يتوفر عليها تحليل الاسم، يتم تتبع عنوان IP حتى إذا كان عنوان IP الطابعة تم تغييره 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 المصنع 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.

بالنسبة لنظام Windows XP/Windows Server 2003 R2/Windows Server 2003، يتم إكمال الإعداد. بالنسبة لنظام Windows Vista/Windows Server 2008 وأحدث، تحقق من تكوين المنفذ.

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

## معلومات ذات صلة

← "مشاركة الطابعة (فقط Windows)" في الصفحة 41



## إعدادات الوظيفة

**تحقق من تكوين منفذ — Windows**

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

1. افتح شاشة الأجهزة والطابعات.

Windows 10/Windows Server 2016

انقر بزر الماوس الأيمن فوق زر البدء أو اضغط عليه مع الاستمرار ثم حدد لوحة التحكم > الأجهزة والطابعات.

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

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

Windows 7/Windows Server 2008 R2

اضغط بدأ > لوحة التحكم > الجهاز والصوت (أو الجهاز) > أجهزة وطابعات.

Windows Vista/Windows Server 2008

اضغط بدأ > لوحة التحكم > الجهاز والصوت > طابعات.

2. افتح شاشة خصائص الطباعة.

Windows 10/Windows 8.1/Windows 8/Windows 7/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012/Windows Server 2008 R2

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

Windows Vista

انقر بزر الماوس الأيمن على رمز الطباعة، ثم حدد تشغيل كمسئول > الخصائص.

Windows Server 2008

انقر بزر الماوس الأيمن على رمز الطباعة، ثم اضغط الخصائص.

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 الطباعة (فقط Windows)**

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

1. حدد لوحة التحكم > عرض الأجهزة والطابعات على خادم الطباعة.

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

3. حدد مشاركة هذه الطباعة ثم أدخل مشاركة الاسم.

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

## إعدادات الوظيفة

## تثبيت برامج تشغيل إضافية (Windows فقط)

إذا كانت إصدارات Windows لأحد الخوادم والعملاء مختلفة، فمن المستحسن تثبيت برامج تشغيل إضافية لخدّام الطباعة.

1. حدد لوحة التحكم < عرض الأجهزة والطابعات على خادم الطباعة.
2. انقر بزر الماوس الأيمن فوق رمز الطباعة الذي تريد مشاركته مع الأجهزة التابعة، ثم انقر فوق خصائص الطباعة < مشاركة.
3. انقر فوق برامج تشغيل إضافية.
- في Windows Server 2012، انقر فوق Change Sharing Options ثم قم بتكوين الإعدادات.
4. حدد إصدارات نظام التشغيل Windows للأجهزة التابعة، ثم انقر فوق موافق.
5. حدد ملف معلومات برنامج تشغيل الطباعة (inf.\*) ثم ثبت برنامج التشغيل.

## معلومات ذات صلة

← "استخدام طباعة مشتركة - Windows" في الصفحة 42

## استخدام طباعة مشتركة - Windows

يجب أن يُبلغ المسؤول العملاء باسم جهاز الكمبيوتر المخصص لخدّام الطباعة وكيفية إضافته إلى هذه الأجهزة. في حالة عدم تكوين برنامج (برامج) تشغيل إضافي بعد، أخبر العملاء بكيفية استخدام الأجهزة والطابعات لإضافة الطباعة المشتركة. في حالة وجود برنامج (برامج) تشغيل إضافي مكون بالفعل على خادم الطباعة، اتبع هذه الخطوات:

1. حدد الاسم المعين لخدّام الطباعة في مستكشف Windows.
2. انقر نقرًا مزدوجًا فوق الطباعة التي تريد استخدامها.

## معلومات ذات صلة

← "مشاركة الطباعة (Windows فقط)" في الصفحة 41

← "تثبيت برامج تشغيل إضافية (Windows فقط)" في الصفحة 42

## إعدادات برنامج تشغيل الطباعة لاتصال النظير إلى النظير

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

## معلومات ذات صلة

← "إعداد برنامج تشغيل الطباعة - Windows" في الصفحة 42

← "إعداد برنامج تشغيل الطباعة - Mac OS" في الصفحة 43

## إعداد برنامج تشغيل الطباعة - Windows

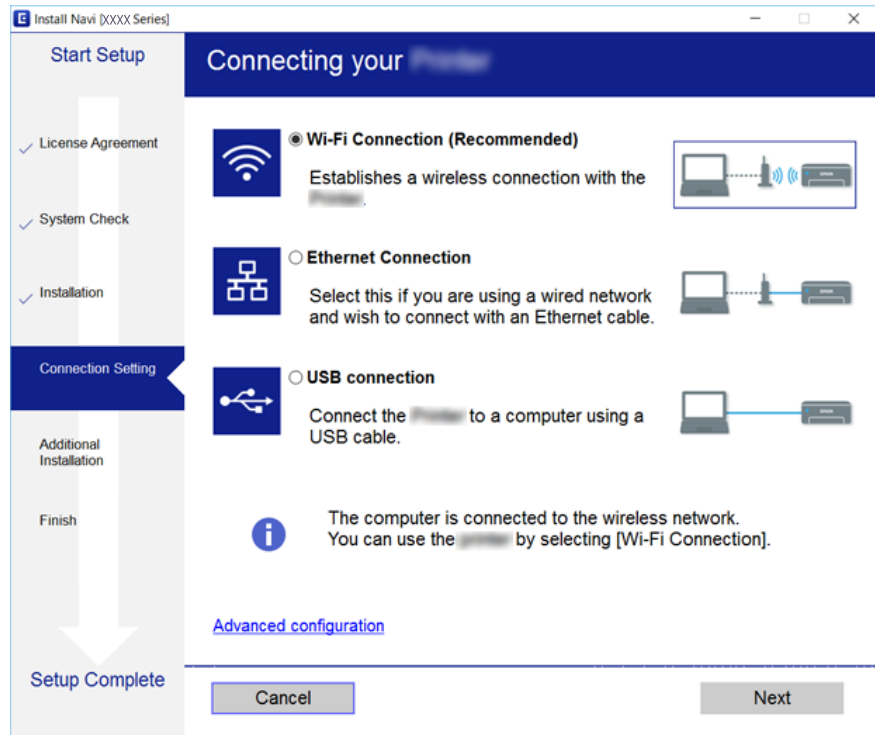
بالنسبة للمؤسسات الصغيرة، نحن نوصي بتثبيت برنامج تشغيل الطباعة على كل كمبيوتر عميل. استخدم برنامج التثبيت على موقع Epson على الويب أو على قرص البرامج.

## ملاحظة:

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

## إعدادات الوظيفة

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 حدد تثبيت البرنامج فحدد تغيير طريقة الاتصال أو إعادة تعيينها ثم انقر فوق التالي.
3. اتبع التعليمات المعروضة على الشاشة.

معلومات ذات صلة

← "EpsonNet SetupManager" في الصفحة 102

## إعداد برنامج تشغيل الطابعة — Mac OS

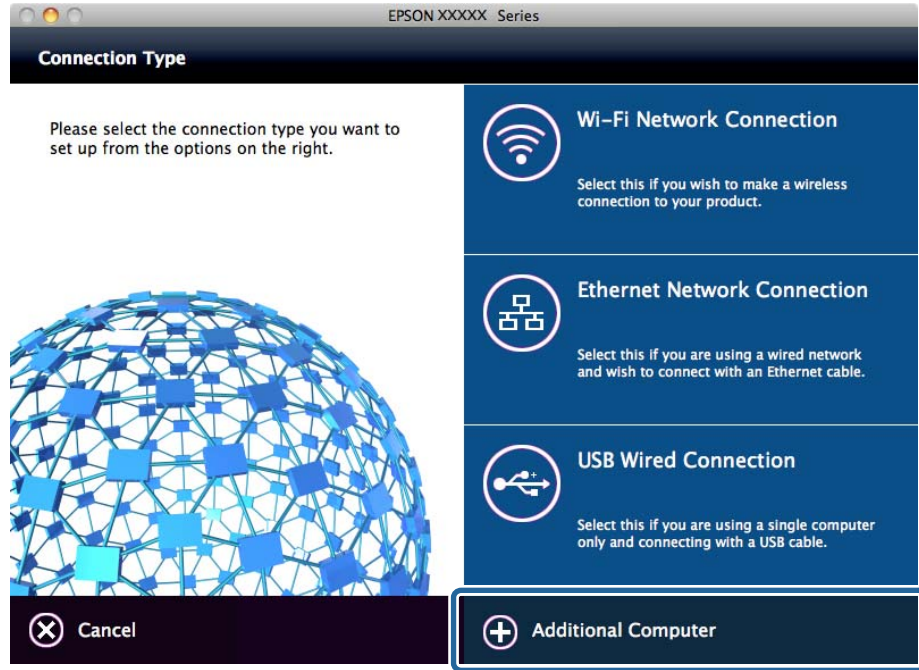
قم بتنزيل البرنامج من الموقع الإلكتروني ثم قم بإجراء إعدادات الاتصال لإضافة حاسوب. قم ببدء الإعداد ضمن البيئة المتوفرة للإنترنت. عندما ترغب في تثبيت برنامج تشغيل الطابعة PostScript من Epson لطابعة تدعم PostScript، راجع دليل المستخدم للطابعة.

1. قم بزيارة موقع الويب التالي من الكمبيوتر الذي ترغب في ضبط إعداداته، ثم أدخل اسم المنتج.  
<http://epson.sn>
2. برجاء الذهاب إلى الإعداد، ثم قم بتنزيل البرنامج.

## إعدادات الوظيفة

3. قم بتشغيل البرنامج، ثم اتبع التعليمات المعروضة على الشاشة.

4. حدد كمبيوتر إضافي على شاشة نوع الاتصال.



5. اتبع التعليمات المعروضة على الشاشة.

## استخدام وظائف المسح الضوئي

يمكنك استخدام وظائف المسح الضوئي من الكمبيوتر أو عن طريق استخدام لوحة تحكم الطابعة.

### المسح الضوئي من جهاز كمبيوتر

تُثبت البرنامج وتحقق من تمكين خدمة مسح الشبكة لإجراء المسح الضوئي عبر الشبكة من الكمبيوتر.

معلومات ذات صلة

← "تثبيت البرنامج" في الصفحة 44

← "التأكد من تمكين المسح الضوئي عبر الشبكة" في الصفحة 45

### تثبيت البرنامج

Epson Scan 2 

يُعد ذلك برنامج تشغيل مساحة ضوئية. إذا كنت تستخدم الجهاز من جهاز كمبيوتر، فثُبت برنامج التشغيل على كل كمبيوتر عميل. إذا تم تثبيت Document Capture / Document Capture Pro، يمكنك إجراء العمليات التي تم تعيينها لأزرار الجهاز.

إذا تم استخدام EpsonNet Setup Manager فسيتم توزيع برنامج تشغيل الطابعة أيضاً كحزمة.

## إعدادات الوظيفة

(Windows)/Document Capture (Mac OS Document Capture Pro) □

يتم تثبيته على كمبيوتر عميل. يمكن طلب المهام المسجلة على كمبيوتر الشبكة حيث تم تثبيت Document Capture Pro /Document Capture وت تشغيلها من لوحة تحكم الجهاز. يمكنك إجراء المسح الضوئي عبر الشبكة من الكمبيوتر. يلزم توفير Epson Scan 2 لإجراء المسح الضوئي.

معلومات ذات صلة

← "EpsonNet SetupManager" في الصفحة 102

## التأكد من تمكين المسح الضوئي عبر الشبكة

يمكنك تعيين خدمة مسح الشبكة عندما تقوم بإجراء المسح الضوئي من كمبيوتر عميل على الشبكة. تم تمكين الإعداد الافتراضي.

1. ادخل إلى تهيئة الويب وحدد علامة التبويب **Scan/Copy < Network Scan**.

2. تأكد من تحديد **Enable scanning** لـ **EPSON Scan**.

إذا تم تحديده، تُستكمل المهام. أغلق **Web Config**.

إذا تمت إزالة تحديده، فحدده وانتقل إلى الخطوة التالية.

3. انقر فوق **Next**.

4. انقر فوق **OK**.

إذا تمت إعادة توصيل الشبكة، فسيتم تمكين الإعدادات.

معلومات ذات صلة

← "الوصول إلى تطبيق **Web Config**" في الصفحة 37

## المسح الضوئي باستخدام لوحة التحكم

يتم إجراء وظيفة المسح الضوئي إلى المجلد ووظيفة المسح الضوئي إلى البريد الإلكتروني باستخدام لوحة التحكم بالطابعة، بالإضافة إلى إرسال نتائج المسح الضوئي إلى البريد الإلكتروني، والمجلدات وما إلى ذلك عن طريق تنفيذ إحدى المهام من الكمبيوتر.

معلومات ذات صلة

← "إعدادات الخوادم والمجلدات" في الصفحة 45

## إعدادات الخوادم والمجلدات

الاسم	الإعدادات	الموقع	المتطلبات
المسح الضوئي إلى مجلد الشبكة (SMB)	إنشاء مجلد الحفظ وإعداد مشاركته	كمبيوتر يحتوي على مكان لمجلد الحفظ	حساب مستخدم إداري للكمبيوتر الذي ينشئ مجلدات حفظ.
وجهة المسح الضوئي إلى مجلد الشبكة (SMB)	وجهة المسح الضوئي إلى مجلد الشبكة (SMB)	جهات الاتصال للجهاز	اسم مستخدم وكلمة مرور لتسجيل الدخول للكمبيوتر الذي يحتوي على مجلد حفظ، وميزة تحديته.

## إعدادات الوظيفة

الاسم	الإعدادات	الموقع	المتطلبات
المسح الضوئي إلى مجلد الشبكة (FTP)	إعداد تسجيل الدخول لخدم FTP	جهات الاتصال للجهاز	معلومات تسجيل الدخول لخدم FTP وميزة تحديث مجلد الحفظ.
المسح الضوئي إلى البريد الإلكتروني	الإعداد الخاص بخدم البريد الإلكتروني	الجهاز	معلومات إعداد خادم البريد الإلكتروني
المسح الضوئي إلى الخدمة السحابية	تسجيل الطابعة في Epson Connect	الجهاز	بيئة الاتصال بالإنترنت
	تسجيل جهة اتصال في Epson Connect	خدمة Epson Connect	تسجيل المستخدم والطابعة في خدمة Epson Connect
المسح الضوئي إلى Document Capture Pro (عند استخدام Document Capture Pro /Document CaptureServer (Pro)	إعداد الخادم لـ Document Capture Pro	الجهاز	عنوان IP، أو اسم المضيف، أو FQDN للكمبيوتر المثبت عليه Document Capture Pro /Document CaptureServer Pro

## معلومات ذات صلة

← "تكوين خادم البريد" في الصفحة 31

← "إدارة المسح الضوئي من لوحة التحكم (Document Capture Pro Server) /" في الصفحة 46 (Document Capture Pro)

## إدارة المسح الضوئي من لوحة التحكم (Document Capture Pro Server) / (Capture Pro)

باستخدام Document Capture Pro Server /Document Capture Pro (وضع الخادم)، يمكنك إدارة طريقة الفرز، وتنسيق الحفظ، ووجهة إعادة توجيهه الخاصة بنتيجة المسح الضوئي الذي يتم تنفيذه من لوحة تحكم الطابعة. يمكنك طلب مهمة مسجلة على الخادم بشكل مسبق وتنفيذها من لوحة تحكم الطابعة.

ثبته على كمبيوتر الخادم.

للحصول على مزيد من المعلومات حول Document Capture Pro Server، اتصل بمكتب Epson المحلي.

## معلومات ذات صلة

← "إعداد Document Capture Pro Server" في الصفحة 46 (Document Capture Pro (وضع الخادم)

### إعداد Document Capture Pro Server / (وضع الخادم)

لاستخدام Document Capture Pro Server، قم بالإعداد على النحو التالي.

1. ادخل إلى Web Config وحدد علامة التبويب Document Capture Pro < Scan/Copy.
  2. حدد Server Mode لـ Mode.
  3. أدخل عنوان الخادم باستخدام Document Capture Pro Server المثبت عليه لـ Server Address. أدخل عدداً من الأحرف يتراوح ما بين 2 إلى 255 حرفاً بتنسيق IPv4، أو IPv6، أو اسم المضيف، أو FQDN. لتنسيق FQDN، يمكنك استخدام أحرف أبجدية رقمية بتنسيق (ASCII (0x20-0x7E)، و"، و-، و" فيما عدا في بداية العنوان ونهايته.
  4. انقر فوق OK.
- إذا تمت إعادة توصيل الشبكة، فسيتم تمكين الإعدادات.

## إعدادات الوظيفة

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## استخدام وظائف الفاكس

مكّن استخدام وظائف الفاكس في الطابعة.

## إعداد Receive Mode

حسب موقفك، قم بإعداد Receive Mode.

1. ادخل إلى Web Config وحدد علامة التبويب **Fax** < **Receive Settings** < **Basic**.2. حدد طريقة الاستلام في **Receive Mode**. **Auto**: يوصى به لمستخدمي الفاكس بكثرة. تستقبل الطابعة الفاكس بشكل تلقائي بعد عدد الرنات الذي قمت بتحديدده. **Manual**: يوصى به للمستخدمين الذين لا يستخدمون الفاكس بكثرة، أو الذين يرغبون في استلام الفاكس بعد الرد على المكالمات من خلال الهاتف المتصل. عند استلام فاكس، التقط السماعة، ثم قم بتشغيل الطابعة.

هام!

إذا لم تقم بتوصيل هاتف بالطابعة، حدد الوضع **Auto**.

ملاحظة:

في حالة تمكين وظيفة **Remote Receive** يمكنك البدء في استلام الفاكس فقط من خلال استخدام الهاتف المتصل.3. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "ضبط إعدادات الفاكس الأساسية باستخدام معالج إعداد الفاكس" في الصفحة 29

← "استلام الفاكسات باستخدام هاتف متصل (Remote Receive)" في الصفحة 48

## الإعدادات الخاصة بجهاز الرد الآلي

يجب ضبط الإعدادات التالية لاستخدام جهاز الرد الآلي.

1. ادخل إلى Web Config وحدد علامة التبويب **Fax** < **Receive Settings** < **Basic**.2. حدد **Auto** لـ **Receive Mode**.3. اضبط إعداد **F/T Ring Times** بالطابعة على عدد أكبر من عدد الرنات الخاصة بجهاز الرد الآلي.إذا تم تعيين إعداد **F/T Ring Times** للطابعة على عدد أقل من عدد نغمات جهاز الرد الآلي، فلن يتمكن جهاز الرد الآلي من استقبال المكالمات الصوتية لتسجيل رسائل صوتية. راجع الأدلة المرفقة مع جهاز الرد الآلي لمعرفة الإعدادات. لا يتم عرض هذا العنصر باستثناء الجهاز الذي يدعم جهاز الرد الآلي.4. انقر فوق **OK**.

## إعدادات الوظيفة

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## استلام الفاكسات باستخدام هاتف متصل (Remote Receive)

باستخدام وظيفة **Remote Receive** يمكنك البدء في استلام الفاكسات من خلال استخدام الهاتف فقط. تتوفر وظيفة **Remote Receive** للهواتف التي تدعم الاتصال بالرنين.

1. ادخل إلى Web Config وحدد علامة التبويب **Fax < Receive Settings < Basic**.2. حدد **Remote Receive** لـ **On**.3. أدخل رمزاً مكوناً من رقمين (يمكن إدخال 0 إلى 9، \*، و #) في خانة **Start Code**. يُعد **Start Code** رمزاً يتم إدخاله في هاتف متصل لبدء استلام الفاكسات.4. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## التعامل مع الفاكسات المستلمة

يمكنك التعامل مع الفاكس المستلم على النحو التالي.

Print Save to Inbox Save to Computer Save to Memory Device Forward 

ملاحظة:

إذا قمت بتحديد جميع الميزات أعلاه، فسيتم حفظ المستندات المستلمة وإرسالها إلى كل وجهة ويمكنك استلام بريد إعلام عند انتهاء العملية. لا يمكنك تحديد **Print** و **Save to Inbox** فقط.

معلومات ذات صلة

← "إعداد إعلام البريد الإلكتروني بعد استلام فاكس" في الصفحة 48

← "ضبط إعدادات الطباعة بالنسبة للفاكسات المستلمة" في الصفحة 49

← "الضبط على حفظ الفاكسات المستلمة في صندوق الوارد" في الصفحة 49

← "إعداد استلام PC-FAX" في الصفحة 50

← "حفظ إعدادات الذاكرة الخارجية" في الصفحة 50

← "إعدادات إعادة التوجيه الخاصة بالفاكسات" في الصفحة 51

## إعداد إعلام البريد الإلكتروني بعد استلام فاكس

عند انتهاء عملية استلام فاكس، يمكن إرسال إعلام بريد إلكتروني.



## إعدادات الوظيفة

يجب تسجيل عنوان الإعلام في جهات الاتصال مقدماً.  
يجب تكوين خادم البريد الإلكتروني لاستخدام هذه الميزة.

1. ادخل إلى Web Config وحدد علامة التبويب **Fax** < **Receive Settings** < **Fax Output**.
2. حدد العناصر التي ترغب في أن يتم إبلاغك بها بالبريد الإلكتروني عندما ينتهي اتصال الفاكس لـ **Email Notifications**.
3. انقر فوق **Select from Contacts** لـ **Recipient**.
4. حدد عنوان الإعلام.
5. انقر فوق **Select** لتعيين الوجهة.
6. انقر فوق **OK**.

معلومات ذات صلة

- ← "الوصول إلى تطبيق Web Config" في الصفحة 37
- ← "تكوين خادم البريد" في الصفحة 31

## ضبط إعدادات الطباعة بالنسبة للفاكسات المستلمة

1. ادخل إلى Web Config وحدد علامة التبويب **Fax** < **Receive Settings** < **Fax Output**.
2. حدد **Printing**.
3. قم بضبط إعدادات **Print Settings** حسب الضرورة.
4. انقر فوق **OK**.

معلومات ذات صلة

- ← "الوصول إلى تطبيق Web Config" في الصفحة 37

## الضبط على حفظ الفاكسات المستلمة في صندوق الوارد

1. ادخل إلى Web Config وحدد علامة التبويب **Fax** < **Receive Settings** < **Fax Output**.
2. حدد **Save to Inbox**.
3. انقر فوق **OK**.
4. حدد **Inbox** < **Receive Settings**.  
عند تعيين كلمة مرور الصندوق، أدخل كلمة المرور لفتح شاشة الإعداد.
5. حدّد هذا الخيار لاستخدامه عند امتلاء صندوق الوارد.  
 **Reject incoming faxes**: لا تُجيب الطابعة مكالمات الفاكس الواردة.
- Receive and print faxes**: تقوم الطابعة بطباعة جميع المستندات المستلمة التي لا يمكن حفظها في صندوق الوارد.
6. عند حماية الإعدادات بكلمة مرور، حدد **Change Password**، ثم قم بإعداد كلمة مرور الصندوق.

## إعدادات الوظيفة

7. انقر فوق OK.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## إعدادات استلام PC-FAX

لاستخدام ميزة استلام PC-FAX، تُثبَّت برنامج تشغيل الطابعة و FAX Utility على الكمبيوتر. عند استخدام برنامج التثبيت لإعداد الطابعة، يتم تثبيتها في الوقت نفسه. في حالة قيامك بتثبيتها بشكل منفرد، استخدم قرص البرامج أو قم بتنزيلها من موقع Epson على الويب. قم بتحويل الفاكس المستلم إلى ملف PDF، واحفظه في الكمبيوتر المتصل. يمكن طباعته في الوقت نفسه.

هام!

 اضبط وضع استلام الطابعة على تلقاء.

 قبل حفظ الفاكسات على الكمبيوتر، يتم حفظها على ذاكرة الطابعة. اترك الكمبيوتر الوجهة قيد التشغيل لأن ذاكرة الطابعة تكون محدودة، وقد لا تتوفر عملية الإرسال والاستلام. يتم عرض كمية البيانات المحفوظة بشكل مؤقت على رمز وضع الفاكس.

1. شغل FAX Utility على جهاز الكمبيوتر المتصل بالطابعة.

2. افتح شاشة إعدادات FAX Utility .

Windows 

حدد إعدادات الفاكس للطابعة &lt; إعدادات الإخراج للفاكسات المستلمة.

Mac OS 

انقر فوق مراقب استلام الفاكس، وحدد طابعتك، ثم انقر فوق إعدادات الاستلام.

3. انقر فوق حفظ الفاكسات على هذا الكمبيوتر وحدد مجلد الوجهة للحفظ.

4. قم بضبط الإعدادات الأخرى حسب الضرورة، ثم أرسل الإعدادات إلى الطابعة.

ملاحظة:

للحصول على مزيد من التوضيح حول عناصر الإعداد والإجراء التفصيلي، راجع تعليمات FAX Utility.

5. اضغط على الإعدادات في لوحة تحكم الطابعة.

6. اضغط على إعدادات عامة &lt; إعدادات الفاكس &lt; إعدادات الاستلام.

7. اضغط على إعدادات الحفظ/إعادة التوجيه &lt; الحفظ/إعادة التوجيه غير المشروط.

8. يتم عرض الإعدادات الحالية. تأكد من تعيين الإعدادات لحفظ الكمبيوتر (حفظ إلى الكمبيوتر).

9. عندما ترغب في حفظ البيانات بالكمبيوتر والطباعة تلقائياً في الوقت نفسه، اضغط على حفظ إلى الكمبيوتر &lt; نعم وطباعة.

ملاحظة:

لإنهاء حفظ البيانات في الكمبيوتر، حدد لا لحفظ إلى الكمبيوتر على لوحة تحكم الطابعة. على Web Config حدد علامة التبويب Fax &lt; Fax Output &lt; Receive Settings، وألغ تحديد Save to Computer، ثم انقر فوق OK.

## حفظ إعدادات الذاكرة الخارجية

1. ادخل إلى Web Config وحدد علامة التبويب Fax Output &lt; Receive Settings &lt; Fax.

## إعدادات الوظيفة

2. حدد **Save to Memory Device**.

3. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## إعدادات إعادة التوجيه الخاصة بالفاكسات

يجب أن تكون وجهة إعادة التوجيه مسجلة بشكل مسبق في جهات الاتصال.

1. ادخل إلى Web Config وحدد علامة التبويب **Fax** < **Receive Settings** < **Fax Output**.

2. حدد **Forward**.

3. انقر فوق **Select from Contacts** على **Where to Forward**.

4. حدد وجهة إعادة التوجيه.

يمكنك تعيين ما يصل إلى خمس جهات.

5. انقر فوق **Select**.

6. قم بإعداد طريقة المعالجة عند فشل إعادة التوجيه لـ **Options When Forwarding Failed**.

7. أدخل عنواناً لرسائل البريد الإلكتروني التي تم إرفاق فاكسات بها على **Email Subject to Forward**.

أدخل 50 حرفاً أو أقل بتنسيق ASCII (0x20-0x7E)، إذا لم تحدد ذلك، فاتركه فارغاً.

8. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## وصف قائمة إعدادات الفاكس

يمكنك تكوين الإعدادات التفصيلية لوظيفة الفاكس في علامة التبويب **Fax** باستخدام Web Config.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## Send Settings

Basic

العنصر	الوصف
PC to FAX Function	يمكنك تحديد سواء إرسال الفاكس المستخدم من الكمبيوتر أم لا.

