EPSON
EXCEED YOUR VISION

دليل المسؤول

NPD5668-00 AR

المحتويات

المحتويات

إعدادات الأمان المتقدمة لـ *Enterprise*

حقوق الطبع والنشر

العلامات التجارية

- ❏ ®EPSON علامة تجارية مسجَّلة، 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.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ 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 الماسحة الضوئية.

معلومات ذات صلة

يؤدي النقر فوق هذا الرمز إلى عرض معلومات ذات صلة.

الأوصاف المستخدمة في هذا الدليل

- لقطات الشاشة الخاصة ببرنامج تشغيل الماسحة الضوئية وشاشات Epson Scan 2 (برنامج تشغيل الماسحة 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"، "Windows XP"، و Windows Server 2016، و"Windows Server 2012 R2" و"Windows Server 2012" و"Windows Server 2008 R2" و"Windows Server 2008" و"Windows Server 2003 R2"، و"Windows Server 2003" إلى أنظمة التشغيل التالية. إضافة إلى ذلك، يُستخدم مصطلح "Windows" للإشارة إلى كل الإصدارات.

- 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، وOS X El Capitan، و OS X Yosemite، وOS X Mavericks، وOS X Mountain Lion، وMac OS X v10.7.x وMac OS X v10.6.8.

مقدمة

مكونات الدليل

يُعد هذا الدليل مخصصًا 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 أيضًا بيئة الشبكة، مثل معلومات خادم الوكيل و DNS واستخدام منفذ الجهاز.

إعدادات الوظيفة

لتوضيح إعدادات كل وظيفة بالجهاز.

إعدادات الأمان الأساسية

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

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، وخادم الوكيل، وخادم DNS، وخادم البريد الإلكتروني لمراقبة الاتصال عبر الإنترنت أو الشبكة.

المستخدم

الشخص الذي يستخدم الأجهزة مثل الطابعات والماسحات الضوئية.

Web Config (صفحة الويب للجهاز)

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

الأداة

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

المسح الضوئي السريع

مصطلح عام للمسح الضوئي من لوحة التحكم بالجهاز.

ASCII (الشفرة القياسية الأمريكية لتبادل المعلومات)

إحدى شفرات الرموز القياسية. يتم تحديد 128 رمزًا، بما في ذلك رموز مثل الحروف الأبجدية (a–z، وA–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	!	"	#	$	%	&	'	(	)	*	+	،	-	.	/
0	1	2	3	4	5	6	7	8	9	:	؛	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	]	\	[	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	}	|	{	~	

* حرف المسافة.

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.

تدفق إعدادات الماسحة الضوئية وإدارتها

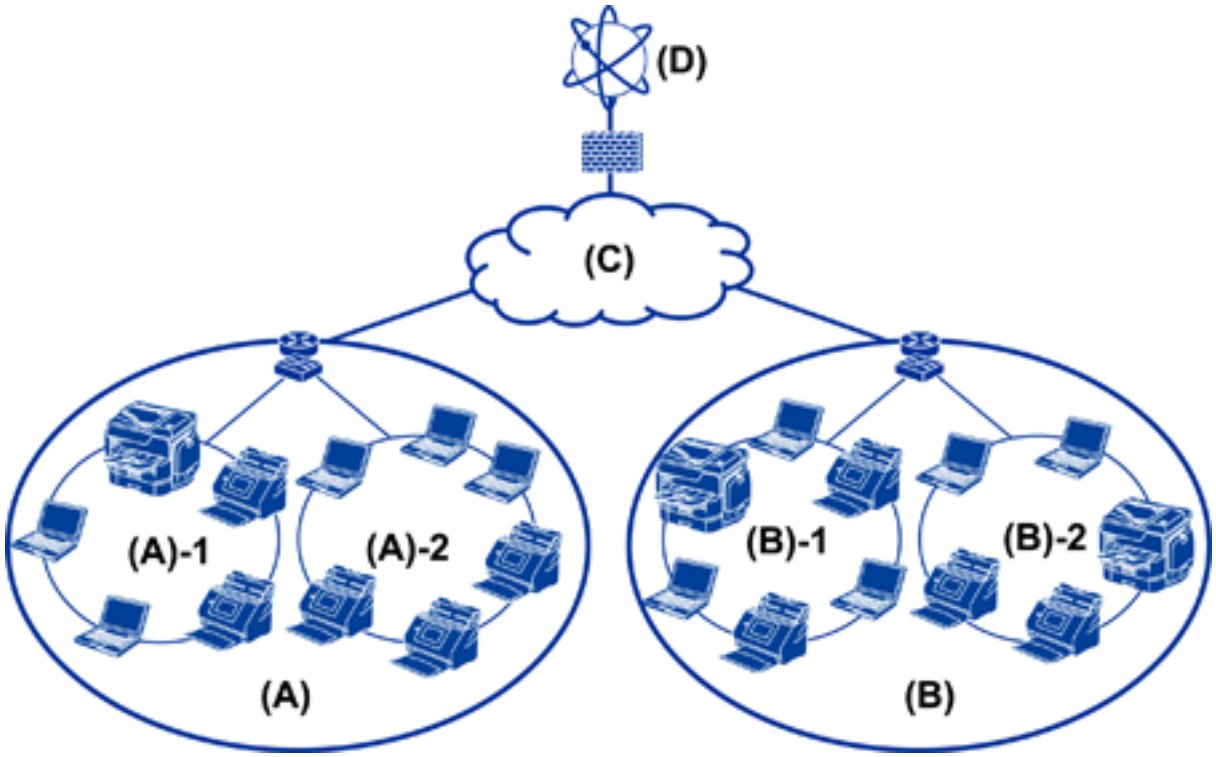
يقوم المسؤول بضبط إعدادات الاتصال بالشبكة، والإعداد المبدئي وصيانة الماسحة الضوئية بحيث تكون متوفرة للمستخدمين.

1. التهيئة
   - ❑ جمع معلومات إعداد الاتصال
   - ❑ تحديد طريقة الاتصال
2. التوصيل
   - ❑ اتصال الشبكة من لوحة التحكم بالماسحة الضوئية
3. إعداد الوظائف
   - ❑ إعدادات برنامج تشغيل الماسحة الضوئية
   - ❑ الإعدادات المتقدمة الأخرى
4. إعدادات الأمان
   - ❑ إعدادات المسؤول
   - ❑ SSL/TLS
   - ❑ الحكم في البروتوكول
   - ❑ إعدادات الأمان المتقدمة (خيار)
5. التشغيل والإدارة
   - ❑ التحقق من حالة الجهاز
   - ❑ التعامل مع ظهور الأحداث
   - ❑ نسخ إعدادات الجهاز احتياطيًا

معلومات ذات صلة

- ⬅ "التجهيز" في الصفحة 10
- ⬅ "الاتصال" في الصفحة 15
- ⬅ "إعدادات الوظيفة" في الصفحة 21
- ⬅ "إعدادات الأمان الأساسية" في الصفحة 31
- ⬅ "إعدادات الإدارة والتشغيل" في الصفحة 39

مثال على بيئة الشبكة



(أ): Office 1

- (أ) – LAN 1: 1
- (أ) – LAN 2: 2

(ب): Office 2

- (ب) – LAN 1: 1
- (ب) – LAN 2: 2

(جـ): WAN

(د): إنترنت

مقدمة حول مثال على إعداد اتصال الماسحة الضوئية

يوجد نوعان رئيسان من الاتصال حسب كيفية استخدام الماسحة الضوئية. كلاهما يصل الماسحة الضوئية بالشبكة المتصل بها الكمبيوتر من خلال موزع الشبكة.

- اتصال الخادم/العميل (الماسحة الضوئية باستخدام خادم Windows، وإدارة المهام)
- اتصال نظير إلى نظير (الاتصال المباشر من خلال كمبيوتر العميل)

معلومات ذات صلة

- "اتصال العميل/الخادم" في الصفحة 12
- "اتصال نظير إلى نظير" في الصفحة 12

اتصال العميل/الخادم

حدد الماسحة الضوئية وإدارة المهام مع Document Capture Pro Server المثبت على الخادم. يُعدّ ذلك أكثر الأمور الملائمة للعمل الذي يستخدم ماسحات ضوئية متعددة لإجراء المسح الضوئي على عدد كبير من المستندات بتنسيق محدد.

معلومات ذات صلة

"تعريفات المصطلحات المستخدمة في هذا الدليل" في الصفحة 8

اتصال نظير إلى نظير

استخدم ماسحة ضوئية فردية مع برنامج تشغيل الماسحة الضوئية مثل Epson Scan 2 المثبت على كمبيوتر العميل. تثبيت Document Capture (Document CapturePro) على كمبيوتر العميل يتيح لك تشغيل المهام على أجهزة كمبيوتر العميل الفردية الخاصة بالماسحة الضوئية.

معلومات ذات صلة

"تعريفات المصطلحات المستخدمة في هذا الدليل" في الصفحة 8

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 مقدمًا.

الأقسام	العناصر	ملاحظة
طريقة اتصال الجهاز	❑ شبكة الإيثرنت	استخدم كبلاً مزدوجًا مجدولاً مصفحًا (STP) من الفئة 5e أو أعلى لاتصال الإيثرنت.
معلومات اتصال LAN	❑ عنوان IP ❑ قناع الشبكة الفرعية ❑ البوابة الافتراضية	إذا قمت بتعيين عنوان IP تلقائيًا باستخدام وظيفة DHCP في جهاز التوجيه، فلا داعي لذلك.
معلومات خادم DNS	❑ عنوان IP لـ DNS الرئيسي ❑ عنوان IP لـ DNS الثانوي	إذا كنت تستخدم عنوان IP ثابتًا كعنوان IP، فقم بتكوين خادم DNS. قم بتكوينه عند تعيينه تلقائيًا باستخدام وظيفة DHCP وعند عدم إمكانية تعيين خادم DNS تلقائيًا.
معلومات خادم الوكيل	❑ اسم خادم الوكيل ❑ رقم المنفذ	قم بتكوينه عند استخدام خادم وكيل لاتصال الإنترنت وعند استخدام خدمة Epson Connect أو وظيفة التحديث التلقائية للبرنامج الثابت.

مواصفات الماسحة الضوئية

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

استخدام رقم المنفذ

راجع "الملحق" الخاص برقم المنفذ الذي تستخدمه الماسحة الضوئية.

معلومات ذات صلة

"استخدام منفذ للماسحة الضوئية" في الصفحة 56

نوع تعيين عنوان IP

يوجد نوعان لتعيين عنوان IP للماسحة الضوئية.

عنوان IP ثابت:

عينّ عنوان IP فريد محدد مسبقًا للماسحة الضوئية.

لا يتم تغيير عنوان IP حتى عند إيقاف تشغيل الماسحة الضوئية أو جهاز التوجيه، لذلك يمكنك إدارة الجهاز بواسطة عنوان IP.

يُعد ذلك النوع مناسبًا لشبكة يتم فيها إدارة العديد من الماسحات الضوئية مثل مكتب كبير أو مدرسة.

التعيين التلقائي عن طريق وظيفة DHCP:

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

إذا لم يكن هذا النوع ملائمًا لتغيير عنوان IP لجهاز محدد، فقم بحفظ عنوان IP مقدمًا ثم قم بتعيينه.

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، والماسحة الضوئية، والإنترنت (الخادم المقابل) بالنيابة عن كل منها. لا يتصل الخادم المقابل إلا بخادم الوكيل فقط. لذلك، يتعذر قراءة معلومات الماسحة الضوئية 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 الماسحة الضوئية، وقناع الشبكة الفرعية، والبوابة الافتراضية، تابع ما يلي.

استخدام لوحة التحكم:

قم بتكوين الإعدادات باستخدام لوحة تحكم الماسحة الضوئية لكل ماسحة ضوئية. اتصل بالشبكة بعد تكوين إعدادات الاتصال الخاصة بالماسحة الضوئية.

استخدام برنامج التثبيت:

إذا تم استخدام برنامج التثبيت، فسيتم تعيين شبكة الماسحة الضوئية والكمبيوتر العميل تلقائيًا. يتوفر الإعداد عن طريق اتباع إرشادات برنامج التثبيت، حتى إذا لم يكن لديك معرفة كبيرة بالشبكة.

استخدام أداة:

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

معلومات ذات صلة

"الاتصال بالشبكة من لوحة التحكم" في الصفحة 15

التجهيز

"الاتصال بالشبكة باستخدام برنامج التثبيت" في الصفحة 19
"تعيين عنوان IP باستخدام " في الصفحة 53EpsonNet Config

الاتصال

يوضح هذا الفصل البيئة أو الإجراءات اللازمة لتوصيل الماسحة الضوئية بالشبكة.

الاتصال بالشبكة

الاتصال بالشبكة من لوحة التحكم

قم بتوصيل الماسحة الضوئية بالشبكة باستخدام لوحة تحكم الماسحة الضوئية.

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

تعيين عنوان IP

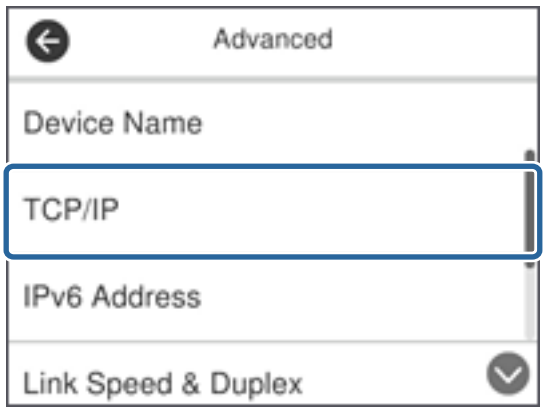
قم بإعداد العناصر الأساسية مثل عنوان IP، وقناع الشبكة الفرعية، والبوابة الافتراضية.

1. قم بتشغيل الماسحة الضوئية.
2. انقر بإصبعك على الشاشة لليسار على لوحة تحكم الماسحة الضوئية، ثم اضغط على **الإعدادات**.

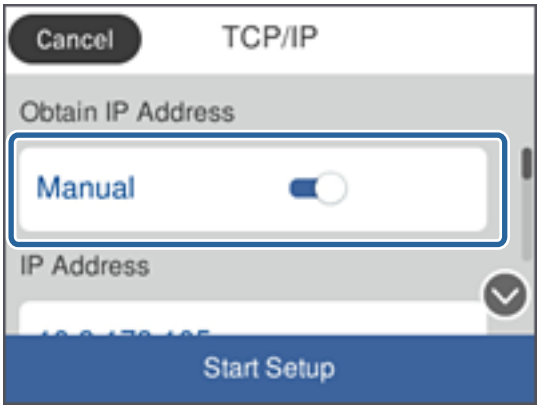
3. اضغط على **إعدادات الشبكة** > **تغيير الإعدادات**.

إذا لم يتم عرض العنصر، فانقر بإصبعك لأعلى على الشاشة لعرضه.

4. اضغط **TCP/IP**.

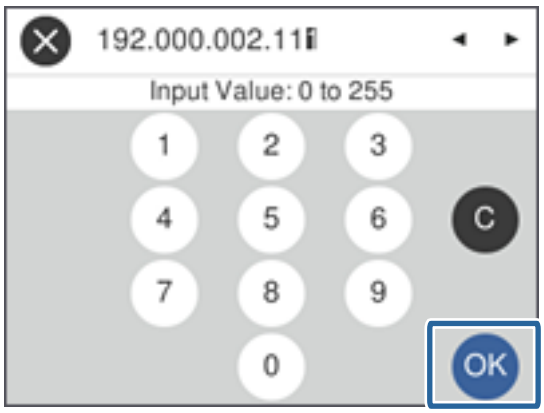


5. حدد **يدوي** لـ **الحصول على عنوان IP**.



ملاحظة:
عند تعيين عنوان *IP* تلقائيًا باستخدام وظيفة *DHCP* في جهاز التوجيه، حدد **تلقائي**. في هذه الحالة، تم تعيين **عنوان *IP***، و**قناع الشبكة الفرعية**، و**البوابة الافتراضية** في الخطوات من *6* إلى *7* تلقائيًا أيضًا، لذلك انتقل إلى الخطوة *8*.

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



تأكد من عرض القيمة على الشاشة السابقة.

7. اضبط **قناع الشبكة الفرعية** و**البوابة 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 **خادمDNS**، 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 **تلقائي** 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 **تلقائي** ، 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 **بدء الإعداد**.

11. اضغط على **إغلاق** على شاشة التأكيد.

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

الاتصال بشبكة الإيثرنت

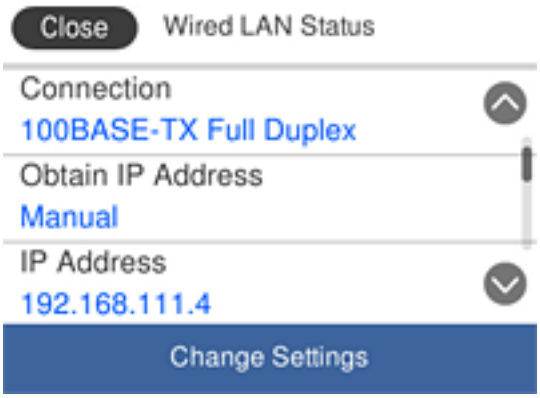
وصّل الماسحة الضوئية بالشبكة باستخدام كابل الإيثرنت، وتحقق من الاتصال.

1. وصّل الماسحة الضوئية وموزع الشبكة (جهاز التبديل L2) بكابل إيثرنت.

   يتغير الرمز في الشاشة الرئيسية إلى .

2. اضغط على على الشاشة الرئيسية.

3. انقر بإصبعك لأعلى على الشاشة، ثم تأكد من صحة حالة الاتصال وعنوان IP.

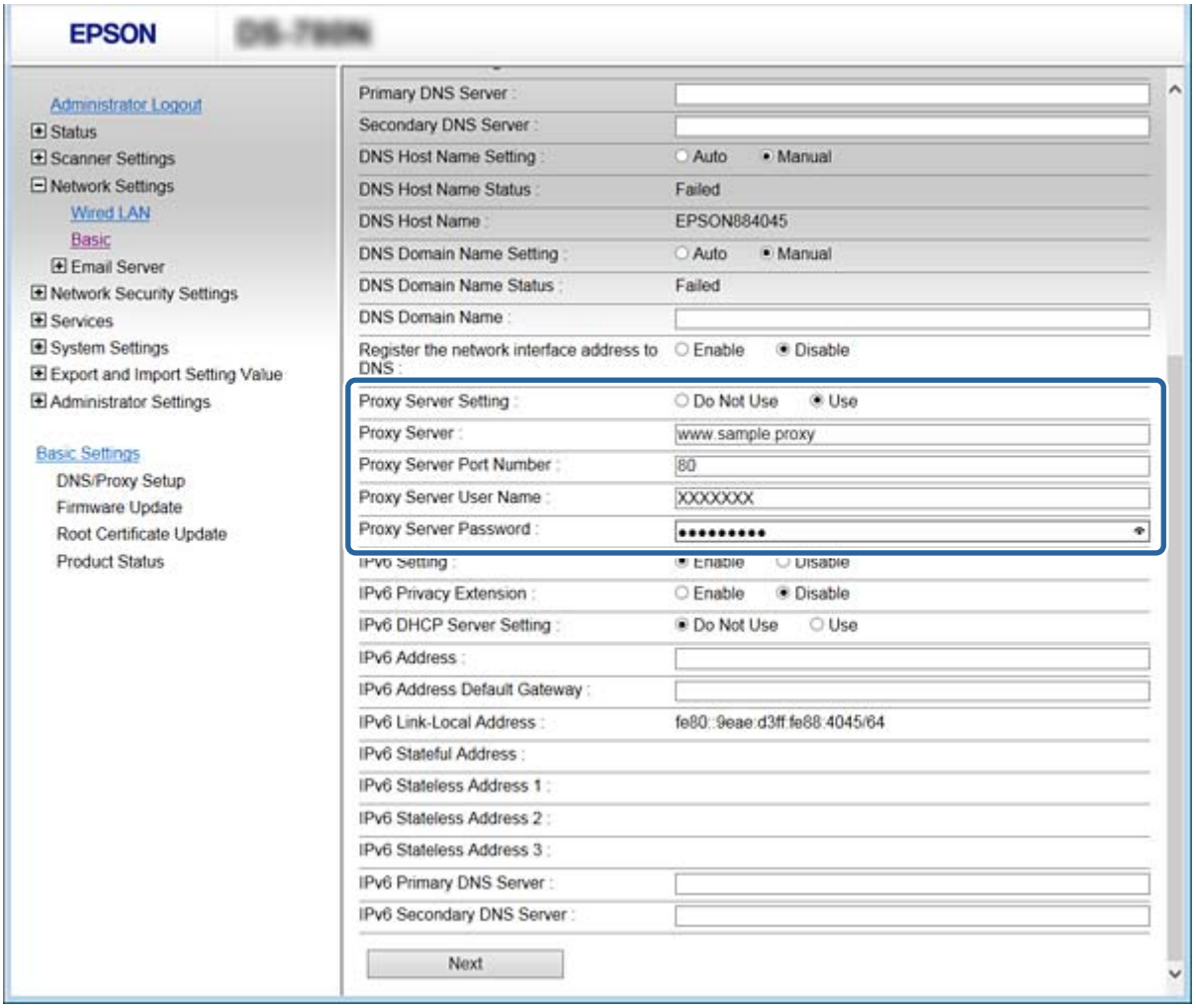


إعداد خادم الوكيل

يتعذر إعداد خادم الوكيل من اللوحة. قم بالتهيئة باستخدام Web Config.

