Wersja 1.0
Styczeń 2011

Xerox® Phaser™ 3635MFP Extensible Interface Platform

Okresowo w niniejszym dokumencie są wprowadzane modyfikacje. Zmiany, nieścisłości techniczne i błędy typograficzne zostaną poprawione w kolejnych wydaniach.

Wersja dokumentu 1.0: styczeń 2011

Tłumaczenie:

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

Spis treści

Wprowadzenie

Platforma Extensible Interface Platform (EIP) firmy Xerox to całkiem nowe możliwości wykorzystania urządzeń marki Xerox. Dzięki platformie EIP używane urządzenie firmy Xerox można dostosować bezpośrednio do własnego charakteru pracy.

- **Użytkownicy końcowi** mogą w prosty sposób udostępniać, przechowywać i drukować informacje.
- **Informatycy** mogą zapewnić swoim klientom dodatkowe bezpieczeństwo danych.
- **Projektanci** mogą w prosty i szybki sposób tworzyć aplikacje z możliwością dostosowania do interfejsu użytkownika urządzenia.

Dostępne są różne opcjonalne rozwiązania programowe, które można nabyć i zainstalować w urządzeniu. Platforma EIP pozwala na precyzyjne dostosowanie urządzenia do indywidualnych procesów roboczych. Xerox EIP (Extensible Interface Platform) pozwala dostawcom oprogramowania i partnerom na opracowywanie dostosowanych programów przy użyciu narzędzi bazujących na sieci Web w celu tworzenia serwerowych aplikacji dostępnych bezpośrednio z poziomu interfejsu użytkownika urządzenia.

Korzyści dla użytkowników końcowych wykorzystujących EIP

- **Uproszczenie** skomplikowanych procedur roboczych i ułatwienie użytkowania urządzenia.
- **Przetwarzanie** papierowych dokumentów na informacje cyfrowe, ułatwiające edycję, przechowywanie i udostępnianie informacji.
- **Dostosowanie** urządzenia do nawyków w pracy bez potrzeby stosowania kompromisów.
- **Kończenie** niektórych zadań całkowicie w urządzeniu; w tym odbieranie dokumentów w sieci bez użycia komputera.
- **Szybsza obsługa** klientów.
- **Integracja** rozwiązań w istniejącej infrastrukturze IT.
- **Zarządzanie** scentralizowanymi rozwiązaniami z dowolnego miejsca na świecie.
- **Rozszerzanie** i dostosowanie urządzenia wraz z rozwojem firmy.
- **Tworzenie** dostosowanych rozwiązań. Platforma EIP bazuje na standardowych technologiach sieci Web, takich jak HTML, CSS, XML czy JavaScript. Wykorzystuje także standardowe, bezpieczne protokoły — HTTPS i SSL.

Przykładowe możliwości platformy EIP

- Używanie menu i języka stosowanych w danej firmie lub grupie roboczej, np. „Search client database” (Przeszukiwanie bazy danych klientów), „Submit form to claims department” (Wysyłanie formularza do działu skarg) lub „Fax to accounts payable” (Faks do księgowości).
- Wszystkie osobiste preferencje mogą się pojawiać w interfejsie użytkownika systemu urządzenia po zeskanowaniu identyfikatora.
- Przekształcenie złożonego przepływu pracy w prosty proces wymagający użycia zaledwie kilku przycisków.
- Wprowadzanie dokumentów papierowych do repozytoriów dokumentów przez naciśnięcie jednego przycisku.

- Wysyłanie dokumentu do sieciowej kolejki wydruku i drukowanie go z poziomu dowolnego urządzenia w sieci po zeskanowaniu identyfikatora.
- Drukowanie codziennych wiadomości i raportów giełdowych bezpośrednio z poziomu interfejsu użytkownika urządzenia Xerox.

Uproszczone procesy

Przekształcenie złożonego przepływu pracy w prosty proces.

