



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.

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.". Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией "Аладдин Р.Д." без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация Apple Inc. Владельцем товарного знака IOS является компания Cisco (Cisco Systems, Inc). Владельцем товарного знака Windows Vista и др. — корпорация Microsoft (Microsoft Corporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев. Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.

Оглавление

Единый Клиент JaCarta	4
Применимость	4
Окружение	4
Для кого предназначен этот документ	5
Аутентификация по сертификатам с применением Единый Клиент JaCarta	5
Требования к системе	5
Поддерживаемые токены	6
Настройка ADFS и MS Azure AD	6
Добавление домена в Azure	6
Синхронизация домена в Azure	11
Проверка установленного AD Connect	19
Настройка Azure AD FS	21
Настройка политик аутентификации AD FS	23
Запуск Решения	26
Дополнение: Настройка AD FS для аутентификации по сертификатам SSO	28
Контакты, техническая поддержка	30
Регистрация изменений	31

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

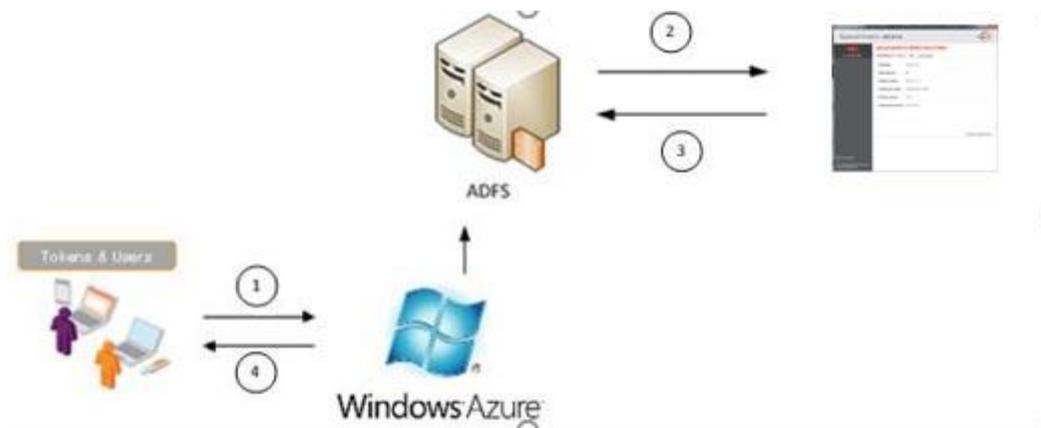
- Единый Клиент JaCarta (ЕК) - версии 2.9 или выше
- MS Azure AD - в облаке
- AS FS - на Windows Server 2012 R2

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

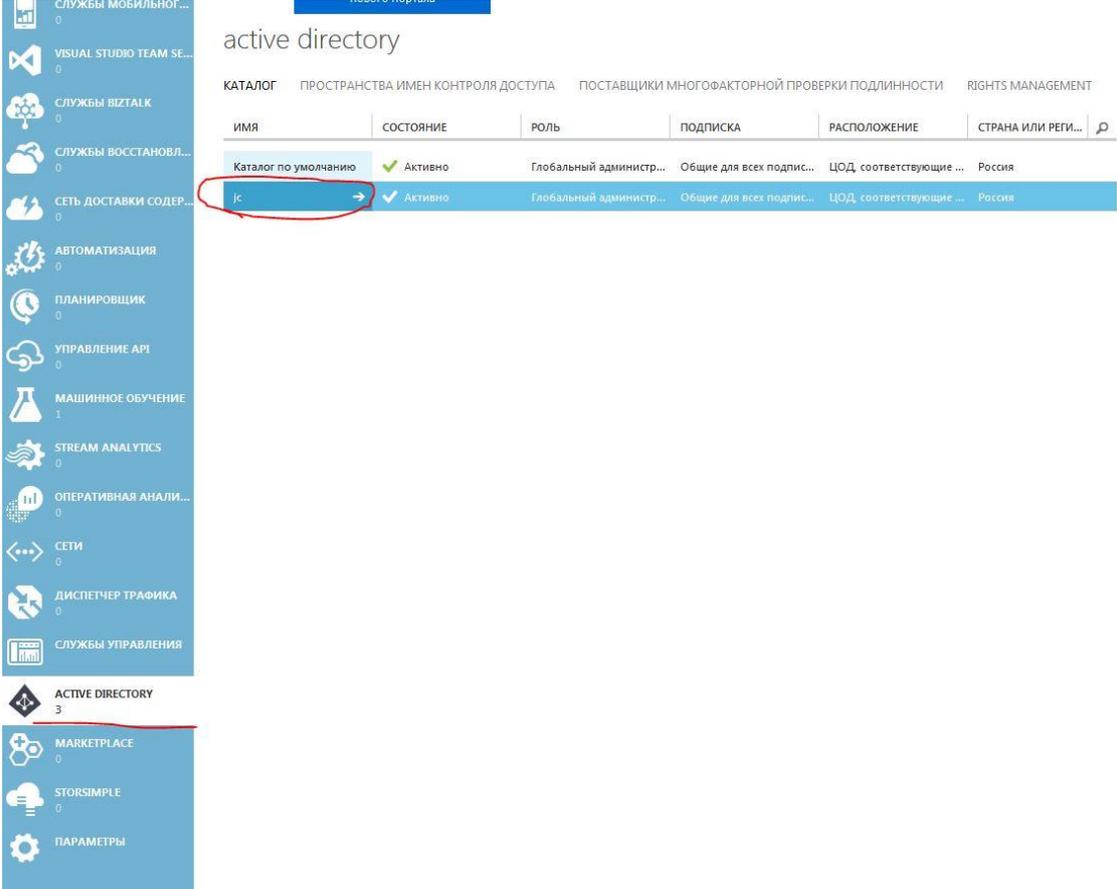
Настройка включает в себя следующие шаги:

- 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.

