Microsoft Azure AD и JaCarta PKI

Руководство по настройке

Листов: 32

Автор: Timofey Alekseev

Аннотация

Данная инструкция предназначена для настройки двухфакторной аутентификации по сертификатам на облачной платформе Microsoft Azure AD.

Оглавление

Единый Клиент JaCarta

Удалённый доступ к ресурсам организации несёт пользу, но и создаёт ряд проблем для IT-департамента. Возможность корректной идентификации пользователей, запрашивающих доступ к информационной системе, достигается за счёт использования комплексных решений контроля доступа.

Внедрение решений для удалённого доступа без строгой аутентификации пользователей равносильно хранению важных данных в сейфовой ячейке, ключ от которой хранится на ближайшем журнальном столике.

Хорошие решения по аутентификации пользователей подразумевают гарантированный доступ к ресурсам компании только авторизованным пользователям.

PKI - эффективный метод аутентификации для систем строгой аутентификации в аспектах функциональности, безопасности и соблюдения зависимостей.

Единый Клиент JaCarta - программное обеспечение, позволяющее строить инфраструктуру с открытыми ключами с применением ключевых носителей JaCarta PKI. Данное программное обеспечение позволяет использовать защищённую передачу информации, основанную на инфраструктуре открытых ключей.

Электронные ключи могут поставляться в различных форм-факторах, включая USB-токены и смарт-карты с широкими возможностями кастомизации (нанесение логотипа, использование корпоративного стиля и т.д.). Все форм-факторы управляются единым интерфейсом, программным обеспечением Единый Клиент JaCarta. Единый Клиент JaCarta имеет унифицированные методы работы, такие, как PKCS#11, CAPI, которые обеспечивают поддержку множества приложений "из коробки", поддерживающих данные интерфейсы. Поддерживаются такие сценарии, как защищённый Web-вход, защищённый вход в систему, шифрование данных, шифрование почты. PKI ключи и сертификаты могут быть созданы, размещены и использованы наиболее безопасным способом при помощи аппаратных либо программных токенов.

JaCarta Management System предлагает Вашей организации комплексную платформу управления жизненным циклом ключей. JMS связывает идентификаторы с пользователями, позволяя контролировать сертификаты, используемые ими. JMS позволяет масштабировать систему без угрозы нарушения работы.

Azure Active Directory (Azure AD) - сервис, основанный на облачной платформе, позволяющий управлять сущностями в информационной системе.

MS Azure AD может быть сконфигурирован для поддержки двухфакторной аутентификации в нескольких режимах. Аутентификация по сертификатам может быть применена совместно с JaCarta PKI.

Применимость

Единый Клиент JaCarta (ЕК) - ПО, предназначенное для работы с токенами и смарт-картами JaCarta.

Окружение

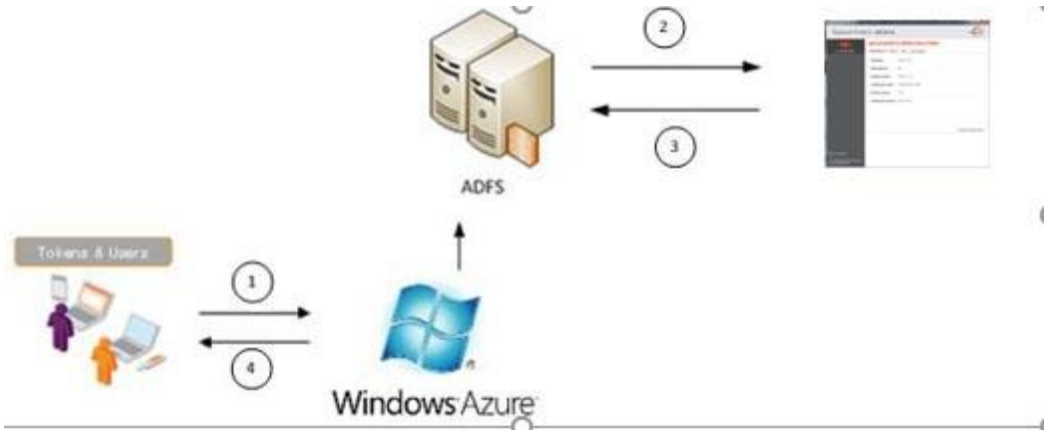
- Единый Клиент JaCarta (ЕК) - версии 2.9 или выше
- MS Azure AD - в облаке
- AS FS - на Windows Server 2012 R2

Для кого предназначен этот документ

Данная инструкция предназначена для системных администраторов, которые знакомы с MS Azure AD и заинтересованы в многофакторной аутентификации для данной системы. Инструкция позволит настроить аутентификация по сертификатам для Azure AD.

Аутентификация по сертификатам с применением Единый Клиент JaCarta

Схема ниже показывает, как пользователь с токеном либо смарт-картой взаимодействует с системой Azure AD.



1. Пользователь пытается получить доступ к Azure AD. Система перенаправляет пользователя на прокси-сервер для аутентификации.
2. После успешной аутентификации пользователь перенаправляется в ЕК для двухфакторной аутентификации. Пользователь использует токен JaCarta PKI, на котором расположен его сертификат и затем вводит PIN-код.
3. Система возвращает аутентификационные данные в ADFS, который, в свою очередь, возвращает данные в AZURE AD, принимая, либо отклоняя пользовательскую аутентификацию.
4. Пользователь получает доступ, либо получает сообщение об ошибке.

Требования к системе

Перед началом настройки убедитесь в корректности следующих пунктов.

- Для аутентификации по сертификатам необходимо установить и настроить роль Центра сертификации для сервера.

Если используется JMS, необходимо установить коннектор. Подробные инструкции можно найти в "JMS Руководство Администратора".

- Пользователь должен иметь на руках токен с корректным сертификатом на нём.
- На клиентской машине должен быть установлен Единый Клиент JaCarta 2.9 или выше.

Поддерживаемые токены

USB токены:

- JaCarta PKI;
- JaCarta PKI/Flash;
- JaCarta PKI/ГОСТ;
- JaCarta PKI/ГОСТ/Flash.

Смарт-карты:

- JaCarta PKI;
- JaCarta PKI/ГОСТ.

⚠ Для смарт-карт требуется считыватель ASEDriveIII USB.

Настройка ADFS и MS Azure AD

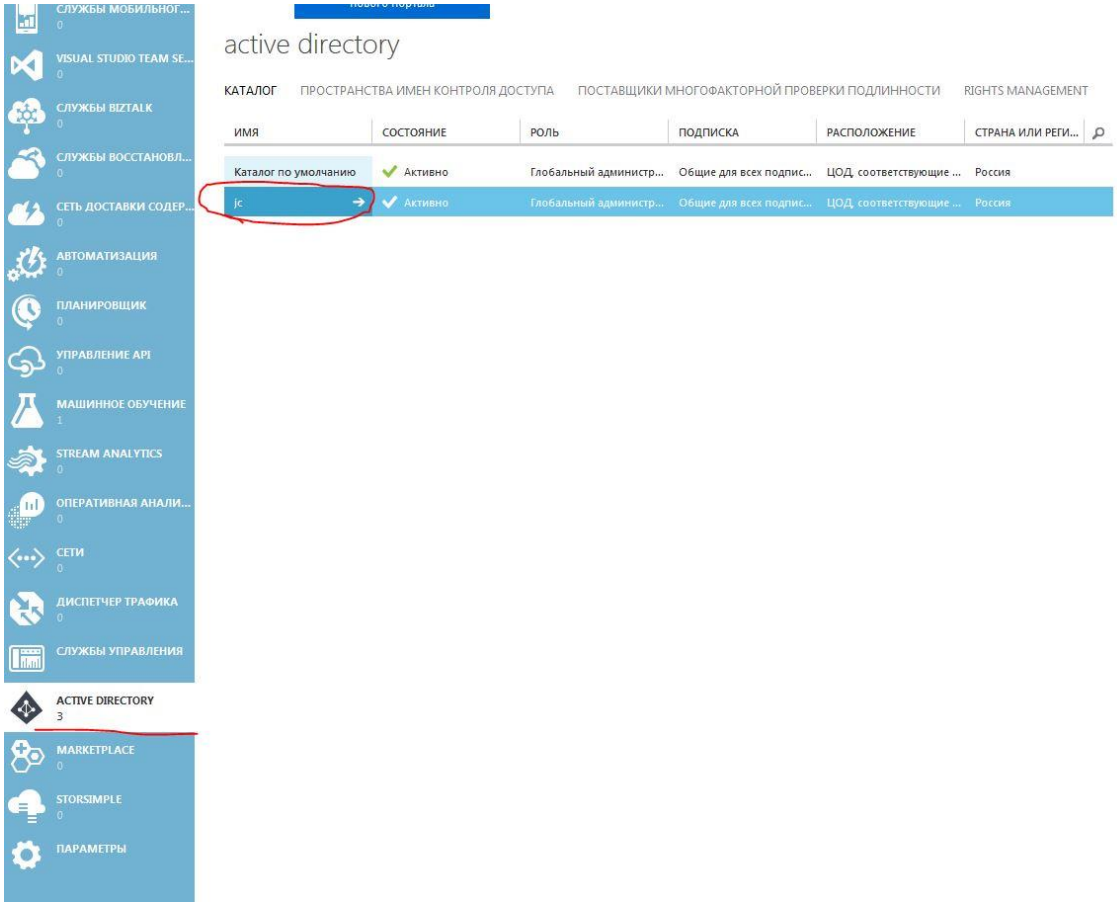
Настройка включает в себя следующие шаги:

1) добавление домена в MS Azure;
2) синхронизация домена с Azure;
3) проверка установленного AD Connect;
4) разрешение Azure AD Federated Domains;
5) настройка политик аутентификации в ADFS.

