?????????? ????????

- Анонимный доступ запрещён
- Блокировка и управление учётными записями
- Доменная аутентификация и единый вход (SSO)
- Идентификация и аутентификация пользователей
- Парольная политика
- Ролевая модель RBAC
- Тайм-аут сессии и автоматическое завершение сеанса
- Технические учётные записи

????????? ?????? ????????

Зона ответственности: Printum

> **Коротко:** Доступ к функциям и данным Printum предоставляется только после успешной аутентификации пользователя. Анонимный доступ к защищенным ресурсам системы не допускается.

??????????

Система должна исключать возможность доступа неавторизованных пользователей к функциям, данным и административным интерфейсам.

Пользователь должен пройти процедуру аутентификации до получения доступа к защищенным ресурсам системы.

??? ??? ???????????? ? Printum

Доступ к Личному кабинету, панели администрирования и другим защищенным разделам системы предоставляется только после успешной аутентификации пользователя.

При обращении к защищенным ресурсам система выполняет проверку подлинности пользователя и его полномочий.

После успешной аутентификации права пользователя определяются назначенной ролью и действующей моделью разграничения доступа.

При завершении пользовательской сессии или истечении срока её действия доступ к защищенным функциям прекращается до повторной аутентификации пользователя.

Для интеграционных взаимодействий используются механизмы аутентификации и авторизации, предусмотренные соответствующим интерфейсом взаимодействия.

?????????? ? ??????????

Фактический перечень доступных функций определяется назначенной пользователю ролью.

После завершения пользовательской сессии или истечения времени её действия пользователю необходимо повторно пройти аутентификацию для получения доступа к системе.

При использовании внешних механизмов аутентификации доступ к системе зависит от корректной работы соответствующей службы авторизации.

?????????? ? ?????????? ???????? ????????

Зона ответственности: Printum

> **Коротко:** Printum поддерживает автоматическую и административную блокировку учетных записей пользователей, ручную разблокировку пользователей, а также централизованное управление учетными записями через панель администрирования.

??????????

Система должна обеспечивать управление жизненным циклом учетных записей пользователей и предотвращать несанкционированный доступ при нарушении требований безопасности.

Блокировка учетных записей позволяет ограничить доступ к системе при попытках подбора пароля, длительном отсутствии активности пользователя или иных событиях, определенных политикой безопасности организации.

??? ??? ??????????? ? Printum

Управление учетными записями пользователей осуществляется через панель администрирования системы.

Администратор может:

- создавать и изменять учетные записи пользователей;
- изменять параметры пользователей;
- назначать роли;
- назначать парольные политики;
- изменять пароль пользователя;
- принудительно требовать смену пароля при следующем входе пользователя в систему.

В рамках парольной политики поддерживается автоматическая блокировка пользователей после превышения допустимого количества неудачных попыток авторизации.

Для настройки доступны следующие параметры:

- количество попыток авторизации до блокировки;
- период блокировки после неудачной авторизации.

Дополнительно поддерживается автоматическая блокировка пользователей при длительном отсутствии активности в системе. Для этого может быть настроен период отслеживания неактивности пользователя.

Администратор системы может вручную разблокировать пользователя через панель администрирования, не дожидаясь окончания периода блокировки.

Настройки блокировки могут отличаться для различных пользователей и подразделений в зависимости от назначенной парольной политики.

?????????? ? ??????????

При использовании доменной авторизации блокировка учетной записи пользователя в службе каталогов может ограничивать возможность входа в систему независимо от настроек Printum.

После изменения пароля пользователя администратором при следующем входе в систему пользователю может потребоваться установить новый пароль.

Автоматическая блокировка пользователей выполняется в соответствии с параметрами назначенной парольной политики.

???????? ????????????? ? ?????? ???? (SSO)

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает доменную аутентификацию и единый вход через LDAP/Active Directory, SAML 2.0 и Kerberos/GSSAPI. Пользователи, группы и организационная структура могут синхронизироваться из корпоративной службы каталогов.

??????????

Система должна поддерживать централизованную аутентификацию пользователей через корпоративную инфраструктуру управления учётными записями.

Использование доменной аутентификации и единого входа позволяет централизованно управлять пользователями, применять корпоративные политики безопасности и снизить необходимость ведения отдельных локальных учётных записей.

??? ??? ??????????? ? Printum

Printum поддерживает интеграцию с корпоративными службами каталогов и механизмами единого входа.

Поддерживаются следующие механизмы аутентификации:

- LDAP / Active Directory;
- SAML 2.0;
- Kerberos / GSSAPI.

