Удаленное обслуживание в Xerox

Информационный документ по безопасности

Версия 4.0

Март 2022

IS 614672/IS 514590

Оглавление

1. Общее применение и целевая аудитория 1-4

2. Ценностное предложение 2-4

3. Удаленное обслуживание 3-5

4. Модели развертывания 4-6

Комбинированная модель развертывания (предпочтительная) 4-7

Модель развертывания Device Direct 4-8

Модель развертывания приложения для управления устройствами 4-9

5. Передача данных и полезные данные 5-10

Источники данных 5-10

Офисные устройства Xerox® 5-10

Производственные устройства Xerox® 5-11

Приложения для управления устройствами Xerox® 5-12

6. Удаленное управление устройствами печати 6-15

Системные требования приложений для управления устройствами 6-16

7. Бизнес-процессы и услуги Xerox® 7-18

8. Сведения о технологии 8-19

Разработка программного обеспечения 8-19

Удобство эксплуатации 8-19

9. Функции безопасности 9-24

Простой протокол управления сетью (SNMP) для Xerox® 9-24

10. Влияние на сеть 10-27

Протоколы, порты и другие сопутствующие технологии 10-27

11. Рекомендации по безопасности 11-29

1. Общее применение и целевая аудитория

Информационный документ по безопасности «Удаленное обслуживание в Xerox» предоставляется в помощь клиентам для того, чтобы они могли разобраться и использовать безопасное решение для удаленных служб, которое лучше всего подходит для их сетевой структуры и политики информационной безопасности. Для обеспечения наиболее безопасного метода конфигурации следует учитывать, что могут потребоваться изменения в брандмауэре подключения к интернету клиента, прокси-серверах или другой сетевой инфраструктуре, имеющей отношение к безопасности.

К целевой аудитории данного документа относятся поставщики технологий, администраторы сети и специалисты по сетевой безопасности, заинтересованные в возможностях удаленных служб и реализации этих функций в целях безопасности.

Рекомендуем изучить документ полностью, чтобы удостовериться в использовании продуктов и услуг Xerox® в сетевой среде клиента.

2. Ценностное предложение

Мы предлагаем безопасный и надежный способ отправки данных об устройстве в нашу систему, сертифицированную по ISO для автоматизации общих задач и улучшения качества обслуживания и поддержки.

- Считывание показаний счетчиков для отчетности отличается точностью и производится автоматически.
- Автоматизированная программа пополнения расходных материалов обеспечивает подачу тонера на основе данных об уровне тонера в принтере, поэтому не нужно отслеживать наличие запасов или запрашивать расходные материалы.
- Отправка диагностических сведений позволяет нам оказывать поддержку вашего устройства на лучшем уровне, часто обеспечивая более быстрое устранение неполадок.
- Для некоторых моделей принтеров может быть предусмотрена проверка наличия важных обновлений программного обеспечения и установление обновлений программно, без вмешательства клиента.См. примечание
- Наши возможности по предоставлению услуг удаленного управления позволяют управлять принтерами как от Xerox, так и от других производителей.
- Благодаря этим услугам наши клиенты могут более эффективно распоряжаться своим временем.

Все вышеописанные услуги предоставляются с учетом требований безопасности.

Примечание: Эту опцию можно отключить для сред, в которых клиенты сертифицируют установленную версию программного обеспечения и хотят контролировать программное обеспечение принтеров при появлении обновлений. Это можно сделать, не отключая остальные возможности удаленных служб.

3. Удаленное обслуживание

Все ресурсы организации, включая сетевые многофункциональные устройства печати (МФУ), первостепенное значение придают безопасности, а ключевой фактор для них – сведения. На сегодня с управлением сетью многофункциональных устройств печати при обеспечении достаточного уровня безопасности связан комплекс уникальных задач, которые часто упускают из виду. Мы осознаем сложность этих задач и учитываем потребности наших клиентов в обеспечении безопасности. Продукция Xerox®, системы Xerox® и предложения удаленных служб разработаны таким образом, чтобы надежно интегрироваться в существующие рабочие процессы наших клиентов, используя при этом новейшие защищенные технологии.

По умолчанию на наши серверы не передают изображения клиентов, полученные в результате печати, факса, сканирования, копирования, а также другая конфиденциальная информация.

Серверы Xerox в США соответствуют строгим требованиям безопасности в отношении управления информационной безопасностью. Наши центры обработки данных и приложения для удаленных служб поддерживают ежегодное соответствие Положению о стандартах для заданий по аттестации (SSA) №16, закона Сарбейнса-Оксли (SOX) и сертифицированы по ISO 27001:2013.

4. Модели развертывания

Клиентам доступна для выбора одна из следующих одинаково безопасных моделей развертывания удаленных служб Xerox®:

- **Комбинированная модель – *(предпочтительная)*** Идеальный вариант – совместное использование функции Device Direct и приложения для управления устройствами, чем обеспечивается наиболее надежный набор данных и возможность управления устройствами.

- **Модель Device Direct** – Device Direct позволяет устройствам печати напрямую связываться с удаленными коммуникационными серверами Xerox® по интернету через брандмауэр клиента для поддержки автоматического пополнения расходных материалов (ASR), автоматического считывания показаний счетчиков (AMR) и создания отчетов о диагностике устройства. Эта модель развертывания предоставляет набор элементов данных со стандартными полезными данными, включающими такие, как неисправности устройства, предупреждения, счетчики, требующие частого техобслуживания детали (HFSI) и другие параметры устройства печати.

- **Модель приложения управления устройствами** — Xerox® Приложения для управления устройствами могут быть развернуты в сети клиента для того, чтобы собрать набор параметров данных с устройств печати для поддержки автоматического пополнения расходных материалов (ASR), автоматического считывания показаний счетчиков (AMR) и создания отчетов о диагностике устройства. Параметры устройств печати собираются и затем безопасным путем передаются на удаленные серверы Xerox. При использовании этой модели развертывания могут передаваться параметры данных с устройств печати как компании Xerox, так и параметры данных с устройств печати других производителей.

