Проверка подлинности карт

Руководство администратора

Декабрь 2020 г.

www.lexmark.com

Содержимое

Общие сведения

Используйте приложение для обеспечения безопасного доступа к принтеру при помощи устройства для считывания с карт. При идентификации пользователей проверка подлинности их учетных данных проводится при помощи одного из перечисленных ниже способов.

- Главный принтер Если главный принтер находится в автономном режиме, резервный принтер функционирует в качестве главного принтера до возвращения главного принтера в онлайн-режим.

  Примечание: При настройке принтеров убедитесь, что они находятся в одной и той же сети.
- Серверы Lightweight Directory Access Protocol (LDAP), Lexmark™ Document Distributor (LDD) или провайдеры службы идентификации, в зависимости от способа проверки подлинности, заданного организацией.

В данном документе приводятся инструкции по настройке, использованию и устранению проблем с приложением.

Настройка предварительных условий

Для настройки приложения необходимо обладать правами администратора.

Доступ к Embedded Web Server

1. Получение IP-адреса принтера. Выполните одно из следующих действий.
   - Найдите IP-адрес на начальном экране принтера.
   - В разделе TCP/IP меню "Сеть/Порты" проверьте IP-адрес.
2. Откройте веб-браузер и в поле адреса введите IP-адрес принтера.

Добавление учетной записи внутреннего пользователя

Учетная запись внутреннего пользователя требуется при использовании функции проверки пользователей на принтере.

1. Из окна Embedded Web Server выберите **Параметры** или **Конфигурация**.
2. В зависимости от модели принтера выполните одно из следующего:
   - Нажмите **Безопасность** > **Настройка безопасности** > **Внутренние учетные записи** > **Добавить внутреннюю учетную запись**
   - Нажмите **Безопасность** > **Изменение настроек безопасности** > **Внутренние учетные записи** > **Добавить внутреннюю учетную запись**
3. Введите данные учетной записи и нажмите **Отправить**.
4. Если требуется, в разделе «Управление внутренними учетными записями» введите пользовательское имя блока для создания, затем укажите необходимые учетные данные пользователя.
5. Нажмите **Отправить**.

Настройка групп для внутренних учетных записей пользователей

1. Из окна Embedded Web Server выберите **Параметры** или **Конфигурация**.
2. В зависимости от модели принтера выполните одно из следующего:
   - Нажмите **Безопасность** > **Настройка безопасности** > **Внутренние учетные записи** > **Настройка групп для использования с внутренними учетными записями**.
   - Нажмите **Безопасность** > **Изменение настроек безопасности** > **Внутренние учетные записи** > **Настройка групп для использования с внутренними учетными записями**.
3. Введите имя группы, а затем нажмите **Добавить**.

4 Добавьте внутренние учетные записи в группу.

5 Нажмите **Отправить**.

Создание шаблона безопасности

Шаблон безопасности создается из блоков безопасности, таких как «Внутренние учетные записи», Kerberos, LDAP, LDAP+GSSAPI и Active Directory. Такие шаблоны применяются к функции управления доступом, чтобы защитить функции и приложения принтера.

1 В Embedded Web Server выберите **Параметры** или **Конфигурация**.

2 В зависимости от модели принтера выполните одно из следующего:

- Нажмите **Безопасность** > **Настройка безопасности** > **Шаблон безопасности** > **Добавить шаблон безопасности**.
- Нажмите **Безопасность** > **Изменение настроек безопасности** > **Шаблоны безопасности** > **Добавить шаблон безопасности**.

3 Введите имя шаблона безопасности, затем выберите один из следующих параметров проверки подлинности:

- Для функции проверки подлинности на принтере при независимой установке выберите блок внутренней учетной записи.
- Для функции проверки подлинности на принтере с помощью компонента вывода на печать Lexmark Print Management (LPM) Serverless Print Release при настройке Active Directory выберите блок LDAP+GSSAPI.
- Для функции проверки подлинности LDAP выберите блок LDAP.

4 Нажмите кнопку **Сохранить шаблон**.

Примечание: Чтобы изменить существующий шаблон безопасности, выберите шаблон безопасности и добавьте или измените авторизацию для шаблона.

Настройка управления доступом

Примечание: При использовании функции **Вход в качестве администратора** убедитесь, что вы настроили шаблон безопасности для внутренних учетных записей. Подробнее см. “Создание шаблона безопасности” на стр. 6.

1 В окне Embedded Web Server выберите **Параметры** или **Конфигурация**.

2 В зависимости от модели принтера выполните одно из следующего:

- Нажмите **Безопасность** > **Изменение настройки безопасности** > **Параметры управления доступом**.
- Нажмите **Безопасность** > **Изменение настройки безопасности** > **Параметры управления доступом**.

