

Version 1.0
Janvier 2011



Xerox® Phaser™ 3635MFP Plate-forme EIP



©2011 Xerox Corporation. XEROX® et XEROX and Design® sont des marques commerciales de Xerox Corporation aux États-Unis et/ou dans d'autres pays.

Des modifications sont périodiquement apportées à ce document. Les mises à jour seront effectuées et les erreurs techniques et typographiques corrigées dans les versions ultérieures.

Version du document 1.0 : janvier 2011

Traduit par :

Xerox
CTC European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
Royaume-Uni

Table des matières

Introduction	4
Avantages d'EIP pour l'utilisateur final	4
Possibilités offertes par EIP - Exemples	4
Processus simplifiés	5
Solutions individuelles	5
Configuration de XEIP	6
Liste de contrôle	6
Activation des Services personnalisés	6
Gestion du certificat numérique de la machine	7
Activation du protocole HTTP sécurisé (SSL)	8
Serveur Proxy	9

Introduction

La plate-forme EIP (Xerox Extensible Interface Platform) offre une multitude de nouvelles possibilités à votre périphérique Xerox. Grâce à EIP, votre périphérique peut maintenant s'adapter à votre mode de travail, et non le contraire.

- **Les utilisateurs finaux** peuvent facilement partager, stocker et imprimer les informations.
- **Le service informatique** peut valoriser et sécuriser l'information pour ses clients.
- **Les développeurs** sont en mesure de créer rapidement et facilement des applications qui peuvent être personnalisées pour l'interface utilisateur du périphérique.

Il est possible d'acheter et d'installer sur votre périphérique plusieurs solutions logicielles en option. EIP vous permet de personnaliser votre périphérique selon vos processus de flux de travail.

La plate-forme Xerox EIP (Extensible Interface Platform) permet aux fournisseurs de logiciels et aux partenaires de développer des programmes personnalisés grâce à des outils Web standard. Ils peuvent ainsi créer des applications serveur accessibles directement à partir de l'interface utilisateur du périphérique.

Avantages d'EIP pour l'utilisateur final

- **Simplification** des flux de travail complexes tout en facilitant l'utilisation du périphérique.
- **Numérisation** des informations contenues dans les documents imprimés ; celles-ci sont ainsi plus faciles à modifier, stocker et partager.
- **Adaptation** du périphérique à vos habitudes de travail, et non le contraire.
- **Exécution** de certaines tâches entièrement sur le périphérique, notamment la récupération de documents sur un réseau sans l'aide d'un ordinateur.
- **Accélération** du service à vos clients.
- **Intégration** des solutions à votre infrastructure informatique existante.
- **Gestion** des solutions centralisées où que vous soyez.
- **Extension** et adaptation du périphérique à votre activité.
- **Création** facile de solutions personnalisées. La plate-forme EIP s'appuie sur les normes Web comme HTML, CSS, XML et JavaScript. Elle utilise également les protocoles sécurisés HTTPS et SSL.

Possibilités offertes par EIP - Exemples

- Utilisation de la langue et de menus spécifiques à votre entreprise ou groupe de travail, par exemple « Recherche dans la base de données client », « Envoyer le formulaire au service Réclamations » ou « Envoyer par télécopie à la comptabilité ».
- Affichage de toutes vos préférences personnelles sur l'interface utilisateur du périphérique sur simple lecture de votre badge d'identification.
- Simplification radicale d'un flux de travail compliqué, de sorte qu'il puisse être mis en œuvre sur sélection de quelques touches seulement.
- Enregistrement d'informations imprimées dans une zone de stockage de documents sur simple sélection d'une touche.

- Envoi d'un document dans une file d'impression réseau et impression de ce document à partir de n'importe quel périphérique du réseau sur lecture de votre badge d'identification.
- Impression des informations du jour ou de relevés directement à partir de l'interface utilisateur du périphérique Xerox.

Processus simplifiés

Transformez un flux de travail complexe en un processus simple.

Imaginez que vous disposiez d'un bouton « Facture » sur votre périphérique qui vous permette tout à la fois d'envoyer une facture au service approprié, d'archiver les informations dans un système de gestion de documents afin de faciliter leur récupération et d'en imprimer un exemplaire pour vos dossiers personnels.

