

4. ??????????

Интеграции с внешними системами: AD, LDAP, SMTP, SSO и другие

- [Интеграция с контроллерами домена](#)
 - [Интеграция с FreeIPA](#)
 - [Интеграция с Samba DC и РЕД АДМ](#)
 - [Интеграция с ALD Pro](#)
 - [Интеграция с Active Directory](#)
 - [Настройка атрибутов домена](#)
 - [Расписание синхронизации с доменом](#)
 - [Как работает синхронизация пользователей с доменом](#)
 - [Объединение доменных учётных записей одного пользователя](#)
 - [Назначение ролей через группы домена](#)
 - [Доменная авторизация и SSO — как работает](#)
 - [Гостевая печать через email — как работает](#)
- [Интеграция с почтовым сервером \(SMTP\)](#)
 - [Настройка подключения к почтовому серверу](#)
 - [Настройка печати через почту](#)
 - [Настройка гостевой печати через почту](#)
- [Отправка событий в SIEM \(Syslog\)](#)
 - [Настройка отправки событий в Syslog](#)
- [SSO](#)
 - [Настройка SSO через SAML 2.0 в Microsoft AD FS](#)
 - [Настройка SSO через Kerberos](#)
 - [Авторизация через доменную учётную запись на МФУ](#)
 - [Методы аутентификации в Принтум — обзор](#)

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

- **Выгружать оргструктуру** — включить для импорта иерархии на основе OU домена.
- **Выгружать группы** — включить для выгрузки групп безопасности.
- **Требуется шифрование** — включить, если домен принимает только зашифрованные запросы.

??? 2. ?????????? ????????

Нажмите кнопку «**Тестовый импорт**». При успешном подключении будет отображено количество отделов, сотрудников и групп. При ошибке — описание проблемы.

??? 3. ?????????????????? ??????????????

В разделе «**Атрибуты**» карточки домена настройте сопоставление атрибутов FreeIPA с полями Printum:

| Поле Printum | Атрибут FreeIPA | | ----- | ----- | | Login (username) | uid | | Идентификатор в домене (unique_id) | uidNumber | | Фамилия (last_name) | sn | | Имя (first_name) | givenName | | Отчество (patronymic) | personalTitle | | Адрес электронной почты (email) | mail | | Доменные группы (domain_groups) |memberOf | | Должность (position) | title | | Путь к папке (smb_path) | homeDirectory | | Срок действия аккаунта (account_expires_at) | krbPrincipalExpiration | | Аккаунт заблокирован (account_lock) | nsAccountLock |

Обязательные атрибуты: Логин, Фамилия, Имя, Идентификатор в домене, Адрес электронной почты.

??? 4. ?????????????? ? ?????????????? ?????????????????

Нажмите «**Сохранить**». В разделе «**Расписание**» настройте периодическую автоматическую синхронизацию (расписание общее для всех доменов).

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

После успешной настройки пользователи из FreeIPA синхронизируются в Printum. Оргструктура и группы импортируются согласно настройкам.

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

- Тестовый импорт показывает количество отделов, сотрудников и групп без ошибок.
 - Пользователи из FreeIPA отображаются в разделе «Сотрудники» системы Printum.
-

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

- [Интеграция с Samba DC и РЕД АДМ](#)
-

Справочник атрибутов: [Атрибуты доменов — справочник](#) — сравнительная таблица по всем контроллерам домена.

Интеграция с контроллерами домена

???????????? ? Samba DC ? ??? ???

????

Настройка интеграции Printum с контроллерами домена Samba DC и РЕД АДМ для синхронизации учётных записей пользователей, импорта оргструктуры и групп безопасности.

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

- Развёрнутый и доступный сервер Samba DC или РЕД АДМ
 - Учётная запись в домене с правами на чтение доменной структуры
 - Настроена интеграция с почтовым сервером (SMTP)
 - Printum запущен и доступен
-

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

??? 1. ????????????? ??????? ? Printum

Перейдите в раздел **Настройки** → **Интеграции** → **Домены** и нажмите кнопку «**Добавить**».

Заполните поля:

- **Название** — любое удобное название для домена.
- **Тип** — выберите соответствующий тип (или).
- **Адрес** — протокол, хост и порт домена (например,).
- **Логин и пароль в домене** — учётная запись с правами на чтение доменной структуры.
- **Фильтр** — фильтр поиска сотрудников. Если оставить пустым, будут импортированы объекты классов Person и User.

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

- Тестовый импорт показывает количество отделов, сотрудников и групп без ошибок.
 - Пользователи из домена отображаются в разделе «Сотрудники» Printum.
-

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

- [Интеграция с FreeIPA](#)
 - [Интеграция с ALD Pro](#)
-

Справочник атрибутов: [Атрибуты доменов — справочник](#) — сравнительная таблица по всем контроллерам домена.

Интеграция с контроллерами домена

???????????? ? ALD Pro

????