3 Нажмите **Приложения устройства** или **Решения устройства**, затем выполните следующее:

- Задайте для Приложение 1 или Решение 1 значение внутренней учетной записи, LDAP+GSSAPI или шаблона безопасности Active Directory.
- Задайте для Приложение 2 или Решение 2 значение шаблона безопасности приложения.

  Примечание: Шаблон безопасности приложения – это приложение с CardAuth в качестве установки аутентификации. Подробнее см. “Создание шаблона безопасности” на стр. 6.
- Задайте для Приложение 3 или Решение 3 значение шаблона безопасности LDAP.

Примечания.

- Если установлен компонент вывода на печать LPM, задайте для управления доступом вывода на печать значение шаблона безопасности приложения.
- Для принтеров с Embedded Solutions Framework (eSF) версии 2.x требуется приложение eSF Security Manager для настройки управления доступом. Список таких принтеров см. в файле *Readme*.

4 Нажмите **Отправить**.

Настройка приложения

Перед началом выполните следующее:

- Отключите параметры «Фон» и «Экран простоя», а также все приложения проверки подлинности.
- Установите следующее:
  - Установщик компонента для проверки подлинности по картам
  - Драйвер устройства чтения карт
  - Устройство чтения карт
  - eSF Security Manager

    Примечание: Для принтеров с eSF версии 2.x требуется приложение eSF Security Manager для настройки управления доступом. Список таких принтеров см. в файле *Readme*.

Открытие страницы конфигурации для приложения

1. Из окна Embedded Web Server выберите **Параметры** или **Конфигурация**.
2. В зависимости от модели принтера выполните следующее:
   - Нажмите **Приложения** > **Управление приложениями**.
   - Нажмите **Решения устройства** > **Решения (eSF)**.
   - Нажмите **Встроенные решения**.
3. Нажмите **Проверка подлинности по карточке** > **Настроить**

Конфигурирование проверки подлинности администратора

Примечание: При использовании функции **Вход в качестве администратора** убедитесь, что вы настроили шаблон безопасности для внутренних учетных записей, PIN-код и пароль. Подробнее см. “Создание шаблона безопасности” на стр. 6.

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе Проверка подлинности пользователя для поля **Управление доступом к входу в качестве администратора** выберите предпочтительный метод входа.

   Примечания.

   - Убедитесь, что выбранный элемент управления доступом настроен с помощью шаблона безопасности. Подробнее см. “Создание шаблона безопасности” на стр. 6.
   - Выбор **Отключено** скрывает опцию **Вход в качестве администратора** с панели принтера.
3. Нажмите **Применить**.

Настройка экрана входа

Экран входа можно настроить следующим образом:

- Разрешить пользователям использовать функции копирования и факса без входа в систему.
- Разрешить пользователям выбирать способ входа в систему.
- Добавить фон экрана входа и настроить сообщение, которое отображается при входе в систему.
- Отключить предупреждение об отсутствии подключенных устройств чтения карт.

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. Настройте параметры в разделе Экран входа.

   Примечание: Для получения дополнительной информации о каждом параметре см. справочную информацию, которая появляется при наведении курсора мыши.
3. Нажмите **Применить**.

Включение функции копирования или факса без выполнения входа

Если функции Разрешить копирование без входа или Разрешить факс без входа включены, выполните следующее:

1. В Embedded Web Server выберите **Параметры** или **Конфигурация**.
2. В зависимости от модели принтера выполните одно из следующего:
   - Нажмите **Безопасность** > **Настройка безопасности** > **Управление доступом** > **Доступ к функциям**.
   - Нажмите **Безопасность** > **Изменение настроек безопасности** > **Параметры управления доступом**.
3. Задайте для функции копирования или факса значение **Без защиты**.
4. Нажмите **Отправить**.

Проверка подлинности на принтере

Функцию проверки подлинности на принтере следует использовать, когда проверка пользователей выполняется через главный принтер.

Настройка проверки подлинности пользователя на принтере

Прежде чем начать, убедитесь в следующем.

- Для управления доступом «Приложение 1» или «Решение 1» задано значение внутренней учетной записи, LDAP+GSSAPI или шаблон безопасности Active Directory.
- Для параметра управления доступом «Приложение 2» или «Решение 2» задано значение шаблона безопасности приложения.

  Примечание: Подробнее см. “Настройка управления доступом” на стр. 6.

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе «Экран входа» задайте для параметра «Способ входа» значение **Вход с картой или в ручном режиме**.

3 В разделе аутентификации пользователя выполните следующее:
- Задайте для «Проверка по карте» значение **На принтере**.
- Задайте для «Управление доступом с регистрацией карты» значение **Приложение 1** или **Решение 1**.
- Задайте для «Управление доступом для входа в ручном режиме» значение **Приложение 1** или **Решение 1**.
- Задайте для «Управление доступом сеанса» значение **Приложение 2** или **Решение 2**.