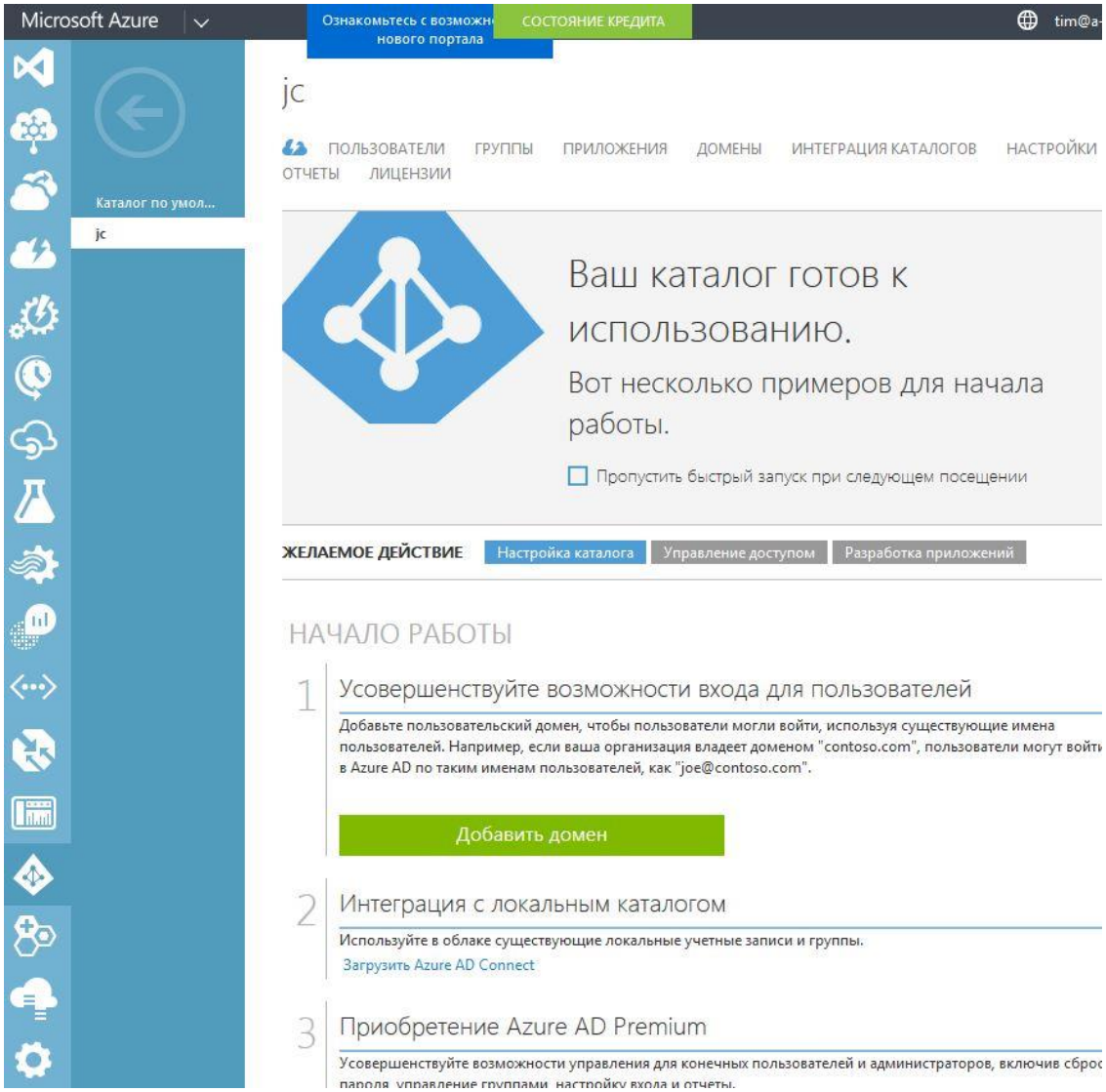
Добавление домена в Azure

1. Залогиньтесь на портале управления Azure.

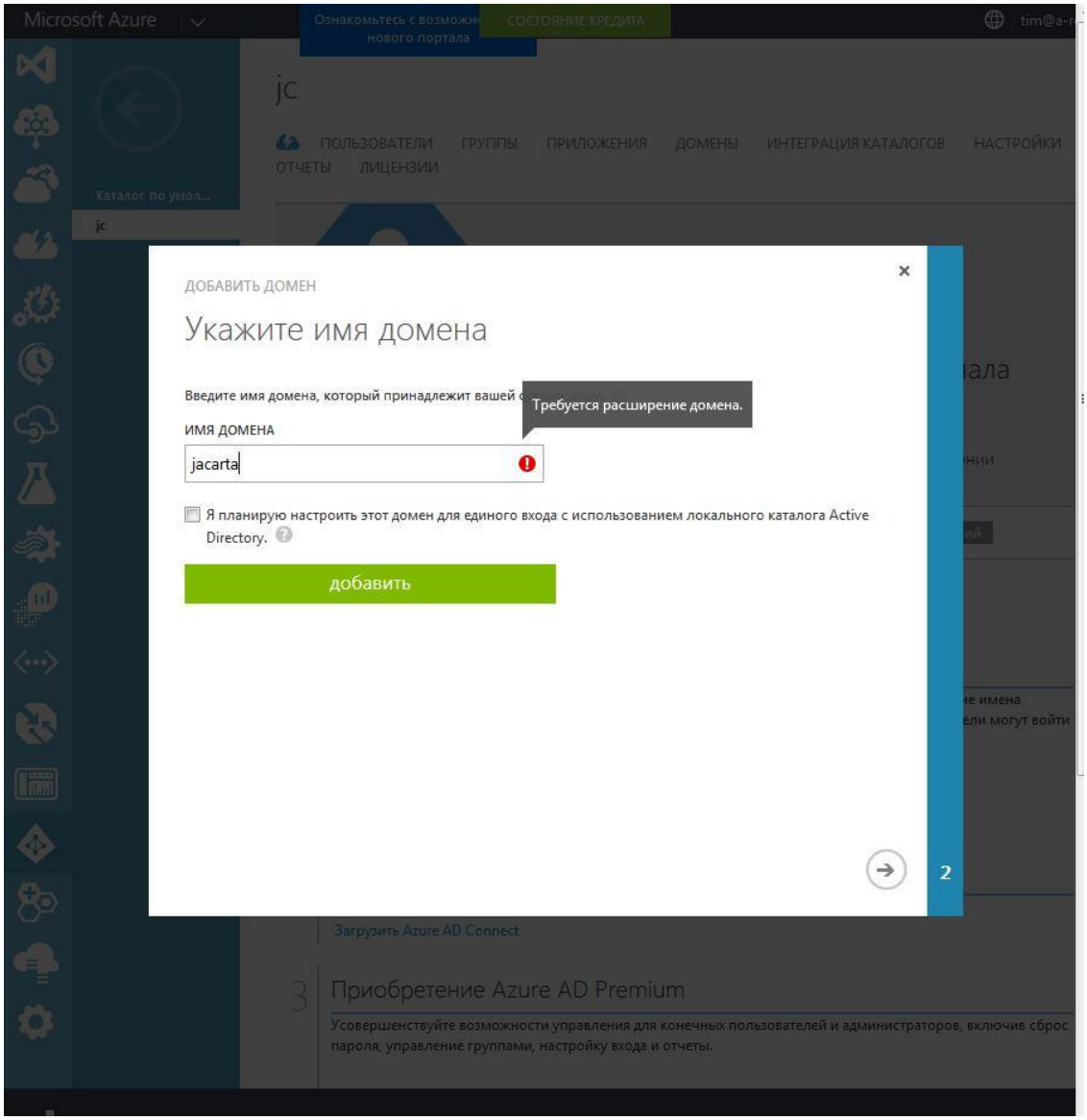
2. В левой панели выберите Active Directory и выберите директорию, которую необходимо настроить.