Настройка интеграции Printum с контроллером домена ALD Pro для синхронизации учётных записей пользователей, импорта оргструктуры и групп безопасности.

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

- Развёрнутый и доступный сервер ALD Pro
 - Учётная запись в домене с правами на чтение доменной структуры
 - Настроена интеграция с почтовым сервером (SMTP)
 - Printum запущен и доступен
-

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

??? 1. ????????????? ??????? ? Printum

Перейдите в раздел **Настройки** → **Интеграции** → **Домены** и нажмите кнопку «**Добавить**».

Заполните поля:

- **Название** — любое удобное название для домена.
- **Тип** — выберите .
- **Адрес** — протокол, хост и порт домена (например,).
- **Логин и пароль в домене** — учётная запись с правами на чтение доменной структуры.
- **Фильтр** — фильтр поиска сотрудников. Если оставить пустым, будут импортированы объекты классов Person и User.
- **Стартовый уровень поиска** — уровень в домене для начала импорта (обычно самый верхний).
- **Выгружать оргструктуру** — включить для импорта иерархии. **Важно:** в ALD Pro нет разделения между группами и отделами, поэтому все отделы будут импортированы как группы.

- **Выгружать группы** — включить для выгрузки групп безопасности.
- **Требуется шифрование** — включить, если домен принимает только зашифрованные запросы.

??? 2. ?????????? ????????

Нажмите кнопку «**Тестовый импорт**». При успешном подключении будет отображено количество отделов, сотрудников и групп.

??? 3. ?????????????????? ????????????

Настройте сопоставление в разделе «**Атрибуты**» карточки домена. Атрибуты ALD Pro отличаются от FreeIPA/Samba в части отчества и срока действия аккаунта:

| Поле Printum | Атрибут ALD Pro | | ----- | ----- | | Логин (username) | uid | | Идентификатор в домене (unique_id) | uidNumber | | Фамилия (last_name) | sn | | Имя (first_name) | givenName | | Отчество (patronymic) | rbtamiddlename | | Адрес электронной почты (email) | mail | | Доменные группы (domain_groups) | memberOf | | Должность (position) | title | | Путь к папке (smb_path) | homeDirectory | | Срок действия аккаунта (account_expires_at) | krbPasswordExpiration | | Аккаунт заблокирован (account_lock) | nsAccountLock |

Обязательные атрибуты: Логин, Фамилия, Имя, Идентификатор в домене, Адрес электронной почты.

??? 4. ?????????????? ? ??????????????? ??????????????????

Нажмите «**Сохранить**». В разделе «**Расписание**» настройте периодическую синхронизацию (расписание общее для всех доменов).

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

Пользователи из ALD Pro синхронизируются в Printum. Поскольку в ALD Pro нет разделения между группами и отделами, все отделы импортируются как группы безопасности.

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

- Тестовый импорт показывает количество отделов, сотрудников и групп без ошибок.
 - Пользователи из ALD Pro отображаются в разделе «Сотрудники» Printum.
-

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

- [Интеграция с FreeIPA](#)
 - [Интеграция с Samba DC и РЕД АДМ](#)
-

Справочник атрибутов: [Атрибуты доменов — справочник](#) — сравнительная таблица по всем контроллерам домена.

????????? ? Active Directory

?????

Настройка интеграции Printum с Microsoft Active Directory для синхронизации пользователей, оргструктуры и групп безопасности.

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

- Развёрнутый и доступный контроллер домена Microsoft Active Directory
 - Учётная запись с правами на чтение доменной структуры (обычно доменный администратор)
 - Настроена интеграция с почтовым сервером (SMTP)
 - Printum запущен и доступен
-

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

??? 1. ??????????????????????

Перейдите в **Настройки** → **Интеграции** → **Домены** и нажмите **«Добавить»**. Заполните поля:

- **Название** — любое удобное название.
- **Тип** — выберите `Microsoft Active Directory`.
- **Адрес** — протокол, хост и порт (например, `ldap://dc.example.com:389` или `ldaps://dc.example.com:636`).
- **Логин и пароль** — УЗ с правами чтения доменной структуры.
- **Фильтр** — фильтр поиска сотрудников (пусто = импорт Person и User).
- **Стартовый уровень поиска** — обычно верхний уровень домена.
- **Атрибут для объединения учётных записей** — например, табельный номер для связи УЗ из разных доменов.
- **Выгружать оргструктуру** — включить для импорта иерархии по OU.
- **Выгружать группы** — включить для выгрузки групп безопасности.

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

- [Настройка атрибутов домена](#)
- [Расписание синхронизации с доменом](#)

Справочник атрибутов: [Атрибуты доменов — справочник](#) — сравнительная таблица по всем контроллерам домена.

Интеграция с контроллерами домена

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

????

Сопоставление атрибутов LDAP-домена с полями пользователей в системе Printum для корректного импорта данных.

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

- Домен добавлен в Printum (Настройки → Интеграции → Домены)
 - Тестовый импорт выполнен успешно
-

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

В таблице доменов раскройте карточку нужного домена (иконка в левом столбце строки). Перейдите в раздел **«Атрибуты»**.