Примечания.
- Если для «Управление доступом с регистрацией карты» задано значение **Нет**, значит вы не можете зарегистрировать свою карту на принтере.
- Чтобы задать для «Управление доступом для входа в ручном режиме» значение **Нет**, для вохда требуется только карта, даже если для «Способ входа» задано значение **Вход с картой или в ручном режиме**.
- Для получения дополнительных сведений о каждом параметре, см. справочную информацию, которая появляется при наведении курсора мыши.

4 Нажмите **Применить**.

Настройка роли принтера

Примечание: Для клиентского принтера необходим как головной, так и резервный принтеры.

1 Из Embedded Web Server перейдите к странице конфигурации приложения.

2 В разделе «Проверка по карте на принтере» выберите роль для данного принтера.
- **Главный** — в принтере хранится список зарегистрированных пользователей.
- **Резервный** — если главный принтер в автономном режиме, резервный принтер принимает роль главного до перехода главного принтера в онлайн-режим.
- **Клиент** — в этом принтере информация о пользователях не хранится. Для проверки учетных данных пользователя требуется главный или резервный принтер.

Примечания.
- При наличии только одного принтера он должен быть настроен в качестве главного.
- При наличии двух принтеров один из них должен быть настроен в качестве главного, а другой — в качестве резервного.
- При наличии трех и более принтеров один из них должен быть настроен в качестве главного, один — в качестве резервного, а остальные — в качестве клиентских.

3 Введите имена хоста или IP-адреса главного и резервного принтеров.

Примечания.
- При настройке резервного принтера необходимо имя хоста или IP-адрес главного принтера.
- При настройке клиентских принтеров требуются имена хоста или IP-адреса главного и резервного принтеров.
- Перед назначением для клиентского принтера нового главного принтера его следует удалить из старого главного принтера.

4 Нажмите **Применить**.

Проверка подлинности пользователей веб-службы

Функцию проверки подлинности через веб-службу следует использовать, когда проверка пользователей выполняется через сервер LDD.

Настройка проверки подлинности пользователя веб-службы

Перед началом убедитесь, что для параметра управления доступом «Приложение 2» или «Решение 2» задано значение шаблона безопасности приложения. Для получения дополнительной информации см. “Настройка управления доступом” на стр. 6.

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе Экран входа задайте для параметра Способ входа значение **Вход с картой или в ручном режиме**.
3. В разделе Проверка подлинности пользователя выполните следующее:
   - Задайте для параметра Проверка по карте значение **Веб-служба**.
   - Задайте для параметра Управление доступом с регистрацией карты и Управление доступом для входа в ручном режиме требуемое значение управления доступом.
   - Задайте для параметра Управление доступом сеанса значение **Приложение 2** или **Решение 2**.

   Примечания.

   - Если для параметра Управление доступом с регистрацией карты задано значение **Нет**, вы не можете зарегистрировать свою карту на принтере.
   - При установке для параметра Управление доступом для входа в ручном режиме значения **Нет** для входа требуется только карта, даже если для параметра Способ входа задано значение **Вход с картой или в ручном режиме**.
   - Для получения дополнительной информации о каждом параметре см. справочную информацию, которая появляется при наведении курсора мыши.
4. Выберите **Проверить сертификат**, чтобы проверить все подключения к серверу. Если параметр Проверить сертификат не выбран, сертификат ЦС не будет проверен.

   Примечание: Параметр Проверить сертификат применим только для проверки службы идентификации и веб-службы.
5. В меню Режим проверки выберите **по цепочке** или **одноранговый**.

   Примечание: По умолчанию установлено значение по цепочке.
6. Загрузите Сертификат SSL для сервера, чтобы установить защищенное подключение к серверу.
7. В поле Проверка хостов введите дополнительные имена хостов (кроме URL сервера по умолчанию) для проверки записей в сертификате. Используйте запятые для разделения нескольких имен хостов.

   Примечание: По умолчанию этот белый список содержит только URL сервера. Введите дополнительные имена хостов в поле Проверка хостов, чтобы включить их в белый список.
8. Нажмите **Применить**.

Настройка параметров веб-службы

1 Из Embedded Web Server перейдите к странице конфигурации приложения.

2 В разделе параметров веб-службы настройте параметры.

Примечание: Для получения дополнительных сведений о каждом параметре, см. справочную информацию, которая появляется при наведении курсора мыши.

3 Нажмите **Применить**.

Проверка подлинности пользователей через службу идентификации

Функцию проверки подлинности через службу идентификации следует использовать, когда проверка пользователей выполняется через сервер службы идентификации, такой как сервер LPM Software as a Service (SaaS).