1. قم بالوصول إلى Web Config وحدد **Basic** < **Network Settings**.
2. حدد **Use** في **Proxy Server Setting**.
3. حدد خادم الوكيل بعنوان IPv4 أو تنسيق FQDN في **الخادم الوكيل**، ثم أدخل رقم المنفذ في **Proxy Server Port Number**. ولخوادم الوكيل التي تتطلب مصادقة، أدخل اسم المستخدم وكلمة المرور لمصادقة خادم الوكيل.

4. انقر فوق زر **Next**.



5. أكد الإعدادات، ثم انقر فوق **الإعدادات**.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22

الاتصال بالشبكة باستخدام برنامج التثبيت

نوصي باسخدام برنامج التثبيت لتوصيل الماسحة الضوئية 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 للطُرز المزودة بقرص برامج والمستخدمين الذين يمتلكون أجهزة كمبيوتر مزودة بمحركات أقراص.)

أدخل قرص البرامج داخل جهاز الكمبيوتر، ثم اتبع التعليمات المعروضة على الشاشة.

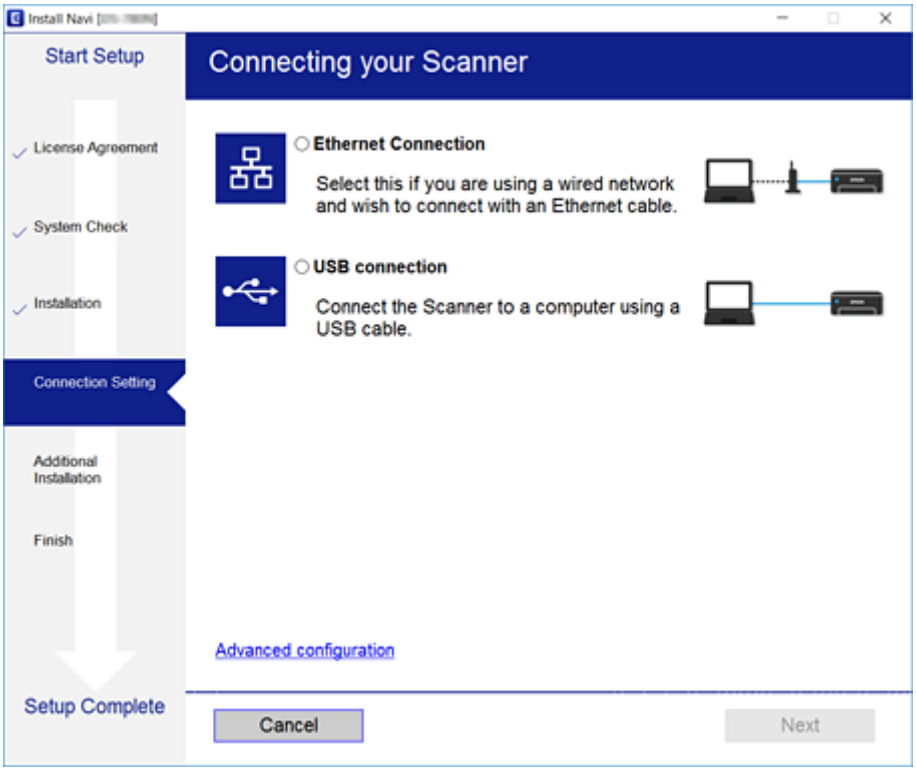
تحديد طرق الاتصال

اتبع التعليمات المعروضة على الشاشة إلى أن يتم عرض الشاشة التالية، ثم حدد طريقة اتصال الماسحة الضوئية بالكمبيوتر.

الاتصال

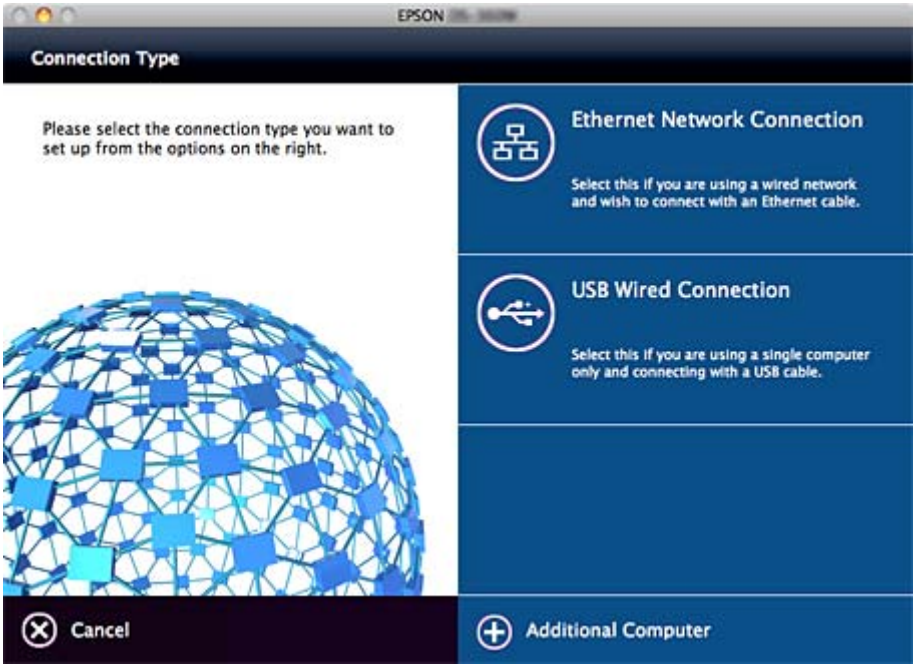
❏ Windows

حدد نوع الاتصال ثم انقر فوق **التالي**.



❏ Mac OS

حدد نوع الاتصال.



اتبع التعليمات المعروضة على الشاشة. تم تثبيت البرنامج الضروري.

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 Web Config

Web Config هو تطبيق مستند على المستعرض وخاص بتكوين إعدادات الماسحة الضوئية.

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

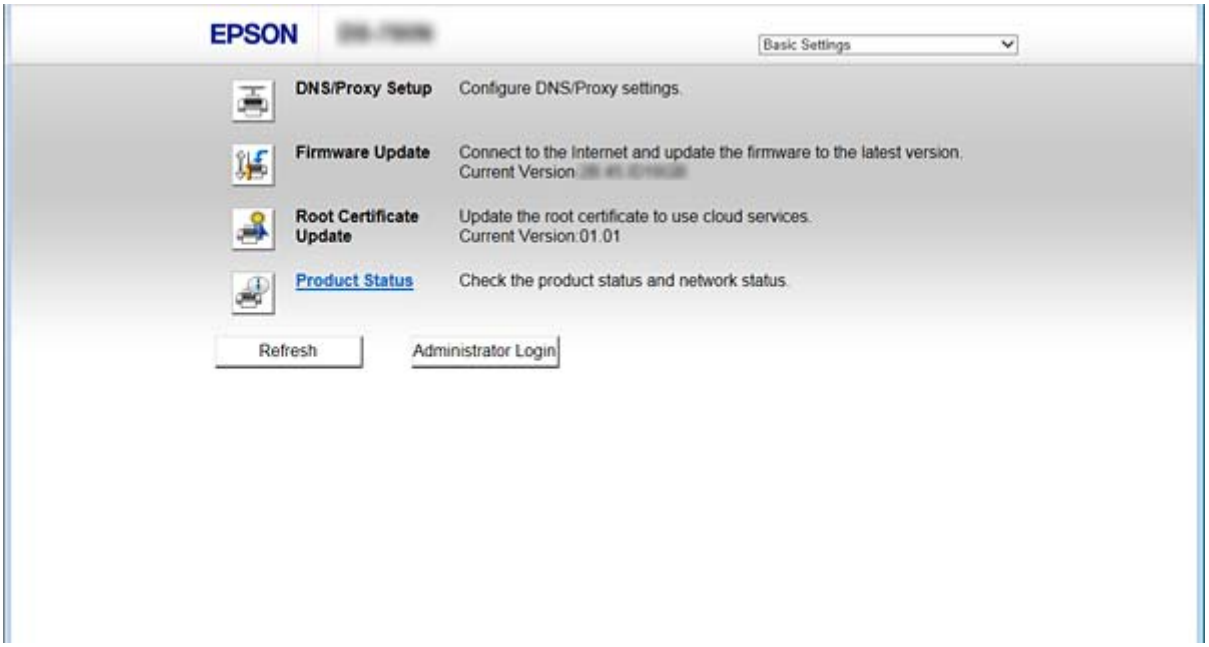
ملاحظة:

يمكنك تأمين الإعدادات من خلال تكوين كلمة مرور المسؤول للماسحة الضوئية.

توجد صفحتا إعداد وفقًا لما هو موضح أدناه.

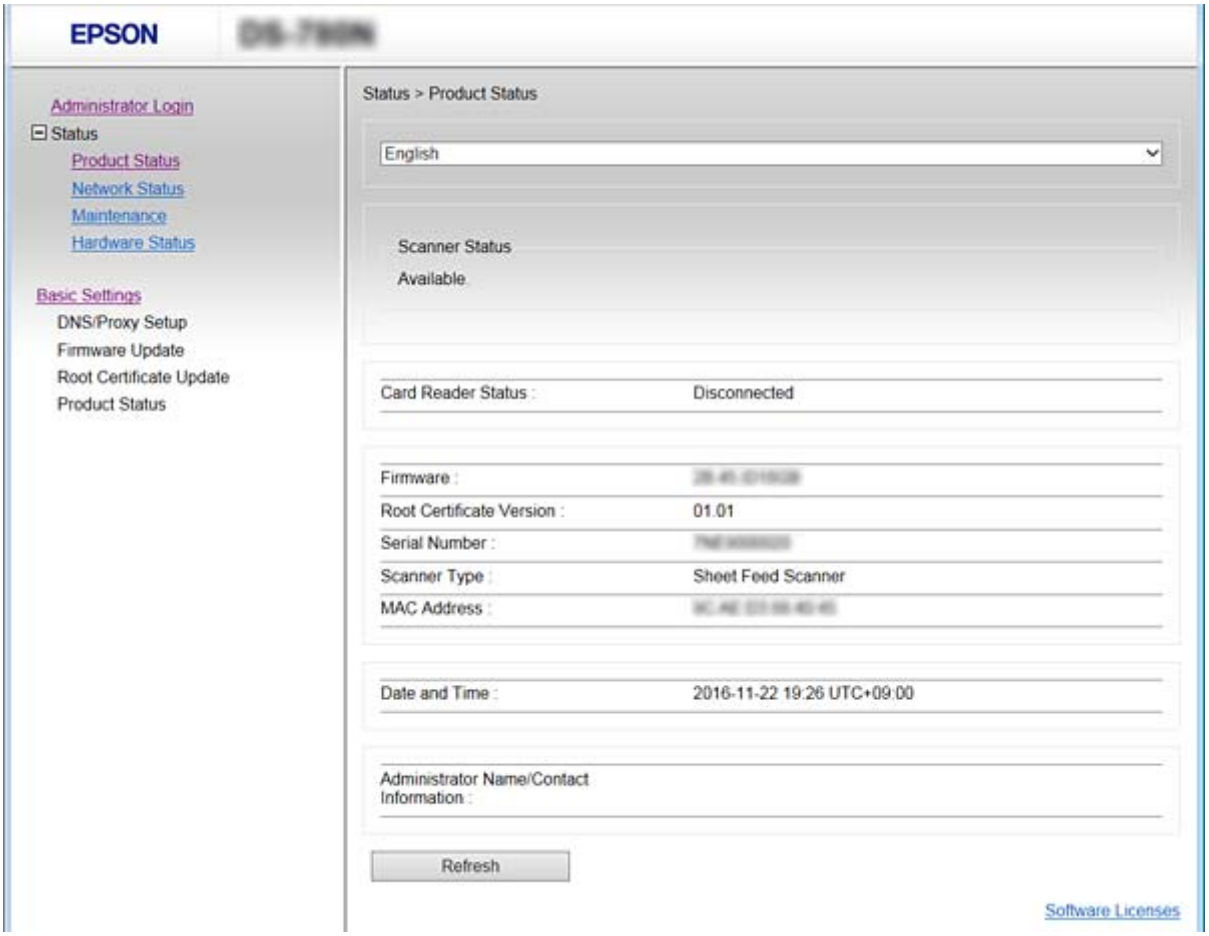
❏ **Basic Settings**

يمكنك تكوين الإعدادات الأساسية للماسحة الضوئية.



❏ **Advanced Settings**

يمكنك تكوين الإعدادات المتقدمة للماسحة الضوئية. هذه الصفحة موجهة للمسؤول بشكلٍ رئيسي.



الوصول إلى تطبيق Web Config

أدخل عنوان IP للماسحة الضوئية في مستعرض الويب. يجب تمكين JavaScript. عند الوصول إلى تطبيق Web Config عبر HTTPS، ستظهر رسالة تحذير في المستعرض نظرًا لاستخدام الشهادة الموقعة ذاتيًا المخزنة في الماسحة الضوئية.

❏ الوصول عبر HTTPS

IPv4: https://<عنوان IP الماسحة الضوئية> (دون < >)

IPv6: https://[عنوان IP الماسحة الضوئية]/ (مع [ ])

❏ الوصول عن طريق بروتوكول HTTP

IPv4: http://<عنوان IP الماسحة الضوئية> (دون < >)

IPv6: http://[عنوان IP الماسحة الضوئية]/ (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 الماسحة الضوئية مسجلاً مع خادم *DNS*، يمكنك استخدام اسم الماسحة الضوئية بدلاً من عنوان *IP* الخاص بها.

معلومات ذات صلة

◆ "اتصال SSL/TLS بالماسحة الضوئية" في الصفحة 59

◆ "حول المصادقة الرقمية" في الصفحة 59

استخدام وظائف المسح الضوئي

حسب كيفية استخدامك للماسحة الضوئية، قم بتثبيت البرنامج التالي وإجراء الإعدادات باستخدامه.

❏ **المسح الضوئي من الكمبيوتر**

❏ أكد على صلاحية خدمة مسح الشبكة باستخدام Web Config (الصلاحية متاحة في شحن المصنع).

❏ ثبّت Epson Scan 2 على جهاز الكمبيوتر وقم بتعيين عنوان IP

❏ عند إجراء المسح الضوئي، قم بتثبيت Document CaptureDocument Capture Pro)) وضبط إعدادات المهام.

❏ **المسح الضوئي من لوحة التشغيل**

❏ عند استخدام Document Capture Pro أو Document Capture Pro Server:

قم بتثبيت Document Capture Pro أو Document Capture Pro Server

إعداد DCP (وضع الخادم، وضع العميل).

❏ عند استخدام بروتوكول WSD:

أكد على صلاحية WSD على Web Config أو لوحة التشغيل (الصلاحية متاحة في شحن المصنع)

إعدادت أجهزة إضافية (كمبيوتر يعمل بنظام تشغيل Windows).

المسح الضوئي من جهاز كمبيوتر

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

معلومات ذات صلة

◆ "تثبيت البرنامج" في الصفحة 24

◆ "تمكين مسح الشبكة" في الصفحة 24

تثبيت البرنامج

❏ Epson Scan 2

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

من خلال EpsonNet SetupManager يُمكن توزيع برامج تشغيل الطابعة كذلك معًا كحزم.

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

قم بتثبيته على كمبيوتر عميل. يُمكنك استدعاء المهام المسجلة على الكمبيوتر وتنفيذها باستخدام DocumentDocument Capture Pro/ Capture المثبت على الشبكة من الكمبيوتر ولوحة تشغيل الماسحة الضوئية.

يُمكنك كذلك إجراء المسح الضوئي من الكمبيوتر عبر الشبكة. يلزم توفير Epson Scan 2 لإجراء المسح الضوئي.

معلومات ذات صلة

"EpsonNet SetupManager" في الصفحة 53

عيّن عنوان IP للماسحة الضوئية إلى Epson Scan 2

حدد عنوان IP للماسحة الضوئية حتى يُمكن استخدامها على الشبكة.

1. ابدأ **Epson Scan 2 Utility** من **قائمة البدء** > **كل البرامج** > **EPSON** > **Epson Scan 2**.

   إذا كانت ماسحة ضوئية أخرى تم تسجيلها بالفعل، فانتقل إلى الخطوة 2.

   إذا لم تكن مسجلة بالفعل، فانتقل إلى الخطوة 4.

2. انقر فوق ▼ على **ماسحة ضوئية**.
3. انقر فوق **الإعدادات**.
4. انقر فوق **تمكين التحرير**، ثم انقر فوق **إضافة**.
5. حدد اسم طراز الماسحة الضوئية من **الطراز**.
6. حدد عنوان IP الخاص بالماسحة الضوئية حتى يُمكن استخدامها من **العنوان** في **البحث عن الشبكة**.

   انقر فوق  وانقر فوق  لتحديث القائمة. إذا لم تعثر على عنوان IP للماسحة الضوئية، فحدد **إدخال عنوان** وأدخل عنوان IP.

7. انقر فوق **إضافة**.
8. انقر فوق **موافق**.

تمكين مسح الشبكة

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

1. قم بالوصول إلى تهيئة الويب وحدد **Services** > **Network Scan**.
2. تأكد من تحديد **Enable scanning** لـ **EPSON Scan**.

   إذا تم تحديده، تُستكمل المهام. أغلق تهيئة الويب.

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 22

المسح الضوئي باستخدام لوحة التحكم

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

عند إرسال نتائج المسح الضوئي، قم بإعداد المهمة باستخدام Document Capture Pro Server أو Document Capture Pro.

للاطلاع على تفاصيل حول الإعدادات وإعداد هذه المهمة، اطلع على مستندات Document Capture Pro Server أو Document Capture Pro أو تعليماته.

معلومات ذات صلة

"إعدادات Document Capture Pro Server/Document Capture Pro" في الصفحة 25
"إعدادات الخوادم والمجلدات" في الصفحة 26

تثبيت البرنامج على الكمبيوتر

❏ **Document Capture Pro Server**

يُعد ذلك إصدار الخادم من Document Capture Pro. قم بتثبيته على خادم Windows. يمكن إدارة أجهزة ومهام متعددة مركزيًا عبر الخادم. يمكن تنفيذ المهام من ماسحات ضوئية متعددة في وقتٍ واحد.

عن طريق استخدام الإصدار المعتمد من Document Capture Pro Server، يمكنك إدارة المهام وإجراء المسح الضوئي على السجل ذي الصلة بالمستخدمين والمجموعات.

لمزيد من التفاصيل حول Document Capture Pro Server، اتصل بمكتب Epson المحلي.

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

فضلاً عن إجراء المسح الضوئي من الكمبيوتر، يمكنك أيضًا استدعاء المهام المسجلة على الكمبيوتر من لوحة التحكم وتنفيذها. لا يمكن تشغيل مهام الكمبيوتر من ماسحات ضوئية متعددة في وقتٍ واحد.

إعدادات Document Capture Pro Server/Document Capture Pro

اضبط الإعدادات لاستخدام وظيفة المسح الضوئي من لوحة تشغيل الماسحة الضوئية.

1. قم بالوصول إلى Web Config وحدد **Services** > **Document Capture Pro**.

2. حدد **وضع التشغيل**.

❏ Server Mode:

حدد ذلك عند استخدام Document Capture Pro Server أو عند استخدام Document Capture Pro فقط للمهام التي تم إعدادها لكمبيوتر محدد.

❏ Client Mode:

اضبط ذلك عند تحديد إعداد المهمة من Document CaptureDocument Capture Pro)) المثبت على جميع أجهزة كمبيوتر العميل في الشبكة بدون تحديد الكمبيوتر.

3. اضبط التالي وفقًا للوضع المحدد.

❏ Server Mode:

في **Server Address**، حدد الخادم الذي تم تثبيت Document Capture Pro Server عليه. يُمكن استخدام عدد من الرموز يتراوح ما بين رمزين إلى 252 رمزًا بتنسيق IPv4، أو IPv6، أو الاسم المضيف، أو FQDN. في تنسيق FQDN، يُمكن استخدام أحرف، وأرقام، وأحرف أبجدية، والعلامات الواصلة بتنسيق ASCII للولايات المتحدة (باستثناء البادئة والخاتمة).

❏ Client Mode:

حدد **Group Settings** لاستخدام مجموعة ماسحات ضوئية محددة من Document CaptureDocument Capture Pro)).

4. انقر فوق **الإعدادات**.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22

إعدادات الخوادم والمجلدات

يحفظ Document Capture Pro وDocument Capture Pro Server البيانات الممسوحة ضوئيًا إلى الخادم أو كمبيوتر العميل مرة واحدة ويستخدم وظيفة الإرسال لتنفيذ مهمة المسح الضوئي إلى المجلد ومهمة المسح الضوئي إلى البريد الإلكتروني.

أنت بحاجة إلى الإذن والمعلومات للإرسال من الكمبيوتر حيثما تم تثبيت Document Capture Pro، Document Capture Pro Server إلى الكمبيوتر أو الخدمة السحابية.

قم بتحضير المعلومات حول المهمة التي ستستخدمها، بالرجوع إلى التالي.

يُمكنك ضبط الإعدادات لهذه المهام باستخدام Document Capture Pro أو Document Capture Pro Server. للاطلاع على تفاصيل حول الإعدادات، اطلع على مستندات Document Capture Pro Server أو Document Capture Pro أو تعليماته.

