

Версія 1.0
Січень 2011 р.



Xerox[®] Phaser[™] 3635MFP Extensible Interface Platform



©2011 Xerox Corporation. XEROX® і XEROX and Design® є товарними знаками корпорації Xerox у США та/або інших країнах.

Цей документ періодично підлягає оновленню. Зміни, технічні неточності та друкарські помилки буде виправлено у подальших виданнях.

Версія документа 1.0: січень 2011 р.

Переклад:

Xerox

CTC European Operations

Bessemer Road

Welwyn Garden City

Hertfordshire

AL7 1BU

UK (Великобританія)

Зміст

Вступ.....	4
Переваги використання платформи EIP для кінцевих користувачів	4
Приклади можливостей, які забезпечує платформа EIP	4
Раціоналізація робочих процесів.....	5
Рішення для індивідуальних можливостей використання пристрою	5
Налаштування платформи XEIP.....	6
Контрольний перелік дій	6
Активація індивідуальних послуг	6
Керування цифровим сертифікатом пристрою	7
Активація протоколу Secure HTTP (SSL)	8
Проксі-сервер	9

Вступ

Платформа Xerox Extensible Interface Platform (EIP) забезпечує кардинально новий спектр можливостей використання пристрою Xerox. Завдяки платформі EIP ви матимете змогу пристосувати пристрій Xerox відповідно до своїх робочих потреб, а не навпаки.

- **Для кінцевих користувачів** - це можливість без зайвих зусиль обмінюватися даними, зберігати їх та друкувати.
- **Для IT-спеціалістів** - це змога розширити можливості роботи та підсилити безпеку інформації своїх клієнтів.
- **Для розробників програмного забезпечення** - це змога оперативно та легко створювати програми з можливістю індивідуального налаштування відповідно до інтерфейсу пристрою.

Ви можете придбати і встановити на свій пристрій кілька додаткових програмних рішень. Платформа EIP дає змогу налаштовувати пристрій відповідно до індивідуальних робочих потреб. Технологія Xerox EIP (Extensible Interface Platform) дозволяє розробникам програм створювати ексклюзивні програми на основі стандартних Інтернет-засобів та серверні додатки з прямим доступом через інтерфейс пристрою.

Переваги використання платформи EIP для кінцевих користувачів

- **Раціоналізація** ускладнених робочих процесів шляхом спрощення способів використання пристрою.
- **Можливість переведення** друкованих документів у цифровий формат для зручності редагування, зберігання та обміну інформацією.
- **Зручність пристосування** пристрою до власних робочих потреб, а не навпаки.
- **Можливість комплексного виконання** завдань на одному пристрої, зокрема, отримання документів у мережі без використання комп'ютера.
- **Оперативність** обслуговування клієнтів.
- **Зручні засоби інтеграції** програмних рішень у наявну IT-інфраструктуру.
- **Централізоване керування** з будь-якої точки світу.
- **Розширення функціональних можливостей** пристрою зі зростанням бізнесу.
- **Можливість зручного створення** програмних рішень під конкретні потреби на основі звичних веб-стандартів: HTML, CSS, XML та JavaScript. Також платформа EIP застосовує стандартні протоколи безпеки – HTTPS та SSL.

Приклади можливостей, які забезпечує платформа EIP

- Можливість використання меню та мови, конкретизованих відповідно до індивідуальних потреб бізнесу чи робочої групи, наприклад, «Пошук у базі даних клієнтів», «Надіслати форму у відділ реклаमाцій» або «Надіслати факс у відділ оплати рахунків».
- Активація особистих налаштувань інтерфейсу системи пристрою завдяки можливості зчитування картки-ідентифікатора.
- Перетворення складного робочого процесу у легке завдання, що передбачає натиснення всього кількох кнопок.
- Введення даних друкованого документа в архів пристрою одним натисненням кнопки.

- Можливість розміщення документа в черзі на друк із будь-якого пристрою мережі, просто провівши карткою-ідентифікатором.
- Запуск друку новин дня чи курсових бюлетенів через інтерфейс пристрою Xerox.

Раціоналізація робочих процесів

Перетворіть кропіткий робочий процес у легке завдання.

Лише уявіть можливість використання на пристрої кнопки «Рахунки», яка одночасно передбачає надсилання рахунку у відповідний відділ, архівацію даних в системі керування документами для зручності подальшого використання і друк копії для вашого особистого зберігання.

