ВЕРСИЯ 8.0.0
АВГУСТ 2024 Г.
702P09306

# Xerox® FreeFlow® Core

Руководство по обеспечению безопасности

Данный программный продукт включает программное обеспечение, разработанное компанией Adobe Systems Incorporated.

Adobe, логотип Adobe, логотип Adobe PDF, PDF Converter SDK, Adobe Acrobat Pro DC, Adobe Reader DC и PDF Library являются товарными знаками или зарегистрированными товарными знаками компании Adobe Systems Incorporated в США и/или других странах.

Браузер Google Chrome™ является товарным знаком Google LLC.

Microsoft®, Windows®, Edge®, Microsoft Language Pack, Microsoft Office 2016, Microsoft Office 2019, Microsoft Office 2021, Microsoft Office 365, Microsoft SQL Server и Internet Explorer® являются зарегистрированными товарными знаками корпорации Microsoft в США и/или других странах.

Apple®, Macintosh®, Mac®, Mac OS® и Safari® являются товарными знаками или зарегистрированными товарными знаками компании Apple Inc. в США и других странах.

Mozilla Firefox является товарным знаком Mozilla Foundation в США и других странах.

BR40387

# Содержание

# Обзор

Содержание этой главы:

## Назначение

В данном Руководстве по обеспечению безопасности изложена информация о безопасности продукции в отношении Xerox® FreeFlow® Core. В этом контексте безопасность продукта определяется способом хранения и передачи данных, поведением продукта в сетевой среде, а также локальным и удаленным способами доступа к продукту. В этом документе описываются конструкция, функции и режимы Xerox® FreeFlow® Core в отношении защиты информации (IA) и защиты конфиденциальной информации клиентов.

Этот документ не содержит обучающую информацию о безопасности и возможностях подключения функций и режимов Xerox® FreeFlow® Core. Подробнее об этих функциях и режимах см. в *Справке Xerox® FreeFlow® Core*. Предполагается, что пользователь имеет практические знания по этим темам.

За безопасность своей сети и продукта FreeFlow отвечает заказчик. Программный продукт FreeFlow не обеспечивает безопасности каких-либо сетевых сред.

## Целевая аудитория

Целевая аудитория данной публикации — это пользователи, которым требуется дополнительная информация по обеспечению безопасности при работе с ПО Xerox® FreeFlow® Core.

## Отказ от ответственности за последствия использования

Содержащаяся в данном документе информация была точной на день публикации; эта информация предоставляется без каких-либо гарантий. Корпорация Xerox® Corporation ни при каких обстоятельствах не несет ответственности за какой-либо ущерб в результате использования или игнорирования пользователем информации, содержащейся в данной публикации, включая прямые, косвенные, случайные убытки, упущенную выгоду или особые убытки, даже если корпорация Xerox® Corporation была предупреждена о возможности таких убытков.