الاسم	الإعدادات	المتطلبات
المسح الضوئي إلى مجلد الشبكة (SMB)	إنشاء مجلد الحفظ وإعداد مشاركته	حساب مستخدم إداري للكمبيوتر الذي يُنشئ مجلدات حفظ.
	وجهة المسح الضوئي إلى مجلد الشبكة (SMB)	اسم مستخدم وكلمة مرور لتسجيل الدخول للكمبيوتر الذي يحتوي على مجلد حفظ، وميزة تحديثه.
المسح الضوئي إلى مجلد الشبكة (FTP)	إعداد تسجيل الدخول لخادم FTP	معلومات تسجيل الدخول لخادم FTP وميزة تحديث مجلد الحفظ.
المسح الضوئي إلى البريد الإلكتروني	الإعداد الخاص بخادم البريد الإلكتروني	معلومات إعداد خادم البريد الإلكتروني
المسح الضوئي إلى Document Capture Pro (عند استخدام Document Capture Pro Server)	إعداد تسجيل الدخول للخدمات السحابية	بيئة الاتصال بالإنترنت تسجيل الحساب للخدمات السحابية

استخدم المسح الضوئي من Windows) WSD فقط)

إذا كان الكمبيوتر يعمل بنظام تشغيل Windows Vista أو الإصدارات الأحدث، يُمكنك استخدام المسح الضوئي من WSD.

عند احتمالية استخدام بروتوكول WSD، سيتم عرض قائمة **الكمبيوتر (WSD)** على لوحة التحكم بالماسحة الضوئية.

1. قم بالوصول إلى Web Config وحدد **Services** > **Protocol**.
2. تأكد من وضع علامة على **Enable WSD** في **WSD Settings**.
إذا تم وضع علامة عليها، تُستكمل المهمة ويجوز لك إغلاق Web Config.
إذا لم يتم وضع علامة عليها، فضع العلامة وتابع إلى الخطوة التالية.
3. انقر فوق زر **Next**.
4. أكد على اختيار الإعدادات، وانقر فوق **الإعدادات**.

ضبط إعدادات النظام

ضبط إعدادات النظام على لوحة التحكم

ضبط سطوع الشاشة

اضبط سطوع شاشة LCD.

1. اضغط على **الإعدادات** على الشاشة الرئيسية.
2. اضغط على **الإعدادات العامة** > **سطوع LCD**.
3. اضغط على أو لتعديل السطوع.
يُمكن إجراء التعديل من درجة واحدة إلى 9 درجات.
4. اضغط **موافق**.

ضبط الصوت

اضبط صوت تشغيل اللوحة وصوت رسالة الخطأ.

1. اضغط على **الإعدادات** على الشاشة الرئيسية.
2. اضغط على **الإعدادات العامة** > **الصوت**.
3. اضبط العناصر التالية حسب الضرورة.
- ❏ صوت التشغيل
اضبط مستوى صوت التشغيل الخاص بلوحة التشغيل.
- ❏ صوت رسالة الخطأ
اضبط مستوى صوت رسالة الخطأ.
4. اضغط **موافق**.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22

الكشف عن التغذية المزدوجة للمستندات الأصلية

حدد وظيفة الكشف عن التغذية المزدوجة للمستندات التي يتم إجراء المسح الضوئي عليها أو لإيقاف المسح الضوئي عند حدوث التغذية المتعددة.

لإجراء المسح الضوئي على المستندات الأصلية التي تُعتبر تمت تغذيتها بأوراق متعددة، مثل الأظرف أو الورق المزود بملصقات، قم بتعيينها إلى إيقاف.

ملاحظة:
يمكن تعيينها كذلك من *Web Config* أو *Epson Scan 2*.

1. اضغط على **الإعدادات** على الشاشة الرئيسية.
2. اضغط على **إعدادات المسح الضوئي الخارجي** > **كشف تغذية مزدوجة بموج فوق صوتي**.
3. اضغط على **كشف تغذية مزدوجة بموج فوق صوتي** لفتحها أو إغلاقها.
4. اضغط **إغلاق**.

تعيين وضع السرعة المنخفضة

اضبط المسح الضوئي على السرعة المنخفضة حتى لا يحدث انحشار للورق عند إجراء المسح الضوئي للمستندات الرقيقة مثل الوريقات.

1. اضغط على **الإعدادات** على الشاشة الرئيسية.
2. اضغط على **إعدادات المسح الضوئي الخارجي** > **بطئ**.
3. اضغط على **بطئ** لفتحها أو إغلاقها.
4. اضغط **إغلاق**.

ضبط إعدادات النظام باستخدام تهيئة الويب

إعدادات توفير الطاقة أثناء فترة الخمول

قم بضبط إعداد توفير الطاقة لفترة خمول الماسحة الضوئية. عيّن الوقت حسب بيئة الاستخدام.

ملاحظة:
يمكنك أيضًا ضبط إعدادات توفير الطاقة على لوحة التحكم بالماسحة الضوئية.

1. قم بالوصول إلى Web Config وحدد **System Settings** > **Power Saving**.
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**.
4. انقر فوق **OK**.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22

إعداد لوحة التحكم

إعداد لوحة التحكم بالمساحة الضوئية. يمكنك ضبط الإعدادات على النحو التالي.

1. قم بالوصول إلى Web Config وحدد **Control Panel** < **System Settings**.
2. اضبط العناصر التالية حسب الضرورة.

❏ Language

حدد اللغة المعروضة على لوحة التحكم.

❏ Panel Lock

إذا حددت **ON**، فسيلزم توفير كلمة مرور المسؤول عند إجرائك 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 مسؤولاً، فسيتم تسجيل خروجك تلقائيًا 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 22

إعداد قيود الواجهة الخارجية

يمكنك تقييد اتصال USB من الكمبيوتر. اضبطه على تقييد المسح الضوئي بخلاف إجرائه عبر الشبكة.

1. قم بالوصول إلى Web Config وحدد **External Interface** < **System Settings**.
2. حدّد **Enable** أو **Disable**.

للتقييد، حدد **Disable**.

3. اضغط **OK**.

مزامنة التاريخ والوقت مع خادم الوقت

إذا كنت تستخدم شهادة المرجع المصدق (CA)، يمكنك الحد من حدوث مشكلات في الوقت.

1. قم بالوصول إلى Web Config وحدد **Time Server** < **Date and Time** < **System Settings**.
2. حدد **Use** لـ **Use Time Server**.
3. أدخل عنوان خادم الوقت لـ **Time Server Address**.

يمكنك استخدام تنسيق IPv4، أو IPv6، أو FQDN. أدخل 252 حرفًا أو أقل. إذا لم تحدد ذلك، فاتركه فارغًا.

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 22

إعدادات الأمان الأساسية

يوضح هذا الفصل إعدادات الأمان الأساسية التي لا تتطلب بيئة خاصة.

مقدمة عن ميزات الأمان الأساسية

نوضح ميزات الأمان الأساسية لأجهزة Epson.

اسم الميزة	نوع الميزة	ما الذي يتم تعيينه	ما الذي يتم حظره
إعداد كلمة مرور المسؤول	قم بتأمين الإعدادات ذات الصلة بالنظام، مثل إعدادات اتصال الشبكة وUSB، حتى لا يُمكن تغييرها إلا من قبل المسؤول.	يعيّن 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 أيضًا الحد من وجود مجموعة كبيرة من المخاطر الأمنية مثل تسرب المعلومات المتعلقة ببيئة الشبكة أو سياسة الأمان.
اتصالات SSL/TLS	عند الوصول إلى خادم Epson على الإنترنت من الجهاز، مثل الاتصال بالكمبيوتر من خلال مستعرض ويب أو تحديث البرنامج الثابت، يتم تشفير محتويات الاتصال باستخدام اتصالات SSL/TLS.	احصل على شهادة موقعة من جهة تصديق (CA)، ثم قم باستيرادها إلى الماسحة الضوئية.	يحظر مسح أي معلومات خاصة بتعريف الجهاز بالشهادة الموقعة من جهة تصديق (CA) التعرض لأي عملية انتحال والوصول غير المعتمد. وبالإضافة إلى ذلك، تتم حماية محتويات اتصال SSL/TLS، ويحظر تسريب بيانات الطباعة ومعلومات الإعداد.
التحكم في البروتوكولات	يتحكم في البروتوكولات المستخدمة للاتصال بين الأجهزة وأجهزة الحاسوب، وتمكين/تعطيل الوظائف.	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.

معلومات ذات صلة

- "حول Web Config" في الصفحة 21
- "EpsonNet Config" في الصفحة 52
- "Epson Device Admin" في الصفحة 52
- "تكوين كلمة مرور المسؤول" في الصفحة 31
- "التحكم في البروتوكولات" في الصفحة 34

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 الماسحة الضوئية، 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 32
- "تكوين كلمة مرور المسؤول باستخدام Web Config" في الصفحة 32
- "EpsonNet Config" في الصفحة 52

"Epson Device Admin" في الصفحة 52

تكوين كلمة مرور المسؤول من لوحة التحكم

يمكنك تعيين كلمة مرور المسؤول من لوحة التحكم بالماسحة الضوئية.

1. اضغط على **الإعدادات** على الشاشة الرئيسية.
2. اضغط على **إدارة النظام** > **إعدادات المسؤول**.
   إذا لم يتم عرض العنصر، فانقر بإصبعك لأعلى على الشاشة لعرض العنصر.
3. اضغط على **كلمة مرور المسؤول** > **تسجيل**.
4. أدخل كلمة مرور جديدة، ثم اضغط على **موافق**.
5. أدخل كلمة المرور مرة أخرى، ثم اضغط على **موافق**.
6. اضغط على **موافق** على شاشة التأكيد.
   يتم عرض شاشة إعدادات المسؤول.
7. اضغط على **إعداد القفل**، ثم اضغط على **موافق** على شاشة التأكيد.
   يتم تعيين إعداد القفل على **شغل**، سيتم طلب كلمة مرور المسؤول عندما تقوم بتمكين عنصر القائمة المغلق.

ملاحظة:

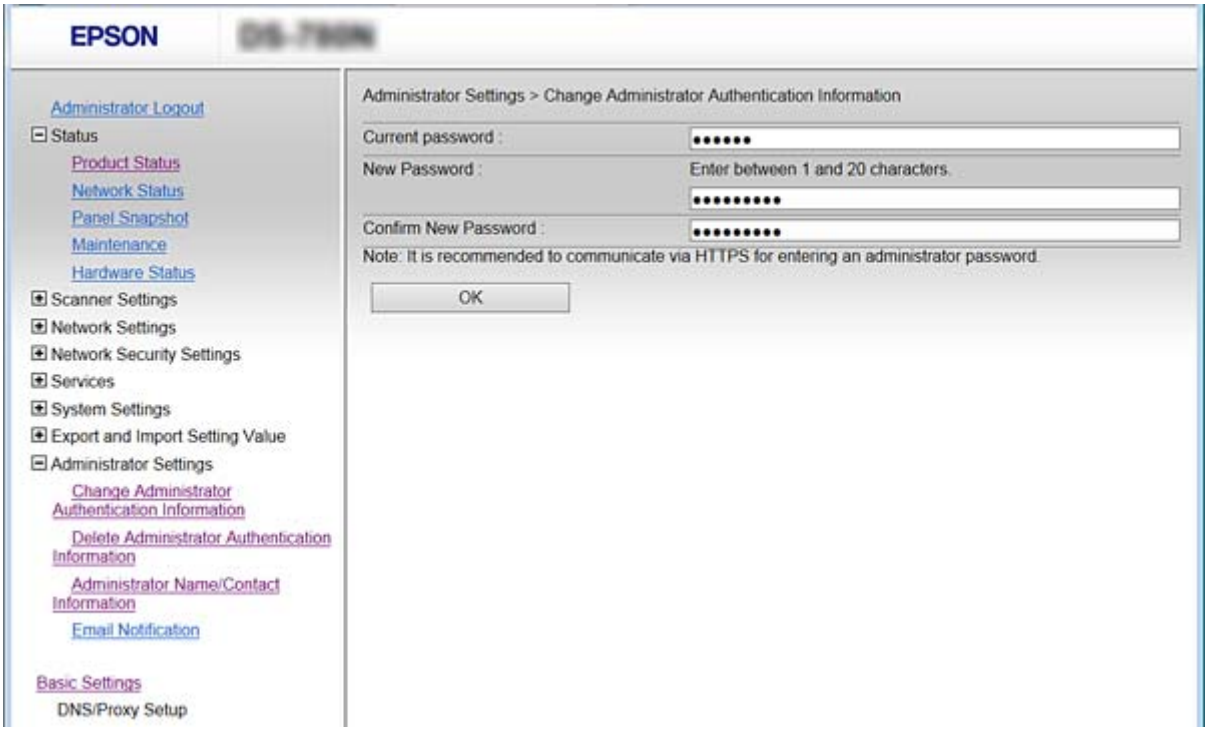
- إذا قمت بتعيين **الإعدادات** > **الإعدادات العامة** > **انتهى وقت العملية** إلى **شغل**، فستقوم الماسحة الضوئية بتسجيل خروجك بعد مرور فترة الخمول على لوحة التحكم.
- يمكنك تغيير كلمة مرور المسؤول أو حذفها عند تحديد **تغيير** أو **إعادة تعيين** على شاشة **كلمة مرور المسؤول** وأدخل كلمة مرور المسؤول.

تكوين كلمة مرور المسؤول باستخدام Web Config

يمكنك تعيين كلمة مرور المسؤول باستخدام Web Config.

1. قم بالوصول إلى Web Config وحدد **Administrator Settings** > **Change Administrator Authentication Information**.

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 22

العناصر التي يتم قفلها عن طريق كلمة مرور المسؤول

لدى المسؤولين امتياز إعداد أو تغيير لجميع الميزات على الأجهزة.

بالإضافة إلى ذلك، إذا قمت بتعيين كلمة مرور المسؤول على أحد الأجهزة، يمكنك تأمينها حتى لا تسمح بتغيير العناصر المرتبطة بإدارة الجهاز.

ما يلي العناصر التي يتمكن المسؤول من التحكم بها.

العنصر	الوصف
إعداد الماسحة الضوئية	إعداد الكشف عن التغذية المزدوجة ووضع السرعة المنخفضة.
إعدادات الاتصال بشبكة إيثرنت	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، ومسح الشبكة وخدمات Document Capture Pro.

إعدادات الأمان الأساسية

العنصر	الوصف
إعداد خادم البريد الإلكتروني	إعداد خادم البريد الإلكتروني الذي تتصل به الأجهزة مباشرة.
إعداد الأمان	إعدادات أمان الشبكة، مثل اتصال SSL/TLS، وتصفية IPsec/IP، وIEEE802.1X.
تحديث شهادة المصدر	تحديث شهادات المصدر مطلوب لمصادقة Document Capture Pro Server وتحديث البرنامج الثابت من Web Config.
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.
إعدادات استعادة الإعدادات الافتراضية	إعداد الماسحة الضوئية لإعادة تعيينها إلى إعدادات المصنع.
إعداد المسؤول	إعداد قفل المسؤول أو كلمة مرور المسؤول.
إعداد الجهاز المعتمد	إعداد المعرف الخاص بجهاز المصادقة. يتم تعيينه عند استخدام الماسحة الضوئية على نظام مصادقة يدعم أجهزة المصادقة.

التحكم في البروتوكولات

يمكنك إجراء المسح الضوئي باستخدام مجموعة متنوعة من الممرات والبروتوكولات. يمكنك كذلك استخدام المسح الضوئي للشبكة من عدد غير محدد من أجهزة الكمبيوتر المتصلة بالشبكة. على سبيل المثال، يسمح لك بإجراء المسح الضوئي فقط باستخدام مجموعة محددة من الممرات والبروتوكولات. يمكنك تقليل المخاطر الأمنية غير المقصودة من خلال تقييد المسح الضوئي من ممرات محددة أو عن طريق التحكم في الوظائف المتاحة.

قم بتهيئة إعدادات البروتوكول.

1. قم بالوصول إلى Web Config وحدد **Services** > **Protocol**.
2. قم بتهيئة كل عنصر.
3. انقر فوق **Next**.
4. انقر فوق **OK**.

تم تطبيق الإعدادات على الماسحة الضوئية.

معلومات ذات صلة

- "الوصول إلى تطبيق Web Config" في الصفحة 22
- "البروتوكولات التي تستطيع تمكينها أو تعطيلها" في الصفحة 34
- "عناصر إعداد البروتوكول" في الصفحة 36

البروتوكولات التي تستطيع تمكينها أو تعطيلها

البروتوكول	الوصف
Bonjour Settings	يمكنك تحديد إمكانية استخدام Bonjour. يتم استخدام Bonjour للبحث عن أجهزة، والمسح الضوئي وما إلى ذلك.
SLP Settings	من الممكن أيضًا تمكين وظيفة SLP أو تعطيلها. تُستخدم SLP لـ Epson Scan 2 وبحث الشبكة في EpsonNet Config.

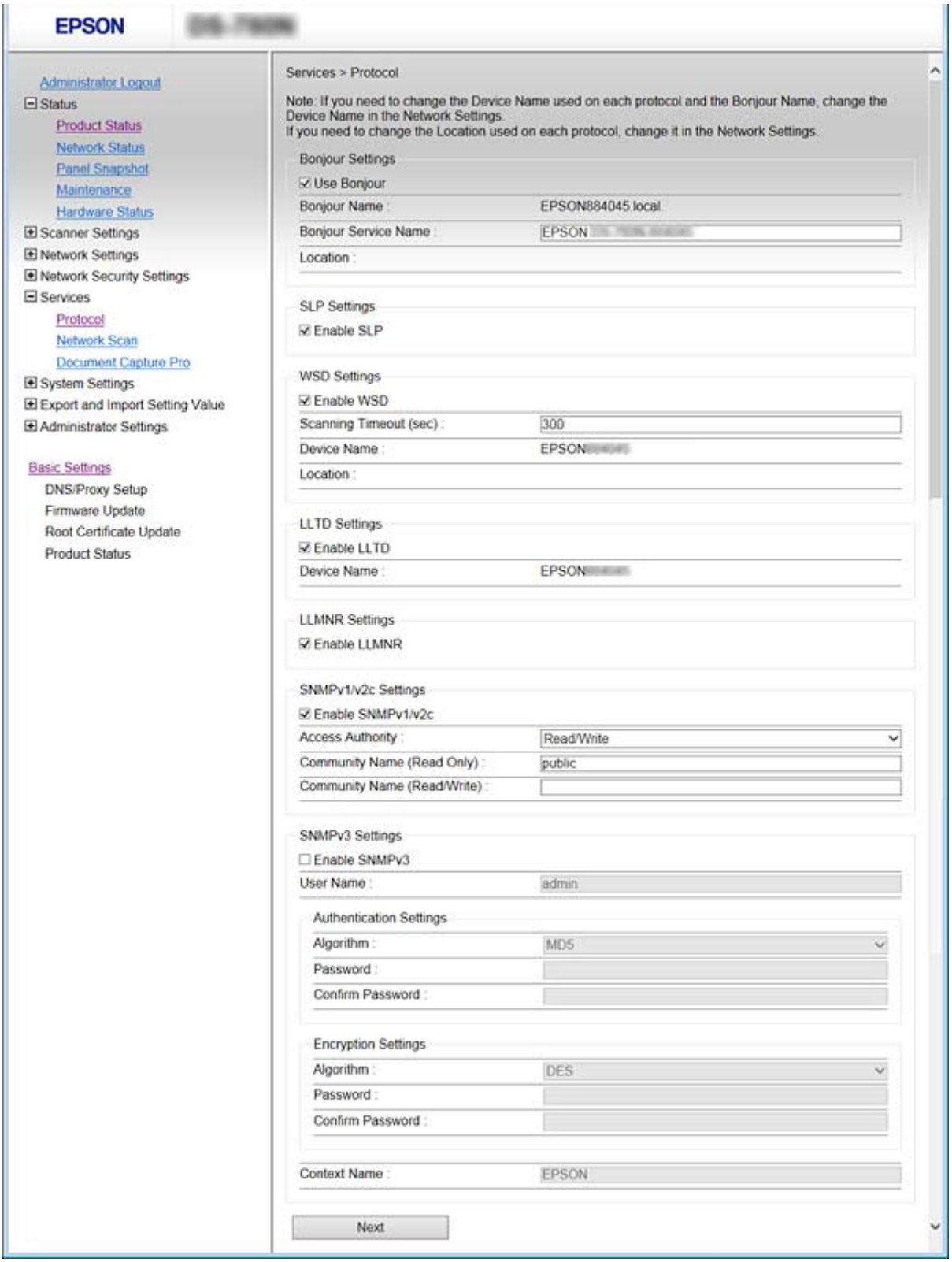
إعدادات الأمان الأساسية

البروتوكول	الوصف
WSD Settings	من الممكن أيضًا تمكين وظيفة WSD أو تعطيلها. عند تمكين هذه الخاصية، يمكنك إضافة أجهزة WSD أو المسح الضوئي من منفذ WSD.
LLTD Settings	من الممكن أيضًا تمكين أو تعطيل وظيفة LLTD. عند تمكينها، يتم عرضها أيضًا على خريطة شبكة Windows.
LLMNR Settings	من الممكن أيضًا تمكين أو تعطيل وظيفة LLMNR. عند تمكينها، يمكنك استخدام تحليل الاسم بدون NetBIOS حتى وإن لم يمكنك استخدام DNS.
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.