Во время первоначальной настройки (мастер установки) нажмите **«Посмотреть атрибуты»** после успешного тестового импорта.

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

Для успешной интеграции должны быть заполнены:

- Логин
 - Фамилия
 - Имя
 - Идентификатор в домене
 - Адрес электронной почты
-

- [Интеграция с ALD Pro](#)
-

Справочник атрибутов: [Атрибуты доменов — справочник](#) — сравнительная таблица по всем контроллерам домена.

Интеграция с контроллерами домена

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

????

Настройка автоматической периодической синхронизации пользователей и оргструктуры из домена в Printum.

??????????

- Домен добавлен и успешно протестирован в Printum
 - Атрибуты домена сопоставлены
-

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

В карточке домена (Настройки → Интеграции → Домены) перейдите в раздел **«Расписание»**.

Важно: расписание синхронизации является общим для всех доменов — изменение расписания в одном домене применится ко всем остальным.

Укажите желаемую периодичность синхронизации и сохраните настройки.

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

Для немедленной синхронизации без ожидания планового запуска:

- В режиме карточек — нажмите кнопку **«Синхронизировать»**.
 - В режиме таблицы — нажмите иконку синхронизации (справа от иконки удаления).
-

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

Пользователи, изменения в оргструктуре и группах автоматически применяются в Printum согласно заданному расписанию.

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

- [Настройка атрибутов домена](#)
- [Интеграция с Active Directory](#)
- [Интеграция с FreeIPA](#)

Интеграция с контроллерами домена

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

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

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

Синхронизация с контроллером домена — основной способ импорта пользователей в Принтум. Администратор не создаёт пользователей вручную: они выгружаются из домена автоматически.

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

- Microsoft Active Directory
- FreeIPA
- Samba
- ALD Pro (под капотом та же Samba с доработками)
- RedDem (за основу взята Samba)
- LDAP-совместимые каталоги

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

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

Синхронизация проходит через два уровня:

1. Контроллер домена → Мониторинг: данные выгружаются и агрегируются.
2. Мониторинг → ПринтМенеджер: пользователи передаются в систему управления.

“ Схема движения данных: AD/LDAP → Мониторинг → ПринтМенеджер

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

В рамках синхронизации из домена выгружается набор атрибутов:

- Логин (accountName)
- Фамилия (SN)
- Имя (givenName)
- Должность
- Отдел
- Группы
- Табельный номер
- Email (mail)
- Номер карты (если есть в домене)

Перечень атрибутов конечный. Доменный **пароль не выгружается и не хранится** в Принтум.

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

Принцип аналогичен интерпретации SNMP-данных в Мониторинге: каждому атрибуту системы указывается, в каком поле домена хранится нужное значение.

Из коробки подставлены стандартные значения атрибутов. Однако администраторы домена могут хранить данные нестандартно. Например:

- табельный номер может быть записан в поле телефона;
- номер карты — в произвольном extensionAttribute.

Если стандартное соответствие не подходит, администратор изменяет маппинг атрибутов в настройках синхронизации и проверяет, что нужное значение появляется корректно.

??? ??????????????????: ??? . ??????????????
??? ??????????

При настройке синхронизации выбирается, что выгружать из домена:

- **Орг. структура (OU)** — подразделения и отделы.
- **Группы безопасности** — произвольные группы пользователей.
- Оба варианта одновременно.

Классически: отделы управляются через OU, произвольные группы — через группы безопасности. Встречаются заказчики, у которых отдел — это группа, а не OU.

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

Не обязательно выгружать всех пользователей домена. Используются стандартные LDAP-фильтры:

- Можно выгрузить только конкретный отдел.
- Удобно для пилотного проекта: взять IT-отдел и работать только с ними.

После того как фильтры и соответствие атрибутов настроены, система будет автоматически поддерживать данные в актуальном состоянии.

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

Синхронизация происходит регулярно по расписанию. **Минимальный интервал — не чаще одного раза в 4 часа.** Для большинства случаев нескольких синхронизаций в день достаточно.

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

- [Модель пользователей в Принтум](#)
- [Объединение доменных учётных записей одного пользователя](#)
- [Назначение ролей через группы домена](#)

Интеграция с контроллерами домена

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

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

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

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

Один физический сотрудник может иметь несколько доменных учётных записей в разных доменах. Принтум позволяет связать их с одним Printum ID, чтобы правила, квоты и статистика применялись к человеку в целом.

????????????????????????????: ????? ? ??????

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

В организациях с разделёнными сетевыми контурами (например, закрытый и открытый контур банка) сотрудник может иметь:

- учётную запись в закрытом контуре — для работы с конфиденциальными данными;
- учётную запись в открытом контуре — для работы с интернет-ресурсами.

Физически это один человек. Его правила печати, квоты и статистика должны быть общими, независимо от того, с какого контура он печатает.

??

????????

