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

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

- Интеграция с контроллерами домена
  - Стандартные атрибуты для поддерживаемых контроллеров домена
  - Расписание синхронизации с доменом
  - Доменная авторизация и SSO — как работает
  - Подключение LDAP-домена
- Интеграция с почтовым сервером (SMTP)
  - Настройка печати через почту
  - Настройка гостевой печати через почту
- Отправка событий в SIEM (Syslog)
  - Настройка отправки событий в Syslog
- Гостевая печать через email — как работает
- 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
- Внешние интеграции
  - Интеграция с DLP-системами
  - Настройка интеграции с DLP InfoWatch

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

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

??????????

При синхронизации пользователей Printum сопоставляет поля системы с атрибутами LDAP-каталога. Приведённые ниже значения используются по умолчанию и рекомендуются для большинства внедрений.

Microsoft Active Directory

Атрибут в Printum	Атрибут в домене	Описание
`username`	`sAMAccountName`	Логин
`unique_id`	`objectSid`	Идентификатор в домене
`last_name`	`sn`	Фамилия
`first_name`	`givenName`	Имя
`patronymic`	`personalTitle`	Отчество
`email`	`mail`	Адрес электронной почты
`domain_groups`	`memberOf`	Доменные группы
`position`	`title`	Должность
`smb_path`	`homeDirectory`	Путь к папке

FreeIPA / Samba DC / ??? ???

Атрибут в Printum	Атрибут в домене	Описание
`username`	`uid`	Логин
`unique_id`	`uidNumber`	Идентификатор в домене
`last_name`	`sn`	Фамилия

Атрибут в Printum	Атрибут в домене	Описание
`first_name`	`givenName`	Имя
`patronymic`	`personalTitle`	Отчество
`email`	`mail`	Адрес электронной почты
`domain_groups`	`memberOf`	Доменные группы
`position`	`title`	Должность
`smb_path`	`homeDirectory`	Путь к папке

ALD Pro

Атрибут в Printum	Атрибут в домене	Описание
`username`	`uid`	Логин
`unique_id`	`uidNumber`	Идентификатор в домене
`last_name`	`sn`	Фамилия
`first_name`	`givenName`	Имя
`patronymic`	`rbtamiddlename`	Отчество
`email`	`mail`	Адрес электронной почты
`domain_groups`	`memberOf`	Доменные группы
`position`	`title`	Должность
`smb_path`	`homeDirectory`	Путь к папке

Примечание: В ALD Pro нет разделения между группами и отделами — все отделы импортируются как группы.

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

Для корректной синхронизации должны быть настроены следующие поля:

- логин;
- фамилия;
- имя;
- идентификатор в домене;
- адрес электронной почты.

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

- Интеграция с Active Directory
- Интеграция с FreeIPA
- Интеграция с Samba DC и РЕД АДМ
- Интеграция с ALD Pro

Справочник атрибутов: Атрибуты доменов — справочник — сравнительная таблица по всем контроллерам домена.

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

????

Настройка автоматической 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 **«Запустить сейчас»**.
- 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 Samba DC и РЕД АДМ
- Интеграция с ALD Pro

???????? ???????????? ? 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 доменной УЗ»**.

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

?????????? LDAP-??????

??????????

Интеграция с LDAP-доменом позволяет автоматически импортировать пользователей, организационную структуру и группы безопасности в Printum.

Поддерживаются следующие службы каталогов:

- Microsoft Active Directory;
- FreeIPA;
- ALD Pro;
- Samba DC;
- РЕД АДМ.

Добавление домена

1. Перейдите в раздел Настройки → Интеграции → Домены.
2. Нажмите Добавить.
3. Заполните параметры подключения:
   - название домена;
   - тип домена;
   - адрес LDAP-сервера;
   - логин и пароль учётной записи с правами чтения каталога.
4. При необходимости настройте:
   - LDAP-фильтр;
   - стартовый уровень поиска;
   - импорт организационной структуры;
   - импорт групп безопасности;
   - атрибут для объединения учётных записей;
   - использование шифрования.
5. Нажмите Тестовый импорт.
6. После успешной проверки сохраните настройки.
7. Настройте сопоставление атрибутов домена.
8. Запустите синхронизацию вручную или дождитесь её выполнения по расписанию.

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

При успешном подключении тестовый импорт отображает количество найденных пользователей, подразделений и групп. После запуска синхронизации пользователи появляются в разделе Пользователи.