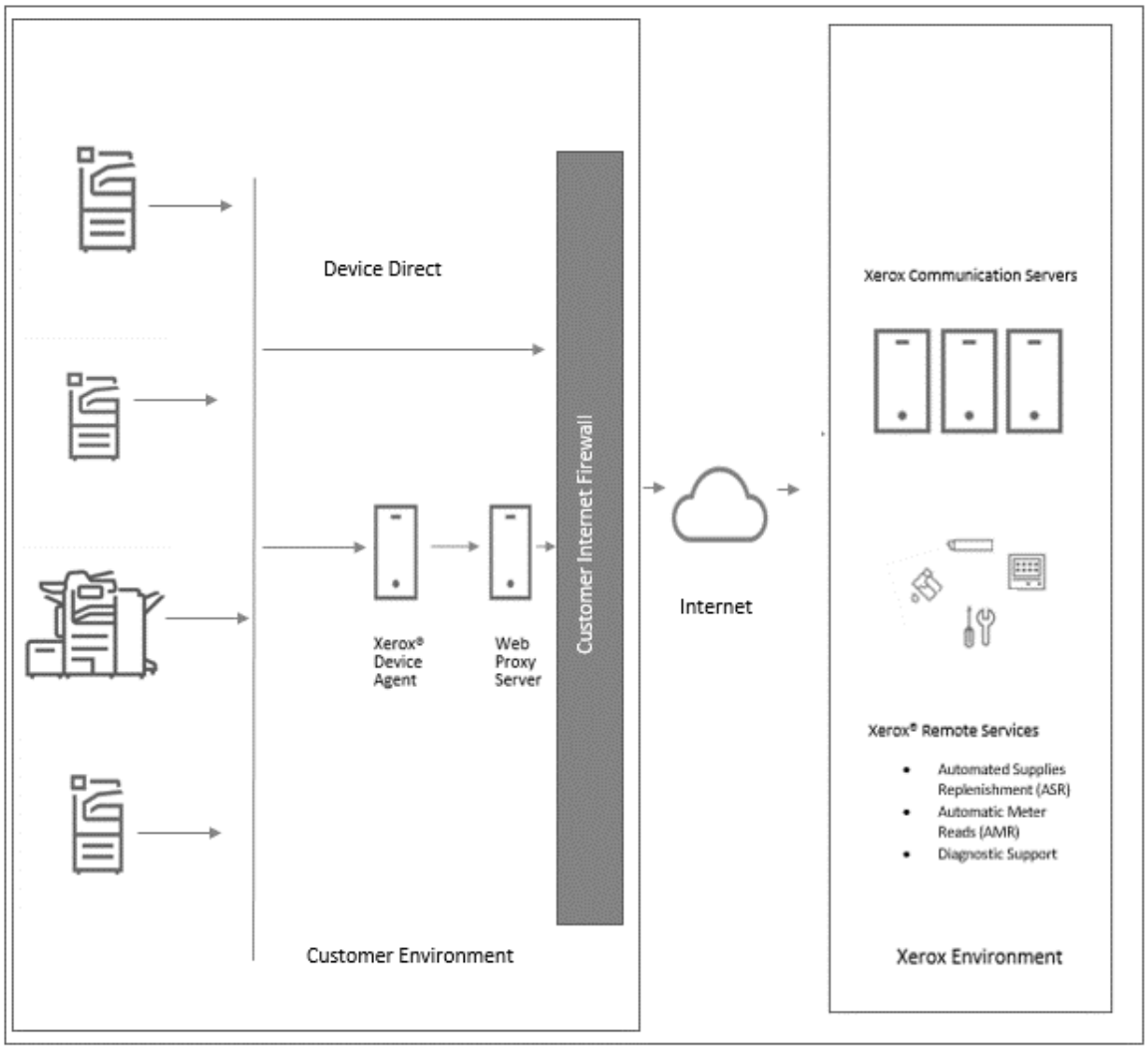
Все модели развертывания удаленных служб Xerox® одинаково безопасны и используют новейшие отраслевые веб-протоколы и порты для создания защищенного, зашифрованного канала при передаче параметров устройств печати на удаленные серверы Xerox, расположенные в наших защищенных центрах обработки данных с резервированием.

Выбор модели развертывания зависит от типа решения наших клиентов по предоставлению услуг печати, политики информационной безопасности и правил передачи параметров данных устройств печати.

Комбинированная модель развертывания (предпочтительная)

Комбинированная модель развертывания применяется в том случае, если клиент приобретает несколько типов соглашений о техническом обслуживании Xerox для своих устройств печати и для достижения более надежного решения по удаленным службам. Когда устройство печати Xerox® устанавливается в сети впервые, Xerox использует удаленные службы по умолчанию для того, чтобы устройство печати автоматически пыталось установить связь с нашими коммуникационными серверами, используя безопасный метод аутентифицированного соединения.

Рис. 1



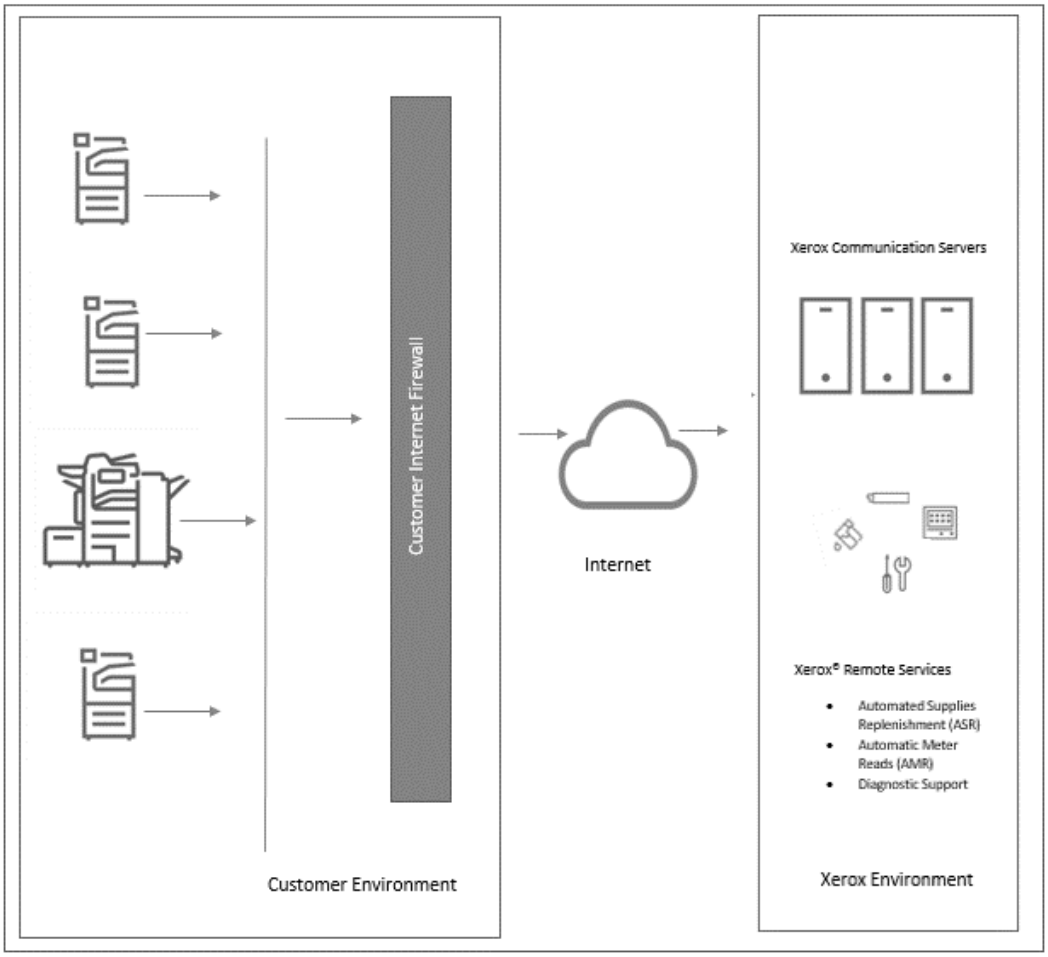
Combination Deployment Model

Модель развертывания Device Direct

Устройства Xerox® с поддержкой удаленного обслуживания используют соединение по протоколу защиты транспортного уровня (TLS) 1.2 через защищенный стандартный порт 443 для внешнего обмена данными с нашими защищенными серверами.

- Устройства печати из среды клиента инициируют все соединения с коммуникационными серверами. Для того, чтобы выполнить соединение требуется использовать стандартную конфигурацию брандмауэра на сайте.
- Для аутентификации устройств печати в инфраструктуре Xerox необходимо использовать действительный URL-адрес коммуникационных серверов (*.xerox.support.com).
- Устройство запрашивает регистрацию на коммуникационных серверах, используя соответствующие учетные данные для проверки подлинности сертификата.
- Коммуникационные серверы проверяют учетные данные, предоставленные устройствами печати, и принимают запросы.
- Коммуникационные серверы защищены безопасным брандмауэром и недоступны из интернета.