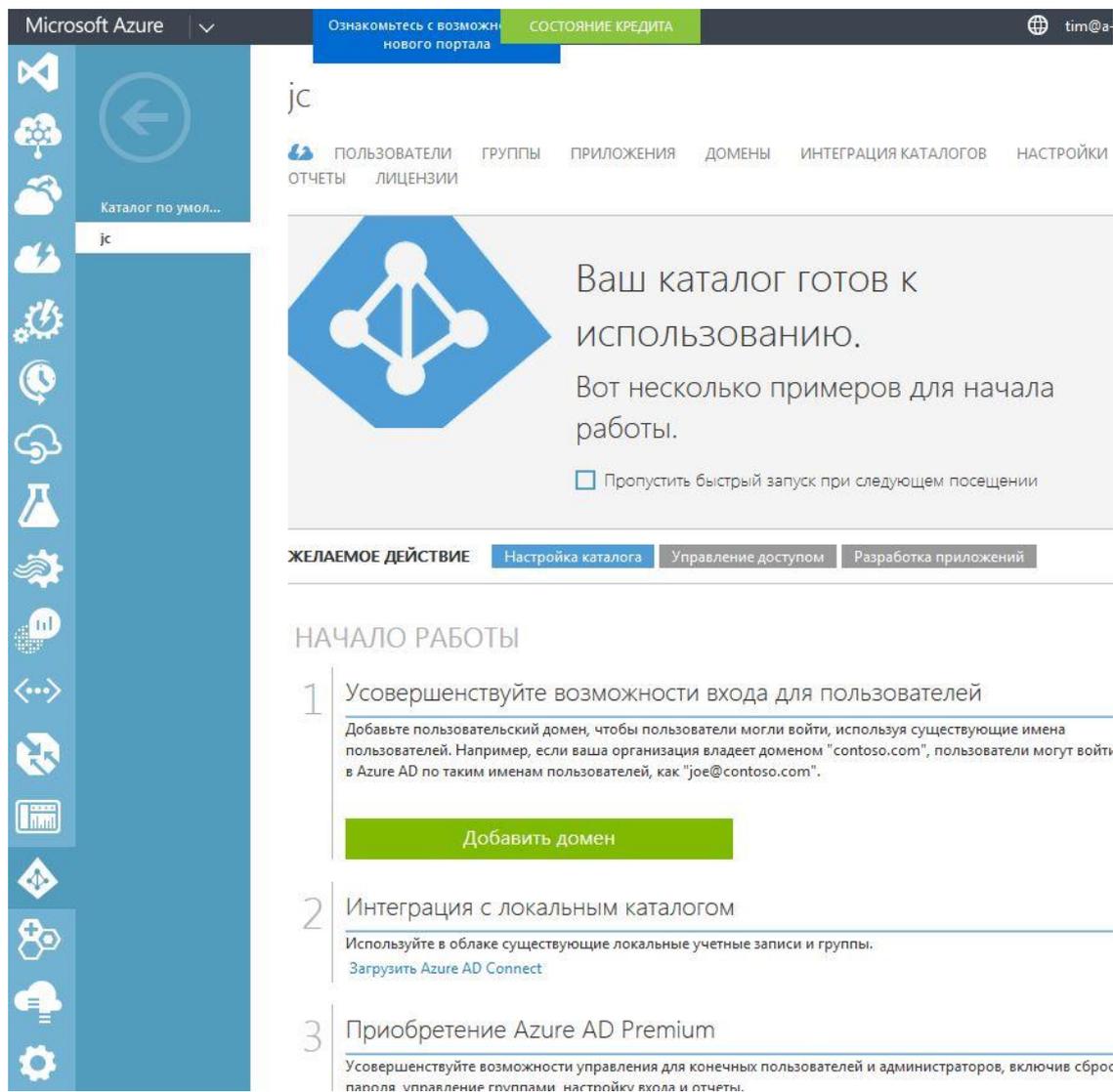
2. В левой панели выберите Active Directory и выберите директорию, которую необходимо настроить.



The screenshot shows the Azure Active Directory console interface. The left-hand navigation pane is visible, with the 'ACTIVE DIRECTORY' section selected. The main content area displays the 'active directory' page, which includes a table of directories. The table has columns for 'ИМЯ' (Name), 'СОСТОЯНИЕ' (Status), 'РОЛЬ' (Role), 'ПОДПИСКА' (Subscription), 'РАСПОЛОЖЕНИЕ' (Location), and 'СТРАНА ИЛИ РЕГИ...' (Country or Region). The 'IS' directory is highlighted with a red circle, indicating it is the one to be configured.

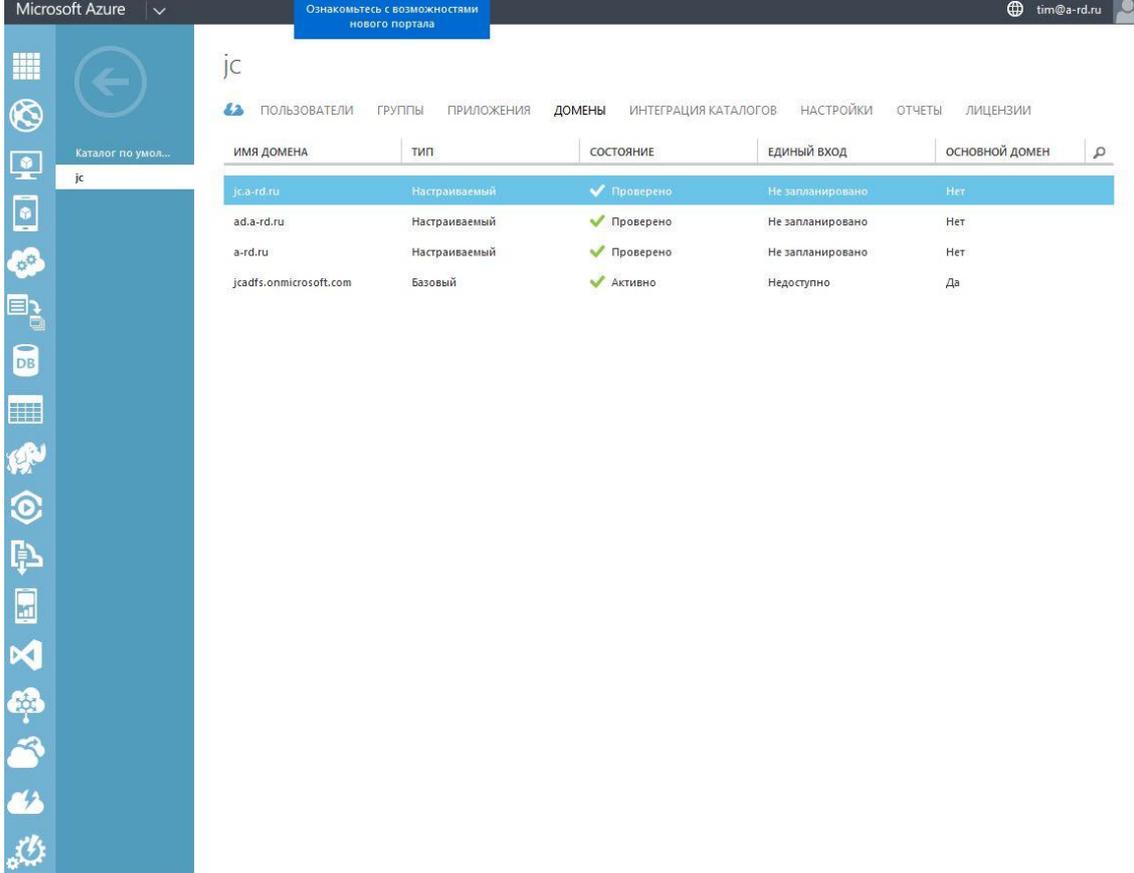
ИМЯ	СОСТОЯНИЕ	РОЛЬ	ПОДПИСКА	РАСПОЛОЖЕНИЕ	СТРАНА ИЛИ РЕГИ...
Каталог по умолчанию	Активно	Глобальный администр...	Общие для всех подпис...	ЦОД соответствующие ...	Россия
IS	Активно	Глобальный администр...	Общие для всех подпис...	ЦОД соответствующие ...	Россия

3. Нажмите Добавить домен.