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

- Как работает синхронизация пользователей с доменом
- Сопоставление атрибутов домена
- Рекомендуемые атрибуты для поддерживаемых контроллеров домена
- Объединение доменных учётных записей одного пользователя

?????????? ? ????????
???????? (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** и укажите следующие параметры:

- **PRINT_MAILBOX_HOST** — адрес IMAP-сервера.

- **PRINT_MAILBOX_PORT** — порт на котором работает IMAP-сервер.
- **PRINT_MAILBOX_NAME** — адрес почты, через который задания попадают в очередь печати. Сотрудник может отправить на него файл, и он попадет в его очередь печати.
- **PRINT_MAILBOX_PASSWORD** — пароль для аутентификации на сервере электронной почты (IMAP); не пароль от электронной почты, а пароль для почтовых приложений. Это разные пароли, для почтовых приложений генерируется у почтового провайдера отдельно. У Яндекса, например, тут:

  https://id.yandex.ru/profile/apppasswords-list .
- **PRINT_MAILBOX_USE_SSL** — флаг, который задает шифрование по протоколу SSL.
- **PRINT_MAILBOX_USE_TLS** — флаг, который задает шифрование по протоколу TLS.

Для добавления документа в очередь печати необходимо, чтобы адрес электронной почты сотрудника, который отправляет документ, совпадал с адресом электронной почты, указанный для этого сотрудника в ПМ.

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

Отправьте тестовое письмо с документом с почты сотрудника на почту, указанную в **PRINT_MAILBOX_NAME**. 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

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

????

Активация гостевой печати через почту — возможность печати для пользователей, которых нет в списке сотрудников Printum.

??? ????????

Гость отправляет письмо с вложением на специальный адрес. Система автоматически создаёт гостевую учётную запись и добавляет задание в гостевую очередь. В ответном письме гость получает PIN-код. Используя PIN-код на МФУ со встроенным приложением, гость авторизуется и распечатывает документ.

???????????

- Настроена интеграция с почтовым сервером (SMTP)
- Настроена печать через почту (параметр `PRINT_MAILBOX_NAME`)

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

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

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

Включите параметр `GUEST_PRINT_VIA_MAIL`.

??? 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)

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

????

Настройка отправки системных событий Printum во внешний Syslog-сервер (SIEM).

???????????

- Syslog-сервер развёрнут и доступен из сети Printum
- Известен адрес и порт Syslog-сервера

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

- Отправка происходит по указанному хосту и порту (например, `192.168.10.10:1514`).
- Допустимые порты: `514`, `1514`, `1468`. Если порт не указан — используется `514`.
- Авторизация по стандарту syslog не поддерживается — логин и пароль указывать не нужно.
- Тело отчёта заполнять не нужно — отправляются все доступные параметры события.

?????????? (TLS)

Для отправки по шифрованному протоколу укажите CA-сертификат и сертификат клиента в формате `.pem`. Шифрование выполняется по протоколу TLS (выбирается максимально возможная версия для сервера). Если нежелательный протокол TLS активирован — запретите его непосредственно на сервере syslog.

Для настройки syslog-сервера обратитесь к его официальной документации.

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

Логи передаются в следующем формате:

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

Поля:

- `event` — уникальный идентификатор события.
- `user` — логин пользователя.
- `location` — название локации (если есть).
- `additional_parameters` — дополнительные параметры события.

???????????

Для проверки прослушиваемого порта (TCP/UDP) на сервере syslog:

```
netstat -tulnp
```

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

События из Printum поступают в Syslog-сервер в заданном формате.

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

Перейдите по адресу `https://<адрес_сервера>:8001/config/integrations/` и выберите раздел **«Внешние интеграции»**. Нажмите **«Добавить»**.

Заполните поля:

Параметр	Описание
Название конфигурации	Произвольное имя интеграции, например «Syslog SIEM»

Параметр	Описание
Хост	Адрес и порт сервера Syslog, например `192.168.10.10:1514`. 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

1. После создания интеграции нажать **«Добавить»** рядом с разделом «Отчёты для отправки» (события или логи безопасности).
2. 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=One
additional_parameters={'foo': 0}
2023-05-25T06:32:44.487278+00:00 test.local Обнаружено новое устройство event=4 user=One
```

```
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

???????? ?????? ????? 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.

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

- Модель пользователей в Принтум
- Настройка гостевой печати через почту

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.