Настройка проверки подлинности пользователя службы идентификации

Перед началом убедитесь, что для параметра управления доступом «Приложение 2» или «Решение 2» задано значение шаблона безопасности приложения. Для получения дополнительной информации см. “Настройка управления доступом” на стр. 6.

1 Из Embedded Web Server перейдите к странице конфигурации приложения.

2 В разделе Экран входа задайте для параметра Способ входа значение **Вход с картой или в ручном режиме**.

3 В разделе Проверка подлинности пользователя выполните следующее:

- Задайте для параметра Проверка по карте значение **Служба идентификации**.
- Задайте для параметра Управление доступом с регистрацией карты значение **Служба идентификации**.
- Задайте для параметра Управление доступом для входа в ручном режиме значение **Служба идентификации**.
- Задайте для параметра Управление доступом сеанса значение **Приложение 2** или **Решение 2**.

Примечания.

- Если для параметра Управление доступом с регистрацией карты задано значение **Нет**, вы не можете зарегистрировать свою карту на принтере.
- При установке для параметра Управление доступом для входа в ручном режиме значения **Нет** для входа требуется только карта, даже если для параметра Способ входа задано значение **Вход с картой или в ручном режиме**.
- Для получения дополнительной информации о каждом параметре см. справочную информацию, которая появляется при наведении курсора мыши.

4 Выберите **Проверить сертификат**, чтобы проверить все подключения к серверу. Если параметр Проверить сертификат не выбран, сертификат ЦС не будет проверен.

Примечание: Параметр Проверить сертификат применим только для проверки службы идентификации и веб-службы.

5 В меню Режим проверки выберите **по цепочке** или **одноранговый**.

Примечание: По умолчанию установлено значение по цепочке.

6 Загрузите Сертификат SSL для сервера, чтобы установить защищенное подключение к серверу.

7 В поле Проверка хостов введите дополнительные имена хостов (кроме URL сервера по умолчанию) для проверки записей в сертификате. Используйте запятые для разделения нескольких имен хостов.

Примечание: По умолчанию этот белый список содержит только URL сервера. Введите дополнительные имена хостов в поле Проверка хостов, чтобы включить их в белый список.

8 Нажмите **Применить**.

Настройка параметров службы идентификации

1 Из Embedded Web Server перейдите к странице конфигурации приложения.

2 Если необходимо, в разделе параметров службы идентификации выберите **Включить экран простоя**.

Примечание: Для принтеров с eSF версии 2.x необходимо приложение eSF Security Manager, когда параметр **Включить экран простоя** отключен. Список таких принтеров см. в файле *Readme*.

3 Введите имя хоста или IP-адрес службы идентификации.

4 Если требуется, введите имя хоста или IP-адрес службы провайдера службы бейджей.

5 Загрузите сертификат сервера SSL для выполнения защищенного подключения к серверу.

6 Если у вас есть идентификатор клиента и секретный код клиента от провайдера службы идентификации, введите их в соответствующие поля.

7 Настройте политику доступа приложения.

- **Продолжить** — продолжение использования принтера, даже при неудачной попытке подключения к серверу службы идентификации.
- **Сбой** — возврат на экран входа в случае сбоя подключения к серверу службы идентификации.

8 Чтобы разрешить пользователям выполнять вход в систему принтера с использованием отдельной учетной записи службы, выберите **Использование учетной записи службы**, затем введите учетные данные учетной записи службы.

9 Нажмите **Применить**.

Проверка подлинности с PIN-кодом

Настройка аутентификации пользователя с PIN-кодом

Перед началом убедитесь, что для параметра управления доступом «Приложение 2» или «Решение 2» задано значение шаблона безопасности приложения. Подробнее см. “Настройка управления доступом” на стр. 6.

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе экрана входа задайте для «Способ входа» значение, для которого есть поддержка аутентификации с PIN-кодом.
3. В разделе аутентификации пользователя выполните следующее:
   - Задайте для «Проверка по карте» значение предпочтительного способа аутентификации.
   - Задайте для «Управление доступом с регистрацией карты» предпочтительное значение управления доступом.
   - Задайте для «Управление доступом с PIN-кодом» значение **Приложение 1** или **Решение 1**.
   - Задайте для «Управление доступом для входа в ручном режиме» предпочтительное значение управления доступом.
   - Задайте для «Управление доступом сеанса» значение **Приложение 2** или **Решение 2**.

   Примечания.

   - Если для «Управление доступом с PIN-кодом» задано значение **Нет**, значит вы не можете зарегистрировать свой PIN-код на принтере.
   - Для получения дополнительных сведений о каждом параметре, см. справочную информацию, которая появляется при наведении курсора мыши.
4. Нажмите **Применить**.