The screenshot shows the Microsoft Azure AD portal interface. At the top, there's a navigation bar with 'Microsoft Azure' on the left, a search bar, and a user profile 'tim@a...'. Below the navigation bar, there's a sidebar with various icons for navigation. The main content area is titled 'jс' and features a navigation menu with items like 'ПОЛЬЗОВАТЕЛИ', 'ГРУППЫ', 'ПРИЛОЖЕНИЯ', 'ДОМЕНЫ', 'ИНТЕГРАЦИЯ КАТАЛОГОВ', 'НАСТРОЙКИ', 'ОТЧЕТЫ', and 'ЛИЦЕНЗИИ'. A large banner message reads: 'Ваш каталог готов к использованию. Вот несколько примеров для начала работы.' Below this, there's a checkbox for 'Пропустить быстрый запуск при следующем посещении'. Underneath, there's a section 'ЖЕЛАЕМОЕ ДЕЙСТВИЕ' with three buttons: 'Настройка каталога', 'Управление доступом', and 'Разработка приложений'. The 'НАЧАЛО РАБОТЫ' section contains three numbered steps: 1. 'Усовершенствуйте возможности входа для пользователей' with a green 'Добавить домен' button; 2. 'Интеграция с локальным каталогом' with a link to 'Загрузить Azure AD Connect'; 3. 'Приобретение Azure AD Premium' with a link to 'Усовершенствуйте возможности управления для конечных пользователей и администраторов, включив сброс пароля, управление группами, настройку входа и отчеты.'

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.



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and a user profile 'tim@a-rd.ru'. The left sidebar contains various service icons. The main content area is titled 'jc' and has a navigation menu with 'ПОЛЬЗОВАТЕЛИ', 'ГРУППЫ', 'ПРИЛОЖЕНИЯ', 'ДОМЕНЫ', 'ИНТЕГРАЦИЯ КАТАЛОГОВ', 'НАСТРОЙКИ', 'ОТЧЕТЫ', and 'ЛИЦЕНЗИИ'. The 'ДОМЕНЫ' tab is selected, displaying a table of domains.

ИМЯ ДОМЕНА	ТИП	СОСТОЯНИЕ	ЕДИНЫЙ ВХОД	ОСНОВНОЙ ДОМЕН
jc.a-rd.ru	Настраиваемый	✓ Проверено	Не запланировано	Нет
ad.a-rd.ru	Настраиваемый	✓ Проверено	Не запланировано	Нет
a-rd.ru	Настраиваемый	✓ Проверено	Не запланировано	Нет
jcadfs.onmicrosoft.com	Базовый	✓ Активно	Недоступно	Да

6. Домен готов к использованию.

Синхронизация домена в Azure

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

The screenshot shows the Azure Active Directory portal interface. On the left, the navigation pane is visible with 'ACTIVE DIRECTORY' selected. The main content area displays the 'active directory' section with a table of directories. The table has columns for 'ИМЯ', 'СОСТОЯНИЕ', 'РОЛЬ', 'ПОДПИСКА', 'РАСПОЛОЖЕНИЕ', and 'СТРАНА ИЛИ РЕГИ...'. The row for 'Ис' is highlighted with a red circle around the name and a red arrow pointing to the right.

ИМЯ	СОСТОЯНИЕ	РОЛЬ	ПОДПИСКА	РАСПОЛОЖЕНИЕ	СТРАНА ИЛИ РЕГИ...
Каталог по умолчанию	Активно	Глобальный администр...	Общие для всех подпис...	ЦОД соответствующие ...	Россия
Ис	Активно	Глобальный администр...	Общие для всех подпис...	ЦОД соответствующие ...	Россия

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

ЖЕЛАЕМОЕ ДЕЙСТВИЕ Настройка каталога Управление доступом Разработка приложений

НАЧАЛО РАБОТЫ

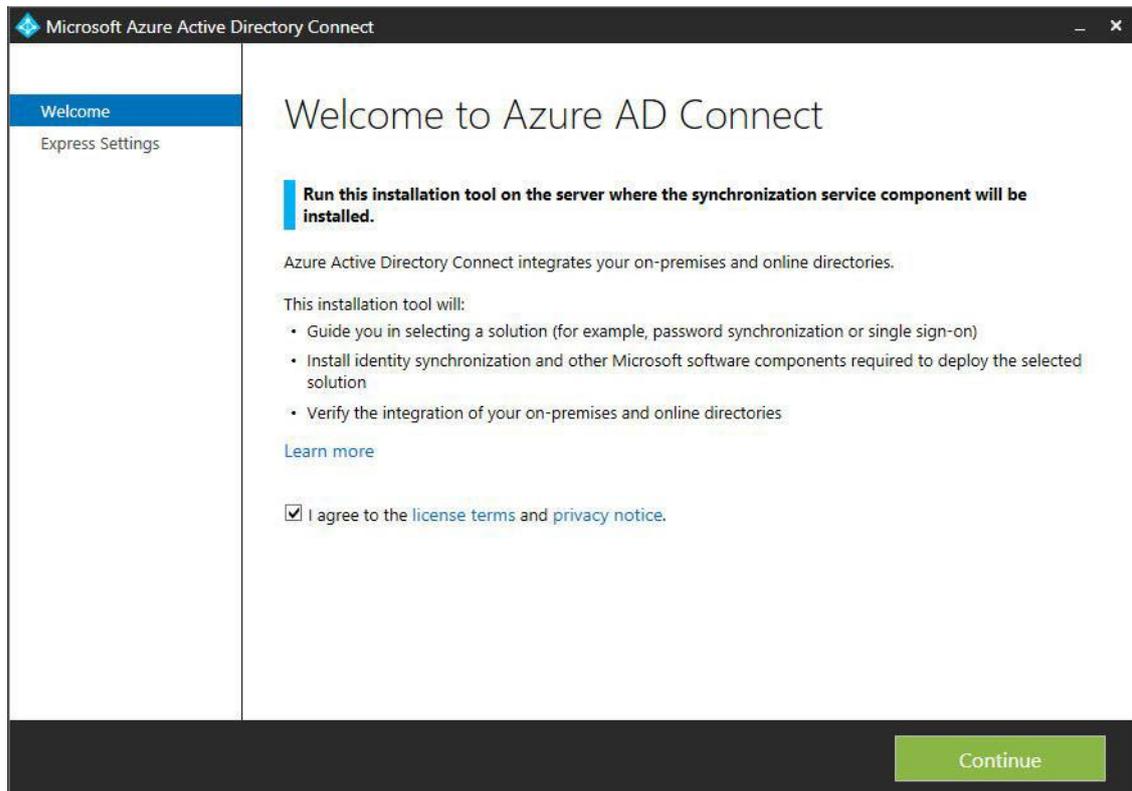
- 1 Усовершенствуйте возможности входа для пользователей**
Добавьте пользовательский домен, чтобы пользователи могли войти, используя существующие имена пользователей. Например, если ваша организация владеет доменом "contoso.com", пользователи могут войти в Azure AD по таким именам пользователей, как "joe@contoso.com".
[Добавить домен](#)
- 2 Интеграция с локальным каталогом**
Используйте в облаке существующие локальные учетные записи и группы.
[Загрузить Azure AD Connect](#)
- 3 Приобретение Azure AD Premium**
Усовершенствуйте возможности управления для конечных пользователей и администраторов, включая пароля, управление группами, настройку входа и отчеты.
[Попробовать](#)