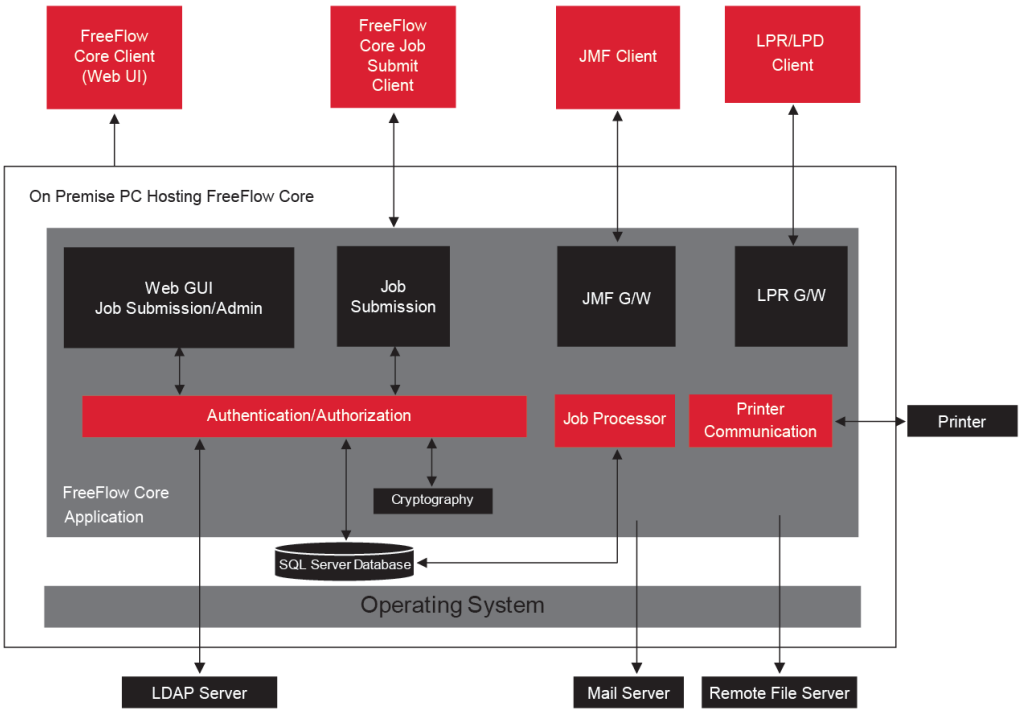
# Описание продукта

Содержание этой главы:



Xerox® FreeFlow® Core представляет собой новое поколение решений от компании Xerox, предназначенных для управления рабочим процессом. FreeFlow Core — это браузерное решение, предлагающее функции интеллектуальной автоматизации и интеграции обработки заданий печати, начиная с подготовки файлов и заканчивая окончательной обработкой. FreeFlow Core обеспечивает автоматизированный рабочий процесс, который легко адаптируется, быстро масштабируется и гарантирует стабильные результаты.

## Структура системного ПО



# Аспекты безопасности отдельных компонентов

Содержание этой главы:

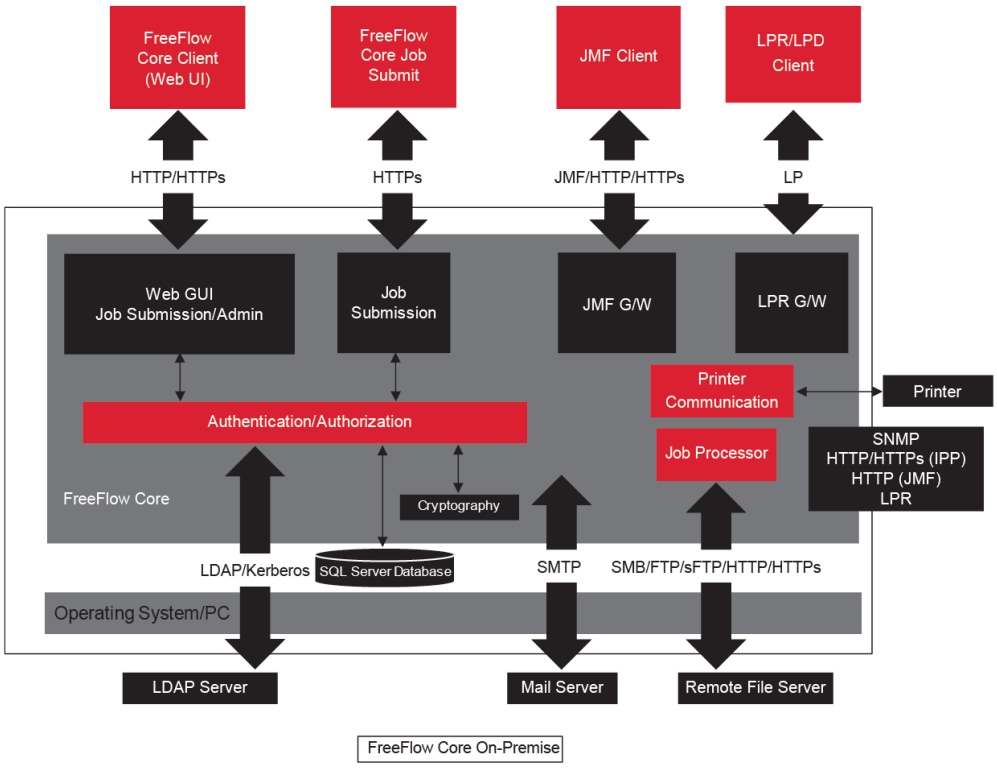
# Доступ к системе

## СЕТЕВЫЕ ПОДКЛЮЧЕНИЯ

Xerox® FreeFlow® Core требует подключения к сети для обработки заданий и взаимодействия с пользователем. См. информацию об обеспечении безопасности для каждого типа сетевого подключения.

Примечание. Для улучшения защиты от угроз безопасности включите брандмауэр Windows на сервере, на котором установлено ПО FreeFlow Core.

FreeFlow Core использует следующие сетевые протоколы.




### Клиент Xerox® FreeFlow® Core

Для подключения к FreeFlow Core требуется веб-браузер с поддержкой HTML5 и CSS3. Для безопасной загрузки клиента Xerox® FreeFlow® Core и защищенной связи между клиентом и Xerox® FreeFlow® Core требуется использование связи по протоколу HTTPS.