Рис. 2



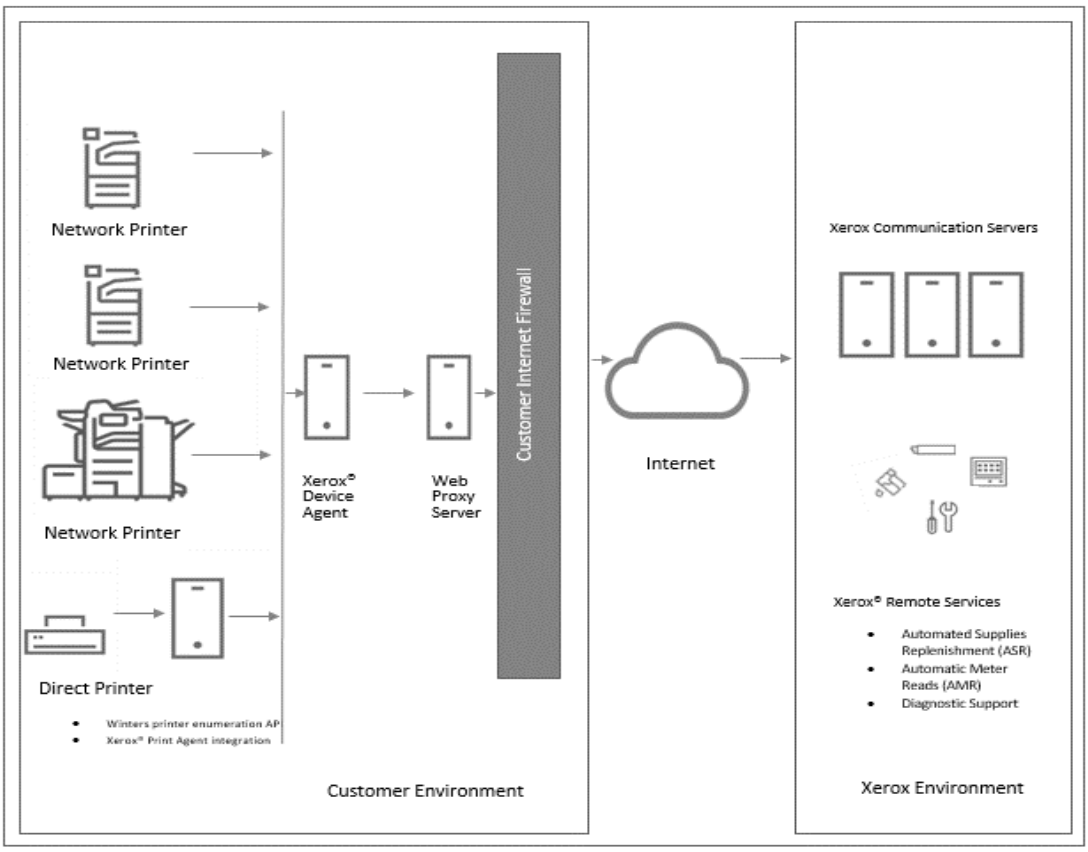
Device Direct Deployment Model

Модель развертывания приложения для управления устройствами

Приложения для управления устройствами (т. е. **Xerox Centre Ware® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition и Xerox Device Manager**) используют подключение по протоколу защиты транспортного уровня (TLS) 1.2 через защищенный стандартный порт 443 для внешнего обмена данными с коммуникационными серверами. Для улучшения безопасности этого канала используются дополнительные функции, которые устанавливаются во время первой установки приложений для управления устройствами:

- Приложение для управления устройствами из среды клиента инициирует все соединения с коммуникационными серверами. Для того, чтобы выполнить соединение, требуется использовать стандартную конфигурацию брандмауэра на сайте.
- Коммуникационные серверы защищены безопасным брандмауэром и недоступны из интернета.
- Приложение для управления устройствами запрашивает регистрацию на удаленных серверах, используя соответствующие учетные данные для проверки подлинности сертификата.
- Коммуникационные серверы проверяют учетные данные, предоставленные устройствами печати, и принимают запросы.
- Приложение для управления устройствами аутентифицирует коммуникационные серверы и активирует службу.

Рисунок 3



Device Management Application Deployment Model

5. Передача данных и полезные данные

Источники данных

Параметры данных устройства печати, которые отправляются в составе передаваемых полезных данных, поступают из следующих источников:

- Офисные сетевые принтеры Xerox®
- Сетевые принтеры других производителей
- Производственные принтеры Xerox®
- Приложения для управления устройствами Xerox®

Примечание: Не все офисные и производственные принтеры Xerox поддерживают удаленное обслуживание Xerox. Полный список продуктов, поддерживающих удаленное обслуживание, можно найти здесь. Параметры устройства печати зависят от продукта и решения по развертыванию удаленных служб Xerox®.

Офисные устройства Xerox®

В **таблице 1** указаны параметры данных устройства, которые могут быть переданы для офисных продуктов Xerox® с поддержкой удаленного обслуживания.

Параметры данных	Подробное описание параметров данных
Идентификатор устройства печати	Указывается модель, уровни микропрограммного обеспечения модуля, серийные номера модулей, даты установки модулей, данные о лицензировании и местоположение, если такие имеются.
Сетевой адрес устройства печати	Указывается адрес управления доступом к среде (MAC), адрес подсети.
Свойства устройства печати	Указывается подробная конфигурация аппаратных компонентов, подробная конфигурация программного модуля, поддерживаемые функции/службы и другое.
Состояние устройства печати	Указываются активные состояния, счетчик случаев неисправностей, журнал регистрации передачи потока данных (DFE), история передачи данных.
Счетчики устройств печати	Указываются показания счетчиков для отчетности, счетчики печати, счетчики копирования, счетчики выполнения больших заданий, счетчики, связанные со спецификой производства, счетчики области сканирования на низкопроизводительных моделях и другое.
Расходные материалы для устройств печати	Указывается изготовитель, модель, серийный номер, название, тип, уровень, вместимость, статус, счетчики срока службы и другое.
Подробные сведения об использовании устройства печати	Указываются данные о требующих частого техобслуживания деталях (HFSI), данные об энергонезависимой памяти (NVM), о замене деталей, журналы передачи потока данных (DFE), подробные диагностические данные, устранение неисправностей.
Проектиро-вание / отладка	Указываются неструктурированные, подробные данные, связанные с отладкой, предназначенные только для использования службой поддержки 3-го уровня.

Параметры данных	Подробное описание параметров данных
Данные, связанные с профессио-нальной деятельностью клиента	Производственные печатные устройства Xerox® воспроизводят данные, связанные с профессиональной деятельностью клиента, для реализации расширенных сценариев поддержки через зашифрованный язык PostScript в Xerox. Клиент сам решает активировать эту функцию или нет. Если клиент решает передать данные, связанные с профессиональной деятельностью (т. е. зашифрованный PostScript), обратно в Xerox, эти данные обрабатываются в соответствии с политиками и стандартами обеспечения информационной безопасности (IS) компании Xerox.

