النسخة ١,٠
يناير ٢٠١١

Xerox® Phaser™ 3635MFP
منصة الواجهة المدودة

ويتم إدخال التعديلات في هذه الوثيقة بشكل دوري. سيتم تصحيح التغييرات والأخطاء الفنية والأخطاء المطبعية في الإصدارات اللاحقة.

نسخة الوثيقة ١,٠: يناير ٢٠١١

المحتويات

مقدمة

تفتح منصة الواجهة المَدُودة (EIP) من Xerox آفاقًا واسعة جديدة من الإمكانيات أمام أجهزة Xerox. فبواسطة EIP, يتمكن جهاز Xerox الخاص بك من أن ينتهج خطك غير أن تنتهج أنت خطه.

- **المستخدمون النهائيون** يتمكنون من مشاركة وتخزين وطباعة المعلومات بسهولة
- **العاملون في مجال تقنية المعلومات** يتمكنون من تقديم قيمة إضافية وحماية المعلومات المحسنة لعملائهم
- **المطورون** يتمكنون من إنشاء التطبيقات بسرعة وبسهولة ويمكن بعد ذلك تخصيص هذه التطبيقات لتلائم واجهة مستخدم الجهاز المعينة

ثمة العديد من الحلول البرمجية الاختيارية التي يمكنك شراؤها وتثبيتها على جهازك. ويمكّنك EIP من تخصيص جهازك ليناسب إجراءات العمل المعينة الخاصة بك. ويمكّن EIP (منصة الواجهة المدودة) من Xerox موفري البرامج وشركاءهم من تطوير البرامج المخصصة بواسطة الأدوات القياسية المستندة إلى الويب وذلك لإنشاء التطبيقات المستندة إلى الملقم والتي يمكن الوصول إليها مباشرة من واجهة مستخدم الجهاز.

فوائد استخدام EIP بالنسبة إلى المستخدم النهائي

- **تبسيط** إجراءات العمل المعقدة جعلاً الجهاز أسهل استخدامًا.
- **نقل** الوثائق المطبوعة إلى معلومات رقمية مما يجعلها أسهل تحريرًا وتخزينًا ومشاركةً.
- **ضبط** الجهاز لينتهج خطك غير أن تنتهج أنت خطه.
- **إكمال** مهام معينة بأكملها من الجهاز بما في ذلك استرجاع الوثائق الموجودة على الشبكة بدون استخدام الكمبيوتر.
- **تقديم خدمة** أسرع لعملائك.
- **دمج** الحلول في بنية تقنية المعلومات الأساسية الموجودة الخاصة بك.
- **إدارة** الحلول المركزة حيثما كنت في جميع أنحاء العالم.
- **توسيع** الجهاز وضبطه بما يناسب أعمالك.
- **إنشاء** الحلول المخصصة بسهولة فـ EIP مستندة إلى قياسات الويب مثل HTML و CSS و XML و JavaScript. كما أنه يستخدم بروتوكولات الحماية العادية – HTTPS و SSL.

مثال على ما يمكن تنفيذه بواسطة EIP

- استخدام القوائم واللغة الخاصة بأعمالك أو مجموعة عملك مثل "البحث في قاعدة بيانات العملاء" أو "إرسال الاستمارة إلى قسم الشكاوى" أو "إرسال الفاكس إلى الحسابات القادرة على الدفع".
- يمكن عرض كافة تفضيلاتك الشخصية على واجهة المستخدم لجهازك وذلك بتمرير بطاقة تعريفك.
- جعل إجراءات العمل المعقدة بسيطة حيث لا يجب إلاّ الضغط على أزرار معدودة.
- تحويل المعلومات المطبوعة إلى مستودع للوثائق بالضغط على زر واحد.
- إرسال المستندات إلى قائمة انتظار الطباعة الشبكية ثم طباعتها من أي جهاز يوجد في الشبكة من خلال تمرير بطاقة تعريفك.
- طباعة نشرة الأخبار اليومية أو تقارير البورصة مباشرة من واجهة مستخدم جهاز Xerox.

إجراءات مبسطة

اجعل إجراءات العمل المعقدة بسيطةً.