LDAP / Active Directory

Printum поддерживает синхронизацию пользователей, групп и организационной структуры из службы каталогов.

Поддерживаются:

- Microsoft Active Directory;
- FreeIPA;

- Samba DC;
- РЕД АДМ;
- ALD Pro.

Синхронизация выполняется независимо для каждого подключённого домена. Ошибки синхронизации одного домена не блокируют обработку остальных доменов.

Пользователи, отсутствующие в службе каталогов в течение нескольких циклов синхронизации, автоматически помечаются как удалённые в домене.

SAML 2.0

Printum поддерживает аутентификацию через внешнего поставщика удостоверений (Identity Provider) по протоколу SAML 2.0.

Автоматическое создание неизвестных пользователей при входе через SAML не используется. Пользователь должен быть предварительно создан или синхронизирован в Printum.

Kerberos / GSSAPI

Printum поддерживает доменную аутентификацию через Kerberos/GSSAPI.

При использовании Kerberos возможно применение механизмов сквозной доменной аутентификации в соответствии с настройками инфраструктуры организации.

????????????? ?????????????

Для SAML и Kerberos настраивается правило сопоставления пользователя внешней системы с учётной записью Printum.

После успешной аутентификации пользователю предоставляется доступ в соответствии с назначенной ролью и действующей моделью разграничения доступа.

??? ????????? ?? ??????????????

Настройка и сопровождение LDAP/Active Directory, SAML, Kerberos/GSSAPI и связанных политик безопасности выполняются администраторами инфраструктуры заказчика.

Для использования доменной аутентификации должны быть настроены соответствующие службы каталогов, поставщики удостоверений и необходимые параметры доверия между системами.

?????????????? ?
??????????????
??????????????

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Printum поддерживает локальную и централизованную аутентификацию пользователей, а также различные способы авторизации на устройствах. Конкретные методы аутентификации зависят от используемых компонентов системы и инфраструктуры заказчика.

??????????

Система должна обеспечивать однозначную идентификацию пользователей и подтверждение их подлинности перед предоставлением доступа к функциям и данным.

Аутентификация пользователей позволяет исключить несанкционированный доступ к системе, обеспечить применение политик безопасности и связать действия пользователя с его учетной записью.

??? ??? ??????????? ? Printum

Перед предоставлением доступа к защищенным функциям системы пользователь проходит процедуру аутентификации.

Printum поддерживает несколько способов аутентификации пользователей:

????????? ??????????????

Для пользователей, созданных непосредственно в системе, используется аутентификация по имени пользователя и паролю.

Парольная политика, блокировка пользователей и управление жизненным циклом учетных записей выполняются средствами Printum.

?????????????? ??????????????

Printum поддерживает интеграцию с корпоративными службами каталогов и системами единого входа.

Поддерживаются:

- LDAP;
- Microsoft Active Directory;
- Kerberos / GSSAPI;
- SAML 2.0.

В этом случае аутентификация пользователей выполняется средствами корпоративной инфраструктуры.

?????????? ?? ??????????

Для встроенных приложений и сценариев защищенной печати поддерживаются различные способы авторизации пользователей на устройствах.

В зависимости от производителя устройства, модели МФУ и используемого встроенного приложения могут использоваться:

- логин и пароль;
- PIN-код;
- RFID-карта;
- иные поддерживаемые производителем механизмы идентификации пользователя.

???????????? ???????? ????????????

После успешной аутентификации действия пользователя в системе выполняются от имени его учетной записи и могут использоваться для применения политик безопасности, разграничения доступа и регистрации событий безопасности.

??? ????????? ?? ??????????????

При использовании LDAP, Active Directory, Kerberos или SAML настройка и сопровождение соответствующих служб выполняются администраторами инфраструктуры заказчика.

Управление доменными учетными записями, группами пользователей и парольными политиками осуществляется средствами корпоративной инфраструктуры.

??????????? ? ???????????

Доступность конкретных способов аутентификации зависит от используемых компонентов системы и конфигурации инфраструктуры.

Доступность способов авторизации на МФУ зависит от производителя устройства, модели МФУ и возможностей установленного встроенного приложения.

При использовании централизованной аутентификации требования к паролям, срокам их действия и блокировке пользователей определяются соответствующей службой аутентификации.

????????? ????????

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает настраиваемую парольную политику для локальных пользователей системы. Администратор может управлять требованиями к сложности паролей, сроками их действия, историей использования, блокировкой пользователей и параметрами пользовательских сессий.

??????????