Наши устройства печати офисного класса передают параметры данных устройства в формате расширяемого языка разметки (XML) в виде сжатого файла .zip. После аутентификации каждый файл передается по зашифрованному каналу на коммуникационные серверы.

Производственные устройства Xerox®

В **таблице 2** указаны параметры данных устройства, которые могут быть переданы для производственных продуктов Xerox® с поддержкой удаленного обслуживания.

	Описание
Идентификатор устройства печати	Указывается модель, уровень микропрограммного обеспечения, серийные номера модулей, дату установки модулей.
Сетевой адрес устройства печати	Указывается адрес управления доступом к среде (MAC), адрес подсети.
Свойства устройства печати	Указывается подробная конфигурация аппаратных компонентов, подробная конфигурация программного модуля, поддерживаемые функции/службы, режимы энергосбережения и другое.
Состояние устройства печати	Указывается общее состояние, подробные данные об оповещениях, историю последних 40 случаев неисправностей, данные о случаях замятия и другое.
Счетчики устройств печати	Указываются показания счетчиков для отчетности, счетчики печати, счетчики копирования, счетчики факсимильных копий, счетчики выполнения больших заданий, счетчики области сканирования, статистика использования и другое.
Расходные материалы для устройств печати	Указывается название расходного материала, тип (например, для обработки изображений, финишной обработки, для бумажного носителя), уровень, вместимость, состояние, размер и другое.
Подробные сведения об использовании устройства печати	Указываются подробные счетчики печати, состояния включения питания, подробные сведения о количестве заменяемых клиентом блоков (CRU), подробные сведения о неисправностях и распределениях CRU, использование встроенной функции оптического распознавания символов (OCR), определение размера тиража, определение использования лотка для бумаги, установленные носители, определение типов носителей, определение размеров носителей, определение длины документа, количество наборов, данные о требующих частого техобслуживания деталях (HFSI), данные об энергонезависимой памяти (NVM), распечатка, количество отмеченных пикселей, средний уровень покрытия области по цветам, неисправности/замятия, подробные счетчики сканирования.
Проектирование / отладка	Указываются подробные сведения об отладке, которые могут содержать сведения, не входящие в вышеперечисленный набор данных. Эти данные могут содержать персональные данные (PII), такие как имена пользователей, адреса электронной почты и данные о работе. Эти данные отправляются только с разрешения клиента и предназначены исключительно для расширенной поддержки при устранении неполадок.

Наши устройства производственного класса передают параметры данных устройства в формате расширяемого языка разметки (XML) в виде сжатого файла .zip. После аутентификации каждый файл передается по зашифрованному каналу на серверы удаленных служб.

Примечание: Файл и содержимое идентифицированных данных зависят от модели продукта.

Приложения для управления устройствами Xerox®

В зависимости от сетевой среды клиента и потребностей в управлении устройствами печати предусмотрено несколько вариантов приложений для управления устройствами. Каждый из них в одинаковой мере безопасен и осуществляет защищенное управления устройствами печати.

Ниже приведен список приложений для управления устройствами: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition и Xerox Device Manager.

Каждое приложение по умолчанию по меньшей мере ежедневно синхронизируется с серверами защищенной связи. Чтобы обеспечить максимальную безопасность ваших данных, коммуникационные серверы размещены в помещении, соответствующем требованиям ISO 27001. Отправляемые данные представляют собой в основном показания счетчиков для счетов, уровни расходных материалов и оповещения принтеров. Данные отправляются в сжатом, зашифрованном и защищенном несколькими механизмами виде:

- Приложение для управления устройствами Xerox инициирует все соединения с коммуникационными серверами Xerox, и для того, чтобы выполнить соединение, требуется использовать стандартную конфигурацию брандмауэра в среде клиента.
- Приложения для управления устройствами Xerox требуют наличия действующего прокси-сервера, если для связи через интернет необходим прокси-сервер.
- Коммуникационные серверы защищены брандмауэром и доступны из интернета.
- Чтобы получить доступ к пользовательскому интерфейсу коммуникационного сервера Xerox, необходимо выполнить аутентификацию. Сведения о хосте приложения для управления устройствами Xerox хранятся в учетной записи на сайте клиента, и доступ к данным учетной записи в коммуникационных серверах Xerox ограничен менеджерами учетных записей коммуникационных серверов Xerox.
- Все коммуникации коммуникационного сервера Xerox регистрируются и доступны для просмотра.
- Данные, отправляемые на ваши сетевые устройства печати, когда они включены, состоят в основном из удаленных команд, которые позволяют администратору поддержки учетной записи во время реализации расширенных сценариев поддержки запрашивать выполнение команд на уровне приложения для управления устройствами Xerox.
- Запросы в основном касаются обновления микропрограммного обеспечения, перезагрузки принтера, печати тестовой страницы и обновления текущего состояния устройства.
- Приложение для управления устройствами Xerox периодически проверяет учетную запись коммуникационных серверов Xerox на наличие командных запросов.
- Результаты операций по командным запросам отправляются на коммуникационные серверы Xerox, где они далее проверяются.

Примечание: Во время установки программного обеспечения требуется однократная регистрация. Эта регистрационная информация содержит поле для указания местоположения устройства и контактной адрес электронной почты.

Приложения для управления устройствами Xerox **(т.е. Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition и Xerox Device Manager)** передают данные параметров печати в формате расширяемого языка разметки (XML) в виде сжатого файла .zip. Затем файл передается по зашифрованным каналам на коммуникационные серверы.

В **таблице 3** указан список параметров данных устройства и описание, которые можно отправить через приложение Xerox® Device Mgmt..

Параметры данных	Подробное описание параметров данных
Идентификатор устройства печати	Указывается изготовитель, модель, описание, уровень микропрограммного обеспечения, серийный номер, инвентарные номера, название системы, контакт, местоположение, состояние управления рабочим местом (рабочим столом), номер телефона/факса и название очереди.
Сетевой адрес устройства печати	Указывается MAC-адрес, IP-адрес, DNS-имя, маска подсети, шлюз по умолчанию IP, последний известный IP-адрес, измененный IP-адрес, часовой пояс, IPX-адрес, номер внешней сети IPX, сервер печати IPX.
Свойства устройства печати	Указываются установленные компоненты, описания компонентов, поддерживаемые функции/службы, скорость печати, поддержка цветов, параметры финишной обработки, поддержка двусторонней печати, технология маркировки, жесткий диск, оперативная память, языковая поддержка, пользовательские свойства.
Состояние устройства печати	Указывается общее состояние, подробные данные, сообщения локальной консоли, состояние компонента, данные извлечения статуса, дата поиска и выявления, метод/тип обнаружения, время безотказной работы устройства, поддерживаемые/включенные функции увеличения и наложения объектов или областей друг на друга.
Счетчики устройства печати	Указывается показания счетчиков для отчетности, счетчики печати, счетчики копирования, счетчики факсимильных копий, счетчики выполнения больших заданий, счетчики области сканирования, статистика использования и целевой объем.
Расходные материалы для устройств печати	Указывается название расходного материала, тип (например, для обработки изображений, финишной обработки, для бумажного носителя), уровень, вместимость, состояние, размер и сопутствующие параметры
Подробное описание использования устройства печати	Данные отслеживания заданий на основе сведений пользователя, к которым относятся характеристики задания (идентификатор, имя документа, владелец, тип документа, тип задания, цвет, двусторонняя печать, требуемый носитель, размер, страницы, наборы, ошибки), целевое назначение (устройство печати, модель, DNS-имя, IP-адрес, MAC-адрес, серийный номер), результаты печати задания (время отправки, время печати задания, напечатанные страницы, цветные/черно-белые страницы, используемый цветной режим, печать нескольких страниц на одном листе), учетные данные (код возврата платежа, цена возврата, источник учета), источник задания печати (рабочее место, название/MAC-адрес сервера печати, название очереди, порт, имя пользователя, идентификатор пользователя), данные управления Xerox (отправляются в Xerox Services Manager).
Идентификац-ионные данные управления устройством	Указываются сведения о главном ПК приложения, такие как DNS-имя, IP-адрес, имя ОС, тип ОС, процессор ПК, объем оперативной памяти (свободной и используемой), объем жесткого диска (свободного и используемого), имя сайта, версия приложения, дата истечения срока действия лицензии приложения, версия .Net, часовой пояс, версия компонента обнаружения, размер основной базы данных, размер базы данных обнаружения, количество принтеров/в зоне действия/не в зоне действия, запущенные важные службы.