معلومات ذات صلة

- "التحكم في البروتوكولات" في الصفحة 34
- "عناصر إعداد البروتوكول" في الصفحة 36

عناصر إعداد البروتوكول



العناصر	إعداد القيمة والوصف
Bonjour Settings	

إعدادات الأمان الأساسية

العناصر	إعداد القيمة والوصف
Use Bonjour	حدد هذه الخاصية للبحث عن أجهزة أو استخدامها من خلال Bonjour.
Bonjour Name	يعرض اسم Bonjour.
Bonjour Service Name	يمُكنك عرض اسم الخدمة Bonjour وتعيينها.
Location	يعرض اسم موقع Bonjour.
SLP Settings	
Enable SLP	حدد هذا العنصر لتمكين وظيفة SLP. تُستخدم لاكتشاف الشبكة في Epson Scan 2 وEpsonNet Config.
WSD Settings	
Enable WSD	حدد هذا العنصر لتمكين إضافة أجهزة باستخدام WSD، ثم الطباعة والمسح الضوئي من منفذ WSD.
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 الماسحة الضوئية 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.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	حدّد هذا العنصر لتمكين SNMPv1/v2c. يتم عرض الماسحات الضوئية التي تدعم SNMPv3 فقط.
Access Authority	حدّد حق الوصول عند تمكين SNMPv1/v2c. حدّد **Read Only** أو **Read/Write**.
Community Name (Read Only)	أدخل من 0 إلى 32 (0x20 إلى ASCII 0x7E) حرفًا.
Community Name (Read/Write)	أدخل من 0 إلى 32 (0x20 إلى ASCII 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 لمصادقة SNMPv3.

إعدادات الأمان الأساسية

العناصر	إعداد القيمة والوصف
Password	أدخل كلمة مرور لمصادقة 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 لتشفير SNMPv3.
Password	أدخل كلمة مرور لتشفير 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.

معلومات ذات صلة

- "التحكم في البروتوكولات" في الصفحة 34
- "البروتوكولات التي تستطيع تمكينها أو تعطيلها" في الصفحة 34

إعدادات الإدارة والتشغيل

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

تأكيد معلومات أحد الأجهزة

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

❏ Product Status

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

❏ Network Status

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

❏ Panel Snapshot

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

❏ Maintenance

تحقق من تاريخ البدء، ومعلومات المسح الضوئي وما إلى ذلك.

❏ Hardware Status

تحقق من حالة الماسحة الضوئية.

معلومات ذات صلة

◆ "الوصول إلى تطبيق Web Config" في الصفحة 22

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 سجّلها في إحدى القوائم. إذا اتصلت أجهزة Epson مثل الطابعات والماسحات الضوئية بمقطع الشبكة نفسه المتصل به كمبيوتر المسؤول، يمكنك العثور عليها حتى إذا لم يتم تعيين عنوان IP لها.

يمكنك أيضًا 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 أيضًا 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 تلقائيًا إلى المسؤول حسب الحالات المعينة.

❏ 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.

معلومات ذات صلة

◆ "Epson Device Admin" في الصفحة 52

استلام إعلامات البريد الإلكتروني عند وقوع أحداث

حول إشعارات البريد الإلكتروني

يمكنك استخدام هذه الميزة لاستلام تنبيهات بالبريد الإلكتروني عند حدوث بعض الأحداث. يمكنك تسجيل حتى 5 عناوين بريد إلكتروني واختيار الأحداث التي ترغب في استلام إشعاراتها.

يجب تكوين خادم البريد الإلكتروني لاستخدام هذه الميزة.

معلومات ذات صلة

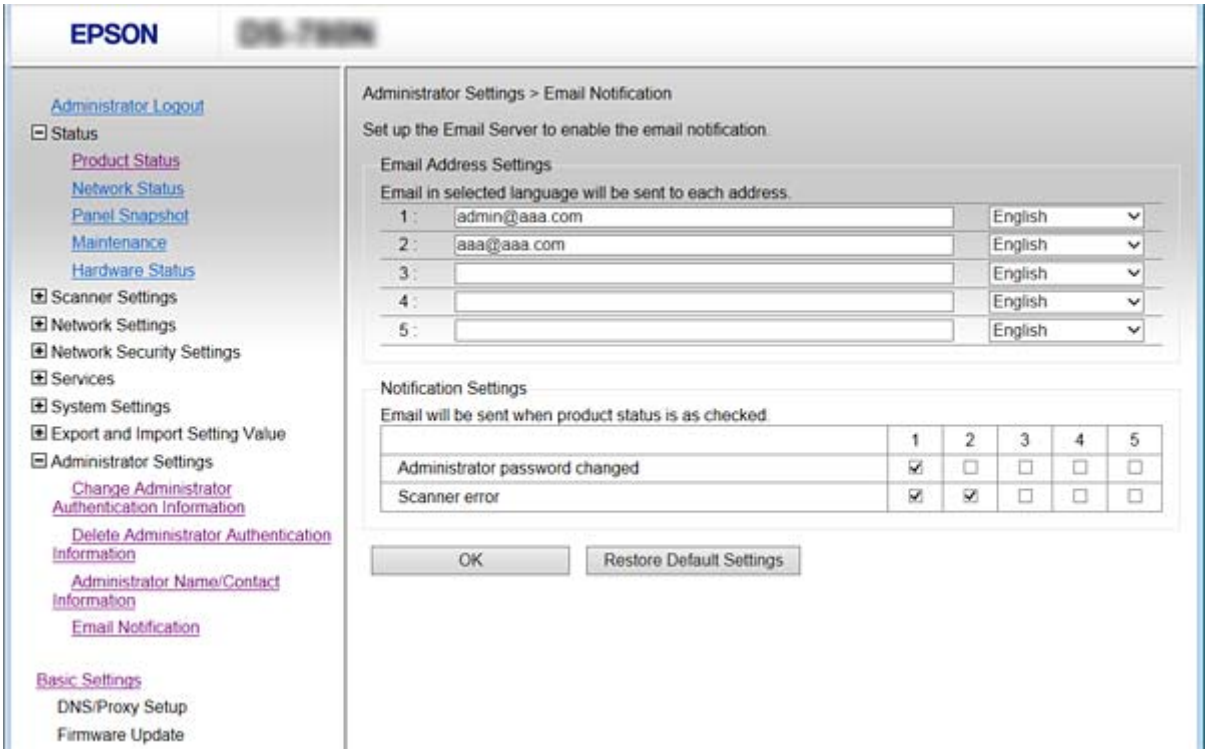
◆ "تكوين خادم البريد" في الصفحة 41

تكوين إشعارات البريد الإلكتروني

لاستخدام الميزة، يجب أن تقوم بتكوين خادم البريد الإلكتروني.

1. قم بالوصول إلى Web Config وحدد **Administrator Settings** > **Email Notification**.
2. أدخل عنوان البريد الإلكتروني الذي ترغب في استلام إشعارات البريد الإلكتروني الخاصة به.
3. حدد لغة إشعارات البريد الإلكتروني.

4. حدد مربعات الإشعارات التي ترغب في استلامها.



5. انقر فوق **OK**.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22
"تكوين خادم البريد" في الصفحة 41

تكوين خادم البريد

تحقق من النقاط التالية قبل التكوين.

❏ الماسحة الضوئية متصلة بالشبكة.

❏ معلومات خادم البريد الإلكتروني للكمبيوتر.

1. قم بالوصول إلى Web Config وحدد **Network Settings** > **Email Server** > **Basic**.

2. أدخل قيمة لكل عنصر.

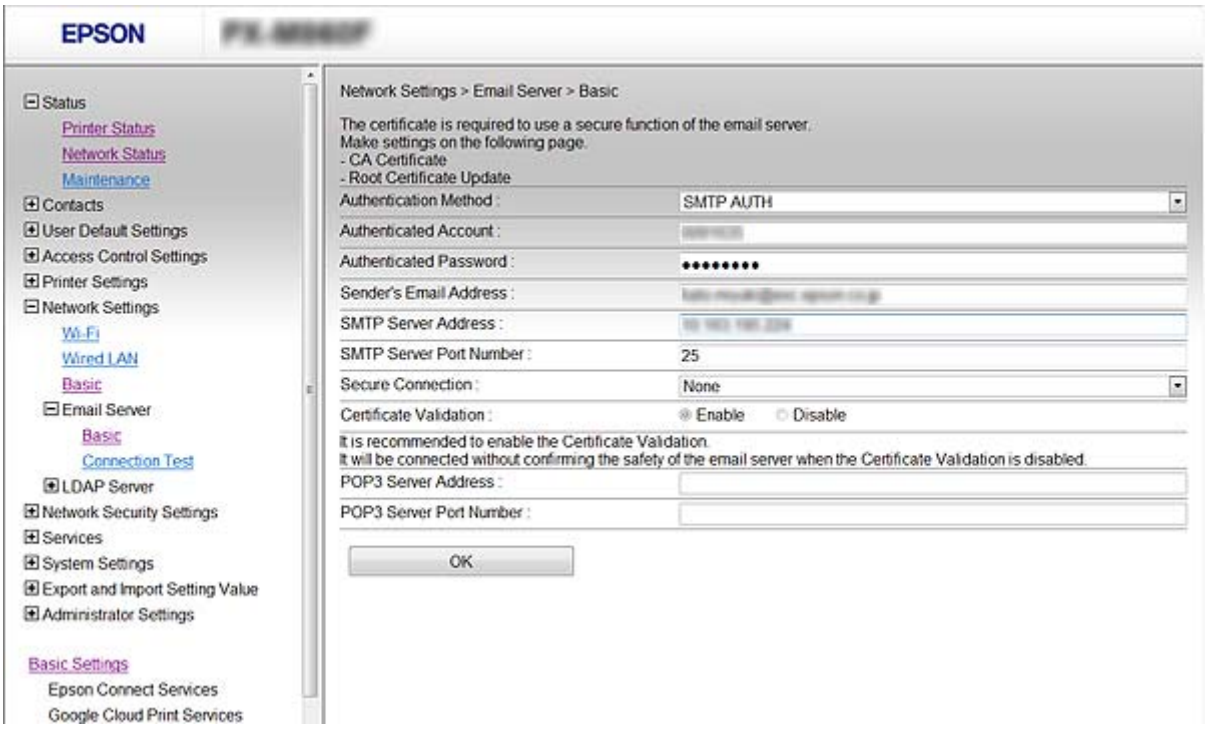
3. حدّد **OK**.

يتم عرض الإعدادات التي قمت بتحديدها.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22
"عناصر إعداد خادم البريد الإلكتروني" في الصفحة 42

عناصر إعداد خادم البريد الإلكتروني



العناصر	الإعدادات والشرح	
Authentication Method	حدد أسلوب المصادقة الذي يتيح للماسحة الضوئية الوصول إلى خادم البريد.	
	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 حرفًا في (0x20–0x7E) ASCII).	
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 رمزًا باستخدام A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	أدخل عنوان البريد الإلكتروني للمرسل. أدخل عدة رموز ما بين 0 و 255 رمزًا بتنسيق (0x20–0x7E) ASCII) فيما عدا: ( ) < > [ ] ; ¥. لا يمكن أن تكون الفاصلة الزمنية "." الرمز الأول.	
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.	

العناصر	الإعدادات والشرح	
Secure Connection	حدّد طريقة التوصيل الآمنة لخادم 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 41

التحقق من اتصال خادم البريد

1. قم بالوصول إلى Web Config وحدد **Network Settings** > **Email Server** > **Connection Test**.
2. حدّد **Start**.

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

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22
"مراجع اختبار اتصال خادم البريد" في الصفحة 43

مراجع اختبار اتصال خادم البريد

الرسائل	الشرح
Connection test was successful.	تظهر هذه الرسالة عند نجاح الاتصال بالخادم.
SMTP server communication error. Check the following. - Network Settings	تظهر هذه الرسالة عند ❑ عدم اتصال الماسحة الضوئية بالشبكة ❑ تعطل خادم SMTP ❑ قطع الاتصال بالشبكة أثناء الاتصال ❑ عدم اكتمال البيانات المستلمة

إعدادات الإدارة والتشغيل

الرسائل	الشرح
POP3 server communication error. Check the following. - Network Settings	تظهر هذه الرسالة عند ❏ عدم اتصال الماسحة الضوئية بالشبكة ❏ تعطل خادم POP3 ❏ قطع الاتصال بالشبكة أثناء الاتصال ❏ عدم اكتمال البيانات المستلمة
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	تظهر هذه الرسالة عند ❏ فشل الاتصال بخادم DNS ❏ 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 ❏ فشل الاتصال بخادم DNS ❏ فشل تحليل الاسم لخادم POP3
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	تظهر هذه الرسالة عند تعذر مصاقة خادم SMTP.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	تظهر هذه الرسالة عند تعذر مصاقة 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 للماسحة الضوئية غير صحيحة أو إذا انتهت صلاحية الشهادة.
The connection is untrusted. Check the following. - CA Certificate	تظهر هذه الرسالة عندما لا تحتوي الماسحة الضوئية 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.
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.

الرسائل	الشرح
Cannot access the product until processing is complete.	تظهر هذه الرسالة عندما تكون الماسحة الضوئية مشغولة.

معلومات ذات صلة

"التحقق من اتصال خادم البريد" في الصفحة 43

تحديث البرنامج الثابت

تحديث البرنامج الثابت باستخدامWeb Config

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

1. قم بالوصول إلى Web Config وحدد **Basic Settings** < **Firmware Update**.
2. انقر فوق **Start**.

   يتم بدء تأكيد البرنامج الثابت، ويتم عرض معلومات البرنامج الثابت إذا تم العثور على برنامج ثابت محدث.
3. انقر فوق **Start**، واتبع الإرشادات الظاهرة على الشاشة.

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

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22
"Epson Device Admin" في الصفحة 52

تحديث البرنامج الثابت عن طريق استخدام Epson Firmware Updater

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

1. انتقل إلى موقع Epson على الويب ونزّل البرنامج الثابت.
2. وصّل 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 الإعدادات احتياطيًا

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

تصدير الإعدادات

تصدير كل إعداد للماسحة الضوئية.

1. قم بالوصول إلى Web Config، ثم حدد **Export** < **Export and Import Setting Value**.
2. حدّد الإعدادات التي تريد تصديرها.

حدّد الإعدادات التي تريد تصديرها. إذا قمت بتحديد الفئة الأصلية، فسيتم اختيار فئات فرعية أيضًا. 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 للماسحة الضوئية مثل اسم الماسحة الضوئية وعنوان *IP*، فحدّد ***Enable to select the individual settings of device*** ثم حدّد عناصر أخرى. لا تستخدم إلا القيم المحددة للماسحة الضوئية البديلة فقط.

معلومات ذات صلة

◆ "الوصول إلى تطبيق Web Config" في الصفحة 22

استيراد الإعدادات

قم باستيراد ملف Web Config الذي تم تصديره إلى الماسحة الضوئية.

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

1. قم بالوصول إلى Web Config، ثم حدد **Import** < **Export and Import Setting Value**.
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 الماسحة الضوئية.

معلومات ذات صلة

◆ "الوصول إلى تطبيق Web Config" في الصفحة 22

حل المشكلات

تلميحات لحل المشكلات

يمكنك معرفة المزيد من المعلومات في الدليل التالي.

❏ دليل المستخدم
يقدِّم تعليمات عن استخدام الماسحة، وصيانتها، وحل المشكلات التي قد تتعرض لها.

فحص سجل الخادم وجهاز الشبكة

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

تهيئة إعدادات الشبكة

استعادة إعدادات الشبكة من لوحة التحكم

يمكنك استعادة جميع إعدادات الشبكة إلى الأوضاع الافتراضية.

1. اضغط على **الإعدادات** على الشاشة الرئيسية.
2. اضغط على **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 تلقائيًا بعد فترة زمنية محددة إذا لم تقم بالضغط على **إغلاق**.

التحقق من الاتصال بين الأجهزة وأجهزة الكمبيوتر

تحقق من الاتصال باستخدام أمر Ping — Windows

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

1. تحقق من عنوان IP الخاص بالماسحة الضوئية للاتصال الذي تريد التحقق منه.
يُمكنك التحقق من ذلك باستخدام Epson Scan 2.

2. عرض شاشة موجة أوامر جهاز الحاسوب.

❏ Windows 10

انقر بزر الماوس الأيمن فوق زر البدء، أو اضغط عليه مع الاستمرار، ثم حدد **موجه الأوامر**.

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

اعرض شاشة التطبيق، ثم حدد **موجه الأوامر**.

❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 أو سابقًا

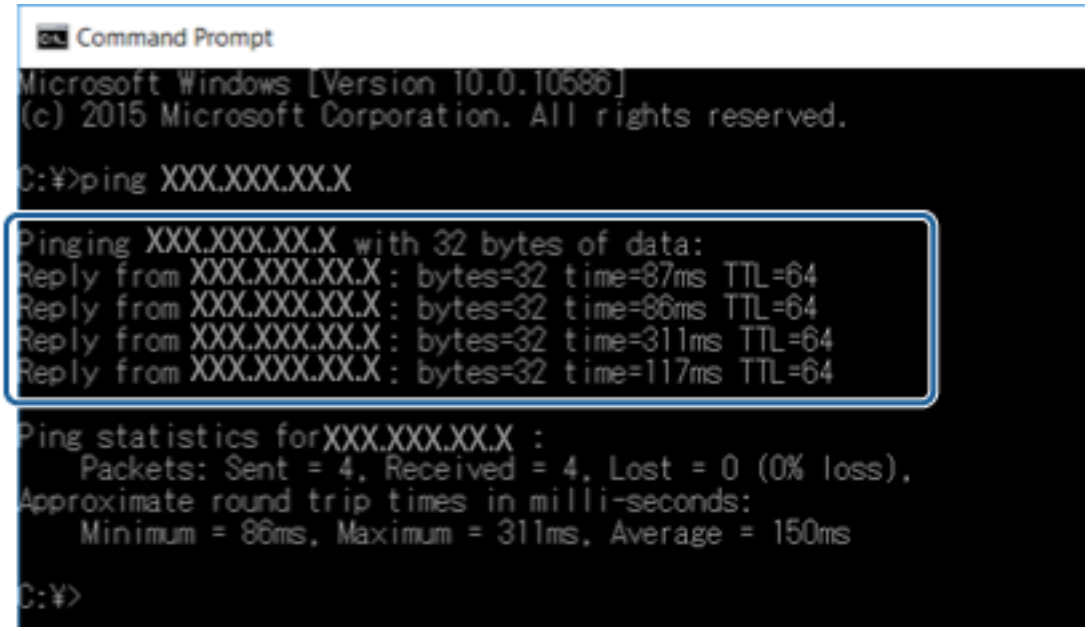
اضغط على زر البدء، وحدد **جميع البرامج** أو **البرامج** > **الملحقات** > **موجه الأوامر**.

3. أدخل "ping xxx.xxx.xxx.xxx"، ثم اضغط على مفتاح الإدخال.

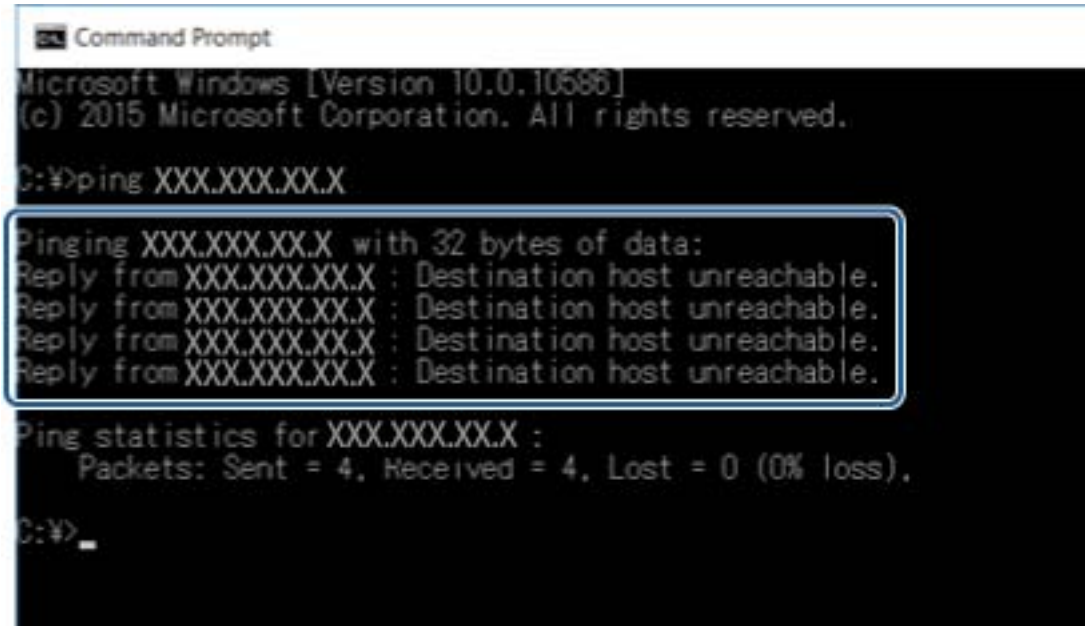
أدخل عنوان IP الخاص بالماسحة الضوئية لـ xxx.xxx.xxx.xxx.

4. تحقق من حالة الاتصال.

إذا كانت الماسحة الضوئية وجهاز الحاسوب متصلين، يتم عرض الرسالة التالية.



