Version 1.0
January 2011

xerox®

Xerox® Phaser™ 3635MFP Extensible Interface Platform

Document Version 1.0: January 2011

Contents

Introduction

Xerox Extensible Interface Platform (EIP) brings a whole new world of possibilities to the Xerox device. With EIP, your Xerox device can now adapt to fit the way you work, not the other way round.

- **End-Users** can easily share, store and print information
- **IT** can add value and information security for their clients
- **Developers** can quickly and easily build applications that can be customized for the device's user interface

There are several optional software solutions that can be purchased and installed on to your device. EIP enables you to customize your device specifically for your workflow processes. Xerox EIP (Extensible Interface Platform) enables software vendors and partners to develop customized programs using standard web-based tools to create server-based applications that can be accessed directly from the device's user interface.

End-user Advantages Using EIP

- **Simplify** complicated workflows while making the device easier to use.
- **Transform** hardcopy documents into digital information, making it easier to edit, store and share information.
- **Adapt** the device to fit your work habits, not the other way round.
- **Complete** some tasks entirely at the device; including retrieving documents on a network without a computer.
- **Serve** your customers faster.
- **Integrate** solutions into your existing IT infrastructure.
- **Manage** centralized solutions from anywhere in the world.
- **Expand** and adapt the device along with your business.
- **Create** customized solutions easily, EIP is based on web standards such as HTML, CSS, XML and JavaScript. It also uses standard secure protocols – HTTPS and SSL.

Example of what EIP can enable

- Use menus and language that is specific to your business or workgroup, such as "Search client database", "Submit form to claims department" or "Fax to accounts payable".
- All of your personal preferences can appear on the user interface of your device system with the swipe your ID badge.
- Turn a complicated workflow into a simple process where only a few buttons need to be pushed.
- Enter hardcopy information into a document repository with the simple touch of a button.
- Send a document to a network print queue and print it from any device on the network with a swipe your ID card.
- Print the day's news or stock reports directly from the Xerox device user interface.

Simplified Processes

Turn a complicated workflow into a simple process.

Imagine an ‘invoices’ button on your device which simultaneously sends an invoice to the right department, archives the information in a document management system for easy retrieval, and prints a copy for your personal records.

Users can quickly scan and capture paper documents, preview thumbnails, and add them to a frequently used document storage location. For example:

A tutor can scan notes directly to a specific course repository for students to access.

A student can scan assessment papers to their course folder for their tutor to mark.

Xerox Extensible Interface Platform utilizes web-based Xerox Partner solutions to enable users to access document repositories at the machine’s control panel.

In addition to these is the **Xerox Secure Access Unified ID System™**, which is designed for organizations such as healthcare companies, financial services firm and educational institutions looking for more security towards their sensitive records. With this system, which combines card readers and software, users can access Xerox devices after swiping or waving their ID card in front of the card reader on the device. For added security, a PIN or password can be built into the software. The Secure Access system can integrate with an organization's existing employee badge ID system.

Additional resources may be required on the device depending on the solution.

For further information, contact your Xerox Sales Representative.

Personal Solutions

EIP makes it easy for you to log in to the device by entering your login details, or swiping your company ID badge.

This not only provides secure access to the device, but now that the device knows who you are, you can access options specific to your job flows - making your work easier.

Configuring XEIP

Information Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

- **Ensure the device is fully functioning on the network**.
- **Ensure your EIP solution is installed and functioning.** Refer to your Xerox Sales Representative for further information.
- **Ensure Secure HTTP SSL is enabled on the device**. (This is optional)
  For details, refer to Enabling Secure HTTP (SSL) on page 8.

  Note: A Machine Digital Certificate must be installed on the device before you can enable Secure HTTP (SSL). For details, refer to Machine Digital Certificate Management on page 7.

Enable Custom Services

At your workstation

1. Open your web browser, enter the *IP address* of the machine in the Address bar or Location field.
2. Click **Enter** to access the device Internet Services.
3. To enable the device for EIP applications:
   a. Click on the **Properties** tab.
   b. Click on **Services**, and then the **Custom Services** link.
   c. On the *Custom Services* page, in the *Enablement* area, for *Custom Services* check the **Enabled** checkbox to enable the service.
   d. In the *Optional Information* area, if required, check the **Enabled** checkboxes for the following:
      - **Export User Password to Custom Service** - if selected, passwords are sent to Custom Service.
      - **Automatically validate signed certificates from server** - if selected, in order for this option to work both the server and the device require to have certificates. These certificates must be issued by an authority that is trusted by the device.
   e. Click on **Apply**.
   f. If prompted, enter your System Administrator ID and passcode. The default System Administrator ID and passcode are “**admin**” and “**1111**” respectively.
4. Generate a digital certificate (if needed), refer to Machine Digital Certificate Management on page 7.
5. Enable SSL (if required), for details, refer to Enabling Secure HTTP (SSL) on page 8.

At the Device

1. Press the **All Services** button.
2. Touch the **Custom Services** button.
3. Touch the **EIP Application** button that you registered. Your XEIP workflow should be accessible from the new button.