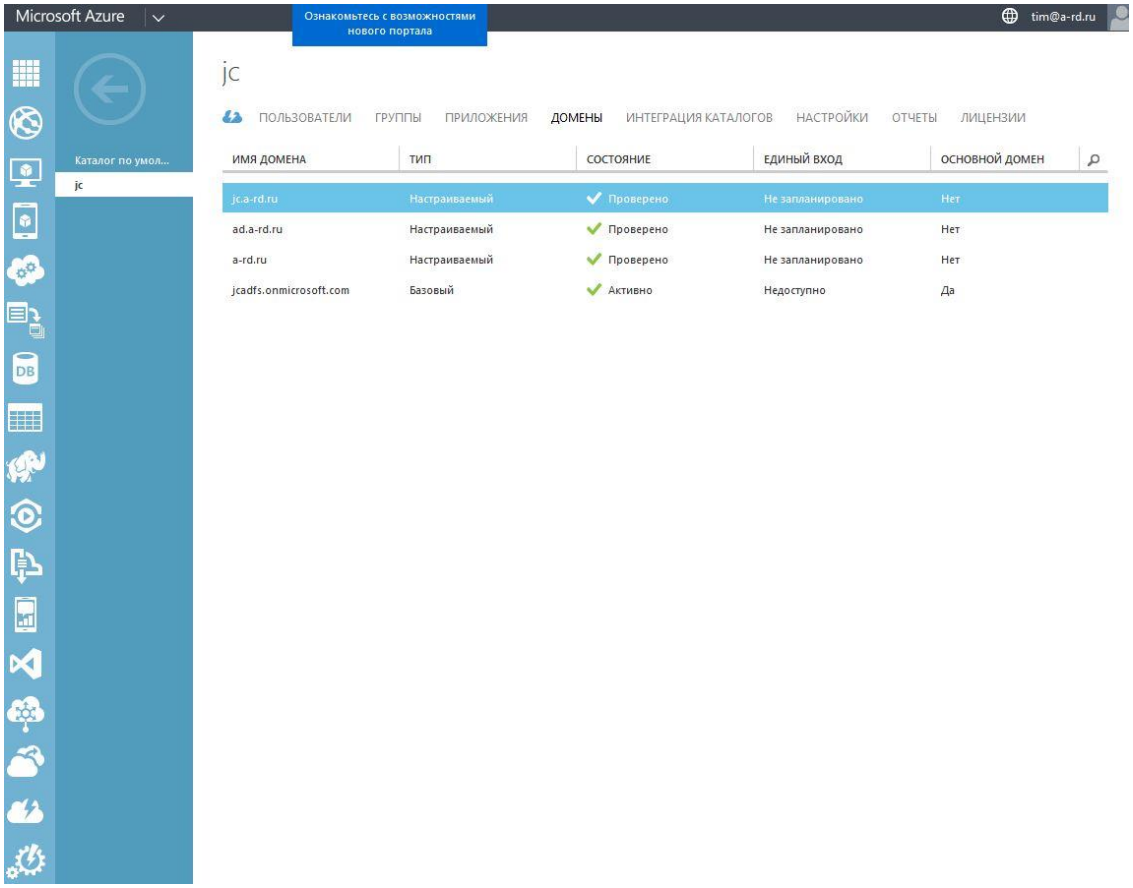
3. Нажмите Добавить домен.



4. В появившемся окне в поле "Имя домена" введите имя и затем нажмите Добавить.



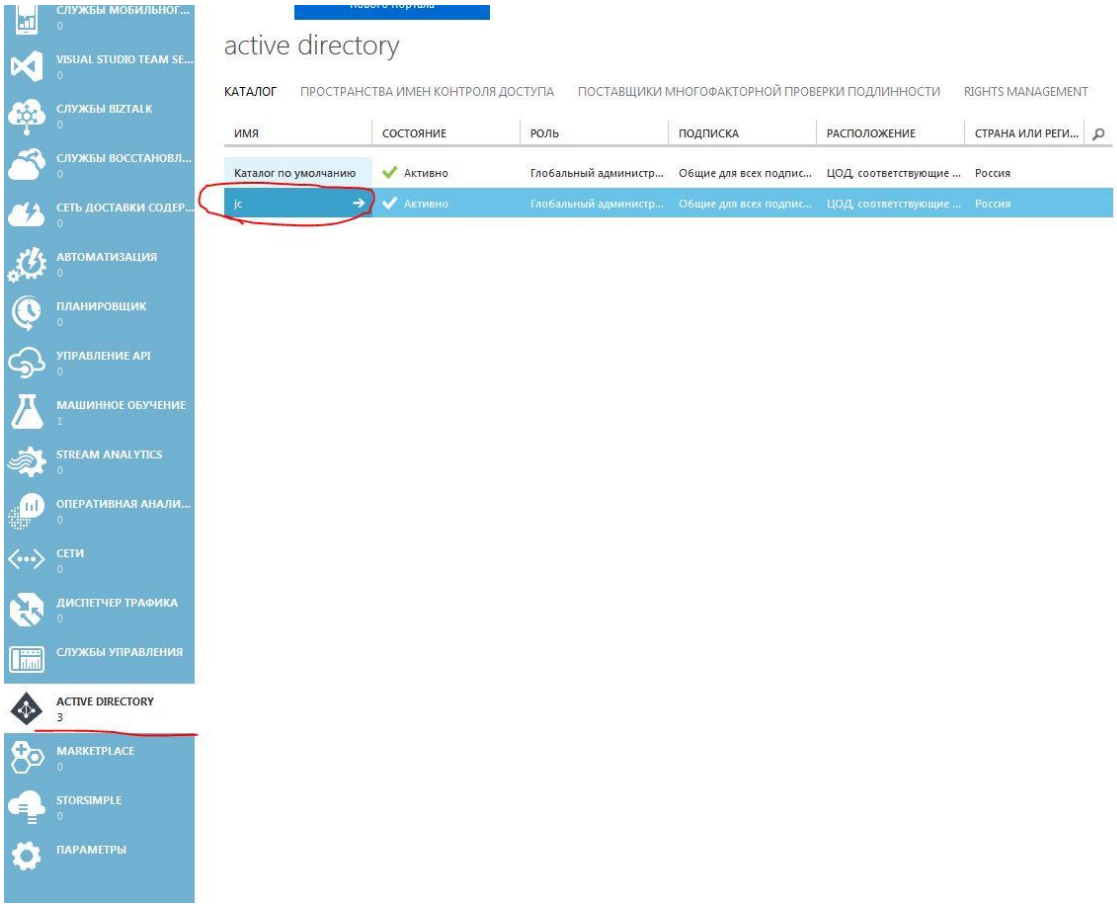
5. В окне Microsoft Azure в правой панели видно, что домен добавлен (вкладка домены), но не подтверждён. Для подтверждения добавьте значения в DNS запись, в соответствии с инструкцией. Затем нажмите Подтвердить.



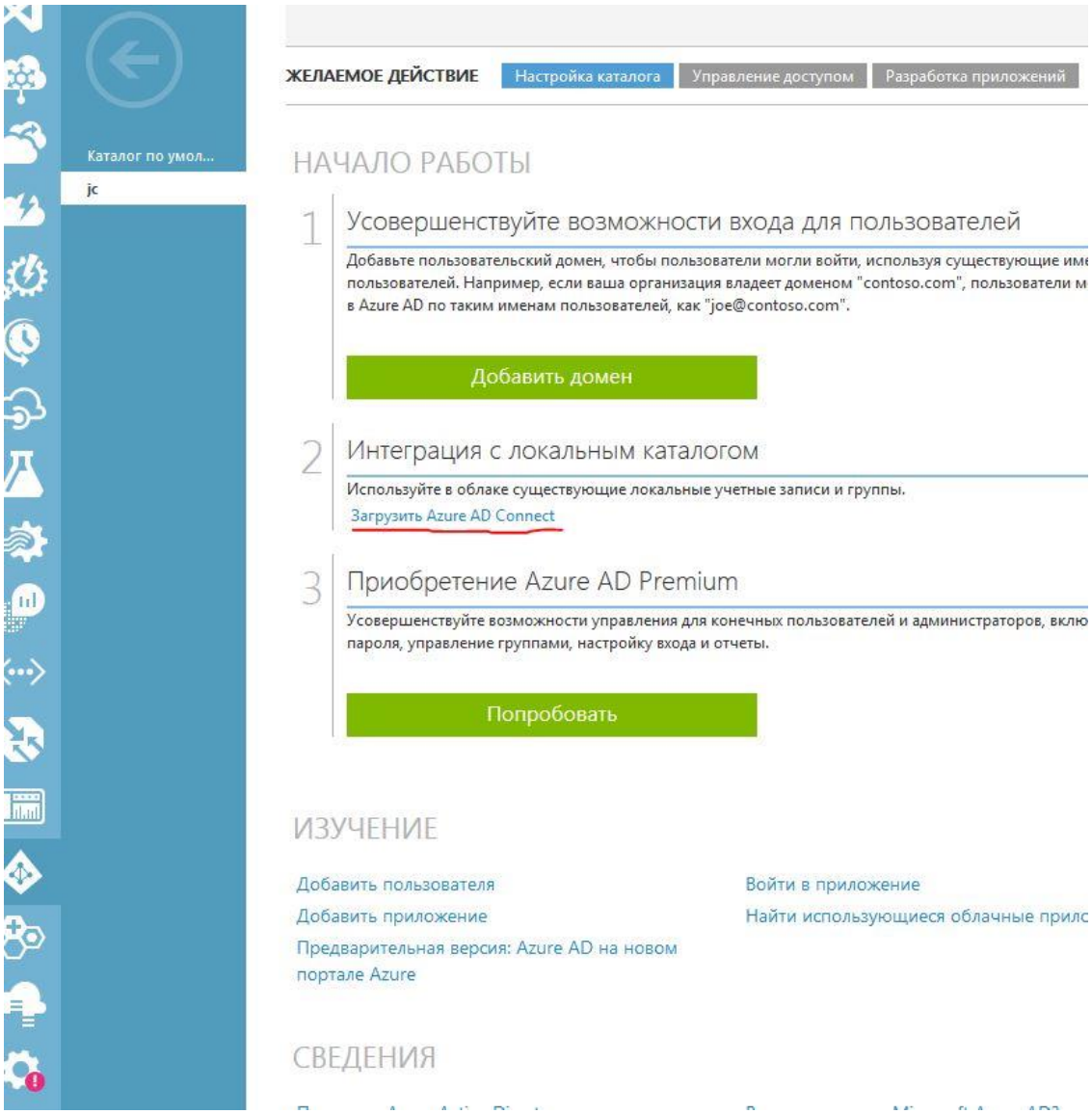
6. Домен готов к использованию.