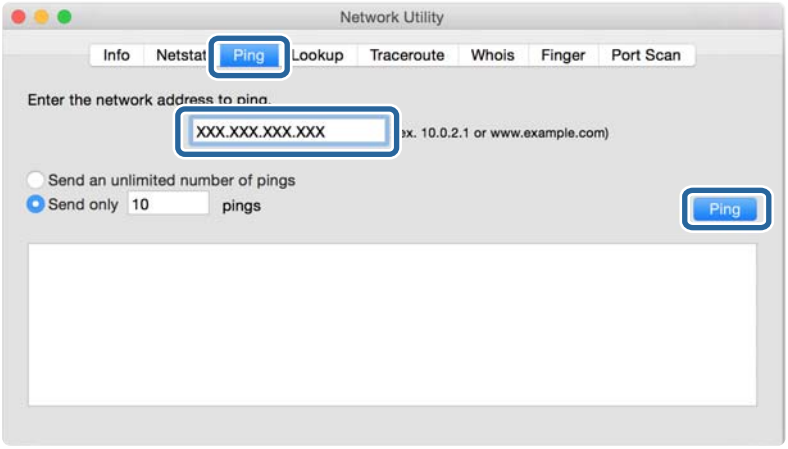
إذا كانت الماسحة الضوئية وجهاز الحاسوب غير متصلين، يتم عرض الرسالة التالية.



تحقق من الاتصال باستخدام أمر Ping — Mac OS

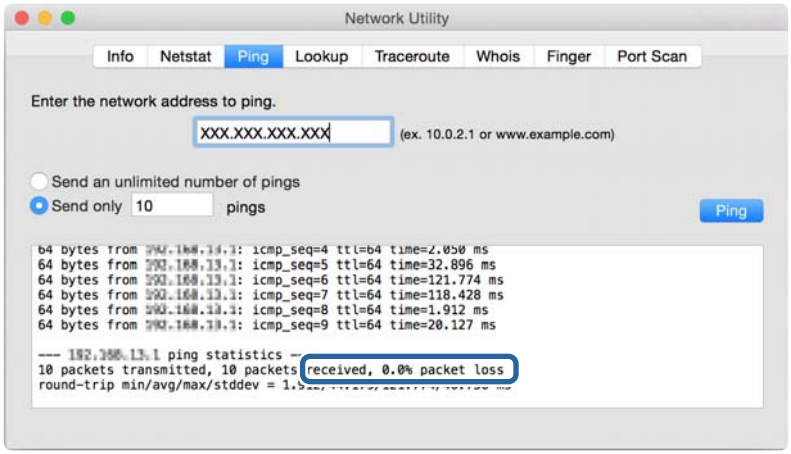
يمُكنك استخدام أمر Ping للتأكد من اتصال الحاسوب بالماسحة الضوئية. اتبع الخطوات أدناه للتحقق من الاتصال باستخدام أمر Ping.

1. تحقق من عنوان IP الخاص بالماسحة الضوئية للاتصال الذي تريد التحقق منه.
   يمُكنك التحقق من ذلك باستخدام Epson Scan 2.
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**.

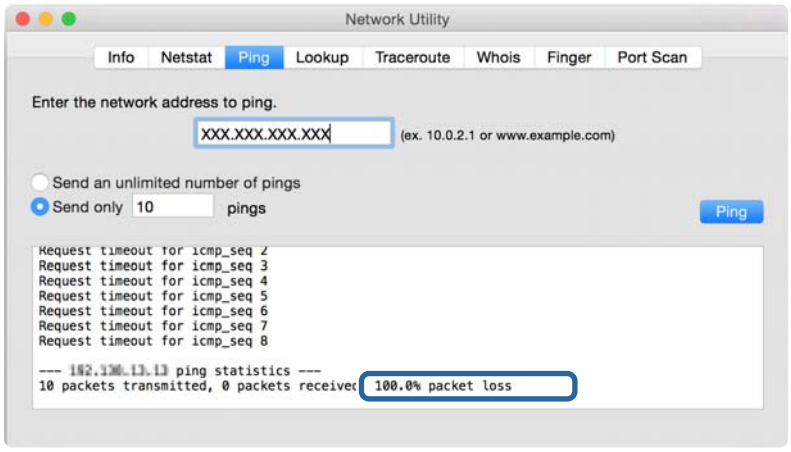


4. تحقق من حالة الاتصال.

إذا كانت الماسحة الضوئية وجهاز الحاسوب متصلين، يتم عرض الرسالة التالية.



إذا كانت الماسحة الضوئية وجهاز الحاسوب غير متصلين، يتم عرض الرسالة التالية.



المشكلات الخاصة باستخدام برنامج الشبكة

تعذّر الوصول إلى تهيئة الويب

هل تم تكوين عنوان IP الخاص بالماسحة الضوئية بشكلٍ صحيح؟

قم بتكوين عنوان IP باستخدام Epson Device Admin أو EpsonNet Config.

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 "منتهي 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 الماسحة الضوئية بشكلٍ صحيح.

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

لا يتطابق عنوان IP الخاص بالماسحة الضوئية المدخل لإعداد **Common Name** من أجل إنشاء شهادة موقعة ذاتيًا أو طلب CSR مع العنوان المدخل في المستعرض. احصل على شهادة وقم باستيرادها مرةً أخرى أو قم بتغيير اسم الماسحة الضوئية.

يتم الوصول إلى الماسحة الضوئية من خلال خادم وكيل.

إذا كنت تستخدم خادمًا وكيلاً مع الماسحة الضوئية، 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 لإعداد **إعدادات تجاوز الوكيل للمضيفين والنطاقات**.

مثال:

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

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

معلومات ذات صلة

◆ "الوصول إلى تطبيق Web Config" في الصفحة 22

◆ "تعيين عنوان IP" في الصفحة 15

◆ "تعيين عنوان IP باستخدام EpsonNet Config" في الصفحة 53

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 برنامجًا مضادًا 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 **Tools** > **Options** > **Timeout** ثم قم بزيادة طول الوقت لإعداد **Communication Error**. لاحظ أن القيام بهذا يمكن أن يؤدي إلى تشغيل تطبيق EpsonNet Config ببطءٍ أكبر.

معلومات ذات صلة

◆ "تشغيل تطبيق EpsonNet Config — Windows" في الصفحة 52

◆ "تشغيل تطبيق EpsonNet Config — Mac OS" في الصفحة 53

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 إعلامات التنبيهات، وإنشاء تقارير لاستخدام الجهاز. يمكنك أيضًا إنشاء قالب يحتوي على عناصر الإعداد وتطبيقها على الأجهزة الأخرى كإعدادات مشاركة. يمكنك تنزيل Epson Device Admin من موقع الويب الخاص بدعم Epson. لمزيدٍ من المعلومات، انظر الوثائق أو التعليمات الخاصة بتطبيق Epson Device Admin.

تشغيل Epson Device Admin (Windows فقط)

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 الماسحة الضوئية، مثل تعيين عنوان IP وتغيير وضع الاتصال. يتم دعم ميزة الإعداد الدفعي على نظام التشغيل Windows. لمزيدٍ من المعلومات، انظر الوثائق أو التعليمات الخاصة بتطبيق EpsonNet Config.

تشغيل تطبيق EpsonNet Config — Windows

حدد **كل البرامج** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

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 SetupManager

EpsonNet SetupManager هو برنامج خاص بإنشاء حزمة للتثبيت البسيط للماسحة الضوئية، مثل تثبيت برنامج تشغيل الماسحة الضوئية وتكوينه، وتثبيت Document Capture Pro. 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 للماسحة الضوئية باستخدام EpsonNet Config. يسمح لك EpsonNet Config بتعيين عنوان IP للماسحة الضوئية التي لم يتم تعيين أي عنوان لها بعد الاتصال باستخدام كابل إيثرنت.

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.

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 عنصر الإعداد.

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

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

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

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

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

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

ضبط الإعدادات الدفعية باستخدام ملف التكوين

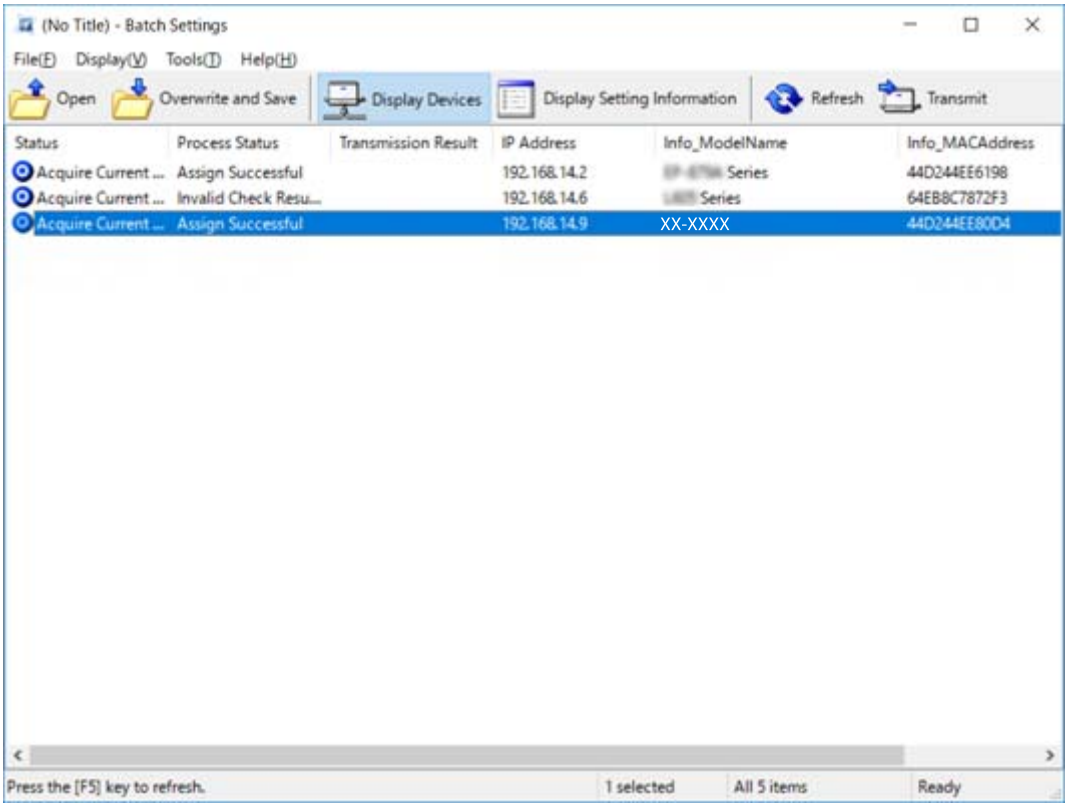
عينّ عناوين IP في ملف التكوين (ملف SYLK) في وقت واحد. عليك إنشاء ملف التكوين قبل بدء التعيين.

1. قم بتوصيل جميع الأجهزة بالشبكة باستخدام كابل إيثرنت.
2. قم بتشغيل الماسحة الضوئية.
3. ابدأ تشغيل EpsonNet Config.

يتم عرض قائمة بالماسحات الضوئية الموجودة على الشبكة. قد يستغرق الأمر فترة من الوقت قبل عرضها.

4. انقر فوق **Tools** > **Batch Settings**.
5. انقر فوق **Open**.
6. على شاشة تحديد الملف، حدد ملف SYLK (*.slk) الذي يحتوي على الإعدادات، ثم انقر فوق **Open**.
7. حدد الأجهزة التي ترغب في إجراء الإعدادات الدفعية لها مع تعيين العمود **Status** على **Unassigned**، وتعيين **Process Status** على **Assign Successful**.

عندما تقوم بإجراء عدة تحديدات، اضغط على Ctrl أو Shift وانقر عليها أو اسحب بالماوس.



8. انقر فوق **Transmit**.
9. عند عرض شاشة إدخال كلمة المرور، أدخل كلمة المرور، ثم انقر فوق **OK**.

إرسال الإعدادات.

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

10. على شاشة **Transmitting Settings** انقر فوق **OK**.

11. تحقق من حالة الجهاز الذي تقوم بتعيينه.

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

الرمز	Status	Process Status	الشرح
	Setup Complete	Setup Successful	تم إكمال الإعداد بشكل عادي.
	Setup Complete	Rebooting	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.
	Setup Complete	Reboot Failed	تعذّر تأكيد الجهاز بعد إرسال الإعدادات. تحقق من تشغيل الجهاز، أو إذا تمت إعادة تشغيله.
	Setup Complete	Searching	البحث عن الجهاز الذي يُشار إليه في ملف الإعدادات.*
	Setup Complete	Search Failed	تعذّر 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 52 Windows
"تشغيل تطبيق EpsonNet Config — " في الصفحة 53 Mac OS

تعيين عنوان IP لكل جهاز

عينّ عنوان IP للماسحة الضوئية باستخدام EpsonNet Config.

1. قم بتشغيل الماسحة الضوئية.
2. قم بتوصيل الماسحة الضوئية بالشبكة باستخدام كابل إيثرنت.
3. ابدأ تشغيل EpsonNet Config.

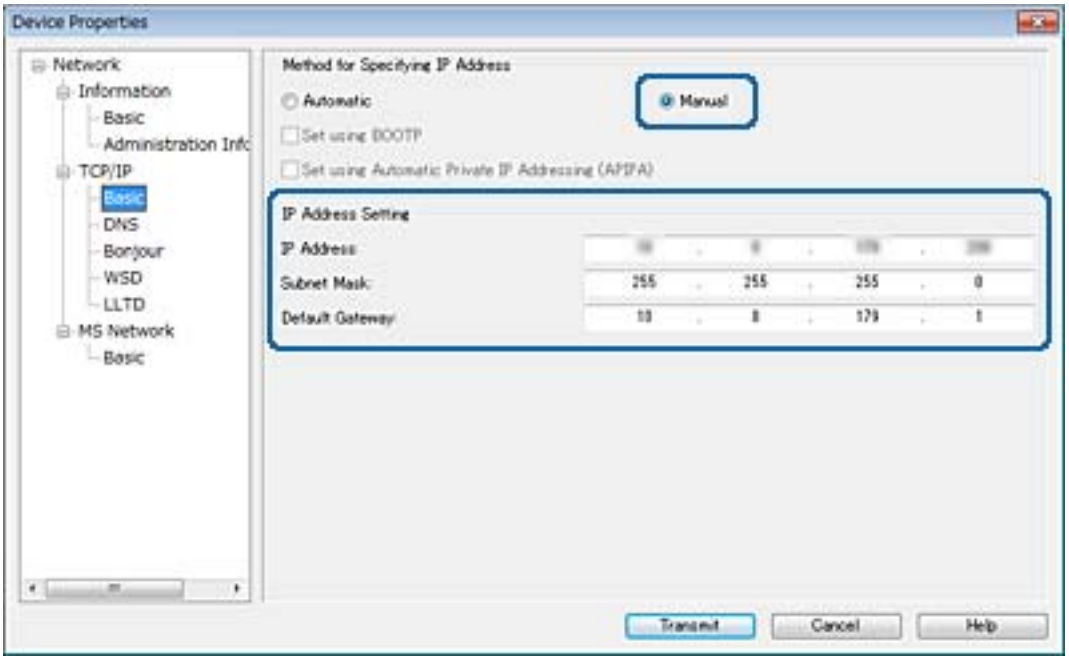
يتم عرض قائمة بالماسحات الضوئية الموجودة على الشبكة. قد يستغرق الأمر فترة من الوقت قبل عرضها.

4. انقر نقرًا مزدوجًا فوق الماسحة الضوئية التي تريد التعيين لها.

ملاحظة:
إذا قمت بتوصيل عدة ماسحات ضوئية من الطراز نفسه، يمكنك تحديد الماسحة الضوئية باستخدام عنوان *MAC*.

5. حدد **Network** > **TCP/IP** > **Basic**.

6. أدخل العناوين لـ **IP Address**، و**Subnet Mask**، و**Default Gateway**.



ملاحظة:
أدخل عنوانًا ثابتًا عند توصيل الماسحة الضوئية بشبكة آمنة.

7. انقر فوق **Transmit**.

تظهر شاشة تأكيد إرسال المعلومات.

8. انقر فوق **OK**.

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 **OK**.

معلومات ذات صلة

◆ "تشغيل تطبيق EpsonNet Config — " في الصفحة 52 Windows
◆ "تشغيل تطبيق EpsonNet Config — " في الصفحة 53 Mac OS

استخدام منفذ للماسحة الضوئية

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

ملحق

المُرسِل (العميل)	الاستخدام	الوجهة (الخادم)	البروتوكول	رقم المنفذ
الماسحة الضوئية	إرسال رسالة بريد إلكتروني (إعلام بريد إلكتروني)	خادم SMTP	(TCP) SMTP	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	اتصال POP قبل SMTP (إعلام بريد إلكتروني	خادم POP	(TCP) POP3	110
	WSD التحكم	كمبيوتر عميل	(TCP) WSD	5357
	فحص جهاز كمبيوتر في حالة المسح الضوئي بالدفع من Document Capture Pro	كمبيوتر عميل	اكتشاف المسح الضوئي بالدفع على الشبكة	2968
	جمع معلومات المهمة في حالة المسح الضوئي بالدفع من Document Capture Pro	كمبيوتر عميل	المسح الضوئي بالدفع على الشبكة	2968
كمبيوتر عميل	اكتشف الماسحة الضوئية من تطبيق مثل EpsonNet Config، وبرنامج تشغيل الماسحة الضوئية.	الماسحة الضوئية	(UDP) ENPC	3289
	اجمع معلومات MIB وقم بإعدادها من تطبيق مثل EpsonNet Config وبرنامج تشغيل الماسحة الضوئية.	الماسحة الضوئية	(UDP) SNMP	161
	البحث عن الماسحة الضوئية WSD	الماسحة الضوئية	WS-Discovery (UDP)	3702
	إعادة توجيه بيانات المسح الضوئي من Document Capture Pro	الماسحة الضوئية	مسح الشبكة (TCP)	1865

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 مفيدًا في تحسين الكفاءة التشغيلية والموافقة. ومع ذلك، فإن المخاطر مثل الوصول غير القانوني، والاستخدام غير القانوني، والتلاعب بالبيانات تتزايد. إذا كنت تستخدم الجهاز في بيئة يمكن فيها الوصول إلى الإنترنت، يكون معدل التعرض للمخاطر مرتفعًا جدًا.

لتجنب التعرض لهذه المخاطرة، تتضمن أجهزة Epson مجموعة متنوعة من تقنيات الأمان.

عيّن الجهاز حسب الضرورة وفقًا للظروف البيئية التي تم إنشاؤها باستخدام معلومات بيئة العميل.

الاسم	نوع الميزة	ما الذي يتم تعيينه	ما الذي يتم حظره
اتصال SSL/TLS	يتم تشفير مسار اتصال الكمبيوتر وأحد الأجهزة باستخدام اتصال SSL/TLS. تتم حماية محتوى الاتصال عبر المتصفح.	عيّن شهادة المرجع المصدق (CA) للخادم وهي تُعد شهادة موقعة من قبل CA (مرجع مصدق) للجهاز.	امنع تسريب معلومات الإعداد ومحتويات البيانات المرسلة للماسحة الضوئية من الكمبيوتر. يمكن أيضًا حماية الوصول إلى خادم Epson على الإنترنت من الجهاز عن طريق استخدام تحديث البرنامج الثابت، وما إلى ذلك.
تصفية 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 غير المؤمّن 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.	مكّن SNMPv3، ثم عيّن المصادقة وطريقة التشفير.	تأكد من إعدادات التغيير في الشبكة، والتزام السرية في مراقبة الحالة.
IEEE802.1X	لا يسمح بالاتصال بشبكة إيثرنت إلا للمستخدم المصرح له فقط. لا يسمح إلا للمستخدم المسموح له باستخدام الجهاز فقط.	إعداد المصادقة لخادم RADIUS (خادم المصادقة).	قم بحماية الاستخدام والوصول غير المعتمد للجهاز.
قراءة بطاقة هوية	يمكنك استخدام الجهاز عن طريق الاحتفاظ ببطاقة الهوية لجهاز معتمد متصل. يمكنك تقييد الحصول على سجلات لكل مستخدم وجهاز، وتقييد الاستخدام المتوفر للأجهزة والميزات المتوفرة لكل مستخدم ومجموعة.	وصّل جهاز مصادقة بالجهاز، ثم عيّن معلومات أحد المستخدمين الموجودين في نظام المصادقة.	امنع الاستخدام غير المعتمد للجهاز وانتحال هويته.

معلومات ذات صلة

- "اتصال SSL/TLS بالماسحة الضوئية" في الصفحة 59
- "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 67
- "استخدام بروتوكول SNMPv3" في الصفحة 77
- "توصيل الماسحة الضوئية بشبكة IEEE802.1X" في الصفحة 79

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.

اتصال SSL/TLS بالمصافحة الضوئية

عندما يتم تعيين شهادة الخادم باستخدام اتصال SSL/TLS (طبقة مأخذ توصيل آمنة/بروتوكول أمان طبقة النقل) بالمصافحة الضوئية، يمكنك تشفير مسار الاتصال بين أجهزة الكمبيوتر. قم بتطبيق ذلك إذا كنت ترغب في منع الوصول عن بُعد 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 مقومًا أساسيًا في نمط الأمان "الثقة في الويب". يجب الحصول على شهادة مرجع مصدق (CA) لمصادقة الخادم من المرجع المصدق الذي أصدر الشهادة.

❏ شهادة موقعة ذاتيًا

الشهادة الموقعة ذاتيًا هي شهادة تصدرها الماسحة الضوئية وتوقعها ذاتيًا. 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 59
- "حذف شهادة موقعة من المرجع المصدق (CA)" في الصفحة 63
- "تحديث شهادة موقعة ذاتيًا" في الصفحة 64

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.

1. قم بالوصول إلى Web Config، ثم حدد **Network Security Settings**. بعد ذلك، حدد **SSL/TLS** > **Certificate** أو **IPsec/IP Filtering** > **Client Certificate** أو **IEEE802.1X** > **Client Certificate**.