- Чтобы включить связь по протоколу HTTPS, для службы Internet Information Services (IIS) необходимо добавить Сертификат сервера. Для этого необходимо воспользоваться инструкциями в документации Windows.
- Если включены соединения HTTPS, необходимо установить настройку Потребовать SSL в Microsoft Internet Information Service (IIS). Из командной строки Windows запустите пакетный файл RequireSSL, который находится в каталоге под названием «Поддержка» в каталоге установки FreeFlow Core или по адресу `C:\Program Files\Xerox\FreeFlow Core`.
- FreeFlow Core поддерживает криптографические протоколы TLS.

Примечание. FreeFlow Core использует настройки операционной системы, поддерживающие протокол TLS. Для использования текущих версий криптографических протоколов рекомендуется устанавливать в операционной системе актуальные обновления.

- Если пользователь не скачивает файлы работ, передача данных заказчика между клиентом и сервером Xerox® FreeFlow® Core не осуществляется.

Примечание. Клиент получает свойства работ, которые содержат данные заказчика.

**Табл. 3.1 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 80 | HTTP | Входящее<br>Примечание. Номер порта зависит от конфигурации сервера IIS. |
| 443 | HTTPS | Входящее<br>Примечание. Номер порта зависит от конфигурации сервера IIS. |

### Роли пользователя

После запуска Xerox® FreeFlow® Core открывается окно входа в систему.

- Для доступа к системе FreeFlow Core пользователям необходимо выполнить вход.
- При отсутствии активности на протяжении 30 минут сеанс пользователя автоматически прерывается.
- В случае ошибок проверки подлинности при входе в ПО FreeFlow Core доступ пользователей к приложению блокируется после трех ошибочных попыток входа.

Примечание. Дополнительные настройки учетной записи пользователя см. в разделе Доступ учетных записей и хранение работ. Администратор FreeFlow Core выполняет конфигурирование настроек.

Порядок назначения ролей пользователей описывается в *Справке Xerox® FreeFlow® Core* в разделе *Настройка доступа пользователя*.

### Роль администратора

Администраторы имеют доступ ко всей системе:

- Функции на вкладках «Управление работами» и «Статус»: Диалоговое окно «Отправить работу» и вкладка «Статус работы».
- Вкладки «Управление принтером» и «Статус»
- Настройка рабочего процесса
- Функции на вкладке «Администрирование»:
  - Горячая папка
  - Уведомления
  - Доступ пользователя
  - Регион
  - Безопасность
  - Отчеты Core
  - Обмен Core
  - Опции очереди
  - Лицензия Core
- Утилиты сервера Core, доступные на рабочем столе сервера:
  - Обмен FreeFlow® Core
  - Настройка FreeFlow® Core
  - Отчеты FreeFlow® Core для утилиты командной строки

Примечание. Не допускается одновременная работа нескольких операторов в системе Xerox® FreeFlow® Core.

### Роль оператора

Операторы имеют доступ к следующим функциям:

- Функции на вкладках «Управление работами» и «Статус»: Диалоговое окно «Отправить работу» и вкладка «Статус работы»
- Вкладки «Управление принтером» и «Статус»

Примечание. Допускается одновременная работа нескольких операторов в Xerox® FreeFlow® Core.

### Роль «Мониторинг состояния работ»

В режиме «Мониторинг состояния работ» доступ к вкладке «Статус работы» возможен только для чтения.

Примечание. Xerox® FreeFlow® Core допускает одновременную работу нескольких пользователей, которым назначена роль «Мониторинг состояния работ».

### Идентификация пользователя

Учетные данные, вводимые в браузерном клиенте Xerox® FreeFlow® Core, при использовании протокола HTTP не шифруются. Для защищенной передачи включите протокол HTTPS и задайте настройку «Потребовать SSL» в IIS, чтобы обеспечить защищенный доступ из браузера к Xerox® FreeFlow® Core.

- Если идентификация пользователей выполняется с помощью Xerox® FreeFlow® Core, данные пользователей не шифруются. Учетные данные хранятся локально и шифруются.
- Если идентификация выполняется с помощью Active Directory, учетные данные перед отправкой в Active Directory не шифруются. Если идентификация выполняется с помощью Active Directory, учетные данные не хранятся локально.
- Настройку идентификации Xerox® FreeFlow® Core можно выполнить с использованием существующей службы Windows Active Directory. Данная настройка использует учетные записи компьютера текущего пользователя в качестве учетных записей для входа клиента Xerox® FreeFlow® Core.