Система должна обеспечивать контроль требований к паролям пользователей, предотвращать использование слабых паролей и обеспечивать защиту учётных записей от несанкционированного доступа.

Парольная политика позволяет реализовать требования организации к сложности паролей, срокам их действия и процедурам управления учётными записями пользователей.

??? ??? ???????????? ? Printum

Для локальных пользователей Printum поддерживает настраиваемые парольные политики.

Администратор может создавать несколько парольных политик и назначать их отдельным пользователям, группам пользователей или подразделениям.

В рамках парольной политики могут настраиваться:

- минимальная длина пароля;
- минимальное количество букв;
- минимальное количество цифр;
- минимальное количество специальных символов;
- срок действия пароля;
- период обязательной смены пароля;
- период запрета повторной смены пароля;
- максимальное количество неудачных попыток аутентификации;
- период блокировки после неудачных попыток входа;
- период блокировки неактивных пользователей;
- количество ранее использованных паролей, запрещённых к повторному использованию;
- период, в течение которого ранее использованные пароли считаются уникальными;

- требование смены пароля при первом входе в систему;
- запрет последовательностей одинаковых символов;
- запрет цифровых и алфавитных последовательностей;
- запрет использования визуально похожих символов («I», «l», «1»).

Printum поддерживает хранение истории паролей и может запрещать повторное использование ранее применявшихся паролей.

При изменении парольной политики пользователи, чьи пароли перестали соответствовать новым требованиям, могут быть обязаны сменить пароль при следующем входе в систему.

Для защиты учётных записей поддерживается автоматическая блокировка пользователя после заданного количества неуспешных попыток аутентификации.

Также поддерживается автоматическая блокировка пользователей, не использовавших систему в течение установленного периода времени.

???????? ???????

Пароли пользователей не хранятся в открытом виде.

Для хранения паролей используются стандартные механизмы Django на основе алгоритма PBKDF2 с HMAC-SHA256 и индивидуальной криптографической солью для каждого пароля.

В процессе аутентификации система выполняет проверку хэша пароля без хранения или передачи пароля в открытом виде.

??? ????????? ?? ??????????????

При использовании локальной аутентификации параметры парольной политики определяются администраторами Printum.

При использовании доменной аутентификации, LDAP, Active Directory, Kerberos или SAML требования к паролям, срокам их действия и блокировке пользователей определяются соответствующей службой аутентификации организации.

??????????? ? ???????????

Парольная политика применяется только к локальным пользователям Printum.

Для пользователей, аутентифицируемых через внешние службы каталогов или системы единого входа, требования к паролям определяются средствами соответствующей инфраструктуры.

??????? ?????? RBAC

Зона ответственности: Printum

> **Коротко:** В Printum реализована гибкая ролевая модель (RBAC), позволяющая разграничивать доступ пользователей к функциям системы, данным, локациям и административным интерфейсам в соответствии с их должностными обязанностями.

??????????

Система должна обеспечивать разграничение прав доступа пользователей и администраторов в соответствии с их полномочиями.

Ролевая модель позволяет реализовать принцип минимальных привилегий, ограничить доступ к функциям системы и данным пользователей, а также разделить административные обязанности между различными категориями сотрудников.

??? ??? ???????????? ? Printum

В Printum используется ролевая модель управления доступом (RBAC), в рамках которой пользователю назначается роль, определяющая его полномочия в системе.

При настройке роли администратор может управлять доступом по нескольким направлениям:

- набор доступных функций;
- уровень доступа к данным пользователей;
- уровень доступа к локациям;
- права администрирования филиалов;
- доступ к административным панелям системы.

При установке системы создаются базовые роли:

- Пользователь;
- Оператор;
- Инженер;
- Администратор;

- Сотрудник СБ.

В зависимости от назначенной роли пользователю могут предоставляться права на:

- работу с устройствами;
- работу со складом;
- просмотр журналов;
- работу с заданиями печати;
- просмотр журнала информационной безопасности;
- управление пользователями;
- управление принтерами;
- управление правилами печати;
- управление интеграциями;
- управление агентами мониторинга;
- управление системными настройками;
- управление импортом и экспортом данных;
- управление локациями и филиалами.

При импорте пользователей из службы каталогов для них может автоматически назначаться роль по умолчанию, определённая администратором системы.

Администратор может изменить роль по умолчанию или назначить импортированным пользователям другие роли в соответствии с принятой моделью разграничения доступа.

Администратор системы может создавать собственные роли, комбинируя необходимые функции и уровни доступа, а также назначать роль по умолчанию для новых пользователей.

?????????? ? ??????????

Фактический набор доступных функций определяется назначенной пользователю ролью.

