Verze 1.0
Leden 2011

Xerox® Phaser™ 3635MFP Extensible Interface Platform

V tomto dokumentu jsou pravidelně prováděny změny. Změny, technické nepřesnosti a typografické chyby budou opraveny v pozdějších vydáních.

Verze dokumentu 1.0: leden 2011

Překlad:

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

Obsah

Úvod

Platforma Xerox Extensible Interface Platform (EIP) poskytuje zařízení Xerox zcela nové možnosti. Díky této platformě se nyní vaše zařízení Xerox dokáže přizpůsobit vašemu způsobu práce místo toho, abyste se přizpůsobovali vy.

- **Koncoví uživatelé** mohou snadno sdílet, ukládat a tisknout informace.
- **Pracovníci IT** mohou poskytovat svým klientům přidanou hodnotu a zvyšovat zabezpečení informací.
- **Vývojáři** mohou snadno a rychle vytvářet aplikace, které lze přizpůsobit uživatelskému rozhraní zařízení.

Existuje několik volitelných softwarových řešení, která lze zakoupit a nainstalovat do zařízení. Pomocí platformy EIP lze zařízení přizpůsobit vašim specifickým pracovním postupům. Na základě platformy Xerox EIP (Extensible Interface Platform) mohou výrobci softwaru a partneři vyvíjet programy na míru pomocí standardních webových nástrojů a vytvářet serverové aplikace, ke kterým lze přistupovat přímo z uživatelského rozhraní zařízení.

Výhody používání platformy EIP pro koncového uživatele

- **Zjednodušení** složitých pracovních postupů a zároveň snadnější používání zařízení
- **Převod** tištěných dokumentů na digitální informace, což usnadňuje úpravy, ukládání a sdílení informací.
- **Přizpůsobení** zařízení vašim pracovním návykům místo toho, abyste se přizpůsobovali vy.
- **Provádění** některých úloh přímo na zařízení, včetně načítání dokumentů ze sítě bez použití počítače.
- Rychlejší **obsluha** zákazníků.
- **Integrace** řešení do vaší stávající infrastruktury IT.
- **Správa** centralizovaných řešení z kteréhokoli místa na světě.
- **Rozšiřování** a přizpůsobování zařízení společně s rozvojem vašeho podnikání.
- Snadné **vytváření** řešení na míru — platforma EIP je založena na webových standardech, jako je HTML, CSS, XML a JavaScript. Používá také standardní zabezpečené protokoly HTTPS a SSL.

Příklady možností, které platforma EIP nabízí

- Používejte nabídky a fráze, které jsou specifické pro vaši obchodní činnost nebo pracovní skupinu, například Hledat v databázi klientů, Odeslat formulář na oddělení reklamací nebo Odfaxovat do účtárny.
- Po protažení vaší identifikační karty se na uživatelském rozhraní zařízení mohou zobrazit všechny vaše uživatelské předvolby.
- Proměňte složitý pracovní postup na jednoduchý proces, který lze dokončit stisknutím několika málo tlačítek.
- Pouhým stisknutím tlačítka uložte informace z tištěného dokumentu do úložiště dokumentů.
- Odešlete dokument do sí"ové tiskové fronty a po protažení své identifikační karty jej vytiskněte na kterémkoli zařízení v síti.

- Tiskněte aktuální přehledy zpráv nebo finanční přehledy přímo z uživatelského rozhraní zařízení Xerox.

Zjednodušené procesy

Proměňte složitý pracovní postup na jednoduchý proces.

Představte si na vašem zařízení tlačítko Faktury, které současně odešle fakturu do příslušného oddělení, uloží informace do archivu v systému pro správu dokumentů, odkud je lze později snadno načíst, a vytiskne kopii pro vaše osobní záznamy.

Uživatelé mohou rychle naskenovat a digitalizovat papírové dokumenty, zobrazit náhledy a uložit dokumenty do úložiště často používaných dokumentů. Příklad:

Vyučující může naskenovat poznámky přímo do úložiště daného kurzu a tím je zpřístupnit studentům.

Student může naskenovat svou práci do složky kurzu, aby ji mohl vyučující oznámkovat.

Platforma EIP využívá webová řešení partnerů společnosti Xerox a umožňuje uživatelům přistupovat k úložištím dokumentů z ovládacího panelu přístroje.