Подключение конфигурации Xerox® FreeFlow® Core к службе Active Directory шифруется согласно конфигурации операционной системы.

**Табл. 3.2 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 80 | HTTP | Входящее<br>Примечание. Номер порта зависит от конфигурации сервера IIS. |
| 88 | Kerberos | Исходящее: Идентификация пользователя<br>Примечание. Номера портов и служб зависят от конфигурации сервера AD. |
| 389636<br>3268<br>3269 | LDAPLDAP TLS<br>LDAP GC<br>LDAP GC TLS | Исходящее: проверка групп Active Directory в ходе настройки идентификации Active Directory<br>Примечание. Номера портов и служб зависят от конфигурации сервера AD. |

### Подключение к SQL Server

Xerox® FreeFlow® Core устанавливает связь с SQL Server с помощью Entity Framework от Microsoft®. Шифрование связи между Xerox® FreeFlow® Core и SQL Server выполняется, когда для SQL Server задано использование шифрованных подключений.

Зашифрованные учетные данные SQL Server хранятся локально на сервере Xerox® FreeFlow® Core.

Для установки программного обеспечения на удаленном сервере SQL Server без прав администратора SQLS создайте в SQLS две пустые базы данных:

- `OapMasterDatabase`
- `OapPlatformDatabase`

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 1433 | SQLS | Входящее: прием подключений от Xerox® FreeFlow® Core.<br>Исходящее: связь с базой данных механизма печати SQL Server<br>Примечание. Номер порта зависит от конфигурации сервера SQLS. |
| 1434 | Служба браузера SQLS | Входящее: прием подключений от Xerox® FreeFlow® Core.<br>Исходящее: связь с базой данных механизма печати SQL Server<br>Примечание. Сервер предоставляет клиенту номер порта для подключения. |

### Пользовательский интерфейс отправки работ

Раздел пользовательского интерфейса «Отправить работу» использует подключение клиента Xerox® FreeFlow® Core для отправки работ. См. раздел Клиент Xerox® FreeFlow® Core.

**Табл. 3.3 Конфигурация брандмауэра**

| ПОР-Т | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 80 | HTTP | Входящее<br>Примечание. Номер порта зависит от конфигурации сервера IIS. |
| 443 | HTTPS | Входящее<br>Примечание. Номер порта зависит от конфигурации сервера IIS. |

### Горячие папки

Общие файловые ресурсы используются для передачи локальной горячей папки в общее пользование, а также для доступа к горячей папке в папках общего пользования Windows. Для шифрования файлов Windows используется файловая система Windows. Для защиты папок Windows используется контроль доступа к учетной записи пользователя Windows.

Примечание. При использовании функции контроля учетных записей пользуйтесь той же служебной учетной записью, что и при настройке раздела *«Установка дополнительного ПО»*. Дополнительные сведения приведены в *Руководстве по установке Xerox® FreeFlow® Core*.

**Табл. 3.4 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 139, 445 | SMB | Входящее: доступ к «горячим» папкам через общий доступ к файлам в Windows<br>Исходящее: использование «горячих» папок в каталогах общего пользования. |
| 20, 21 | FTP | Входящее: доступ к «горячим» папкам через FTP |

### Обработка манифеста

В ходе отправки манифеста ПО Xerox® FreeFlow® Core извлекает файлы, перечисленные в манифесте. Доступ к этим файлам возможен через подключенные диски, файлы пути UNC, URI-идентификаторы HTTP, HTTPS, FTP или sFTP.

Примечание. Протоколы URI HTTP и FTP не поддерживают шифрование.

Общие файловые ресурсы используются для передачи локальной горячей папки в общее пользование, а также для доступа к горячей папке в папках общего пользования Windows. Для шифрования файлов Windows используется файловая система Windows. Для защиты папок Windows используется контроль доступа к учетной записи пользователя Windows.

Примечание. При использовании функции контроля доступа к учетным записям пользователей пользуйтесь той же служебной учетной записью, что и при настройке опциональных процедур установки. Указания по актуальному преобразованию файлов MS Office см. в *Примечаниях к выпуску Xerox® FreeFlow® Core*. Этот документ доступен на веб-странице FreeFlow® Core https://xerox.com/automate. В верхней части страницы щелкните **Ресурсы владельца**, а затем щелкните **Примечания к выпуску**, в которых подробно перечислены системные требования.