Les utilisateurs peuvent numériser et capturer rapidement des documents sur papier, les enregistrer dans des emplacements de stockage fréquemment utilisés et afficher des aperçus sous forme de vignettes. Par exemple :

Un enseignant peut numériser ses notes directement dans une zone de stockage spécifique à la formation, à laquelle les étudiants ont accès.

Un étudiant peut numériser ses copies d'évaluation dans le dossier de la formation afin que l'enseignant puisse les corriger.

La plate-forme EIP utilise les solutions Web Xerox Partner pour permettre aux utilisateurs d'accéder aux zones de stockage de documents à partir du panneau de commande de la machine.

Le système **Xerox Secure Access Unified ID System™**, destiné aux organisations comme les organismes de santé, les fournisseurs de services financiers et les établissements d'enseignement qui recherchent une sécurité accrue pour leurs données sensibles, est également à votre disposition. Grâce à ce système, qui allie lecteur de cartes et logiciel, les utilisateurs sont en mesure d'accéder aux périphériques Xerox sur lecture de leur badge d'identification. Pour plus de sécurité, un code PIN ou un mot de passe peut être intégré au logiciel. Le système Secure Access peut s'intégrer au système d'identification par badge actuellement utilisé par l'organisation.

Des ressources supplémentaires sont éventuellement requises sur le périphérique en fonction de la solution.

Pour plus d'informations, contactez le Service Clients Xerox.

Solutions individuelles

EIP vous permet d'accéder aisément au périphérique au moyen de vos informations de connexion ou de votre badge d'identification.

Non seulement l'accès est sécurisé, mais une fois que le périphérique vous a identifié, vous pouvez accéder aux options spécifiques de vos flux de travail, ce qui présente l'avantage de faciliter votre travail.

Configuration de XEIP

Liste de contrôle

Avant d'entamer la procédure d'installation, veillez à ce que les éléments suivants soient disponibles ou que les opérations suivantes aient été effectuées.

- **Assurez-vous que le périphérique est entièrement opérationnel sur le réseau.**
- **Assurez-vous que votre solution EIP est installée et qu'elle est opérationnelle.** Prenez contact avec votre interlocuteur Xerox pour de plus amples informations sur ce point.
- **Assurez-vous que le protocole HTTP sécurisé (SSL) est activé sur le périphérique.** (Facultatif)
Pour plus d'informations, reportez-vous à [Activation du protocole HTTP sécurisé \(SSL\)](#), page 8.

Remarque : un certificat numérique de machine doit être installé sur le périphérique avant d'activer le protocole HTTP sécurisé (SSL). Pour plus d'informations, reportez-vous à [Gestion du certificat numérique de la machine](#), page 7.

Activation des Services personnalisés

Sur votre poste de travail

1. Lancez le navigateur, saisissez l'*adresse IP* de la machine dans la barre d'adresse ou le champ Emplacement.
2. Appuyez sur **Entrer** pour accéder aux services Internet du périphérique.
3. Pour activer les applications EIP sur le périphérique :
 - a. Cliquez sur l'onglet **Propriétés**.
 - b. Cliquez sur **Services**, puis sur le lien **Services personnalisés**.
 - c. Dans la zone *Activation* de la page *Services personnalisés*, cochez la case **Activé** pour *Services personnalisés* afin d'activer ces services.
 - d. Dans la zone *Informations optionnelles*, cochez au besoin les cases **Activé** pour les options suivantes :
 - **Exporter le mot de passe dans les services personnalisés** : lorsque cette option est sélectionnée, les mots de passe sont envoyés au service personnalisé.
 - **Valider automatiquement les certificats signés provenant du serveur** : pour que cette option soit opérationnelle, le serveur ainsi que le périphérique doivent disposer de certificats. Ces derniers doivent être émis par une autorité de certification considérée comme une autorité de confiance par le périphérique.
 - e. Cliquez sur **Appliquer**.
 - f. Si vous y êtes invité, saisissez votre ID d'administrateur système et votre code d'accès.
Par défaut, ils correspondent respectivement à « **admin** » et « **1111** ».
4. Générez un certificat numérique (le cas échéant). Reportez-vous à [Gestion du certificat numérique de la machine](#), page 7.
5. Activez SSL (le cas échéant). Pour plus d'informations, reportez-vous à [Activation du protocole HTTP sécurisé \(SSL\)](#), page 8.

