????????? 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.
