Версия 1.0
Януари 2011 г.

Xerox® Phaser™ 3635MFP Платформа за разширяем интерфейс

Периодически този документ претърпява промени. Промените, техническите неточности и печатните грешки ще бъдат коригирани в следващите издания.

Версия на документа 1.0: Януари 2011

Преведено от:

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

Съдържание

Въведение

Платформата за разширяем интерфейс (EIP) на Xerox отваря един нов свят на възможности за Xerox устройствата. С помощта на EIP Вашето Xerox устройство вече може да бъде адаптирано към Вашия начин на работа, а не обратното.

- **Крайните потребители** могат лесно да споделят, съхраняват и отпечатват информация.
- **Специалистите по информационни технологии** могат да добавят стойност и информационна сигурност за клиентите си.
- **Софтуерните разработчици** могат бързо и лесно да разработват приложения, които могат да бъдат настройвани според нуждите към потребителския интерфейс на устройството.

Има няколко опционални софтуерни решения, които могат да бъдат закупени и инсталирани на Вашето устройство. EIP дава възможност да настроите устройството си специфично за Вашия работен процес. Xerox EIP (Платформата за разширяем интерфейс) дава възможност на доставчиците на софтуер и партньорите им да разработват специфични програми, като използват стандартни уеб-базирани инструменти, за да създават приложения, базирани на сървъри, които са достъпни директно от потребителския интерфейс на устройството.

Предимства за крайния потребител от използването на EIP

- **Опростяване** на сложни работни потоци, като същевременно се улеснява използването на устройството.
- **Преобразуване** на документи на хартиен носител в дигитална информация, като по този начин се улеснява редакцията, съхранението и споделянето на информацията.
- **Адаптиране** на устройството към Вашите работни навици, а не обратното.
- **Изпълнение** на някои задачи изцяло от устройството, включително извличане на документи от мрежа без наличието на компютър.
- **Обслужване** на Вашите клиенти по-бързо.
- **Интегриране** на решения във Вашата вече съществуваща ИТ инфраструктура.
- **Управляване** на централизирани решения откъдето и да е по света.
- **Разширяване** и адаптиране на устройството заедно с Вашия бизнес.
- **Създаване** на специализирани решения лесно. EIP е базирана на уеб стандарти, като HTML, CSS, XML и JavaScript. Тя също така използва стандартните защитени протоколи – HTTPS и SSL.

Примери за това, какво може EIP да ви даде възможност да правите

- Използване на менюта и език, който е специфичен за Вашия бизнес или работна група, като например "Търсене в клиентската база данни", "Подаване на формуляр в отдела за искове" или "Изпращане на факс до отдел за изплащане на сметки".
- Всички Ваши персонални настройки могат да бъдат показани на потребителския интерфейс на Вашето устройство само с използването на ИД картата Ви.
- Преобразуване на сложни работни потоци в прости процеси, при които е необходимо само да се натиснат няколко бутона.

- Въвеждане на информация от хартиен носител в хранилище за документи само с натискането на един бутон.
- Изпращане на документ в мрежова опашка за печат и разпечатването му от което и да е устройство в мрежата само с използването на ИД картата Ви.
- Отпечатване на новините за деня или борсовите справки директно от потребителския интерфейс на Xerox устройството.

Опростени процеси

Превърнете сложен работен поток в един прост процес.

Представете си бутон "фактури" на Вашето устройство, който едновременно изпраща фактура в подходящия отдел, архивира информацията в система за управление на документи с цел лесното й намиране и отпечатва копие за Вашия личен архив.

Потребителите могат бързо да сканират и въвеждат хартиени документи, да правят предварителен преглед на умалени изображения, както и да ги добавят в често използвано място за съхранение на документи. Например:

Преподавател може да сканира лекции директно в специално за целта място за съхранение, достъпно за студентите.

Студент може да сканира курсова работа в неговата курсова папка, за да може преподавателят да я оцени.

Платформата за разширяем интерфейс на Xerox използва уеб-базирани решения на Партньори на Xerox, за да даде възможност на потребителите за достъп до хранилища за документи от контролния панел на устройството.