Користувачі отримують змогу швидко сканувати документи, переглядати ескізи та зберігати файли у сховищі для часто використовуваних документів. Приклад:

Викладач сканує документи безпосередньо в спеціальний архів певного курсу, забезпечуючи таким чином доступ до них своїм студентам.

Студент сканує реферат у папку певного курсу, подаючи його в такий спосіб на огляд викладачеві.

Платформа Xerox Extensible Interface Platform застосовує веб-рішення Xerox Partner для забезпечення можливості доступу користувачів до сховищ документів через панель керування пристрою.

Крім того, платформа підтримує використання системи **Xerox Secure Access Unified ID System™**, розробленої для медичних установ, фірм, що надають фінансові послуги, та освітніх закладів, конфіденційна інформація яких потребує посиленого захисту. Ця система передбачає використання відповідного програмного забезпечення та пристроїв для зчитування ідентифікаційних карток. Користувачі отримуватимуть доступ до пристрою Xerox, провівши своєю карткою-ідентифікатором або помахавши нею перед пристроєм для зчитування карток. В якості додаткового параметра захисту може використовуватись PIN-код чи пароль, вбудований у програмне забезпечення. Систему безпеки Secure Access можна поєднати із наявною системою ідентифікаційних карток працівників компанії.

Залежно від використовуваного рішення пристрій може вимагати залучення додаткових ресурсів.

Звертайтеся за докладнішими відомостями до торгового представника компанії Xerox.

Рішення для індивідуальних можливостей використання пристрою

Платформа EIP забезпечує зручні можливості входу в систему пристрою шляхом введення особистих облікових даних або зчитування даних із картки-ідентифікатора.

Це гарантує не лише безпеку доступу до пристрою, але й можливості використання індивідуальних параметрів, що відповідають вашим конкретним потребам і таким чином спрощують процес роботи.

Налаштування платформи XEIP

Контрольний перелік дій

Перш ніж почати процедуру встановлення, виконайте перелічені нижче дії.

- **Упевніться, що пристрій функціонує в мережі належним чином.**
- **Перевірте, чи на пристрої встановлено платформу EIP і чи працює вона належним чином.** Докладніші відомості можна отримати у торгового представника компанії Xerox.
- **Перевірте, чи на пристрої активовано протокол Secure HTTP SSL.** (На вибір). Докладніше про це читайте в розділі [Активація протоколу Secure HTTP \(SSL\)](#) на стор. 8.

Примітка: Щоб активувати протокол Secure HTTP (SSL), на пристрої необхідно встановити цифровий сертифікат. Докладніше про це читайте в розділі [Керування цифровим сертифікатом пристрою](#) на стор. 7.

Активація індивідуальних послуг

На робочому комп'ютері

1. Відкрийте веб-браузер, введіть в адресному рядку чи полі розташування *IP-адресу* пристрою.
2. Натисніть **Enter** (Вхід), щоб увійти в меню Інтернет-послуг пристрою.
3. Щоб активувати на пристрої програми EIP:
 - a. Виберіть вкладку **Properties** (Властивості).
 - b. Виберіть пункт **Services** (Послуги), а тоді пункт **Custom Services** (Індивідуальні послуги).
 - c. На сторінці *Custom Services* (Індивідуальні послуги) у розділі *Enablement* (Активація) позначте для параметра *Custom Services* (Індивідуальні послуги) пункт **Enabled** (Активовано), щоб дозволити використання послуг.
 - d. У розділі *Optional Information* (Додаткові відомості), якщо потрібно, позначте пункт **Enabled** (Активовано) для таких параметрів:
 - **Export User Password to Custom Service** (Експортування пароля користувача в систему індивідуальних послуг) - у разі вибору цього параметра паролі надсилатимуться в систему індивідуальних послуг.
 - **Automatically validate signed certificates from server** (Автоматична перевірка підписаних сертифікатів сервера) - для роботи цього параметра необхідно, щоб сервер та пристрій мали сертифікати. Ці сертифікати мають бути видані центром сертифікації, якому довіряє пристрій.
 - e. Натисніть кнопку **Apply** (Застосувати).
 - f. У разі відображення запиту введіть ідентифікатор і пароль системного адміністратора. Стандартний ідентифікатор і пароль системного адміністратора **admin** і **1111** відповідно.
4. Створіть (за потреби) цифровий сертифікат. Дивіться розділ [Керування цифровим сертифікатом пристрою](#) на стор. 7).
5. Активуйте (за потреби) протокол SSL. Дивіться розділ [Активація протоколу Secure HTTP \(SSL\)](#) на стор. 8).