ИЗУЧЕНИЕ

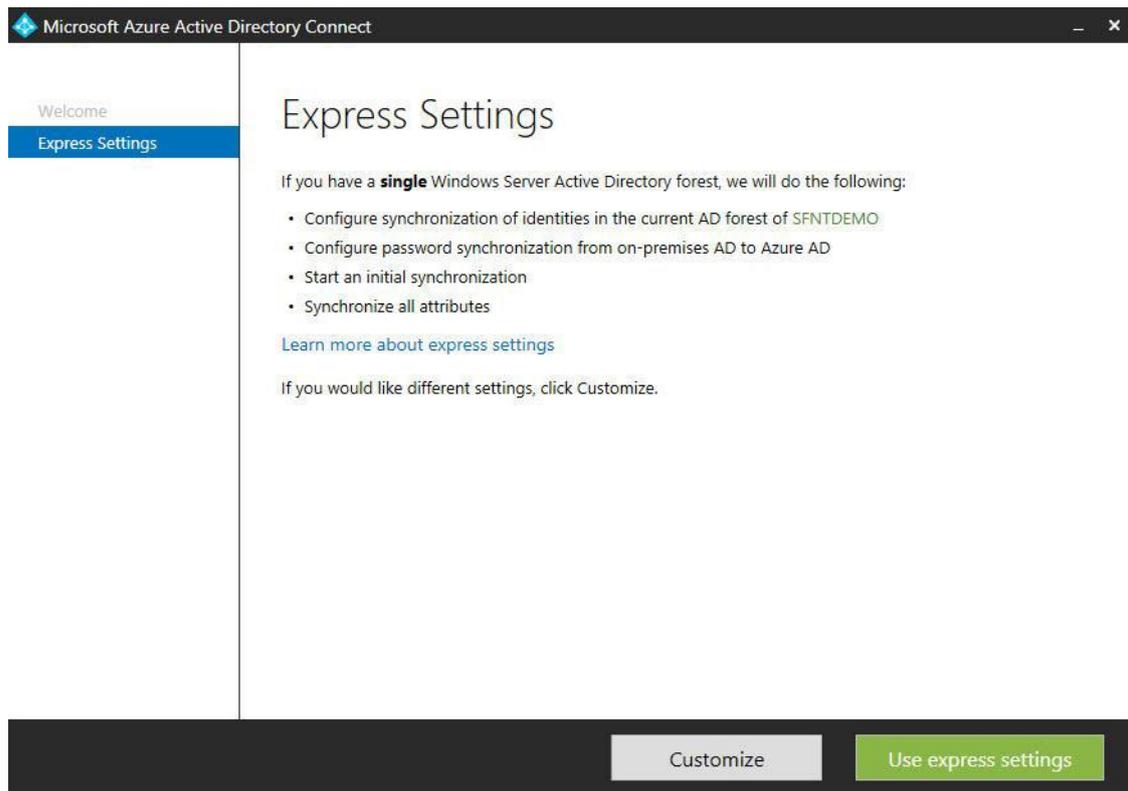
- [Добавить пользователя](#)
- [Добавить приложение](#)
- [Предварительная версия: Azure AD на новом портале Azure](#)
- [Войти в приложение](#)
- [Найти используемые облачные приложения](#)

СВЕДЕНИЯ

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.

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure

Connect to Azure AD

Enter your Azure AD credentials: ?

USERNAME
[blurred email address]

PASSWORD
[masked password]

Previous Next

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

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure

Connect to AD DS

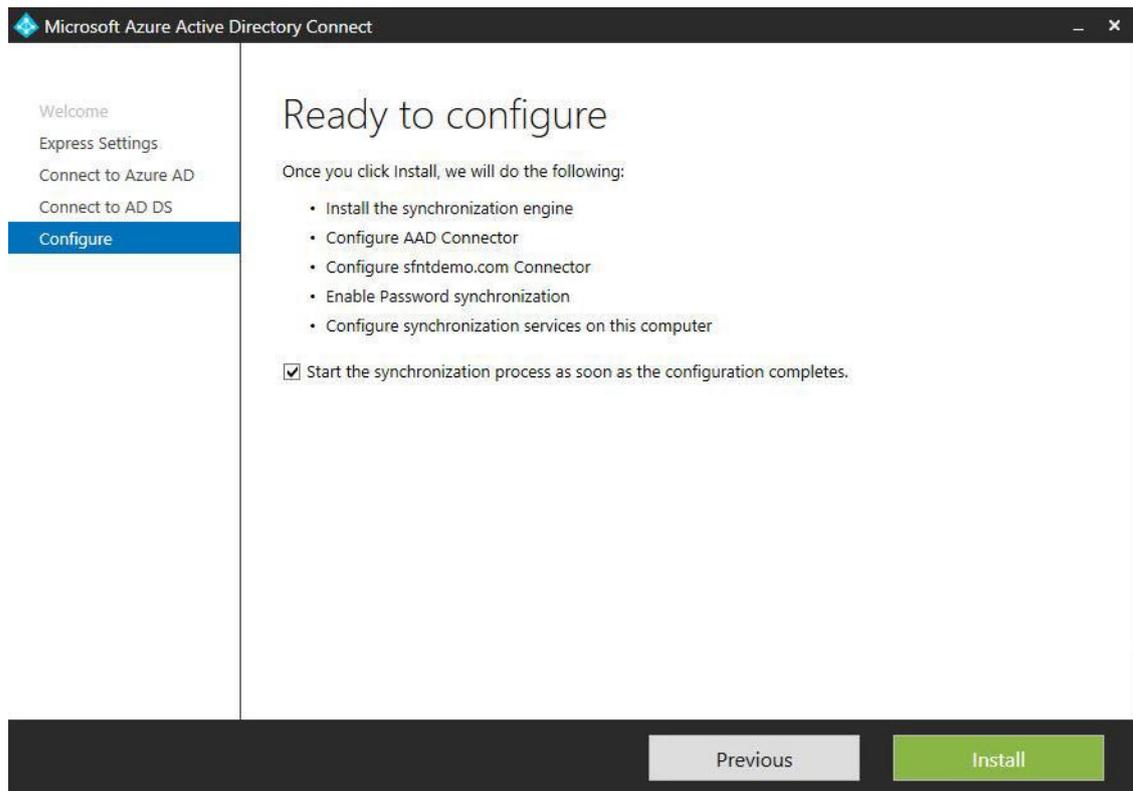
Enter the Active Directory Domain Services enterprise administrator credentials: ?