При настройке синхронизации задаётся **атрибут для объединения**. Если у двух доменных учётных записей совпадает значение этого атрибута, они будут привязаны к одному Printum ID при импорте.

Типичные атрибуты для объединения:

- **Email (mail)** — если корпоративный email прописан в обеих учётках.
- **Табельный номер** — если он хранится в каком-либо атрибуте домена (например, в поле telephoneNumber).

“ Пример: у сотрудника Дмитрия есть учётка в закрытом контуре (d.dvoynikov@internal) и учётка в открытом контуре (d.dvoynikov@bank.ru). В обеих учётках в поле mail прописан один и тот же email — d.dvoynikov@bank.ru. При синхронизации Принтум определит совпадение и привяжет обе учётки к одному Printum ID.

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

После объединения:

- Правила печати применяются к Printum ID — одинаково для обеих учётки.
- Квоты считаются суммарно по всем учёткам.
- Статистика печати объединяется.
- Роли назначаются на уровне Printum ID.

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

- [Модель пользователей в Принтум](#)
- [Как работает синхронизация пользователей с доменом](#)

Интеграция с контроллерами домена

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

Назначение Принтум позволяет автоматически назначать роли, правила печати и МФУ для прямой печати на основе членства пользователей в группах домена. Администратор управляет доступами к печати так же, как управляет любыми другими правами — через контроллер домена. Что такое роль в Принтум Роль определяет: Доступ к данным — по локациям (например, только московский филиал) и по пользователям (собственные данные, конкретные сотрудники или группа). Доступный функционал — что пользователь может делать в системе. Стандартные роли поставляются из коробки. При необходимости можно создать свою роль: с нуля или клонировав существующую с добавлением/удалением прав. Роль можно задать как роль по умолчанию — она будет присваиваться всем новым пользователям при импорте. Как работает назначение роли через группу домена Группы домена синхронизируются в Принтум вместе с пользователями. В Принтум для группы настраивается соответствующая роль. При синхронизации все члены группы получают указанную роль. Новый сотрудник, добавленный в группу в домене, при следующей синхронизации автоматически получает нужную роль в Принтум — без каких-либо действий в самом Принтум. Пример: в домене есть группа «Администраторы». В Принтум для этой группы настроена роль «Администратор». Заказчик нанял нового IT-специалиста, добавил его в домене в группу «Администраторы». При следующей синхронизации пользователь появится в Принтум уже с ролью «Администратор» — в самом Принтум ничего настраивать не нужно. Назначение правил через группы Аналогично ролям, через группы домена можно автоматически применять правила печати. Правило — это условие (атрибуты задания: количество страниц, цветность, формат) плюс действие (запретить, разрешить только на определённых устройствах и т.д.). Пример: администратор создаёт в домене группу «Запрет цветной печати». В Принтум для этой группы задаётся правило — запрет цветной печати. Чтобы ограничить нового сотрудника, достаточно добавить его в эту группу в домене. После синхронизации запрет применится автоматически. Назначение МФУ для прямой печати через группы Если используется схема с Клиентом ПМ, МФУ для прямой печати (без авторизации) также назначаются через группы домена или OU. Пример: для OU «Бухгалтерия» назначен МФУ Куосега для прямой печати. Клиент ПМ автоматически создаёт этот МФУ на рабочей станции каждого сотрудника бухгалтерии. Новый бухгалтер появляется в домене в OU «Бухгалтерия» — при следующей синхронизации у него на компьютере сам по себе появится нужный МФУ. Администратору Принтум ничего делать не нужно. Итог: интеграция в процесс управления пользователями За счёт синхронизации с доменом Принтум встраивается в привычный для администраторов процесс управления доступами. Нанимая, увольняя или перемещая сотрудников между группами в контроллере домена, администратор одновременно управляет и их доступами к печати. Связанные страницы Как работает синхронизация пользователей с доменом Модель пользователей в Принтум

Интеграция с контроллерами домена

????????? ?????????????? ? SSO
— ??? ???????????

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

Начиная с версии 4.2, Принтум поддерживает доменную авторизацию и Single Sign-On (SSO). Это позволяет пользователям входить в Личный кабинет с помощью доменного логина и пароля, не создавая отдельный пароль в Принтум.

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

Это ключевой принцип безопасности. Принтум:

- не импортирует доменные пароли;
- не хранит доменные пароли;
- не кэширует credentials пользователей.

При авторизации с доменным паролем Принтум передаёт введённые учётные данные контроллеру домена и проверяет корректность пароля **на стороне контроллера домена**. В самой системе пароль не сохраняется.

??? ?????????????? ?? ?????????? 4.2

В версии 4.1 пользователь при входе в Личный кабинет вводил:

- Логин — доменный (импортированный при синхронизации).
- Пароль — внутренний пароль Принтум (не доменный).

Внутренний пароль задавался самим пользователем через почту. Это не создавало проблем безопасности, но часто требования заказчиков предполагали использование исключительно доменного пароля.