Kromě těchto řešení existuje systém **Xerox Secure Access Unified ID System™**. Tento systém je navržený pro organizace, jako jsou společnosti z oblasti zdravotnictví, firmy poskytující finanční služby a vzdělávací instituce, které požadují vyšší zabezpečení svých citlivých záznamů. S tímto systémem, který kombinuje čtečky karet a software, mohou uživatelé přistupovat k zařízením Xerox protažením své identifikační karty nebo jejím přiložením ke čtečce na zařízení. Zabezpečení lze dále zvýšit přidáním kódu PIN nebo hesla do softwaru. Systém Secure Access je možné integrovat se stávajícím systémem identifikačních karet zaměstnanců v organizaci.

V závislosti na řešení mohou být na zařízení vyžadovány další prostředky.

Další informace vám poskytne obchodní zástupce společnosti Xerox.

Osobní řešení

Platforma EIP umožňuje snadné přihlášení k zařízení zadáním přihlašovacích údajů nebo protažením identifikační karty vaší společnosti.

Nejenže tak získáte zabezpečený přístup k zařízení, ale díky tomu, že zařízení zná vaši identitu, máte přístup k možnostem specifickým pro vaše úkoly, což vám usnadní práci.

Konfigurace platformy XEIP

Kontrolní seznam informací

Před zahájením instalace zkontrolujte, zda jsou splněny následující předpoklady.

- **Zkontrolujte, zda je zařízení plně funkční v síti**.
- **Zkontrolujte, zda je řešení EIP nainstalované a funkční.** Další informace vám poskytne obchodní zástupce společnosti Xerox.
- **Zkontrolujte, zda je na zařízení povolený protokol Secure HTTP (SSL)**. (Tento krok je volitelný.) Podrobnosti najdete v části Povolení protokolu Secure HTTP (SSL) na straně 8.

  Poznámka: Dříve než bude možné povolit protokol Secure HTTP (SSL), musí být na zařízení nainstalovaný digitální certifikát přístroje. Podrobnosti najdete v části Správa digitálních certifikátů přístroje na straně 7.

Povolení uživatelských služeb

Na pracovní stanici

1. Spus"te webový prohlížeč a do panelu Adresa nebo do pole Umístění zadejte *adresu IP* přístroje.
2. Stisknutím klávesy **Enter** přejděte k Internetovým službám zařízení.
3. Povolení aplikací EIP v zařízení:
   a. Klepněte na kartu **Properties** (Vlastnosti).
   b. Klepněte na možnost **Services** (Služby) a potom na odkaz **Custom Services** (Uživatelské služby).
   c. Na stránce *Custom Services* (Uživatelské služby) v oblasti *Enablement* (Povolení) povolte služby zaškrtnutím políčka *Enabled* (Povoleno) u možnosti **Custom Services** (Uživatelské služby).
   d. V případě potřeby zaškrtněte v oblasti *Optional Information* (Volitelné informace) políčka **Enabled** (Povoleno) u následujících možností:
      - **Export User Password to Custom Service** (Exportovat uživatelské heslo do uživatelské služby) — je-li tato možnost vybrána, budou hesla odesílána do uživatelské služby.
      - **Automatically validate signed certificates from server** (Automaticky ověřovat podepsané certifikáty ze serveru) — je-li tato možnost vybrána, musí být na serveru i na zařízení uloženy certifikáty. Tyto certifikáty musí být vystaveny autoritou, které zařízení důvěřuje.
   e. Klepněte na tlačítko **Apply** (Použít).
   f. Pokud se zobrazí výzva, zadejte ID a heslo správce systému. Výchozí ID a heslo správce systému je **admin** a **1111**.
4. V případě potřeby vygenerujte digitální certifikát podle pokynů v části Správa digitálních certifikátů přístroje na straně 7.
5. V případě potřeby povolte protokol SSL. Podrobnosti najdete v části Povolení protokolu Secure HTTP (SSL) na straně 8.

Na zařízení

1. Stiskněte tlačítko **Všechny služby**.
2. Stiskněte tlačítko **Custom Services** (Uživatelské služby).
3. Stiskněte tlačítko **aplikace EIP**, kterou jste zaregistrovali. Pomocí tohoto nového tlačítka byste měli mít přístup k vašemu pracovnímu postupu XEIP.