В допълнение към това е **Xerox Secure Access Unified ID System™**, която е предназначена за организации от типа на компании, работещи в здравеопазването, фирми за финансови услуги и образователни институции, които се нуждаят от по-голяма сигурност за поверителните документи. С тази система, комбинираща картови четци и софтуер, потребителите могат да получат достъп до Xerox устройства, след като прокарат ИД картата си през картовия четец на устройството или я раздвижат пред него. За допълнителна сигурност в софтуера може да бъдат вграден ПИН или парола. Системата за защитен достъп може да бъде интегрирана със съществуващата система за ИД карти на служителите на организацията.

Може да има нужда от допълнителни ресурси за устройството в зависимост от решението.

За допълнителна информация се свържете с търговския представител на Xerox.

Персонални решения

EIP улеснява влизането в устройството, като Ви дава възможност да въведете данните си за влизане или да използвате служебната си ИД карта.

Това не само осигурява защитен достъп до устройството, а също така и сега, след като устройството знае кой е потребителят, можете да използвате специфични за Вашите работни потоци опции, което улеснява работа Ви.

Конфигуриране на XEIP

Списък за проверка

Преди започването на инсталационната процедура, моля, погрижете се следните неща да са в наличност или да са изпълнени.

- **Уверете се, че устройството функционира напълно в мрежата**.
- **Погрижете се Вашето EIP решение да бъде инсталирано и да функционира.** Консултирайте се с търговския представител на Xerox за допълнителна информация.
- **Погрижете се Secure HTTP SSL да бъде активиран на устройството**. (Това е по желание) За допълнителна информация вижте Активиране на Secure HTTP (SSL) на страница 9.

  Забележка: Преди да бъде активиран Secure HTTP (SSL), на устройството трябва да бъде инсталиран цифров сертификат на устройство. За допълнителна информация вижте Управление на цифрови сертификати на устройство на страница 7.

Активиране на Custom Services (Услуги, зададени от потребителя)

От работната станция

1. Отворете уеб браузъра и въведете *IP адреса* на устройството в адресната лента или в полето Location (Място).
2. Щракнете **Enter** (Влизане), за да влезете в Internet Services (Интернет услуги) на устройството.
3. За да активирате устройството за EIP приложения:
   a. Щракнете върху раздела **Properties** (Свойства).
   b. Щракнете връзката **Services** (Услуги) и след това **Custom Services** (Услуги, зададени от потребителя).
   c. На страницата *Custom Services* (Услуги, зададени от потребителя) в областта *Enablement* (Активиране), поставете отметка в квадратчето **Enabled** (Активирано) за *Custom Services* (Услуги, зададени от потребителя), за да активирате услугата.
   d. В областта *Optional Information* (Незадължителна информация), ако е необходимо, поставете отметка в квадратчето **Enabled** (Активирано) за следните опции:
      - **Export User Password to Custom Service** (Експортиране на потребителска парола в Услуги, зададени от потребителя) – ако бъде избрано, паролите се изпращат в Custom Service (Услуги, зададени от потребителя).
      - **Automatically validate signed certificates from server** (Автоматично валидиране на подписани сертификати от сървъра) – ако бъде избрана тази опция, за да работи, е необходимо както сървърът, така и устройството да имат сертификати. Тези сертификати трябва да бъдат издадени от орган с установена от устройството надеждност.
   e. Щракнете **Apply** (Прилагане).
   f. Ако се получи подкана, въведете идентификацията и паролата си на системен администратор. Идентификацията и паролата на системния администратор по подразбиране са "**admin**" и "**1111**".

4. Генерирайте цифров сертификат (ако е необходимо). За справка вижте Управление на цифрови сертификати на устройство на страница 7.
5. Активирайте SSL (ако е необходимо). За подробности вижте Активиране на Secure HTTP (SSL) на страница 9.

От устройството

1. Натиснете бутона **All Services** (Всички услуги).
2. Натиснете бутона **Custom Services** (Услуги, зададени от потребителя).
3. Натиснете бутона **EIP Application** (EIP приложение), който регистрирахте. От новия бутон ще имате достъп до Вашия XEIP работен поток.

Управление на цифрови сертификати на устройство

1. Отворете уеб браузъра и въведете *IP адреса* на устройството в адресната лента или в полето Location (Място).
2. Щракнете **Enter** (Влизане), за да влезете в Internet Services (Интернет услуги) на устройството.
3. Щракнете върху раздела **Properties** (Свойства).
4. Ако се получи подкана, въведете идентификацията и паролата си на системен администратор. Идентификацията и паролата на системния администратор по подразбиране са "**admin**" и "**1111**".
5. Щракнете **Security** (Сигурност).
6. Щракнете връзката **Machine Digital Certificate** (Цифров сертификат на устройство) в дървото на директориите.
7. В областта *Machine Digital Certificate* (Цифров сертификат на устройство) щракнете бутона **Create New Certificate** (Създаване на нов сертификат).
8. В областта *Create New Certificate* (Създаване на нов сертификат) изберете една от следните опции:
   - **Self Signed Certificate: Establish a Self Signed Certificate on this machine** (Самоподписан сертификат: Създаване на самоподписан сертификат на това устройство) – устройството подписва собствения си сертификат като надежден и създава публичния ключ на сертификата, който да бъде използван за SSL криптиране.
   - **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** (Заявка за подписване на сертификат: Изтегляне на заявка за подписване на сертификат, която да бъде обработена от надежден сертифициращ орган) – на устройството може да бъде качен сертификат от сертифициращ орган или от сървър, функциониращ като сертифициращ орган.
9. Щракнете **Continue** (Продължаване).

10. Въведете данни в следните полета според направения избор:

За *Self Signed Certificate* (Самоподписан сертификат):	За *Certificate Signing Request* (Заявка за подписване на сертификат):
• **2 Letter Country Code (Двубуквен код на държава)** • **State/Province Name (Име на щат/провинция)** • **Locality Name (Име на населено място)** • **Organization Name (Име на организация)** • **Organization Unit (Отдел в организацията)** • **E-mail Address (Електронен адрес)** • **Days of Validity (Дни на валидност)**	• **2 Letter Country Code (Двубуквен код на държава)** • **State/Province Name (Име на щат/провинция)** • **Locality Name (Име на населено място)** • **Organization Name (Име на организация)** • **Organization Unit (Отдел в организацията)** • **E-mail Address (Електронен адрес)**

11. Щракнете **Apply** (Прилагане).
12. В зависимост от Вашия избор, ако сте избрали:
    - *Self Signed Certificate* (Самоподписан сертификат): настоящият статус показва **A Self Signed Certificate is established on this machine** (Създаден е самоподписан сертификат на това устройство).
    - *Certificate Signing Request* (Заявка за подписване на сертификат): показва се формулярът **Certificate Signing Request (CSR)** (Заявка за подписване на сертификат).

    a. Ако сте избрали **Certificate Signing Request** (Заявка за подписване на сертификат), щракнете бутона **Save As** (Запазване като)

    b. От диалоговия прозорец изберете или **X.509 (.pem)**, или **DER** формат, и щракнете **Save** (Запазване).

    c. В менюто *File Download* (Изтегляне на файл) щракнете **Save** (Запазване), изберете мястото на работната си станция и щракнете **Save** (Запазване), за да запишете файла. След като сертификатът бъде подписан от надежден сертифициращ орган, той е готов да бъде съхранен на устройството.

    d. Върнете се в екрана **Machine Digital Certificate Management** (Управление на цифрови сертификати на устройство) в областта *Machine Digital Certificate* (Цифрови сертификати на устройство) и щракнете бутона **Upload Signed Certificate** (Качване на подписан сертификат).

    e. Щракнете **Browse** (Преглед), намерете файла в работната си станция и щракнете **Open** (Отваряне).

    f. Щракнете **Upload Certificate** (Качване на сертификат).

Активиране на Secure HTTP (SSL)

Забележка: Преди да бъде активиран Secure HTTP (SSL), на устройството трябва да бъде инсталиран цифров сертификат на устройство. За допълнителна информация вижте Управление на цифрови сертификати на устройство на страница 7.

