Содержание

Руководство по настройке интеграции с Active Directory

> Текущая инструкция актуальна для версии **ADVANTA 3.20** и выше.
>
> Инструкция по настройке Active Directory для ADVANTA 3.19 и более ранних версий продукта.
>
> О том, как изменить настройки после обновления системы с 3.19 на 3.20 см. на странице описания обновления 3.20.

Один домен

Общая информация

> Данный тип интеграции позволяет подключаться к Адванте с использованием Active Directory с компьютеров, размещенных **в одном домене**. При этом допускается, что сервер с системой может находится вне домена, а географически – в любой части мира.

Интеграционное решение ориентировано на компоненты Active Directory:

1. Служба федерации Active Directory (AD FS).
2. Служба каталогов Active Directory; доступ к ней осуществляется по LDAP.

Службы федерации Active Directory используются для аутентификации пользователей. AD FS позволяет использовать технологию единого входа (SSO). В нашем случае важно, что AD FS использует Встроенную Аутентификацию Windows, что позволяет входить в систему без ввода логина и пароля (требует настройки в IE и Firefox). Если пользователи будут использовать AD FS только находясь в домене, то не обязательно делать эту службу доступной во внешнюю сеть.

Службы каталогов AD используются для импорта пользователей из AD в систему и для выбора учетной записи AD при связывании с пользователем. Связывание происходит по полю SID.

> **Важно!**
>
> Чтобы использовать интеграцию с Active Directory, обращение к системе Адванта должно выполняться по **протоколу https**.

Установка службы федерации Active Directory (в домене клиента)

> **Важно!**
>
> Сервер со службой федерации Active Directory (AD FS) должен находиться в домене на сервере клиента. При этом можно установить службу на сервер с контроллером домена (AD), однако служба технической поддержки компании Microsoft не рекомендует производить подобные установки: службы AD и ADFS должны быть размещены на различных хостах (ВМ). При этом сервер IIS может находиться как на сервере (клиента) внутри доменной сети, так и на внешнем хостинге.

Windows Server 2008R2

1. Установите IIS – инструкция по установке.
2. Запустите файл установки службы федерации Active Directory 2.0. Скачать можете здесь. Откроется мастер установки AD FS 2.0 → «Далее».
3. На шаге «Лицензионное соглашение» поставить чек-бокс «**Я принимаю условия лицензионного соглашения**» → «Далее».
4. На шаге «Роль сервера» выберите роль «**Сервер федерации**» → «Далее».
5. На шаге «Установка необходимого программного обеспечения» мастер установки автоматически проверит наличие необходимых для службы федерации компонентов. → «Далее».
6. После завершения работы мастера поставьте чек-бокс «**Когда мастер закроется, запустить оснастку управления AD FS 2.0**» для дальнейшей настройки службы. → «Готово».

Windows Server 2012

1. Откройте «Диспетчер серверов».
2. Управление → Добавить роли и компоненты
3. На шаге «Перед началом работы» (если такой появится) → «Далее».
4. На шаге «Тип установки» выберите «**Установка ролей и компонентов**» → «Далее».
5. На шаге «Выбор сервера» **выберите сервер**, на котором будет установлена служба федерации Active Directory → «Далее».
6. На шаге «Роли сервера» поставьте чек-бокс напротив роли «**Службы федерации Active Directory**».
   Мастер добавления ролей и компонентов предложит добавить компоненты, необходимые для Службы федерации Active Directory. → «Добавить компоненты» → «Далее»
7. Шаг «Компоненты» остаётся без изменений → «Далее».
8. На шаге «Службы федерации Active Directory (AD FS)» → «Далее».
9. В промежуточном шаге «Службы ролей» должен быть активен чек-бокс «**Служба федерации**» → «Далее».
10. В промежуточном шаге «Службы ролей» ничего не меняйте → «Далее».
11. На шаге «Подтверждение» → «Установить».
12. После установки необходимых компонентов закройте мастер установки.

Начальная настройка AD FS

Этап 1. В диспетчере служб IIS

Установите сертификат в Доверенные корневые центры сертификации через сервер ADFS или на сервере IIS.