Синхронизация домена в Azure

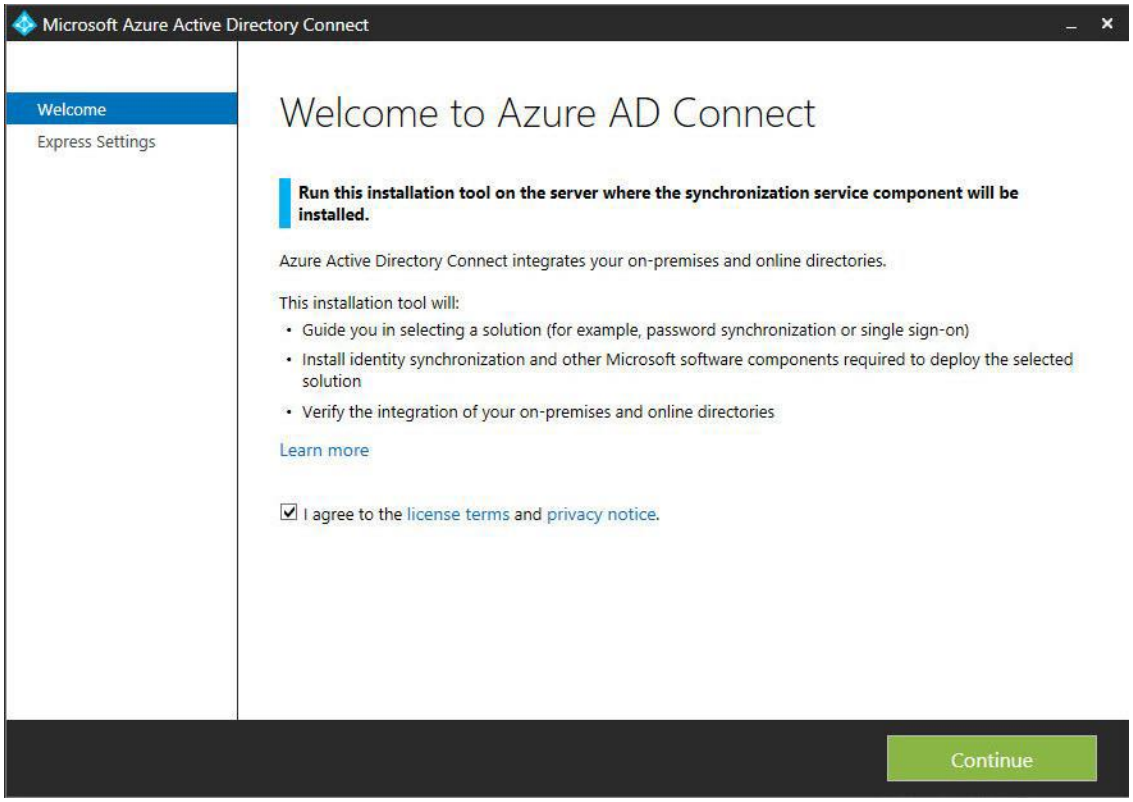
1. В левой панели выберите ACTIVE DIRECTORY, затем в правой панели выберите Ваш каталог.



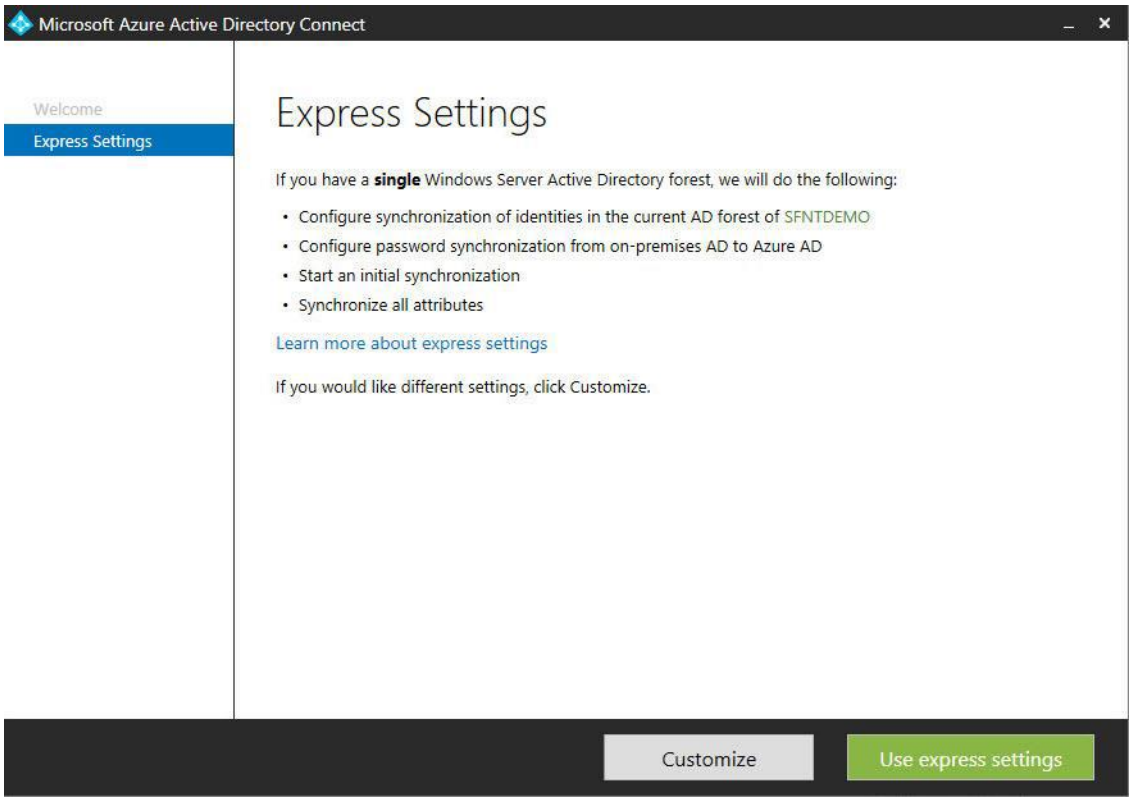
2. Под пунктом Интеграция с локальным каталогом выберите Загрузить Azure AD Connect.



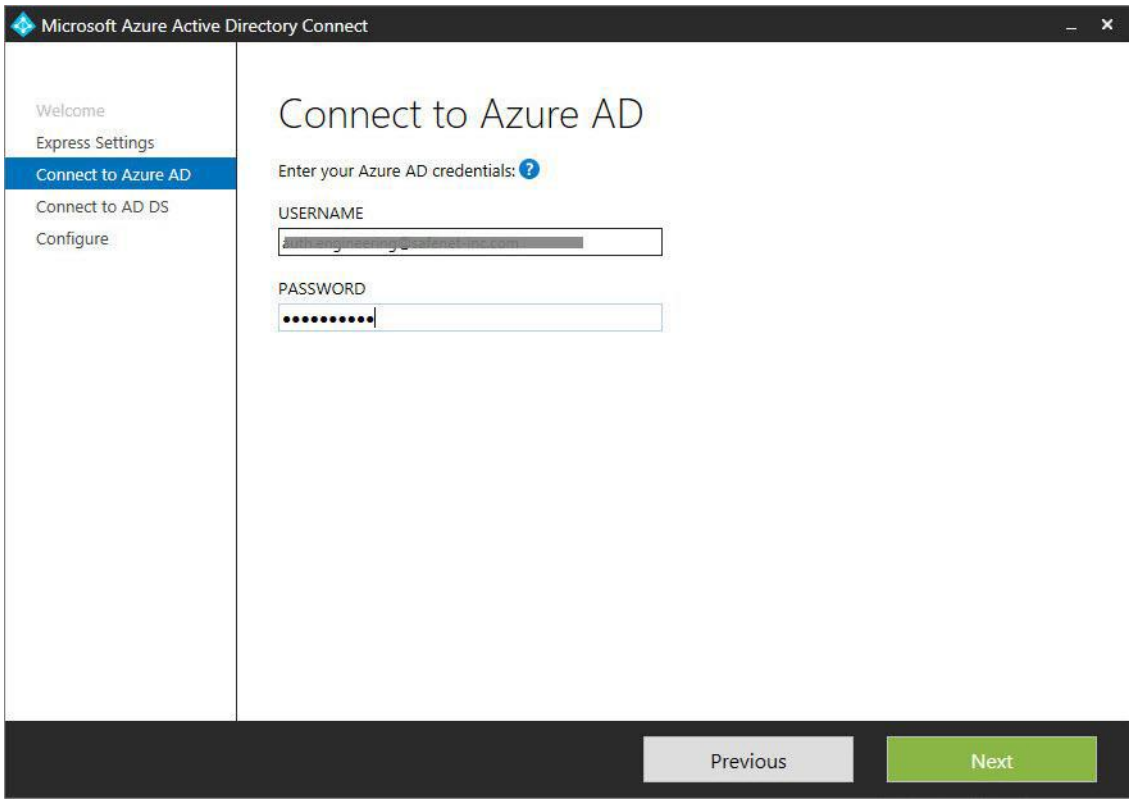
3. Установите Azure AD Connect на машину, которая является частью домена для соединения с Azure. В Microsoft Azure Active Directory Connect нажмите Продолжить.