??? 4. ????????? ????? ??????????? IdP

1. Перейдите в **Диспетчер серверов → Средства → Управление AD FS**.
2. В разделе **«Отношения доверия проверяющей стороны»** откройте настройку созданного ранее сервиса.
3. Во вкладке **«Наблюдение»** нажмите **«Проверить URL-адрес»** справа от строки адреса скачивания XML-файла с метаданными.
4. После успешной проверки скопируйте адрес, введите в браузере — файл метаданных будет скачан на ваш компьютер.

??? 5. ????????? SAML 2.0 ? ???????

1. Перейдите в раздел **«Настройки доменной авторизации»** в административной панели Мониторинга.
2. Нажмите **«Добавить настройки доменной авторизации»**.
3. Заполните поля:
   - **Тип** — выберите `SAML 2.0`.
   - **Метаданные IdP** — загрузите скачанный файл метаданных.
   - **Приватный ключ и Сертификат** — оставьте пустыми для автогенерации, либо загрузите свою пару ключ–сертификат.
4. Нажмите **«Сохранить»**.
5. В столбце **«Метаданные SP»** нажмите **«Открыть»** и сохраните данные в файл — это файл метаданных Service Provider для загрузки в AD FS.

??? 6. ??????????? Relying Party Trust ? AD FS

1. Откройте **Управление AD FS**: **Диспетчер серверов → Средства → Управление AD FS**.
2. Выберите **«Отношения доверия проверяющей стороны»**, затем **«Добавить отношение проверяющей стороны»**.
3. На первом шаге оставьте выбор **«Поддерживающие утверждения»** и нажмите **«Запустить»**.
4. На втором шаге выберите **«Импорт данных о проверяющей стороне из файла»**, загрузите файл метаданных SP (сохранённый на шаге 5). Нажмите **«Далее»**.
5. Введите произвольное название для отношения доверия и нажмите **«Далее»**.

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. ?????????? ??????? ?????? ??????????? (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»**.

?????????

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. Создайте специального пользователя в домене для аутентификации Printum. Этот пользователь не обязан быть пользователем системы Printum.
2. 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.

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

SSO

?????? ?????????????? ? ??????? — ?????

??????????

Принтум поддерживает несколько механизмов интеграции с корпоративным каталогом пользователей. Каждый из них решает свою задачу. Понимание различий позволяет выбрать правильную комбинацию при внедрении.

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

Технология	Назначение	Когда использовать
LDAP	Каталог пользователей, синхронизация	Всегда при доменной интеграции
SAML 2.0	Федеративная аутентификация	SSO через IdP (AD FS, Keycloak и др.)
Kerberos	Прозрачный SSO	Windows-домен, браузерный доступ
SSO	Пользовательский опыт единого входа	Результат настройки SAML или Kerberos

---

LDAP ? SAML ? SSO — ? ??? ???????

LDAP

LDAP — это протокол доступа к каталогу. В контексте Принтум он используется для **синхронизации пользователей**: импорта учётных записей из Active Directory в базу данных Принтум. LDAP не отвечает за вход пользователя — он только обеспечивает наличие пользователей в системе.

SAML 2.0

SAML 2.0 — это протокол **федеративной аутентификации**. При использовании SAML пользователь проходит аутентификацию на стороне Identity Provider (например, AD FS). После успешного входа IdP передаёт в Printum подписанное SAML Assertion — утверждение, подтверждающее личность пользователя и набор его атрибутов. 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 **«Авторизоваться с помощью доменной УЗ»** 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 `unique_id` → 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).

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

?????????? ? DLP-??????????

??????????

Интеграция с DLP-системами предназначена для передачи документов, полученных на МФУ, в системы предотвращения утечек данных (DLP) для последующего анализа. Решение позволяет включить операции с документами на МФУ в общий контур контроля документооборота и информационной безопасности организации.

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

Большинство DLP-систем контролируют электронные каналы передачи данных: электронную почту, файловые хранилища, веб-трафик и другие информационные потоки. При этом операции, выполняемые непосредственно на МФУ, часто остаются вне зоны автоматического контроля. В результате служба информационной безопасности не имеет возможности автоматически анализировать документы, обрабатываемые пользователями на устройствах печати. Printum получает цифровой образ документа и передаёт его во внешнюю DLP-систему для проверки.