Если IIS установлен, то сделать это можно так:

1. Запустите Диспетчер служб IIS.
2. Выберите локальный сервер.
3. На начальной странице локального сервера → меню «**Сертификаты сервера**».
4. На странице «Сертификаты сервера»:
    1. добавьте сертификат:
        - либо заверенный, купленный у вендора,
        - либо созданный в центре сертификации AD CS (если эта служба установлена).

        > Использовать самозаверенный сертификат не рекомендуется.
        > Для каждого пользователя, который заходит через AD будет предупреждение в браузере. Во многих браузерах чтобы продолжить работу с таким сертификатом, надо проделать определенные действия, например, добавить сайт в исключения, что многим пользователям будет не под силу.

    2. В поле «Понятное имя сертификата» впишите имя, например: `ADFS_Certificate`
    3. В разделе «Выбрать хранилище сертификата для нового сертификата:» → «Личный».
    4. Закройте Диспетчер служб IIS.

Этап 2. Настройка на сервере

Windows Server 2008R2: После установки AD FS 2.0 оснастка управления должна была запуститься автоматически.
Если этого не произошло, запустите оснастку вручную: Пуск → Все программы → Администрирование → **Управление AD FS 2.0**.

Windows Server 2012: В диспетчере серверов нажмите на значок уведомлений (флаг с восклицательным знаком в треугольнике) → в окне «Конфигурация после развертывания» клик на «**Запустить оснастку управления AD FS**».

1. В открывшейся оснастке → «Мастер настройки сервера федерации AD FS».
2. На шаге «Добро пожаловать!» включите чек-бокс «**Создать службу федерации**» → «Далее».
3. На шаге «Выберите тип развертывания» → «**Изолированный сервер федерации**» → «Далее».
4. На шаге «Имя службы федерации» можно выбрать SSL-сертификат для веб-сайта.
   Т.к. ранее при настройках создавался только один сертификат (ADFS_Certificate), он

подставится по умолчанию, без права выбора сертификатов.
Если сертификатов больше, выберите нужный.
→ «Далее».

5. На шаге «Сводка» мастер настройки покажет, какие параметры будут настроены для служб AD FS. → «Далее» → «Закрыть»
Если оснастка AD FS закрылась, запустите её заново.
6. В оснастке управления AD FS клик по ссылке «**Обязательно: добавьте доверенную проверяющую сторону**» → «Запустить».
7. На шаге «Выберите источник данных» включите чек-бокс «**Ввод данных о проверяющей стороне вручную**» → «Далее».
8. На шаге «Укажите отображаемое имя», в поле «Отображаемое имя:» введите имя для проверяющей стороны (например: advanta), и, при необходимости, любые примечания. → «Далее».
9. На шаге «Выберите профиль» установите значение напротив пункта «**Профиль AD FS**». → «Далее».
10. На шаге «Настройте сертификат» можно указать дополнительный сертификат шифрования маркера, если это необходимо. → «Далее».
11. На шаге «Настройте URL-адрес»:
    - включите чек-бокс «**Включить поддержку пассивного протокола WS-Federation**»,
    - в поле «URL-адрес пассивного протокола WS-Federation проверяющей стороны» введите адрес страницы `ADFS_Login.aspx` в вашей системе (например: `https://your.system.ru/streamline/ADFS_Login.aspx`).
    → «Далее».
12. На шаге «Настройте идентификаторы» в поле «Идентификатор отношения доверия проверяющей стороны:» введите адрес вашей системы (например: `https://your.system.ru/streamline`). → «Далее».
13. На шаге «Выберите правила авторизации выдачи» → «Разрешить доступ к этой проверяющей стороне всем пользователям».
Или, после настройки мастера, настройте конкретных пользователей. → «Далее».
14. На шаге «Готовность для добавления отношения доверия» можете проверить все настройки и нажмите «Далее».
15. На шаге «Готово» включите чек-бокс «**Открыть диалоговое окно «Изменение правил утверждений» для этого отношения доверия проверяющей стороны после закрытия мастера**» → «Закрыть».
16. Откроется окно «Изменение правил утверждений для advanta (отображаемое имя, которое вы ввели ранее)».
    1. На вкладке «Правило Преобразования выдачи» → «Добавить правило...».
    2. В мастере добавления правила преобразования утверждения:
        1. на шаге «Выберите тип правила», выберите шаблон правила утверждения: «**Отправка утверждений с помощью настраиваемого правила**». → «Далее».
        2. на шаге «Настройте правило утверждения»:
            - в поле «Имя правила утверждения:» введите имя: `sid`;
            - В поле «Настраиваемое правило:» введите правило: `c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"]=>issue(claim = c);` (копировать вместе со знаком ;)
            - → «Готово».
17. После этого снова появится окно «Изменение правил утверждений для advanta» → «OK».