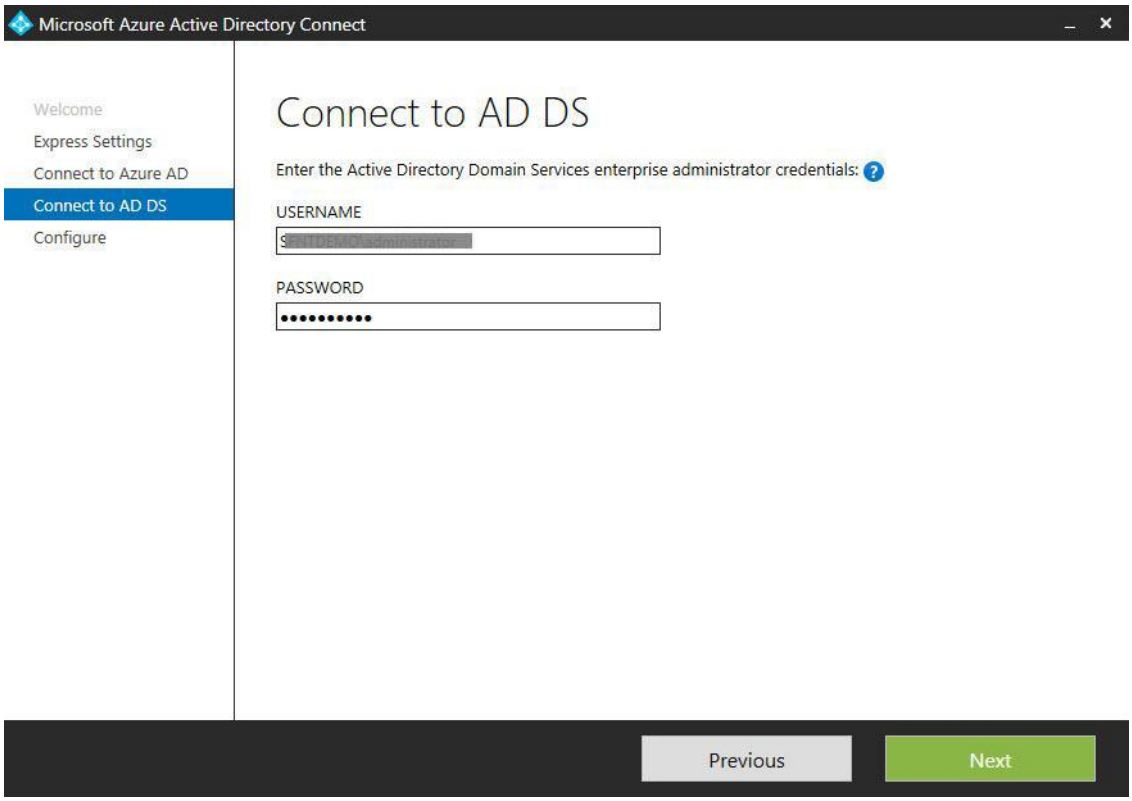
4. Нажмите Использовать настройки по умолчанию.



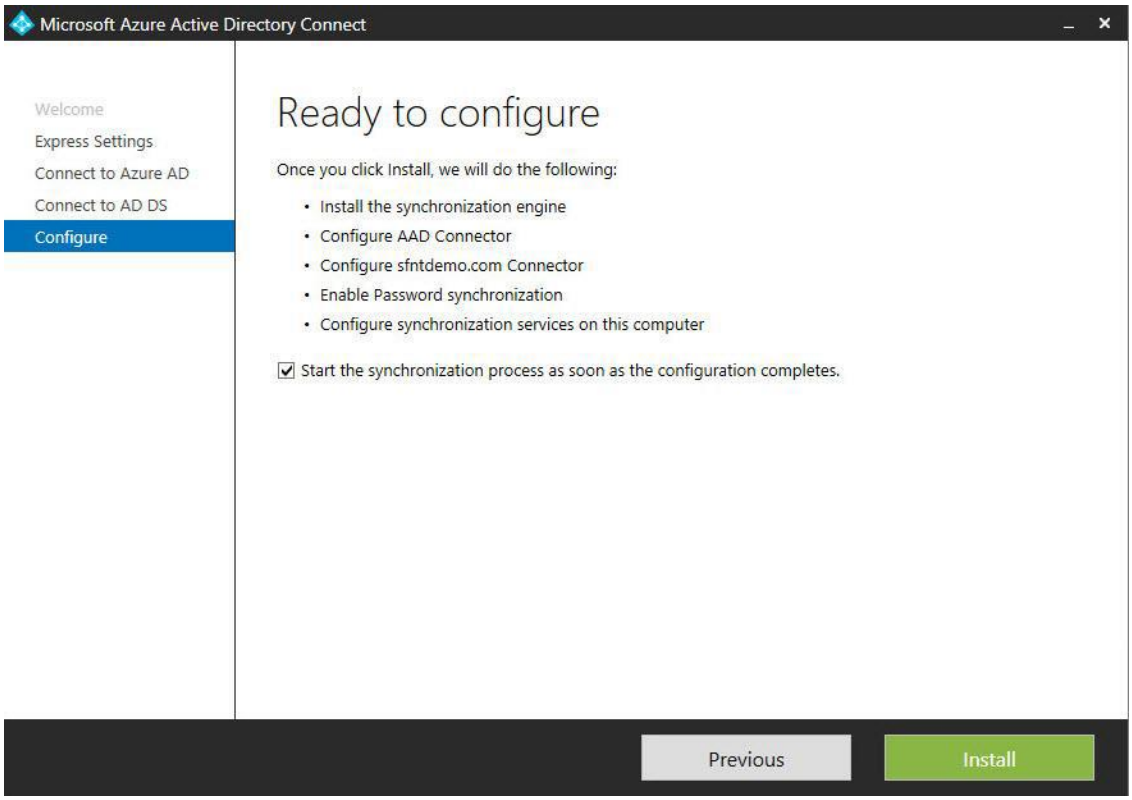
5. Введите логин и пароль администратора Azure AD и затем кликните Next.



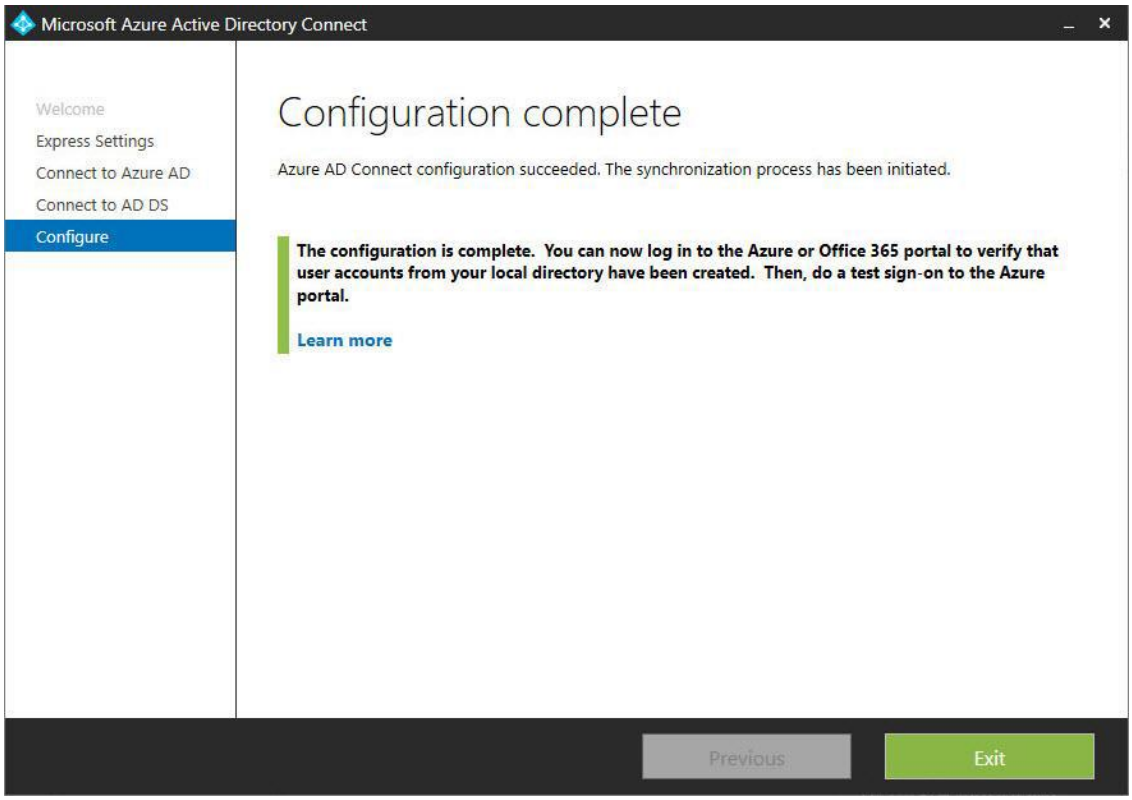
6. Введите логин и пароль администратора AD и нажмите Продолжить.