Funkcjonalny przycisk „faktur” na urządzeniu, który jednocześnie wysyła fakturę do odpowiedniego działu, archiwizuje informacje w systemie zarządzania dokumentami, ułatwiając jego odszukiwanie i drukuje kopię dla własnych potrzeb użytkownika.

Użytkownicy mogą szybko skanować i przechwytywać dokumenty papierowe, przeglądać miniatury i dodawać je do lokalizacji zapisu często używanych dokumentów. Na przykład:

Nauczyciel może skanować notatki bezpośrednio do repozytorium określonego kursu i udostępnić je uczestnikom.

Uczestnik może skanować prace zaliczeniowe do swojego folderu kursu i przekazywać je nauczycielowi do oceny.

Xerox Extensible Interface Platform wykorzystuje partnerskie rozwiązania firmy Xerox oparte na sieci Web, aby umożliwić użytkownikom dostęp do repozytoriów dokumentów przy użyciu panelu sterującego urządzenia.

Oprócz tego dostępny jest system **Xerox Secure Access Unified ID System™** przeznaczony dla takich organizacji jak instytucje zdrowotne, firmy usługowo-finansowe i instytucje edukacyjne wymagającego większego poziomu bezpieczeństwa poufnych danych. Dzięki temu systemowi, składającemu się z czytników kart i odpowiedniego oprogramowania, użytkownicy mogą uzyskiwać dostęp do urządzeń Xerox po zeskanowaniu identyfikatora za pomocą czytnika zainstalowanego w urządzeniu. W celu zwiększenia poziomu bezpieczeństwa w oprogramowaniu można zintegrować funkcję ochrony kodem PIN lub hasłem. System Secure Access można zintegrować z istniejącym systemem rejestrowania pracowników stosowanym w organizacji.

W zależności od rozwiązania w urządzeniu mogą być wymagane dodatkowe zasoby.

Aby uzyskać więcej informacji, należy skontaktować się z przedstawicielem handlowym firmy Xerox.

Rozwiązania osobiste

Platforma EIP ułatwia logowanie do urządzenia przez wprowadzenie danych logowania lub zeskanowanie firmowego identyfikatora.

Zapewnia to nie tylko bezpieczny dostęp do urządzenia, lecz także umożliwia identyfikację użytkownika w urządzeniu, co z kolei pozwala na skonfigurowanie opcji dostępu zgodnie z wymogami określonego przepływu pracy, znacznie ułatwiając pracę.

Konfigurowanie platformy XEIP

Lista kontrolna informacji

Przed rozpoczęciem procedury instalacji należy sprawdzić, czy są dostępne lub zostały wykonane następujące pozycje.

- **Sprawdzić, czy urządzenie prawidłowo działa w sieci**.
- **Sprawdzić, czy rozwiązania EIP zostało zainstalowane i działa prawidłowo.** Więcej informacji można uzyskać od przedstawiciela handlowego firmy Xerox.
- **Sprawdzić, czy w urządzeniu jest włączony bezpieczny protokół HTTP SSL**. (Opcjonalnie) Szczegółowe informacje można znaleźć w rozdziale Włączanie bezpiecznego protokołu HTTP (SSL) na stronie 8.

  Uwaga: Przed uaktywnieniem bezpiecznego protokołu HTTP (SSL) w urządzeniu należy zainstalować cyfrowy certyfikat urządzenia. Szczegółowe informacje można znaleźć w rozdziale Zarządzanie cyfrowymi certyfikatami urządzenia na stronie 7.