Machine Digital Certificate Management

1. Open your web browser, enter the *IP address* of the machine in the Address bar or Location field.
2. Click **Enter** to access the device Internet Services.
3. Click on the **Properties** tab.
4. If prompted, enter your System Administrator ID and passcode. The default System Administrator ID and passcode are "**admin**" and "**1111**" respectively.
5. Click on **Security**.
6. Click on **Machine Digital Certificate** link in the directory tree.
7. In the *Machine Digital Certificate* area, click on **Create New Certificate** button.
8. In the *Create New Certificate* area, select one of the following:
   - **Self Signed Certificate: Establish a Self Signed Certificate on this machine** - the device signs its own certificate as trusted and creates the public key for the certificate to be used in SSL encryption.
   - **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** - a certificate from a Certified Authority or a server functioning as a Certificate Authority can be uploaded to the machine.
9. Click on **Continue**.
10. Enter details in the following fields for the required selection:

For *Self Signed Certificate*:	For *Certificate Signing Request*:
• **2 Letter Country Code** • **State/Province Name** • **Locality Name** • **Organization Name** • **Organization Unit** • **E-mail Address** • **Days of Validity**	• **2 Letter Country Code** • **State/Province Name** • **Locality Name** • **Organization Name** • **Organization Unit** • **E-Mail Address**

11. Click on **Apply**.
12. Depending on your selection, if you selected:
    - *Self Signed Certificate*: the Current Status displays **A Self Signed Certificate is established on this machine**.
    - *Certificate Signing Request*: the **Certificate Signing Request (CSR)** form displays.

    a. If you selected **Certificate Signing Request**, click on the **Save As** button

    b. From the pop-up dialog box, select either **X.509 (.pem)** or **DER** format, click on **Save**.

    c. From the *File Download* pop-up menu, click on **Save**, select the location on your workstation and click on **Save** to save the file.
    Once the certificate is signed by a trusted certificate authority, it is ready to be saved onto the machine.

    d. Return to **Machine Digital Certificate Management** screen, in the *Machine Digital Certificate* area, click on **Upload Signed Certificate** button.

    e. Click on **Browse**, locate the file on your workstation, and click on **Open**.

    f. Click on **Upload Certificate**.

Enabling Secure HTTP (SSL)

Note: A Machine Digital Certificate must be installed on the device before you can enable Secure HTTP (SSL). For details, refer to Machine Digital Certificate Management on page 7.

At your workstation

1. Open your web browser, enter the *IP address* of the machine in the Address bar or Location field.
2. Click **Enter** to access the device Internet Services.
3. Click on the **Properties** tab.
4. If prompted, enter your System Administrator ID and passcode. The default System Administrator ID and passcode are “**admin**” and “**1111**” respectively.
5. Click on **Connectivity**, and then **Protocols**.
6. Click on the **HTTP** link in the directory tree.
7. In the *Configuration* area:
   a. For *Protocol* check the **Enable** checkbox to enable HTTP communications with the device.
   b. In the *Port Number* field, enter the port number the device’s Web server will use for client HTTP connections. The default port number is 80.
   c. For *HTTP Security Mode*, select one of the following from the drop-down menu:
      - **Disable SSL**
      - **Enable SSL** - to enable Secure Socket Layer (SSL) for secure (HTTPS) communication.
      - **Require SSL** - to make Secure Socket Layer (SSL) mandatory.

   Note: If Secure HTTP is enabled, to access CentreWare Internet Services, all pages will contain **https://** in the URL for the Web page.

   d. In the *Keep Alive Timeout* field enter how long the Web server will wait for an HTTP response from a client before terminating its session. The default is 10 seconds.
8. Click on **Apply**.

Proxy Server

A proxy server acts as a filter for clients seeking services and servers that provide these. The proxy server filters requests and if the requests confirm to the proxy server’s filtering rules, the request is granted and allows the connection.

A proxy server has two main purposes:

- To keep any devices behind it anonymous for security purposes.
- To decrease the amount of time needed to access a resource by caching content, such as Web pages from a web.

At your workstation

1. Open your web browser, enter the *IP address* of the machine in the Address bar or Location field.
2. Click **Enter** to access the device Internet Services.
3. Click on the **Properties** tab.
4. If prompted, enter your System Administrator ID and passcode. The default System Administrator ID and passcode are “**admin**” and “**1111**” respectively.

5. Click on **Connectivity**, and then **Protocols**.
6. Click on **Proxy Server** link in the directory tree.
7. In the *HTTP Proxy Server* area:
    a. Check the **Auto Detect Proxy Settings** checkbox to auto detect proxy settings using WPAD protocol.
    Uncheck this checkbox to disable auto proxy detection and use manual proxy settings.
    b. For *HTTP Proxy Server*, check the **Enabled** checkbox, To manually set the proxy settings.
    c. Select either **IP Address** or **Hostname**.
    d. Enter the appropriately formatted address and port number in the **IP Address and Port** or **Host Name and Port** field, the default port number is 8080.
8. Click on **Apply**.

Note: Proxy server settings are used for EIP, Smart eSolutions, HTTP(s) Network Scanning and HTTP(s) Template Pool Downloading.

Note: Automatically detecting proxy settings may overwrite manual settings. Disable Auto Detect Proxy Settings to ensure use of manual settings.