تخيل وجود زر "فاتورة" على جهازك والذي يرسل الفواتير فعلاً إلى القسم المناسب ثم يخزن المعلومات مؤرشفةً في نظام لإدارة الوثائق لتسهيل استرجاعها لاحقًا وكذلك يطبع نسخة منها لتصنِّفها في سجلاتك الشخصية.

ذلك ويتمكن المستخدمون من مسح مستنداتهم الورقية ضوئيًا والتقاطها وعرض صور مصغرة منها وإضافتها إلى موقع يخزن فيه المستندات الكثيرة الاستخدام. مثال:

يتمكن الأساتذة من مسح الملاحظات ضوئيًا بشكل مباشر إلى مستودع القسم ليصل إليها الطلاب في وقت لاحق.

ويتمكن الطلاب من مسح أوراق وجباتهم ضوئيًا إلى مجلد القسم الخاص بهم ليراجعها الأساتذة.

وتستغل منصة الواجهة المدودة من Xerox حلولاً إنترنتية لشركاء Xerox وذلك لتمكين المستخدمين من الوصول إلى مستودعات الوثائق من لوحة التحكم في الجهاز.

وبالإضافة إليها ثمة نظام **Xerox Secure Access Unified ID System™** الذي يستهدف المنظمات مثل شركات المنتجات الصحية وشركات الخدمات المالية والمؤسسات التربوية التي تبحث عن المزيد من الأمان بالنسبة إلى سجلاتهم الحساسة. ومن خلال هذا النظام الذي يتضمن قُرَّاء البطاقات والبرامج معًا يتمكن المستخدمون من الوصول إلى أجهزة Xerox بعد عرض أو تمرير بطاقات تعريفهم في قارئ البطاقات الخاص بالجهاز. ولتحسين الحماية يمكن إدخال PIN أو كلمة مرور إلى البرنامج. ويمكن دمج نظام Secure Access (الوصول المحمي) في نظام بطاقات تعريف المستخدَمين الموجود الخاص بالمنظمة.

وقد يُطلب توفر موارد إضافية في الجهاز اعتمادًا على الحل المستخدم.

للاطلاع على المزيد من المعلومات، اتصل بمندوب مبيعات Xerox الخاص بك.

حلول شخصية

يسهل EIP تسجيل الدخول إلى الجهاز بإدخال تفاصيل تسجيل الدخول الخاصة بك أو تمرير بطاقة تعريف شركتك.

ولا يوفر ذلك الوصول المحمي إلى الجهاز فحسبُ بل يمنحك خيارات وصول خصيصة لنوع العمل الذي تقوم به مما يجعل عملك أسهل وذلك لأن الجهاز يعرف الآن من أنت.

تكوين XEIP

أشياء يجب التحقق منها

قبل البدء في إجراء التثبيت، الرجاء التحقق من توفر أو تنفيذ كل مما يلي.

- **تحققْ من أن الجهاز يعمل على ما يرام في الشبكة.**
- **تحققْ من تثبيت وعمل حل EIP الخاص بك.** اتصل بمندوب مبيعات Xerox للمزيد من المعلومات.
- **تحققْ من تمكين Secure HTTP SSL على الجهاز.** (إنما ذلك اختياري)

للاطلاع على التفاصيل, راجع تمكين (SSL) Secure HTTP في الصفحة ٨.

ملاحظة: يجب تثبيت Machine Digital Certificate (شهادة رقمية للجهاز) على الجهاز قبل أن يمكنك تمكين Secure HTTP (SSL). للاطلاع على التفاصيل, راجع إدارة Machine Digital Certificate (الشهادات الرقمية اللجهاز) في الصفحة ٧.