USERNAME

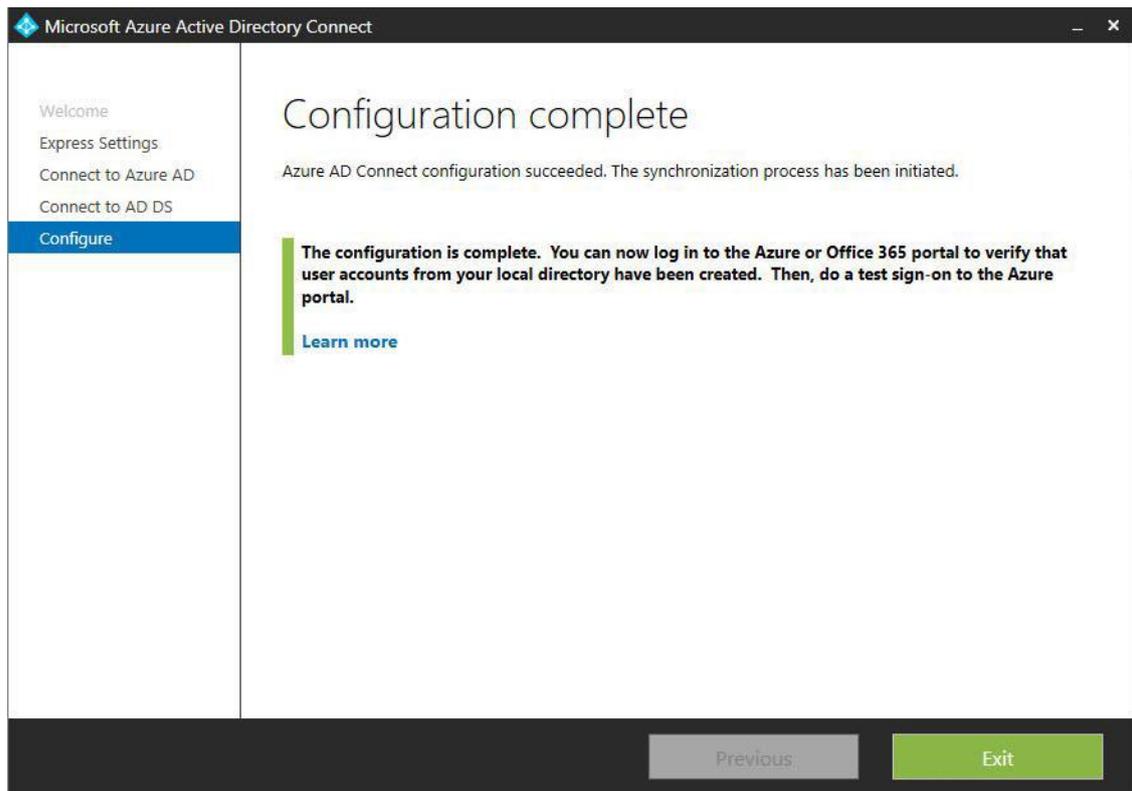
PASSWORD

Previous Next

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.

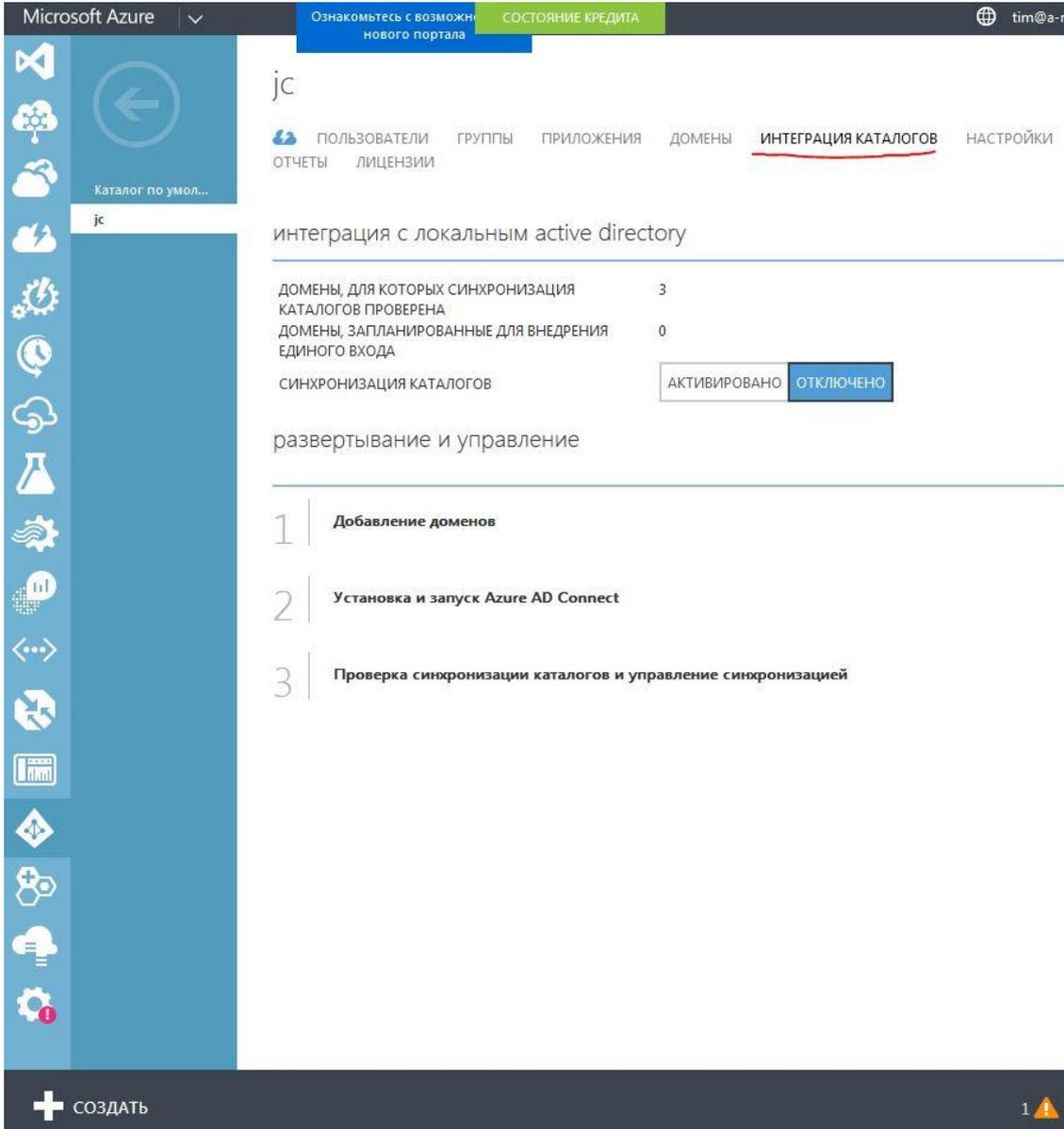
1. Залогиньтесь на портал Azure.
2. В левой панели нажмите Active Directory, затем в правой панели выберите Вашу директорию.

active directory

КАТАЛОГ ПРОСТРАНСТВА ИМЕН КОНТРОЛЯ ДОСТУПА ПОСТАВЩИКИ МНОГОФАКТОРНОЙ ПРОВЕРКИ ПОДЛИННОСТИ RIGHTS MANAGEMENT

ИМЯ	СОСТОЯНИЕ	РОЛЬ	ПОДПИСКА	РАСПОЛОЖЕНИЕ	СТРАНА ИЛИ РЕГИ...
Каталог по умолчанию	Активно	Глобальный администр...	Общие для всех подпис...	ЦОД соответствующие ...	Россия
Ис	Активно	Глобальный администр...	Общие для всех подпис...	ЦОД соответствующие ...	Россия

3. Нажмите вкладку Интеграция каталогов.



The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with 'Microsoft Azure' and a dropdown arrow, a blue button 'Ознакомьтесь с возможностями нового портала', a green button 'СОСТОЯНИЕ КРЕДИТА', and a user profile 'tim@...'. Below this is a left-hand navigation pane with various icons and a search bar containing 'jc'. The main content area is titled 'jc' and has a sub-header 'интеграция с локальным active directory'. There are several tabs: 'ПОЛЬЗОВАТЕЛИ', 'ГРУППЫ', 'ПРИЛОЖЕНИЯ', 'ДОМЕНЫ', 'ИНТЕГРАЦИЯ КАТАЛОГОВ' (which is underlined in red), and 'НАСТРОЙКИ'. Below the tabs, there are statistics: 'ДОМЕНЫ, ДЛЯ КОТОРЫХ СИНХРОНИЗАЦИЯ КАТАЛОГОВ ПРОВЕРЕНА' with a value of 3, and 'ДОМЕНЫ, ЗАПЛАНИРОВАННЫЕ ДЛЯ ВНЕДРЕНИЯ ЕДИНОГО ВХОДА' with a value of 0. There are two buttons: 'АКТИВИРОВАНО' and 'ОТКЛЮЧЕНО'. Below this is a section 'развертывание и управление' with a numbered list of steps: 1. 'Добавление доменов', 2. 'Установка и запуск Azure AD Connect', and 3. 'Проверка синхронизации каталогов и управление синхронизацией'. At the bottom left is a '+ СОЗДАТЬ' button, and at the bottom right is a notification icon with the number '1'.

