



3DEXPERIENCE®

3DEXPERIENCE Platform 2020x Installation guide

review v1 / 10.10.2019

Apache & SSL

Sergey SHEBARSHOV

Infrastructure Consultant

Sergey.SHEBARSHOV.intern@3ds.com

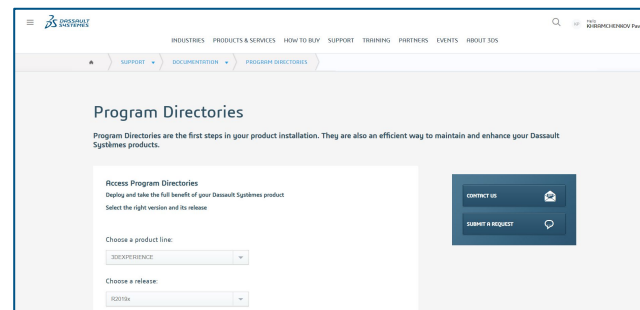
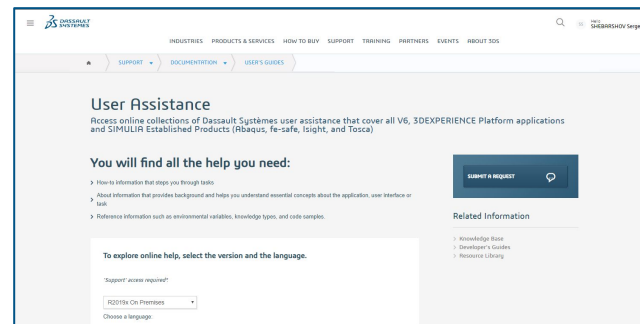


Общие положения

Допущения и ограничения

- ▶ Данный материал представляет собой описание процесса установки **3DEXPERIENCE Platform 2020x***
- ▶ Данный материал был подготовлен на основе следующих источников:
 - ▷ **User Assistance** – официальной документации по продуктам Dassault Systèmes (см. раздел **Installation and Setup | Install | 3DEXPERIENCE Platform** и др.)
<https://www.3ds.com/support/documentation/users-guides/>
 - ▷ **Program Directory** – содержит описание требований к Аппаратной и Программной части инфраструктуры **3DEXPERIENCE Platform**, список закрыты и закрытых исправлений, обзор новых функций продуктов и т.д.
<https://www.3ds.com/support/documentation/program-directories/>
 - ▷ **Best Practices** – официальные лучшие практики по установке и апгрейду **3DEXPERIENCE 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 **3DEXPERIENCE Platform**, развернутой у заказчика

▶ Процедура апгрейда **3DEXPERIENCE Platform** описана в данном документе. Коды 3ds для авторизации методов DS White Papers/Best Practices) подходов к обновлению Платформы на тестовой среде



Общие положения

Допущения и ограничения

- ▶ Апгрейд и установка компонентов **3DEXPERIENCE 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 **3DEXPERIENCE Platform**, рекомендуется выполнять все действия на виртуальной машине в среде гипервизора VMWare ESXi или Microsoft Hyper-V
- ▶ Апгрейд и установка всех компонентов **3DEXPERIENCE 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\System32\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:\ul> - 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" в конфигурационном файле Apache, который расположен по следующему пути
 - 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

Apache24/...

...bin/

httpd.exe - Основной бинарный исполняемый файл

...conf/

- Все файлы настроек находятся здесь и в подпапках

ssl/

- Все SSL-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

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

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>

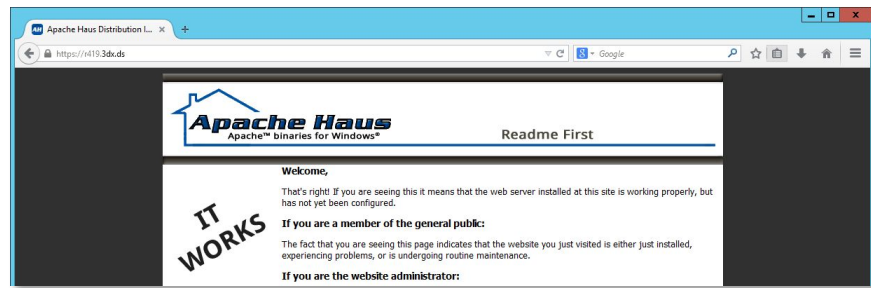
или, если 81 порт занят

- ▷ <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



Первичная настройка сервера Apache HTTPD

- Отредактируйте файл **httpd.conf** в папке C:\Apache24\conf

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

- 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
```

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:

<u>Сервис</u>	<u>порт TomEE</u>	<u>HTTPS</u>	<u>Конечная точка сервиса</u>
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"`

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
```

```
520 #           but a statically compiled-in mod_ssl.  
521 #  
522 <IfModule ssl_module>  
523 #Include conf/extra/httpd-ssl.conf  
524 #Include conf/extra/httpd-ahssl.conf  
525 SSLRandomSeed startup builtin  
526 SSLRandomSeed connect builtin  
527 </IfModule>  
528 <IfModule http2_module>  
529     ProtocolsHonorOrder On  
530     Protocols h2 h2c http/1.1  
531 </IfModule>  
532  
533 # Configuration file for the 3DEXPERIENCE platform  
534 Include conf/vhosts/3dx.conf
```

Normal text file

Конфигурирование виртуального хоста

Apache

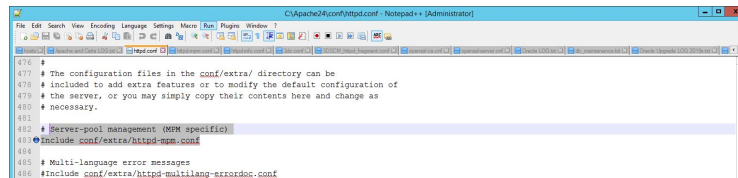
Изменение основного файла настроек Apache HTTPD

- ▶ Подключите файл настроек для Server-pool management (MPM specific) в
C:\Apache24\conf\vhosts\httpd.conf :

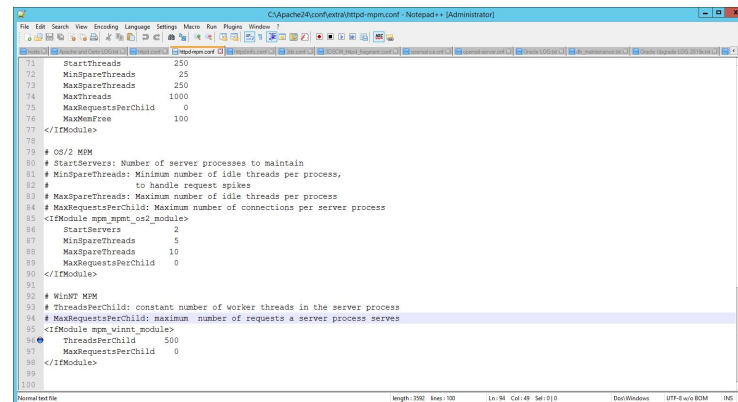
- ▷ Include conf/extra/httpd-mpm.conf

- ▶ В файле
C:\Apache24\conf\extra\httpd-mpm.conf
отредактируйте параметр ThreadsPerChild,
увеличив исходное значение:

- ▷ <IfModule mpm_winnt_module>
 - ▷ ThreadsPerChild 500
 - ▷ MaxRequestsPerChild 0
 - ▷ </IfModule>



```
476 #
477 # The configuration files in the conf/extra/ directory can be
478 # included to add extra features or to modify the default configuration of
479 # the server, or you may simply copy their contents here and change as
480 # necessary.
481
482 # Server-pool management (MPM specific)
483 Include conf/extra/httpd-mpm.conf
484
485 # Multi-language error messages
486 Include conf/extra/httpd-multilang-errordoc.conf
```

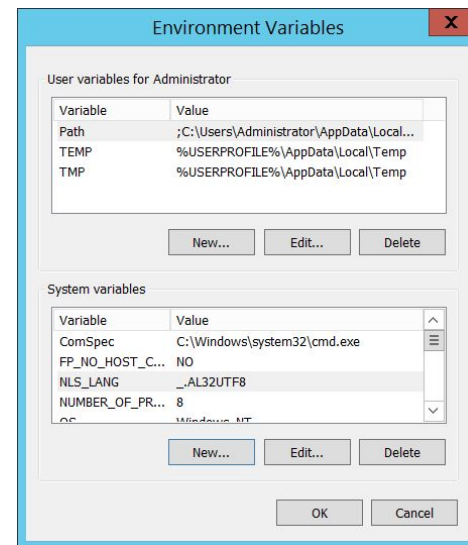
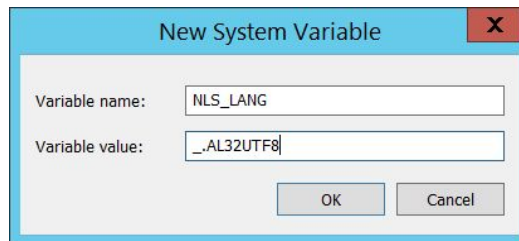


```
71 StartThreads 250
72 MinSpareThreads 25
73 MaxSpareThreads 250
74 MaxThreads 1000
75 MaxRequestsPerChild 0
76 MaxMemFree 100
77 </IfModule>
78
79 # OS/2 MPM
80 # StartServers: Number of server processes to maintain
81 # MinSpareThreads: Minimum number of idle threads per process,
82 # to handle request spikes
83 # MaxSpareThreads: Maximum number of idle threads per process
84 # MaxRequestsPerChild: Maximum number of connections per server process
85 <IfModule mpm_os2_module>
86 StartServers 2
87 MinSpareThreads 5
88 MaxSpareThreads 10
89 MaxRequestsPerChild 0
90 </IfModule>
91
92 # WinNT MPM
93 # ThreadsPerChild: constant number of worker threads in the server process
94 # MaxRequestsPerChild: maximum number of requests a server process serves
95 <IfModule mpm_winnt_module>
96 ThreadsPerChild 500
97 MaxRequestsPerChild 0
98 </IfModule>
99
100
```

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

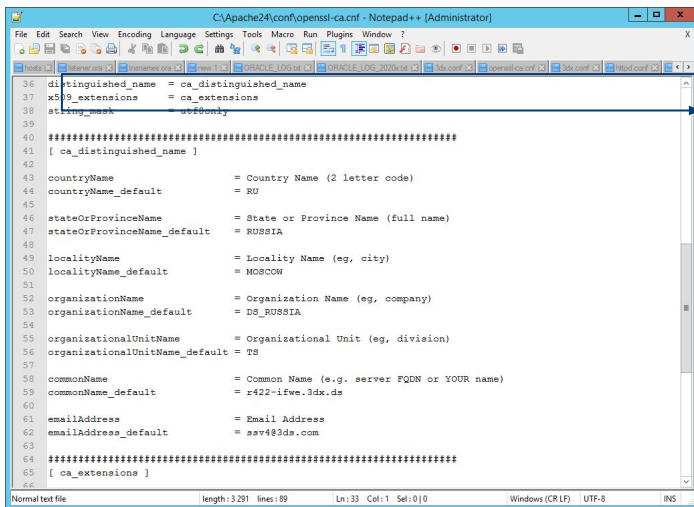
- ▶ В папке `C:\Apache24\conf` используем два файла-шаблона с настройками для создания сертификатов:
 - ▷ `openssl-ca.cnf`
 - ▷ `openssl-server.cnf`
- ▶ URL'ы для сертификатов сервера Платформы задаются в файле `openssl-server.cnf`:

```
[ 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

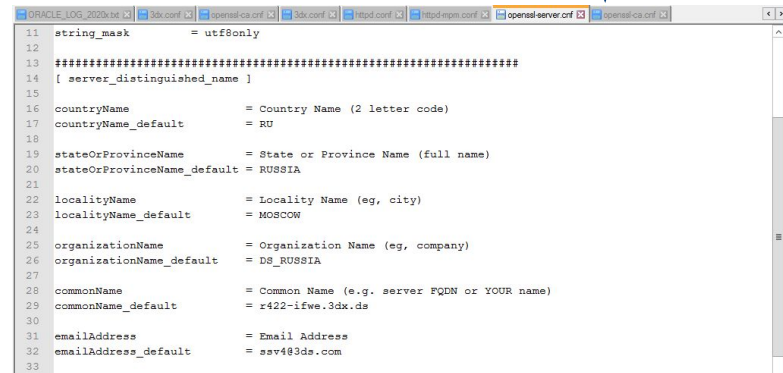
Подготовительные шаги

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



```
C:\Apache24\conf\openssl-ca.cnf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
36 distinguished_name = ca_distinguished_name
37 x509_extensions = ca_extensions
38 string_mask = utf8only
39
40 #####
41 [ ca_distinguished_name ]
42
43 countryName = Country Name (2 letter code)
44 countryName_default = RU
45
46 stateOrProvinceName = State or Province Name (full name)
47 stateOrProvinceName_default = RUSSIA
48
49 localityName = Locality Name (eg, city)
50 localityName_default = MOSCOW
51
52 organizationName = Organization Name (eg, company)
53 organizationName_default = DS_RUSSIA
54
55 organizationalUnitName = Organizational Unit (eg, division)
56 organizationalUnitName_default = TS
57
58 commonName = Common Name (e.g. server FQDN or YOUR name)
59 commonName_default = r422-ifwe.3dx.ds
60
61 emailAddress = Email Address
62 emailAddress_default = ssv4@3ds.com
63
64 #####
65 [ ca_extensions ]
66
```

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



```
C:\Apache24\conf\openssl-server.cnf - Notepad++ [Administrator]
11 string_mask = utf8only
12
13 #####
14 [ server_distinguished_name ]
15
16 countryName = Country Name (2 letter code)
17 countryName_default = RU
18
19 stateOrProvinceName = State or Province Name (full name)
20 stateOrProvinceName_default = RUSSIA
21
22 localityName = Locality Name (eg, city)
23 localityName_default = MOSCOW
24
25 organizationName = Organization Name (eg, company)
26 organizationName_default = DS_RUSSIA
27
28 commonName = Common Name (e.g. server FQDN or YOUR name)
29 commonName_default = r422-ifwe.3dx.ds
30
31 emailAddress = Email Address
32 emailAddress_default = ssv4@3ds.com
33
```

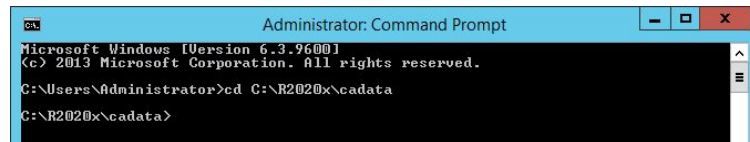
```
certificate = $base_dir/r422-ifwe_cacert.crt # The CA certificate
private_key = $base_dir/r422-ifwe_cakey.key # The CA private key
```

SSL сертификаты

CA сертификат и CA приватный ключ

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

Все команды OpenSSL должны выполняться в контексте этой папки



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd C:\R2020x\cadata
C:\R2020x\cadata>
```

- Создайте **CA сертификат** и **CA приватный ключ** с помощью этой (однотрочной) 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**

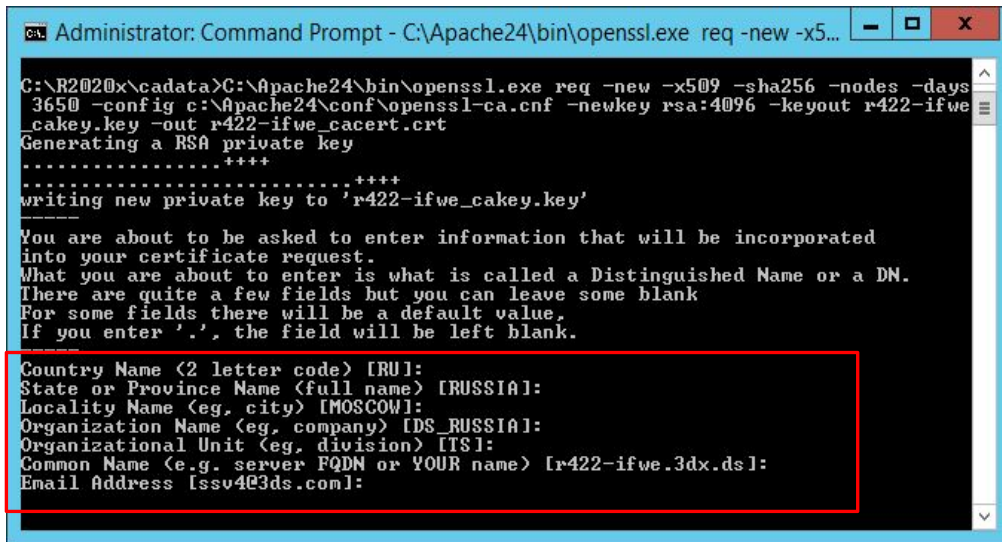


```
Administrator: Command Prompt - C:\Apache24\bin\openssl.exe req -new -x5...
C:\R2020x\cadata>C:\Apache24\bin\openssl.exe req -new -x509 -sha256 -nodes -days 3650 -config c:\Apache24\conf\openssl-ca.cnf -newkey rsa:4096 -keyout r422-ifwe_cakey.key -out r422-ifwe_cacert.crt
Generating a RSA private key
.....++++
writing new private key to 'r422-ifwe_cakey.key'
```

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:



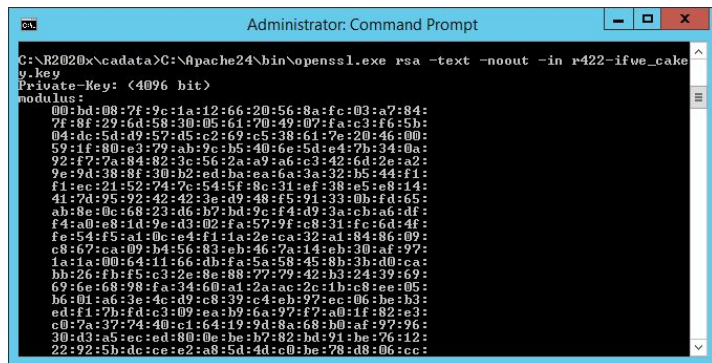
```
C:\R2020x\cadata>C:\Apache24\bin\openssl.exe req -new -x509 -sha256 -nodes -days 3650 -config c:\Apache24\conf\openssl-ca.cnf -newkey rsa:4096 -keyout r422-ifwe_cakey.key -out r422-ifwe_cacert.crt
Generating a RSA private key
.....++++
writing new private key to 'r422-ifwe_cakey.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [RU]:
State or Province Name (full name) [RUSSIA]:
Locality Name (eg, city) [MOSCOW]:
Organization Name (eg, company) [DS_RUSSIA]:
Organizational Unit (eg, division) [TS]:
Common Name (e.g. server FQDN or YOUR name) [r422-ifwe.3dx.ds]:
Email Address [ssu4@3ds.com]:
```

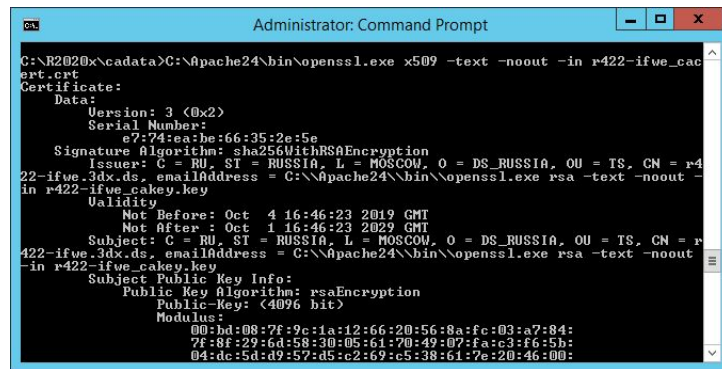
SSL сертификаты

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`



```
Administrator: Command Prompt
C:\R2020\cadata>C:\Apache24\bin\openssl.exe rsa -text -noout -in r422-ifwe_cakey.key
Private-Key: (4096 bit)
modulus:
00:bd:08:7f:9c:1a:12:66:20:56:8a:fc:03:a7:84:
7f:8f:29:6d:58:30:05:61:70:49:07:fa:c3:f6:5b:
04:de:5d:d9:57:d5:c2:69:c5:38:61:7e:20:46:00:
59:1f:80:e3:79:ab:9c:b5:40:6e:5d:ed:7b:34:0a:
92:f7:7a:84:82:3c:56:2a:a9:a6:c3:42:6d:2e:a2:
9e:9d:38:8f:30:b2:ed:ba:ea:6a:3a:32:b5:44:f1:
f1:ec:24:52:74:7c:54:5f:8c:31:ef:38:a5:e0:44:
41:7d:95:92:42:42:3e:d9:48:f5:91:33:0b:fd:65:
ab:8e:0c:68:23:d6:b7:bd:9c:f4:d9:3a:cb:a6:df:
f4:a0:e8:1d:9e:d3:02:fa:57:9f:c8:31:fc:6d:4f:
fe:54:f5:a1:0c:e4:f1:1a:2e:ca:32:a1:84:86:09:
c9:67:ca:09:b8:56:80:eb:46:7a:14:eb:30:af:97:
1a:1a:00:64:11:66:db:fa:5a:58:45:8b:3b:d0:ca:
bb:26:fb:f5:c3:2e:8e:88:77:79:42:h3:24:39:69:
69:6e:68:98:fa:34:60:a1:2a:ac:2c:1b:c8:ee:05:
b6:01:a6:3e:4c:d9:c8:39:c4:eb:77:ec:06:be:b3:
ed:f1:7b:fd:c3:09:ea:b6:a9:7f:77:ab:1f:82:c3:
e0:7a:37:74:40:c1:64:19:9d:8a:68:b0:af:97:96:
30:d3:a5:ec:ed:80:0e:be:b7:82:bd:91:be:76:12:
22:92:5b:dc:ce:e2:a8:5d:4d:c0:be:78:d8:06:cc:
```



```
Administrator: Command Prompt
C:\R2020\cadata>C:\Apache24\bin\openssl.exe x509 -text -noout -in r422-ifwe_cacert.crt
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
e7:74:aa:66:35:2e:5e
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = RU, ST = RUSSIA, L = MOSCOW, O = DS_RUSSIA, OU = TS, CN = r422-ifwe.3dx.ds, emailAddress = C:\Apache24\bin\openssl.exe rsa -text -noout -in r422-ifwe_cakey.key
Validity
Not Before: Oct 4 16:46:23 2019 GMT
Not After : Oct 1 16:46:23 2029 GMT
Subject: C = RU, ST = RUSSIA, L = MOSCOW, O = DS_RUSSIA, OU = TS, CN = r422-ifwe.3dx.ds, emailAddress = C:\Apache24\bin\openssl.exe rsa -text -noout -in r422-ifwe_cakey.key
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
00:bd:08:7f:9c:1a:12:66:20:56:8a:fc:03:a7:84:
7f:8f:29:6d:58:30:05:61:70:49:07:fa:c3:f6:5b:
04:de:5d:d9:57:d5:c2:69:c5:38:61:7e:20:46:00:
```


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`

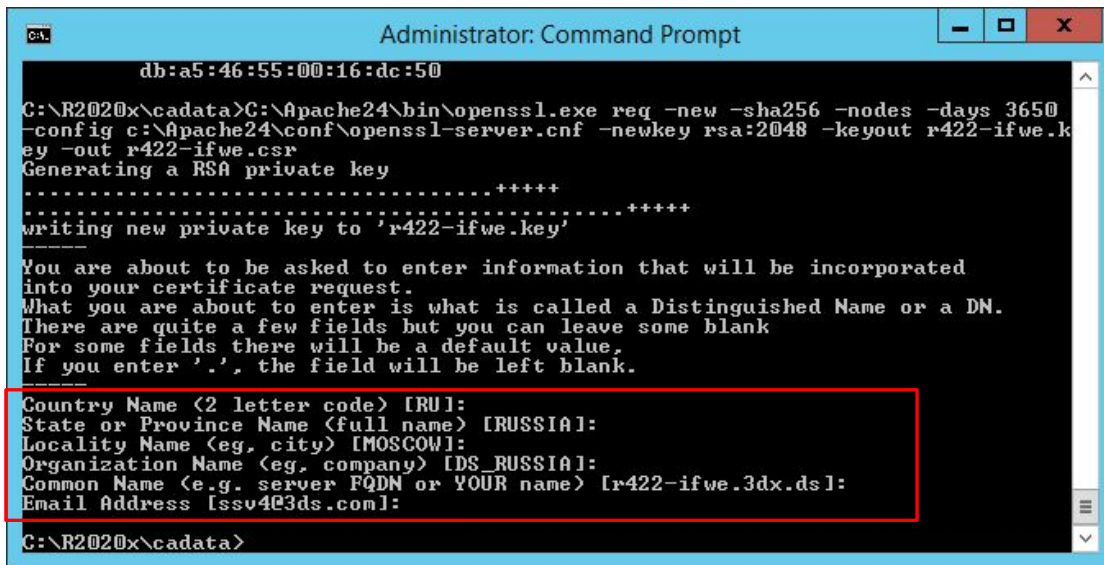
В результате выполнения команды
будут созданы следующие файлы:
запрос на подпись серверного
сертификата и приватный ключ

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**:



```
C:\> db:a5:46:55:00:16:dc:50

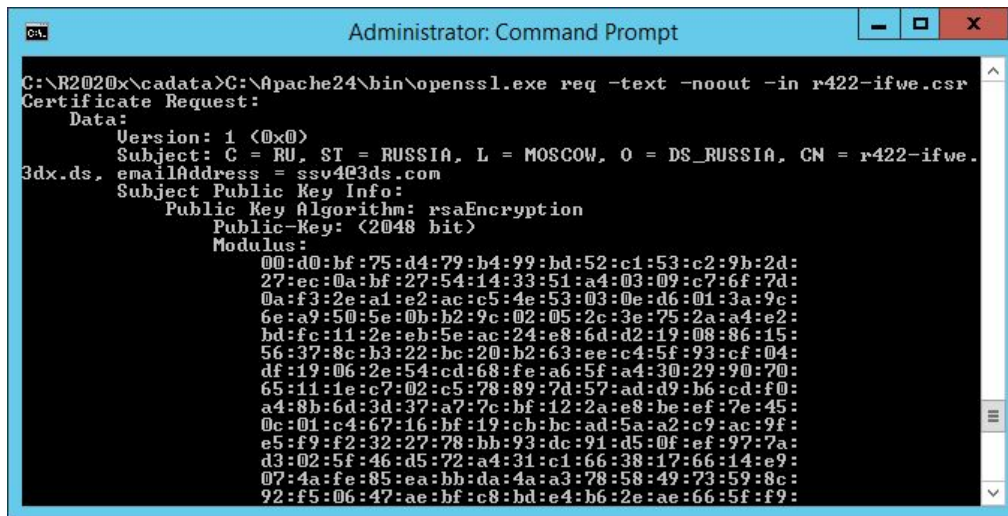
C:\R2020x\cadata>C:\Apache24\bin\openssl.exe req -new -sha256 -nodes -days 3650
-config c:\Apache24\conf\openssl-server.cnf -newkey rsa:2048 -keyout r422-ifwe.k
ey -out r422-ifwe.csr
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'r422-ifwe.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) [RUSSIA]:
Locality Name (eg, city) [MOSCOW]:
Organization Name (eg, company) [DS_RUSSIA]:
Common Name (e.g. server FQDN or YOUR name) [r422-ifwe.3dx.ds]:
Email Address [ssv4@3ds.com]:

C:\R2020x\cadata>
```

SSL сертификаты

Проверка СА приватного ключа СА 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`



```
C:\R2020x\cadata>C:\Apache24\bin\openssl.exe req -text -noout -in r422-ifwe.csr
Certificate Request:
  Data:
    Version: 1 (0x0)
    Subject: C = RU, ST = RUSSIA, L = MOSCOW, O = DS_RUSSIA, CN = r422-ifwe.
3dx.ds, emailAddress = ssv4@3ds.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:d0:bf:75:d4:79:b4:99:bd:52:c1:53:c2:9b:2d:
        27:ec:0a:bf:27:54:14:33:51:a4:03:09:c7:6f:7d:
        0a:f3:2e:a1:e2:ac:c5:4e:53:03:0e:d6:01:3a:9c:
        6e:a9:50:5e:0b:b2:9c:02:05:2c:3e:75:2a:a4:e2:
        bd:fc:11:2e:eb:5e:ac:24:e8:6d:d2:19:08:86:15:
        56:37:8c:b3:22:bc:20:b2:63:ee:c4:5f:93:cf:04:
        df:19:06:2e:54:cd:68:fe:a6:5f:a4:30:29:90:70:
        65:11:1e:c7:02:c5:78:89:7d:57:ad:d9:b6:cd:f0:
        a4:8b:6d:3d:37:a7:7c:bf:12:2a:e8:be:ef:7e:45:
        0c:01:c4:67:16:bf:19:cb:bc:ad:5a:a2:c9:ac:9f:
        e5:f9:f2:32:27:78:bb:93:dc:91:d5:0f:ef:97:7a:
        d3:02:5f:46:d5:72:a4:31:c1:66:38:17:66:14:e9:
        07:4a:fe:85:ea:bb:da:4a:a3:78:58:49:73:59:8c:
        92:f5:06:47:ae:bf:c8:bd:e4:b6:2e:ae:66:5f:f9:
```

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):

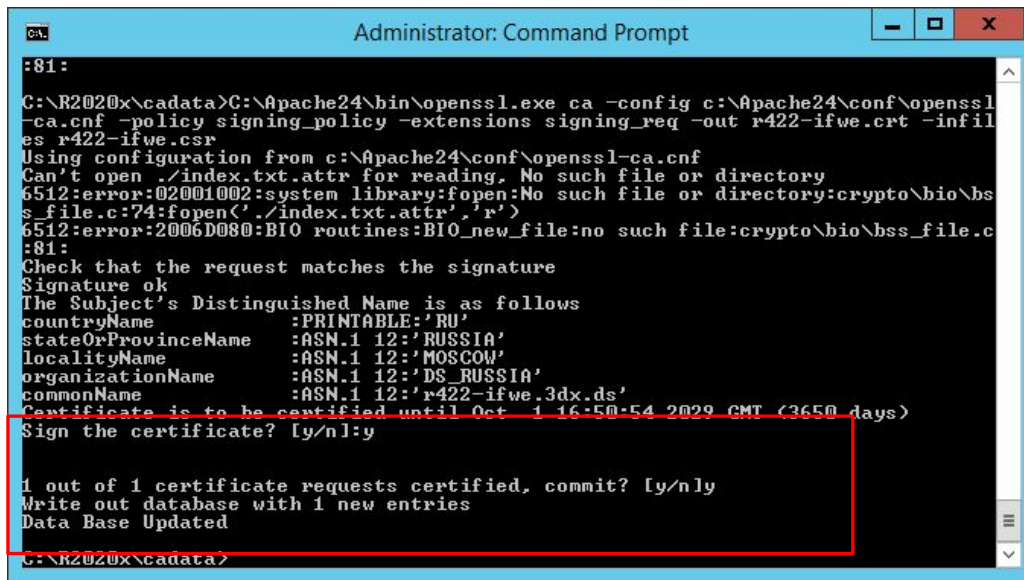
- ▷ `C:\Apache24\bin\openssl.exe ca -config c:\Apache24\conf\openssl-ca.cnf -policy signing_policy -extensions signing_req -out r422-ifwe.crt -infiles r422-ifwe.csr`

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:



```
Administrator: Command Prompt

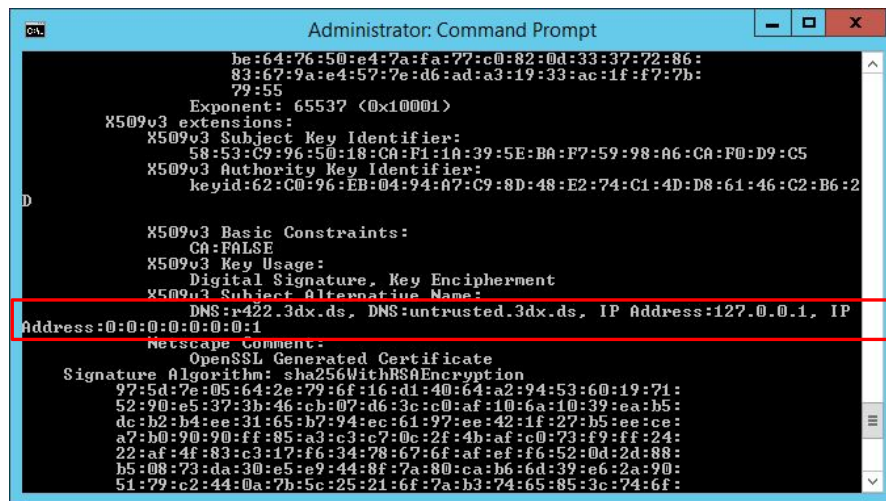
:81:
C:\R2020x\cadata>C:\Apache24\bin\openssl.exe ca -config c:\Apache24\conf\openssl
-ca.cnf -policy signing_policy -extensions signing_req -out r422-ifwe.crt -infil
es r422-ifwe.csr
Using configuration from c:\Apache24\conf\openssl-ca.cnf
Can't open ./index.txt.attr for reading, No such file or directory
6512:error:02001002:system library:fopen:No such file or directory:crypto\bio\bss
s_file.c:74:fopen('./index.txt.attr','r')
6512:error:2006D080:BIO routines:BIO_new_file:no such file:crypto\bio\bss_file.c
:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'RU'
stateOrProvinceName     :ASN.1 12:'RUSSIA'
localityName            :ASN.1 12:'MOSCOW'
organizationName        :ASN.1 12:'DS_RUSSIA'
commonName               :ASN.1 12:'r422-ifwe.3dx.ds'
Certificate is to be certified until Oct  1 16:50:54 2029 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
C:\R2020x\cadata>
```

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`



```
Administrator: Command Prompt

be:64:76:50:e4:7a:fa:77:c0:82:0d:33:37:72:86:
83:67:9a:e4:57:7e:d6:ad:a3:19:33:ac:1f:f7:7b:
79:55
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
 58:53:C9:96:50:18:CA:F1:1A:39:5E:BA:F7:59:98:A6:CA:F0:D9:C5
X509v3 Authority Key Identifier:
 keyid:62:C0:96:EB:04:94:A7:C9:8D:48:E2:74:C1:4D:D8:61:46:C2:B6:2
D

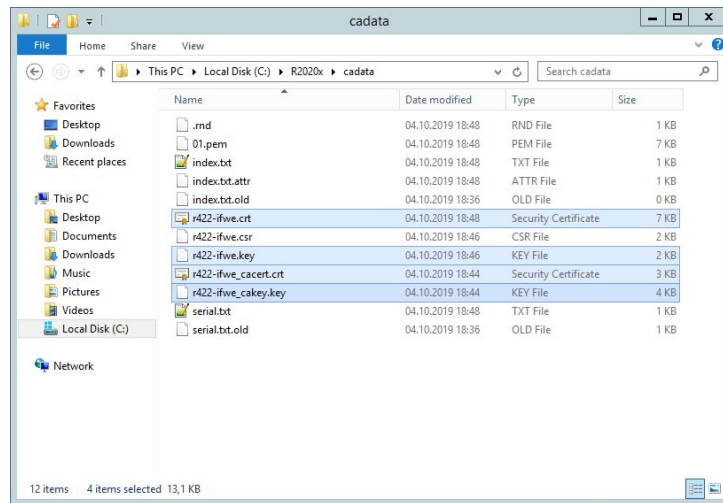
X509v3 Basic Constraints:
 CA:FALSE
X509v3 Key Usage:
 Digital Signature, Key Encipherment
X509v3 Subject Alternative Name:
 DNS:r422.3dx.ds, DNS:untrusted.3dx.ds, IP Address:127.0.0.1, IP
Address:0:0:0:0:0:0:0:1
Netscape Comment:
 OpenSSL Generated Certificate
Signature Algorithm: sha256WithRSAEncryption
97:5d:7e:05:64:2e:79:6f:16:d1:40:64:a2:94:53:60:19:71:
52:90:e5:37:3b:46:cb:07:d6:3c:c0:af:10:6a:10:39:ea:b5:
dc:b2:b4:ee:31:65:b7:94:ec:61:97:ee:42:1f:27:b5:ee:ce:
a7:b0:90:90:ff:85:a3:c3:c7:0c:2f:4b:af:c0:73:f9:ff:24:
22:af:4f:83:c3:17:f6:34:78:67:6f:af:ef:f6:52:0d:2d:88:
b5:08:73:da:30:e5:e9:44:8f:7a:80:ca:b6:6d:39:e6:2a:90:
51:79:c2:44:0a:7b:5c:25:21:6f:7a:b3:74:65:85:3c:74:6f:
```

Проверьте, что параметр **Subject**
Alternative Name задан корректно

SSL сертификаты

Результат

- После выполнения вышеизложенных действий, в папке **C:\R2019x\cadata** будут следующие важные 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



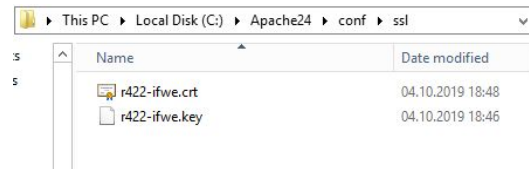
SSL сертификаты

Размещение серверного приватного ключа и сертификата

- ▶ Скопируйте файлы **r422-ifwe.key** и **r422-ifwe.crt**

из `C:\R2020x\cadata`

в `C:\Apache24\conf\ssl`

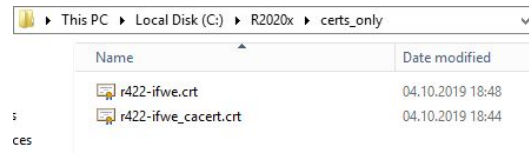


- ▶ Серверный сертификат также должен быть импортирован в виртуальную машину Java, которая используется для сервисов Платформы
- ▶ Мастер установки сервисов Платформы автоматически импортирует сертификаты:
 - ▷ Мастеру установки необходимо предоставить папку, в которой будут находиться только сертификаты (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`

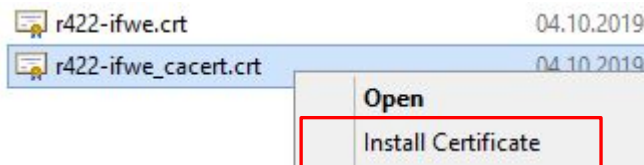
в `C:\R2020x\certs_only`



Установка СА сертификата на сервере платформы

Установка СА сертификата в ОС Windows

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

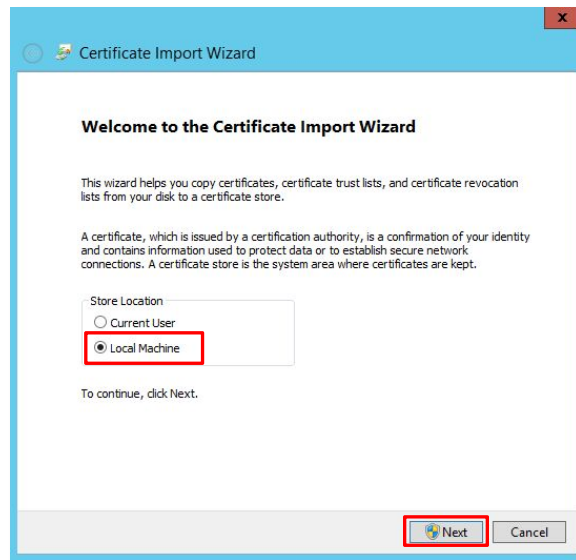


Данная процедура выполняется на сервере и всех клиентах, с которых вы хотите получить доступ к платформе

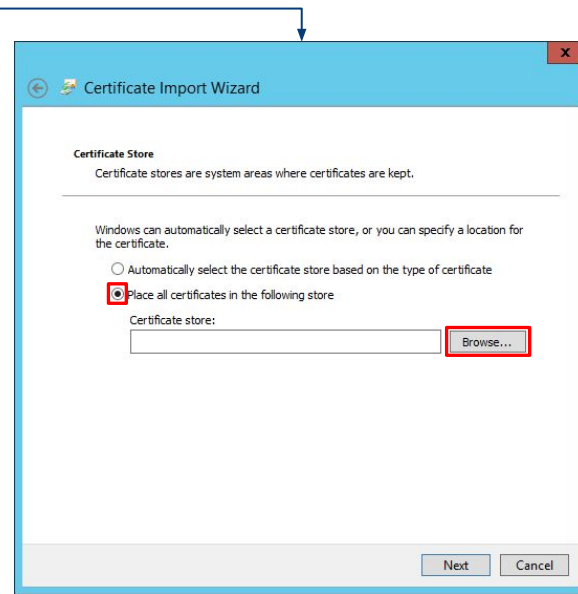
Установка СА сертификата на сервере

платформы

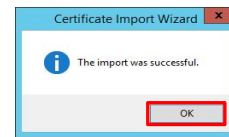
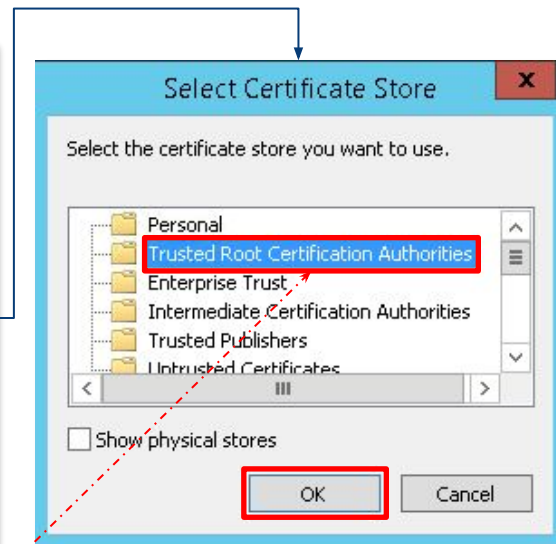
Установка СА сертификата в ОС Windows



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



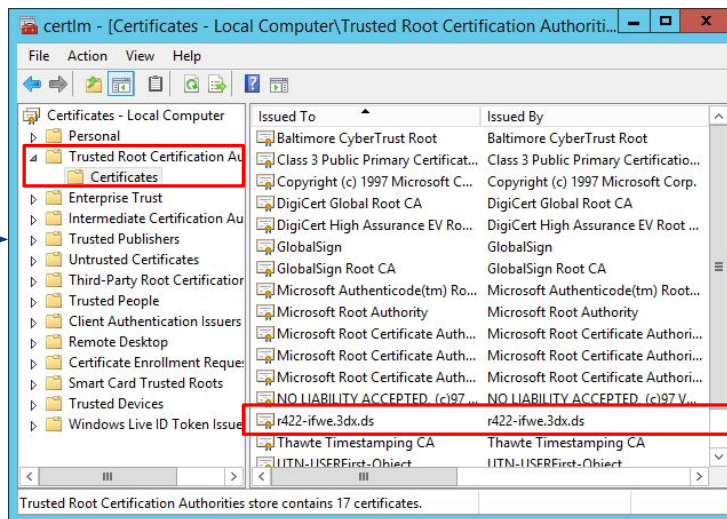
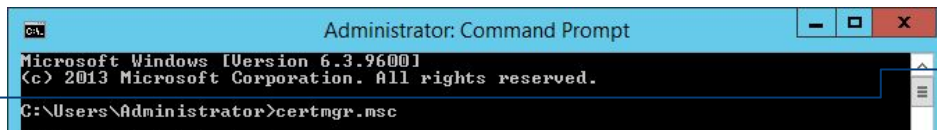
Выберите хранилище Trusted Root Certification Authorities



Установка СА сертификата на сервере платформы

Установка СА 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:

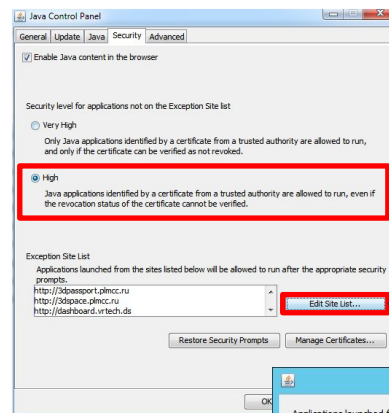
```
### SSL certificate and server private key
SSLCertificateFile      conf/ssl/r422-ifwe.crt
SSLCertificateKeyFile   conf/ssl/r422-ifwe.key
```
- ▶ Убедитесь, что сертификат и ключ прописаны правильно (при использовании параметров из презентации, значения в 3dx.conf заведомо правильные)
- ▶ Перезапустите 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

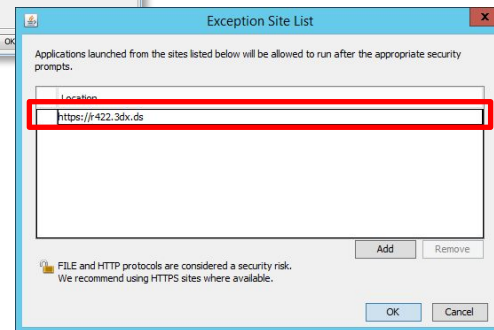
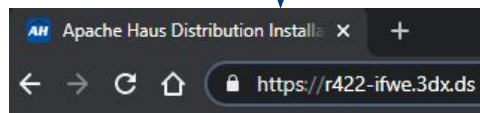
Добавление URL доступа к Платформе в “Trusted Sites”

- ▶ 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`

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



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

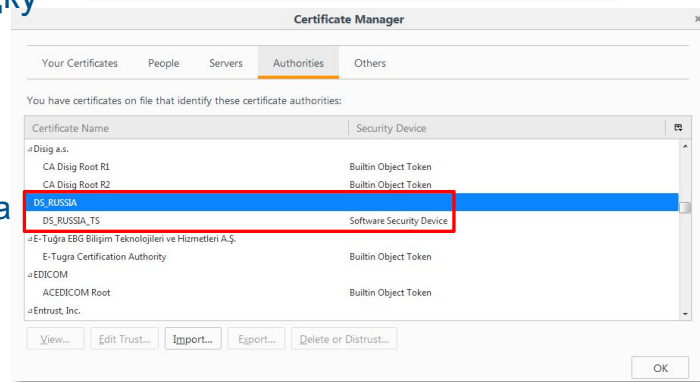
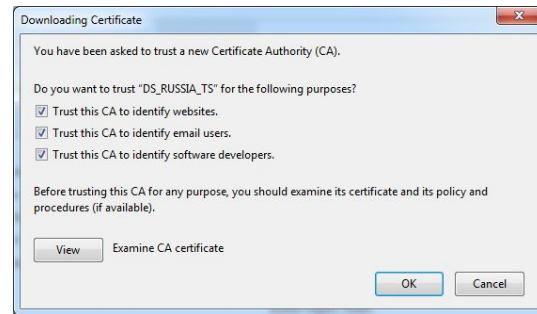


Управление сертификатами certificates

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)