2. انقر فوق خيار **Generate** الخاص بإعداد **CSR**.

   يتم فتح صفحة إنشاء طلب CSR.

3. أدخل قيمة لكل عنصر.

ملاحظة:
يتنوع طول المفتاح والاختصارات المتاحة وفقًا للمرجع المصدق. قم بإنشاء طلب وفقًا لقواعد كل مرجع مصدق.

4. انقر فوق **OK**.

يتم عرض رسالة اكتمال الطلب.

5. حدّد **Network Security Settings**. بعد ذلك، حدد **SSL/TLS** > **Certificate**، أو **IPsec/IP Filtering** > **Client Certificate** أو **IEEE802.1X** > **Client Certificate**.

6. انقر فوق أحد أزرار تنزيل **CSR** وفقًا 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 بالماسحة الضوئية.

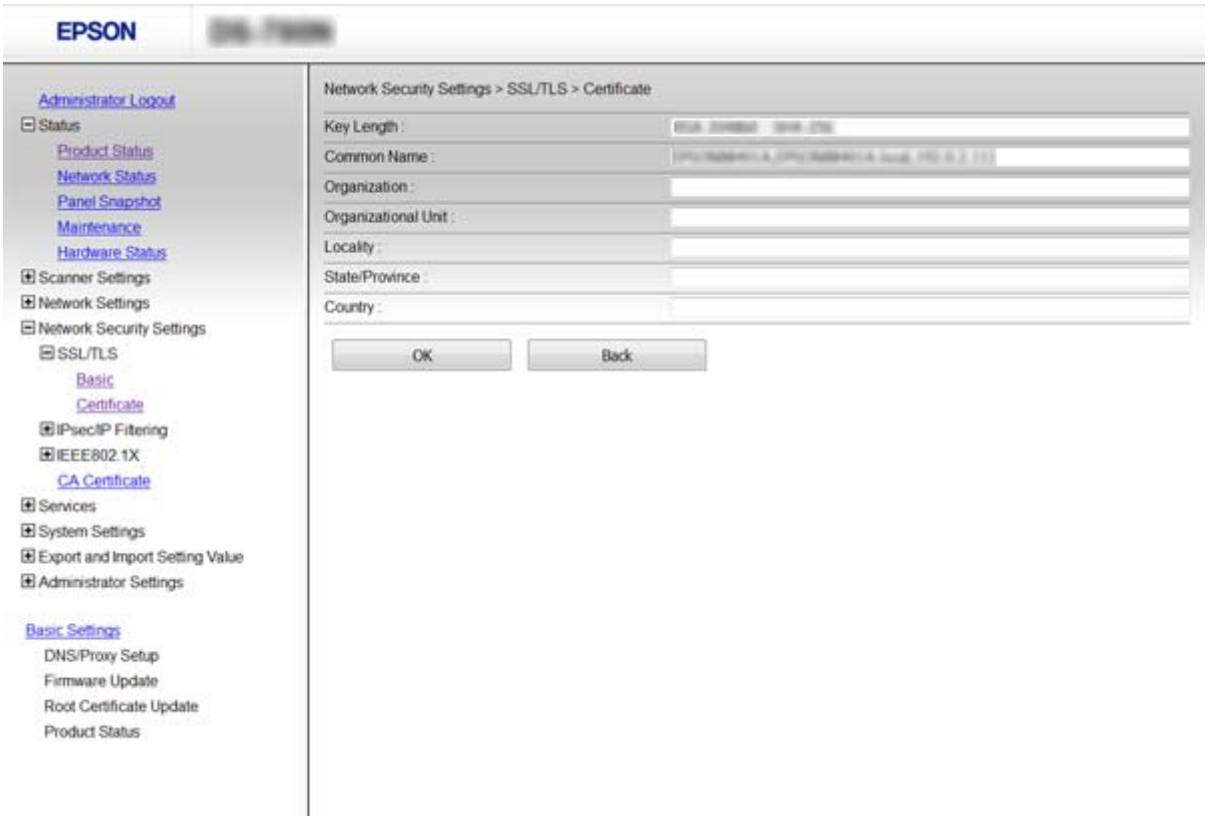
يكتمل الحصول على CA-signed Certificate عندما تحفظ إحدى الشهادات في إحدى الوجهات.

معلومات ذات صلة

- "الوصول إلى تطبيق Web Config" في الصفحة 22
- "عناصر إعداد طلب CSR" في الصفحة 61
- "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 62

إعدادات الأمان المتقدمة لـ Enterprise

عناصر إعداد طلب *CSR*



العناصر	الإعدادات والشرح
Key Length	حدد طول مفتاح طلب CSR.
Common Name	يمكن إدخال عدة أحرف تتراوح ما بين حرف واحد حتى 128 حرفًا. إذا كان هذا عنوان IP، فلا بد أن يكون عنوان IP ثابتًا. مثال: عنوان URL للوصول إلى: https\Web Config :10.152.12.225// اسم شائع: 10.152.12.225
Organization /Organizational Unit /Locality /State/Province	يُمكنك إدخال ما بين 0 إلى 64 رمزًا 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 59

استيراد شهادة موقعة من المرجع المصدق (CA)

هام:

❏ تأكد من تعيين تاريخ الماسحة الضوئية ووقتها بشكلٍ صحيح.

❏ إذا كنت تحصل على شهادة باستخدام طلب *CSR* تم إنشاؤه من تطبيق *Web Config*، فسيمكنك استيراد الشهادة مرةً واحدة.

1. قم بالوصول إلى Web Config ثم حدد **Network Security Settings**. بعد ذلك، حدد **SSL/TLS** > **Certificate**، أو **IPsec/IP Filtering** > **Client Certificate** أو **IEEE802.1X** > **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 قيماً للعناصر المطلوبة وفقًا لما يلي.

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

❏ **Private Key**: لا تقم بالتكوين لاحتواء الماسحة الضوئية 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**.

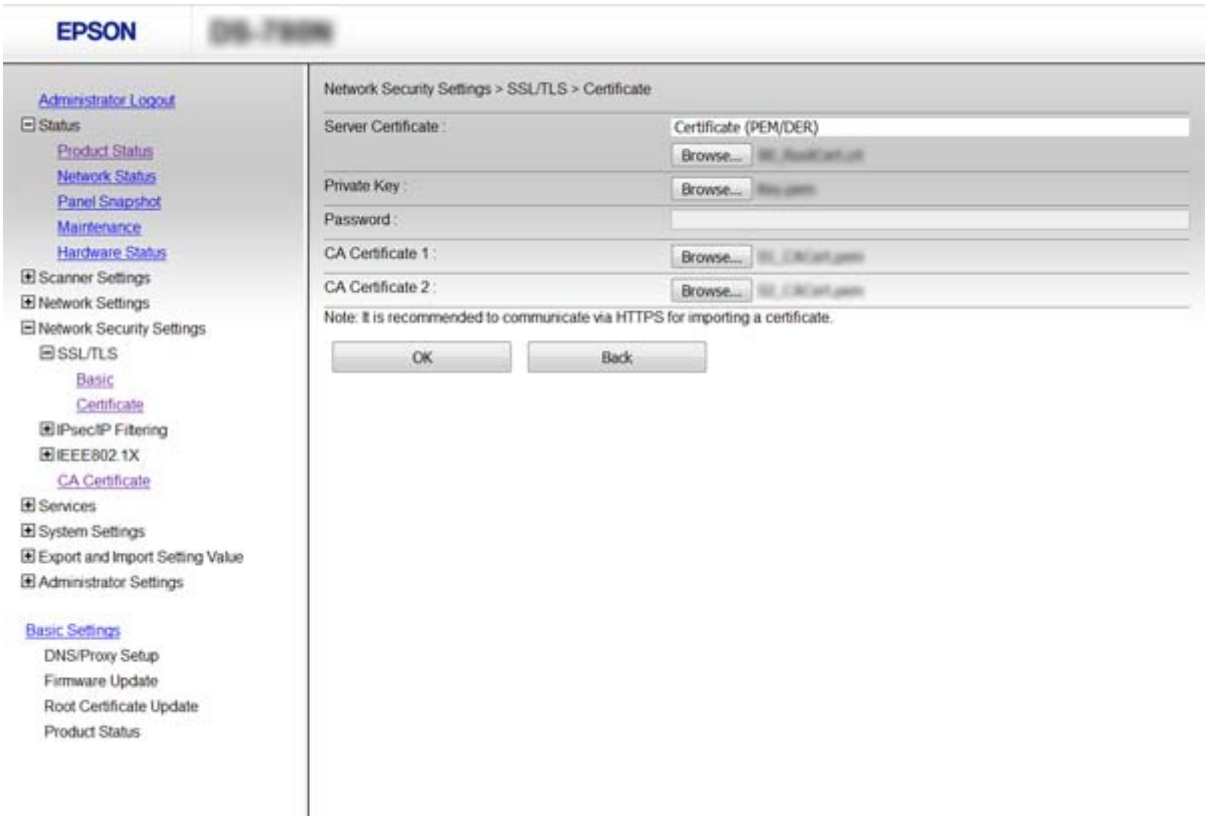
   يتم عرض رسالة اكتمال الطلب.

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

معلومات ذات صلة

◆ "الوصول إلى تطبيق Web Config" في الصفحة 22
◆ "عناصر إعداد استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 63

عناصر إعداد استيراد شهادة موقعة من المرجع المصدق (CA)



العناصر	الإعدادات والشرح
Server Certificate أو Client 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 ملفًا عند الضرورة.
CA Certificate 2	إذا كان تنسيق الشهادة **Certificate (PEM/DER)**، فقم باستيراد شهادة من المرجع المصدق الذي يصدر **CA Certificate 1**. حدد ملفًا عند الضرورة.

معلومات ذات صلة

"استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 62

حذف شهادة موقعة من المرجع المصدق (CA)

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

هام:

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

1. قم بالوصول إلى Web Config، ثم حدد **Network Security Settings**. بعد ذلك، حدد **SSL/TLS** > **Certificate**، أو **IPsec/IP Filtering** > **Client Certificate** أو **IEEE802.1X** > **Client Certificate**.
2. انقر فوق **Delete**.
3. قم بالتأكيد على أنك تريد حذف الشهادة في الرسالة المعروضة.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22

تحديث شهادة موقعة ذاتيًا

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

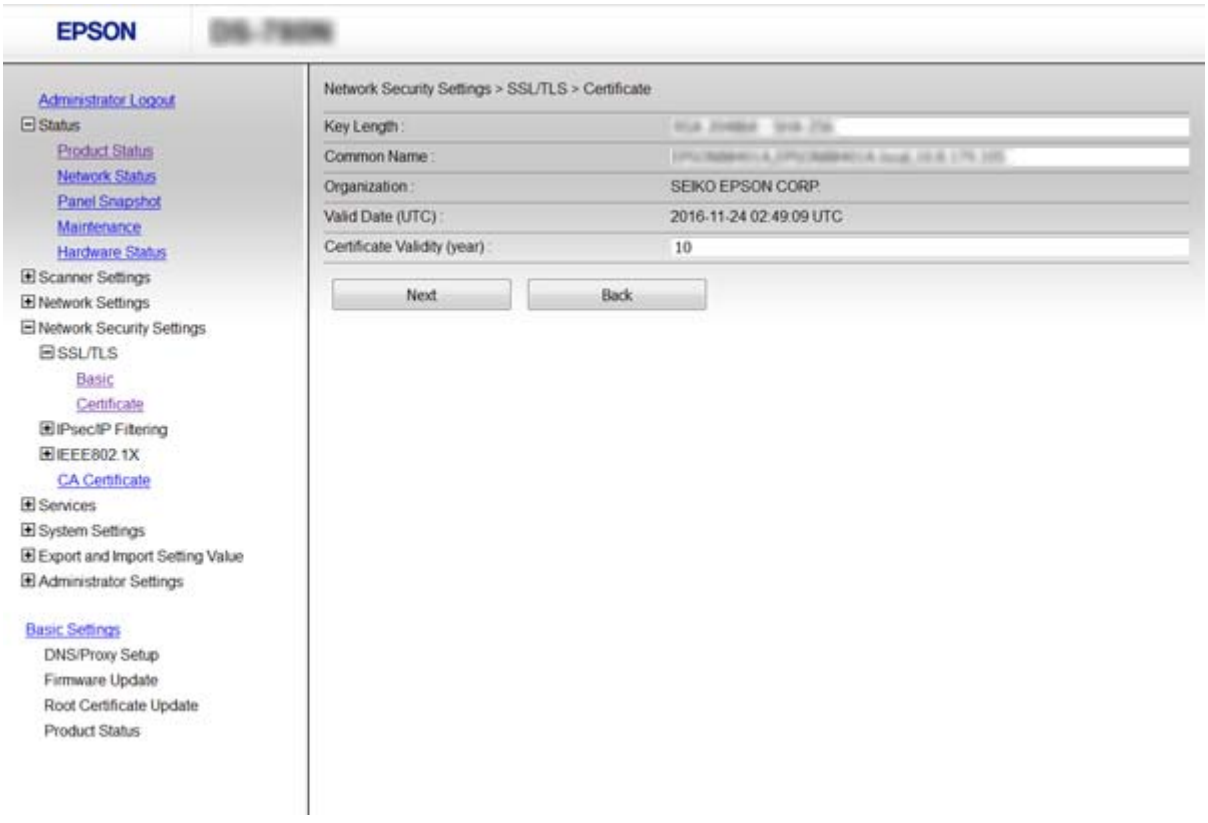
استخدم شهادة موقعة ذاتيًا مؤقتًا حتى تحصل على شهادة موقعة من المرجع المصدق (CA) وتقوم باستيرادها.

1. قم بالوصول إلى Web Config وحدد **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. انقر فوق **Update**.
3. أدخل **Common Name**.

أدخل عنوان IP أو أي معرف مثل اسم FQDN للماسحة الضوئية. يمكن إدخال عدة أحرف تتراوح ما بين حرف واحد حتى 128 حرفًا.

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

4. حدد فترة صلاحية للشهادة.



5. انقر فوق **Next**.

يتم عرض رسالة تأكيد.

6. انقر فوق **OK**.

الماسحة الضوئية قيد التحديث.

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

معلومات ذات صلة

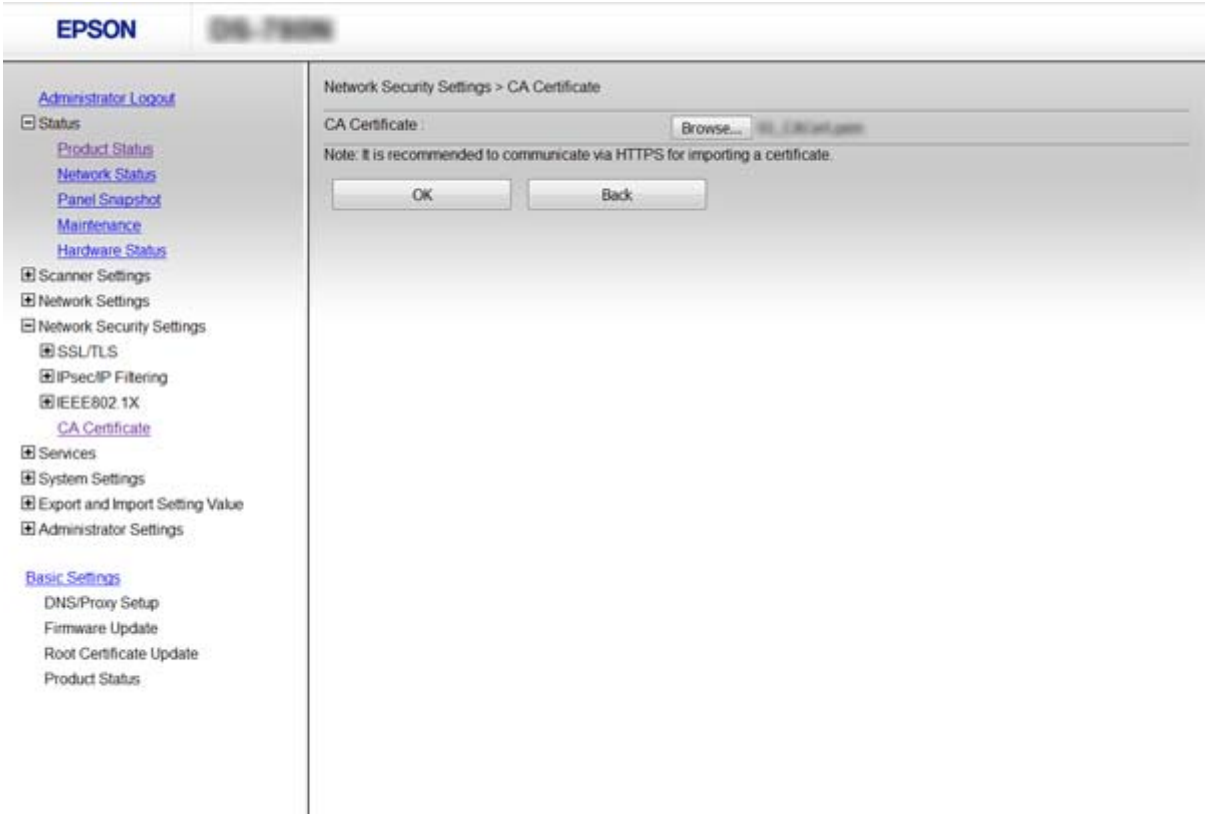
"الوصول إلى تطبيق Web Config" في الصفحة 22

تهيئة CA Certificate

يمكنك استيراد وعرض وحذف CA Certificate.

استيراد CA Certificate

1. قم بالوصول إلى Web Config، ثم حدد **Network Security Settings** > **CA Certificate**.
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.

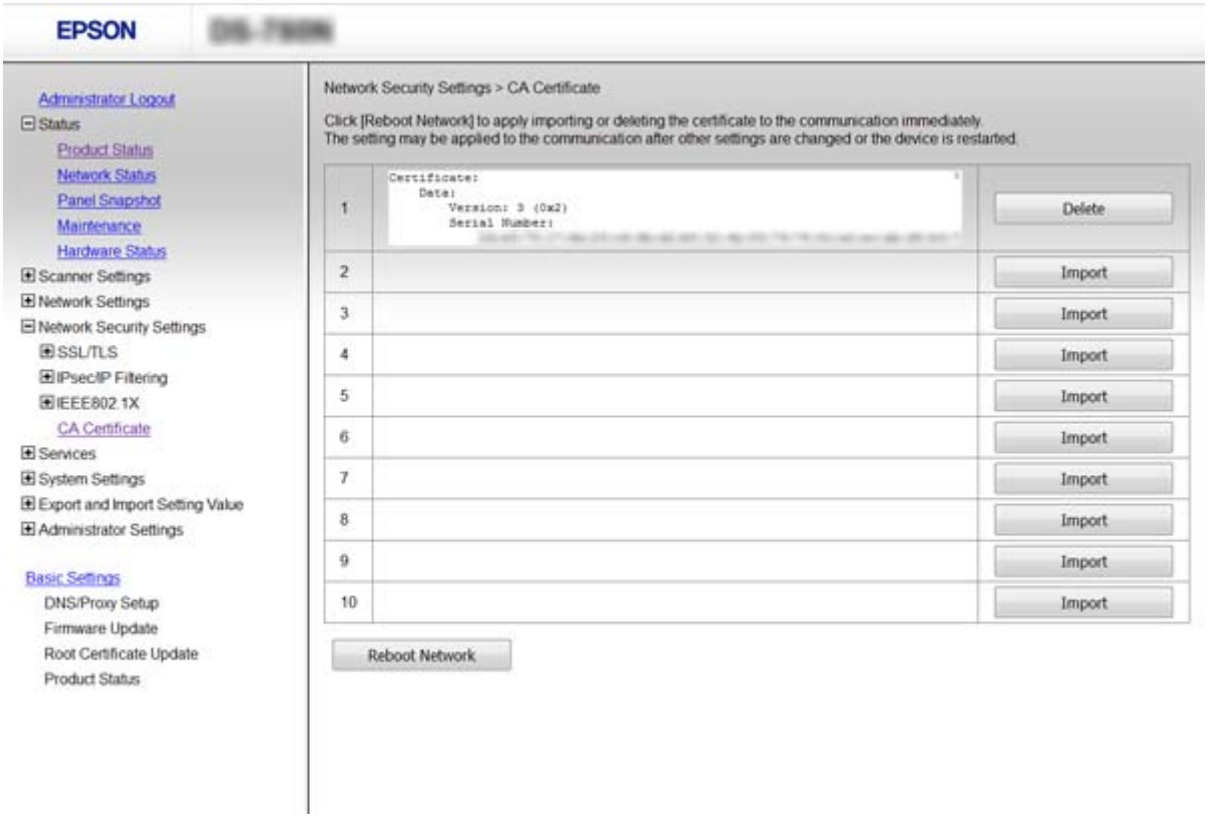
معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22

حذف CA Certificate

يمكنك حذف CA Certificate التي تم استيرادها.

1. قم بالوصول إلى Web Config، ثم حدد **Network Security Settings** > **CA Certificate**.
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 22

الاتصال المشفر باستخدام تصفية IPsec/IP

حول IPsec/IP Filtering

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

لتصفية البيانات الواردة إلى الشبكة، قم بتكوين السياسة الافتراضية. تسري السياسة الافتراضية على جميع المستخدمين أو المجموعات المتصلة بالماسحة الضوئية. 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 الماسحة الضوئية 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 Default Policy

1. قم بالوصول إلى Web Config وحدد **Network Security Settings** < **IPsec/IP Filtering** < **Basic**.
2. أدخل قيمة لكل عنصر.
3. انقر فوق **Next**.