Správa digitálních certifikátů přístroje

1. Spus"te webový prohlížeč a do panelu Adresa nebo do pole Umístění zadejte *adresu IP* přístroje.
2. Stisknutím klávesy **Enter** přejděte k Internetovým službám zařízení.
3. Klepněte na kartu **Properties** (Vlastnosti).
4. Pokud se zobrazí výzva, zadejte ID a heslo správce systému. Výchozí ID a heslo správce systému je **admin** a **1111**.
5. Klepněte na možnost **Security** (Zabezpečení).
6. V adresářovém stromě klepněte na odkaz **Machine Digital Certificate** (Digitální certifikát přístroje).
7. V oblasti *Machine Digital Certificate* (Digitální certifikát přístroje) klepněte na tlačítko **Create New Certificate** (Vytvořit nový certifikát).
8. V oblasti *Create New Certificate* (Vytvořit nový certifikát) vyberte jednu z následujících možností:
   - **Self Signed Certificate: Establish a Self Signed Certificate on this machine** (Certifikát podepsaný držitelem: Zřídit na tomto přístroji certifikát podepsaný držitelem) — zařízení podepíše svůj vlastní certifikát jako důvěryhodný a vytvoří veřejný klíč, aby bylo možné tento certifikát používat při šifrování SSL.
   - **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** (Požadavek na podepsání certifikátu: Stáhnout požadavek na podepsání certifikátu, který zpracuje důvěryhodná certifikační autorita) — na přístroj lze uložit certifikát od certifikační autority nebo ze serveru, který funguje jako certifikační autorita.
9. Klepněte na tlačítko **Continue** (Pokračovat).
10. Zadejte podrobnosti do následujících polí podle požadovaného výběru:

Self Signed Certificate **(Certifikát podepsaný držitelem):**	***Certificate Signing Request*** **(Požadavek na podepsání certifikátu):**
• **2 Letter Country Code (2místný kód země)** • **State/Province Name (Název státu nebo provincie)** • **Locality Name (Název místa)** • **Organization Name (Název organizace)** • **Organization Unit (Organizační jednotka)** • **E-mail Address (E-mailová adresa)** • **Days of Validity (Dny platnosti)**	• **2 Letter Country Code (2místný kód země)** • **State/Province Name (Název státu nebo provincie)** • **Locality Name (Název místa)** • **Organization Name (Název organizace)** • **Organization Unit (Organizační jednotka)** • **E-mail Address (E-mailová adresa)**

11. Klepněte na tlačítko **Apply** (Použít).
12. V závislosti na vybrané možnosti:
    - *Self Signed Certificate* (Certifikát podepsaný držitelem): V poli Current Status (Aktuální stav) se zobrazí zpráva **A Self Signed Certificate is established on this machine** (Na tomto přístroji je zřízen certifikát podepsaný držitelem).
    - *Certificate Signing Request* (Požadavek na podepsání certifikátu): Zobrazí se formulář **Certificate Signing Request (CSR)** (Požadavek na podepsání certifikátu (CSR)).

    a. Pokud jste vybrali možnost **Certificate Signing Request** (Požadavek na podepsání certifikátu), klepněte na tlačítko **Save As** (Uložit jako).

    b. V místním dialogovém okně vyberte formát **X.509 (.pem)** nebo **DER** a klepněte na tlačítko **Save** (Uložit).

    c. V místní nabídce *File Download* (Stažení souboru) klepněte na tlačítko **Save** (Uložit), vyberte umístění na pracovní stanici a klepnutím na tlačítko **Save** (Uložit) soubor uložte. Jakmile bude certifikát podepsán důvěryhodnou certifikační autoritou, bude jej možné uložit do přístroje.

    d. Vra″te se na obrazovku **Machine Digital Certificate Management** (Správa digitálních certifikátů přístroje) a v oblasti *Machine Digital Certificate* (Digitální certifikát přístroje) klepněte na tlačítko **Upload Signed Certificate** (Odeslat podepsaný certifikát).

    e. Klepněte na tlačítko **Browse** (Procházet), vyhledejte soubor na pracovní stanici a klepněte na tlačítko **Open** (Otevřít).

    f. Klepněte na tlačítko **Upload Certificate** (Odeslat certifikát).

Povolení protokolu Secure HTTP (SSL)

Poznámka: Dříve než bude možné povolit protokol Secure HTTP (SSL), musí být na zařízení nainstalovaný digitální certifikát přístroje. Podrobnosti najdete v části Správa digitálních certifikátů přístroje na straně 7.