Под Синхронизацией каталогов будет указано время последней синхронизации.

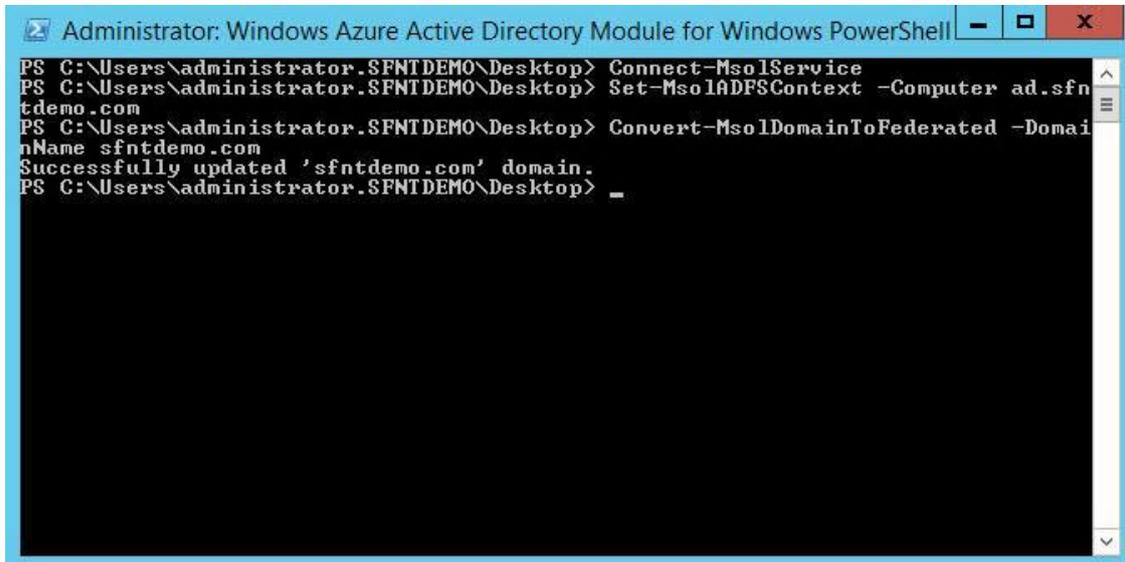
Настройка Azure AD FS

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.

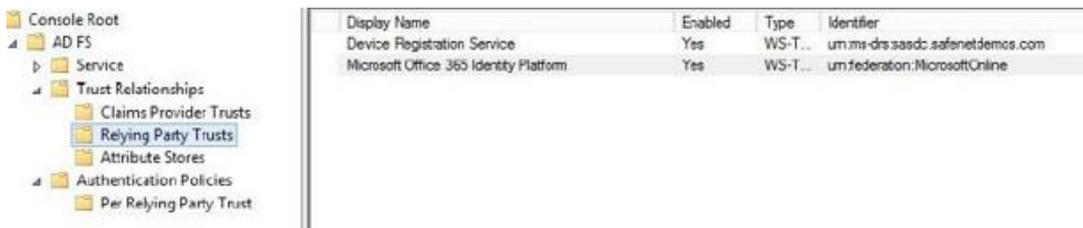


```
Administrator: Windows Azure Active Directory Module for Windows PowerShell
PS C:\Users\administrator.SFNTDEMO\Desktop> Connect-MsolService
PS C:\Users\administrator.SFNTDEMO\Desktop> Set-MsolADFSContext -Computer ad.sfn
tdemo.com
PS C:\Users\administrator.SFNTDEMO\Desktop> Convert-MsolDomainToFederated -Domain
Name sfntdemo.com
Successfully updated 'sfntdemo.com' domain.
PS C:\Users\administrator.SFNTDEMO\Desktop> _
```

6. Откройте консоль AD FS Management.

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

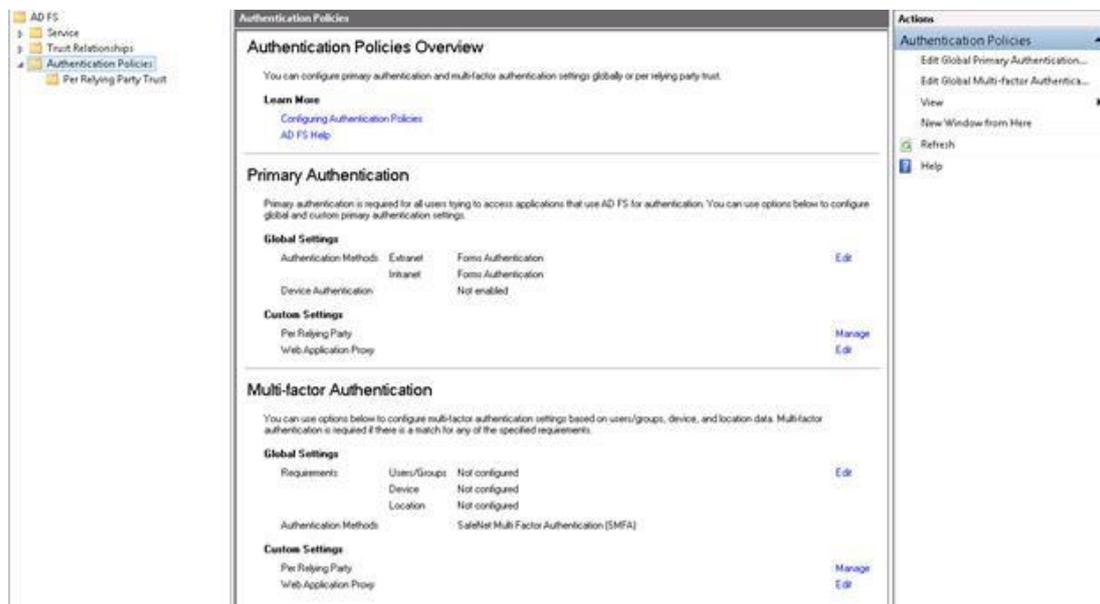
В правой панели Microsoft Office 365 Identity Platform должно отображаться как доверенная.



Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	um.ms-drs.sasdc.safenetdemos.com
Microsoft Office 365 Identity Platform	Yes	WS-T...	um.federation:MicrosoftOnline

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.



The screenshot shows the 'Edit Global Authentication Policy' window with two tabs: 'Primary' and 'Multi-factor'. The 'Primary' tab is active. Below the tabs, there is instructional text: 'Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in. If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.'