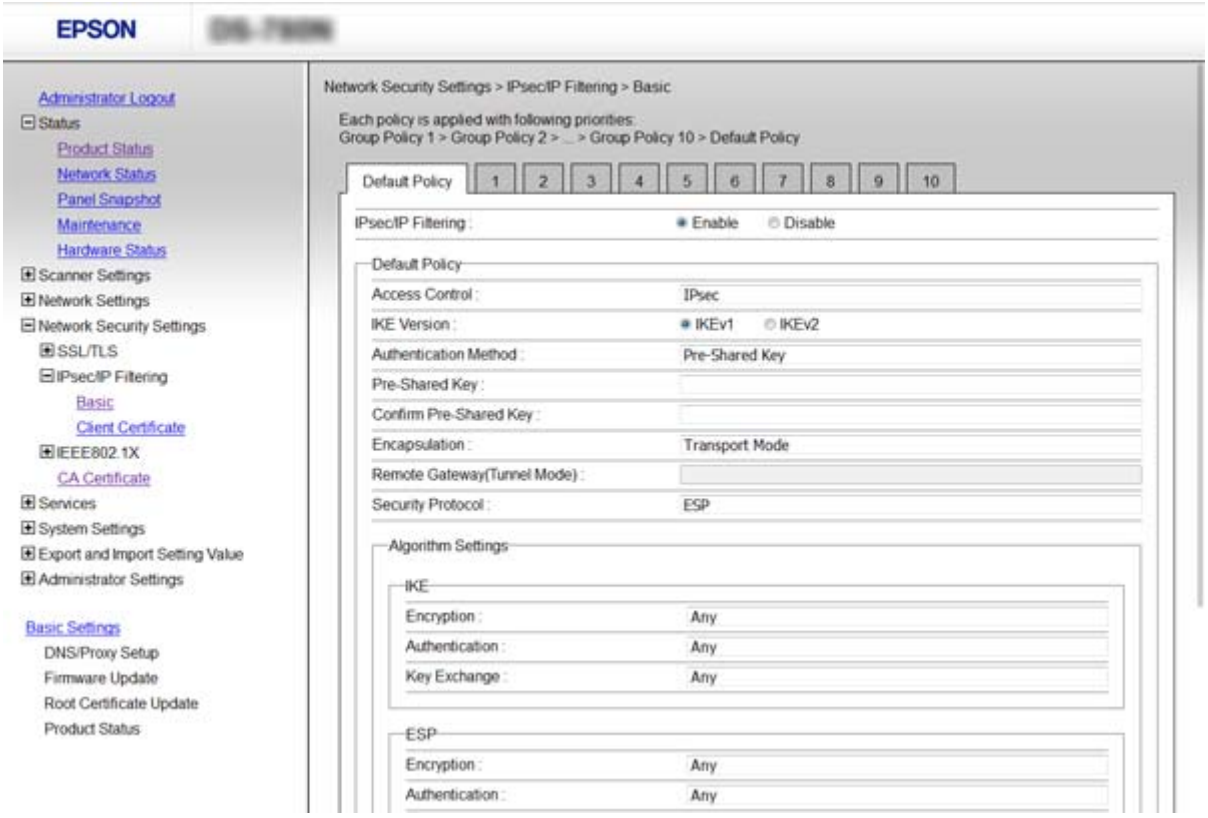
   يتم عرض رسالة تأكيد.
4. انقر فوق **OK**.

   الماسحة الضوئية قيد التحديث.

معلومات ذات صلة

◄ "الوصول إلى تطبيق Web Config" في الصفحة 22
◄ "عناصر إعداد Default Policy" في الصفحة 68

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.	
	Permit Access	حدد هذه الطريقة للسماح بمرور حزم بيانات IP المكونة.
	Refuse Access	حدد هذه الطريقة لرفض مرور حزم بيانات IP المكونة.
	IPsec	حدد هذه الطريقة للسماح بمرور حزم بيانات IPsec المكونة.
IKE Version	حدد IKEv1 أو IKEv2 لإصدار IKE. حدد أحدهما وفقًا للجهاز المتصل به المصادقة الضوئية.	
IKEv1	يتم عرض العناصر التالية عند تحديد **IKEv1** لـ **IKE Version**.	
	Authentication Method	لتحديد **Certificate**، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدمًا.
	Pre-Shared Key	إذا قمت بتحديد **Pre-Shared Key** من أجل **Authentication Method**، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفًا.
	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	لتحديد **Certificate**، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدمًا.
	ID Type	حدد نوع معرف الماسحة الضوئية.
	ID	أدخل معرف الماسحة الضوئية الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، و"#"، و"=" بدلاً من الحرف الأول. **Distinguished Name**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". **IP Address**: أدخل تنسيق IPv4 أو IPv6. **FQDN**: أدخل مزيجًا من الأحرف يتراوح بين حرف واحد إلى 255 حرفًا باستخدام A–Z، و a–z، و0–9، و"-"، ونقطة (.). **Email Address**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". **Key ID**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E).
	Pre-Shared Key	إذا قمت بتحديد **Pre-Shared Key** من أجل **Authentication Method**، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفًا.
	Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.
Remote	Authentication Method	لتحديد **Certificate**، تحتاج إلى الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها مقدمًا.
	ID Type	حدد نوع معرف الجهاز الذي تريد مصادقته.
	ID	أدخل معرف الماسحة الضوئية الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، و"#"، و"=" بدلاً من الحرف الأول. **Distinguished Name**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". **IP Address**: أدخل تنسيق IPv4 أو IPv6. **FQDN**: أدخل مزيجًا من الأحرف يتراوح بين حرف واحد إلى 255 حرفًا باستخدام A–Z، و a–z، و0–9، و"-"، ونقطة (.). **Email Address**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". **Key ID**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E).
	Pre-Shared Key	إذا قمت بتحديد **Pre-Shared Key** من أجل **Authentication Method**، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفًا.
	Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.
Encapsulation	إذا قمت بتحديد **IPsec** من أجل **Access Control**، فلابد أن تقوم بتكوين وضع تغليف.	
	Transport Mode	إذا كنت تستخدم الماسحة الضوئية على شبكة LAN نفسها فقط، فحدد هذا. يتم تشفير حزم بيانات IP الطبقة 4 أو ما بعدها.
	Tunnel Mode	إذا كنت تستخدم ماسحة ضوئية 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 حرفًا.	
Security Protocol	**IPsec** لـ **Access Control**، حدد خيارًا.	
	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 التشفير لـ AH. يتوفر ذلك عند تحديد **AH** لـ **Security Protocol**.

معلومات ذات صلة

"تكوين Default Policy" في الصفحة 67

تكوين Group Policy

1. قم بالوصول إلى Web Config وحدد **Network Security Settings** < **IPsec/IP Filtering** < **Basic**.
2. انقر فوق علامة التبويب المرقمة التي ترغب في تكوينها.
3. أدخل قيمة لكل عنصر.
4. انقر فوق **Next**.

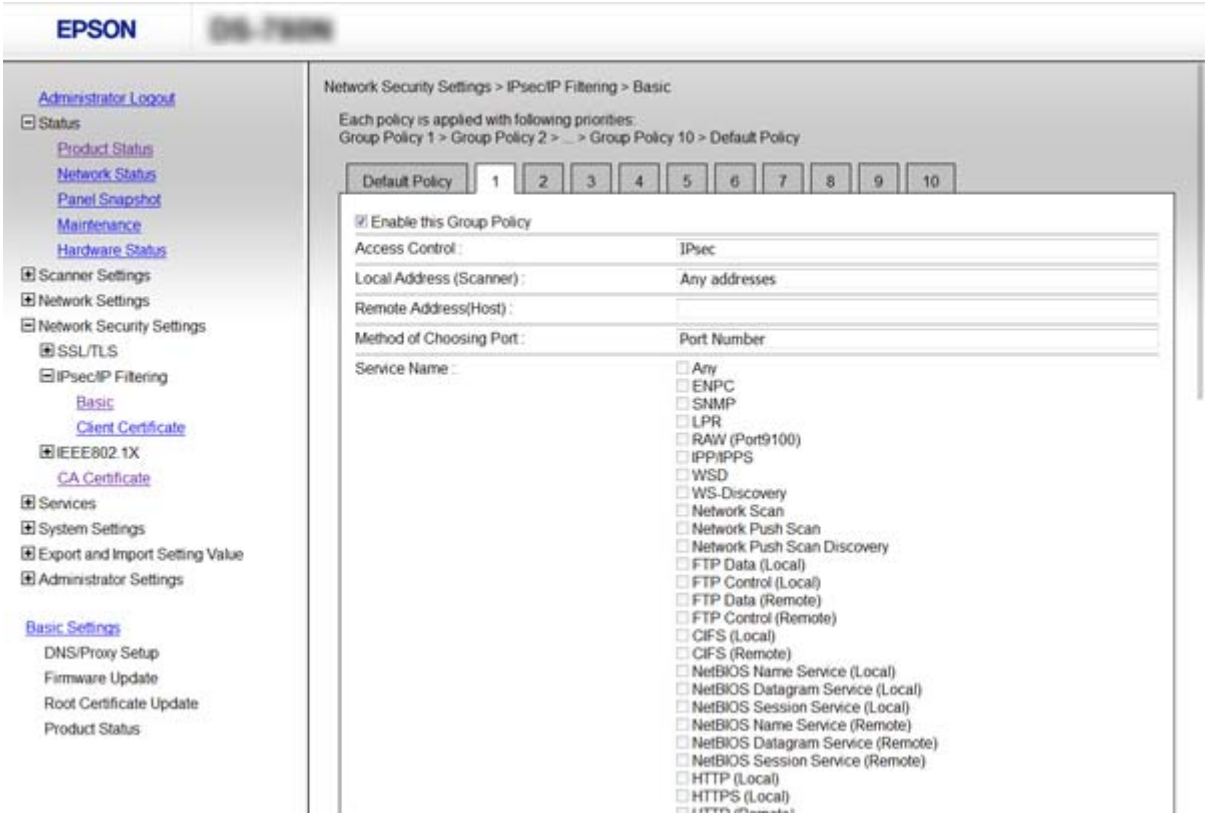
   يتم عرض رسالة تأكيد.
5. انقر فوق **OK**.

   الماسحة الضوئية قيد التحديث.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22
"عناصر إعداد Group Policy" في الصفحة 71

عناصر إعداد Group Policy



العناصر	الإعدادات والشرح	
Enable this Group Policy	يمكنك تمكين سياسة مجموعة أو تعطيلها.	
Access Control	قم بتكوين طريقة تحكم لنقل حزم بيانات IP.	
	Permit Access	حدد هذه الطريقة للسماح بمرور حزم بيانات IP المكونة.
	Refuse Access	حدد هذه الطريقة لرفض مرور حزم بيانات IP المكونة.
	IPsec	حدد هذه الطريقة للسماح بمرور حزم بيانات IPsec المكونة.
Local Address (Scanner)	حدد عنوان IPv4 أو عنوان IPv6 الذي يتوافق مع بيئة شبكتك. إذا تم تعيين عنوان IP تلقائيًا، يمكنك تحديد **Use auto-obtained IPv4 address**.	
Remote Address(Host)	أدخل عنوان IP للجهاز من أجل التحكم في الوصول. يجب أن يتكون عنوان IP من 43 حرفًا أو أقل. إذا لم تدخل عنوان IP، فسيتم التحكم في جميع العناوين. **ملاحظة:** في حالة تعيين عنوان *IP* تلقائيًا (على سبيل المثال، بواسطة بروتوكول *DHCP*)، فقد يصبح الاتصال غير متاح. قم بتكوين عنوان *IP* ثابت.	
Method of Choosing Port	حدد طريقةً لتحديد المنافذ.	
Service Name	إذا قمت بتحديد **Service Name** من أجل **Method of Choosing Port**، فحدد خيارًا.	

إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح	
Transport Protocol	إذا قمت بتحديد **Port Number** من أجل **Method of Choosing Port**، فلابد 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 كحدٍ 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 كحدٍ 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 وفقًا للجهاز المتصل به الماسحة الضوئية.	
IKEv1	يتم عرض العناصر التالية عند تحديد **IKEv1** لـ **IKE Version**.	
	Authentication Method	إذا قمت بتحديد **IPsec** من أجل **Access Control**، فحدد خيارًا. تعتبر الشهادة المستخدمة هي السياسة الافتراضية نفسها.
	Pre-Shared Key	إذا قمت بتحديد **Pre-Shared Key** من أجل **Authentication Method**، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفًا.
	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 خيارًا. تعتبر الشهادة المستخدمة هي السياسة الافتراضية نفسها.
	ID Type	حدد نوع معرف الماسحة الضوئية.
	ID	أدخل معرف الماسحة الضوئية الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، و"#"، و"=" بدلاً من الحرف الأول. **Distinguished Name**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". **IP Address**: أدخل تنسيق IPv4 أو IPv6. **FQDN**: أدخل مزيجًا من الأحرف يتراوح بين حرف واحد إلى 255 حرفًا باستخدام A–Z، و a–z، و0–9، و"-"، ونقطة (.). **Email Address**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". **Key ID**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E).
	Pre-Shared Key	إذا قمت بتحديد **Pre-Shared Key** من أجل **Authentication Method**، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفًا.
	Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.
Remote	Authentication Method	إذا قمت بتحديد **IPsec** من أجل **Access Control**، فحدد خيارًا. تعتبر الشهادة المستخدمة هي السياسة الافتراضية نفسها.
	ID Type	حدد نوع معرف الجهاز الذي تريد مصادقته.
	ID	أدخل معرف الماسحة الضوئية الذي يتوافق مع نوع المعرف. لا يمكنك استخدام "@"، و"#"، و"=" بدلاً من الحرف الأول. **Distinguished Name**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "=". **IP Address**: أدخل تنسيق IPv4 أو IPv6. **FQDN**: أدخل مزيجًا من الأحرف يتراوح بين حرف واحد إلى 255 حرفًا باستخدام A–Z، و a–z، و0–9، و"-"، ونقطة (.). **Email Address**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E). يجب عليك إدراج "@". **Key ID**: أدخل من حرف واحد إلى 128 حرفًا 1-بايت ASCII (0x20 إلى 0x7E).
	Pre-Shared Key	إذا قمت بتحديد **Pre-Shared Key** من أجل **Authentication Method**، فأدخل مفتاحًا مشتركًا مسبقًا مكونًا من عددٍ من الأحرف يتراوح ما بين حرف واحد و 127 حرفًا.
	Confirm Pre-Shared Key	أدخل المفتاح الذي قمت بتكوينه للتأكيد.
Encapsulation	إذا قمت بتحديد **IPsec** من أجل **Access Control**، فلابد أن تقوم بتكوين وضع تغليف.	
	Transport Mode	إذا كنت تستخدم الماسحة الضوئية على شبكة LAN نفسها فقط، فحدد هذا. يتم تشفير حزم بيانات IP الطبقة 4 أو ما بعدها.
	Tunnel Mode	إذا كنت تستخدم ماسحة ضوئية 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 حرفًا.
Security Protocol		إذا قمت بتحديد **IPsec** من أجل **Access Control**، فحدد خيارًا.
	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**.

معلومات ذات صلة

- "تكوين Group Policy" في الصفحة 70
- "مجموعة من Local Address (Scanner) و Remote Address(Host) على Group Policy" في الصفحة 74
- "مراجع أسماء الخدمة في سياسة المجموعة" في الصفحة 75

مجموعة من Local Address (Scanner) و Remote Address(Host) على Group Policy

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

*1 إذا تم تحديد **IPsec** لـ **Access Control**، فلا يمكنك تحديده بطول بادئة.

*2 إذا تم تحديد **IPsec** لـ **Access Control**، يمكنك تحديد عنوان ارتباط بيانات الشبكة المحلية (fe80::) لكن سيتم تعطيل سياسة المجموعة.

*3 باستثناء عناوين ارتباط بيانات الشبكة المحلية 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 ماسحة ضوئية من التطبيقات مثل EpsonNet Config وبرنامج تشغيل الماسحة الضوئية
SNMP	UDP	161	أي منفذ	الحصول على MIB وتكوينه من تطبيقات مثل EpsonNet Config وبرنامج تشغيل الماسحة الضوئية Epson
WSD	TCP	أي منفذ	5357	تحكم WSD
WS-Discovery	UDP	3702	أي منفذ	البحث عن ماسحة ضوئية من WSD
Network Scan	TCP	1865	أي منفذ	إرسال بيانات المسح الضوئي من Document Capture Pro
Network Push Scan Discovery	UDP	2968	أي منفذ	البحث عن كمبيوتر من الماسحة الضوئية.
Network Push Scan	TCP	أي منفذ	2968	الحصول على معلومات حول وظيفة المسح الضوئي بالدفع من Document Capture Pro أو Document Capture
HTTP (Local)	TCP	80	أي منفذ	خادم HTTP(S) (إرسال بيانات Web Config و WSD)
HTTPS (Local)	TCP	443	أي منفذ	
HTTP (Remote)	TCP	أي منفذ	80	عميل HTTP(S) (اتصال بين 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:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: أدخل حتى 127 حرفًا.

Group Policy:

لا تقم بالتكوين.

قبول المسح الضوئي باستخدام Epson Scan 2 وإعدادات الماسحة الضوئية

يوضح هذا المثال السماح بالربط بين بيانات المسح الضوئي وتكوين الماسحة الضوئية باستخدام خدمات محددة.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: حدد المربع.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: عنوان IP للجهاز التابع

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

❏ **Service Name**: حدد مربع **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** و **HTTPS (Local)**.

استلام الوصول من عنوان IP محدد فقط

يسمح هذا المثال لعنوان IP محدد بالوصول إلى الماسحة الضوئية.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**:**Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: حدد المربع.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: عنوان IP للجهاز التابع للمسؤول

ملاحظة:

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

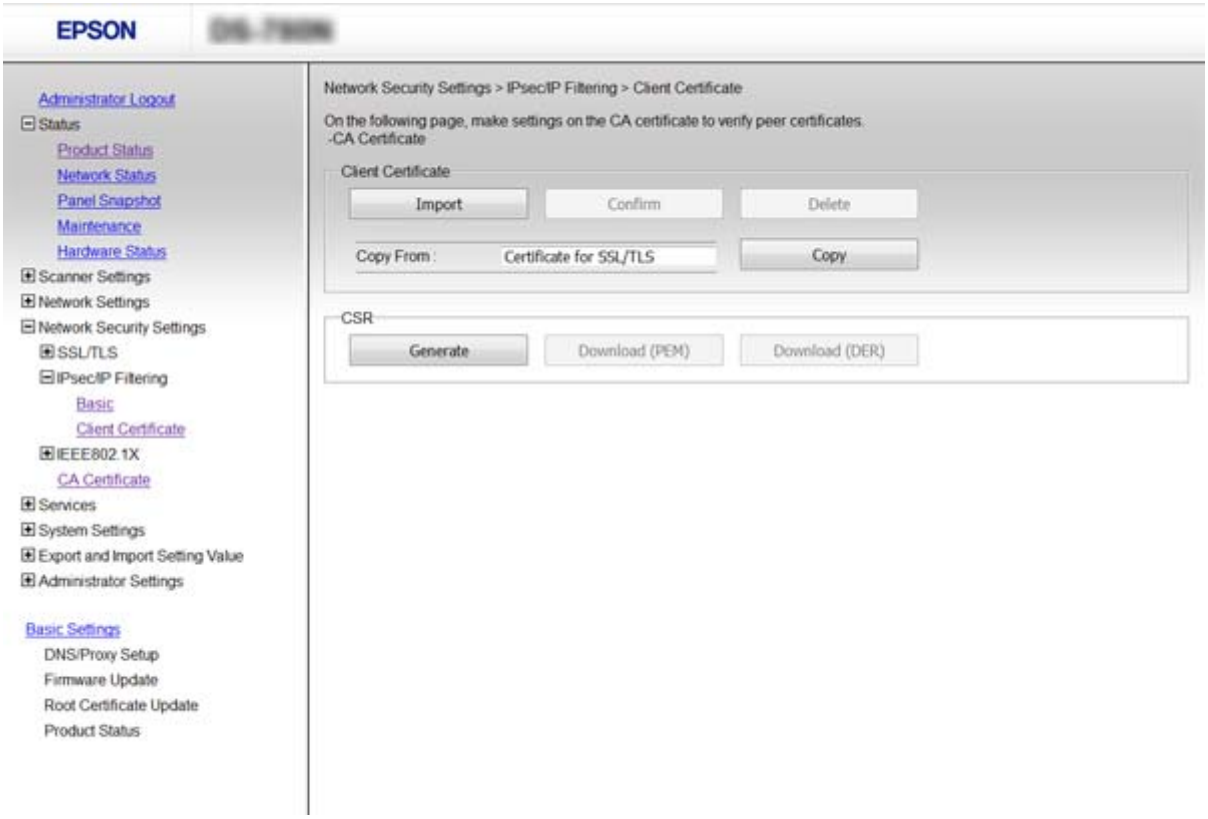
تهيئة شهادة لـ IPsec/IP Filtering

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

1. قم بالوصول إلى Web Config وحدد **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

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 22

"الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها" في الصفحة 59

استخدام بروتوكول SNMPv3

معلومات عن SNMPv3

يعد SNMP بروتوكولاً يقوم بإجراء المراقبة والتحكم لجمع معلومات الأجهزة المتصلة بالشبكة. يُعد SNMPv3 إصداراً لميزة 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 الماسحة الضوئية تدعم بروتوكول SNMPv3، يمكنك مراقبة الوصول إلى الماسحة الضوئية والتحكم فيه.

