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

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

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

????

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

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

??????????

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).