????????????? ?????????????????? (????????? 4.2+)

В Личном кабинете появляется кнопка «**Авторизоваться с помощью доменного логина и пароля**».

Оба варианта авторизации могут работать параллельно:

- Внутренний пароль Принтум — для тех, кто его создал.
- Доменный пароль — для тех, кто предпочитает использовать корпоративные учётные данные.

Если заказчик переходит на доменную авторизацию, внутренняя парольная политика Принтум становится менее актуальной: пароли соответствуют требованиям политики домена.

SSO (Single Sign-On)

SSO добавлен в версии 4.2. При использовании SSO пользователю не нужно вводить логин и пароль вручную — авторизация происходит автоматически на основе текущей доменной сессии.

В Личном кабинете появляется кнопка входа через SSO.

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

Принтум поддерживает настраиваемые парольные политики для внутренних паролей:

- Минимальная длина.
- Требования к составу (цифры, спецсимволы).
- Срок действия пароля.
- Требование смены пароля.

Можно задать несколько парольных политик для разных групп пользователей. Есть политика по умолчанию. При использовании доменной авторизации настройка внутренней политики остаётся на усмотрение администратора.

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

- [Модель пользователей в Принтум](#)
- [Как работает синхронизация пользователей с доменом](#)

Интеграция с контроллерами домена

????????? ??????? email
— ??? ??????????

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

Гостевая печать через email позволяет напечатать документ пользователю, которого нет в домене и в Принтум. Это удобно для посетителей, внешних подрядчиков и любых людей, у которых нет корпоративной учётной записи.

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

1. Администратор создаёт специальный почтовый ящик для приёма документов на печать (например, `print@company.ru`).
2. Гость отправляет документ как вложение к письму на этот адрес (например, с планшета или личного телефона).
3. Принтум автоматически создаёт для него временную учётную запись.
4. Гостю в ответ приходит письмо с PIN-кодом.
5. Гость подходит к устройству, вводит PIN-код, видит своё задание (или несколько, если отправил несколько писем) и выбирает, что распечатать.

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

- Функционал должен быть включён администратором в настройках Принтум.
- Документ передаётся как вложение к письму.
- Доступ к физическому устройству необходим для получения распечатки.

“ Даже если посторонний человек узнает адрес почтового ящика и отправит туда документ, получить распечатку он не сможет: для этого нужен физический доступ к устройству и PIN-код из ответного письма.

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

Функционал «печать через email» используется в двух сценариях:

- **Гостевая печать** — пользователь не в домене, не в Принтум. Ему автоматически создаётся временная учётная запись и высылается PIN-код.
- **Печать сотрудника через почту** — сотрудник, который уже есть в системе, отправляет документ по почте. Он авторизуется под своей существующей учётной записью, PIN-код не нужен.

????????

Функционал прошёл стресс-тест: система Принтум участвовала в мероприятии, где сотрудники 17 организаций одновременно использовали печать через email.

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

- [Модель пользователей в Принтум](#)

???????????? ? ??????????
?????????? (SMTP)

Интеграция с почтовым сервером (SMTP)

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

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

?????

Подключение Printum к SMTP-серверу для отправки уведомлений, восстановления паролей и системных писем.

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

- SMTP-сервер доступен из сети, где развёрнут Printum
 - Имеется учётная запись для аутентификации на SMTP-сервере
-

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

??? 1. ?????????? ??????????

Перейдите в **Настройки** → **Интеграции** → **Почта**.

??? 2. ?????????????? ?????? ??????????????????

- **SMTP-сервер** — адрес сервера по имени или IP-адресу.
- **Порт SMTP-сервера** — порт для подключения.
- **Имя пользователя** — логин для аутентификации на SMTP-сервере.
- **Пароль** — пароль для аутентификации.
- **Адрес отправителя** — адрес, от имени которого приходят письма. Обычно SMTP-серверы требуют совпадения с параметром «Имя пользователя».
- **Адрес службы поддержки** — адрес по умолчанию для получения уведомлений.
- **Использовать TLS** — включить шифрование по протоколу TLS.
- **Использовать SSL** — включить шифрование по протоколу SSL.

??? 3. ?????????? ?????????? ????????

Заполните поле «**Почта для тестового письма**» и нажмите «**Отправить тестовое письмо**»
. Если письмо с темой [Printum] Тестовое сообщение получено — интеграция настроена корректно.

??? 4. ????????????

Нажмите кнопку «**Сохранить**».

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

- Без почты не работают уведомления системы.
 - Вы не получите уведомление об окончании лицензии.
 - Пользователи не смогут сменить или восстановить пароль.
-

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

Тестовое письмо получено. Системные уведомления Printum отправляются через настроенный SMTP-сервер.

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

- [Настройка печати через почту](#)
- [Настройка гостевой печати через почту](#)

Интеграция с почтовым сервером (SMTP)

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

?????

????

Настройка функции отложенной печати через электронную почту: пользователь отправляет письмо с вложением на специальный адрес, вложение добавляется в его персональную очередь печати.