Włączanie usług użytkownika

W stacji roboczej

1. Otwórz przeglądarkę internetową, wpisz *adres IP* urządzenia w pasku adresu lub w polu Location (Lokalizacja).
2. Kliknij przycisk **Enter** (Przejdź), aby uzyskać dostęp do usług internetowych urządzenia.
3. Aby umożliwić stosowanie aplikacji EIP w urządzeniu:
   a. Kliknij kartę **Properties (Właściwości)**.
   b. Kliknij pozycję **Services** (Usługi), a następnie łącze **Custom Services** (Usługi użytkownika).
   c. Na stronie *Custom Services (Usługi użytkownika)* w obszarze *Enablement* (Włączenie) zaznacz pole wyboru **Enabled (Włączone)** dla opcji *Custom Services*, aby włączyć usługę.
   d. W obszarze *Optional Information* (Informacje opcjonalne), zaznacz w razie potrzeby pola wyboru **Włączone** dla następujących opcji:
      - **Export User Password to Custom Service** (Eksportuj hasło użytkownika do usługi użytkownika) — zaznaczenie tej opcji powoduje przesłanie haseł do usługi użytkownika.
      - **Automatically validate signed certificates from server** (Automatycznie weryfikuj podpisane certyfikaty z serwera) — jeżeli ta opcja zostanie zaznaczona, na serwerze i w urządzenia muszą być obecne certyfikaty. Te certyfikaty muszą zostać wydane przez instytucję zaufaną przez urządzenie.
   e. Kliknij polecenie **Apply** (Zastosuj).
   f. W razie potrzeby wpisz identyfikator administratora systemu i hasło. Domyślny identyfikator administratora systemu to „**admin**”, a domyślne hasło to „**1111**”.
4. Wygeneruj cyfrowy certyfikat (w razie potrzeby), patrz Zarządzanie cyfrowymi certyfikatami urządzenia na stronie 7.
5. Włącz protokół (w razie potrzeby); szczegółowe informacje można znaleźć w rozdziale Włączanie bezpiecznego protokołu HTTP (SSL) na stronie 8.

W urządzeniu

1. Naciśnij przycisk **Wsz. Usługi**.
2. Naciśnij przycisk **Custom Services** (Usługi użytkownika).
3. Naciśnij przycisk zarejestrowanej **aplikacji EIP**. Przepływ pracy XEIP jest teraz dostępny po naciśnięciu nowego przycisku.

Zarządzanie cyfrowymi certyfikatami urządzenia

1. Otwórz przeglądarkę internetową, wpisz *adres IP* urządzenia w pasku adresu lub w polu Location (Lokalizacja).
2. Kliknij przycisk **Enter** (Przejdź), aby uzyskać dostęp do usług internetowych urządzenia.
3. Kliknij kartę **Properties (Właściwości)**.
4. W razie potrzeby wpisz identyfikator administratora systemu i hasło. Domyślny identyfikator administratora systemu to „**admin**”, a domyślne hasło to „**1111**”.
5. Kliknij polecenie **Security** (Bezpieczeństwo).
6. Kliknij łącze **Machine Digital Certificate** (Cyfrowy certyfikat urządzenia) w strukturze drzewa.
7. W obszarze *Machine Digital Certificate* kliknij przycisk **Create New Certificate** (Utwórz nowy certyfikat).
8. W obszarze *Create New Certificate* wybierz jedną z następujących opcji:
   - **Self Signed Certificate: Establish a Self Signed Certificate on this machine** (Certyfikat z podpisem własnym: Utwórz w urządzeniu samodzielnie podpisany certyfikat) — urządzenie zatwierdza własny certyfikat jako zaufany i tworzy publiczny klucz certyfikatu stosowany przy szyfrowaniu SSL.
   - **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** (Żądanie podpisania certyfikatu: Pobierz żądanie podpisania certyfikatu do przetworzenia przez zaufaną instytucję) — możliwość załadowania do urządzenia certyfikatu podpisanego przez zaufaną instytucję lub pochodzący z serwera pełniącego funkcję takiej instytucji.
9. Kliknij polecenie **Continue** (Kontynuuj).
10. Wprowadź szczegółowe informacje w odpowiednich polach wybranej opcji:

W przypadku *certyfikatu z podpisem własnym*:	**W przypadku *żądania podpisania certyfikatu*:**
• **Dwuliterowy kod kraju** • **Nazwa województwa** • **Nazwa miejscowości** • **Nazwa organizacji** • **Jednostka w organizacji** • **Adres e-mail** • **Liczba dni ważności**	• **Dwuliterowy kod kraju** • **Nazwa województwa** • **Nazwa miejscowości** • **Nazwa organizacji** • **Jednostka w organizacji** • **Adres e-mail**

11. Kliknij polecenie **Apply** (Zastosuj).

12. W zależności od wybranej opcji:
    - *Self Signed Certificate* (Certyfikat z podpisem własnym): bieżący status będzie wskazywać **A Self Signed Certificate is established on this machine** (W urządzeniu utworzono certyfikat z podpisem własnym).
    - *Certificate Signing Request* (Żądanie podpisania certyfikatu): zostanie wyświetlony formularz **Certificate Signing Request (CSR)** (Żądanie podpisania certyfikatu — CSR).
    a. Jeżeli została wybrana opcja **Certificate Signing Request** (Żądanie podpisania certyfikatu), kliknij przycisk **Save As** (Zapisz jako).
    b. W podręcznym oknie dialogowym wybierz format **X.509 (.pem)** lub **DER** i kliknij przycisk **Save** (Zapisz).
    c. W menu podręcznym *File Download* (Pobieranie pliku) kliknij przycisk **Save** (Zapisz), wybierz lokalizację w stacji roboczej i kliknij przycisk **Save** (Zapisz), aby zapisać plik. Po podpisaniu certyfikatu przez odpowiednią instytucję można go zapisać w urządzeniu.
    d. Wróć do ekranu **Machine Digital Certificate Management** (Zarządzanie cyfrowymi certyfikatami urządzenia) i w obszarze *Machine Digital Certificate* (Cyfrowy certyfikat urządzenia) kliknij przycisk **Upload Signed Certificate** (Załaduj podpisany certyfikat).
    e. Kliknij przycisk **Browse** (Przeglądaj), zlokalizuj plik w stacji roboczej, a następnie kliknij przycisk **Open** (Otwórz).
    f. Kliknij polecenie **Upload Certificate** (Załaduj certyfikat).

Włączanie bezpiecznego protokołu HTTP (SSL)

Uwaga: Przed uaktywnieniem bezpiecznego protokołu HTTP (SSL) w urządzeniu należy zainstalować cyfrowy certyfikat urządzenia. Szczegółowe informacje można znaleźć w rozdziale Zarządzanie cyfrowymi certyfikatami urządzenia na stronie 7.

W stacji roboczej

1. Otwórz przeglądarkę internetową, wpisz *adres IP* urządzenia w pasku adresu lub w polu Location (Lokalizacja).
2. Kliknij przycisk **Enter** (Przejdź), aby uzyskać dostęp do usług internetowych urządzenia.
3. Kliknij kartę **Properties (Właściwości)**.
4. W razie potrzeby wpisz identyfikator administratora systemu i hasło. Domyślny identyfikator administratora systemu to „**admin**”, a domyślne hasło to „**1111**”.
5. Kliknij pozycję **Connectivity** (Łączność), a następnie **Protocols** (Protokoły).
6. Kliknij łącze **HTTP** w strukturze drzewa.
7. W obszarze *Configuration* (Konfiguracja):
    a. Dla opcji *Protocol* (Protokół) zaznacz pole wyboru **Enable** (Włącz), aby włączyć komunikację z urządzeniem za pośrednictwem protokołu HTTP.
    b. W polu *Port Number* (Numer portu) wpisz numer portu używanego przez serwer sieci Web urządzenia do nawiązywania połączeń z klientem HTTP. Domyślny numer portu to 80.

c. Dla ustawienia *HTTP Security Mode* (Tryb zabezpieczeń HTTP) wybierz jedną z następujących opcji z menu rozwijanego:
   - **Disable SSL (Wyłącz SSL)**
   - **Enable SSL** (Włącz SSL) — uaktywnienie warstwy Secure Socket Layer (SSL) w celu nawiązywania bezpiecznej komunikacji (HTTPS).
   - **Require SSL** (Żądaj SSL) — połączenie z szyfrowaniem SSL będzie wymagane.

