# ?????? ?????????????? ? ??????? — ?????

## ??????????

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).