Versión 1.0
Enero de 2011

Xerox® Phaser™ 3635MFP Extensible Interface Platform

Se realizan cambios a este documento periódicamente. Los cambios del producto, así como las correcciones de posibles inexactitudes técnicas y tipográficas, se incorporarán en ediciones subsiguientes.

Versión del documento 1.0: enero de 2011

Traducido por:

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

Índice

Introducción 4
Ventajas de EIP para el usuario final 4
Ejemplo de las funciones que ofrece EIP 4
Procesos simplificados 5
Soluciones personales 5
Configuración de XEIP 6
Lista de control de la información 6
Activación de los servicios personalizados 6
Gestión del Certificado digital de la máquina 7
Activación de HTTP protegido (SSL) 8
Servidor proxy 9

Introducción

Xerox Extensible Interface Platform (EIP) abre un nuevo abanico de posibilidades para los dispositivos de Xerox. Con EIP, los dispositivos de Xerox ahora pueden adaptarse a sus procesos de trabajo, y no a la inversa.

- Los **usuarios finales** pueden compartir, almacenar e imprimir información de manera más sencilla
- El **departamento de TI** ofrecer valor añadido y seguridad de la información a sus clientes
- Los **desarrolladores** pueden crear aplicaciones de manera rápida y sencilla y personalizarlas en función de la interfaz de usuario del dispositivo

Puede adquirir e instalar en su dispositivo varias soluciones de software opcionales. EIP permite personalizar el dispositivo específicamente para sus procesos de flujos de trabajo. Xerox EIP permite que los proveedores y socios desarrollen programas personalizados mediante el uso de herramientas web estándar para crear aplicaciones basadas en servidor a las que se pueda acceder directamente desde la interfaz de usuario del dispositivo.

Ventajas de EIP para el usuario final

- **Simplifica** flujos de trabajo complicados y facilita el uso del dispositivo.
- **Transforma** documentos impresos en información digital, de manera que sea más fácil editar, almacenar y compartir información.
- **Adapta** el dispositivo en función de sus metodologías de trabajo, y no a la inversa.
- **Completa** algunas tareas totalmente en el dispositivo, incluida la recuperación de documentos en una red sin necesidad de utilizar un equipo.
- **Presta servicio** a los clientes de forma más rápida.
- **Integra** soluciones en la infraestructura de TI existente.
- **Administra** soluciones centralizadas desde cualquier lugar del mundo.
- **Expande** y adapta el dispositivo de acuerdo con el desarrollo de su empresa.
- **Crea** soluciones personalizadas fácilmente. EIP está basado en estándares web como HTML, CSS, XML y JavaScript. También utiliza protocolos de seguridad como HTTPS y SSL.

Ejemplo de las funciones que ofrece EIP

- Uso de menús y lenguajes específicos de su empresa o grupo de trabajo, como "Búsqueda en la base de datos de clientes", "Envío de formularios al departamento de reclamaciones" o "Envío a cuentas por pagar".
- Todas sus preferencias personales pueden aparecer en la interfaz de usuario del dispositivo con sólo pasar la tarjeta de identificación.
- Conversión de flujos de trabajo complicados en procesos simples, en los que sólo se necesita tocar algunos botones.
- Introducción de información impresa en un depósito de documentos con sólo tocar un botón.
- Envío de documentos a una cola de impresión en red e impresión desde cualquier dispositivo de la red pasando la tarjeta de identificación.

- Impresión de las noticias del día o los informes financieros directamente desde la interfaz de usuario del dispositivo Xerox.

Procesos simplificados

Convierta un flujo de trabajo complicado en un proceso sencillo.

Imagínese un botón de "facturación" en el dispositivo que envíe simultáneamente una factura al departamento correcto, que archive la información en un sistema de administración de documentos para recuperarla fácilmente y que imprima una copia para sus registros personales.

Los usuarios pueden escanear y capturar rápidamente documentos impresos, acceder a vistas en miniatura y agregarlas a una ubicación de almacenamiento de documentos usados con frecuencia. Por ejemplo:

Un tutor puede escanear notas directamente a un depósito del curso específico para que los alumnos accedan a ellas.

Un estudiante puede escanear documentos de evaluación a la carpeta del curso para que el tutor los califique.

Xerox Extensible Interface Platform utiliza soluciones basadas en web de socios Xerox para permitir que los usuarios accedan a los depósitos de documentos desde el panel de control de la máquina.

Además, **Xerox Secure Access Unified ID System™** se ha diseñado para empresas de asistencia médica, compañías de servicios financieros e instituciones educativas que desean tener más seguridad para los registros confidenciales. Con este sistema, que combina lectores de tarjetas y software, los usuarios pueden acceder a los dispositivos Xerox pasando o acercando la tarjeta de identificación al lector de tarjetas del dispositivo. Para más seguridad, se puede incorporar un PIN o una contraseña en el software. El sistema de acceso seguro puede integrarse con el sistema de tarjetas de identificación existente en una empresa.

Es posible que se necesiten otros recursos en el dispositivo en función de la solución.

Para obtener más información, póngase en contacto con el personal de ventas de Xerox.

Soluciones personales

EIP facilita la conexión al dispositivo mediante la introducción de los datos de conexión o de la tarjeta de identificación de la empresa.

Esto proporciona acceso seguro al dispositivo y, además, como el dispositivo lo reconoce, puede acceder a opciones específicas de sus flujos de trabajo, lo cual facilita su trabajo.

Configuración de XEIP

Lista de control de la información

Antes de iniciar el procedimiento de instalación, asegúrese de que los elementos siguientes estén disponibles o se hayan seguido estos pasos.

- **Asegúrese de que el dispositivo funciona correctamente en la red**.
- **Asegúrese de que la solución EIP se ha instalado y funciona.** Para obtener más información, póngase en contacto con el personal de ventas de Xerox.
- **Asegúrese de que se ha activado HTTP protegido (SSL) en el dispositivo** (opcional). Si desea obtener más información, consulte Activación de HTTP protegido (SSL) en la página 8.

  Nota: se debe haber instalado un certificado digital de la máquina en el dispositivo antes de activar HTTP protegido (SSL). Si desea obtener más información, consulte Gestión del Certificado digital de la máquina en la página 7.

Activación de los servicios personalizados

En la estación de trabajo

1. Abra el navegador web, introduzca la *dirección IP* de la máquina en la barra de direcciones o en el campo Ubicación.
2. Haga clic en **Intro** para acceder a los Servicios de Internet del dispositivo.
3. Para activar las aplicaciones de EIP del dispositivo:
   a. Haga clic en la ficha **Propiedades**.
   b. Haga clic en **Servicios** y, a continuación, en el enlace **Servicios personalizados**.
   c. En la página *Servicios personalizados*, en el área *Activación*, para activar el servicio *Servicios personalizados*, seleccione la casilla de verificación **Activado**.
   d. En el área *Información opcional*, si es preciso, seleccione las casillas de verificación **Activado** para los siguientes elementos:
      - **Exportar clave a servicios personalizados**: si se ha seleccionado, se envían las claves al servicio personalizado.
      - **Validar automáticamente certificados firmados desde el servidor**: si se ha seleccionado, para que esta opción funcione correctamente, el certificado y el dispositivo deben tener certificados. Una autoridad de confianza del dispositivo debe emitir estos certificados.
   e. Haga clic en **Aplicar**.
   f. Si es preciso, introduzca la ID del administrador del sistema y la clave. La ID del administrador del sistema y la clave son "**admin**" y "**1111**" respectivamente.
4. Genere un certificado digital (si es preciso); consulte Gestión del Certificado digital de la máquina en la página 7.
5. Active SSL (si es preciso); si desea obtener más información, consulte Activación de HTTP protegido (SSL) en la página 8.

En el dispositivo

1. Pulse el botón **Todos los servicios**.
2. Pulse el botón **Servicios personalizados**.
3. Pulse el botón de la **aplicación EIP** que registró. Debe ser posible acceder al flujo de trabajo de XEIP desde el botón nuevo.

Gestión del Certificado digital de la máquina

1. Abra el navegador web, introduzca la *dirección IP* de la máquina en la barra de direcciones o en el campo Ubicación.
2. Haga clic en **Intro** para acceder a los Servicios de Internet del dispositivo.
3. Haga clic en la ficha **Propiedades**.
4. Si es preciso, introduzca la ID del administrador del sistema y la clave. La ID del administrador del sistema y la clave son "**admin**" y "**1111**" respectivamente.
5. Haga clic en **Seguridad**.
6. Haga clic en el enlace **Certificado digital de la máquina** en el árbol de directorios.
7. En el área *Certificado digital de la máquina*, haga clic en el botón **Crear certificado nuevo**.
8. En el área *Crear certificado nuevo*, seleccione una de las siguientes opciones:
   - **Certificado autofirmado: Debe establecer en esta máquina un Certificado autofirmado**: el dispositivo firma su propio certificado y crea la clave pública para utilizar el certificado en cifrado SSL.
   - **Solicitud de firma de certificado: Descargue una Solicitud de firma de certificado para su proceso por una Autoridad de certificados fiable**: se puede cargar en la máquina un certificado de una Autoridad de certificados o de un servidor que sirva como Autoridad de certificados.
9. Haga clic en **Continuar**.
10. Introduzca los datos en los campos siguientes para las opciones requeridas:

Para *Certificado autofirmado*:	Para *Solicitud de firma de certificado*:
• **Código del país de 2 letras** • **Provincia** • **Localidad** • **Organización** • **Unidad de organización** • **Dirección electrónica** • **Días de validez**	• **Código del país de 2 letras** • **Provincia** • **Localidad** • **Organización** • **Unidad de organización** • **Dirección electrónica**

11. Haga clic en **Aplicar**.
12. Dependiendo de la opción, si seleccionó:
    - *Certificado autofirmado*: el Estado actual muestra **Se ha establecido un certificado autoafirmado en esta máquina**.
    - *Solicitud de firma de certificado*: se muestra el formulario **Solicitud de firma de certificado (SFC)**.
    a. Si seleccionó **Solicitud de firma de certificado**, haga clic en el botón **Guardar como**.

b. En el cuadro de diálogo desplegable, seleccione el formato **X.509 (.pem)** o **DER**, y haga clic en **Guardar**.

c. En el menú desplegable *Descarga de archivos*, haga clic en **Guardar**, seleccione la ubicación en la estación de trabajo y haga clic en **Guardar** para guardar el archivo. Cuando una autoridad de certificados de confianza ha firmado el certificado, está listo para guardarse en la máquina.

d. Vuelva a la pantalla **Gestión del Certificado digital de la máquina**, en el área *Certificado digital de la máquina*, y haga clic en **Cargar certificado firmado**.

e. Haga clic en **Examinar**, localice el archivo en la estación de trabajo y haga clic en **Abrir**.

f. Haga clic en **Cargar certificado**.

Activación de HTTP protegido (SSL)

Nota: se debe haber instalado un certificado digital de la máquina en el dispositivo antes de activar HTTP protegido (SSL). Si desea obtener más información, consulte Gestión del Certificado digital de la máquina en la página 7.

En la estación de trabajo

1. Abra el navegador web, introduzca la *dirección IP* de la máquina en la barra de direcciones o en el campo Ubicación.
2. Haga clic en **Intro** para acceder a los Servicios de Internet del dispositivo.
3. Haga clic en la ficha **Propiedades**.
4. Si es preciso, introduzca la ID del administrador del sistema y la clave. La ID del administrador del sistema y la clave son "**admin**" y "**1111**" respectivamente.
5. Haga clic en **Conectividad** y, a continuación, en **Protocolos**.
6. Haga clic en el enlace **HTTP** en el árbol de directorios.
7. En el área *Configuración*:
   a. Para *Protocolo*, seleccione la casilla de verificación **Activado** para activar la comunicación HTTP con el dispositivo.
   b. En el campo *Número del puerto*, introduzca el número del puerto que utilizará el servidor web del dispositivo para las conexiones HTTP cliente. El número de puerto prefijado es 80.
   c. Para el *modo de seguridad HTTP*, seleccione una de las opciones siguientes en el menú desplegable:
      - **Desactivar SSL**
      - **Activar SSL**: para activar SSL para comunicaciones (HTTPS) protegidas.
      - **Requiere SSL**: para que SSL sea obligatorio.

   Nota: Si se ha activado HTTP protegido, para acceder a los Servicios de Internet de CentreWare, todas las páginas tendrán **https://** en la URL para la página web.

   d. En el campo *Espera para mantener activa* especifique cuánto esperará el servidor web una respuesta de HTTP del cliente antes de terminar la sesión. El valor prefijado es 10 segundos.
8. Haga clic en **Aplicar**.

Servidor proxy

Un servidor proxy actúa como filtro para los clientes que desean servicios y servidores que los proporcionen. El servidor proxy filtra solicitudes y si las solicitudes se ajustan a las reglas de filtrado del servidor proxy, se acepta la solicitud y se permite la conexión.

Un servidor proxy tiene dos propósitos principales:

- Mantener anónimos los dispositivos por motivos de seguridad.
- Disminuir la cantidad de tiempo necesario para acceder a un recurso guardando en caché el contenido, por ejemplo páginas web.

En la estación de trabajo

1. Abra el navegador web, introduzca la *dirección IP* de la máquina en la barra de direcciones o en el campo Ubicación.
2. Haga clic en **Intro** para acceder a los Servicios de Internet del dispositivo.
3. Haga clic en la ficha **Propiedades**.
4. Si es preciso, introduzca la ID del administrador del sistema y la clave. La ID del administrador del sistema y la clave son "**admin**" y "**1111**" respectivamente.
5. Haga clic en **Conectividad** y, a continuación, en **Protocolos**.
6. Haga clic en el enlace **Servidor proxy** en el árbol de directorios.
7. En el área *Servidor proxy HTTP*:
   a. Seleccione la casilla de verificación **Detección automática a través de WPAD** para autodetectar la configuración proxy mediante el protocolo WPAD. Anule la selección de la casilla de verificación para desactivar la detección automática del proxy y configurar manualmente el proxy.
   b. Para *Servidor proxy HTTP*, seleccione la casilla de verificación **Activado** para configurar manualmente las opciones del proxy.
   c. Seleccione **Dirección IP** o **Nombre del host**.
   d. Introduzca la dirección y el número de puerto con el formato correcto en el campo **Dirección IP y puerto** o **Nombre de host y puerto**; el número de puerto prefijado es 8080.
8. Haga clic en **Aplicar**.

   Nota: las opciones del servidor proxy se utilizan para EIP, Smart eSolutions, escaneado de red de HTTP(s) y descarga de plantillas HTTP(s).

   Nota: es posible que la detección automática de las opciones del proxy sobrescriba la configuración manual. Desactive Detección automática a través de WPAD para asegurarse de utilizar la configuración manual.