## إعدادات الوظيفة

العنصر	الوصف
Auto Rotation	إذا تم تعيين مستند على الاتجاه العمودي على ورق بحجم A4 في وحدة التغذية التلقائية للمستندات أو زجاج الماسحة الضوئية، فسيتم إرساله كمستند بحجم A3 عادة. إذا قمت بتمكين الإعداد، فسيتم تدوير المستند وإرساله بحجم A4.
Batch Send	يمكن إرسال عدة مستندات ذات الوجهة نفسها تلقائيًا. يمكنك إرسال ما يصل إلى خمسة مستندات (إجمالي 100 صفحة). يقلل ذلك من عدد عمليات الإرسال مما يؤدي إلى توفير تكاليف الإرسال.
Quick memory send	بعد قراءة الصفحة الأولى من المستند، تبدأ عملية إرسال الفاكس. عادة ما يتم حفظ المستند الممسوح ضوئيًا أولاً، ثم يتم إرساله. ومع ذلك، يتم إجراء الإرسال السريع للذاكرة بالتوازي مع إرسال المسح الضوئي والفاكس، لذلك يمكنك تقليل وقت التشغيل الإجمالي.
Save Failure Data	يتم حفظ المستند الذي فشلت عملية إرساله في الذاكرة.
Auto Redial Count	حدد عدد مرات إعادة الاتصال عند إجراء محادثات هاتفية أو عند حدوث خطأ.
Auto Redial Interval	حدد وقت الاتصال التالي.
Fax Header	إعدادات ترويسة الفاكس ورقم الهاتف. يعرض محتوى الإعداد هنا ترويسة إرسال المستند. يمكن أن تتكون ترويسة الفاكس مما يصل إلى 40 حرفًا بتنسيق Unicode (UTF-8). إذا لم تحدد ذلك، فاتركه فارغًا.
Others	يمكنك إضافة ترويسة فاكس ليتم عرضها في ترويسة المستند المرسل. يمكن تحديد ترويسة الفاكس التي تم إدخالها هنا عند إرسال الفاكس. يمكنك إدخال ما يصل إلى 40 حرفًا بتنسيق Unicode (UTF-8) وتسجيل ما يصل إلى 20 وجهة.
Your Phone Number	إعدادات رقم الهاتف. يعرض محتوى الإعداد هنا ترويسة إرسال المستند. أدخل ما يصل إلى 30 حرفًا أو أقل باستخدام 0-9، أو +، أو مسافة. إذا لم تحدد ذلك، فاتركه فارغًا.

## Send Stored Document Box

حدد القائمة للتبديل إلى شاشة التحرير الخاصة بصندوق الإرسال. عند تعيين كلمة مرور لصندوق الإرسال، وعدم تكوين كلمة مرور المسؤول، انتقل إلى شاشة إدخال كلمة المرور. عند تعيين كلمة مرور المستخدم، انتقل إلى شاشة التحرير بغض النظر عن إعداد كلمة المرور لصندوق الإرسال.

العنصر	الوصف
Change Password	حدد سواء تغيير كلمة مرور الصندوق أم لا.
Box Password	عين كلمة مرور للصندوق. أدخل ما يصل إلى 20 حرفًا أو أقل بتنسيق ASCII (0x20-0x7E). إذا لم تحدد ذلك، فاتركه فارغًا.
Confirm Password	أدخل كلمة المرور للتأكيد.

## Polling Send Box

العنصر	الوصف
Change Password	حدد سواء تغيير كلمة مرور الصندوق أم لا.
Box Password	عين كلمة مرور للصندوق. أدخل ما يصل إلى 20 حرفًا أو أقل بتنسيق ASCII (0x20-0x7E). إذا لم تحدد ذلك، فاتركه فارغًا.
Confirm Password	أدخل كلمة المرور للتأكيد.
Auto Delete After Polling Send	حدد سواء حذف المستند المرسل بعد الإرسال حسب الطلب أم لا.
Notify Send Result	حدد سواء إرسال إشارات البريد الإلكتروني بعد الإرسال حسب الطلب أم لا.
Recipient	قم بإعداد وجهة لإعلامات البريد الإلكتروني.

## Board Box (الشاشة العلوية)

## إعدادات الوظيفة

العنصر	الوصف
Number	رقم فهرس الصندوق.
Name	اسم الصندوق.
Edit	حدد الصندوق وانقر فوق <b>Edit</b> للانتقال إلى شاشة التحرير. عند تعيين كلمة مرور لصندوق الإرسال، وعدم تكوين كلمة مرور المسؤول، انتقل إلى شاشة إدخال كلمة المرور. عند تعيين كلمة مرور المستخدم، انتقل إلى شاشة التحرير بغض النظر عن إعداد كلمة المرور لصندوق الإرسال.

## Board Box (شاشة التحرير)

العنصر	الوصف
Number	رقم فهرس الصندوق.
Name	أدخل اسم الصندوق. أدخل ما يصل إلى 30 حرفاً أو أقل بتنسيق Unicode (UTF-8) دون أحرف التحكم. إذا لم تحدد ذلك، فاتركه فارغاً. يتم حساب الحرف مزدوج البايت والأحرف ذات البايت الواحد كحرف واحد.
Change Password	حدد سواء تغيير كلمة مرور الصندوق أم لا.
Box Password	عين كلمة مرور للصندوق. أدخل ما يصل إلى 20 حرفاً أو أقل بتنسيق ASCII (0x20-0x7E). إذا لم تحدد ذلك، فاتركه فارغاً.
Confirm Password	أدخل كلمة المرور للتأكيد.
Subaddress(SEP)	عين العنوان الفرعي للمربع. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، أو *، أو #، أو المسافات. إذا لم تحدد ذلك، فاتركه فارغاً.
Password(PWD)	عين كلمة المرور الخاصة بالعنوان الفرعي. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، أو *، أو #، أو المسافات. إذا لم تحدد ذلك، فاتركه فارغاً.
Auto Delete After Polling Send	حدد سواء حذف المستند المرسل بعد الإرسال حسب الطلب أم لا.
Notify Send Result	حدد سواء إرسال إشارات البريد الإلكتروني بعد الإرسال حسب الطلب أم لا.
Recipient	قم بإعداد وجهة لإعلامات البريد الإلكتروني.

## Receive Settings

## Basic

العنصر	الوصف
Receive Mode	حدد وضع الاستلام. يختلف عنصر الإعداد حسب منطقة الاستخدام أو دولته.
DRD	إذا كنت مشتركاً في خدمة DRD التي تدعمها شركة الهاتف الذي تفتنيه، يمكنك تحديد نمط مشغل النغمات لاستلام الفاكس. تُعد DRD (خدمة الرنين المميزة) خدمة يتمكن من استخدامها العديد من أرقام الهاتف مع خط هاتف، وتوفر العديد من شركات الهاتف هذه الخدمة. (يختلف اسم الخدمة حسب الشركة). يتم تقديم نمط رنين لكل رقم هاتف. يمكنك استخدام نمط واحد للمكالمات الصوتية ونمط آخر لمكالمات الفاكس. يتم عرض <b>On</b> و <b>Off</b> بصفته إعدادات لخدمة الرنين المميزة حسب منطقتك.
Rings to Answer	حدد عدد النغمات لاستلام الفاكس بعد رنين الهاتف. يختلف عنصر الإعداد حسب منطقة الاستخدام أو دولته.
Remote Receive	عند الرد على مكالمة تحتوي على فاكس باستخدام هاتف خارجي، أدخل رمز البدء لبدء استلام الفاكس باستخدام الهاتف. قم بتعيين ما إذا كان يتم استخدام الاستلام عن بُعد أم لا.
Start Code	عين رمز البدء الخاص بـ <b>Remote Receive</b> . أدخل حرفين باستخدام 0-9، و *، و #.

## إعدادات الوظيفة

العنصر	الوصف
Receiving Paper Size	حدد حجم الورق لاستلام الفاكس.

## Fax Output

العنصر	الوصف
Fax Output	عين طريقة معالجة المستندات المستلمة. عند تحديد عدة طرق، يتم حفظ المستند نفسه في كل وجهة، ويتم نقله أيضاً إلى الوجهة. يتعدّر تحديد <b>Print</b> و <b>Save to Inbox</b> فقط.
Printing	طباعة المستندات المستلمة.
Save to Inbox	يمكنك تخزين 100 مستند مستلم كحد أقصى في صندوق الوارد الخاص بالطابعة. عند تعيين ذلك، لا تتم طباعة المستندات المستلمة تلقائياً. يمكنك فحص لوحة تحكم الطابعة، ثم طباعة المستندات الضرورية فقط.
Save to Computer	قم بتحويل المستندات المستلمة إلى التنسيق PDF وحفظها على الكمبيوتر المتصل بالطابعة. تتوفر ميزة الحفظ والطباعة في الوقت نفسه. يمكنك البدء في ذلك باستخدام FAX Utility. قم بتثبيت FAX Utility على جهاز الكمبيوتر مقدماً.
Save to Memory Device	قم بتحويل المستندات المستلمة إلى التنسيق PDF ثم حفظها على جهاز ذاكرة خارجي متصل بالطابعة. تتوفر ميزة الحفظ والطباعة في الوقت نفسه.
Forward	يتم نقل المستندات المستلمة إلى آلة فاكس أخرى، وتحويلها إلى تنسيق PDF، ثم تُنقل إلى المجلد أو عنوان البريد الإلكتروني الموجود في الشبكة. سيتم حذف المستندات التي تم نقلها. يجب عليك تسجيل جهات الاتصال مقدماً. علاوة على ذلك، إذا كانت الوجهة التي حددتها عنوان بريد إلكتروني، فعليك تكوين خادم البريد الإلكتروني.
Print Settings	إعداد الطباعة لطباعة المستندات المستلمة.

## إعدادات الوظيفة

العنصر	الوصف
Auto Reduction	عندما يكون حجم المستند المستلم أكبر من حجم الورق المحمّل في الطابعة، يتم تقليصه ليناسب حجم الورق، ثم تتم طباعته. حسب المستند، قد يتعدّر تقليص حجمه. عند تعطيله، تتم طباعة عدة صفحات دون تقليل الحجم، وتكون الصفحة الثانية فارغة.
Auto Rotation	عند استلام مستندات بحجم A5، B5، وA4، وLetter ذات اتجاه أفقي، يتم تدويرها تلقائياً للطباعة بحجم الورق المناسب.
Acting Print	حدد طريقة الطباعة عندما يكون حجم المستندات المستلمة أكبر من حجم الورق الذي تم تحميله في الطابعة. عند تحديد <b>On(Split to pages)</b> يقوم بتقسيم المستند بشكل طولي. عند تحديد <b>On (Reduce to Fit)</b> يكون الحد الأدنى لنسبة التصغير 50%.
Overlap When Split	لتقسيم الطباعة، عيّن سواء تداخل المطبوعات أم لا. عند تفعيله، أدخل مقدار التداخل من 1 حتى 15.
Delete Print Data After Split	لتقسيم الطباعة، عيّن سواء حذف الحافة العلوية أو السفلية للصورة. عند تفعيله، أدخل مقدار الحذف من 1 حتى 30.
Add Reception Information	حدد سواء طباعة معلومات الاستلام في ترويسة الفاكس المستلم أم لا.
Collation Stack	الطباعة من آخر صفحة في المستند المستلم، ثم فرزها بترتيب الصفحات الصحيح. قد لا يتم تطبيق ذلك عندما تكون ذاكرة استلام المستندات منخفضة.
2-Sided	حدد سواء استخدام الطباعة على الوجهين للمستندات المستلمة أم لا.
Binding(Copy)	حدد اتجاه التجليد عند الطباعة على الوجهين.
Print Start Timing	حدد إعدادات موعد بدء طباعة المستندات المستلمة.
Print Suspend Time	احفظ هذه الفترة (في منطقة زمنية محددة) في ذاكرة المستند المستلم دون طباعته. ستتم طباعته تلقائياً عند وقت إعادة التشغيل. يمكنك استخدام ميزة منع الضوضاء في الليل فضلاً عن الحماية من تسريب المعلومات السرية أثناء عدم وجودك.
Time to Stop	عيّن وقت إيقاف طباعة المستندات المستلمة.
Time to Restart	عيّن وقت بدء طباعة المستندات المستلمة.
Quiet Mode	عيّن الوضع الصامت على تفعيل أو تعطيل.
Forward Settings	
Where to Forward	قم بتكوين إعدادات نقل المستندات المستلمة. انقر فوق <b>Select from Contacts</b> ، ثم حدد وجهة لنقل المستندات المستلمة. يمكنك تحديد ما يصل إلى 5 وجهات.
Options When Forwarding Failed	حدد هذه العملية عند فشل نقل المستند المستلم.
Email Subject to Forward	أدخل موضوع البريد الإلكتروني المكون من 50 حرفاً أو أقل بتنسيق ASCII عندما تكون وجهة النقل الخاصة بالمستندات المستلمة بريداً إلكترونياً. إذا لم تحدد ذلك، فاتركه فارغاً.
Email Notifications	عيّن سواء الإبلاغ عبر البريد الإلكتروني عند اكتمال معالجة المستند المستلم أم لا.

## إعدادات الوظيفة

العنصر	الوصف
Receive	يتم الإبلاغ عندما تسلم فاكس.
Printing	يتم الإبلاغ عندما تنتهي من طباعة فاكس مستلم.
Save to Memory Device	يتم الإبلاغ عندما تنتهي من تخزين فاكس مستلم على جهاز ذاكرة خارجي.
Forward	يتم الإبلاغ عندما تنتهي من نقل فاكس مستلم.
Recipient	عينَ وجهة للبريد الإلكتروني لإكمال العملية. انقر فوق <b>Select from Contacts</b> للتحديد من جهات الاتصال.

## Conditions Output Settings (الشاشة العلوية)

العنصر	الوصف
Number	رقم فهرس الصندوق.
Name	اسم الصندوق.
Edit	حدد الصندوق وانقر فوق <b>Edit</b> للانتقال إلى شاشة التحرير.
Delete	احذف الصندوق المحدد.

## Conditions Output Settings (شاشة التحرير)

العنصر	الوصف
Enable this Conditions Output Settings.	مكّن الصندوق السري الذي تم تعيينه.
Number	رقم فهرس الإخراج الشرطي.
Name	أدخل اسم الصندوق. أدخل ما يصل إلى 30 حرفاً أو أقل بتنسيق Unicode (UTF-8) دون أحرف التحكم وإذا لم تحدد ذلك، فاتركه فارغاً. يتم حساب الحرف مزدوج البايت والأحرف ذات البايت الواحد كحرف واحد.
Condition(s)	عينَ حالات توزيع المستندات المستلمة.
Number	عينَ رقم هاتف المرسل باعتباره حالة. حدد الحالة للمطابقة، ثم أدخل رقم الهاتف. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، أو +، أو *، أو #، أو مسافة لرقم الهاتف. إذا لم تحدد ذلك، فاتركه فارغاً.
Subaddress(SUB)	عينَ العنوان الفرعي باعتباره حالة. عند تحديد <b>Equals</b> ، أدخل العنوان الفرعي للمطابقة. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، أو *، أو #، أو مسافة للعنوان الفرعي. إذا لم تحدد ذلك، فاتركه فارغاً.
Password(SID)	عينَ كلمة المرور للعنوان الفرعي باعتباره حالة. عند تحديد <b>Equals</b> ، أدخل كلمة المرور للمطابقة. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، أو *، أو #، أو مسافة لكلمة المرور. إذا لم تحدد ذلك، فاتركه فارغاً.
Receiving Time	عينَ تحديد الفترة التي يتم فيها تطبيق الحالة. يشبه الإعداد الإضافي تعطيل إعداد الحالة، ولا يتم تطبيق الإخراج الشرطي.
Start Time	عينَ فترة البدء التي يتم فيها تطبيق الحالة.
End Time	عينَ فترة الانتهاء التي يتم فيها تطبيق الحالة.



## إعدادات الوظيفة

العنصر	الوصف
Fax Output	عين طريقة المعالجة لوقت تطابق الموقف مع الحالات.
Printing	حدد الطباعة في الوقت الذي تتطابق فيه المستندات المستلمة مع الحالات.
Save to Fax Box	حدد التخزين في صندوق الوارد أو الصندوق السري في الوقت الذي تتطابق فيه المستندات المستلمة مع الحالات. حدد اسم <b>Inbox</b> و <b>Personal Box</b> من القائمة المنسدلة.
Save to Memory Device	حدد التخزين في جهاز ذاكرة خارجي في الوقت الذي تتطابق فيه المستندات المستلمة مع الحالات.
Forward	حدد النقل في الوقت الذي تتطابق فيه المستندات المستلمة مع الحالات. انقر فوق <b>Select from Contacts</b> لتحديد وجهة النقل من جهات الاتصال.
Options When Forwarding Failed	حدد هذه العملية عند فشل المعالجة الشريطية.
Email Notifications	عين سواء الإبلاغ عن طريق البريد الإلكتروني عند إكمال الإخراج الشريطي أم لا.
Receive	يتم الإبلاغ عندما تقوم بتخزين المستندات المستلمة في صندوق البريد أو الصندوق السري.
Printing	يتم الإبلاغ عندما تنتهي من طباعة فاكس مستلم.
Save to Memory Device	يتم الإبلاغ عندما تنتهي من تخزين فاكس مستلم على جهاز ذاكرة خارجي.
Forward	يتم الإبلاغ عندما تنتهي من نقل فاكس مستلم.
Recipient	عين وجهة للبريد الإلكتروني لإكمال العملية. انقر فوق <b>Select from Contacts</b> لتحديد من جهات الاتصال.
Report Settings	عين التقرير الخاص بالإخراج الشريطي.
Transmission Report	حدد حالة للإخراج من تقرير نتيجة الإخراج الشريطي.

## Fax Block Settings

العنصر	الوصف
Rejection Fax	عين رفض الفاكسات الواردة من رقم جهة أخرى.
Rejection Number List	إذا تواجد رقم هاتف جهة أخرى في قائمة رقم الرفض، فعين سواء رفض الفاكسات الواردة أم لا.
Fax Header Blank Blocked	إذا تم حظر رقم هاتف جهة أخرى، فعين سواء رفض الفاكسات الواردة أم لا.
Unregistered Contacts	إذا لم يكن رقم الهاتف التابع لجهة أخرى موجوداً في جهات الاتصال، فعين سواء رفض الفاكسات الواردة أم لا.
Rejection Number List	سجل رقم الهاتف التابع لجهة أخرى لرفض الفاكسات والمكالمات الواردة. يمكنك تسجيل ما يصل إلى 30 وجهة. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، أو *، أو #، أو مسافة لرقم الهاتف التابع لجهة أخرى، ثم انقر فوق <b>Add</b> . يمكنك أيضاً التسجيل من <b>Add from Call History</b> . لحذف رقم (أرقام) هاتف مسجل، حدده، ثم انقر فوق <b>Delete</b> . انقر فوق <b>OK</b> على الصفحة لإضافة رقم الهاتف المسجل.

## إعدادات الوظيفة

## Inbox

حدد القائمة للتبديل إلى شاشة التحرير الخاصة بصندوق الوارد. عند تعيين كلمة مرور لصندوق الوارد، وعدم تكوين كلمة مرور المسؤول، انتقل إلى شاشة إدخال كلمة المرور. عند تعيين كلمة مرور المستخدم، انتقل إلى شاشة التحرير بغض النظر عن إعداد كلمة المرور لصندوق الوارد.

العنصر	الوصف
Change Password	حدد سواء تغيير كلمة مرور الصندوق أم لا.
Box Password	عين كلمة مرور للصندوق. أدخل ما يصل إلى 20 حرفاً أو أقل بتنسيق ASCII (0x20-0x7E). وإذا لم تحدد ذلك، فاتركه فارغاً.
Confirm Password	أدخل كلمة المرور للتأكيد.
Operation Fax Data Full	عين العملية عندما تكون ذاكرة صندوق الوارد ممتلئة.

## Personal Box (شاشة التحرير)

حدد القائمة للتبديل إلى شاشة التحرير الخاصة بصندوق الوارد. عند تعيين كلمة مرور لصندوق الوارد، وعدم تكوين كلمة مرور المسؤول، انتقل إلى شاشة إدخال كلمة المرور. عند تعيين كلمة مرور المستخدم، انتقل إلى شاشة التحرير بغض النظر عن إعداد كلمة المرور لصندوق الوارد.

العنصر	الوصف
Number	رقم فهرس الصندوق.
Name	أدخل اسم الصندوق. أدخل ما يصل إلى 30 حرفاً أو أقل بتنسيق Unicode (UTF-8) دون أحرف التحكم. إذا لم تحدد ذلك، فاتركه فارغاً. يتم حساب الحرف مزدوج البايت والأحرف ذات البايت الواحد كحرف واحد.
Change Password	حدد سواء تغيير كلمة مرور الصندوق أم لا.
Box Password	عين كلمة مرور للصندوق. أدخل ما يصل إلى 20 حرفاً أو أقل بتنسيق ASCII (0x20-0x7E). إذا لم تحدد ذلك، فاتركه فارغاً.
Confirm Password	أدخل كلمة المرور للتأكيد.

## Report Settings

العنصر	الوصف
Forwarding Report	عين سواء طباعة تقرير عن نقل المستند المستلم أم لا.
Backup Error Report	عين سواء طباعة التقرير في حالة النسخ الاحتياطي التلقائي بعد فشل إرسال الفاكس أم لا.
Fax Log Auto Print	عين سواء طباعة سجل الفاكس تلقائياً أم لا. حدد <b>On(Every 30)</b> لطباعة سجل بعد إتمام كل 30 مهمة من مهام الفاكس. حدد <b>On(Time)</b> لطباعة السجل في وقت محدد. ولكن إذا زاد عدد مهام الفاكس عن 30، تتم طباعة السجل قبل الوقت المحدد. إذا حددت <b>On(Time)</b> ، فسيتم أيضاً تعيين وقت الطباعة.
Attach Image to Report	لطباعة <b>Last Transmission Report</b> مع صورة للصفحة الأولى من المستند المرسل. حدد <b>On(Large Image)</b> لطباعة الجزء العلوي من الصفحة من دون تصغير حجمها. حدد <b>On(Small Image)</b> لطباعة الصفحة بالكامل مع تصغير حجمها بحيث يلائم حجم التقرير.
Report Format	عين تنسيق عرض تقرير سجل الفاكس وتقرير نتيجة الإرسال. إذا كان تنسيق العرض <b>Detail</b> ، فسيتم عرض رموز الخطأ.
Output Method	حدد وجهة إخراج التقرير.
Where to Forward (When the report output destination is [Forward])	حدد الوجهة عند تعيين وجهة إخراج التقرير على <b>Forward</b> . انقر فوق <b>Select from Contacts</b> لتحديد وجهة من جهات الاتصال.

## إعدادات الوظيفة

## Line Settings

العنصر	الوصف
Line Type	حدد نوع الخط الذي وصّيت الطابعة به. عند استخدام الطابعة في بيئة تستخدم امتدادات وتتطلب رموز وصول خارجية، مثل 0 و 9، للوصول إلى خط خارجي، حدد <b>PBX</b> وسجّل رمز الوصول. بعد تسجيل رمز الوصول، أدخل # (علامة التجزئة) بدلاً من رمز الوصول عند إرسال فاكس إلى رقم فاكس خارجي. بالنسبة إلى البيئات التي تستخدم مودم DSL أو مهائناً طرفياً، يوصى أيضاً بتعيين <b>PBX</b> .
Access Code	قم بتعيين ما إذا كان يتم استخدام رمز الوصول أم لا. قم بالتسجيل عند استخدام <b>PBX</b> وعندما يكون رمز الوصول مطلوباً للوصول الخارجي. إذا تم تمكينه، أدخل ما يصل إلى أربعة أحرف أو أقل باستخدام 0-9، أو *، أو # عند الوصول. إذا لم تحدد ذلك، فاتركه فارغاً.
Dial Mode	حدد نوع نظام الهاتف الذي وصّيت الطابعة به. عند الضبط على <b>Pulse</b> ، يمكنك بشكل مؤقت تحويل وضع طلب الاتصال من النبضات إلى الرنين من خلال الضغط على * (يتم إدخال الحرف "T") أثناء إدخال الأرقام على الشاشة العلوية للفاكس. قد لا يتم هذا الإعداد وفقاً لمنطقتك أو بلدك.
Fax Speed	اضبط سرعة إرسال الفاكس. عندما تحدث أخطاء الاتصال في كثير من الأحيان أو عند استخدام هاتف IP في إحدى البيئات، يوصى بالخيار <b>Slow(9600, bps)</b> .
ECM	لمعالجة الأخطاء بشكل تلقائي عند إرسال الفاكس (وضع معالجة الأخطاء)، الذي ينتج بشكل أساسي عن التشويش في خط الهاتف. في حالة تعطيل تلك الميزة، لا يمكنك إرسال أو استلام المستندات بالألوان.
Dial Tone Detection	لاكتشاف نغمة الرنين قبل البدء في الاتصال. إذا كانت الطابعة متصلة بـ <b>PBX</b> (أنظمة شبكة الهاتف الخاصة) أو هاتف IP، فلا يمكنك طلب الاتصال بالرقم. في تلك الحالة، غير إعداد <b>Line Type</b> إلى <b>PBX</b> . إذا لم يفلح هذا الإجراء، فعطّل تلك الميزة. إلا أن تعطيل تلك الميزة قد يؤدي إلى إسقاط الخانة الرقمية الأولى من رقم الفاكس وإرسال الفاكس إلى رقم خاطئ.

## Security Settings

العنصر	الوصف
Direct Dialing Restrictions	مكّن تلك الميزة لتعطيل الإدخال اليدوي لأرقام فاكس المستلم والسماح للمشغل بتحديد مستلمين فقط من قائمة جهات الاتصال أو سجل الإرسال. حدد <b>Enter Twice</b> لمطالبة المشغل بإدخال رقم الفاكس مرة أخرى إذا كان الرقم قد تم إدخاله يدوياً.
Confirm Address List	لعرض شاشة تأكيد المستلم قبل بدء الإرسال.
Backup Data Auto Clear	للاستعداد لأي توقف مفاجئ بسبب انقطاع الكهرباء أو أي تشغيل خاطئ، تخزن الطابعة في ذاكرتها نسخاً احتياطية مؤقتة من المستندات المرسلّة والمستلمة. مكّن هذا الخيار لمحو النسخ الاحتياطية تلقائياً عند اكتمال إرسال مستند أو استلامه بنجاح وبعدها تصبح النسخ الاحتياطية غير ضرورية.

## استخدام وظيفة PC-FAX

عند تثبيت FAX Utility على كمبيوتر عميل متصل بشبكة أو كابل USB، يتم تمكين إرسال الفاكسات واستقبالها.  
قم بإعداد ما يلي.

1. ادخل إلى Web Config وحدد علامة التبويب **Fax < Send Settings < Basic**.

2. حدد **Use PC to FAX Function**.

3. انقر فوق **OK**.

## إعدادات الوظيفة

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## استخدام جهات الاتصال

## ميزات إعداد الواجهة

يمكنك استخدام قائمة جهات اتصال الطابعة أو خادم LDAP لاختيار وجهة لميزات المسح الضوئي والفاكس.

ملاحظة:

☐ قد تتوفر الميزات المتاحة وفقاً للطراز. لمزيد من التفاصيل، انظر وثائق الطابعة.

☐ يمكنك التبديل بين قائمة جهات اتصال الطابعة وLDAP باستخدام لوحة تحكم الطابعة.

☐ لاستخدام ميزات البريد الإلكتروني، يجب تكوين خادم بريد.

معلومات ذات صلة

← "تكوين جهات الاتصال" في الصفحة 60

← "التعاون بين خادم LDAP والمستخدمين" في الصفحة 64

← "تكوين خادم البريد" في الصفحة 31

## تكوين جهات الاتصال

يمكن أن تتضمن قائمة جهات الاتصال الأنواع التالية من الوجهات:

☐ Fax: وجهة الفاكس

☐ Email: وجهة البريد الإلكتروني

☐ FTP/Network Folder (SMB): وجهة بيانات المسح الضوئي وبيانات إعادة توجيه الفاكسات

## مقارنة تكوين جهات الاتصال

توجد ثلاث أدوات لتكوين جهات اتصال الطابعة: Web Config، وEpsonNet Config، ولوحة تحكم الطابعة. يتضمن الجدول أدناه الفروق بين هذه الأدوات. استخدام EpsonNet Config سيفتح Web Config، ويمكنك بعد ذلك التكوين باستخدام Web Config.

