Versiunea 1.0
Ianuarie 2011

# Xerox® Phaser™ 3635MFP Extensible Interface Platform

Acestui document i se aduc modificări periodice. Modificările, incorectitudinile tehnice şi erorile tipografice vor fi corectate în ediţiile următoare.

Versiunea documentului 1.0: ianuarie 2011

Tradus de:

Xerox
CTC European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
UK

# Cuprins

# Introducere

Xerox Extensible Interface Platform (EIP) oferă un întreg univers cu totul nou de posibilități pentru dispozitivul Xerox. Cu EIP, dispozitivul Xerox se poate adapta acum pentru a se potrivi modului în care lucrați şi nu invers.

- **Utilizatorii finali** pot partaja, stoca şi imprima cu uşurință informațiile
- **Departamentul IT** poate oferi un plus de valoare şi securitate a informațiilor pentru clienții săi
- **Dezvoltatorii** pot realiza rapid şi uşor aplicații care pot fi personalizate pentru interfața cu utilizatorul a dispozitivului

Există mai multe soluții software opționale care pot fi achiziționate şi instalate pe dispozitivul dvs. EIP vă permite să personalizați dispozitivul special pentru procesele legate de fluxul dvs. de lucru. Xerox EIP (Extensible Interface Platform) le permite producătorilor de software şi partenerilor acestora să realizeze programe personalizate, folosind instrumente standard bazate pe web pentru a crea aplicații server care pot fi accesate direct din interfața cu utilizatorul a dispozitivului.

## Avantajele utilizatorului final rezultate din utilizarea EIP

- **Simplificarea** fluxurilor de lucru complicate combinată cu o utilizare mai uşoară a dispozitivului.
- **Transformarea** documentelor imprimate pe hârtie în informații digitale, ceea ce face informațiile mai uşor de editat, stocat şi partajat.
- **Adaptarea** dispozitivului pentru a corespunde obiceiurilor dvs. şi nu invers.
- **Îndeplinirea** anumitor sarcini integral de la dispozitiv, inclusiv recuperarea documentelor în rețea fără ajutorul unui computer.
- **Deservirea** mai rapidă a clienților dvs.
- **Integrarea** soluțiilor în infrastructura IT existentă.
- **Gestionarea** soluțiilor centralizate de oriunde din întreaga lume.
- **Extinderea** şi adaptarea dispozitivului împreună cu afacerea dvs.
- **Crearea** cu uşurință a soluțiilor personalizate, EIP fiind bazat pe standarde web precum HTML, CSS, XML şi JavaScript. Acesta utilizează, de asemenea, protocoalele standard de securitate - HTTPS şi SSL.

## Exemplu de ceea ce se poate face cu EIP

- Utilizați meniuri şi limbaje specifice pentru afacerea sau grupul de lucru, precum „Căutare bază de date client”, „Trimitere formular la departamentul reclamații” sau „Fax la Conturi furnizori”.
- Toate preferințele personale pot apărea în interfața cu utilizatorul a sistemului dispozitivului prin trecerea legitimației cu ID prin fața cititorului de carduri.
- Transformați un flux de lucru complicat într-un proces simplu în care nu trebuie decât să fie apăsate câteva butoane.
- Introduceți informațiile imprimate pe hârtie într-un director de depozitare a documentelor printr-o simplă atingere a unui buton.
- Trimiteți un document la o coadă de imprimare în rețea şi imprimați-l de la orice dispozitiv din rețeaua respectivă prin trecerea cardului cu ID prin fața cititorului de carduri.

- Imprimați ştirile zilei sau raporturile despre stocuri direct de la interfața cu utilizatorul a dispozitivului Xerox.

## Procese simplificate

Transformați un flux de lucru complicat într-un proces simplu.

Imaginați-vă un buton „facturi” pe dispozitivul dvs. care trimite simultan o factură la departamentul corect, arhivează informațiile într-un sistem de gestionare a documentelor pentru recuperare rapidă şi imprimă o copie pentru evidențele dvs. personale.

Utilizatorii pot scana şi realiza capturi ale documentelor pe hârtie, previzualiza miniaturi şi adăuga aceste miniaturi într-o locație de stocare a documentelor frecvent utilizate, totul foarte rapid.
De exemplu:

Un profesor poate scana notițele direct într-un director specific cursului, pe care elevii îl pot accesa.

Un elev poate scana documentele de evaluare în folderul cursului pentru ca profesorul să le poată nota.