Настройка службы каталогов Active Directory на сервере с установленной Адвантой (сервер IIS)

> Прежде чем приступать к настройкам, проверьте наличие/добавьте на сервер приложения файл `ADFS_Login.aspx` в корень приложения.

Службы каталогов AD должны быть доступны для сервера IIS по LDAP. Для системы «Адванта» настройка службы выполняется в конфигурационных файлах, находящимися в папке с веб-контентом системы.

Настройки интеграции со службой AD FS

> **Только для Windows Server 2008R2**
>
> 1. На сервере службы федерации в IIS перейти к сайту AD FS: Сайты –> Default Web Site –> AD FS → ls . Данный пункт актуален только для старых версий AD FS, начиная с версии службы федерации 3.0 в Windows Server 2012, IIS на сервер со службой федерации устанавливать необходимости нет.
> 2. На странице сайта раздел «Проверка подлинности» → включить компонент «Проверка подлинности Windows».
> 3. Перейти в дополнительные параметры данного компонента → в настройке «Расширенная защита» установить «Выключена».

для настройки ADFS нужно указать два параметра в `client.config` в секции `<appSettings>`:

`<add key="AdfsRealm" value="https://system.a2test.local/streamline" />`	Где `a2test` – название домена вашей инсталляции ADVANTA. Идентификатор проверяющей стороны, берется из оснастки ADFS «Отношение доверия/Отношение доверия проверяющей стороны/Идентификатор проверяющей стороны»
`<add key="AdfsIssuer" value="https://adfs.a2test.local" />`	Где `a2test` – название домена вашей инсталляции ADVANTA. Адрес сервиса ADFS

Также есть два дополнительных параметра:

- `AdfsMode` – режим проверки сертификата
  - по умолчанию `Default` – строгий режим, который проверяет всю цепочку сертификатов. Параметр не обязательный. Если сертификат - купленный, параметр можно не указывать. В этом случае умолчанию и будет указан данный параметр
  - можно задать режим `Thumbprint` – данный режим применяется, если сертификат

самозаверенный. Этот режим проверяет только даты и отпечаток сертификата, в этом режиме нужно обязательно задать следующий параметр:

```
<add key="AdfsMode" value="Thumbprint" />
```

- `Thumbprint` – если в AdfsMode указано Thumbprint, в этом случае необходимо указать отпечаток сертификата: оснастка AD FS → Сертификаты (Service communications) → CN=ServerADFS.your.domain.local → Состав → Отпечаток.) При этом обязательно надо указать дополнительный параметр:

```
 <add key="AdfsThumbprint"
value="0cafe3b7025e9cfe48f83f5dcdff36122c6fcbb6" >
```

Внимание!

При копировании отпечатка через графический интерфейс, он может скопироваться с дополнительными невидимыми символами. Поэтому при копировании используйте команду `certutil`.

- Настройка интеграции со службой AD FS в файле web.config (до версии 3.03.2166.x)
- Настройка интеграции со службой AD FS в файле web.config (до версии 3.19 включительно)

Настройка LDAP в файле client.config

В главном разделе `<configuration>` после закрывающего тега `</configSections>` добавить следующее:

```
<ldapService ldapPath="LDAP://адрес сервера с AD FS/" baseDN="база поиска объектов в AD">
  <authenticationTypes>
     <add authenticationType="Secure" />
     <add authenticationType="Signing" />
     <add authenticationType="Sealing" />
   </authenticationTypes>
</ldapService>
```

- `ldapPath` – адрес службы. Значение по умолчанию (LDAP://) можно использовать, когда сервер приложения находится в домене. Иначе нужно указать действительный адрес службы и порт, если порт отличается от стандартного (389). Например: LDAP://ad.domain.local/
- `baseDN` – базовый DN каталога пользователей.
  - Если не указан, то используется дефолтный DN, который определен в самой службе каталогов. Лучше указывать действительный DN. Например:

```
DC=domain,DC=local
```

- `authenticationTypes` – типы аутентификации.
  Влияют на защищенность (шифрование и подпись) передаваемых данных.
  По умолчанию: Secure, Signing, Sealing.