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

Пользователь отправляет письмо с вложением (документ, PDF и др.) на специальный почтовый адрес, настроенный в системе. Загрузка писем выполняется по протоколу IMAP. Вложения автоматически добавляются в персональную очередь пользователя в Printum.

??????????

- Настроена интеграция с почтовым сервером (SMTP)
 - Имеется почтовый ящик для приёма писем с заданиями печати (IMAP-доступ)
-

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

??? 1. ?????????? ?????????? ?????? ????
????????? ??????????

Перейдите в панель администратора ПринтМенеджера: **Настройки → Системные настройки → Настройки электронной почты.**

Укажите адрес почтового ящика в параметре `PRINT_MAILBOX_NAME` — на этот адрес пользователи будут отправлять документы для печати.

??? 2. ?????????? IMAP-?????????????

Настройте параметры IMAP-подключения к почтовому ящику для получения писем системой.

??? 3. ??????????

Отправьте тестовое письмо с документом на настроенный адрес. Убедитесь, что задание появилось в очереди пользователя в Printum.

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

После отправки письма с вложением документ появляется в персональной очереди пользователя и доступен для печати на устройстве.

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

- [Настройка подключения к почтовому серверу](#)
- [Настройка гостевой печати через почту](#)

??? 2. ?????????

Отправьте письмо с документом с адреса, которого нет в списке сотрудников, на адрес `PRINT_MAILBOX_NAME`. Убедитесь, что:

- В мониторинге и ПринтМенеджере создан сотрудник-гость в группе «Гости».
 - На адрес отправителя пришло ответное письмо с PIN-кодом.
 - Гость может авторизоваться на МФУ по PIN-коду и распечатать задание.
-

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

Пользователь, не зарегистрированный в системе, получает PIN-код по почте и может распечатать отправленный документ через МФУ.

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

- [Настройка подключения к почтовому серверу](#)
- [Настройка печати через почту](#)

????????? ???? ? SIEM
(Syslog)

Параметр	Описание
Хост	Адрес и порт сервера Syslog, например <code>192.168.10.10:1514</code> . Допустимые порты: 514, 1514, 1468. Если порт не указан — используется 514
Тип интеграции	Выбрать Syslog
Locations	Локации, события которых передаются. Если не выбрать — передаются все события
Интервал между обменами	Время в минутах (минимум 1 минута)
Включено	Активировать интеграцию после создания
CA сертификат	Для шифрования по TLS — CA-сертификат в формате .pem
Сертификат	Файл SSL-сертификата клиента (.pem, без кодовой фразы)

Важно: авторизация по стандарту Syslog не поддерживается — логин и пароль указывать не нужно.

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

Syslog

- После создания интеграции нажать **«Добавить»** рядом с разделом «Отчёты для отправки» (события или логи безопасности).
- Заполнить поля:
 - Внешняя интеграция** — выбрать созданную интеграцию.
 - Тело отчёта** — поля для включения в отчёт (оставить пустым — передаются все поля).

Для каждой интеграции допускается только один конструктор отчётов. Для передачи данных по нескольким пользователям необходимо создать несколько интеграций.

??????? ?????????? Syslog

Пример лога:

```
2023-05-25T06:15:21.930828+00:00 local Обнаружено новое устройство event=2 user=0ne
additional_parameters={'foo': 0}
2023-05-25T06:32:44.487278+00:00 test.local Обнаружено новое устройство event=4 user=0ne
```

```
location="Офис в Иваново" additional_parameters={'foo': 0}
```

Поля события:

Поле	Тип	Описание
event	число	Уникальный ID события
user	строка	Логин пользователя
location	строка	Название локации (если есть)
additional_parameters	JSON	Дополнительные параметры события

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

Поле	Тип	Описание
event_group	строка	Группа событий
event_name	строка	Название события
event_name_unique_id	число	ID события
timestamp	строка	Время в формате ISO (пример: "2005-08-09T18:31:42")
operation_subject	строка	Субъект операции
operation_object	строка	Объект операции
result	строка	Результат операции
event_level	строка	Уровень критичности
changed_params	JSON	Изменённые параметры

????????? TLS

Для передачи по зашифрованному каналу укажите CA-сертификат и сертификат клиента в формате .pem. Версия TLS выбирается максимально возможная для сервера Syslog. Если нужна конкретная версия TLS — запретите нежелательные протоколы на стороне сервера Syslog.

Для проверки порта Syslog на сервере:

```
netstat -tulnp
```

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

- [Настройка подключения к почтовому серверу](#)
- [Управление пользователями — обзор](#)

SSO

SSO

??????????? SSO ?????? SAML 2.0 ? Microsoft AD FS

?????

Настройка единого входа (SSO) в Принтум через протокол SAML 2.0 с использованием Microsoft Active Directory Federation Services (AD FS) в качестве Identity Provider.