Настройка параметров PIN-кода

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В меню Требуемые учетные данные раздела Параметры PIN-кода выберите метод входа.
   - Userid и PIN — для аутентификации требуется имя пользователя и PIN-код.
   - Только PIN — для аутентификации требуется PIN-код.
3. Введите адрес веб-сервера, затем выберите минимальную длину PIN-кода.
4. Введите сообщение для неверного PIN-кода.
5. Нажмите **Применить**.

Проверка подлинности через LDAP

Функцию проверки подлинности через LDAP следует использовать, когда проверка пользователей выполняется через сервер LDAP.

Настройка аутентификации пользователя LDAP

Прежде чем начать, убедитесь в следующем.

- Для параметра управления доступом «Приложение 2» или «Решение 2» задано значение шаблона безопасности приложения.
- Для параметра управления доступом «Приложение 3» или «Решение 3» задано значение шаблона безопасности LDAP.

  Примечание: Подробнее см. “Настройка управления доступом” на стр. 6.

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе «Экран входа» задайте для параметра «Способ входа» значение **Вход с картой или в ручном режиме**.
3. В разделе аутентификации пользователя выполните следующее:
   - Задайте для «Проверка по карте» значение **LDAP**.
   - Задайте для «Управление доступом с регистрацией карты» значение **Приложение 3** или **Решение 3**.
   - Задайте для «Управление доступом для входа в ручном режиме» значение **Приложение 3** или **Решение 3**.
   - Задайте для «Управление доступом сеанса» значение **Приложение 2** или **Решение 2**.

   Примечания.

   - Если для «Управление доступом с регистрацией карты» задано значение **Нет**, значит вы не можете зарегистрировать свою карту на принтере.
   - Чтобы задать для «Управление доступом для входа в ручном режиме» значение **Нет**, для вохда требуется только карта, даже если для «Способ входа» задано значение **Вход с картой или в ручном режиме**.
   - Для получения дополнительных сведений о каждом параметре, см. справочную информацию, которая появляется при наведении курсора мыши.
4. Нажмите **Применить**.

Настройка параметров LDAP

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе параметров LDAP настройте параметры.

   Примечания.

   - Если выбрано **Использовать адресную книгу**, приложение использует параметры LDAP, которые уже настроены в учетных записях принтера.
   - Для получения дополнительных сведений о каждом параметре, см. справочную информацию, которая появляется при наведении курсора мыши.

3 Нажмите **Применить**.

Настройка приложения

1 Из Embedded Web Server перейдите к странице конфигурации приложения.

2 Выполните одно или несколько из указанных ниже действий.

- Чтобы персонализировать начальный экран принтера, настройте параметры начального экрана.
- Для отображения сообщений регистрации в разделе дополнительных параметров выберите **Отображать сообщение начала регистрации** и **Отображать сообщение завершения регистрации**.
- Чтобы был слышен *звуковой сигнал* после удачной попытки входа, в разделе дополнительных настроек выберите **Включить звуковой сигнал при удачном входе**, затем отрегулируйте тональность звукового сигнала.
- Чтобы использовать профиль после успешного входа, в разделе дополнительных настроек введите имя профиля в поле «Профиль регистрации».

Примечание: Для получения дополнительных сведений о каждом параметре, см. справочную информацию, которая появляется при наведении курсора мыши.

3 Нажмите **Применить**.

Просмотр доступных профилей

1 Из окна Embedded Web Server выберите **Параметры** или **Конфигурация**.

2 Нажмите **Управление ярлыками** > **Управление ярлыками профилей**.

Отображение областей для учетных записей пользователей

Функция «Использовать выбранную область» применима только, если способы входа для регистрации карты и входа в ручном режиме – Kerberos, Active Directory или LDAP+GSSAPI. Кроме того, эта функция применима только, если для проверки по карте задано значение «Веб-служба» или на основе принтера.

Для регистрации карты, если эта функция активирована, идентификатор зарегистрированного бейджа должен быть в формате username@realm.

Для входа в ручном режиме, если эта функция активирована, имя пользователя, отображаемое на панели управления принтера, должно быть в формате username@realm.

Такие параметры не применимы для входа с PIN и регистрации с PIN.

Для активации этой функции выполните следующее:

1 Из Embedded Web Server перейдите к странице конфигурации приложения.

2 В разделе дополнительных параметров выберите **Использовать выбранную область**.

3 Нажмите **Применить**.

Экспорт или импорт файла конфигурации

1 Из Embedded Web Server перейдите к странице конфигурации приложения.

2 Экспорт или импорт файла конфигурации.

Примечания.

- В случае возникновения ошибки **Переполнение памяти JVM** повторяйте операцию экспорта, пока не будет сохранен файл параметров.
- При возникновении таймаута и отображении пустого экрана, обновите веб-браузер, затем нажмите кнопку **Применить**.