**Табл. 3.5 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 139, 145 | SMB | Исходящее: получение файлов, указанных в манифесте, из общих папок |
| 20, 21 | FTP | Исходящее: извлечение файлов, указанных в манифесте. |
| 80 | HTTP | Исходящее: извлечение файлов, указанных в манифесте. |

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 443 | HTTPS | Исходящее: получение файлов с использованием URL-адресов HTTPS, указанных в манифесте |
| 22 | sFTP | Исходящее: получение файлов с использованием протокола Secure FTP, как указано в манифесте |

### Line Printer Daemon (LPD)

Примечание. Команды LP (линейный принтер) не поддерживают защищенные подключения.

**Табл. 3.6 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 515 | LP | Входящее: получение запросов удаленного линейного принтера (LPR) и команд LP |
| 721 – 731 | LPR | Исходящее: отправка запросов LPR на принтер с поддержкой LPD. |

### Команды JMF и сигналы состояния принтера

Формат Job Messaging Format (JMF) отправляет команды и сигналы на клиент JMF для поддержки защищенных соединений. При получении файлов JMF поддерживается связь по протоколу HTTPS.

Примечание. Для защищенной передачи JMF отправьте MIME-пакет с файлами JMF, JDF и PDF.

Включение связи по протоколу HTTPS для команд JMF:

1. Чтобы добавить сертификат в хранилище ключей Java, войдите в установочный каталог Xerox® FreeFlow® Core и запустите утилиту `installJMFCertificate.bat`.
2. Перезапустите службу Xerox® FreeFlow® Core JMF Server.
3. Для проверки установки перейдите по адресу `http://<имя-хоста>:7759/FreeFlowCore`. При правильной конфигурации защищенного JMF в браузере отображается страница ошибки `HTTP Status 404`.

**Табл. 3.7 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 7751 | JMF | Входящее: получение команд JMF. |
| Разные | JMF | Исходящее: возврат сигналов JMF о состоянии принтера<br>Примечание. Номер порта зависит от клиента, запрашивающего сигнал состояния JMF, или от возвращаемого сигнала JMF. |
| 7759 | sJMF | Входящее: получение защищенных команд JMF. |

### Узлы рабочего процесса

Компоненты рабочего процесса, которые получают или сохраняют файлы работ, могут использовать подключенные диски, файлы пути UNC, URI-идентификаторы HTTP, HTTPS и FTP. URI-идентификаторы поддерживают получение файлов работ, таких как MAX, JMF.

Примечание. Протоколы URI HTTP и FTP не поддерживают шифрование.

Для шифрования общих файловых ресурсов при их общем использовании применяется файловая система Windows. Для защиты общих файловых ресурсов используется контроль доступа к учетной записи пользователя Windows.

Примечание. При использовании функции контроля учетных записей пользуйтесь той же служебной учетной записью, что и при настройке раздела *«Установка дополнительного ПО»*. Дополнительные сведения приведены в *Руководстве по установке Xerox® FreeFlow® Core*.

**Табл. 3.8 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 139, 445 | SMB | Входящее: получение файлов, указанных в предустановке компонента рабочего процесса<br>Исходящее: сохранение файлов в общих каталогах. |
| 20, 21 | FTP | Исходящее: получение файлов, указанных в предустановке компонента рабочего процесса |

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 80 | HTTP | Исходящее: получение файлов, указанных в предустановке компонента рабочего процесса |
| 443 | HTTPS | Исходящее: получение файлов, указанных в предустановке компонента рабочего процесса |

### Печать Xerox® FreeFlow® Core

Xerox® FreeFlow® Core для определения типа DFE (цифровой препроцессор) использует нешифрованное подключение по протоколу SNMP и HTTP с командами IPP, JMF и XBDS. В строке сообщества SNMP для принтера/DFE должно стоять значение по умолчанию. Если значение по умолчанию в строке сообщества SNMP для принтера/DFE изменено, необходимо зарегистрировать обновленный параметр в FreeFlow Core. Убедитесь в том, что для всех принтеров, зарегистрированных в FreeFlow Core, используется одна и та же строка сообщества SNMP. Инструкции по обновлению строки сообщества SNMP см. в примечаниях к выпуску Xerox FreeFlow Core.

Нешифрованное подключение используется для следующих операций:

- получение списка очередей DFE;
- получение списка виртуальных принтеров на EFI DFE;
- получение возможностей принтера;
- операции работы в DFE;
- получение сведений об учете работы. Эта операция неприменима в случае JMF.
- Отправка работы печати на принтер с использованием LPR.

При подключении к DFE, на котором настроена поддержка защищенного протокола IPP, отправляемые данные печати шифруются. Включите защищенный протокол IPP с помощью опции Защищенная печать в настройках Назначение принтера. Для обмена данными между FreeFlow Core и DFE используются протоколы шифрования TLS и SHA256.