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

- Windows Server 2012 или выше с актуальными обновлениями и патчами
 - SSL-сертификат для домена AD FS (самоподписанный или от доверенного центра сертификации)
 - DNS-запись для ADFS-сервера, например `adfs.yourdomain.com` (или FQDN домена, если ADFS развёрнут на контроллере домена)
 - Настроена интеграция с доменом в Принтум (пользователи импортированы)
 - Сопоставлены атрибуты домена, в том числе `unique_id`
-

??? 1. ?????????????? ?????????? AD FS

DNS

- Если ADFS разворачивается не на контроллере домена — создайте DNS-запись для сервера (например, `adfs.yourdomain.com`).
- Если ADFS разворачивается на контроллере домена — используйте FQDN-имя домена. Чтобы узнать FQDN: откройте оснастку «**Active Directory — пользователи и компьютеры**», раскройте «**Domain Controllers**», выберите запись компьютера, откройте свойства. В строке «**DNS-имя**» будет указана полная запись.

SSL-???????????????

- Получите SSL-сертификат для вашего ADFS-домена: самоподписанный или от доверенного центра сертификации.

2. AD FS

1. Откройте **Server Manager**.
2. Выберите **Add roles and features**.
3. В мастере выберите **Role-based or feature-based installation**.
4. Выберите сервер из пула.
5. На странице выбора ролей выберите **Active Directory Federation Services**.
6. Следуйте инструкциям мастера и завершите установку.

3. AD FS

1. После установки откройте **AD FS Management** из меню **Administrative Tools**.
2. В правой панели выберите **Configure the federation service on this server**.
3. Выберите **Create the first federation server in a federation server farm**.
4. Укажите имя вашего SSL-сертификата.
5. Укажите имя вашего ADFS-сервера (например, `adfs.yourdomain.com`).
6. Укажите учётные данные администратора для создания базы данных конфигурации.
7. Выберите хранилище базы данных: SQL Server или встроенная база данных (Windows Internal Database). При выборе SQL Server убедитесь, что у вас есть соответствующие права и доступ.
8. Завершите мастер и перезагрузите сервер, если требуется.

ADFS

```
Get-Service adfssrv
```

Если сервис не запущен, выполните:

```
Start-Service adfssrv
```

После завершения настройки будет доступен для скачивания файл метаданных IdP.

6. Настройте политику управления доступом или оставьте значение по умолчанию. Нажмите **«Далее»**.
 7. На финальном экране оставьте галочку **«Настроить политику выдачи утверждений для данного приложения»** активной и нажмите **«Завершить»**.
-

7. Настройка правил утверждений (Claim Rules)

1. В открывшемся окне **«Изменить политику подачи запросов»** нажмите **«Добавить правило»**.
 2. В поле **«Шаблон правила утверждений»** выберите **«Отправка атрибутов LDAP как утверждений»**, нажмите **«Далее»**.
 3. Введите произвольное имя правила.
 4. В поле **«Хранилище атрибутов»** выберите **Active Directory**.
 5. В разделе **«Сопоставление атрибутов»**:
 - В столбце **«Атрибут LDAP»** — укажите атрибут, сопоставленный с `unique_id` при настройке импорта из домена. По умолчанию для Active Directory — `objectSid`.
 - В столбце **«Тип исходящего утверждения»** — выберите **«ИД имени»**.
 6. Нажмите **«Готово»**.
-

8. Проверка настроек

После успешной настройки в форме аутентификации в Личном кабинете или административной панели появится кнопка аутентификации через домен.

SSO

?????????? SSO ??????

Kerberos

????

Настройка единого входа (SSO) в Printum через протокол Kerberos. Пользователь, однажды прошедший аутентификацию в домене, автоматически получает доступ к Printum без повторного ввода пароля.

??????????

- Настроена интеграция с доменом (пользователи импортированы)
 - Доступ к контроллеру домена для создания сервисного пользователя и SPN
 - Printum доступен по FQDN или IP-адресу
-

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

??? 1. ?????????????? ?? ?????????? ??????????????????
?????????

1.1. Создайте сервисного пользователя

Создайте специального пользователя в домене для аутентификации Printum. Этот пользователь не обязан быть пользователем системы Printum.

1.2. Создайте SPN

Создайте Service Principal Name (SPN) для сервисного пользователя:

```
setspn -A HTTP/<host or ip> <username>
```

Где `<host or ip>` — хостнейм или IP-адрес сервера Printum, `<username>` — имя сервисного пользователя.