لوحة تحكم الطابعة	Web Config	الميزات
✓	✓	تسجيل الواجهة
✓	✓	تحرير الواجهة
✓	✓	إضافة مجموعة
✓	✓	تحرير مجموعة
✓	✓	حذف وجهة أو مجموعات
-	✓	حذف جميع الوجهات
-	-	نسخ وجهات أو مجموعات

## إعدادات الوظيفة

لوحة تحكم الطابعة	Web Config	الميزات
-	✓	استيراد ملف
-	✓	التصدير إلى ملف
✓	✓	تعيين وجهات للاستخدام المتكرر
✓	-	فرز الوجهات المعينة للاستخدام المتكرر

## ملاحظة:

يمكنك أيضاً تكوين وجهة الفاكس باستخدام *FAX Utility*.

## تسجيل وجهة لجهات الاتصال

1. ادخل إلى Web Config وحدد Scan/Copy أو علامة التبويب **Contacts < Fax**.

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 37
- ← "عناصر إعدادات الوجهة" في الصفحة 62
- ← "نسخ جهات الاتصال والإعدادات احتياطياً" في الصفحة 88

## إعدادات الوظيفة

## عناصر إعدادات الوجهة

EPSON L3-10000FP

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 (SID/PWD) : \_\_\_\_\_

Apply Back

العناصر	الإعدادات والشرح
إعدادات عامة	
Name	أدخل الاسم المعروف في جهات الاتصال المكون من 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، يتم عرضه على الشاشة العلوية من الفاكس والمسح الضوئي، ويمكنك تحديد الوجهة دون عرض جهات الاتصال.
Fax	
Fax Number	أدخل عدداً من الأحرف يتراوح بين حرف واحد إلى 64 حرفاً باستخدام 0-9، -، *، #، والمسافة.
Fax Speed	حدد سرعة الاتصال للوجهة.
Subaddress (SUB/SEP)	عين العنوان الفرعي للمربع. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، *، #، أو المسافات. إذا لم تحدد ذلك، فاتركه فارغاً.
Password (SID/PWD)	عين كلمة المرور الخاصة بالعنوان الفرعي. أدخل ما يصل إلى 20 حرفاً أو أقل باستخدام 0-9، *، #، أو المسافات. إذا لم تحدد ذلك، فاتركه فارغاً.

## إعدادات الوظيفة

العناصر	الإعدادات والشرح
Email	
Email Address	أدخل عددًا من الأحرف يتراوح بين حرف واحد إلى 255 حرفًا باستخدام A-Z، a-z، و0-9، و!#\$%&'*+، -./^?_{ }~@.
Network Folder (SMB)	
Save to	"\مسار المجلد" أدخل المكان الذي يوجد به المجلد المستهدف ما بين حرف واحد و253 حرفًا بتنسيق Unicode (UTF-8)، مع حذف "\".
User Name	أدخل اسم المستخدم للوصول إلى مجلد الشبكة بنحو 30 حرفًا أو أقل بتنسيق Unicode (UTF-8). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1f، 0x7F).
Password	أدخل كلمة المرور للوصول إلى مجلد الشبكة بنحو 20 حرفًا أو أقل بتنسيق Unicode (UTF-8). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1f، 0x7F).
FTP	
Save to	أدخل اسم الخادم ما بين حرف واحد إلى 253 حرفًا بتنسيق ASCII (0x20-0x7E)، مع حذف "://ftp".
User Name	أدخل اسم المستخدم للوصول إلى خادم FTP بنحو 30 حرفًا أو أقل بتنسيق Unicode (UTF-8). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1f، 0x7F). إذا كان الخادم يسمح بالاتصالات المجهولة، أدخل اسم المستخدم كمجهول وFTP. إذا لم تحدد ذلك، فاتركه فارغًا.
Password	أدخل كلمة مرور للوصول إلى خادم FTP حتى 20 حرفًا أو أقل بتنسيق Unicode (UTF-8). ومع ذلك، تجنب استخدام أحرف التحكم (0x00 إلى 0x1f، 0x7F). إذا لم تحدد ذلك، فاتركه فارغًا.
Connection Mode	حدد وضع الاتصال من القائمة. في حالة تحديد جدار حماية بين الطابعة وخادم FTP، فحدد <b>Passive Mode</b> .
Port Number	أدخل رقم منفذ خادم FTP ما بين حرف واحد إلى 65535 حرفًا.

## معلومات ذات صلة

← "تسجيل وجهة لجهات الاتصال" في الصفحة 61

## تسجيل وجهة بمثابة مجموعة

في حالة تعيين نوع الوجهة على Fax أو Email، فإنه يمكنك تسجيل الوجهة بمثابة مجموعة.

1. ادخل إلى Web Config وحدد Scan/Copy أو علامة التبويب Fax < Contacts.

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

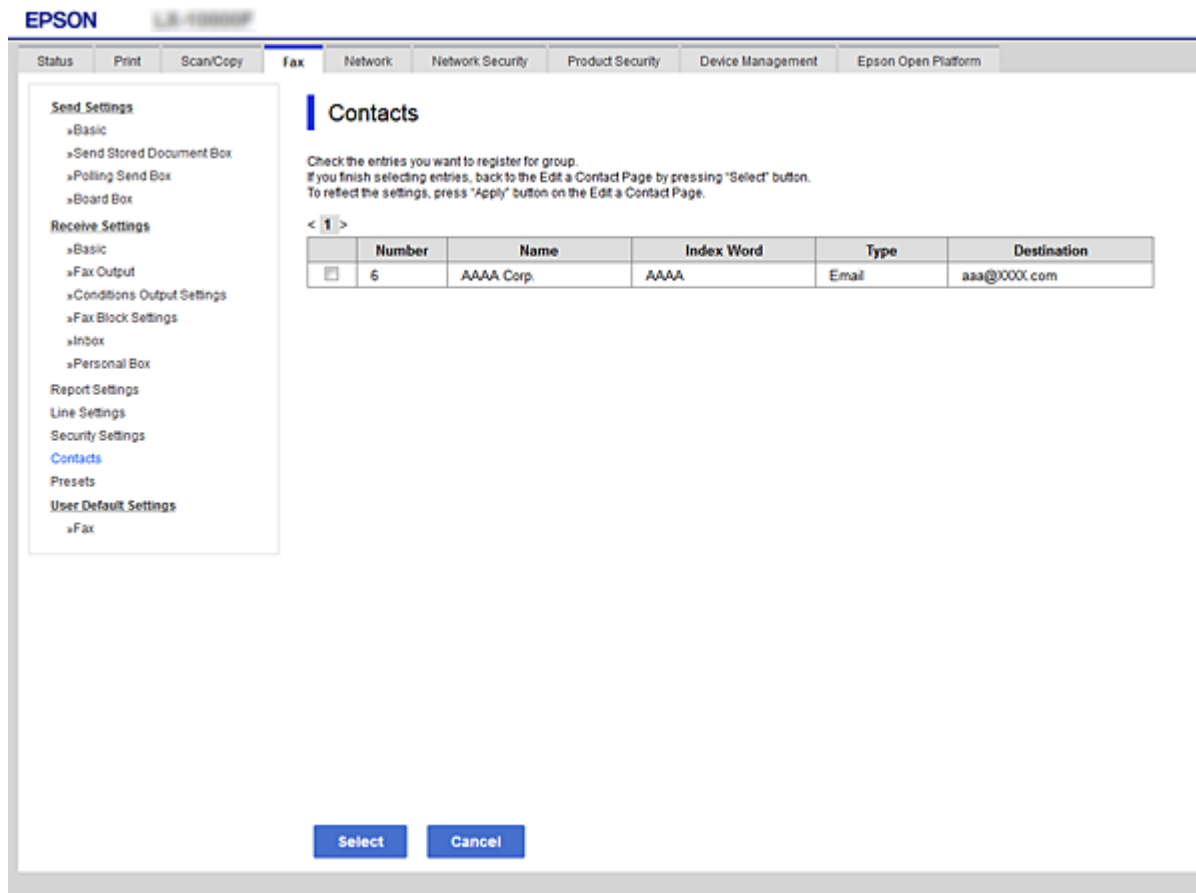
3. حدد مجموعة من Type.

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**.



6. أدخل **Index Word** و **Name**.

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 37

← "نسخ جهات الاتصال والإعدادات احتياطياً" في الصفحة 88

## التعاون بين خادم LDAP والمستخدمين

عند التعاون مع خادم LDAP، يمكنك البحث عن وجهة وتحديدها للبريد الإلكتروني أو الفاكس من جهات الاتصال على خادم LDAP.

معلومات ذات صلة

← "تكوين خادم LDAP" في الصفحة 65



## إعدادات الوظيفة

## تكوين خادم LDAP

1. ادخل إلى Web Config وحدد علامة التبويب **Basic < LDAP Server < Network**.
  2. أدخل قيمة لكل عنصر.
  3. حدد **OK**.
- يتم عرض الإعدادات التي قمت بتحديدتها.

## معلومات ذات صلة

- ◀ "الوصول إلى تطبيق Web Config" في الصفحة 37
- ◀ "عناصر إعداد خادم LDAP" في الصفحة 65

## عناصر إعداد خادم LDAP

The screenshot shows the Epson Web Config interface for the LDAP Server Basic settings. The navigation menu on the left includes: 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, and Google Cloud Print Services. The main content area is titled "LDAP Server > Basic" and contains the following fields:

- Use LDAP Server:** Radio buttons for "Use" (selected) and "Do Not Use".
- LDAP Server Address:** Text field containing "190.0.2.088".
- LDAP server Port Number:** Text field containing "389".
- Secure Connection:** Dropdown menu set to "SSL/TLS".
- Certificate Validation:** Radio buttons for "Enable" (selected) and "Disable".
- Search Timeout (sec):** Text field containing "10".
- Authentication Method:** Dropdown menu set to "Anonymous Authentication".
- Kerberos Realm to be Used:** Dropdown menu set to "Not Set".
- User Name:** Text field.
- Password:** Text field.

Below the fields, there is a note: "The certificate is required to use a secure function of the LDAP server. Make settings on the following page. - CA Certificate." and a note: "Configure Kerberos Settings before using Kerberos authentication." An "OK" button is located at the bottom of the page.

العناصر	الإعدادات والشرح
Use LDAP Server	حدّد Use أو Do Not Use.
LDAP Server Address	أدخل عنوان خادم LDAP. أدخل عددًا من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفًا بتنسيق IPv4، أو IPv6، أو FQDN. لتتنسيق FQDN، يمكنك استخدام أحرف أبجدية رقمية بتنسيق ASCII (0x20-0x7E)، و "-" فيما عدا في بداية العنوان ونهايته.
LDAP server Port Number	أدخل رقم منفذ خادم LDAP ما بين حرف واحد إلى 65535 حرفًا.

## إعدادات الوظيفة

العناصر	الإعدادات والشرح
Secure Connection	حدد طريقة التشفير للاتصال بخادم LDAP.
Certificate Validation	حدد ما إذا كنت تريد التحقق من صحة الشهادة عند الاتصال بخادم LDAP أم لا.
Search Timeout (sec)	عين طول وقت البحث قبل انقضاء المهلة باستخدام عددٍ من الأحرف الأبجدية الرقمية يتراوح ما بين 5 إلى 300.
Authentication Method	حدد أحد الأساليب. إذا حددت <b>Kerberos Authentication</b> ، فحدد <b>LDAP Server &lt; Kerberos Settings</b> لضبط إعدادات <b>Kerberos</b> .
Kerberos Realm to be Used	إذا حددت <b>Kerberos Authentication</b> لـ <b>Authentication Method</b> ، فحدد نطاق <b>Kerberos</b> الذي ترغب في استخدامه.
User Name	أدخل اسم المستخدم الخاص بخادم LDAP بنحو 128 حرفاً أو أقل بتنسيق Unicode (UTF-8). لا يمكنك استخدام رموز التحكم، مثل 0x00-0x1F و 0x7F. لا يستخدم هذا الإعداد عند تحديد <b>Anonymous Authentication</b> بصفته <b>Authentication Method</b> . إذا لم تحدد ذلك، فاتركه فارغاً.
Password	أدخل كلمة المرور الخاصة بمصادقة خادم LDAP بنحو 128 حرفاً أو أقل بتنسيق Unicode (UTF-8). لا يمكنك استخدام رموز التحكم، مثل 0x00-0x1F و 0x7F. لا يستخدم هذا الإعداد عند تحديد <b>Anonymous Authentication</b> بصفته <b>Authentication Method</b> . إذا لم تحدد ذلك، فاتركه فارغاً.

## معلومات ذات صلة

← "تكوين خادم LDAP" في الصفحة 65

← "إعدادات Kerberos" في الصفحة 66

## إعدادات Kerberos

إذا حددت **Kerberos Authentication** لـ **Authentication Method** الخاصة بـ **LDAP Server < Basic**، فاضبط إعدادات **Kerberos** التالية من علامة التبويب **Network < Kerberos Settings**. يمكنك ضبط ما يصل إلى 10 إعدادات خاصة بإعدادات **Kerberos**.

العناصر	الإعدادات والشرح
Realm (Domain)	أدخل نطاق مصادقة <b>Kerberos</b> يتكون من 255 حرفاً أو أقل بتنسيق ASCII (0x20-0x7E). إذا لم تحدد ذلك، فاتركه فارغاً.
KDC Address	أدخل عنوان خادم مصادقة <b>Kerberos</b> . أدخل 255 حرفاً أو قل إما بتنسيق IPv4، وإما IPv6، وإما FQDN. إذا لم تحدد ذلك، فاتركه فارغاً.
Port Number (Kerberos)	أدخل رقم منفذ خادم <b>Kerberos</b> ما بين حرف واحد إلى 65535 حرفاً.

## تكوين إعدادات بحث خادم LDAP

1. ادخل إلى Web Config وحدد علامة التبويب **Network < LDAP Server < Search Settings**.

2. أدخل قيمة لكل عنصر.

3. انقر فوق **OK** لعرض نتيجة الإعداد.

يتم عرض الإعدادات التي قمت بتحديدتها.

## إعدادات الوظيفة

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "عناصر إعداد بحث خادم LDAP" في الصفحة 67

## عناصر إعداد بحث خادم LDAP

العناصر	الإعدادات والشرح
Search Base (Distinguished Name)	إذا أردت البحث عن نطاق عشوائي، فحدد اسم نطاق خادم LDAP. أدخل ما بين 0 إلى 128 حرفاً بتنسيق Unicode (UTF-8). إذا لم تكن تبحث عن سمة عشوائية، فاترك هذا الخيار فارغاً. مثال على دليل الخادم المحلي: dc=local,dc=server
Number of search entries	حدد عدد مدخلات البحث ما بين 5 إلى 500. يتم حفظ العدد المحدد من مدخلات البحث وعرضه مؤقتاً. حتى إذا كان عدد مدخلات البحث يزيد عن العدد المحدد وظهور رسالة خطأ، فمن الممكن اكتمال البحث.
User name Attribute	حدد اسم السمة الذي يتم عرضه عند البحث عن أسماء المستخدمين. أدخل ما بين 1 إلى 255 رمزاً بتنسيق Unicode (UTF-8). يجب أن يكون الرمز الأول a-z، أو A-Z. مثال: uid, cn
User name Display Attribute	حدد اسم السمة الذي يتم عرضه بمثابة اسم المستخدم. أدخل ما بين 0 إلى 255 حرفاً بتنسيق Unicode (UTF-8). يجب أن يكون الحرف الأول a-z، أو A-Z. مثال: sn, cn

## إعدادات الوظيفة

العناصر	الإعدادات والشرح
Fax Number Attribute	حدد اسم السمة الذي يتم عرضه عند البحث عن أرقام الفاكس. أدخل مزيجاً من الرموز يتراوح بين 1 إلى 255 رمزاً باستخدام A-Z و a-z، و 0-9، و- . يجب أن يكون الرمز الأول a-z، أو A-Z. مثال: رقم هاتف الفاكس
Email Address Attribute	حدد اسم السمة الذي يتم عرضه عند البحث عن عناوين البريد الإلكتروني. أدخل مزيجاً من الرموز يتراوح بين 1 إلى 255 رمزاً باستخدام A-Z و a-z، و 0-9، و- . يجب أن يكون الرمز الأول a-z، أو A-Z. مثال: البريد
- Arbitrary Attribute 1 Arbitrary Attribute 4	يمكنك تحديد سمات عشوائية أخرى للبحث عنها. أدخل ما بين 0 إلى 255 حرفاً بتنسيق (UTF-8 Unicode). يجب أن يكون الحرف الأول a-z أو A-Z. إذا لم ترد البحث عن سمات عشوائية، فاترك هذا الإعداد فارغاً. مثال: ou, o

## معلومات ذات صلة

← "تكوين إعدادات بحث خادم LDAP" في الصفحة 66

## التحقق من اتصال خادم LDAP

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

2. حدد **Start**.

يتم بدء اختبار الاتصال. بعد الاختبار، يتم عرض تقرير الفحص.

## معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "مراجع اختبار اتصال خادم LDAP" في الصفحة 68

## مراجع اختبار اتصال خادم LDAP

الرسائل	الشرح
Connection test was successful.	تظهر هذه الرسالة عند نجاح الاتصال بالخادم.
Connection test failed. Check the settings.	تظهر هذه الرسالة للأسباب التالية: <input type="checkbox"/> عنوان خادم LDAP أو رقم المنفذ غير صحيح. <input type="checkbox"/> حلول وقت انقضاء المدة. <input type="checkbox"/> يتم تحديد <b>Do Not Use</b> بصفته <b>LDAP Server</b> . <input type="checkbox"/> إذا تم تحديد <b>Kerberos Authentication</b> بصفته <b>Authentication Method</b> ، تكون الإعدادات مثل <b>KDC Address, Realm (Domain)</b> و <b>Port Number (Kerberos)</b> غير صحيحة.
Connection test failed. Check the date and time on your product or server.	تظهر هذه الرسالة عند فشل الاتصال نظراً لعدم تطابق إعدادات الوقت الخاصة بالطابعة وخادم LDAP.

## إعدادات الوظيفة

الرسائل	الشرح
Authentication failed. Check the settings.	تظهر هذه الرسالة للأسباب التالية: <input type="checkbox"/> User Name و/أو Password غير صحيحين. <input type="checkbox"/> إذا تم تحديد Kerberos Authentication بصفته Authentication Method، فقد لا يتم تكوين الوقت/التاريخ.
Cannot access the printer until processing is complete.	تظهر هذه الرسالة عندما تكون الطابعة مشغولة.

معلومات ذات صلة

← "التحقق من اتصال خادم LDAP" في الصفحة 68

## 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.

Panel Lock 

إذا حددت ON، سيلزم توفير كلمة مرور المسؤول عند إجراء أي عملية تتطلب الحصول على إذن من المسؤول. إذا لم يتم تعيين كلمة مرور المسؤول، يتم 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.

3. انقر فوق OK.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## إعدادات توفير الطاقة أثناء فترة الخمول

قم بضبط إعداد توفير الطاقة لفترة خمول الطابعة. عين الوقت حسب بيئة الاستخدام.

ملاحظة:

يمكنك أيضاً ضبط إعدادات توفير الطاقة على لوحة التحكم بالطابعة.

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

## إعدادات الوظيفة

2. أدخل فترة **Sleep Timer** للانتقال إلى وضع توفير الطاقة عندما يكون الجهاز في فترة الخمول. يمكنك تعيين ما يصل إلى 240 دقيقة بحساب الدقائق.
3. حدد مدة إيقاف التشغيل لـ **Power Off Timer**. إذا كنت تستخدم وظيفة الفاكس، فقم بتعيينها على **None**.
4. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## إعداد الصوت

- اضبط إعدادات الصوت عند تشغيل لوحة التحكم، والطباعة، والفاكس، وما إلى ذلك.
1. ادخل إلى Web Config وحدد علامة التبويب **Sound < Device Management**.
  2. اضبط العناصر التالية حسب الضرورة.
    - Normal Mode
    - اضبط الصوت عند تعيين الطابعة على **Normal Mode**.
    - Quiet Mode
    - اضبط الصوت عند تعيين الطابعة على **Quiet Mode**. يتم تمكين ذلك عند تمكين أحد العناصر التالية.
    - لوحة تحكم الطابعة:
    - الإعدادات < إعدادات عامة < إعدادات الطابعة < الوضع الصامت
    - الإعدادات < إعدادات عامة < إعدادات الفاكس < إعدادات الاستلام < إعدادات الطباعة < الوضع الصامت
    - Web Config:
    - علامة التبويب **Fax < Receive Settings < Fax Output < Quiet Mode**
  3. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## مزامنة التاريخ والوقت مع خادم الوقت

- إذا كنت تستخدم شهادة المرجع المصدق (CA)، يمكنك الحد من حدوث مشكلات في 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 252 حرفاً أو أقل. إذا لم تحدد ذلك، فاتركه فارغاً.

## إعدادات الوظيفة

4. أدخل **Update Interval (min)**.

يمكنك تعيين فترة تصل إلى 10800 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 37

## 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

Scan to Cloud

Copy

Fax

1. ادخل إلى Web Config وحدد الوظائف التي ترغب في تعيين القيم الافتراضية لها لعلامة التبويب **Scan/Copy < User Default Settings**.

حدد علامة التبويب **Scan/Copy < User Default Settings** لتعيين القيمة الافتراضية للفاكس.

2. عين كل عنصر.

3. انقر فوق **OK**.

إذا كانت مجموعة القيم غير صالحة، فسيتم عرض القيمة الصالحة التي يتم تعديلها تلقائيًا. أكد القيمة المعدلة وانقر فوق **OK** مرة أخرى.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## تسجيل الإعدادات المستخدمة بشكل متكرر كإعداد سابق

يمكنك حفظ الإعدادات مثل وظيفة المسح الضوئي والنسخ والفاكس كإعدادات مسبقة. سجلها بعد إنهاء إعدادات كل وظيفة.

يمكنك ضبط الوظائف التالية.

Scan to Network Folder/FTP

Scan to Email

Scan to Memory Device

## إعدادات الوظيفة

Scan to Cloud Copy Fax 

1. ادخل إلى Web Config وحدد Scan/Copy أو علامة التبويب Presets < Fax.
2. حدد الرقم المسجل وانقر فوق Edit.
3. حدد Type الإعداد المسبق الذي ترغب في تعيينه.  
ملاحظة: بعد التسجيل، يتعدّر تغيير Type. إذا كنت ترغب في تغيير Type بعد التسجيل، فاحذف الإعداد المسبق ثم أعد تسجيله.
4. انقر فوق Next.
5. قم بإعداد كل عنصر.  
أدخل Name يتكون من حرف واحد حتى 30 حرفاً بتنسيق Unicode (UTF-8).
6. انقر فوق OK.  
إذا كانت مجموعة القيم غير صالحة، فسيتم عرض القيمة الصالحة التي يتم تعديلها تلقائياً. أكد القيمة المعدلة وانقر فوق OK مرة أخرى.

## معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## استخدام شبكة MS

- يمكنك تحديد ما إذا كان يمكنك تمكين مشاركة شبكة MS أم لا. عند تمكين هذا، يمكنك إرسال النتيجة الممسوحة ضوئياً والفاكس المستلم إلى المجلد المشترك من قبل مجموعة العمل.
1. ادخل إلى Web Config وحدد علامة التبويب MS Network < Network.
  2. حدد Use Microsoft network sharing.
  3. أدخل اسم مجموعة العمل التي تنتمي إليها الطابعة في Workgroup Name بحيث يكون في نطاق 15 حرفاً أو أقل بتنسيق ASCII.
  4. انقر فوق Next.
  5. أكد الإعدادات، ثم انقر فوق OK.

## معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## Print Settings

## Basic

اضبط العملية الأساسية للطابعة.



## إعدادات الوظيفة

حدد ما إذا كنت تريد تعطيل **Speed Priority** أم لا وحدد وجهة إخراج الورق للنسخ والفاكس وما إلى ذلك.

**Paper Source Settings**

اضبط حجم الورق المراد تحميله في كل مصدر للورق ونوعه.

**Interface Settings**

حدد لغة الطباعة لمهام الطباعة المرسله مباشرة عبر جهاز USB أو الشبكة.

**Error Settings**

عين أخطاء الجهاز التي سيتم عرضها.

**Paper Size Notice** 

حدد ما إذا كنت تريد عرض خطأ على لوحة التحكم عندما يكون حجم الورق في مصدر ورق محدد مختلفاً عن حجم الورق الخاص ببيانات الطباعة أم لا.

**Paper Type Notice** 

حدد ما إذا كنت تريد عرض خطأ على لوحة التحكم عندما يكون نوع الورق في مصدر ورق محدد مختلفاً عن نوع الورق الخاص ببيانات الطباعة أم لا.

**Auto Error Solver** 

حدد ما إذا كان سيتم إلغاء الخطأ تلقائياً إذا لم تكن هناك عملية قيد التنفيذ على لوحة التحكم لمدة 5 ثوانٍ بعد عرض الخطأ أم لا.

**Universal Print Settings**

اضبط الإعدادات للطباعة من الأجهزة الخارجية عن طريق برنامج تشغيل الطباعة.

## استخدام خدمة Epson Connect

باستخدام خدمة Epson Connect المتوفرة على الإنترنت، يمكنك الطباعة من هاتفك الذي أو جهاز الكمبيوتر اللوحي أو الكمبيوتر المحمول، في أي وقت وبشكل عملي في أي مكان.

الميزات المتوفرة على الإنترنت على النحو التالي.

Remote Print Driver	Scan to Cloud	الطباعة عن بعد عبر Epson iPrint	Email Print
✓	✓	✓	✓

راجع موقع بوابة Epson Connect الإلكترونية على الويب للاطلاع على التفاصيل.

<https://www.epsonconnect.com/>

<http://www.epsonconnect.eu> (أوروبا فقط)

# إعدادات سلامة المنتج

يوضح هذا الفصل إعدادات الأمان للجهاز.

## مقدمة عن ميزات سلامة المنتج

يقدم هذا القسم وظيفة سلامة أجهزة Epson.

اسم الميزة	نوع الميزة	ما الذي يتم تعيينه	ما الذي يتم حظره
إعداد كلمة مرور المسؤول	يقفل إعدادات النظام، مثل إعداد اتصال الشبكة أو USB، والإعداد التفصيلي لاستلام/إرسال الفاكس أو نقله، والإعدادات الافتراضية للمستخدم.	يعين أحد المسؤولين كلمة مرور للجهاز. يتوفر التكوين أو التحديث من أي مكان من Web Config، ومن لوحة التحكم، ومن Epson Device Admin، ومن EpsonNet Config.	يتم حظر قراءة المعلومات المخزنة في الجهاز مثل المعرف، وكلمة المرور، وإعدادات الشبكة، وجهات الاتصال وتغييرها بشكل غير قانوني. يتم أيضاً الحد من وجود مجموعة كبيرة من المخاطر الأمنية مثل تسرب المعلومات المتعلقة ببيئة الشبكة أو سياسة الأمان.
إعداد التحكم في الوصول	يقوم بالحد من الوظائف التي يمكن استخدامها على الأجهزة، مثل الطباعة، والمسح الضوئي، والنسخ، وإرسال الفاكسات لكل مستخدم. إذا قمت بتسجيل الدخول باستخدام حساب مستخدم مسجل مقدماً، فسيتم السماح لك باستخدام بعض الوظائف المحددة.	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 التعرض لتسرب البيانات وعرضها بشكل غير مشروع عن طريق تقليل عدد الوظائف وفقاً للمحتوى التجاري ودور المستخدم. وبالإضافة إلى ذلك، بعد تسجيل الدخول من لوحة التحكم، سيتم تسجيل خروجك تلقائياً إذا لم تكن هناك أي مهمة جارية لفترة محددة من الوقت.
إعداد الواجهة الخارجية	يتحكم في الواجهة، مثل منفذ USB ومنفذ NFC الذي يتصل بالجهاز.	مكن منفذ USB لتوصيل أجهزة خارجية مثل ذاكرة USB وNFC واتصال USB بالكمبيوتر أو عطله.	<input type="checkbox"/> التحكم بمنفذ USB: يقلل من إمكانية أخذ البيانات من خلال عملية مسح ضوئي غير مصرح بها للمستندات السرية. <input type="checkbox"/> NFC: يمنع الطباعة غير القانونية باستخدام NFC. <input type="checkbox"/> اتصال USB للكمبيوتر: يمنع الاستخدام غير المصرح به للجهاز عن طريق حظر الطباعة أو المسح الضوئي دون المرور عبر الشبكة.
إعداد معالجة البيانات المحفوظة	مسح بيانات المهمة المخزنة مؤقتاً في القرص الصلب المدمج في الجهاز تلقائياً. كما يمكنك أيضاً مسح جميع البيانات المخزنة في القرص الصلب بأمان.	حدد ما إذا كان سيتم الحذف تلقائياً عند انتهاء المهمة أم لا. يمكنك أيضاً مسح جميع البيانات إذا كنت ترغب في التخلص من الجهاز.	عن طريق الاستبدال بنمط معين، يمكنك منع أي شخص من استعادة البيانات واستخدامها حتى إذا تمت إزالة القرص الصلب.