Управление приложением

Примечание: Страница состояния для приложения доступна только при использовании функции проверки подлинности на принтере.

Доступ к странице состояния приложения

Для контроля активности принтера используйте страницу состояния.

1. В окне Embedded Web Server выберите **Приложения** > **Проверка подлинности по карточке**.
2. Обратите внимание на следующую информацию:
   - **Состояние** — отображение сообщений о состоянии активности принтера
     - **Не настроено** — принтер не настроен.
     - **Автономный режим** — активность принтера и передача данных отсутствуют
     - **Онлайн** — принтер активен.
   - **Время непрерывной работы** — указывает на продолжительность работы приложения.
   - **(этот принтер)** — используемый в данный момент принтер.
   - **Последняя активность** — информация о последней активности главного принтера.
   - **Количество пользователей** — общее количество зарегистрированных пользователей.
   - **Состояние регистрации** — указывает на состояние принтера – в автономном режиме или онлайн.
   - **Последняя синхронизация с главным принтером** — время последнего обновления резервного принтера данными с главного принтера.
   - **Последний контакт с главным принтером** — время последнего обмена данными между резервным принтером и главным принтером.
   - **Последняя синхронизация в качестве главного принтера** — последний раз, когда резервный принтер выступал в качестве главного.
   - **Последняя активность в качестве главного принтера** — последняя активность резервного принтера в качестве главного.
   - **Продолжительность работы в качестве главного принтера** — продолжительность работы резервного принтера в качестве главного.
   - **Кем обслуживается в настоящее время** — клиентский принтер, недавно связывавшийся с главным или резервным принтером.
   - **Последняя активность с резервным принтером** — последний раз, когда клиентский принтер связывался с резервным принтером.

Управление учетными записями пользователей и клиентскими принтерами

Примечание: Эта функция отображается только если принтер функционирует в качестве главного принтера.

1 Из Embedded Web Server перейдите к странице статуса приложения.

2 Доступны следующие действия:

Удаление учетных записей пользователей

а В разделе «Главный» выберите **Удалить пользователей**.

б Ввод одного или нескольких идентификаторов пользователей, последующее их удаление.

Добавление клиентских прнтеров

а В разделе «Клиенты» выберите **Добавить клиентов**.

б Ввод одного или нескольких IP-адресов принтера, последующее их удаление.

Удаление клиентских принтеров

Примечание: Клиентские принтеры можно удалять, когда главный принтер в автономном режиме или приложение удалено.

а В разделе «Клиенты» выберите один или несколько клиентских принтеров.

б Нажмите **Удалить клиентов**.

Переназначение ролей принтера

1 Конфигурируйте новый главной принтер.

а Из Embedded Web Server нового главного принтера перейдите к странице конфигурации приложения.

б В разделе «Проверка по карте на принтере» задайте «Роль» для **Главный**.

в Введите имя хоста или IP-адрес резервного принтера.

г Нажмите **Применить**.

2 Припишите резервный принтер к новому главному.

а Из Embedded Web Server резервного принтера перейдите к странице конфигурации приложения.

б В разделе «Проверка по карте на принтере» введите имя хоста и IP-адрес нового главного принтера.

в Нажмите **Применить**.

3 Удалите клиентский принтер из текущего главного принтера.

а Из Embedded Web Server текущего главного принтера перейдите к странице состояния приложения.

б В разделе «Клиенты» удалите клиентский принтер.

4 Переназначьте клиентский принтер для нового главного принтера. Выполните одно из следующих действий.

С помощью страницы конфигурации для приложения

а Из Embedded Web Server клиентского принтера перейдите к странице конфигурации приложения.

б В разделе «Проверка по карте на принтере» задайте «Роль» для **Клиент**.

в Введите имя хоста или IP-адрес нового главного принтера.

Примечание: Убедитесь, что имя хоста или IP-адрес резервного принтера верное.

г Нажмите **Применить**.

С помощью страницы состояния главного принтера

а Из Embedded Web Server новый главного принтера перейдите к странице состояния приложения.

б В разделе «Клиенты» выберите **Добавить клиентов**.

в Введите IP-адрес клиентского принтера, а затем добавьте его.

Использование приложения

Регистрация пользователей

1 Коснитесь своей карточкой устройства чтения карт.

2 На панели управления принтера введите свои учетные данные.

Примечание: Если используется Kerberos, Active Directory или LDAP+GSSAPI для регистрации с картой, выберите область.

3 Следуйте указаниям на дисплее.

Регистрация с PIN-кодом

Перед началом убедитесь, что для способа входа выбрана поддержка проверки подлинности с PIN-кодом.

1 На панели управления принтера коснитесь **Вход с PIN**.

2 Следуйте указаниям на дисплее.

