Versione 1.0
gennaio 2011

Xerox® Phaser™ 3635MFP Extensible Interface Platform

Versione del documento 1.0: gennaio 2011

Traduzione:

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

Sommario

Introduzione

La tecnologia Xerox EIP (Extensible Interface Platform) apre un universo di nuove possibilità al dispositivo Xerox. Con EIP, sarà il vostro dispositivo Xerox ad adattarsi al vostro modo di lavorare, anziché viceversa.

- **Gli utenti finali** possono condividere, archiviare e stampare informazioni più agevolmente
- **I responsabili IT** possono aggiungere valore e sicurezza delle informazioni ai propri clienti
- **Gli sviluppatori** possono creare facilmente e rapidamente applicazioni personalizzabili per l'interfaccia utente del dispositivo

Esistono varie soluzioni software opzionali che possono essere acquistate e installate nel dispositivo. Con EIP potete personalizzare il dispositivo specificatamente per i vostri processi di flusso di lavoro. Xerox EIP (Extensible Interface Platform) consente ai fornitori di software e ai partner di sviluppare programmi personalizzati utilizzando strumenti per il web standard per creare applicazioni per web a cui è possibile accedere direttamente dall'interfaccia utente del dispositivo.

Vantaggi per l'utente finale che utilizza la tecnologia EIP

- **Semplifica** flussi di lavoro complessi facilitando al contempo l'utilizzo del dispositivo.
- **Trasforma** documenti cartacei in file digitali, facilitando la modifica, l'archiviazione e la condivisione delle informazioni.
- **Adatta** il dispositivo alle vostre abitudini di lavoro… anziché il contrario.
- **Completa** alcune attività interamente presso il dispositivo; ad esempio, recuperare documenti su una rete senza bisogno di un PC.
- **Assistenza** più rapida ai vostri clienti.
- **Integrazione** di soluzioni nella vostra infrastruttura IT esistente.
- **Gestione** di soluzioni centralizzate da qualunque parte del mondo.
- **Espansione** e adattamento del dispositivo alle vostre esigenze aziendali.
- **Creazione** semplice di soluzioni personalizzate. La tecnologia EIP è basata su standard web quali HTML, CSS, XML e JavaScript. Utilizza inoltre protocolli sicuri standard: HTTPS e SSL.

Esempi di cosa consente di fare la tecnologia EIP

- Usare menu e linguaggi specifici del vostro business o gruppo di lavoro, come "Cerca database clienti", "Invia modulo al reparto reclami", o "Invia per fax a conto creditori diversi".
- Possibilità di visualizzare tutte le vostre preferenze personali sull'interfaccia utente del vostro dispositivo semplicemente strisciando il vostro tesserino di identificazione.
- Trasformare un flusso di lavoro complesso in un processo semplice che richiede di premere soltanto pochi tasti.
- Immettere informazioni cartacee in un archivio documenti semplicemente premendo un pulsante.
- Inviare un documento a una coda di stampa in rete e stamparlo da qualunque dispositivo sulla rete semplicemente strisciando il vostro tesserino di identificazione.
- Stampare i comunicati del giorno o i report sui titoli azionari direttamente dall'interfaccia utente del dispositivo Xerox.

Processi semplificati

Trasformare un flusso di lavoro complesso in un processo semplice.

Immaginate sul vostro dispositivo un pulsante "fatture" con cui è possibile inviare contemporaneamente una fattura al reparto corretto, archiviare le informazioni in un sistema di gestione documenti per facilitarne il recupero e stampare una copia per le registrazioni personali.

Gli utenti possono scansire e acquisire rapidamente i documenti cartacei, visualizzare anteprime e aggiungerli alle aree documenti utilizzate di frequente. Ad esempio:

Un tutor può scansire note direttamente in un archivio corsi specifico a cui possono accedere gli studenti.

Uno studente può scansire documenti di valutazione nella propria cartella dei corsi per consentire al tutor di esprimere il voto.