### معلومات ذات صلة

- ← "حول تهيئة الويب" في الصفحة 36
- ← "EpsonNet Config" في الصفحة 101
- ← "Epson Device Admin" في الصفحة 101
- ← "تكوين كلمة مرور المسؤول" في الصفحة 75
- ← "تقييد الميزات المتوفرة" في الصفحة 78
- ← "إعداد قيود الواجهة الخارجية" في الصفحة 80
- ← "ضبط إعدادات معالجة البيانات المحفوظة" في الصفحة 81

## تكوين كلمة مرور المسؤول

عندما تقوم بتعيين كلمة مرور المسؤول، لن يتمكن المستخدمون الآخرون بخلاف المسؤول من تغيير إعدادات مسؤول النظام. يمكنك تعيين كلمة مرور المسؤول وتغييرها باستخدام إما Web Config، وإما لوحة تحكم الطابعة، وإما البرنامج (Epson Device Admin أو EpsonNet Config). عند استخدام البرنامج، راجع المستند المتعلق بكل برنامج.

### معلومات ذات صلة

- ← "تكوين كلمة مرور المسؤول من لوحة التحكم" في الصفحة 75
- ← "تكوين كلمة مرور المسؤول باستخدام Web Config" في الصفحة 75
- ← "EpsonNet Config" في الصفحة 101
- ← "Epson Device Admin" في الصفحة 101

## تكوين كلمة مرور المسؤول من لوحة التحكم

يُمكنك تعيين كلمة مرور المسؤول من لوحة تحكم الطابعة.

1. اضغط على الإعدادات في لوحة تحكم الطابعة.
2. اضغط على إعدادات عامة < إدارة النظام < إعدادات الأمان.
3. اضغط على إعدادات المسؤول.
4. اضغط على كلمة مرور المسؤول < تسجيل.
5. أدخل كلمة مرور جديدة، ثم اضغط على موافق.
6. أدخل كلمة المرور مرة أخرى، ثم اضغط على موافق.
7. اضغط على موافق على شاشة التأكيد.  
يتم عرض شاشة إعدادات المسؤول.
8. اضغط على إعداد القفل، ثم اضغط على موافق على شاشة التأكيد.

### ملاحظة:

يمكنك 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

يمكنك 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 **Administrator Login**، ثم أدخل كلمة مرور المسؤول.
- لحذف كلمة مرور المسؤول، انقر فوق **Administrator Settings < Delete Administrator Authentication Information**، ثم أدخل كلمة مرور المسؤول.

## معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## العناصر التي يتم قفلها عن طريق كلمة مرور المسؤول

لدى المسؤولين امتياز إعداد أو تغيير لجميع الميزات على الأجهزة. بالإضافة إلى ذلك، إذا تم تعيين كلمة مرور المسؤول على أحد الأجهزة، فإنها تقفل عنصر إعداد الشبكة ولا تسمح بتغييره وتقييد ميزات المستخدم المرتبطة بإدارة الجهاز. ما يلي العناصر التي يتمكن المسؤول من التحكم بها.

## إعدادات سلامة المنتج

العنصر	الوصف
معلومات الصيانة (Web Config فقط)	تأكيد المعلومات المتعلقة بإجمالي صفحات الطباعة، وحجم الورق، والألوان/الأسود والأبيض، وصفحات الطباعة على الوجهين ووجه واحد، وطباعة الصفحات لكل لغة للطباعة.
صيانة جهات الاتصال	تسجيل وجهة جهات الاتصال وتحريرها.
الإعداد الافتراضي للمستخدم	الإعداد الافتراضي للفاكس والمسح الضوئي السريع.
التحكم في الوصول	الإعداد الخاص بالمستخدم والوظائف الذي يتيح استخدامها.
إعداد الطباعة	إعدادات لغة الطباعة، وإعدادات التشغيل الخاصة بحدوث خطأ، وما إلى ذلك.
إعدادات الفاكس	إعدادات الفاكس العامة لوضع الاستقبال، والإرسال، والإخراج، والاتصال.
إعدادات الاتصال بشبكة إيثرنت وشبكة Wi-Fi	قم بتغيير اسم الأجهزة وعنوان IP، وإعداد خادم DNS أو خادم الوكيل، وتغييرات الإعداد المتعلقة باتصالات الشبكة.
إعداد خدمات المستخدم	الإعداد الخاص بالتحكم في بروتوكولات الاتصال أو MS Network، والمسح الضوئي عبر الشبكة، وخدمات Wi-Fi Direct.
إعداد خادم البريد الإلكتروني	إعداد خادم البريد الإلكتروني الذي تتصل به الأجهزة مباشرة.
إعداد خادم LDAP	إعداد استخدام جهات الاتصال على خادم LDAP كواجهة للبريد الإلكتروني أو الفاكس.
إعداد الأمان	إعدادات أمان الشبكة، مثل اتصال SSL/TLS، وتصفية IPsec/IP، وIEEE802.1X.
إعداد الاتصال بالخدمات السحابية	إعداد الاتصال لخدمة Epson Connect أو للخدمات السحابية لشركة أخرى. وتحديث شهادة الجذر التي تُعد ضرورية للخدمات السحابية.
تحديث البرنامج الثابت	تحقق من البرنامج الثابت للأجهزة وقم بتحديثه.
إعدادات الوقت والمؤقت	إعدادات فترة الانتقال الخاصة بوضع السكون، وإيقاف التشغيل التلقائي، والتاريخ/الوقت، ومؤقت عدم التشغيل، والإعدادات الأخرى المتعلقة بالمؤقت.
إعداد الوضع الافتراضي	إعداد لوحة التحكم عند تشغيل الطباعة. يمكنك تعيين ميزات الشاشة لأي شيء مثل النسخ والفاكس، بدلاً من الشاشة الرئيسية.
إعدادات الصفحة الرئيسية	إعداد مكان الصفحة الرئيسية ولون خلفيتها.
التأكيد الافتراضي لشاشة الحالة	إعداد شاشة حالة مهمة الطباعة أو الطباعة التي يتم عرضها عن طريق الضغط على حالة المهمة في لوحة التحكم.
إعداد المسح الضوئي	إعداد خادم البريد الإلكتروني، وتأكيد الوجهة قبل المسح الضوئي، وإعداد Document Capture Pro.
إعداد المفضلة	تسجيل المفضلة وحذفها.
تسجيل/حذف الحد المسموح به من جهات الاتصال*	إزالة تسجيل جهات الاتصال وحذفها من عناصر الإعداد التي يتم قفلها بكلمة مرور المسؤول.
إعداد الوصول إلى السجل	إعداد عرض المعلومات التفصيلية حول تاريخ المهام، مثل سجل المهمة، وآخر فاكس، والمحفوظات المرسله الخاصة بـ مسح ضوئي إلى البريد الإلكتروني.
إعداد طباعة السجلات والتقارير*	إعداد طباعة السجلات والتقارير، مثل سجل حفظ مسح ضوئي إلى مجلد الشبكة/FTP، وتقارير الفاكس.
إعداد اللغة*	إعداد اللغة المعروضة على لوحة التحكم.
الإعدادات التي تؤثر على سرعة الطباعة*	إعدادات الطباعة التي تؤثر على سرعة الطباعة، مثل ورق سميك، و الوضع الصامت، و أولوية سرعة الطباعة.
إعداد عرض البيانات الشخصية*	إعداد عرض مسار المجلد، مثل وجهة مسح ضوئي إلى مجلد الشبكة/FTP.
إعداد معلومات إرسال الطباعة	إعداد معلومات الإرسال الخاصة بعدد المطبوعات.

## إعدادات سلامة المنتج

العنصر	الوصف
إعداد الكشف عن تغذية مزدوجة*	إعداد الكشف عن تغذية مزدوجة للمستند المراد مسحه ضوئياً.
حذف الذاكرة الداخلية	إعدادات حذف البيانات من الذاكرة الداخلية للطابعة.
حذف جميع مهام الطباعة المحمية بكلمة مرور	إعداد حذف جميع مهام الطباعة المحمية بكلمة مرور.
إعدادات استعادة الإعدادات الافتراضية	إعداد إعادة تعيين الطابعة إلى إعدادات المصنع.
إعداد المسؤول	إعداد قفل المسؤول أو كلمة مرور المسؤول.
إعداد Epson Open Platform	إعداد تمكن Epson Open Platform. يتم تعيينه عند استخدام الطابعة على نظام مصادقة يدعم Epson Open Platform. مثل Epson Print Admin.
إعداد الجهاز المعتمد	إعداد المعرف الخاص بجهاز المصادقة. يتم تعيينه عند استخدام الطابعة على نظام مصادقة يدعم أجهزة المصادقة، مثل Epson Print Admin.

\* يمكنك الحذف من العناصر المقفلة.

## معلومات ذات صلة

← "تغيير إعدادات العناصر المقفلة بكلمة مرور المسؤول" في الصفحة 78

## تغيير إعدادات العناصر المقفلة بكلمة مرور المسؤول

بالنسبة لبعض الوظائف، يمكنك التبديل بين إدراج إلى العناصر المقفلة بكلمة مرور المسؤول والحذف منها.

1. اضغط على الإعدادات في لوحة تحكم الطابعة.
2. اضغط على إعدادات عامة < إدارة النظام > إعدادات الأمان.
3. اضغط على Restrictions.
4. اضغط على العنصر الخاص بالوظيفة التي تريد تغيير إعدادها، ثم اضبط الوضع على تشغيل أو إيقاف.

## تقييد الميزات المتوفرة

يمكنك إنشاء حتى 10 مستخدمين مميزين وتقييد ميزات الطابعة المتاحة لكل مستخدم. يجب أن يقوم المستخدمون بتسجيل الدخول باستخدام اسم المستخدم وكلمة المرور باستخدام لوحة تحكم الطابعة. يمكن أن يقوم المستخدمون بتسجيل الخروج يدوياً أو ستقوم الطابعة بتسجيل خروجهم تلقائياً بعد فترة من الوقت.

إذا أردت تقييد الطباعة من برنامج تشغيل الطابعة وبرنامج تشغيل الماسح الضوئي، فاستخدم برنامج التشغيل المخصص للطابعة.

إذا كنت تستخدم الطابعة من كمبيوتر يعمل بنظام Windows، فإنه يمكنك تعيين اسم المستخدم وكلمة مرور لبرنامج تشغيل الطابعة وبرنامج تشغيل الماسح الضوئي مقدماً. ستقوم الطابعة بمصادقة المستخدم تلقائياً عند استخدام الكمبيوتر ولن تحتاج إدخال كلمة مرور في كل مرة. لمزيد من المعلومات حول استخدام برنامج التشغيل، انظر تعليمات برنامج التشغيل.

لا يمكنك استخدام هذه الميزة في Mac OS.

## إعدادات سلامة المنتج

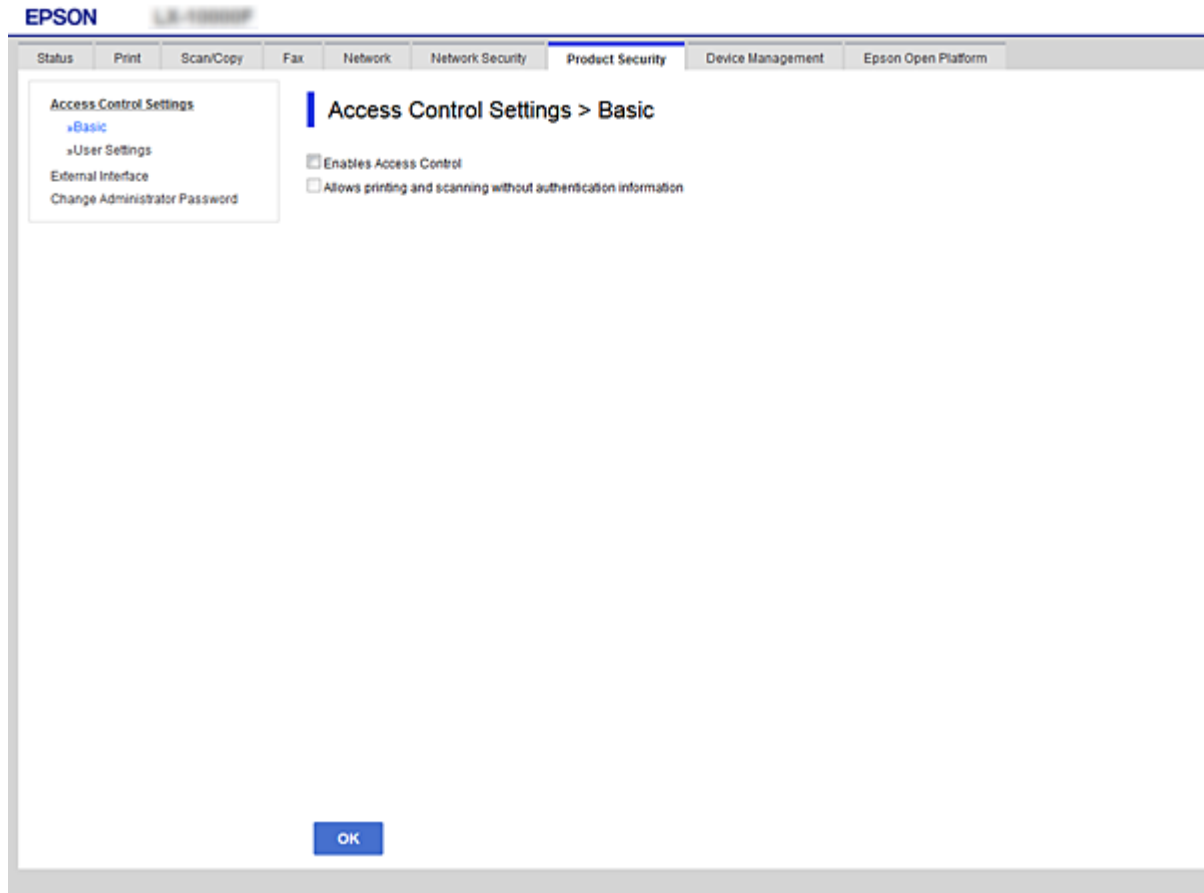
## تكوين التحكم في الوصول

1. ادخل إلى Web Config وحدد علامة التبويب **Product Security < Access Control Settings < Basic**.

2. حدد مربع **Enables Access Control** وانقر فوق **OK**.

**هام:** إذا قمت بإلغاء تحديد مربع **Allows printing and scanning without authentication information**، فلن يتم استلام المهام غير المصدق عليها المرسله من المصادر التالية:

- برنامج التشغيل الافتراضي لنظام التشغيل
- برنامج تشغيل الطابعة *PCL*/برنامج تشغيل الطابعة *PostScript*
- خدمات الويب مثل *Epson Connect* و *Google Cloud Print*
- الهواتف الذكية والأجهزة المحمولة الأخرى



3. حدد علامة التبويب **Product Security < Access Control Settings < User Settings**.

4. انقر فوق **Add**، ثم أدخل قيمة لكل عنصر.

5. انقر فوق **Apply**.

**ملاحظة:**

يتم عرض خيار **Delete** عند تحرير مستخدم مسجل. انقر فوقه لحذف أحد المستخدمين.

## إعدادات سلامة المنتج

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "عناصر إعدادات المستخدم" في الصفحة 80

## عناصر إعدادات المستخدم

The screenshot shows the Epson Web Config interface for 'Access Control Settings > User Settings'. The 'Number' field is set to 1. The 'User Name' field contains 'PrintAdmin'. The 'Password' field is masked with asterisks. Below the fields, there are checkboxes for enabling or disabling functions: Copy, Scan, Fax, Print from Memory Device, Print from Computer, and Color Print. The 'Apply' and 'Back' buttons are at the bottom.

العناصر	الإعدادات والشرح
User Name	أدخل اسم العرض على القائمة باستخدام عددٍ من الرموز يتراوح ما بين 1 إلى 14 رمزاً بتنسيق ASCII ((0x20-0x7E).
Password	أدخل ما بين 0 إلى 20 حرفاً بتنسيق ASCII (0x20-0x7E). إذا كنت تريد استعادة كلمة المرور إلى الوضع الافتراضي، فاترك هذا الإعداد فارغاً.
Select the check box to enable or disable each function.	يتم السماح باستخدام الوظائف المحددة.

## إعدادات قيود الواجهة الخارجية

يمكنك تقييد استخدام اتصال USB من الكمبيوتر. اضبط إعدادات القيود لتقييد إجراء الطباعة والمسح الضوئي عبر أي وسيلة بخلاف الشبكة.

ملاحظة:

يمكنك أيضاً ضبط إعدادات القيود على لوحة التحكم بالطابعة.



## إعدادات سلامة المنتج

1. ادخل إلى Web Config وحدد علامة التبويب **External Interface < Product Security**.
2. حدّد **Enable** أو **Disable**.
- إذا كنت ترغب في تقييده، فحدد **Disable**.
3. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## ضبط إعدادات معالجة البيانات المحفوظة

يمكنك ضبط الإعدادات لمعالجة البيانات المخزنة في القرص الصلب الداخلي.

تُحفظ مهام الطباعة والنسخ والمسح الضوئي مؤقتاً في القرص الصلب من أجل معالجة البيانات لإجراء طباعة معتمدة وكمية كبيرة من النسخ والمسح الضوئي والطباعة وما إلى ذلك. اضبط الإعدادات لمسح هذه البيانات بأمان.

### Sequential Deletion from Hard Disk

عند التمكين، يتم مسح البيانات المستهدفة بالتتابع عندما تصبح غير ضرورية، على سبيل المثال عند اكتمال الطباعة أو المسح الضوئي. وتُعد البيانات المستهدفة المراد حذفها بمثابة البيانات المكتوبة أثناء تمكين هذه الوظيفة.

ونظراً لضرورة الوصول إلى القرص الصلب، سيتم تأجيل وقت الدخول في وضع توفير الطاقة.

### محو كل الذاكرة

لمسح جميع البيانات الموجودة على القرص الصلب. لا يمكنك إجراء عمليات أخرى أو إيقاف تشغيل الجهاز أثناء التنسيق.

سرعة عالية: لمسح جميع البيانات بأمر مسح مخصص.

استبدال: لمسح جميع البيانات بأمر مسح مخصص، ولاستبدال البيانات الأخرى في جميع الأماكن لمسح جميع البيانات.

معلومات ذات صلة

← "ضبط الإعدادات للحذف المتسلسل" في الصفحة 81

← "تنسيق القرص الصلب الداخلي" في الصفحة 81

## ضبط الإعدادات للحذف المتسلسل

ملاحظة:

كما يمكنك أيضاً ضبط الإعدادات من لوحة التحكم بالجهاز.

1. ادخل إلى Web Config وحدد **Stored Data < Device Management**.
2. حدّد **ON** لـ **Sequential Deletion from Hard Disk**.
3. انقر فوق **OK**.

## تنسيق القرص الصلب الداخلي

1. اضغط على الإعدادات على الشاشة الرئيسية في لوحة التحكم بالجهاز.

## إعدادات سلامة المنتج

2. اضغط على إعدادات عامة < إدارة النظام > إعدادات محو محرك الأقراص الثابتة.
3. اضغط على محو كل الذاكرة.
4. اضغط على سرعة عالية أو استبدال حسب الغرض.
5. اضغط على نعم على شاشة التأكيد.
6. اضغط على موافق على شاشة الإكمال.


## 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 تشغيل لـ الإعدادات < 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

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

2. انقر فوق Administrator Login.

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 أحد الأجهزة

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

## إعدادات الإدارة والتشغيل

Product Status 

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

Network Status 

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

Maintenance 

تحقق من اليوم الأول للمطبوعات، وعدد استبدال الحبر، والصفحات المطبوعة، وعدد المطبوعات لكل لغة، وعدد الملفات المحسوحة ضوئياً، وما إلى ذلك.

Hardware Status 

تحقق من حالة كل ماسحة ضوئية وميزة الفاكس.

Job History 

تحقق من سجل المهام الخاص بمهمة الطباعة، ومهمة الاستلام، ومهمة الإرسال.

Panel Snapshot 

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

## معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## إدارة الأجهزة (Epson Device Admin)

يمكنك إدارة العديد من الأجهزة وتشغيلها باستخدام Epson Device Admin. يسمح لك Epson Device Admin بإدارة الأجهزة الموجودة في شبكة مختلفة. يحدد ما يلي ميزات الإدارة الرئيسية.

للحصول على مزيد من المعلومات بشأن الوظائف، واستخدام البرنامج، اطلع على مستندات Epson Device Admin أو تعليماته.

اكتشاف الأجهزة 

يمكنك اكتشاف الأجهزة الموجودة على الشبكة، ثم سجلها في إحدى القوائم. إذا اتصلت أجهزة Epson مثل الطابعات والمساحات الضوئية بمقطع الشبكة نفسه المتصل به كمبيوتر المسؤول، فيمكنك العثور عليها حتى إذا لم يتم تعيين عنوان IP لها.

يمكنك أيضاً اكتشاف الأجهزة التي تتصل بأجهزة الكمبيوتر الموجودة على الشبكة باستخدام كابل USB. يجب تثبيت Epson Device USB Agent على الكمبيوتر.

إعداد الجهاز 

يمكنك إنشاء قالب يحتوي على عناصر الإعداد مثل واجهة الشبكة ومصدر الورق، وتطبيقها على الأجهزة الأخرى كإعدادات مشاركة. عند توصيله بالشبكة، يمكنك تعيين عنوان IP على جهاز لم يتم تعيين عنوان IP له.

مراقبة الأجهزة 

يمكنك الحصول على معلومات حول الحالة والمعلومات التفصيلية بانتظام للأجهزة الموجودة على الشبكة. يمكنك أيضاً مراقبة الأجهزة المتصلة بأجهزة الكمبيوتر على الشبكة بواسطة كابلات USB والأجهزة التابعة لشركات أخرى التي تم تسجيلها بقائمة الجهاز. لمراقبة الأجهزة المتصلة بواسطة كابلات USB، عليك تثبيت Epson Device USB Agent.

إدارة التنبيهات 

يمكنك مراقبة التنبيهات الخاصة بحالة الأجهزة والعناصر المستهلكة. يرسل النظام رسائل بريد إلكتروني للإعلام تلقائياً إلى المسؤول حسب الحالات المعنية.

إدارة التقارير 

يمكنك إنشاء تقارير منتظمة لأن النظام يخزن البيانات المتعلقة باستخدام الجهاز والعناصر المستهلكة. يمكنك بعد ذلك حفظ هذه التقارير التي تم إنشاؤها وإرسالها بالبريد الإلكتروني.

## استلام إعلانات البريد الإلكتروني عند وقوع أحداث

### حول إشعارات البريد الإلكتروني

يمكنك استخدام هذه الميزة لاستلام تنبيهات بالبريد الإلكتروني عند حدوث بعض الأحداث، مثل نفاذ الورق من طابعتك. يمكنك تسجيل حتى 5 عناوين بريد إلكتروني واختيار الأحداث التي ترغب في استلام إشعاراتها. يجب تكوين خادم البريد الإلكتروني لاستخدام هذه الميزة.

### تكوين إشعارات البريد الإلكتروني

لاستخدام الميزة، يجب أن تقوم بتكوين خادم البريد الإلكتروني.

1. ادخل إلى Web Config وحدد علامة التبويب **Email Notification < Device Management**.
2. أدخل عنوان البريد الإلكتروني الذي ترغب في استلام إشعارات البريد الإلكتروني الخاصة به.
3. حدد لغة إشعارات البريد الإلكتروني.

## إعدادات الإدارة والتشغيل

4. حدد مربعات الإشعارات التي ترغب في استلامها.

**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	2	3	4	5
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 type="checkbox"/>	<input checked="" 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

5. انقر فوق OK.

معلومات ذات صلة

- ◀ "الوصول إلى تطبيق Web Config" في الصفحة 37
- ◀ "تكوين خادم البريد" في الصفحة 31

## تحديث البرنامج الثابت

### تحديث البرامج الثابتة للطابعة باستخدام لوحة التحكم

يمكنك تحديث البرامج الثابتة للطابعة باستخدام لوحة التحكم في حالة اتصال الطابعة بشبكة الإنترنت. يمكنك أيضاً ضبط الطابعة للتحقق بانتظام من توافر تحديثات للبرامج الثابتة وإشعارك عند توافر أي تحديثات.

1. اضغط على الإعدادات على الشاشة الرئيسية.

2. اضغط على إعدادات عامة > إدارة النظام > تحديث البرامج الثابتة.

ملاحظة:

اضغط على إشعار > تشغيل لضبط الطابعة للتحقق بانتظام من وجود تحديثات متوفرة للبرامج الثابتة.

## إعدادات الإدارة والتشغيل

3. اضغط على بدء التحقق.
- تبدأ الطابعة في البحث عن التحديثات المتوفرة.
4. إذا أبلغتك 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

لتحديث البرنامج الثابت باستخدام Web Config. يجب توصيل الجهاز بالإنترنت.

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**، واتباع 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 37

◀ "Epson Device Admin" في الصفحة 101

## تحديث البرنامج الثابت عن طريق استخدام Epson Firmware Updater

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 بالجهاز 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 جهات الاتصال والإعدادات احتياطياً

عن طريق تصدير عناصر الإعداد على Web Config، يمكنك نسخ العناصر إلى الطابعات الأخرى.

### تصدير الإعدادات

تصدير كل إعداد للطابعة.

1. ادخل إلى Web Config ثم حدد علامة التبويب **Device Management < Export and Import Setting Value < Export**.
2. حدّد الإعدادات التي تريد تصديرها.
3. 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.
- حيث تحتاج إلى كلمة مرور لاستيراد الملف. أو اتركها فارغة إذا لم ترغب في تشفيره.
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 37

### 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 حدد 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. حدد الإعدادات التي تريد استيرادها، ثم انقر فوق **Next**.
  5. انقر فوق **OK**.
- تم تطبيق الإعدادات على الطابعة.



## حل المشكلات

### تلميحات لحل المشكلات

يمكنك معرفة المزيد من المعلومات في الأدلة التالية.

□ دليل المستخدم

بتعليقات حول استخدام الطابعة، واستبدال وحدة التزويد بالحبر، والصيانة، وحل المشكلات.

□ موقع ويب Epson Connect

<https://www.epsonconnect.com/>

يقدم معلومات حول ميزات Epson Connect وحل المشكلات.

### فحص سجل الخادم وجهاز الشبكة

إذا حدثت مشكلة في اتصال الشبكة، فقد تكون قادراً على تحديد السبب عن طريق فحص سجل خادم البريد الإلكتروني أو خادم LDAP أو الحالة باستخدام سجل النظام الخاص بجهاز الشبكة، مثل جهاز التوجيه، أو الأوامر.

### تهيئة إعدادات الشبكة

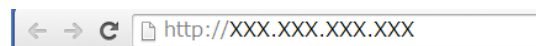
#### تعطيل Wi-Fi من تهيئة الويب

لاستخدام Web Config، ينبغي أن تحتوي الطابعات والأجهزة على عنوان IP ليتم توصيله بنفس الشبكة.

1. افحص عنوان IP الخاص بالطابعة.