تمكين الخدمات المخصصة

في محطة العمل

١. افتح مستعرض الويب ثم أدخل *عنوان الـ IP* للجهاز في شريط العنوان أو حقل Location (الموقع).
٢. انقر فوق **Enter** (إدخال) للوصول إلى خدمات الإنترنت للجهاز.
٣. لتمكين تشغيل تطبيقات EIP على الجهاز:
   أ. انقر فوق علامة التبويب **Properties** (خصائص).
   ب. انقر فوق **Services** (خدمات), ثم على رابط **Custom Services** (خدمات مخصصة).
   ج. من الصفحة *Custom Services* (خدمات مخصصة), في المنطقة *Enablement* (تمكين), بالنسبة إلى *Custom Services* (خدمات مخصصة) حدد مربع الاختيار **Enabled** (ممكّن) لتمكين الخدمة.
   د. من منطقة *Optional Information* (معلومات اختيارية) وفي حال طولبت بذلك حدد مربع الاختيار **Enabled** (ممكّن) بالنسبة إلى كل مما يلي:
      - **Export User Password to Custom Service** (تصدير كلمة مرور المستخدم إلى الخدمة المخصصة) - في حالة تحديده ستُرسل كلمات المرور إلى الخدمات المخصصة.
      - **Automatically validate signed certificates from server** (المصادقة التلقائية على الشهادات الموقعة الواردة من الملقم) - في حالة تحديده وليعمل هذا الخيار يجب حوزة كل من الملقم والجهاز على الشهادات. ويجب إصدار الشهادات من قبل سلطة يصادق الجهاز عليها.
   ه. انقر فوق **Apply** (تطبيق).
   و. إذا طولبت بذلك, أدخل معرف مسؤول النظام الخاص بك ورمز المرور. ويكون معرف مسؤول النظام الافتراضي ورمز المرور المناسب "**admin**" و "١١١١".
٤. أصدر شهادةً رقمية (إذا كنت بحاجة إليها). راجع إدارة Machine Digital Certificate (الشهادات الرقمية اللجهاز) في الصفحة ٧.
٥. مكّن SSL (إن وجب ذلك). للاطلاع على التفاصيل, راجع تمكين (SSL) Secure HTTP في الصفحة ٨.

من الجهاز

١. اضغط زر **All Services** (كافة الخدمات).
٢. المس زر **Custom Services** (خدمات مخصصة).
٣. المس زر **EIP Application** (تطبيق EIP) الذي سجلته. ومن المتوقع أن يمكنك الوصول إلى إجراء عمل XEIP الخاص بك من خلال الزر الجديد.

إدارة Machine Digital Certificate (الشهادات الرقمية للجهاز)

١. افتح مستعرض الويب ثم أدخل *عنوان الـ IP* للجهاز في شريط العنوان أو حقل Location (الموقع).
٢. انقر فوق **Enter** (إدخال) للوصول إلى خدمات الإنترنت للجهاز.
٣. انقر فوق علامة التبويب **Properties** (خصائص).
٤. إذا طولبت بذلك, أدخل معرف مسؤول النظام الخاص بك ورمز المرور. ويكون معرف مسؤول النظام الافتراضي ورمز المرور المناسب "**admin**" و "**١١١١**".
٥. انقر فوق **Security** (الحماية).
٦. انقر فوق الرابط **Machine Digital Certificate** (الشهادات الرقمية للجهاز) من شجرة الدليل.
٧. من منطقة *Machine Digital Certificate* (الشهادات الرقمية للجهاز), انقر فوق زر **Create New Certificate** (إنشاء شهادة جديدة).
٨. من منطقة *Create New Certificate* (إنشاء شهادة جديدة), اختر واحدًا مما يلي:

- **Self Signed Certificate: Establish a Self Signed Certificate on this machine** (شهادة بالتوقيع الذاتي: إنشاء شهادة بالتوقيع الذاتي على هذا الجهاز) - يوقّع الجهاز شهادته بصفتها موثوقة وينشئ المفتاح العمومي ليمكن استخدام الشهادة مع تشفير SSL.
- **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** (طلب توقيع الشهادة: تنزيل نموذج طلب توقيع الشهادة لتعالجه سلطة الشهادات الموثوق بها) - يمكن تحميل الشهادات إلى الجهاز من سلطة موثوق بها أو من ملقم يمثل سطلة شهادات.