7. Нажмите Установить.



8. Нажмите Выход.

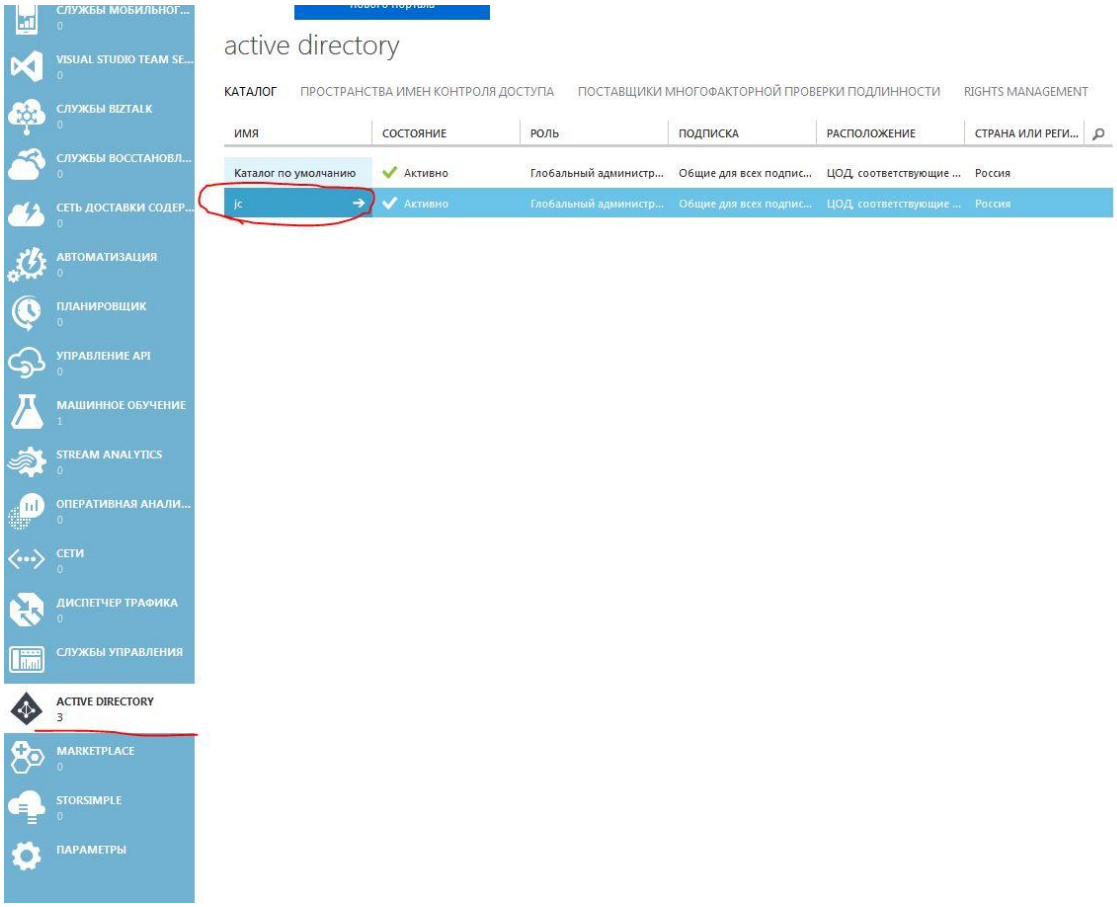


После завершения процесса синхронизации пользователи AD смогут получить доступ к Azure.

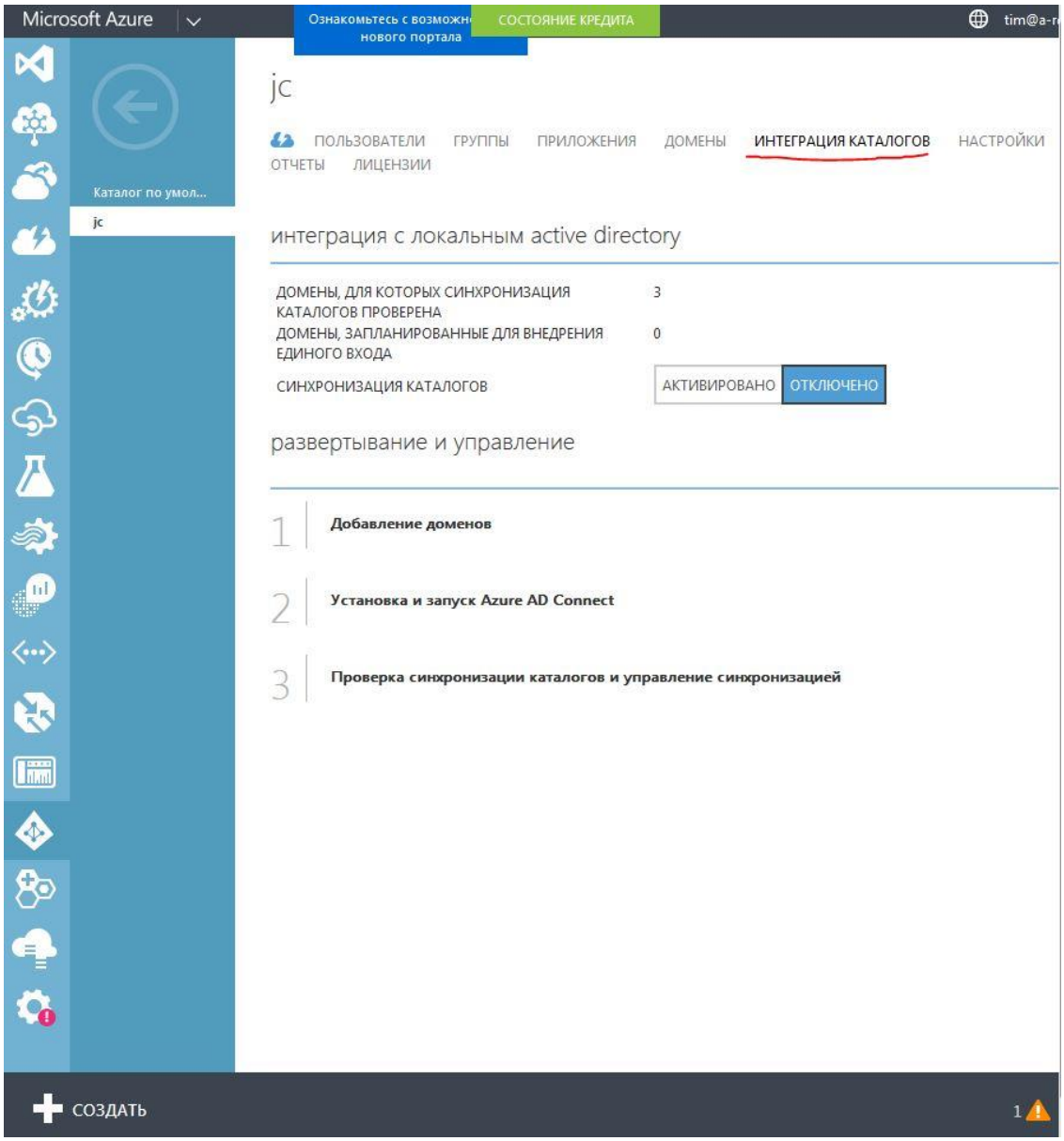
Проверка установленного AD Connect

После успешной инсталляции Azure AD Connect Вы можете проверить процесс синхронизации на портале Azure. Также можно сверить время начала синхронизации.

1. Залогиньтесь на портал Azure.
2. В левой панели нажмите Active Directory, затем в правой панели выберите Вашу директорию.



3. Нажмите вкладку Интеграция каталогов.



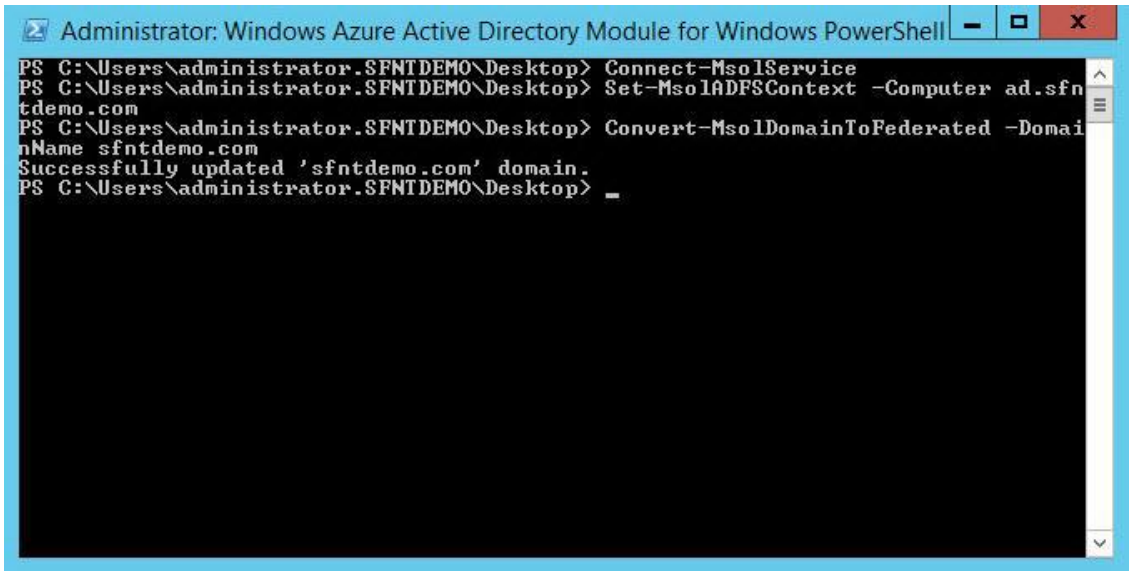
Под Синхронизацией каталогов будет указано время последней синхронизации.

