????????? 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

Revision #6
Created 2026-05-09 16:32:46 UTC by DD
Updated 2026-06-14 18:58:33 UTC by DD