#### Включение защищенного протокола IPP для отправки работ на сервер печати FreeFlow

Чтобы включить защищенный протокол IPP для отправки работ на сервер печати FreeFlow, выполните следующее:

1. Добавьте сертификат TLS для сервера печати FreeFlow.
2. Выберите **Включить TLS** в окне настройки сервера печати Xerox® FreeFlow®.
3. Для получения сертификата TLS от сервера печати FreeFlow используйте утилиту Xerox® FreeFlow® Core Certificate.

Примечание. После успешной конфигурации IPP на экране появляется сообщение `об успешной установке сертификата`.

**Включение защищенного протокола IPP для отправки работ на контроллер Fiery**

Чтобы включить защищенный протокол IPP для отправки работ на контроллер Fiery, выполните следующее:

1. Для запуска пользовательского интерфейса Fiery введите в любом браузере IP-адрес Fiery.
2. В левой области выберите **Настройка Fiery**.
3. Введите реквизиты для входа в систему контроллера Fiery.
4. Выберите **Безопасность** и создайте самоподписанный сертификат или введите данные сертификата от CA.
5. На экране настройки включите **SSL\TLS**.
6. После включения SSL\TLS появится сообщение о перезагрузке контроллера.
7. Выберите **Да**.
8. Запустите **утилиту для настройки Core в Windows** в Xerox® FreeFlow® Core.
9. Перейдите на вкладку **Сертификат Core**, введите IP-адрес контроллера Fiery и выберите **Извлечь сертификат**.

   Появится сообщение `Сертификат успешно установлен`.
10. Настройте принтер в Xerox® FreeFlow® Core с опцией защищенной печати на экране Управление принтером.

Xerox® FreeFlow® Core не поддерживает связь с DFE через защищенный JMF.

**Табл. 3.9 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 161, 162 | SNMP v1/v2 | Исходящее: определение типа DFE при установке назначения принтера и извлечении сертификата. |
| 80 | HTTP | Входящее: JDF-принтер получает файл печати по протоколу HTTP.<br>Исходящее: определение типа DFE при установке назначения принтера и извлечении сертификата. |
| – | ICMP | Исходящее: проверка наличия устройства перед извлечением сертификата. |
| 631 | IPP v1.0/v1.1 | Исходящее: отправка работ на DFE, получение статуса работ и отправка команд работ на DFE. |
| 4004 | JMF | Входящее: Получение сообщений `ReturnQueueEntry` от принтера |

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| Порт 8010 или порт JMF, определенный принтером | JMF v1.3/v1.4 | Исходящее: идентификация типа DFE в процессе регистрации принтера и отправка работы на DFE. |
| 443 | HTTPS | Исходящее: связь принтера с DFE. |
| 515, 721–731 | LPR | Исходящее: Отправление запросов LPR на принтер с поддержкой LPD |

**Уведомления по электронной почте**

Xerox® FreeFlow® Core представляет собой почтовый клиент, подключаемый к доступному почтовому серверу SMTP или почтовому серверу Google. Пользователю предоставляется возможность шифрования уведомлений, отправляемых по эл. почте, с последующим подключением к почтовому серверу, поддерживающему шифрование. Протокол TLS обеспечивает шифрование подключения между службой уведомления и сервером SMTP.

Зашифрованные учетные данные хранятся локально.

**Табл. 3.10 Конфигурация брандмауэра**

| ПОРТ | ПРОТОКОЛ ИЛИ ПРИЛОЖЕНИЕ | ТИП ПОДКЛЮЧЕНИЯ БРАНДМАУЭРА |
|---|---|---|
| 25, 465, 587 | SMTP | Исходящее: Отправление уведомлений по электронной почте<br>Примечание. Номер порта и использование защищенного подключения зависят от конфигурации сервера SMTP. |

## Соответствие Федеральному стандарту по обработке информации (FIPS) и Генеральному регламенту о защите персональных данных (GDPR)

Xerox® FreeFlow® Core работает в операционной системе Windows, поддерживающей соответствие стандарту FIPS 140-2. Информацию о том, как обеспечить соответствие стандарту FIPS, см. в документации по Microsoft. По умолчанию FreeFlow Core запускается в режиме соответствия FIPS.

FreeFlow Core не поддерживает шифры DES/3DES.

Если требуется печать через защищенный протокол IPP с дайджест-аутентификацией, отключите режим соответствия FIPS, в результате чего FreeFlow Core перестанет соответствовать требованиям о криптографической защите.