Настройка Azure AD FS

1. Залогиньтесь на сервере AD FS, как администратор домена.
2. Откройте Windows Azure AD Module для PowerShell.
3. В командной строке введите Connect-MsolService, затем нажмите Enter.
4. В окне ввода учётных данных введите логин и пароль администратора Azure.

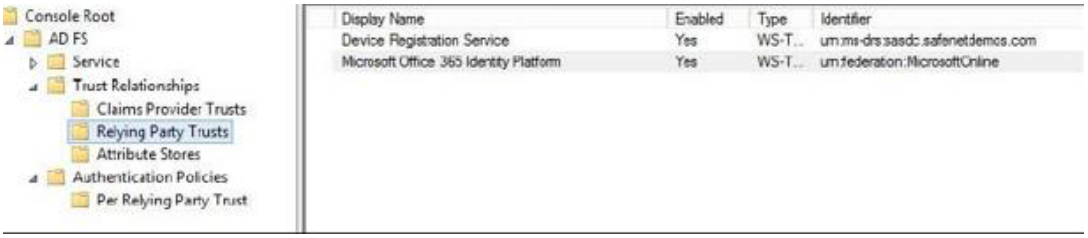
5. В командной строке выполните следующие шаги:

- введите Set-MsolADFSContext -Computer <имя компьютера AD FS>, затем Enter;
- введите Convert-MsolDomainToFederated -DomainName <имя домена>, затем Enter.



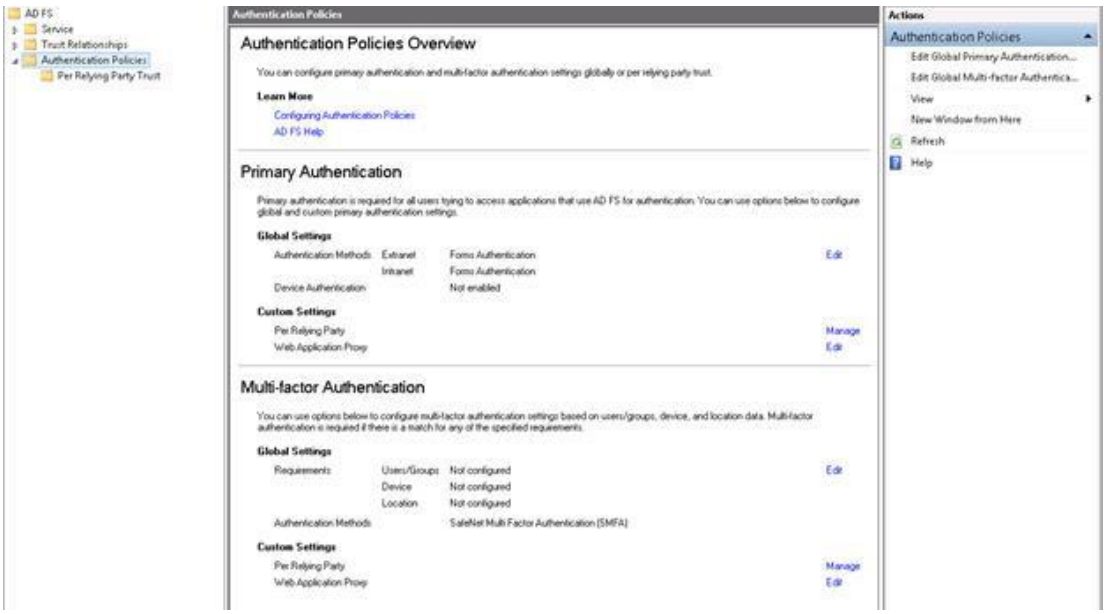
6. Откройте консоль AD FS Management.
7. В левой панели, под Console Root, нажмите AD FS > Trust Relationships > Relying Party Trusts.

В правой панели Microsoft Office 365 Identity Platform должно отображаться как доверенная.



Настройка политик аутентификации AD FS

1. В консоли администратора AD FS, в левой панели, под AD FS нажмите Authentication Policies.
2. В правой панели нажмите Edit Global Primary Authentication.

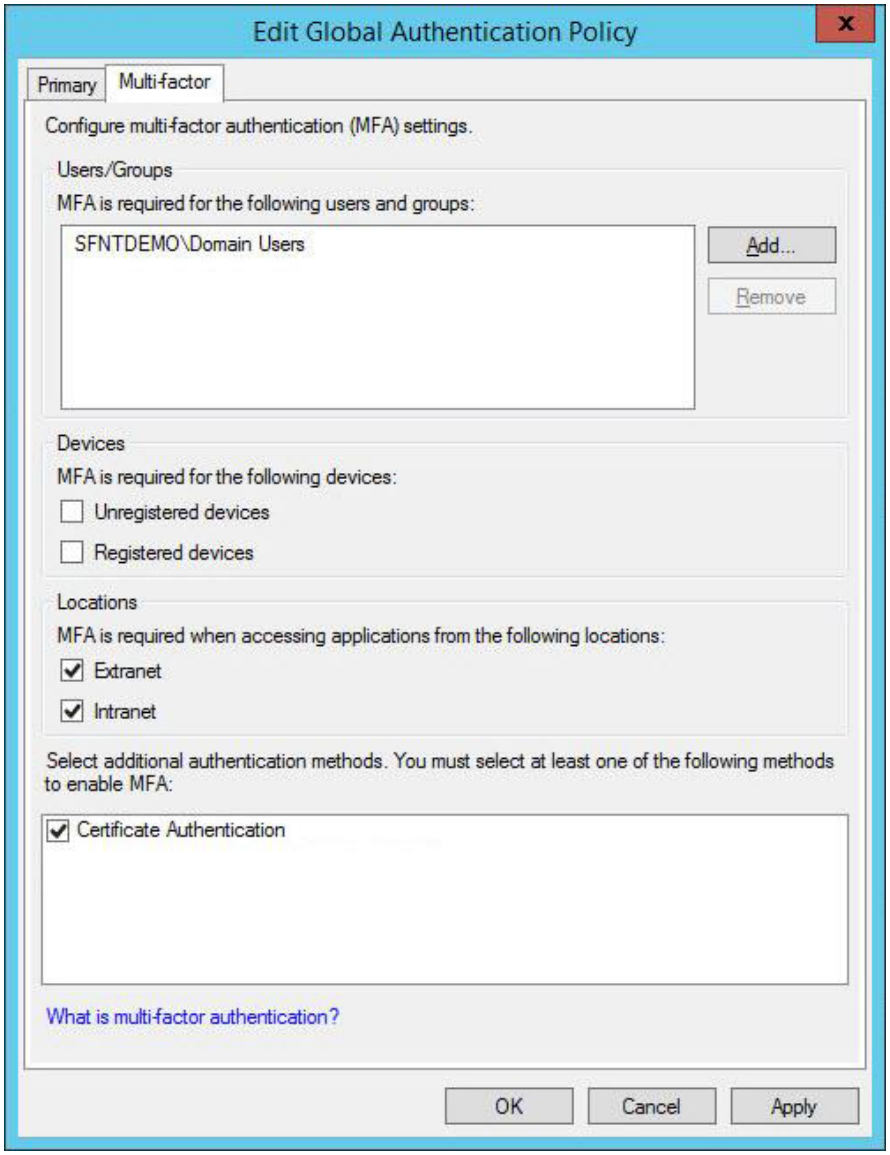


3. В окне Edit Global Authentication Policy в первой вкладке убедитесь в том, что Forms Authentication выбрана для Extranet и Intranet.

Для выбора механизма аутентификации по сертификатам единственным механизмом убедитесь в том, что Certificate Authentication выставлена и в Extranet, и в Intranet.

4. Нажмите на вкладку Multi-factor и выполните следующие шаги:

- под Users/Groups добавьте требуемые группы или пользователей, для которых потребуется многофакторная аутентификация;
- под Locations выберите Extranet и/или Intranet, в соответствии с предпочитаемой конфигурацией;
- выберите Certificate Authentication как дополнительный метод аутентификации;
- нажмите OK.