Параметры данных	Подробное описание параметров данных
Диспетчер устройств Режим корпоративной безопасности	Обычный режим = приложение Xerox Device Agent связывается с Xerox Services Manager, ежедневно. Настройки могут быть изменены удаленно без необходимости выезда на место, даже при отключенном графике опроса. Режим блокировки = кроме синхронизации сведений о принтере, связь с приложением Xerox Services Manager отсутствует, и настройки необходимо изменять на месте. IP-адреса оборудования и принтера Xerox Device Agent передаются приложению Xerox Services Manager.
Управление устройствами и политика контроля печати	Указывается имя ПК конечного пользователя, используемый сервер печати, используемая очередь печати, метка времени неисполнения, имя документа, имя конечного пользователя, задание двухсторонней печати, цвет задания, общее количество оттисков задания, стоимость задания, предпринятые действия, уведомление конечного пользователя, отображаемое сообщение, название политики печати, правило политики печати.

6. Удаленное управление устройствами печати

Персонал расширенной поддержки Xerox может выполнять следующие действия через устройство напрямую или через приложение для управления устройствами Xerox.

В таблице 4 показаны дополнительные действия по решению проблемы, на выполнение которых клиент дал разрешение в сценарии расширенной поддержки. Разрешение клиента на выполнение этих функций должно быть получено в обязательном порядке.

Данные	Описание
Действия, выполняемые на устройствах печати	• Получить состояние устройства = получить последнее состояние с устройства печати • Перезагрузить устройство = выполнить последовательность выключения/включения питания на устройстве печати. • Обновить устройство = установить новое программное обеспечение/ микропрограмму на устройство печати (файл.DLM через порт 9100) • Устранить неполадки устройства = пропинговать устройство + получить последнее состояние с устройства печати • Печать тестовой страницы = отправка тестового задания на устройство печати для проверки маршрута печати (создание отчета о конфигурации) • Начать управление устройством = выполнять периодическую передачу данных устройства печати на внешние коммуникационные серверы Xerox®. **Примечание: Каждое действие можно отключить от использования по запросу в административной части конфигурации приложений для управления устройствами Xerox®, которые поддерживают эту функцию.**
Действия, выполняемые в приложениях для управления устройствами	К параметрам каждого приложения для управления устройствами, которыми можно управлять, относятся: операция обнаружения, частота экспорта данных, параметры связи по протоколу SNMP (повторные попытки, время ожидания, имена сообществ), профили оповещений и частота обновления программного обеспечения приложения для автоматического управления устройством.
Удаленное управление программным обеспечением	У некоторых устройств предусмотрена возможность автоматического удаленного управления программным обеспечением. Эти устройства отправляют запрос в среду Xerox, чтобы проверить наличие новых обновлений программного обеспечения для данного устройства. Если таковые имеются, устройство сможет отправить запрос на обновление программного обеспечения, и оно будет обновлено в назначенное время. Однако если в вашей среде запрещено автоматическое обновление программного обеспечения, опция удаленного управления программным обеспечением может быть отменена только без прерывания работы стандартных удаленных служб.

Системные требования приложений для управления устройствами

Минимальные требования несколько отличаются в зависимости от предложений. См. руководство пользователя, руководство по оценке безопасности и/или руководство по сертификации для получения информации об основных требованиях к соответствующим приложениям для управления устройствами.

При установке прилагается файл readme, в котором рассматриваются дополнительные и особые системные требования для соответствующего устанавливаемого приложения для управления устройствами.

- Приложения для управления устройствами совместимы с функциями безопасности, встроенными в операционную систему Windows®. Они основаны на фоновой службе Windows®, работающей под учетными данными локальной системной учетной записи, чтобы обеспечить превентивный мониторинг принтеров и полезные данные параметров печати, которые будут передаваться в Xerox. Пользовательский интерфейс, отображающий полезные данные параметров печати, доступен только для опытных пользователей и администраторов, имеющих доступ к ОС Windows®.

- Для предотвращения прерывания автоматической связи с удаленными службами рекомендуется, чтобы приложение для управления устройствами было загружено на компьютер, который включен постоянно или в основное рабочее время.

- Рекомендуется установить на хост-компьютеры поддерживаемую операционную систему корпорации Microsoft®. Однако приложения для управления устройствами Xerox могут быть запущены на операционной системе Apple® версии 10.9.4 или более поздней версии с помощью программы для эмуляции Parallels Desktop. Приложение не запустится в исходной среде Macintosh. Подробнее о поддержке см. в соответствующих руководствах пользователя. Там можно найти требования для запуска в операционной системе Macintosh.

- Рекомендуется установить на хост-компьютеры последние критические исправления и наборы обновлений от корпорации Microsoft®.

- Необходимо загрузить и проверить на работоспособность сетевой протокол управления передачей/интернет-протокол (TCP/IP).

- Для установки прикладного программного обеспечения управления устройствами на клиентском оборудовании необходимо обладать правами администратора.

- Необходимы устройства с поддержкой протокола SNMP и возможность маршрутизации протокола SNMP по сети. Не требуется включать протокол SNMP на компьютере, на котором будут установлены приложения для управления устройствами Xerox®, или на других сетевых компьютерах.

- Перед установкой приложения необходимо установить Microsoft®.NET Framework.

- Приложение не следует устанавливать на компьютер, на котором установлены другие приложения на основе протокола SNMP или другие инструменты управления печатью Xerox®, так как они могут мешать работе друг друга.

Конфигурации базы данных

- Приложение устанавливает механизм базы данных SQL Server Compact Edition (SQL CE) и файлы базы данных, в которых хранятся данные принтера и параметры приложения в каталоге установки. Лицензирование базы данных для приложения не требуется. Xerox® Device Agent также поддерживает существующие экземпляры SQL Server, как описано выше.

Неподдерживаемые конфигурации

В этом разделе описаны конфигурации, которые не поддерживаются.

- Установка приложения на компьютер с другим приложением для управления устройствами Xerox, например Xerox Device Manager.

- Встроенное программное обеспечение операционной системы Mac OS® (т. е. Xerox Device Agent может работать на платформе Apple Mac только при установленном программном обеспечении эмуляции Parallels).

- Любые версии операционных систем UNIX®, операционные системы Linux®, системы Windows® управляются через клиент Novell, а операционные системы Windows® 7, Windows® XP, Windows® Vista, Windows NT®4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 и 2008 R2, Windows® Server 2003, Windows® 8 RT управляются через службы терминалов для приложений, а установка на системы Windows выполняется через контроллеры домена.

Поскольку данное приложение было протестировано только в среде VMware® Lab Manager/рабочем месте, другие виртуальные среды не поддерживаются.

7. Бизнес-процессы и услуги Xerox®

Данные, полученные от устройств офисной печати Xerox®, устройств производственной печати Xerox® и приложений для управления устройствами Xerox в рамках решения удаленного обслуживания, используются для перечисленных ниже бизнес-процессы Xerox:

В таблице 5 приведены названия и описание бизнес-процессов и услуг, которые поддерживаются в рамках решения удаленного обслуживания.

Название бизнес-процесса	Описание
Автоматическое считывание показаний счетчика	Данные о показаниях счетчиков используются в процессе выставления счетов.
Автоматическое пополнение расходных материалов / автоматическое пополнение запчастей	Тонер автоматически отправляется клиентам на основании данных об исчерпании расходных материалов, полученных от печатающих устройств. Некоторые сменные компоненты автоматически отправляются клиентам, когда они необходимы для их печатных устройств. Эти опции доступны только для тех клиентов, которые выбирают контракты на дозированное снабжение.
Удобство обслуживания (помощник по обслуживанию)	Удаленное управление устройством предоставляет подробные сведения о неисправностях, которые при необходимости может просмотреть обслуживающий персонал Xerox, чтобы ускорить подготовку к визиту на место или диагностику и устранение проблем.
Поддержка третьего уровня (проектирование/отладка)	Сотрудники службы поддержки могут отлаживать сложные неполадки, если им предоставляется доступ к подробным инженерным и отладочным журналам.
Разработка продукта	Данные о производительности и использовании принтера применяют для определения улучшений продукта для будущих версий.

Основные данные устройства печати собираются, передаются, сохраняются и архивируются в центре обработки данных Xerox, сертифицированном по стандарту ISO-27001, и хранятся в соответствии с политиками хранения корпоративных данных Xerox.

Рабочие процессы и практики, обеспечивающие поддержку и защиту программных систем удаленного обслуживания, основаны на передовом опыте ITIL и политиках информационной безопасности Xerox, которые полностью соответствуют стандартам системы управления информационной безопасностью ISO 27002 Международной организации по стандартизации. Клиенты могут рассчитывать на то, что управление, защита и хранение данных устройств соответствует основным принципам информационной безопасности: конфиденциальности, целостности, доступности, аутентификации и невозможности отказа.

8. Сведения о технологии

В этом разделе представлены дополнительные сведения о технологии, которые обычно требуются специалистам по информационным технологиям (ИТ) и специалистам по безопасности, которые управляют рисками, получая гарантии безопасной практики разработки. Такие гарантии позволяют им сертифицировать наши устройства печати и приложения для управления устройствами для использования в сетевой среде клиента.

Разработка программного обеспечения

Наши обязательства по обеспечению безопасности продукции Xerox начинаются на ранних этапах разработки продукции, где разработчики Xerox следуют формальному жизненному циклу разработки средств обеспечения безопасности, который решает проблемы безопасности путем идентификации, анализа, определения приоритетов, кодирования и тестирования. Многие устройства печати Xerox® сертифицированы по стандарту Common Criteria ISO IEC 15408 или в настоящее время активно проходят сертификацию.

Удобство эксплуатации

Удаленные службы Xerox выполняют следующие типы операций в сети. Эти операции зависят от настроенного метода развертывания.

Таблица 6.

Метод развертывания	Используемое приложение	Информационный поток в сети	Удобство эксплуатации сети
Функция Device Direct	Нет	Внутренний	Устройство печати Xerox® пытается обнаружить веб-прокси-сервер (автоматически или направляется на определенный адрес)
		Внутренний	Устройства печати Xerox® можно запрограммировать на создание запросов к серверу Simple Mail Transport Protocol (SMTP) для отправки предупреждающих сообщений по электронной почте определенному списку получателей.
		Внешний по отношению к сети	Устройства печати Xerox® преодолевает брандмауэр компании для доступа в интернет (HTTPS через порт 443)
		Внешний по отношению к сети	Устройства печати Xerox® аутентифицируется с помощью своего сертификата на удаленном сервере коммуникационном сервере Xerox перед передачей любых параметров данных
		Внешний по отношению к сети	Устройства печати Xerox® автоматически передает данные параметров устройств печати по зашифрованному каналу (HTTPS через порт 443) на коммуникационные серверы Xerox® в определенное время ежедневно или по запросу клиента.

Метод развертывания	Используемое приложение	Информационный поток в сети	Удобство эксплуатации сети
		Внешний по отношению к сети	Устройство печати Xerox® автоматически отправляет запросы к коммуникационным серверам Xerox® по зашифрованному каналу (HTTPS через порт 443) в определенное время каждый день для получения списка действий, которые необходимо выполнить (например, отправить данные для выставления счетов сейчас, добавить услугу и другое).
		Внешний по отношению к сети	Односторонняя передача по требованию данных журнала работ по проектированию устройства печати Xerox® по зашифрованному каналу (HTTPS через порт 443) на коммуникационный сервер Xerox®
Функция Device Direct	Нет	Исходящий, инициированный разработчиком для получения последнего программного обеспечения	Устройство отправляет запрос на удаленный сервер управления программным обеспечением для проверки наличия обновлений программного обеспечения / безопасности. Если среда клиента запрещает автоматическое обновление программного обеспечения, опция удаленного управления программным обеспечением может быть отменена только без прерывания стандартных удаленных служб.
Приложения для управления устройствами	Centre Ware® Web	Внутренний	Каждое приложение обнаруживает веб-прокси-сервер (автоматически или направляется на определенный адрес)
		Внутренний	Каждое приложение получает данные о возможностях устройств печати по всей сети через протокол SNMP
		Внутренний	Каждое приложение получает конфигурацию устройств печати по всей сети через протокол SNMP.
		Внутренний	Каждое приложение получает состояние устройств печати по всей сети через протокол SNMP
		Внутренний	Каждое приложение получает данные о расходных материалах устройств печати по всей сети через протокол SNMP
		Внутренний	Каждое приложение может перезагрузить устройство печати через протокол SNMP или через веб-интерфейс устройства печати
		Внутренний	Каждое приложение может отправить тестовую страницу на определенное устройство печати
		Внутренний	Каждое приложение может запустить веб-страницу устройства печати
		Внешний **(только исходящий)**	Каждое приложение преодолевает брандмауэр компании для доступа в интернет (HTTPS через порт 443)
		Внешний **(только исходящий)**	Каждое приложение аутентифицируется с помощью своего сертификата на удаленном коммуникационном сервере Xerox перед передачей любых параметров данных