Xerox Extensible Interface Platform utilizează soluții Xerox Partner bazate pe web care le permit utilizatorilor accesarea directoarelor de depozitare a documentelor de la panoul de comandă al aparatului.

La toate acestea se adaugă **Xerox Secure Access Unified ID System™**, care este conceput pentru organizații precum companiile de servicii medicale, firmele de servicii financiare şi instituțiile educaționale care sunt interesate de o mai mare securitate a evidențelor confidențiale. Cu acest sistem, care combină cititoarele de carduri şi software-ul, utilizatorii pot accesa dispozitivele Xerox după trecerea sau mişcarea cardului ID în fața cititorului de carduri de pe dispozitiv. Pentru securitate suplimentară, se poate include un cod PIN sau o parolă în software. Sistemul de acces securizat se poate integra în sistemul de legitimații cu ID ale angajaților existent într-o organizație.

Este posibil să fie necesare resurse suplimentare pe dispozitiv, în funcție de soluție.

Pentru informații suplimentare, contactați reprezentanța de vânzări Xerox.

## Soluții personale

EIP uşurează conectarea la dispozitiv prin introducerea detaliilor de conectare sau trecerea legitimației cu ID-ul companiei prin fața cititorului de carduri.

Aceasta nu oferă doar acces securizat la dispozitiv, ci, din momentul în care dispozitivul vă identifică, puteți accesa opțiuni specifice pentru fluxul dvs. de lucrări - ceea ce vă uşurează munca.

# Configurarea XEIP

## Lista de informații

Înainte de a începe procedura de instalare, asigurați-vă că elementele următoare sunt disponibile sau au fost executate.

- **Asigurați-vă că dispozitivul funcționează la întreaga capacitate în rețea**.
- **Asigurați-vă că soluția EIP este instalată şi funcționează.** Pentru informații suplimentare, contactați reprezentanța de vânzări Xerox.
- **Asigurați-vă că securitatea HTTP SSL este activată pe dispozitiv**. (Opțional) Pentru detalii, consultați Activarea securității HTTP (SSL) la pagina 9.

  Notă: Un certificat digital al aparatului trebuie instalat pe dispozitiv înainte de a putea activa securitatea HTTP (SSL). Pentru detalii, consultați Administrarea certificatului digital al aparatului la pagina 7.

## Activarea serviciilor personalizate

**La stația de lucru**

1. Deschideți browserul web, introduceți *adresa IP* a aparatului în bara de adrese sau în câmpul Locație.
2. Apăsați pe **Enter** pentru a accesa Internet Services (Serviciile Internet) ale dispozitivului.
3. Pentru a activa aplicațiile EIP pe dispozitiv:
   a. Faceți clic pe fila **Properties** (Proprietăți).
   b. Faceți clic pe **Services** (Servicii) şi apoi pe link-ul **Custom Services** (Servicii personalizate).
   c. În pagina *Custom Services* (Servicii personalizate), în zona *Enablement* (Activare), pentru *Custom Services* (Servicii personalizate) selectați caseta de validare **Enabled** (Activat) pentru a activa serviciul.
   d. În zona *Optional Information* (Informații opționale), selectați, dacă este necesar, casetele de validare **Enabled** (Activat) pentru următoarele:
      - **Export password to Custom Services** (Exportare parolă către serviciu personalizat) - dacă este selectată, parolele sunt trimise către serviciul personalizat.
      - **Automatically validate signed certificates from server** (Validare automată certificate semnate din server) - dacă este selectată, pentru ca această opțiune să funcționeze atât pe server cât şi pe dispozitiv, este nevoie de certificate. Aceste certificate trebuie să fie emise de o autoritate de încredere pentru dispozitiv.
   e. Faceți clic pe **Apply** (Aplicare).
   f. Dacă vi se solicită, introduceți ID-ul şi codul de acces ale administratorului de sistem. ID-ul şi codul de acces implicite pentru administratorul de sistem sunt „**admin**”, respectiv „**1111**”.
4. Generați un certificat digital (dacă este necesar), consultați Administrarea certificatului digital al aparatului la pagina 7.
5. Activați SSL (dacă este necesar), pentru detalii, consultați Activarea securității HTTP (SSL) la pagina 9.

**La dispozitiv**

1. Apăsați butonul **Toate Serviciile**.
2. Atingeți butonul **Custom Services** (Servicii personalizate).
3. Atingeți butonul **EIP Application** (Aplicație EIP) pe care l-ați înregistrat. Fluxul de lucru XEIP ar trebui să fie accesibil de la noul buton.