Xerox Extensible Interface Platform utilizza soluzioni per il web di Partner Xerox per consentire agli utenti di accedere agli archivi documento sul pannello comandi della macchina.

Inoltre, è disponibile il **Sistema ID unico per Xerox Secure Access™**, concepito per organizzazioni quali aziende sanitarie, imprese di servizi finanziari e istituti di istruzione che desiderano maggiore protezione per le loro registrazioni importanti. Grazie a questo sistema, con cui è possibile associare lettori di schede e software, gli utenti possono accedere ai dispositivi Xerox dopo aver semplicemente strisciato o passato il tesserino di identificazione davanti al lettore di schede sul dispositivo. Per una maggiore sicurezza, è possibile creare un PIN o una parola di accesso nel software. Il sistema Secure Access può integrarsi con un sistema ID esistente con tesserino dei dipendenti dell'organizzazione.

È possibile che sul dispositivo siano richieste risorse aggiuntive a seconda della soluzione.

Per ulteriori informazioni, contattare il rappresentante del servizio vendite Xerox.

Soluzioni personali

EIP semplifica l'accesso al dispositivo mediante l'immissione dei dettagli di connessione o il passaggio del tesserino di identificazione dell'azienda.

Questo metodo non solo garantisce un accesso sicuro al dispositivo, ma dal momento in cui si è riconosciuti dal dispositivo, consente anche di accedere a opzioni specifiche per i propri flussi di lavoro facilitando le operazioni.

Configurazione di XEIP

Elenco di controllo delle informazioni

Prima di avviare la procedura di installazione, controllare che i seguenti elementi siano disponibili o di aver eseguito le seguenti operazioni.

- **Accertarsi che il dispositivo sia completamente funzionante in rete**.
- **Accertarsi che la soluzione EIP sia installata e funzionante.** Per ulteriori informazioni, rivolgersi al proprio rappresentante del servizio vendite Xerox.
- **Accertarsi che HTTP SSL protetto sia abilitato nel dispositivo**. (Questa impostazione è opzionale) Per informazioni dettagliate, fare riferimento a Abilitazione di HTTP (SSL) protetto a pagina 8.

  Nota: prima di poter abilitare HTTP (SSL) protetto, è necessario che un certificato digitale del sistema sia installato nel dispositivo. Per informazioni dettagliate, fare riferimento a Gestione certificato digitale del sistema a pagina 7.

Abilita servizi personalizzati

Nella workstation

1. Aprire il browser Web, inserire l'*indirizzo IP* della macchina nella barra dell'indirizzo o nel campo Posizione.
2. Fare clic su **Invio** per accedere ai Servizi Internet del dispositivo.
3. Per abilitare il dispositivo alle applicazioni EIP:
   a. Fare clic sulla scheda **Proprietà**.
   b. Fare clic su **Servizi**, quindi sul collegamento **Servizi personalizzati**.
   c. Nella pagina *Servizi personalizzati*, all'interno della sezione *Abilitazione*, per *Servizi personalizzati* selezionare la casella di controllo **Abilitato** per abilitare il servizio.
   d. Nella sezione *Informazioni opzionali*, se richiesto, selezionare le caselle di controllo **Abilitato** per le seguenti opzioni:
      - **Esporta la parola di accesso dell'utente in Servizio personalizzato** - se selezionata, le parole di accesso vengono inviate al servizio personalizzato.
      - **Convalida automaticamente i certificati firmati dal server** - se selezionata, affinché questa opzione funzioni, il server e il dispositivo richiedono certificati. Questi certificati devono essere emessi da un'autorità considerata attendibile dal dispositivo.
   e. Fare clic su **Applica**.
   f. Se richiesto, inserire il codice di accesso e l'ID dell'amministratore del sistema. Il codice di accesso e l'ID dell'amministratore del sistema predefiniti sono rispettivamente "**1111**" e "**admin**".
4. Generare un certificato digitale (se necessario), fare riferimento a Gestione certificato digitale del sistema a pagina 7.
5. Abilitare SSL (se richiesto); per informazioni dettagliate, fare riferimento a Abilitazione di HTTP (SSL) protetto a pagina 8.

Nel dispositivo

1. Premere il pulsante **Tutti i servizi**.
2. Toccare il pulsante **Servizi personalizzati**.
3. Toccare il pulsante **Applicazione EIP** registrato. Il flusso di lavoro XEIP deve essere accessibile dal nuovo pulsante.

Gestione certificato digitale del sistema

1. Aprire il browser Web, inserire l'*indirizzo IP* della macchina nella barra dell'indirizzo o nel campo Posizione.
2. Fare clic su **Invio** per accedere ai Servizi Internet del dispositivo.
3. Fare clic sulla scheda **Proprietà**.
4. Se richiesto, inserire il codice di accesso e l'ID dell'amministratore del sistema. Il codice di accesso e l'ID dell'amministratore del sistema predefiniti sono rispettivamente "**1111**" e "**admin**".
5. Fare clic su **Sicurezza**.
6. Fare clic sul collegamento **Certificato digitale del sistema** nell'albero di directory.
7. Nella sezione *Certificato digitale del sistema*, fare clic sul pulsante **Crea nuovo certificato**.
8. Nella sezione *Crea nuovo certificato*, selezionare una delle seguenti opzioni:
   - **Certificato autofirmato: Definire un certificato digitale autofirmato per questo sistema** - il dispositivo firma il proprio certificato come attendibile e crea la chiave pubblica che consente di utilizzare il certificato nella crittografia SSL.
   - **Richiesta di firma certificato: Scaricare una richiesta di firma certificato da elaborare tramite un'autorità di certificazione attendibile** - è possibile caricare nella macchina un certificato da una autorità certificata o da un server che funge da autorità di certificazione.
9. Fare clic su **Continua**.
10. Inserire i dettagli nei campi seguenti per la selezione richiesta:

Per *Certificato autofirmato*:	Per *Richiesta di firma certificato*:
• **Codice paese a 2 lettere** • **Stato/Provincia** • **Nome località** • **Nome organizzazione** • **Unità organizzazione** • **Indirizzo e-mail** • **Giorni di validità**	• **Codice paese a 2 lettere** • **Stato/Provincia** • **Nome località** • **Nome organizzazione** • **Unità organizzazione** • **Indirizzo e-mail**

11. Fare clic su **Applica**.
12. In base alla scelta effettuata, se è stato selezionato:
    - *Certificato autofirmato*: come stato corrente viene visualizzato **Per questo sistema è stato definito un certificato digitale autofirmato**.
    - *Richiesta di firma certificato*: viene visualizzato il modulo **Richiesta di firma del certificato**.

    a. Se è stato selezionato **Richiesta di firma certificato**, fare clic sul pulsante **Salva con nome**

    b. Dalla finestra di dialogo a comparsa, selezionare il formato **X.509 (.pem)** o **DER**, fare clic su **Salva**.

c. Dal menu a comparsa *Download del file*, fare clic su **Salva**, selezionare la posizione nella workstation e fare clic su **Salva** per salvare il file. Una volta che il certificato è firmato da un'autorità di certificazione attendibile, è pronto per essere salvato nella macchina.

d. Tornare alla schermata **Gestione certificato digitale del sistema**, nella sezione *Certificato digitale del sistema*, fare clic sul pulsante **Carica certificato firmato**.

e. Fare clic su **Sfoglia**, individuare il file nella workstation e fare clic su **Apri**.

f. Fare clic su **Carica certificato**.

Abilitazione di HTTP (SSL) protetto

Nota: prima di poter abilitare HTTP (SSL) protetto, è necessario che un certificato digitale del sistema sia installato nel dispositivo. Per informazioni dettagliate, fare riferimento a Gestione certificato digitale del sistema a pagina 7.

Nella workstation

1. Aprire il browser Web, inserire l'*indirizzo IP* della macchina nella barra dell'indirizzo o nel campo Posizione.
2. Fare clic su **Invio** per accedere ai Servizi Internet del dispositivo.
3. Fare clic sulla scheda **Proprietà**.
4. Se richiesto, inserire il codice di accesso e l'ID dell'amministratore del sistema. Il codice di accesso e l'ID dell'amministratore del sistema predefiniti sono rispettivamente "**1111**" e "**admin**".
5. Fare clic su **Connettività**, quindi su **Protocolli**.
6. Fare clic sul collegamento **HTTP** nell'albero di directory.
7. Nella sezione *Configurazione*:
   a. Per *Protocollo* selezionare la casella di controllo **Abilita** per abilitare le comunicazioni HTTP con il dispositivo.
   b. Nel campo *Numero porta*, inserire il numero di porta che sarà utilizzato dal server Web del dispositivo per le connessioni client HTTP. Il numero di porta di default è 80.
   c. Per *Modalità di protezione HTTP*, selezionare una delle seguenti opzioni dal menu a discesa:
      - **Disabilita SSL**
      - **Abilita SSL** - per abilitare Secure Socket Layer (SSL) per comunicazioni (HTTPS) sicure.
      - **SSL obbligatorio** - per rendere obbligatorio Secure Socket Layer (SSL).

   Nota: se HTTP protetto è abilitato, per accedere a Servizi Internet CentreWare, tutte le pagine conterranno **https://** nell'URL della pagina Web.

   d. Nel campo *Timeout connessione* inserire il tempo per cui il server Web rimane in attesa di una risposta HTTP da un client prima di interrompere la sessione. Il valore di default è 10 secondi.
8. Fare clic su **Applica**.

Server proxy

Un server proxy agisce come filtro per client alla ricerca di servizi e i server che li forniscono. Il server proxy filtra le richieste e se queste sono conformi alle regole filtro del server proxy, la richiesta viene concessa e la connessione viene stabilita.

Un server proxy ha due scopi principali:

- Mantenere anonimo qualsiasi dispositivo a fini di protezione.
- Ridurre il tempo necessario per accedere a una risorsa mediante memorizzazione del contenuto nella cache, quali pagine Web da un web.

Nella workstation

1. Aprire il browser Web, inserire l'*indirizzo IP* della macchina nella barra dell'indirizzo o nel campo Posizione.
2. Fare clic su **Invio** per accedere ai Servizi Internet del dispositivo.
3. Fare clic sulla scheda **Proprietà**.
4. Se richiesto, inserire il codice di accesso e l'ID dell'amministratore del sistema. Il codice di accesso e l'ID dell'amministratore del sistema predefiniti sono rispettivamente "**1111**" e "**admin**".
5. Fare clic su **Connettività**, quindi su **Protocolli**.
6. Fare clic sul collegamento **Server proxy** nell'albero di directory.
7. Nella sezione *Server proxy HTTP*:
   a. Selezionare la casella di controllo **Rilevamento automatico via WPAD** per rilevare automaticamente le impostazioni proxy utilizzando il protocollo WPAD. Deselezionare questa casella di controllo per disabilitare il rilevamento proxy automatico e utilizzare le impostazioni proxy manuali.
   b. Per *Server proxy HTTP*, selezionare la casella di controllo **Abilitato** per configurare manualmente le impostazioni proxy.
   c. Selezionare **Indirizzo IP** o **Nome host**.
   d. Immettere l'indirizzo e il numero di porta correttamente formattati nel campo **Indirizzo IP e porta** o **Nome host e porta**; il numero di porta di default è 8080.
8. Fare clic su **Applica**.

   Nota: le impostazioni del server proxy vengono utilizzate per EIP, Smart eSolutions, Scansione in rete HTTP e Download gruppo di modelli HTTP.

   Nota: è possibile che il rilevamento automatico delle impostazioni proxy sovrascriva le impostazioni manuali. Disabilitare Rilevamento automatico via WPAS per garantire l'uso delle impostazioni manuali.