Метод развертывания	Используемое приложение	Информационный поток в сети	Удобство эксплуатации сети
		Внешний **(только исходящий)**	Каждое приложение автоматически передает данные параметров устройств печати по зашифрованному каналу (HTTPS через порт 443) на коммуникационные серверы Xerox® в определенное время каждый день
		Внешний **(только исходящий)**	Каждое приложение автоматически отправляет запросы к коммуникационным серверам Xerox® по зашифрованному каналу (HTTPS через порт 443) в определенное время каждый день для получения списка действий, которые необходимо выполнить.
Приложения для управления устройствами	Xerox Device Agent Partner Edition для мониторинга подключенных к сети устройств печати	Внутренний	Каждое приложение Xerox Device Agent обнаруживает веб-прокси-сервер (автоматически или направляется на определенный адрес)
		Внутренний	Каждое приложение Xerox Device Agent получает возможности устройств печати по всей сети через протокол SNMP
		Внутренний	Каждое приложение Xerox® Device Agent получает конфигурацию устройств печати по всей сети через протокол SNMP
		Внутренний	Каждое приложение Xerox Device Agent получает статус устройств печати по всей сети через протокол SNMP
		Внутренний	Каждое приложение Xerox Device Agent получает данные о расходных материалах устройств печати по всей сети через протокол SNMP
		Внутренний	Каждое приложение Xerox Device Agent может запросить у устройства печать отчет о конфигурации
		Внутренний	Каждое приложение Xerox Device Agent может запустить веб-страницу устройства печати
		Внутренний	Каждое приложение Xerox Device Agent может обновить программное обеспечение устройства печати через отправку задания на печать. (. DLM-файл через порт 9100)
		Внешний **(только исходящий)**	Каждое приложение Xerox Device Agent преодолевает брандмауэр компании для доступа в интернет (HTTPS через порт 443).
		Внешний **(только исходящий)**	Каждое приложение аутентифицируется с помощью своего сертификата на удаленном коммуникационном сервере Xerox перед передачей любых параметров данных
		Внешний **(только исходящий)**	Каждое приложение Xerox Device Agent автоматически передает данные параметров устройств печати по зашифрованному каналу (HTTPS через порт 443) на коммуникационные серверы Xerox® в определенное время каждый день
		Внешний **(только исходящий)**	Каждое приложение Xerox Device Agent автоматически запрашивает коммуникационные серверы по зашифрованному каналу (HTTPS через порт 443) в определенное время каждый день о получении списка действий, которые необходимо выполнить.

Метод развертывания	Используемое приложение	Информационный поток в сети	Удобство эксплуатации сети
Приложения для управления устройствами	Xerox® Device Manager для мониторинга подключенных к сети устройств печати	Внутренний	Приложения Xerox Device Manager / Xerox Device Agent для обнаружения веб-прокси-сервера (автоматически или направляется на определенный адрес)
		Внутренний	Приложения Xerox Device Manager / Xerox Device Agent получают возможности устройств печати по всей сети через протокол SNMP
		Внутренний	Приложения Xerox Device Manager / Xerox Device Agent получают конфигурацию устройств печати по всей сети через протокол SNMP
		Внутренний	Приложения Xerox Device Manager / Xerox Device Agent получают статус устройств печати по всей сети через протокол SNMP
		Внутренний	Приложения Xerox Device Manager / Xerox Device Agent получают данные о расходных материалах устройств печати по всей сети через протокол SNMP
		Внутренний	Приложения Xerox Device Manager / Xerox Device Agent могут запросить у устройства печать отчета о конфигурации
		Внутренний	Приложения Xerox Device Manager / Xerox Device Agent могут запускать веб-страницу устройства печати
		Внутренний	Приложения Xerox Device Manager / Xerox Device Agent могут обновлять программное обеспечение устройства печати через отправку задания на печать
		Внутренний	Приложение Xerox Device Manager поддерживает SNMPv3 связь с устройствами печати
		Внутренний	Приложение Xerox Device Manager может вносить изменения в конфигурацию устройств печати через протокол SNMP и веб-интерфейс
		Внутренний	Приложение Xerox Device Manger извлекает журналы учета на основе заданий из определенных многофункциональных устройств печати Xerox®
		Внутренний	Приложение Xerox Device Manager управляет/применяет политики контроля печати
		Внешний **(только исходящий)**	Приложения Xerox Device Manager / Xerox Device Agent преодолевают брандмауэр компании для доступа в интернет (HTTPS через порт 443)
		Внешний **(только исходящий)**	Каждое приложение аутентифицируется с помощью своего сертификата на удаленном коммуникационном сервере Xerox перед передачей любых параметров данных
		Внешний **(только исходящий)**	Приложения Xerox Device Manager / Xerox Device Agent автоматически передают данные устройств печати на коммуникационные серверы Xerox® по зашифрованному каналу (HTTPS через порт 443) в определенное время каждый день

Метод развертывания	Используемое приложение	Информационный поток в сети	Удобство эксплуатации сети
		Внешний **(только исходящий)**	Приложения Xerox Device Manager / Xerox Device Agent автоматически запрашивают коммуникационные серверы Xerox по зашифрованному каналу (HTTPS через порт 443) в определенное время каждый день для получения списка действий, которые необходимо выполнить
	Приложение для управления устройствами	Внешнее, двунаправленное	Xerox Device Manager ежедневно связывается с Xerox Services Manager и позволяет администраторам удаленно изменять настройки, избегая необходимости вызова специалистов на место.

9. Функции безопасности

ПРОСТОЙ ПРОТОКОЛ УПРАВЛЕНИЯ СЕТЬЮ (SNMP) ДЛЯ XEROX®

Простой протокол управления сетью (SNMP) – это наиболее широко используемый инструмент управления сетью для установления связи между системами управления сетью и сетевыми принтерами. Приложения для управления устройствами используют протокол SNMP во время операций обнаружения для получения подробной информации об устройстве печати. Приложения для управления устройствами Xerox® поддерживают протоколы SNMP v1/v2 и v3. Подробнее см. в соответствующих руководствах по сертификации приложений для управления устройствами Xerox®.

Протокол SNMP v3 поддерживает несколько моделей безопасности, которые могут существовать одновременно в рамках одного объекта SNMP. SNMPv3 обеспечивает более строгую защиту за счет добавления криптографической защиты к SNMPv2. Кроме того, SNMPv3 совместим с предыдущими версиями и широко используется в надежных сетях.

Приложения для управления устройствами Xerox (Centre Ware® Web / Xerox Device Manager, Xerox Device Agent) могут взаимодействовать с платформами устройств, которые соответствуют Федеральному стандарту по обработке информации FIPS 140-2 в своих реализациях SNMPv3.

Приложения для управления устройствами Xerox не используют службу Windows SNMP или службу Windows SNMP Trap. Если эти службы были установлены ранее, их **необходимо** отключить на любом персональном компьютере (ПК) или сервере, на котором установлено приложение для управления устройствами Xerox.

Приложения для управления устройствами Xerox используют разработанный компанией Xerox агент SNMP, который:

- Содержит специальный механизм кодирования/декодирования
- Полностью управляется сетью .NET
- Использует исполняемый файл .NET, что обеспечивает улучшенную безопасность для предотвращения атак на уязвимости программного обеспечения, такие как недопустимые манипуляции с указателями, переполнение буфера и проверка привязки.

Приложения для управления устройствами Xerox используют функции безопасности, доступные в операционной системе (ОС) Windows, в том числе:

- Аутентификация и авторизация пользователей
- Настройка и управление службами
- Развертывание и управление групповыми политиками

Брандмауэр подключения к интернету Windows (ICF), в том числе и:

- Настройки ведения журналов безопасности
- Параметры ICMP

Приложения для управления устройствами Xerox: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, SQL CE приложение Microsoft® SQL Server и **Xerox Device Manager** используют Microsoft® SQL Server.