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

При выполнении пользователем операции копирования или сканирования Printum получает цифровой образ документа и автоматически передаёт его во внешнюю DLP-систему. После получения документа дальнейший анализ выполняется средствами DLP-системы в соответствии с её политиками безопасности. Printum не анализирует содержимое документов и не принимает решения о блокировке операций.

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

Передача документов выполняется автоматически и не требует действий пользователя. Если в системе разрешено хранение образов документов, Printum выполняет повторные попытки передачи при временной недоступности DLP-системы. Если в организации запрещено хранение образов документов, передача выполняется до удаления документа из системы. В этом режиме повторные попытки передачи не выполняются. Проверка

содержимого документов, формирование инцидентов и принятие решений выполняются средствами DLP-системы.

??????????

Для использования интеграции требуется Printum версии 4.4 или выше и встроенное приложение Printum на МФУ.

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

Настройка интеграции с DLP InfoWatch

????????? ????????? ? DLP InfoWatch

??????????

Интеграция с DLP-системами позволяет автоматически передавать документы, полученные в результате операций копирования и сканирования, во внешнюю систему для последующего анализа. Настройка выполняется в разделе внешних интеграций Printum.

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

1. Откройте панель администратора Мониторинга.
2. Перейдите в раздел «Внешние интеграции».
3. Для добавления интеграции выполните одно из действий:
   - нажмите «Добавить» рядом с разделом;
   - нажмите «Добавить внешнюю интеграцию» внутри раздела.
4. В форме создания интеграции укажите::
   - **Описание конфигурации** — наименование интеграции.
     Пример: Infowatch
   - **Адрес сервера, Хост** — полный адрес.
     - Пример: `https://server.company.ru:9106/xapi/push/event`
   - **Локации** — параметр не используется при настройке интеграции с DLP.
   - **Тип интеграции** — выберите InfoWatch
   - **Интервал между обменами данных** — рекомендуется установить значение 5 минут.
   - **Имя учетной записи для авторизации** — логин для аутентификации в системе.
   - **Пароль или токен для авторизации** — пароль для аутентификации в системе.
   - **Включено** — установите чек-бокс , чтобы интеграция была активна после завершения настройки
   - **Проверка SSL** — включает проверку сертификата сервера.
     - при использовании самоподписанных сертификатов отключите проверку или укажите CA-сертификат.
   - **CA сертификат** — сертификат центра сертификации (при необходимости).

- **Сертификат** — SSL-сертификат клиента (.pem). Сертификат не должен требовать кодовую фразу.
- **Передавать файлы копирования** — включает передачу документов копирования.
- **Передавать файлы сканирования** — включает передачу документов сканирования.

Важно: Параметр «Передавать файлы печати» не используется.

5. Нажмите «Сохранить».

После сохранения интеграция будет активирована и начнёт работать после синхронизации между Мониторингом и ПринтМенеджером (по умолчанию синхронизация выполняется 1 раз в час; при необходимости выполните синхронизацию вручную).

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

1. Выполните копирование или сканирование на МФУ.

Важно: на устройстве должно быть установлено встроенное приложение Printum; для операций копирования должна быть активирована функция сохранения образа документа.

2. Перейдите в панель администратора ПринтМенеджера в разделе **«Напечатанные задания, которые нужно отправить во внешнюю интеграцию»** по адресу `https:/адрес_сервера.test:8080/config/integrations/printedjobintegrationstate/`
3. В разделе отображаются задания со следующими параметрами:
   - **РЕЗУЛЬТАТ ОТПРАВКИ** — индикатор успешной отправки задания;
   - **CREATED AT WITH SECONDS** — время создания задания;
   - **PROCESSED AT WITH SECONDS** — время отправки задания.
4. Возможные статусы заданий:
   - **Отправляется** — задание находится в процессе передачи;
   - **Отправлено** — задание успешно передано;
   - **Не отправлено** — задание не было передано.

Критерий успешности: наличие заданий со статусом «Отправлено».

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

- Передача документов выполняется асинхронно и не блокирует действия пользователя.
- Максимальное время попыток передачи документа составляет 2,5 часа. Если за это время документ не удалось передать во внешнюю систему, дальнейшие попытки передачи не выполняются.

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

Если документы не передаются во внешнюю систему, рекомендуется проверить:

- доступность сервера DLP;
- корректность адреса сервера;
- правильность логина и пароля;
- корректность сертификатов;
- настройки проверки SSL;
- наличие CA-сертификата.

Подробная информация об ошибках передачи фиксируется в журналах системы.

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

Интеграция с DLP-системами