FreeFlow Core соответствует Генеральному регламенту ЕС о защите персональных данных (GDPR)

# Общие сведения о защите

## ИДЕНТИФИКАЦИЯ СЛУЖЕБНОЙ УЧЕТНОЙ ЗАПИСИ, УТИЛИТ И ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ (CLI)

Служебные учетные записи FreeFlow Core, Утилиты и CLI теперь используют идентификациюWindows. Она осуществляется путем добавления служебной учетной записи или учетной записи пользователя, вошедшего в систему, в локальную группу Windows под названием FreeFlow Core Security. Дополнительную информацию см. в *примечаниях к выпуску ПО Xerox FreeFlow Core*.

## ЗАЩИТА ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ

### Защита документов и файлов

FreeFlow Core не производит явного шифрования файлов, переданных на обработку, до их сохранения в файловой системе ПК.

Документальные источники содержат персональную идентификационную информацию и другие конфиденциальные данные. Поэтому пользователь обязан обращаться с данной цифровой информацией, применяя наилучшие методы защиты информации.

### Персональная идентификационная информация

При регистрации лицензии на ПО FreeFlow Core происходит сбор персональной идентификационной информации (ПИИ). Собирается следующая информация:

- Название компании
- Ключ активации и серийный номер
- ID хоста / UUID системы
- Имя пользователя
- Адрес (улица, город, область, почтовый индекс, страна)
- Адрес электронной почты (необязательно)

Эта информация передается в защищенном виде на хост лицензирования Xerox.

Информация ПИИ, в частности адрес электронной почты пользователя, используемый для восстановления пароля, хранится в системе FreeFlow Core. Эта информация шифруется.

# Доступ учетных записей и хранение работ

### ПАРОЛИ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЯ

Допускается повторное использование пароля до 10 раз. Количество повторов для использования пароля можно настроить.

### БЛОКИРОВКА УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

В случае ошибки проверки подлинности с использованием Клиента Xerox FreeFlow Core, доступ пользователей блокируется после трех ошибочных попыток входа на период до 30 минут. Количество неудачных попыток входа в систему и период блокировки можно настроить.

### ВЫХОД ИЗ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

При отсутствии активности на протяжении 30 минут сеанс пользователей в системе Клиент Xerox® FreeFlow® Core автоматически прерывается. Продолжительность срока бездействия можно настроить.

### АКТИВНОСТЬ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

Журнал аудита данных о входе пользователя в систему FreeFlow Core находится в Журнале событий Windows, в разделе **Приложение** в папке **Журналы Windows**.

### УДЕРЖАНИЕ РАБОТ

Срок хранения работ в FreeFlow Core составляет 24 часа после завершения обработки.

Конфигурация принтера FreeFlow Core позволяет изменять срок хранения перед автоматическим удалением завершенных работ. По истечении 24 часов устройство FreeFlow Core удаляет завершенные работы.

Для удаления работ вручную следует использовать графический веб-интерфейс FreeFlow Core.

### СВОЙСТВА РАБОТ

Включает ограничение скачивания файлов в Свойства работ для работы, отображаемой в разделе Управление работами и статус работ в FreeFlow Core.

## Права учетных записей пользователя

Для конфигурации учетной записи службы Xerox® FreeFlow® Core можно использовать локальную учетную запись администратора или учетную запись без прав администратора. При использовании учетной записи члена локальной группы администраторов никаких специальных действий не требуется.

При использовании учетной записи без прав администратора требуются дополнительные права помимо прав стандартной группы пользователей. Настройка FreeFlow® Core автоматически предоставляет дополнительные права, как указано в следующей таблице:

| НАСТРОЙКА ПОЛИТИКИ ГРУППЫ | ПОСТОЯННОЕ ИМЯ |
|---|---|
| Работа в режиме операционной системы | SeTcbPrivilege |
| Настройка квот памяти для процесса | SeIncreaseQuotaPrivilege |
| Локальный вход в систему | SeInteractiveLogonRight |
| Создание резервных копий файлов и каталогов | SeBackupPrivilege |
| Создание маркерного объекта | SeCreateTokenPrivilege |
| Создание глобальных объектов | SeCreateGlobalPrivilege |
| Создание постоянных общих объектов | SeCreatePermanentPrivilege |
| Отладка программ | SeDebugPrivilege |
| Загрузка и выгрузка драйверов устройств | SeLoadDriverPrivilege |
| Вход в качестве пакетного задания | SeBatchLogonRight |
| Вход в качестве службы | SeServiceLogonRight |
| Управление журналом аудита и безопасности | SeSecurityPrivilege |
| Выполнение задач по обслуживанию томов | SeManageVolumePrivilege |
| Профилирование одного процесса | SeProfileSingleProcessPrivilege |
| Профилирование производительности системы | SeSystemProfilePrivilege |
| Замена маркера уровня процесса | SeAssignPrimaryTokenPrivilege |

Примечание. Права, приведенные в таблице, определены согласно https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-rights-assignment.