Приложения для управления устройствами Xerox могут быть настроены на использование дополнительных функций безопасности Microsoft®, включая, где это применимо:

- Включение регистрации учетной записи пользователя
- Шифрование системы доменных имен (DNS)
- Ограничение привилегий учетной записи пользователя для доступа к базе данных (т. е. права владельца базы данных)
- Реализация определяемых пользователем номеров портов

Для передачи данных на удаленные коммуникационные серверы Xerox требуется регистрационный ключ Xerox и действующая учетная запись Xerox.

На внешние коммуникации приложения для управления устройствами Xerox может влиять брандмауэр подключения к интернету Windows. (Мы рекомендуем клиентам внести URL-адрес Xerox в белый список брандмауэра клиента (*.support.xerox.com) и указать IP-адрес, который может получить доступ к этому URL-адресу).

Приложения для управления устройствами Xerox работают в фоновом режиме с использованием учетных данных локальной системной учетной записи для автоматического запроса сетевых устройств печати по протоколу SNMP и периодической передачи параметров устройств печати обратно на коммуникационные серверы Xerox.

Доступ к пользовательскому интерфейсу (UI) и функциям приложения Xerox Device Manager контролируется с помощью следующих привилегий с учетом ролей:

- Группы Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators и Centre Ware® Web Customers.
- Имена пользователей и пароли для приложений не передаются по сети; вместо них используются маркеры доступа (согласно разработке ОС Windows®).
- Приложение Xerox Device Manager обеспечивает безопасность на основе управления подачей печати, ограничивая задания на основе политики использования цвета, типа документа, стоимости задания, времени суток, контроля доступа групп пользователей, политики двусторонней печати, разрешенных оттисков заданий и квот печати.

Примечание: Использование протокола SNMP любым приложением для удаленных служб Xerox® не представляет риска для безопасности ИТ-среды клиента, поскольку весь трафик на основе SNMP, генерируемый или потребляемый этими приложениями, происходит в пределах внутренней сети клиента, за брандмауэром. Служба Windows SNMP и служба Windows SNMP Trap по умолчанию не включены в ОС Windows.

Режим корпоративной безопасности

По умолчанию проведение ***плановой*** синхронизации приложения Xerox Device Agent с защищенным коммуникационным сервером выполняется *ежедневно*. Обратите внимание, что время суток может быть установлено по выбору.

Предусмотрено два режима корпоративной безопасности: **Обычный** и **с блокировкой**.

Если выбран **обычный** режим, приложение для управления устройствами ежедневно связывается с Xerox Services Manager. Настройки могут быть изменены без необходимости выезда на место, даже при отключенном графике опроса. ***(Рекомендуемый режим)***.

В режиме **с блокировкой**, помимо синхронизации данных, связанных с принтером, отсутствует связь с коммуникационными серверами, и настройки необходимо изменять на месте. Кроме того, IP-адреса оборудования и принтера Xerox Device Agent не сообщаются коммуникационному серверу. Этот режим ограничивает все другие преимущества удаленного обслуживания, включая автоматическое выставление счетов и контроль за расходными материалами, а также диагностические данные, используемые для технической поддержки.

Примечание: Если в версии Xerox Device Agent нет вкладки «Corporation Security Mode», приложение работает в обычном режиме.

10. Влияние на сеть

Сетевые инструкции компании, как правило, включают или отключают определенные сетевые порты на маршрутизаторах и/или серверах. Большинство ИТ-отделов уделяют больше внимания портам, используемым приложением для исходящего трафика. Отключение определенных портов может повлиять на функциональность приложения. См. таблицу ниже, чтобы узнать, какие порты используются при работе приложения. Если приложение должно сканировать несколько сегментов сети или подсетей, маршрутизаторы должны разрешить протоколы, связанные с этими номерами портов.

Протоколы, порты и другие сопутствующие технологии

В таблице 7 указаны протоколы, порты и технологии, используемые удаленными службами Xerox®.

Номер порта	Протокол	Использование	Поток данных в сети
Зависит от протоколов верхнего уровня	**Интернет-протокол (IP)**	**Основной канал для передачи всех данных**	**Внутренний + внешний (только исходящий)**
Не указано	Протокол управления сообщениями в сети (ICMP)	Обнаружение устройств печати + устранение неполадок	Внутренний
25	Протокол обмена почтовыми сообщениями (SMTP)	Устройство печати + приложение удаленного прокси-сервера Оповещения по электронной почте	Внутренний
53	Службы доменных имен (DNS)	Используется для операций обнаружения устройств печати по DNS	Внутренний
80	Протокол передачи гипертекстовых файлов (HTTP)	Запросы веб-страницы устройства печати + запросы веб-страницы приложения для управления устройствами	Внутренний
135	Протокол дистанционного вызова процедур (RPC)	Обнаружение устройства печати	Внутренний

Номер порта	Протокол	Использование	Поток данных в сети
161	Простой протокол управления сетью (SNMP v1 / v2C / v3)	Протокол промышленного стандарта, используемый для обнаружения сетевых устройств печати + Получение данных о состоянии, счетчиках и расходных материалах + Получение и применение конфигурации устройств печати. Имена сообществ по умолчанию: «public» (открытые) (GET), «private» (закрытые) (SET).	Внутренний
443	Безопасный протокол передачи гипертекстовых файлов (HTTPS)	Запросы защищенной веб-страницы устройства печати (если настроено) + Запросы защищенной веб-страницы приложения Remote Proxy (если настроено) + Передача данных устройства печати обратно на коммуникационные серверы Xerox® + связь управления печатью обратно в Xerox® Device Manager	Внутренний + внешний (только исходящий)
515, 9100, 2000, 2105	Отправка заданий на печать через порты TCP/IP LPR и Raw	Обновление программного обеспечения устройства печати + Печать тестовой страницы диагностики	Внутренний

11. Рекомендации по безопасности

- Всегда обновляйте устройства печати до новейшей версии микропрограммного/программного обеспечения. Компания Xerox тщательно отслеживает уязвимости и при необходимости заранее предоставляет клиентам исправления и обновления для системы безопасности.
- По возможности отключайте неиспользуемые порты и протоколы на устройствах печати. Обычно это делается для устройств печати офисного класса через пользовательский веб-интерфейс (UI) и для устройств печати производственного класса – через локальный пользовательский интерфейс (UI).
- Используйте функции управления доступом пользователей на устройствах печати, если они доступны. Обычно это делается для устройств печати офисного класса через пользовательский веб-интерфейс (UI) и для устройств печати производственного класса – через локальный пользовательский интерфейс (UI).
- По возможности используйте безопасные протоколы. Обычно это делается для офисных устройств печати через пользовательский веб-интерфейс (UI) и для производственных устройств печати – через локальный пользовательский интерфейс (UI).
- Включите функции безопасности, встроенные в устройство (например, перезапись изображения, шифрование данных сканирования, шифрование потока печати, шифрование диска, безопасная печать, зашифрованные файлы .pdf, аутентификация доступа CAC/PIV).

Подробнее об удаленных службах в Xerox см. на Xerox.com/RemoteServices.

Дополнительную и специальную информацию о механизмах обеспечения защиты и возможностях ряда приложений для управления устройствами Xerox см. в соответствующих руководствах:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Для компании Xerox важное место занимает обеспечение превентивной защиты от современных угроз как контента, так и безопасной работы устройств. По адресу www.xerox.com/security можно получить доступ к полной информации о безопасности, обновлениям, бюллетеням, информационным документам, исправлениям и многому другому.