## Administrarea certificatului digital al aparatului

1. Deschideți browserul web, introduceți *adresa IP* a aparatului în bara de adrese sau în câmpul Locație.
2. Apăsați pe **Enter** pentru a accesa Internet Services (Serviciile Internet) ale dispozitivului.
3. Faceți clic pe fila **Properties** (Proprietăți).
4. Dacă vi se solicită, introduceți ID-ul şi codul de acces ale administratorului de sistem. ID-ul şi codul de acces implicite pentru administratorul de sistem sunt „**admin**”, respectiv „**1111**”.
5. Faceți clic pe **Security** (Securitate).
6. Faceți clic pe link-ul **Machine Digital Certificate** (Certificat digital aparat) din structura directorului.
7. Din zona *Machine Digital Certificate* (Certificat digital aparat), faceți clic pe butonul **Create New Certificate** (Creare certificat nou).
8. În zona *Create New Certificate* (Creare certificat nou), selectați una dintre opțiunile următoare:
   - **Self Signed Certificate: Establish a Self Signed Certificate on this machine** (Certificat autosemnat: definirea unui certificat autosemnat pe acest aparat) - dispozitivul semnează propriul certificat ca fiind de încredere şi creează o cheie publică pentru utilizarea certificatului în criptarea SSL.
   - **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** (Solicitare semnare certificat: descărcarea unei cereri de semnare a unui certificat care să fie procesată de o autoritate de certificare de încredere) - un certificat de la o autoritate de certificare sau de la un server care funcționează ca o autoritate de certificare poate fi încărcat pe aparat.
9. Faceți clic pe **Continue** (Continuare).

10. Introduceți detalii în câmpurile următoare pentru selecția dorită:

| **Pentru *Self Signed Certificate* (Certificat autosemnat):** | **Pentru *Certificate Signing Request* (Solicitare semnare certificat):** |
|---|---|
| • **2 Letter Country Code (Codul țării format din 2 litere)**<br>• **State/Province Name (Numele statului/provinciei)**<br>• **Locality Name (Numele localității)**<br>• **Organization Name (Denumirea organizației)**<br>• **Organization Unit (Unitatea organizației)**<br>• **E-mail Address (Adresa e-mail)**<br>• **Days of Validity (Zile de valabilitate)** | • **2 Letter Country Code (Codul țării format din 2 litere)**<br>• **State/Province Name (Numele statului/provinciei)**<br>• **Locality Name (Numele localității)**<br>• **Organization Name (Denumirea organizației)**<br>• **Organization Unit (Unitatea organizației)**<br>• **E-mail Address (Adresa e-mail)** |

11. Faceți clic pe **Apply** (Aplicare).
12. În funcție de selecția dvs., dacă ați selectat:
    - *Self Signed Certificate* (Certificat autosemnat): starea curentă afişează **A Self Signed Certificate is established on this machine** (Un certificat autosemnat este definit pe acest aparat).
    - *Certificate Signing Request* (Solicitare semnare certificat): este afişat formularul **Certificate Signing Request** (Solicitare semnare certificat).

    a. Dacă ați selectat **Certificate Signing Request** (Solicitare semnare certificat), faceți clic pe butonul **Save As** (Salvare ca)

    b. Din caseta de dialog intermediară, selectați fie formatul **X.509 (.pem)** , fie formatul **DER** şi faceți clic pe **Save** (Salvare).

    c. Din meniul intermediar *File Download* (Descărcare fişier), faceți clic pe **Save** (Salvare), selectați locația de pe stația de lucru şi faceți clic pe **Save** (Salvare) pentru a salva fişierul. După semnarea certificatului de către o autoritate de certificare de încredere, acesta poate fi salvat pe aparat.

    d. Reveniți la ecranul **Machine Digital Certificate Management** (Administrare certificat digital aparat), în zona *Machine Digital Certificate* (Certificat digital aparat), faceți clic pe butonul **Upload Signed Certificate** (Încărcare certificat semnat).

    e. Faceți clic pe **Browse** (Răsfoire), localizați fişierul pe stația de lucru şi faceți clic pe **Open** (Deschidere).

    f. Faceți clic pe **Upload Certificate** (Încărcare certificat).

## Activarea securității HTTP (SSL)

Notă: Un certificat digital al aparatului trebuie instalat pe dispozitiv înainte de a putea activa securitatea HTTP (SSL). Pentru detalii, consultați Administrarea certificatului digital al aparatului la pagina 7.