Вход в систему принтера в ручном режиме

1 На панели управления принтера выберите один из следующих пунктов:

- **Вход с помощью PIN-кода**
- **Вход в ручном режиме**
- **Вход в качестве администратора**

Примечание: При выборе **Вход в качестве администратора** получение другой информации о пользователях с сервера LDAP невозможно.

2 Введите учетные данные для входа.

Примечание: Если используется Kerberos, Active Directory®или LDAP+GSSAPI для входа в ручном режиме, выберите область.

3 Следуйте указаниям на дисплее.

Поиск и устранение неисправностей

Ошибка приложения

Попробуйте воспользоваться одним из следующих способов.

Проверка системного журнала

1. Из окна Embedded Web Server выберите **Параметры** или **Конфигурация**.
2. В зависимости от модели принтера выполните следующее:
   - Нажмите **Приложения** > **Управление приложениями**.
   - Нажмите **Решения устройства** > **Решения (eSF)**.
   - Нажмите **Встроенные решения**.
3. Нажмите **Система** > **Журнал**.
4. Выбор и подтверждение верных фильтров.
5. На основании записей файла журнала устраните проблему.

Обратитесь к представителю Lexmark

Приложение не запускается с обновленной версией компонента вывода на печать SaaS

Попробуйте воспользоваться одним из следующих способов.

Убедитесь, что компонент вывода на печать настроен верно

Если приложение Print Management SaaS было обновлено до версии Print Release v2.0 или выше, необходимо отключить функции «Фон» и «Экран простоя». Назначьте управление доступом с проверкой подлинности по картам компоненту вывода на печать, затем проверьте правильность настройки компонента вывода на печать. Дополнительные сведения см. в *Руководстве администратора по компоненту вывода на печать*.

Обратитесь к представителю Lexmark

Ошибка проверки подлинности

Попробуйте воспользоваться одним из следующих способов.

Увеличение таймаута принтера

Если используется служба идентификации в качестве способа проверки по картам, принтеру может потребоваться больше времени для обмена данными с службой идентификации.

1. Из окна Embedded Web Server выберите **Параметры** или **Конфигурация**.
2. Нажмите **Общие параметры** > **Таймауты**
3. Увеличьте таймаут экрана спящий режим.
4. Нажмите **Отправить**.

Убедитесь, что принтер подключен к сети

Для получения дополнительной информации см. *Руководство пользователя* принтера.

Убедитесь в том, что сервер безопасности включен в сеть и не используется

Для получения дополнительной информации свяжитесь с системным администратором.

Пользователь заблокирован

Возможно, пользователь достиг максимального допустимого количества ошибок при входе в систему.

Увеличение времени блокировки и допустимое количество неудачных попыток входа

1. Из Embedded Web Server выполните следующие действия, в зависимости от модели принтера:
   - Нажмите **Настройки** > **Безопасность** > **Прочие настройки безопасности** > **Ограничения при входе в систему**.
   - Нажмите **Конфигурация** > **Безопасность**.
2. Увеличение времени блокировки и допустимое количество неудачных попыток входа или автоматическая задержка выхода.
3. Нажмите **Отправить**.

Невозможно зарегистрировать клиентский принтер

Попробуйте воспользоваться одним из следующих способов.

Убедитесь, что главной и резервный принтеры подключены к сети

Подробнее см. “Доступ к странице состояния приложения” на стр. 18.

Убедитесь, что главной и резервный принтеры настроены надлежащим образом.

Подробнее см. “Настройка проверки подлинности пользователя на принтере” на стр. 9.

Можно зарегистрировать не более 23 клиентских принтеров

Подробнее см. “Управление учетными записями пользователей и клиентскими принтерами” на стр. 19.

Обратитесь к представителю Lexmark

Невозможно проверить карту

Попробуйте воспользоваться одним из следующих способов.

Задать способ входа в систему для карты и ручной вход в систему

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе «Экран входа» задайте для параметра «Способ входа» значение **Вход с картой или в ручном режиме**.
3. Нажмите **Применить**.

Обратитесь к представителю Lexmark

Не удается найти сведения об области

Попробуйте воспользоваться одним из следующих способов.

Для некоторых способы входа для входа в ручном режима или регистрации по карте, таких как локальные учетные данные или LDAP, не требуется выбор области. Способы входа, для которых требуется выбор области – Kerberos, Active Directory и LDAP+GSSAPI.

Отключение выбора области

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе дополнительных параметров отмените выбор **Использовать выбранную область**.
3. Нажмите **Применить**.

Изменение способа входа

1. Из Embedded Web Server перейдите к странице конфигурации приложения.
2. В разделе проверки подлинности пользователей задайте для параметров «Управление доступом с регистрацией карты» и «Управление доступом входа в ручном режиме» значение **Приложение 1** или **Решение 1**.
3. Нажмите **Применить**.