Sur le périphérique

1. Appuyez sur la touche **Tous services**.
2. Appuyez sur la touche **Services personnalisés**.
3. Appuyez sur la touche **Application EIP** que vous avez enregistrée. Votre flux de travail XEIP devrait être accessible à partir de la nouvelle touche.

Gestion du certificat numérique de la machine

1. Lancez le navigateur, saisissez l'*adresse IP* de la machine dans la barre d'adresse ou le champ Emplacement.
2. Appuyez sur **Entrer** pour accéder aux services Internet du périphérique.
3. Cliquez sur l'onglet **Propriétés**.
4. Si vous y êtes invité, saisissez votre ID d'administrateur système et votre code d'accès. Par défaut, ils correspondent respectivement à « **admin** » et « **1111** ».
5. Cliquez sur **Sécurité**.
6. Cliquez sur le lien **Certificat numérique de la machine** dans l'arborescence.
7. Dans la zone *Certificat numérique de la machine*, cliquez sur le bouton **Créer un nouveau certificat**.
8. Dans la zone *Créer un nouveau certificat*, sélectionnez l'une des options suivantes :
 - **Certificat auto-signé : Établir un certificat auto-signé sur cette machine** : le périphérique accepte son propre certificat comme certificat de confiance en l'auto-signant et crée la clé publique du certificat à utiliser lors du cryptage SSL.
 - **Requête de signature de certificat : Télécharger une requête de signature de certificat à traiter par une autorité de certification** : un certificat provenant d'une autorité de confiance ou d'un serveur faisant office d'autorité de confiance peut être téléchargé vers la machine.
9. Cliquez sur **Continuer**.
10. Saisissez ces informations dans les champs suivants pour la sélection voulue :

Pour <i>Certificat auto-signé</i> :	Pour <i>Requête de signature de certificat</i> :
<ul style="list-style-type: none">• Code pays de 2 lettres• Nom de l'état ou de la province• Nom de la localité• Nom de l'organisation• Unité de l'organisation• Adresse électronique• Jours de validité	<ul style="list-style-type: none">• Code pays de 2 lettres• Nom de l'état ou de la province• Nom de la localité• Nom de l'organisation• Unité de l'organisation• Adresse électronique

11. Cliquez sur **Appliquer**.

12. Si vous avez choisi :

- *Certificat auto-signé* : l'état actuel affiche **Un certificat auto-signé a été établi sur cette machine.**
- *Requête de signature de certificat* : le formulaire de **Demande de signature de certificat (CSR)** s'affiche.
 - a. Si vous avez choisi **Requête de signature de certificat**, cliquez sur le bouton **Enregistrer sous**.
 - b. Dans la boîte de dialogue qui s'affiche, sélectionnez le format **X.509 (.pem)** ou **DER**, puis cliquez sur **Enregistrer**.
 - c. Dans le menu contextuel *Téléchargement de fichier*, cliquez sur **Enregistrer**, sélectionnez l'emplacement sur votre poste de travail, puis cliquez sur **Enregistrer** pour enregistrer le fichier. Une fois le certificat signé par une autorité de certification de confiance, il peut être enregistré sur la machine.
 - d. Revenez à l'écran **Gestion du certificat numérique de la machine** et dans la zone *Certificat numérique de la machine*, cliquez sur le bouton **Télécharger un certificat signé**.
 - e. Cliquez sur **Parcourir**, localisez le fichier sur votre poste de travail, puis cliquez sur **Ouvrir**.
 - f. Cliquez sur **Télécharger le certificat**.

Activation du protocole HTTP sécurisé (SSL)

Remarque : un certificat numérique de machine doit être installé sur le périphérique avant d'activer le protocole HTTP sécurisé (SSL). Pour plus d'informations, reportez-vous à [Gestion du certificat numérique de la machine](#), page 7.

Sur votre poste de travail

1. Lancez le navigateur, saisissez l'*adresse IP* de la machine dans la barre d'adresse ou le champ Emplacement.
2. Appuyez sur **Entrer** pour accéder aux services Internet du périphérique.
3. Cliquez sur l'onglet **Propriétés**.
4. Si vous y êtes invité, saisissez votre ID d'administrateur système et votre code d'accès. Par défaut, ils correspondent respectivement à « **admin** » et « **1111** ».
5. Cliquez sur **Connectivité**, puis sur **Protocoles**.
6. Cliquez sur le lien **HTTP** dans l'arborescence.
7. Dans la zone *Configuration* :
 - a. Pour *Protocole*, cochez la case **Activer** pour activer la communication HTTP avec le périphérique.
 - b. Dans le champ *Numéro de port*, saisissez le numéro du port que le serveur Web du périphérique va utiliser pour les connexions client HTTP. Le numéro de port par défaut est 80.
 - c. Pour le *Mode de sécurité HTTP*, sélectionnez l'une des options suivantes dans le menu déroulant :
 - **Désactiver SSL**
 - **Activer SSL**, afin d'activer Secure Socket Layer (SSL) pour la communication sécurisée (HTTPS).

- **SSL requis**, afin de rendre SSL obligatoire.

Remarque : si le protocole HTTP sécurisé est activé, lors de l'accès aux Services Internet CentreWare, l'adresse URL de toutes les pages Web doit contenir **https://**.

- d. Dans le champ *Délai d'inactivité autorisé*, indiquez le délai pendant lequel le serveur Web attend une réponse HTTP provenant d'un client avant de fermer la session. La valeur par défaut est de 10 secondes.
8. Cliquez sur **Appliquer**.

Serveur Proxy

Un serveur proxy fait office de filtre entre les clients recherchant des services et les serveurs les fournissant. Le serveur proxy filtre les demandes et les accepte si elles se conforment à ses règles de filtrage. La connexion est alors autorisée.

Un serveur proxy a deux objectifs principaux :

- maintenir l'anonymat des périphériques pour des raisons de sécurité ;
- réduire le temps requis pour accéder à une ressource en plaçant le contenu en mémoire cache, par exemple des pages Web.

Sur votre poste de travail

1. Lancez le navigateur, saisissez l'*adresse IP* de la machine dans la barre d'adresse ou le champ Emplacement.
2. Appuyez sur **Entrer** pour accéder aux services Internet du périphérique.
3. Cliquez sur l'onglet **Propriétés**.
4. Si vous y êtes invité, saisissez votre ID d'administrateur système et votre code d'accès. Par défaut, ils correspondent respectivement à « **admin** » et « **1111** ».
5. Cliquez sur **Connectivité**, puis sur **Protocoles**.
6. Cliquez sur le lien **Serveur proxy** dans l'arborescence.
7. Dans la zone *Serveur proxy HTTP* :
 - a. Cochez la case **Détection automatique via WPAD** pour détecter automatiquement les paramètres du proxy au moyen du protocole WPAD. Désélectionnez cette case pour désactiver la détection automatique et utiliser les paramètres de proxy manuels.
 - b. Pour configurer manuellement les paramètres de proxy, cochez la case **Activé** pour *Serveur proxy HTTP*.
 - c. Sélectionnez **Adresse IP** ou **Nom d'hôte**.
 - d. Saisissez l'adresse et le numéro de port au format approprié dans le champ **Adresse IP et port** ou **Nom d'hôte et port**. Le numéro de port par défaut est 8080.
8. Cliquez sur **Appliquer**.

Remarque : les paramètres de serveur proxy sont utilisés pour EIP, Smart eSolutions, la numérisation réseau HTTP(S) et le téléchargement de groupe de modèles HTTP(S).

Remarque : il est possible que la détection automatique des paramètres de proxy remplace les paramètres manuels. Désélectionnez la case Détection automatique via WPAD pour garantir l'utilisation de ces derniers.