٩. انقر فوق **Continue** (متابعة).
١٠. أدخل التفاصيل في الحقول التالية بالنسبة إلى الخيار المطلوب:

بالنسبة إلى *Certificate Signed Self* (شهادة بالتوقيع الذاتي):	**بالنسبة إلى *Request Signing Certificate* (طلب توقيع الشهادة):**
• **رمز الدولة المكون من حرفين** • **اسم الولاية/المحافظة** • **اسم المنطقة** • **اسم المنظمة** • **القسم من المنظمة** • **عنوان البريد الإلكتروني** • **مدة الصلاحية بالأيام**	• **رمز الدولة المكون من حرفين** • **اسم الولاية/المحافظة** • **اسم المنطقة** • **اسم المنظمة** • **القسم من المنظمة** • **عنوان البريد الإلكتروني**

١١. انقر فوق **Apply** (تطبيق).
١٢. اعتمادًا على اختيارك فإذا اخترت:

- *Self Signed Certificate* (شهادة بالتوقيع الذاتي): يعرض في Current Status (الحالة الحالية) **A Self Signed Certificate is established on this machine** (إنشاء شهادة بالتوقيع الذاتي على هذا الجهاز).
- *Certificate Signing Request* (طلب توقيع الشهادة): سيعرض نموذج **Certificate Signing Request (CSR)** (طلب توقيع الشهادة).

أ. في حالة اختيارك **Certificate Signing Request** (طلب توقيع الشهادة), انقر فوق الزر **Save As** (حفظ باسم)
ب. ومن مربع الحوار المنبثق, اختر من صيغة **X.509 (.pem)** أو **DER** وانقر فوق **Save** (حفظ).
ج. من القائمة المنبثقة *File Download* (تنزيل الملف), انقر فوق **Save** (حفظ) ثم حدد لموقع على محطة العمل الخاصة بك وانقر فوق **Save** (حفظ) لحفظ الملف.
وبعد توقيع سلطة الشهادات الموثوق بها على الشهادة, ستكون الشهادة جاهزة للحفظ في الجهاز.

د. عدْ إلى شاشة **Machine Digital Certificate Management** (إدارة الشهادات الرقمية للجهاز) وفي منطقة *Machine Digital Certificate* (الشهادات الرقمية للجهاز), انقر فوق **Upload Signed Certificate** (تحميل شهادة موثوق بها).

ه. انقر فوق **Browse** (استعراض) ثم ابحث عن الملف في محطة العمل الخاصة بك وانقر فوق **Open** (فتح).

و. انقر فوق **Upload Certificate** (تحميل الشهادة).

تمكين Secure HTTP (SSL)

ملاحظة: يجب تثبيت Machine Digital Certificate (شهادة رقمية للجهاز) على الجهاز قبل أن يمكنك تمكين Secure HTTP (SSL). للاطلاع على التفاصيل, راجع إدارة Machine Digital Certificate (الشهادات الرقمية اللجهاز) في الصفحة ٧.

في محطة العمل

١. افتح مستعرض الويب ثم أدخل *عنوان الـ IP* للجهاز في شريط العنوان أو حقل Location (الموقع).

٢. انقر فوق **Enter** (إدخال) للوصول إلى خدمات الإنترنت للجهاز.

٣. انقر فوق علامة التبويب **Properties** (خصائص).

٤. إذا طولبت بذلك, أدخل معرف مسؤول النظام الخاص بك ورمز المرور. ويكون معرف مسؤول النظام الافتراضي ورمز المرور المناسب "**admin**" و "١١١١".

٥. انقر فوق **Connectivity** (الاتصال) ثم **Protocols** (بروتوكولات).

٦. انقر فوق الرابط **HTTP** من شجرة الدليل.

٧. من منطقة *Configuration* (تكوين):

أ. بالنسبة إلى *Protocol* (بروتوكول) حدد مربع الاختيار **Enable** (تمكين) لتمكين اتصالات HTTP مع الجهاز.

ب. في الحقل *Port Number* (رقم المنفذ), إدخل رقم المنفذ الذي سيستخدمه ملقم ويب الجهاز من أجل اتصالات HTTP. ويكون رقم المنفذ الافتراضي ٨٠.