يمكنك التحقق من هذا من شاشة حالة الشبكة على لوحة تحكم الطابعة، أو تقرير الاتصال، أو عمود [عنوان IP] لورقة حالة الشبكة.

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



3. حدد علامة التبويب **Wi-Fi < Network**، ثم حدد **Disable Wi-Fi**.

4. تحقق من الرسالة، ثم حدد موافق.

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

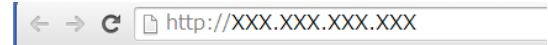
لاستخدام Web Config، ينبغي أن تحتوي الطابعات والأجهزة على عنوان IP ليتم توصيله بنفس الشبكة.

1. افحص عنوان IP الخاص بالطابعة.

يمكنك التحقق من هذا من شاشة حالة الشبكة على لوحة تحكم الطابعة، أو تقرير الاتصال، أو عمود [عنوان IP] لورقة حالة الشبكة.

## حل المشكلات

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



3. حدد علامة التبويب **Wi-Fi Direct < Network**.

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

5. انقر فوق **Next**.

6. 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  على الشاشة الرئيسية.

2. اضغط على راوتر.

يتم عرض حالة الشبكة.

3. اضغط على بدء الإعداد.

4. اضغط على إعداد Wi-Fi.

5. اضغط على أخرى < تعطيل Wi-Fi.

6. تحقق من الرسالة، ثم اضغط على بدء الإعداد.

7. عندما تظهر رسالة الاكتمال، اضغط على إغلاق.

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

## فصل اتصال Wi-Fi Direct (نقطة الوصول البسيطة) من لوحة التحكم

ملاحظة:

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

1. اضغط على  على الشاشة الرئيسية.

2. اضغط على **Wi-Fi Direct**.

يتم عرض معلومات **Wi-Fi Direct**.

3. اضغط على بدء الإعداد.

4. اضغط على تعطيل **Wi-Fi Direct**.

5. تحقق من الرسالة، ثم اضغط على تعطيل الإعدادات.

## حل المشكلات

6. عندما تظهر رسالة الاكتمال، اضغط على إغلاق.  
تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بالضغط على إغلاق.

## استعادة إعدادات الشبكة من لوحة التحكم

يمكنك استعادة جميع إعدادات الشبكة إلى الأوضاع الافتراضية.

1. اضغط على الإعدادات على الشاشة الرئيسية.
2. اضغط على إعدادات عامة < إدارة النظام < استعادة الإعدادات الافتراضية < إعدادات الشبكة.
3. تحقق من الرسالة، ثم اضغط على نعم.
4. عندما تظهر رسالة الاكتمال، اضغط على إغلاق.  
تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بالضغط على إغلاق.

## 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 أدناه للتحقق من الاتصال باستخدام أمر Ping.

1. تحقق من عنوان IP الخاص بوحدة الطباعة للاتصال الذي تريد 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.  
Windows 10/Windows Server 2016   
انقر بزر الماوس الأيمن فوق زر البدء، أو اضغط عليه مع الاستمرار، ثم حدد موجة الأوامر.  
Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012   
عرض شاشة التطبيق، ثم اختر موجة الأوامر.  
Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008   
اضغط على زر إبدأ، وحدد جميع البرامج أو البرامج < الملاحظات < موجة الأوامر.
3. أدخل "ping xxx.xxx.xxx.xxx"، ثم اضغط على مفتاح الإدخال.  
أدخل عنوان IP الخاص بالطابعة لـ xxx.xxx.xxx.xxx.

## حل المشكلات

4. تحقق من حالة الاتصال.

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

```

Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X: bytes=32 time=87ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=86ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=311ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=117ms TTL=64

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 86ms, Maximum = 311ms, Average = 150ms

C:\>

```

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

```

Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>_

```

## تحقق من الاتصال باستخدام أمر Ping — Mac OS

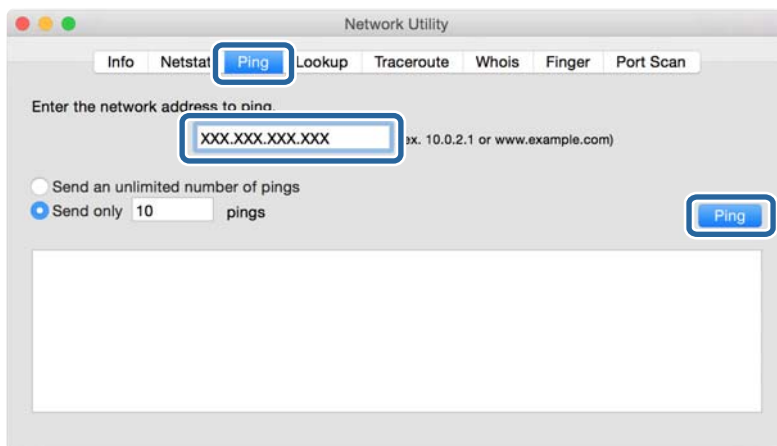
يُمكنك استخدام أمر Ping للتأكد من اتصال الحاسوب بالطابعة. اتبع الخطوات أدناه للتحقق من الاتصال باستخدام أمر Ping.

1. تحقق من عنوان IP الخاص بوحدة الطباعة للاتصال الذي تريد التحقق منه.

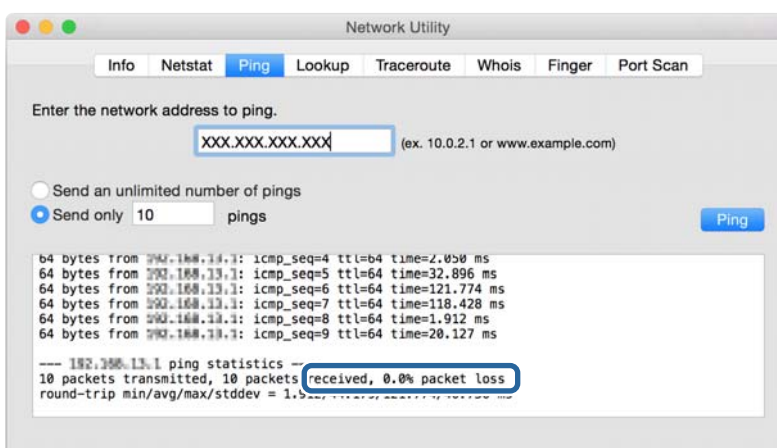
يمكنك التحقق من هذا من شاشة حالة الشبكة على لوحة تحكم الطباعة، أو تقرير الاتصال، أو عمود IP Address لورقة حالة الشبكة.

## حل المشكلات

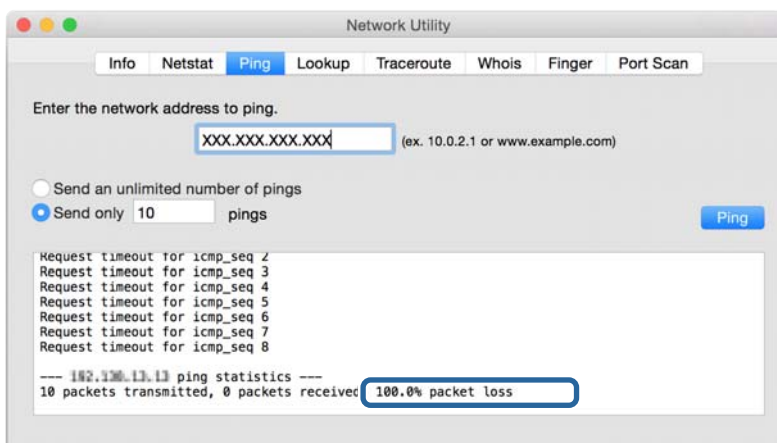
2. تشغيل أداة مساعدة للشبكة.  
أدخل "أداة مساعدة للشبكة" في Spotlight.
3. اضغط على علامة Ping، أدخل عنوان IP الذي قمت بالتحقق منه في الخطوة رقم 1 ثم اضغط على Ping.



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



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



## طباعة تقرير الاتصال بالشبكة

يمكنك طباعة تقرير اتصال شبكة ما للتحقق من حالة الاتصال بين الطابعة ونقطة الوصول.

1. قم بتحميل الورق.
2. اضغط على الإعدادات على الشاشة الرئيسية.
3. اضغط على إعدادات عامة > إعدادات الشبكة > التحقق من الاتصال.  
يبدأ فحص الاتصال.
4. اضغط على طباعة تقرير الفحص.
5. اضغط على ابدأ الطباعة لطباعة تقرير الاتصال بالشبكة.  
إذا حدث خطأ، فتتحقق من تقرير الاتصال بالشبكة، ثم اتبع الحلول المطبوعة.
6. اضغط على إغلاق.  
تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بالضغط على إغلاق.

معلومات ذات صلة

← "الرسائل والحلول الخاصة بتقرير اتصال الشبكة" في الصفحة 95

## 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-7)

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	PASS
Communication Mode Check	PASS
Security Mode Check	PASS
MAC Address Filtering Check	PASS
Security Key/Password Check	FAIL
IP Address Check	Unchecked
Detailed IP Setup Check	Unchecked

Network Status

Printer Model	XX-XXX XXX Series
IP Address	0.0.0.0
Subnet Mask	255.255.255.0
Default Gateway	
Network Name (SSID)	XXXXXXXXXXXX
Communication Mode	WPA2-PSK (AES)
Signal Strength	Poor
MAC Address	44:D2:44:DA:C0:43

أ- رمز الخطأ

ب- رسائل حول بيئة الشبكة

أ- رمز الخطأ

الرمز	الحل
E-1	<input type="checkbox"/> تأكد من اتصال كابل الإيثرنت بالطابعة، أو موزع الشبكة، أو أجهزة الشبكة الأخرى. <input type="checkbox"/> تأكد من تشغيل موزع الشبكة أو أجهزة الشبكة الأخرى.

## حل المشكلات

الرمز	الحل
E-2	<input type="checkbox"/> تأكد من تشغيل نقطة الوصول.
E-3	<input type="checkbox"/> تحقق من اتصال الحاسوب أو الأجهزة الأخرى بنقطة الوصول بشكل صحيح.
E-7	<input type="checkbox"/> ضع الطابعة بالقرب من نقطة الوصول. قم بإزالة أي عوائق بينهما.
	<input type="checkbox"/> إذا قمت بإدخال SSID بشكل يدوي، فتتحقق من صحته. تحقق من SSID من خلال الجزء الخاص بـ <b>Network Status</b> بتقرير اتصال الشبكة.
	<input type="checkbox"/> لإنشاء شبكة من خلال الضغط على زر الإعداد، عليك التأكد من أن نقطة الوصول تدعم WPS. إذا كانت لا تدعم WPS، فلن يمكنك إنشاء شبكة من خلال الضغط على زر الإعداد.
	<input type="checkbox"/> تأكد من استخدام أحرف ASCII (حروف ورموز أبجدية رقمية) فقط لـ SSID. لا تستطيع الطابعة عرض SSID الذي يحتوي على أي أحرف مخالفة لأحرف ASCII.
	<input type="checkbox"/> تحقق من معرف خدمة الشبكة وكلمة المرور قبل الاتصال بنقطة الوصول. إذا كنت تستخدم نقطة وصول مع الإعدادات الافتراضية الخاصة بها، فستجد معرف الشبكة وكلمة المرور على الملصق. إذا كنت تجهل معرف الشبكة وكلمة المرور، فاتصل بالشخص الذي قام بإعداد نقطة الوصول، أو راجع الوثائق المرفقة مع نقطة الوصول.
	<input type="checkbox"/> عندما تريد الاتصال بمعرف خدمة الشبكة المنتج باستخدام وظيفة الربط على جهاز ذكي، تحقق من معرف خدمة الشبكة وكلمة المرور في الوثائق المرفقة مع الجهاز الذكي.
	<input type="checkbox"/> إذا تم قطع اتصال شبكة Wi-Fi فجأة، فتتحقق مما يلي. إذا كان أي من تلك الأشياء قابلاً للتطبيق، فقم بإعادة ضبط إعدادات الشبكة باستخدام الملصق. يمكنك تشغيله من خلال الموقع الإلكتروني التالي. <a href="http://epson.sn">http://epson.sn</a> < الإعداد
	<input type="checkbox"/> تمت إضافة جهاز ذكي آخر على شبكة الإنترنت من خلال الضغط على زر الإعداد.
	<input type="checkbox"/> تم إعداد شبكة Wi-Fi باستخدام أي طريقة أخرى تختلف عن الضغط على زر الإعداد.
E-5	تأكد من ضبط نوع الأمان الخاص بنقطة الوصول على أحد الخيارات التالية. إذا لم يتم ضبطه على هذا النحو، فقم بتغيير نوع الأمان في نقطة الوصول ثم قم بإعادة ضبط إعدادات شبكة الطابعة. <input type="checkbox"/> WEP-64 بت (40 بت) <input type="checkbox"/> WEP-128 بت (104 بت) <input type="checkbox"/> (WPA PSK (TKIP/AES)* <input type="checkbox"/> (WPA2 PSK (TKIP/AES)* <input type="checkbox"/> (WPA (TKIP/AES <input type="checkbox"/> (WPA2 (TKIP/AES * : يعرف أيضاً WPA PSK باسم WPA الشخصي. يعرف أيضاً WPA2 PSK باسم WPA2 الشخصي.
E-6	<input type="checkbox"/> تأكد من تعطيل تصفية عنوان MAC. إذا كان مفعلاً، فقم بتسجيل عنوان MAC الخاص بالطابعة حتى لا تتم تصفيته. انظر الوثائق المرفقة مع نقطة الوصول للحصول على التفاصيل. يمكنك التحقق من عنوان MAC من خلال الجزء الخاص بـ <b>Network Status</b> بتقرير اتصال الشبكة. <input type="checkbox"/> إذا تم تفعيل المصادقة الخاصة بنقطة الوصول التي تمت مشاركتها في طريقة الأمان الخاصة بـ WEP، فتأكد من صحة مفتاح المصادقة ومؤشرها.
E-8	<input type="checkbox"/> قم بتمكين وظيفة DHCP في نقطة الوصول عند ضبط عنوان IP الذي تم الحصول عليه للطابعة على التشغيل التلقائي. <input type="checkbox"/> إذا تم ضبط التشغيل اليدوي لعنوان IP الذي حصلت عليه الطابعة، فإن عنوان IP الذي قمت بضبطه يدوياً يكون خارج النطاق (على سبيل المثال: 0 0 0 0) ويكون معطلاً. قم بتعيين عنوان IP صالح من لوحة التحكم بالطابعة أو Web Config.



## حل المشكلات

الرمز	الحل
E-9	<p>تحقق مما يلي.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> تم تشغيل الأجهزة.</li> <li><input type="checkbox"/> بإمكانك الدخول إلى الإنترنت وأجهزة الحاسوب، أو أجهزة الشبكة الأخرى على نفس الشبكة من الأجهزة التي ترغب في توصيلها بالطابعة.</li> </ul> <p>إذا كانت لا تعمل بعد التحقق مما ذكر أعلاه، فقم بإعادة ضبط إعدادات الشبكة باستخدام المثبت. يمكنك تشغيله من خلال الموقع الإلكتروني التالي.</p> <p><a href="http://epson.sn">http://epson.sn</a> &lt; الإعداد</p>
E-10	<p>تحقق مما يلي.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> تم تشغيل الأجهزة الأخرى على نفس الشبكة.</li> <li><input type="checkbox"/> تكون عناوين الشبكة (عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية) صحيحة إذا قمت بضبط التشغيل اليدوي لعنوان IP الذي تم الحصول عليه للطابعة.</li> </ul> <p>قم بإعادة ضبط عنوان الشبكة إذا كانت تلك الخطوات غير صحيحة. يمكنك التحقق من عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية من خلال الجزء الخاص بـ <b>Network Status</b> بتقرير اتصال الشبكة.</p> <p>عند تمكين وظيفة DHCP، قم بتغيير عنوان IP الذي تم الحصول عليه للطابعة على التشغيل التلقائي. إذا كنت تريد ضبط عنوان IP بشكل يدوي، فتحقق من عنوان IP الخاص بالطابعة من خلال الجزء الخاص بـ <b>Network Status</b> بتقرير اتصال الشبكة، ثم حدد التشغيل اليدوي من على شاشة إعدادات الشبكة. قم بضبط قناع الشبكة الفرعية على القيمة [255.255.255.0].</p>
E-11	<p>تحقق مما يلي.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> أن يكون عنوان البوابة الافتراضي صحيحاً عندما تقوم بضبط إعدادات TCP/IP الخاص بالطابعة على التشغيل اليدوي.</li> <li><input type="checkbox"/> أن يكون الجهاز الذي تم ضبطه كبوابة افتراضية قيد التشغيل.</li> </ul> <p>قم بضبط عنوان البوابة الافتراضية الصحيح. يمكنك التحقق من عنوان البوابة الافتراضية من خلال الجزء الخاص بـ <b>Network Status</b> بتقرير اتصال الشبكة.</p>
E-12	<p>تحقق مما يلي.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> تم تشغيل الأجهزة الأخرى على نفس الشبكة.</li> <li><input type="checkbox"/> صحة عناوين الشبكة (عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية) إذا قمت بإدخالها بشكل يدوي.</li> <li><input type="checkbox"/> تماثل عناوين الشبكة الخاصة بالأجهزة الأخرى (قناع الشبكة الفرعية، والبوابة الافتراضية).</li> <li><input type="checkbox"/> عدم تعارض عنوان IP مع أي أجهزة أخرى.</li> </ul> <p>إذا كانت لا تعمل حتى بعد التحقق مما ذكر أعلاه، فحاول القيام بما يلي.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> قم بضبط إعدادات الشبكة على جهاز الكمبيوتر المتصل بنفس الشبكة التي تتصل بها الطابعة باستخدام المثبت. يمكنك تشغيله من خلال الموقع الإلكتروني التالي.</li> </ul> <p><a href="http://epson.sn">http://epson.sn</a> &lt; الإعداد</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> يمكنك تسجيل العديد من كلمات المرور في نقطة الوصول التي تستخدم نوع الأمان الخاص بـ WEP. إذا تم تسجيل العديد من كلمات المرور، فتأكد من ضبط كلمة المرور الأولى المسجلة على الطابعة.</li> </ul>

## حل المشكلات

الرمز	الحل
E-13	<p>تحقق مما يلي.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> تشغيل أجهزة الشبكة مثل نقطة الوصول، وموزع الشبكة، وجهاز التوجيه.</li> <li><input type="checkbox"/> عدم ضبط TCP/IP الخاص بأجهزة الشبكة بشكل يدوي. (إذا تم ضبط إعدادات TCP/IP الخاصة بالطابعة تلقائياً أثناء إجراء ضبط TCP/IP الخاص بأجهزة الشبكة الأخرى بشكل يدوي، فقد تختلف شبكة الطابعة عن الشبكة الخاصة بالأجهزة الأخرى).</li> </ul> <p>إذا كانت لا تعمل حتى بعد التحقق مما ذكر أعلاه، فحاول القيام بما يلي.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> قم بضبط إعدادات الشبكة على جهاز الكمبيوتر المتصل بنفس الشبكة التي تتصل بها الطابعة باستخدام المثبت. يمكنك تشغيله من خلال الموقع الإلكتروني التالي. <a href="http://epson.sn">http://epson.sn</a> &lt; الإعداد</li> <li><input type="checkbox"/> يمكنك تسجيل العديد من كلمات المرور في نقطة الوصول التي تستخدم نوع الأمان الخاص بـ WEP. إذا تم تسجيل العديد من كلمات المرور، فتأكد من ضبط كلمة المرور الأولى المسجلة على الطابعة.</li> </ul>

## ب- رسائل حول بيئة الشبكة

الرسالة	الحل
*Multiple network names (SSID) that match your entered network name (SSID) have been detected. Confirm network name (SSID).	يمكن ضبط نفس SSID على العديد من نقاط الوصول. تحقق من الإعدادات في نقاط الوصول، وقم بتغيير SSID.
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 نقطة الوصول، وإزالة أي عوائق بين نقطة الوصول والطابعة، قم بتشغيل نقطة الوصول. إذا ظلت غير متصلة، فراجع الوثائق المرفقة مع نقطة الوصول.
*No more devices can be connected. Disconnect one of the connected devices if you want to add another one.	يمكنك توصيل حتى أربعة أجهزة من أجهزة الكمبيوتر والأجهزة الذكية من خلال الاتصال بشبكة Wi-Fi Direct (نقطة الوصول البسيط) بشكل متزامن. لإضافة جهاز كمبيوتر أو جهاز ذكي آخر، قم أولاً بفصل أحد الأجهزة المتصلة.

## طباعة ورقة حالة الشبكة

يمكنك التحقق من المعلومات المفصلة حول الشبكة عن طريق طباعتها.

1. قم بتحميل الورق.
  2. اضغط على الإعدادات على الشاشة الرئيسية.
  3. اضغط على إعدادات عامة < إعدادات الشبكة > حالة الشبكة.
  4. اضغط على ورقة حالة الطباعة.
  5. تحقق من الرسالة، ثم اضغط على إبدأ الطباعة.
  6. اضغط على إغلاق.
- تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بالضغط على إغلاق.

## المشكلات الخاصة باستخدام برنامج الشبكة

### يتعذر الوصول إلى تطبيق Web Config

هل تم تكوين عنوان IP الخاص بالطابعة بشكل صحيح؟

قم بتكوين عنوان IP باستخدام تطبيق EpsonNet Config أو لوحة تحكم الطابعة. يمكنك التأكد من معلومات الإعداد الحالية باستخدام ورقة حالة الشبكة أو من لوحة تحكم الطابعة.

هل مستعرضك يدعم تشفيرات مجموعة بيانات Encryption Strength الخاصة بـ SSL/TLS؟

تشفيرات مجموعة بيانات Encryption Strength الخاصة بـ SSL/TLS على النحو التالي. لا يمكن الوصول إلى تطبيق Web Config إلا من خلال مستعرض يدعم تشفيرات مجموعة البيانات التالية. 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

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

إذا كانت الشهادة منتهية الصلاحية، فاحصل على الشهادة مرةً أخرى. إذا كانت الرسالة تظهر قبل تاريخ انتهاء صلاحية الشهادة، فتأكد من تكوين تاريخ الطابعة بشكل صحيح.

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

لا يتطابق عنوان IP الخاص بالطابعة المدخل لإعداد Common Name من أجل إنشاء شهادة موقعة ذاتياً أو طلب CSR مع العنوان المدخل في المستعرض. احصل على شهادة وقم باستيرادها مرةً أخرى أو قم بتغيير اسم الطابعة.

يتم الوصول إلى الطابعة من خلال خادم وكيل.

إذا كنت تستخدم خادمًا وكيلًا مع الطابعة، فلا بد أن تقوم بتكوين إعدادات الوكيل في المستعرض لديك.

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

192.168.\*.\*: العنوان المحلي 192.168.XXX.XXX، قناع الشبكة الفرعية 255.255.0.0

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "تعيين عنوان IP" في الصفحة 17

← "تعيين عنوان IP باستخدام" في الصفحة 102 EpsonNet Config

## حل المشكلات

## لا يتم عرض اسم الطراز و/أو عنوان IP على تطبيق EpsonNet Config

هل قمت بتحديد حظر أو إلغاء أو إيقاف التشغيل عند عرض شاشة أمان Windows أو شاشة جدار حماية؟

إذا قمت بتحديد حظر، أو إلغاء، أو إيقاف تشغيل، فلن يتم عرض عنوان IP واسم الطراز على تطبيق EpsonNet Config أو تطبيق EpsonNet Setup.

لتصحيح هذا الأمر، قم بتسجيل تطبيق EpsonNet Config بمثابة استثناء باستخدام جدار حماية Windows وبرنامج أمان تجاري. إذا كنت تستخدم برنامجاً مضاداً للفيروسات أو برنامج أمان، فأغلقه ثم حاول استخدام تطبيق EpsonNet Config.

هل إعداد انقضاء مهلة خطأ الاتصال قصير للغاية؟

قم بتشغيل تطبيق EpsonNet Config وحدد أدوات < خيارات > المهلة ثم قم بزيادة طول الوقت لإعداد خطأ في الاتصال. لاحظ أن القيام بهذا يمكن أن يؤدي إلى تشغيل تطبيق EpsonNet Config ببطء أكبر.

## معلومات ذات صلة

← "تشغيل تطبيق EpsonNet Config — في الصفحة 101 Windows

← "تشغيل تطبيق EpsonNet Config — في الصفحة 102 Mac OS

## ملحق

### تقديم برنامج الشبكة

يوضح ما يلي البرنامج الذي يكوّن الأجهزة ويديرها.

#### Epson Device Admin

Epson Device Admin تطبيق يتيح لك تثبيت الأجهزة على الشبكة، ومن ثم تهيئة الأجهزة وإدارتها. يمكنك الحصول على معلومات تفصيلية عن الجهاز مثل الحالة والعناصر المستهلكة، وإرسال إعلانات التنبيهات، وإنشاء تقارير لاستخدام الجهاز. يمكنك أيضاً إنشاء قالب يحتوي على عناصر الإعداد وتطبيقها على الأجهزة الأخرى كإعدادات مشاركة. 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

يتيح تطبيق EpsonNet Config للمسؤول تكوين إعدادات شبكة الطابعة، مثل تعيين عنوان IP وتغيير وضع الاتصال. يتم دعم ميزة الإعداد الدفعي على نظام التشغيل Windows. لمزيد من المعلومات، انظر الوثائق أو التعليمات الخاصة بتطبيق EpsonNet Config.



#### تشغيل تطبيق EpsonNet Config Windows

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

## ملحق

## 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 Config.

## EpsonNet Print (Windows فقط)

EpsonNet Print هو برنامج للنسخ على شبكة TCP/IP. 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 الطابعة 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.

## تعيين عنوان IP باستخدام EpsonNet Config

يمكنك تعيين عنوان IP للطابعة باستخدام EpsonNet Config. يسمح لك EpsonNet Config بتعيين عنوان IP للطابعة التي لم يتم تعيين أي عنوان لها بعد الاتصال باستخدام كابل إيثرنت. عند الاتصال بشبكة Wi-Fi، قم بالاتصال بالإنترنت مرة، ثم غير الاتصال بشبكة Wi-Fi.

## تعيين عنوان IP باستخدام الإعدادات الدفعية

## إنشاء ملف للإعدادات الدفعية

باستخدام عنوان MAC واسم الطراز باعتبارهما مفاتيح، يمكنك إنشاء ملف SYLK جديد لتعيين عنوان IP.

عند توصيل الطابعة بشبكة Wi-Fi، قم بتعيين عنوان IP عن طريق اتباع الإجراءات، ثم غير الاتصال بشبكة Wi-Fi.

1. افتح تطبيق جداول البيانات (مثل Microsoft Excel) أو محرر نص.

2. أدخل "Info\_MACAddress"، و"Info\_ModelName"، و"TCPIP\_IPAddress" في الصف الأول باعتبارها أسماء عناصر الإعداد.

أدخل عناصر الإعداد للسلاسل النصية التالية. للتفريق بين الأحرف الكبيرة/الأحرف الصغيرة والأحرف مزدوجة البايت/ذات البايت الواحد، إذا كان هناك حرف واحد مختلفاً، فلن يتم التعرف على العنصر.

أدخل اسم عنصر الإعداد كما هو موضح أدناه، وإلا فلا يمكن أن يتعرف EpsonNet Config على عناصر الإعداد.

## ملحق

TCPIP_IPAddress	Info_ModelName	Info_MACAddress

3. أدخل عنوان MAC، واسم الطراز، وعنوان IP لكل واجهة شبكة.

TCPIP_IPAddress	Info_ModelName	Info_MACAddress
192.168.100.102	ALC-XXXXX	0000XXXX0001
192.168.100.103	ALC-XXXXX	0000XXXX0002
192.168.100.104	ALC-XXXXX	0000XXXX0003

4. أدخل اسماً ثم قم بحفظ ملف بصيغة SYLK (\*.slk).