При изменении роли пользователя новые полномочия начинают действовать после повторной авторизации пользователя в системе.

????-??? ?????? ? ?????????????? ?????????? ??????

Зона ответственности: Printum

> **Коротко:** Printum поддерживает ограничение времени жизни пользовательских сессий, автоматическое завершение сеансов при бездействии пользователя и контроль одновременных сессий.

??????????

Система должна обеспечивать автоматическое завершение пользовательских сессий после истечения заданного периода времени или отсутствия активности пользователя.

Данный механизм снижает риск несанкционированного доступа к системе в случаях, когда пользователь оставил рабочее место без завершения работы или не выполнил выход из системы вручную.

??? ??? ??????????? ? Printum

Управление пользовательскими сессиями осуществляется в рамках парольной политики.

Для каждой парольной политики могут быть настроены следующие параметры:

- общее время пользовательской сессии;
- максимальное время неактивности пользователя;
- максимальное время неактивности пользователя на принтере;
- разрешение или запрет одновременных сессий пользователя.

По истечении установленного времени действия сессии пользователь автоматически теряет авторизацию в системе.

Если пользователь не выполняет действий в течение заданного периода времени, его сессия автоматически завершается. При следующем обращении к панели администрирования или

Личному кабинету пользователю потребуется повторно пройти аутентификацию.

Для работы на устройствах также может быть настроен отдельный тайм-аут неактивности пользователя на принтере.

Printum поддерживает контроль одновременных сессий пользователя. Если использование дублирующих сессий запрещено, открытие новой сессии приводит к завершению ранее открытой сессии этого пользователя.

Администратор системы может принудительно завершать активные пользовательские сессии через раздел управления сессиями в панели администрирования.

?????????? ? ??????????

Изменение параметров управления пользовательскими сессиями применяется только к новым сессиям после повторной авторизации пользователя.

При запрете дублирующих сессий открытие новой сессии приводит к завершению предыдущей сессии пользователя. Несохраненные изменения могут быть потеряны.

После завершения сессии пользователю необходимо повторно пройти аутентификацию для продолжения работы с системой.

?????????? ??????? ??????

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Для взаимодействия внутренних компонентов и интеграции с внешними сервисами Printum использует отдельные технические учётные записи. Пароли технических сервисов могут изменяться администраторами системы и не связаны с учётными записями пользователей.

??????????

Система должна обеспечивать использование отдельных технических учётных записей для выполнения служебных операций и взаимодействия компонентов системы.

Использование сервисных учётных записей позволяет разделить действия пользователей и внутренних процессов системы, а также обеспечить независимое управление их полномочиями и учётными данными.

??? ??? ???????????? ? Printum

Для работы внутренних сервисов и компонентов Printum используются отдельные технические учётные записи и сервисные пароли.

В зависимости от конфигурации системы технические учётные записи могут использоваться для:

- PostgreSQL;
- Redis;
- ClickHouse;
- CUPS;
- FTP;
- служб каталогов;
- других интеграционных сервисов.

Пароли сервисов хранятся отдельно от пользовательских учётных записей и могут быть изменены администратором системы.

Для большинства внутренних сервисов при установке используются автоматически сгенерированные сложные пароли.

Рекомендуется использовать пароли длиной не менее 16 символов с использованием цифр, букв разных регистров и специальных символов.

Администратор может изменять пароли технических сервисов без изменения пользовательских учётных записей.

В отказоустойчивых конфигурациях изменение паролей должно быть синхронизировано между всеми компонентами системы, использующими соответствующий сервис.

??? ????????? ?? ????????????

Для подключения к внешним системам могут использоваться отдельные технические учётные записи.

К таким системам относятся:

- LDAP и Active Directory;
- SMTP-серверы;
- FTP-серверы;
- другие внешние сервисы, используемые в конкретной инфраструктуре.

Создание, сопровождение и управление жизненным циклом таких учётных записей выполняется администраторами инфраструктуры заказчика.

При изменении паролей внешних сервисов соответствующие параметры подключения должны быть обновлены в настройках Printum.

?????????? ? ??????????

Пароли технических сервисов не связаны с пользовательскими учётными записями и не изменяются средствами парольной политики пользователей.

После изменения паролей внутренних сервисов может потребоваться обновление конфигурационных файлов и перезапуск компонентов системы.

В отказоустойчивых конфигурациях изменение паролей должно быть выполнено на всех узлах, использующих соответствующий сервис.

Для хранения конфиденциальных параметров конфигурации может использоваться шифрование конфигурационных файлов средствами системы.