# Безопасность

Содержание этой главы:



В компании Xerox вопросы безопасности всегда стоят на первом плане. Как один из ведущих разработчиков в области цифровых технологий, компания Xerox несет обязательства по обеспечению надежности и безопасности цифровой информации, идентификации потенциально уязвимых мест и активному устранению проблем в целях ограничения рисков.

Компания Xerox стремится предоставлять максимально безопасный программный продукт на основе имеющейся информации и технологий, сохраняя характеристики продукта, стоимость, функциональность и производительность.

Компоненты программного решения Xerox® FreeFlow® Core оцениваются на предмет соответствия требованиям безопасности с использованием коммерчески доступных средств проверки на уязвимости и возможность проникновения. Уязвимости приложения устраняются по результатам проведенного нами тестирования.

Компания Xerox по мере необходимости выпускает бюллетени по вопросам безопасности. Бюллетень по вопросам безопасности публикуется на веб-сайте Xerox Security по адресу https://www.xerox.com/security где также можно ознакомиться с руководством по безопасности продуктов. На этом сайте содержится актуальная информация о потенциальных угрозах для принтера, технические описания, данные о сертификации Common Criteria, сведения об Intel Security McAfee и специальный портал, где можно задать специалистам компании Xerox вопросы, связанные с безопасностью.

## Антивирусная защита

В компании Xerox принимают особые меры, чтобы поставляемое ею программное обеспечение не содержало вирусов. Xerox рекомендует установить на сервере FreeFlow Core модули Anti-Virus Detection и End-Point Intrusion Detection and Prevention. Это ПО и операционная система обновляются актуальными патчами безопасности согласно рекомендациям соответствующих поставщиков.

Для повышения производительности рекомендуется исключить установочные каталоги Xerox® FreeFlow® Core и SQL Server из области проверки антивирусной программы.

Следующие файлы можно исключить из антивирусной проверки:

- <Установочный каталог FreeFlow Core>\Logs
- <Установочный каталог FreeFlow Core>\Platform\Logs
- <Установочный каталог FreeFlow Core>\JobSubmit\Logs
- <Установочный каталог FreeFlow Core>\Config
- <Установочный каталог FreeFlow Core>\Platform\Config
- <Каталог данных пользователя FreeFlow Core>\
- Папки, не входящие в каталог данных пользователя FreeFlow Core, используемые FreeFlow Core

# Обновление программного обеспечения

Компания Xerox не несет ответственность за состояние операционной системы, в которой работает ПО Xerox® FreeFlow® Core. Пользователь обязан поддерживать систему в обновленном состоянии и устанавливать соответствующие настройки и пакеты исправлений. Обновляйте систему Microsoft® Windows® не реже одного раза в месяц.

При обновлении Windows для установки обновлений пользуйтесь функцией **Центр обновления Windows**. Не рекомендуется устанавливать дополнительные предварительные обновления, поскольку они могут влиять на стабильность работы сервера Xerox® FreeFlow® Core.

Обновления для программы FreeFlow Core можно найти по адресу https://www.support.xerox.com/support/core/software/enus.html. Пользователи могут устанавливать обновления программного обеспечения самостоятельно.

# Дополнительные сведения и ресурсы

### Безопасность @ Xerox

Компания Xerox ведет актуальную общедоступную веб-страницу, где содержится самая последняя информация о безопасности ее продуктов. См. www.xerox.com/security.

### Ответы на известные уязвимости

Компанией Xerox создан документ, в котором подробно описана Политика управления уязвимостями и раскрытия информации Xerox, используемая для обнаружения и устранения уязвимостей в программном и аппаратном обеспечении Xerox. Этот документ можно скачать на странице: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

### Дополнительные ресурсы

| РЕСУРС БЕЗОПАСНОСТИ | URL |
|---|---|
| Часто задаваемые вопросы о безопасности | www.xerox.com/en-us/information-security/frequently-asked-questions |
| Бюллетени, информационные сообщения и обновления системы безопасности | www.xerox.com/security |
| Архив новостей о безопасности | security.business.xerox.com/en-us/news/ |
| Центр доверия Xerox | https://trust.corp.xerox.com/ |