1.3. Сгенерируйте keytab-файл

```
ktpass /out krb5.keytab /princ HTTP/<hostname or IP with port>@<domain.name> /mapuser <account name>@<domain.name> /ptype KRB5_NT_PRINCIPAL /crypto ALL /pass <account password> /kvno 0
```

Параметры:

- `<hostname or IP with port>` — хостнейм или IP мониторинга с портом бэкенда (8001), например: `192.168.10.10:8001` или `domainname:8001`
- `<domain.name>` — имя домена (проверить: `echo %USERDOMAIN%` в CMD на контроллере домена)
- `<account name>` и `<account password>` — логин и пароль сервисного пользователя

??? 2. ?????????? ? Printum

1. Перейдите в раздел «**Авторизация через Домен**».
2. Добавьте новую запись или отредактируйте существующую.
3. Заполните поля:
 - **Тип** — выберите `Kerberos`.
 - **Keytab для Kerberos** — загрузите сгенерированный файл `krb5.keytab`.
 - **Формат имени пользователя** — если логин в формате `username`, выберите «обрезать до первого символа @»; если в формате `username@domain.suffix` — «полностью».
 - **Атрибут пользователя для сопоставления** — для Kerberos использовать **Имя пользователя (username)**.

??? 3. ?????????? ?????????? ?? ??? ????????????????

Настройте браузер для работы с Kerberos согласно документации вашего браузера.

Если Printum доступен по IP-адресу (а не по доменному имени), разрешите обращение по IP. На Windows — добавьте запись в реестр:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters"  
/v TryIPSPN /t REG_DWORD /d 1 /f
```

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

Перейдите на страницу авторизации Printum и выберите «**Авторизоваться при помощи доменной УЗ**». Аутентификация должна произойти автоматически без запроса пароля.

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

- [Авторизация через доменную учётную запись на МФУ](#)
- [Настройка атрибутов домена](#)

SSO

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

????

Настройка авторизации пользователей на МФУ с использованием логина и пароля доменной учётной записи через протокол LDAP.

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

Функционал поддерживается только на устройствах HP.

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

- Настроена интеграция с доменом
 - МФУ HP подключено и синхронизировано с ПринтМенеджером
-

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

??? 1. ?????????? ?????????? ????????????????

1. Откройте панель администратора Мониторинга.
2. В разделе **Constance** → **Настройки** → **Global options** найдите параметр `ALLOW_DOMAIN_AUTH_ON_PRINTERS`.
3. Установите галочку, чтобы разрешить доменную авторизацию на МФУ.

??? 2. ?????????????????????? ? ??????????????????????

Перейдите в раздел «**Принтменеджеры**», вкладку «**Принтменеджеры**» и нажмите «Синхронизировать», либо дождитесь автоматической синхронизации (по умолчанию раз в час).

??? 3. ?????????? ?????????? ?????????? (??????????????)

При авторизации система последовательно перебирает все домены согласно порядковому номеру. Измените порядок в настройках домена для ускорения аутентификации.

??? 4. ?????????????? ?????????????? ?????????? (???? ??????????????)

Логин подставляется в формате `domain\username`, где `domain` — название домена из настроек интеграции. Если название не совпадает с фактическим префиксом, настройте его:

Мониторинг → Импорт из доменов → Домены → настройки домена → поле «Префикс для логина при авторизации». Укажите нужный префикс или , если префикс не нужен.

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

Пользователи авторизуются на поддерживаемых МФУ HP, введя логин и пароль доменной учётной записи.

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

- [Настройка SSO через Kerberos](#)

SAML 2.0

SAML 2.0 — это протокол **федеративной аутентификации**. Пользователь аутентифицируется на стороне Identity Provider (например, AD FS), и IdP передаёт в Принтум подписанное утверждение (assertion) о том, кто этот пользователь. Принтум сопоставляет assertion с существующей учётной записью и открывает сессию.

SSO

SSO (Single Sign-On) — это **пользовательский опыт**: возможность войти в систему один раз и получить доступ ко всем сервисам без повторного ввода пароля. SSO — это результат правильно настроенного SAML или Kerberos, а не отдельная технология.

??? SAML ?????? ? ???????
???????????????????? ????????

Механизм входа через SAML в Принтум работает следующим образом:

1. Пользователь нажимает кнопку «Войти через домен» в Личном кабинете или административной панели.
2. Принтум перенаправляет браузер пользователя на IdP (AD FS).
3. IdP аутентифицирует пользователя и возвращает SAML assertion в Принтум.
4. Принтум извлекает из assertion значение атрибута `name_id` и ищет пользователя с совпадающим `unique_id` в своей базе.
5. Если пользователь найден — создаётся сессия.

Важно: пользователи **не создаются автоматически** из SAML assertion. Учётная запись должна быть заранее создана в Принтум — как правило, путём синхронизации через LDAP. SAML только *аутентифицирует* уже существующего пользователя, но не регистрирует нового.

Этап	Технология	Что происходит
Импорт пользователей	LDAP	Учётные записи из AD попадают в Принтум
Вход пользователя	SAML 2.0	Assertion от IdP → поиск по <code>unique_id</code> → сессия
Единый вход	SSO	Пользователь входит один раз без повторного ввода пароля

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

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

- **LDAP** — для синхронизации пользователей из Active Directory в Принтум.
- **SAML 2.0 (AD FS)** — для федеративной аутентификации и SSO через браузер.
- **Kerberos** — для прозрачного SSO в Windows-домене (альтернатива SAML для браузерных клиентов).