Версия 1.0
январь 2011 г.

Xerox® Phaser™ 3635MFP Расширяемая интерфейсная платформа

В данный документ периодически вносятся изменения. Изменения и исправления технических неточностей и типографических ошибок будут внесены в последующие редакции.

Версия документа 1.0: январь 2011 г.

Переведено:

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

Содержание

Введение

Расширяемая интерфейсная платформа EIP (Extensible Interface Platform) Xerox расширяет возможности устройств Xerox. Благодаря платформе EIP устройство Xerox можно адаптировать к потребностям пользователей вместо того, чтобы к нему приспосабливаться.

- **конечные пользователи** с легкостью могут сохранять данные, обмениваться ими и выводить их на печать;
- **ИТ-специалисты** могут повысить эффективность своей деятельности и обеспечить безопасность данных для клиентов;
- **разработчики** получают возможность быстрого и простого создания приложений, которые можно настраивать в соответствии с интерфейсом пользователя устройства.

Вы можете приобрести и установить на устройство различное дополнительное программное обеспечение. Платформа EIP позволяет настраивать устройство в соответствии с конкретными условиями производственного процесса. Расширяемая интерфейсная платформа EIP (Extensible Interface Platform) Xerox позволяет поставщикам ПО и партнерам разрабатывать настраиваемые программы с помощью стандартных средств на основе веб-интерфейса и создавать серверные приложения, доступ к которым можно получать непосредственно из интерфейса пользователя устройства.

Преимущества использования платформы EIP для конечных пользователей

- **Упрощение** сложных рабочих процессов и взаимодействия с устройством.
- **Преобразование** печатных копий в цифровой формат упрощает процесс редактирования, хранения данных и обмена ими.
- **Возможность** адаптировать устройство к своим потребностям, а не наоборот.
- **Выполнение** некоторых задач только с помощью устройства, включая получение документов из сети без использования компьютера.
- **Повышение** скорости обслуживания клиентов.
- **Интеграция** решений в существующую ИТ-инфраструктуру.
- **Удаленное управление** централизованными решениями из любого расположения.
- **Расширение** функций и адаптация устройства к росту бизнеса.
- **Простое создание** настроенных решений — платформа EIP основана на веб-стандартах, таких как HTML, CSS, XML и JavaScript. Она также использует стандартные протоколы безопасности — HTTPS и SSL.

Примеры возможностей, обеспечиваемых EIP

- Использование меню и языка, наиболее удобных для компании или рабочей группы, например «Поиск в базе данных клиентов», «Отправка формы в отдел рекламаций» или «Отправка факса в отдел счетов к оплате».
- Все личные настройки могут отображаться в интерфейсе пользователя системы устройства при считывании идентификационной карточки пользователя.

- Превращение сложного рабочего процесса в простую процедуру, требующую нажатия всего нескольких кнопок.
- Ввод данных с печатной копии в хранилище документов одним прикосновением к сенсорному экрану.
- Отправка документа в сетевую очередь печати и печать на любом устройстве в сети при считывании идентификационной карточки пользователя.
- Печать новостей или отчетов о наличных запасах непосредственно из интерфейса пользователя устройства Xerox.

Упрощение рабочих процессов

Превращение сложного рабочего процесса в простую процедуру.

Представьте себе, что на устройстве есть кнопка «Счета», которая позволяет отправить счет в нужный отдел, сохранить данные в системе управления документами для последующего извлечения и напечатать копию для себя.

Пользователи могут быстро сканировать и сохранять данные печатных копий, просматривать эскизы и добавлять их в хранилище часто используемых документов. Например:

преподаватель может отсканировать заметки и сохранить их непосредственно в хранилище конкретного учебного курса, чтобы учащиеся могли с ними ознакомиться;

учащийся может отсканировать выполненную контрольную работу, сохранив ее в папку своего курса, чтобы преподаватель мог поставить оценку.

Расширяемая интерфейсная платформа Xerox использует решения партнеров Xerox на основе веб-интерфейса для предоставления доступа к хранилищам документов с панели управления аппарата.

Кроме того, специалистами Xerox разработана система **Xerox Secure Access Unified ID System™** (Система унифицированных ID безопасного доступа Xerox), предназначенная для таких организаций, как медицинские учреждения, фирмы, предоставляющие финансовые услуги, и учебные учреждения, которым требуется обеспечивать конфиденциальность своих архивов. С помощью этой системы, объединяющей устройства чтения карт и программное обеспечение, пользователи могут получать доступ к устройствам Xerox. Для этого нужно просто провести идентификационную карточку над устройством чтения карт на аппарате или вставить карточку в устройство. Для обеспечения дополнительной безопасности можно встроить в программное обеспечение ПИН-код или пароль. Эту систему безопасного доступа можно интегрировать в имеющуюся в организации систему идентификации сотрудников.

В зависимости от конкретного решения это может потребовать дополнительных ресурсов устройства.

Для получения дополнительных сведений обратитесь к торговому представителю Xerox.

Персонализация

Платформа EIP упрощает вход в систему устройства путем ввода реквизитов для входа в систему или использования идентификационной карточки сотрудника.