ج. بالنسبة إلى *HTTP Security Mode* اختر أحد الخيارات التالية من القائمة المنسدلة:

- **Disable SSL (تعطيل SSL)**
- **Enable SSL** (تمكين SSL) - لتمكين Secure Socket Layer (SSL) بالنسبة إلى الاتصالات الآمنة (HTTPS).
- **Require SSL** (المطالبة بـ SSL) - لجعل Secure Socket Layer (SSL) إلزاميًا.

ملاحظة: في حالة تمكين HTTP فللوصول إلى CentreWare Internet Services (خدمات الإنترنت CentreWare) ستحتوي كافة الصفحات على **https://** في عنوان الـ URL الخاص بمواقع الويب.

د. في الحقل *Keep Alive Timeout* (مهلة النشاط) أدخل مدة انتظار ملقم الويب جوابَ الـ HTTP من العميل قبل إنهاء الجلسة. وتكون المدة الافتراضية ١٠ ثوان.

٨. انقر فوق **Apply** (تطبيق).

ملقم وكيل

يمثل الملقم الوكيل مصفاة بالنسبة إلى العملاء التي تطلب الخدمات والملقمات التي توفرها. ويرشح الملقم الوكيل الطلبات وإذا وافقت الطلبات قواعد التصفية الخاصة بالملقم الوكيل فيُسمح بتلبية الطلب ويتاح الاتصال.

وللملقم الوكيل غرضان أساسيان:

- الاحتفاظ بهوية الأجهزة المستترة وراءه مجهولةً لأغراض الأمان.
- جعل المدة المطلوبة للوصول إلى الموارد أقصر وذلك من خلال تخزين المحتويات مثل صفحات الويب مؤقتًا.

في محطة العمل

١. افتح مستعرض الويب ثم أدخل *عنوان الـ IP* للجهاز في شريط العنوان أو حقل Location (الموقع).
٢. انقر فوق **Enter** (إدخال) للوصول إلى خدمات الإنترنت للجهاز.
٣. انقر فوق علامة التبويب **Properties** (خصائص).
٤. إذا طولبت بذلك, أدخل معرف مسؤول النظام الخاص بك ورمز المرور. ويكون معرف مسؤول النظام الافتراضي ورمز المرور المناسب "**admin**" و "١١١١".
٥. انقر فوق **Connectivity** (الاتصال) ثم **Protocols** (بروتوكولات).
٦. انقر فوق الرابط **Proxy Server** (ملقم وكيل) من شجرة الدليل.
٧. من منطقة *HTTP Proxy Server* (ملقم HTTP الوكيل):
   أ. حدد مربع الاختيار **Auto Detect Proxy Settings** (اكتشاف إعدادات الملقم الوكيل تلقائيًا) لاكتشاف إعدادات الملقم الوكيل تلقائيًا بواسطة بروتوكول WPAD.
   ولتعطيل الاكتشاف التلقائي للملقم الوكيل ألغ تحديد مربع الاختيار هذا فستحتاج بعدئذ إلى إدخال إعدادات الملقم الوكيل يدويًا.
   ب. بالنسبة إلى *HTTP Proxy Server* (ملقم HTTP الوكيل), حدد مربع الاختيار **Enabled** (ممكّن) لإدخال إعدادات الملقم الوكيل يدويًا.
   ج. حدد إما **IP Address** (عنوان IP) أو **Hostname** (اسم مضيف).
   د. أدخل العنوان ورقم المنفذ بالشكل الصحيح في الحقل **IP Address and Port** (عنوان الـ IP والمنفذ) أو **Host Name and Port** (اسم المضيف والمنفذ) علمًا بأن رقم المنفذ الافتراضي هو ٨٠٨٠.
٨. انقر فوق **Apply** (تطبيق).

ملاحظة: يتم استخدام إعدادات الملقم الوكيل من أجل EIP و Smart eSolutions ومسح الشبكة لـ HTTP(s) وتنزيل مجموعة قوالب HTTP(s).

ملاحظة: قد يؤدي الاكتشاف التلقائي لإعدادات الملقم الوكيل إلى كتابة الإعدادات اليدوية من جديد. عطّل Auto Detect Proxy Settings (اكتشاف إعدادات الملقم الوكيل تلقائيًا) لضمان استخدام الإعدادات اليدوية.