1. قم بالوصول إلى Web Config وحدد **Services** > **Protocol**.

2. أدخل قيمة لكل عنصر من عناصر **SNMPv3 Settings**.
3. انقر فوق **Next**.

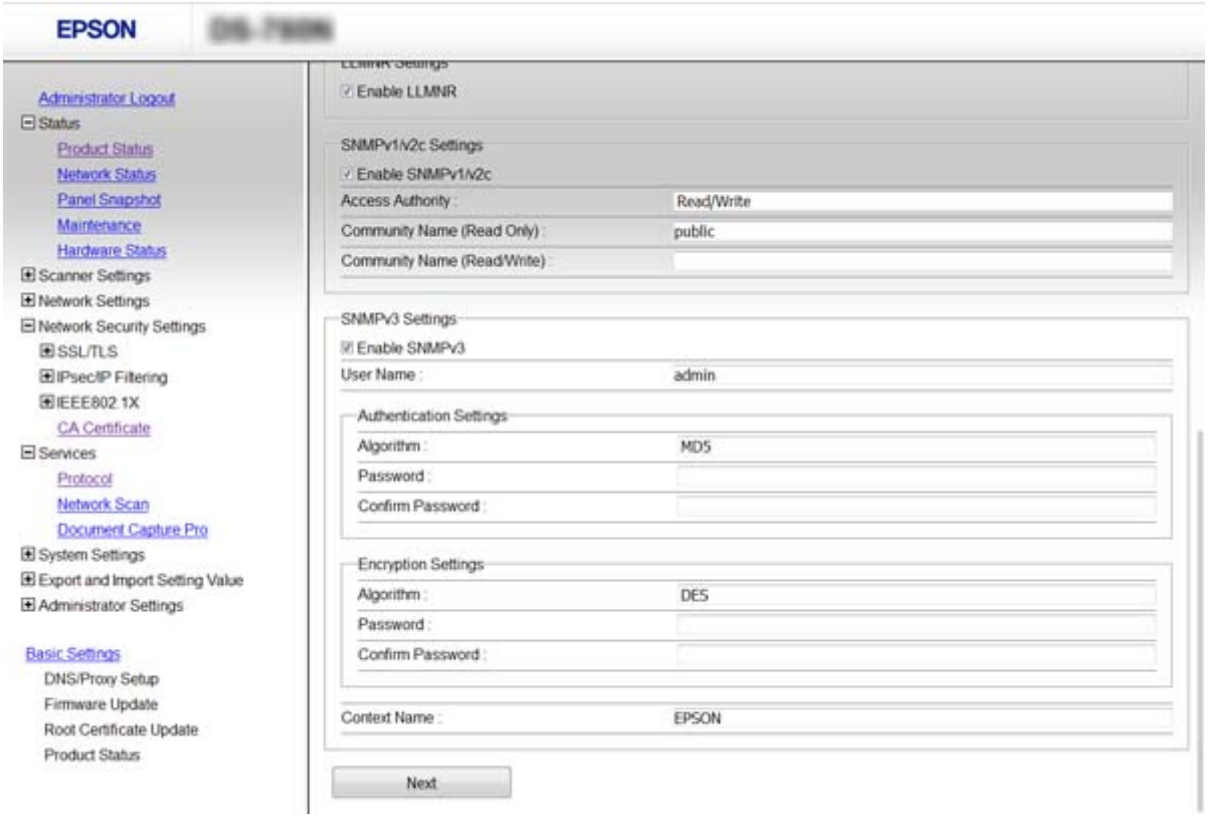
   يتم عرض رسالة تأكيد.
4. انقر فوق **OK**.

   الماسحة الضوئية قيد التحديث.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22
"عناصر إعداد SNMPv3" في الصفحة 78

عناصر إعداد SNMPv3



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	
Algorithm	حدد خوارزمية للمصادقة.
Password	أدخل ما بين 8 إلى 32 حرفًا بتنسيق (ASCII (0x20-0x7E.
Confirm Password	أدخل كلمة المرور التي قمت بتكوينها للتأكيد.

إعدادات الأمان المتقدمة لـ Enterprise

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

معلومات ذات صلة

"تكوين SNMPv3" في الصفحة 77

توصيل الماسحة الضوئية بشبكة IEEE802.1X

تكوين شبكة IEEE802.1X

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

1. قم بالوصول إلى Web Config وحدد **Network Security Settings** < **IEEE802.1X** < **Basic**.
2. أدخل قيمة لكل عنصر.
3. انقر فوق **Next**.

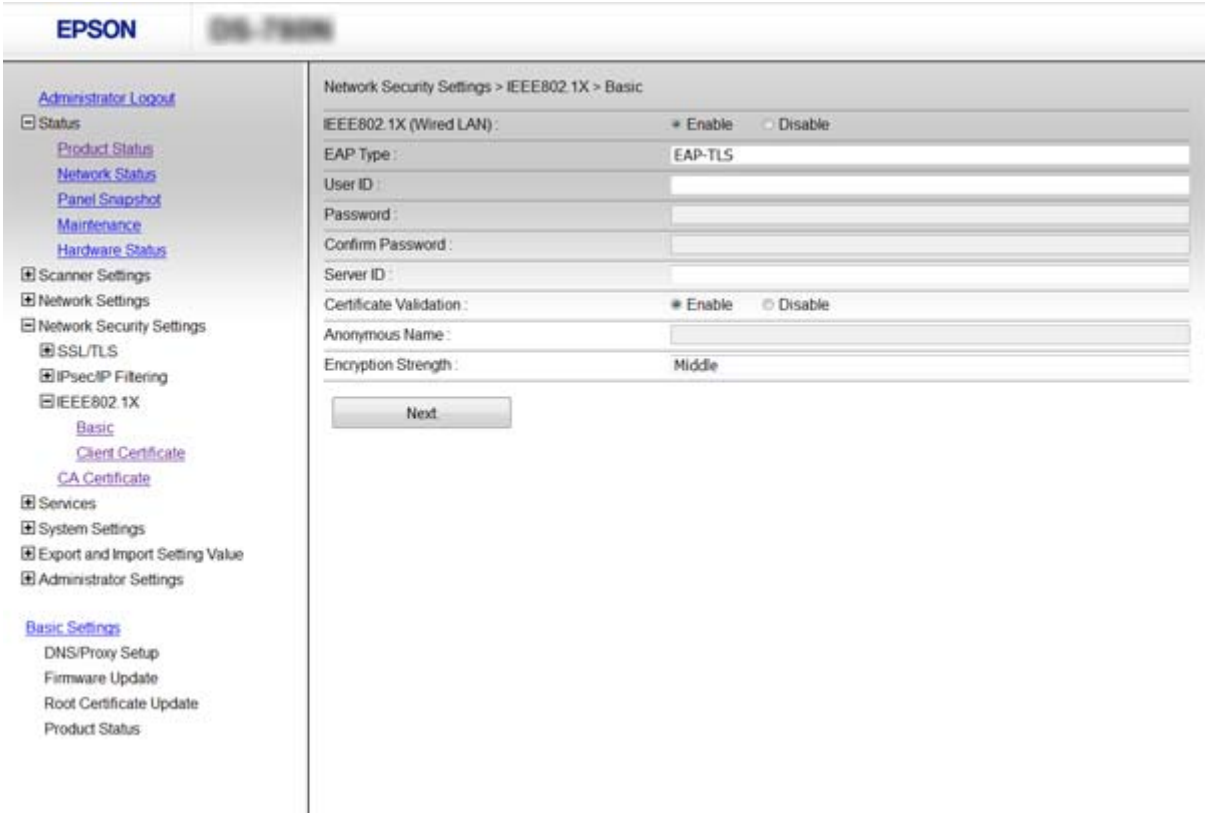
   يتم عرض رسالة تأكيد.
4. انقر فوق **OK**.

   الماسحة الضوئية قيد التحديث.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22
"عناصر إعداد شبكة IEEE802.1X" في الصفحة 80
"تعذر الوصول إلى الطابعة أو الماسحة الضوئية بعد تكوين IEEE802.1X" في الصفحة 84

عناصر إعداد شبكة IEEE802.1X



العناصر	الإعدادات والشرح	
IEEE802.1X (Wired LAN)	يمكنك تمكين إعدادات الصفحة أو تعطيلها (**IEEE802.1X** > **Basic**) بالنسبة إلى IEEE802.1X (LAN السلكية).	
EAP Type	حدد أحد الخيارات لأسلوب المصادقة بين الماسحة الضوئية وخادم RADIUS.	
	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 1-بايت ASCII (0x20 إلى 0x7E) حرفًا.	
Password	قم بتكوين كلمة مرور لمصادقة الماسحة الضوئية. أدخل من 1 إلى 128 1-بايت ASCII (0x20 إلى 0x7E) حرفًا. إذا كنت تستخدم أحد خوادم Windows كخادم RADIUS يمكنك إدخال ما يصل إلى 127 حرفًا.	
Confirm Password	أدخل كلمة المرور التي قمت بتكوينها للتأكيد.	
Server ID	يمكن تكوين معرِّف خادم للمصادقة مع خادم RADIUS محدد. يتحقق المصدق مما إذا كان معرف الخادم ورد في خانة subject/subjectAltName لشهادة الخادم المرسلة من خادم RADIUS أم لا. أدخل من 0 إلى 128 1-بايت ASCII (0x20 إلى 0x7E) حرفًا.	
Certificate Validation	يمكنك تعيين التحقق من صحة الشهادة بغض النظر عن أسلوب المصادقة. قم باستيراد الشهادة في **CA Certificate**.	

إعدادات الأمان المتقدمة لـ Enterprise

العناصر	الإعدادات والشرح	
Anonymous Name	إذا قمت بتحديد **PEAP-TLS** أو **PEAP/MSCHAPv2** من أجل **Authentication Method**، فبإمكانك تكوين اسم مجهول بدلاً من معرف المستخدم للعبارة 1 من مصادقة PEAP. أدخل من 0 إلى 128 1-بايت ASCII (0x20 إلى 0x7E) حرفًا.	
Encryption Strength	يمكنك تحديد إحدى القيم التالية.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

معلومات ذات صلة

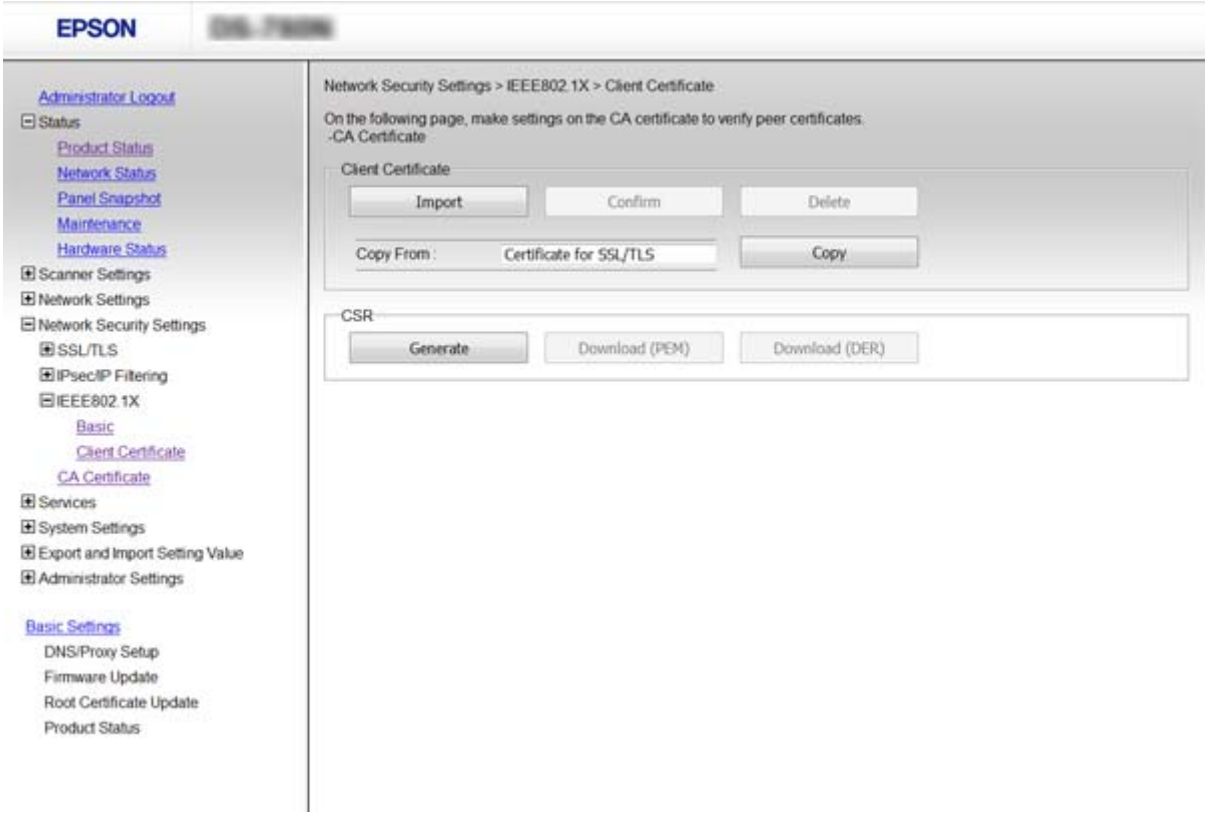
"تكوين شبكة IEEE802.1X" في الصفحة 79

تهيئة شهادة لـ IEEE802.1X

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

1. قم بالوصول إلى Web Config وحدد **Network Security Settings** < **IEEE802.1X** < **Client Certificate**.
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 22

"الحصول على شهادة موقعة من المرجع المصدق (CA) واستيرادها" في الصفحة 59

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 التحكم بالمساحة الضوئية.

1. اضغط على **الإعدادات** > **إعدادات الشبكة**.
2. اضغط **تغيير الإعدادات**.
3. اضغط على العناصر التي ترغب في تعطيلها.
   - ❏ **ترشيح IPsec/IP**
   - ❏ **IEEE802.1X**
4. عندما تظهر رسالة الاكتمال، اضغط على **متابعة**.

استعادة وظيفة الأمان باستخدام تهيئة الويب

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

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

تعطيل تصفية *IPsec/IP* باستخدام *Web Config*

1. قم بالوصول إلى Web Config وحدد **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
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 22

المشكلات الخاصة باستخدام ميزات أمان الشبكة

نسيان مفتاح مشترك مسبقًا

قم بتكوين المفتاح مرةً أخرى باستخدام تطبيق Web Config.

لتغيير المفتاح، قم بالوصول إلى Web Config وحدد **Network Security Settings** < **IPsec/IP Filtering** < **Basic** < **Default Policy** أو **Group Policy**.

عندما تُغير المفتاح المشترك مسبقًا، قم بتهيئته لأجهزة الحاسوب.

معلومات ذات صلة

"الوصول إلى تطبيق Web Config" في الصفحة 22

يتعذر الاتصال باستخدام اتصال IPsec

هل تستخدم خوارزمية غير مدعمة لإعدادات الكمبيوتر؟

تدعم الماسحات الضوئية الخوارزميات التالية.

أساليب الأمان	الخوارزميات
خوارزمية التشفير IKE	AES-CBC-128، وAES-CBC-192، وAES-CBC-256، وAES-GCM-128*، وAES-GCM-192*، وAES-GCM-256*، و3DES
خوارزمية المصادقة IKE	SHA-1، وSHA-256، وSHA-384، وSHA-512، وMD5
خوارزمية تبادل المفاتيح IKE	DH Group1، DH Group2، DH Group5، DH Group14، DH Group15، DH Group16، DH Group17، DH Group18، DH Group19، DH Group20، DH Group21، DH Group22، DH Group23، DH Group24، DH Group25، DH Group26، DH Group27*، DH Group28*، DH Group29*، DH Group30*
خوارزمية التشفير ESP	AES-CBC-128، وAES-CBC-192، وAES-CBC-256، وAES-GCM-128، وAES-GCM-192، وAES-GCM-256، و3DES
خوارزمية المصادقة ESP	SHA-1، وSHA-256، وSHA-384، وSHA-512، وMD5
خوارزمية المصادقة AH	SHA-1، وSHA-256، وSHA-384، وSHA-512، وMD5

* متوفر IKEv2 فقط

معلومات ذات صلة

"الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 67

يتعذر الاتصال فجأة

هل عنوان IP الخاص بالماسحة الضوئية غير صالح أو تم تغييره؟

قم بتعطيل IPsec من لوحة التحكم بالماسحة الضوئية.

إذا كان DHCP منتهي الصلاحية، أو إعادة التمهيد أو عنوان IPv6 منتهي الصلاحية أو لم يتم الحصول عليه، فقد لا يتم العثور على عنوان IP المسجل لـ Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) الخاص بالماسحة الضوئية.

استخدم عنوان IP ثابت.

هل عنوان IP الخاص بالحاسوب غير صالح أو تم تغييره؟

قم بتعطيل IPsec من لوحة التحكم بالماسحة الضوئية.

إذا كان DHCP منتهي الصلاحية، أو إعادة التمهيد أو عنوان IPv6 منتهي الصلاحية أو لم يتم الحصول عليه، فقد لا يتم العثور على عنوان IP المسجل لـ Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) الخاص بالماسحة الضوئية.

استخدم عنوان IP ثابت.

معلومات ذات صلة

◆ "الوصول إلى تطبيق Web Config" في الصفحة 22
◆ "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 67

تعذر الاتصال بعد تهيئة تصفية IPsec/IP

قد تكون قيمة التعيين غير صحيحة.

قم بتعطيل تصفية IPsec/IP من لوحة التحكم بالماسحة الضوئية. ثم قم بتوصيل الماسحة الضوئية والحاسوب وإجراء إعدادات تصفية IPsec/IP مرة أخرى.

معلومات ذات صلة

◆ "الاتصال المشفر باستخدام تصفية IPsec/IP" في الصفحة 67

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

قد تكون الإعدادات غير صحيحة.

قم بتعطيل IEEE802.1X من لوحة التحكم بالماسحة الضوئية. قم بتوصيل الماسحة الضوئية والحاسوب، ثم قم بتكوين IEEE802.1X مرة أخرى.

معلومات ذات صلة

◆ "تكوين شبكة IEEE802.1X" في الصفحة 79

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 الماسحة الضوئية بعد إرسال الطلب إلى المرجع المصدق؟
احصل على شهادة موقعة من المرجع المصدق مرةً أخرى باستخدام طلب CSR.

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 62

تعذر تحديث شهادة ذاتية التوقيع

هل تم إدخال Common Name؟

لا بد من إدخال **Common Name**.

هل تم إدخال رموز غير مدعمة في Common Name؟ على سبيل المثال، الرموز اليابانية غير مدعمة.

أدخل عددًا من الرموز يتراوح ما بين 1 إلى 128 رمزًا 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 ذاتيًا" في الصفحة 64

يتعذر إنشاء طلب CSR

هل تم إدخال Common Name؟

لابد من إدخال **Common Name**.

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

أدخل عددًا 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 59

ظهور تحذير مرتبط بشهادة رقمية

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

الرسائل	السبب/الحل
Cannot use the Server Certificates that include more than three CA certificates.	**السبب:** يحتوي ملف الشهادة بتنسيق PKCS#12 على أكثر من 3 شهادات مرجع مصدق (CA). **الحل:** قم باستيراد كل شهادة عند التحويل من تنسيق PKCS#12 إلى تنسيق PEM، أو قم باستيراد ملف الشهادة بتنسيق PKCS#12 الذي يتضمن حتى شهادتي مرجع مصدق (CA).
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**السبب:** الشهادة منتهية الصلاحية. **الحل:** ❏ إذا كانت الشهادة منتهية الصلاحية، فاحصل على شهادة جديدة وقم باستيرادها. ❏ إذا كانت الشهادة غير منتهية الصلاحية، فتأكد من تعيين تاريخ الماسحة الضوئية ووقتها بشكلٍ صحيح.
Private key is required.	**السبب:** لا يوجد مفتاح خاص مزدوج مع الشهادة. **الحل:** ❏ إذا كانت الشهادة بتنسيق PEM/DER وتم الحصول عليها من طلب CSR باستخدام جهاز كمبيوتر، فحدد ملف المفتاح الخاص. ❏ إذا كانت الشهادة بتنسيق PKCS#12 وتم الحصول عليها من طلب CSR باستخدام جهاز كمبيوتر، فقم بإنشاء الملف الذي يتضمن المفتاح الخاص.
	السبب: قمت بإعادة استيراد شهادة PEM/DER التي تم الحصول عليها من طلب CSR باستخدام تطبيق Web Config. **الحل:** إذا كانت الشهادة بتنسيق PEM/DER وتم الحصول عليها من طلب CSR باستخدام تطبيق Web Config، يمكنك استيرادها مرةً واحدةً فقط.
Setup failed.	**السبب:** يتعذر إتمام التكوين بسبب فشل الاتصال بين الماسحة الضوئية والكمبيوتر أو تعذرت قراءة الملف نتيجة لبعض الأخطاء. **الحل:** بعد فحص الملف المحدد والاتصال، قم باستيراد الملف مرةً أخرى.

معلومات ذات صلة

"حول المصادقة الرقمية" في الصفحة 59

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 مرةً أخرى.

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

إعدادات الأمان المتقدمة لـ Enterprise

معلومات ذات صلة

- "حذف شهادة موقعة من المرجع المصدق (CA)" في الصفحة 63
- "استيراد شهادة موقعة من المرجع المصدق (CA)" في الصفحة 62