Это не только обеспечивает защиту доступа к устройству, но и дает возможность пользователям получать доступ к разным параметрам, характерным для их рабочих задач, упрощая их работу.

Настройка XEIP

Необходимые компоненты

Перед началом установки убедитесь в наличии следующих компонентов и выполнении указанных процедур.

- **Убедитесь в том, что устройство полноценно функционирует в сети**.
- **Убедитесь в том, что решение EIP установлено и функционирует.** Для получения дополнительных сведений обратитесь к торговому представителю Xerox.
- **На устройстве должен быть включен протокол HTTPS (SSL)**. (Это необязательное условие, дополнительные сведения см. в разделе Включение протокола HTTPS (SSL) на стр. 8).

  Примечание. Перед включением протокола HTTPS (SSL) необходимо установить на устройство цифровой сертификат аппарата. Дополнительные сведения см. в разделе Управление цифровыми сертификатами аппарата на стр. 7.

Включение пользовательских режимов

На рабочей станции

1. Откройте веб-браузер, введите *IP-адрес* аппарата в адресную строку или в поле «Расположение».
2. Нажмите кнопку **Ввод**, чтобы перейти на страницу службы Internet Services устройства.
3. Включение устройства для работы с приложениями EIP
   a. Перейдите на вкладку **Свойства**.
   b. Нажмите кнопку **Режимы**, затем щелкните ссылку **Пользовательские режимы**.
   c. На странице *Пользовательские режимы* в области *Включение* установите для опции *Пользовательские режимы* флажок **Включено**.
   d. При необходимости в области *Дополнительная информация* установите флажки **Включено** для следующих параметров:
      - **Экспорт пароля в пользовательские режимы** — при установке этого флажка пароли отправляются в пользовательский режим.
      - **Автоматически подтверждать подписанные сертификаты с сервера** — при установке этого флажка для работы данной опции требуется, чтобы сертификаты были установлены и на устройстве, и на сервере. Эти сертификаты должны быть выпущены центром сертификации, с которым у устройства установлены отношения доверия.

e. Нажмите кнопку **Применить**.

f. При получении запроса введите идентификатор системного администратора и пароль. Идентификатор системного администратора по умолчанию **admin**, пароль — **1111**.

4. При необходимости создайте цифровой сертификат (см. раздел Управление цифровыми сертификатами аппарата на стр. 7).
5. При необходимости включите протокол SSL (см. раздел Включение протокола HTTPS (SSL) на стр. 8).

На устройстве

1. Нажмите кнопку **Все режимы**.
2. Нажмите кнопку **Пользовательские режимы** на сенсорном экране.
3. Нажмите кнопку **EIP Application** (Приложение EIP), зарегистрированную в системе. Эта новая кнопка будет использоваться для перехода к созданному рабочему процессу XEIP.

Управление цифровыми сертификатами аппарата

1. Откройте веб-браузер, введите *IP-адрес* аппарата в адресную строку или в поле «Расположение».
2. Нажмите кнопку **Ввод**, чтобы перейти на страницу службы Internet Services устройства.
3. Перейдите на вкладку **Свойства**.
4. При получении запроса введите идентификатор системного администратора и пароль. Идентификатор системного администратора по умолчанию **admin**, пароль — **1111**.
5. Нажмите кнопку **Безопасность**.
6. Щелкните ссылку **Цифровой сертификат аппарата** в дереве каталога.
7. В области *Цифровой сертификат аппарата* нажмите кнопку **Создать новый сертификат**.
8. В области *Создать новый сертификат* выберите один из следующих вариантов:
   - **Самоподписанный сертификат: Установить самоподписанный сертификат на этом аппарате** — устройство подписывает собственный сертификат как доверенный и создает открытый ключ сертификата, который будет использоваться при шифровании по протоколу SSL.
   - **Запрос о подписи сертификата: Загрузите запрос о подписи сертификата для обработки доверенным центром сертификации** — на аппарат можно передать сертификат, созданный центром сертификации (ЦС) или сервером, выполняющим роль ЦС.
9. Нажмите кнопку **Продолжить**.

10. Выбрав нужный вариант, введите данные в следующие поля.

Для самоподписанного сертификата	*Для запроса подписи сертификата*
• **Двубуквенный код страны** • **Название области/края** • **Название населенного пункта** • **Название организации** • **Подразделение** • **Адрес эл. почты** • **Срок действия (дней)**	• **Двубуквенный код страны** • **Название области/края** • **Название населенного пункта** • **Название организации** • **Подразделение** • **Адрес эл. почты**