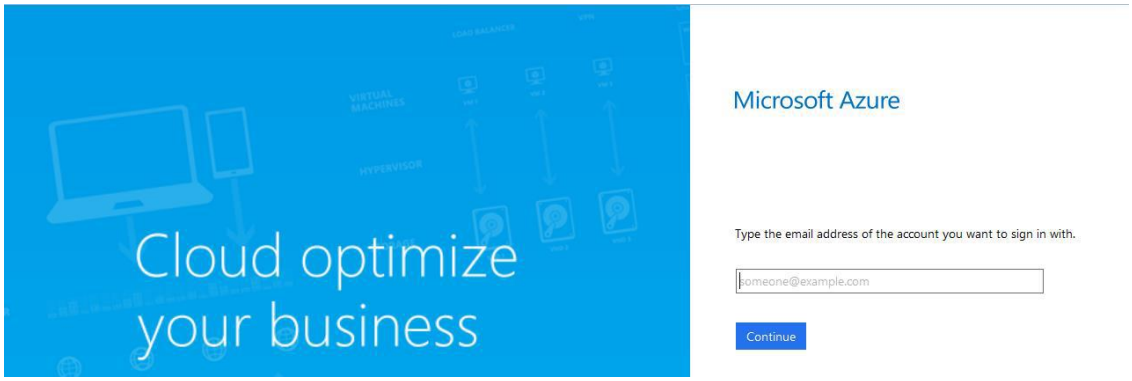


Запуск Решения

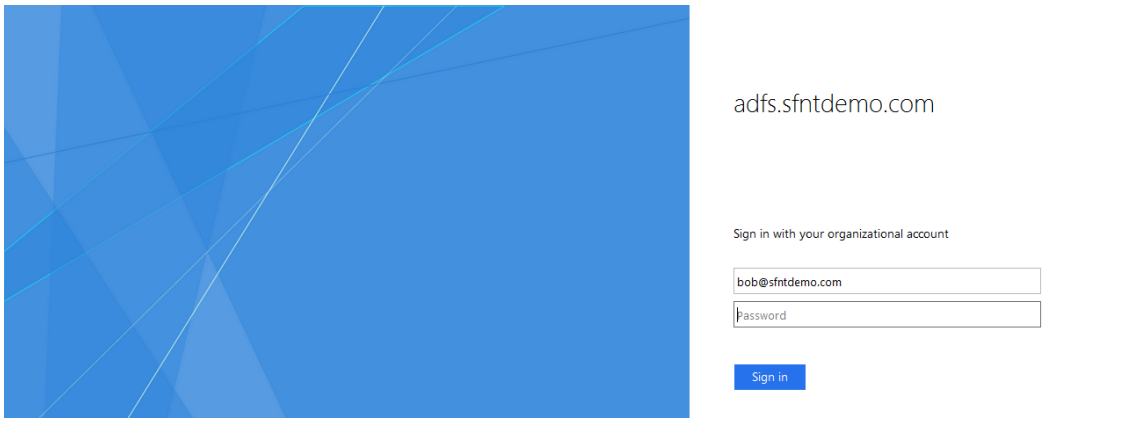
1. В Web-браузере откройте страницу:

https://accounts.activedirectory.windowsazure.com

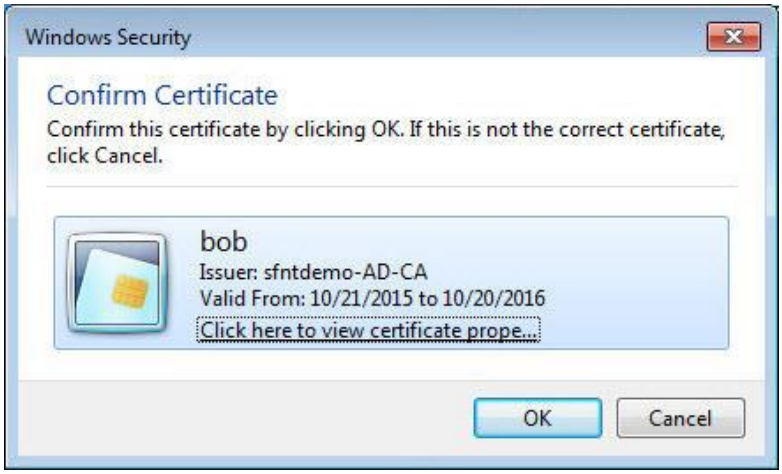
2. В панели доступа Azure введите имя пользователя AD, затем нажмите Далее.



Вы будете перенаправлены на страницу логина Вашей организации. Введите пароль AD и нажмите Вход.



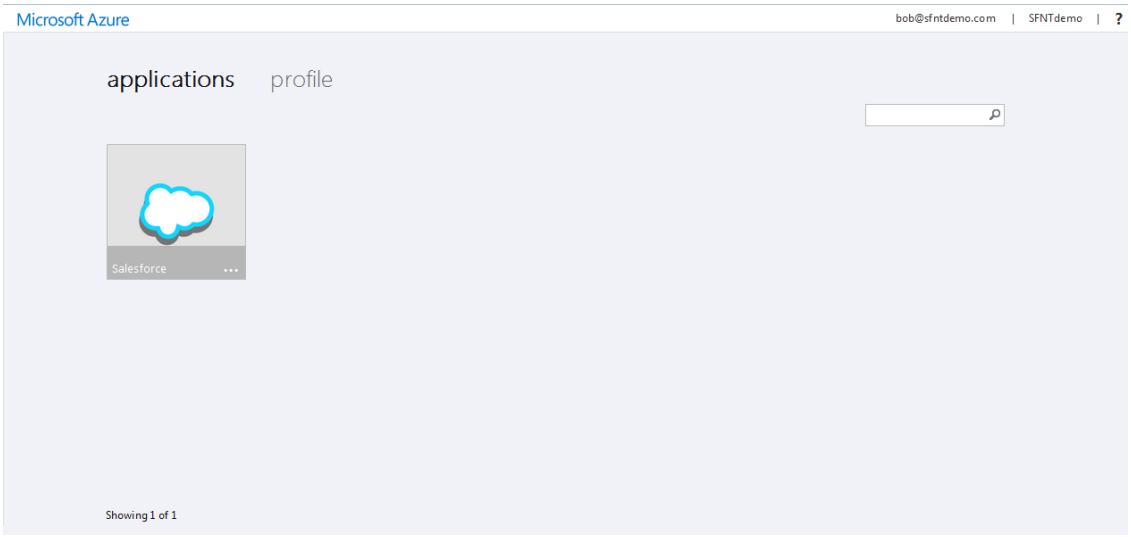
3. Браузер отобразит все доступные на машине сертификаты. Выберите сертификат, требуемый для входа.
4. Нажмите OK.



5. В окне ввода PIN-кода токена введите Ваш PIN-код.

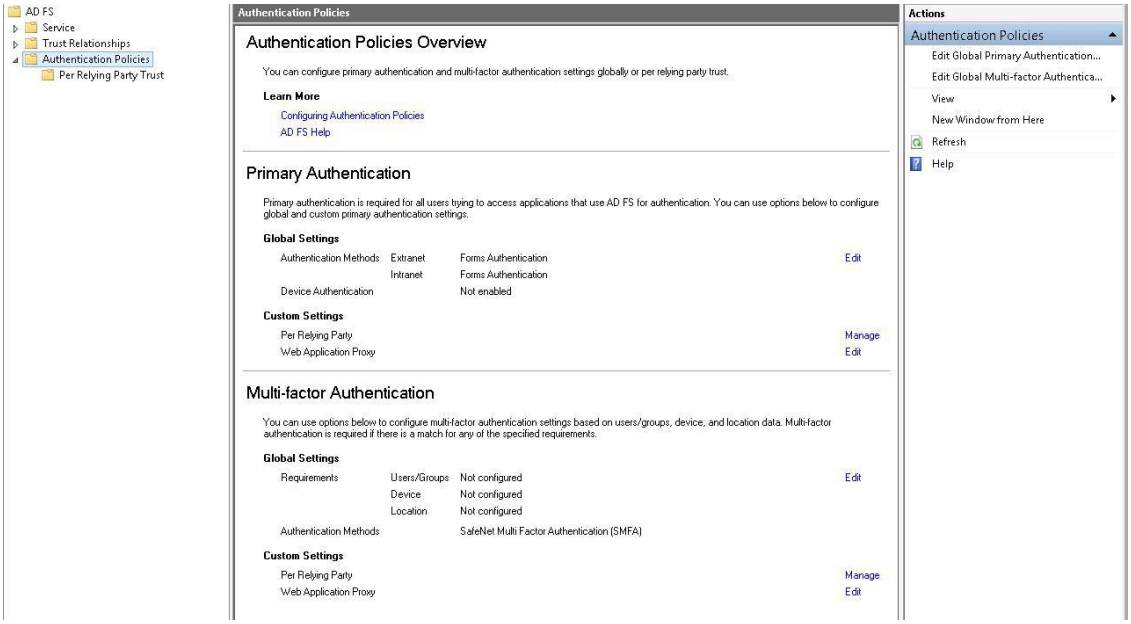
После успешной аутентификации Вы будете перенаправлены в панель доступа Azure Acess Panel.

Теперь Вы можете использовать приложения без какой-либо дополнительной аутентификации.



Дополнение: Настройка AD FS для аутентификации по сертификатам SSO

1. В консоли управления AD FS в левой панели под AD FS нажмите Authentication Policies.
2. В правой панели нажмите Edit Global Primary Authentication.



3. В окне Edit Global Authentication Policy в главной вкладке убедитесь в том, что Certificate Authentication выбран для Extranet и Intranet.

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru