3DEXPERIENCE Platform 2020x Installation guide

review v1 / 10.10.2019

Apache & SSL

Sergey SHEBARSHOV
Infrastructure Consultant
Sergey.SHEBARSHOV.intern@3ds.com

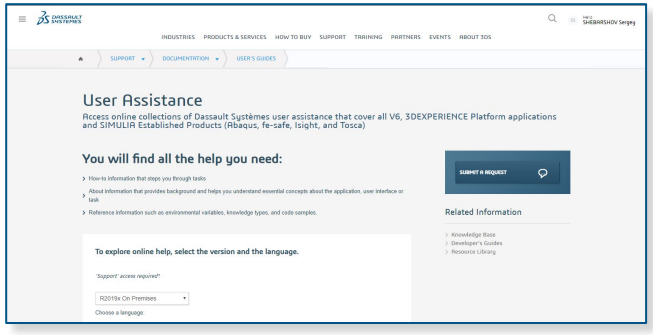
3DEXPERIENCE®

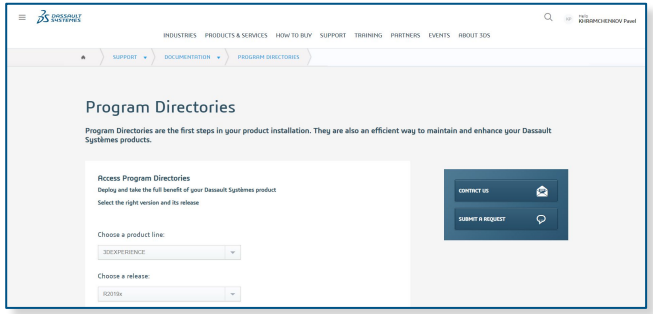
DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

Общие положения

Допущения и ограничения

- Данный материал представляет собой описание процесса установки **3D**EXPERIENCE Platform 2020x*
- Данный материал был подготовлен на основе следующих источников:
  - **User Assistance** – официальной документации по продуктам Dassault Systémes (см. раздел **Installation and Setup | Install |** **3D**EXPERIENCE Platform и др.) https://www.3ds.com/support/documentation/users-guides/
  - **Program Directory** – содержит описание требований к Аппаратной и Программной части инфраструктуры **3D**EXPERIENCE Platform, список закрыты и закрытых исправлений, обзор новых функций продуктов и т.д. https://www.3ds.com/support/documentation/program-directories/
  - **Best Practices** – официальные лучше практики по установке и апгрейду **3D**EXPERIENCE Platform https://www.3ds.com/support/documentation/best-practices/
- Данный материал является справочным, может содержать ошибки и не является прямой инструкцией по применению при апгрейде **3D**EXPERIENCE Platform, развернутой у заказчика
- Процедура апгрейда **3D**EXPERIENCE Platform, описанная в данном документе, была отработана на тестовой среде





* Может рассматриваться, как обучающий материал только совместно с самостоятельным глубоким изучением официальных источников информации (документация, курсы 3DS, Community, Blogs, DS White Papers/Best Practices)

Общие положения

Допущения и ограничения

- Апгрейд и установка компонентов **3D**EXPERIENCE Platform в соответствии с данным материалом подходит как для Физических Машин, так и для Виртуальных: протестировано для VMWare ESXi (6.0.2, 6.5.0, 6.7.0)
- Для простоты выполнения процедуры апгрейда и последующего администрирования серверной инфраструктуры **3D**EXPERIENCE Platform, рекомендуется выполнять все действия на виртуальной машине в среде гипервизора VMWare ESXi или Microsoft Hyper-V
- Апгрейд и установка всех компонентов **3D**EXPERIENCE Platform и любого другого ПО производится из под встроенного аккаунта Administrator (имя пользователя должно быть на латинице)
- Запуск любых установщиков, ярлыков, командной строки CMD осуществляется с помощью “Run as Administrator” через контекстное меню
- Пакетные *.bat файлы рекомендуется запускать из командной строки CMD

Конечные точки сервисов

- ”Конечная точка сервиса” - это URL, по которому доступна ваша служба/сервис для клиентских приложений
  - Состоит из базового URL и имени конечной точки службы/сервиса
- Для каждой службы Платформы 3DEXPERIENCE должны быть определены и зарезервированы конечные точки сервисов прежде, чем вы перейдете к процессу установки
- Пример:
  - `platform.3ds.ru/3dspace`
  - `platform.3ds.ru/3dpassport`
  - `platform.3ds.ru/3ddashboard`
  - `untrusted.3ds.ru`
  - `platform.3ds.ru/3dswym`

Для тестового сервера, который не доступен извне, это могут быть записи в файле “hosts”

Пример URL для доступа к сервису Платформы 3DSpace (только с использованием HTTPS):

См. базовый URL и имена конечных точек сервисов Платформы на следующем слайде

Конечные точки сервисов

Внесение изменений в файл “hosts” на виртуальной машине

- В рамках мастер-класса, используем единый URL для всех конечных точек сервисов платформы:

  `https://r422-ifwe.3dx.ds/3dspace`

  `https://r422-ifwe.3dx.ds/3dpassport`

  И т. д.

- Откройте файл “hosts”, расположенный по следующему пути `C:\Windows\Systems32\drivers\etc`
  - Чтобы внести изменения в этот файл, его необходимо открыть как Администратор, например, с помощью Notepad++
- Добавить следующие строки в конце файла, указав IP-адрес вашей виртуальной машины, а так же FQDN сервера Платформы:

  ```
  192.168.36.14  r422-ifwe.3dx.ds
  192.168.36.14  untrusted.3dx.ds
  ```

- **Сохраните изменения!**
- Проверьте доступность “r422-ifwe.3dx.ds” и “untrusted.3dx.ds” с помощью команды ping

Установка сервера Apache HTTPD

Введение

- Для работы платформы необходим **Apache Haus** версии 2
  - https://www.apachehaus.com
- В мастер-классе используется дистрибутив (есть в комплекте ПО к мастер-классу)
  - httpd-2.4.38-o110j-x64-vc14.zip
  - Для корректной работы необходим VC++ 2015 (vcredist_x86 и vcredist_x64 есть в комплекте ПО к мастер-классу)
- Распаковать архив и скопировать папку Apache24 в корень диска C:\
  - C:\Apache24
- Проверить свободен ли 80 порт (порт Apache по умолчанию) с помощью команды из командной строки:
  - netstat –a –b | find “80” или с помощью утилиты
- Если 80 порт занят, изменить ”Listen 80” на ”Listen 81” конфигурационном файле Apache, который расположен по следующему пу
  - C:\Apache24\conf\httpd.conf

Всегда проверяйте соответствие используемой версии Apache официальным требованиям с помощью Program Directory, раздел Servers H/W & S/W Requirements

Для проверки портов можно использовать утилиту “CurrPorts” от Nirsoft: http://www.nirsoft.net/utils/cports.html

Структура папок сервера Apache HTTPD

Важные папки и файлы

Если вы вносите изменения в настроечные файлы, структуру папок, добавляете новые файлы, то необходимо перезапустить службу Apache, для того, чтобы изменения вступили в силу

Apache24/…

…bin/

httpd.exe - Основной бинарный исполняемый файл

…conf/ - Все файлы настроек находятся здесь и в подпапках

ssl/ - Все SLL-связанные файлы, такие как приватные ключи и сертификаты

vhosts/ - Дополнительные конфигурационные файлы, которые вызываются из основного файла настроек httpd.conf

httpd.conf - Основной файл настроек Apache

…logs/ - Файлы Журналов

…modules/ - Модули, обеспечивающие дополнительную функциональность (например, SSL), активируются в файле настроек httpd.conf

Установка сервера Apache HTTPD

- С привилегиями администратора из командной строки CMD выполните следующие команды для того, чтобы зарегистрировать Apache в качестве службы Windows:

```
C:\Apache24\bin\httpd.exe -k install
C:\Apache24\bin\httpd.exe -k restart
```

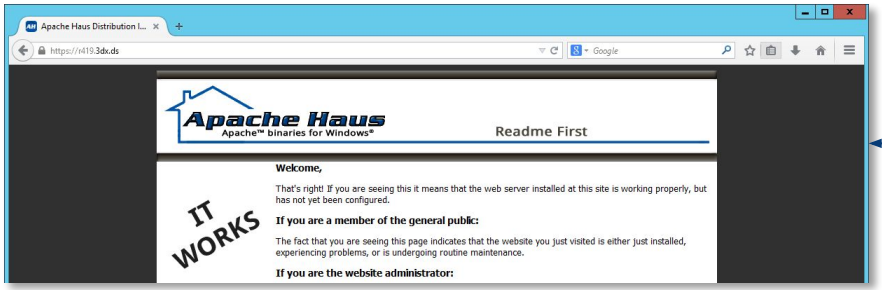
- Убедитесь, что у вас есть доступ к стартовой странице Apache:
  - http://r422-ifwe.3dx.ds

  или, если 81 порт занят
  - http://r422-ifwe.3dx.ds:81

Возможно появление ошибки ”MSVCR110.dll” / ”VCRUNTIME140.dll” при выполнении команды install. Для ее устранения необходимо скачать и установить библиотеки ”Microsoft Visual C++ Redistributable” с сайта Microsoft (есть в комплекте ПО к мастер-классу)

Ссылка на скачивание VC++ 2012 Update 4 (x64): https://www.microsoft.com/en-us/download/details.aspx?id=30679

Если эта страница отображается, то это означает, что служба запущена, а сервер Apache HTTPD работает корректно



DASSAULT SYSTEMES

Первичная настройка сервера Apache HTTPD

- Отредактируйте файл **httpd.conf** в папке C:\Apache24\co
  - Разблокируйте следующие модули для того, чтобы активировать

```
99> LoadModule cache_module modules/mod_cache.so
100> LoadModule cache_disk_module modules/mod_cache_disk.so
110> LoadModule deflate_module modules/mod_deflate.so
117> LoadModule filter_module modules/mod_filter.so
118> LoadModule headers_module modules/mod_headers.so
142> LoadModule proxy_module modules/mod_proxy.so
150> LoadModule proxy_http_module modules/mod_proxy_http.so
154> LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
160> LoadModule rewrite_module modules/mod_rewrite.so
168> LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
173> LoadModule ssl_module modules/mod_ssl.so
```

  - Заблокируйте следующие строки, для того чтобы деактивировать загрузку SSL конфигурации по умолчанию (строки находятся в конце файла httpd.conf):

```
523> #Include conf/extra/httpd-ssl.conf
524> #Include conf/extra/httpd-ahssl.conf
```

Всегда сверяйтесь с Program Directory на предмет полного необходимого перечня активных модулей Apache для корректной работы 3DEXPERIENCE Platform

Первичная настройка сервера Apache HTTPD

- В `C:\Apache24\conf` будем использовать существующую папку `ssl`:
  - Удалите все файлы шаблонов в `C:\Apache24\conf\ssl`
  - Эта папка будет использована для хранения файлов ключей (.key) и сертификатов (.crt)
- В `C:\Apache24\conf` создайте папку `vhosts`:
  - `C:\Apache24\conf\vhosts`
  - Эта папка будет использоваться для хранения файлов настроек (.conf) конфигурации обратного прокси (reverse proxy)

Порты TomEE и HTTPS

Резервирование уникальных портов для TomEE:

Сервис	порт TomEE	HTTPS	Конечная точка сервиса
3DPassport	8080	443	ru2-ifwe.3dx.ds/3dpassport
3DSpace с CAS	8090	443	ru2-ifwe.3dx.ds/3dspace
3DDashboard	9000	443	ru2-ifwe.3dx.ds/3ddashboard
3DSearch	9010	443	ru2-ifwe.3dx.ds/federated
3DSwym	9020	443	ru2-ifwe.3dx.ds/3dswym
3DComment	9030	443	ru2-ifwe.3dx.ds/3dcomment
3DNotification	9040 [1]	443	ru2-ifwe.3dx.ds/3dnotification
3DDashboard untrusted	N/A	443	untrusted.3dx.ds
3DSpace без CAS	8070 [2]	-	ru2-ifwe.3dx.ds:8070/nocas [3]
3DOrchestrate [4]	8060	443	ru2-ifwe.3dx.ds/3dorchestrate

1) Порт для NodeJS демона

2) Порт 8070 для No CAS TomEE нельзя изменить в процессе установки

3) Запрещено в качестве пользователя напрямую обращаться по порту 8070 к службе 3DSpace, используйте только CAS авторизацию

4) Зарезервировано для 3DOrchestrate, установка этого сервиса не входит в рамки мастер-класса

Перед началом установки Платформы убедитесь, что предлагаемый к использованию перечень портов свободен и доступен для использования. Используйте специальные инструменты сетевой диагностики или команду `netstat -a -b | find "порт"`

DASSAULT SYSTEMES

Конфигурирование виртуального хоста Apache

Файл настроек виртуальных хостов Apache для Платформы 3DX

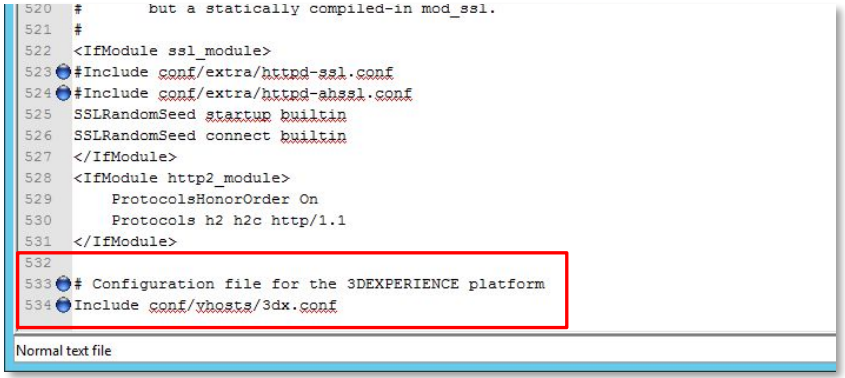
- Шаблон файла настроек Apache есть в комплекте документации к мастер-классу:
  - `3dx.conf`
- Скопируйте файл 3dx.conf в папку `C:\Apache24\conf\vhosts`

Конфигурирование виртуального хоста Apache

Изменение основного файла настроек Apache HTTPD

- Добавьте следующие строки в файл `C:\Apache24\conf\httpd.conf`

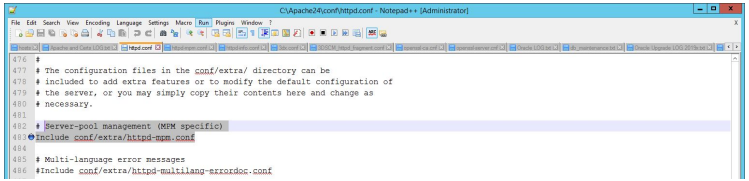
```
# Configuration file for the 3DEXPERIENCE platform
Include conf/vhosts/3dx.conf
```

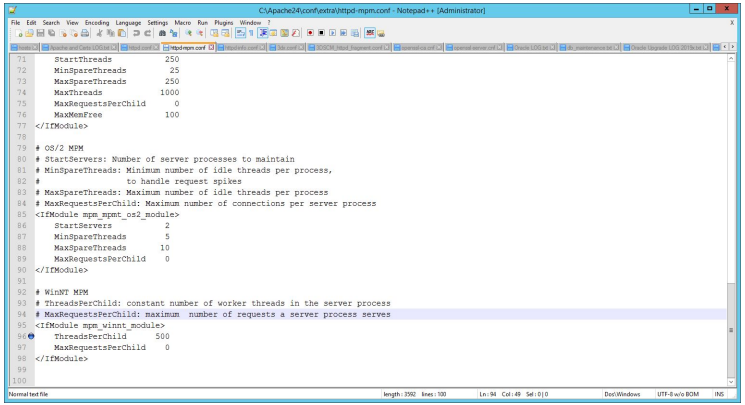


Конфигурирование виртуального хоста Apache

Изменение основного файла настроек Apache HTTPD

- Подключите файл настроек для Server-pool management (MPM specific) в `C:\Apache24\conf\vhosts\httpd.conf` :
  - `Include conf/extra/httpd-mpm.conf`
- В файле `C:\Apache24\conf\extra\httpd-mpm.conf` отредактируйте параметр ThreadsPerChild, увеличив исходное значение:
  - `<IfModule mpm_winnt_module>`
  - `    ThreadsPerChild      500`
  - `    MaxRequestsPerChild    0`
  - `</IfModule>`

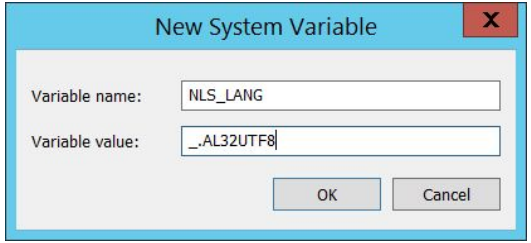


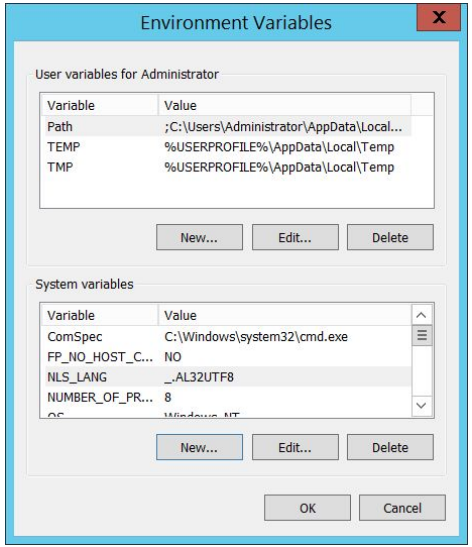


Конфигурирование виртуального хоста Apache

Настройка переменной среды для правильной работы сервисов

- Установить переменную среды Windows:
  - `NLS_LANG=_.AL32UTF8`
  - Данный параметр необходим для корректной работы служб 3DEXPERIENCE Platform в пакетном режиме с данными в Unicode (например, синхронизации учетных записей пользователей 3DPassport с русскими данными типа Имени и Фамилии с остальными сервисами Платформы)





Конфигурирование виртуального хоста Apache

Перезапуск службы Apache

- После внесения изменений в любые настройки Apache, необходимо перезапустить соответствующую службу
- Перезапустить службу можно через диспетчер служб (Services.msc) или вручную (рекомендуется использовать этот способ) с помощью соответствующей команды из командной строки:
  - `C:\Apache24\bin\httpd.exe -k restart`
- Результатом перезапуска службы будет ошибка:

```
AH00526: Syntax error on line 29 of c:/Apache24/conf/vhosts/3dx.conf:
SSLCertificateFile: file 'c:/Apache24/conf/ssl/servercert.crt' does not exist or
is empty
```

- Это ожидаемый результат, поскольку мы еще не создали SSL сертификаты, которые указаны в файле 3dx.conf (ранее мы подключили его загрузку через основной файл настроек httpd.conf), поэтому текущая конфигурация с точки зрения SSL является неработоспособной
- Теперь необходимо перейти к созданию SSL сертификатов

SSL сертификаты

Краткий перечень шагов по созданию самоподписных сертификатов

- Создание CA сертификата (создание собственного CA, **Certificate Authority**)
- Создание серверного сертификата для FQDN “r422-ifwe.3dx.ds” and “untrusted.3dx.ds”
  - Этот серверный сертификат будет **подписан** созданным нами CA
- Импорт CA сертификата в ОС на сервере и клиентских машинах
  - Импорт в “Trusted Root Certificate Authority”
  - Все сертификаты, подписанные созданным нами CA, будут автоматически рассматриваться как надежные

Дополнительная информация о обратном прокси и сертификатах находится в презентации:
“2 – Введение – Мастер-класс по Установке 3DX R2020x FD01.pptx”

Необходимо обязательно использовать “Subject Alternate Name” при создании сертификатов, чтобы обеспечить их работоспособность с последними версиями web-браузеров

SSL сертификаты

OpenSSL - введение

- OpenSSL - криптографический пакет с открытым исходным кодом для работы с SSL/TLS. Позволяет создавать ключи RSA, DH, DSA и сертификаты X.509, подписывать их, формировать CSR и CRT. Также имеется возможность шифрования данных и тестирования SSL/TLS соединений.
- В сетевом окружении библиотеки программного обеспечения OpenSSL используются в приложениях, которые должны обеспечивать надежную связь и защиту от перехвата данных или должны установить личность контрагента. OpenSSL нашел широкое применение в интернет-серверах, обслуживающих большинство веб-сайтов
- Основная библиотека, написанная на языке программирования C, реализует основные криптографические функции и предоставляет различные служебные функции. Благодаря обёртке системного вызова (враппер), возможно использовать библиотеку OpenSSL в различных компьютерных языках программирования
- Доступна для большинства UNIX-подобных операционных систем (включая Solaris/OpenSolaris, Linux, Mac OS X, QNX4, QNX6 и четырёх операционных систем BSD с открытым исходным кодом), а также для OpenVMS и Microsoft Windows.

SSL сертификаты

Подготовительные шаги

- Сертификаты создаются с помощью инструмента OpenSSL из комплекта Apache, который расположен по следующему пути:
  - `C:\Apache24\bin\openssl.exe`
- Скопируйте файлы openssl-ca.cnf и openssl-server.cnf в папку `C:\Apache24\conf`
  - Данные файлы есть в комплекте документации к мастер-классу
- Создайте папку с именем 2019x для установки Платформы:
  - `C:\R2020x\`
- Создайте папку для хранения файла CA сертификата:

  `C:\R2020x\cadata`
- В папке “cadata” создайте два файла:
  - Пустой текстовый файл с именем “index.txt”
  - Текстовый файл с именем “serial.txt” с содержимым “01” без кавычек

SSL сертификаты

OpenSSL – файлы с настройками

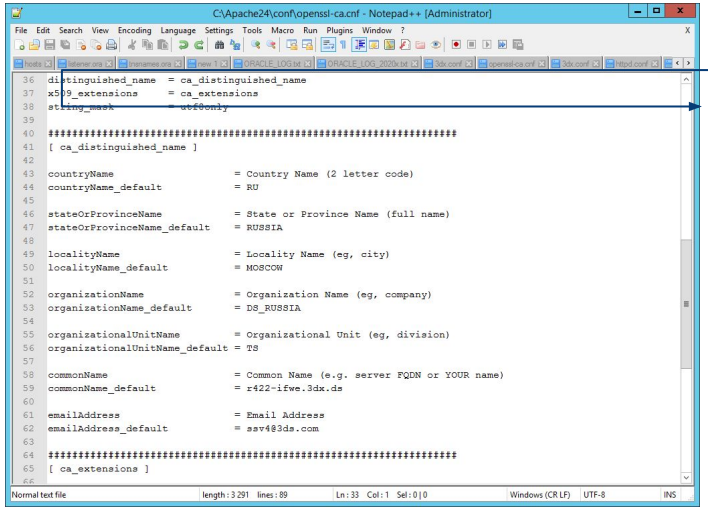
- В папке `C:\Apache24\conf` используем два файла-шаблона с настройками для создания сертификатов:
  - **openssl-ca.cnf**
  - **openssl-server.cnf**
- URL'ы для сертификатов сервера Платформы задаются в файле openssl-server.cnf:

```
[ alternate_names ]

DNS.1    = r422-ifwe.3dx.ds       # URL для сервера 3DEXPERIENCE

DNS.2    = untrusted.3dx.ds       # URL для неподписанных виджетов
   (виджетов собственной разработки)
```

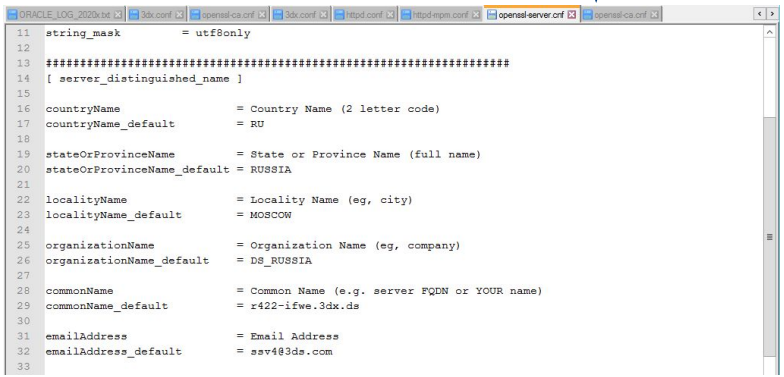
SSL сертификаты

Подготовительные шаги

- Редактируйте файлы настроек openssl-ca.cnf и openssl-server.cnf в папке `C:\Apache24\conf` со своими параметрами:



В файл **openssl-ca.cnf** и **openssl-server.cnf** добавьте данные о своей организации.
organizationName – название вашей компании
commonName – имя вашего сертификата




```
certificate       = $base_dir/r422-ifwe_cacert.crt   # The CA certifcate
private_key       = $base_dir/r422-ifwe_cakey.key    # The CA private key
```

SSL сертификаты

CA сертификат и CA приватный ключ

- Откройте командную строку с привилегиями администратора и перейдите в папку C:\R2019x\cadata:

```
cd C:\R2020x\cadata
```

Все команды OpenSSL должны выполняться в контексте этой папки

- Создайте CA сертификат и CA приватный ключ с помощью этой (однострочной) команды:

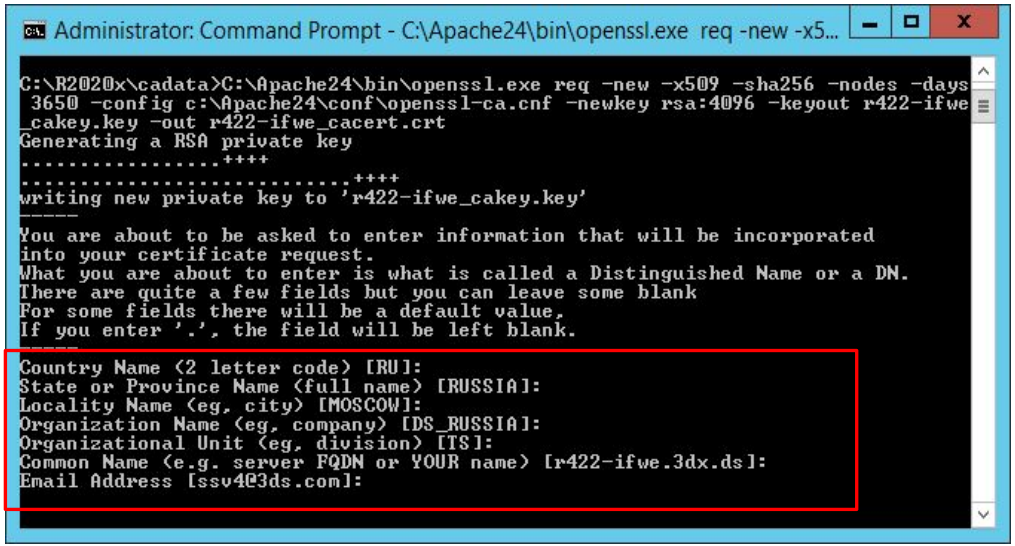
```
C:\Apache24\bin\openssl.exe req -new -x509 -sha256 -nodes -days
3650 -config c:\Apache24\conf\ openssl-ca.cnf -newkey rsa:4096
-keyout r422-ifwe_cakey.key -out r422-ifwe_cacert.crt
```