От работната станция

1. Отворете уеб браузъра и въведете *IP адреса* на устройството в адресната лента или в полето Location (Място).
2. Щракнете **Enter** (Влизане), за да влезете в Internet Services (Интернет услуги) на устройството.
3. Щракнете върху раздела **Properties** (Свойства).
4. Ако се получи подкана, въведете идентификацията и паролата си на системен администратор. Идентификацията и паролата на системния администратор по подразбиране са "**admin**" и "**1111**".
5. Щракнете **Connectivity** (Свързаност) и след това **Protocols** (Протоколи).
6. Щракнете **HTTP** връзката в дървото на директориите.
7. В областта *Configuration* (Конфигурация):
   a. За *Protocol* (Протокол) поставете отметка в квадратчето **Enable** (Активиране), за да активирате HTTP комуникациите с устройството.
   b. В полето *Port Number* (Номер на порт) въведете номера на порта, който уеб сървърът на устройството ще използва за HTTP връзка с клиенти. Номерът на порт по подразбиране е 80.
   c. За *HTTP Security Mode* (HTTP режим на сигурност) изберете една от следните опции от падащото меню:
      - **Disable SSL (Деактивиране на SSL)**
      - **Enable SSL** (Активиране на SSL) – за да активирате Secure Socket Layer (SSL) за защитени (HTTPS) комуникации.
      - **Require SSL** (Изискване на SSL) – за да направите Secure Socket Layer (SSL) задължителен.

   Забележка: Ако е активиран защитен HTTP, всички уеб страници за достъп до CentreWare Internet Services ще съдържат **https://** в URL адреса на страницата.

   d. В полето *Keep Alive Timeout* (Време на изчакване преди прекъсване) въведете колко да изчака уеб сървърът за HTTP отговор от клиента, преди да прекрати сесията с него. Стойността по подразбиране е 10 секунди.
8. Щракнете **Apply** (Прилагане).

Прокси сървър

Прокси сървърът действа като филтър за клиенти, търсещи услуги и сървъри, които ги предоставят. Прокси сървърът филтрира заявките и ако те отговарят на правилата на прокси сървъра за филтриране, заявката бива допусната и връзката позволена.

Прокси сървърът има две основни задачи:

- Да поддържа анонимността на устройствата, които са зад него, с оглед на тяхната сигурност.
- Да намали времето необходимо за достъп до ресурсите чрез кеширане на съдържанието им, като например страници от уеб сайт.

От работната станция

1. Отворете уеб браузъра и въведете *IP адреса* на устройството в адресната лента или в полето Location (Място).
2. Щракнете **Enter** (Влизане), за да влезете в Internet Services (Интернет услуги) на устройството.
3. Щракнете върху раздела **Properties** (Свойства).
4. Ако се получи подкана, въведете идентификацията и паролата си на системен администратор. Идентификацията и паролата на системния администратор по подразбиране са "**admin**" и "**1111**".
5. Щракнете **Connectivity** (Свързаност) и след това **Protocols** (Протоколи).
6. Щракнете върху връзката **Proxy Server** (Прокси сървър) в дървото на директориите.
7. В областта *HTTP Proxy Server* (HTTP прокси сървър):
   a. Поставете отметка в квадратчето **Auto Detect Proxy Settings** (Автоматично откриване на прокси настройките), за да бъдат открити автоматично прокси настройките чрез WPAD протокол. Махнете отметката в това квадратче, за да деактивирате автоматичното откриване на прокси настройките и да ги зададете ръчно.
   b. За *HTTP Proxy Server* (HTTP прокси сървър) поставете отметка в квадратчето **Enabled** (Активирано), за да зададете ръчно прокси настройките.
   c. Изберете **IP Address** (IP адрес) или **Hostname** (Име на хост).
   d. Въведете подходящо форматиран адрес и номер на порт в полето **IP Address and Port** (IP адрес и порт) или **Host Name and Port** (Име на хост и порт). Номерът на порт по подразбиране е 8080.
8. Щракнете **Apply** (Прилагане).

   Забележка: Настройките на прокси сървъра се използват за EIP, Smart eSolutions, HTTP(s) Мрежово сканиране и HTTP(s) Изтегляне от съвкупността от шаблони.

   Забележка: Автоматичното откриване на прокси настройките може да отмени ръчно зададените. За да сте сигурни, че ще се използват ръчните настройки, деактивирайте автоматичното откриване на прокси настройки.