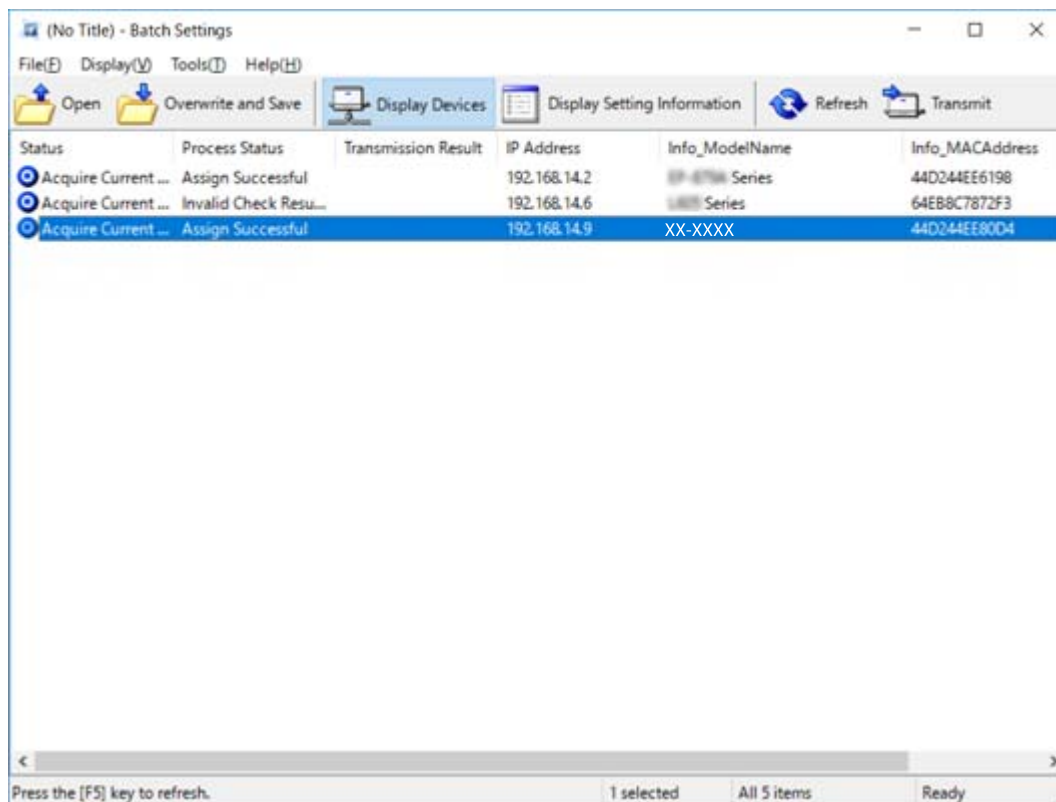
### ضبط الإعدادات الدفعية باستخدام ملف التكوين

عين عناوين IP في ملف التكوين (ملف SYLK) في وقت واحد. عليك إنشاء ملف التكوين قبل بدء التعيين. عند توصيل الطابعة بشبكة Wi-Fi، قم بتعيين عنوان IP عن طريق اتباع الإجراءات، ثم غير الاتصال بشبكة Wi-Fi.

1. قم بتوصيل جميع الأجهزة بالشبكة باستخدام كابل إيثرنت.
2. قم بتشغيل الطابعة.
3. ابدأ تشغيل EpsonNet Config.
4. انقر فوق أدوات > إعدادات الدفعية.
5. انقر فوق فتح.
6. على شاشة تحديد الملف، حدد ملف SYLK (\*.slk) الذي يحتوي على الإعدادات، ثم انقر فوق فتح.

## ملحق

7. حدد الأجهزة التي ترغب في إجراء الإعدادات الدفعية لها مع تعيين العمود الحالة على غير معين، وتعيين حالة العملية على نجاح التعيين.  
عندما تقوم بإجراء عدة تحديدات، اضغط على Ctrl أو Shift وانقر عليها أو اسحب بالماوس.

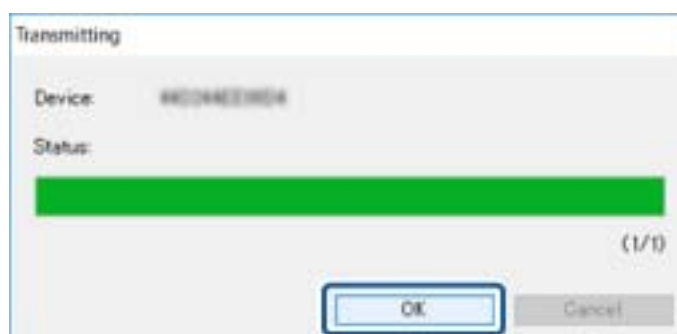


8. انقر فوق إرسال.

9. عند عرض شاشة إدخال كلمة المرور، أدخل كلمة المرور، ثم انقر فوق موافق.  
إرسال الإعدادات.

**هام:** يتم إرسال المعلومات إلى واجهة الشبكة حتى يكتمل مقياس التقدم. لا توقف تشغيل الجهاز أو مهائئ اللاسلكي، ولا تقم بإرسال أي بيانات إلى الجهاز.

10. على شاشة إعدادات الإرسال انقر فوق موافق.





## ملحق

11. تحقق من حالة الجهاز الذي تقوم بتعيينه.

للأجهزة التي توضح  أو ، تحقق من محتويات ملف الإعدادات، أو إعادة تشغيل الجهاز بشكل عادي.

الرمز	الحالة	حالة العملية	الشرح
	إكمال الإعداد	نجاح الإعداد	تم إكمال الإعداد بشكل عادي.
	إكمال الإعداد	إعادة التشغيل	عندما يتم إرسال المعلومات، يجب إعادة تشغيل كل جهاز لتمكين الإعدادات. يتم إجراء عملية التحقق لتحديد ما إذا كان يمكن الاتصال بالجهاز بعد إعادة التشغيل أم لا.
	إكمال الإعداد	فشل إعادة تشغيل	تعذر تأكيد الجهاز بعد إرسال الإعدادات. تحقق من تشغيل الجهاز، أو إذا تمت إعادة تشغيله.
	إكمال الإعداد	جارِ البحث	البحث عن الجهاز الذي يُشار إليه في ملف الإعدادات.*
	إكمال الإعداد	فشل البحث	تعذر التحقق من الأجهزة التي يتم إعدادها بالفعل. تحقق من تشغيل الجهاز، أو إذا تمت إعادة تشغيله.*

\* عندما يتم عرض معلومات الإعداد فقط.

## معلومات ذات صلة

- ← "تشغيل تطبيق EpsonNet Config — في الصفحة Windows101"
- ← "تشغيل تطبيق EpsonNet Config — في الصفحة Mac OS102"

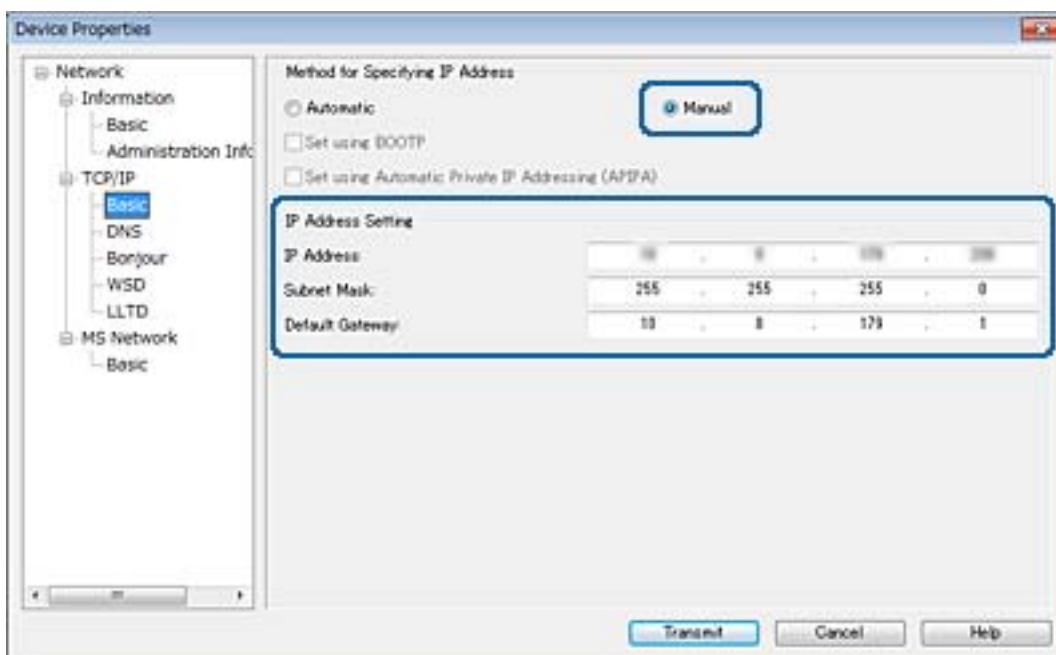
## تعيين عنوان IP لكل جهاز

عينَ عنوان IP للطابعة باستخدام EpsonNet Config.

1. قم بتشغيل الطابعة.
2. قم بتوصيل الطابعة بالشبكة باستخدام كابل إيثرنت.
3. ابدأ تشغيل EpsonNet Config.  
يتم عرض قائمة بالطابعات الموجودة على الشبكة. قد يستغرق الأمر فترة من الوقت قبل عرضها.
4. انقر نقرًا مزدوجًا فوق الطابعة التي تريد تعيين لها.  
ملاحظة:  
إذا قمت بتوصيل عدة طابعات من الطراز نفسه، يمكنك تحديد الطابعة باستخدام عنوان MAC.
5. حدد الشبكة < TCP/IP < أساسي.

## ملحق

6. أدخل العناوين لـ عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية.



## ملاحظة:

أدخل عنواناً ثابتاً عند توصيل الطابعة بشبكة آمنة.

7. انقر فوق إرسال.

تظهر شاشة تأكيد إرسال المعلومات.

8. انقر فوق موافق.

تظهر شاشة استكمال الإرسال.

## ملاحظة:

يتم إرسال المعلومات إلى الجهاز، ثم تظهر رسالة "تم استكمال التكوين بنجاح". لا توقف تشغيل الجهاز، ولا تقم بإرسال أي بيانات إلى الخدمة.

9. انقر فوق موافق.

## معلومات ذات صلة

← تشغيل تطبيق EpsonNet Config — في الصفحة 101 Windows

← تشغيل تطبيق EpsonNet Config — في الصفحة 102 Mac OS

## 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 إعداد زر الضغط (WPS)" في الصفحة 107

← "ضبط إعدادات Wi-Fi عن طريق إعداد رمز تعريف الشخصي (WPS)" في الصفحة 108

## ملحق

## ضبط إعدادات Wi-Fi عن طريق إعداد زر الضغط (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  |  على الشاشة الرئيسية.

2. اضغط على راوتر.

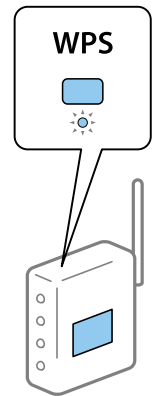
3. اضغط على بدء الإعداد.

4. اضغط على إعدادات Wi-Fi.

إذا قمت بضبط إعدادات الإيثرنت، فتتحقق من الرسالة ثم اضغط على نعم.

5. اضغط على إعداد زر الأمر (WPS).

6. اضغط باستمرار على زر [WPS] في نقطة الوصول حتى وميض ضوء الحماية.



إذا كنت لا تعرف مكان الزر [WPS]، أو إذا لم يكن هناك أي أزرار في نقطة الوصول، فراجع الوثائق المرفقة مع نقطة الوصول لمعرفة التفاصيل.

7. اضغط على بدء الإعداد.

8. اضغط على إغلاق.

تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بالضغط على 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 بالشبكة وتحقق من الحل.

9. اضغط على إغلاق على شاشة إعدادات اتصال الشبكة.

## 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  |  على الشاشة الرئيسية.
2. اضغط على راوتر.
3. اضغط على بدء الإعداد.
4. اضغط على إعداد Wi-Fi.
- إذا قمت بضبط إعدادات الإيثرنت، فتتحقق من الرسالة ثم اضغط على نعم.
5. اضغط على أخرى < إعداد رمز PIN (WPS)
6. 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.
7. اضغط على بدء الإعداد.
8. اضغط على إغلاق.
- تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بالضغط على 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.
9. اضغط على إغلاق على شاشة إعدادات اتصال الشبكة.

## 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.

## معلومات ذات صلة

- ← "تغيير الاتصال من الاتصال بشبكة إيثرنت إلى الاتصال بشبكة Wi-Fi" في الصفحة 109
- ← "تغيير الاتصال من الاتصال بشبكة Wi-Fi إلى اتصال الإيثرنت" في الصفحة 109

## ملحق

## 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

← "ضبط إعدادات Wi-Fi يدوياً من خلال لوحة التحكم" في الصفحة 23

## التغيير إلى الاتصال بشبكة Wi-Fi باستخدام تهيئة الويب

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 *EpsonNet Config* أو *Epson Device Admin*. للحصول على مزيد من التفاصيل، راجع الدليل أو التعليمات الخاصة بكل برنامج.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "EpsonNet Config" في الصفحة 101

← "Epson Device Admin" في الصفحة 101

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

## تغيير اتصال الشبكة إلى إيثرنت باستخدام لوحة التحكم

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

1. اضغط على الإعدادات على الشاشة الرئيسية.
2. اضغط على إعدادات عامة < إعدادات الشبكة < إعداد شبكة LAN السلكية.

## ملحق

3. تحقق من الرسالة، ثم اضغط على بدء الإعداد.
4. تحقق من الرسالة، ثم اضغط على موافق.  
تغلق الشاشة تلقائياً بعد فترة زمنية محددة إذا لم تقم بالضغط على موافق.
5. وصل الطابعة بجهاز توجيه باستخدام كابل الإيثرنت.

## معلومات ذات صلة

← "الاتصال بشبكة الإيثرنت" في الصفحة 22

## 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 (جهاز التبديل L2) بكابل إيثرنت.

## ملاحظة:

يمكنك أيضاً تغيير طريقة الاتصال باستخدام *EpsonNet Config* أو *Epson Device Admin*. للحصول على مزيد من التفاصيل، راجع الدليل أو التعليمات الخاصة بكل برنامج.

## معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "EpsonNet Config" في الصفحة 101

← "Epson Device Admin" في الصفحة 101

## 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 إلى المجلد من الطابعة)	الطابعة
21				
445	(TCP) SMB	خادم الملف		
137	(UDP) NetBIOS			
138				
139	(TCP) NetBIOS			
25	(TCP) SMTP	خادم SMTP	إرسال البريد الإلكتروني (عند استخدام المسح الضوئي إلى البريد الإلكتروني من الطابعة)	
465	SMTP SSL/TLS (TCP)			
587	SMTP STARTTLS (TCP)			
110	(TCP) POP3	خادم POP	اتصال POP قبل SMTP (عند استخدام المسح الضوئي إلى البريد الإلكتروني من الطابعة)	
443	HTTPS	خادم Epson Connect	عند استخدام Epson Connect	
5222	XMPP			
443	HTTPS	خادم خدمة الطباعة السحابية من Google	عند الطباعة من خدمة الطباعة السحابية من Google	
5222	XMPP			
389	(TCP) LDAP	خادم LDAP	جمع معلومات المستخدم (استخدام جهات الاتصال من الطابعة)	
636	LDAP SSL/TLS (TCP)			
389	LDAP STARTTLS (TCP)			
88	Kerberos	خادم KDC	مصادقة المستخدم عند إرسال رسالة بريد إلكتروني مصادقة المستخدم عند جمع معلومات المستخدم (عند استخدام جهات الاتصال من الطابعة)	
5357	(TCP) WSD	كمبيوتر عميل	WSD التحكم	
2968	اكتشاف المسح الضوئي بالدفع على الشبكة	كمبيوتر عميل	فحص جهاز كمبيوتر في حالة المسح الضوئي بالدفع من Document Capture Pro	

## ملحق

المُرسل (العميل)	الاستخدام	الوجهة (الخادم)	البروتوكول	رقم المنفذ
كمبيوتر عميل	اكتشف الطابعة من تطبيق مثل EpsonNet Config، وبرنامج تشغيل الطابعة، وبرنامج تشغيل الماسحة الضوئية.	الطابعة	(UDP) ENPC	3289
	اجمع معلومات MIB وقم بإعدادها من تطبيق مثل EpsonNet Config، وبرنامج تشغيل الطابعة، وبرنامج تشغيل الماسحة الضوئية.	الطابعة	(UDP) SNMP	161
	إرسال بيانات LPR	الطابعة	(TCP) LPR	515
	إرسال بيانات RAW	الطابعة	(Port9100) RAW (TCP)	9100
	البحث عن طابعة WSD	الطابعة	WS-Discovery (UDP)	3702
	إعادة توجيه بيانات المسح الضوئي من Document Capture Pro	الطابعة	مسح الشبكة (TCP)	1865
	جمع معلومات المهمة في حالة المسح الضوئي بالدفع من Document Capture Pro	الطابعة	المسح الضوئي بالدفع على الشبكة	2968



# إعدادات الأمان المتقدمة لـ Enterprise

---

في هذا الفصل، نقوم بتوضيح ميزات الأمان المتقدمة.

## إعدادات الأمان ومنع وقوع المخاطر

عند توصيل جهاز بشبكة، يمكنك الوصول إليه من مكان بعيد. وبالإضافة إلى ذلك، يمكن أن يشارك العديد من الأشخاص الجهاز، الأمر الذي يُعد مفيداً في تحسين الكفاءة التشغيلية والموافقة. ومع ذلك، فإن المخاطر مثل الوصول غير القانوني، والاستخدام غير القانوني، والتلاعب بالبيانات تزداد. إذا كنت تستخدم الجهاز في بيئة يمكن فيها الوصول إلى الإنترنت، يكون معدل التعرض للمخاطر مرتفعاً جداً.

بالنسبة للأجهزة التي لم تحصل على الحماية من الخارج، فسيكون من الممكن قراءة جهات الاتصال وسجلات مهمة الطباعة المخزنة في الطباعة من الإنترنت.

لتجنب التعرض لهذه المخاطر، فإن طابعات Epson تحتوي على مجموعة متنوعة من تقنيات الأمان. عيّن الجهاز حسب الضرورة وفقاً للحالات البيئية التي تم إنشاؤها باستخدام معلومات البيئة الخاصة بالعميل.

الاسم	نوع الميزة	ما الذي يتم تعيينه	ما الذي يتم حظره
اتصالات SSL/TLS	يتم تشفير محتوى الاتصال باستخدام اتصالات SSL/TLS عند الوصول إلى خادم Epson على الإنترنت من الجهاز، مثل الاتصال بالكمبيوتر من خلال مستعرض ويب، واستخدام Epson Connect، وتحديث البرنامج الثابت.	احصل على شهادة موقعة من جهة تصديق (CA)، ثم قم باستيرادها إلى الطباعة.	يحظر مسح أي معلومات خاصة بتعريف الجهاز بالشهادة الموقعة من جهة تصديق (CA) التعرض لأي عملية اتصال والوصول غير المعتمد. وبالإضافة إلى ذلك، تتم حماية محتويات اتصال SSL/TLS، ويحظر تسريب بيانات الطباعة ومعلومات الإعداد.
التحكم في البروتوكول	للتحكم في البروتوكولات والخدمات المستخدمة للاتصال بين الأجهزة وأجهزة الكمبيوتر، ويمكن الميزات مثل الطباعة، والمسح الضوئي، وإرسال PCFAX 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 IPsec بحماية البيانات عن طريق وحدة حزمة IP (التشفير والمصادقة)، يمكنك توصيل بروتوكول المسح الضوئي والطباعة غير الآمن بسلامة.	قم بإنشاء سياسة أساسية وأخرى فردية لتعيين العميل ونوع البيانات التي يمكن أن تصل إلى الجهاز.	قم بحماية الوصول غير المعتمد، والتلاعب ببيانات الاتصال للجهاز واعتراضها.
SNMPv3	تمت إضافة ميزات مثل مراقبة الأجهزة المتصلة في الشبكة، وسلامة البيانات لبروتوكول SNMP لسبل التحكم، والتشفير، ومصادقة المستخدم، وما إلى ذلك.	مكن SNMPv3، ثم عيّن المصادقة وطريقة التشفير.	تأكد من إعدادات التغيير في الشبكة، والتزام السرية في مراقبة الحالة.
IEEE802.1X	لا يسمح إلا للمستخدم المصرح له الاتصال بشبكة Wi-Fi وإيثرنت فقط. لا يسمح إلا للمستخدم المسموح له باستخدام الجهاز فقط.	إعداد المصادقة لخادم RADIUS (خادم المصادقة).	قم بحماية الاستخدام والوصول غير المعتمد للجهاز.
النظام الأساسي المفتوح من Epson	Epson Open Platform هو عبارة عن نظام أساسي يعرض واجهة المستخدم التي يقدمها الخادم على لوحة تحكم الجهاز ويقوم بتنفيذ مهام مختلفة.	مكن Epson Open Platform على الجهاز وسجل الجهاز مع نظام المصادقة. عند استخدام جهاز المصادقة، عيّن معلومات المستخدم داخل نظام المصادقة.	يحمي من الاستخدام غير المعتمد للجهاز، والتخلص من المواد المطبوعة (المستندات السرية) أو عرضها، وتسريب المعلومات.

### معلومات ذات صلة

- ← "اتصال SSL/TLS بالطباعة" في الصفحة 115
- ← "التحكم باستخدام البروتوكولات" في الصفحة 123
- ← "الاتصال المشفر باستخدام تشفية IPsec/IP" في الصفحة 127
- ← "استخدام بروتوكول SNMPv3" في الصفحة 139

## إعدادات الأمان المتقدمة لـ Enterprise

← "توصيل الطابعة بشبكة IEEE802.1X" في الصفحة 141

← "باستخدام Epson Open Platform" في الصفحة 145

## إعدادات ميزة الأمان

عند إعداد تصفية 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 بعد والوصول غير المعتمد.

## حول المصادقة الرقمية

□ شهادة موقعة بواسطة مرجع مصدق (CA)

يجب الحصول على شهادة موقعة من مرجع مصدق (CA) من مرجع مصدق. يمكنك التأكد من تأمين الاتصالات باستخدام شهادة موقعة من مرجع مصدق. يمكنك استخدام شهادة موقعة من مرجع مصدق (CA) لكل ميزة خاصة بالأمان.

□ شهادة المرجع المصدق (CA)

تشير شهادة المرجع المصدق (CA) إلى وجود جهة خارجية تأكدت من هوية الخادم. يعد هذا الإجراء مقوماً أساسياً في نمط الأمان "الثقة في الويب". يجب الحصول على شهادة مرجع مصدق (CA) لمصادقة الخادم من المرجع المصدق الذي أصدر الشهادة.

□ شهادة موقعة ذاتياً

الشهادة الموقعة ذاتياً هي شهادة تصدرها الطابعة وتوقعها ذاتياً. تكون هذه الشهادة غير موثوقة ويتعذر عليها تجنب الاحتيال. إذا كنت تستخدم هذه الشهادة لشهادة SSL/TLS، فقد يتم عرض تنبيه أمان على المستعرض. يمكنك استخدام هذه الشهادة فقط لاتصال SSL/TLS.

## معلومات ذات صلة

← "الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها" في الصفحة 115

← "حذف شهادة موقعة من المرجع المصدق (CA)" في الصفحة 119

← "تحديث شهادة موقعة ذاتياً" في الصفحة 120

## 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** أو **Client Certificate < IEEE802.1X**.
2. انقر فوق خيار **Generate** الخاص بإعداد **CSR**.  
يتم فتح صفحة إنشاء طلب **CSR**.
3. أدخل قيمة لكل عنصر.  
**ملاحظة:**  
يتمتع طول المفاتيح 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**.  
اتبع 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

EPSON L3-10000P

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

Protocol  
CA Certificate  
Root Certificate Update  
SSL/TLS  
»Basic  
»Certificate  
IPsec/IP Filtering  
»Basic  
»Client Certificate  
IEEE802.1X  
»Basic  
»Client Certificate

**SSL/TLS > Certificate**

Key Length : RSA 2048bit - SHA-256

Common Name : EPSON/10.152.12.225/EPSON/10.152.12.225

Organization :

Organizational Unit :

Locality :

State/Province :

Country :

OK Back

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. مثال: عنوان URL للوصول إلى: httpsWeb Config: 10.152.12.225// اسم شائع: 10.152.12.225
/Organizational Unit /Organization State/Province /Locality	يمكنك إدخال ما بين 0 إلى 64 رمزاً 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 115

## استيراد شهادة موقعة من المرجع المصدق (CA)

هام!

تأكد من تعيين تاريخ الطابعة ووقتها بشكل صحيح.

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 *Certificate < SSL/TLS*، أو *IPsec/IP Filtering* *Client Certificate < IEEE802.1X* أو *Client Certificate*.

2. انقر فوق **Import**

يتم فتح صفحة استيراد شهادة.

3. أدخل قيمة لكل عنصر.

بناءً على مكان إنشاء طلب CSR وتنسيق ملف الشهادة، يمكن أن تتنوع الإعدادات المطلوبة. أدخل قيمةً 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**: لا تقم بالتكوين.

**CA Certificate 2/CA Certificate 1**: اختياري

شهادة بتنسيق PEM/DER تم الحصول عليها من الكمبيوتر

**Private Key**: يجب أن تقوم بتعيينه.

**Password**: لا تقم بالتكوين.

**CA Certificate 2/CA Certificate 1**: اختياري

شهادة بتنسيق PKCS#12 تم الحصول عليها من الكمبيوتر

**Private Key**: لا تقم بالتكوين.

**Password**: اختياري

**CA Certificate 2/CA Certificate 1**: لا تقم بالتكوين.

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 37"

← "عناصر إعداد استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 119

## إعدادات الأمان المتقدمة لـ Enterprise

عناصر إعداد استيراد شهادة موقعة من المرجع المصدق (CA)

The screenshot shows the EPSON Network Security settings page for SSL/TLS Certificate. The page is titled "SSL/TLS > Certificate" and includes a navigation menu on the left with options like Protocol, CA Certificate, Root Certificate Update, SSL/TLS, IPsec/IP Filtering, and IEEE802.1X. The main content area contains fields for Server Certificate, Private Key, Password, CA Certificate 1, and CA Certificate 2, each with a "Browse" button. A note at the bottom states: "Note: it is recommended to communicate via HTTPS for importing a certificate." Buttons for "OK" and "Back" are located at the bottom of the page.

العناصر	الإعدادات والشرح
Client Certificate أو Server Certificate	حدد تنسيق الشهادة.
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	أدخل كلمة مرور لتشفير المفتاح الخاص.
CA Certificate 1	إذا كان تنسيق الشهادة (Certificate (PEM/DER)، فقم باستيراد شهادة من المرجع المصدق 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 118

## حذف شهادة موقعة من المرجع المصدق (CA)

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

## إعدادات الأمان المتقدمة لـ Enterprise

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.

## تحديث شهادة موقعة ذاتياً

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

استخدم شهادة موقعة ذاتياً مؤقتاً حتى تحصل على شهادة موقعة من المرجع المصدق (CA) وتقوم باستيرادها.

1. ادخل إلى Web Config وحدد علامة التبويب Network Security < SSL/TLS < Certificate.
  2. انقر فوق Update.
  3. أدخل Common Name.
- أدخل عنوان IP أو أي معرف مثل اسم FQDN للطابعة. يمكن إدخال عدة أحرف تتراوح ما بين حرف واحد حتى 128 حرفاً.

ملاحظة:

يمكنك فصل الأسماء المميزة (CN) باستخدام الفاصلة.



## إعدادات الأمان المتقدمة لـ Enterprise

4. حدد فترة صلاحية للشهادة.