11. Нажмите кнопку **Применить**.
12. В зависимости от выбранного варианта, при выборе
    - *самоподписанного сертификата* в области "Текущий статус" отображается сообщение **На этом аппарате установлен самоподписанный сертификат**;
    - *запроса подписи сертификата* отображается форма **Запрос о подписи сертификата**.
    a. Выбрав **запрос подписи сертификата**, нажмите кнопку **Сохранить как**.
    b. В появившемся диалоговом окне выберите формат **X.509 (.pem)** или **DER** и нажмите кнопку **Сохранить**.
    c. Во всплывающем меню *Загрузить файлы* нажмите кнопку **Сохранить**, выберите нужное расположение на рабочей станции и нажмите кнопку **Сохранить**, чтобы сохранить файл. После подписания сертификата доверенным центром сертификации он готов к сохранению на аппарат.
    d. Вернитесь к экрану **Управление цифровым сертификатом аппарата** и в области *Цифровой сертификат аппарата* нажмите кнопку **Выгрузить подписанный сертификат**.
    e. Нажмите кнопку **Обзор**, найдите файл в системе рабочей станции и нажмите кнопку **Открыть**.
    f. Нажмите кнопку **Выгрузить сертификат**.

Включение протокола HTTPS (SSL)

Примечание. Перед включением протокола HTTPS (SSL) необходимо установить на устройство цифровой сертификат аппарата. Дополнительные сведения см. в разделе Управление цифровыми сертификатами аппарата на стр. 7.

На рабочей станции

1. Откройте веб-браузер, введите *IP-адрес* аппарата в адресную строку или в поле «Расположение».
2. Нажмите кнопку **Ввод**, чтобы перейти на страницу службы Internet Services устройства.
3. Перейдите на вкладку **Свойства**.
4. При получении запроса введите идентификатор системного администратора и пароль. Идентификатор системного администратора по умолчанию **admin**, пароль — **1111**.
5. Щелкните **Подключения**, а затем **Протоколы**.

6. Щелкните ссылку **HTTP** в дереве каталога.
7. В области *Конфигурация* настройте следующие параметры:
   a. В поле *Протокол* установите флажок **Включить**, чтобы включить обмен данными с устройством по протоколу HTTP.
   b. В поле *Номер порта* введите номер порта, который будет использоваться веб-сервером устройства для клиентских подключений HTTP. Номер порта по умолчанию — 80.
   c. В раскрывающемся меню *Режим безопасности HTTP* выберите один из следующих вариантов:
      - **Отключить SSL;**
      - **Включить SSL**, чтобы включить протокол шифрования SSL (Secure Socket Layer) для защищенных подключений по протоколу HTTPS;
      - **Требует шифрования SSL**, чтобы задать обязательное использование протокола SSL.

   Примечание. Если включен протокол HTTPS, для получения доступа к интернет-службам CentreWare Internet Services все страницы в URL-адресе веб-страницы должны содержать элемент **https://**.

   d. В поле *Тайм-аут проверки активности* введите время ожидания веб-сервером ответа HTTP от клиента до прекращения сеанса подключения. Значение по умолчанию: 10 секунд.
8. Нажмите кнопку **Применить**.

Прокси-сервер

Прокси-сервер играет роль фильтра для клиентов, которым требуется получить доступ к определенным службам и серверам, предоставляющим их. Прокси-сервер фильтрует запросы, удовлетворяет их и разрешает подключение, если запросы отвечают правилам фильтрации прокси-сервера.

Прокси-сервер выполняет две основные задачи:

- сохранение анонимности подключенных к нему устройств с целью обеспечения безопасности;
- сокращение времени, необходимого для получения доступа к ресурсу, благодаря кэшированию содержимого, такого как веб-страницы.

На рабочей станции

1. Откройте веб-браузер, введите *IP-адрес* аппарата в адресную строку или в поле «Расположение».
2. Нажмите кнопку **Ввод**, чтобы перейти на страницу службы Internet Services устройства.
3. Перейдите на вкладку **Свойства**.
4. При получении запроса введите идентификатор системного администратора и пароль. Идентификатор системного администратора по умолчанию **admin**, пароль — **1111**.
5. Щелкните **Подключения**, а затем **Протоколы**.
6. Щелкните ссылку **Прокси-сервер** в дереве каталога.

7. В области *Прокси-сервер HTTP* настройте следующие параметры:
   a. Установите флажок **Автообнаружение через WPAD**, чтобы настроить автоматическое определение параметров прокси-сервера с помощью протокола WPAD. Снимите этот флажок, чтобы отключить автоматическое определение прокси-сервера и выполнить настройки параметров вручную.
   b. В поле *Прокси-сервер HTTP* установите флажок **Включено**, чтобы выполнить ручную настройку параметров прокси-сервера.
   c. Выберите **IP-адрес** или **Имя хоста**.
   d. В поле **IP-адрес и порт** или **Имя и порт хоста** введите адрес и номер порта в правильном формате (значение порта по умолчанию — 8080).
8. Нажмите кнопку **Применить**.

   Примечание. Параметры прокси-сервера используются функциями EIP, Smart eSolutions, HTTP(s) Network Scanning (Сетевое сканирование по HTTP(s)) и HTTP(s) Template Pool Downloading (Загрузка пула шаблонов по HTTP(s)).

   Примечание. Установка автоматического определения параметров прокси-сервера может привести к перезаписи ручных настроек. Отключите эту функцию, чтобы гарантировать использование параметров, заданных вручную.