**La stația de lucru**

1. Deschideți browserul web, introduceți *adresa IP* a aparatului în bara de adrese sau în câmpul Locație.
2. Apăsați pe **Enter** pentru a accesa Internet Services (Serviciile Internet) ale dispozitivului.
3. Faceți clic pe fila **Properties** (Proprietăți).
4. Dacă vi se solicită, introduceți ID-ul şi codul de acces ale administratorului de sistem. ID-ul şi codul de acces implicite pentru administratorul de sistem sunt „**admin**”, respectiv „**1111**”.
5. Faceți clic pe **Connectivity** (Conectivitate) şi apoi pe **Protocols** (Protocoale).
6. Faceți clic pe link-ul **HTTP** din structura directorului.
7. În zona *Configuration* (Configurare):
   a. Pentru *Protocol*, selectați caseta de validare **Enable** (Activare) pentru a activa comunicațiile HTTP cu dispozitivul.
   b. În câmpul *Port Number* (Număr port), introduceți numărul portului pe care serverul web al dispozitivului îl va utiliza pentru conexiunile HTTP client. Numărul de port implicit este 80.
   c. Pentru *HTTP Security Mode* (Mod securitate HTTP), selectați una dintre opțiunile următoare din meniul derulant:
      - **Disable SSL (Dezactivare SSL)**
      - **Enable SSL** (Activare SSL) - pentru a activa Secure Socket Layer (SSL) pentru comunicarea securizată (HTTPS).
      - **Requires SSL** (Necesită SSL) - pentru a face Secure Socket Layer (SSL) obligatoriu.

   Notă: Dacă securitatea HTTP este activată, pentru a accesa CentreWare Internet Services, toate paginile vor conține **https://** în URL pentru pagina Web.

   d. În câmpul *Keep Alive Timeout* (Expirare menținere activă), introduceți durata pe care serverul web va aştepta un răspuns HTTP de la un client înainte de a încheia sesiunea. Valoarea implicită este de 10 secunde.
8. Faceți clic pe **Apply** (Aplicare).

## Serverul proxy

Un server proxy acționează ca un filtru pentru clienții care solicită servicii şi serverele care le oferă. Serverul proxy filtrează solicitările şi, în cazul în care solicitările confirmă regulile de filtrare ale serverului proxy, solicitarea este acceptată şi se permite conexiunea.

Un server proxy are două scopuri principale:

- Să păstreze toate dispozitivele din spatele său anonime, din motive de securitate.
- Să reducă timpul necesar pentru accesarea unei resurse prin reținerea conținutului, cum ar fi paginile web dintr-o rețea.

**La stația de lucru**

1. Deschideți browserul web, introduceți *adresa IP* a aparatului în bara de adrese sau în câmpul Locație.
2. Apăsați pe **Enter** pentru a accesa Internet Services (Serviciile Internet) ale dispozitivului.
3. Faceți clic pe fila **Properties** (Proprietăți).
4. Dacă vi se solicită, introduceți ID-ul şi codul de acces ale administratorului de sistem. ID-ul şi codul de acces implicite pentru administratorul de sistem sunt „**admin**”, respectiv „**1111**”.
5. Faceți clic pe **Connectivity** (Conectivitate) şi apoi pe **Protocols** (Protocoale).
6. Faceți clic pe link-ul **Proxy Server** (Server proxy) din structura directorului.
7. În zona *HTTP Proxy Server* (Server proxy HTTP):
   a. Selectați caseta de validare **Auto Detection via WPAD** (Detectare automată prin WPAD) pentru a detecta automat setările proxy folosind protocolul WPAD. Deselectați această casetă de validare pentru a dezactiva detectarea proxy şi a utiliza setările proxy manuale.
   b. Pentru *HTTP Proxy Server* (Server proxy HTTP), selectați caseta de validare **Enabled** (Activat) pentru a seta manual setările proxy.
   c. Selectați fie **IP Address** (Adresă IP), fie **Hostname** (Nume gazdă).
   d. Introduceți adresa şi numărul portului în formatul corect în câmpul **IP Address and Port** (Adresă IP şi port) sau **Host Name and Port** (Nume gazdă şi port). Numărul implicit al portului este 8080.
8. Faceți clic pe **Apply** (Aplicare).

   Notă: Setările serverului proxy sunt folosite pentru EIP, Smart eSolutions, scanarea în rețea HTTP(s) şi descărcarea modelelor HTTP(s).

   Notă: Detectarea automată a setărilor proxy poate suprascrie setările manuale. Dezactivați opțiunea Auto Detection via WPAD (Detectare automată prin WPAD) pentru a asigura utilizarea setărilor manuale.