Na pracovní stanici

1. Spus″te webový prohlížeč a do panelu Adresa nebo do pole Umístění zadejte *adresu IP* přístroje.
2. Stisknutím klávesy **Enter** přejděte k Internetovým službám zařízení.
3. Klepněte na kartu **Properties** (Vlastnosti).
4. Pokud se zobrazí výzva, zadejte ID a heslo správce systému. Výchozí ID a heslo správce systému je **admin** a **1111**.
5. Klepněte na možnost **Connectivity** (Připojení) a potom na možnost **Protocols** (Protokoly).
6. V adresářovém stromu klepněte na odkaz **HTTP**.
7. V oblasti *Configuration* (Konfigurace):

    a. V části *Protocol* (Protokol) zaškrtnutím políčka **Enable** (Povolit) povolte komunikaci HTTP se zařízením.

    b. Do pole *Port Number* (Číslo portu) zadejte číslo portu, které bude používat webový server zařízení pro klientská připojení HTTP. Výchozí číslo portu je 80.

    c. V rozevírací nabídce *HTTP Security Mode* (Režim zabezpečení HTTP) vyberte jednu z následujících možností:
        - **Disable SSL (Zakázat protokol SSL)**

- **Enable SSL** (Povolit protokol SSL) — povolení protokolu SSL (Secure Socket Layer) pro zabezpečenou komunikaci (HTTPS).
- **Require SSL** (Požadovat protokol SSL) — nastavení protokolu SSL (Secure Socket Layer) jako povinného.

Poznámka: Pokud je povolen protokol Secure HTTP, při přístupu k Internetovým službám CentreWare bude adresa URL všech webových stránek obsahovat údaj **https://**.

d. Do pole *Keep Alive Timeout* (Časová prodleva Keep Alive) zadejte, jak dlouho bude webový server čekat na odpověď HTTP od klienta, než ukončí relaci. Výchozí hodnota je 10 sekund.

8. Klepněte na tlačítko **Apply** (Použít).

Proxy server

Proxy server funguje jako filtr mezi klienty, kteří hledají služby, a servery, které tyto služby poskytují. Proxy server filtruje požadavky. Pokud požadavek odpovídá pravidlům pro filtrování, bude schválen a proxy server umožní připojení.

Proxy server plní dva hlavní účely:

- uchovávat zařízení za proxy serverem anonymní z důvodů zabezpečení;
- zkracovat dobu potřebnou pro přístup ke zdroji uchováváním obsahu, například webových stránek z webu, v mezipaměti.

Na pracovní stanici

1. Spus"te webový prohlížeč a do panelu Adresa nebo do pole Umístění zadejte *adresu IP* přístroje.
2. Stisknutím klávesy **Enter** přejděte k Internetovým službám zařízení.
3. Klepněte na kartu **Properties** (Vlastnosti).
4. Pokud se zobrazí výzva, zadejte ID a heslo správce systému. Výchozí ID a heslo správce systému je **admin** a **1111**.
5. Klepněte na možnost **Connectivity** (Připojení) a potom na možnost **Protocols** (Protokoly).
6. V adresářovém stromě klepněte na odkaz **Proxy Server**.
7. V oblasti *HTTP Proxy Server* (Proxy server HTTP):
   a. Zaškrtněte políčko **Auto Detect Proxy Settings** (Automatické zjištění nastavení proxy), pokud chcete automaticky zjiš"ovat nastavení proxy pomocí protokolu WPAD. Zrušením zaškrtnutí tohoto políčka zakážete automatické zjiš"ování proxy a použijete ruční nastavení proxy.
   b. V části *HTTP Proxy Server* (Proxy server HTTP) zaškrtněte políčko **Enabled** (Povolen), abyste mohli ručně zadat nastavení proxy.
   c. Vyberte možnost **IP Address** (Adresa IP) nebo **Hostname** (Název hostitele).
   d. Do polí **IP Address and Port** (Adresa IP a port) nebo **Host Name and Port** (Název hostitele a port) zadejte adresu v příslušném formátu a port. Výchozí číslo portu je 8080.

8. Klepněte na tlačítko **Apply** (Použít).

   Poznámka: Nastavení proxy serveru využívají služby EIP, Smart eSolutions, Snímání v síti HTTP(s) a Stahování z fondu šablon HTTP(s).

   Poznámka: Automatické zjiš"ování nastavení proxy může přepsat ruční nastavení. Chcete-li zajistit použití ručního nastavení, zakažte možnost Auto Detect Proxy Settings (Automatické zjištění nastavení proxy).