В результате выполнения команды будут созданы следующие файлы: CA приватный ключ и CA сертификат

SSL сертификаты

CA сертификат и CA приватный ключ

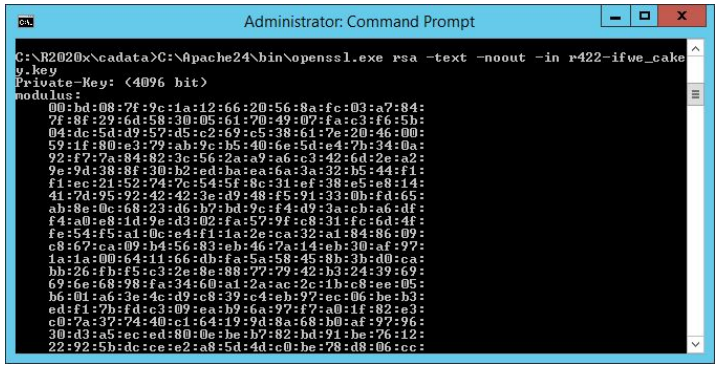
- Нажимайте ENTER для каждого вопроса, чтобы принять значения, заданные в файле настроек openssl-ca.cnf, либо вводите свою информацию:

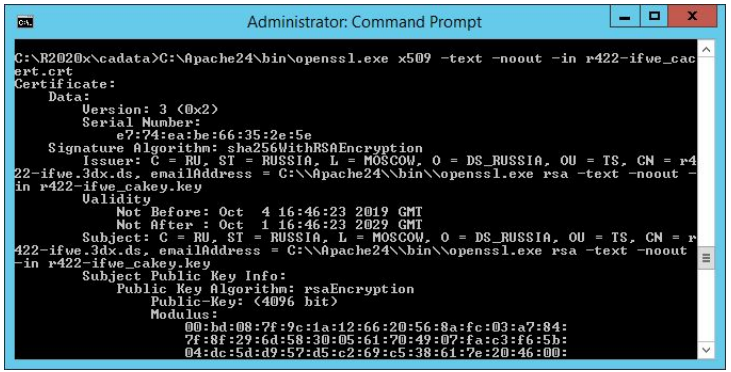


SSL сертификаты

CA сертификат и CA приватный ключ

- Проверьте CA приватный ключ (из командной строки с привилегиями администратора выполните следующую однострочную команду):
  - `C:\Apache24\bin\openssl.exe rsa -text -noout -in r422-ifwe_cakey.key`
- Проверьте CA сертификат (из командной строки с привилегиями администратора выполните следующую однострочную команду):
  - `C:\Apache24\bin\openssl.exe x509 -text -noout -in r422-ifwe_cacert.crt`





SSL сертификаты

Создание запроса на подпись серверного сертификата и приватного ключа

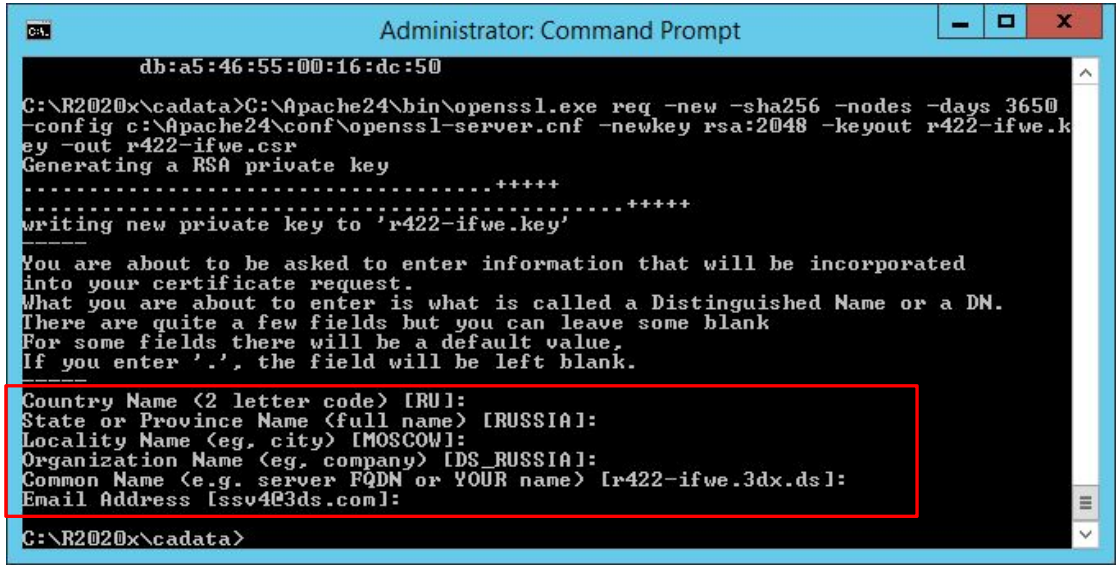
- Откройте командную строку с привилегиями администратора и перейдите в папку C:\R2020x\cadata
  - `cd C:\R2020x\cadata`
- Создание запроса на подпись сертификата и приватного ключа (это однострочная команда):
  - `C:\Apache24\bin\openssl.exe req -new -sha256 -nodes -days 3650 -config c:\Apache24\conf\openssl-server.cnf -newkey rsa:2048 -keyout r422-ifwe.key -out r422-ifwe.csr`

В результате выполнения команды будут созданы следующие файлы: запрос на подпись серверного сертификата и приватный ключ

SSL сертификаты

Создание запроса на подпись серверного сертификата и приватного ключа

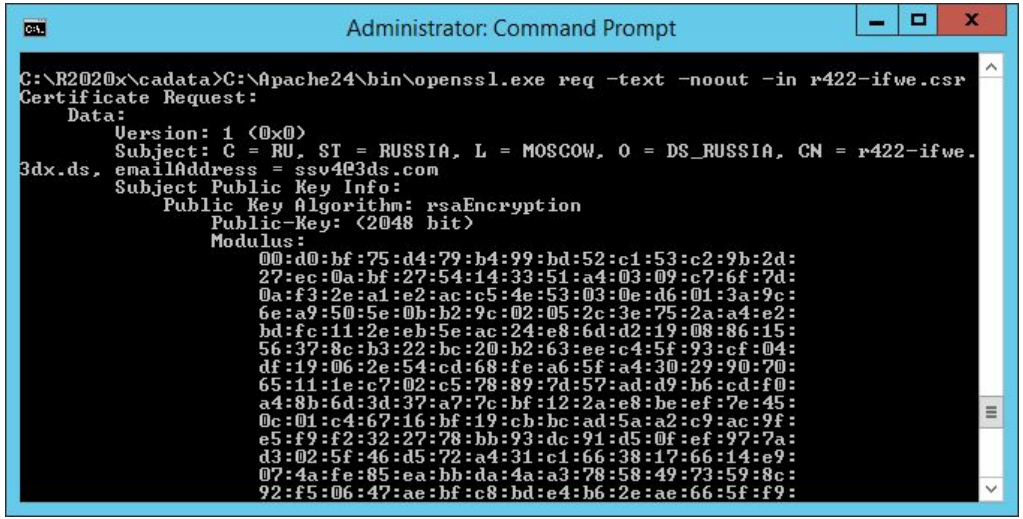
- Нажимайте ENTER для каждого вопроса, чтобы принять значения, заданные в файле настроек openssl-server.cnf:



SSL сертификаты

Проверка CA приватного ключа CA сертификата

- Проверьте запрос на подпись серверного сертификата (из командной строки с привилегиями администратора выполните следующую однострочную команду):
  - `C:\Apache24\bin\openssl.exe req -text -noout -in r422-ifwe.csr`



SSL сертификаты

Создание и подпись серверного сертификата

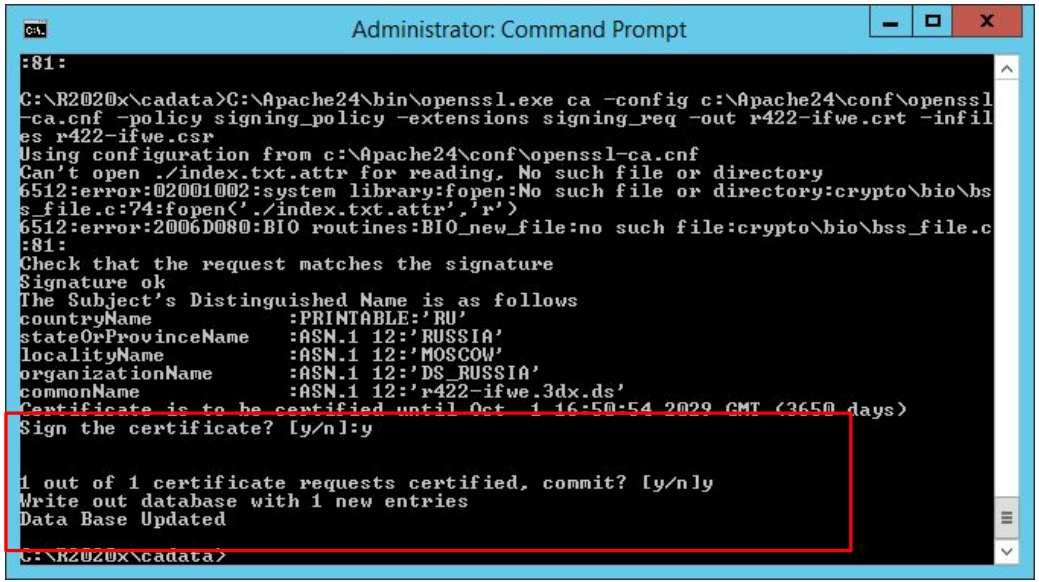
- Откройте командную строку с привилегиями администратора и перейдите в папку C:\R2020x\cadata:
  - `cd C:\R2020x\cadata`
- Создайте и подпишите серверный сертификат (это однострочная команда):
  - `C:\Apache24\bin\openssl.exe ca -config c:\Apache24\conf\openssl-ca.cnf -policy signing_policy -extensions signing_req -out r422-ifwe.crt -infiles r422-ifwe.csr`

В результате выполнения команды будет создан файл: подписанный серверный сертификат

SSL сертификаты

Создание и подпись серверного сертификата

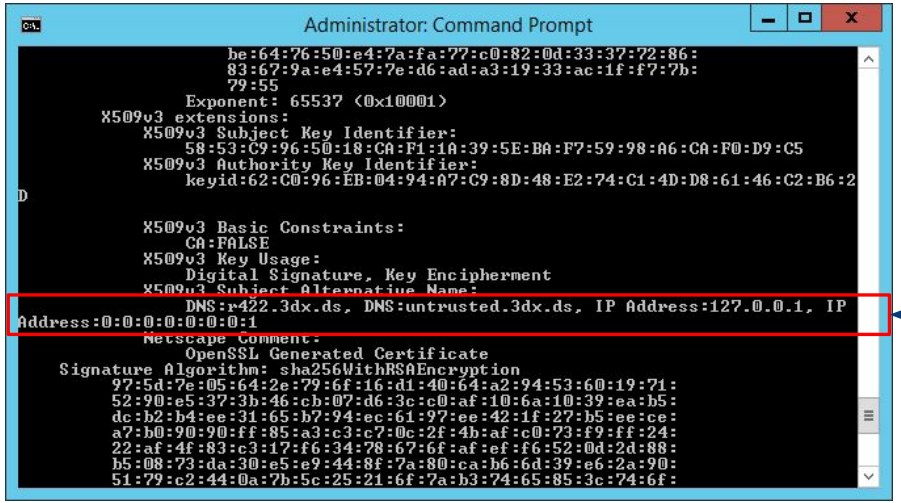
- Ответьте ”y” и нажмите ENTER для каждого вопроса:



SSL сертификаты

Проверка серверного сертификата

- Проверьте подписанный серверный сертификат (из командной строки с привилегиями администратора выполните следующую однострочную команду):
  - `C:\Apache24\bin\openssl.exe x509 -text -noout -in r422-ifwe.crt`

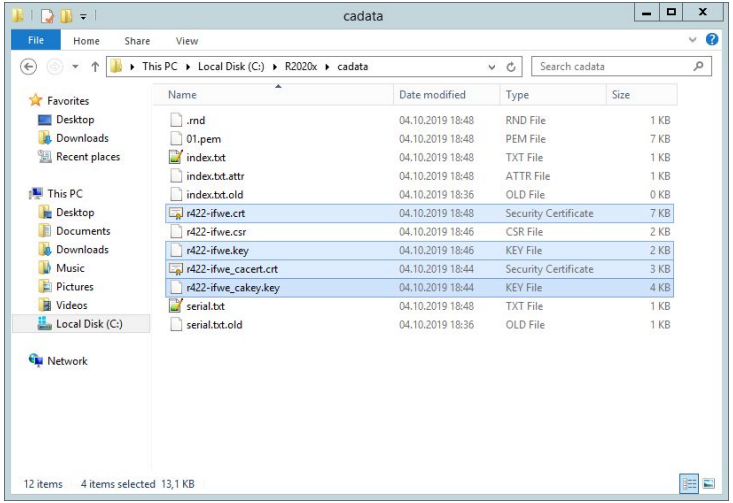


Проверьте, что параметр Subject Alternative Name задан корректно

SSL сертификаты

Результат

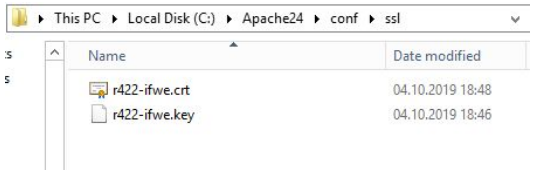
- После выполнения вышеизложенных действий, в папке C:\R2019x\cadata будут следующие важный для установки Платформы файлы:
  - r422-ifwe_cakey.key
    - CA приватный ключ
  - r422-ifwe_cacert.crt
    - CA сертификат, который необходим для подписи серверного сертификата
  - r422-ifwe.key
    - Серверный приватный ключ (хранить в безопасном месте!)
  - r422-ifwe.crt
    - Серверный сертификат, подписанный с помощью созданного нами CA



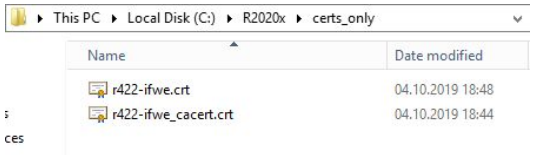
SSL сертификаты

Размещение серверного приватного ключа и сертификата

- Скопируйте файлы r422-ifwe.key и r422-ifwe.crt
  ИЗ `C:\R2020x\cadata`
  В `C:\Apache24\conf\ssl`



- Серверный сертификат также должен быть импортирован в виртуальную машину Java, которая используется для сервисов Платформы
- Мастер установки сервисов Платформы автоматически импортирует сертификаты:
  - Мастеру установки необходимо предоставить папку, в которой будут находиться только сертификаты (и ничего больше), поэтому необходимо создать папку:
    - `C:\R2020x\certs_only`
- Скопируйте файлы r422-ifwe.crt и r422-ifwe_cacert.crt
  ИЗ `C:\R2020x\cadata`
  В `C:\R2020x\certs_only`

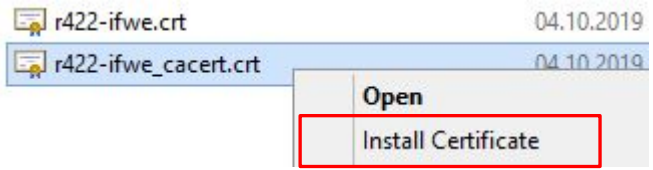


DASSAULT SYSTEMES

Установка CA сертификата на сервере платформы

Установка CA сертификата в ОС Windows

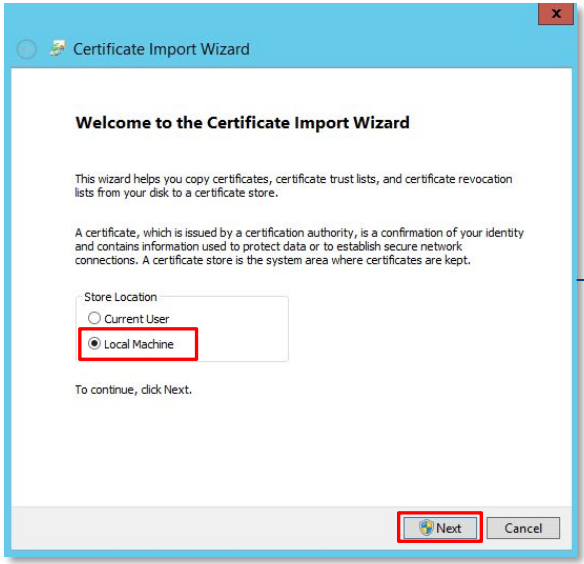
- Правый клик на файле ru2-ifwe_cacert.crt и в контекстном меню выберите Install Certificate

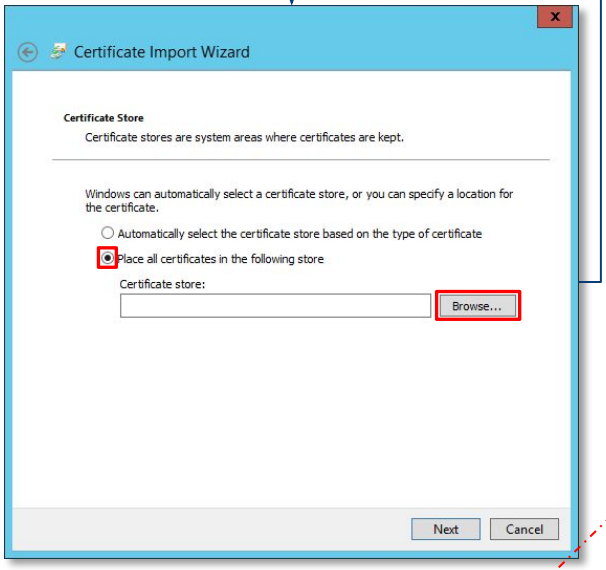


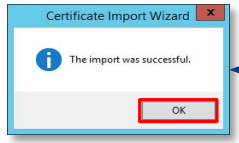
Данная процедура выполняется на сервере и всех клиентах, с которых вы хотите получить доступ к платформе

Установка CA сертификата на сервере платформы

Установка CA сертификата в ОС Windows







Данная процедура выполняется на сервере и всех клиентах, с которых вы хотите получить доступ к платформе

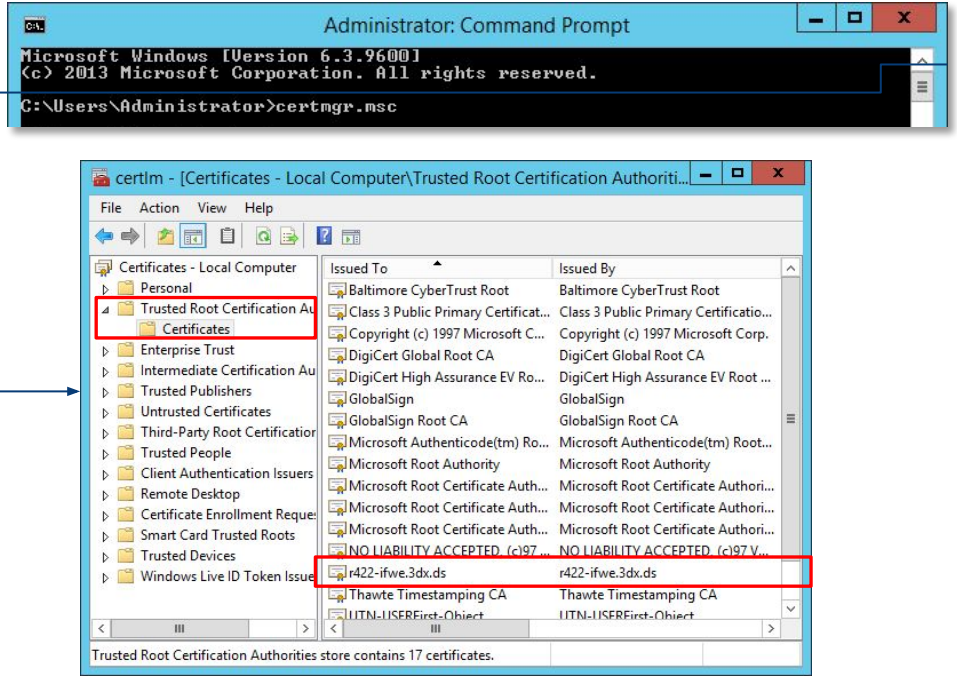
Выберите хранилище Trusted Root Certification Authorities

DASSAULT SYSTEMES

Установка CA сертификата на сервере платформы

Установка CA сертификата в ОС Windows

- Запустите “certmgr.msc” и убедитесь, что сертификат успешно импортирован



Данная процедура выполняется на сервере и всех клиентах, с которых вы хотите получить доступ к платформе

SSL сертификаты

Обновление конфигурации виртуального хоста Apache

- Откройте файл-шаблон `C:\Apache24\conf\vhosts\3dx.conf` в Notepad++
- Серверный сертификат и приватный ключ должны быть указаны следующим образом:

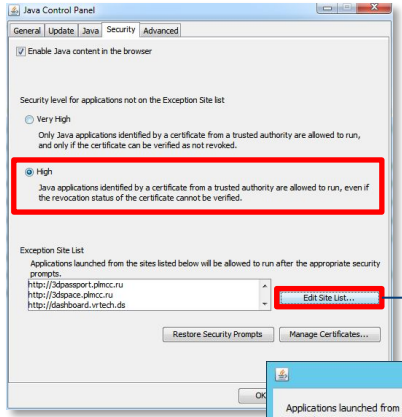
```
### SSL certificate and server private key
SSLCertificateFile    conf/ssl/r422-ifwe.crt
SSLCertificateKeyFile conf/ssl/r422-ifwe.key
```

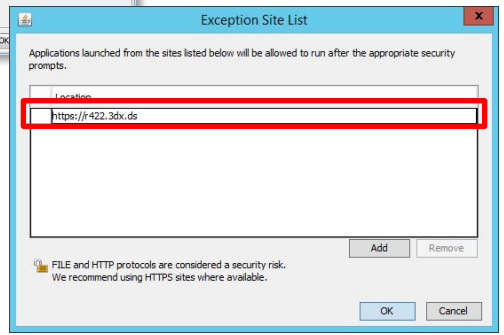
- Убедитесь, что сертификат и ключ прописаны правильно (при использовании параметров из презентации, значения в 3dx.conf заведомо правильные)
- Перезапустите службу Apache из командной строки с помощью команды:
  - `C:\Apache24\bin\httpd.exe -k restart`
  - Если все предыдущие действия были выполнены правильно, то служба успешно запустится
- Если служба Apache не запускается:
  - Диагностируйте проблему (в первую очередь проверьте файлы настроек Apache) и выполните запуск с помощью команды `C:\Apache24\bin\httpd.exe -k start`

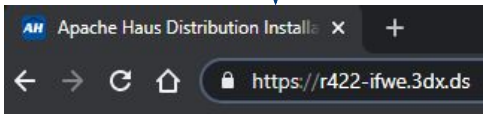
Настройка Java

Добавление URL доступа к Платформе в “Trusted Sites”

- В панели управления Windows найдите и запустите “Java Control Panel”
- Перейдите в закладку “Security”
  - Установите уровень безопасности “High”
  - Нажмите кнопку “Edit Site List…” и добавьте в список исключений URL сервера платформы: `https://r422-ifwe.3dx.ds`







Данная процедура выполняется на сервере и всех клиентах, с которых вы хотите получить доступ к платформе

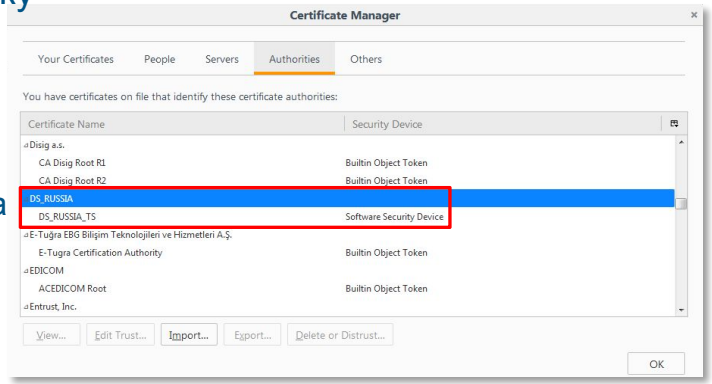
Если вы планируете использовать веб-браузер, в том числе Firefox, для доступа к Платформе непосредственно с сервера (виртуальной машины), то выполните аналогичные действия на сервере

DASSAULT SYSTEMES

Управление сертификатами certificates

Импорт CA сертификата в Firefox

- Браузер Firefox использует собственный менеджер сертификатов, поэтому в него тоже необходимо импортировать CA сертификат
- Запустите Firefox, откройте “Settings” и закладку “Advanced/Certificates”
- Нажмите на ”View Certificates” и перейдите в закладку ”Authorities”
- Нажмите ”Import…” и импортируйте файл CA сертификата (ru2-ifwe_cacert.crt)
  - Выберите ”Trust this CA to identify websites” как показано на картинке

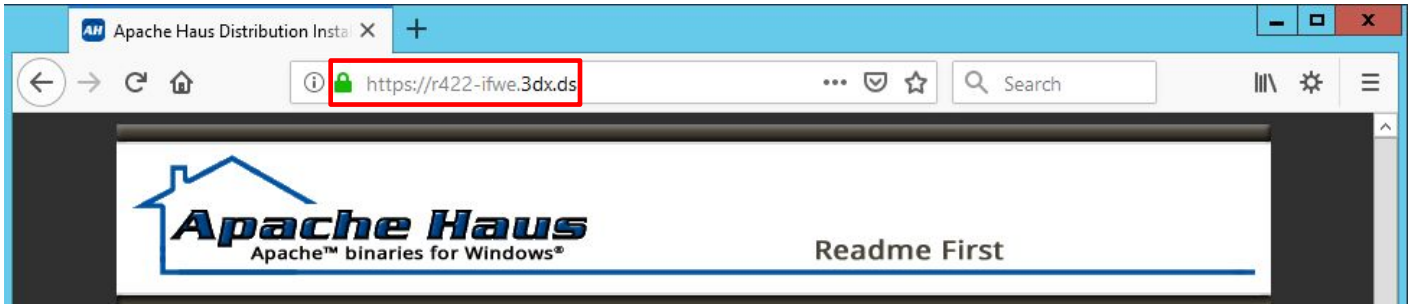


Данная процедура выполняется на сервере и всех клиентах, с которых вы хотите получить доступ к платформе

SSL сертификаты

Тестирование Apache с протоколом HTTPS

- На сервере, откройте браузер и перейдите по адресу https://r422-ifwe.3dx.ds
- Убедитесь, что стартовая страница Apache отображается без уведомлений для сертификатов (зеленый замок)



DASSAULT SYSTEMES