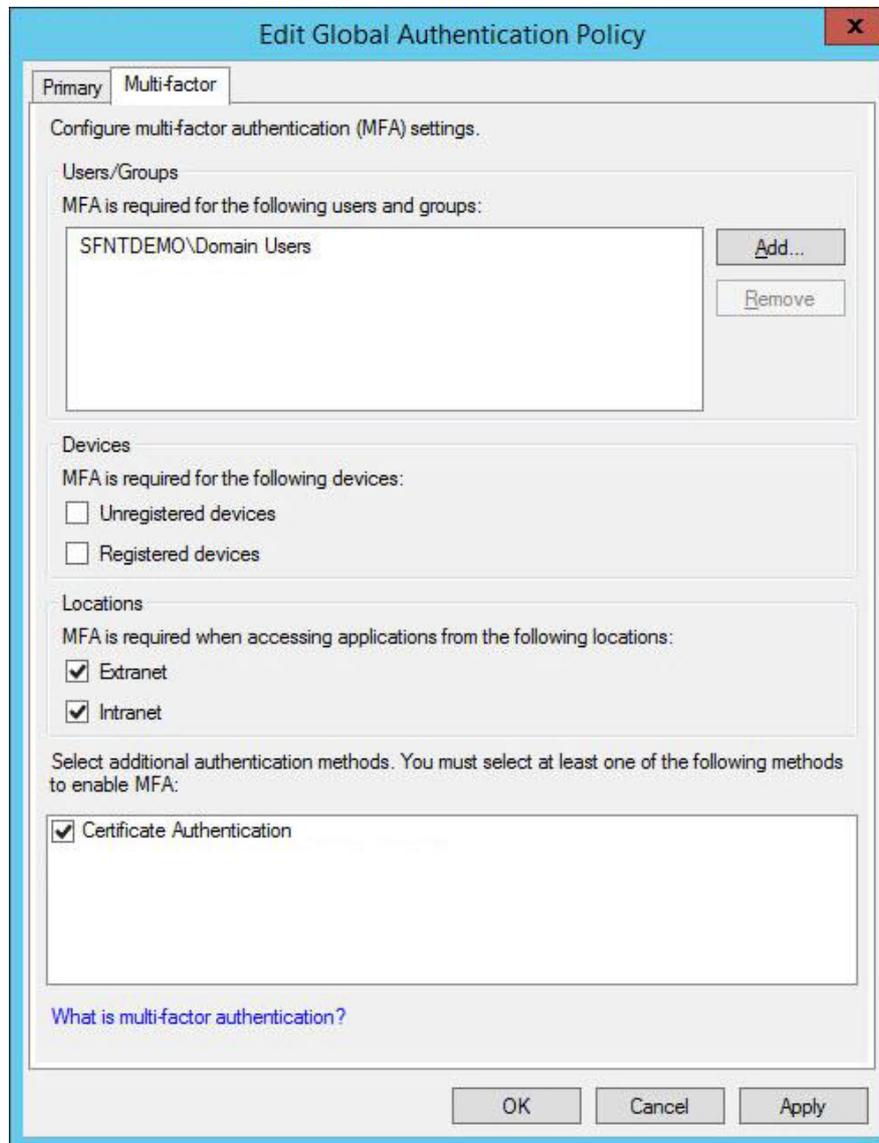
The window is divided into two sections: 'Extranet' and 'Intranet'. Each section contains a list of authentication methods with checkboxes:

- Extranet:**
 - Forms Authentication
 - Certificate Authentication
- Intranet:**
 - Forms Authentication
 - Windows Authentication
 - Certificate Authentication

 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 ОК.



The screenshot shows the 'Edit Global Authentication Policy' dialog box with the 'Multi-factor' tab selected. The dialog is titled 'Edit Global Authentication Policy' and has a close button (X) in the top right corner. It contains the following sections:

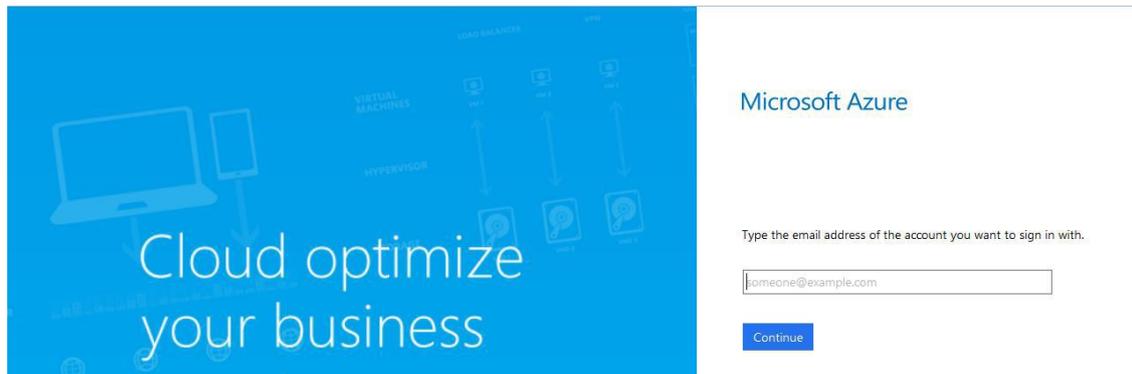
- Primary** (selected) | **Multi-factor**
- Configure multi-factor authentication (MFA) settings.
- Users/Groups**
MFA is required for the following users and groups:
SFNTDEMO\Domain Users
Buttons: Add..., Remove
- Devices**
MFA is required for the following devices:
 Unregistered devices
 Registered devices
- Locations**
MFA is required when accessing applications from the following locations:
 Extranet
 Intranet
- Select additional authentication methods. You must select at least one of the following methods to enable MFA:
 Certificate Authentication
- [What is multi-factor authentication?](#)
- Buttons: OK, Cancel, Apply

Запуск Решения

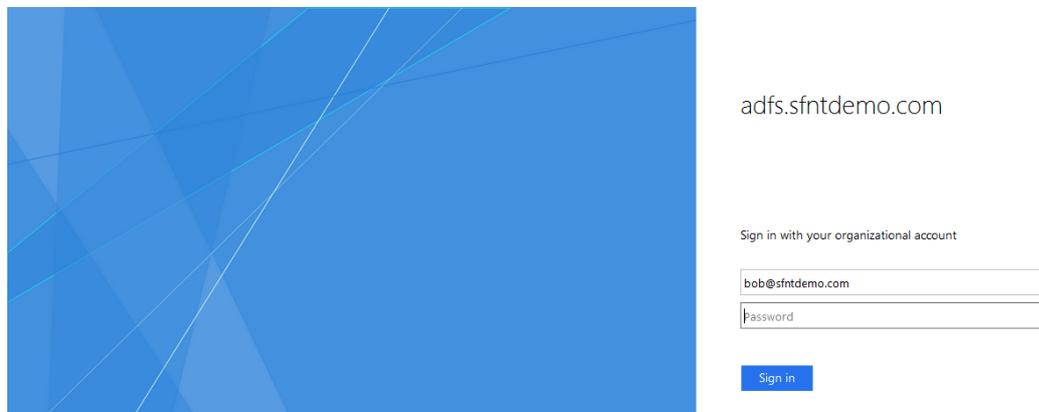
1. В Web-браузере откройте страницу:

<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.