   Uwaga: Jeżeli jest włączony bezpieczny protokół HTTP, to w celu uzyskania dostępu do usług CentreWare Internet Services w adresie URL każdej strony będzie się znajdować ciąg znaków **https://**.

d. W polu *Keep Alive Timeout* (Czas utrzymania połączenia) można ustawić, ile czasu serwer sieci Web będzie oczekiwać na odpowiedź HTTP z klienta przed zakończeniem sesji. Domyślne ustawienie to 10 sekund.

8. Kliknij polecenie **Apply** (Zastosuj).

Serwer proxy

Serwer proxy działa jak filtr dla usług wyszukujących klientów i serwerów obsługujących odpowiednią funkcję. Serwer proxy filtruje żądania, a następnie, jeżeli żądania są zgodne z regułami filtrowania serwera, udziela dostępu i umożliwia nawiązanie połączenia.

Serwer proxy ma dwa podstawowe zadania:

- Zapewnianie anonimowości urządzeń ze względów bezpieczeństwa.
- Zmniejszenie czasu wymaganego na uzyskanie dostępu do zasobu przez zapisywanie treści w pamięci podręcznej (np. stron sieci Web).

W stacji roboczej

1. Otwórz przeglądarkę internetową, wpisz *adres IP* urządzenia w pasku adresu lub w polu Location (Lokalizacja).
2. Kliknij przycisk **Enter** (Przejdź), aby uzyskać dostęp do usług internetowych urządzenia.
3. Kliknij kartę **Properties (Właściwości)**.
4. W razie potrzeby wpisz identyfikator administratora systemu i hasło. Domyślny identyfikator administratora systemu to „**admin**”, a domyślne hasło to „**1111**”.
5. Kliknij pozycję **Connectivity** (Łączność), a następnie **Protocols** (Protokoły).
6. Kliknij łącze **Proxy Server** (Serwer proxy) w strukturze drzewa.
7. W obszarze *HTTP Proxy Server* (Serwer proxy HTTP):
   a. Zaznacz pole wyboru **Auto Detect Proxy Settings** (Wykryj ustawienia serwera proxy automatycznie), aby automatycznie wykryć ustawienia proxy przy użyciu protokołu WPAD. Usuń zaznaczenie tego pola, aby wyłączyć automatyczne wykrywanie proxy i ręcznie wprowadzić odpowiednie ustawienia.
   b. Przy opcji *HTTP Proxy Server* (Serwer proxy HTTP) zaznacz pole wyboru **Enabled** (Włączony), aby ręcznie wprowadzić ustawienia proxy.
   c. Wybierz pole **IP Address** (Adres IP) lub **Hostname** (Nazwa hosta).
   d. Wpisz adres i numer portu w odpowiednim formacie w polu **IP Address and Port** (Adres IP i port) lub **Host Name and Port** (Nazwa hosta i port); domyślny numer portu to 8080.

8. Kliknij polecenie **Apply** (Zastosuj).

   Uwaga: Ustawienia serwera proxy są stosowane przez usługi EIP, Smart eSolutions, HTTP(s) Network Scanning (Skanowanie sieciowe HTTP(s)) oraz HTTP(s) Template Pool Downloading (Pobieranie puli szablonów HTTP(s)).

   Uwaga: Automatyczne wykrywanie ustawień proxy może spowodować zastąpienie ustawień ręcznych. Wyłączy funkcję automatycznego wykrywania ustawień serwera proxy, aby użyć ustawień ręcznych.