> Если в службе каталогов настроен SSL (требует установки Certification Authority), то нужно указать SecureSocketsLayer в authenticationTypes.

В раздел `<configSections>` добавить тег:

```
<section name="ldapService" type="Config.LDAPConfigurationSection, smcorelib" />
```

Безопасность

Службы федерации и приложение не обмениваются напрямую, только через браузер. Пользователь вводит логин и пароль для доступа к веб-сервисам AD FS, а приложение никогда не получает эти данные. Вместо логина и пароля приложение получает от AD FS утверждения, а именно доменный `sid` пользователя. Передача утверждений происходит с использованием шифрования. Также утверждения подписываются в AD FS, используя SAML. Доверие приложения к сервису утверждений основано на подписи, которая проверяется по отпечатку сертификата.

Важно использовать заверенный сертификат для веб-сервисов AD FS (этот сертификат устанавливается в IIS). Это не тот сертификат, который используется для подписи и шифрования утверждений.

> Если сертификат не заверен центром сертификации (создан самозаверенный), то нужно будет установить его на рабочие станции пользователей в корневые центры сертификации. В этом случае экспортируется сертификат, созданный на шаге 4 в подразделе «Начальная настройка AD FS»

Настройка рабочих станций

1. Установить сертификат в Доверительные корневые центры сертификации.
2. Добавить систему в надежные сайты (Свойства браузера → Безопасность → Надежные сайты → Сайты → Добавить сайт `https://`имя системы в сертификате безопасности → Закрыть).

Настройка интеграции с AD в системе (AD FS)

После выполнения всех настроек, описанных выше, активируйте синхронизацию с AD в системе ADVANTA.

Для этого под учетными данными администратора системы:

1. перейти в пункт меню «Администрирование» → «Общие настройки» → «Настойки Active Directory»;
2. в портлете «Настройки связи с Active Directory (с использованием службы ADFS)» установить чек-бокс в «Разрешить проверку учетных данных в Active Directory (с использованием службы ADFS)».

Далее, чтобы в систему можно было заходить под доменными учетными данными пользователей, нужно загрузить этих пользователей из AD. Здесь **два варианта:**

1. Загрузка новых пользователей из AD в систему, в настройках Active Directory, после активации синхронизации, появится кнопка «Загрузить из Active Directory». С помощью этой кнопки можно загрузить всех необходимых пользователей в систему. В этом случае в системе создаются новые пользователи с привязкой к доменной учетной записи.
2. Привязка уже существующего пользователя системы к AD. Для этого, под учетными данными администратора системы, нужно перейти в пункт меню «Команда в лицах» - «Список». Выбрать необходимого пользователя из списка и перейти в карточку редактирования этого пользователя, нажав левой кнопкой мыши по ссылке данного пользователя. В портлете «Учетная запись Active Directory» необходимо нажать кнопку-ссылку «Задать», где можно будет выбрать необходимую доменную учетную запись для привязки пользователя.

Если сервер с системой не включен в домен, при нажатии кнопки «Загрузить из Active Directory» возникнет ошибка подключения к Active Directory. В этом случае необходимо нажать кнопку «учетная запись» и ввести в появившемся окне логин и пароль доменного пользователя. Логин должен вводиться в формате `domain\user` или `user@domain.local`.

Мультидоменность

ВНИМАНИЕ!

Использование зарезервированных символов XML в конфигурационном файле запрещено (& «<'>).

Мультидоменная авторизация позволяет проводить аутентификацию пользователей с помощью Active Directory, находящихся в различных доменах внутри организации. При этом **необходимо, чтобы сервер с системой находился в корневом домене**, а также наличие двусторонних транзитивных отношений между корневым и остальными доменами.

> Мультидоменность работает по протоколу NTLM.

Настройки на сервере IIS

1. Для авторизации на сервере через AD необходимо установить службу «Windows – проверка подлинности» (`Windows Authentication`).

Windows Server 2008 R2:

1. Открыть диспетчер сервера.
2. Перейти в пункт «Роли».
3. На вкладке «Службы ролей» нажать на кнопку «Добавить службы ролей».
4. В пункте «Безопасность» включить пункт «Windows - проверка подлинности».
5. Нажать «Далее».
6. «Установить».

Windows Server 2012:

1. Открыть диспетчер серверов.
2. «Управление» → «Добавить роли и компоненты».
3. На шаге «Перед началом работы» нажать «Далее».
4. На шаге «Тип установки» выбрать «Установка ролей или компонентов» и нажать «Далее».
5. На шаге «Выбор сервера» выбрать текущий сервер.
6. Перейти в пункт «Роль веб-сервера(IIS)» → «Службы ролей».
7. В пункте «Безопасность» включить пункт «проверка подлинности Windows».
8. Нажать «Далее», затем «Установить».

После установки службы «Windows - проверка подлинности» откройте Диспетчер служб IIS:

1. Перейти в раздел «Сайты» → Default Web Site (сайт с установленной системой).
2. Затем перейти в подраздел «Проверка подлинности» (в области просмотра возможностей).
3. Включить компонент «Проверка подлинности Windows».
4. Включить компонент «Анонимная проверка подлинности».
5. Все остальные компоненты выключить, если они включены.

2. Настройка client.config:

- добавляем теги в `<configuration><configSections>`:

```
<section name="ldapService" type="Config.LDAPConfigurationSection,
smcorelib"/>
<section name="adDomains" type="Config.ADDomainsConfiguration,
smcorelib"/>
```

- добавляем тег в корень после тега <configSections>:

```
<adDomains>
  <domains>
    <add name="Имя домена" login="Логин пользователя" password="Пароль"
ldappath="LDAP://Адрес LDAP(127.0.0.1:389)" />
  </domains>
</adDomains>
```

где:

- значение «Имя домена» – любое понятное имя домена, которое будет использоваться в дереве при загрузке пользователей из каталога;
- значение «Логин пользователя» – логин любого пользователя того домена, от куда будет производиться загрузка пользователей;
- значение «Пароль» – пароль пользователя, логин которого использовался в значении «Логин пользователя» (выше);
- значение »LDAP://Адрес LDAP« – адрес службы LDAP (например: LDAP://192.168.0.200:389 или LDAP://domain.local:389).

> Для добавления нескольких доменов нужно добавить соответствующее количество строк, начинающихся с тега «add name...».

Ссылка на пример файла Client.config с настройками интеграции под NTLM

Настройка рабочих станций

Добавить систему в раздел Местная интрасеть (Свойства браузера → Безопасность → Местная интрасеть → Сайты → Добавить сайт с адресом системы → Закрыть).

Настройка интеграции с AD в системе (NTLM)

После выполнения всех вышеописанных настроек, необходимо активировать синхронизацию с AD в самой системе. Для этого под учетными данными администратора системы:

1. перейти в пункт меню «Администрирование» → «Общие настройки» → «Настойки Active Directory»;
2. в портлете «Настройки связи с Active Directory (с использованием NTLM)» поставить чек-бокс напротив «Разрешить проверку учетных данных в Active Directory (с использованием NTLM)» .

Далее, чтобы пользователи могли заходить в систему под своими доменными учетными записями, их нужно загрузить в систему из AD. Здесь **два варианта:**

1. Загрузка новых пользователей из AD в систему, в настройках Active Directory, после активации синхронизации, появится кнопка «Загрузить из Active Directory». С помощью этой кнопки можно загрузить всех необходимых пользователей в систему. В этом случае в системе создаются новые пользователи с привязкой к доменной учетной записи.
2. Привязка уже существующего пользователя системы к AD. Для этого, под учетными данными администратора системы, нужно перейти в пункт меню «Команда в лицах» - «Список». Выбрать необходимого пользователя из списка и перейти в карточку редактирования этого пользователя, нажав левой кнопкой мыши по ссылке данного пользователя. В портлете «Учетная запись Active Directory» необходимо нажать кнопку-ссылку «Задать», где можно будет выбрать необходимую доменную учетную запись для привязки пользователя.