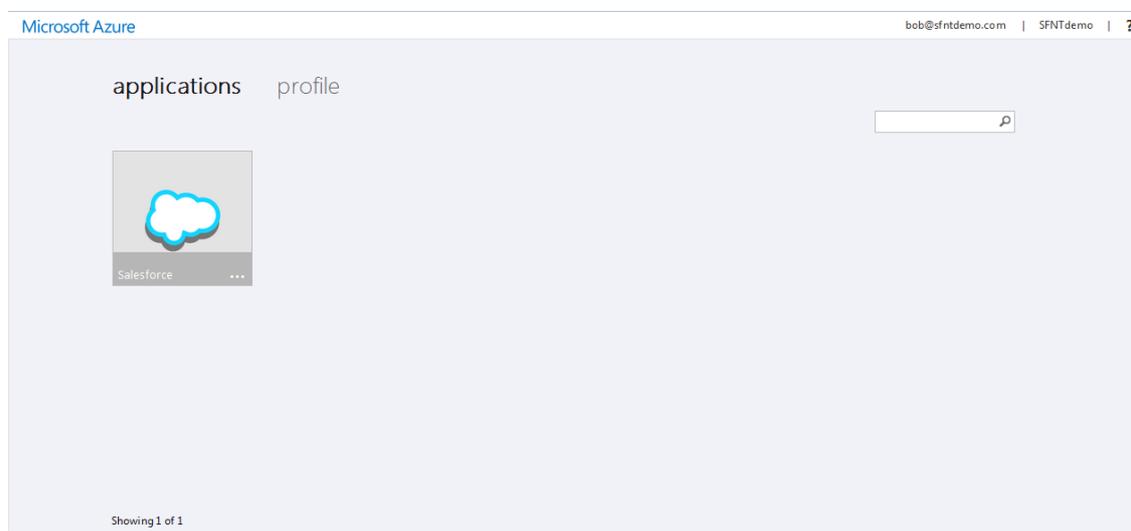


3. Браузер отобразит все доступные на машине сертификаты. Выберите сертификат, требуемый для входа.
4. Нажмите ОК.



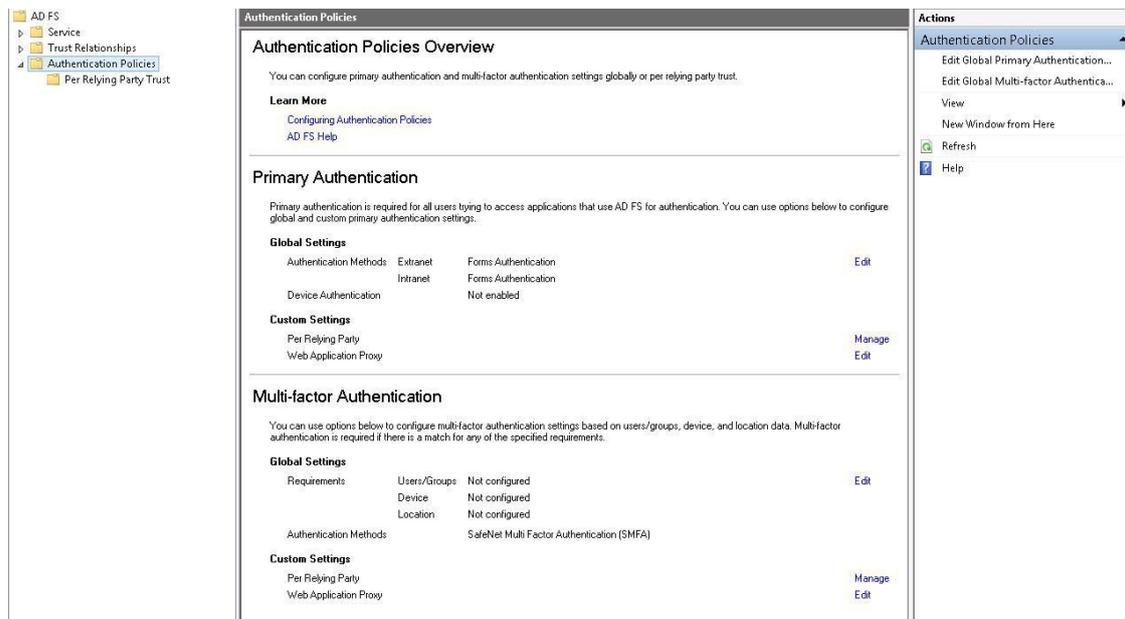
5. В окне ввода PIN-кода токена введите Ваш PIN-код.

После успешной аутентификации Вы будете перенаправлены в панель доступа Azure Access Panel. Теперь Вы можете использовать приложения без какой-либо дополнительной аутентификации.

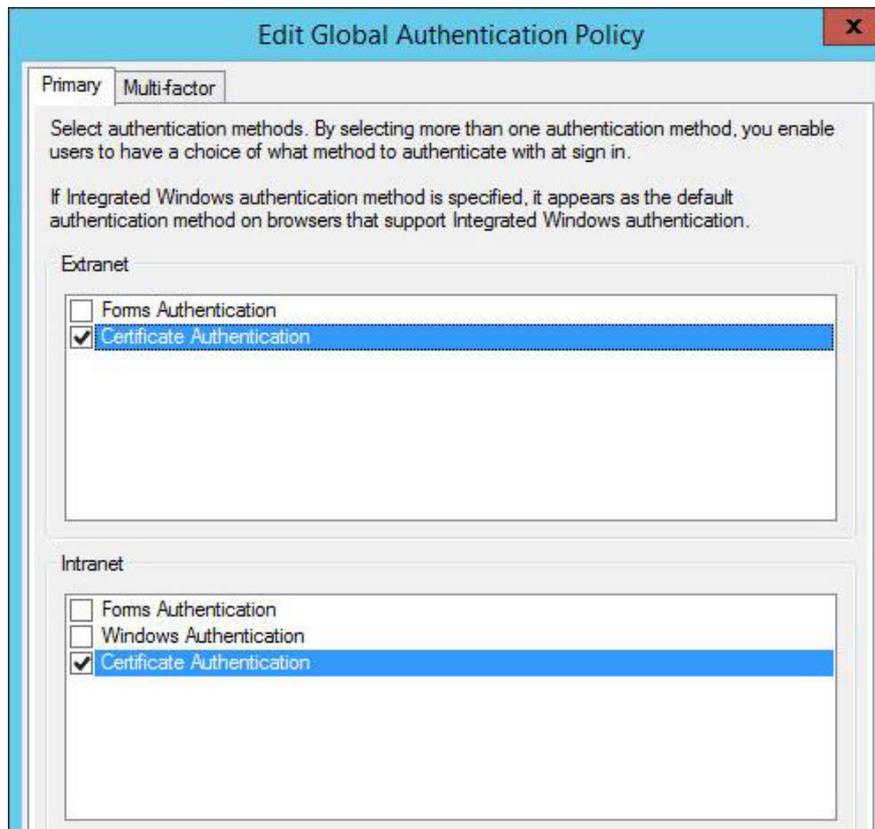


Дополнение: Настройка AD FS для аутентификации по сертификатам SSO

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.



The screenshot shows the 'Edit Global Authentication Policy' window with the 'Primary' tab selected. The window title is 'Edit Global Authentication Policy' with a close button (X) in the top right corner. Below the tabs, there is a text block: 'Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in. If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.'

Under the 'Extranet' section, there is a list of authentication methods:

- Forms Authentication
- Certificate Authentication

Under the 'Intranet' section, there is a list of authentication methods:

- Forms Authentication
- Windows Authentication
- Certificate Authentication

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

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.

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