Обратитесь к представителю Lexmark

Невозможно подключиться к серверу LDAP

Попробуйте воспользоваться одним из следующих способов.

Проверьте параметры LDAP

Подробнее см. “Настройка параметров LDAP” на стр. 15.

Обратитесь к представителю Lexmark

Часто задаваемые вопросы

Почему я не могу добавить или удалить клиентский принтер, когда резервный принтер выступает в роли главного?

Клиентский принтер можно удалить или добавить, только когда главный принтер подключен к сети.

Можно ли удалить клиентский принтер и переназначить для него новый главный принтер, если текущий главный принтер находится в автономном режиме?

Да, для этого выполните следующее:

1. Из Embedded Web Server клиентского принтера установите приложение.
2. Задайте роль «клиентский принтер» и конфигурировать его, приписав к новому главному и резервному принтеру. Подробнее см. “Настройка роли принтера” на стр. 10.

Что делать, если я случайно удалил приложение с принтера?

1. Из Embedded Web Server установите приложение.
2. Задать роль для этого принтера. Подробнее см. “Настройка роли принтера” на стр. 10.

   Примечание: Убедитесь, что был установлен главной принтер, резервный, затем клиентский, соблюдая такую последовательность.
3. Конфигурировать принтер с учетом его роли.

   Примечания.

   - Если приложение переустановлено на главном принтере, назначьте для него резервный принтер.
   - Если приложение переустановлено на резервном принтере, назначьте для него главный принтер.
   - Если приложение переустановлено на клиентском принтере, назначьте для него главный принтер и резервный принтер.
   - Подробнее см. “Переназначение ролей принтера” на стр. 19.

Почему не видно кнопки копирования или факса на экране блокировки, даже когда это было активировано без выполнения входа?

Задайте управления доступом к функциям копирования или факса значение **Без защиты**. Подробнее см. “Настройка экрана входа” на стр. 9.

Что будет при одинаковых параметрах управления доступом для «Управления доступом для входа в ручном режиме» и «Управление доступом сеанса»?

Для доступа к функциям принтера с начального экрана необходимо ввести свои учетные данные при входе в ручном режиме.

Можно ли настроить разные параметры управления доступом для «Управления доступом для входа в ручном режиме» и «Проверка по карте»?

Да, если не используется проверка подлинности Служба идентификации, в таком случае задайте для параметров Управления доступом для входа в ручном режиме и Проверка по карте значение **Служба идентификации**.

Почему функция Вход в качестве администратора не работает с сетевыми учетными записями?

Функция **Вход в качестве администратора** применима только для шаблонов безопасности Внутренние учетные записи, PIN-код и Пароль.

Уведомления

Уведомление о редакции

Декабрь 2020 г.

Следующий пункт не относится к тем странам, где подобное условие противоречит местному законодательству: КОМПАНИЯ LEXMARK INTERNATIONAL, INC. ПРЕДОСТАВЛЯЕТ ЭТУ ПУБЛИКАЦИЮ «КАК ЕСТЬ» БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, КАК ЯВНЫХ, ТАК И ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КОММЕРЧЕСКОГО УСПЕХА ИЛИ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЗАДАЧИ. В некоторых областях не разрешен отказ от оговоренных явно или подразумеваемых гарантий при определенных сделках, поэтому данное положение, возможно, к Вам не относится.

В настоящем издании могут содержаться технические неточности или типографские ошибки. Содержащаяся здесь информация периодически корректируется; данные изменения будут включены в последующие издания. В любое время в описываемые продукты или программы могут быть внесены изменения или усовершенствования.

Упоминание в этом документе изделий, программ или услуг не означает, что изготовитель намерен поставлять их во все страны, в которых он осуществляет свою деятельность. Любые упоминания изделий, программ или услуг не означают и не предполагают, что может быть использовано только это изделие, программа или услуга. Вместо них может быть использовано любое эквивалентное изделие, программа или услуга, если при этом не нарушаются существующие права интеллектуальной собственности. Пользователь сам несет ответственность за оценку и проверку работы настоящего изделия в связи с использованием других изделий, программ или услуг, кроме явно указанных изготовителем.

Для получения технической поддержки Lexmark перейдите на веб-сайт **http://support.lexmark.com**.

Для получения информации о политике конфиденциальности Lexmark, регулирующей использование настоящего продукта, перейдите по адресу **www.lexmark.com/privacy**.

Подробнее о расходных материалах и загружаемых файлах см. на веб-сайте **www.lexmark.com**.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Товарные знаки

Наименование Lexmark и логотип Lexmark являются товарными знаками Lexmark International, зарегистрированными в США и/или других странах.

Другие товарные знаки являются собственностью соответствующих владельцев.

Указатель

Р

С

У

Ф

Ч

Ш

Э