На пристрої

1. Натисніть кнопку **All Services** (Усі послуги).
2. Натисніть кнопку **Custom Services** (Індивідуальні послуги).
3. Натисніть зареєстровану вами кнопку **EIP Application** (Програма EIP). Внаслідок цього з'явиться нова кнопка, що забезпечуватиме доступ до послуг XEIP.

Керування цифровим сертифікатом пристрою

1. Відкрийте веб-браузер, введіть в адресному рядку чи полі розташування *IP-адресу* пристрою.
2. Натисніть **Enter** (Вхід), щоб увійти в меню Інтернет-послуг пристрою.
3. Виберіть вкладку **Properties** (Властивості).
4. У разі відображення запиту введіть ідентифікатор і пароль системного адміністратора. Стандартний ідентифікатор і пароль системного адміністратора **admin** і **1111** відповідно.
5. Натисніть кнопку **Security** (Безпека).
6. Виберіть у дереві каталогів пункт **Machine Digital Certificate** (Цифровий сертифікат пристрою).
7. У розділі *Machine Digital Certificate* (Цифровий сертифікат пристрою) натисніть кнопку **Create New Certificate** (Створити новий сертифікат).
8. У розділі *Create New Certificate* (Створити новий сертифікат) виберіть один із параметрів:
 - **Self Signed Certificate: Establish a Self Signed Certificate on this machine** (Самопідписаний сертифікат: встановити на пристрої самопідписаний сертифікат) - пристрій завіряє власний сертифікат як надійний і створює загальнодоступний ключ для сертифіката, що використовується в кодуванні SSL.
 - **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** (Запит підпису сертифіката: завантажити запит підпису сертифіката для обробки довіреним центром сертифікації) - передбачає завантаження на пристрій сертифіката, виданого центром сертифікації або сервером, що працює як центр сертифікації.
9. Натисніть кнопку **Continue** (Продовжити).
10. У вказаних нижче полях введіть дані відповідно до вибраного параметра.

У разі застосування самопідписаного сертифіката:	У разі застосування запиту підпису сертифіката:
<ul style="list-style-type: none">• Код країни з двох букв• Назва регіону• Назва населеного пункту• Назва організації• Назва підрозділу• Адреса електронної пошти• Термін дії	<ul style="list-style-type: none">• Код країни з двох букв• Назва регіону• Назва населеного пункту• Назва організації• Назва підрозділу• Адреса електронної пошти

11. Натисніть кнопку **Apply** (Застосувати).

12. Якщо вибрано параметр:

- *Self Signed Certificate* (Самопідписаний сертифікат): відображається поточний стан **A Self Signed Certificate is established on this machine** (На пристрої встановлено самопідписаний сертифікат).
- *Certificate Signing Request* (Запит підпису сертифіката): відображається форма **Certificate Signing Request (CSR)** (Запит підпису сертифіката).
- a. Якщо вибрано параметр **Certificate Signing Request** (Запит підпису сертифіката), натисніть кнопку **Save As** (Зберегти як).
- b. У спливному діалоговому вікні виберіть формат **X.509 (.pem)** або **DER** і натисніть кнопку **Save** (Зберегти).
- c. У спливному меню *File Download* (Завантаження файлу) виберіть пункт **Save** (Зберегти), вкажіть місце збереження на комп'ютері і натисніть **Save** (Зберегти), щоб зберегти файл. Після підписання сертифіката довіреним центром сертифікації його можна зберегти на пристрої.
- d. Поверніться до екрана **Machine Digital Certificate Management** (Керування цифровим сертифікатом пристрою) і в розділі *Machine Digital Certificate* (Цифровий сертифікат пристрою) натисніть кнопку **Upload Signed Certificate** (Завантажити підписаний сертифікат).
- e. Натисніть кнопку **Browse** (Огляд), знайдіть збережений на комп'ютері файл і виберіть **Open** (Відкрити).
- f. Натисніть кнопку **Upload Certificate** (Завантажити сертифікат).

Активация протоколу Secure HTTP (SSL)

Примітка: Щоб активувати протокол Secure HTTP (SSL), на пристрої необхідно встановити цифровий сертифікат. Докладніше читайте в розділі [Керування цифровим сертифікатом пристрою](#) на стор. 7.