The screenshot shows the EPSON Web Config interface for the 'Network Security' section, specifically the 'SSL/TLS > Certificate' configuration page. The interface includes a navigation menu on the left with options like 'Protocol', 'CA Certificate', 'Root Certificate Update', 'SSL/TLS', 'IPsec/IP Filtering', and 'IEEE802.1X'. The main configuration area contains the following fields:

Key Length :	RSA 2048bit - SHA-256
Common Name :	EPSON/SEIKO EPSON CORP JAPAN, Ltd. 1985.78
Organization :	SEIKO EPSON CORP
Valid Date (UTC) :	2017-04-10 05:42:51 UTC
Certificate Validity (year) :	10

At the bottom of the configuration area, there are two buttons: 'Next' and 'Back'.

5. انقر فوق **Next**.

يتم عرض رسالة تأكيد.

6. انقر فوق **OK**.

الطابعة قيد التحديث.

ملاحظة:

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

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## تهيئة CA Certificate

يمكنك استيراد وعرض وحذف CA Certificate.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

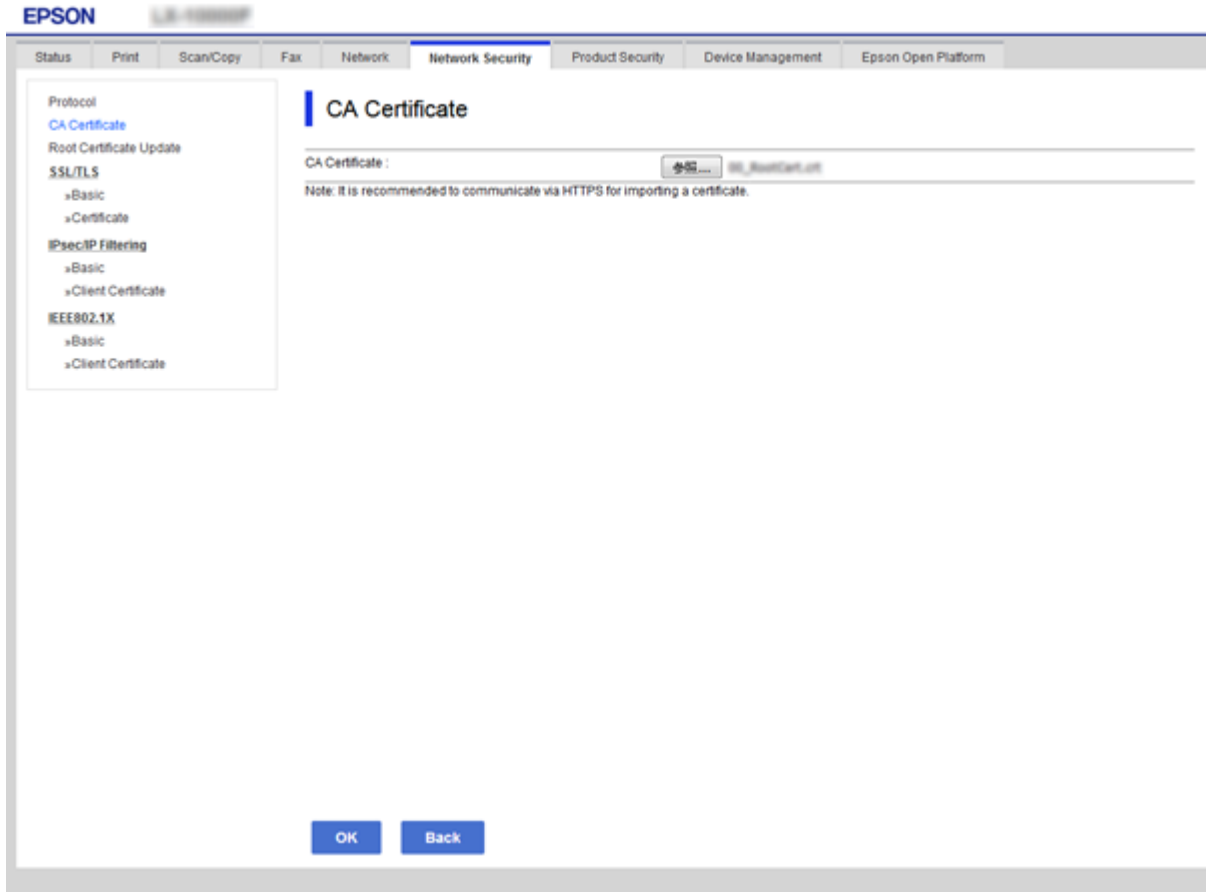
← "عناصر إعداد طلب CSR" في الصفحة 117

← "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 118

## إعدادات الأمان المتقدمة لـ Enterprise

## استيراد شهادة المرجع المصدق (CA)

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

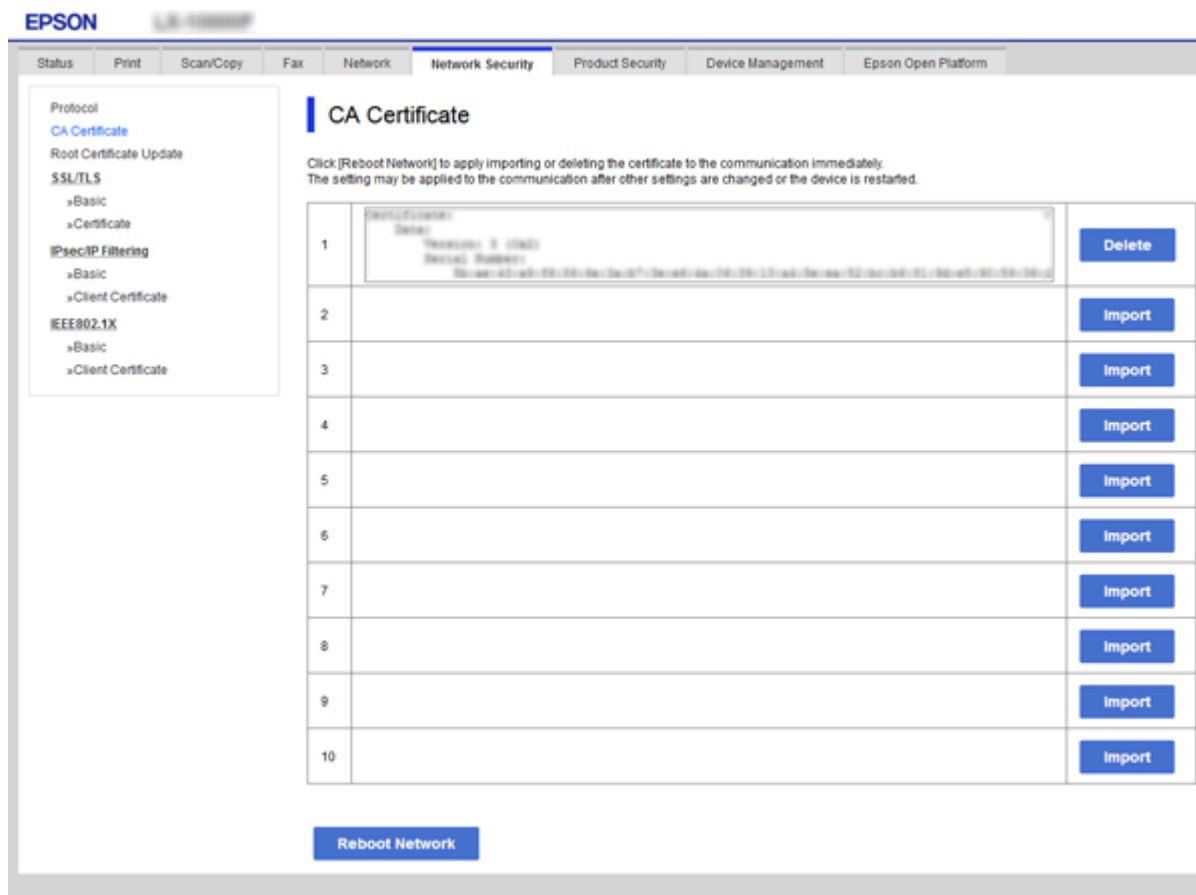
## حذف شهادة المرجع المصدق (CA)

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.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## التحكم باستخدام البروتوكولات

يمكنك الطباعة باستخدام مجموعة متنوعة من الممرات والبروتوكولات. إذا كنت تستخدم طباعة متعددة الوظائف، يمكنك استخدام المسح الضوئي للشبكة و PC-FAX من عدد غير محدد من أجهزة الكمبيوتر المتصلة بالشبكة. يمكنك خفض المخاطر الأمنية غير المقصودة من خلال تقييد الطباعة 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**.

## إعدادات الأمان المتقدمة لـ Enterprise

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، وللطباعة، وما إلى ذلك.
SLP Settings	من الممكن أيضاً تمكين أو تعطيل وظيفة SLP. تُستخدم SLP مع وظيفتي المسح الضوئي بالدفع وبحث الشبكة في EpsonNet Config.
WSD Settings	من الممكن أيضاً تمكين أو تعطيل وظيفة WSD. عند تمكينها، يمكنك إضافة أجهزة WSD أو إجراء الطباعة والمسح الضوئي من منفذ WSD.
LLTD Settings	من الممكن أيضاً تمكين أو تعطيل وظيفة LLTD. عند تمكينها، يتم عرضها أيضاً على خريطة شبكة Windows.
LLMNR Settings	من الممكن أيضاً تمكين أو تعطيل وظيفة LLMNR. عند تمكينها، يمكنك استخدام تحليل الاسم بدون NetBIOS حتى وإن لم تتمكن من 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 يمكنك 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.

## إعدادات الأمان المتقدمة لـ Enterprise

## عناصر إعداد البروتوكول

**Protocol**

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

**Bonjour Settings**

Use Bonjour

Bonjour Name : EPSON®  
Bonjour Service Name : EPSON LX-10000F  
Location :  
Top Priority Protocol : IPP

**SLP Settings**

Enable SLP

**WSD Settings**

Enable WSD

Printing Timeout (sec) : 300  
Scanning Timeout (sec) : 300  
Device Name : EPSON®  
Location :  
WSD Secure Print :  Enable  Disable

**LLTD Settings**

Enable LLTD  
Device Name : EPSON®

**LLMNR Settings**

Enable LLMNR

**LPR Settings**

Allow LPR Port Printing

**Next**

العناصر	إعداد القيمة والوصف
Bonjour Settings	
Use Bonjour	حدد هذه الخاصية للبحث عن الجهاز أو استخدامه من خلال Bonjour.
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.
UPnP Settings	
Enable UPnP	حدّد هذا العنصر للسماح لجهاز الكمبيوتر بالبحث عن الطابعات باستخدام UPnP. لا يتم عرض هذه الخاصية سوى للطابعات التي تدعم UPnP.
Device Name	يعرض اسم جهاز UPnP.
Location	يعرض اسم موقع UPnP.
SLP Settings	
Enable SLP	حدد هذا العنصر لتمكين وظيفة SLP. يُستخدم مع وظيفتي المسح الضوئي بالدفع وبحث الشبكة في EpsonNet Config.

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر	إعداد القيمة والوصف
WSD Settings	
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.
Scanning Timeout (sec)	أدخل قيمة مهلة الاتصال لمسح WSD الضوئي في مدة تتراوح بين 3 إلى 3600 ثانية.
Device Name	يعرض اسم جهاز WSD.
Location	يعرض اسم موقع WSD.
LLTD Settings	
Enable LLTD	حدد هذا العنصر لتمكين LLTD. يتم عرض الطابعة في خريطة شبكة Windows.
Device Name	يعرض اسم جهاز LLTD.
LLMNR Settings	
Enable LLMNR	حدد هذا العنصر لتمكين LLMNR. يمكنك استخدام تحليل الاسم بدون NetBIOS حتى وإن لم يمكنك استخدام DNS.
LPR Settings	
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	
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	
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)	يعرض URLs (http و https) لـ IPP عندما تكون الطابعة متصلة بشبكة LAN سلكية أو Wi-Fi. يُعد URL قيمة مشتركة لعنوان IP الخاص بالطابعة ورقم المنفذ واسم طابعة IPP.
URL (شبكة Wi-Fi Direct)	لعرض URLs (http و https) 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	

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر	إعدادات 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	
Enable SNMPv1/v2c	حدّد هذا العنصر لتمكين SNMPv1/v2c. يتم عرض الطابعات التي تدعم SNMPv3 فقط.
Access Authority	حدّد حق الوصول عند تمكين SNMPv1/v2c. حدّد <b>Read Only</b> أو <b>Read/Write</b> .
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	
Enable SNMPv3	يتم تمكين SNMPv3 عند تحديد المربع.
User Name	أدخل عددًا من الأحرف يتراوح بين حرف واحد إلى 32 حرفًا باستخدام الأحرف ذات البايت 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

إذا كانت الطابعة تدعم تصفية IPsec/IP، يمكنك تصفية البيانات الواردة إلى الشبكة بناءً على عناوين IP والخدمات والمنفذ. من خلال تجميع عوامل التصفية، يمكنك تكوين الطابعة لقبول أجهزة تابعة وبيانات محددة أو منع أيًا منهما. بالإضافة إلى هذا، يمكنك تحسين مستوى الأمان من خلال استخدام بروتوكول IPsec.

## إعدادات الأمان المتقدمة لـ Enterprise

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. 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.

ملاحظة:

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

## تكوين السياسة الافتراضية

1. ادخل إلى Web Config وحدد 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

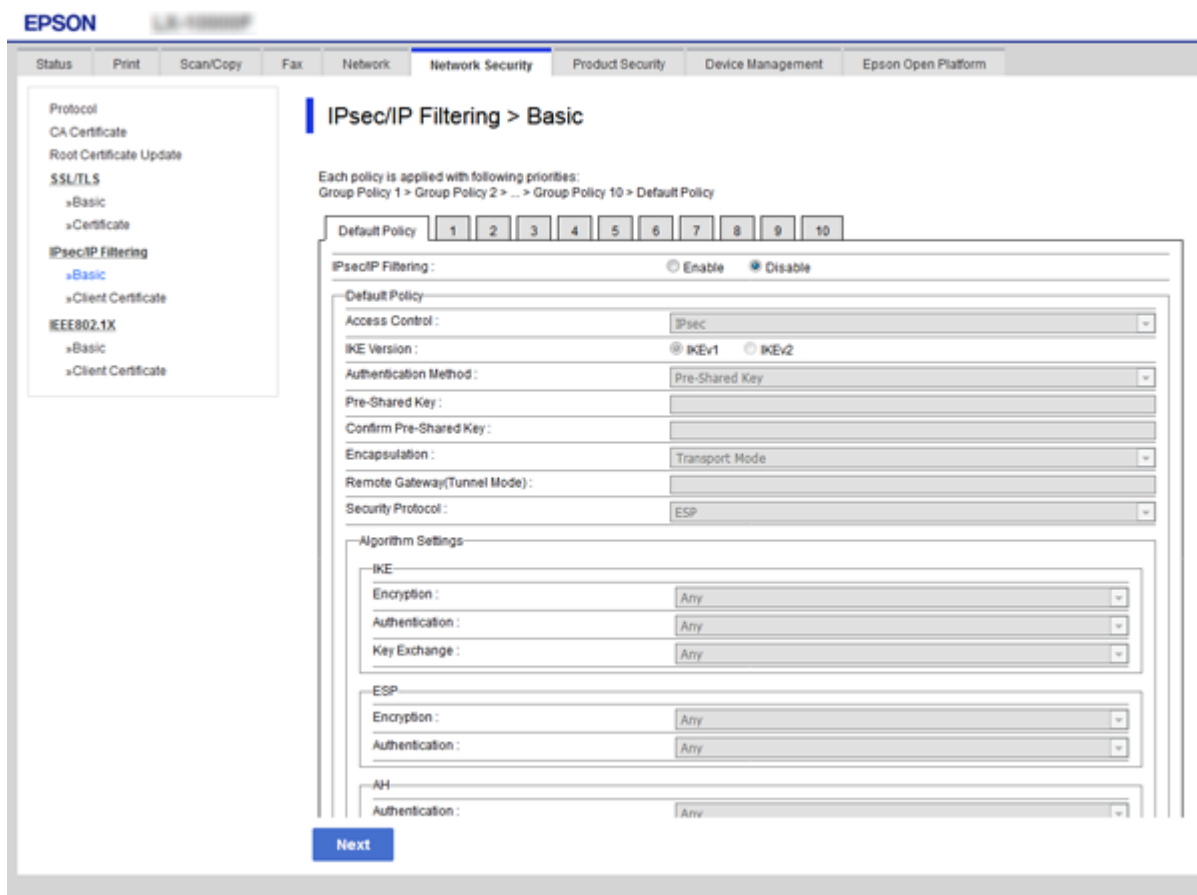
← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "عناصر إعداد Default Policy" في الصفحة 129



## إعدادات الأمان المتقدمة لـ Enterprise

## عناصر إعداد 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.	
	حدد هذه الطريقة للسماح بمرور حزم بيانات IP المكونة.	Permit Access
	حدد هذه الطريقة لرفض مرور حزم بيانات IP المكونة.	Refuse Access
IPsec	حدد هذه الطريقة للسماح بمرور حزم بيانات IPsec المكونة.	IPsec
	حدد IKEv1 أو IKEv2 لإصدار IKE.	IKE Version
IKEv1	حدد أحدهما وفقاً للجهاز المتصل به الطابعة.	IKE Version
	يتم عرض العناصر التالية عند تحديد IKE Version لـ IKEv1.	IKE Version
	لتحديد Certificate، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدماً.	Authentication Method
	إذا قمت بتحديد Pre-Shared Key من أجل Authentication Method، فأدخل مفتاحاً مشتركاً مسبقاً مكوناً من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفاً.	Pre-Shared Key
أدخل المفتاح الذي قمت بتكوينه للتأكيد.	Confirm Pre-Shared Key	
IKEv2	يتم عرض العناصر التالية عند تحديد IKE Version لـ IKEv2.	

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح
Local	Authentication Method لتحديد <b>Certificate</b> ، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدماً.
	ID Type إذا قمت بتحديد <b>Pre-Shared Key</b> لـ <b>Authentication Method</b> ، فحدد نوع معرف الطابعة.
	ID أدخل معرف الطابعة الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، "#"، و"=" بدلاً من الحرف الأول. <b>Distinguished Name</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". <b>IP Address</b> : أدخل تنسيق IPv4 أو IPv6. <b>FQDN</b> : أدخل مزيجاً من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفاً باستخدام A-Z، a-z، و 0-9، و "-"، و نقطة (.). <b>Email Address</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". <b>Key ID</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E).
Remote	Pre-Shared Key إذا قمت بتحديد <b>Pre-Shared Key</b> من أجل <b>Authentication Method</b> ، فأدخل مفتاحاً مشتركاً مسبقاً مكوناً من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفاً.
	Confirm Pre-Shared Key أدخل المفتاح الذي قمت بتكوينه للتأكيد.
	Authentication Method لتحديد <b>Certificate</b> ، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدماً.
Encapsulation	ID Type إذا حددت <b>Pre-Shared Key</b> لـ <b>Authentication Method</b> ، فحدد نوع معرف الجهاز الذي تريد مصادقته.
	ID أدخل معرف الطابعة الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، "#"، و"=" بدلاً من الحرف الأول. <b>Distinguished Name</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". <b>IP Address</b> : أدخل تنسيق IPv4 أو IPv6. <b>FQDN</b> : أدخل مزيجاً من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفاً باستخدام A-Z، a-z، و 0-9، و "-"، و نقطة (.). <b>Email Address</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". <b>Key ID</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E).
	Pre-Shared Key إذا قمت بتحديد <b>Pre-Shared Key</b> من أجل <b>Authentication Method</b> ، فأدخل مفتاحاً مشتركاً مسبقاً مكوناً من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفاً.
Encapsulation	Confirm Pre-Shared Key أدخل المفتاح الذي قمت بتكوينه للتأكيد.
	Transport Mode إذا قمت بتحديد <b>IPsec</b> من أجل <b>Access Control</b> ، فلا بد أن تقوم بتكوين وضع تغليف.
	Tunnel Mode إذا كنت تستخدم طابعة على شبكة تدعم استخدام الإنترنت مثل <b>IPsec-VPN</b> ، فحدد هذا الخيار. يتم تشفير عنوان حزم بيانات IP وبياناتها.

## إعدادات الأمان المتقدمة لـ Enterprise

الإعدادات والشرح		العناصر
إذا قمت بتحديد Tunnel Mode من أجل Encapsulation، فأدخل عنوان البوابة الافتراضي المكون من عددٍ من الأحرف يتراوح ما بين حرف واحد و 39 حرفاً.		Remote Gateway(Tunnel Mode)
IPsec لـ Access Control، حدد خياراً.		Security Protocol
حدد هذا الخيار لضمان سلامة المصادقة والبيانات وتشفير البيانات.	ESP	
حدد هذا الخيار لضمان سلامة المصادقة والبيانات. حتى في حالة حظر تشفير البيانات، فإنه يمكنك استخدام IPsec.	AH	
*Algorithm Settings		
حدد خوارزمية التشفير لـ IKE.	Encryption	IKE
تختلف العناصر حسب إصدار IKE.		
حدد خوارزمية المصادقة لـ IKE.	Authentication	
حدد خوارزمية تبادل المفاتيح لـ IKE.	Key Exchange	
تختلف العناصر حسب إصدار IKE.		
حدد خوارزمية التشفير لـ ESP.	Encryption	ESP
يتوفر ذلك عند تحديد ESP لـ Security Protocol.		
حدد خوارزمية المصادقة لـ ESP.	Authentication	
يتوفر ذلك عند تحديد ESP لـ Security Protocol.		
حدد خوارزمية التشفير لـ AH.	Authentication	AH
يتوفر ذلك عند تحديد AH لـ Security Protocol.		

\* بالنسبة 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.

معلومات ذات صلة

← "تكوين السياسة الافتراضية" في الصفحة 128

## تكوين سياسة المجموعة

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**.
  5. انقر فوق **OK**.
- الطابعة قيد التحديث.

## إعدادات الأمان المتقدمة لـ Enterprise

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

← "عناصر إعداد Group Policy" في الصفحة 132

## عناصر إعداد Group Policy

The screenshot shows the Epson Web Config interface for the 'IPsec/IP Filtering > Basic' configuration. The interface includes a navigation menu on the left with options like 'Protocol', 'CA Certificate', 'SSL/TLS', 'IPsec/IP Filtering', and 'IEEE802.1X'. The main configuration area has a status bar at the top with tabs for 'Status', 'Print', 'Scan/Copy', 'Fax', 'Network', 'Network Security', 'Product Security', 'Device Management', and 'Epson Open Platform'. Below the status bar, there's a section for 'IPsec/IP Filtering > Basic' with a sub-section for 'Basic'. The configuration area includes a 'Default Policy' tab, a 'Next' button, and a list of services to be filtered. The 'Enable this Group Policy' checkbox is checked. The 'Access Control' dropdown is set to 'IPsec'. The 'Local Address(Printer)' dropdown is set to 'Any addresses'. The 'Remote Address(Host)' field is empty. The 'Method of Choosing Port' dropdown is set to 'Port Number'. The 'Service Name' list includes various protocols and services, with checkboxes for selection.

العناصر	الإعدادات والشرح	
Enable this Group Policy	يمكنك تمكين سياسة مجموعة أو تعطيلها.	
Access Control	قم بتكوين طريقة تحكم لنقل حزم بيانات IP.	
	حدد هذه الطريقة للسماح بمرور حزم بيانات IP المكونة.	Permit Access
	حدد هذه الطريقة لرفض مرور حزم بيانات IP المكونة.	Refuse Access
	حدد هذه الطريقة للسماح بمرور حزم بيانات IPsec المكونة.	IPsec
Local Address(Printer)	حدد عنوان IPv4 أو عنوان IPv6 الذي يتوافق مع بيئة شبكتك. إذا تم تعيين عنوان IP تلقائياً، يمكنك تحديد <b>Use auto-obtained IPv4 address</b> . <b>ملاحظة:</b> في حالة تعيين عنوان IPv6 تلقائياً، فقد يصبح الاتصال غير متوفر. كَوِّن عنوان IPv6 ثابتاً.	

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح	
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. <b>ملاحظة:</b> في حالة تعيين عنوان IP تلقائياً (على سبيل المثال، بواسطة بروتوكول DHCP)، فقد يصبح الاتصال غير متوفر. 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.	
	Any Protocol	حدد هذا للتحكم في جميع أنواع البروتوكول.
	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.
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 لإصدار IKE. حدد أحدهما وفقاً للجهاز المتصل به الطابعة.	
IKEv1	يتم عرض العناصر التالية عند تحديد IKEv1 لـ IKE Version.	
	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 و 127 حرفاً.
Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.	
IKEv2	يتم عرض العناصر التالية عند تحديد IKEv2 لـ IKE Version.	

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح
Local	Authentication Method إذا قمت بتحديد IPsec من أجل Access Control، فحدد خياراً. تعتبر الشهادة المستخدمة هي السياسة الافتراضية نفسها.
	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. <b>Distinguished Name</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". <b>IP Address</b> : أدخل تنسيق IPv4 أو IPv6. <b>FQDN</b> : أدخل مزيجاً من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفاً باستخدام A-Z، a-z، و 0-9، و"-"، و"نقطة". <b>Email Address</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". <b>Key ID</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E).
Remote	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 و 127 حرفاً.
	Confirm Pre-Shared Key أدخل المفتاح الذي قمت بتكوينه للتأكيد.
	Authentication Method إذا قمت بتحديد IPsec من أجل Access Control، فحدد خياراً. 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. <b>Distinguished Name</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". <b>IP Address</b> : أدخل تنسيق IPv4 أو IPv6. <b>FQDN</b> : أدخل مزيجاً من الأحرف يتراوح ما بين حرف واحد إلى 255 حرفاً باستخدام A-Z، a-z، و 0-9، و"-"، و"نقطة". <b>Email Address</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". <b>Key ID</b> : أدخل من حرف واحد إلى 128 حرفاً 1-بايت ASCII (0x20 إلى 0x7E).
	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 و 127 حرفاً.
Encapsulation	Confirm Pre-Shared Key أدخل المفتاح الذي قمت بتكوينه للتأكيد.
	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.

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر		الإعدادات والشرح
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 و 39 حرفاً.
Security Protocol		إذا قمت بتحديد IPsec من أجل Access Control، فحدد خياراً.
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		
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 المصادقة لـ AH. يتوفر ذلك عند تحديد AH لـ Security Protocol.

\* بالنسبة 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.

## معلومات ذات صلة

- ← "تكوين سياسة المجموعة" في الصفحة 131
- ← "الجمع بين Local Address(Printer) و Remote Address(Host) على Group Policy" في الصفحة 135
- ← "مراجع أسماء الخدمة في سياسة المجموعة" في الصفحة 136

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

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

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

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

## إعدادات الأمان المتقدمة لـ Enterprise

\*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	البحث عن طابعة من التطبيقات مثل EpsonNet Config، وبرنامج تشغيل الطابعة، وبرنامج تشغيل الماسحة الضوئية
SNMP	UDP	161	أي منفذ	الحصول على MIB وتكوينه من تطبيقات مثل EpsonNet Config، وبرنامج تشغيل الطابعة والماسحة الضوئية من Epson
LPR	TCP	515	أي منفذ	إرسال بيانات LPR
RAW (Port9100)	TCP	9100	أي منفذ	إرسال بيانات RAW
WSD	TCP	أي منفذ	5357	تحكم WSD
WS-Discovery	UDP	3702	أي منفذ	البحث عن طابعة من WSD
Network Scan	TCP	1865	أي منفذ	إرسال بيانات المسح الضوئي من Document Capture Pro
Network Push Scan	TCP	أي منفذ	2968	الحصول على معلومات حول وظيفة المسح الضوئي بالدفع من Document Capture Pro
Network Push Scan Discovery	UDP	2968	أي منفذ	تم تنفيذ البحث عن جهاز كمبيوتر في حالة المسح الضوئي بالدفع من Document Capture Pro
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 (إرسال بيانات المسح واستلام بيانات الفاكس) 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 لإرسال بيانات المسح واستلام بيانات الفاكس)
CIFS (Local)	TCP	445	أي منفذ	خادم CIFS (مشاركة مجلد شبكة)
CIFS (Remote)	TCP	أي منفذ	445	عميل CIFS (إرسال بيانات المسح وبيانات الفاكس المستلمة إلى أحد المجلدات)



## إعدادات الأمان المتقدمة لـ Enterprise

اسم الخدمة	نوع البروتوكول	رقم المنفذ المحلي	رقم المنفذ البعيد	الميزات المتحكم بها
NetBIOS Name Service (Local)	UDP	137	أي منفذ	خادم CIFS (مشاركة مجلد شبكة)
NetBIOS Datagram Service (Local)	UDP	138	أي منفذ	
NetBIOS Session Service (Local)	TCP	139	أي منفذ	
NetBIOS Name Service (Remote)	UDP	أي منفذ	137	عميل CIFS (إرسال بيانات المسح وبيانات الفاكس المستلمة 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) اتصال بين Epson Connect أو الطباعة السحابية من Google أو 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

## إعدادات الأمان المتقدمة لـ Enterprise

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).