На робочому комп'ютері

1. Відкрийте веб-браузер, введіть в адресному рядку чи полі розташування *IP-адресу* пристрою.
2. Натисніть **Enter** (Вхід), щоб увійти в меню Інтернет-послуг пристрою.
3. Виберіть вкладку **Properties** (Властивості).
4. У разі відображення запиту введіть ідентифікатор і пароль системного адміністратора. Стандартний ідентифікатор і пароль системного адміністратора **admin** і **1111** відповідно.
5. Натисніть пункт **Connectivity** (З'єднання), а потім - пункт **Protocols** (Протоколи).
6. Виберіть у дереві каталогів пункт **HTTP**.
7. У розділі *Configuration* (Конфігурація):
 - a. Позначте для параметра *Protocol* (Протокол) пункт **Enable** (Активувати), щоб дозволити з'єднання HTTP із пристроєм.
 - b. У полі *Port Number* (Номер порту) введіть номер порту, який використовуватиметься веб-сервером пристрою для клієнтських з'єднань HTTP. Стандартний номер порту - 80.

c. Для параметра *HTTP Security Mode* (Режим безпеки HTTP) у розкритому меню виберіть один із пунктів:

- **Disable SSL (Вимкнути SSL)**
- **Enable SSL (Увімкнути SSL)** - використовується для увімкнення протоколу Secure Socket Layer (SSL) для безпечного з'єднання (HTTPS).
- **Require SSL (Вимагати SSL)** - передбачає обов'язкове використання протоколу Secure Socket Layer (SSL).

Примітка: Якщо активовано протокол Secure HTTP, URL-адреси всіх сторінок, призначених для доступу до програми CentreWare Internet Services, починатимуться з **https://**.

d. У полі *Keep Alive Timeout* (Час очікування) введіть тривалість сеансу, упродовж якого веб-сервер очікуватиме на відповідь HTTP від клієнта. Стандартне значення - 10 секунд.

8. Натисніть кнопку **Apply** (Застосувати).

Проксі-сервер

Проксі-сервер працює в якості фільтра клієнтів, які виконують пошук послуг та серверів, що їх забезпечують. Проксі-сервер фільтрує запити згідно з власними правилами відбору і в разі відповідності дозволяє їх і встановлює з'єднання.

Проксі-сервер має два основні завдання:

- зберігати анонімність пристроїв з метою безпеки;
- скорочувати час, необхідний для доступу до певного ресурсу, наприклад Інтернет-сторінки, завдяки використанню кеш-пам'яті.

На робочому комп'ютері

1. Відкрийте веб-браузер, введіть в адресному рядку чи полі розташування *IP-адресу* пристрою.
2. Натисніть **Enter** (Вхід), щоб увійти в меню Інтернет-послуг пристрою.
3. Виберіть вкладку **Properties** (Властивості).
4. У разі відображення запиту введіть ідентифікатор і пароль системного адміністратора. Стандартний ідентифікатор і пароль системного адміністратора **admin** і **1111** відповідно.
5. Натисніть пункт **Connectivity** (З'єднання), а потім - пункт **Protocols** (Протоколи).
6. Виберіть у дереві каталогів пункт **Proxy Server** (Проксі-сервер).
7. У розділі *HTTP Proxy Server* (Проксі-сервер HTTP):
 - a. позначте пункт **Auto Detect Proxy Settings** (Автоматично визначати параметри проксі), щоб автоматично визначати параметри проксі за допомогою протоколу WPAD; скасуйте позначення цього пункту, щоб вимкнути автоматичне визначення і встановити параметри проксі вручну.
 - b. Позначте для параметра *HTTP Proxy Server* (Проксі-сервер HTTP) пункт **Enabled** (Активовано), щоб встановити параметри проксі вручну.
 - c. Виберіть пункт **IP Address** (IP-адреса) або **Hostname** (Ім'я хосту).
 - d. Введіть адресу і номер порту у відповідному форматі в полі **IP Address and Port** (IP-адреса і порт) або **Host Name and Port** (Ім'я хосту і порт). Стандартний номер порту - 8080.

8. Натисніть кнопку **Apply** (Застосувати).

Примітка: Параметри проксі-сервера використовуються для платформи EIP, програм Smart eSolutions, HTTP(s) Network Scanning та HTTP(s) Template Pool Downloading.

Примітка: Автоматично визначені параметри проксі можуть перезаписувати параметри, встановлені вручну. Вимкніть функцію автоматичного визначення параметрів проксі, щоб гарантувати використання параметрів, встановлених вручну.