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.

## تكوين شهادة لتصفية IPsec/IP

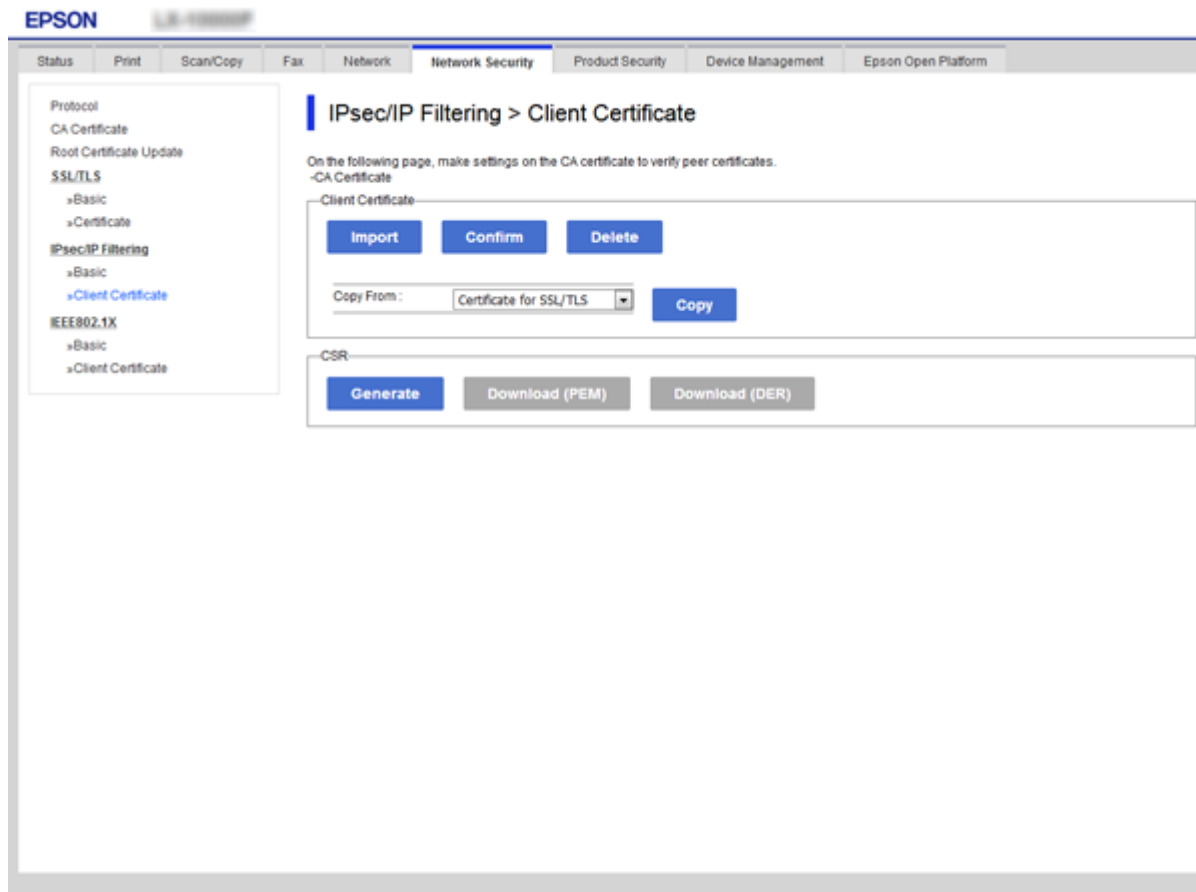
قم بتهيئة شهادة العميل لتصفية IPsec/IP. إذا كنت ترغب في تهيئة المرجع المصدق، فإذهب إلى CA Certificate.

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 IEEE802.1X 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 37
- ◀ "الحصول على شهادة موقعة من المرجع المصدق (CA)" في الصفحة 115

## استخدام بروتوكول SNMPv3

### معلومات عن SNMPv3

يعد SNMP بروتوكولاً يقوم بإجراء المراقبة والتحكم لجمع معلومات الأجهزة المتصلة بالشبكة. يُعد SNMPv3 إصداراً مليماً أمان الإدارة الذي تم تحسينه.

عند استخدام SNMPv3، يمكن أن تتم مصادقة مراقبة حالة اتصال SNMP وتغييرات الإعداد الخاصة به (الحزمة) وتشفيرها لحماية اتصال SNMP (الحزمة) من مخاطر الاتصال بالشبكة، مثل التصنت على المحادثات الهاتفية، والانتحال، والتلاعب.

### تكوين SNMPv3

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

## إعدادات الأمان المتقدمة لـ Enterprise

1. ادخل إلى Web Config ثم حدد علامة التبويب Protocol < Network Security.
  2. أدخل قيمة لكل عنصر من عناصر SNMPv3 Settings.
  3. انقر فوق Next.
  4. انقر فوق OK.
- الطابعة قيد التحديث.

## معلومات ذات صلة

- ← "الوصول إلى تطبيق Web Config" في الصفحة 37
- ← "عناصر إعدادات SNMPv3" في الصفحة 140

## عناصر إعدادات SNMPv3

The screenshot shows the Epson Web Config interface for an L3110 printer. The 'Network Security' tab is selected. The left sidebar contains a tree view with 'Protocol' expanded. The main content area shows the following settings:

- URL(Wi-Fi Direct):** https://192.168.78.51/ipp/print
- Printer Name:** ipp/print
- Location:**
- FTP Settings:**
  - Enable FTP Server
  - Communication Timeout (sec):** 120
- SNMPv1v2c Settings:**
  - Enable SNMPv1v2c
  - Access Authority:** Read/Write
  - Community Name (Read Only):** public
  - Community Name (Read/Write):**
- SNMPv3 Settings:**
  - Enable SNMPv3
  - User Name:** admin
  - Authentication Settings:**
    - Algorithm:** MD5
    - Password:**
    - Confirm Password:**
  - Encryption Settings:**
    - Algorithm:** DES
    - Password:**
    - Confirm Password:**
  - Context Name:** EPSON

A 'Next' button is visible at the bottom of the configuration area.

العناصر	الإعدادات والشرح
Enable SNMPv3	يتم تمكين SNMPv3 عند تحديد خانة الاختيار.
User Name	أدخل عددًا من الحروف يتراوح من 1 إلى 32 حرفًا باستخدام حروف 1 بايت.
Authentication Settings	

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح
Algorithm	حدد خوارزمية للمصادقة.
Password	أدخل ما بين 8 إلى 32 حرفاً بتنسيق (0x20-0x7E ASCII).
Confirm Password	أدخل كلمة المرور التي قمت بتكوينها للتأكيد.
Encryption Settings	
Algorithm	حدد خوارزمية للتشفير.
Password	أدخل ما بين 8 إلى 32 حرفاً بتنسيق (0x20-0x7E ASCII).
Confirm Password	أدخل كلمة المرور التي قمت بتكوينها للتأكيد.
Context Name	أدخل عدداً من الحروف يتراوح من 1 إلى 32 حرفاً باستخدام حروف 1 بايت.

معلومات ذات صلة

← "تكوين SNMPv3" في الصفحة 139

## توصيل الطابعة بشبكة IEEE802.1X

## تكوين شبكة IEEE802.1X

إذا كانت الطابعة تدعم شبكة IEEE802.1X، يمكنك استخدام الطابعة على شبكة ذات مصادقة متصلة بخادم RADIUS ولوحة موزع بمثابة المصدق.

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

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.

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 37

← "عناصر إعداد شبكة IEEE802.1X" في الصفحة 142

← "تعذر الوصول إلى الطابعة أو الماسحة الضوئية بعد تكوين IEEE802.1X" في الصفحة 149

## إعدادات الأمان المتقدمة لـ Enterprise

## عناصر إعداد شبكة IEEE802.1X

The screenshot shows the Epson Network Security configuration interface. The main heading is "IEEE802.1X > Basic". The interface includes a navigation menu on the left with options like Protocol, CA Certificate, Root Certificate Update, SSL/TLS, IPsec/IP Filtering, and IEEE802.1X. The main content area contains the following settings:

- IEEE802.1X (Wired LAN):  Enable  Disable
- IEEE802.1X (Wi-Fi): Disable
- Connection Method: Wired LAN
- EAP Type: PEAP/MSCHAPv2
- User ID: [Empty field]
- Password: [Empty field]
- Confirm Password: [Empty field]
- Server ID: [Empty field]
- Certificate Validation:  Enable  Disable
- Anonymous Name: [Empty field]
- Encryption Strength: Middle

At the bottom, there are two buttons: "Next" and "Wi-Fi Setup".

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.						
	<table border="1"> <tr> <td>EAP-TLS</td> <td>تحتاج إلى الحصول على شهادة موقعة من مرجع مصدق (CA) واستيرادها.</td> </tr> <tr> <td>PEAP-TLS</td> <td></td> </tr> <tr> <td>PEAP/MSCHAPv2</td> <td>تحتاج إلى تكوين كلمة مرور.</td> </tr> </table>	EAP-TLS	تحتاج إلى الحصول على شهادة موقعة من مرجع مصدق (CA) واستيرادها.	PEAP-TLS		PEAP/MSCHAPv2	تحتاج إلى تكوين كلمة مرور.
EAP-TLS	تحتاج إلى الحصول على شهادة موقعة من مرجع مصدق (CA) واستيرادها.						
PEAP-TLS							
PEAP/MSCHAPv2	تحتاج إلى تكوين كلمة مرور.						
User ID	قم بتكوين معرف لاستخدامه كأسلوب مصادقة لأحد خوادم RADIUS. أدخل من 1 إلى 128 بايت ASCII (0x20 إلى 0x7E) حرفاً.						
Password	قم بتكوين كلمة مرور لمصادقة الطابعة. أدخل من 1 إلى 128 بايت ASCII (0x20 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.						

## إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح	
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 ASCII (0x20 إلى 0x7E) حرفاً.	
Certificate Validation	يمكنك تعيين التحقق من صحة الشهادة بغض النظر عن أسلوب المصادقة. قم باستيراد الشهادة في <b>CA Certificate</b> .	
Anonymous Name	إذا قمت بتحديد <b>PEAP-TLS</b> أو <b>PEAP/MSCHAPv2</b> من أجل <b>Authentication Method</b> ، فيمكنك تكوين اسم مجهول بدلاً من معرف المستخدم للعبارة 1 من مصادقة PEAP. أدخل من 0 إلى 128 -بايت ASCII (0x20 إلى 0x7E) حرفاً.	
Encryption Strength	يمكنك تحديد إحدى القيم التالية.	
	AES256/3DES	High
	AES256/3DES/AES128/RC4	Middle

معلومات ذات صلة

← "تكوين شبكة IEEE802.1X" في الصفحة 141

## تكوين شهادة لاتصال IEEE802.1X

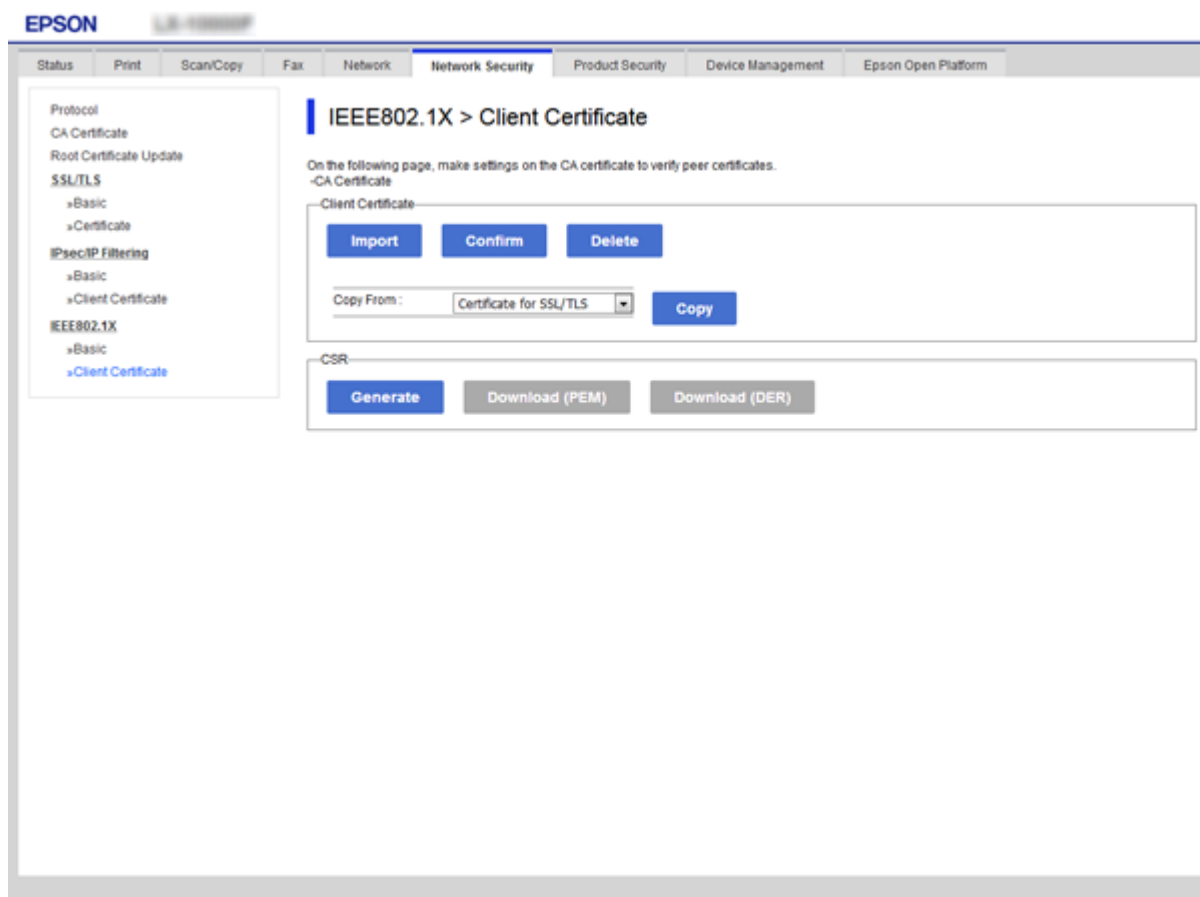
تهيئة شهادة العميل لـ IEEE802.1X. إذا كنت ترغب في تهيئة شهادة المرجع المصدق، فإذهب إلى **CA Certificate**.

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

## إعدادات الأمان المتقدمة لـ Enterprise

## 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 37

← "الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها" في الصفحة 115

## التحقق من حالة شبكة IEEE802.1X

يمكنك التحقق من حالة شبكة IEEE802.1X من خلال طباعة ورقة حالة الشبكة. لمزيد من المعلومات حول طباعة ورقة حالة الشبكة، انظر وثائق الطابعة.

حالة IEEE802.1X	معرف الحالة
ميزة IEEE802.1X معطلة.	Disable
نجحت مصادقة IEEE802.1X والاتصال بالشبكة متاح.	EAP Success
لم تكتمل مصادقة IEEE802.1X.	Authenticating
فشلت المصادقة حيث لم يتم تعيين معرف المستخدم.	Config Error
فشلت المصادقة حيث إن شهادة الجهاز التابع منتهية الصلاحية.	Client Certificate Error
فشلت المصادقة حيث لا يوجد رد من خادم RADIUS و/أو المصدق.	Timeout Error



## إعدادات الأمان المتقدمة لـ Enterprise

حالة IEEE802.1X	معرف الحالة
فشلت المصادقة لعدم صحة معرف مستخدم الطابعة و/أو بروتوكول الشهادة.	User ID Error
فشلت المصادقة لعدم تطابق معرف خادم الشهادة 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 PEAP/MSCHAPv2، فسيكون معرف المستخدم غير صحيح أو كلمة المرور غير صحيحة.	EAP Failure

## باستخدام Epson Open Platform

### نظرة عامة حول Epson Open Platform

Epson Open Platform هو نظام أساسي للجهاز من Epson يمكنه استخدام واجهة المستخدم التي يوفرها خادم نظام المصادقة. يمكنك الحصول على سجلات كل جهاز ومستخدم بالتعاون مع الخادم، وتكوين قيود على الجهاز والوظائف التي يمكن استخدامها لكل مستخدم ومجموعة. يمكن استخدامه مع Epson Print Admin (نظام المصادقة من Epson) أو نظام مصادقة تابع لجهة خارجية. إذا قمت بتوصيل جهاز مصادقة، يمكنك أيضاً إجراء مصادقة المستخدم باستخدام بطاقة الهوية.

### تكوين Epson Open Platform

مكّن Epson Open Platform بحيث يمكنك استخدام الجهاز من نظام المصادقة.

1. ادخل إلى Web Config ثم حدد علامة التبويب **Epson Open Platform < Product key**.

2. أدخل قيمة لكل عنصر.

Serial Number

يتم عرض الرقم التسلسلي للجهاز.

Epson Open Platform Version

حدد إصدار Epson Open Platform. يختلف الإصدار المماثل حسب نظام المصادقة.

## إعدادات الأمان المتقدمة لـ Enterprise

Enter product key 

أدخل مفتاح المنتج الذي تم الحصول عليه من موقع الويب المخصص. راجع دليل Epson Open Platform للحصول على تفاصيل مثل كيفية الحصول على مفتاح المنتج.

3. انقر فوق **Next**.

يتم عرض رسالة تأكيد.

4. انقر فوق **OK**.

الطابعة قيد التحديث.

## التحقق من نظام المصادقة وتكوينه

يمكنك التحقق من نظام المصادقة الذي يستخدم Epson Open Platform وتكوينه من علامة التبويب **Epson Open Platform < Authentication System**.

حسب نظام المصادقة، قد يمكن تكوينه تلقائياً من نظام المصادقة أو يمكنك إدخال القيمة عند توصيل الجهاز وتسجيله. للحصول على مزيدٍ من المعلومات، راجع الدليل المرفق مع نظام المصادقة.

Basic 

يمكنك التحقق من إعدادات خادم نظام المصادقة حتى يتم الاتصال بـ Epson Open Platform. فضلاً عن القيمة التي كتبها نظام المصادقة.

Connection Test 

يمكنك التحقق من الاتصال بنظام المصادقة مع القيمة المحددة في **Basic**. انقر فوق **Start** للتحقق من الاتصال وعرض النتيجة.

## تكوين جهاز المصادقة

يمكنك تكوين جهاز المصادقة المستخدم في نظام المصادقة من علامة التبويب **Card Reader < Device Management**.

كوّنهُ عند تحديد جهاز المصادقة المراد استخدامه أو عند التحقق من قراءة جهاز المصادقة. للحصول على مزيدٍ من المعلومات، راجع دليل نظام المصادقة.

## 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. اضغط على الإعدادات &lt; إعدادات عامة &lt; إعدادات الشبكة.

2. اضغط على متقدم.

## إعدادات الأمان المتقدمة لـ Enterprise

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

تعطيل تصفية IPsec/IP

تعطيل IEEE802.1X

4. اضغط على متابعة على شاشة التأكيد.

5. عندما تظهر رسالة الاكتمال، اضغط على إغلاق.

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

## استعادة وظيفة الأمان باستخدام تهيئة الويب

بالنسبة لـ IEEE802.1X، قد لا يتم التعرف على الأجهزة على الشبكة. في تلك الحالة، عطل الوظيفة باستخدام لوحة تحكم الطابعة.

بالنسبة لتصفية IPsec/IP، يمكنك تعطيل الوظيفة إذا تمكنت من الوصول إلى الجهاز من الكمبيوتر.

## تعطيل تصفية IPsec/IP باستخدام تهيئة الويب

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

2. حدد **Disable** لـ **IPsec/IP Filtering** في **Default Policy**.

3. انقر فوق **Next**، ثم قم بإلغاء تحديد **Enable this Group Policy** لجميع سياسات المجموعة.

4. انقر فوق **OK**.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37

## المشكلات الخاصة باستخدام ميزات أمان الشبكة

## نسيان مفتاح مشترك مسبقاً

قم بتكوين المفتاح مرةً أخرى باستخدام تطبيق Web Config.

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

عندما تُغير المفتاح المشترك مسبقاً، قم بتهيئته لأجهزة الحاسوب.

معلومات ذات صلة

← "الوصول إلى تطبيق Web Config" في الصفحة 37



## إعدادات الأمان المتقدمة لـ Enterprise

## يتعذر إنشاء منفذ طباعة IPP آمن

هل تم تحديد الشهادة الصحيحة بمثابة شهادة الخادم لاتصال SSL/TLS؟  
إذا كانت الشهادة المحددة غير صحيحة، فقد تفشل عملية إنشاء منفذ. تأكد من استخدام الشهادة الصحيحة.

هل تم استيراد شهادة المرجع المصدق (CA) إلى الكمبيوتر للوصول 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 127

## تعذر الاتصال بعد تهيئة تصفية IPsec/IP

قد تكون قيمة التعيين غير صحيحة.  
قم بتعطيل تصفية IPsec/IP من لوحة التحكم للطابعة. ثم قم بتوصيل الطابعة والكمبيوتر وإجراء إعدادات تصفية IPsec/IP مرة أخرى.

معلومات ذات صلة

← "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 127

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

قد تكون الإعدادات 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 141

## المشكلات الخاصة باستخدام شهادة رقمية

## تعذر استيراد شهادة موقعة من المرجع المصدق (CA)

هل تتطابق الشهادة الموقعة من المرجع المصدق (CA) والمعلومات الموجودة على طلب CSR؟  
إذا لم تكن الشهادة الموقعة من المرجع المصدق (CA) 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 المرجع المصدق؟  
احصل على شهادة موقعة من المرجع المصدق مرةً أخرى باستخدام طلب CSR.

## إعدادات الأمان المتقدمة لـ Enterprise

هل الشهادة الموقعة من المرجع المصدق أكبر من 5 كيلو بايت؟  
لا يمكنك استيراد شهادة موقعة من المرجع المصدق أكبر من 5 كيلو بايت.

هل كلمة مرور استيراد الشهادة صحيحة؟  
إذا نسيت كلمة المرور، فإنه يتعذر عليك استيراد الشهادة.

معلومات ذات صلة

← "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 118

## تعذر تحديث شهادة ذاتية التوقيع

هل تم إدخال Common Name؟  
لا بد من إدخال Common Name.

هل تم إدخال رموز غير مدعومة في Common Name؟ على سبيل المثال، الرموز اليابانية غير مدعومة.  
أدخل عدداً من الرموز يتراوح ما بين 1 إلى 128 رمزاً بتنسيق IPv4، أو IPv6، أو الاسم المضيف، أو FQDN بلغة (ASCII (0x20-0x7E).

هل 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

← "تحديث شهادة موقعة ذاتياً" في الصفحة 120

## يتعذر إنشاء طلب CSR

هل تم إدخال Common Name؟  
لا بد من إدخال Common Name.

هل تم إدخال أحرف غير مدعومة في State/Province, Locality, Organizational Unit, Organization, Common Name؟ على سبيل المثال، الرموز اليابانية غير مدعومة.

أدخل عدداً من الرموز بتنسيق IPv4، أو IPv6، أو الاسم المضيف، أو FQDN بلغة (ASCII (0x20-0x7E).

هل 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 115

## إعدادات الأمان المتقدمة لـ Enterprise

## ظهور تحذير مرتبط بشهادة رقمية

الرسائل	السبب/الحل
Enter a Server Certificate.	<p><b>السبب:</b> لم تقم بتحديد ملف لاستيراده.</p> <p><b>الحل:</b> حدد ملفاً وانقر فوق <b>Import</b>.</p>
CA Certificate 1 is not entered.	<p><b>السبب:</b> لم يتم إدخال شهادة المرجع المصدق (1 CA) وتم إدخال شهادة المرجع المصدق (2 CA) فقط.</p> <p><b>الحل:</b> قم باستيراد شهادة المرجع المصدق (1 CA) أولاً.</p>
Invalid value below.	<p><b>السبب:</b> توجد رموز غير مدعومة في مسار الملف و/أو كلمة المرور.</p> <p><b>الحل:</b> تأكد من إدخال الرموز بشكل صحيح للعنصر.</p>
Invalid date and time.	<p><b>السبب:</b> لم يتم تعيين تاريخ الطابعة ووقتها.</p> <p><b>الحل:</b> قم بتعيين التاريخ والوقت باستخدام Web Config، أو EpsonNet Config أو لوحة تحكم الطابعة.</p>
Invalid password.	<p><b>السبب:</b> لا تتطابق كلمة المرور المعينة لشهادة المرجع المصدق (CA) وكلمة المرور المدخلة.</p> <p><b>الحل:</b> أدخل كلمة المرور الصحيحة.</p>
Invalid file.	<p><b>السبب:</b> لم تقم باستيراد ملف شهادة بتنسيق X509.</p> <p><b>الحل:</b> تأكد من تحديد الشهادة الصحيحة المرسله بواسطة مرجع مصدق موثوق فيه.</p>
	<p><b>السبب:</b> الملف الذي تقوم باستيراده كبير للغاية. يصل الحد الأقصى لحجم الملف إلى 5 كيلو بايت.</p> <p><b>الحل:</b> إذا قمت بتحديد الملف الصحيح، فقد تكون الشهادة تالفة أو ملفقة.</p>
	<p><b>السبب:</b> السلسلة المضمنة في الشهادة غير صحيحة.</p> <p><b>الحل:</b> لمزيد من المعلومات حول الشهادة، انظر موقع الويب الخاص بالمرجع المصدق.</p>

## إعدادات الأمان المتقدمة لـ Enterprise

السبب/الحل	الرسائل
<p><b>السبب:</b> يحتوي ملف الشهادة بتنسيق PKCS#12 على أكثر من 3 شهادات مرجع مصدق (CA).</p> <p><b>الحل:</b> 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><b>السبب:</b> الشهادة منتهية الصلاحية.</p> <p><b>الحل:</b> <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 بشكل صحيح.</p>	The certificate has expired. Check if the certificate is valid, or check the date and time on your printer.
<p><b>السبب:</b> لا يوجد مفتاح خاص مزدوج مع الشهادة.</p> <p><b>الحل:</b> <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><b>السبب:</b> قمت بإعادة استيراد شهادة PEM/DER التي تم الحصول عليها من طلب CSR باستخدام تطبيق Web Config.</p> <p><b>الحل:</b> إذا كانت الشهادة بتنسيق PEM/DER وتم الحصول عليها من طلب CSR باستخدام تطبيق Web Config، يمكنك استيرادها مرة واحدة فقط.</p>	
<p><b>السبب:</b> يتعذر إتمام التكوين بسبب فشل الاتصال بين الطابعة والكمبيوتر أو تعذرت قراءة الملف نتيجة لبعض الأخطاء.</p> <p><b>الحل:</b> بعد فحص الملف المحدد والاتصال، قم باستيراد الملف مرة أخرى.</p>	Setup failed.

معلومات ذات صلة

← "حول المصادقة الرقمية" في الصفحة 115

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

هل يوجد ملف نسخة احتياطية للشهادة؟

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

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



## إعدادات الأمان المتقدمة لـ Enterprise

### معلومات ذات صلة

- ◀ "حذف شهادة موقعة من المرجع المصدق (CA)" في الصفحة 119
- ◀ "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 118